GE

Grid Solutions

Multilin™ G100

Substation Gateway

Product Documentation Set

994-0156

Version 2.30 R0

imagination at work

GE Information

Copyright Notice

© 2021, General Electric Company. All rights reserved.

The information contained in this online publication is the exclusive property of General Electric Company, except as otherwise indicated. You may view, copy and print documents and graphics incorporated in this online publication (the "Documents") subject to the following: (1) the Documents may be used solely for personal, informational, non-commercial purposes; (2) the Documents may not be modified or altered in any way; and (3) Gen- eral Electric Company withholds permission for making the Documents or any portion thereof accessible via the internet . Except as expressly provided herein, you may not use, copy, print, display, reproduce, publish, license, post, transmit or distribute the Documents in whole or in part without the prior written permission of General Electric Company.

The information contained in this online publication is proprietary and subject to change without notice. The software described in this online publication is supplied under license and may be used or copied only in accordance with the terms of such license.

Trademark Notices

GE, Multilin™ and are trademarks and service marks of General Electric Company.

* Trademarks of General Electric Company.

IEC is a registered trademark of Commission Electrotechnique Internationale. IEEE is a registered trademark of the Institute of Electrical and Electronics Engineers, Inc. Internet Explorer, Microsoft, and Windows are registered trademarks of Microsoft Corporation.

Other company or product names mentioned in this document may be trademarks or registered trademarks of their respective companies.

This printed manual is recyclable.

Please return for recycling where facilities exist.

Table of Contents

994-0155 G100 Substation Gateway Instruction Manual V100 R1 1
Copyright Notice 2
Trademark Notices 2
Figures 6
Tables 7
About this Document 8
Product Support 10
Chapter 1 - Introduction to G100 12
Chapter 2 - Unpacking and Inspection 20
Chapter 3 - Installing the G100 23
Chapter 4 - Interfaces and Indicators 32
Chapter 5 - Specifications 60
Chapter 6 - Removing the G100 from Service 64
Appendix A ... Standards & Compliance 65
Appendix B ... Warranty 67
Appendix C ... Glossary of terms used in this document 68
Modification Record 70

MIS-0115 G100 Firmware Release Notes V230 R1 71
COPYRIGHT NOTICE 72
TRADEMARK NOTICES 72
About this Document 75
1. Version 2.20 (19-May-2021) 77
2. Version 2.30 (29-July-2021) 86

SWM0101 MCP Software Configuration Guide V300 R1 98
Copyright Notice 99
Trademark Notices 99
Security Notice 99
Table of Contents 100
Figures 115
About this Document 117
Product Support 119
Chapter 1 - MCP Basics 120
Chapter 2 - Introducing MCP Features 180
Chapter 3 - MCP HMI Runtime 183
Chapter 4 - MCP Local Configuration Utility (mcpcfg) 252
Chapter 5 - MCP Settings GUI 348
Chapter 6 - DS Agile Studio Configuration 440
Chapter 7 - MCP Pseudo Points 794
Chapter 8 - EdgeManager and PETC 844
Appendix A ... Secure Terminal Emulator 846
Appendix B ... Secure File Browser 848
Appendix C - GenASCII Client - Time Sequence Diagrams and Sample Configuration for FEP Devices 849
Appendix D - Configuring a Linux-based Enterprise Server 855
Appendix E - Running Cron Jobs on the MCP 856
Appendix F ... Shell commands 858
Appendix G ... Security Certificates Creation for MCP 862
Appendix H ... List of Factory Default open ports (TCP and UDP) 871
Appendix I ... Modbus Protocol Support 872
Glossary 875

Modification Record 878

SWM0102 MCP Analog Reports User Guide V200 R1 879
Copyright Notice 880
Trademark Notices 880
Contents 881
About this Document 882
Product Support 884
1 Creating Template Using iReport Designer 885
2 Importing Templates 924
3 Offline Report Viewer 927
4 Online Report Viewer 929
5 Analog Report Generation - Configuration 932

SWM0103 Integration of MCP with OpenVPN Client V200 R2 939
COPYRIGHT NOTICE 940
TRADEMARK NOTICES 940
About this Document 945
Product Support 947
1. Overview 948
2. Setting up a Certification Authority 950
3. Server & Client Certificate Generation 954
4. Installing Certificates 961
5. Configuring VPN in MCP 971
6. Exporting VPN Client Configuration 977
7. Configuring OpenVPN Client 979
8. Revoking a Client certificate 983
9. Running OpenVPN Client as Windows Service using NSSM 985
A. Certificate Error Messages Logged by OpenVPN Configuration 992
B. OpenVPN Server Log Messages 996
C. VPN Client from Ubuntu PC 999
D. List of Acronyms 1000

SWM0104 Enterprise File Synchronization of MCP Sync Manager V200 R2 1002
COPYRIGHT NOTICE 1003
TRADEMARK NOTICES 1003
About this Document 1007
Product Support 1009
1. Overview 1010
2. Installation of copssh and cwRsyncServer 1011
3. Configuring MCP Sync Manager 1024
4. Setting up Public Key Authentication 1026
A. Uninstalling cwRsyncServer and Copssh 1028
B. Diagnostics 1029
C. List of Acronyms 1030

SWM0107 LogicLinx on a Multilin MCP Quick Start Guide V200 R1 1033
Prerequisites 1033
Differences between the 16-bit and the 32-bit versions of the LogicLinx editor 1033
To configure LogicLinx on your MCP gateway device: 1033

Owned and Mapped Points 1035
Internal Transition Counters 1035
Frequently Asked Questions 1035
Additional Documents 1036
Product Support 1036
Copyright Notice 1036
Trademark Notice 1037
Modification Record 1037

SWM0109 Secure Integration of SCADA Third Party Equipment with MCP V200 R2 1038
COPYRIGHT NOTICE 1039
TRADEMARK NOTICES 1039
About this Document 1046
Product Support 1048
1. Overview 1049
2. Setting up a Certification Authority 1051
3. Certificate Generation 1055
4. Installing Certificates 1060
5. Configuring Secure Connections on the MCP 1063
6. Configuring a Secure Connection with Tactical Software Serial IP 1068
7. Configuring a Secure Connection with Stunnel 1072
8. Revoking a client certificate 1075
A. Error Messages 1077
B. Connection Security 1078
C. List of Acronyms 1080

SWM0111 Configuring the MCP for Centralized LDAP Authentication using Windows AD V200 R0 1083
Product Support 1089
About this Document 1091
Chapter 1: Windows 2012 Active Directory 1093
Appendix A: Checking DN Format 1155
Appendix B: Third-party CA Certificate 1159
Appendix C: Troubleshooting 1173
Appendix D: List of Acronyms 1177
Appendix E: Revision History 1178

SWM0112 Configuring the MCP for Centralized LDAP Authentication using Open LDAP Server V200 R0. 1179
Configuring the MCP device for Centralized LDAP Authentication 1181
Product Support 1183
About this Document 1185
Chapter 1: Open LDAP Server 1186
Chapter 2: Configure the LDAP on MCP 1213
Appendix A: Troubleshooting 1241
Appendix B: List of Acronyms 1244
Appendix C: Revision History 1246

SWM0113 Configuring the MCP for Centralized LDAP Authentication using 389 Directory Server V200 R0. 1247
Product Support 1251
About this Document 1253
Chapter 1: 389 Directory Server 1254

Chapter 2: Configure the LDAP on MCP ... 1276
Appendix A: Troubleshooting ... 1304
Appendix B: List of Acronyms ... 1307
Appendix C: Revision History ... 1309

SWM0116 G100 Substation Gateway Quick Start Guide V100 R1 ... 1310
What's in the Box? ... 1310
Prerequisites ... 1312
G100 Interface Options ... 1312
Setup & Configuration Tools ... 1312
G100 Gateway Settings GUI ... 1313
G100 Snapshot Compatibility ... 1324
G100 Snapshot Management ... 1324
Default Users ... 1326
Getting Started ... 1326
G100 Runtime HMI ... 1349
List of factory default open ports ... TCP and UDP ... 1352
Additional Documentation ... 1353
Product Support ... 1353
Copyright Notice ... 1354
Modification Record ... 1354

SWM0122 Configuring UEFI Settings on G100 User Guide V100 R0 ... 1355
Introduction ... 1359
UEFI Overview ... 1361
UEFI Setup Information ... 1363
Appendices ... 1389

SWM0123 G100 Secure Deployment User Guide V100 R0 ... 1391
Introduction ... 1395
Initial Hardening Setup ... 1397
Secure Configuration of the G100 ... 1403
Removing Configuration and Sensitive Data ... 1409
Customer Support SSH Access ... 1411
Appendices ... 1413

TN0116 MCP Firmware Upgrade and Restore to Defaults Workflows V300 R2 ... 1417
Overview ... 1417
Prerequisites ... 1417
Section 1: Using DSAS "MCP Firmware Upgrade" tool to create the USB disk image ... 1418
Section 2: Use the external USB to upgrade the existing firmware and configuration ... 1430
Section 3: Use the external USB to re-image the MCP ... 1436
Section 4: Troubleshooting ... 1438
Product Support ... 1439
Copyright Notice ... 1439
Trademark Notice ... 1439
Modification Record ... 1440

TN0123 Installing Service Updates on MCP V100 R1 ... 1441

Overview 1441
Installing Service Updates 1441
Product Support 1450
Copyright Notice 1450
Trademark Notice 1450
Modification Record 1451

AN0015 MCP Snapshot and Configuration Workflows V200 R1 1452
Product Support 1483
Copyright Notice 1483
Modification Record 1484

MIS-0110 Open Source License Information V230 R0 1485
GNU General Public License | Version 1, Febrauary 1989 1486
GNU General Public License | Version 2, June 1991 1490
GNU General Public License | Version 3, 29 June 2007 1495
GNU Lesser General Public License | Version 2.1, Febrauary 1999 1503
GNU Library| Lesser General Public License 1505
Apache License | Version 2.0, January 2004 1510
OpenSSL License 1513
Net-SNMP License 1514
BSD License 1518
BSD License 2.0 | 3-Clause License | Revised BSD License 1523
Simplified BSD License | 2-Clause License | Free BSD License 1524
Generic License - CGIC 1524
Generic License - Zlib 1525
Generic License - Linux-PAM 1526
Copyright Notice 1527
Trademark Notice 1527
Modification Record 1527

NTEK-A022M-0CS DNP3 Server (DPA) for the Multifunction Controller Platform 1528
COPYRIGHT NOTICE 1529
TRADEMARK NOTICES 1529
1. DNP3 Server Application on MCP - Device Profile Document 1532

NTEK-A023M-0CS DNP3 Client (DCA) for the Multifunction Controller Platform 1543
COPYRIGHT NOTICE 1544
TRADEMARK NOTICES 1544
1. DNP3 Client Application on MCP - Device Profile Document 1547

NTEK-A024M-0CS IEC 60870-5-101-104 Server (DPA) for the Multifunction Controller Platform 1561
COPYRIGHT NOTICE 1562
TRADEMARK NOTICES 1562
1. IEC 60870-5-101 DPA Interoperability Profile 1564
2. IEC 60870-5-104 DPA Interoperability Profile 1576

NTEK-A025M-0CS IEC 60870-5-103 Client (DCA) for the Multifunction Controller Platform 1590

COPYRIGHT NOTICE 1591
TRADEMARK NOTICES 1591
1. Interoperability Tables 1594

NTEK-A027M-0CS IEC 61850 Client (DCA) for the MCP - Conformance Statement V200 R2 1604
COPYRIGHT NOTICE 1605
TRADEMARK NOTICES 1605
Contents 1606
1. Protocol Implementation Conformance Statement (PICS) 1608
2. Model Implementation Conformance Statement (MICS) 1615
3. Protocol Implementation eXtra Information for Testing (PIXIT) 1618
4. TISSUES Implementation Conformance Statement (TICS) 1628

NTEK-A031M-0CS IEC 60870-5-101_104 Client (DCA) for the Multifunction Controller Platform 1633
COPYRIGHT NOTICE 1634
TRADEMARK NOTICES 1634
1. IEC 60870-5-101 Client Interoperability Profile 1636
2. IEC 60870-5-104 Client Interoperability Profile 1646

PRBT-0429 MCP NERC CIP5 Response V300 R0 1659
Overview 1659
Frequently Asked Questions (MCP) 1674
Product Support 1677
Copyright Notice 1677
Trademark Notice 1678
Document Revision History 1678

GE
Grid Solutions

Multilin™ G100

Substation Gateway

Instruction Manual

994-0155
Version 1.00 Revision 1

IEC 61850

REGISTERED ISO 9001 GE MULTILIN

WORLDWIDE 10 YEAR WARRANTY

imagination at work

GE Information

Copyright Notice

©2021, General Electric Company. All rights reserved.

The information contained in this online publication is the exclusive property of General Electric Company, except as otherwise indicated. You may view, copy and print documents and graphics incorporated in this online publication (the "Documents") subject to the following: (1) the Documents may be used solely for personal, informational, non-commercial purposes; (2) the Documents may not be modified or altered in any way; and (3) General Electric Company withholds permission for making the Documents or any portion thereof accessible via the internet. Except as expressly provided herein, you may not use, copy, print, display, reproduce, publish, license, post, transmit or distribute the Documents in whole or in part without the prior written permission of General Electric Company.

The information contained in this online publication is proprietary and subject to change without notice. The software described in this online publication is supplied under license and may be used or copied only in accordance with the terms of such license.

Trademark Notices

GE, Multilin and are trademarks and service marks of General Electric Company.

* Trademarks of General Electric Company.

IEC is a registered trademark of Commission Electrotechnique Internationale. IEEE is a registered trademark of the Institute of Electrical and Electronics Engineers, Inc. Internet Explorer, Microsoft, and Windows are registered trademarks of Microsoft Corporation. DisplayPort™ are trademarks owned by the Video Electronics Standards Association (VESA®) in the United States and other countries. Intel® and Intel® Celeron® are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries.

Other company or product names mentioned in this document may be trademarks or registered trademarks of their respective companies.

This printed manual is recyclable.

Please return for recycling where facilities exist.

Table of Contents

Copyright Notice 2
Trademark Notices 2
Figures 6
Tables 7
About this Document 8
Purpose 8
Intended Audience 8
Additional documentation 8
How to use this document 8
Safety words and definitions 9
Product Support 10
Access the GE Grid Solutions web site 10
Search GE Grid Solutions Technical Support Library 10
Contact GE Grid Solutions technical support 10
GE Grid Solutions address 11
Product returns 11
Chapter 1 - Introduction to G100 12
Safety precautions 12
Warning symbols 13
Informational symbols 13
Hardware overview 14
Top Panel 15
Bottom Panel 16
Front Panel 17
Order Code 18
Spares and Accessories 19
Chapter 2 - Unpacking and Inspection 20
Electro Static Discharge - ESD 20
Initial inspection 21
Unpacking 22
Chapter 3 - Installing the G100 23
Installation 23
Wall / Panel Mounting instructions 23
DIN Rail Mounting instructions 26

Installation of optional D.20 HDLC Card 27
Grounding 30
Power Supply 30
Power-On Self-Test (POST) 31
Super Capacitor and Real Time Clock (RTC) 31
Chapter 4 - Interfaces and Indicators 33
UEFI Settings 33
General Purpose IO (GPIO) 33
Binary Inputs (DI): 8 33
Binary Outputs (DO): 4 35
Analog DC Inputs (AI): 4 37
D.20 Link Connections 40
G100 D.20 HDLC PCIe card 41
Supplying power through the D.20 Link 42
D.20 Peripheral Types 43
Peripheral compatibility with the D.20 HDLC PCIe card 43
D.20 Connection topologies 45
Serial ports (RS232/485, RJ45, labelled 1-4) 49
RS-485 Serial Connections 51
Default Serial Maintenance port (port 4, RS232) 52
Ethernet ports 53
TP Ethernet ports and LED indications (labelled 1, 2) 54
SFP Ethernet ports (labelled 3, 4) 54
Time synchronization IRIG-B input (2 pin connector) 56
DP Display Port 57
USB ports 59
Internal Buzzer 59
Chapter 5 - Specifications 61
G100 Product Specifications 61
System 61
Communications 61
Electrical 62
G100 Environmental Specifications 62
Temperature and Humidity 62

Ingress Protection (IEC 60529) 62
Mechanical Specifications 63
Weight 63
Dimensions 63
Storage recommendations 64
Storage conditions 64
Chapter 6 - Removing the G100 from Service 65
Remove configuration data and sensitive information from the G100 65
Removing configuration data on a PC 65
Appendix A – Standards & Compliance 66
Compliance Standards 66
Appendix B – Warranty 68
Warranty 68
Appendix C – Glossary of terms used in this document 69
Modification Record 71

Figures

Figure 1: G100 Top Panel....15
Figure 2: G100 Bottom Panel....16
Figure 3: G100 Front Panel....17
Figure 4: Single D.20 terminated, single link - Topology....45
Figure 5: Dual D.20 link terminated - Topology....46
Figure 6: Single D.20 link, redundant LAN - Topology....47
Figure 7: Redundant D.20 link, redundant LAN - Topology....48
Figure 8: Modular connector 8P8C (RJ45) pins....51
Figure 9: G100 connection using RS485 2-wire....52

Tables

Table 1: Warning symbols that may appear on the G100 and in this manual 13
Table 2: Informational symbols that appear on the G100 and in this manual 13
Table 3: G100 Order Code 18
Table 4: GPIO DI connector pin assignments 34
Table 5: GPIO DO connector pin assignments 36
Table 6: GPIO AI connector pin assignments 38
Table 7: GPIO AI Voltage / Current selection jumper 39
Table 8: D.20 Port A and B pin out and configuration options 41
Table 9: Default D.20 Relay settings 42
Table 10: D20A Analog Input Module Compatibility 43
Table 11: D20S Status Input Module Compatibility 44
Table 12: D20K Control Output Module Compatibility 44
Table 13: D20C Combination Input/Output Module Compatibility 45
Table 14: Repeater/Splitter Compatibility 45
Table 15: Single D.20 terminated, Single Link - Default settings 46
Table 16: Dual D.20 link terminated – Default settings 47
Table 17: Single D.20 link, redundant LAN - Default settings 48
Table 18: Redundant D.20 link, redundant LAN - Default settings 49
Table 19: RJ45 Pin outs for Serial Port Signals 50
Table 20: SFP modules supported by the G100 55
Table 21: Ethernet cables required by the G100 56
Table 22: IRIG-B input connector pin assignments 56
Table 23: IRIG-B input signal selection TTL/RS-232 57

About this Document

Purpose

This manual provides information about installing, setting up, using and maintaining your G100 Substation Gateway. This manual does not provide any procedures for configuring the G100 software

Intended Audience

This manual is intended for use by field technicians and maintenance personnel who are responsible for the installation, wiring and maintenance of SCADA equipment. This guide assumes that the user is experienced in:

- Electrical utility applications
- Electrical wiring and safety procedures
- Related other manufacturers' products, such as protective relays and communications equipment

Additional documentation

For further information about the G100, refer to the following documents.

- G100 Substation Gateway Quick Start Guide (SWM0116)
- MCP Software Configuration Guide (SWM0101)
- Configuring UEFI Settings on G100 User Guide (SWM0122)
- Module layouts, as available
- G100 Online Help

How to use this document

This document describes how to install the G100.

Procedures are provided for all component options available for the G100. The components included in your G100 depend on what was ordered for your substation application. Follow only the procedures that apply to your G100 model.

To check what options are included in your G100, see *Order Code*.

Safety words and definitions

Before attempting to install or use the device, review all safety indicators in this document to help prevent injury, equipment damage or downtime.

The following safety and equipment symbols are used in this document:

DANGER	**Indicates a hazardous situation which, if not avoided, will result in death or serious injury.**
WARNING	**Indicates a hazardous situation which, if not avoided, could result in death or serious injury.**
CAUTION	**Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.**
NOTICE	**Indicates practices that are not related to personal injury.**
NOTE	**Important information about the product, product handling which must be given attention.**

Product Support

If you need help with any aspect of your G100 product, you can:

- Access the G100 Web site
- Search the GE Technical Support library
- Contact Technical Support

Also covered are:

- The GE Grid Solutions address
- Instructions on returning a G100

Access the GE Grid Solutions web site

The G100 Web site provides fast access to technical information, such as manuals, release notes and knowledge base topics.

Visit us on the Web at: http://www.gegridsolutions.com

Search GE Grid Solutions Technical Support Library

This site serves as a document repository for post-sales requests. To get access to the Technical Support Web site, go to:

Visit us on the Web at: http://sc.ge.com/*SASTechSupport

Contact GE Grid Solutions technical support

GE Grid Solutions Technical Support is open 24 hours a day, seven days a week for you to talk directly to a GE representative.

In the U.S. and Canada, call toll-free: 1 800-547-8629

International customers, please call: + 1 905-927-7070

Or e-mail to G100 Local region contact support:

- ga.supportNAM@ge.com - North America
- ga.supportLAM@ge.com - Latin America
- ga.supportCEAP@ge.com - China, East Asia, Pacific
- ga.supportERCIS@ge.com - Europe, Russia, Commonwealth of Independent States
- ga.supportIND@ge.com - India

- ga.supportMENAT@ge.com - Middle East, North Africa, Turkey

Have the following information ready to give to Technical Support:

- Ship to address (the address that the product is to be returned to)
- Bill to address (the address that the invoice is to be sent to)
- Contact name
- Contact phone number
- Contact fax number
- Contact e-mail address
- Product number / serial number
- Description of problem

Technical Support will provide you with a case number for your reference.

GE Grid Solutions address

The GE Grid Solutions company address is:

GE Grid Solutions

650 Markland Street

Markham, Ontario

Canada L6C 0M1

Product returns

A Return Merchandise Authorization (RMA) number must accompany all equipment being returned for repair, servicing, or for any other reason. Before you return a product, please contact GE's Grid Solutions to obtain an RMA number and instructions for return shipments.

You are sent the RMA number and RMA documents via fax or e-mail. Once you receive the RMA documents, attach them to the outside of the shipping package and ship to GE.

Product returns are not accepted unless accompanied by the Return Merchandise Authorization number.

Chapter 1 - Introduction to G100

Before you begin installing and using the G100, review the information in this chapter, including the following topics:

- Safety precautions
- Warning symbols
- Informational symbols
- Hardware overview
- Order Code
- Spares and Accessories

Read and thoroughly understand this guide before installing and operating the unit. Save these instructions for later use and reference.

Failure to observe the instructions in this manual may result in serious injury or death.

Safety precautions

Follow all safety precautions and instructions in this manual.

Only qualified personnel should install and work on the G100. Maintenance personnel should be familiar with the technology and the hazards associated with electrical equipment.

- *Never* work alone.
- Class 1 Equipment. This equipment must be earthed. The power plug must be connected to a properly wired earth ground socket outlet. An improperly wired socket outlet could place hazardous voltages on accessible metal parts.
- This product contains components rated as Class 1 Laser Products.
- A ground wire (18AWG) is required to be connected from the G100 chassis to protective earth.
- This product is intended to be supplied by a UL listed DC power supply or DC power source which is rated for 12/24/48Vdc, 5/2.5/1.25A minimum, Tma = 70 degree C, and the altitude of operation = 5000m.
- The device can only be used in a fixed location. Ensure that the protective earth connection is verified by qualified personnel.
- Before performing visual inspections, tests, or maintenance on this equipment, isolate or disconnect all hazardous live circuits and sources of electric power. Assume that all circuits are live until they have been completely de-energized, tested, and tagged. Pay particular attention to the design of the power system. Consider all sources of power, including the possibility of back feed.
- Turn off all power supplying the equipment in which the G100 is to be installed before installing and wiring the G100.
- Operate only from the power source specified on the installed power supply module.
- Beware of potential hazards and wear appropriate personal protective equipment, safety shoes, eye protection and gloves.
- The successful operation of this equipment depends upon proper handling, installation, and operation. Neglecting fundamental installation requirements may lead to personal injury as well as damage to electrical equipment or other property.
- All electronic components within the G100 are susceptible to damage from electrostatic discharge. To prevent damage when handling this product use approved static control procedures.
- Hazardous voltages can cause shock, burns or death. To prevent exposure to hazardous voltages, disconnect and lock out all power sources before servicing and removing components.

- If the G100 is used in a manner not specified in this manual, the protection provided by the equipment may be impaired.
- Changes or modifications made to the unit not authorized by GE could void the warranty.

Warning symbols

Table 1 explains the meaning of warning symbols that may appear on the G100 or in this manual.

Table 1: Warning symbols that may appear on the G100 and in this manual

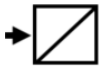
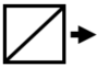
Symbol	Description
	The relevant circuit is direct current.
	The relevant circuit is alternating current.
	Caution: Refer to the documentation for important operation and maintenance instructions. Failure to take or avoid specified actions could result in loss of data or physical damage.
	Warning: Dangerous voltage constituting risk of electric shock is present within the unit. Failure to take or avoid specified actions could result in physical harm to the user.
	Protective Ground Terminal
	Caution: Hot Surface

Informational symbols

Table 1 explains the meaning of informational symbols that may appear on the G100 or in this manual.

Table 2: Informational symbols that appear on the G100 and in this manual

Symbol	Description
	Power On
	CPU Status

	Ethernet Port
	Serial Port
	IRIG-B Time In
	Display Port
	Analog DC Input (AI)
	Binary Input (DI)
	Binary Output (DO)

Hardware overview

MCP is the Multifunction Controller Platform family of Substation Gateways by GE Grid Solutions.

G100 is the smaller member of the family, together with G500.

G100 is based on Intel® Apollo Lake SOC, with Intel Atom X5-E3930 1.3GHz Processor to provide quality performance with low power consumption and wide operating temperature. It has 8 Gigabytes of SoDIMM 204 pin DDR3L memory.

The G100 is distinguished by the noticeable lack of a hard drive and fan, employing instead the rugged and reliable Solid State Drive (SSD) mass storage and engineered heat sink.

The G100 supports various communication media types through a choice of input/output (I/0):

- Serial: 4 factory installed ports, RS-232 and RS-485 configurable, accessible via individual RJ45 connectors.
- Ethernet: 2 factory installed RJ45 Ethernet interfaces with to 2 additional SFP cages..
- D.20 Link HDLC ports: A dual channel PCIe card for communication with up to 60 – D.20 Peripherals channel, including redundant D.20 link configuration.
- IRIG-B TTL input
- Local General Purpose IO (GPIO) interface, providing:

- 8 Binary Inputs (DI), wetted internally from main unit power supply circuit using single common (positive voltage through external contacts). The binary inputs are individually isolated internally.
- 4 Binary Outputs (DO), isolated, as N.O. (Normal Open) single contact
- 4 DC Analog Input (AI) channels, +5V DC/ 20mA

The G100 device has 3 noticeable side panels for operation.

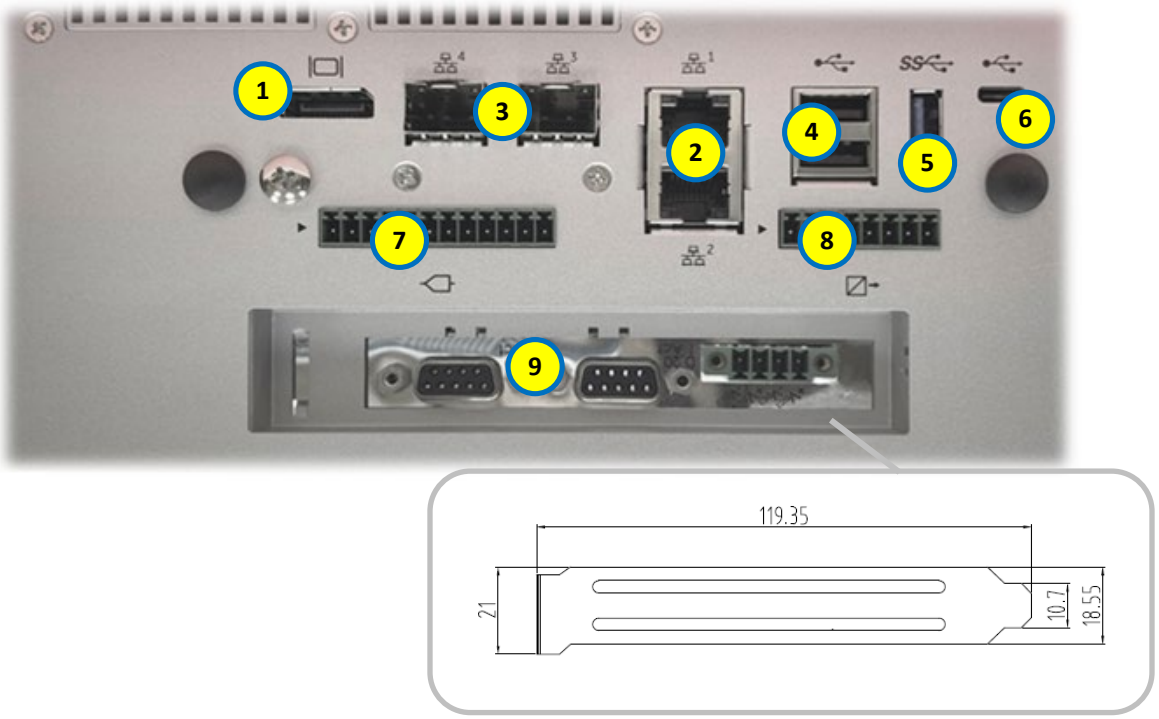
NOTE **The names of each side panel as referenced in this document assume a G100 being positioned vertically.**

Top Panel

The top panel of the G100 provides access to:

1. 1x DP display port
2. 2x TP Ethernet ports with LED indications (labelled 1, 2)
3. 2x SFP Ethernet ports (labelled 3, 4)
4. 2x USB2 ports
5. 1x USB3 port
6. 1x USB-C port (future, currently not used)
7. 4x Analog Input (AI) connections (12 pin connector)
8. 4x Binary Output (DO) connections (8 pin connector)
9. D.20 HDLC connections, with LED indications (optional, in PCIe slot)

Figure 1: G100 Top Panel

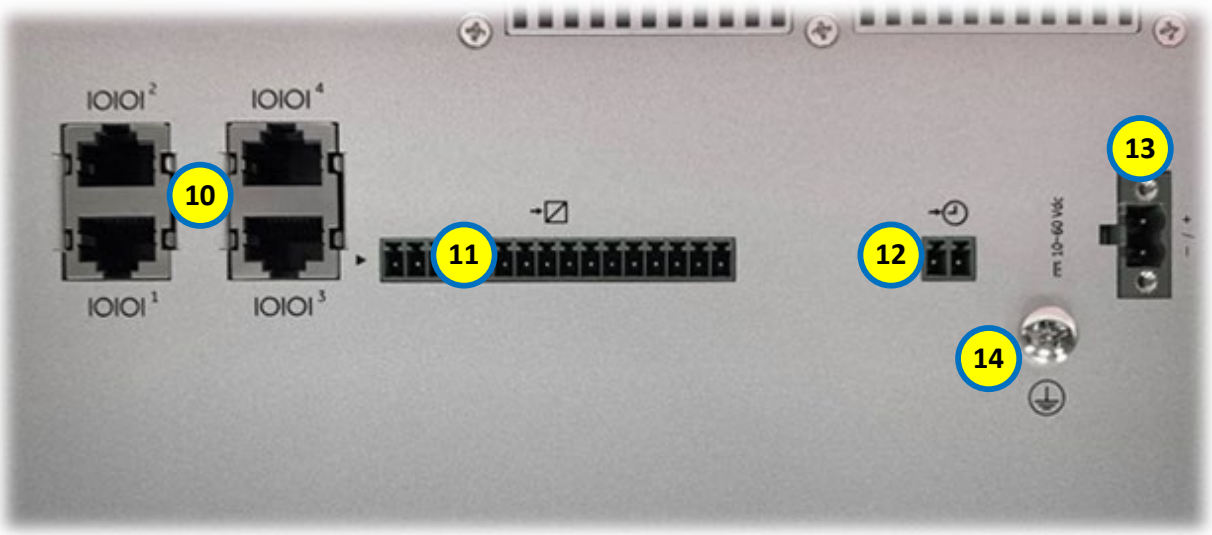


Bottom Panel

The bottom panel of the G100 provides access to:

10. 4x Serial ports (RS232/485, RJ45, labelled 1-4)
11. 8x Binary Input (DI) connections (16 pin connector)
12. Time synchronization input with IRIG-B TTL input (2 pin connector)
13. Power Supply connection (2 pin connector)
14. Protective Earth (PE) Ground connection (screw)

Figure 2: G100 Bottom Panel

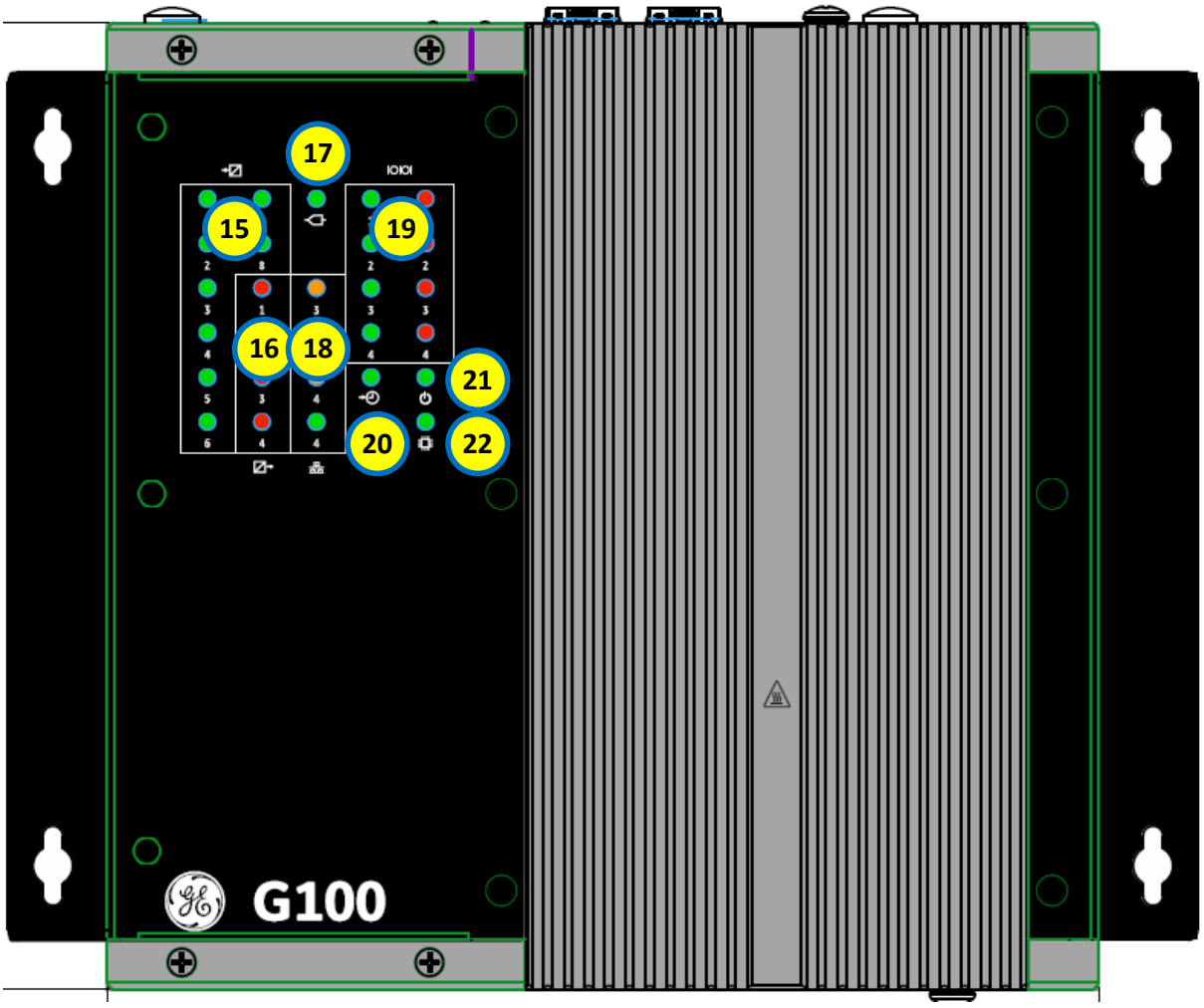


Front Panel

The front panel of the G100 provides the following LED indications:

15. 8x LED for Binary Input (DI)
16. 4x LED for Binary Output (DO)
17. LED for Analog Input (AI) sampling indication
18. SFP Ethernet (3, 4) link status LED
19. 4x Serial ports status LED
20. IRIG-B Input status LED
21. Power On LED
22. CPU/HW status LED, is ON when the unit operates normally

Figure 3: G100 Front Panel



Order Code

Table 3: G100 Order Code

		Hardware configuration														-	Software configuration				
Order Code Item	**G100 -**	**A**	**A**	**L**	**-**	**D**	**A**	**-**	**4**	**T**	**T**	*****	*****	**-**	*****	**U**	**U**	**-**	******	*******	**- UU**	**Description**
CPU and Memory		A																				1.3GHz 2-core CPU, 8GB RAM
Storage			A																			16GB Solid State Drive
Power Supply				L																		12–54VDC (10.8-59.4 absolute min/max)
Digital Input / Output						D																8x DI 12/24/48Vdc, 5mA & 4x DO 60Vdc (max.), 1A
DC Analog Inputs							A															4x ±5Vdc/ 20mA analog input
Serial Ports									4													4x Serial Ports, RS-232/ RS-485 independently configurable and isolated
Ethernet Interface - Built In										T	T											10/100/1000BASE-TX (RJ45 copper)
Ethernet Interface - SFP type												C	C									100BASE-TX (RJ45 copper) [0123-0004]
												T	T									1000BASE-TX (RJ45 copper) [580-3786]
												F	F									100BASE-FX (LC fiber multimode) [580-3784]
												S	S									1000BASE-SX (LC fiber multimode) [580-3785]
												L	L									1000BASE-LX (LC fiber single-mode) [580-3787]
												U	U									Not Required
PCIe Expansion Module															D							2x D.20 Link Ports [528-1007LF]
															U							Not Required
Firmware Version																			00			Latest Firmware Version (Default)
																			B2			v2.2 firmware version
Licenses																				xxx		SW Licenses (ARRM, IEC61850-Client, LogicLinx IEC 61131-3)

To know the Order Code of your G100, run ***mcpsi*** command through the Shell access utility (see Quick Start Guide and Software Manual for more details).

"As-Built" is the order code at factory build time.

"As-Is" is the order code at the time when the user runs the command.

In the example below, after the unit was built in the factory, there were added and configured two Fiber Optic SFP (F) and a D.20 PCIe card (D).

```
admin@G100:~$ mcpsi
Retrieving the GE Multilin MCP system information, please wait ...
================================================================================
                      GE Multilin MCP System Information
================================================================================
Model Number:
    As-Built:      G100-AAL-DA-4TTUU-UUU-B2022-UU
    As-Is   :      G100-AAL-DA-4TTFF-DUU-B2022-UU
```

Please visit the online store for application licenses ordering codes. For latest configuration and options, please visit the online store and search for G100:

https://store.gegridsolutions.com/Home.aspx

Spares and Accessories

	MCP-S	-	*	-	*	Description	
Spare type							
			1		|	SFP Transceiver	
			3		|	PCIe Card	
SFP Transceiver options							
					F	SFP Module 100BASE-FX LC TRANSCEIVER OPTICAL MULTI-MODE 1300nm -40 TO 85C [580-3784]	These options are onlyavailable when Spare type is SFP Transceiver
					S	SFP Module 1000BASE-SX LC TRANSCEIVER OPTICAL MULTI-MODE 850nm -40 TO 85C [580-3785]	
					T	SFP Module 1000BASE-TX RJ45 TRANSCEIVER COPPER -40 TO 85C W/WO RX_LOS [580-3786]	
					L	SFP Module 1000BASE-LX LC TRANSCEIVER OPTICAL SINGLE-MODE 1310nm -40 TO 85C (580-3787)	
					C	SFP Module 10/100BASE-TX RJ45 TRANSCEIVER COPPER -40 TO 85C W/WO RX_LOS [0123-0004] (G100 Only)	
D.20 Card options							
					E	G100 PCIe D.20 HDLC CARD, 2x D.20 Link Ports (528-1007LF)	This option is only available when Spare type is PCIe Card

Chapter 2 - Unpacking and Inspection

This chapter covers the suggested inspection and preparation considerations and background information necessary prior to using the G100.

Unpacking, initial inspection, and first time operation of the G100 are covered.

Following the procedures given in the chapter is recommended, and they will verify proper operation before the product is integrated into your system.

⚠WARNING

Hot Surface: During operation of the G100 the surface of the heat sink, can reach a temperature of 60°C and above. Therefore, be careful and do not touch it with bare fingers.

Electro Static Discharge - ESD

The discharge of static electricity, known as Electro Static Discharge or ESD, is a major cause of electronic component failure. The Industrial Computer has been packed in a static-safe bag which protects it from ESD while it is in the bag. Before removing the Boards or any other electronic product from its static-safe bag, be prepared to handle it in a static-safe environment.

You should wear a properly-functioning anti-static strap and ensure you are fully grounded. Any surface upon which you place on the unprotected G100 should be static- safe, usually facilitated by the use of anti-static mats. From the time the board is removed from the anti-static bag until it is in the card cage and functioning properly, extreme care should be taken to avoid “zapping” the board with ESD. You should be aware that you could “zap” the board without you knowing it; a small discharge, imperceptible to the eye and touch, can often be enough to damage electronic components. Extra caution should be taken in cold and dry weather when electrostatic charge easily builds up.

Only after ensuring that both you and the surrounding area are protected from ESD, carefully remove the board or module from the shipping carton by grasping the module on its edges. Place the board, in its anti-static bag, flat down on a suitable surface. You may then remove the board from the anti-static bag by tearing the ESD warning labels.

Initial inspection

After unpacking the products, you should inspect it for visible damage that could have occurred during shipping or unpacking. If damage is observed (usually in the form of bent component leads or loose socketed components), contact GE Technical Support for additional instructions. Depending on the severity of the damage, it may be necessary to return the product to the factory for repair.

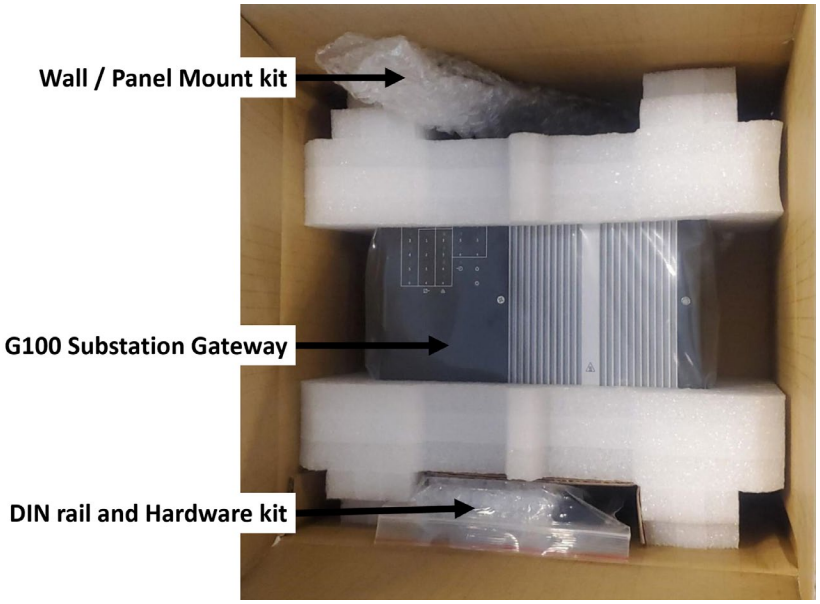
⚠WARNING

DO NOT apply power to the product if it has visible damage!

Doing so may cause further, possibly irreparable damage, as well as introduce a fire or shock hazard.

The G100 shipment will include the following:

- G100 Substation Gateway
- Wall / Panel mounting kit
    - Wall / panel mounting bracket (quantity 2)
- DIN rail and Hardware kit
    - DIN Rail (quantity 1)
    - Screws (quantity 6)
- Analog DC Input (AI) connector (quantity 1)
- Binary Input (DI) connector (quantity 1)
- Binary Output (DO) connector (quantity 1)
- Power input connector (quantity 1)
- IRIG-B input connector (quantity 1)



Unpacking

Please read the manual carefully before unpacking the board or module or fitting the device into your system. Also adhere to the following:

- Observe all precautions for electrostatic sensitive modules
- Do not place the board on conductive surfaces, anti-static plastic, or sponge, which can cause shocks and lead to board trace damage.
- Do not exceed the specified operational temperatures.
- Keep all original packaging material for future storage or warranty shipments of the board.

Although the products are carefully packaged to protect against the rigors of shipping, it is still possible that shipping damage can occur. Careful inspection of the shipping carton should reveal some information about how the package was handled by the shipping service. If evidence of damage or rough handling is found, you should notify the shipping service and GE Technical Support as soon as possible.

PCIe Cards and storage devices may also have temperature restrictions

Retain all packing material in case of future need.

⚠WARNING

Before installing or removing any board, please ensure that the system power and external supplies have been turned off!

Chapter 3 - Installing the G100

This chapter covers the installation of the G100 and initial power-on operations.

⚠WARNING

Before you install and operate the G100, read and follow the safety guidelines and instructions in *Safety precautions*.

Installation

The G100 device can be installed as either wall / panel mounted, or DIN Rail mounted.

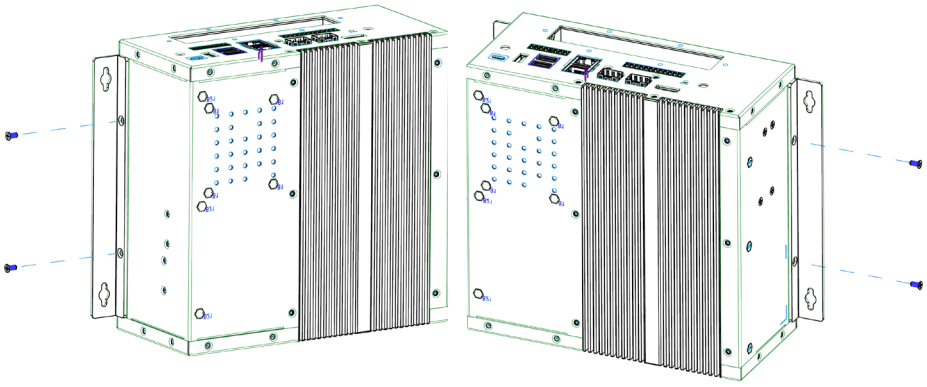
The G100 shall be installed in:

- Pollution Degree II, non-hazardous and restricted access location,
- Environment where the ambient temperature does not exceed the rating of the product,
- Air flow is not restricted

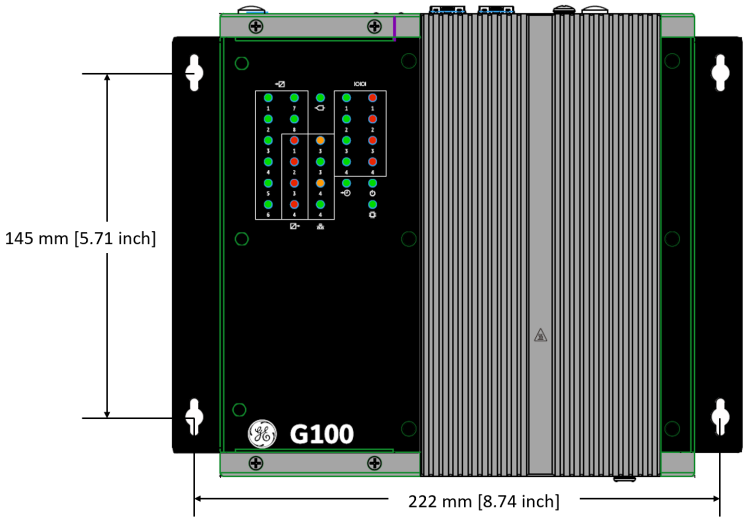
Wall / Panel Mounting instructions

Please see following instructions to mount it.

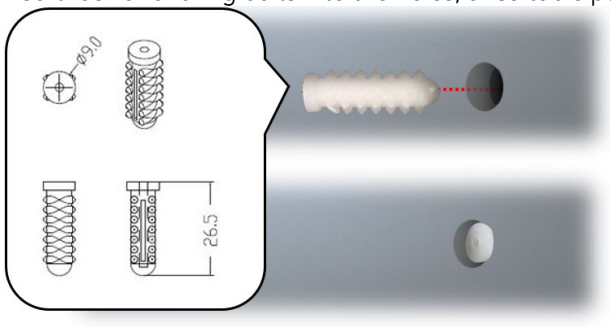
1. Mount the wall/panel mount bracket as shown below.
    a. Locate and retrieve the wall/panel mount brackets from the G100 carton.
    b. Locate and removed the 2x M3 screws on the left side of the chassis closest to the rear.
    c. Position one of the wall/panel mount brackets to the chassis, aligning the mounting holes in the bracket to the chassis.
    d. Reinstall the 2 screws removed in the step above on the left side of the chassis to secure the bracket to the chassis. The recommended torque setting for the M3 screws are 5.2 in-lb [0.59 Nm].
    e. Repeat the above steps for the mounting the bracket to the right side of the chassis.



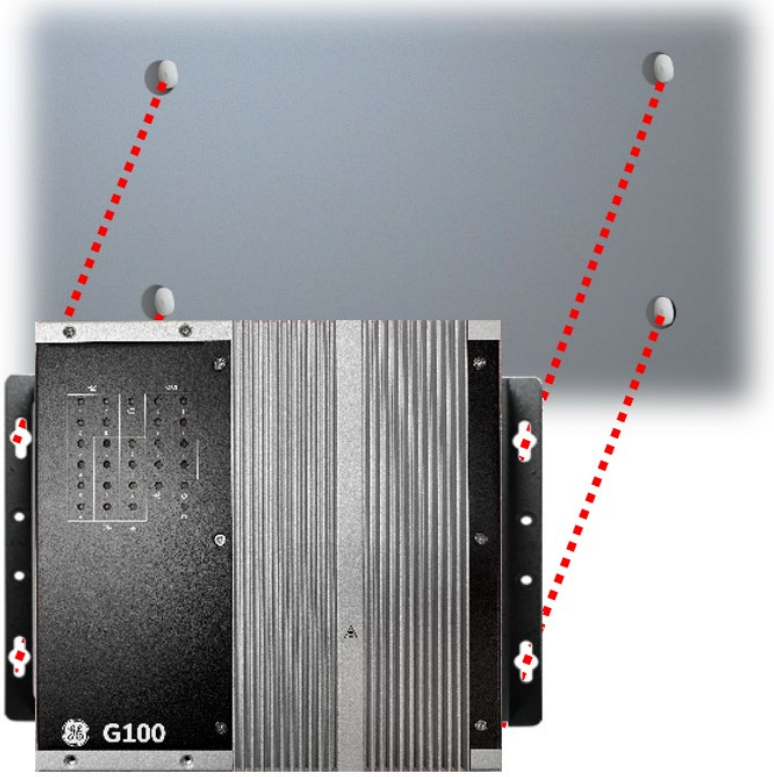
2. On the wall / panel, measure the exact place where you want to install the G100 and drill four holes that match the four mounting holes on both brackets.



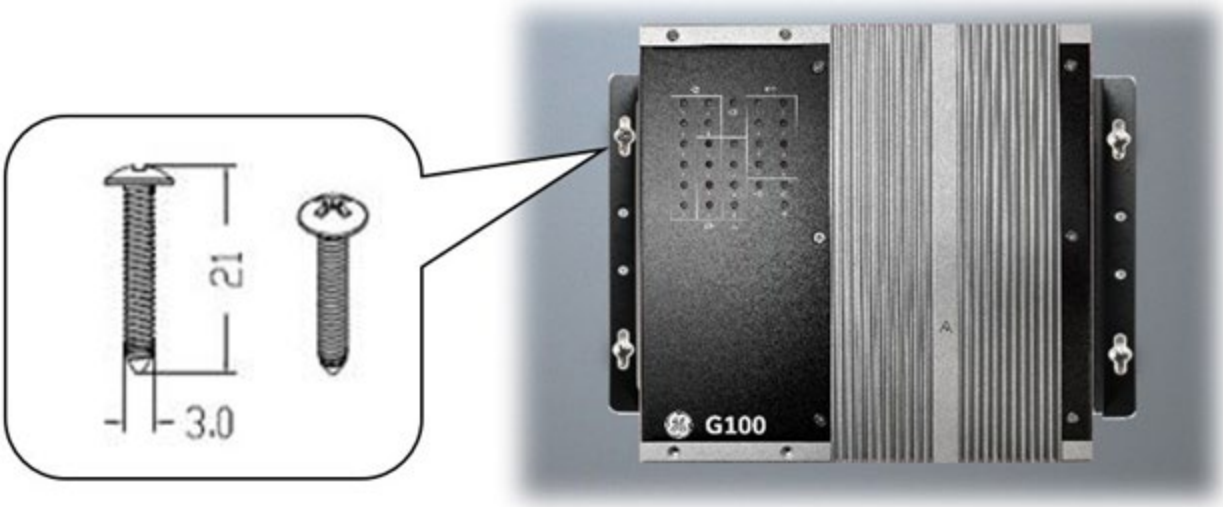
3. Insert four anchoring bolts into the holes, or suitable panel nuts that match your mounting screws.



4. Align the G100 brackets with the four bolts / nuts you just installed on the wall / panel.



5. Drive the mounting screws into the anchoring bolts / nuts to secure the G100.



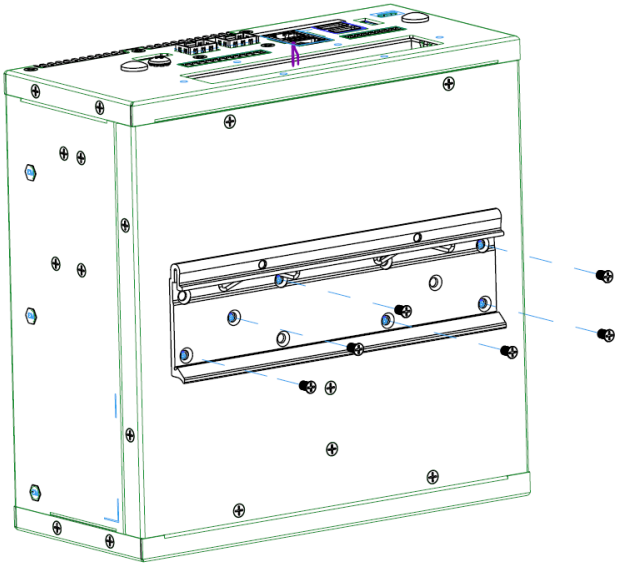
DIN Rail Mounting instructions

Please see following instructions to mount it.

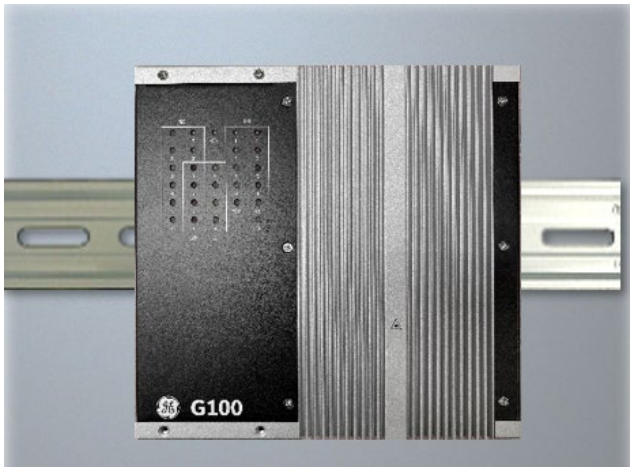
1. Mount the DIN rail as shown below.
    a. Locate and retrieve the DIN rail bracket and mounting screws from the G100 carton.
    b. Position the DIN rail bracket to the rear of the chassis, aligning the mounting holes in the rail to the chassis.
    c. Install the 6 screws provided with the DIN rail bracket to secure the bracket to the chassis. The recommended torque setting for the 6/32 screws are 5.2 in-lb [0.59 Nm].

NOTE

The top of the DIN rail bracket should be positioned to align with the top of the G100 chassis.



2. Position the G100 on a slight angle and slowly lower until the top of the DIN bracket on the G100 engages the DIN rail. Pull the G100 firmly downward and press flat against the wall/panel until the DIN rail bracket locks into position.

1. 

Installation of optional D.20 HDLC Card

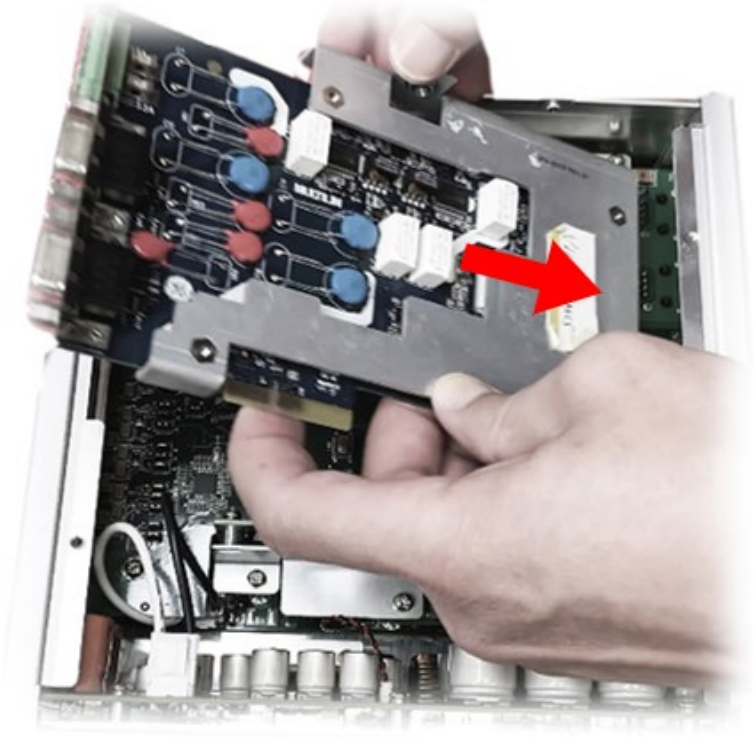
The optional D.20 HDLC card can be ordered already installed with the unit at factory time, or can be installed later, as follows.

NOTICE

Before you open the G100 chassis to install the D.20 HDLC Card, read and follow the guidelines and instructions in Electro Static Discharge - ESD

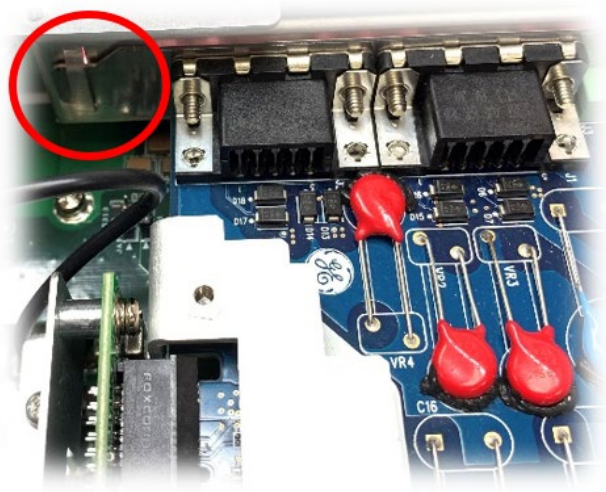
1. To install the D.20 HDLC card, flip over the system and loosen and remove the eight screws indicated below so that the chassis cover can be removed.

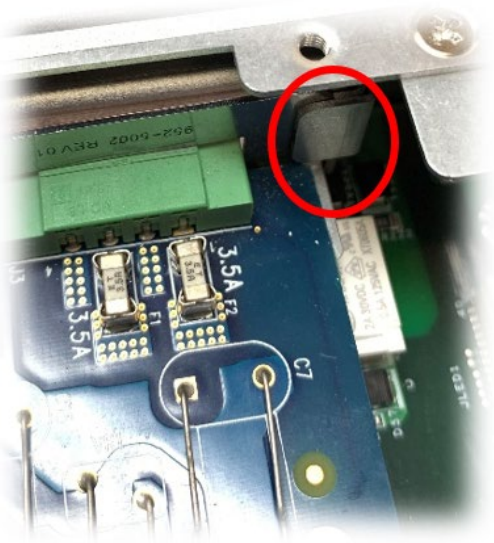
2. Place the card into the system as shown in the picture.



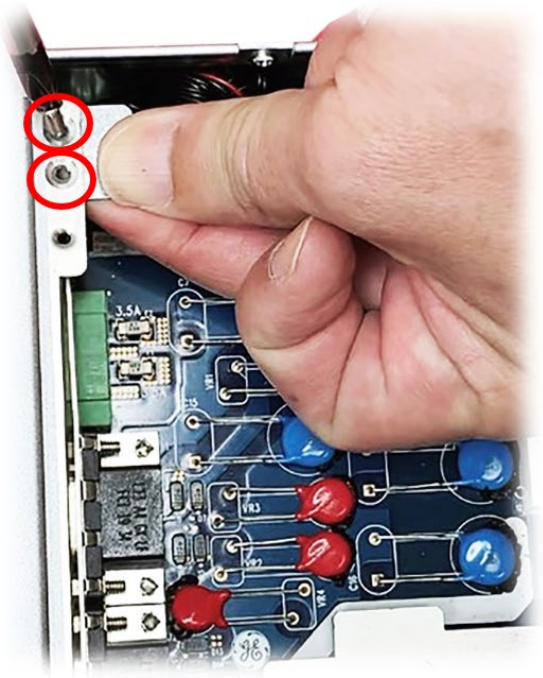
3. Align the notch of the module with the socket key in the slot and carefully insert the card into the slot.

4. Make sure the card slot has complete insert to these 2 metal sheets.

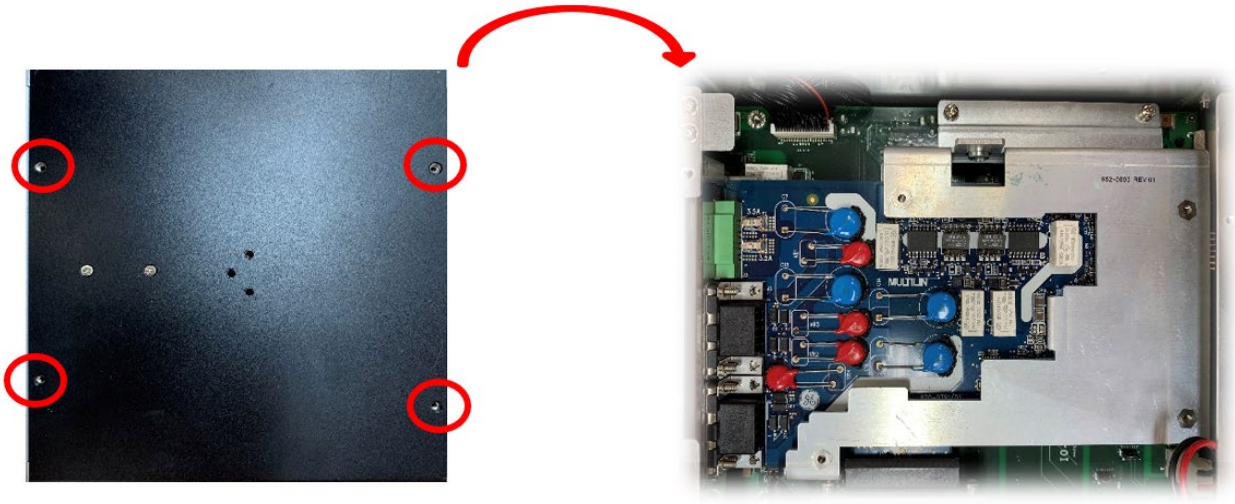




5. Connect the metal sheets with the system by securing the two screws.



6. Place the cover back to the system and secure it with eight screws.



Grounding

It is required to connect the G100 chassis to cabinet ground, which then MUST BE CONNECTED TO Building Protective Earth (PE) ground using the ground connection screw located near the G100 power supply connector on the bottom side panel.

⚠WARNING An improperly wired ground connection could place hazardous voltages on accessible metal parts.

Power Supply

The G100 is intended to be powered by a UL list DC power supply or DC power source, via one 2 Pin DC-IN connector located on the bottom side panel.

The power input is rated 12/24/48Vdc, 5/2.5/1.25A minimum, Tmax = 70 degree C, and the altitude of operation = 5000m.

The device has a maximum power consumption of 60 W.

Make sure you connect the “+”and “- wires according to the label adjacent to the connector.

Wires	The conductor size is from 16 AWG to 12 AWG and Strip Length is 7mm. After plugging cable lines into the mating connector, plug the mating connector to the product and secure the plug with the two screws.
Breaker circuit	A 20A IEC/USA/Canada breaker circuit is required as pre fuse.
Disconnect device	A readily accessible disconnect device shall be incorporated external to the unit.
Inrush current	The inrush current is typically 8A when powering up.
Reverse polarity protection	The product is equipped with built-in reverse polarity protection. If + and - are swapped the unit will not power-up and harm to neither the power supply nor the unit will occur.
Overcurrent protection	The overcurrent protection function interrupts an uncontrolled fault current or overcurrent before serious damage can occur, such as overheating of the equipment. The internal fuse is rated for 10A continuous current. If that current is exceeded by factor 10 the fuse will blow in between 1ms and 10ms. The fuse is placed in ”+“connection of the power supply.

Power-On Self-Test (POST)

Each time the G100 boots up it must pass the POST (Power-On Self-Test).

If the G100 does not pass POST, the board will fail the POST and “beep” in a specific pattern. Please contact GE’s Grid Solution support in this case.

Full completion of the POST and applications available to run may take up to 3 minutes.

NOTICE **UEFI and POST messages are displayed on the Video output (DP) port, and if enabled on the maintenance serial port. Refer to section “Default Serial Maintenance port (port 4, RS232)” on page 52 for additional information on the serial maintenance port.**

Super Capacitor and Real Time Clock (RTC)

The G100 does not include a battery. Instead, the G100 contains one super capacitor, powering the real-time clock (RTC). This super capacitor will power the RTC for at least 5 days with no connection to power.

After this super capacitor discharges, UEFI settings will default to their factory default values (see section *UEFI Settings*) and the **RTC** time will be reset **internally** to an invalid time (e.g. 12:00 AM, 01-10-2000), and will be later updated to the correct time after the system will be powered on again and time synchronized again.

When the system is subsequently powered up, the system time will be initialized to the RTC time if the super capacitor was not discharged. If the super capacitor was discharged, the system time will be initialized to the last time when the system was still powered on.

Chapter 4 - Interfaces and Indicators

This chapter covers the interfaces of the G100 Substation Gateway.

UEFI Settings

Please refer to the document *Configuring UEFI Settings on G100 User Guide (SWM0122)* for details.

G100 device has the following UEFI settings that will revert to default values after the internal super capacitor has been discharged due to the device being powered off for extended time (typically more than 5 days).

These UEFI settings are applicable only while the G100 is starting.

After the applications started, these settings are over-written by the values configured in *MCP Local Configuration Utility (mcpcfg)* or *MCP Settings GUI* (which are persistent).

- Default Serial Maintenance Port used as UEFI (boot) console when KVM is not available (Advanced->Serial Port Console Redirection)
  - Console Redirection is set to Disabled for COM1-COM3, please do not change these settings.
  - Console Redirection for COM4 should be enabled/disabled and have the "Bits per second", to be same as in *the Serial Maintenance Port in MCP Studio (See MCP Software Configuration Guide SWM0101 > Serial Maintenance Port).*
- Default Serial Ports Modes (Advanced->Super IO Configuration)
  - Please ensure are enabled/disabled as required for secure hardening purposes and set to RS-232.

Users should check again these UEFI settings when the G100 is powered on again, and adjust as necessary.

General Purpose IO (GPIO)

G100 is equipped with an internal General Purpose Input/Output (GPIO) interface.

The available GPIO signal types are as follows.

Binary Inputs (DI): 8

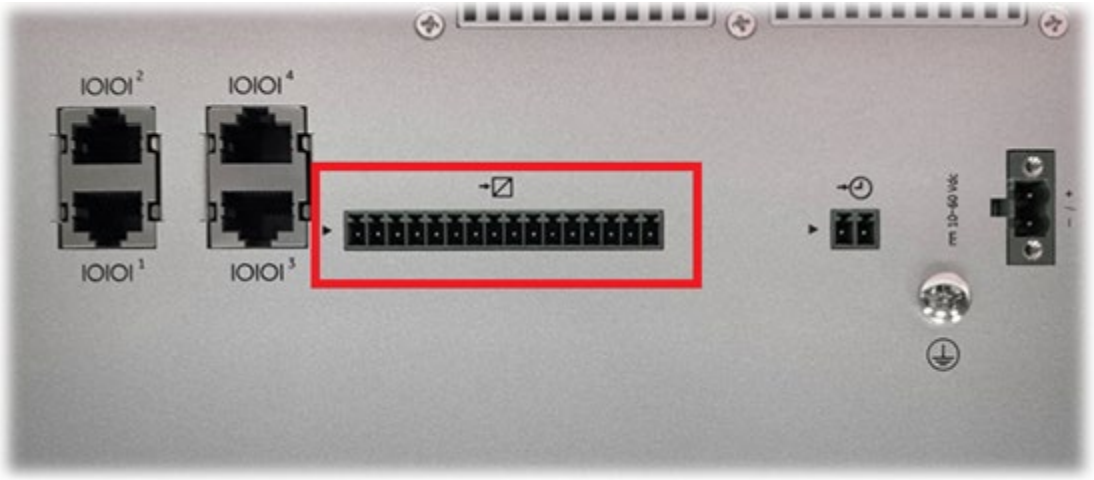
All DI are wetted internally from main power supply circuit using single common for all 8 channels.

Each DI channel can be triggered by N.O. potential free external contacts, with the wetted positive voltage being switched through the external contacts.

The DI wetting voltage is protected internally by the main fuse.

The DI voltage supply is the same as the G100 Power Supply: 12/24/48 VDC, with each DI channel consuming typically 5mA.

DI wiring is via a pluggable connector, pitch 3.5mm x 16 pins, located on the bottom side panel:

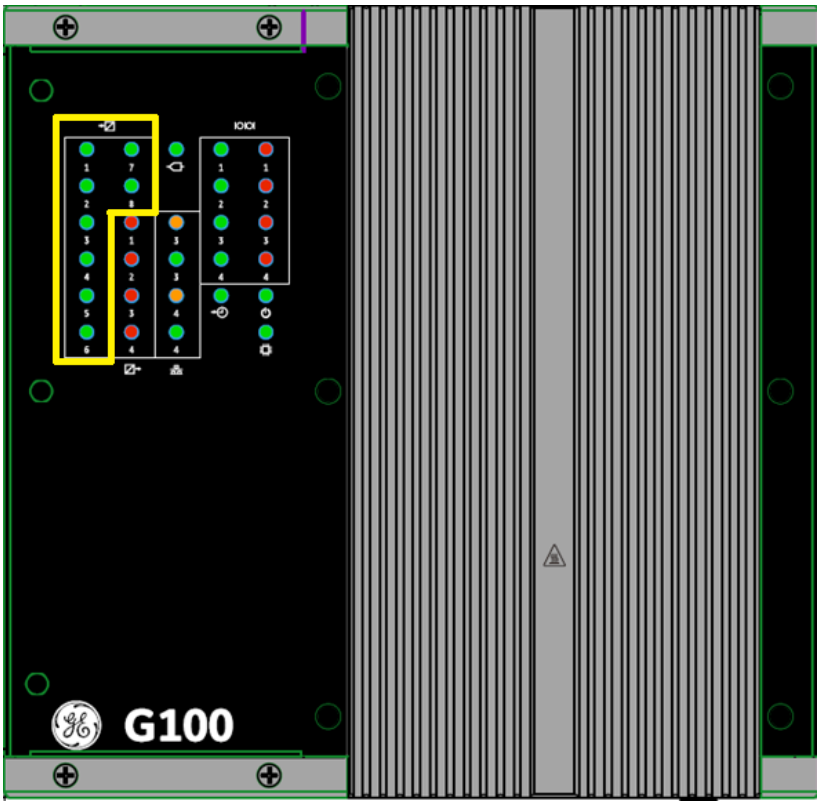


The small arrow on the left indicates PIN 1.

Table 4: GPIO DI connector pin assignments

PIN NO.	DESCRIPTION
1 (arrow)	DI_1
2	DI_COM (+)
3	DI_2
4	DI_COM (+)
5	DI_3
6	DI_COM (+)
7	DI_4
8	DI_COM (+)
9	DI_5
10	DI_COM (+)
11	DI_6
12	DI_COM (+)
13	DI_7
14	DI_COM (+)
15	DI_8
16	DI_COM (+)

Each DI channel is indicated as “input active” (ON) at runtime via a numbered LED located on the front side of the G100:

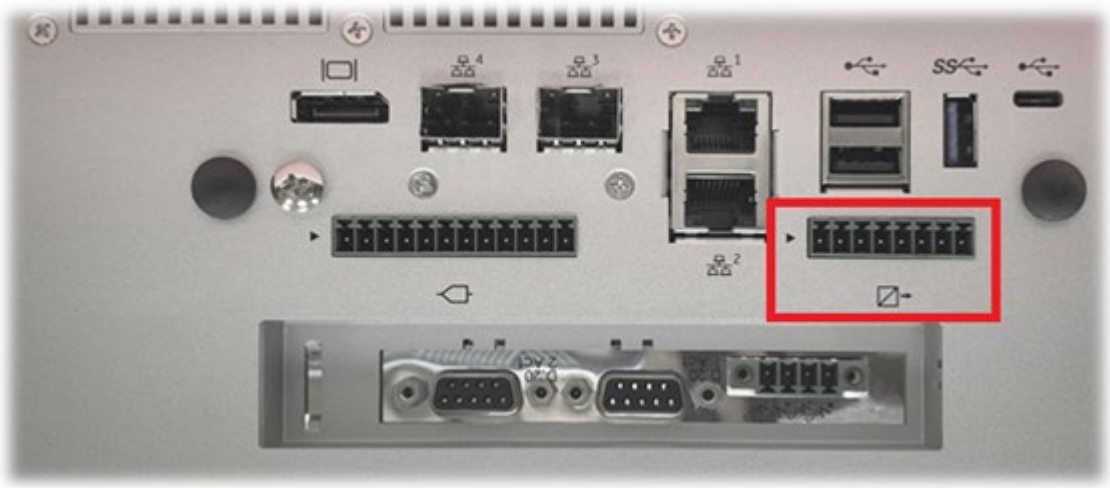


Binary Outputs (DO): 4

Each DO channel is isolated and independent, and provides a N.O. (Normal Open) dry relay single contact, rated at 10 – 60 VDC / 1A (Max.).

NOTE The DO channels are not fused internally.

DO wiring is via a pluggable connector, pitch 3.5mm x 8 pins, located on the top side panel:

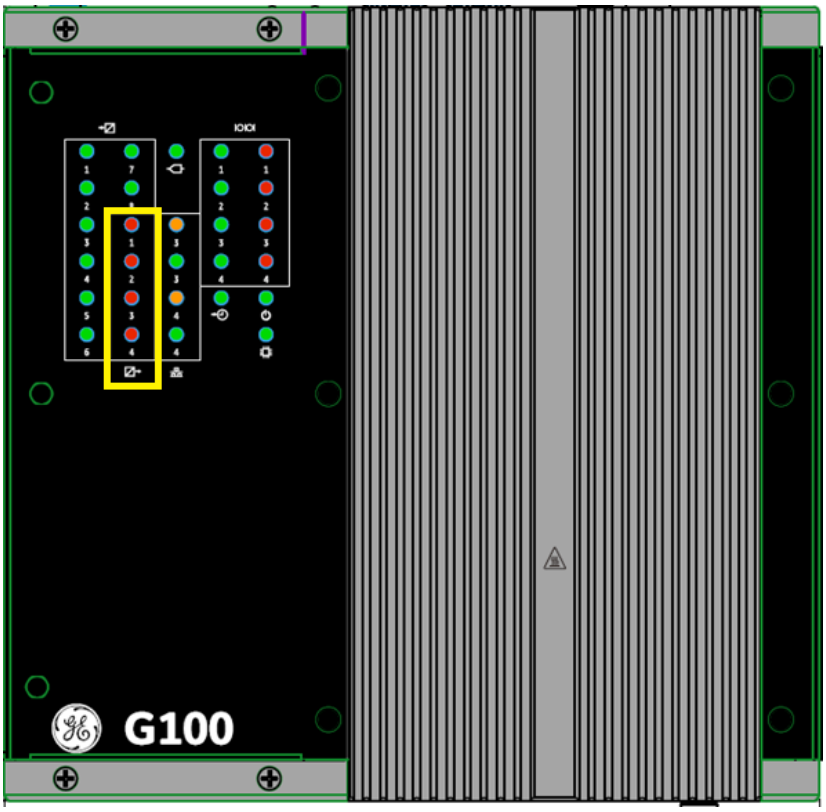


The small arrow on the left indicates PIN 1.

Table 5: GPIO DO connector pin assignments

PIN NO.	DESCRIPTION
1 (arrow)	RELAY1_NO1
2	RELAY1_COM1
3	RELAY2_NO1
4	RELAY2_COM1
5	RELAY3_NO1
6	RELAY3_COM1
7	RELAY4_NO1
8	RELAY4_COM1

Each DO channel is indicated as “active” (ON) at runtime via a numbered LED located on the front side of the G100:



NOTE

The DO operation types are PULSE, LATCH_ON and LATCH_OFF.

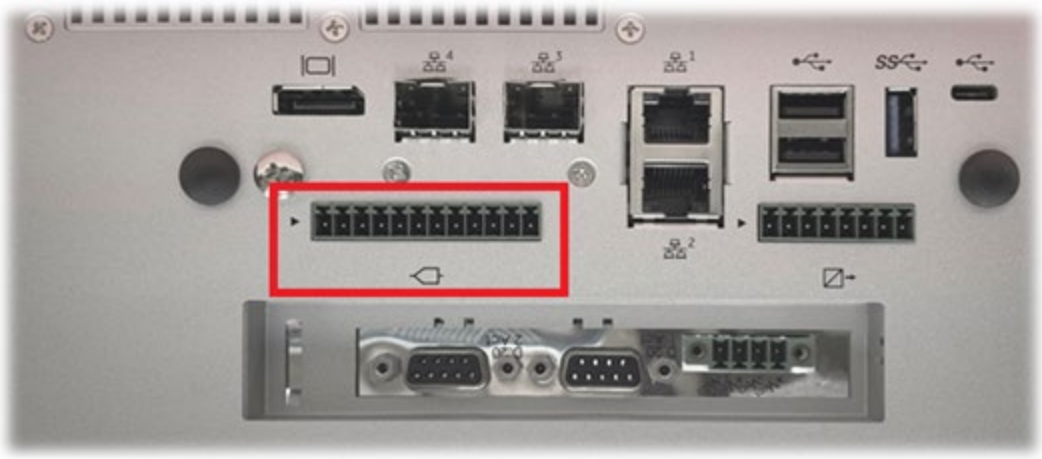
At runtime, commands received as CLOSE/ON are translated to LATCH_ON, and commands received as TRIP/OFF are translated to LATCH_OFF. The PULSE command types are executed as PULSE, according to their associated count and duration parameters

Analog DC Inputs (AI): 4

Each AI channel is configurable via internal jumpers as Full Scale either +5 VDC (Default setting) or 20 mA.

The resolution is 12-bit plus sign, self calibrating.

AI wiring is via a pluggable connector, pitch 3.5mm x 12 pins, located on the top side panel:



The small arrow on the left indicates PIN 1.

Table 6: GPIO AI connector pin assignments

PIN NO.	DESCRIPTION
1 (arrow)	A_VIN0+/IIN0 +
2	A_VIN0 -
3	AGND_ISO_CHS
4	A_VIN1+/IIN1 +
5	A_VIN1 -
6	AGND_ISO_CHS
7	A_VIN2+/IIN2 +
8	A_VIN2 -
9	AGND_ISO_CHS
10	A_VIN3+/IIN3 +
11	A_VIN3 -
12	AGND_ISO_CHS

NOTE

In the pin description, "_CHS" is the shield connection for each AI channel (all CHS are common wired internally).

The jumpers for Voltage or Current input selection are located on the GPIO internal board and their settings are as follows:

Jumper JAI12~JAI15	
1-2 (Default)	Voltage
2-3	Current

Table 7: GPIO AI Voltage / Current selection jumper

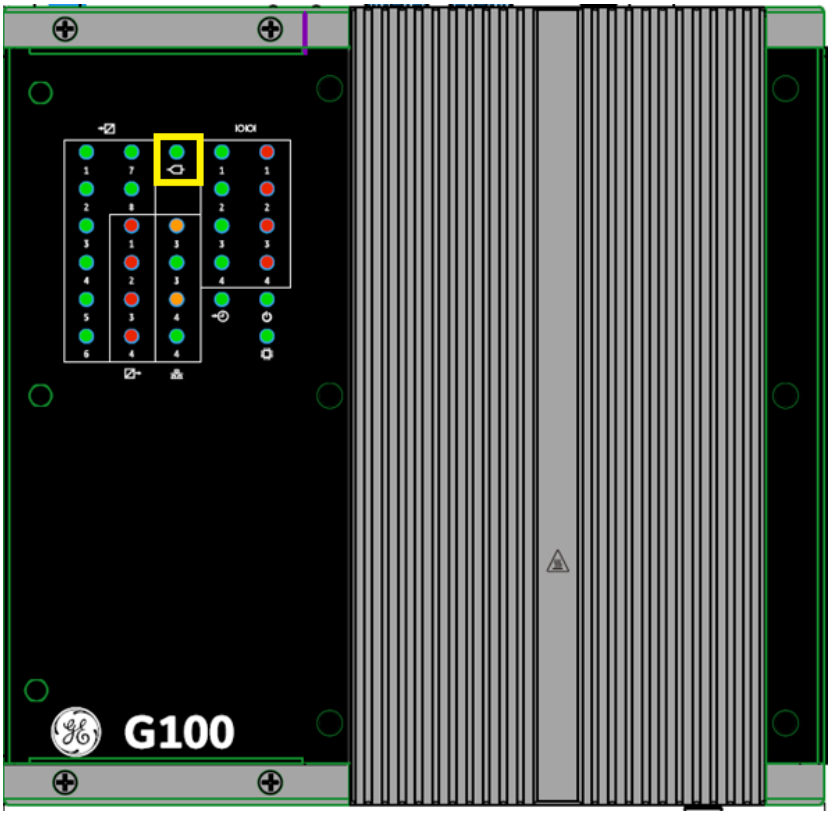
Jumper JAI12	DESCRIPTION
1-2 (Default)	V_IN_CH_1
2-3	I_IN_CH_1

Jumper JAI13	DESCRIPTION
1-2 (Default)	V_IN_CH_2
2-3	I_IN_CH_2

Jumper JAI14	DESCRIPTION
1-2 (Default)	V_IN_CH_3
2-3	I_IN_CH_3

Jumper JAI15	DESCRIPTION
1-2 (Default)	V_IN_CH_4
2-3	I_IN_CH_4

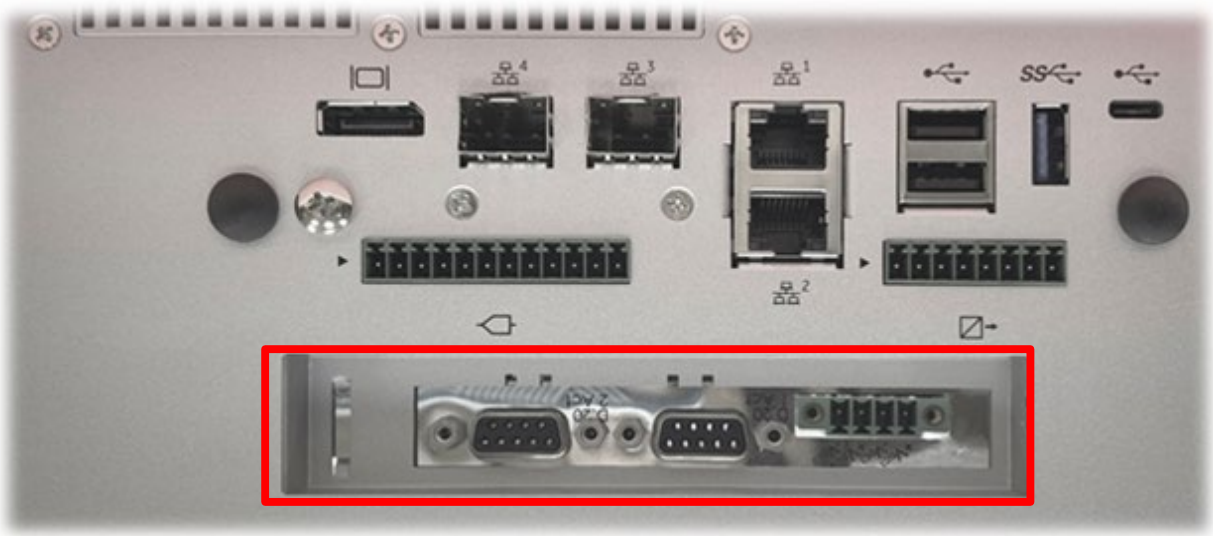
AI sampling is indicated at runtime via one LED (for all AI channels) located on the front side of the G100:



D.20 Link Connections

G100 is able to communicate with D20 peripheral modules.

To communicate with D20 peripheral I/O modules the G100 requires the installation and configuration of the optional D.20 HDLC PCIe card.



D.20 Communications between the D.20 HDLC PCIe card and the D20 peripheral I/O modules are carried over a proprietary high-speed, high-level data link control (HDLC) protocol called the D.20 Link.

The D.20 HDLC PCIe card supports two D.20 Link communications ports. The G100 system can be ordered from the factory with the D.20 HDLC PCIe card pre-installed using the Product configurator through the Online Store or can be installed infield by ordering the D.20 HDLC PCIe card as an accessory from the MCP Substation Gateway Spare Parts and following the “Installation of optional D.20 HDLC Card” on page 27.

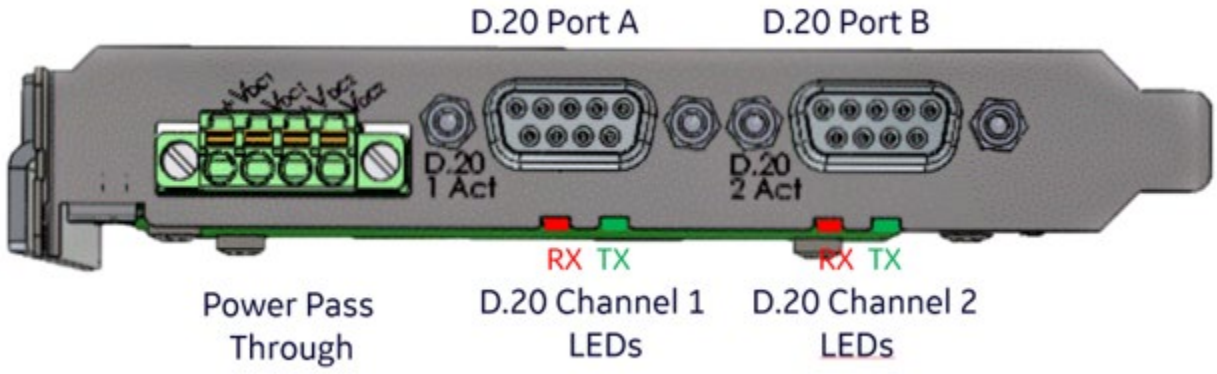
NOTE

G100 is limited by performance to communicate with up to **60** D.20 peripheral I/O modules.

Please consider the G500 product for more D20 peripheral I/O modules (up to the maximum of 120).

G100 D.20 HDLC PCIe card

The D.20 HDLC PCIe card is equipped with a Power Pass Through connector, two D.20 ports and four LEDs.



The Power Pass Through connector allows the D.20 peripheral connected to the D.20 Link to be powered through the D.20 port. The Power Pass Through requires one or two external power supplies to be connected. Refer to “Supplying power through the D.20 Link” on page 29 section for further details.

Two sets of LEDs are present on the D.20 HDLC PCIe card to indicate activity status. The first set of LEDs, on the left labeled D.20 1 Act, shows the transmit and receive activity on D.20 Channel 1 and the second set to show activity on D.20 Channel 2 on the right labeled D.20 2 Act. The receive LEDs will flash red and the transmit LEDs will flash green.

The D.20 HDLC PCIe card has two D.20 ports. Each port contains D.20 Channel 1, D.20 Channel 2, DC Supply 1, and DC Supply 2. For D.20 port A, the above signals are always available. For D.20 port B, D.20 Channel 1 and D.20 Channel 2 are configurable but DC Supply 1 and DC Supply 2 are always available. Refer to Table 1: D.20 Port A and B pin out and configuration options and Table 2: Default D.20 Relay settings. D.20 Port B settings are software controlled and are accessible through the Settings GUI on your G100. Refer to SWM0101 for further details on configuration.

Table 8: D.20 Port A and B pin out and configuration options

Pin Number	D.20 port A	D.20 Port B	
1	No Connection	No Connection	
2	D.20 Channel 1 TX/RX	D.20 Channel 2 TX/RX	OPEN
3	D.20 Channel 1 TX/RX -	D.20 Channel 2 TX/RX -	OPEN
4	VDC1 +	VDC1 +	

5	VDC1 -	VDC1 -	
6	D.20 Channel 2 TX/RX	D.20 Channel 1 TX/RX	OPEN
7	D.20 Channel 2 TX/RX -	D.20 Channel 1 TX/RX -	OPEN
8	VDC2 +	VDC2 +	
9	VDC2 -	VDC2 -	

End of link termination is required at each end of the D.20 Link and is critical for proper operation. The D.20 HDLC PCIe card has two relays which control the End of Link termination, one for each D.20 Channel. Refer to Table 2: Default D.20 Relay settings. End of Link termination settings are software controlled and are accessible through the Settings GUI on your G100. Refer to SWM0101 for further details on configuration.

Table 9: Default D.20 Relay settings

D.20 Relay setting	Default setting
End of Link termination on channel 1	Enabled
End of Link termination on channel 2	Enabled
D.20 channel 1 to D.20 port B connection	Disabled
D.20 channel 2 to D.20 port B connection	Disabled

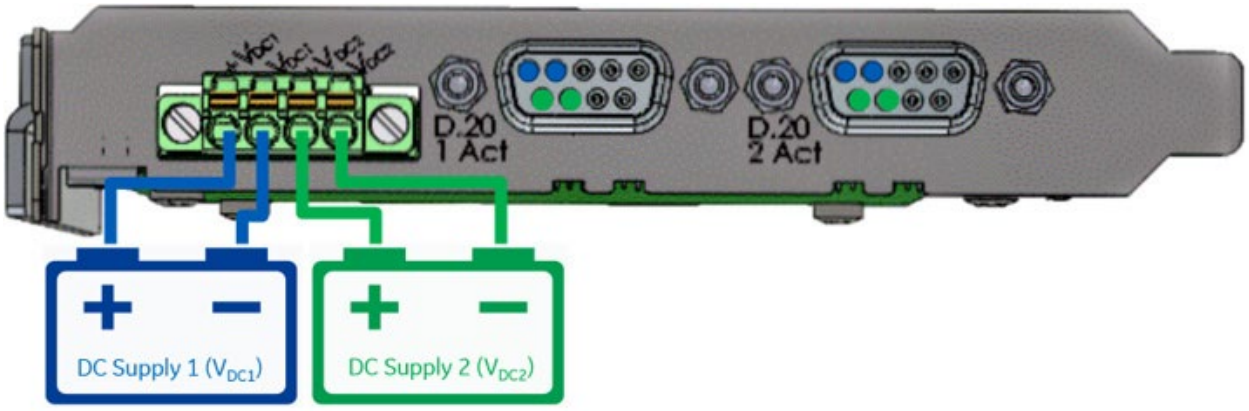
Supplying power through the D.20 Link

Power is typically supplied to peripheral devices directly through the WESTERM boards or inject power into the D.20 link using the D.20 DC Interface module (520-0154). However, with the D.20 HDLC PCIe card the Power Pass Through connections can be utilized to inject power into the D.20 link to supply power to peripheral devices through the D.20 ports.

One or two independent power supplies can be connected to DC Supply 1 (VDC1) and DC Supply 2 (VDC2). DC Supply 1 (VDC1) is connected through to pins 4 and 5 on both D.20 ports (DB9 connector), respectively DC Supply 2 (VDC2) is connected to pins 8 and 9.

The DC supply load on the D.20 port by the peripheral link must not to exceed 3.5A and 20 -60 VDC

The Power Pass Through connections are protected to 3.5A



D.20 Peripheral Types

D.20 Peripheral I/O modules are intelligent modules containing an on-board microprocessor. They are configured as slaves to the G100. In this way, specific I/O processing is distributed throughout the to the appropriate I/O module.

There are four types of I/O peripherals supported by the D.20 HDLC PCIe:

- D20A analog input
- D20S digital inputs
- D20K digital output
- D20C combination input/output

Optional high-voltage peripherals are also available.

Redundant D.20 communication channels are available on all peripherals. To utilize this function redundant D.20 LAN cards are required to be installed on the D.20 Peripheral I/O modules. D.20 A, S and K Peripheral I/O modules require 540-0207 and D.20 C requires 540-0209.

The D.20 HDLC PCIe card is only compatible with CCU BASE and PCOMMON v3.00 or higher.

NOTE

Refer to Peripheral Compatibility with the D.20 HDLC PCIe card section in this manual for complete list of D.20 Peripheral I/O compatibility.

For further information on I/O peripherals, see the D20/D200 Installation and Operations Guide (part number 994-0078); see section: Connections and Configuration.

Peripheral compatibility with the D.20 HDLC PCIe card

Use the tables in this section to check compatibility with existing D.20 Peripheral I/O modules and devices.

Table 10: D20A Analog Input Module Compatibility

Component	GE Item #	Description	Compatible release	Date of release
WESDAC	511-0101	WESDAC D20A TYPE 1 VERSION 1	REL 21-higher	April 1998

WESDAC	511-0102	WESDAC D20AHV	All	
WESDAC	511-0103	WESDAC D20AHV2	All	
WESTERM	517-0163	WESTERM D20A TYPE 1 VERSION 1	All	
	517-0178	WESTERM D20 AD	All	
Redundant D.20 LAN	540-0207	WESDAC D20 ASK D.20 I/F	All	
PCOMMON	306	PCOMMON v3.06	All	
	305	PCOMMON v3.05	All	
	301	PCOMMON v3.01	All	
	300	PCOMMON v3.00	All	

Table 11: D20S Status Input Module Compatibility

Component	GE Item #	Description	Compatible release	Date of release
WESDAC	507-0101	WESDAC D20S TY1 VER 1	REL 18-higher	March 1998
WESDAC	507-0103	WESDAC D20SHV2	All	
WESTERM	517-0165	WESTERM D20S TYPE 1 VERSION 1	All	
Redundant D.20 LAN	540-0207	WESDAC D20 ASK D.20 I/F	All	
PCOMMON	306	PCOMMON v3.06	All	
	305	PCOMMON v3.05	All	
	301	PCOMMON v3.01	All	
	300	PCOMMON v3.00	All	

Table 12: D20K Control Output Module Compatibility

Component	GE Item #	Description	Compatible release	Date of release
WESDAC	508-0101	WESDAC D20K TYPE 1 VERSION 1	REL 17-higher	April 1998
WESDAC	508-0102	WESDAC D20KHV	All	
WESTERM	517-0164	WESTERM D20K TYPE 1 VERSION 1	All	
Redundant D.20 LAN	540-0207	WESDAC D20 ASK D.20 I/F	All	

PCOMMON	306	PCOMMON v3.06	All	
	305	PCOMMON v3.05	All	
	301	PCOMMON v3.01	All	
	300	PCOMMON v3.00	All	

Table 13: D20C Combination Input/Output Module Compatibility

Component	GE Item #	Description	Compatible release	Date of release
WESDAC	504-0002	WESDAC D20C+	REL 20-higher	September 1996
WESDAC	504-0003	WESDAC D20CHV	All	
WESTERM	517-0180	WESTERM D20 CD	All	
Redundant D.20 LAN	540-0209	WESDAC D20C D.20/WESMAINT I/F	All	
PCOMMON	305	PCOMMON v3.05	All	
	300	PCOMMON v3.00	All	

Table 14: Repeater/Splitter Compatibility

Component	GE Item #	Description	Compatible release	Date of release
REPEATER	520-0117	D.20 COMMUNICATION INTERFACE	REL 13 -higher	April 1999
SPLITTER	520-0118	D.20 FIBER OPTIC SPLITTER 4-WA	REL 11 -higher	April 1999
GFO	520-0148	WESDAC D.20 RS485/GFO I/F 48V	REL 09 -higher	December 1994

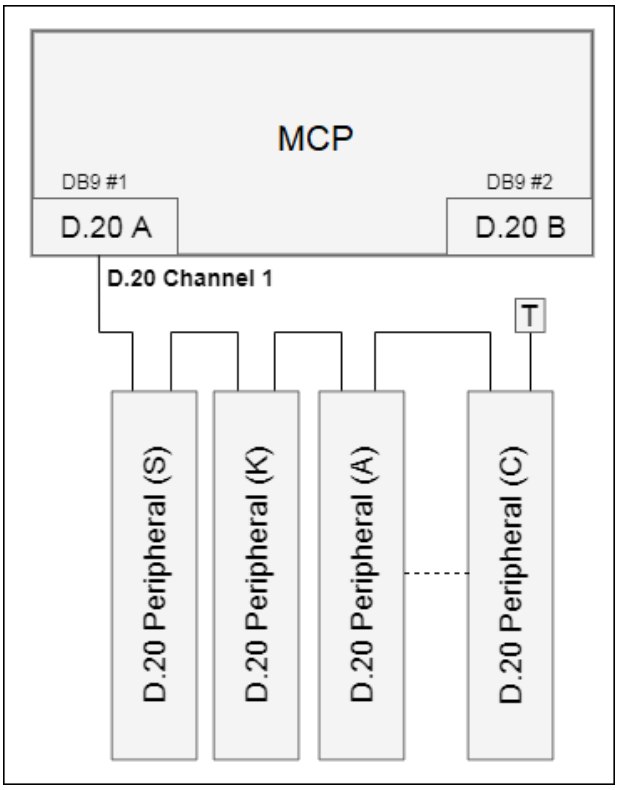
D.20 Connection topologies

The D.20 HDLC PCIe card supports the below D.20 topologies:

- Single D.20 terminated, single link
- Dual D.20 link terminated
- Single D.20 link, redundant LAN
- Redundant D.20 link, redundant LAN

Single D.20 terminated, single link

Figure 4: Single D.20 terminated, single link - Topology



D.20 redundant LAN daughter card can optionally be installed with the corresponding configuration (Single Link) in DSAS.

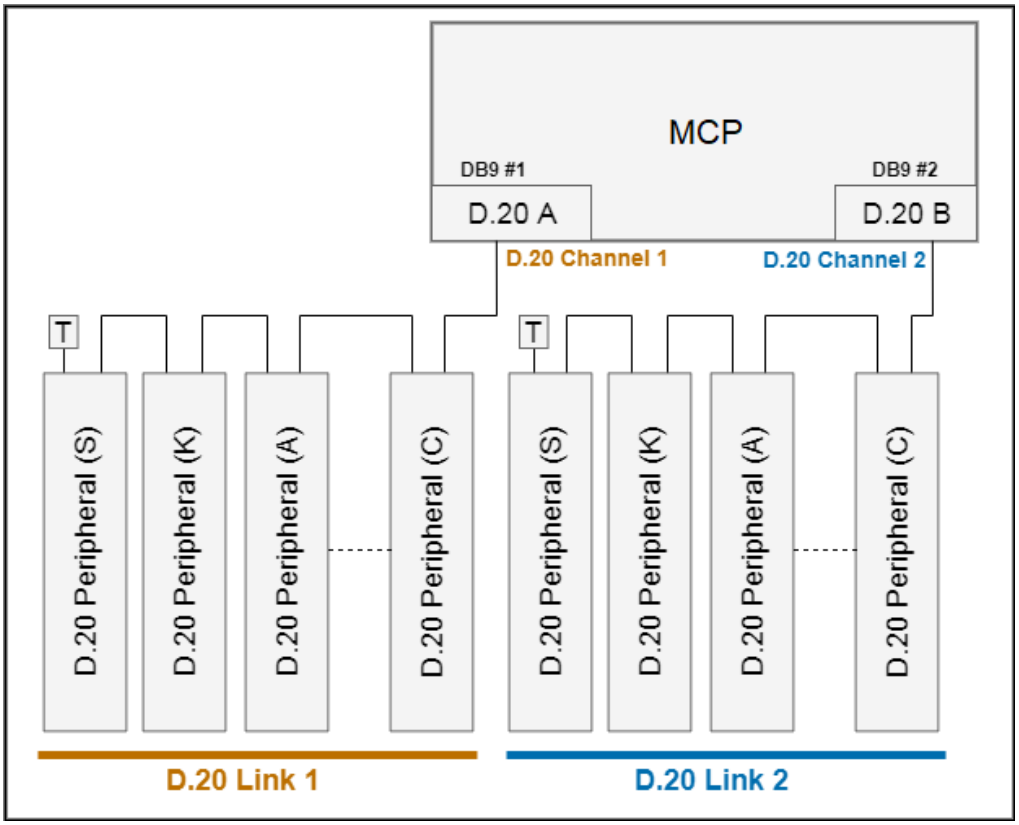
The last D.20 peripheral must be terminated with D.20 terminator (GE part#: 977-0049).

Table 15: Single D.20 terminated, Single Link - Default settings

Function	State
End of Link - D.20 Channel 1	ON
End of Link - D.20 Channel 2	ON
Port B - D.20 Channel 1 (pin 6/7)	OFF
Port B - D.20 Channel 2 (pin 2/3)	OFF

Dual D.20 link terminated

Figure 5: Dual D.20 link terminated - Topology



D.20 redundant LAN daughter card can optionally be installed with the corresponding configuration (Redundant Link) in DSAS.

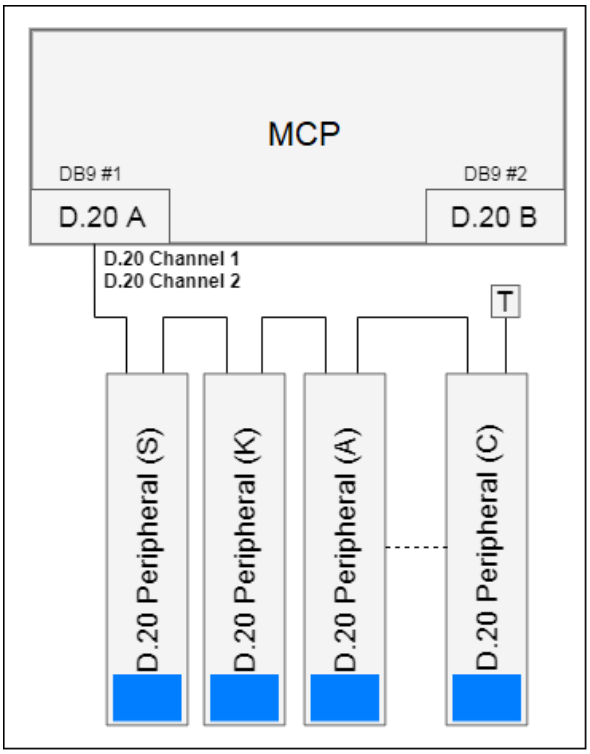
The last D.20 peripheral must be terminated with D.20 terminator (GE part#: 977-0049).

Table 16: Dual D.20 link terminated – Default settings

Function	State
End of Link - D.20 Channel 1	ON
End of Link - D.20 Channel 2	ON
Port B - D.20 Channel 1 (pin 6/7)	OFF
Port B - D.20 Channel 2 (pin 2/3)	ON

Single D.20 link, redundant LAN

Figure 6: Single D.20 link, redundant LAN - Topology



D.20 redundant LAN daughter card (GE part#: 540-0209 for D.20C and GE part#: 540-0207 for D.20A,S,K) must be installed with the corresponding configuration (Redundant Link) in DSAS.

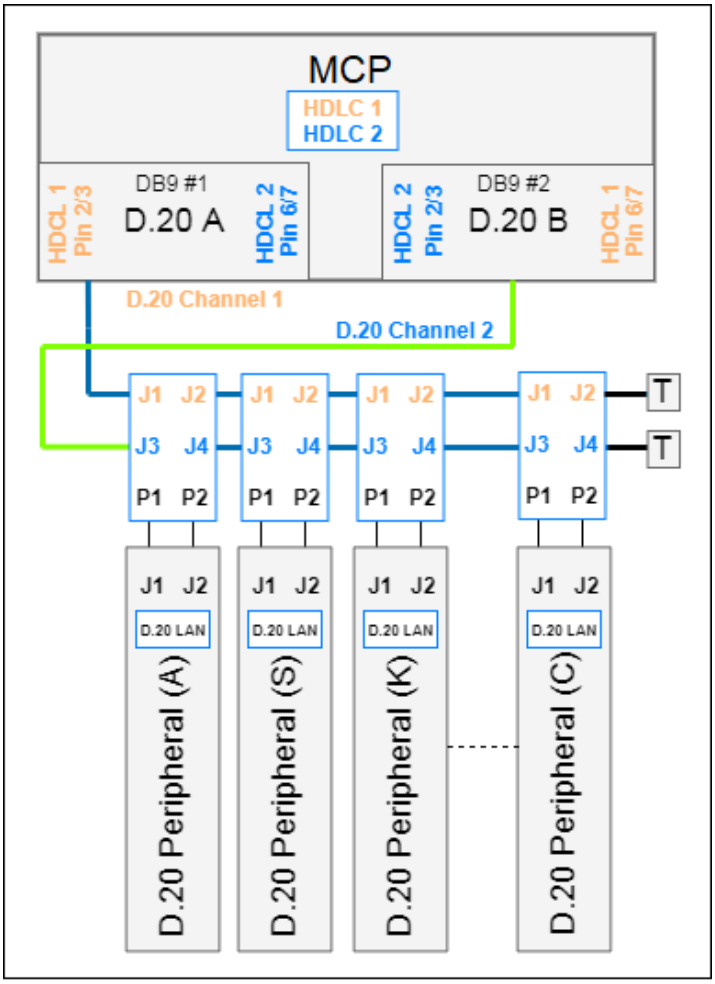
The last D.20 peripheral must be terminated with D.20 terminator (GE part#: 977-0049).

Table 17: Single D.20 link, redundant LAN - Default settings

Function	State
End of Link - D.20 Channel 1	ON
End of Link - D.20 Channel 2	ON
Port B - D.20 Channel 1 (pin 6/7)	OFF
Port B - D.20 Channel 2 (pin 2/3)	OFF

Redundant D.20 link, redundant LAN

Figure 7: Redundant D.20 link, redundant LAN - Topology



D.20 redundant LAN daughter card (GE part#: 540-0209 for D.20C and GE part#: 540-0207 for D.20A,S,K) must be installed.

D.20 link adapter must be installed on each D.20 peripheral (GE part#: 540-0313)

The D.20 Link crossover cable must be installed from CCU D.20 Port B to peripheral link (GE part#: 977-0561)

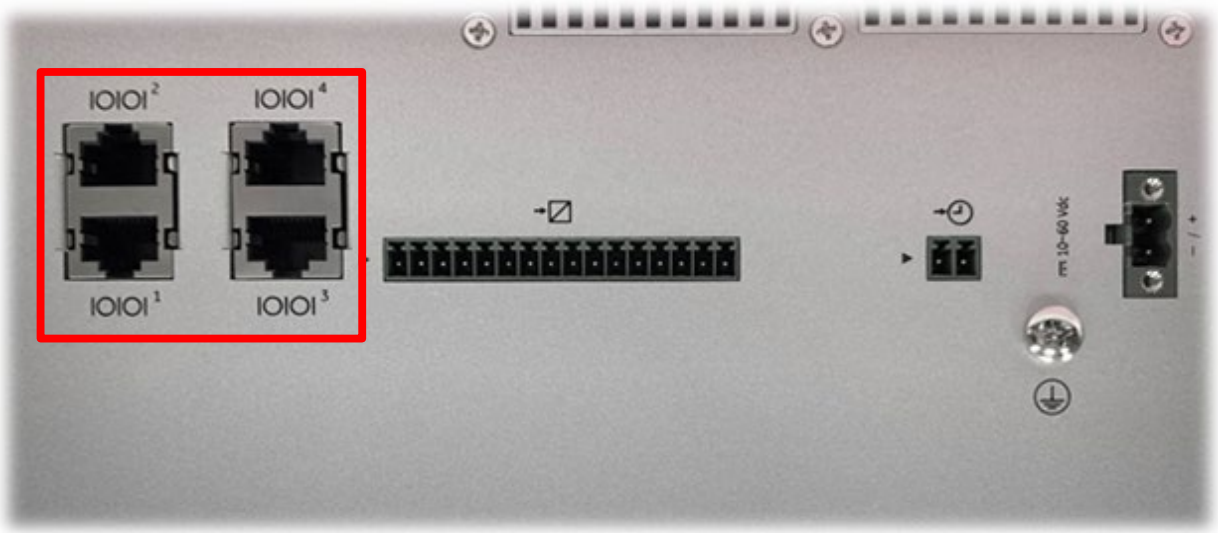
The last D.20 peripheral must be terminated with D.20 terminator (GE part#: 977-0049)

Table 18: Redundant D.20 link, redundant LAN - Default settings

Function	State
End of Link - D.20 Channel 1	ON
End of Link - D.20 Channel 2	ON
Port B - D.20 Channel 1 (pin 6/7)	ON
Port B - D.20 Channel 2 (pin 2/3)	ON

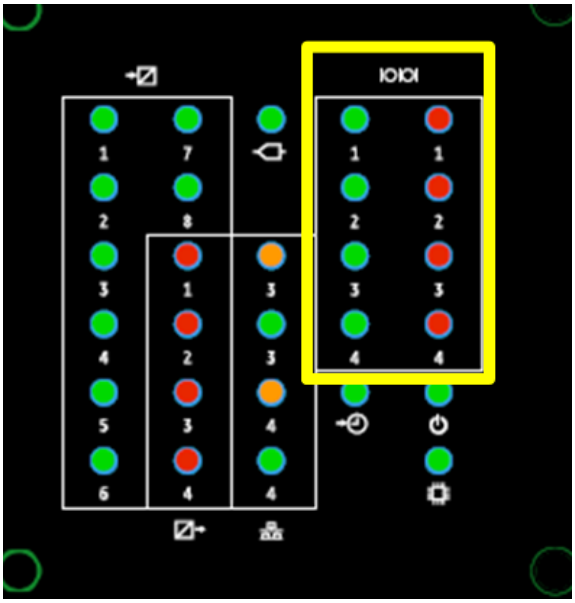
Serial ports (RS232/485, RJ45, labelled 1-4)

The G100 has 4 Built-in Serial ports available as RJ45 connectors on the bottom panel of the unit.



Each serial port has LED activity (Tx/Rx) indicators on the front panel:

- Tx Activity (Green)
- Rx Activity (Red)



The serial ports are isolated from the rest of the system at 1.5KV AC / 2.1KV DC.

The serial ports support the following communication modes:

- RS232
- RS485 2-Wire

For every port an Rx Termination Resistor of 120 Ohms can be enabled through the software interface.

The pin assignment of the Serial Interfaces is dependent on the operation mode selected for the interface:

Table 19: RJ45 Pin outs for Serial Port Signals

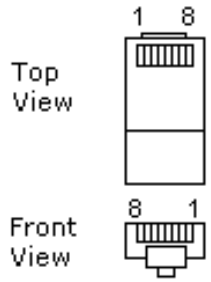
EIA568	TIA/EIA 568A	RJ45 Pin out	RS232	RS485 2-Wire
		1	Rx	D-
		2	CTS	D+
		3	Tx	-
		4	GND	GND
		5	IRIG-B OUT	IRIG-B OUT
		6	RTS	-
		7	-	-
		8	DCD	-

NOTE

IRIG-B OUT is available only when an IRIG-B IN signal is connected. The G100 does not have an internal IRIG-B signal generator.

The supported levels are compliant to TTL by a load of 120Ohm or higher. It is current limited and protected against damage by short to GND (Pin 4).

Figure 8: Modular connector 8P8C (RJ45) pins



Shielded twisted pair cables shall be used for wiring.

RS-485 Serial Connections

The G100 can be configured to communicate with RS-232 or RS-485 2-wire type devices using the 4 Built-in Serial Ports.

Each serial port can be independently configured through the Settings GUI. All port configurations persist through a power cycle and when power is lost.

In RS-485 mode End of Link Termination (120 Ohm) can be enabled through the Settings GUI.

NOTE

When enabled in Settings, End of Link Termination is active only when the device is powered on and applications are running. This has no operational impact because the G100 is meant to act as a master to other devices

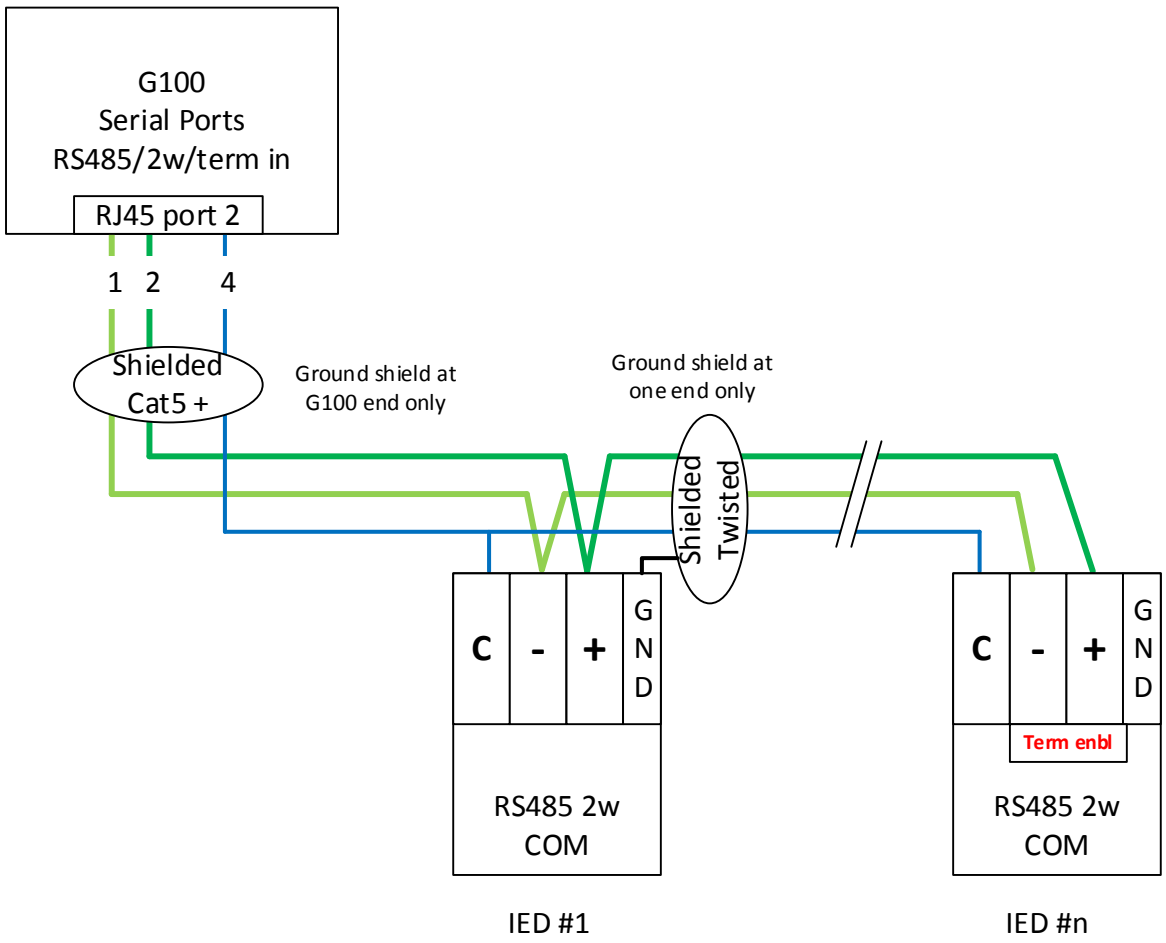
The cables must be shielded and the shield of each RS-485 cable section should be grounded at one end only. This prevents circulating currents and can reduce surge-induced current on long communication lines.

Signal ground on pin4 is to be considered different then shield on cable.

When creating custom cables, it is recommended to only wire the required pins.

The following diagram illustrates how to wire the G100 units using RS485 2-wire.

Figure 9: G100 connection using RS485 2-wire



Default Serial Maintenance port (port 4, RS232)

When running the *Factory Default* configuration, G100 has one serial maintenance port enabled, which is **always allocated to Port 4**.

This maintenance port allows users to perform the following workflows:

- Intercept POST and access UEFI settings (useful when a KVM is not connected to G100)
- Access Shell for maintenance actions after the applications started

The following documents provide details for each workflow:

- Configuring UEFI Settings on G100 User Guide (SWM0122)
- G100 Substation Gateway Quick Start Guide (SWM0116)
- MCP Substation Gateway Software Configuration Guide (SWM0101)

NOTICE

While the serial maintenance port is enabled as #4, this same port cannot be used for other applications.

The serial maintenance port can be disabled as following:

- In UEFI for the POST access only. Make sure that UEFI is set to RS232.
- In Settings for Shell access and use by other runtime applications.

If the serial maintenance port is disabled, users can still access the device using either the KVM or Ethernet ports.

UEFI allocation of the serial maintenance port is intended for UEFI access in absence of KVM (during startup), and it is different than Settings serial maintenance port "shell" access (during normal operation).

NOTICE

If the serial maintenance port was disabled, and the IP addresses are not known – then access can be done using KVM.

NOTICE

Do not change maintenance port assignment in UEFI from port # 4 !

Ethernet ports

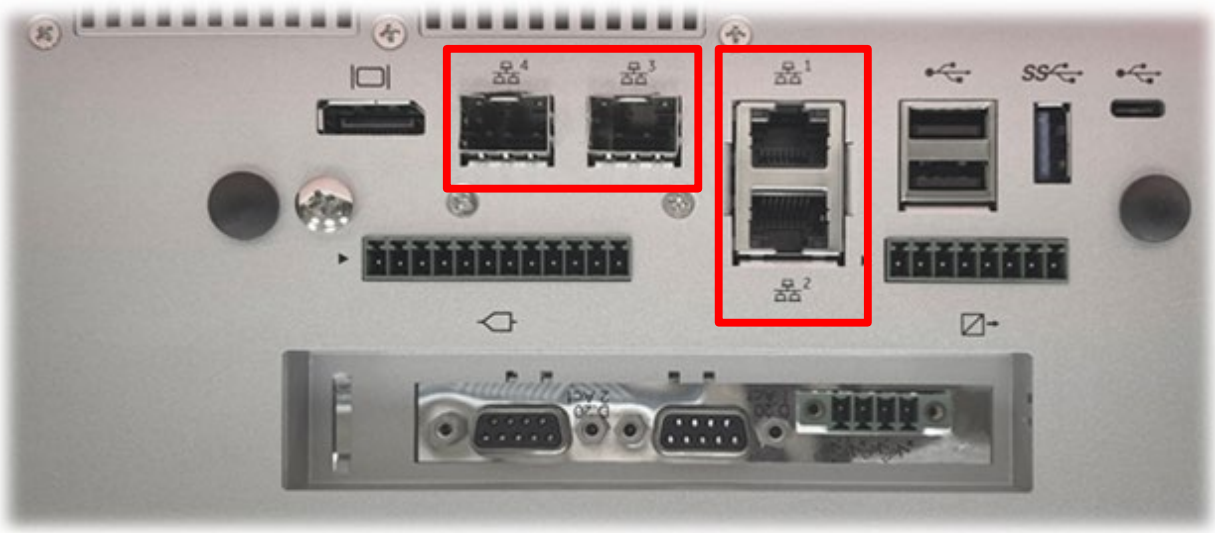
The top panel of the G100 provides 4 independent Ethernet ports, labelled 1 to 4.

NOTICE

The G100 Ethernet ports use separate MAC addresses.

The G100 Ethernet ports cannot be configured as Redundant Single MAC.

G100 does not support PRP (Parallel Redundancy Protocol IEC62439-3).



TP Ethernet ports and LED indications (labelled 1, 2)

Ports 1 and 2 are RJ45 Copper (RJ45 10/100/1000BASE-TX) with separate NICs (LAN1/2).

Each RJ45 port has LED indicators inside the RJ45 connector:

- Activity (Green)
- Link (Orange)

Each RJ45 port is isolated to 1.5KV AC / 2.1KV DC

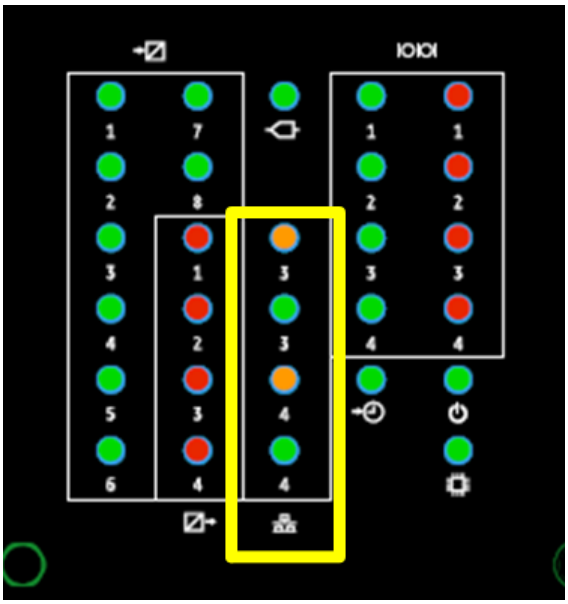
SFP Ethernet ports (labelled 3, 4)

Ports 3 and 4 are SFP with separate NICs (LAN3/4).

Into each slot an SFP module can be inserted.

Each SFP port has LED indicators on the front panel:

- Activity (Green)
- Link (Orange)



Each SFP port is isolated to 1.5KV AC / 2.1KV DC

For corresponding SFP modules and order codes see following sections in this document:

Order Code

Spares and Accessories

The following table presents in detail the SFP modules supported by the G100.

Table 20: SFP modules supported by the G100

Item	Description	Manufacturer	Mfg Part
580-3784	SFP Module 100BASE-FX LC TRANSCEIVER OPTICAL	AVAGO	HFBR-57E0APZ
580-3785	SFP Module 1000BASE-SX LC TRANSCEIVER OPTICAL	AVAGO	AFBR-5710ALZ
		FINISAR	FTLF8519P3BTL
580-3786	SFP Module 1000BASE-TX RJ45 TRANSCEIVER COPPER	FINISAR	FCLF8522P2BTL
		FOXCONN	ABCU-5730ARZ
		FOXCONN	ABCU-5731ARZ
0123-0004	SFP Module 10/100BASE-TX RJ45 TRANSCEIVER COPPER	AXCEN	AXFE-R1S4-05H3
580-3787	SFP Module 1000Base-LX LC TRANSCEIVER OPTICAL SINGLE-MODE 5km 1310nm -40 to 85C	FOXCONN (AVAGO)	AFCT-5715ALZ

The cables required to make physical connections to the G100 are as follows:

Table 21: Ethernet cables required by the G100

Media	Designation	Cable	Connector
Twisted Pair Ethernet	100/1000BASE-TX	UTP (Unshielded Twisted Pair) – Cat-5 or better	RJ45
Fiber optic	100BASE-FX	Fiber optic cable multimode	LC
Fiber optic	1000BASE-SX	Fiber optic cable multimode	LC

⚠CAUTION This product contains components rated as Class 1 Laser Products.

NOTE

G100 cannot read the SFP model automatically. Each SFP Ethernet port must be configured correctly to match the installed SFP type, in the Settings utilities (***mcpcfg, Settings GUI***) – please see the *G100 Quick Start Guide* and *MCP Software Configuration Guide* documents.

A device reboot is required for new SFP settings to take effect.

Time synchronization IRIG-B input (2 pin connector)

The bottom panel of the unit provides one IRIG-B input connector.

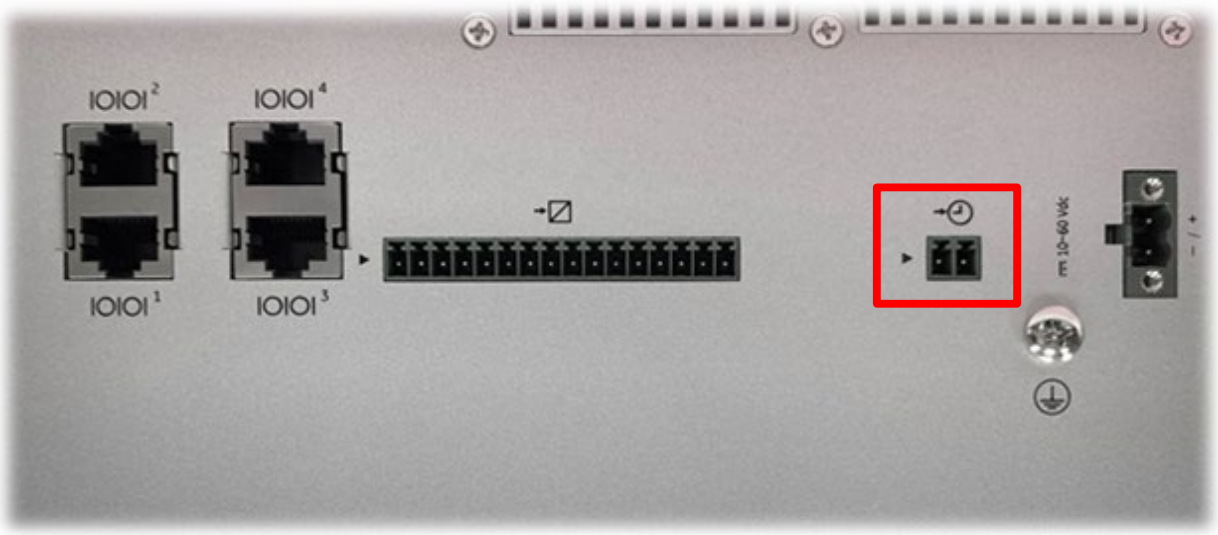
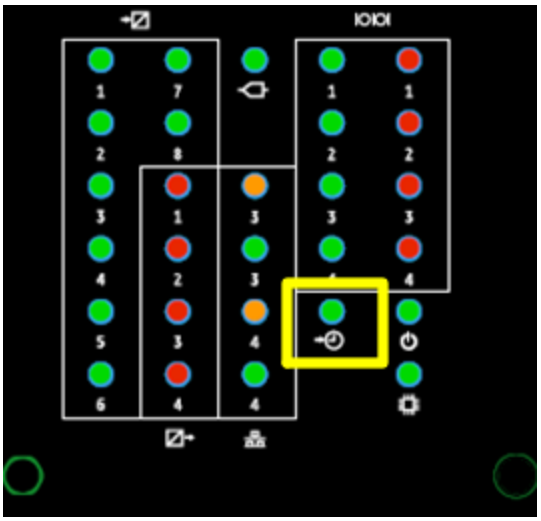


Table 22: IRIG-B input connector pin assignments

PIN NO.	DESCRIPTION
1 (arrow)	SIGNAL
2	GND

This input can be used to synchronize the precision timer of the unit. The supported IRIG-B formats are B002 and B006.

Presence of an IRIG-B signal is indicated by one LED located on the front panel:



When configured as B006 the clock requires a corresponding configuration where the year and quality are included in the IRIG-B signal. If the clock is not configured to provide the year the G100 will show the year 2000.

This Port is isolated from the rest of system with an isolation voltage of 1.5kV AC / 2.1kV DC.

The supported levels are compliant to TTL or TIA232, selectable by an internal jumper:

Green PIN HEADER 1x3 Male 180° 2.0mm DIP

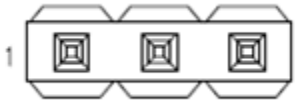


Table 23: IRIG-B input signal selection TTL/RS-232

Jumper JIRIGB1	DESCRIPTION
1-2	TTL
2-3	RS232

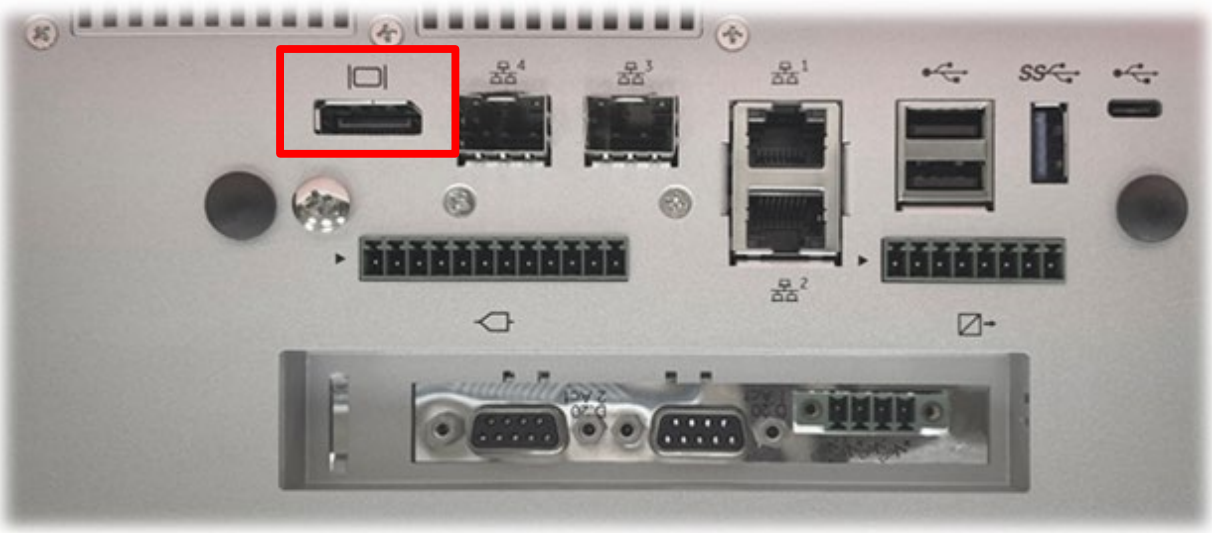
NOTICE

G100 does not support PTP IEEE1588.

NTP and SNTP are supported.

DP Display Port

The top panel of the unit provides one DisplayPort™ connector.



The interface is DisplayPort™ Version 1.2 and DP++ compliant which is used mainly to enable installation personnel to connect a display for the initial configuration of the device, or a Local Runtime HMI display.

NOTE Multi Stream Transport (MST) for multiple attached displays is not supported.

The DisplayPort™ is fused internally. For normal operation don't exceed 0.5 A.

Users are recommended to use passive DP++ to HDMI and passive DP++ to DVI-D. Use of active adapters is not encouraged as they limit higher frequency refresh rates, and limit display sizes.

NOTE G100 doesn't support Touch Screen Panel controls due to the absence of external vendor USB drivers. It's recommended to use a Windows Panel PC and the Remote HMI application instead.

USB ports

The top panel of the unit provides the following USB ports:

One USB 3.0 type A connector, mainly used to enable maintenance personnel to connect their equipment and storage devices for software updates.

The USB 3.0 A port is fused internally. For normal operation don't exceed 0.9 A per connector.

The maximum cable length for USB 3.0 cables is 3m (=118in).

Using longer cables than specified for each port might result in data loss.

Two USB 2.0 Type A connectors. Main purpose of these connectors is to enable installation personnel to connect Mouse, Keyboard and equivalent equipment for initial configuration of the device.

Each USB 2.0 A connector is fused separately. For normal operation don't exceed 0.9 A per connector. The cumulative current draw of all four ports is limited to 1A due to thermal and power budget restrictions.

The maximum cable length for USB 2.0 cables is 3m (=118in).

The USB Type C connector is for future applications, currently not used. Please do not connect external devices to it.

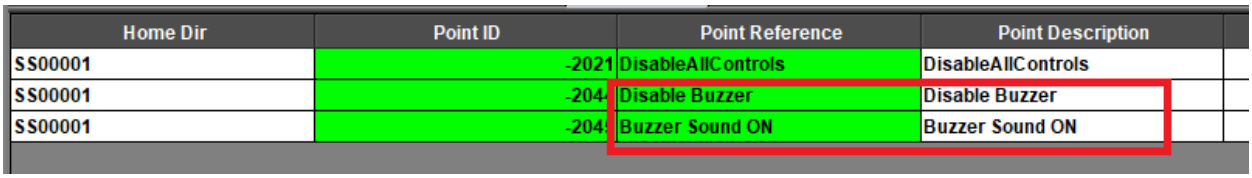
Internal Buzzer

The G100 has an internal buzzer, which is intended for local and close proximity general purpose usage.

NOTE

This buzzer has a very low volume and as such is not suitable for critical operators' notifications.

The Local HMI and the DO points in the database can operate the buzzer, subject to above note on low sound level.



Home Dir	Point ID	Point Reference	Point Description
SS00001	-2021	DisableAllControls	DisableAllControls
SS00001	-204	Disable Buzzer	Disable Buzzer
SS00001	-204	Buzzer Sound ON	Buzzer Sound ON

Chapter 5 - Specifications

G100 Product Specifications

System

Processor	Intel Atom X5-E3930 1.3GHz Processor
Memory	8GB SoDIMM 204 pin DDR3L (up to 1866MHz)
Storage	16GB mSATA SSD
Real Time Clock (RTC)	When powered off, the real-time clock remains active for 5 days
Operating system	Predix Edge OS (Kernel 4.14)
LED indicators	Power indicator, CPU Status indicator, IRIG-B Input indicators, 2x SFP Ethernet port indicators, 2x TP Ethernet port indicators, 4X Serial port indicators, 8x DI channel indicator, 4x DO channel indicator, AI sampling indicator

Communications

Ethernet connections	2 RJ45 Ethernet ports + 2 SFP modules 1000BASE-LX 850nm 5km (LC fiber single-mode) 100BASE-FX 1300nm 2km (LC fiber single-mode) 100BASE-FX 1300nm 15km (LC fiber single-mode) 100/1000BASE-TX (RJ45 copper medium, Cat-5 or better) 100BASE-FX (LC fiber multimode) 1000BASE-SX (LC fiber multimode)
Serial communications	4x serial interfaces accessible via individual RJ45 connectors Serial interfaces use 16550 compatible UART. Support baud rates 300, 600, 1200, 2400, 4800, 9600, ... 921k. Software controlled mode of operation between RS232 or RS485 2-wire. Software controlled termination resistor (120 ohm) for RS485 mode (termination is not active while powered off). All software selection persist when power cycled. IRIG-B available on all serial interfaces.

D.20 Link HDLC Communications	A dual channel card is available to communicate D.20 Link protocol to up 60 D20 Peripherals per channel. Each channel communicates at 250kbps. Channels are isolated from each and from other internal circuits.
Time synchronization	IRIG-B (TTL) Input Connector available as 2 positions removable Phoenix terminal block on bottom panel
Video Output	DisplayPort (DP) version 1.2 available on top panel
USB Ports	1x USB 3.0 Type A (male) on top panel 2x USB 2.0 Type A (male) on top panel 1x USB 2.0 Type C (male) on top panel (Future use)

Electrical

G100 rated input	Nominal 12/24/48 VDC ±10%, 5A/2.5A/1.25A Minimum/Maximum DC voltage: 10 VDC to 60 VDC
GPIO (DI/DO/AI)	Isolation rating: $820V_{RMS}/1150V_{DC}$

G100 Environmental Specifications

Temperature and Humidity

Storage	-40°C to 85°C
Operating Conditions	-40°C to 70°C
Humidity	5%~90% relative humidity, non-condensing

Ingress Protection (IEC 60529)

IP40 (protected from most wires and slender screwstools greater than 1 millimeter).

Mechanical Specifications

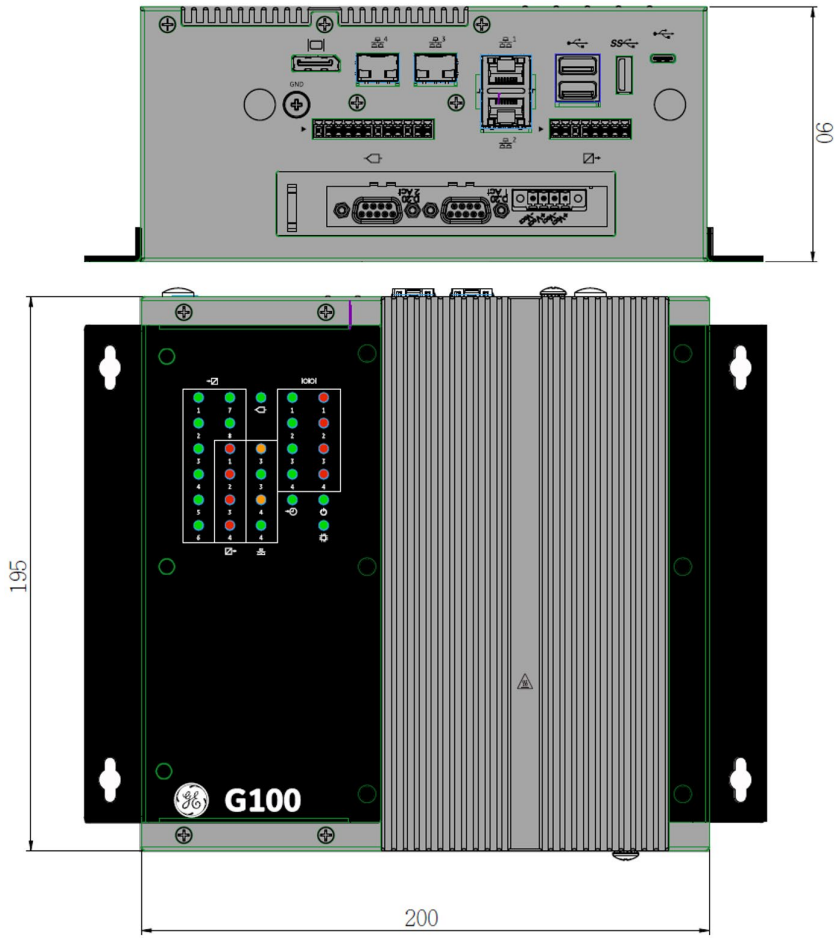
Weight

Part	Weight in kg
G100	2.47
D.20 Link HDLC PCIe Card	0.18
Packaging + accessories	2.15

Dimensions

All dimensions are in mm

200 (L) x 90(W) x 195(H) mm



Storage recommendations

Storage conditions

Always store the G100 in an environment compatible with operating conditions. Recommended environmental conditions for storage are:

- Temperature: -40°C to +85°C
- Relative humidity: 5% to 95%, non-condensing

Exposure to excessive temperature or other extreme environmental conditions might cause damage and/or unreliable operation.

To avoid deterioration and early failure of electrolytic capacitors, power up units that are stored in a de-energized state once every 12 months, for one hour continuously.

Chapter 6 - Removing the G100 from Service

Before you begin installing and using the G100, review the information in this chapter, including the following topics:

When the G100 is to be removed from service, it is necessary to:

- Remove the configuration data and sensitive information from:
  - The G100
  - The PC used to remotely configure the G100
- Dispose of the equipment.

Remove configuration data and sensitive information from the G100

In the event that it is necessary to remove the configuration data and sensitive information from the G100 (for example, the G100 is being disposed of or being returned for maintenance [i.e., RMA]), this chapter provides the data removal procedure.

For additional information, please refer to "SWM0123 G100 Secure Deployment User Guide".

To remove configuration data and sensitive information from the G100:

1. For an RMA: GE recommends restoring the unit to factory default state using the procedure in Section3 of TN0116 MCP Firmware Upgrade and Restore to Defaults Workflows.
2. For hardware decommissioning and disposal: GE recommends that you destroy the device as per NIST* recommendations.

* Publication 800-88 Revision 1. Guidelines for Media Sanitization, Recommendations of the National Institute of Standards and Technology:

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

Removing configuration data on a PC

When a PC application is used to configure the G100, configuration data resides on the data storage media (e.g., hard drives, memory cards, etc.) of the PC running the configuration application.

The G100 configuration data can be removed from the PC by either:

- Recommended: Physically removing and destroying the data storage media, or
- Using a program to securely wipe (that is, completely erase) the data storage media (that is, not just reformat or remove the names of the files from the file allocation table).

Appendix A – Standards & Compliance

Compliance Standards

The G100 complies with the tests listed below.

Standard	Description	Test Level / Class	Pass Criteria
IEEE 1613	IEEE Standard Environmental and Testing Requirements for Communications Networking Devices Installed in Electric Power Substations	Per standard	
IEC 61850-3	Communication Networks and systems for power Utility Automation-Part 3	Per standard	
IEC 62368-1	Audio/Video, Information And Communication Technology Equipment - Part 1: Safety Requirements	Per standard	
IEC 60068-2-1	Cold	-40°C for 16hours	A
	Cold start	1hour soak, 3 power ups every 10 mins	A
IEC 60068-2-2	Dry Heat	+70°C for 16hours	A
	Hot start	1hour soak, 3 power ups every 10 mins	A
IEC 60068-2-78	Damp Heat, steady-state	+40°C, 95%RH, non-condensing, 96hours	A
IEC 60068-2-6 IEC 60255-21-1	Vibration (sinusoidal)	0.5g, 1 sweep, 3 axes, with EUT energized 1g, 10 sweep, 3 axes, with EUT non-energized	A
IEC 60068-2-27	Shock Response Shock Withstand	5g, 3 +/- shocks, 3 axes, with EUT energized. 15g, 3 +/- shocks, 3 axes, with EUT non-energized.	A
IEC 60068-2-27	Bump (Non-operating test)	10g, 1k bumps, 6 axes, with EUT non-energized.	No damage, functions
IEC 60068-2-31	Drop & Topple	100mm non-energized	No damage, functions
IEC 60255-21-3	Seismic	1-35Hz; X axis: 7.5mm, 2g; Y axis: 3.5mm, 1g	A
EN 60255-27	Product safety requirements: information technology equipment	Impulse: 1/5kV$_{PEAK}$ Dielectric: 820V$_{RMS}$/1150V$_{DC}$ Insulation Resistance: >100MΩ	No damage, breakdown or flashover
CISPR22	Radiated RF Emission Conducted Emission	Radiated Emissions: 30 MHz to 6 GHz NA	Class A

IEC 61000-4-2 IEEE C37.90.3	Immunity to Electrostatic Discharge	8kV - Contact/15kV – Air	A
IEC 61000-4-3 IEEE C37.90.2	Immunity to Radiated RF	80 MHz- 3 GHz @ 10V/m (35V/m)	A
IEC 61000-4-4 IEEE C37.90.1	Immunity to Fast Transient Burst	4kV/5kHz	A/B
IEC 61000-4-5 IEEE 1613	Immunity to Surge	Power and Signal ports: 4/2/1/0.5kV	A/B
IEC 61000-4-6	Immunity to Conducted RF	10Vrms/150kHz-80MHz	A
IEC 61000-4-18 IEEE C37.90.1	Immunity to Damped Oscillatory	2.5kV/1MHz	A/B
IEC 61000-4-8	Immunity to Power Magnetic Field	100A/m @ 180s 1000A/m @ 3s	A
IEC 61000-4-11	Immunity to Voltage Dip and Interrupt	100% @ 5, 10-200msec (10msec increments)	A
IEC 61000-4-16	Immunity to Conducted CM Disturbances (DC-150kHz)	30Vrms & 300Vrms	A/B
IEC 61000-4-17	Ripple on DC power supply	10% AC ripple on DC Power Port	A
IEC 61000-4-29	Dip and Interrupt on DC power supply	Voltage Dips: 40%/70% for 0.01 sec Interruptions: 0% for 0.01 sec Variations: 85% to 120% for 10 sec	A

Appendix B – Warranty

Warranty

For products shipped as of October 1st, 2013, G100 warrants most of its GE manufactured products for 10 years. For warranty details including any limitations and disclaimers, see the GE Grid Solutions Terms and Conditions at:

https://www.gegridsolutions.com/multilin/warranty.htm

Appendix C – Glossary of terms used in this document

D

DP: Display Port

G

GUI: Graphical User Interface (also called Human Machine Interface – HMI)

GW / GTW: Gateway (in Substation Automation context)

H

HMI: Human Machine Interface (also called Graphical User Interface – GUI)

HMI Client: Client-side functionality that resides in the user's browser

HMI Server: Server-side functionality that resides on the G100 and provides services to the client-side browsers

HTTP: HyperText Transfer Protocol

HTTPS: Designated the use of HTTP but with a different default port and an additional encryption/authentication layer between HTTP and TCP

I

IED: Intelligent Electronic Device

IP: Internet Protocol

IRIG-B: Inter Range Instrumentation Group (IRIG) - an American standardized network time code format

L

LAN: Local Area Network

M

MAC: Media Access Control

MCP: Multifunction Controller Platform

N

NIC: Network Interface Card

NTP: Network Time Protocol

NVRAM: Non-Volatile Random Access Memory

P

P: Power

PRP: Parallel Redundancy Protocol

PTP: Precision Time Protocol

R

RTC: Real-time clock

S

SCADA: Supervisory Control And Data Acquisition

SNTP: Simple Network Time Protocol

SSH: Secure Shell

T

TCP: Transmission Control Protocol

U

UR: Universal Relay

URL: Universal Resource Locator

Modification Record

Version	Revision	Date	Change Description
1.00	0	25th May, 2021	Initial release.
1.00	1	5th July, 2021	Updated GPIO DO types and Compliance standards

GE

Grid Solutions

G100 Firmware Release Notes

Firmware Release Notes

MIS-0115

Version 2.30 Revision 1

GE Information

imagination at work

COPYRIGHT NOTICE

© 2021, General Electric Company. All rights reserved.

The information contained in this online publication is the exclusive property of General Electric Company, except as otherwise indicated. You may view, copy and print documents and graphics incorporated in this online publication (the "Documents") subject to the following: (1) the Documents may be used solely for personal, informational, non-commercial purposes; (2) the Documents may not be modified or altered in any way; and (3) General Electric Company withholds permission for making the Documents or any portion thereof accessible via the internet. Except as expressly provided herein, you may not use, copy, print, display, reproduce, publish, license, post, transmit or distribute the Documents in whole or in part without the prior written permission of General Electric Company.

The information contained in this online publication is proprietary and subject to change without notice. The software described in this online publication is supplied under license and may be used or copied only in accordance with the terms of such license.

TRADEMARK NOTICES

GE and are trademarks and service marks of General Electric Company.

* Trademarks of General Electric Company.

IEC is a registered trademark of Commission Electrotechnique Internationale. IEEE is a registered trademark of the Institute of Electrical and Electronics Engineers, Inc. Internet Explorer, Microsoft, and Windows are registered trademarks of Microsoft Corporation.

Other company or product names mentioned in this document may be trademarks or registered trademarks of their respective companies.

This printed manual is recyclable.

Please return for recycling where facilities exist.

Contents

COPYRIGHT NOTICE 2

TRADEMARK NOTICES 2

About this Document 5

Purpose 5
Intended Audience 5
Additional Documentation 5
Product Support 5
GE Grid Solutions Web Site 5
GE Technical Support Library 5
Contact Technical Support 6

1. Version 2.20 (19-May-2021) 7

Software Versions 7
Predix Edge OS and Other Firmware Versions 7
Key Functions and Changes 7
1.1 Enhancements 8
1.2 Fixed Defects 8
1.3 Known Issues 8
1.3.1 Cyber Security 8
1.3.2 Clients 8
1.3.3 Servers 9
1.3.4 Automation 9
1.3.5 Configuration/Settings 10
1.3.6 HMI 10
1.3.7 Pass-through 10
1.3.8 System 10
1.3.9 Documentation 10
1.3.10 Hardware 11
Capability and Capacity 11
1.4 Standalone (non-redundant) 11
1.4.1 Performance Test Levels 11
1.4.2 Performance Test Results 12
1.4.3 HMI Response times 13
1.5 Redundancy 13
Time Sync Accuracy (IRIG-B/NTP) 13
Application List 13

2. Version 2.30 (29-July-2021) 16

Software Versions 16
Predix Edge OS and Other Firmware Versions 16
Key Functions and Changes 16
2.1 Enhancements 17
2.1.1 Cyber Security 17
2.1.2 Clients 17

2.1.3 Servers....17
2.1.4 Automation....18
2.1.5 Configuration/Settings....18
2.1.6 HMI....18
2.1.7 Pass-through....18
2.1.8 System....18
2.1.9 Documentation....18
2.1.10 Hardware....18
2.2 Fixed defects....18
2.2.1 Cyber Security....18
2.2.2 Clients....18
2.2.3 Servers....19
2.2.4 Automation....19
2.2.5 Configuration/Settings....19
2.2.6 HMI....19
2.2.7 Pass-through....19
2.2.8 System....19
2.2.9 Documentation....20
2.2.10 Hardware....20
2.3 Known Issues....20
2.3.1 Cyber Security....20
2.3.2 Clients....20
2.3.3 Servers....20
2.3.4 Automation....21
2.3.5 Configuration/Settings....21
2.3.6 HMI....22
2.3.7 Pass-through....22
2.3.8 System....22
2.3.9 Documentation....22
2.3.10 Hardware....22
Capability and Capacity....22
2.4 Standalone (non-redundant)....23
2.4.1 Performance Test Levels....23
2.4.2 Performance Test Results....24
2.4.3 HMI Response times....24
2.5 Redundancy....24
Time Sync Accuracy (IRIG-B/NTP)....24
Application List....25
MODIFICATION RECORD....27

About this Document

Purpose

The purpose of this document is to outline features, capabilities and issues known to exist within the G100 Substation Gateway at the time of release.

As part of the MCP Family of Gateway products, G100 applications are shared with the G500 product.

Intended Audience

This document is an external document intended for both GE Staff and Customers. It highlights the features and capabilities of the G100 firmware.

Additional Documentation

For further information about the G100, refer to the following documents:

- *G100 Quick Start Guide (SWM0116)*
- *G100 Substation Gateway Instruction Manual (994-0155)*
- *MCP Software Configuration Guide (SWM0101)*
- *Configuring UEFI Settings on G100 User Guide (SWM0122)*

Product Support

If you need help with any aspect of your GE Grid Solutions product, you can:

- Access the GE Grid Solutions Web site
- Search the GE Technical Support library
- Contact Technical Support

GE Grid Solutions Web Site

The GE Grid Solutions Web site provides fast access to technical information, such as manuals, release notes and knowledge base topics.

Visit us on the Web at: http://www.gegridsolutions.com

GE Technical Support Library

This site serves as a document repository for post-sales requests. To get access to the Technical Support Web site, go to: http://sc.ge.com/*SASTechSupport

Contact Technical Support

For help with any aspect of your GE Grid Solutions product, please contact our support team, 24/7, as follows:

Region	E-mail	Telephone
Global Contact Centre	ga.support@ge.com	+44 1785 250070
Central and East Asia andPacific	ga.supportCEAP@ge.com	+61 414 730 964
India	ga.supportIND@ge.com	+91 44 22648000
Middle East, North Africa andTurkey	ga.supportMENAT@ge.com	+971 42929467
Europe, Russia, CIS and Sub-Saharan Africa	ga.supportERCIS@ge.com	+34 94 4858854
North America	ga.supportNAM@ge.com	+1 877 605 6777
Latin America	ga.supportLAM@ge.com	+55 11 36187308

1. Version 2.20 (19-May-2021)

Software Versions

The first release of the G100 product is based on, and has common features with G500 version 2.10, adapted to the smaller form factor platform.

The following defines the software versions required for interaction with the G100.

Package	Version	Notes
G100 Firmware	2.2.291	G100 Firmware Version.
DS Agile MCP Studio	2.3.0	Supported DS Agile MCP Studio Software.
G100 HMI Viewer	2.2.291	Supported G100 HMI 64-bit Software.

Predix Edge OS and Other Firmware Versions

The following defines the firmware versions supported for Predix Edge Linux OS and UEFI in the G100 v2.2.291.

Package/Firmware	Version	Notes
Predix Edge OS	2.5.0	Supported GE's Secured Linux Operating System Version.
UEFI	FLEBG100A00006T010	Supported UEFI Version of G100.

Key Functions and Changes

G100 is part of the Multi-Function Controller Platform (MCP) family, together with G500.

The main differences between G500 and G100 are in capability, capacity, redundancy and time synchronization methods.

G100 is designed to provide a reliable and accurate collection of data (metering, status, events and faults) from serial or LAN based intelligent substation devices to master applications such as SCADA, EMS, DMS or other enterprise applications. With its modern and robust cyber security features, the G100 is designed for smooth integration into NERC CIP and Cyber Security environments while consolidating functions such as ethernet communications, time synchronization, HMI and SCADA applications.

G100 supports the following key features as part of v2.20.

Advanced Gateway : G100 collects operational and non-operational data from substation protection, control, monitoring, RTU, and intelligent devices, pre-processes the data and moves it up to EMS and DMS SCADA systems providing centralized substation management.

Advanced Automation : G100 provides the computing platform necessary to automate substation procedures, such that intricate processes are carried out safely and efficiently by creating advanced custom automation programs using IEC 61131 compliant tools and perform basic math functions on data points using the built-in calculator tool.

Datalogging and Alarm Management : G100 supports logging of analog and binary events, including alarm management. Users have access to view and extract logged data via Runtime HMI corresponding screens (Trending, SOE, Historical Data, Active Alarms).

Automated Records (files) Retrieval and Management (ARRM)	:	G100 supports automated extraction of data files from IEDs, such as digital fault recording (DFR) records, event files, device information files, etc. Acquired files can be securely pushed automatically to remote systems.
Secure Passthrough Remote Access and VPN	:	G100 allows users to securely access substation devices from remote locations through validated interactive sessions hosted by the G500.
User Authentication	:	G100 provides Role Based Access Control (RBAC) with Local Account Authentication.
Runtime HMI	:	G100 provides user interaction with Role Based Access Control via a portable Runtime HMI application that runs in the Local unit KVM interface, as well as Remote in Windows based computers. There is no requirement to install Java/JRE on the Windows computers.
Support for Predix Edge Connectivity	:	G100 uses GE's Hardened *Predix EDGE* Operating System (Linux Yocto based) and supports secured connectivity for enrolling the unit into Predix Edge Manager. Predix Edge Manager is a GE hosted Cloud application that provides asset / fleet management of enrolled devices.

1.1 Enhancements

N/A - This G100 version is the first release of G100.

1.2 Fixed Defects

N/A - This G100 version is the first release of G100.

1.3 Known Issues

This G100 version inherits some known issues from G500 v2.10.

1.3.1 Cyber Security

Please refer to Product & Cyber Security Advisories on the GE Grid Solutions web site.

1.3.2 Clients

GE Internal Reference #	Description
D-12697	The value of GPIO Digital Point (DO) is always set to '1' even after completion of PULSE command in GPIO client. However, the functionality of DO command in GPIO client is working as per the control configuration i.e., PULSE ON period followed by PULSE OFF period, however the DO value in HMI still set as "1" only.
B-13475 D-09915	SEL Binary Client doesn't support Double Precision Scaling Factors.

GE Internal Reference #	Description
D-05002	ARRM file retrieval from SEL 1xx/2xx relays (using GENASCII) is not possible.

1.3.3 Servers

GE Internal Reference #	Description
D-12567	The time sync accuracy of G100 when IEC101 Server (Unbalanced/Balanced) is used as a time sync source is > +/- 4 msec.
B-11967	No support for events in NVRAM in IEC101/104 Server. Events that have not been yet transmitted to Master (Clients) are lost if G100 is power cycled / restarted. However – the integrity polls will continue to provide accurate database representation.
B-11968	No support for events in NVRAM in DNP3 Server. Events that have not been yet transmitted to Master (Clients) are lost if G100 is power cycled / restarted. However – the integrity polls will continue to provide accurate database representation.

1.3.4 Automation

GE Internal Reference #	Description
D-05033	Suppressed quality through Input Point Suppression (IPS) application is not reported to Masters. DNP3 and IEC 101-104 Servers send Online Quality rather than the substituted/last reported quality when points are suppressed.
D-12703	Load Shedding: There is no persistency of zone assignments across power restarts when user sets the zones through Analog Setpoint commands.
B-11969	DEM is responsible for handling alarms. Events/Alarms that have not been yet committed to the SQL database are lost if G500 is power cycled / restarted. However – the integrity polls will continue to provide accurate database representation.
D-12702	The EVE/CEV file retrieval from SEL relays using either SEL Binary or GenASCII client connections are not working, when SEL relays are configured with virtual serial ports for communication.
DCSSUP-19948, D-12000	Restore the last value for variables configured in Logic Linx wizard does not work at runtime (defaults to 0 always).

1.3.5 Configuration/Settings

GE Internal Reference #	Description
D-10388	TACACS+ remote authentication can be enabled and activated even if the TACACS+ Server is not available in that moment. This will conduct to a device that can only be accessed using Emergency Access process, if TACACS+ server is not available.
D-10825	Online Editor / SNMP Agent Browser is not able to retrieve OID data if gathering data from target device takes more than 60 seconds. Workaround: configure the SNMP client offline, using OID from the end device (e.g., using a 3rd party MIB browser).

1.3.6 HMI

GE Internal Reference #	Description
B-14982	The product references in the Runtime (Local/Remote) HMI logs need to be changed as "MCP".
D-05463	If a used point group is deleted from the systemwide configuration then points belonging to that group are not visible in the point group summary. However, if user changes the point group allocation from the corresponding instantiated client map file(s) then points will be visible in the point group summary.

1.3.7 Pass-through

None

1.3.8 System

GE Internal Reference #	Description
B-14973	The software licensing application reports core license 012 as "G500 Core", it should be "MCP Core". There is no functional impact.
D-10227	Email does not send messages when an alarm is activated.
D-05714	Update of only Edge OS is not supported. If only Edge OS updates are required, the complete G100 firmware image needs to be updated.

1.3.9 Documentation

None

1.3.10 Hardware

None

Capability and Capacity

The G100 2.20 database and connectivity sizes are limited to a maximum of:

- Up to 24,000 total RTDB real data points (not counting pseudo points), originating from:
  - Up to 60 IEDs, and
  - Up to 60 D.20 IO modules
- Up to 4 concurrent Master connections
- Up to 2 Runtime HMI sessions

1.4 Standalone (non-redundant)

G100 2.20 provides the following performance capabilities in Standalone (non-redundant) Mode.

1.4.1 Performance Test Levels

The performance of G100 2.20 is tested under maximum configured system size using the activity levels and disturbance scenarios presented next.

Requirement	**Steady State** **Normal Loading**	**Avalanche** **Heavy Loading**
G100 Hardware (CPU / RAM)	2 core CPU / 8 GB RAM	2 core CPU / 8 GB RAM
Loading Signal changes (continuously/sec)	AI - 1200 DI – 12	All points changing twice in 2 secs
Number of IEDs connected to G100	60 DNP + 60 D.20 Peripherals [11 A cards, 30 C1 cards, 2 C2 cards, 14 S cards, 3 K cards]	60 DNP + 60 D.20 Peripherals [11 A cards, 30 C1 cards, 2 C2 cards, 14 S cards, 3 K cards]
G100 total RTDB Point count	24000	24000
Points / IED (400 total)	225 - AI, 125 - DI, 20 - DO, 20 - AO, 10 - ACC + D.20 points from 60 peripherals.	225 - AI, 125 - DI, 20 - DO, 20 - AO, 10 - ACC + D.20 points from 60 peripherals.
Total number of Servers & supported points in each Server	4 DI = 1875 i.e., = 125 * 60 /4	4 DI = 1875 i.e., = 125 * 60 /4

Requirement	Steady State Normal Loading	Avalanche Heavy Loading
	AI = 3375 i.e., = 225 * 60 /4 AO = 300 i.e., = 20 * 60 / 4 AO = 300 i.e., = 20 * 60 / 4 ACC = 150 i.e., = 10 * 60/ 4	AI = 3375 i.e., = 225 * 60 /4 AO = 300 i.e., = 20 * 60 / 4 AO = 300 i.e., = 20 * 60 / 4 ACC = 150 i.e., = 10 * 60/ 4
Remote G100 HMI connections	1 connection	1 connection
Local G100 HMI connections	1 connection (single monitor)	1 connection (single monitor)
Datalogger / Periodic reports	120 AI mapped / 12 reports	120 AI mapped / 12 reports
ARRM	5 sessions / IED	5 sessions / IED
Alarms	12 / sec	12 / sec (twice within 2 secs)

1.4.2 Performance Test Results

The standalone performance test results are presented below.

Table 1.1: Standalone Performance test results

Activity	Minimum	Median	Maximum
Loading Condition	Steady State Normal Loading		
CPU utilization – (%)	50	68	100
Average Memory Usage (GB)	1.151	1.225	1.316
Event latency (msecs)	161	502	2678
Control latency (msecs)	1	25	168

NOTE: Under steady state normal loading conditions, the control latency was measured by simulating one control every 5 seconds continuously from the Master station.

1.4.3 HMI Response times

G100 2.20 HMI response times under steady state normal loading conditions are presented below.

Table 1.2: User Interface Response Time – Steady State Normal Loading

Activity	Minimum (seconds)	Median (seconds)	Maximum (seconds)
Screen Access (Point Summary)	0.7	1.4	2
Screen Access (Comm Summary/Connections Page)	1	2.5	4
System Logs	0.6	2.5	5
Alarm ACK Delay (Single Alarm)	1	1.5	2
DI/AI Update to Point Summary Screen	1	1	1
Datalogger	1	1.6	3

1.5 Redundancy

G100 doesn't support system/device redundancy in release 2.20.

Time Sync Accuracy (IRIG-B/NTP)

G100 supports only software based IRIG-B TTL and software based NTP Time Sync.

Time accuracy with IRIG-B TTL input is typically +/- 1ms.

Application List

The following applications are available in this released firmware version.

Application	Support in Standalone
Runtime HMI	✓ Available
One Line Viewer	✓ Available
Config GUI / Schemas	✓ Available
System Library	✓ Available
C++ System Library	✓ Available
Connection Parser	✓ Available
Calculator	✓ Available
Hardware Asset Management Application (HAMA)	✓ Limited points availability (see MCP Software Configuration Guide SWM0101)
PTP Time Sync	× Not Available
IRIG-B/NTP Time Sync (Software based)	✓ Available

Application	Support in Standalone
D.20 Client	✓ Available
GPIO Client	✓ Available
Modbus Client	✓ Available
Modbus-TCP/SSH Client	✓ Available
SEL® Binary Client	✓ Available
Analog Data Logger	✓ Available
Generic ASCII Client	✓ Available
Modbus Server	✓ Available
DNP 3.0 Server	✓ Available
DNP 3.0 Client	✓ Available
Digital Event Manager	✓ Available
Database Server	✓ Available
DNP 3.0 TCP/IP Transport Layer	✓ Available
DNP 3.0 Server Serial Transport Layer	✓ Available
DNP 3.0 DIDO	✓ Available
IEC 60870-5-101/104 Server	✓ Available
IEC 60870-5-103 Client	✓ Available
IEC 61850 Client	✓ Available
IEC 60870-5-101/104 Client	✓ Available
Event Logger	✓ Available
Real-Time Database	✓ Available
LogicLinx IEC 61131-3 Soft Logic	✓ Available
Redundancy Manager	× Not Available (Only Standalone mode is available)
System Point Manager	✓ Available
Load Shedding and Curtailment	✓ Available
Control Lockout Manager	✓ Available
Software Watchdog	✓ Available
Configuration Manager	✓ Available
IP Changer	✓ Available
MD5SUM Builder	✓ Available
System Status Manager	✓ Available
Virtual Serial Ports	✓ Available
SNMP Client	✓ Available
Automated Record Retrieval Manager	✓ Available
Software Licensing Subsystem	✓ Available

Application	Support in Standalone
Third-party components	✓ Available
Terminal Services	✓ Available
mcpcfg utility	✓ Available
E-mail Utility	✓ Available
IO Traffic Monitor	✓ Available
Firewall	✓ Available
Edge OS & Drivers	✓ Available
Secure Enterprise Connectivity	✓ Available
Genconn	✓ Available
HMI Access Manager	✓ Available
Sync Service Library	✓ Available
Sync Server Application	✓ Available
Analog Report Generator	✓ Available
OpenVPN	✓ Available

2. Version 2.30 (29-July-2021)

Software Versions

The following defines the software versions required for interaction with the G100.

Package	Version	Notes
G100 Firmware	2.3.57	G100 Firmware Version.
DS Agile MCP Studio	2.4.0	Supported DS Agile MCP Studio Software.
G100 HMI Viewer	2.3.57	Supported G100 HMI 64-bit Software.

Predix Edge OS and Other Firmware Versions

The following defines the firmware versions supported for Predix Edge Linux OS and UEFI in the G100 v2.3.57.

Package/Firmware	Version	Notes
Predix Edge OS	2.5.0	Supported GE's Secured Linux Operating System Version.
UEFI	FLEBG100A00006V107	Supported UEFI Version of G100.

Key Functions and Changes

G100 v2.30 is a maintenance release after G100 v2.20.

The *Features*, *Capability and Capacity*, *Time Synchronization* and *Applications* list in v2.30 are similar as v2.20.

G100 is part of the Multi-Function Controller Platform (MCP) family, together with G500.

The main differences between G500 and G100 are in capability, capacity, redundancy and time synchronization methods.

G100 is designed to provide a reliable and accurate collection of data (metering, status, events and faults) from serial or LAN based intelligent substation devices to master applications such as SCADA, EMS, DMS or other enterprise applications. With its modern and robust cyber security features, the G100 is designed for smooth integration into NERC CIP and Cyber Security environments while consolidating functions such as ethernet communications, time synchronization, HMI and SCADA applications.

G100 supports the following key features as part of this version:

Advanced Gateway : G100 collects operational and non-operational data from substation protection, control, monitoring, RTU, and intelligent devices, pre-processes the data and moves it up to EMS and DMS SCADA systems providing centralized substation management.

Advanced Automation : G100 provides the computing platform necessary to automate substation procedures, such that intricate processes are carried out safely and efficiently by creating advanced custom automation programs using IEC 61131 compliant tools and perform basic math functions on data points using the built-in calculator tool.

Datalogging and Alarm Management : G100 supports logging of analog and binary events, including alarm management. Users have access to view and extract logged data via Runtime HMI corresponding screens (Trending, SOE, Historical Data, Active Alarms).

Automated Records (files) Retrieval and Management (ARRM)	:	G100 supports automated extraction of data files from IEDs, such as digital fault recording (DFR) records, event files, device information files, etc. Acquired files can be securely pushed automatically to remote systems.
Secure Passthrough Remote Access and VPN	:	G100 allows users to securely access substation devices from remote locations through validated interactive sessions hosted by the G500.
User Authentication	:	G100 provides Role Based Access Control (RBAC) with Local Account Authentication.
Runtime HMI	:	G100 provides user interaction with Role Based Access Control via a portable Runtime HMI application that runs in the Local unit KVM interface, as well as Remote in Windows based computers. There is no requirement to install Java/JRE on the Windows computers.
Support for Predix Edge Connectivity	:	G100 uses GE's Hardened *Predix EDGE* Operating System (Linux Yocto based) and supports secured connectivity for enrolling the unit into Predix Edge Manager. Predix Edge Manager is a GE hosted Cloud application that provides asset / fleet management of enrolled devices.

2.1 Enhancements

This G100 version adds the following new features compared to previous version:

2.1.1 Cyber Security

None.

2.1.2 Clients

None

2.1.3 Servers

GE Internal Reference #	Description
E-04347	Added support in DNP3 DPA to assign Analog/Digital Input event change notifications through Class 0.
E-04348	Enhanced the support in DNP3DPA for incrementing the sequence number when all the application layer retries are exhausted.
E-04349	Enhanced the support in DNP3DPA for reporting local IIN flag/bit when a digital output point goes offline.
E-04350	Enhanced the support in DNP3DPA for updating the retry value of unsolicited messages based on the value of the application layer retry count.
E-04351	Added support in DNP3 DPA to increase the RTS modem control pre-transmission delay from 400ms to 2000ms.
E-04352	Added support in DNP3DPA to read the DCD status while establishing the serial connections with the SCADA Master.
E-04353	Enhanced DNP3DPA to set the G100 clock only when all other clock sources (NTP/IRIG-B) are failed.

2.1.4 Automation

None

2.1.5 Configuration/Settings

None

2.1.6 HMI

None

2.1.7 Pass-through

None

2.1.8 System

GE Internal Reference #	Description
B-14606/ B-14700	Added support for IRIG-B Input quality in G100 through Hardware Asset Management Application (HAMA).

2.1.9 Documentation

None

2.1.10 Hardware

None

2.2 Fixed defects

This version of G100 has fixes for the following defects compared to previous version:

2.2.1 Cyber Security

Please refer to Product & Cyber Security Advisories on the GE Grid Solutions web site.

2.2.2 Clients

GE Internal Reference #	Description
D-12697	The value of Digital Output (DO) is always set to '1' even after completion of PULSE command in GPIO client.
D-12815	Local I/O analogue value and timestamp in GPIO client go to zero randomly.
D-12818	The analogue values on the local I/O GPIO client jumps to a value of -25 randomly.
D-12698	Removed unused Device Online DI pseudo point from GPIO client.

2.2.3 Servers

None

2.2.4 Automation

GE Internal Reference #	Description
D-12703	The zone assignments in Load Shedding DTA are not persisted across power restarts when user sets the zones through Analog Setpoint commands.
D-12702	The EVE/CEV file retrieval from SEL Binary/GenASCII client connections through ARRM is not working when SEL relays are configured with virtual serial ports for communication.
D-12828	The EVE/CVE file retrieval from GenASCII client through ARRM is not working when SEL 3x relay is configured with the physical serial ports for communication.
D-12784	G100 logs unwanted synchronized/not-synchronized SOE events from IRIG-B.

2.2.5 Configuration/Settings

GE Internal Reference #	Description
D-12753/ D-12767	G100 applications are not running if the Maintenance serial Port is Disabled in the connections page.
D-12801	The order in which Digital Input GPIO IED points appear in the offline editor is different when compared to the online editor

2.2.6 HMI

GE Internal Reference #	Description
D-12716/ R-01418	The HMI Object transparency ignored in one line viewer during runtime.

2.2.7 Pass-through

None

2.2.8 System

GE Internal Reference #	Description
D-12700	The settings of UEFI are lost after super cap drains/discharges.
D-12741	The issue of UEFI COM4 console redirection ends up on COM3 which further prevents the G100 firmware upgrade.
D-12872	In case of a faulty mSATA card, the MCP utilities write the G100 firmware upgrade on the USB itself.
D-12855	Customer Support Access to Edge OS host requires a reboot of G100.

2.2.9 Documentation

GE Internal Reference #	Description
D-12699	Updates to online help to remove description for unused Device Online DI pseudo point.
B-15308/ B-15305	Updates for XCA certificate creation procedure & VPN client configuration parameters

2.2.10 Hardware

None

2.3 Known Issues

2.3.1 Cyber Security

Please refer to Product & Cyber Security Advisories on the GE Grid Solutions web site.

2.3.2 Clients

GE Internal Reference #	Description
B-13475 D-09915	SEL Binary Client doesn't support Double Precision Scaling Factors.
D-05002	ARRM file retrieval from SEL 1xx/2xx relays (using GEN ASCII) is not possible.
D-12835	SEL Binary Client could not process the interleaved responses when unsolicited and poll messages come simultaneously from SEL relays.
D-12834	Modbus Client could not process PRF events comes from SR 369 relay.
D-12853	Local GPIO Client Command Failed accumulator pseudo point is not incrementing on TTL failure

2.3.3 Servers

GE Internal Reference #	Description
D-12567	The time sync accuracy of G100 when IEC101 Server (Unbalanced/Balanced) is used as a time sync source is > +/- 4 msec.
B-11967	No support for events in NVRAM in IEC101/104 Server. Events that have not been yet transmitted to Master (Clients) are lost if G100 is power cycled / restarted. However – the integrity polls will continue to provide accurate database representation.

GE Internal Reference #	Description
B-11968	No support for events in NVRAM in DNP3 Server. Events that have not been yet transmitted to Master (Clients) are lost if G100 is power cycled / restarted. However – the integrity polls will continue to provide accurate database representation.

2.3.4 Automation

GE Internal Reference #	Description
D-05033	Suppressed quality through Input Point Suppression (IPS) application is not reported to Masters. DNP3 and IEC 101-104 Servers send Online Quality rather than the substituted/last reported quality when points are suppressed.
B-11969	DEM is responsible for handling alarms. Events/Alarms that have not been yet committed to the SQL database are lost if G500 is power cycled / restarted. However – the integrity polls will continue to provide accurate database representation.
DCSSUP-19948, D-12000	Restore the last value for variables configured in LogicLinx wizard does not work at runtime (defaults to 0 always).

2.3.5 Configuration/Settings

GE Internal Reference #	Description
D-10388	TACACS+ remote authentication can be enabled and activated even if the TACACS+ Server is not available in that moment. This will conduct to a device that can only be accessed using Emergency Access process, if TACACS+ server is not available.
D-10825	Online Editor / SNMP Agent Browser is not able to retrieve OID data if gathering data from target device takes more than 60 seconds. Workaround: configure the SNMP client offline, using OID from the end device (e.g., using a 3rd party MIB browser).
D-12810	The order in which pseudo points appear in the offline editor is different when compared to the online editor for the applications Modbus DCA, D.20 DCA and SNMP DCA.

2.3.6 HMI

GE Internal Reference #	Description
B-14982	The product references in the Runtime (Local/Remote) HMI logs need to be changed as "MCP".
D-05463	If a used point group is deleted from the systemwide configuration then points belonging to that group are not visible in the point group summary. However, if user changes the point group allocation from the corresponding instantiated client map file(s) then points will be visible in the point group summary.

2.3.7 Pass-through

None

2.3.8 System

GE Internal Reference #	Description
B-14973	The software licensing application reports core license 012 as "G500 Core", it should be "MCP Core". There is no functional impact.
D-10227	Email does not send messages when an alarm is activated.
D-05714	Update of only Edge OS is not supported. If only Edge OS updates are required, the complete G100 firmware image needs to be updated.
D-12887	G100 GPIO input_overrun warning messages are logged periodically (~30 s) in the kernel log on loaded systems. The impact is that the MCP support bundle will not be able to retrieve a kernel log event older than approximately 22 days on a busy system, so ensure MCP support bundle is created, if necessary, soon after a kernel event that may need to be investigated.

2.3.9 Documentation

None

2.3.10 Hardware

None

Capability and Capacity

In this release version the G100 database and connectivity sizes are limited to a maximum of:

- Up to 24,000 total RTDB real data points (not counting pseudo points), originating from:
  - Up to 60 IEDs, and
  - Up to 60 D.20 IO modules
- Up to 4 concurrent Master connections
- Up to 2 Runtime HMI sessions

2.4 Standalone (non-redundant)

In this release version G100 provides the following performance capabilities in Standalone (non-redundant) Mode.

2.4.1 Performance Test Levels

In this release version G100 is tested under maximum configured system size using the activity levels and disturbance scenarios presented next.

Requirement	Steady State Normal Loading	Avalanche Heavy Loading
G100 Hardware (CPU / RAM)	2 core CPU / 8 GB RAM	2 core CPU / 8 GB RAM
Loading Signal changes (continuously/sec)	AI - 1200 DI – 12	All points changing twice in 2 secs
Number of IEDs connected to G100	60 DNP + 60 D.20 Peripherals [11 A cards, 30 C1 cards, 2 C2 cards, 14 S cards, 3 K cards]	60 DNP + 60 D.20 Peripherals [11 A cards, 30 C1 cards, 2 C2 cards, 14 S cards, 3 K cards]
G100 total RTDB Point count	24000	24000
Points / IED (400 total)	225 - AI, 125 - DI, 20 - DO, 20 - AO, 10 - ACC + D.20 points from 60 peripherals.	225 - AI, 125 - DI, 20 - DO, 20 - AO, 10 - ACC + D.20 points from 60 peripherals.
Total number of Servers & supported points in each Server	4 DI = 1875 i.e., = 125 * 60 /4 AI = 3375 i.e., = 225 * 60 /4 AO = 300 i.e., = 20 * 60 / 4 AO = 300 i.e., = 20 * 60 / 4 ACC = 150 i.e., = 10 * 60/ 4	4 DI = 1875 i.e., = 125 * 60 /4 AI = 3375 i.e., = 225 * 60 /4 AO = 300 i.e., = 20 * 60 / 4 AO = 300 i.e., = 20 * 60 / 4 ACC = 150 i.e., = 10 * 60/ 4
Remote G100 HMI connections	1 connection	1 connection
Local G100 HMI connections	1 connection (single monitor)	1 connection (single monitor)
Datalogger / Periodic reports	120 AI mapped / 12 reports	120 AI mapped / 12 reports
ARRM	5 sessions / IED	5 sessions / IED
Alarms	12 / sec	12 / sec (twice within 2 secs)

2.4.2 Performance Test Results

The standalone performance test results are presented below.

Table 2.1: Standalone Performance test results

Activity	Minimum	Median	Maximum
Loading Condition	Steady State Normal Loading		
CPU utilization – (%)	35	75	100
Average Memory Usage (GB)	0.849	1.201	1.261
Event latency (msecs)	172	518	2595
Control latency (msecs)	12	25	254

NOTE: Under steady state normal loading conditions, the control latency was measured by simulating one control every 5 seconds continuously from the Master station.

2.4.3 HMI Response times

G100 HMI response times under steady state normal loading conditions are presented below.

Table 2.2: User Interface Response Time – Steady State Normal Loading

Activity	Minimum (seconds)	Median (seconds)	Maximum (seconds)
Screen Access (Point Summary)	0.7	1.4	2
Screen Access (Comm Summary/Connections Page)	1	2.5	4
System Logs	0.6	2.5	5
Alarm ACK Delay (Single Alarm)	1	1.5	2
DI/AI Update to Point Summary Screen	1	1	1
Datalogger	1	1.6	3

2.5 Redundancy

G100 doesn't support system/device redundancy in release 2.30.

Time Sync Accuracy (IRIG-B/NTP)

G100 supports only software based IRIG-B TTL and software based NTP Time Sync.

Time accuracy with IRIG-B TTL input is typically +/- 1ms.

Application List

The following applications are available in this released firmware version.

Application	Support in Standalone
Runtime HMI	✓ Available
One Line Viewer	✓ Available
Config GUI / Schemas	✓ Available
System Library	✓ Available
C++ System Library	✓ Available
Connection Parser	✓ Available
Calculator	✓ Available
Hardware Asset Management Application (HAMA)	✓ Limited points availability (see MCP Software Configuration Guide SWM0101)
PTP Time Sync	× Not Available
IRIG-B/NTP Time Sync (Software based)	✓ Available
D.20 Client	✓ Available
GPIO Client	✓ Available
Modbus Client	✓ Available
Modbus-TCP/SSH Client	✓ Available
SEL® Binary Client	✓ Available
Analog Data Logger	✓ Available
Generic ASCII Client	✓ Available
Modbus Server	✓ Available
DNP 3.0 Server	✓ Available
DNP 3.0 Client	✓ Available
Digital Event Manager	✓ Available
Database Server	✓ Available
DNP 3.0 TCP/IP Transport Layer	✓ Available
DNP 3.0 Server Serial Transport Layer	✓ Available
DNP 3.0 DIDO	✓ Available
IEC 60870-5-101/104 Server	✓ Available
IEC 60870-5-103 Client	✓ Available
IEC 61850 Client	✓ Available
IEC 60870-5-101/104 Client	✓ Available
Event Logger	✓ Available
Real-Time Database	✓ Available
LogicLinx IEC 61131-3 Soft Logic	✓ Available

Application	Support in Standalone
Redundancy Manager	× Not Available (Only Standalone mode is available)
System Point Manager	✓ Available
Load Shedding and Curtailment	✓ Available
Control Lockout Manager	✓ Available
Software Watchdog	✓ Available
Configuration Manager	✓ Available
IP Changer	✓ Available
MD5SUM Builder	✓ Available
System Status Manager	✓ Available
Virtual Serial Ports	✓ Available
SNMP Client	✓ Available
Automated Record Retrieval Manager	✓ Available
Software Licensing Subsystem	✓ Available
Third-party components	✓ Available
Terminal Services	✓ Available
mcpcfg utility	✓ Available
E-mail Utility	✓ Available
IO Traffic Monitor	✓ Available
Firewall	✓ Available
Edge OS & Drivers	✓ Available
Secure Enterprise Connectivity	✓ Available
Genconn	✓ Available
HMI Access Manager	✓ Available
Sync Service Library	✓ Available
Sync Server Application	✓ Available
Analog Report Generator	✓ Available
OpenVPN	✓ Available

MODIFICATION RECORD

VERSION	REV.	DATE	CHANGE DESCRIPTION
2.20	0	19th May, 2021	First version, created for G100 Firmware Version 2.20 (document version starts with 2.20 to be in synch with firmware version)
2.30	0	29th July, 2021	Updated for G100 Firmware Version 2.30
2.30	1	20th August, 2021	Updated Cyber Security sections

GE
Grid Solutions

Multilin™ MCP

Substation Gateways

Software Configuration Guide

SWM0101

Version 3.00 Revision 1

imagination at work

GE information

Copyright Notice

©2021, General Electric Company. All rights reserved.

The information contained in this online publication is the exclusive property of General Electric Company, except as otherwise indicated. You may view, copy and print documents and graphics incorporated in this online publication (the "Documents") subject to the following: (1) the Documents may be used solely for personal, informational, non-commercial purposes; (2) the Documents may not be modified or altered in any way; and (3) General Electric Company withholds permission for making the Documents or any portion thereof accessible via the internet. Except as expressly provided herein, you may not use, copy, print, display, reproduce, publish, license, post, transmit or distribute the Documents in whole or in part without the prior written permission of General Electric Company.

The information contained in this online publication is proprietary and subject to change without notice. The software described in this online publication is supplied under license and may be used or copied only in accordance with the terms of such license.

Trademark Notices

GE, Multilin and are trademarks and service marks of General Electric Company.

* Trademarks of General Electric Company.

IEC is a registered trademark of Commission Electrotechnique Internationale. IEEE is a registered trademark of the Institute of Electrical and Electronics Engineers, Inc. Internet Explorer, Microsoft, and Windows are registered trademarks of Microsoft Corporation.

Other company or product names mentioned in this document may be trademarks or registered trademarks of their respective companies.

This printed manual is recyclable.

Please return for recycling where facilities exist.

Security Notice

Many of the MCP's network services are unauthenticated and unencrypted (for example, DNP3/TCP Master). It is the user's responsibility to ensure these services are protected from unauthorized use.

Even though the MCP includes a host firewall, it is recommended that an external network firewall be placed on the electronic security perimeter as an additional layer of protection.

Table of Contents

Copyright Notice 2
Trademark Notices 2
Security Notice 2
Table of Contents 3
Figures 19
About this Document 21
Purpose 21
Intended Audience 21
Additional Documentation 21
How to Use this Guide 21
Safety words and definitions 22
Product Support 23
GE Grid Solutions Web Site 23
GE Technical Support Library 23
Contact Technical Support 23
Chapter 1 - MCP Basics 24
MCP Multi-function Controller Platform 24
MCP Substation Gateway 24
Key Benefits 24
UEFI Settings 26
MCP Time Synchronization 27
MCP Settings 29
MCP Firmware Version Information 29
Local Configuration Utility (mcpcfg) or MCP Settings GUI 29
MCP Configuration 30
System/PC Requirements 30
DS Agile MCP Studio Software Version Information 30
Snapshots 32
Snapshot Management 34
Redundancy - Snapshots 55
Project and Archive Management 56

MCP Runtime HMI 65
Local HMI 66
Remote HMI 72
MCP Applications 76
MCP System Redundancy 76
Types of MCP Applications - Functionality 76
Types of MCP Applications - Architecture 76
Types of MCP Applications - Automation Features 78
MCP License Types – Online store 78
Types of MCP Applications - Configuration 78
User Roles 80
Default Users 80
HMI User Access Levels 80
User Authentication 81
Chapter 2 - Introducing MCP Features 84
Substation Gateway Features 84
Security Features 84
Advanced Gateway 84
Advanced Automation 84
Fault Recording/Datalogging 85
Secure Remote Access 85
Edge Connectivity 85
Local HMI 86
Chapter 3 - MCP HMI Runtime 87
Runtime HMI Navigation 88
Main Display Area 88
Power Bar 89
Change Displayed Information 101
Internationalization 102
Manage Alarms 108
Digital Event Management 108
Alarm Types 109
Alarm Groups 109

Double Point Alarms 109
Active Alarms 110
Historical Events 112
View Data 113
View Data 113
Real-Time Database 114
Data types 114
Data Quality Status 115
Point Details 121
View Point Details 123
View Events 128
Connections 129
Logs 132
Trends 141
Execute Commands 142
Issue a Command 143
Acknowledge an Alarm (One-Line Viewer) 144
Acknowledge an Alarm Group (One-Line Viewer) 144
Analog Output Interface 144
Analog Set-point Interface 145
Digital Control Interface 145
Digital Output Interface 146
Navigate to Active Alarm Page (One-Line Viewer) 148
Point Forcing Interface 148
DataSource Types 149
Raise/Lower Control Interface 151
Tag/Inhibit Interface 152

Global Controls Disable 152
Operator Notes 153
Operator Notes 153
Chapter 4 - MCP Local Configuration Utility (mcpcfg) 156
Introduction 157
Date and Time 158
Select Time Source 159
Configure Time Output 167
Timestamps and Time Zones on MCP 171
Time Sync Settings and Runtime Functionality 173
PTP Use Case Scenarios 174
Networking 177
Background 178
Network Modes 178
Substation LAN IED Types 179
Network Configuration 180
Network LAN Scenarios 188
Subnet Overlapping Rules 192
Custom Routing 194
Network Summary 197
Administrators User Management 197
Default Users 197
User Management Overview 208
Configure User HMI Home Page 209
Auto Login 209
Other Services/Settings 211
Configure Remote HMI Non-Observer Privileges 211
Configure Rsyslog service 213
Configure Secure Access 216
Configure Firewall 218
Configure Host Names 221
Configure Time & Time Sync 221

Reset System Logs 221
Reset Database Tables 221
Reset File Persistence Data 223
Local HMI 223
Configure Sync Manager 226
Redundancy 229
ARRM - Automatic Record Retrieval Manager 232
Suppress Forced Qualities To Masters 233
Emulate D20 RTU IEC101 DPA Unbalanced Mode Functionality 236
Configure IEC101+104 DPA Startup Quality Event Suppress Interval 237
Configure Serial Port Modes (RS-232/485) 238
Configure D.20 Port Hardware Settings 240
EdgeOS Host Access 240
Clear Chassis Intrusion State 241
Restore Clone Snapshot 243
Restore to Factory Default 248
Reboot device 250
Chapter 5 - MCP Settings GUI 252
Introduction 252
How to access/logout 253
Login – Local MCP 253
Login – Remote MCP 253
Initial Setup 253
Logout 262
MCP Settings Workflows 263
Configure Authentication 265
Configure Network Settings 279
Configure Network Interfaces 282
Configure Secure Access 295
Configure Firewall 299
Configure Host Names 301
Configure Time & Time Sync 303

Reset System Logs 310
Reset Database Tables 311
Reset File Persistence Data 313
Local HMI 314
Configure Sync Manager 316
Redundancy 318
ARRM 328
Suppress Forced Qualities To Masters 330
Emulate D20 RTU IEC101 DPA Unbalanced Mode Functionality 332
Configure IEC101+104 DPA Startup Quality Event Suppress Interval 333
Configure Serial Port Modes (RS-232/485) 334
Configure D.20 Port Settings 335
EdgeOS Host Access 336
Clear Chassis Intrusion State 338
Restore Clone Snapshot 338
Restore to Factory Default 341
Reboot Device 343
Chapter 6 - DS Agile Studio Configuration 344
DS Agile Studio MCP Configuration steps 346
Configuration file format 347
Configure System Wide Options 347
Systemwide tab 347
AI Text Enumeration Tab 360
Build Client Map Files 360
GPIO Configuration steps (G100 only) 361
D.20 Peripheral Client 364
Client Map 371
DNP3 Client 373
Modbus Client 378
SEL Binary Client 383
IEC 60870-5-103 Client 385
IEC 60870-5-101+104 Client 391

Generic ASCII Client 399
SNMP Client Properties 409
IEC 61850 Client 412
MCP Redundancy 412
About Redundancy 412
Redundancy Summary 415
Operational States 416
MCP Redundancy Configuration Combinations 416
Configure the MCP for Redundancy 419
System Points 426
Non-Sync Mode 428
Validating the Redundant Connections 429
Changeover during Standby Start-up 430
Communications 442
Connection 442
Configure Serial Communications 443
Configure Network Communications 452
Configure D.20 458
Configuring Client Applications 464
Client Configuration Overview 464
DNP3 Multi-drop 465
DNP IED Block 467
IEC 60870-5-101 Multi-drop 470
IEC 60870-5-103 Multi-drop 472
IEC 60870-5-104 IED Block 474
Modbus Multi-drop 475
Modbus TCP or TCP/SSH IED Block 476
Generic ASCII Client 477
SEL Binary 479
LogicLinx Device 480
SNMP Block 481
Configure to acquire files (ARRM) 481

Automated Record Retrieval Manager Overview 481
ARRM Configuration 482
ARRM Viewer 482
ARRM Pseudo Points 483
Enterprise Synchronization 484
Applications - ARRM 484
File Set Template - Standard 491
File Set Template – Sel ASCII 493
About Oscillography files and IEEE File 494
Connection Polling 495
ARRM FTP Directory Delta Support for Different ftp ls Formats 497
Sample File Set Templates for Relay Models 498
ARRM ASCII Directory Delta Support 499
Configure Automation Features 501
Configuration Overview 502
System Point Manager 502
Accumulator Freeze 503
Alarm 513
Calculator 520
Input Point Suppression 547
Remote Logging (Rsyslog) 548
Configure Datalogger 550
Configure the Data Logger 550
Report Types 550
Storage Allocation 552
Save Report 553
Load Report 553
Manage Reports 553
Select Points 554
Change Scaling 555
HAMA - Hardware Asset Management Application 555
Hardware Asset Management Application (HAMA) 555

Analog Inputs 556
Digital Inputs 563
Accumulator Points 566
Text Points 569
Build Server Map Files 570
Server Maps 571
DNP3 Server 572
MODBUS Server 579
IEC 60870-5-101+104 Server 583
Configuring Server Applications 596
Server Configuration Overview 596
DNP3 Serial Master Stations 596
IEC 60870-5-101 Master Station 605
Modbus Serial Master Station 610
DNP3 Network Master Stations 611
IEC 60870-5-104 Master Station 612
Modbus TCP Master 615
Build HMI One-Line Diagrams 616
One-Line Viewer 617
View One-Line Diagrams 617
Executing One-Line Diagram Commands 618
Create Analog Reports 659
Analog Report Generation - Overview 659
Analog Report - Viewing 660
Analog Report Generation - Configuration 663
Configure System Security 668
Security Features 669
System Security 669
Password Complexity 669
Connection Security 669
User Accounts and Authentication 671
Setting Up a User Account 674

Secure Access 675
Software Licensing Tools 675
Firewall Settings 679
Automatic logout 680
System Utilities 680
Utilities 681
Utilities Log In 681
Certificate Import 682
Certificate Management 682
Export Database 685
Generate Gateway Key Pair 689
Exporting VPN Client Configuration File 689
Upload SSL server Certificate/Server Key 691
Miscellaneous Utilities 693
Utilities Overview 693
Setting up a Terminal Session 693
Pass-Through Connections 694
Direct Connect (mcpconnect) 695
MCP Configuration Manager 696
Chapter 7 - MCP Pseudo Points 698
Application Pseudo Points 699
Analog Reports 699
Analog Reports – Analog Input Points 699
Analog Reports – Digital Input Points 699
Calculator 700
Calculator – Accumulator Points 700
Calculator – Analog Input Points 700
Calculator – Digital Input Points 700
Calculator – Digital Output Points 700
Data Logger 701
Data Logger – Analog Input Points 701
Data Logger – Digital Input Points 701

Data Logger – Digital Output Points 701
Digital Event Management 701
Digital Event Manager – Analog Input Points 701
Digital Event Manager – Digital Input Points 702
Digital Event Manager – Digital Output Points 702
DNP 3.0 Serial with MCP as Master Application 703
DNP 3.0 Serial with MCP as Master – Accumulator Points 703
DNP 3.0 Serial with MCP as Master – Digital Input Points 703
DNP 3.0 Serial with MCP as Master – Digital Output Points 704
DNP 3.0 Serial with MCP as Slave Application 705
DNP 3.0 Serial with MCP as Slave – Accumulator Points 705
DNP 3.0 Serial with MCP as Slave – Analog Input Point 705
DNP 3.0 Serial with MCP as Slave – Digital Input Points 705
DNP 3.0 Serial with MCP as Slave – Digital Output Points 705
DNP 3.0 Ethernet with MCP as Master Application 706
DNP 3.0 Ethernet with MCP as Master – Accumulator Points 706
DNP 3.0 Ethernet with MCP as Master – Digital Input Points 706
DNP 3.0 Ethernet with MCP as Master – Digital Output Points 707
DNP 3.0 Ethernet with MCP as Slave Application 708
DNP 3.0 Ethernet with MCP as Slave – Accumulator Points 708
DNP 3.0 Ethernet with MCP as Slave – Analog Input Point 708
DNP 3.0 Ethernet with MCP as Slave – Digital Input Points 708
DNP 3.0 Ethernet with MCP as Slave – Digital Output Points 709
GENASCII Serial with MCP as Master Application 709
DCA Pseudo Points 709
IED Pseudo Points 710
IEC 60870-5-101 with MCP as Master Application 713
IEC 101 with MCP as Master - Device Level 713
IEC 101 with MCP as Master – DCA Level 715
IEC 60870-5-101 with MCP as Slave Application 716
IEC 101 with MCP as Slave - Accumulator Points 716
IEC 101 with MCP as Slave – Analog Input Points 717
IEC 101 with MCP as Slave – Digital Input Points 717

IEC 101 with MCP as Slave – Digital Output Points 718
IEC 60870-5-104 with MCP as Master Application 718
IEC 104 with MCP as Master - Device Level 718
IEC 104 with MCP as Master – DCA Level 720
IEC 60870-5-104 with MCP as Slave Application 722
IEC 104 with MCP as Slave - Accumulator Points 722
IEC 104 with MCP as Slave – Analog Input Points 723
IEC 104 with MCP as Slave – Digital Input Points 723
IEC 104 with MCP as Slave – Digital Output Point 723
IEC 60870-5-103 with MCP as Master Application 724
IEC 103 with MCP as Master - Device Level 724
IEC 103 with MCP as Master – DCA Level 726
IEC 61850 with MCP as Master Application 727
IEC 61850 Application – Global Points 729
IEC 61850 Application - Global, Digital Output Points 729
IEC 61850 Application - Global, Digital Input Points 729
IEC 61850 Application – Per-Device Points 730
IEC 61850 Application, Per-Device - Digital Output Points 730
IEC 61850 Application, Per-Device - Digital Input Points 730
IEC 61850 Application, Per-Device - Analog Input Points 731
Load Shed 732
LoadShed – Accumulator Points 732
LoadShed – Analog Input Points 732
LoadShed – Digital Input Points 733
LoadShed – Digital Output Points 733
LogicLinx 733
LogicLinx – Accumulator Points 733
LogicLinx – Analog Input Points 733
LogicLinx – Digital Input Points 733
LogicLinx – Digital Output Points 734
Modbus Ethernet with MCP as Master Application 734
Modbus Ethernet with MCP as Master – Accumulator Points 734
Modbus Ethernet with MCP as Master – Digital Input Points 734

Modbus Ethernet with MCP as Master – Digital Output Point 735
Modbus Ethernet with MCP as Master – Analog Input Point 735
Modbus Ethernet with MCP as Slave Application 735
Modbus Ethernet with MCP as Slave – Accumulator Points 735
Modbus Ethernet with MCP as Slave – Analog Input Point 736
Modbus Ethernet with MCP as Slave – Digital Input Points 736
Modbus Ethernet with MCP as Slave – Digital Output Points 736
Modbus Serial with MCP as Master Application 736
Modbus Serial with MCP as Master – Accumulator Points 736
Modbus Serial with MCP as Master – Digital Input Points 737
Modbus Serial with MCP as Master – Digital Output Point 737
Modbus Serial with MCP as Slave Application 737
Modbus Serial with MCP as Slave – Accumulator Points 737
Modbus Serial with MCP as Slave – Analog Input Point 738
Modbus Serial with MCP as Slave – Digital Input Points 738
Modbus Serial with MCP as Slave – Digital Output Points 738
Modbus TCP/SSH Client - SSH Tunnel Interface 739
Redundancy Manager 741
Redundancy Manager – Analog Input Points 741
Redundancy Manager – Digital Input Points 741
Redundancy Manager – Digital Output Points 742
SEL Binary Serial with MCP as Master Application 742
Accumulators 742
Analog Input 742
Digital Input 743
Digital Output 744
Text Points 744
System Status Manager 744
System Status Manager – Analog Input Points 744
System Status Manager – Digital Output Points 745
System Status Manager – Digital Input Points 745
System Status Manager – Text Points 745

D.20 Peripheral Link Client Pseudo Points ... 745
D.20 Peripheral Link Client: Per – Peripheral Pseudo Points ... 745
D.20 Peripheral Link Client – Global Pseudo points ... 746
GPIO Client Pseudo Points ... 747
GPIO Client: Pseudo Points ... 747
Chapter 8 - EdgeManager and PETC ... 748
Downloading and Running Predix Edge Technician Console ... 749
Device Status ... 749
Configuring the Network and Proxy Settings ... 749
Appendix A – Secure Terminal Emulator ... 750
Connect to MCP Secure Terminal Emulator through SSH ... 750
Connect to MCP Secure Terminal Emulator through Serial Port ... 751
Appendix B – Secure File Browser ... 752
Appendix C - GenASCII Client - Time Sequence Diagrams and Sample Configuration for FEP Devices ... 753
Time Sequence of Message Transactions ... 753
Time Sequence of Message Transaction with Support for delayed message processing as False ... 754
Time Sequence of Message Transaction with Support for delayed message processing as True ... 755
Sample Configuration where response is expected within definite period ... 757
Appendix D - Configuring a Linux-based Enterprise Server ... 759
SSH Server ... 759
Rsync utility ... 759
Installation Steps ... 759
Appendix E - Running Cron Jobs on the MCP ... 760
Scheduling background jobs in MCP using Cron utility ... 760
Appendix F – Shell commands ... 762
mcpcsb ... 762
mcpsi ... 763
Version info from Firmware container ... 764
get_version from HAMA container ... 764
musb: USB Mount command ... 765
Good USB ... 765
Corrupted USB ... 765
No USB ... 765

musb unmount: USB unmount command 765
Appendix G – Security Certificates Creation for MCP 766
Overview 766
Setting up a Certification Authority 766
Setting up the XCA Certification Authority 766
Certificate Generation 768
Creating a CA-Signed Server Certificate 768
Installing Certificates 769
Installing Server Certificate and Private Key on the MCP 770
Installing CA Certificate for use by the MCP Runtime HMI Viewer 771
Appendix H – List of Factory Default open ports (TCP and UDP) 775
Overview 775
Appendix I – Modbus Protocol Support 776
Read Coils Status (Function Code 1) 776
Read Input Status (Function Code 2) 776
Read Holding Registers (Function Code 3) 776
Read Input Registers (Function Code 4) 776
Write Single Coil (Function Code 5) 777
Write Single Register (Function Code 6) 777
Data Representation for Write Single Register 778
Glossary 779
Modification Record 782

Figures

Figure 1.1: G500 System Overview 25
Figure 1.2: G100 System Overview 26
Figure 1.3: Monitor A becomes Primary and Monitor B is extended 67
Figure 1.4: Monitor A (connected to Display Port0/DP2) becomes Primary and Monitor B (connected to Display Port 1/ DP1) becomes extended 68
Figure 1.5: Login HMI screen 69
Figure 1.6: MCP Home Page 70
Figure 1.7: MCP Login Screen 71
Figure 1.8: Remote HMI Login 72
Figure 1.9: Username and Password window 72
Figure 1.10: MCP Home page 73
Figure 1.11: Logout from the MCP Runtime HMI 74
Figure 1.12 Data applications within the MCP 77
Figure 3.1: Main Display 88
Figure 3.2: Tree view 89
Figure 3.3: Typical Power Bar 89
Figure 4.1: MCP operates as a slave clock 175
Figure 4.2: MCP operates as a boundary clock 176
Figure 4.3: Best Master Clock Scenario 177
Figure 4.4: Sample VLAN configuration of Net1 182
Figure 4.5: Configure Network Interfaces 184
Figure 4.6: Configure Net0 Interface 185
Figure 4.7: Configure Net1 - Net2 185
Figure 4.8: Enable Redundant mode 186
Figure 4.9: Enable PRP Mode 187
Figure 4.10: HAMA Points 188
Figure 4.11: MIXED: Single/Dual LAN + PRP Scenario Diagram 189
Figure 4.12: Legacy Single, Redundant and Dual LAN Scenario Diagram 190
Figure 4.13: PRP only Scenario 191
Figure 4.14: Mixed: Legacy Single/Redundant/Dual LAN + PRP Scenario 191
Figure 4.15: Legacy Single and Dual LAN Scenario Diagram 192
Figure 4.16 Custom Routing Example - Block Diagram 195
Figure 4.17: ARRM Connections 233
Figure 6.1: Storage 351

Figure 6.2 G100 Serial Maintenance Port control 443
Figure 6.3: System Log Retrieval 549
Figure 6.4: Multiple LRU Overview 601
Figure 6.5 Example Remote LRU Configuration 601
Figure 6.6 Data Logger - Data Flow 687

About this Document

Purpose

This guide provides detailed information on how to configure the software of the Multilin™ MCP Substation Gateway. Although this document describes all the configurable software applications in the MCP, only the applications you purchased for your MCP are available to you.

NOTICE

This document applies to the entire MCP family (G100/G500) unless otherwise indicated.
Screen captures may show G100 or G500 in some areas, however the workflow applies to products in the MCP family (G100/G500), unless otherwise indicated.

This document reflects functions available in the following product versions:

- **G100 V2.20, V2.30**
- **G500 V2.10**

Intended Audience

This document is a helpful resource for utility personnel and system engineers who are implementing the MCP in an overall substation automation system, and protection engineers who are controlling network devices. It is intended for readers who have knowledge of substation automation equipment and applications.

Additional Documentation

For further information about the MCP, refer to the following documents.

- *G100 Substation Gateway Instruction Manual (994-0155)*
- *G500 Substation Gateway Instruction Manual (994-0152)*
- *MCP HMI Online Help*
- *DS Agile MCP Studio Online Help*
- *G100 Quick Start Guide (SWM0116)*
- *G500 Quick Start Guide (SWM0106)*
- *Configuring UEFI Settings on G100 User Guide (SWM0122)*
- *Configuring UEFI Settings on G500 User Guide (SWM0110)*

How to Use this Guide

This guide describes how to configure the MCP. The MCP employs sophisticated applications that contain many advanced features and capabilities. To successfully configure and operate the MCP for your substation environment, it is highly recommended that you work through this entire guide.

Where appropriate, a detailed Table of Contents is provided at the beginning of a chapter.

If you need assistance, contact General Electric Company GE Grid Solutions Technical Support.

In configuration tables, “N/A” in the “Default” column indicates there is no default setting provided, and “X” indicates the number is automatically incremented.

Safety words and definitions

Before attempting to install or use the device, review all safety indicators in this document to help prevent injury, equipment damage or downtime.

The following safety and equipment symbols are used in this document:

⚠DANGER	**Indicates a hazardous situation which, if not avoided, will result in death or serious injury.**
⚠WARNING	**Indicates a hazardous situation which, if not avoided, could result in death or serious injury.**
⚠CAUTION	**Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.**
NOTICE	**Indicates practices that are not related to personal injury.**
NOTE	**Important information about the product, product handling which must be given attention.**

Product Support

If you need help with any aspect of your GE Grid Solutions product, you can:

- Access the GE Grid Solutions Web site
- Search the GE Technical Support library
- Contact Technical Support

GE Grid Solutions Web Site

The GE Grid Solutions Web site provides fast access to technical information, such as manuals, release notes and knowledge base topics.

Visit us on the Web at: http://www.gegridsolutions.com

GE Technical Support Library

This site serves as a document repository for post-sales requests. To get access to the Technical Support Web site, go to: http://sc.ge.com/*SASTechSupport

Contact Technical Support

For help with any aspect of your GE Grid Solutions product, please contact our support team, 24/7, as follows:

Region	E-mail	Telephone
Global Contact Centre	ga.support@ge.com	+44 1785 250070
Central and East Asia andPacific	ga.supportCEAP@ge.com	+61 414 730 964
India	ga.supportIND@ge.com	+91 44 22648000
Middle East, North Africa andTurkey	ga.supportMENAT@ge.com	+971 42929467
Europe, Russia, CIS and Sub-Saharan Africa	ga.supportERCIS@ge.com	+34 94 4858854
North America	ga.supportNAM@ge.com	+1 877 605 6777
Latin America	ga.supportLAM@ge.com	+55 11 36187308

Chapter 1 - MCP Basics

MCP Multi-function Controller Platform

GE's advanced Multi-function Controller Platform (MCP) offers a high-capacity, secure, substation hardened set of modular and expandable hardware and software components designed to simplify deployment, operation, and maintenance of automation systems for a variety of applications including:

- Transmission & Primary distribution centralized automation,
- Secure substation automation systems

The MCP family is currently composed of the following Substation Gateway models:

- G100 – please refer to *G100 Substation Gateway Instruction Manual (994-0155)*
- G500 – please refer to *G500 Substation Gateway Instruction Manual (994-0152)*

The MCP implementation makes it possible for a single device to host multiple functions and applications such as Supervisory Control and Data Acquisition (SCADA) Concentrator, Remote terminal Unit (RTU), Human Machine Interface, Ethernet Switch functions, Data Storage among others. Consolidation of functions reduces the cost of deployment and operation while increasing system reliability through a reduced number of devices in the system.

MCP Substation Gateway

GE's MCP Substation Gateway is a secure, hardened, advanced substation gateway that collects metering, status, event, and fault report data from serial or LAN based intelligent substation devices. The MCP summarizes data from the substation devices and makes it available locally /remotely through a stand-alone HTTPS based HMI. It supports serial and/or LAN connections to SCADA masters such as EMS, DMS or other enterprise applications.

With its modern and robust cyber security features, the MCP is designed for smooth integration into NERC CIP and Cyber Security environments while consolidating functions such as Ethernet communications, time synchronization, HMI and SCADA applications.

Key Benefits

- Standardize Substation Architectures with a cost-effective IEC 61850-3 compliant platform capable of handling small to large systems.
- Simplify Engineering and operations through consolidation of functions.
- Reduce equipment cost by eliminating dedicated HMI computers, external Ethernet.
- Optimize Cyber Security management with hardened Linux based operating system and container technologies enabling modular updates instead of single image updates.
- Improve time synchronization performance internal IRIG-B Signal Generation.

Figure 1.1: G500 System Overview

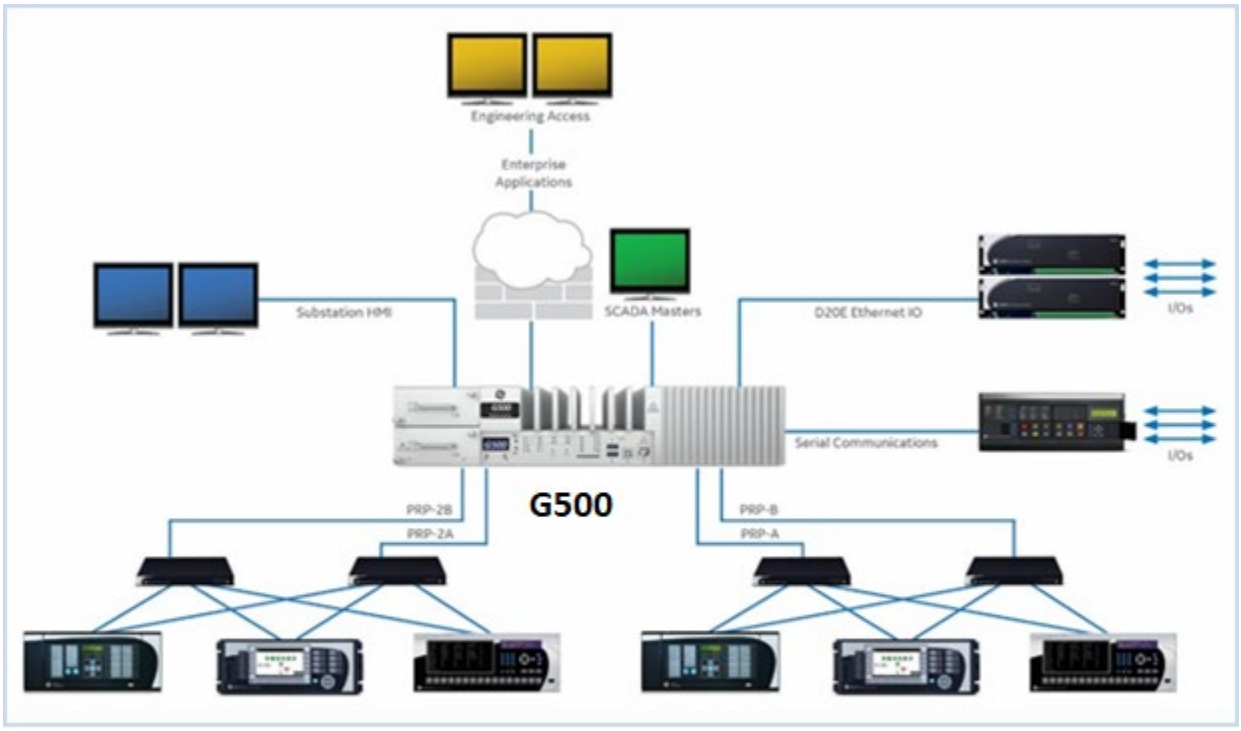
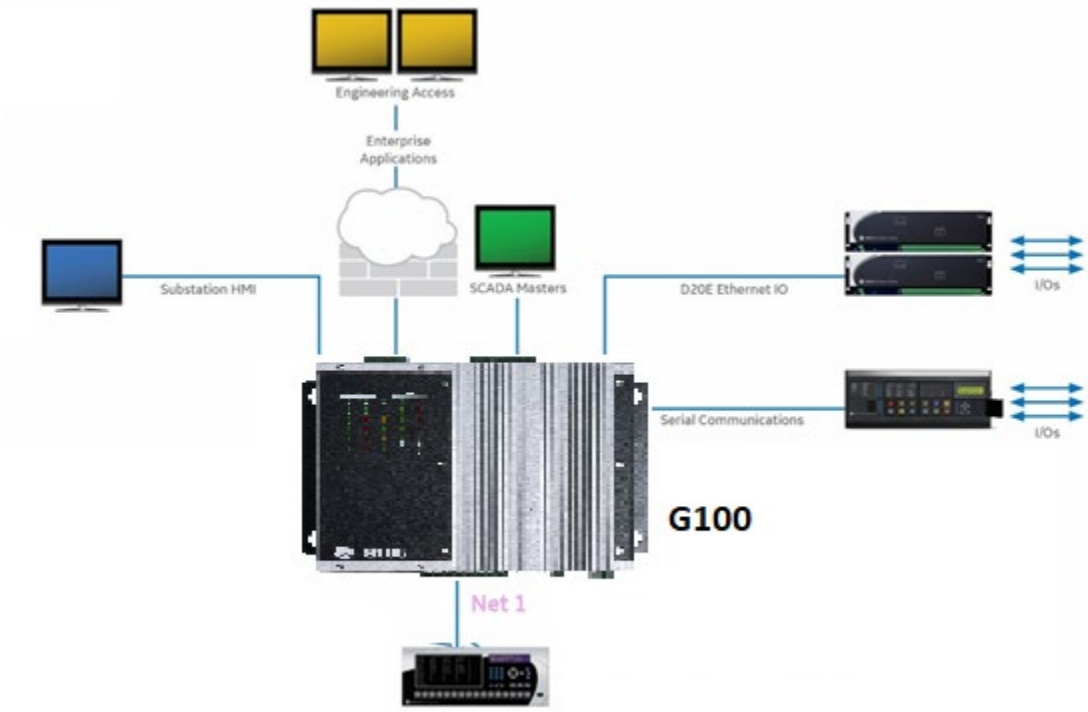


Figure 1.2: G100 System Overview



UEFI Settings

The G100 and G500 have different UEFI settings, described in the documents below, for each product model:

- *Configuring UEFI Settings on G100 User Guide (SWM0122)*
- *Configuring UEFI Settings on G500 User Guide (SWM0110)*

NOTICE

G100 device has the following UEFI settings that will revert to default values after the internal super capacitor has been discharged due to the device being powered off for extended time (typically more than 5 days).

These UEFI settings are applicable only while the G100 is starting.

After the applications started, these settings are over-written by the values configured in *MCP Local Configuration Utility (mcpcfg)* or *MCP Settings GUI*.

- Default Serial Maintenance Port used as UEFI (boot) console when KVM is not available (Advanced->Serial Port Console Redirection)
  - Console Redirection is set to Disabled for COM1-COM3, please do not change these settings.
  - Console Redirection for COM4 should be enabled/disabled and have the “Bits per second”, to be same as in *the Serial Maintenance Port in MCP Studio (See* Serial Maintenance Port *on page 443)*.
- Default Serial Ports Modes (Advanced->Super IO Configuration)
  - Please ensure are enabled/disabled as required for secure hardening purposes and set to RS-232.

Users should check again these UEFI settings when the G100 is powered on again, and adjust as necessary.

MCP Time Synchronization

Time Synchronization Configuration

Time synchronization configuration workflows use:

- Online MCP Local Configuration Utility (***mcpcfg***) or MCP ***Settings GUI*** for configuring time synchronization for PTP/IRIG-B/NTP
- DS Agile MCP Studio configuration tool for configuring SCADA based time synchronization

Time Synchronization Input

G100 accepts the following methods for time synchronization input sources (IN):

- IRIG-B TTL
  - B002 without YEAR information
  - B006 with YEAR information
- NTP
- SCADA

G500 accepts the following methods for time synchronization input sources (IN):

- PTP (Precision Time Protocol - IEEE 1588)
- IRIG-B TTL
  - B002 without YEAR information
  - B006 with YEAR information
- NTP
- SCADA

Time Synchronization Output

G100 provides the following time synchronization output signals (OUT):

- IRIG-B TTL – only repeater of IRIG-B IN
- NTP
- SCADA

G500 provides the following time synchronization output signals (OUT):

- PTP (Precision Time Protocol - IEEE 1588)
- IRIG-B TTL (B002 without YEAR information)
- NTP
- SCADA

SCADA Time Synchronization Applications

MCP provides time synchronization using the following SCADA communication protocols:

- DNP3 Master (Server) as Time Source Input
- IEC60870-101/104 Master (Server) as Time Source Input
- DNP3 Slave (Client) as Time Signal to IEDs (OUT)
- IEC60870-101/104 Slave (Client) as Time Signal to IEDs (OUT)

Table 1.1: Available Time Sync Combinations

IN \ OUT	PTP OUT	IRIG-B TTL OUT	NTP OUT	SCADA OUT (to IEDs)
PTP IN	✓ G500	✗ Not Available	✓ MCP	✓ MCP
IRIG-B TTL IN	✗ Not Available	✓ MCP Note 2	✓ MCP	✓ MCP
NTP IN	✗ Not Available	✗ Not Available	✓ MCP	✓ MCP
SCADA IN (from Masters)	✗ Not Available	✗ Not Available	✓ MCP	✓ MCP
NONE IN	✗ Not Available	✗ Not Available	✓ MCP Note 1	✓ MCP Note 1

NOTE

MCP indicates is applicable to both G100 and G500.

NTP/ SCADA are being driven from the software.

Note 1 In absence of any valid time source input, the MCP CPU is free running. Please refer to the G100 and G500 Instruction Manuals and Data Sheets for free running clock accuracy data (ppm deviation).

G500:

- PTP/ IRIG-B OUT in G500 are being driven from an internal high accuracy FPGA.
- When PTP/IRIG-B Input is enabled and a valid PTP/ IRIG-B Signal is present, G500 FPGA synchronizes the time to the CPU and an internal Real Time Clock (RTC), and the CPU in turn provides time as a source to NTP OUT or SCADA OUT (i.e. to IEDs via supported SCADA protocols).
- The internal RTC is powered by a super capacitor, and its value is used at startup if the super capacitor was not discharged. If the super capacitor was discharged the system will use the last valid time when was last powered on. Please refer to the G500 Instruction Manual and Data Sheet for the super capacitor time availability when the unit is powered off.
- When NTP/SCADA are used as time synchronization input sources, the internal CPU does not act as a time source of synchronization to the G500 FPGA and the G500 PTP/IRIG-B outputs are disabled.

G100:

- **Note 2** IRIG-B OUT in G100 is repeated from the IRIG-B IN signal, there is no internal FPGA to generate the signal
- When IRIG-B Input is enabled and a valid IRIG-B Signal is present, G100 software based decoding synchronizes the time to the CPU, which in turn provides time as a source to an internal Real Time Clock (RTC), NTP OUT or SCADA OUT (i.e. to IEDs via supported SCADA protocols).
- The internal RTC is powered by a super capacitor, and its value is used at startup if the super capacitor was not discharged. If the super capacitor was discharged the system will use the last valid time when was last powered on. Please refer to the G100 Instruction Manual and Data Sheet for the super capacitor time availability when the unit is powered off.
- When NTP/SCADA are used as time synchronization input sources, the G100 does not provide an IRIG-B OUT time signal.

NOTICE

A system's Time-Sync accuracy cannot be guaranteed if you enable multiple time-sync inputs.

In the Gateway Configuration Utility (mcpcfg, Settings GUI), it is not allowed to configure more than one time source input from PTP / IRIG-B / NTP. If one of these time sources is configured, please make sure the time synchronization in SCADA applications are all disabled to avoid conflicts.

Or, if the time synchronization from one of the SCADA Master applications is configured, all the PTP/IRIG-B/NTP time sources should be disabled to avoid conflicts.

MCP Settings

This part of the configuration is associated with the MCP hardware, UEFI, Serial port settings, LAN configuration, Time settings, Administrators User management etc.

These configuration settings are performed online using either MCP Local Configuration Utility (mcpcfg) or MCP Settings GUI, or a browser-based utility called Predix Edge Technician Console (PETC) or the MCP Runtime HMI.

MCP Firmware Version Information

» To check firmware release information:

1. Go to the MCP command line interface using Secure Terminal Emulator.
2. Type **cat /home/ MCP_APPS/version_banner**.
3. Press **Enter**.

Local Configuration Utility (mcpcfg) or MCP Settings GUI

MCP supports Local configuration utility (mcpcfg) or MCP Settings GUI to manage the MCP real time/hardware/system settings.

Serial Ports Settings

All the MCP supported serial port modes (RS232/485) are configured using online MCP Local Configuration Utility (mcpcfg) or MCP Settings GUI.

Ethernet Settings

All the MCP network interfaces are configured using online MCP Local Configuration Utility (mcpcfg) or MCP Settings GUI. In addition to the Gateway connectivity, a browser-based utility called Predix Edge Technician Console (PETC) is used to configure the Maintenance Port for Edge connectivity.

Refer to Chapter 8 - EdgeManager and PETC for port availability and additional information.

The remaining Ethernet Ports are used for SCADA/Gateway connections and Edge Connectivity which can be enabled on one designated port. User can configure them using "single" mode of configuration using mcpcfg.

Administrators User Setup

MCP comes from the factory has a default administrator user “defadmin”. Only minimal configuration options (i.e. Adding a New/Nominated administrator user, Configuring IP Addresses, Rebooting the unit and Restoring MCP Snapshots) are available using default administrator user.

The default administrator (defadmin) user will be deleted automatically once the default administrator (defadmin) is logged out and logs in successfully with the newly added administrator user.

MCP Configuration

This section provides an overview of each DS Agile MCP studio and the basic steps to configuring the MCP.

G100 devices can be converted to G500 devices.

G500 devices can be converted to G100 devices, with the user required to resolve and re-alocate the less available ports in G100 (Serial, Net).

This part of the configuration is associated with the configuring Gateway/SCADA specific configuration using DS Agile MCP Studio’s offline and online configuration tools. This configuration includes configuring IEDs/master stations/automation applications/HMI settings/security settings or system configurations etc. The user would like to customize the following aspects of the MCP configuration management through offline and online editors using DS Agile MCP studio:

- Communication connections
- Device data collection
- Master Station data presentation
- Alarm annunciation
- Data calculation
- Data logging
- Operational (One-Line) diagrams
- User management
- HMI preferences
- E-mail notification
- Open VPN and Secure SCADA
- Passthrough and Terminal server
- Device Redundancy

System/PC Requirements

Minimum Windows 7 x64, 10 x64 and 8GB Memory required for DS Agile MCP Studio and MCP Runtime HMI.

The MCP Runtime HMI runs as a standalone application, so the installation of the Java/JRE on the Windows PC is not required.

DS Agile MCP Studio Software Version Information

Refer to DS Agile Studio Configuration Guide for the supported DS Agile MCP Version details.

Offline Editor

The Offline Editor is used to create, edit and update the software configuration of the MCP. The Offline Configuration Tool is a component of the DS Agile MCP Studio.

Offline Editor (DS Agile MCP Studio) is used to:

- Set up MCP communications to devices and masters (serial or network connections)
- Select and/or create point maps (for devices and masters)
- Configure alarms
- Create custom data calculations
- Set system preferences
- Create one-line diagrams
- Create Secure SCADA and Open VPN server configurations

All these configurations changes will not take effect until “Sync To” operation is performed through DS Agile MCP studio.

One-Line designer

The One-Line Designer is a specialized drawing tool for creating substation one-line diagrams and forms, such as a Digital Event Manager panel. The One-Line Designer is accessed from within the DS Agile MCP Studio Offline Editor/Configuration Tool.

You must have either Administrator or Supervisor privileges to access the offline configuration tool. It is suggested that either one Administrator or Supervisor user at a time can be logged in to perform configuration functions.

This manual provides detailed information on the configurable settings in the MCP, and how to configure the MCP to work with various aspects of the substation system.

For more information about using the MCP offline Configuration Tool, functions and screens refer to the MCP online Help in DS Agile MCP Studio.

Online Editor

The Online Editor monitor the status of your substation network, view data, execute control commands and change the system set-up by connecting to the MCP. In addition to this, Online Editor can also be used to configure MCP SCADA and Gateway configuration including One-Line Diagrams. The Online Editor includes the following components:

- Online Editor is used to view and control the operation of the MCP.
- Online Editor includes optional One-Line Viewer for viewing one-line diagrams.
- Power Bar buttons also give access to MCP display screens and utilities.
- SCADA/Gateway configuration including One-Line Designer in the Connected Mode to MCP.

IEC 61850 Loader (optional)

The IEC 61850 Loader (referred to as the Loader) is specifically designed to configure the MCP to communicate to IEC 61850 compliant server devices using the MCP's IEC 61850 client application. The Loader makes use of the self-description capabilities of the IEC 61850 protocol and device information files provided by most devices to simplify and speed up configuration of the IEC 61850 client application.

The IEC 61850 Loader within DS Agile MCP studio is used to configure and upload the IEC 61850 client application to the MCP.

For more information on using the IEC 61850 Loader, see the Loader Help in DS Agile MCP studio.

LogicLinx (optional)

LogicLinx is a tool that enables the user to create automation applications that have traditionally been too costly or difficult to implement - all without hard wiring. Using any or all the IEC 61131-3 programming languages, the user can create automation routines that run on the MCP.

LogicLinx automation routines are created using the LogicLinx editor. The LogicLinx Wizard within DS Agile MCP Studio is then used to configure and upload the LogicLinx application to your MCP.

For more information on using LogicLinx, refer to the LogicLinx on a MCP *Quick Start Guide (GE Ref Number-SWM0107)*.

Snapshots

"Snapshot" is an archived image of the device configuration taken (that is, *saved*) at a given time, in the form of a special compressed file. It can be saved using DS Agile MCP Studio, which includes all settings required to completely recover a MCP device.

- Multiple snapshots can be saved for the same device configuration, at different times, using different names with different storage paths.
- A snapshot can be *restored* to the same device or to a different device.
- The MCP Gateway device must be configured for SSH and SFTP services, for this feature to be used.
- The Snapshots greatly reduce time when replacing hardware (MCP) and copying a reference configuration to multiple devices, eliminating the need for additional manual configuration

Snapshot restoration updates the new MCP (i.e., target MCP) with the following hardware and software settings as were defined in the original MCP (i.e., source MCP), at the time of the snapshot was taken, if the respective options were selected to be saved:

- User Authentication
- Network Settings
- Network Interfaces
- Secure Access
- Firewall settings
- Host Names
- Time settings and time synchronization
- Local HMI settings – except number of displays and displays resolution which are specific to the MCP being restored
- Synch Manager
- Redundancy (except paired keys when the MCP target is already paired as redundant) (Not supported in G100)
- Emulation of D20 IEC101 DPA Unbalanced Mode and quality event suppression at startup
- Serial port modes (RS232/485, 2/4 wires)
- Configuration implemented in MCP Studio:
    - Connections
    - Client and Server Map files
    - System Point Manager
    - Alarms
    - Calculator
    - Data Logger (storage may need to be re-adjusted if the target MCP has different storage sizes)

- Load Shed
- Systemwide (storage may need to be re-adjusted if the target MCP has different storage sizes)
- Access (Local users, Automatic HMI login settings, VPN Client List)
- ARRM
- AI Text Enumeration
- One-line Screens
- Analog Reports
- IEC61850 Client
- LogicLinx

Cyber security related Certificates are not included in the Snapshot, and therefore cannot be restored. To comply with cyber security requirements, all certificates must be imported again to the target MCP, after the snapshot is restored. All secure connections using certificates must be re-associated with the new imported certificates (e.g. Secure Connection Relay, VPN Server, etc.)

Snapshot restoration results in a MCP configured into Local Authentication mode, even though snapshot contains the Remote Authentication (this is to avoid possible lockout scenarios). However, all the Remote Authentication configuration settings will get restored as part of snapshot. User need to re-install the certificates and reconfigure the Remote Authentication using the restored configurations.

The keys associated with Sync Manager (rsync/SSH, SFTP), Modbus TCP/SSH secure tunnel and ARRM SFTP are not restored with snapshot due to cyber security requirements, and these sessions shall have to be re-paired again by user.

License file (key) is not restored with the snapshot because this is hardware ID specific.

MCP enrollment in EdgeManager Cloud and associated settings are not restored with the snapshot. Refer to Predix Edge Technician Console - See **PETC** for more details.

Snapshot Compatibility

The following table shows the Snapshot Compatibilities between DSAS and GE's Gateway devices:

FULL "Clone" Snapshot compatibility Configuration+Settings (using DSAS 2.1 or later)		Restore snapshot (Configuration and Settings) **to target device:**				Restore snapshot (Only Configuration part) **to offline device:**			
Save snapshot **from device:**		**D400**	**MCP (G500/G100 within same type)**			**D400**	**MCP (G500/G100 within same type)**		
		Any version	**1.00**	**1.10**	**2.00 or later**	**Any version**	**1.00**	**1.10**	**2.00 or later**
D400	<= 5.20	YES ONLY same D400 and same version	N/A	N/A	N/A	YES Direct same version	N/A	N/A	N/A

	5.30 or later	YES ONLY same D400 and same version	N/A	N/A	N/A	YES Direct same version	Indirect Via Create MCP	Indirect Via Create MCP	Indirect Via Create MCP
MCP	1.00	N/A	YES ONLY same MCP	N/A	YES ANY MCP	N/A	YES Direct	Indirect Via Offline Upgrade	Indirect Via Offline Upgrade
	1.10	N/A	N/A	YES ANY MCP	YES ANY MCP	N/A	N/A	YES Direct	Indirect Via Offline Upgrade
	2.00 or later	N/A	N/A	N/A	YES ANY MCP	N/A	N/A	N/A	YES Direct same version

Note: The above table also shows the snapshot compatibility of DSAS with D400® Substation Gateway.

Snapshot Management

Using DS Agile MCP Studio:

- Snapshots can be saved from the MCP using only administrator user credentials.
- Snapshots can be restored to the MCP using the "**defadmin**" default credentials or any other configured administrator user credentials.

Types of Snapshots

There are two types of snapshots:

1. **Standard Snapshot**
   - Standard Snapshot is used between one MCP to any MCP of same firmware version.
   - Standard snapshot may contain user credentials, internal saved secrets, Network settings and Logs – if the user selects the option to include them.
   - The name of the Standard Snapshot ends with the extension - ***.MCPSnapshot.DS7zip**
     - e.g. ***MCP_V100*.MCPSnapshot.DS7zip**, while saving the Standard Snapshot (the *italic* text is entered as *name* by the user)
2. **MCP Clone Snapshot**
   - MCP Clone snapshots contain all information associated with a running MCP (configurations, settings, users, internal configured "secrets" for IED access, etc. – except certificates).
   - MCP Clone Snapshots are the primary instrument used as source image in "disaster recovery" workflows.
   - MCP Clone Snapshots may be used with the same firmware version or across different firmware versions from one version to a newer one.
   - The name of the MCP Clone Snapshot contains the extension - ***.MCPCloneSnapshot.DS7zip**

- e.g: ***Test5_1_dot_0*.MCPCloneSnapshot.DS7zip**, while saving the MCP Clone Snapshot (the *italic* text is entered as *name* by the user)

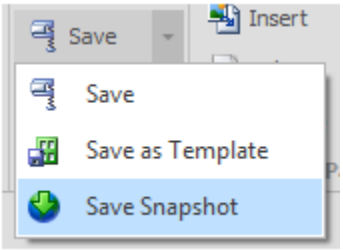
Please refer to the Application Note *AN0015 MCP Snapshot and Configuration Workflows* for a full understanding of the included data types in snapshots of both types and their associated save / restore options in workflows.

Saving a Standard Snapshot

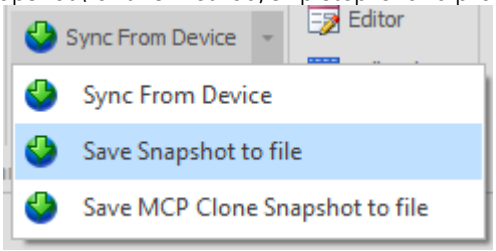
1. Select the device for which Standard snapshot to be saved. The device appears within a green box with anchor points, as shown below:

2. Various methods to save Standard Snapshot are given below with detailed steps. Standard snapshot can be saved by any of the below methods:
   a. Right click on the device,
   Archive → Save → Save Snapshot

   b. From the top ribbon,
   Save → Save Snapshot

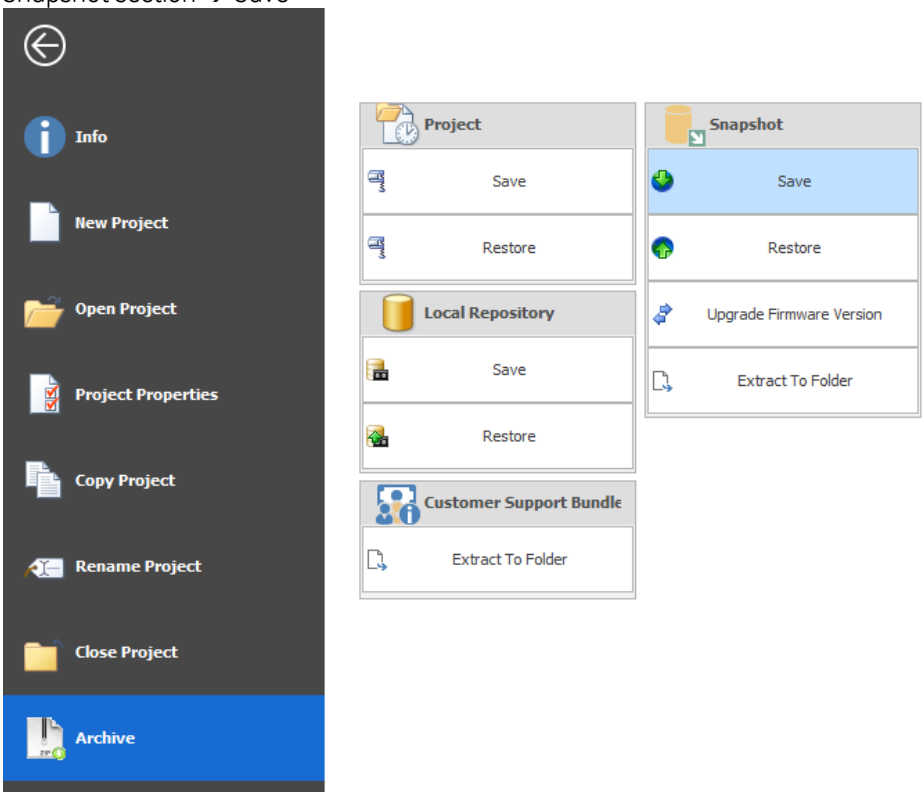


   c. Sync from Device → Save Snapshot (for this method, skip step '3' and proceed to step '4')

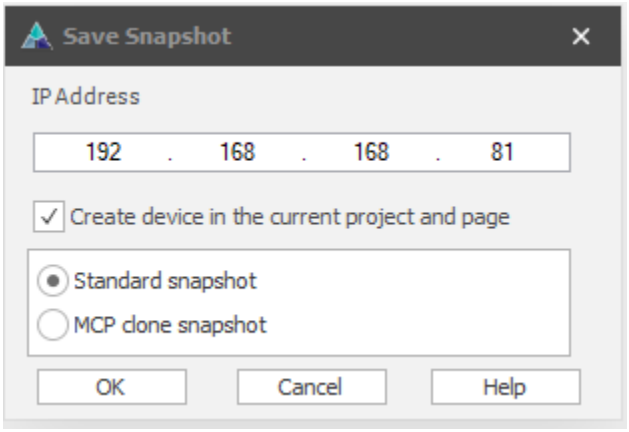


   d. File menu,

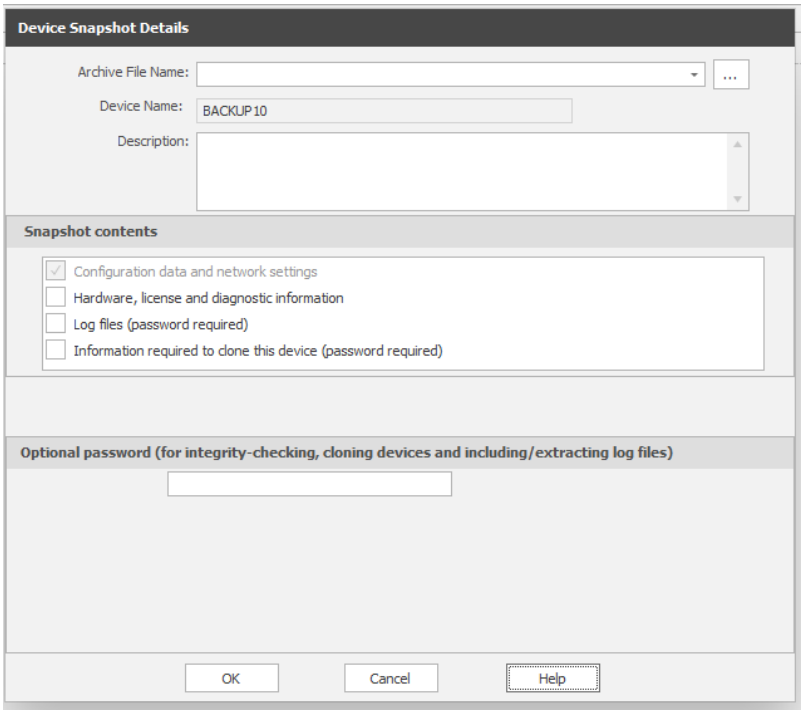
i. Archive → Snapshot section → Save



3. Then (except for step '*2(c)*'), specify the IP address of the source MCP and type of snapshot as 'Standard', as shown below:



4. Then, a window "Device Snapshot Details" pops up, as shown below.



5. Specify the below details:
   - **Archive** (snapshot) **File Name**
     - Type in the file name and path (or)
     - Click the **[...]** button to navigate to the storage location.
   - View the **Device Name**. This read-only field shows the DS Agile Studio device name.
     - Type a **Description** into this free-form text field.

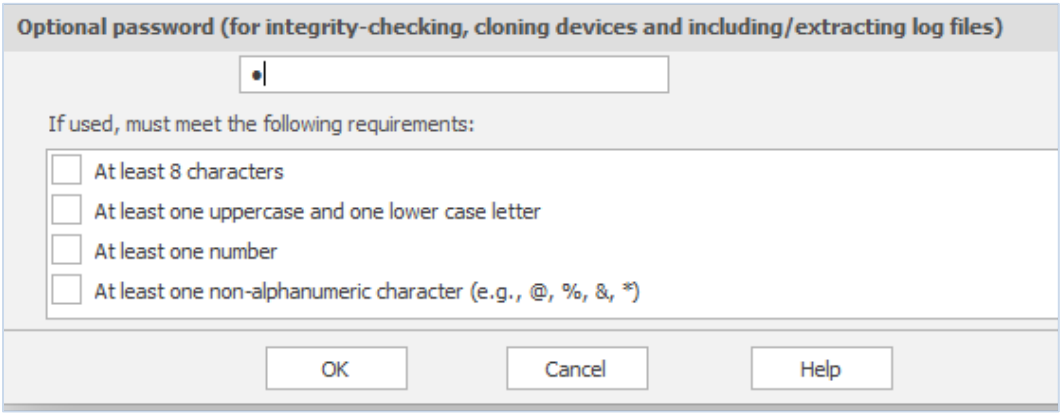
   Choose what data is to be saved in the device **Snapshot contents** by selecting the required checkboxes:

Configuration data and network settings	:	All snapshots contain configuration data and network settings; this checkbox is always selected by default.
Log files	:	Log files are created by the MCP Gateway device.
Hardware, license and diagnostic information	:	This information is used by the GE Grid Solutions Technical Support team.
Information required to clone the device (password required)	:	This additional information allows you to clone an existing configuration.

6. Type in an **Optional password (for integrity checking)** and make sure it meets password strength requirements.
7. If the device contains internal configuration "secrets" (e.g. IED or ARRM passwords used for Machine to Machine connections) – a password is mandatory to protect the snapshot. Alternatively, the user has a choice to remove the "secrets".

   Important: This password is used only to protect the snapshot that will be created. This is separate from any passwords used for user credentials or other "secrets" configured in the device. Ensure that this snapshot password is available if restoration is required later. There is no alternative method through GE Grid Solutions to obtain the correct password.

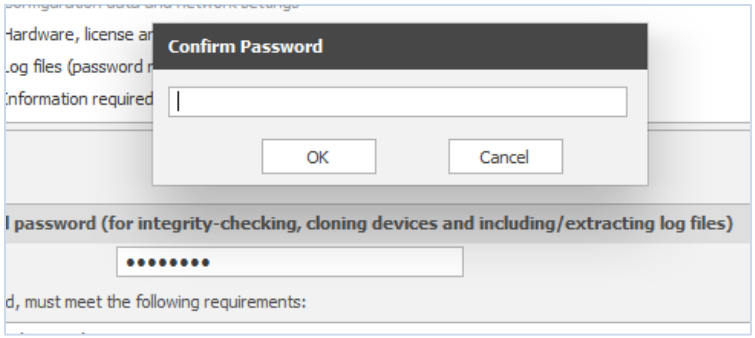
When you begin typing characters in the password field, additional information is presented, guiding you to meet password strength requirements.



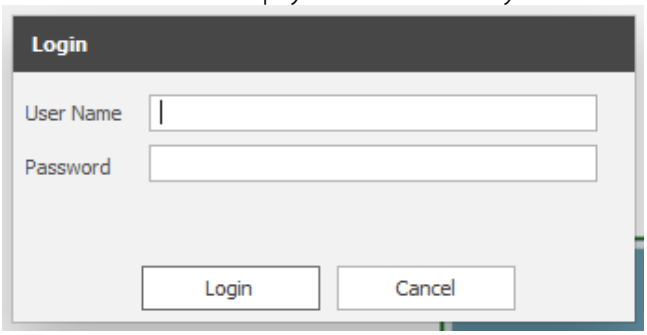
The tracking and checking of snapshot (archive) file integrity and non-tampering may be disabled from the Global System Preferences window:

i. For all **Snapshot contents** options except Information required to clone the device, the snapshot file may be optionally secured by specifying a password.
ii. If the device contains internal configuration "secrets", a password is mandatory to protect the snapshot. Alternatively, the user has a choice to remove the "secrets".
iii. If a password is provided, DS Agile Studio can check the snapshot (archive) file for **integrity and non-tampering** at restoration time.
iv. If a password is not provided, the snapshot (archive) file is valid, but does not contain information used for integrity and tamper-proof checking at restoration time.
v. When a password is provided, the snapshot file content – except (Information required to clone the device) – is not encrypted, allowing users who forgot the password to restore the snapshot data, but without the integrity check.
vi. For the **Snapshot contents: Information required to clone the device** option, sensitive data and information is included in the snapshot file; consequently, a password must be provided.
    - Sensitive data and information contain configured local user accounts, internal secrets like credentials used for IED access (e.g. SEL Binary access), ARRM secured file transfers parameters, and Dial-in and Email configuration.
    - If the **Snapshot contents: Information required to clone the device** option was chosen and a password is not typed in, the snapshot process does not continue, and you are prompted again to:
        - De-select the **Information required to clone the device** option (or)
        - Provide a password.

8. Upon clicking **OK**, a window pops up to re-enter and confirm the password, as shown below. Type in the password again and proceed.



9. Then, device login window pops up, as shown below. Authenticate as a valid administrator user, by providing the **User Name** and **Password** for the physical MCP Gateway device.

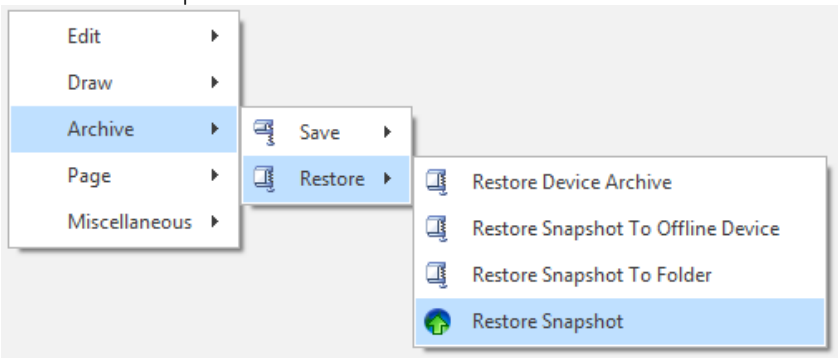


10. After successful login**,** the configuration files are downloaded from the MCP device and get saved in the specified location.

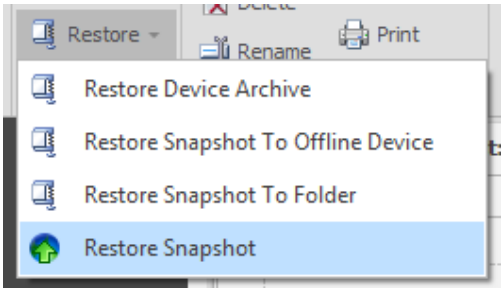
Restoring Standard Snapshot to a Device

1. Select the device for which Standard snapshot to be restored. The device appears within a green box with anchor points, as shown below:

2. Various methods to restore Standard Snapshot to a Device are given below with detailed steps. Standard snapshot can be restored by any of the below methods:
   a. Right click on the device,
      i. Archive → Restore → Restore Snapshot

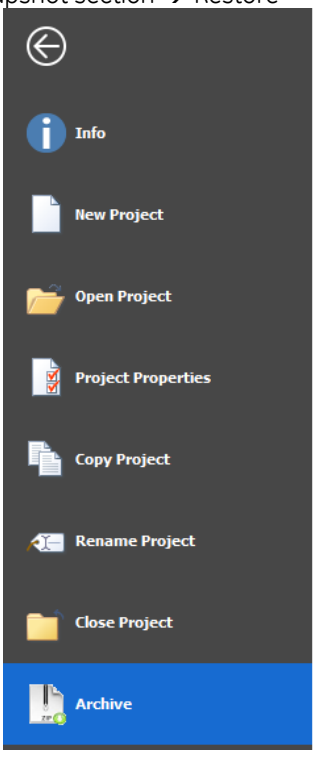


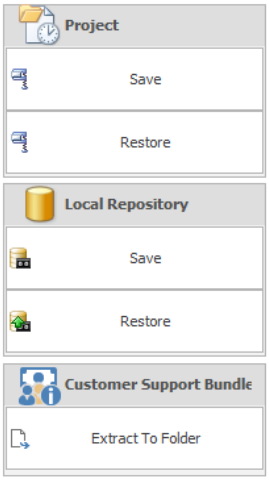
b. From the top ribbon,
- Restore → Restore Snapshot

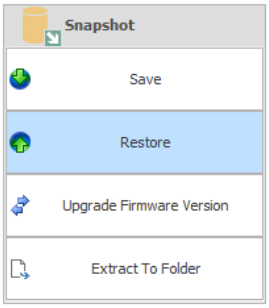


- Sync To Device → Restore Snapshot to Device

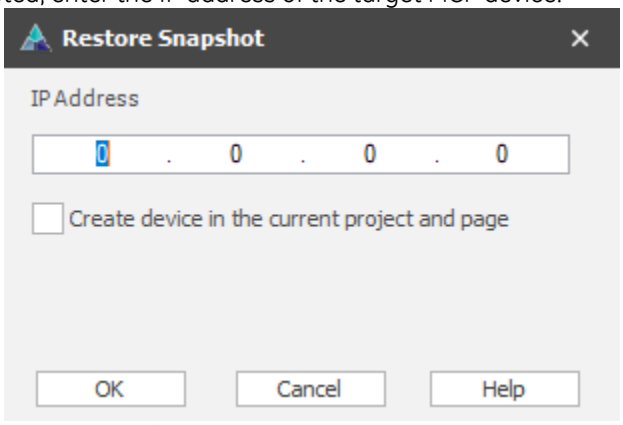
c. File menu,
- Archive → Snapshot section → Restore





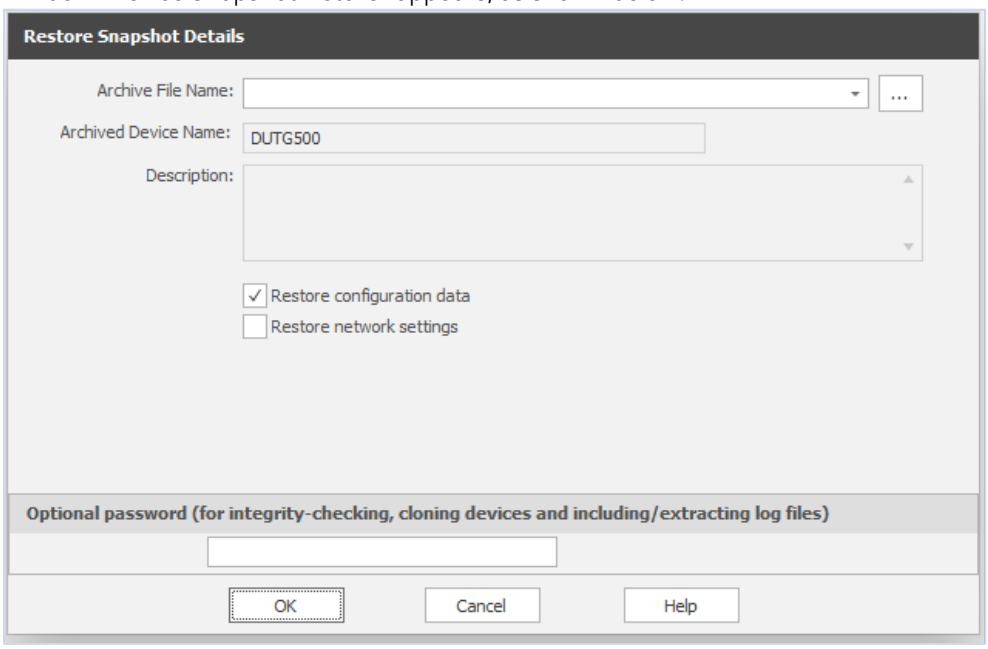


1. If prompted, enter the IP address of the target MCP device:

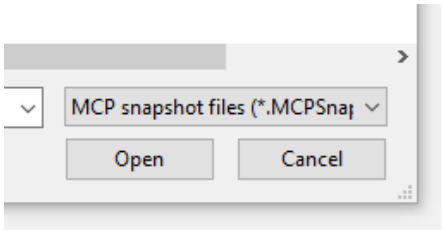


Note: if the workflow was started in the context of a device in the project, the IP address configured for that device will be used automatically.

3. Then, a window "Device Snapshot Details" appears, as shown below:

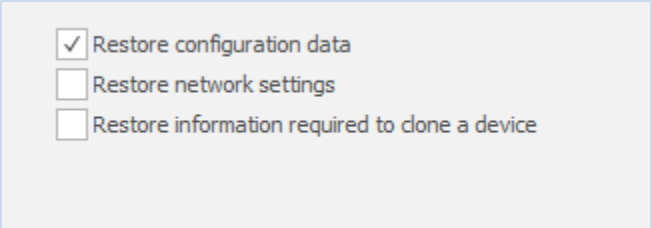


4. Specify the below details:
   - **Archive** (snapshot) **File Name**
     - Type in the file name and path (or)
     - Click the **[...]** button to navigate to the snapshot file location.
     - By default standard snapshots are filtered:



   - View the **Archived Device Name**. This read-only field shows the name of the archived device.
   - View the **Description** in this read-only text field; this is the description entered when the snapshot was saved.

- Select which type of data is to be restored:



Restore Configuration data : This option is selected by default as a minimum to be restored

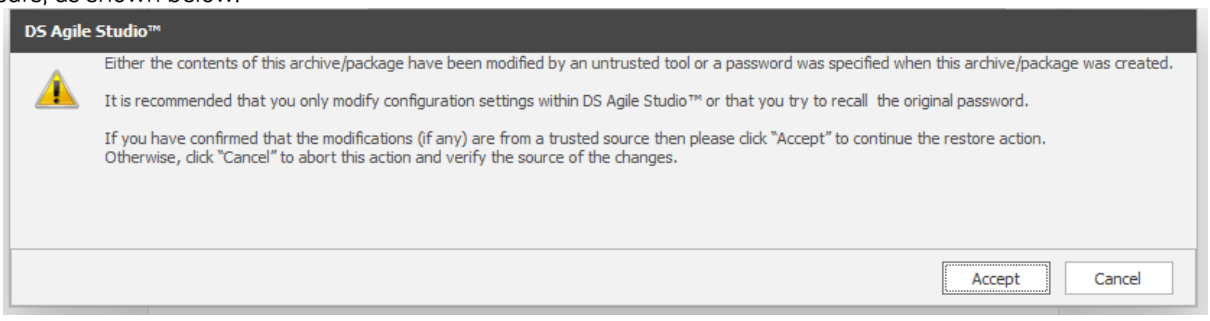
Restore network settings : This option is selected to restore the network settings

Restore information required to clone a device : This option is not available, if the snapshot file does not contain cloning information. To proceed with this type of data restoration, the correct password must be provided.

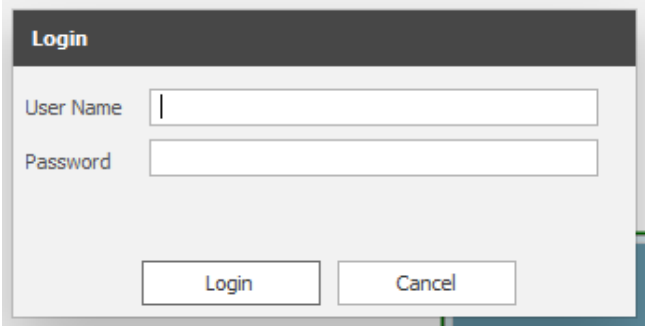
Hint:
Selecting this option will restore all saved users and their credentials and will overwrite existing users and credentials in the target MCP.
This is useful for deploying snapshots into MCP devices using the defadmin user account.
In some other cases it may be desired to restore the configuration and network settings, but not the previous saved users credentials, because they were lost, and restoring them would conduct to a MCP device that cannot be accessed. In this case, do not select this option.

- Type in an **Optional password (for integrity checking)**.
  - If the correct password (i.e. the same password entered when the snapshot was saved) is provided at this time, DS Agile Studio will check the snapshot (archive) file for **integrity and non-tampering** and proceed to restoration of chosen data.
  - If a password is not provided at this time, the snapshot (archive) file is restored – except the cloning data – but cannot be checked for integrity and tamper proof.
  - If a password is not provided for a snapshot file that was created with encrypted cloning sensitive information – then the restoration continues without the sensitive data information being recovered. In this case, all sensitive data will have to be re-entered again using the corresponding configuration fields.
  - Information can only be restored for cloning when the correct password is provided.

5. Click **OK** and then the "Device Snapshot Details" window closes, and a Restoration confirmation window appears, as shown below:



6. Click **Accept**, and then a login window appears, as shown below:

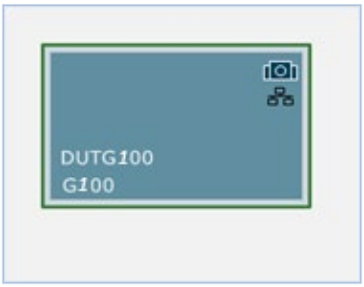


7. Authenticate as a valid administrator user and login to the device, by providing the **User Name** and **Password** for the physical MCP Gateway device
8. DS Agile Studio uploads the data file (Standard Snapshot) to the MCP Gateway device.

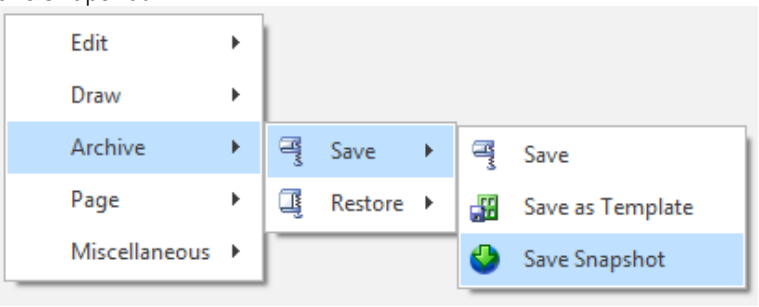
NOTE When restoring a snapshot image, the following data is not restored on the target device, even if was included in the snapshot file:
- Log files
- Hardware, license and diagnostic information

Saving an MCP Clone Snapshot

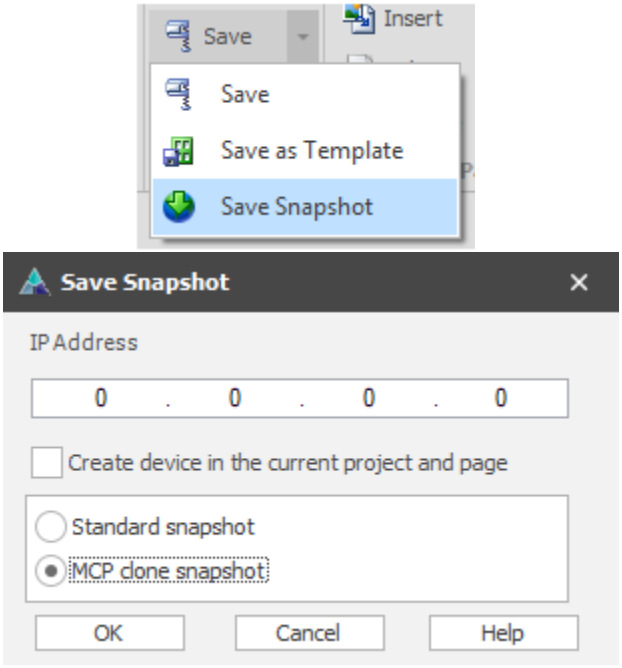
1. Select the device for which MCP Clone snapshot to be saved. The device appears within a green box with anchor points, as shown below:



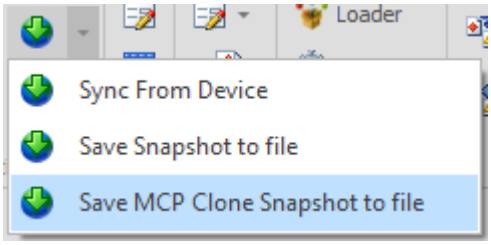
2. Various methods to save MCP Clone Snapshot are given below with detailed steps. MCP Clone snapshot can be saved by any of the below methods:
   a) Right click on the device,
   Archive → Save → Save Snapshot



   b) From the top ribbon,
   Save → Save Snapshot

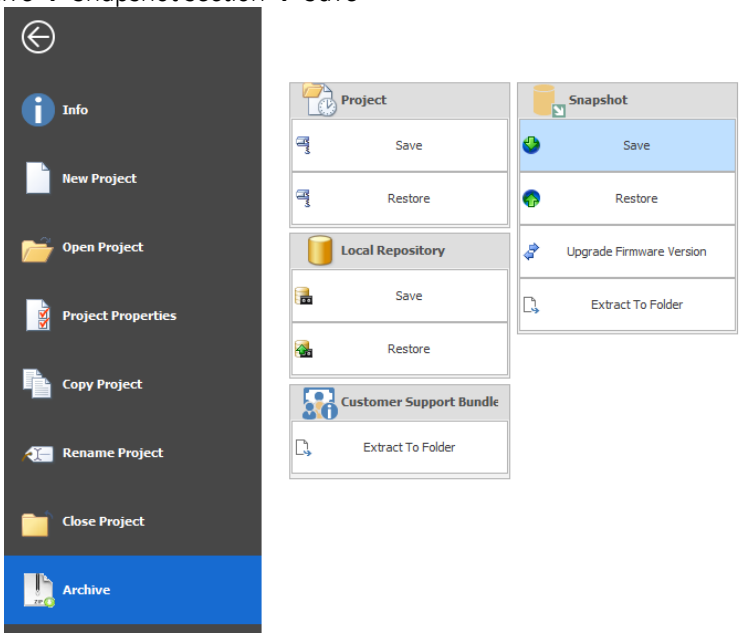


c) Sync from Device → Save Snapshot (for this method, skip step '3' and proceed to step '4')

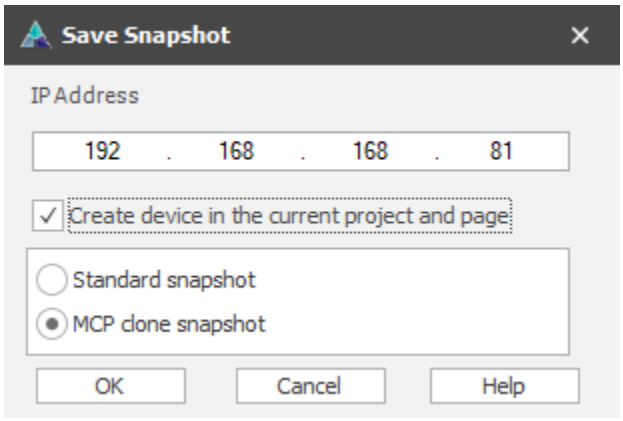


d) File menu,

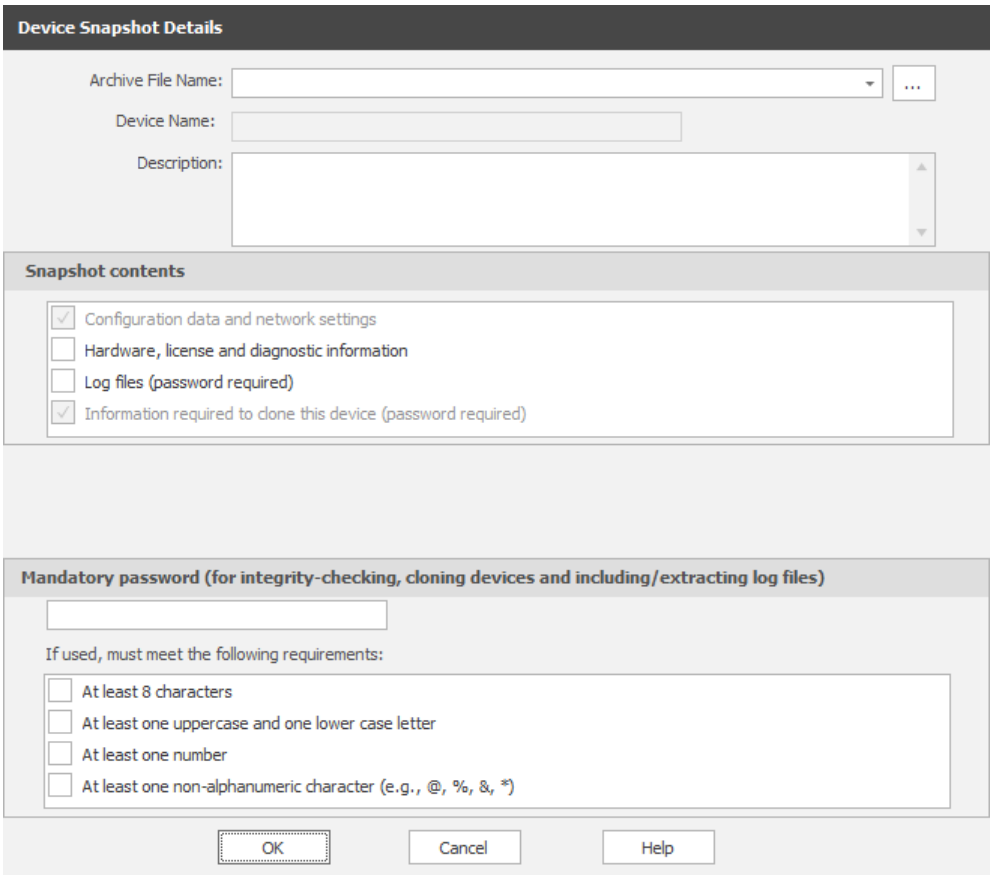
- Archive → Snapshot section → Save



3. Then (except for step '*2(c)*'), specify the IP address of the source MCP and type of snapshot as 'MCP Clone', as shown below:



4. Then, a window "Device Snapshot Details" pops up, as shown below.



5. Specify the below details:
   - **Archive** (snapshot) **File Name**
     - Type in the file name and path (or)
     - Click the **[...]** button to navigate to the storage location.
   - View the **Device Name**. This read-only field shows the DS Agile Studio device name.
   - Type a **Description** into this free-form text field.

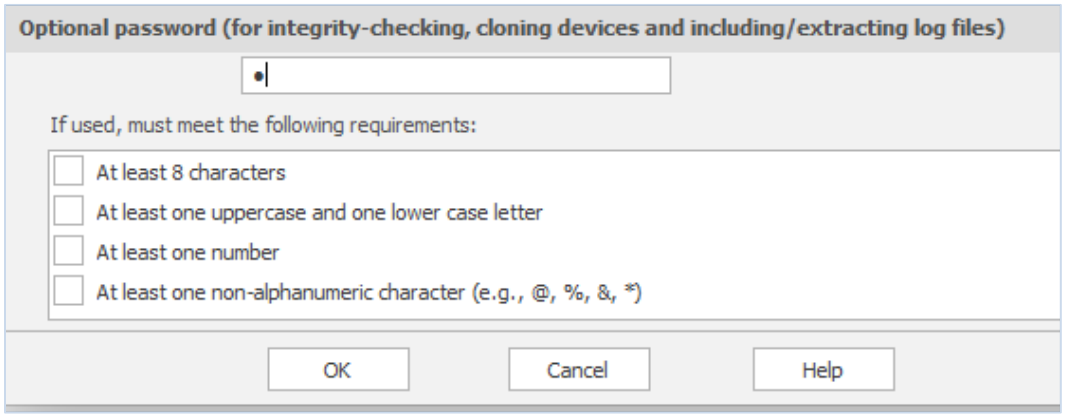
   Choose what data is to be saved in the device **Snapshot contents** by selecting the required checkboxes:

Configuration data and network settings	:	All snapshots contain configuration data and network settings; this checkbox is always selected by default.
Log files	:	Log files are created by the MCP Gateway device.
Hardware, license and diagnostic information	:	This information is used by the GE Grid Solutions Technical Support team.
Information required to clone the device (password required)	:	This information allows you to clone an existing configuration; this checkbox is always selected by default when saving MCP Clone snapshots.

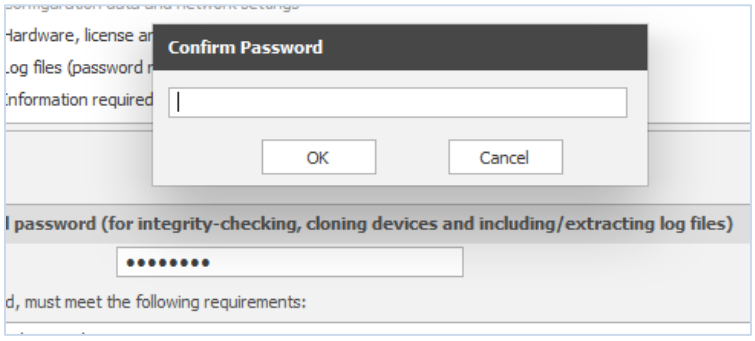
6. Type in the **Mandatory password** and make sure it meets password strength requirements.

   Important: This password is used only to protect the snapshot that will be created. This is separate from any passwords used for user credentials or other "secrets" configured in the device. Ensure that this snapshot password is available if restoration is required later. There is no alternative method through GE Grid Solutions to obtain the correct password.

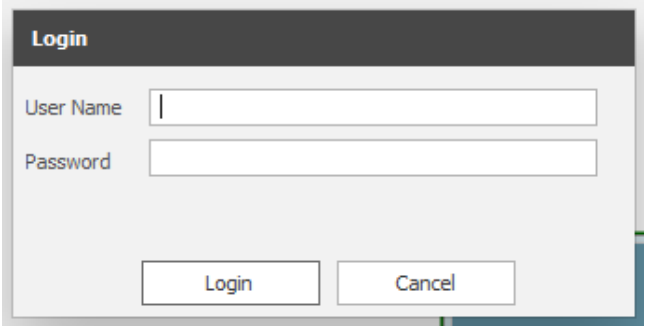
   When you begin typing characters in the password field, additional information is presented, guiding you to meet password strength requirements.



7. Upon clicking **OK**, a window pops up to confirm the password, as shown below. Type in the password again and proceed.



8. Then, device login window pops up, as shown below. Authenticate as a valid administrator user, by providing the **User Name** and **Password** for the physical MCP Gateway device.

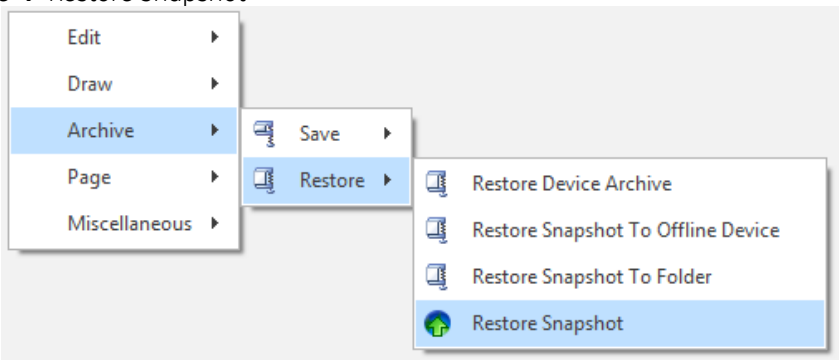


9. After successful login, the configuration files are downloaded from the MCP device and get saved in the specified location.

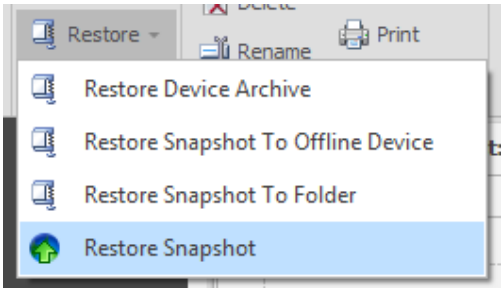
Restoring MCP Clone Snapshot to a Device (using DSAS)

2. Select the device for which the clone snapshot is to be restored. The device appears within a green box with anchor points, as shown below:

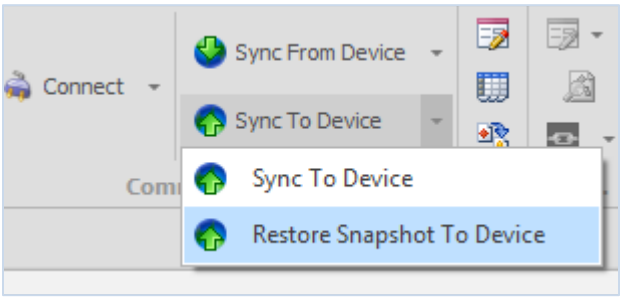
3. Various methods to restore Standard Snapshot to a Device are given below with detailed steps. Clone snapshot can be restored by any of the below methods:
   a. Right click on the device,
      i. Archive → Restore → Restore Snapshot



   b. From the top ribbon,
      - Restore → Restore Snapshot

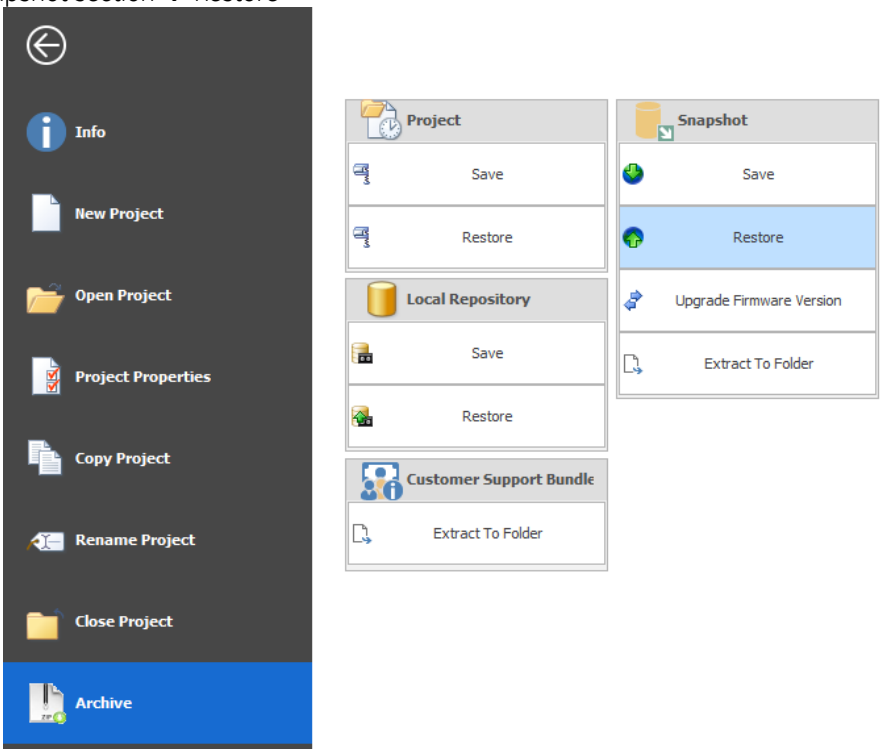


      - Sync To Device → Restore Snapshot to Device

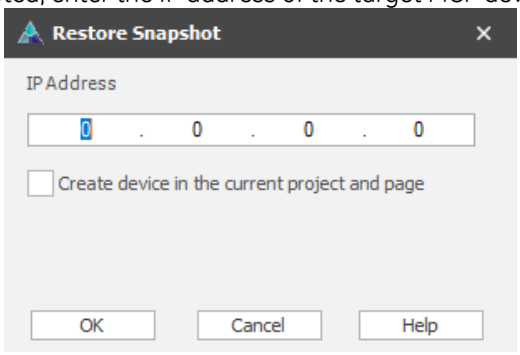


c. File menu,

- Archive → Snapshot section → Restore

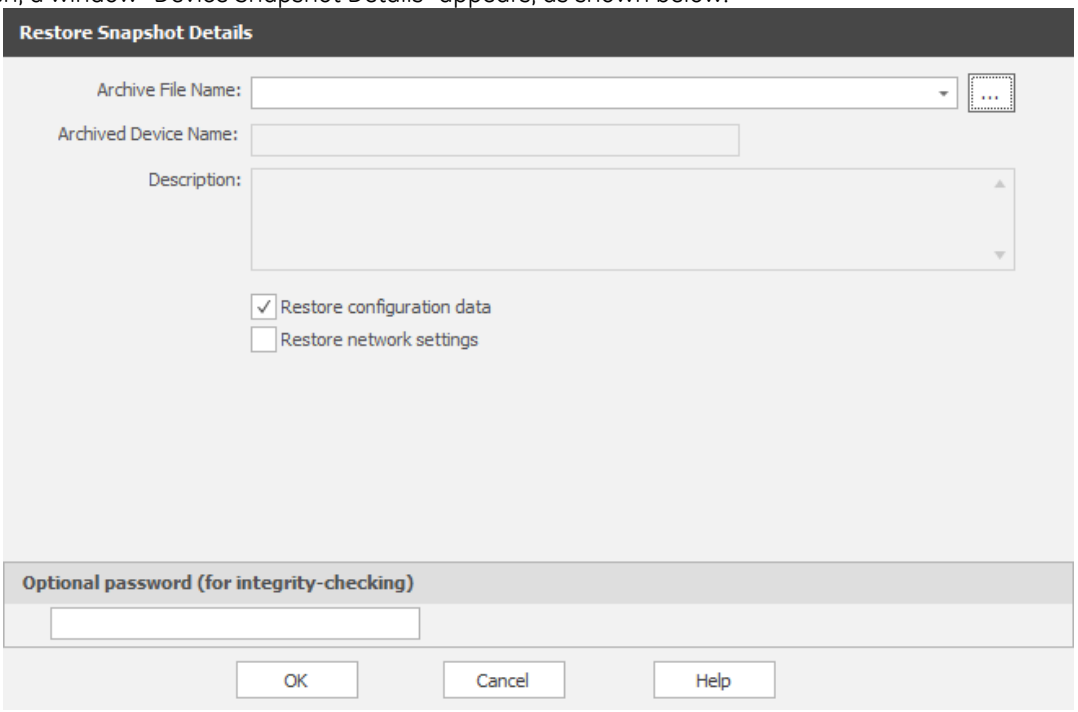


4. If prompted, enter the IP address of the target MCP device:

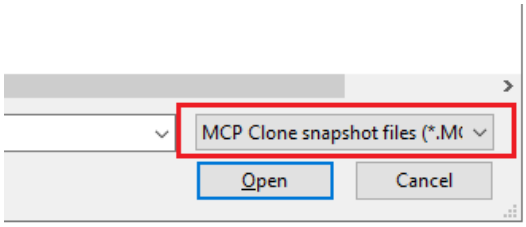


Note: if the workflow was started in the context of a device in the project, the IP address configured for that device will be used automatically.

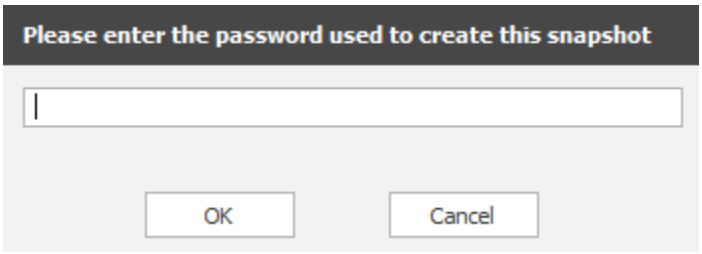
5. Then, a window "Device Snapshot Details" appears, as shown below:



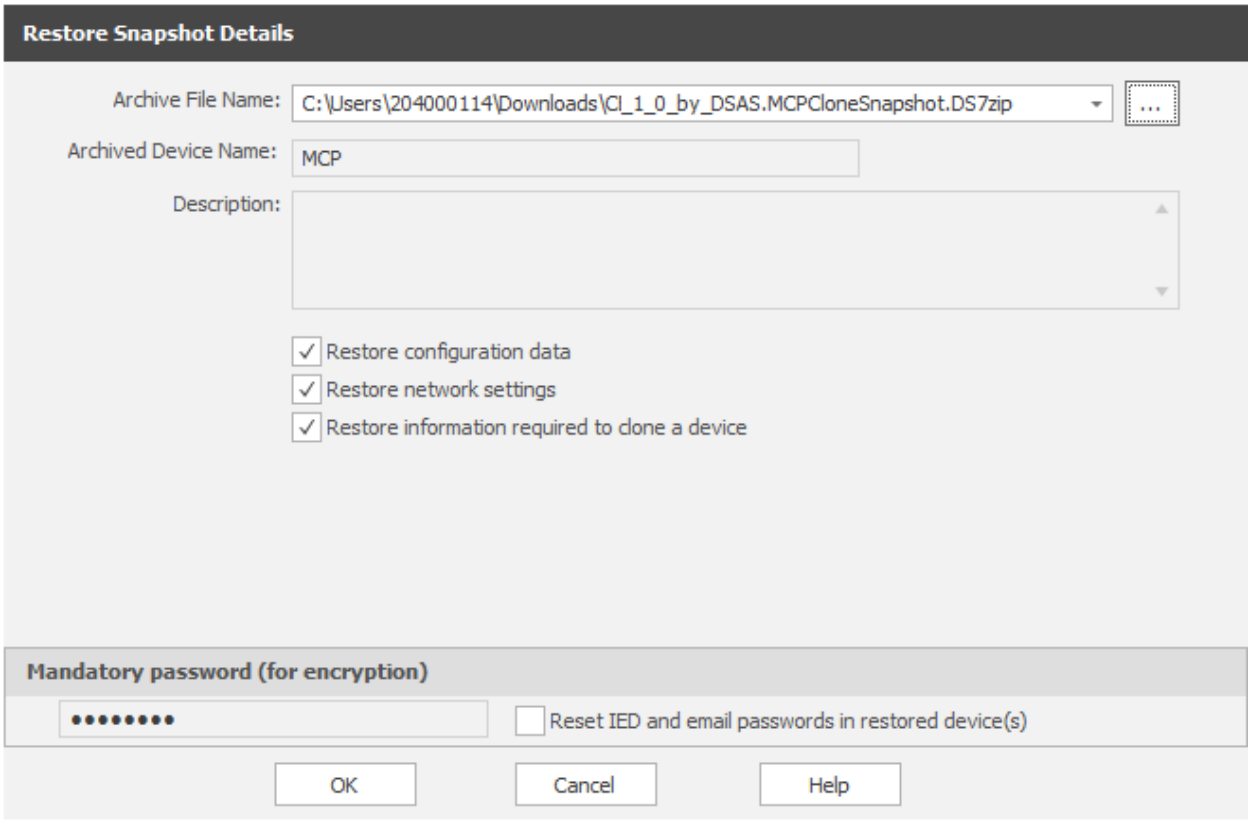
6. Specify the below details:
   - **Archive** (snapshot) **File Name**
     - Type in the file name and path (or)
     - Click the **[...]** button to navigate to the snapshot file location
     - Select the snapshot filter to MCP Clone:



   - Enter the password for the selected MCP Clone snapshot:

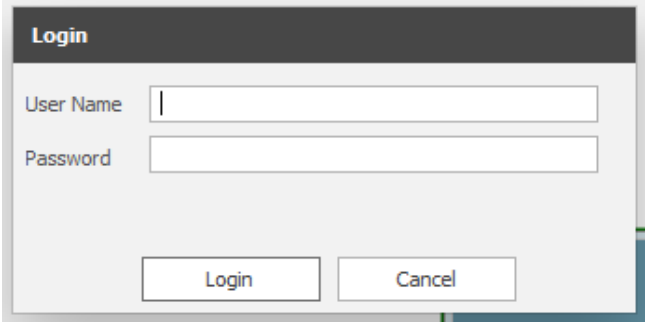


- Wait for the Processing message to end (it may take few minutes)
- The window will now change as following:



- View the **Archived Device Name**. This read-only field shows the name of the archived device.
- View the **Description** in this read-only text field; this is the description entered when the snapshot was saved.
- For MCP Clone snapshots all data types are selected to be restored and cannot be changed.
- At this step, if the selected MCP snapshot contains internal configuration "secrets", an option will be available to reset (erase) all.

7. Click **OK** and then a login window appears, as shown below:

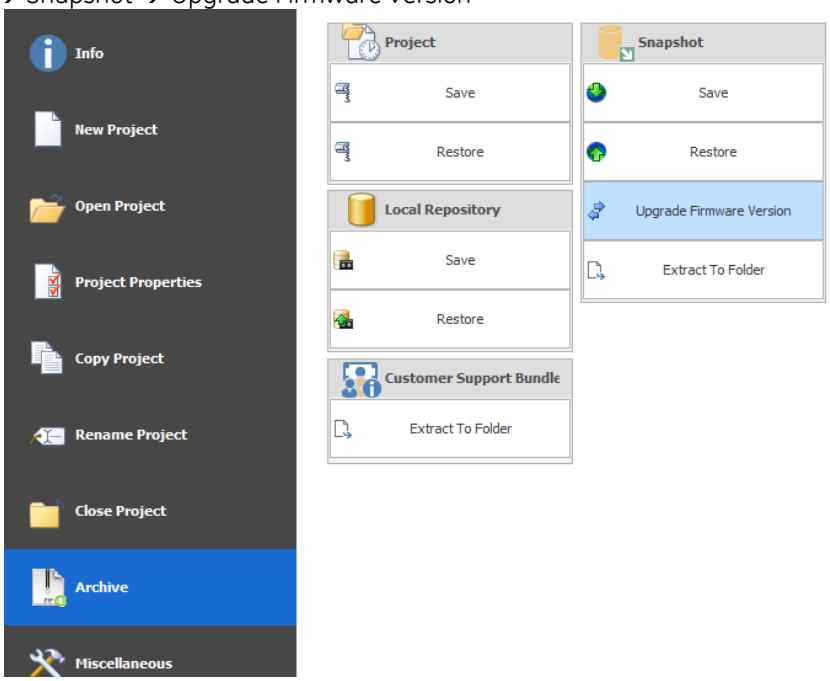


8. Authenticate as a valid administrator user and login to the device, by providing the **User Name** and **Password** for the physical MCP Gateway device
9. DS Agile Studio uploads the data file (Clone Snapshot) to the MCP Gateway device.

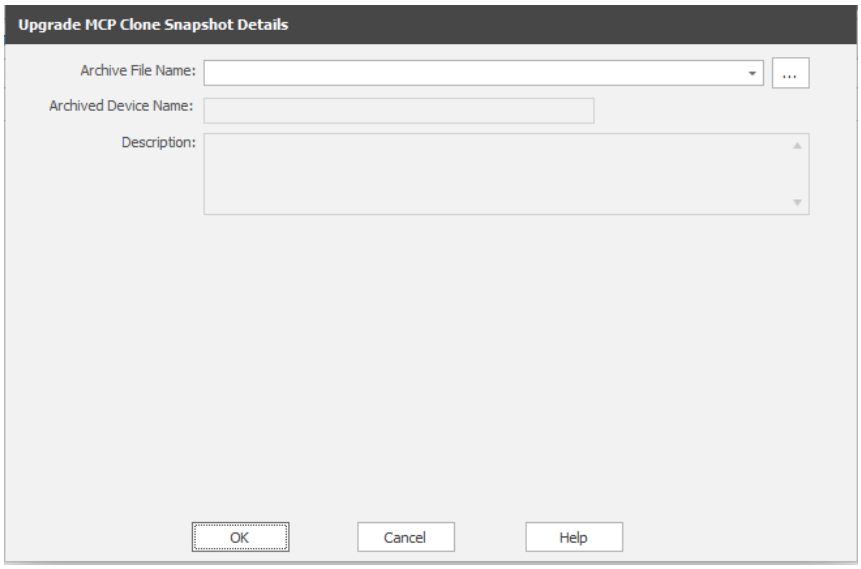
NOTE When restoring a clone snapshot image, the following data is not restored on the target device, even if was included in the snapshot file:
- Log files
- Hardware, license and diagnostic information

Upgrading MCP Clone Snapshot

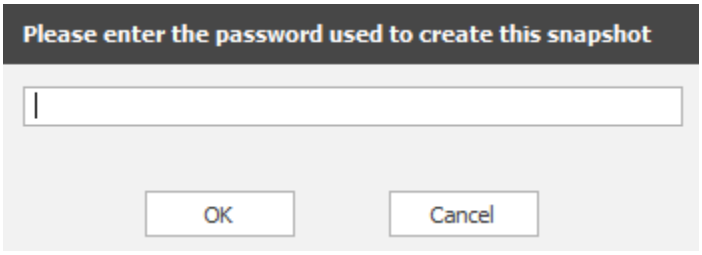
1. Open the file menu to upgrade the firmware version of the saved snapshot, as shown below :
   File → Archive → Snapshot → Upgrade Firmware Version



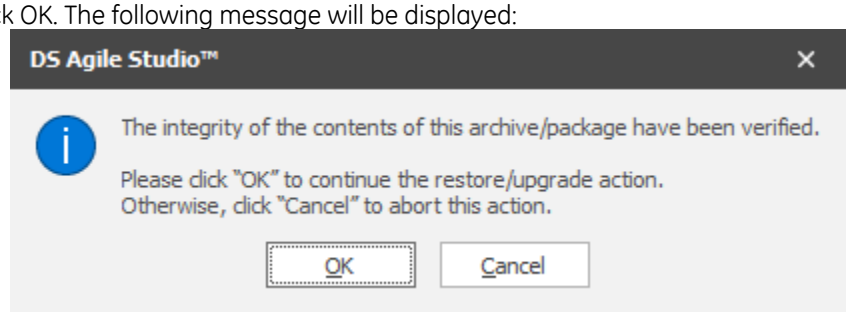
2. Upon clicking 'Upgrade Firmware Version', a window 'Upgrade MCP Clone Snapshot details' pops up, as shown below:



3. Specify and check the below details:
   - **Archive** (snapshot) **File Name**
     - Type in the file name and path (or)
     - Click the **[...]** button to navigate to the storage location.
   - Select desired MCP Clone snapshot
   - Enter the password for the selected clone snapshot:



   - View the **Archived Device Name**. This read-only field shows the name of the archived device.
   - View the **Description** in this read-only text field; this is the description entered when the snapshot was saved.
4. Click OK. The following message will be displayed:



5. This completes the upgrade procedure of the Clone snapshot and will be saved in the specified location as {ArchiveFilename}_v220.MCPCloneSnapshot.DS7zip

Restoring MCP Clone Snapshot using USB

An MCP Clone Snapshot can be restored to MCP in online (mcpcfg and settings GUI) and offline (USB) modes.

Online Clone Snapshot Restore (Using mcpcfg)

- Place the MCP Clone snapshot(s) on a USB formatted FAT32, e.g. using Windows File Explorer.
- Insert the USB in the target MCP
- Connect to MCP using Secure Terminal and with valid administrator user credentials.
- Launch mcpcfg -> Gateway Settings menu and the Select option #22 'Restore Clone Snapshot' from the menu, as shown below:

```
============================================================
        Gateway Settings Menu
============================================================

        0.   Back
        1.   Configure Authentication
        2.   Configure Network Settings
        3.   Configure Network Interfaces
        4.   Configure Secure Access
        5.   Configure Firewall
        6.   Configure Host Names
        7.   Configure Time & Time Sync
        8.   Reset System Logs
        9.   Reset Database Tables
        10.  Reset File Persistence Data
        11.  Local HMI
        12.  Configure Sync Manager
        13.  Redundancy
        14.  ARRM
        15.  Suppress Forced Qualities To Masters
        16.  Emulate D20 RTU IEC101 DPA Unbalanced Mode Functionality
        17.  Configure IEC101+104 DPA Startup Quality Event Suppress Interval
        18.  Configure Serial Ports
        19.  Configure D.20 Port Settings
        20.  EdgeOS Host
        21.  Clear Chassis Intrusion State
        22.  Restore Clone Snapshot
        23.  Restore Factory Default
        24.  Reboot Device

Enter Your Choice : ( Between 0 and 24 ): 22
```

- Confirm and acknowledge the Snapshot restoration (followed by a reboot) by pressing 'Y', as shown below:

```
============================================================
        Gateway Settings Menu
        Restore Clone Snapshot
============================================================


WARNING!!! This action needs REBOOT of the device.

Do you want to Restore Clone Snapshot[Y/N]: Y
```

- Then, list of clone snapshots available in the USB will be displayed on the screen, as shown below.

```
        ----------------------------------------
        List of Snapshots present in the USB.
        ----------------------------------------
                0.   Back
                1.   RAMU.MCPCloneSnapshot.DS7zip
                2.   TANTIMESYNC.MCPCloneSnapshot.DS7zip

        Enter Your Choice : ( Between 0 and 2 ): 1
```

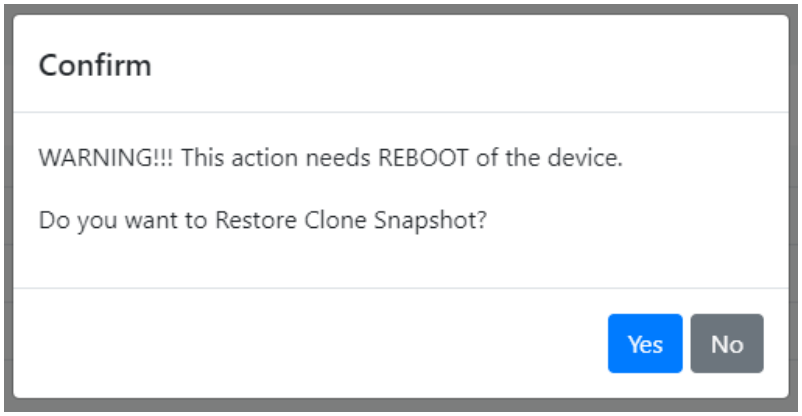
- Select the required snapshot to restored and enter corresponding password.
- Follow the instructions displayed on the screen to copy the clone snapshot from USB to MCP.
- After the automatic reboot, clone snapshot will be restored into the MCP.

Online Clone Snapshot Restore (Using Settings GUI)

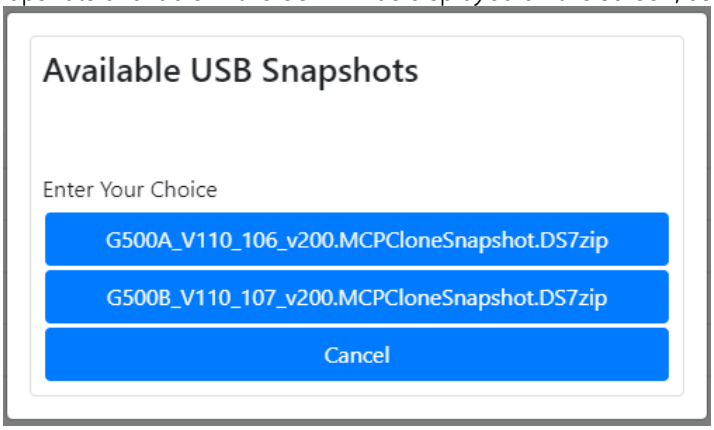
- Place the MCP Clone snapshot(s) on a USB formatted FAT32, e.g. using Windows File Explorer.
- Insert the USB in the target MCP

- Launch settings GUI and login to the device with valid user credentials.
- Select 'Restore Clone Snapshot' option from the settings menu, as shown below:

- Confirm and acknowledge the Snapshot restoration (followed by a reboot) by clicking 'Yes', as shown below:



- Then, list of clone snapshots available in the USB will be displayed on the screen, as shown below.



- Select the required snapshot to restore and enter corresponding password
- Follow the instructions displayed on the screen
- After the automatic reboot, clone snapshot will be restored into the MCP

1. **Offline Upgrade (Using Firmware Upgrade)**
   - Follow the procedure described in the TN-0116.

NOTE When restoring a snapshot image, the following data is not restored on the target device, even if was included in the snapshot file:
   - Log files
   - Hardware, license, and diagnostic information

Redundancy - Snapshots

This is not supported in MCP.

In case of Redundant configuration of MCPs, below steps can be followed for saving the snapshots (Standard/MCP Clone Snapshot) from a pair of Redundant MCP's and restore them into ANY pair of Redundant MCP's.

Applicable for Both Standard/MCP Clone Snapshots

Setup the Redundancy in Source MCP's

1. Login both the MCP's with their respective IP address through mcpcfg or Settings GUI.
2. Configure Redundancy in both the MCP's, refer Configure the MCP for Redundancy.
3. Reboot both the MCP's.
4. Using DSAS (Online/Offline Editors) configure the first MCP device or MCP-A
5. Apply "**Sync To**" or do the "Commit" changes from DSAS to upload the configuration into the first MCP device or MCP-A.
6. Go to the **Runtime HMI → Point Details → Redundancy Manager** and apply DO command on "**Sync Config**" DO pseudo point.
7. After this command, the configuration from the first MCP device or MCP-A will be synced to second MCP or MCP-B and both the MCP's will be configured into the redundancy mode.

Save the Snapshots from Source MCP's

Snapshots (Standard or MCP Clone Snapshots) need to be saved separately from both the redundant source MCP's (say MCP-A and MCP-B). Please refer Saving a Standard Snapshot procedure detailed in the earlier section to save the Standard Snapshot, for each MCP (i.e., MCP-A and MCP-B).

Similarly, in case of saving MCP Clone snapshot, please refer to the procedure explained in Saving an MCP Clone Snapshot section, for each MCP (i.e., MCP-A and MCP-B).

Upgrade the Snapshots from Source MCP's

In case of MCP Clone Snapshot, the snapshot needs to be upgraded. This can be done by following the procedure detailed in Upgrading MCP Clone Snapshot section, for snapshot from each MCP.

Restore the Snapshots to Target MCP's

For Snapshot restoration, the saved (and upgraded snapshot, in case of MCP Clone Snapshot) snapshot need to be restored for both the redundant target MCP's (i.e., MCP-A and MCP-B) individually. Please refer Restoring Standard Snapshot procedure detailed in the earlier section to restore the Standard Snapshot, for each MCP (i.e., MCP-A and MCP-B). Similarly, in case of restoring MCP Clone snapshot, please refer to the procedure explained in Restoring MCP Clone Snapshot, for each MCP (i.e., MCP-A and MCP-B).

NOTE: While restoring MCPA snapshot, MCPB must be powered OFF and vice versa.

NOTE: Power ON both the MCP's once the snapshots are restored successfully.

Setup the Redundancy in the Target MCP's

1. Login MCP with the IP address in the Snapshot or the Target MCP through mcpcfg or Settings GUI.
2. Select the option '13. Redundancy' → '9. Setup Public Key Authentication with PEER Gateway'.
3. Enter Password of Peer administrator user configured in each Redundancy configuration.
4. Reboot both the MCP's.
5. After reboot, go to the active's MCP runtime HMI and then navigate to Redundancy Manager Point details page and apply DO command on "**Sync Config**" DO pseudo point.
6. Go to Redundancy Manager Analog inputs Point details page and verify peer MCP enters standby state
7. Now, reboot the standby MCP to synch the settings files.

NOTE: Both the MCP's must have same time while performing **Keytransfer** and **Sync Config**, if not, select **Time Source** option in both the devices and **Enable Time Sync with Standby** option from mcpcfg/Settings GUI -> Redundancy.

Project and Archive Management

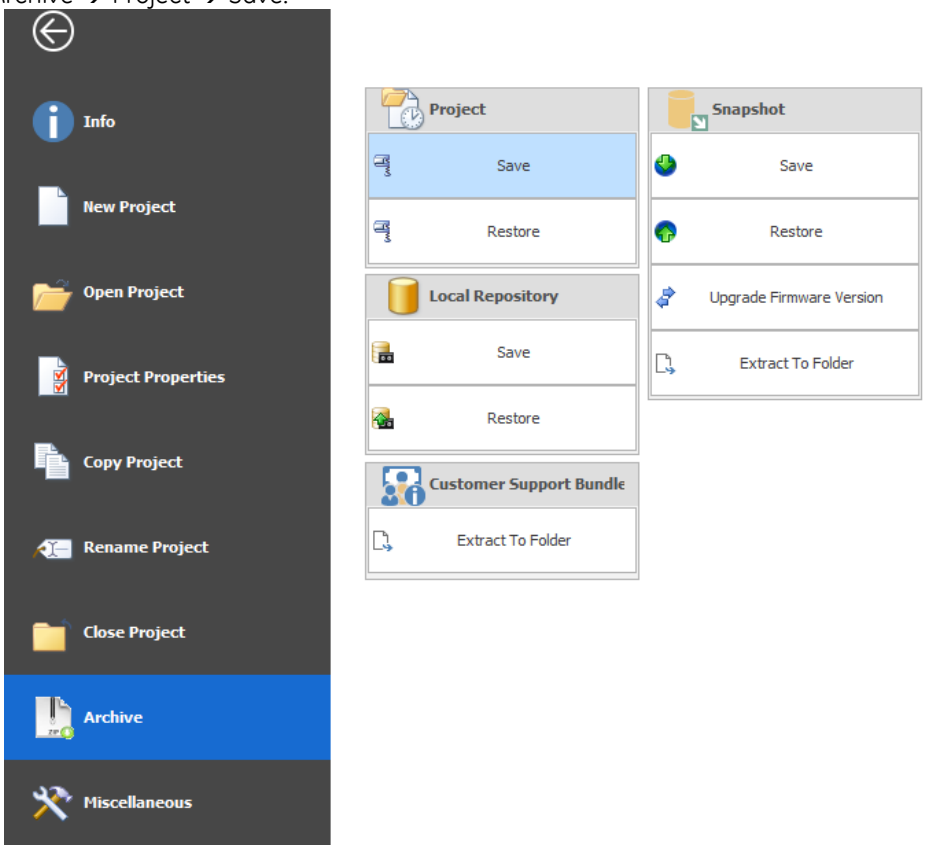
DS Agile MCP Studio has the option to archive an entire project and restore it to same or different machines in which DS Agile MCP Studio has installed. Project can contain many devices. DS Agile MCP Studio can save/restore all the devices available in the project page.

Individual devices can also be archived or restored.

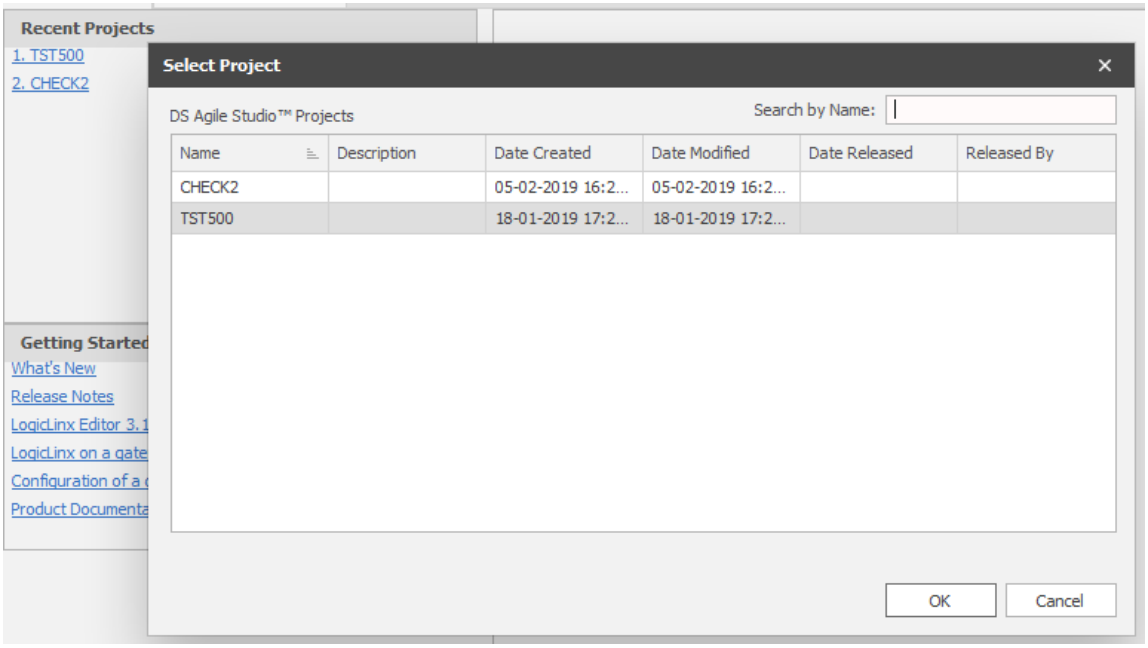
The following sections explain the procedure to archive and restore a project with MCP devices using DS Agile MCP Studio.

Save a Project Archive

1. Go to the File menu on the top left corner of the DS Agile MCP Studio and archive the project (as shown below): File → Archive → Project → Save.

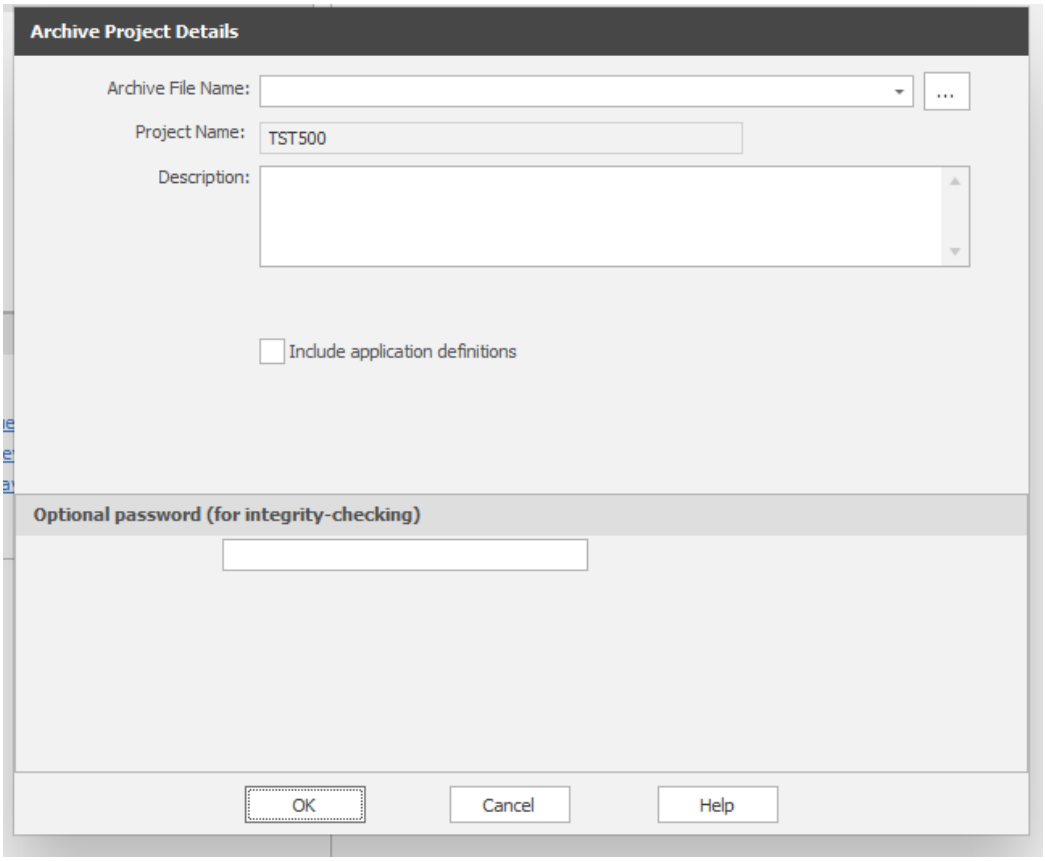


2. A window pops up with list of projects, as shown below:



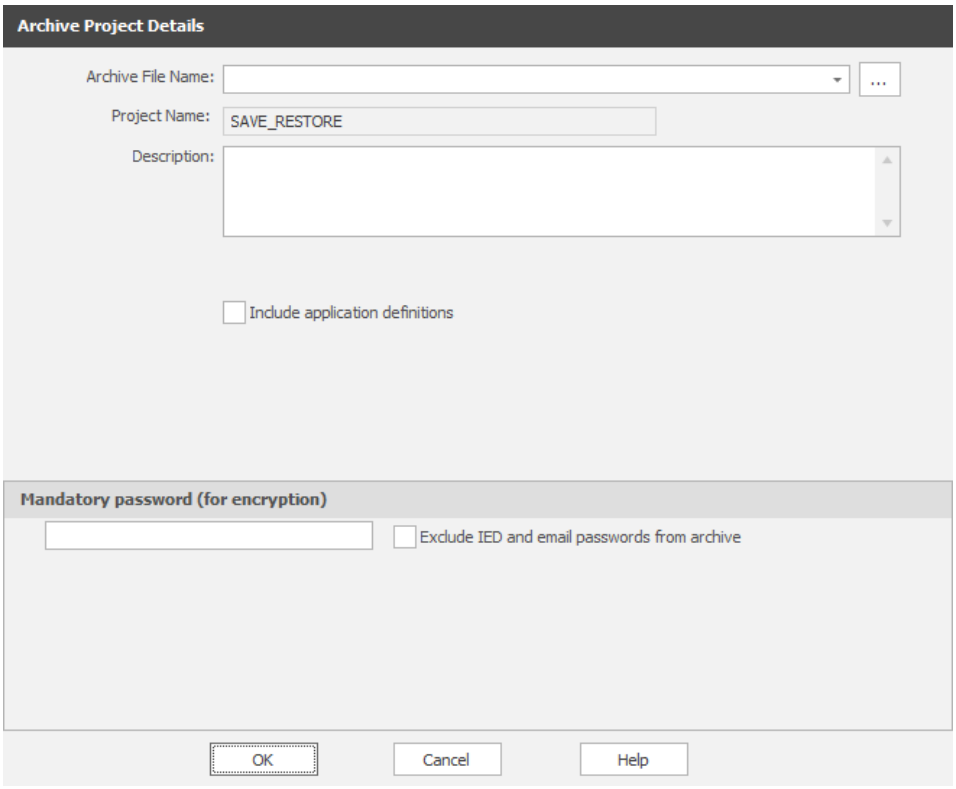
3. Select the desired Project to be archived and click 'OK'.

4. Alternatively, right click on the project name in the tree on the left area and select **Archive Project**
5. The Archive Project details window shows:

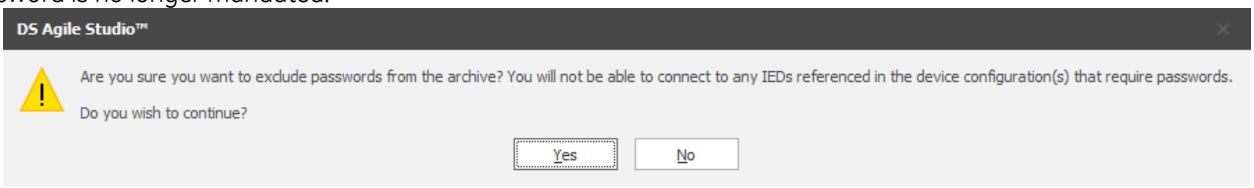


6. Specify the below details:
    - **Archive File Name**
        - Type in the file name and path (or)
        - Click the **[...]** button to navigate to the storage location.
    - Type in the **Description (optional)**.
    - Type in an **Optional password (for integrity checking)**, if the Project needs to be saved with.
7. Click **OK**.
8. Project will be saved now at the specified file location with ***name*. project.DS7zip**. It can be used to restore in the same machine or in a different machine, as per user need.

9. If the project contains MCP devices with internal “secrets”, the following dialog will be displayed at step 5 above:



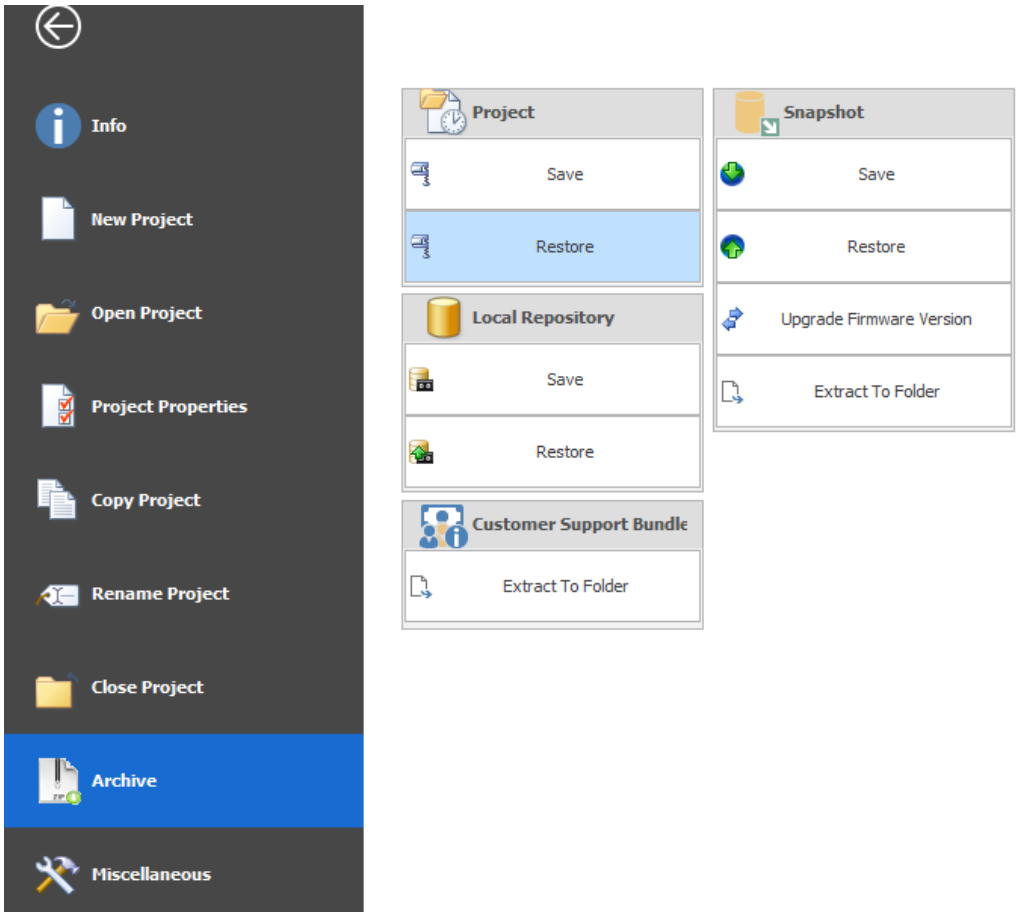
10. In this case the password is mandatory, to protect the secrets in the archive. Alternatively, the secrets can be removed by checking the box **Exclude IED and email passwords from archive**, in which case a password is no longer mandated.



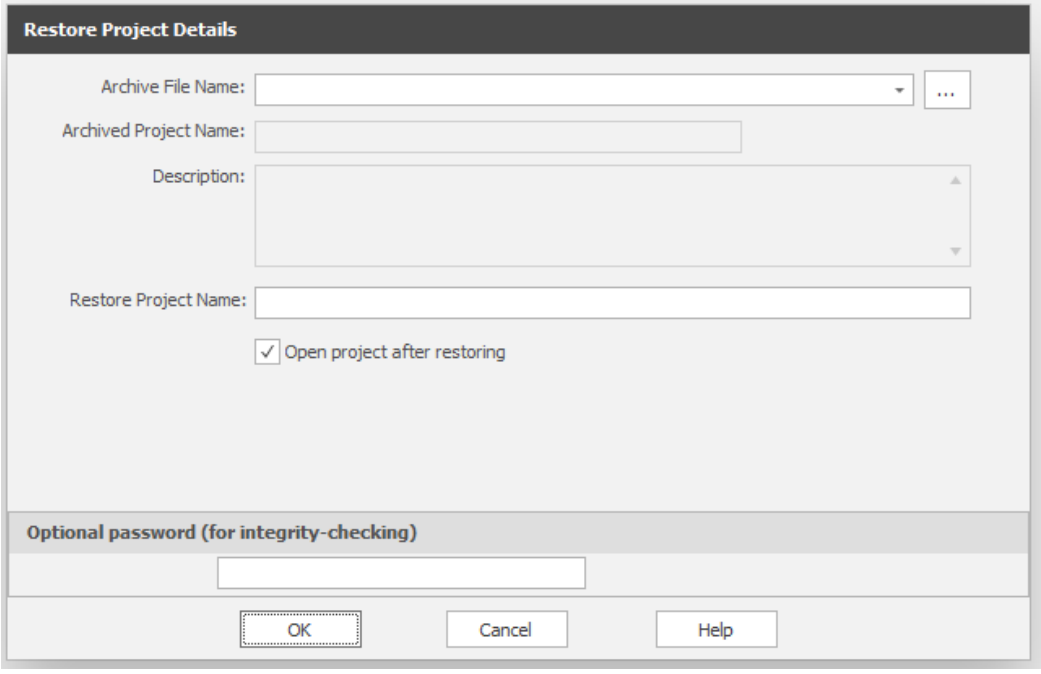
Note: once excluded, they cannot be recovered, and will have to be entered manually.

Restore a Project Archive

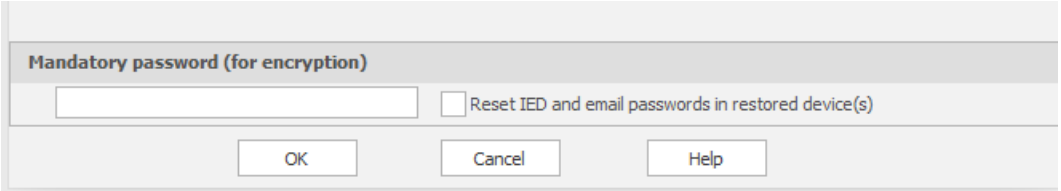
1. Go to the File menu on the top left corner of the DS Agile MCP Studio and restore the project (as shown below): File → Archive → Project → Restore



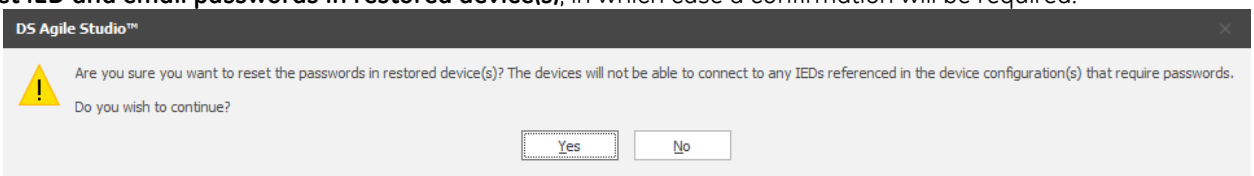
2. Upon clicking 'Restore', a window 'Restore Project Details' pops up, as shown below, in which details of archived project to be entered:



3. Specify the below details:
    - **Archive File Name,** which needs to be restored
        - Type in the file name and path (or)
        - Click the **[...]** button to navigate to the storage location.
    - Type in the **password (for integrity checking),** if the Project was saved with a Password.
4. Click **OK**.
5. Project will get restored now.
6. If the project contains encrypted "secrets", the dialog at step 2 will prompt to enter the mandatory archive password:



7. Alternatively, the secrets can be removed from all restored devices inside the project by checking the box **Reset IED and email passwords in restored device(s)**, in which case a confirmation will be required:



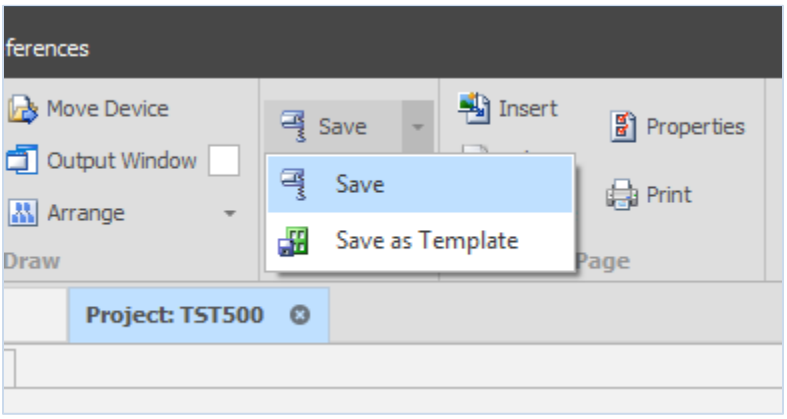
Note: once reset, they cannot be recovered, and will have to be entered manually.

The following sections explain the procedure to save and restore the MCP's device as an archive using DS Agile MCP Studio.

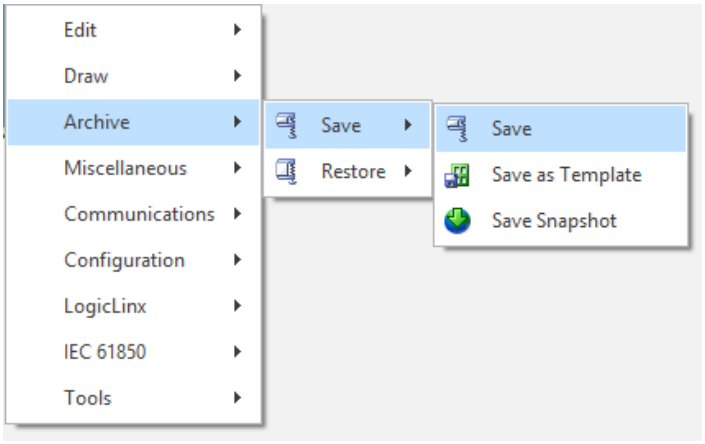
Save a MCP Device Archive

1. Select the device to save as an archive. The device appears within a green box with anchor points, as shown below:

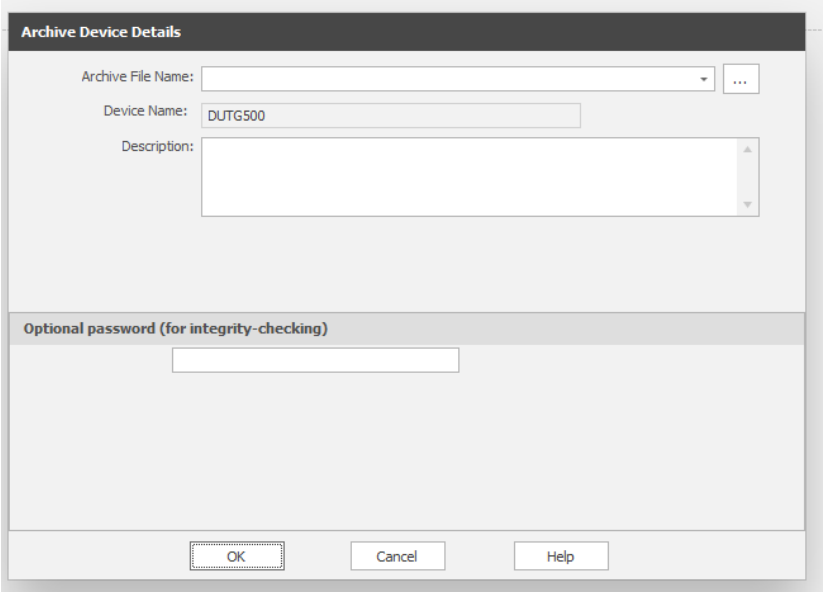
2. Then, click on the **Save** option, as shown below:



3. Alternatively, right click on the MCP device and select Archive → Save → Save option:



4. The Archive Device details window is shown:

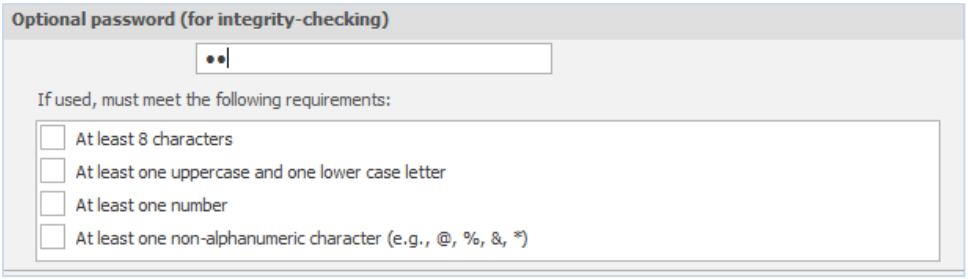


5. Specify the below details :
   - **Archive File Name**

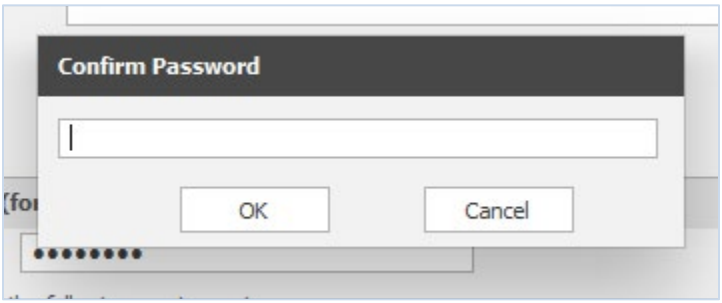
- Type in the File name and path (or)
- Click the **[...]** button to navigate to the storage location

- Type a **Description** of the device (Not Mandatory)
- Type in an **Optional password** (for integrity checking)

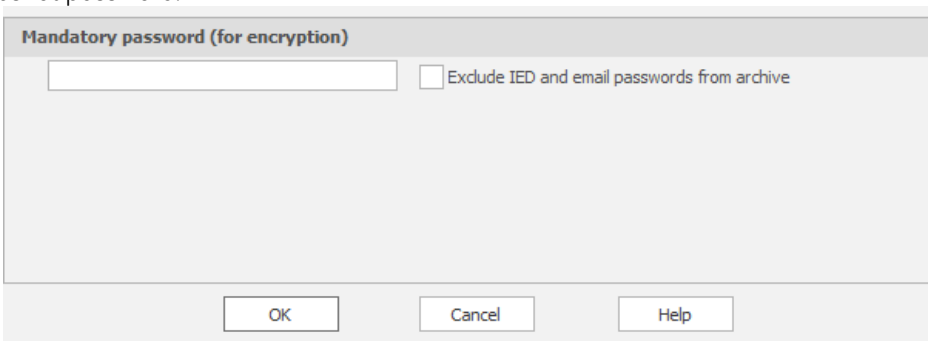
When you begin typing characters in the password field, additional information is presented, guiding you to meet password strength requirements.



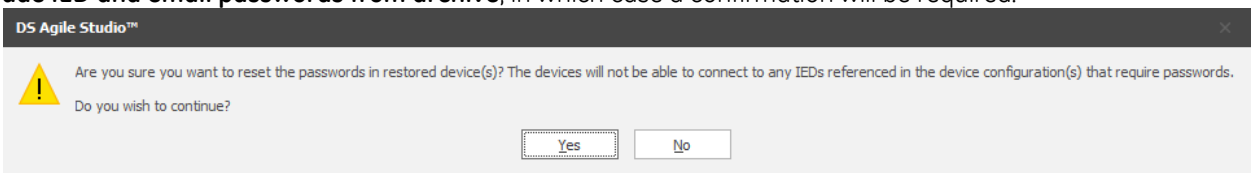
6. Re-enter the password and confirm the same, as shown below:



7. Device will be saved now at the specified file location as ***name*.device.DS7zip**. It can be used to restore, as needed.
8. If the device contains encrypted "secrets", the dialog at step 4 will prompt to enter the mandatory snapshot password:



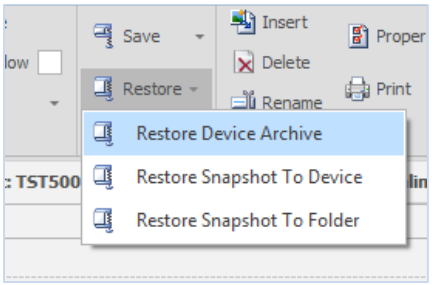
9. Alternatively, the secrets can be removed from all restored devices inside the project by checking the box **Exclude IED and email passwords from archive**, in which case a confirmation will be required:



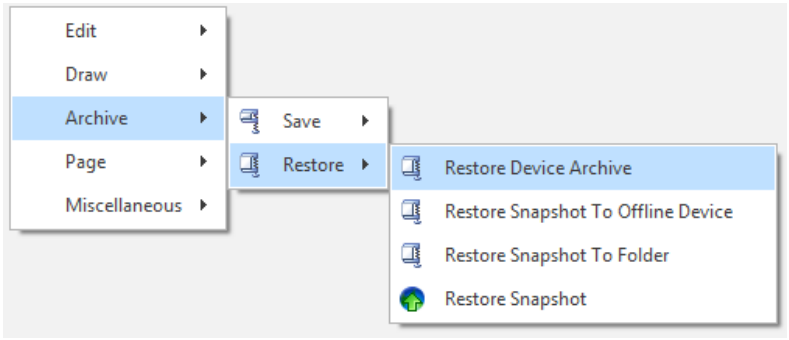
Note: once excluded, they cannot be recovered, and will have to be entered manually.

Restore a MCP Device Archive

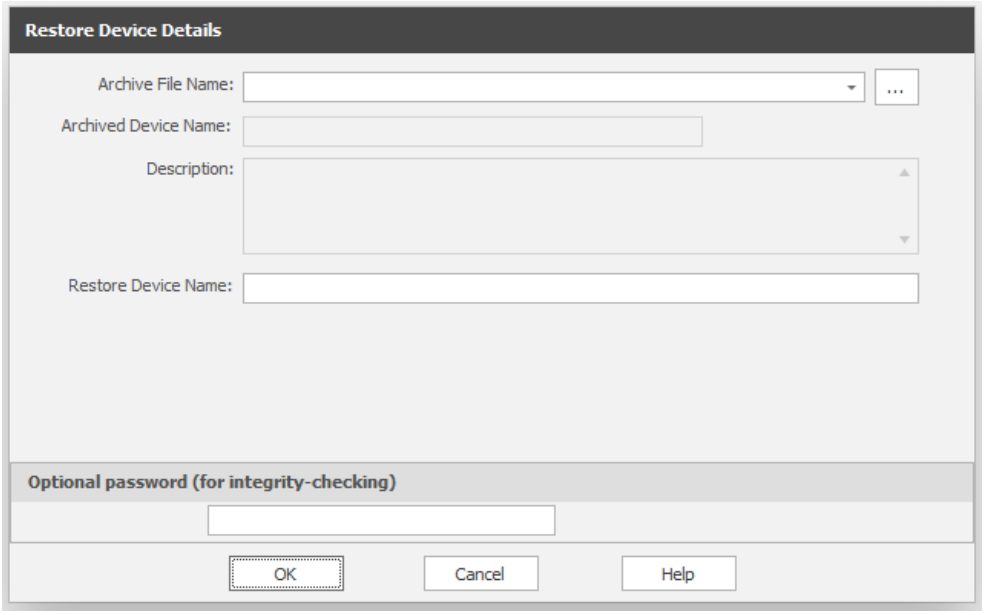
1. From ribbon, inside an open project, click on 'Restore' option, as shown below: Restore → Restore Device Archive.



2. Alternatively, right click on the project empty canvass and select Archive → Restore → Restore Device Archive.

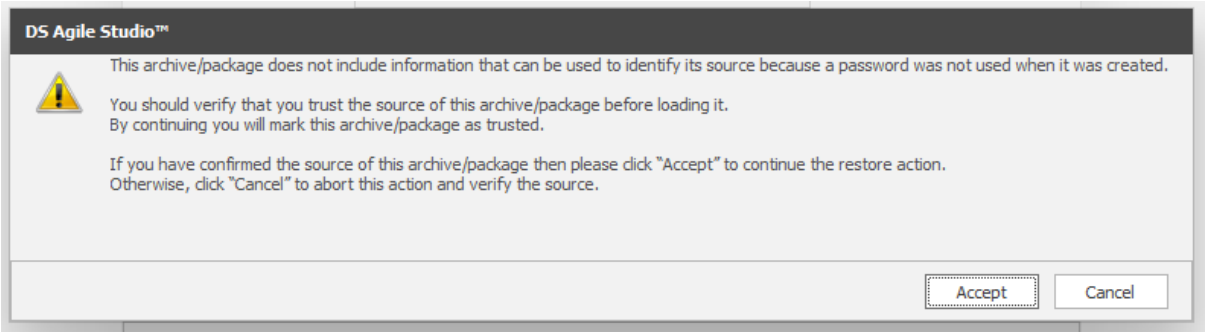


3. Upon clicking 'Restore Device Archive', a window 'Restore Device Details' appears, as shown below, in which details of archived device to be entered.



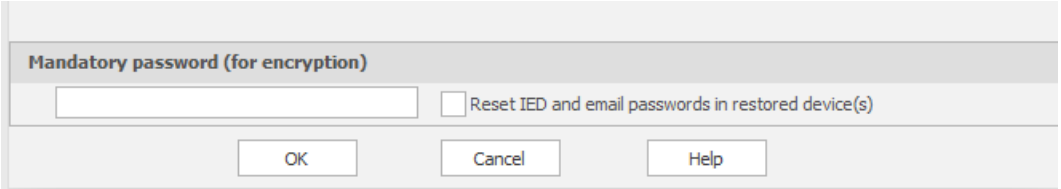
4. Specify the below details:
   - **Archive File Name**
     - Type in the file name and path (or)
     - Click the **[...]** button to navigate to the storage location.
   - Type in the **password (for integrity checking)** if the archive file was saved with a password

5. Click **OK** and then verify that you trust the source of the archive/package and click **Accept**; the archive file is restored to the device, as shown below:

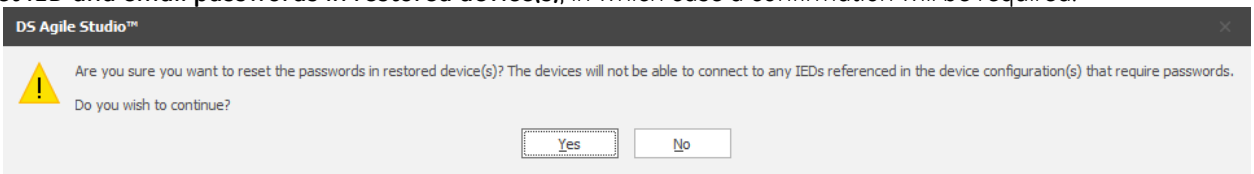


6. Then, DS Agile Studio popup will be displayed, indicating that the device has been restored.

7. If the device archive contains encrypted "secrets", the dialog at step 3 will prompt to enter the mandatory archive password:



8. Alternatively, the secrets can be removed from all restored devices inside the project by checking the box **Reset IED and email passwords in restored device(s)**, in which case a confirmation will be required:



Note: once reset, they cannot be recovered, and will have to be entered manually.

MCP Runtime HMI

The MCP Runtime Human machine interface (HMI) is your window into the MCP. Through the HMI you can monitor the status of your substation network, view data, execute control commands and change the system set-up.

The MCP Runtime HMI supports:

- Used to view and control the operation of the power network.
- Includes the optional One Line Viewer for viewing one-line diagrams.
- Accessed from the Power bar buttons to view the MCP display screens and utilities.

The MCP HMI is available in two forms:

- Local HMI
- Remote HMI

NOTE Multiple users can use the Remote HMI simultaneously.

A Local HMI is also available for accessing the MCP through a local substation computer setup (via the display port). The Local HMI provides the same operator functions for local display and control as the remote HMI with few exceptions. For more information refer to Local HMI.

The MCP is protected by a Log In screen that requires a username and password to access the HMI. Your user access level determines the screens and functions available to you.

Local HMI

The Local HMI provides access to the MCP through a local substation computer setup (via the display port)

MCP supports Local HMI by connecting the monitors using the display ports.

G100 supports 1 monitor and G500 supports 2 monitors.

Configure Screen Layout:

Screen Layout and resolutions may be configured using Screen Layout utility. This utility can be launched from Local HMI start menu using MCP -> **System** -> **Screen Layout** as shown below.

The minimum resolution supported in Local HMI is 1280x1024 and the recommended resolution is FHD (1920x1024) or higher.

Configuring Monitor Layout:

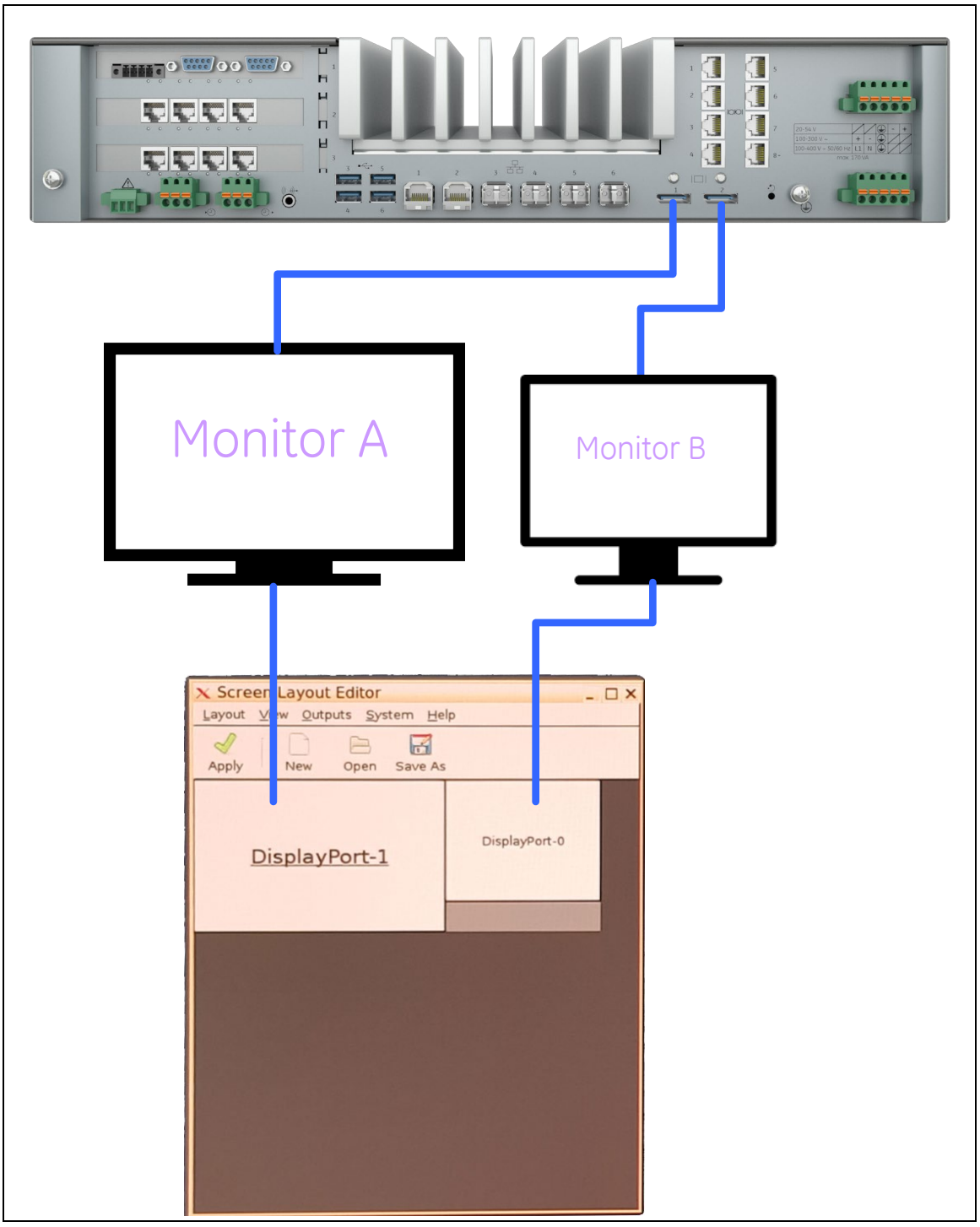
Multiple monitors can be connected to MCP via display ports (G500 only).

When single monitor is connected, the connected monitor becomes the Primary (G100 and G500).

When 2 monitors are connected to the G500, by default, the monitor connected to display port (labelled as DP 1, at the rear side of the device) becomes Primary. And the monitor connected to display port (labelled DP 2 at the rear side of the device) becomes extended monitor as shown below.

1. Monitor A - connected to DP 1 (shown as Display Port 1 on Screen Layout).
2. Monitor B - connected to DP 2 (shown as Display Port 0 on Screen Layout).

Figure 1.3: Monitor A becomes Primary and Monitor B is extended



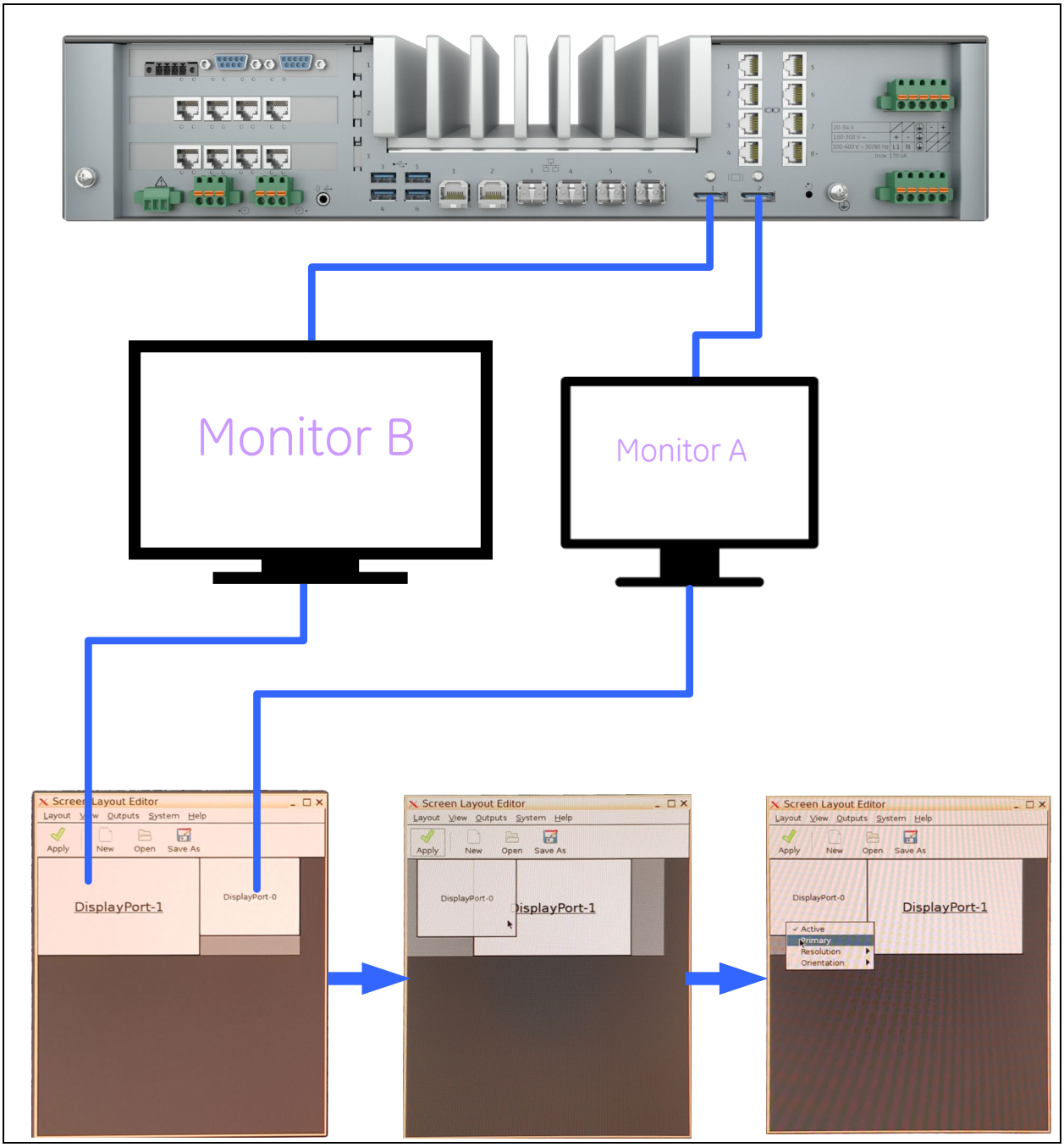
The user can reconfigure the layout without changing the backend connections by dragging & dropping the monitors and placing at the required position on Screen Layout canvas as described below.

e.g. When user configures connections such that Monitor A is connected to DP 2 and Monitor B is connected to DP1 however chooses Monitor A as Primary and Monitor B as extended.

In this case by default Monitor B becomes Primary and Monitor A will move in extended mode. Now, open the Screen Layout utility and drag the Monitor B (shown as Display port 1/DP1) to the right and Monitor A (Display Port 0/DP 2) to the left.

Right click on Monitor A (Display Port 0/DP 2) and select it as Primary. Now click **Apply** button and close the utility. These layout changes described above are shown below.

Figure 1.4: Monitor A (connected to Display Port0/DP2) becomes Primary and Monitor B (connected to Display Port 1/ DP1) becomes extended



NOTE The configured layout will always be persisted once the Screen Layout utility is closed. And whenever the HMI is relaunched, it will open as per the last configured layout.

Login to Local HMI

Local HMI will be started automatically once MCP is powered on and a monitor is connected to a display port.

If Local HMI is configured with Auto Login, then Local HMI will be launched automatically, and MCP Home Page comes with the configured user privileges. Refer to Local HMI Auto Log in for more details.

If Local HMI is not configured with Auto Login, then user would need to connect to Local HMI as described below.

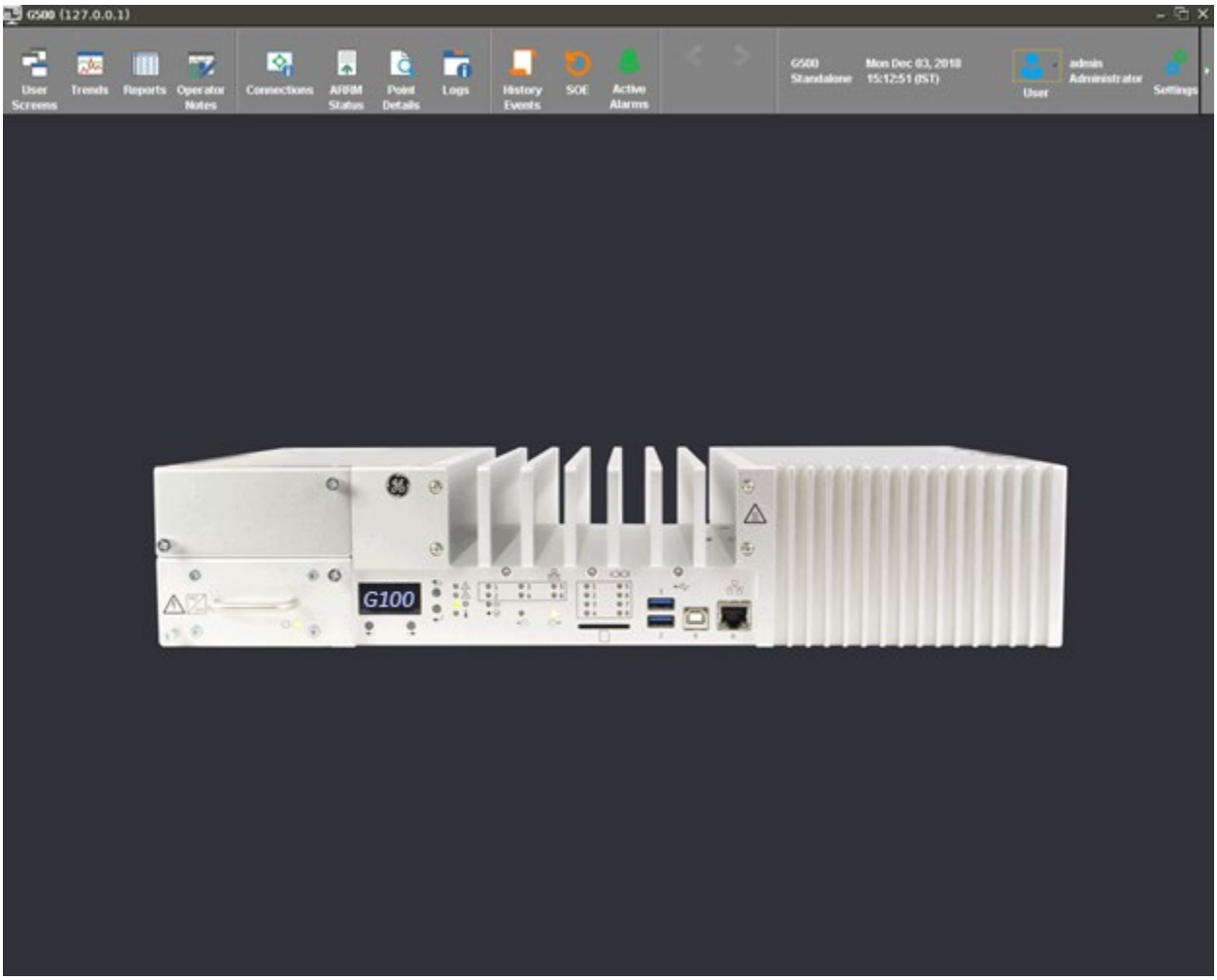
>> To log into the HMI:

1. Type in your Username and Password. MCP doesn't have default HMI user and it is required to nominated administrator user to access HMI and create other HMI users.
2. Click **Login**.
   Result: The below screen appears.

Figure 1.5: Login HMI screen

3. Type in your Username and Password. MCP doesn't have default HMI user and it is required to create a nominated administrator user to access HMI and create other HMI users.
4. Click **Login**.
   Result: If your login is successful, the below MCP Home page appears.

Figure 1.6: MCP Home Page



NOTE

The User Login level/role determines which MCP HMI features and functions the user can have access to/support.

The MCP Local HMI contains a lock out feature which prevents you from logging in after several failed attempts for a set period.

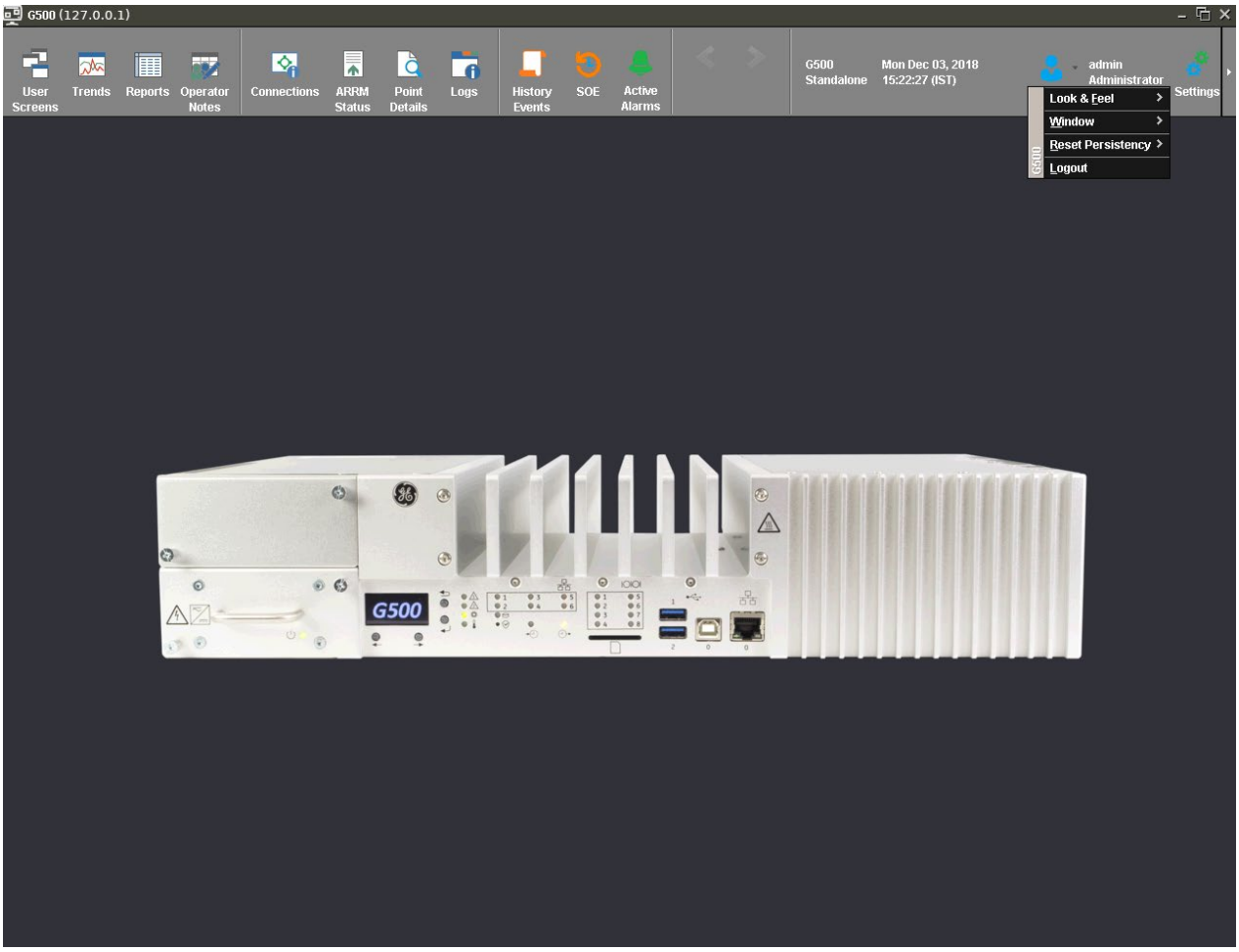
Logout from Local HMI

It is suggested to logout from the MCP Local HMI once work is finished with MCP Local HMI to secure the system. Logging out terminates the respective user session with the MCP and closes all MCP Local HMI displays and windows.

» To Logout from the MCP Local HMI:

- Click the **Logout** button on the Power bar.

Figure 1.7: MCP Login Screen



Result: The MCP Local HMI closes and the MCP Login to Local HMI screen appears.

Connecting to MCP Command Prompt

MCP Local HMI supports connection to MCP Command prompt using built-in shell. User can connect to the MCP command prompt using either default administrator credentials or nominated administrator credentials.

» To Connect to MCP Command Prompt:

Click on the icon available on menu bar to connect to the command line prompt from the Local HMI. Once the shell or window is launched then provide the administrator-level user credentials (Default Administrator or Nominated Administrator) to connect to the MCP from the command line.

Standby HMI Redirects to Active

If MCP redundancy is enabled, the current redundancy state of the MCP can also be seen in the Local HMI Power Bar. If the Standby MCP HMI redirects to the Active MCP when redundancy is enabled, both the Local HMI monitors connected to each MCP unit points to Active MCP only. The Local HMI Power Bar on each MCP Utility indicates whether the Local HMI is showing information for its(this) MCP or the redundant (PEER) MCP.

Remote HMI

The Remote HMI provides access to the MCP from a remote computer setup.

Log in to Remote HMI

» To log in to the HMI:

1. Double click on MCP Runtime HMI which comes as apart of DS-Agile Studio Package.
   Result: The below screen appears.

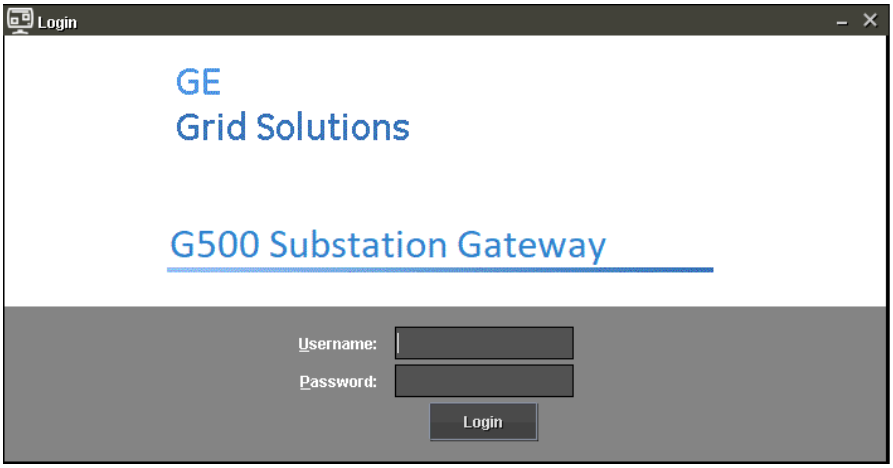
Figure 1.8: Remote HMI Login

Note: The login mode is always secure HTTPS and the default port number is 443.

2. Apply **Connect** after entering the Host IP.

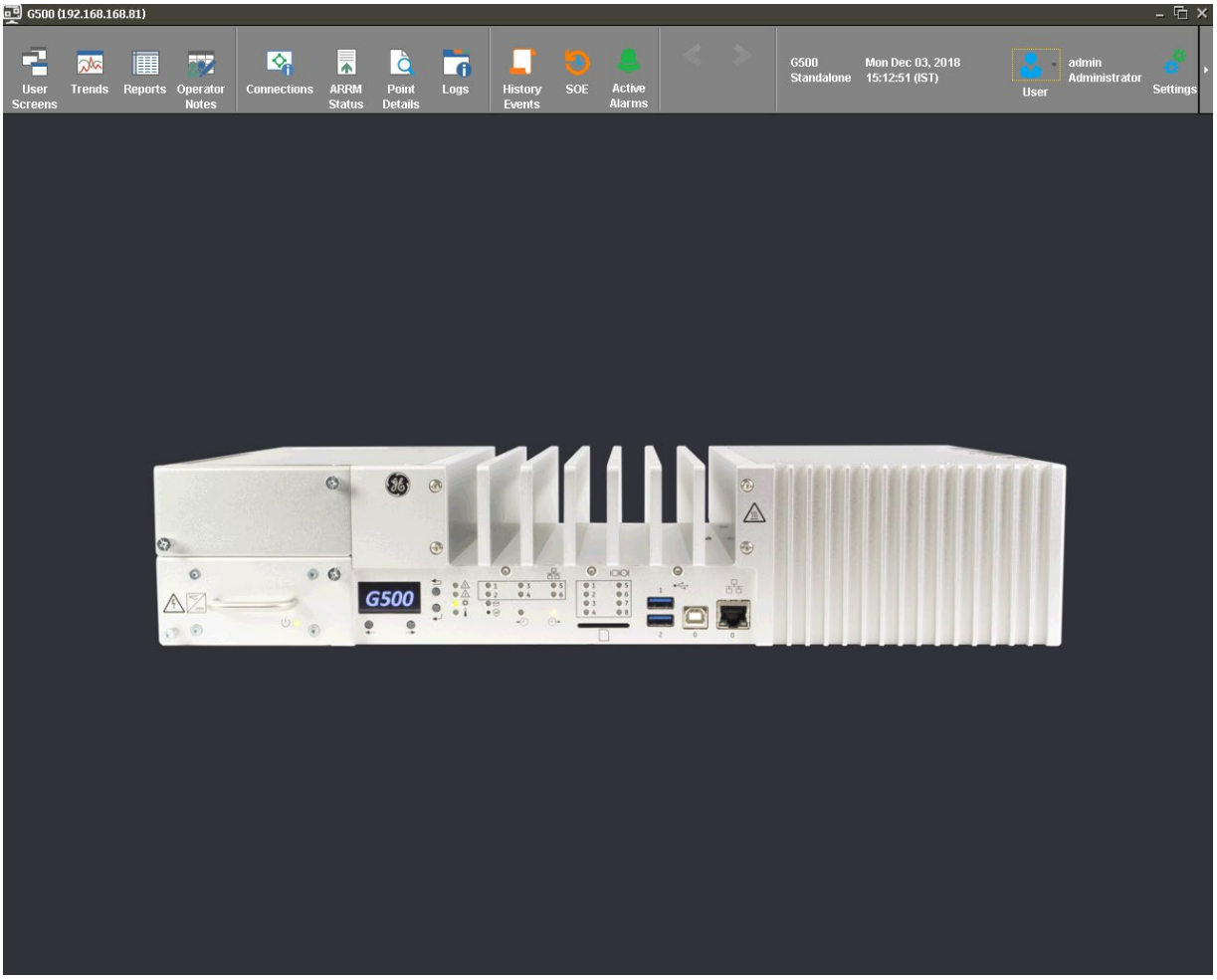
Result: The below screen appears.

Figure 1.9: Username and Password window



3. Type in your Username and Password. MCP doesn't have default HMI user and it is required to nominated administrator user to access HMI and create other HMI users.
4. Click **Login**.
   Result: If your login is successful, the below Figure 1.6: MCP Home Page appears.

Figure 1.10: MCP Home page



NOTE

The User Login level/role determines which MCP HMI features and functions the user can have access to/support.

The MCP contains a lock out feature which prevents you from logging in after several failed attempts for a set period.

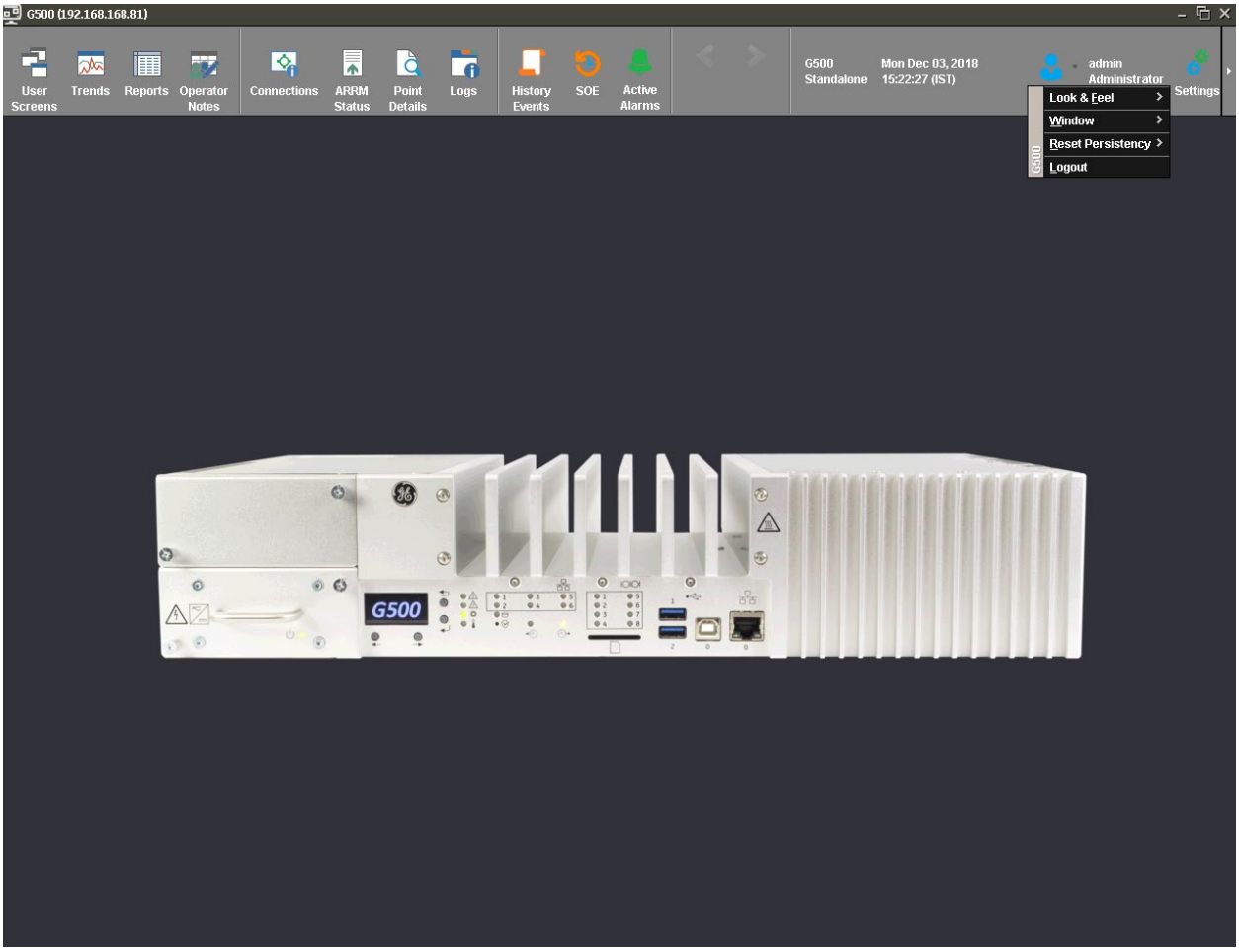
Logout from Remote HMI

It is suggested to logout from the MCP HMI once work is finished with MCP HMI to secure the system. Logging out terminates the respective user session with the MCP and closes all MCP HMI displays and windows.

» To Logout from the MCP Runtime HMI:

- Click the **Logout** button on the Power bar.

Figure 1.11: Logout from the MCP Runtime HMI



Result: The MCP Runtime HMI closes and the MCP Login to Local HMI screen appears.

Install MCP Runtime HMI

The remote MCP Runtime HMI requires Windows x64 bit OS. This is available via GE support channels and consists of a single installation file named "MCPHMI_x64_v.*abc*.exe" – where "*abc*" represents the version (this must match the MCP firmware version).

Installation of Java/JRE on the Windows PC is not required.

To install the MCP Runtime HMI

1. DoubleClick the "SetupMCPHMI_x64_*vabc*.exe" install file
2. Select OK at the Windows security prompt
3. Select Next in the installation wizard
4. Select Finish to complete the install
5. Launch the MCP HMI from the Start Menu or install folder

Install Location: C:\Program Files\MCP Runtime HMI*abc*\MCPHMI_x64_v*abc*.exe

Accessing Remote HMI Using Shortcut

1. Double click on "MCPHMI_x64_v1.0.exe" file <shortcut> or launch from the start menu.
2. Enter the IP Address (assigned in Task 3) of the MCP.

a. The TCP port of the MCP HMI is always 443. If you need to use a different TCP port, due to routing rules existing between the PC and MCP, you may enter it in the form of IP: TCP, for e.g. 10.10.11.50:30500

3. Login with the user credentials created through mcpcfg (defadmin) or Settings GUI (Administrator Group Users).
4. Click **Log In**.

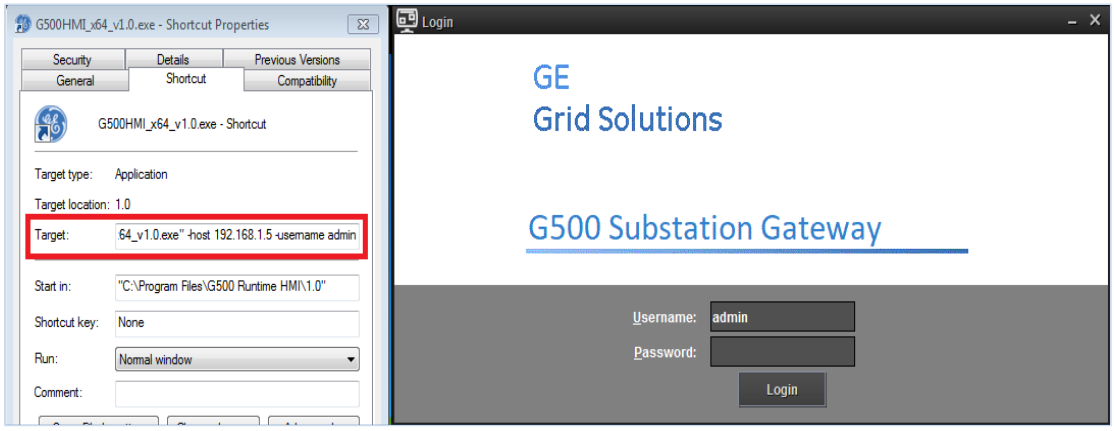
NOTE Users can be assigned with different HMI access levels. Refer Administrators User Management section for additional details.

Remote HMI Auto Login

By customizing a MCP Runtime HMI shortcut the user can predefine the login User, IP Address, or Remote Port.

1. Locate the MCP Runtime HMI shortcut.
2. Copy the shortcut to the desktop, or a desired location, or pin it to Taskbar or Start Menu.
3. Right click on the shortcut and select "Properties".
4. Add the below parameters to the shortcut at the location "Target" as seen in the below table:

Target Parameters		Shortcut Target content
IP Address	:	C:\Program Files\MCP Runtime HMI\1.0\MCPHMI_x64_v1.0.exe -host 192.168.168.81
IP Address & Port (e.g. for local port re-direct)	:	C:\Program Files\MCP Runtime HMI\1.0\MCPHMI_x64_v1.0.exe -host 127.0.0.1 -port 30500
Only User Name	:	C:\Program Files\MCP Runtime HMI\1.0\MCPHMI_x64_v1.0.exe -username admin1
Shortcut with All Parameters	:	C:\Program Files\MCP Runtime HMI\1.0\MCPHMI_x64_v1.0.exe -host 192.168.168.81 -port 30500 -username admin1



NOTE Shortcut properties display updated "Target" data launches the HMI with the IP and pre-defiled password.

5. Double clicking the newly created shortcut will launch the MCP Runtime HMI using the parameters configured in the Target.

MCP Applications

MCP System Redundancy

This is not supported in G100.

The MCP redundancy solution uses two MCPs connected through serial and/or network links - one in active mode and one in standby mode. If the active unit fails, the standby unit becomes active and takes over system operation.

MCP System Redundancy is configured using MCP System Utilities (mcpcfg) or MCP Settings GUI .

The three redundancy modes which are available on the MCP are:

Warm Standby redundancy	:	Two MCP units are connected using network and optional Primary and backup serial links. Data synchronization is minimal, restricted to field Accumulator points, local command quality, and configurations. See the DS Agile Studio help for more details. Connection to an RS232 switch panel is optional
Hot Standby redundancy	:	Two MCP units are connected using network and optional Primary and backup serial links. In Hot standby redundancy, two MCP units are kept in constant synchronization with respect to their real-time databases. Connection to an RS232 switch panel is optional.
No redundancy/Standalone (Default)	:	If No Redundancy is configured, then all configured applications in MCP run independently on each MCP

Types of MCP Applications - Functionality

The MCP is an advanced substation SCADA gateway device that encompasses the functionality of several typical substation devices in one. It can carry out a variety of functions, including:

Data Collection	:	Collect data from Intelligent Electronic Devices (IEDs) installed in the substation.
Data Presentation	:	Present collected data to a Supervisory Control and Data Acquisition (SCADA) system.
Data Translation	:	Manipulate the data comes to Data Collection applications and Provides to Data Presentation Applications. Also, Monitor devices for alarm conditions and issue alarms to the operator for action.
Substation HMI	:	Visually present the substation in one-line diagrams and display communications data to a system operator to monitor, control and operate the substation locally, or remotely over a network.
Terminal server	:	Provide transparent access (also known as pass-through) to connected devices using vendor-supplied PC programs.

Types of MCP Applications - Architecture

The MCP makes use of three types of embedded software applications to collect, present and manipulate data. These are called client, server and automation applications respectively. The input and output data of these applications is stored in a real-time database, commonly referred to as the System Point Database.

Client applications

This type of application typically interfaces with a substation device over a communications channel and collects data points from it. The client application writes input point values to the real-time database and may process control requests. Known previously within GE embedded devices as a Data Collection Application (DCA).

Server applications

This type of application typically allows the MCP to communicate with a master station or host computer over a communications channel. The server application reads input point values from the real-time database and sends control requests to it. Known previously within GE embedded devices as a Data Presentation Application (DPA).

Automation applications

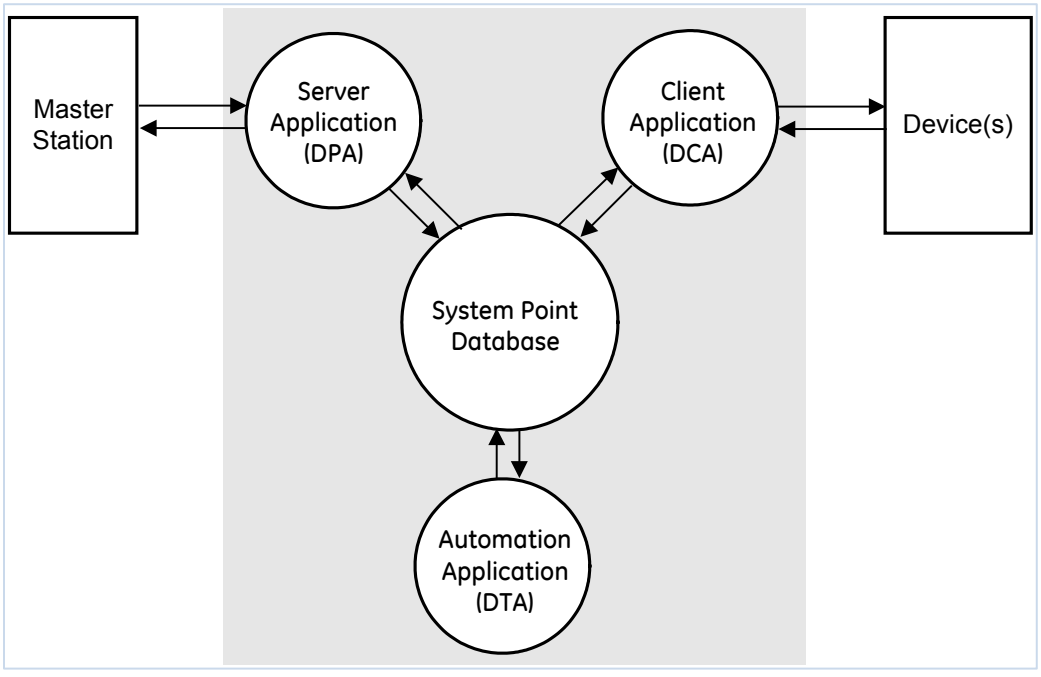
This type of application manipulates data within the real-time database. The automation application can examine the status and values of input points in the real-time database and accept control requests from server applications or other automation applications. The automation application can process this data and then update the values of the input points owned by the automation application or output points belonging to another application. Known previously within GE embedded devices as a Data Translation Application (DTA).

System Point Database

Information collected by the MCP is stored in a central database on the MCP called the System Point Database. This data base includes all types of system information, including communication statistics, present values, peak values and event records. The real-time database is dynamically updated for all the MCP system inputs/outputs as substation events take place and information is exchanged between applications.

Figure 3 illustrates a simplified relationship between the three application types and the system point database within the MCP.

Figure 1.12 Data applications within the MCP



Types of MCP Applications - Automation Features

This manual describes the standard and optional MCP automation features available in MCP . The applications available depend on MCP Order Code and License.

Feature	Standard	Optional
Accumulator Freeze	✓	
Analog Report Generation	✓	
Automated Record Retrieval Manager (ARRM)		✓
Calculator	✓	
Data Logger	✓	
Digital Event Manager (Alarm)	✓	
Firewall	✓	
Hybrid Model for MCP Redundancy	✓	
Input Point Suppression	✓	
Internationalization	✓	
Load Shed and Curtailment	✓	
LogicLinx Executor		✓
One Line Viewer	✓	
Secure Enterprise Connectivity	✓	
System Point Manager	✓	
System Status Manager	✓	
Terminal Services	✓	

MCP License Types – Online store

MCP Online store has the below License Options and their respective value of each Option.

License Options	Value
Automatic Record Retrieval Manager (ARRM)	002
IEC61850 (Client)	004
IEC 61131-3 Logic Engine (LogicLinx)	016

e.g. If MCP includes all the License Options then the combined License value is 002 + 004 + 016 = 022.

Types of MCP Applications - Configuration

This section lists the configurable applications that may be available for MCP. The applications available depend on MCP Order Code and License.

The below table lists the MCP applications that are available with the:

- Standalone mode
- Warm Standby redundancy mode – Not available in G100
- Hot Standby redundancy mode – Not available in G100

NOTICE Not all protocols are supported in the various Redundancy modes. Carefully review product documentation and configure Redundancy accordingly.

NOTICE Redundancy mode is not supported in G100.

Application Name	Standalone	Redundancy Mode		License required
		Warm Standby	Hot Standby	
DNP3	✓	✓	✓	
Generic ASCII	✓	✓	✖ Not Available	
IEC® 60870-5-101+104	✓	✓	✖ Not Available	
IEC 60870-5-103	✓	✓	✖ Not Available	
IEC 61850	✓	✓	✓	Yes
SEL Binary	✓	✓	✖ Not Available	
MODBUS Mulit-Drop®	✓	✓	✓	
MODBUS TCP/SSMODBUS TCP®	✓	✓	✓	
SSMODBUS TCP/SSH®	✓	✓	✓	
D.20	✓	✖ Not Available	✖ Not Available	
SNMP	✓	✓	✖ Not Available	
IEC 60870-5-101+104	✓	✓	✖ Not Available	
DNP3	✓	✓	✓	
MODBUS®	✓		✖ Not Available	
Alarm	✓	✓	✓	
Calculator	✓	✓	✓	
Data Logger	✓	✓	✖ Not Available	
System Point Manager	✓	✓	✓	
LogicLinx®	✓	✓	✓	Yes
ARRM (Automated Record Retrieval Manager)	✓	✓	✖ Not Available	Yes
Load Shed and Curtailment	✓	✓	✖ Not Available	
Analog Reports	✓	✓	✖ Not Available	
Runtime HMI	✓	✓	✓	
Online Configuration Tool	✓	✓	✓	
Offline Configuration Tool	✓	✓	✓	
System Utilities	✓	✓	✓	
System Point Database	✓	✓	✓	
HMI Access Manager	✓	✓	✓	
User Management	✓	✓	✓	
One-Line Designer & Viewer	✓	✓	✓	

IEC 61850 Loader	✓	✓	✓	Yes
Secure Enterprise Connectivity	✓	✓	✓	
VPN Server	✓	✓	✓	
HAMA (Hardware Asset Manager Application)	✓	✓	✖ Not Available	

User Roles

Default Users

The MCP unit that comes from the factory has two types of default users.

defadmin : The MCP default administrator defadmin is used to connect to MCP from Secure Terminal Emulator client from the command line interface of Local HMI. The default password of default administrator user is **defadmin**. When user logins using defadmin, below set of operations only can be performed.

- To change or configure IP Address
- To add a nominated administrator-level user(s).
- To restore MCP Snapshots
- To reboot the MCP.

NOTE The default administrator (defadmin) user will be deleted automatically once the default administrator (defadmin) is logged out and logs in successfully with the newly added administrator user.

root : The MCP default **root** user is available from serial maintenance port. The default password for the **root** user is **geroot**.

- Restricted to local access only

NOTE It is strongly suggested to change the password of the **root** user by using MCP Local Configuration Utility (mcpcfg) or MCP Settings GUI . Also, the User is responsible for the new root password. And in case root password is lost then there is no back door and Return Materials Authorization (RMA) is required to recover. Refer to **User Management** section for more details.

HMI User Access Levels

Users are assigned one of the below four levels of access to the MCP Runtime HMI:

Observer : View only privileges for all runtime screens.

Operator : Same as Observer, adds substation operation privileges to operate controls, force points and do maintenance tagging.

Supervisor : Same as Operator, adds privileges to access and modify configuration, runtime HMI Users.

Administrator : Same as Supervisor, adds full privileges to access and modify all configuration and settings, perform runtime debugging, add system administration users. Also, OpenVPN

and its related configuration can be created or modified with administrator privileges only.

User assigned access level appears in the top right corner of the title bar of the MCP HMI screen when you log in. User access levels are configured on the User Management tab on the Access page in Runtime HMI.

The privilege level SSHPassThrough is not available to access the MCP HMI. Users configured under this privilege level or role are only allowed access for SSH Secure Tunnel to Pass-through and Terminal Server Connections.

User Level Permissions

Administrator-level users have Supervisor-level access to all configuration, runtime, operation, and system screens in the MCP Online/Runtime HMI.

Only Administrator-level users have access to run commands at the MCP command line interface when the sudo command is used. OpenVPN configuration and Runtime viewers are only available from Runtime HMI using administrator-level users only.

The following table indicates the system privileges for each access level.

HMI Function	Administrator	Supervisor	Operator	Observer
Access built-in TELNET/SSH client	Y (see note)	Y (see note)	Y (see note)	N
Acknowledge Alarms	Y	Y	Y	N
Clear Logs	Y	N	N	N
Enable/Disable Device	Y	Y	Y	N
Add/Delete Operator Notes	Y	Y	Y	N
Execute Digital/Analog Controls	Y	Y	Y	N
Place/Remove Alarm Inhibit	Y	Y	Y	N
Place/Remove Control Inhibit	Y	Y	Y	N
Place/Remove Local force	Y	Y	Y	N
Place/Remove Scan Inhibit	Y	Y	Y	N
Place/Remove Tags	Y	Y	Y	N
Enable/Disable Unsolicited Responses	Y	Y	Y	N
View Alarms	Y	Y	Y	Y
View Events	Y	Y	Y	Y
View I/O Traffic	Y	Y	Y	Y
View Logs (Except OpenVPN Log)	Y	Y	Y	Y
View Operator Notes	Y	Y	Y	Y
View One-Line Diagrams	Y	Y	Y	Y
View Point Summary & Detail Pages	Y	Y	Y	Y
View Communication Statistics	Y	Y	Y	Y
View OpenVPN Log	Y	N	N	N

By default, access to the SSH clients and other command-line tools is limited to Administrator level and Passthrough-level users only. This setting is available through the mcpcfg tool.

See mcpcfg - Gateway Configuration Utility for more information.

User Authentication

When user log in to the MCP, user account is authenticated by the system. The following items are verified:

- Username exists
- User entered password corresponds to the configured password
- User assigned permission levels
- Total number of simultaneous users permitted for user security permission level is not exceeded
- Record of log in

If user have a problem logging into the system, check the above items for a conflict.

Authentication Modes

MCP supports both Local and Remote Authentication Modes and the Local Authentication Mode is enabled by default.

Authentication Rules

Authentication rules for different user types and services are provided in the following table:

Service	User Type						Additional Security Notes
	Admin User Types		HMI User Types			SSHPassThrough	
	root	Administrator	Supervisor	Operator	Observer		
Local HMI	Not Allowed	Allowed	Allowed	Allowed	Allowed	Not Allowed	The Local HMI session is automatically started with Operator privileges without prompting for user credentials, if the Systemwide configuration > Access Manager > Local UI Automatic Login parameter is set to true.
Maintenance Network Port	Allowed (Command Prompt)	Allowed (Command Prompt)	Not Allowed	Not Allowed	Not Allowed	Not Allowed	
Remote HMI	Not Allowed	Allowed	Allowed	Allowed	Allowed	Not Allowed	
SSH (Secure Remote Login)	Not Allowed	Allowed (Command Prompt)	Not Allowed	Not Allowed	Not Allowed	Not Allowed	
SFTP (Secure File Transfer)	Not Allowed	Allowed (Command Prompt)	Not Allowed	Not Allowed	Not Allowed	Not Allowed	
Pass-through Connection (Telnet & TLS)	Not Allowed	Allowed	Allowed	Not Allowed	Not Allowed	Not Allowed	Pass-through for remote TCP clients is enabled using **Pass Through Access** in Security parameters under **Configuration** > **Systemwide** and select **Secure Type** under **Configuration** > **Connection to Telnet or TLS**. Pass-through is allowed without Login/Password if its Pass-through password Authentication is disabled in MCP Config Tool (mcpcfg) or MCP Settings GUI > **Configure Authentication**.

Service	User Type						Additional Security Notes
	Admin User Types		HMI User Types			SSHPassThrough	
	root	Administrator	Supervisor	Operator	Observer		
Terminal Server Connection (Telnet & TLS)	Not Allowed	Allowed	Allowed	Allowed	Not Allowed	Not Allowed	Terminal Server is allowed without Login/Password, if its application parameter **Password Authentication** is set to No. Terminal Server for remote TCP clients is enabled by selecting "Secure Type" under **Configuration** > **Connection to Telnet or TLS**. Terminal Server application parameter **Minimum Privilege Level** specifies if Operator user is allowed or not.
Pass-through Connection (SSH Secure Tunnel)	Not Allowed	Allowed	Not Allowed	Not Allowed	Not Allowed	Allowed	Pass-through for remote SSH clients is enabled using **Pass Through Access** in Security parameters under **Configuration** > **Systemwide** and select **Secure Type** under **Configuration** > **Connection to SSH Secure Tunnel**. Pass-through for SSH Secure Tunnel is always allowed with Login/Password,
Terminal Server Connection (SSH Secure Tunnel)	Not Allowed	Allowed	Not Allowed	Not Allowed	Not Allowed	Allowed	Terminal Server for remote TCP clients is enabled by selecting **Secure Type** under Configuration > Connection to SSH Secure Tunnel. Terminal Server for SSH Secure Tunnel is always allowed with Login/Password. The parameter **Minimum Privilege Level** for SSH Secure Tunnel is always SSHPassThrough only.

Chapter 2 - Introducing MCP Features

Substation Gateway Features

GE's MCP Substation Gateway supports the following key features:

Security Features

The MCP supports the following security features:

- NERC compliant passwords, with strong complexity rules and one-way encryption
- Full auditing including Syslog integration to enterprise systems
- SFTP for secure network-based firmware upgrades and configuration file transfers
- SSH for secure network access to the maintenance facility
- SSH for secure programming and connection to the IEC 61131 programing facility
- Integration with LDAP/AD centralized RBAC

Advanced Gateway

The MCP collects data from substation protection, control, monitoring, RTU, and intelligent devices, pre-processes the data and moves it up to EMS and DMS SCADA systems providing centralized substation management.

Gateway features include:

- Data collection, concentration, and visualization
- Includes embedded General Purpose IO module (G100 only)
- IEC 61850 Gateway
- Device Redundancy
- Built in Media Conversion
- Files Retrieval capabilities
- Built-in HMI

Advanced Automation

The MCP provides the computing platform necessary to automate substation procedures, such that intricate processes are carried out safely and efficiently by creating advanced custom automation programs using IEC 61131 compliant tools and perform basic math functions on data points using the built-in calculator tool.

Automation features include:

- HMI & One Line Viewer
- Mathematical Control Logic using Calculator
- Programmable Logic using LogicLinx
- Accumulator Freeze
- Analog Value Selection

- Control Lockout
- Double Point Association
- Input Point Suppression
- Redundant I/O
- SOE & Alarm Management
- Analog Averaging
- Mail Box Functionality
- Parallel Redundancy Protocol
- Precision Time Protocol (PTP IEEE 1588)
- Hardware Asset Management Application
- System Status Manager
- Load Shedding and Curtailment

Fault Recording/Datalogging

Using pass-through connections, users can extract valuable non-operational data such as digital fault recording (DFR) records, event, and oscillography files. The user can also access the historical log files and upload the archived data for trending and analysis.

Fault recording features include:

- Automatic Record Retrieval Manager (ARRM)
- ARRM Runtime Viewer

Datalogging features include:

- Data Logger
- Trend Viewer
- Data Base Exporter
- Online & Offline Tabular Reports (Analog Reports)

Secure Remote Access

The MCP allows maintenance and relay engineers to securely access substation devices, locally or remotely, through advanced visualization and communication tools, increasing productivity.

Secure remote access features include:

- Build-in Firewall
- Access to Operational and Non-operational Data (rsync/SFTP/TLS/HTTPS)
- Pass-through/Terminal Server (SSH/TLS)
- Role Based Access Control
- Local Authentication, Authorization and Auditing(syslog)
- Virtual Serial Ports
- Electronic Access Point (EAP) - OpenVPN

Edge Connectivity

The MCP allows built in support for the Edge Manager Connectivity for the fleet level and local device management.

Edge Connectivity feature includes:

- Secure and Hardened Linux Based Predix Edge OS
- Predix Edge Technician Console Support for Local Device Management
- EdgeManager Connectivity through WAN to support Fleet Level Device Management.

Local HMI

The MCP supports built-in Local HMI for accessing the MCP through the display port(s). The Local HMI provides the same functions for local display and control as the remote HMI with few exceptions/additions.

Local HMI feature includes:

- Supports monitor (G100 supports 1 monitor and G500 supports 2 monitors) using Display Port (DP)
- Configurable Screen Resolutions and Screen Layouts
- Audio Buzzer for Alarm Management
- File Explorer Functionality

Chapter 3 - MCP HMI Runtime

This chapter contains the following sections which provides the details about the MCP Runtime HMI.

Runtime HMI Navigation
- Main Display Area
- Power Bar
- Change Displayed Information
- Internationalization

Manage Alarms
- Digital Event Management
- Alarm Types
- Alarm Groups
- Double Point Alarms
- Active Alarms
- Historical Alarms

View Data
- View Data
- Real-Time Database
- Data types
- Data Quality Status
- Point Summary
- View Point Details
- View Events
- Connections
- Logs
- Trends

Execute Commands
- Issue a Command
- Acknowledge an Alarm (One-Line Viewer)
- Acknowledge an Alarm Group (One-Line Viewer)
- Analog Output Interface
- Analog Set-point Interface
- Digital Control Interface
- Digital Output Interface
- Navigate to Active Alarm Page (One-Line Viewer)
- Point Forcing Interface
- DataSource Types
- Raise/Lower Control Interface
- Tag/Inhibit Interface
- Global Controls Disable

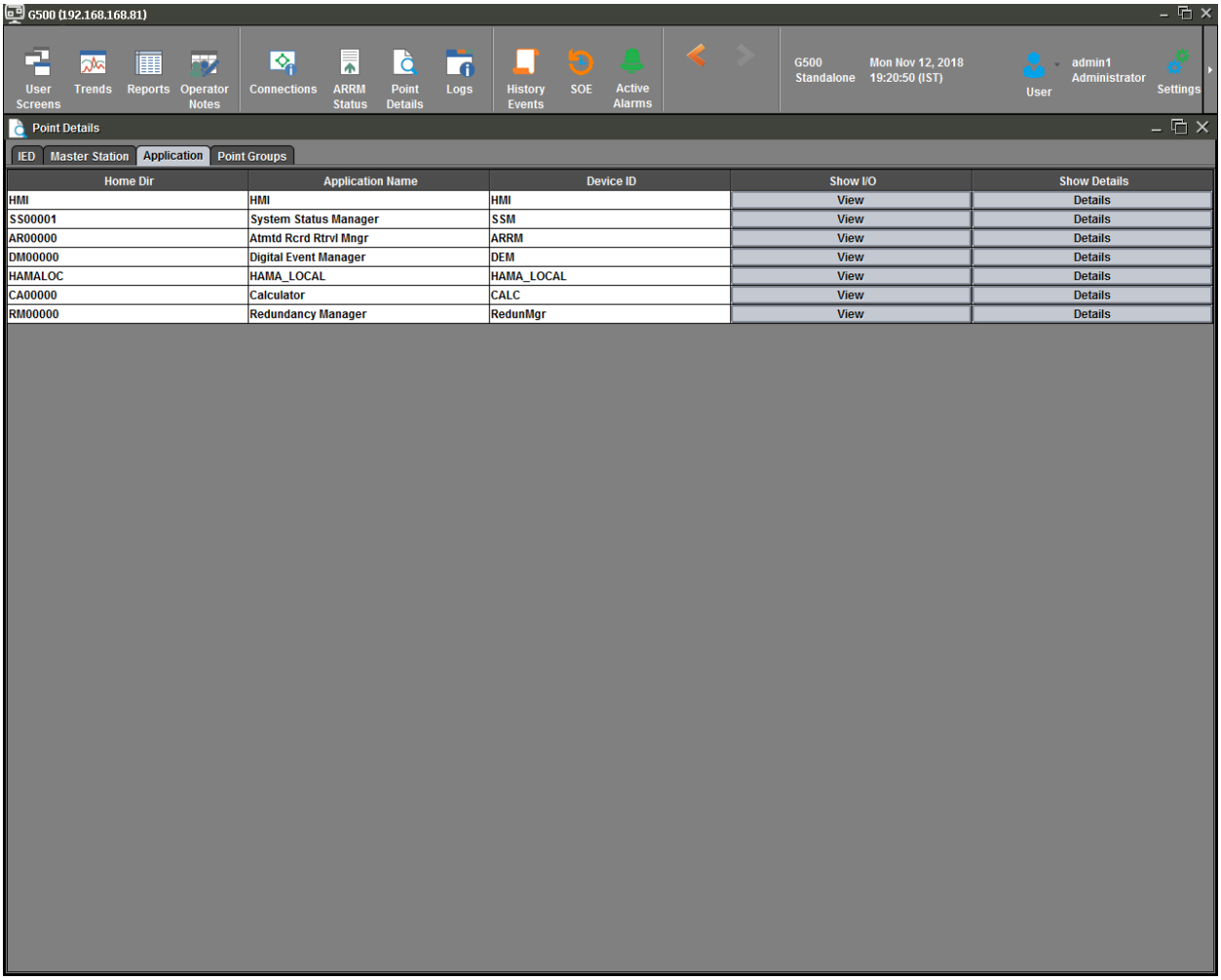
Operator Notes

Runtime HMI Navigation

Main Display Area

The main display area is where most MCP data display pages are presented for viewing or entering information. The Power bar is located across the top of the screen and contains buttons to navigate to the MCP display pages and functions. To go to a display, click a Power bar button.

Figure 3.1: Main Display



To view the Help topic for the MCP HMI screen you are currently viewing, click the **Help** button on the Power bar.

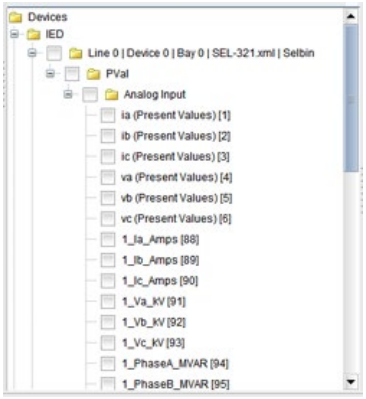
Popup Windows

Popup windows appear for certain functions so that you can edit information or perform an action, for example, **I/O Traffic Viewer**. Most popup windows include a **Help** button. Click **OK** or the **Close** button on the title bar to close the popup window.

Tree views

Many display pages present a tree view (shown below in the left pane) for finding and selecting relevant data. The tree view lists MCP system elements in a hierarchy, typically: Devices > device type > device name > point group > point type > point names.

Figure 3.2: Tree view

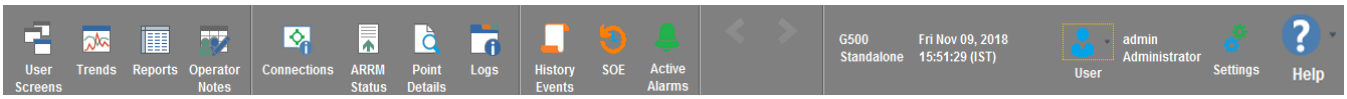


Collapse and expand parts of the list by clicking the + or - at each level. When you find what you are looking for, click to select the item. A check appears in the checkbox next to the item to indicate it is selected. When you select or de-select items in the tree view, the adjacent data display typically updates for the selected information.

Power Bar

The Power bar is located across the top of the main display area and contains buttons to navigate to the MCP display pages and functions.

Figure 3.3: Typical Power Bar



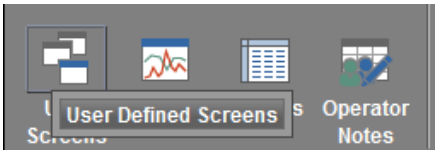
Standard Power bar buttons include:

- User Screens
- Trends
- Reports
- Operator Notes
- Connections
- ARRM Status
- Point Details
- Logs
- History Events
- SOE
- Active Alarms
- File Explorer
- Settings
- User
- Help

The MCP HMI Power Bar buttons can NOT be customized. If navigation across multiple screens is required within One-line Diagrams, the required screen navigation buttons must be custom-configured within the One-line diagrams workspace.

To go to a specific display, click the Power bar button.

A tooltip indicates the function of the Power bar button when you hover over the button with the pointer.



NOTE If MCP redundancy is enabled, the Power Bar in Local HMI will display an indication to reflect the current redundancy state of the MCP.
Not supported in G100.

If Standby HMI redirects to Active MCP feature is enabled, the Power Bar in Local HMI will display an indication to reflect the HMI pointing to self or PEER MCP. For details see the Local HMI section of the G500 Instruction Manual (GE part number 994-0152) or G100 Instruction Manual (GE part number 994-0155).

User Screens

The User Defined Screens (also referred to as the Single Line Diagram - SLD) Viewer displays:

- The main drawing (main.dra) by default.
- Simplified schematic diagrams during runtime that represent the interconnections in a substation, including devices and the real-time values and/or state of selected ports and points.

These custom-built diagrams are built using the following two types of objects from the MCP HMI library:

- Static objects that do not change during runtime. Examples of static objects are buttons, labels, lines and other shapes used to lay out the drawing.
- Dynamic objects that represent a data source and are updated continually as new information becomes available. Examples of dynamic objects are circuit breakers, switches and value boxes. The source of the data can be the real-time database, the Active Alarms (Digital Event Manager) application or other MCP resources.

The **User Defined Screens** are designed and configured using the One-Line Designer.

The following related action can be performed: Issue a Command.

Trends

The Trending also known as Data Logger application allows you to graphically monitor and record data from devices connected to the MCP. You can also save and review historical reports created by the application.

Reports

The Reports screen also known as Analog Report View allows you to view online and offline analog reports.

Periodic logging of the analog parameter information is required for records, periodic maintenance and preventive maintenance of the substation equipment. The Analog Report application allows you to record the

Analog Data of various devices connected to the MCP. It allows you to configure the MCP to capture the configured Analog Input values with Quality Attributes at regular intervals of time and format.

The Analog Report application allows you to choose existing record templates or create and import new templates to log reports. It also allows you to back up the generated reports. The reports can be stored in html, pdf, or xls format.

Operator Notes

The **Operator Notes** page lists operator notes that have been entered by users and stored in the MCP database.

Note records

Each note record displays the following information:

Table 3.1: Note Records

Button	Description
Note Number	Automatically assigned number to identify the note.
Sequence Number	Sequence Number to identify the original note or comments added to the note. Sequence Number 0 indicates the original note and greater than 0 indicates the comment(s) added to the original note.
Operator Name	MCP HMI user name of the note author (original or commented).
Date Created	Date and time that the note or comment was created.
Notes	Free-form text entered by the note author.

The following related actions can be performed from the GUI:
Add a Note
Edit a Note
Operator Notes Log
Sort Records

Connections

The connections also known as **Communications Summary** page lists the most recent communication statistics between the MCP and configured device or master station connections.

The following related actions can be performed:

View Device Communications

View Master Station Communications

View Pseudo points – Detailed Communication Statistics

Enable/Disable Device Communications

ARRM Status

The Automated Record Retrieval Manager retrieves and stores record files from devices connected to your MCP. The ARRM Viewer can be used to view the status of this application and to initiate manual transfers. You can also retrieve downloaded records from the MCP using any FTP/SCP/SFTP client as needed or on a scheduled basis.

You can also configure the MCP to automatically download files to a remote location using the Sync Manager utility. For more information refer to the MCP Instruction Manual Configure Sync Manager section or to the MCP Online Help >Configure Sync Manager topic.

Point Details

The **Point Details also known as Point Summary** page lists system elements (and identifying information) for which points have been configured, categorized by:

- IED Point Summary
- Master Station Point Summary
- Application Point Summary
- Point Groups Summary

The following related actions can be performed:

- View I/O (IED and Master Station only)
- View Point Details

Logs

The **Logs** also known as System logs page provides a report utility to display a list of system activities maintained by the MCP and stored in the real-time database. The logs are useful for troubleshooting and tracking purposes. The following reports are available:

- Control Log
- Diagnostic Log
- System Event Log
- User Activity Log
- Analog Report Log
- VPN Server Log (Available only to Administrator class/role users)

⚠CAUTION

SYSLOG-based event logging (i.e., System Event Log, Diagnostic Log, Control Log and User Activity Log) should not be used for real time and Mission Critical purposes. Data presented in the SYSLOG may not be updated in real time to correctly indicate the status of monitored and controlled equipment.

For example, a power line could be listed as inactive in a system log, while in fact the power line is active and its status in the system log may be updated significantly later in terms of real time applications.

Only use SYSLOG-based event logging for system management, security auditing, general informational and debugging messages.

The following related actions can be performed:

View a Log

Clear a log

History Events

A historical alarm is an alarm that has been archived from the **Active Alarms** list. The History Events also known as **Historical Alarms** page provides a search utility to filter, sort and display historical alarm records stored in the real-time database.

To be archived to the **Historical Alarms** page, an alarm must meet the following conditions:

- "Deviation" alarm is acknowledged and has returned to normal state
- "On update" alarm is acknowledged

"Double Point" alarm is acknowledged and the pair of source points have moved into a non-alarmable state

SOE

The **SOE** page provides a search utility to filter, sort and display Sequence of Event (SOE) items stored in the MCP.

Active Alarms

The **Active Alarms** page lists all active alarm events on every alarm-enabled point in the MCP database. The display automatically updates whenever the MCP generates a new alarm, or when the status of an existing alarm changes. The total number of active alarms in the system database is shown in the bottom left corner of the window.

The **Active Alarms** button on the Power bar visually indicates the status of active alarms in the MCP:

Blinking red when unacknowledged active alarms exist

Steady green when no active alarms are present

Steady yellow when acknowledged active alarms are present

The Alarm application must be configured to view the Active Alarms button and page. The icons shown above are system defaults and can be modified on the **Alarms** tab of the **Configuration** tool.

The MCP does not raise alarms on points that are offline.

File Explorer

With a USB key connected to one of the MCP USB ports you can:

- Browse files and folders in the user folder and datalog folder according to:
  - File name with modified date and file size
  - Folder name with modified date
- Copy selected files from the user folder and the datalog folder to the USB key.

Do not back up your user folder using the Copy function, since some sensitive files are hidden and cannot be copied due to security reasons; for example, User Certificates, MCP Password and Shadow files etc.

File Explorer Viewer is only available in the Local HMI mode.

The USB must be formatted with **FAT32** and must have a partition table.

» To mount the USB key:

1. Connect USB keys to the MCP USB ports.
2. Click the **Mount USB** button below the file tree.
   Result: The mounted USB keys appear on the file tree as **usb1** and **usb2**.

Once a USB key is mounted, you can copy and save files.

NOTE USB key is mounted under the /mnt/usb/ location.

» To select a file or multiple files under the user folder or under the datalog folder:

- For a single file, left click the file.
- For multiple files, left-click the first file and [Ctrl]+left-click the additional files.

» To copy selected file(s) to the USB key:

1. Select a file or multiple files.
2. Right-click the file(s).
   Result: A popup menu appears.
3. Select **Copy to USB Key** command.
   Result: A Save To dialog window appears.
4. Navigate to the destination.
5. Click **Save**.

» To unmount the USB key:

- Click the **Umount USB** button below the file tree.

Settings

The Settings page has Access and Utilities to provides access to software tools installed on your MCP device.

Access

All available options under Access page are listed along with a description of the functionality they provide.

User Management

The User Management Tab on the Access page allows the user to set up accounts for MCP users, including usernames, passwords and access level.

Add a User

» To add a user:

1. Click Add to create a new user account.
   Result: The Add User window appears.
2. Enter the user information.
3. Click OK.
   Result: The User Management table is saved.

Change a User Account

» To change a user account:

1. Click on the user record from the list in the User Management table. Result: The Update User window appears.

2. Change the user information as required.
3. Click OK. Result: The User Management table is saved.

Delete a User

» To delete a user:

1. Click on a user record from the list in the User Management table. Result: The Update User window appears.
2. Click Delete. Result: The Delete confirmation popup appears.
3. Click Yes to confirm the deletion.

Configure User Home Page

» To configure the User Homepage:

1. Click on the user record from the list in the User Management table.
   Result: The Update User window appears.
2. Update the user information as required.
3. Select the user Home Page from the dropdown list.
4. Click OK.
   Result: The User Management table is saved.

Authentication

The Authentication tab on the Access page allows the user to configure either:

Local Mode : Local authentication makes use of files stored locally to control user authentication, as opposed to connecting to a remote server to obtain username and password information.

Remote Mode : Remote authentication makes use of user account information stored on remote server. The MCP supports three remote authentication modes:

- Cisco® TACACS+
- LDAP

Automatic Login

The Automatic Login on the Access page allows the user to setup Local and Remote HMI auto login accounts.

Local UI Automatic Login : Select to skip the Local HMI log in when a user logs into the MCP through the local substation computer setup and go directly to the Local HMI main page (home page). Default is False.

SECURITY NOTICE: If Local UI Auto Login is set to true, the Local HMI will perform an automatic login using the selected user privilege level and name, without additional human authentication required. It is up to the system's Engineer / Operations to assess the effect and application of this behavior at runtime.

Local UI Automatic Login Wait Time : This parameter can only be configured if "Local UI Automatic Login" is set to true. The Local UI Automatic Login Wait Time parameter represents the wait time (in seconds) that is available for the user to interrupt the system from entering the Local Graphical UI's Main Page from the Command Line Interface.

Local Automatic Login Privilege Level : This parameter can only be configured if the Local UI Automatic Login parameter is set to true. The Local Automatic Login Privilege Level parameter provides the user with the option to configure the Default Privilege Level when navigating to the Local Graphical UI.

Local Automatic Login User : This parameter can only be configured if the Local UI Automatic Login parameter is set to true. The Local Automatic Login User parameter allows the user to choose

the default user from the list of users configured under each Privilege Level (Operator/Observer).

Remote UI Automatic Login : Select to skip the Remote HMI log in when a user logs into the MCP through the Remote substation computer and go directly to the Remote HMI main page (home page). Default is False.

SECURITY NOTICE: If Remote UI Auto Login is set to true, the Remote HMI will perform an automatic login using the selected user privilege level and name, without additional human authentication required. It is up to the system's Engineer / Operations to assess the effect and application of this behavior at runtime.

Remote UI Automatic Login Wait Time : This parameter can only be configured if "Remote UI Automatic Login" is set to true.

The Remote UI Automatic Login Wait Time parameter represents the wait time (in seconds) that is available for the user to interrupt the system from entering the Remote UI's Main Page from the Command Line Interface.

Remote Automatic Login Privilege Level : This parameter can only be configured if the Remote UI Automatic Login parameter is set to true.

The Remote Automatic Login Privilege Level parameter provides the user with the option to configure the Default Privilege Level when navigating to the Remote Graphical UI.

Remote Automatic Login User : This parameter can only be configured if the Remote UI Automatic Login parameter is set to true.

The Remote Automatic Login User parameter allows the user to choose the default user from the list of users configured under each Privilege Level (Operator/Observer).

VPN Client

The VPN Client on the Access page allows the User to create VPN Client settings including Routing and White list options.

Table 3.2: VPN Client settings

Settings	Description	Range	Default
Client Name	The client names. This name must match the Common Name of the client certificate.	Text string 32 characters are allowed	Client1
Enabled	Selected if the Client is enabled. Not selected if the Client is disabled	Enabled Disabled	Enabled
Routing List and White List	Click Configure to access the Configure Routing List and the White List.		

Table 3.3: Routing List and White List

Settings	Description	Range	Default
Routing List	Drop-down list of Route IP Address &Subnet Mask in CIDR notation. **Note:** The Routing List contains a list of configured networks (including VLANs & PRP) in the MCP. This list can't be edited by the User.	Valid IP4 Address/Net mask	172.12.232.0/16

White List	The MCP VPN Server will provide configuration option for "IP/Port/Protocol Whitelist" for each VPN client to allow the incoming connections based on the combination of destination IP Address, protocol and Port number through VPN tunnel. The MCP VPN Server provides a configuration option for "IPAddress/Port/Protocol Whitelist" for each VPN client to allow the incoming connections based on the combination of destination IP Address, protocol and Port number through VPN tunnel.	IP Address: Valid IP4 Address Port No: Valid TCP/UDP Port Number Protocol: From the below drop-down list: • TCP • UDP • TCP+UDP • Any ICMP • Useful ICMP • Useful ICMP+ Ping The ICMP Type/Code allowed combinations are described in the ICMP White List Options table.	IP Address: 172.12.232.106 Port: 22 Protocol: TCP

NOTE: Port Number is available for TCP, UDP and TCP+UDP protocols only in White List configuration.

Table 3.4: ICMP White List options

ICMP White List options	Type	Code
Any ICMP	All	All
Useful ICMP and Useful ICMP + Ping	3 (Destination Unreachable)	All
	0 (Echo reply)	0
	11 (Time Exceeded)	0 (TTL expired in transit)
	11 (Time Exceeded)	1 (Fragment reassembly time expired)
Useful ICMP + Ping	8 (Echo request)	0

Utilities

All available utilities are listed along with a description of the functionality they provide. The following related actions can be performed:

Utilities Log In : This Utility is used for an SSH (Secure Shell) terminal session to the MCP. This option is available from local HMI and Remote HMI. This option is only available to Administrator-level users.

To login to SSH Shell user must have Administrator access and your username and password.

Certificate Import : This utility allows to import certificates and Certificate Revocation Lists (CRLs) from an externally mounted filesystem or the local import directories. This option is available only from local HMI and for Administrator-level users. For more details refer to Appendix G – Security Certificates Creation for MCP.

Certificate Management : This utility allows to manage Local Certificates, Issuer Certificates, and Certificate Revocation Lists. Available only from local HMI and for Administrator-level users. For more details refer to Appendix G – Security Certificates Creation for MCP.

Export Trending/SOE Database : This utility allows to Export/Backup Local Database. This option is available from local HMI and Remote HMI. This option is available to all user levels except Observer-level users.

Generate Gateway Key Pair : Generate Public/Private key pairs in the MCP for the SSH terminal session. This option is available from local HMI and Remote HMI. This option is available to all user levels except Observer-level users.

This MCP HMI utility provides an option to:

- Save the generated Public key to the host computer
- Delete the existing keys.

Exporting VPN Client Configuration File : Export VPN Client Configuration File into a PC/Shared Location/USB. The VPN Client File is used to configure the VPN Client to establish VPN Connection. This option is available only from local HMI and for Administrator-level users.

Upload SSL Server Certificate / Server Key : This MCP HMI utility provides an option to:

- Upload P12 file (PKCS#12) with SSL Server Certificate and Server Key to the device.

This utility allows to enable secured communication between HMI client and MCP device.

This option is available only from local HMI and for Administrator-level users.

The following table lists the available access to different features across the different HMI tools.

Table 3.5: Access to various features of HMI Tools

	Online Config	Local Runtime Viewer	Remote Runtime Viewer
SSH Terminal	Enabled for admin	Enabled for admin	NA
Certificate Import	Enabled for admin	Enabled for admin	NA
Certificate Management	Enabled for admin	Enabled for admin	NA
Export Database ()	NA	Enabled for operator, supervisor and admin	Enabled for operator, supervisor and admin
Generate Gateway Key Pair	Enabled for supervisor and admin	Generate Key Pair - Enabled for supervisor and admin Save Public Key – Enabled for Operator, supervisor and admin Delete Keys - Enabled for supervisor and admin	Save Public Key – Enabled for Operator, supervisor and admin
Export VPN Client	Enabled for admin user only	Enabled for admin	NA
Upload SSL Server Certificate/Key	Enabled for admin user only	Enabled for admin	NA

User

This User setting provide options to configure the appearance of the windows.

Look & Feel - This option allows MCP user to change the look & feel of the windows launched. MCP HMI support multiple themes. Default is GADX.

Themes supported:

1. GADX (Default)
2. Acryl
3. Noire

MCP saves the last configured theme and re-opens the windows with the same theme after re-login.

Window - This option allows to configure the mode in which the main windows and sub windows launch. Default is Docked.

Modes supported:

1. **Docked:** In this mode, all windows when launched, attach to the main window.
2. **Floating:** In this mode, all windows when launched, open as an independent window.
3. **Single:** In this mode, all windows when launched, open as an independent window.

Whenever any window is opened, its position is persisted so that after re-login, MCP opens all the last opened windows in the same state at the same position.

In addition to mode configuration, it also provides option to launch Debugging window for troubleshooting.

User can opt to re-arrange the opened windows in different style.

- Tiled
- Horizontal
- Vertical
- Cascade

User can click “Close All” to close all the opened windows.

Reset Persistency - This option allows MCP to clear all the persisted state of windows.

The Persistency is a default feature both in Remote and Local HMI and will be used to for the below purposes.

a. Persistence of sorting order of the columns, column filters, column width in all the tabular screens or windows.

b. Vertical and horizontal re-sizing of all layout boundaries between screen areas of same screen.

c. Size and position of all windows in floating mode, except location of child pop up dialogs.

d. Persistency is transferrable from one machine to another user (Use case: allow a given user to have the same layout settings across different machines).

e. Persistency is transferrable from one user to another (Use case: allow a given user to give her/his layout settings to another user in the same Windows OS machine, or across machines).

f. Persistency information can be transferred using USB storage, email attachments, Cloud storage from a Windows OS machine.

The Runtime Remote HMI persistency information is generally stored in the Windows OS Machine in the below path:

C:\Users\<User Login Name or User LoginID>\AppData\Local\MCP\RUNTIME_VIEWER

The Reset Persistency is used for the below purposes.

a. User change the resolution of the desktop is changed and current opened window is too big.
b. User wants to reset the current persistency of the size of the connection window.
c. User wants to reset the current sorting persistency of the connection window.
d. User wants to reset the order and column width of point details window.
e. User wants to rest the current column order and width of the Logs window (Control Log/System Event Log/Diagnostic Log/User Activity Log etc..).

This option also has an option to reset the persistency of current user or all users.

If user selects the option to reset the persistency of current user, then all the persistency related information of the HMI user that applied this setting will be cleared.

And, if user selects the option to rest the persistency of all users then all the persistency related information of all the HMI users will be cleared.

Only supervisor and administrator can reset all users, individual operators and observers can only reset his own persistency files.

Logout - When you are finished working with the MCP HMI, you should log out to secure the system. Logging out terminates your user session with the MCP and closes all MCP HMI displays and windows.

» To exit from the MCP HMI:

- Click the **Logout** button on the Power bar.

The MCP HMI closes, and the MCP Login screen appears.

Help

When you click the **Help -> Content** button on the Power bar, the MCP Substation Gateway Online Help opens and displays the topic associated with the MCP page you are currently viewing. The MCP online Help guides you through the displays and functionality of the MCP HMI. The online Help is supplied by the MCP Web server and is not stored on your PC.

There are a few different ways to find information within the MCP Online Help system.

» To find a topic in Help, use one of the following navigation tools:

- Click the **Contents** button to browse through topics by category.
- Click the **Search** tab to search for specific words or phrases contained in Help topics - enter text and select topics from the displayed list.
- Click the **Index** tab to see a list of keywords - either type the word you're looking for or scroll through the list.

» To view Help topics, use one or more of the following techniques:

- On the MCP HMI page you are currently viewing, click the **Help** button on the Power bar to view the Help topic associated with that page.

- In the Help window, use the **Contents**, **Search** and **Index** buttons to find specific topics.
- In a Help topic, click underlined links to jump to the associated topic.

» To print a Help topic

1. Right-click while hovering anywhere on the MCP HMI Online Help window.
2. Select the Print command

Change Displayed Information

Sort Records

Sorting changes the order in which data appears on the screen.

On many display pages, you can change the order in which records appear by choosing a different field to sort by and by choosing to sort records in ascending or descending order.

On most MCP HMI displays, you can change how information appears on the screen.

» To change the sort order of records:

1. Click a field column heading: for example, **Active Alarms** page > **Alarm Date** column heading.
   Result: The records are sorted according to that column heading and an arrow appears in the heading to indicate that the records are sorted in ascending order.
2. Click the field column heading again to change the order from ascending to descending .

   The records are sorted either:

   - Chronologically for date/time information, or
   - Alphanumerically for all other data types

   Result: The records appear in the new sort order.

NOTE When you sort data, only the display on your screen changes, the data is not refreshed from the system database.

Tip: Many pages support customization of columns. Right-click the column heading to add or remove columns from the data grid. You can also drag-and-drop column headings to re-order them horizontally.

Move a Table Column

» To move a column:

- Select a field heading and drag to a new column location.
  Result: The records appear in the new field order.

  NOTE The data is not refreshed when you change the column order.

Resize a Table Column

» To resize a column:

- Position the cursor over the left or right border of a column heading until a double-headed arrow display. Drag left or right to change the column width.
  Result: Columns to the right of the changed column resize to accommodate the changed column width.

Filter Events

Filtering presents all, or a subset of available data from the database.

On some displays, you can filter data by selecting the desired criteria for the records to be retrieved from the database. The following pages can be configured to display different sets of data:

- Active Alarms (configured)
- Historical Alarms (user selectable)
- SOE List (user selectable)
- System Event Log (user selectable)
- Point Details (configured)

Configured filtering is preset in the DS Agile MCP Studio Configuration tool. User-selectable filtering is set by the user on the HMI Runtime screens.

Internationalization

The MCP HMI is:

- Internationalized to adapt to different languages and regional settings.
- Ready to be localized to reflect regional languages, number formats, and date/time formats.

Externalization

The text and labels in the MCP HMI are externalized to resource bundle files so that they may be localized without the involvement of an engineering team.

The following items are not internationalized:

- MCP Configuration Command-line utilities.
- Any text or data coming from external devices (for example, auto-discovered names from a SEL relay).
- File Names, Login Screens, Secret Signatures, Usernames and passwords.
- All graphics and icons.
- GE corporate identities, logos and indicia.

Localization

Localization is the process of adapting an internationalized HMI for a specific region or language by adding locale-specific components and translating text.

For the MCP HMI, localization involves:

1. Translating resource bundle files into specific language.
2. Installing resource bundle files to MCP.
3. Configuring Locale settings.

Localization for a region should be performed by personnel trained in localization for that region. Please contact GE Grid Solutions Technical Support for procedure to create and install resource bundle files to the MCP.

Local Settings

The following local settings can be configured in the MCP HMI:

- HMI language
- Number format
- Data/time formats
- Decimal separator

- Grouping separator

» To reconfigure the local settings:

1. Access the MCP HMI.
2. Click the **Configuration** Power bar button.
3. Click the **Systemwide** tab.
4. In the left pane, click **System** > **Security** and change the security settings, if desired.

Configuration Parameters Supporting Unicode Strings

The below table provides a list of key parameters that can be configured as Unicode UTF-8 strings.

Table 3.6: Configuration Parameters

Configuration Screen	Parameter / Field
Connection	Line ID
	Device ID
	Bay ID
Client Maps	Point Description
	On State (For DI and DO points)
	Off State (For DI and DO points)
System Point Manager	Double Point: Point Description, State
	Point Description for points associated with groups of Accumulator Freeze, Analog Value Selection, Control Lockout, Input Point Suppression, Redundant I/O and Control in progress features.
Alarm	Alarm Description
	Text State 0, Text State 1
	Alarm Groups: Point Description for points associated with groups.
Calculator	Expression: Name, Expression Notes
	Expression: Result Point Description
Load Shed	Feeders: Feeder Description
	Zones: Zone Description
ARRM	Applications →File Set: Point Description for points associated with File Set.
AI Text Enumeration	Text
	Invalid Value Text
One Line Designer	All Elements: Name, Caption
	Alarm Element: Offline – Text Neutral – Text Ack'd Alarm – Text Alarm, No Ack – Text Reset, No Ack - Text
	DataSource → Digital Control DataSource: On State Control Text Off State Control Text State 00/01/10/11 Text
	DataSource → Digital Status DataSource: State 00/01/10/11 Text
Analog Report	Reports → Parameter Map: Value NOTE Unicode is supported for parameter's value, if exporting or viewing online/offline in PDF format.

Language Locale IDs

The following table lists the allocated language Locale IDs. This is not an indication that localized resources are available in these languages; please contact GE Grid Automation Technical Support for currently available language packs.

Table 3.7: Languages - Locale ID's

Language	Country	Locale ID
Albanian	Albania	sq_AL
Arabic	Algeria	ar_DZ
Arabic	Bahrain	ar_BH
Arabic	Egypt	ar_EG
Arabic	Iraq	ar_IQ
Arabic	Jordan	ar_JO
Arabic	Kuwait	ar_KW
Arabic	Lebanon	ar_LB
Arabic	Libya	ar_LY
Arabic	Morocco	ar_MA
Arabic	Oman	ar_OM
Arabic	Qatar	ar_QA
Arabic	Saudi Arabia	ar_SA
Arabic	Sudan	ar_SD
Arabic	Syria	ar_SY
Arabic	Tunisia	ar_TN
Arabic	United Arab Emirates	ar_AE
Arabic	Yemen	ar_YE
Belarusian	Belarus	be_BY
Bulgarian	Bulgaria	bg_BG
Catalan	Spain	ca_ES
Chinese (Simplified)	China	zh_CN
Chinese (Simplified)	Singapore	zh_SG(*)
Chinese (Traditional)	Hong Kong	zh_HK
Chinese (Traditional)	Taiwan	zh_TW
Croatian	Croatia	hr_HR
Czech	Czech Republic	cs_CZ
Danish	Denmark	da_DK
Dutch	Belgium	nl_BE
Dutch	Netherlands	nl_NL
English	Australia	en_AU
English	Canada	en_CA
English	India	en_IN
English	Ireland	en_IE

Language	Country	Locale ID
English	Malta	en_MT(*)
English	New Zealand	en_NZ
English	Philippines	en_PH(*)
English	Singapore	en_SG(*)
English	South Africa	en_ZA
English	United Kingdom	en_GB
English	United States	en_US
Estonian	Estonia	et_EE
Finnish	Finland	fi_FI
French	Belgium	fr_BE
French	Canada	fr_CA
French	France	fr_FR
French	Luxembourg	fr_LU
French	Switzerland	fr_CH
German	Austria	de_AT
German	Germany	de_DE
German	Luxembourg	de_LU
German	Switzerland	de_CH
Greek	Cyprus	el_CY(*)
Greek	Greece	el_GR
Hebrew	Israel	iw_IL
Hindi	India	hi_IN
Hungarian	Hungary	hu_HU
Icelandic	Iceland	is_IS
Indonesian	Indonesia	in_ID(*)
Irish	Ireland	ga_IE(*)
Italian	Italy	it_IT
Italian	Switzerland	it_CH
Japanese (Gregorian calendar)	Japan	ja_JP
Japanese (Imperial calendar)	Japan	ja_JP_JP
Korean	South Korea	ko_KR
Latvian	Latvia	lv_LV
Lithuanian	Lithuania	lt_LT
Macedonian	Macedonia	mk_MK
Malay	Malaysia	ms_MY(*)
Maltese	Malta	mt_MT(*)
Norwegian (Bokmål)	Norway	no_NO
Norwegian (Nynorsk)	Norway	no_NO_NY
Polish	Poland	pl_PL

Language	Country	Locale ID
Portuguese	Brazil	pt_BR(*)
Portuguese	Portugal	pt_PT(*)
Romanian	Romania	ro_RO
Russian	Russia	ru_RU
Serbian (Cyrillic)	Bosnia and Herzegovina	sr_BA(*)
Serbian (Cyrillic)	Montenegro	sr_ME(*)
Serbian (Cyrillic)	Serbia	sr_RS(*)
Serbian (Latin)	Bosnia and Herzegovina	sr_Latn_BA(**)
Serbian (Latin)	Montenegro	sr_Latn_ME(**)
Serbian (Latin)	Serbia	sr_Latn_RS(**)
Slovak	Slovakia	sk_SK
Slovenian	Slovenia	sl_SI
Spanish	Argentina	es_AR
Spanish	Bolivia	es_BO
Spanish	Chile	es_CL
Spanish	Colombia	es_CO
Spanish	Costa Rica	es_CR
Spanish	Dominican Republic	es_DO
Spanish	Ecuador	es_EC
Spanish	El Salvador	es_SV
Spanish	Guatemala	es_GT
Spanish	Honduras	es_HN
Spanish	Mexico	es_MX
Spanish	Nicaragua	es_NI
Spanish	Panama	es_PA
Spanish	Paraguay	es_PY
Spanish	Peru	es_PE
Spanish	Puerto Rico	es_PR
Spanish	Spain	es_ES
Spanish	United States	es_US(*)
Spanish	Uruguay	es_UY
Spanish	Venezuela	es_VE
Swedish	Sweden	sv_SE
Thai (Western digits)	Thailand	th_TH
Thai (Thai digits)	Thailand	th_TH_TH
Turkish	Turkey	tr_TR
Ukrainian	Ukraine	uk_UA
Vietnamese	Vietnam	vi_VN

(*) Data for these locales are derived from the Unicode Consortium's Common Locale Data Repository release 1.4.1 on an "AS-IS" basis.

(**) Data for these locales are derived from the Unicode Consortium's Common Locale Data Repository release 1.9 on an "AS-IS" basis.

Manage Alarms

This chapter contains the following sections and sub-sections:

Digital Event Management

Alarm Types

Alarm Groups

Double Point Alarms

Active Alarms

View Active Alarms

Acknowledge an Alarm

Enable or Mute an Audible Alarm

Enable or Mute an Alarm Buzzer

Historical Alarms

View Historical

Digital Event Management

In the substation-monitoring environment, alarms are used to indicate the occurrence of an event that requires attention, for example, the opening of a breaker due to an over-current condition.

The MCP monitors a given set of digital input points for alarm conditions. Each configured alarm by default has no associated pseudo points. However, if the “individual digital input indications” parameter is set in an alarm group, then a single digital input pseudo point is created for each alarm in the group.

Digital Event Management (DEM) allows mapping of individual binary points from the RTDB (“source points”) into Alarm Groups, resulting in alarm grouping and alarm reduction.

Abnormal source point conditions (such as, offline) are automatically translated into configurable alarm events, without the need of additional logic.

Additional alarm events occurring in a group already in alarm, causes the “re-flash” (pulsing) of a dedicated associated point associated with each group without additional logic being required.

The time stamp of the alarm group output and re-flash points follow the time stamp event of the source point that caused the group change.

In addition to the Alarm Grouping and re-flash functionality in the RTDB, DEM also provides the HMI Active Alarm page and provides support for Alarm Annunciator functions – created and enabled automatically when configuring DEM.

Upon detecting an alarm condition on a source point or a group of points, the MCP creates a record in the database and presents the alarm to the operator on the MCP Active Alarms page for further action. Once an alarm is acknowledged it is archived by moving it from the **Active Alarms** page to the **Historical Alarms** page.

You can:

- View Active Alarms
- View Historical Events
- Acknowledge an Alarm
- Configure Alarms, including double-point alarms, alarm points and alarm settings
- Enable or Mute an Audible Alarm

Alarm Types

The following alarms types are configurable:

Deviation Alarms (2-state)	:	Generates an active alarm when the point state changes from normal to alarmable and archives the alarm only when the point state returns to normal and the alarm is acknowledged.
On Update Alarms (2-state)	:	Generates an active alarm when the alarm state changes from one state to another and archives the alarm when the alarm is acknowledged. In effect, two alarms are created: the first alarm is generated when the source point changes from ON to OFF, and a second alarm is generated when the source point changes from OFF to ON.
Double Point Alarms (4-state)	:	Two alarm types are generated – an **OnUpdate Alarm** and a **Deviation Alarm**.

You can only select pre-configured double points for this type of alarm.

- An **On Update Alarm** is generated when the double point is in the transit state (both points = 0) or in the invalid state (both points = 1) and the state persists longer than the configured invalid period of time. The On Update alarm is archived when it is acknowledged.
- A **Deviation Alarm** is generated when the double point is in the open state (open point = 1, close point = 0) and is put in the reset state when the double point returns to the close state (open point = 0, close point = 1). The Deviation alarm is archived when the alarm state is reset, *and* it is acknowledged.

The Digital Event Manager does not support the "," (comma) character in the Point, Point State, Alarm and Alarm State field descriptions. If the user has used commas in these field descriptions during configuration, the commas are automatically replaced with spaces during runtime processing.

The MCP does not raise alarms on points that are offline.

Alarm Groups

Digital Event Management supports alarm groups named Group1, Group2, Group3, and so on, plus a System alarm group. Based on your alarm group settings, individual alarms within an alarm group are displayed with the configured foreground color, background color, blinking rate and sound for the current alarm state.

You can think of an alarm group as a summary - if a given alarm group is in the normal state, then all alarms belonging to the group are normal. Alarm group indications are further grouped into a System alarm to indicate if any input point in the group is in an alarm condition.

Double Point Alarms

The Double Point feature of the System Point Manager allows you to associate two digital input points to form a double point indication.

Active Alarms

The **Active Alarms** page lists all active alarm events on every alarm-enabled point in the MCP database. The display automatically updates whenever the MCP generates a new alarm, or when the status of an existing alarm changes. The total number of active alarms in the system database is shown in the bottom left corner of the window.

The **Active Alarms** button on the Power bar visually indicates the status of active alarms in the MCP:

Blinking red when unacknowledged active alarms exist

Steady green when no active alarms are present

Steady yellow when acknowledged active alarms are present

The MCP does not raise alarms on points that are offline.

View Active Alarms

The **Active Alarms** page lists all active alarm events on every alarm-enabled point in the MCP database. Active alarms are in one of the following states:

- Normal (Deviation)
- In Alarm (On Update)

By default, the alarms are listed with the most recent alarms appearing at the top of the list.

Alarm records

The following details are available for each alarm record.

Table 3.8: Alarm Records

Setting	Description
Acknowledged Date	Date and time (to millisecond) when the alarm was acknowledged.
Record ID	A unique number to identify the alarm record.
Acknowledge (Button) – Active Alarms Only	Click to manually acknowledge the alarm
Acknowledged (Acknowledge Indicator)	A checkmark appears if the active alarm has already been acknowledged (manually or automatically).
State Description	Describes the point state when the associated alarm value is in the Alarm state. Typically, the point is in the: ON if the alarm value is in alarm the state and OFF if the alarm value is in the Normal state.
Alarm Date	Date and time (to millisecond) when the alarm was created.
Alarm ID (Alarm Identifier)	A unique ID of an alarm.
Reference	Describes the alarm point. It defaults to the name of the alarm point.
Type	Indicates the type of alarm: "On Update" or "Absolute".
Value	Indicates the alarm state: 0, typically the Normal state or 1, typically the Alarm state.
Device ID	Identifies the device associated with this alarm point.

Setting	Description
Groups (Active Alarms Only)	Alarm group to which the point's alarm is associated.
Line ID	Identifies the electrical transmission line associated with the device of this alarm point.
Originator	The source of the control command. See Originators for more information.
Reset Date	Date and time (to millisecond) when the alarm was reset.
Reset (Reset Indicator)	When a checkmark is displayed, it indicates that alarm has returned to Normal state.
Sequence ID	Sequence ID of the alarm record.
Archived (Historical Alarms Only)	When a checkmark is displayed, it indicates that alarm has been archived.
Archived Date (Historical Alarms Only)	Date and time (to millisecond) when the alarm was archived.
Username	Identifies the Username that acknowledged the alarm
Description	Describes the alarm point. It defaults to the source point.
Home Directory	Home directory of the source producer / application
Bay ID	Bay ID description of the Home directory
Device Type	Device Type of the Home directory

The fields which appear on the Active Alarms page are configurable.

The fields which appear on the Historical Alarms page are user selectable.

NOTES:

- **Critical Alarms** are shown in a separate tab in the lower half of the window. All other alarm groups can be accessed by clicking the tabs in the top half of the window.
- If one or more digital input points have the force, alarm inhibit, or scan inhibit quality flags set, a message saying "Alarms have been suppressed" is shown at the bottom of the screen.
- The MCP does not raise alarms on points that are offline.
- Active Alarm Viewer retains the last saved sorting criteria/filters for the fields when navigating away and back.

» To view alarms:

1. Click the **Active Alarms** button on the Power bar.
2. Select a **Group** tab or **All Alarms** (includes System alarms) tab to view the current active alarms. You can filter by **Line ID**, **Device ID**, and/or **Bay ID**.

Each tab lists active alarm records generated by the MCP. Alarms that need to be acknowledged are visually indicated by color and flashing as configured in the alarm settings.

Tip: Right-click any column heading to customize the columns shown. You can also drag-and-drop column headings to re-order them horizontally.

» To create an alarm group tab:

1. Click the **Add Alarm Group** button.
   Result: A popup window appears.
2. Select the desired alarm group.
3. Click **OK**.

» To delete an alarm group tab:

- Click the red **x** on the right side of the tab.

Acknowledge an Alarm

Alarms are acknowledged on the **Active Alarms** page. You can manually acknowledge an individual alarm, selected alarms or a group of alarms. "On Update" alarms are acknowledged automatically only if the **Ack Method** is set to Automatic.

» To acknowledge an alarm:

1. Select one or more alarms on the **Active Alarms** page.
2. Click Acknowledge Alarm(s).

» To acknowledge all alarms in an alarm group:

- On an alarm group tab on the **Active Alarms** page, click **Acknowledge Group**.

When you acknowledge an alarm or alarm group:

- "Acknowledge Indicator" field is checked
- Acknowledged alarm record changes in foreground color, background color and blink rate as configured in alarm settings
- Acknowledged alarm record is moved from the Active Alarms page to the Historical Alarms page

NOTES:

- Deviation alarms that are acknowledged continue to appear on the Active Alarms page until they return to a normal (non-alarmable) state.
- You cannot remove an acknowledgement once an alarm has been acknowledged.
- Dynamic alarm objects can be acknowledged directly on a one-line diagram

Enable or Mute an Audible Alarm

You can activate a sound to be played when a new alarm is received.

» To enable/mute an audible alarm:

- On the **Active Alarms** page, click **Enable Alarm Sound** or **Disable Alarm Sound** to toggle the audible alarm on or off.

NOTE To hear audible alarms in the MCP HMI, the volume must not be muted in Windows. Check the Volume control on the Windows taskbar. Click the control to change the volume setting.

Enable or Mute an Alarm Buzzer

The buzzer will be activated based on the configuration values. This buzzer can be activated or deactivated when a new alarm is received.

» To enable/mute buzzer

- On the **Active Alarms** page, click **Enable Buzzer** or **Disable Buzzer** to toggle the buzzer on or off.

Historical Events

A historical event is an alarm that has been archived from the **Active Alarms** list. The **Historical Events** page provides a search utility to filter, sort and display historical alarm records stored in the real-time database.

To be archived to the **Historical Events** page, an alarm must meet the following conditions:

- "Deviation" alarm is acknowledged *and* has returned to normal state
- "On update" alarm is acknowledged

- "Double Point" alarm is acknowledged and the pair of source points have moved into a non-alarmable state

View Historical Events

The **Historical Events** page provides a search utility to filter, sort and display historical alarm records stored in the MCP.

» To view historical events:

1. Click the **Historical Events** button on the Power bar. A new window opens.
2. All the available historical alarm records are shown. You can filter by **Line ID**, **Device ID**, and/or **Bay ID**, and you can choose the number of records to show on each page.
3. You can save the records in CSV format by clicking the **Export Data** button. This exports all available data, even across multiple pages. Records that are filtered out are not included.

Tip: Right-click any column heading to customize the columns shown. You can also drag-and-drop column headings to re-order them horizontally.

View Data

This chapter contains the following sections and sub-sections:

View Data

Real-Time Database

Data types

Data Quality Status

Point Summary

View Point Details

View Events

Connections

Logs

Trends

View Data

User can view:

- Events
- Active Alarms
- Historical Alarms
- Point Details
- Communications Traffic
- System Logs
- Analog Report

Real-Time Database

The MCP communicates with devices connected to the electric power network. These devices monitor and record several types of information, which can be generally classified as:

- Present values (PVal) that reflect the state of the power system at an instance in time.
- Peak demand values that reflect the minimum and maximum power flow conditions encountered.
- Demand values.
- Disturbance or fault records - time-stamped record of a disturbance, fault or other similar event within the power system, considered to be a serious alarm condition.

The real-time database (RTDB) is a core component of the MCP. It resides within the MCP and acts as a central container for all data that is collected and may need to be exchanged between MCP applications. The real-time database stores the value of all input/output data collected by the MCP in the form of point data, as well as the occurrence of events that take place (for example, disturbance or fault records). The MCP can manipulate the data from devices to produce additional local/pseudo data points. The real-time database is commonly referred to as the system point database.

The following general types of information are stored:

- Point data and values
- Analog set point status
- Digital control status
- Tagging/Inhibit status
- Force value status
- Statistics

Data is organized and presented to the User in the following formats:

Table 3.9: Data Formats

Format	Description
Record	Single set of data pieces, for example, an alarm record or SOE record.
Field	Single piece of information or data that is of the same type across all records, for example, Device ID.
Sort key	Field information that is used to select the type of information to display from the database.
Filter criteria	Specific parameters used to isolate and select appropriate records from the database.

The following related actions can be performed:
View Active Alarms
View Historical alarms

Data types

The real-time database (RTDB) stores the following data types:

Table 3.10: Data Types

Format	Abbreviation	Data Type	Description
Digital Input (also Binary Input)	DI (BI)	One-bit Integer	Typically represents the On/Off state of a physical device. May also indicate any single bit value that is derived from other data or used to indicate that a condition exists or that a process is in a state. If not representing the state of a physical device, it is referred to as a pseudo point.

Digital Output (also Binary Output)	DO (BO)	One-bit Integer	Used as a means to control the On/Off state of a physical device, or in the case of a pseudo output, to initiate the function or operation associated with the output.
Analog Input	AI	64 bits Real	Typically represents the value of a physical device that is capable of sensing and reporting a range of discrete values. May also be used as a pseudo point to represent the output of a process or any other derived value that cannot be represented as a single bit.
Analog Output	AO	64 bits Real	Used to control the value provided to an external device or process.
Accumulator	ACC	64 bits Integer	Typically represents the accumulated value of a counting operation. This count could be the number of times a digital input changed state, or the amount of energy carried by a conductor over a certain period. May also be used as a pseudo point to represent the number of times a operation took place or how often a function was executed.
Text	TXT	132 bytes Character 255 bytes characters only for 61850 Client applications	Typically used to represent the description of an event such as a protective fault report.

Data Quality Status

Quality details are provided for each configured point or object to inform the operator of the status of the data shown. The quality status and quality attribute (also referred to as the quality flags) are stored in the MCP database along with the point/object and are updated as the status or value of the point or object changes. The current quality status and quality attribute are presented on the **Point Details** page and **One-Line Viewer**.

Quality status

The current quality status is presented for each point and object and indicates the general nature of the data stored for the point. Quality status can be one of:

Normal - The data is considered correct and there are no actions or exceptions marked on the point

Invalid - The data is not accurate or up-to-date due to the status of the device

Questionable - The data is likely to be inaccurate or out-of-date due to the status of the device

The foreground and background colors for **Point Value** and **Quality Status** (based on configured display settings) change to alert the user regarding the current quality state. The default color settings to indicate quality status are:

Table 3.11: Quality Status

Quality Status	Foreground Color	Background Color
Normal	Black	Green
Invalid	Pink	Grey
Questionable	Black	Grey
Zombie	Maroon	Grey

Engaged Quality	Black	Spring green

Quality Attributes

The MCP provides the following quality attributes for each point:

Table 3.12: Quality Attributes

Indicator	Quality Attribute	Description
T	Tagged	The point has been tagged with additional information, such as a note.
M	Manual (Local) force	An operator has forced the point value and/or quality to static values at the point of origin. The point is no longer being updated with actual data
R	Remote force	The device is reporting that the point has been forced to a static value remotely. The point is no longer being updated with actual data.
S	Scan inhibited	An operator has blocked scanning of the point. The point is no longer being updated with actual data.
A	Alarm inhibited	An operator has blocked alarms on this point. All alarms derived from this point cannot be raised.
C	Control inhibited (also called Output inhibited)	An operator has blocked output requests on this point. All output requests directed to this point are rejected.
XX	Chatter (for Digital Input) / Over- Range (for Analog Input)	This attribute means Chatter for Digital Inputs and Over-Range for Analog Inputs. Chatter indicates that the device is reporting that the point is experiencing an excessive number of state changes and that a chatter filter may be engaged. Over-Range indicates that the device is reporting that the point value has exceeded its maximum measurement range.
X	Invalid	Functions as a summary flag for: • Offline • Chatter • Over Range • Overflow • Reference Check When quality is "Invalid", the data reported by the MCP may not be an accurate representation of the actual data source.
?	Questionable	Functions as a summary flag for the Communication Lost and Old Data flags, where: • Communication Lost indicates that the MCP has lost communication with the reporting device, or that the device itself has lost communication with the source of the point data • Old Data indicates that the value has not been updated within a configured time interval. Old Data can be set under various conditions: 1) Scan Inhibit is applied and new data is available; 2) Data is reported directly by a 61850-capable device; 3) Communication congestion is preventing the device from being scanned as required by the user configuration settings. When quality is "Questionable", the data reported by the MCP may not be an accurate representation of the actual data source.

Indicator	Quality Attribute	Description
OD	Old Data	Old Data indicates that the value has not been updated within a configured time interval. Old Data can be set under various conditions: 1) Scan Inhibit is applied and new data is available; 2) Data is reported directly by a 61850-capable device; 3) Communication congestion is preventing the device from being scanned as required by the user configuration settings.
O	Offline	Offline indicates that the MCP is not communicating with the device
CX	Comm Lost	The MCP is unable to communicate with the device or application reporting the point.
OR	Over-Range	Over-Range indicates that the device is reporting that the point value has exceeded its maximum measurement range
CK	Reference Check	Reference Check indicates that the device is reporting that one or more of the references used to determine the value of the field point are outside allowable tolerances
OF	Overflow	Overflow indicates that the device is reporting that the point value has exceeded its maximum reporting range. For accumulators, this means that the value has rolled over.
2	Secondary Source	The data of this point is being reported from a Secondary source. Refer to **Redundant I/O** for more information.
2x	Secondary Source Invalid	The Secondary source of this point is invalid. This flag is applied regardless of whether the Primary source is being reported as itself or as the Secondary source. Refer to **Redundant I/O** for more information.
2F	Secondary Source Inhibit	The Secondary source of this point is being inhibited (see above for inhibit types). This flag is applied regardless of whether the Primary source is being reported as itself or as the Secondary source. Refer to **Redundant I/O** for more information.
LC	Local Control Active	This point belongs to a local control group that is currently active. Refer to **Control Lockout** for more information on this feature.
RC	Remote Control Active	This point belongs to a remote-control group that is currently active. Refer to **Control Lockout** for more information on this feature.
P	Suppressed	Suppression is active on this point. Refer to **Input Point Suppression** for more information on this feature.
Z	Zombie	Zombie indicates when a MCP firmware application becomes non-functional after restart attempts.

In some places, quality attributes (flags) are presented as a numeric value instead of a list of discrete flags. Each discrete flag is represented as a bit encoded value, as following:

Bit	MCP (legacy) Quality Attribute
0	Offline
1	Restart
2	Comm Lost
3	Remote force
4	Reference Check
5	Chatter

5	Overflow
5	Rollover
6	Old Data
7	Test
9	Questionable
10	Invalid
11	Remote Scan Inhibit
15	Remote Timestamp
16	Control inhibited (also called Output inhibited)
17	Alarm inhibited
18	Scan inhibited
19	Tagged
20	Manual (Local) force

To determine which quality flags are set you need to convert the decimal numeric value to binary and, starting from the right side, first bit is Bit 0, then immediately followed to the left by Bit 1, etc.

Please note that, depending on the tool you use to convert to binary - the leading zero bits (i.e. most left ones which are only 0) may not be shown.

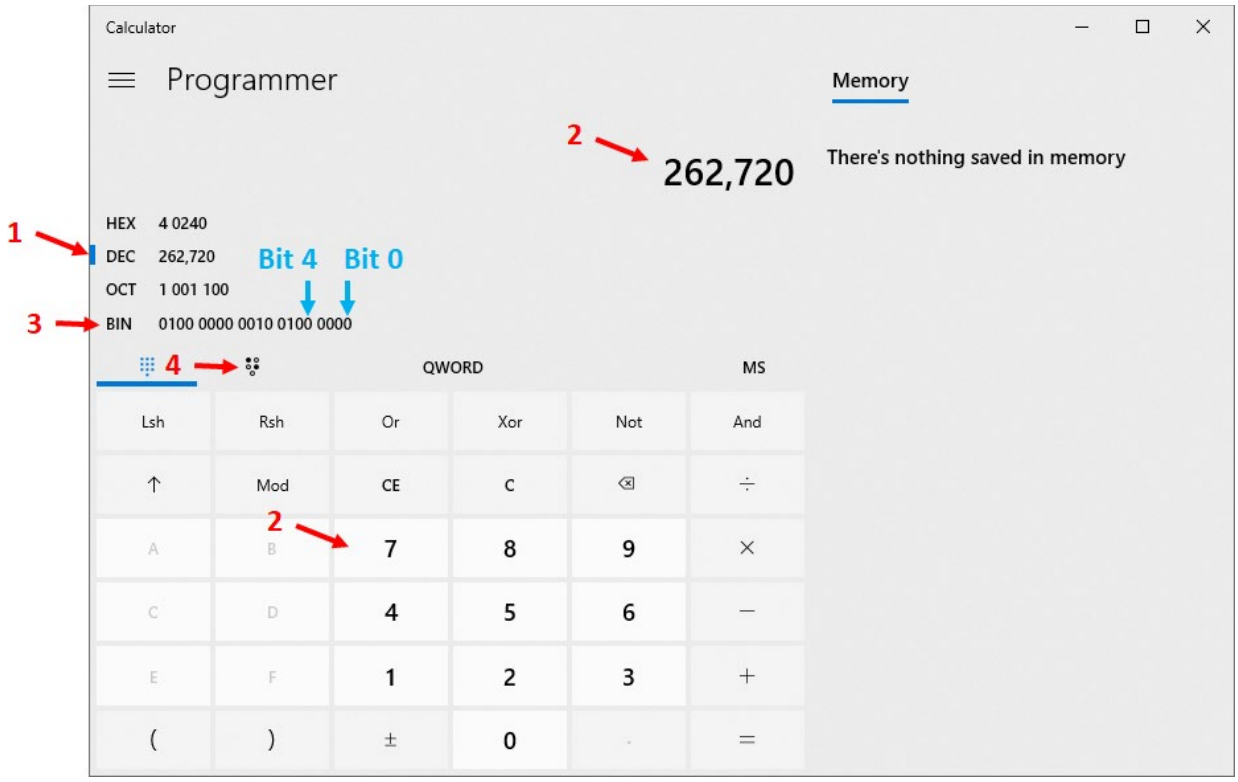
For example, the numeric value is 262720.

Using for example the Calculator application within Windows 10, set to Programmer mode:

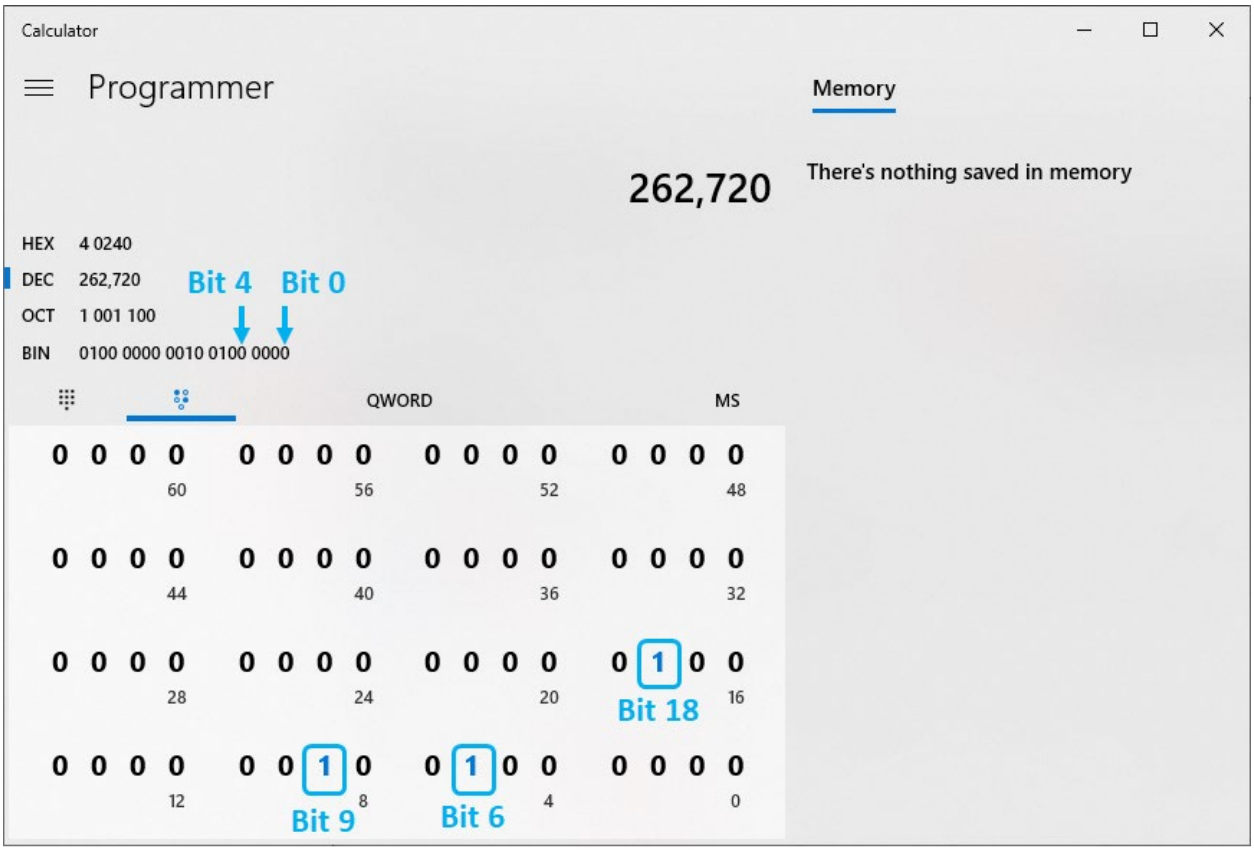
1. Make sure you are in Decimal mode (click on DEC)

2. Enter the decimal value

3. Look at the BIN filed, it shows the binary bit encoded representation



4. In this calculator application you may also click on the binary toggle button (4), and see a detailed bit wise representation, as following:



In the above example, the set (=1) bits are 6, 9, and 18.

Based on the encoded table this means:

- Old Data
- Questionable
- Scan inhibited

» To view data quality:

The User can view quality information for individual data points and objects from the following pages and screens:

- Point Details
- One-Line Viewer
- Local force interface
- Tag/inhibit interface
- Analog output interface
- Digital output interface

The quality attributes (except Zombie Quality) are presented in abbreviated format (see **Indicator** in table above) on the Point Detail pages and One-Line Viewer.

User can force quality attributes from the **One-Line Viewer** or **Point Details** pages if the user have Operator or Supervisor permission levels.

Forcing data quality and values

If the user has an operator or supervisor privilege level, then they can force the system to stop responses for data quality attributes in the following ways:

- Alarm inhibit (the associated data point does not cause an alarm)
- Control inhibit (the associated data point does not cause a control to activate)
- Scan inhibit (the associated data point does not update the database)

In addition, if the user has an operator or supervisor privilege level, then they can force a data value on a data point.

Forcing quality can be performed locally or remotely.

Point Details

The **Point Details** page lists system elements (and identifying information) for which points have been configured, categorized by:

- IED
- Master Station
- Application
- Point Groups

The following related actions can be performed:
View I/O (IED and Master Station only)
View point details

IED Point Summary

The **IED Point Summary** page lists the configured devices in the system. The following information is provided for each device:

Table 3.13: IED Point Summary

Point Name	Description
Home Dir	System location of the device/application.
Line ID	Electrical transmission line associated with the device.
Device ID	Description of the device.
Bay ID	The name of the bay containing the device.
Device Type	Name of the client map file used with the specific device.
Details	Protocol address of the device (i.e. DNP device address, IP Address, or serial port number, etc.).

The user can display the recorded sequence of event (SOE) and protective relay fault (PRF) events for a selected device.

» To view SOE/PRF events:

- Click the **SOE/PRF** button for a selected device on the **IED Point Summary** page. Result: The **SOE/PRF List** window opens showing the stored SOE and PRF event records for the selected device.

SOE List

Table 3.14: SOE List

Event Record	Description
Event Date Time	Date and time (to millisecond) when the event was created.
Point Description	Description of the point in the map file.
State	Value of the state (1 = ON, 0 = OFF)
State Descriptor	Description of the state.

PRF List

Table 3.15: PRF List

Event Record	Description
Event Date Time	Date and time (to millisecond) when the event was created.
Fault Distance	Description of the point in the map file.
Trip Description	Description of the state.

The following related actions can be performed:
View I/O
View point details
Enable/disable IED communications

Master Station Point Summary

The **Master Station Point Summary** page lists the configured master stations in the system. The following information is provided for each master station:

Table 3.16: Master Station Point Summary

Field	Description
Home Dir	System location of the device/application.
Map File	Name of the server map file used with the specific master.
Name	Description of the master station.
Details	Protocol address of the device (i.e. DNP device address, IP Address, or serial port number, etc.).

The following related actions can be performed:
View I/O
View point details

Application Point Summary

The **Application Point Summary** page lists the configured applications in the system. The following information is provided for each application:

Table 3.17: Application Point Summary

Field	Description
Home Dir	System location of the device/application.
Application Name	Description of the application.
Application Address	A unique identifier for the application, usually used to identify pseudo points.

The following related actions can be performed:
View I/O
View point details

Point Groups Summary

The **Point Groups Summary** page lists the configured point groups in the system. The available information is provided for each point group:

- Tree view of selectable point groups for **Present Value**, **Peak Demand** and **Demand** data
- Tabbed panes for each data type: **Accumulator**, **Analog Input**, **Analog Output**, **Digital Input** and **Digital Output**, **All** showing point details

The following related action can be performed:
View point details

I/O Traffic Viewer

The **I/O Traffic Viewer** lists real-time communication messages between the MCP and a selected device or master station. The display automatically scrolls and refreshes as new messages are exchanged.

» To view I/O:

- Click the View button on the IED/Master Station Communications Summary page or the Monitor button on the Point Summary page or Detailed Statistics window.

  The **I/O Traffic Viewer** window opens. Each message includes the following information:

  - Direction of message flow (incoming or outgoing)
  - Date and time of message
  - Message content in ASCII or HEX text (as configured)
  - Message type

On this screen, user can:

- Show/Hide Info Messages
- Pause/Resume the display of messages
- Clear all messages from the buffer
- Change the buffer size

When I/O communication messages exceed the buffer size, the oldest message is removed to make room for the new message. The default buffer size for the screen text area is 32 KB.

» To change the buffer size:

1. In the I/O Traffic Viewer window, click Buffer Size.
2. Enter a value and click **OK**.

The buffer size is changed as the user specified.

Tip: User can copy and paste text from the message window using the browser's copy and paste functions (e.g. **Ctrl**-**C** to copy and **Ctrl**-**V** to paste).

View Point Details

» To view point details:

1. On the **Point Summary** page, click the **Details** button for a selected connection (IED, Master Station, Application, Point Group). The **Point Details** page displays.
2. Select a point type tab, for example **Analog Input**. All the configured points and point details appear.
3. Use the page navigation buttons to select and scroll pages quickly.
4. Click **Close** when you are done.

Multiple Point Details windows may be open; they must be closed manually. Up to 8 windows may be open.

Tip: If more than 20 points exist for the selected type, the point display is broken up across multiple pages. Use the navigation buttons shown at the bottom of the window to move through the points list.

Maintenance Mode

A checkbox at the top of the point details window allows you to toggle **Maintenance Mode** on and off. This allows the user to view actual point details on system points that are affected by system features like input point suppression and redundant I/O. Enabling maintenance mode adds the **Last Reported Value**, **Last Reported Quality**, and **Last Reported Time** fields to the data grid.

The following related actions can be performed:
Sort records
Issue a command

Point Details

The **Point Details** page lists all configured points and real-time point values in the real-time database. The **Point Details** page displays one tabbed pane per point type:

- Accumulator
- Analog Input
- Analog Output
- Digital Input
- Digital Output
- Text
- All Points
- Pseudo Points

Point values update at a configured interval to display the most current values.

Tips

- If more than 20 points exist for the selected type, the point display is broken up across multiple pages. 20 points are shown per page with page numbers and navigation buttons shown at the bottom of the window.
- Pseudo points and values are available from the **IED/Master Station Communications Summary** pages.

The following related actions can be performed:
View point details
Issue a command

Accumulator tab

Accumulators typically represent the accumulated value of a counting operation. This count could be the number of times a digital input changed state, or the amount of energy carried by a conductor over a certain period. May also be used as a pseudo point to represent the number of times an operation took place or how often a function was executed.

The following point information is provided for each accumulator point on the **Point Details** page:

- Point ID
- Point reference
- Point description
- Running value - current value
- Quality attributes

- Updated time
- Frozen value
- Freeze date and time
- Clear date and time

The quality status of Running value and Quality Attributes are visually indicated according to configured color settings for Invalid, Questionable or Normal.

Point values update at a configured interval to display the most current values.

If more than 30 points exist for the selected type, the point display is broken up across multiple pages. Use the navigation buttons shown at the bottom of the window to move through the points list.

The following related actions can be performed:
View point details
Issue a command

Analog Input tab

Analog inputs typically represent the value of a physical device that is capable of sensing and reporting a range of discrete values. An analog input may also be used as a pseudo point to represent the output of a process or any other derived value that cannot be represented as a single bit.

The following point information is provided for each analog input point on the **Point Details** page:

- Point ID
- Point reference
- Point description
- Point value - scaled value
- Quality Attributes
- Updated time

The quality status of Point value and Quality attributes are visually indicated according to configured color settings for Invalid, Questionable or Normal.

Point values update at a configured interval to display the most current values.

If more than 30 points exist for the selected type, the point display is broken up across multiple pages. Use the navigation buttons shown at the bottom of the window to move through the points list.

The following related actions can be performed:
View point details
Issue a command

Analog Output tab

Analog outputs are typically used to control the value provided to an external device or process.

The following point information is provided for each analog output point on the **Point Details** page:

- Point ID
- Point reference
- Point description
- Point value - scaled value
- Quality attributes
- Updated time

The quality status of Point value and Quality attributes are visually indicated according to configured color settings for Invalid, Questionable or Normal.

Point values update at a configured interval to display the most current values.

If more than 30 points exist for the selected type, the point display is broken up across multiple pages. Use the navigation buttons shown at the bottom of the window to move through the points list.

The following related actions can be performed:
View point details
Issue a command

All Points tab

The **All** tab on the **Point Details** page lists all configured data points in the system point database.

The following point information is provided for each point on the **Point Details** page:

- Point ID
- Point reference
- Point description
- Point value - current present value
- Quality Attributes
- Updated time
- Data type

The quality status of Point value and Quality attributes are visually indicated according to configured color settings for Invalid, Questionable or Normal.

Point values update at a configured interval to display the most current values.

If more than 30 points exist for the selected type, the point display is broken up across multiple pages.

Use the navigation buttons shown at the bottom of the window to move through the points list.

The following related actions can be performed:
View point details
Issue a command

Digital Input tab

Digital inputs (also referred to as binary inputs) typically represent the On/Off state of a physical device. A digital input may also indicate any single bit value that is derived from other data or used to indicate that a condition exists or that a process is in a state. If not representing the state of a physical device, it is referred to as a pseudo point.

The following point information is provided for each digital input point on the **Point Details** page:

- Point ID
- Point reference
- Point description
- Point value - current present value
- Quality Attributes
- Updated time
- State description

The quality status of Point value and Quality attributes are visually indicated according to configured color settings for Invalid, Questionable or Normal.

NOTE Point values update at a configured interval to display the most current values.

TIP If more than 30 points exist for the selected type, the point display is broken up across multiple pages. Use the navigation buttons shown at the bottom of the window to move through the points list.

The following related actions can be performed:
View point details
Issue a command

Digital Output tab

Digital outputs (also referred to as binary outputs or control outputs) are used to control the On/Off state of a physical device, or in the case of a pseudo output, to initiate the function or operation associated with the output.

The following point information is provided for each digital output point on the **Point Details** page:

- Point ID
- Point reference
- Point description
- Point value - current present value
- Quality Attributes
- Updated time
- State description

The quality status of Point value and Quality attributes are visually indicated according to configured color settings for Invalid, Questionable or Normal.

NOTE Point values update at a configured interval to display the most current values.

TIP If more than 30 points exist for the selected type, the point display is broken up across multiple pages. Use the navigation buttons shown at the bottom of the window to move through the points list.

The following related actions can be performed:
View point details
Issue a command

Text tab

Text points are typically used to represent the description of an event such as a protective fault report. They may also be used as a pseudo point to represent the output of a process or any other derived value that cannot be represented as a single bit or analog value.

The following point information is provided for each text point on the **Point Details** page:

- Current Value
- Last Reported Value
- Current Quality Flags
- Last Reported Quality Flags
- Last Reported Timestamp
- Tag Description
- Point Description

The quality status of Point value and Quality attributes are visually indicated according to configured color settings for Invalid, Questionable or Normal.

NOTE Point values update at a configured interval to display the most current values.

If more than 30 points exist for the selected type, the point display is broken up across multiple pages. Use the navigation buttons shown at the bottom of the window to move through the points list.

The following related actions can be performed:

View point details
Issue a Command

View Events

The **SOE/PRF** page provides a search utility to filter, sort and display sequence of events (SOEs) and protective relay faults (PRFs) records stored in the MCP.

» To view events:

1. Click the **SOE/PRF** button on the Power bar. A new window opens.
2. Select the **SOE** tab for sequence of events records. Select the **PRF** tab for protective relay fault records.
3. The records are shown in the data table. You can filter by **Line ID**, **Device ID**, and/or **Bay ID**, and you can choose the number of records to show on each page.
4. User can save the records in CSV format by clicking the **Export Data** button. This exports all available data, even across multiple pages. Records that are filtered out are not included.

Right-click any column heading to customize the columns shown. You can also drag-and-drop column headings to re-order them horizontally.

Event Records

The following details are available for each event record (depending on the record type):

Table 3.18: Event Records

Field	Event Type		Description
	SOE	PRF	
Record ID	✓		A unique number to identify the event record.
Event ID		✓	
Trip Description		✓	An alphanumeric value indicating the type of failure recorded.
Fault Code		✓	A numeric value indicating the type of failure recorded.
Fault Distance		✓	A numeric value indicating where the fault is located. The protective relay calculates this value and provides it to the MCP device in the fault message.
Source Point ID	✓		The identification number of the point.
Source Point Reference	✓		A short, ASCII text identifier for the source point.
Source Point Description	✓		A user-defined, localized, description of the source point.
Point Type	✓		The type of point associated with the event (single or double point).
Event Value	✓		Value of the state (1 = ON, 0 = OFF)
Event Date	✓	✓	Date and time of the event as reported by the device or application.
Archived Date	✓		The date and time when the event was recorded in the system database.
Originator	✓		The source of the control command. See Originators for more information.
Quality	✓		The quality flag associated with the record.
State Description	✓		Text description of the state (ON = 1, OFF = 0)
Home Directory	✓	✓	System location of the device/application.
Line ID	✓	✓	Electrical transmission line associated with the device of this event.

Device ID	✓	✓	Device associated with this event.
Bay ID	✓	✓	Name of the bay associated with this event.
Device Type	✓	✓	Name of the client map file used with the specific device.

Connections

Communications Summary

The **Communications Summary** page lists the most recent communication statistics between the MCP and configured device or master station connections.

The following related actions can be performed:
View device communications
View master station communications
View pseudo points (detailed communication statistics
Enable/Disable device communications

IED Communications Summary

The **IED Communications Summary** displays the status of configured devices in the system. The display includes:

Table 3.19: IED Communication Summary

Point Name	Description
Home Dir	System location of the device/application.
Line ID	Electrical transmission line associated with the device.
Device ID	Description of the device.
Bay ID	Description of the substation bay.
Device Type	Name of the client map file used with the specific device.
IED Details	Protocol address of the device (i.e. DNP device address, IP Address, or serial port number, etc.).
Total Transactions	Total number of failed and successful transactions
Total Transaction Failures	Total number of failed transactions
Percentage efficiency	Communications efficiency of the data link calculated from **{1 - (Total Transaction Failures / Total Transactions)} x 100%** Total Transactions and Total Transaction Failures information is refreshed each second.

The following related actions can be performed:
View I/O
View pseudo points (detailed communication statistics)
Enable/disable device communications

Master Station Communications Summary

The **Master Station Communications Summary** displays the status of configured master stations in the system. The display includes:

Table 3.20: Master Station Communication Summary

Field	Description
Home Dir	System location of the device/application.
Map File	Name of the server map file used with the specific master.
Master Station Name	Description of the master station.
Details	Protocol address of the device (i.e. DNP device address, IP Address, or serial port number).
Total Transactions	Total number of failed and successful transactions
Total Transaction Failures	Total number of failed transactions
Percentage efficiency	Communications efficiency of the data link calculated from **{1 - (Total Transaction Failures / Total Transactions)} x 100%** NOTE Total Transactions and Total Transaction Failures information is refreshed each second.

The following related actions can be performed:
View I/O
View pseudo points (detailed communication statistics)

Detailed Communication Statistics - IED

Device communications statistics and other device specific information are supplied as pseudo point values in the real-time database.

» To view pseudo points:

- Click the Display button on the IED Communications Summary page.

  The **IED Detailed Statistics** window opens. The pseudo points vary according to the type of device and protocol configured.

Standard Pseudo Points

The following standard pseudo points available for each device:

Table 3.21: Standard Pseudo Points available for each device

Pseudo Point Name	Description
DCA Status	Set (1) if client application running (Digital input)
Device Disable	State follows state of **Disable Device** point (Digital input). See **Disable Device** below.
Device Online	Set (1) if client application is collecting data from the device (Digital input)
Primary Port Status	Set (1) if Primary port is in use (Digital input)
Backup Port Status	Set (1) if backup port is in use. Set to 0 if not configured (Digital input)
Msg Sent	Number of messages sent to device on either the Primary or backup channel (Accumulator).
Msg Received	Number of messages received from device on either the Primary or backup channel (Accumulator).
Msg Time Outs	Number of messages that did not receive acknowledgement from device on either the Primary or backup channel (Accumulator).
Msg Error	Number of failed transactions on either the Primary or backup channels due to an explicit rejection message from the device or transport layer. In other words, transactions that failed for any reason other than a timeout. Examples include a negative acknowledgement or a TCP connection refusal. MsgError plus MsgTimeOuts is equal to the Total Transaction Failures for the device.
Update Count	Number of points updated in the real-time database (Accumulator)

Operations Requested	Number of commands received from the RTDB (Accumulator)
Operations Failed	Number of commands rejected (Accumulator)
Send Time Sync	Pulse ON (1) to send a time synchronization request to the device.
Disable Device	Latched ON (1) if polling disabled. Latched OFF (0) if normal polling enabled. (Digital output)
Send Restart	Initiates restart/initialization sequence with the device.

NOTE Communications statistics update at a configured interval to display the most current values.

Detailed communication statistics – Master Station

Host communications statistics and other host specific information are supplied as pseudo point values in the real-time database.

» To view pseudo points:

- Click the Display button on the Master Communications Summary page.

  The **Master Station Detailed Statistics** window opens. The pseudo points vary according to the type of host and protocol configured.

Standard Pseudo Points

The following standard pseudo points available for each host:

Table 3.22: Standard Pseudo Points available for each host

Pseudo Point Name	Description
Master Add	Protocol address of the master station.
DPA Process ID	Linux Process id of the Network Server process on the MCP that communicates with the master station.
DPA Status	Set (1) if server application running (Digital input)
Primary Port Status	Set (1) if Primary port is in use (Digital input)
Backup Port Status	Set (1) if backup port is in use. Set to 0 if not configured (Digital input)
Master Msg In	Number of messages received from master station (Accumulator)
Master Msg Out	Number of messages sent to master station (Accumulator)
Remote Msg Ack Time Outs	Number of messages that did not receive acknowledgement from master station (Accumulator)
Rem Operations Requested	Number of commands received from the RTDB (Accumulator)
Rem Operations Failed	Number of commands rejected (Accumulator)
BI Change Events Out	Number of events acknowledged by the master station.
Force Controls Lockout	Latched ON (1) if controls request from master station are being rejected. Latched OFF (0) if controls requests are being accepted and sent to target device. (Digital output)

NOTE Communications statistics update at a configured interval to display the most current values.

Enable/Disable Device Communications

On the **IED Communication Summary** display, click **Enable/Disable** to resume/suspend communications between the MCP and a selected device for scheduled polling and control operations.

NOTE You must have Operator or Supervisor privileges to use the Enable/Disable communications function.

I/O Traffic Viewer

The **I/O Traffic Viewer** lists real-time communication messages between the MCP and a selected device or master station. The display automatically scrolls and refreshes as new messages are exchanged.

» To view I/O:

- Click the View button on the IED/Master Station Communications Summary page or the Monitor button on the Point Summary page or Detailed Statistics window.

  The **I/O Traffic Viewer** window opens. Each message includes the following information:

  - Direction of message flow (incoming or outgoing)
  - Date and time of message
  - Message content in ASCII or HEX text (as configured)
  - Message type

On this screen, you can:

- Show/Hide Info Messages
- Pause/Resume the display of messages
- Clear all messages from the buffer
- Change the buffer size

When I/O communication messages exceed the buffer size, the oldest message is removed to make room for the new message. The default buffer size for the screen text area is 32 KB.

» To change the buffer size:

1. In the I/O Traffic Viewer window, click Buffer Size.
2. Enter a value and click **OK**.
   Result: The buffer size is changed as you specified.

Tip: You can copy and paste text from the message window using your browser's copy and paste functions (e.g., **Ctrl**-**C** to copy and **Ctrl**-**V** to paste).

Logs

The **Logs** also known as **System Logs** page provides a report utility to display a list of system activities maintained by the MCP and stored in the real-time database. The logs are useful for troubleshooting and tracking purposes. The following reports are available:

- Control Log
- Diagnostic Log
- System Event Log
- User Activity Log
- Analog Report Log
- VPN Server Log (Available only to Administrator class users/roles)

⚠CAUTION SYSLOG-based event logging (i.e., System Event Log, Diagnostic Log, Control Log and User Activity Log) should not be used for real time and Mission Critical purposes. Data presented in the SYSLOG may not be updated in real time to correctly indicate the status of monitored and controlled equipment.

For example, a power line could be listed as inactive in a system log, while in fact the power line is active and its status in the system log may be updated significantly later in terms of real time applications.

Only use SYSLOG-based event logging for system management, security auditing, general informational and debugging messages.

The following related actions can be performed:
View a log
Clear a log

Control Log

The **Control Log** lists command requests initiated by the master station or MCP and MCP responses. The following types of command events are logged:

- Analog set points
- Digital controls
- Forcing of data values (from HMI or master station)
- Forcing of data quality flags (from HMI or master station)
- Addition/removal of information tag

The log can support 8192 records.

The following related actions can be performed:
Sort records
Clear records (Supervisor only)

Diagnostic Log

The **Diagnostic Log** lists application specific error messages. The following types of events are logged:

- Loss/recovery of device or master station communications
- Switching between Primary and Backup serial channels
- Communication errors
- Internal errors (for example, unable to connect, read/write errors)
- Data errors originating in device (for example, invalid date from protective relay)

The log can support 16384 records.

The following related actions can be performed:
Sort records
Clear records (Supervisor only)

System Event Log

The **System Event Log** lists time-stamped system events. The following types of system events are logged:

- Application restarts
- Application failure to start errors
- Watchdog timer-based application restarts
- Buffer overflows
- Failure to log to SOE (sequence of event)
- Failure to log alarms
- Forcing of data values (from HMI or master station)
- Forcing of data quality flags (from HMI or master station)
- Addition/removal of information tag

- Loss/recovery of time sync
- Loss of events
- Corrupt configuration

The log can support 32768 log records.

The following related actions can be performed:
Sort records
Clear a log

User Activity Log

The **User Activity Log** contains event records relating to user interaction with the MCP. The following pieces of information may be included in each log entry:

- Application Type
- Date/Time
- User Name
- Source IP Address
- Source Subnet Address
- Privilege Level
- User Text

You may see entries like the following in the user log: *(pam_unix) session opened for user root by (uid=0)*
(pam_unix) session closed for user root

These entries, denoted by the *pam_unix* prefix, are caused by the internal operation of the MCP security system and can be disregarded. They do not indicate that someone has logged into the MCP using the root account.

The following related actions can be performed:
Sort records
Clear records (Supervisor only)

Analog Report Log

The **Analog Report Log** lists time-stamped analog report events. The following types of analog report events are logged:

- New report is generated
- Report is automatically deleted by the Analog Report application
- Report has been manually deleted by a user
- Reports(s) has been downloaded by a user
- Downloading report failed
- Deleting report failed

The following related actions can be performed:
Sort records
Clear a log

VPN Server Log

The MCP HMI provides support for the VPN Server Log; this log is only available to Administrator Users. This Log is accessed through the System Logs button and can be used for diagnostic purposes.

This log is also available to Administrator or Root Users through the MCP command prompt using command:

sudo tail -f /mnt/datalog/Logs/openvpn.log

View a Log

The **System Logs** page provides a search utility to filter, sort and display system logs records.

» To view a log:

1. Click the **System Logs** button on the Power Bar.
2. Click the tab for the log to be viewed.
3. Sort the logs using the drop-down menus at the top of the screen (e.g., **Home directory**).
4. Click the **Refresh Filters** button to include entries created since the window has been opened

Tip: You can copy and paste text from the report window using your browser's copy and paste functions (e.g., Ctrl-C to copy and Ctrl-V to paste) or **export the data in a *.csv format.**

NOTE: In Local HMI, the logs (.csv files) must be exported to **/home/hmi/logs** or into the USB mounted on the MCP.

The following related actions can be performed:
Sort records
Clear a log

Clear a log

You may need to clear a log if the buffer has reached the maximum number of records. Login with Administrator credentials via sudo mcpcfg or MCP settings and clear the system logs.

» To clear a log:

1. Select a log from the **System Logs** page.
2. Click **Clear Log** and click **OK** to confirm deletion.

All log entries are deleted from the system database.

System Log Records

Control Log

Table 3.23: Control Log

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Message ID</td><td>Message ID is a unique identifier for the Control Log messages.
<table>
<tr><th>Message ID</th><th>Message description</th></tr>
<tr><td>1</td><td>Set point operation</td></tr>
<tr><td>2</td><td>Control operation</td></tr>
<tr><td>3</td><td>Counter operation</td></tr>
<tr><td>4</td><td>Local command operation</td></tr>
<tr><td>5</td><td>Invalid command</td></tr>
</table></td></tr>
<tr><td>Date</td><td>Date and time (to millisecond) when the command was created.</td></tr>
<tr><td>Command Type</td><td>Consists of one of the following Command Types:
Set Point
Control
Counter
Local Command - Consists of one of the following types.
Force Value
Force Quality
Force Value and Quality
Unforce
Scan Inhibit
Resume Scan
Output Inhibit
Permit Output
Alarm Inhibit
Permit Alarm
Apply Tag
Remove Tag
Invalid
Invalid</td></tr>
<tr><td>Operation Type</td><td>Each Command Type (except Local Command) consists of one of the following Operation types:
Select
Operate
Select Before Operate
Direct Operate
Direct Operate No Ack
Freeze
Clear
Freeze and Clear
No Operation
Invalid</td></tr>
</table>

Field	Description
Control Type	Control Type (Digital Control only) consists of one of the following types: • Trip • Close • Pulse On • Pulse Off • Latch On • Latch Off • Invalid
Set Point Value (Analog Output Commands only)	Requested Value in the AO command.
On Time	On Time period (in milliseconds) for the Digital Controls.
Off Time	Off Time period (in milliseconds) for the Digital Controls.
Count	Repeat Count value for the Digital Controls.
Input Direction	Direction of the Command which consists of: • Consumer writes the command to RTDB. • Producer reads command from RTDB. • Producer sends the command response to RTDB.
Status	Status of the command.
Global ID	A unique identifier generated by the RTDB for each command except for the command with the operation type "Operate". In the case of "Operate", the identifier is the previous command identifier used for "Select".
Home Directory	Home Directory of the device/application.
Point ID	A 32-bit signed integer for the point that is unique within a home directory.
Point Reference	User defined point reference (ASCII string) of the point.
Originator	The source of the command. If the command originates from the remote HMI, this is the ID of the Secession.
User Description	An optional ASCII text field into which the user has entered additional information.

System Event Log

Table 3.24: System Event Log

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Message ID</td><td>Message ID is a unique identifier for the System Event Log messages.
<table>
<tr><th>Message ID</th><th>Enumeration</th><th>Description</th></tr>
<tr><td>1</td><td>APPL_STARTS</td><td>MsgText_Application_Starts</td></tr>
<tr><td>2</td><td>APPL_RESTARTS</td><td>MsgText_Application_Restarts</td></tr>
<tr><td>3</td><td>CHILD_STARTS</td><td>MsgText_Child_Starts</td></tr>
<tr><td>4</td><td>CHILD_RESTARTS</td><td>MsgText_Child_Restarts</td></tr>
<tr><td>5</td><td>CHILD_TERMINATES</td><td>MsgText_Child_Terminates</td></tr>
<tr><td>6</td><td>WATCHDOG_TIMER_APPL_RESTARTS</td><td>MsgText_WatchDog_Timer_Appl_Restarts</td></tr>
<tr><td>7</td><td>APPL_FAILUE_TO_START_ERROR</td><td>MsgText_Application_Failed_to_Start_Error</td></tr>
<tr><td>8</td><td>BUFFER_OVERFLOW</td><td>MsgText_Buffer_Overflows_DPA_Or_DTA</td></tr>
<tr><td>9</td><td>FAIL_TO_LOG_SOE</td><td>MsgText_Failure_to_Log_SOE</td></tr>
<tr><td>10</td><td>FAIL_TO_LOG_ALARMS</td><td>MsgText_Failure_to_Log_Alarms</td></tr>
</table></td></tr>
</table>

	11	FORCING_DATA_VALUES	MsgText_Forcing_of_Data_Values_HMI_Or_Master_Station
	12	FORCING_DATA_FLAGS	MsgText_Forcing_Data_Quality_Flags
	13	APPLY_INFORMATION_TAG	MsgText_Apply_Information_on_Tag
	14	REMOVE_INFORMATION_TAG	MsgText_Removal_Information_on_Tag
	15	LOSS_OF_TIMESYNC	MsgText_Loss_of_Time_Sync
	16	RECOVERY_OF_TIMESYNC	MsgText_Recovery_of_Time_Sync
	17	DST_MISMATCH	DST_Flag_Mismatch_Between_Time_Recieved_From_IED_and_Zoneinfo_File
	18	LOSS_OF_EVENTS	MsgText_Loss_of_Events_DCA_Or_DTA
	19	INCORRECT_CONFIGURATION	MsgText_Incorrect_Configuration
	20	XML_PARSE_ERROR	MsgText_XML_Parse_Error
	21	MCP_START_ACTIVE_MODE	Msg_Text_Gateway_Started_in_Active_Mode
	22	MCP _SWITCH_TO_STANDBY_MODE	Msg_Text_Gateway_switching_to_Standby_Mode
	23	MCP _CONFIG_SYNC_SUCCESS	Msg_Text_Gateway_configuration_sync_to_Standby_Success
	24	MCP _CONFIG_SYNC_FAILED	Msg_Text_Gateway_configuration_sync_to_Standby_Failed
	25	MCP _RX_HB_FROM_STANDBY	Msg_Text_Received_HB_from_Standby
	26	MCP _SENT_RESTART_ALL_APPS	Msg_Text_Sent_message_to_SWWatchdog_to_restart_all_Apps
	27	MCP _SENT_STOP_ALL_APPS	Msg_Text_Sent_message_to_SWWatchdog_to_stop_all_Apps
	28	DAEMONIZE_FAILED	Msg_Text_Daemonize_call_failed
	29	MCP _FAIL	Msg_Text_Failing_Gateway
	30	MCP_START_NONREDUNDANT_MODE	Msg_Text_Gateway_started_in_Non_Redundant_Mode
	31	MCP _START_STANDBY_MODE	Msg_Text_Gateway_started_in_Standby_Mode
	32	MCP _SWITCH_TO_ACTIVE_MODE	Msg_Text_Gateway_Switching_to_Active_Mode
	33	MCP_RTDB_CONSUMER_DELAY_START	Msg_Text_Consumer_started_late_may_miss_events
	33	MCP_RTDB_CONSUMER_DELAY_START	Msg_Text_Consumer_started_late_may_miss_events
	34	RECEIVED_RESTART	MsgText_Received_Restart_IIN
	35	RECEIVED_NEED_CONFIG	MsgText_Received_Need_Config_IIN
	36	MCP_FAILED	MsgText_Gateway_Failed
	37	MCP_RESTART_ALL_APPS	MsgText_Gateway_restart_all_applications
	38	CRITICAL_APPL_FAILED	MsgText_Critical_Application_Failed
	39	MCP_KILL_APPL	MsgText_Kill_Application
	40	PERCENTAGE_APPL_FAILED	MsgText_Percentage_applications_Failed
	41	EMERGENCY_ACCESS_CODE_CLEARED	MsgText_Emergency_Access_Code_has_been_cleared
	42	EMERGENCY_ACCESS_CODE_CLEAR_FAIL	MsgText_Emergency_Access_Code_failed_to_be_clear
	43	EMERGENCY_ACCESS_CODE_GEN	MsgText_Emergency_Access_Code_has_been_generated
	44	EMERGENCY_ACCESS_CODE_GEN_FAIL	MsgText_Emergency_Access_Code_failed_to_be_generate
	45	EMERGENCY_ACCESS_CODE_AUTHENTICATED	MsgText_Emergency_Access_Code_has_been_authenticated
	46	EMERGENCY_ACCESS_CODE_AUTH_FAIL	MsgText_Emergency_Access_Code_has_failed_authentication

	47	EMERGENCY_ACCESS_CODE_EXPIRED	MsgText_Emergency_Access_Code_has_expired
	48	RECIEVED_SIGNAL	MsgText_Recieved_signal
	49	MAX_RESTARTS	MsgText_Max_restarts_for_terminal_server
	50	MISSED_MAX_HEART_BEATS	MsgText_Missed_max_heart beats_for_terminal_server
	51	RESTART_MAIN_CONTROLLER	MsgText_Restarting_main_controller_Too_many_broken_threads
	52	NO_SERVERS_FOUND	MsgText_No_servers_found
	53	DATALOG_INFO_MSG	MsgText_DataLogger_Info_Message
	54	DATALOG_ERR_MSG	MsgText_DataLogger_Error_Message
	55	CONNECT_TCP_MSG	MsgText_TCP_Connect_Message
	56	DISCONNECT_TCP_MSG	MsgText_TCP_Disconnect_Message
	57	RESET_TCP_SERVER_MSG	MsgText_Resetting_TCP_Server_Message
	58	TCP_SERVER_ERR_MSG	MsgText_TCP_Server_Unknown_Error_Message
	59	PAM_START_ERR_MSG	MsgText_Failed_to_fork_authentication_child_process_Message
	60	VALID_APP_LICENCE_MSG	MsgText_Valid_application_license_Message
	61	INVALID_APP_LICENCE_MSG	MsgText_Invalid_application_license_Message
	62	LICENCE_NOT_FOUND_MSG	MsgText_Application_license_not_found
	63	APP_LICENCE_ADDDED_MSG	MsgText_Application_license_added
	64	APP_LICENCE_ADD_FAIL_MSG	MsgText_Couldnot_add_new_application_ID
	65	APPL_LICENCE_NOT_FOUND_MSG	MsgText_Application_license_not_found_in_license_file
	66	TRIAL_LICENCE_NOT_ENABLED_MSG	MsgText_Trial_License_not_enabled
	67	TRIAL_LICENCE_ENABLED_MSG	MsgText_Trial_license_already_enabled
	68	TRIAL_LICENCE_EXPIRED_MSG	MsgText_Trial_license_already_expired
	69	NO_APPL_LICENCE_MSG	MsgText_Application_License_does_not_exist
	70	UNABLE_TO_CONNECT_TO_AMPLSOLVER_MSG	MsgText_Unable_to_connect_to_amplsolver
	71	RESTORE_CLONE_SNAPSHOT_SUCCESSFUL	MsgText_Restore_Clone_Snapshot_Successful
	72	RESTORE_CLONE_SNAPSHOT_FAIL	MsgText_Restore_Clone_Snapshot_Failed
	73	RESTORE_STANDARD_SNAPSHOT_SUCCESSFUL	MsgText_Restore_Standard_Snapshot_Successful
	74	RESTORE_STANDARD_SNAPSHOT_FAIL	MsgText_Restore_Standard_Snapshot_Failed
	75	FIRMWARE_UPGRADE_SUCCESSFUL	MsgText_Firmware_Upgrade_Successful
	76	FIRMWARE_UPGRADE_FAIL	MsgText_Firmware_Upgrade_Failed
	77	UPGRADE_RUNTIME_DATA_SUCCESSFUL	MsgText_Upgrade_Runtime_Data_Successful
	78	UPGRADE_RUNTIME_DATA_FAIL	MsgText_Upgrade_Runtime_Data_Failed
	79	SCHEMA_VERSION_CHECK_SUCCESSFUL	MsgText_Schema_Version_Check_Successful
	80	SCHEMA_VERSION_CHECK_FAIL	MsgText_Schema_Version_Check_Failed
	81	FIRMWARE_VERSION_CHECK_SUCCESSFUL	
	82	FIRMWARE_VERSION_CHECK_FAIL	MsgText_Firmware_Version_Check_Failed
	83	INVALID_SYSLOG_MESSAGE_ID	MsgText_Invalid_SysLog_Message_ID
Event Date	Date and time (to millisecond) when the event was created.		

Message Class	Type of message.
Description	Brief description of the event. Some of the most commonly used messages are: • CHILD Started • CHILD Re-started • Application Started • Application Re-started etc.
Application	Unique identification number for the application.
Connection Type	Connection or Communication type of the application instance.
Home Directory	Home directory of the device/application.
Instance	The execution instance of the application starting with the number one.
Misc	This is an optional ASCII text of size 512 bytes for the user to log additional information.

Diagnostic Log

Table 3.25: Diagnostic Log

Field	Description
Message ID	System assigned number to identify the message.
Message Class	Type of the message.
Date	Date and time (to millisecond) when the event was created.
Description	Brief description of the event.
Application	Unique Identification number of the application.
Application Interface	The execution instance of the application.
Home Directory	Home Directory of the device/application.
User Action	This is optional text for additional user-logged information.

User Activity Log

Table 3.26: User Activity Log

Field	Description
Application Type	
Date	Date and time (to millisecond) when the event was created.
Username	ASCII name of the user who issued the command.
IP Address	IP Address of the remote user.
Subnet IP	Subnet IP of the remote user.
Description	Brief description of the event.
Privilege Level	Privilege level of the user.

Analog Report Log

Table 3.27: Analog Report Log

Field	Description
Message ID	System assigned number to identify the message.
Date	Date and time (to millisecond) when the event was created.
Message Class	Type of message.
Description	Brief description of the event.
File	Name of the file to be created or deleted.
Username	Optional text to be added for user-logged information.
User Action	Optional text to be added for user-logged information.

The following related actions can be performed:
Sort records
View a log

Trends

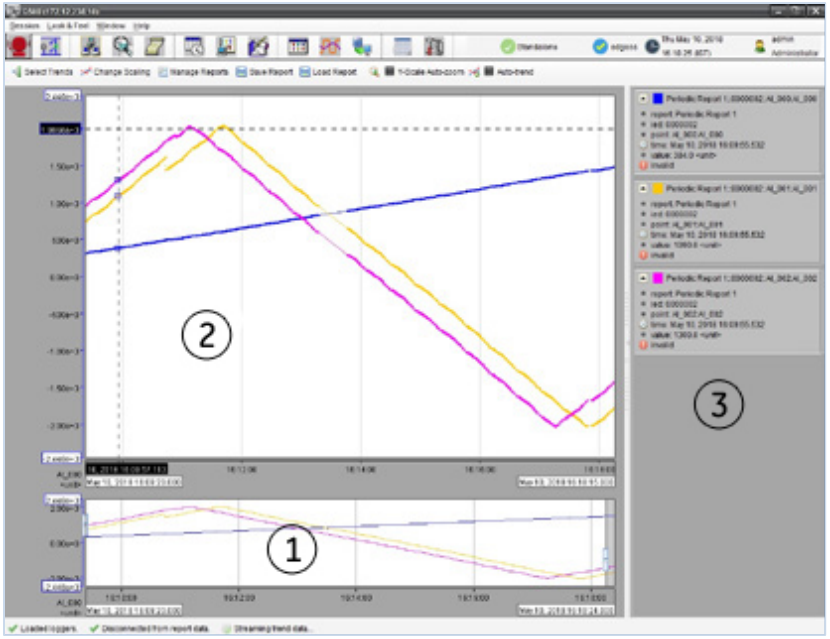
The Trending also known as Data Logger application allows you to graphically monitor and record data from devices connected to the MCP. You can also save and review historical reports created by the application.

Using the Trends

When the Trends is opened, click the **Select Points** button to choose the points to be graphed. Up to 10 points can appear at one time.

Screen Areas

The Trends window is comprised of several areas.



Screen Area	Description
1. Summary Area	The summary area shows the entire timeframe of all selected points. You can use the left and right sliding markers to zoom a portion of this timeframe within the viewing area. Click and drag the area between the markers to re-position the timeframe.
2. Viewing Area	The viewing area is a larger graph detailing the selected portion of the summary area. When you click the graph, crosshairs are shown pinpointing the date and value. The closest points are highlighted, and their attributes are shown in the point detail pane. Click and drag to highlight a portion of the viewing area to launch a popup detail window showing the selected area.
3. Point Detail Pane	The point detail pane shows detailed attributes for the points selected in the viewing area.

Options

Y-Scale Auto-zoom

When selected, the Y-axis scale of the Viewing Area automatically expands and contracts to fit the largest visible deviation. This setting does not affect the scale of the Summary Area.

Auto-trend

When selected, the viewing area always shifts to show the latest information received. For this option to be available, enable **No End Date** in the **Select Points** window.

Execute Commands

This chapter contains the following sections:

Issue a Command

Acknowledge an Alarm (One-Line Viewer)

Acknowledge an Alarm Group (One-Line Viewer)

Analog Output Interface

Analog Set-point Interface

Digital Control Interface

Digital Output Interface

Navigate to Active Alarm Page (One-Line Viewer)

Point Forcing Interface

DataSource Types

Raise/Lower Control Interface

Tag/Inhibit Interface

Global Controls Disable

Control Lockout Feature

Issue a Command

The MCP supports the following control operations:

- Repeated control operations in quick succession (window remains open until cancelled)
- Separate Select and Operate commands
- For IEDs that do not support Trip/Close commands to the same point, the Trip command can be sent to one digital output point and the Close command can be sent to another digital output point.
- Specification of control command attributes at runtime

You can execute a command on a data point from the **Point Details** page or the **One-Line Viewer**.

» To issue a command:

1. Select an item.

   In One-Line Viewer, the Digital Output interface can be opened on any of the following three ways:

   - Double click
   - Left click and then select Digital Output Interface
   - Right click and then select Digital Output Interface

   In Point Details, the Digital Output interface can be opened in either of the following ways:

   - Double click and then select the Digital Output Interface
   - Right click and then select Digital Output Interface
2. Select a command option.
3. In the command interface window, enter the desired command settings:

This command is only applicable to the command interface window on the viewpoint details page.

Set up one control command as follows:

a. Select Function Code.

   One of: Direct Operate, Direct Operate with No ACK, Select, Operate, Select Before Operate

b. Select Control Code.

   One of Pulse On, Pulse Off, Latch On, Latch Off, Trip, Close

c. Enter a Pulse On time.

   Trip/Close and Pulse On/Off controls only

d. Enter a Pulse Off time.

   Trip/Close and Pulse On/Off controls only

The above options do not show at run time when using objects within the one-line screens.

4. Click **Execute** or **OK** to send the command request.

A message confirms whether the command was successful.

In a distributed system, the only reliable way to determine the success of a control operation is through a hardwired digital input or analog input point providing the feedback of the process state being controlled. The popup window that indicates when a control has been sent only indicates that the MCP has sent the control to a downstream device.

If you do not complete an action within a pre-defined period, the operation is cancelled and the window closes.

Acknowledge an Alarm (One-Line Viewer)

If an alarm panel has been configured in a one-line diagram, you can manually acknowledge alarms directly in the **One-Line Viewer**. Alarm panel is configured using the **One-Line Designer**.

» To acknowledge an alarm object:

1. Go to the **One-Line Viewer** and open the alarm panel drawing.
2. Select the object that is in alarm and click. The Acknowledge Alarm window opens.

   NOTE: Alarm panel objects can be configured for acknowledgement using a single or double-click.

3. Click **OK** to confirm the acknowledgement.
4. Click **OK** to confirm the completion of the command.

When you acknowledge an alarm object:

- "Acknowledge Indicator" field is checked on the Active Alarms page.
- Acknowledged alarm object changes in foreground color, background color and blink rate as configured in alarm settings.

  NOTE: You cannot remove an acknowledgement once an alarm has been acknowledged.

Acknowledge an Alarm Group (One-Line Viewer)

If an alarm panel has been configured on an Alarm group in a one-line diagram, you can manually acknowledge the alarm Group (all the alarms at once within the configured Alarm group) directly in the **One-Line Viewer**. Alarm panel is configured using the **One-Line Designer**.

» To acknowledge an alarm object configured on Alarm Group

1. Go to the **One-Line Viewer** and open the alarm panel drawing.
2. Select the object that is in alarm (the alarm object is in alarm mode when any point in the group is in alarm state) and click. The Acknowledge Alarm window opens.

   NOTE: Alarm panel objects can be configured for acknowledgement using a single or double-click.

3. Click **OK** to confirm the acknowledgement.
4. Click **OK** to confirm the completion of the command.

When you acknowledge an alarm object:

- "Acknowledge Indicator" field is checked on the Active Alarms page.
- Acknowledged alarm object changes in foreground color, background color and blink rate as configured in alarm settings.

  NOTE: You cannot remove an acknowledgement once an alarm has been acknowledged.

Analog Output Interface

The **Analog Output Interface** allows you to execute a set point command on an analog output point.

» To open the Analog Output Interface:

- Right-click an analog output data object on the **One-Line Viewer** *or* an analog output point on the **Point Details** page and select **Analog Output Interface**.

The **Analog Output Interface** displays the following information:

- Line ID/Device ID
- Point description

- Point value
- Quality Attributes

The quality status is visually indicated according to configured color settings.

» To execute a set point:

1. Right-click an analog output data object on the **One-Line Viewer** *or* analog output point on the **Point Detail** page and select **Analog Output Interface**.
2. Enter a Set Point Value.
3. Select the Function Code.
4. Click **Execute** to send the request.
   Result: A message confirms whether the command was successful.

NOTE If you do not complete an action within a pre-defined period of time, the operation is cancelled and the window closes.

Analog Set-point Interface

The **Analog Set Point Interface** allows you to view point status and execute a set point command on an analog set point object's output point.

» To open the Analog Set Point Interface:

- Right-click an analog set point data object on the **One-Line Viewer** and select **Analog Set Point Interface**.

The **Analog Set Point Interface** displays the following information:

- IED/Point descriptor
- Quality Attributes
- Feedback point value (engineering units)

The quality status of the feedback point value and Quality attribute are visually indicated according to configured color settings.

» To execute a set point command:

1. Right-click an analog output data object on the **One-Line Viewer** and select **Analog Set Point Interface**.
2. Enter a **Set Point Value** within the shown configured range of values.
3. Click **Execute** to send the request.
   Result: A message confirms whether the command was successful.

NOTE If you do not complete an action within a pre-defined period, the operation is cancelled and the window closes.

Digital Control Interface

The **Digital Control Interface** supports multiple datasources. Each datasource allows you to viewpoint status and execute a control command on a digital control object's output point. Two-state and four-state feedback controls are supported.

» To open the Digital Control Interface:

- Right-click a digital control data object on the **One-Line Viewer** and select **Digital Control Interface**.

The **Digital Control Interface** displays the following information:

- IED/Point descriptor (Secondary output point as well, if configured)
- Quality attributes

- Present state: **Open** or **Closed** for 2-state feedback controls *or* **Open**, **Closed**, **In Transi**t or **Invalid** for 4-state feedback controls

The quality status of the state and Quality attribute are visually indicated according to configured color settings.

» To execute a control command:

1. Right-click a digital control data object on the **One-Line Viewer** and select **Digital Control Interface**.
   Result: The Digital Control Interface window appears.
2. Select a datasource.
3. Verify the point status.
4. Click the **On** or **Off** control state button.
   Result: The selected state button displays in green.
5. Click **Execute** to send the request.
   Result: A message confirms whether the command was successful.

NOTE If you do not complete an action within a pre-defined period, the operation is cancelled and the window closes.

Digital Output Interface

The **Digital Output Interface** allows you to issue control requests on digital output points.

» To open the Digital Output Interface:

- Right-click a digital output data object on the **One-Line Viewer** *or* a digital output point on the **Point Details** page and select **Digital Output Interface**.
  Result: The **Digital Output Interface** displays the following information:
  - Line ID/Device ID
  - Point description
  - Quality Attributes
  - Digital output state

The quality status of the Point value and Quality attribute are visually indicated according to configured color settings.

» To execute a control command on a digital output point:

1. Right-click a digital output data object on the **One-Line Viewer** *or* a digital output point on the **Point Details** page and select **Digital Output Interface**.
2. Verify the point status.
3. Set up one control command as follows:
   - Select **Function Code**. One of Direct Operate, Direct Operate with No ACK, Select, Operate, Select Before Operate
   - Select **Control Code**. One of Pulse On, Pulse Off, Latch On, Latch Off, Trip, Close
   - Enter a **Pulse On** time (Trip/Close and Pulse On/Off controls only)
   - Enter a **Pulse Off** time (Trip/Close and Pulse On/Off controls only)
4. Click **Execute** to send the request.
   Result: A message confirms whether the command was successful.

NOTE In a distributed system, the only reliable way to determine the success of a control operation is through a hardwired digital input or analog input point providing the feedback for the process state being controlled. The popup window that indicates when a control has been sent only indicates that the MCP has sent the control to a downstream device.

NOTE If you do not complete an action within a pre-defined period, the operation is cancelled and the window closes.

How Inputs to the Digital Output Interface are Used by DCAs

Inputs to the Digital Output Interface of the MCP HMI and One-Line Viewer (OLV) are utilized by the following DCA applications:

Table 3.28: DCA Applications

	Function Code	Control Code	Pulse On Duration	Pulse Off Duration	Number of Pulses	Notes
IEC 61850 DCA	Don't Care	Any	Send as a part of control object	Send as a part of control object	Send as a part of control object	The function provided by the user is not considered. The function code depends on the control model of the point configured at the Server.
Modbus DCA	Don't Care	Trip Pulse Off Latch Off	Don't Care	Don't Care	Don't Care	Modbus DCA sends an OFF command to the IED. Modbus protocol doesn't support control code, Pulse on/off duration and number of pulses.
	Don't Care	Close Pulse On Latch On	Don't Care	Don't Care	Don't Care	Modbus DCA sends an OFF command to the IED. Modbus protocol doesn't support control code, Pulse on/off duration and number of pulses.
DNP DCA	Don't Care	Any	Send as a part of control object	Send as a part of control object	Send as a part of control object	The function code and control specifications specified by the user are considered.
	Direct Operate		Send as a part of control object	Send as a part of control object	Send as a part of control object	The function code specified by the user is overridden by the "Direct Operate" and sent to the IED. Control specification parameters specified by the user are considered.
	Direct Operate with No Ack	Any	Send as a part of control object	Send as a part of control object	Send as a part of control object	The function code specified by the user is over-written by the "Direct Operate No Ack" and sent to the IED. Control specification parameters specified by the user are considered.
	SBO	Any	Send as a part of control object	Send as a part of control object	Send as a part of control object	The function code specified by the user is over-written by the "SBO" and sent to the IED. Control specification parameters specified by the user are considered.
IEC 101/104 DCA	Direct Operate		Send as a part of control object	Send as a part of control object	Send as a part of control object	The function code specified by the user is over-written by the "Direct Operate" and sent to the IED. Control specification parameters specified by the user are considered.
	SBO	Any	Send as a part of control object	Send as a part of control object	Send as a part of control object	The function code specified by the user is over-written by the "SBO" and sent to the IED. Control specification parameters specified by the user are considered.
IEC 103 DCA	Don't Care	Any	Send as a part of control object	Send as a part of control object	Send as a part of control object	The function code and control specifications specified by the user are considered.
SEL Binary DCA	Don't Care	Any	Send as a part of control object	Send as a part of control object	Send as a part of control object	The function code and control specifications specified by the user are considered.

Navigate to Active Alarm Page (One-Line Viewer)

If an alarm panel has been configured in a one-line diagram, you can navigate to Active Alarms page directly from the **One-Line Viewer**. Alarm panel is configured using the **One-Line Designer**.

1. Go to the **One-Line Viewer** and open the alarm panel drawing.
2. Select the alarm object and click. It navigates to the Active Alarm page.
   NOTE: Alarm panel objects can be configured for navigation using a single or double-click.
3. If navigation is invoked on alarm object configured on group of points, it navigates to the active alarm page with the respective group tab selected.
4. If navigation is invoked on alarm object configured on a point, it navigates to the active alarm page.

Point Forcing Interface

The **Point Forcing Interface** allows you to view the point status and manually enter (force) the value of any type of data point.

» To open the Point Forcing Interface:

1. Click a data object on the **One-Line Viewer** *or* a point on the **Point Details** page.
2. Select **Point Forcing Interface**.
   Result: The following options may appear:
   - Feedback
   - Control

The **Point Forcing Interface > Feedback** window shows the following information:

- DataSource
- Status
- Value(s)
- Tag(s)
- DataSource Status/Control for the Quality attributes

The **Point Forcing Interface > Control** window shows the following information:

- Line ID/Device ID
- Data type
- Point name
- Point value
- Quality attributes

NOTES:

- Values are in engineering units for Analog Input and Analog Output points.
- The quality status of the Point value and Quality attribute are visually indicated according to configured color settings.

» To force a value on the One-Line Viewer page:

1. Click an object on the One-Line Viewer drawing.
2. Select **Point Forcing Interface**
3. Select **Feedback** or **Control**.
   Result: The DataSource Feedback Force or the DataSource Control Feedback Force window appears.

» To force a value on the Point Details page:

1. Right-click a point on the **Point Details** page.
2. Select **Point Forcing Interface**.
   Result: The Point Status window appears.
3. Verify the point quality status in the **Point Status Control** pane.

4. Click a Point Status button to force a value. Click the button again to toggle the state.
   Result: A message confirms whether the force action was successful or not.
5. Click **Close**.
   Result: The Point Status window closes.

DataSource Types

The following table summarizes the functionality associated with each DataSource type.

Table 3.29: DataSource Types

DS type	Control 1	Control 2	Feedback	Feedback Value	Control
Accumulator Status			1ACC	Any integer>=0	NA
Alarm				Alarm Group – NA Individual Alarm - NA	NA
Analog Set Point	1AO		1AI	Feedback AI: any float value	AO - between min and max
Analog Status			1AI	Feedback AI: any float value	NA
Digital Control	1DO	1DO	2DI	Set 2/4 state depending on the Primary feedback Secondary feedback DI Point: State 00/01/10/11 Text	Primary/Secondary DO State (defined for open/close state desc): 0 or 1
Digital Status			2DI	Set 2/4 state depending on the Primary & Secondary DI Point: State 00/01/10/11 Text	NA
Raise/Lower Control	1DO	1DO	1AI	AI Feedback: any float value	Primary/Secondary DO Point State (defined for open/close state desc : 0 or 1
TEXT			1TXT	NA	NA

DataSource Feedback Force – Window Elements

Force Feedback is only applicable to Analog Output and Digital Output points which are configured as feedback points in the DataSource. A typical use case: Force Feedback can change a 2 Feedback State (00/01) point or a 4 Feedback State (00/01/10/11) point in one operation by changing multiple feedback points' values in one command.

The table below describes the fields and controls on the window for the following datasource types used in Point Forcing Interface > Feedback:

- Digital Control
- Analog Status
- Raise/Lower Control
- Analog Set Point
- Digital Status
- Accumulator Status

Table 3.30: Window Elements - DataSource Feedback

Element	Description
Datasource	The Datasource assigned to the Data Source Value in the One-Line Designer.
Status	Indicates the Data Quality Status.
Value	Indicates the current value for the Datasource. The **Force Value** button can be used to force the value to one of the following, depending on the Datasource type: • **Digital Control:** Force 2 States depending on the Primary IED point value. The valid states and the corresponding text are: o When the point feedback value is 00, the text appears as Off (default) o When the point feedback value is 01, the text appears as On (default) Force 4 States depending on the Primary and Secondary IED point states. The valid states and the corresponding text are: o When the point feedback value is 00, the text appears as Opened (default) o When the point feedback value is 01, the text appears as In Transit (default) o When the point feedback value is 10, the text appears as Closed (default) o When the point feedback value is 11, the text appears as Invalid (default) • **Analog Status:** Force the Analog Input point value. Enter a floating-point number. • Raise/Lower Control: Force the Analog Input point value. Enter a floating-point number. • **Analog Set Point:** Force the Analog Input point value. Enter a floating-point number. • **Digital Status:** Force 2 States depending on the Primary Feedback Point 00/01(default text is Off and On); Force 4 States depending on the Primary and Secondary Digital Input Feedback point: state. Valid states are: 00/01/10/11 (default text strings are In Transit, Open, Closed and Invalid) • Digital Status: Force 2 States depending on the Primary IED point value. The valid states and the corresponding text are: o When the point feedback value is 00, the text appears as Off (default) o When the point feedback value is 01, the text appears as On (default) Force 4 States depending on the Primary and Secondary IED point states. The valid states and the corresponding text are: o When the point feedback value is 00, the text appears as Opened (default) o When the point feedback value is 01, the text appears as In Transit (default) o When the point feedback value is 10, the text appears as Closed (default) o When the point feedback value is 11, the text appears as Invalid (default) • **Accumulator Status:** Force the Accumulator point value to the entered positive number
Tag(s)	Indicates the current Tag status. See for Tag/inhibit interface further information.
Datasource Status/Control	Indicates the status of the Quality attributes, including the state of any current control actions.

DataSource Control Force – Window Elements

Force Control is only applicable to Analog Output and Digital Output points which are configured as Primary point and Secondary points in the DataSource. The point values can be changed by manual force, depending upon the datasource type.

The table below describes the fields and controls on the window for the following datasource types used in Point Forcing Interface > Control:

- Digital Control
- Raise/Lower Control
- Analog Set Point

Table 3.31: Window Elements - DataSource Control

Element	Description
Datasource	The Datasource assigned to the Data Source Value in the One-Line Designer.
Status	Indicates the Data Quality Status.
Primary Point	Indicates the Primary point name which is providing the Datasource.
Primary Point Value	Indicates the current value for the Datasource. The **Force Value** button can be used to force the value to one of the following, depending on the Datasource type: • **Digital Control:** Force Primary or Secondary Digital Input point state. Select 0 or 1. • **Raise/Lower Control:** Force the Primary or Secondary Digital Output point state. Select 0 or 1. • **Analog Set Point:** Force the Analog Output point value. The valid range is determined by the min to max values specified in the Analog Set Point Datasource.
Secondary Point	Indicates the Secondary point name which is providing the Datasource.
Secondary Point Value	See the description for the Primary Point Value.
Tag(s)	Indicates the current Tag status. See for Tag/inhibit interface further information.
Datasource Status/Control	Indicates the status of the Quality attributes, including the state of any current control actions.

Raise/Lower Control Interface

The **Raise Lower Control Interface** allows you to viewpoint status and execute a raise or lower command on a raise/lower control object's output point. Raise/Lower control is available on configured buttons and transformer objects.

» To open the Raise Lower Control Interface:

- Right-click a raise/lower data object on the **One-Line Viewer** and select **Raise/Lower Control Interface**.

The **Raise Lower Control Interface** displays the following information:

- IED/Point descriptor (Secondary output point as well, if configured)
- Quality Attributes
- Analog Feedback point description and value (engineering units)
- Present state

The quality status of the Point value and Quality attribute are visually indicated according to configured color settings.

» To execute a raise/lower control command:

1. Right-click a raise/lower control data object on the **One-Line Viewer** and select **Raise/Lower Control Interface**.
2. Verify the point status.
3. Click the **Raise** or **Lower** control state button.
4. **NOTE:** The selected state button displays in green.
5. Click **Execute** to send the request.

A message confirms whether the command was successful.

If you do not complete an action within a pre-defined period, the operation is cancelled and the window closes.

Tag/Inhibit Interface

The **Tag/Inhibit Interface** allows you to view the point status and tag or inhibit the value of any type of data point. The MCP supports tagging on the following data types:

- Analog inputs
- Digital inputs
- Accumulators
- Analog outputs
- Digital outputs

» To open the Tag/Inhibit Interface:

1. Right-click a data object on the **One-Line Viewer** *or* right-click a point on the **Point Details** page.
2. Select **Point Forcing Interface**.
   Result: The Point Status window appears.

   The **Point Status** window displays the following information:

   - Line ID/Device ID
   - Data type
   - Point Reference
   - Point value
   - Point quality
   - Point name
   - Quality attributes

NOTES:

- Values are in engineering units for Analog Input and Analog Output points.
- The quality status of the Point value and Quality attribute are visually indicated according to configured color settings

Example Actions

» To add a tag (text label) to a One-Line Viewer diagram:

1. With the Point Status window open, click the **Tagged (T)** button.
   Result: The Tag window appears.
2. Type in the desired text for the tag label.
3. Click **OK**.
   Result: The Tag window closes.
   Result: The tag text appears in the Tag field and as a tooltip for the elements in the One-Line Viewer.

» To inhibit an action:

- With the Point Status window, open, click either the **Scan Inhibit (S)** button and/or the **Alarm Inhibit (A)** button.
  Result: The Old Data (OD) button automatically becomes active when the Scan Inhibit (S) button is clicked.

  Result: The corresponding flag letters S, A and OD appear in the Point Summary, Point Groups table > Quality Attributes column, and in the One Line diagram.

Global Controls Disable

The MCP provides a **Global Controls Disable** feature that allows an operator to prevent all control commands from being executed.

Specifically, when the Global Controls Disable point is turned ON, a lock out is placed on all digital output commands. This means all control requests are rejected and digital output points are prevented from operating until the Global Controls Disable point is turned OFF. When an output command is rejected, a message appears to the operator that the command was rejected due to the "Global Control Lockout".

The Global Controls Disable point is a pseudo point owned by the System Status Manager. The Global Controls Disable point name and location is configured under the RTDB configuration options.

» To execute a Global Control, Disable command:

1. Go to the System Status Manager Point Details page.
2. On the Digital Output tab, right-click the DisableAllControls point and select Digital Output Interface. The Digital Control window displays.
3. Verify the Point Value. A value of 0 indicates the point is currently OFF.
4. Under Function Code, select Direct Operate.
5. Under Control Code, select Latch On.
   NOTE: Pulse On and Close control commands can also be used, if supported by your protocol.
6. Click Execute to send the request.
   Result: A message confirms whether the command was successful.

If you do not complete an action within a pre-defined period, the operation is cancelled and the window closes.

Control Lockout Feature

The Control Lockout feature of the System Point Manager allows you to ensure that only a single master station can access a group of controls at one time, and can lock out groups of controls to allow for safer local maintenance. You can create up to 8 remote control groups and up to 1000 local control groups. Any digital output (except for those owned by the System Point Manager application) can be included in one remote and one local group.

⚠WARNING	**The MCP Control Lockout feature is not a replacement or equivalent of LOTO (Lockout – Tagout). Use standard safety procedures to implement Lockout - Tagout and to perform maintenance operations.**

Operator Notes

This chapter contains the following sections:

Operator Notes

Operator Notes Log - Note records

Add a Note

Edit a Note

Operator Notes Log

Operator Notes

The **Operator Notes** page lists all the operator notes that have been entered by users and stored in the MCP database.

Operator Notes Log - Note records

Each note record displays the following information:

Table 3.32: Operator Notes

Button	Description
Note Number	Automatically assigned number to identify the note.
Sequence Number	Sequence Number to identify the original note or comments added to the note. Sequence Number 0 indicates the original note and greater than 0 indicates the comment(s) added to the original note.
Operator Name	MCP HMI username of the note author (original or commented).
Date Modified	Date and time that the note or comment was created.
Notes	Free-form text entered by the note author.

Only a super user (root) can delete operator notes and operator notes log using mcpcfg configuration utility. Use **Option 9. Reset Database Tables > 4. Delete Operator Note records** from mcpcfg configuration utility to delete operator notes. This is the same as for all other entries (SOE, Alarm etc.).

If you type a PLUS (+) sign into an Operator Note, it appears as a blank space.

The following related actions can be performed from the GUI:

Add a Note
Edit a Note
Operator Notes Log

Add a Note

You enter a note from the **Operator Notes** page.

» To add a note:

1. Click

or press **[Ctrl]-n**.
Result: The Operator's Notes window appears.
2. Enter your note text into the **Operator's Notes** box. Text can be up to 256 characters.
3. Click **OK** to save the note.
Result: The note is saved and added to the list of notes in chronological order.

Edit a Note

You edit a note from the **Operator Notes** page.

» To edit a note:

1. Double-click a note row.
Result: The Operator Notes window appears.
2. Edit your note.

   NOTE: An existing note can be updated by adding a new comment, but the initial note cannot be modified. This behavior is like paper-based operator logbooks. New Text and comment can be up to 256 characters, but the total size of the original note and all the comments for a note cannot exceed 2048 characters.

3. Click **OK** to save the note.
Result: The new comment for the note is saved.

Operator Notes Log

The MCP copies a mirror file of the Operator Note entries from the mSQL database into a file called "operator_notes.log", located under /mnt/datalog/Logs. This file is updated automatically every time the Operator Notes is updated in the mSQL database. This file can be used by the MCP Sync Manager to synchronize with higher level Enterprise systems.

The content of this file is in human readable format, delimited with "|" and with the times converted to the Local Time Zone that is configured in the MCP.

The format of the file content is:

Note Number | Operator Name | Date Created | Date Modified | Operator Note /Comment(s)

The Operator note comment(s) added to the note are separated by a semi colon ";".

Example of the file content:

1|supervisor|2015-05-26 13:16:57.936 MDT|2015-05-26 13:16:57.936 MDT |This Note is created by Supervisor.

2|operator_abc2015-05-27 05:18:23.111 MDT|2015-05-27 05:18:23.111 MDT |This is an Operator ABC.

2|operator_abc|2015-05-27 05:18:23.111 MDT2015-05-28 13:16:57.936 MDT |This is an Operator ABC; Added a new Comment.

NOTE: While typing in the operator log note, if you press the:

- PLUS (**+**) key, a blank space appears in the operator notes log file.
- **Enter** key, "&&" appears in the operator notes log file.
- Single quote (') key, "~~" appears in the operator notes log file

Chapter 4 - MCP Local Configuration Utility (mcpcfg)

This chapter provides settings instructions to users of **MCP Local Configuration Utility (*"mcpcfg"*)**.

This interface is the Shell based equivalent of the *Chapter 5 - MCP Settings GUI*.

Date and Time
- Select Time Source
- Configure Time Output
- Timestamps and Time Zones on MCP
- Time Sync Settings and Runtime Functionality
- PTP Use Case Scenarios

Networking
- Network Modes
- Substation LAN IED Types
- Network Configuration
- Network LAN Scenarios
- Subnet Overlapping Rules
- Custom Routing
- Network Summary

User Management
- Default Users
- User Management Overview
- Configure User HMI Home Page
- Auto Login

Other Services/Settings
- Configure Remote HMI Non-Observer Privileges
- Configure Rsyslog service
- Configure Secure Access
- Configure Firewall
- Configure host names
- Configure Time & Time Sync
- Reset system logs
- Reset Database tables
- Reset file persistence data
- Local HMI
- Configure sync manager
- Redundancy
- ARRM - Automatic Record Retrieval Manager

Suppress forced qualities to masters
Emulate D20 RTU IEC101 DPA Unbalanced Mode Functionality
Configure IEC101+104 DPA Startup Quality Event Suppress Interval
Configure Serial Port Modes (RS-232/485)
EdgeOS Host Access
Configure D.20 Port Hardware Settings
EdgeOS Host
Clear Chassis Intrusion State
Restore Clone Snapshot
Restore factory default
Reboot device

Introduction

The MCP Gateway Local Configuration Utility (mcpcfg) is used to configure system level settings on the MCP. To launch **mcpcfg** from the MCP command line the user must type "**sudo mcpcfg**" and the user password when prompted.

"sudo" is a key cyber-security feature that strengthens the non-repudiation and protects from the attacks from of malware that will try to execute privileged operations while user is are logged in under their account.

Typing **"sudo"** in front of functions in the MCP command line will prompt for the user's password before executing the command. Failing to use **"sudo"** will prevent the command from executing.

Using the Gateway Local Configuration Utility, User can perform the following actions:

1. Configure Authentication
2. Configure Network Settings
3. Configure Network Interfaces
4. Configure Secure Access
5. Configure Firewall
6. Configure Host Names
7. Configure Time & Time Sync
8. Reset System Logs
9. Reset Database Tables
10. Reset File Persistence Data
11. Local HMI
12. Configure Sync Manager
13. Redundancy (not available in G100)
14. ARRM
15. Suppress Forced Qualities To Masters
16. Emulate D20 RTU IEC101 DPA Unbalanced Mode Functionality
17. Configure IEC101+104 DPA Startup Quality Event Suppress Interval
18. Configure Serial Ports
19. Configure D.20 Port Settings
20. EdgeOS Host
21. Clear Chassis Intrusion State

22. Restore Clone Snapshot
23. Restore Factory Default
24. Reboot Device

General Note: for consistency within the MCP family, the mcpcfg menu options in are kept the same between G100 and G500 and in same order but will return "functionality not available" when accessing a non available option in G100. This allows users to use same scripted actions on both G100 and G500 common settings.

Date and Time

The **Configure Time & Time Sync** menu allows you set the MCP's internal date and time as well as modify options associated with time synchronization. The Time and Time synchronization settings are described below.

Settings		Description
Show Time and Current Settings	:	Use this function to display the time, time zone, and synchronization settings currently configured.
Set System Clock	:	Use this function to configure the current calendar date and time of day. **Note**: The MCP system time is automatically set to the firmware build time whenever the MCP reboots and the system time is less than the firmware build time.
Set System Time Zone	:	Use this function to configure the desired time zone.
Select Time Source	:	Use this function to select and configure the time synchronization source (PTP, IRIG-B or NTP). More details are described below.
Configure Time Output	:	Use this function to configure the time synchronization output. More details are described below.

NOTE: Whenever system time goes back after time sync, the clock on Task Bar in local HMI will stop updating till the updated time reaches back the time before time sync.

Please refer to section ***UEFI Settings***

The G100 and G500 have different UEFI settings, described in the documents below, for each product model:

- *Configuring UEFI Settings on G100 User Guide (SWM0122)*
- *Configuring UEFI Settings on G500 User Guide (SWM0110)*

NOTICE

G100 device has the following UEFI settings that will revert to default values after the internal super capacitor has been discharged due to the device being powered off for extended time (typically more than 5 days).

These UEFI settings are applicable only while the G100 is starting.

After the applications started, these settings are over-written by the values configured in *MCP Local Configuration Utility (mcpcfg)* or *MCP Settings GUI*.

- Default Serial Maintenance Port used as UEFI (boot) console when KVM is not available (Advanced->Serial Port Console Redirection)

  - Console Redirection is set to Disabled for COM1-COM3, please do not change these settings.
  - Console Redirection for COM4 should be enabled/disabled and have the "Bits per second", to be same as in *the Serial Maintenance Port in MCP Studio (See* Serial Maintenance Port *on page 443)*.
- Default Serial Ports Modes (Advanced->Super IO Configuration)
  - Please ensure are enabled/disabled as required for secure hardening purposes and set to RS-232.

Users should check again these UEFI settings when the G100 is powered on again, and adjust as necessary.

MCP Time Synchronization for time sources (IN) and signals (OUT) available options and combinations.

Select Time Source

Step 1: Connect to MCP and login using a user with Administrator privileges.

Step 2: Execute the command "**mcpcfg**" to launch the configuration Menu.

```
================================================================
        Gateway Settings Menu
================================================================

        0.   Back
        1.   Configure Authentication
        2.   Configure Network Settings
        3.   Configure Network Interfaces
        4.   Configure Secure Access
        5.   Configure Firewall
        6.   Configure Host Names
        7.   Configure Time & Time Sync
        8.   Reset System Logs
        9.   Reset Database Tables
        10.  Reset File Persistence Data
        11.  Local HMI
        12.  Configure Sync Manager
        13.  Redundancy
        14.  ARRM
        15.  Suppress Forced Qualities To Masters
        16.  Emulate D20 RTU IEC101 DPA Unbalanced Mode Functionality
        17.  Configure IEC101+104 DPA Startup Quality Event Suppress Interval
        18.  Configure Serial Ports
        19.  Configure D.20 Port Settings
        20.  EdgeOS Host
        21.  Clear Chassis Intrusion State
        22.  Restore Clone Snapshot
        23.  Restore Factory Default
        24.  Reboot Device

Enter Your Choice : ( Between 0 and 24 ):
```

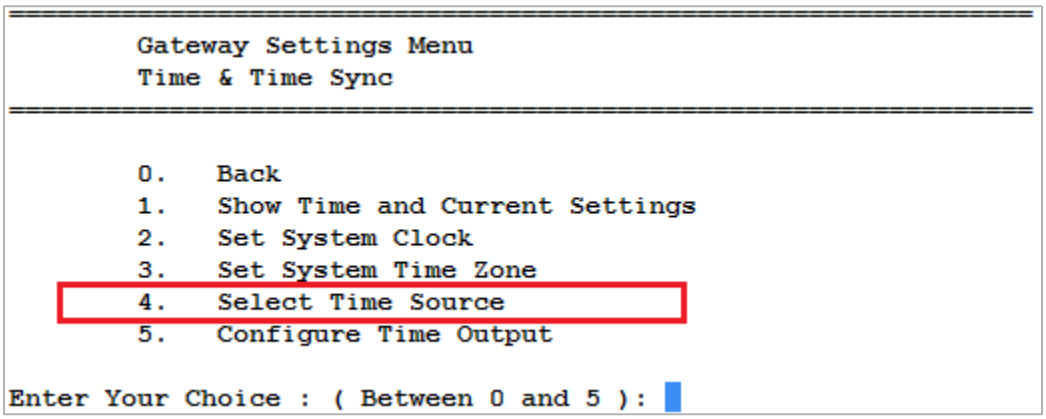
Step 3: Select option **7** → **Configure Time &Time Sync**.

```
================================================================
        Gateway Settings Menu
================================================================

         0.   Back
         1.   Configure Authentication
         2.   Configure Network Settings
         3.   Configure Network Interfaces
         4.   Configure Secure Access
         5.   Configure Firewall
         6.   Configure Host Names
         7.   Configure Time & Time Sync
         8.   Reset System Logs
         9.   Reset Database Tables
         10.  Reset File Persistence Data
         11.  Local HMI
         12.  Configure Sync Manager
         13.  Redundancy
         14.  ARRM
         15.  Suppress Forced Qualities To Masters
         16.  Emulate D20 RTU IEC101 DPA Unbalanced Mode Functionality
         17.  Configure IEC101+104 DPA Startup Quality Event Suppress Interval
         18.  Configure Serial Ports
         19.  Configure D.20 Port Settings
         20.  EdgeOS Host
         21.  Clear Chassis Intrusion State
         22.  Restore Clone Snapshot
         23.  Restore Factory Default
         24.  Reboot Device

Enter Your Choice : ( Between 0 and 24 ):
```

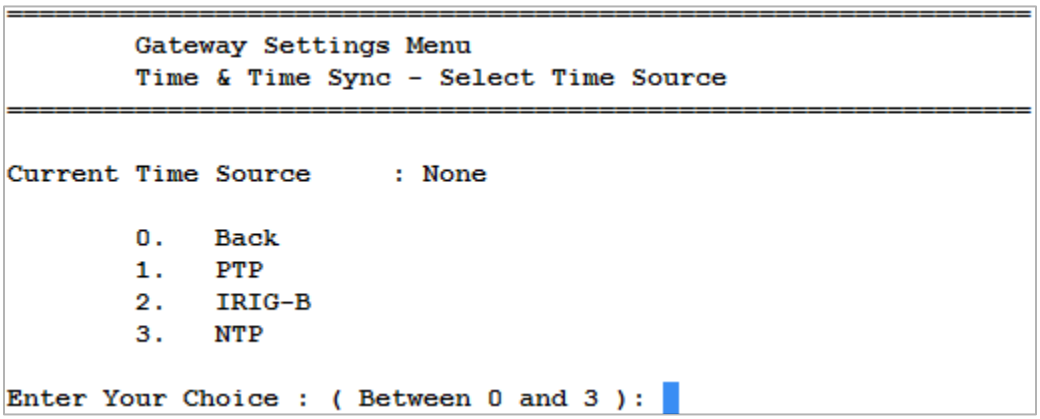
Step 4: The following screen will be launched on selection Option **7**.

```
================================================================
        Gateway Settings Menu
        Time & Time Sync
================================================================

        0.   Back
        1.   Show Time and Current Settings
        2.   Set System Clock
        3.   Set System Time Zone
        4.   Select Time Source
        5.   Configure Time Output

Enter Your Choice : ( Between 0 and 5 ):
```

Step 5: In the **Time & Time Sync** Menu, select option **4** → "**Select Time Source**"



Then the following "**Time & Time Sync – Select Time Source**" screen will be launched:



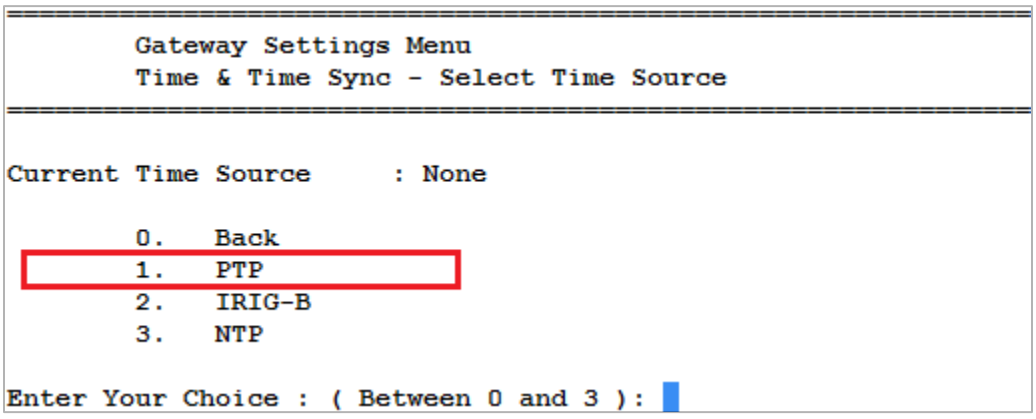
This menu displays a list of time sources which the user can configure and enable/disable. More details about each time sync mechanism are described below.

Configure PTP IN (not available in G100)

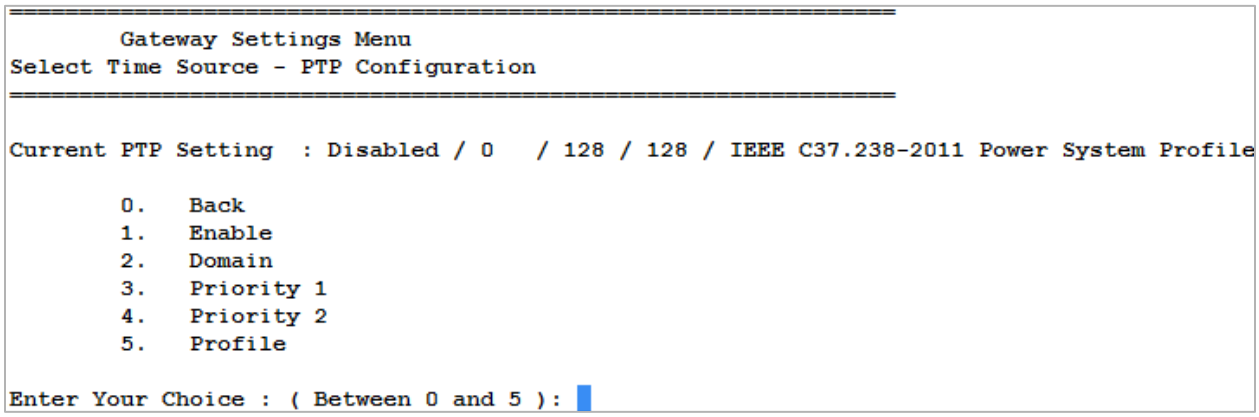
G100 does not support PTP.

Configures the G500 to use PTP to calibrate the system clock.

Step 1: In the "**Time & Time Sync - Select Time Source**" menu, select option **1→PTP:**



The following screen will be launched:



Use this menu to enable or disable the PTP time source. Also, this menu displays a list of PTP configuration parameters which the user can configure based on their PTP Network Design.

NOTE In G500, there are three PTP ports, which are NET1-2, NET3-4, NET5-6 respectively. If PTP input is enabled, all three PTP ports will be in listening mode at startup and then one port will go into slave mode if a valid master clock is present on the PTP port.

NOTE PTP functionality is not available on the front G500 Maintenance port.

NOTE To configure/enable the PTP output, PTP Input must be enabled first.

Step 2: The user can disable/enable PTP input and change the PTP parameters by selecting the individual options as the following table shows:

Option	Name	Description
1	Enable/Disable	Enable or Disable the PTP input. Default Value: 0 (disabled)
2	Domain	A logical grouping of clocks that synchronize to each other using the protocol, but that are not necessarily synchronized to clocks in another domain. It can be a value between 0 to 255. Default Value: 0
3	Priority 1	A user configurable designation that a clock belongs to an ordered set of clocks from which a master is selected. It can be a value between 0 to 255 Default Value: 128
4	Priority 2	A user configurable designation that provides finer grained ordering among otherwise equivalent clocks. It can be a value between 0 to 255 Default Value: 128
5	Profile	The set of allowed Precision Time Protocol (PTP) features applicable to a device. In MCP we support two PTP profiles namely:

		• IEEE 1588-2008 Default Profile (*J.4 PEER-to-PEER Default PTP profile*) • IEEE C37.238-2011 Power System Profile Default Value: IEEE C37.238-2011 Power System Profile

NOTE Default values are according to IEC61850-9-3 Ed.1 2016-05, Clause 8/Table 1.

NOTE When the PTP input is enabled and the output is disabled (i.e., slave only), Priority 1 and Priority 2 settings will be ignored.

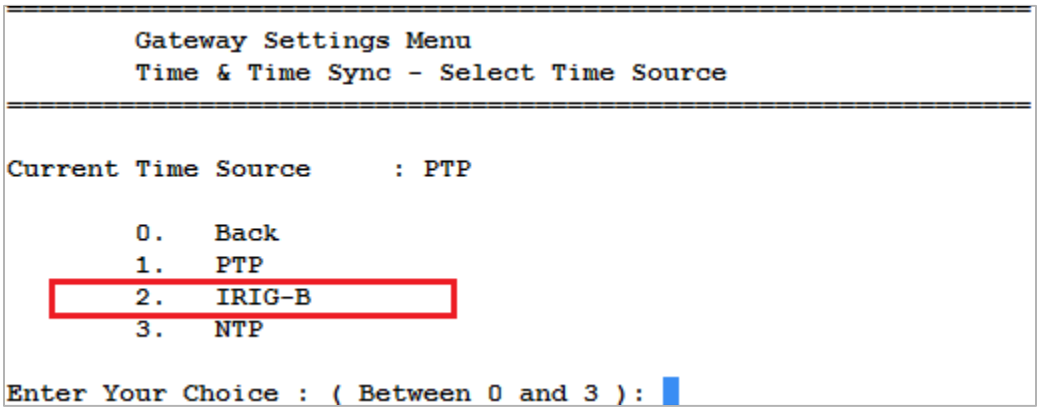
NOTE Any PTP setting changes require device reboot to take effect. This rule applies to both PTP IN and PTP OUT.

NOTE If the PTP IN is enabled, the system time will be synced to the configured and enabled PTP source only after seeing valid and good PTP signal once. Here "good" means the PTP master clock class is 6 or 7, and the UtcOffsetValid is true.

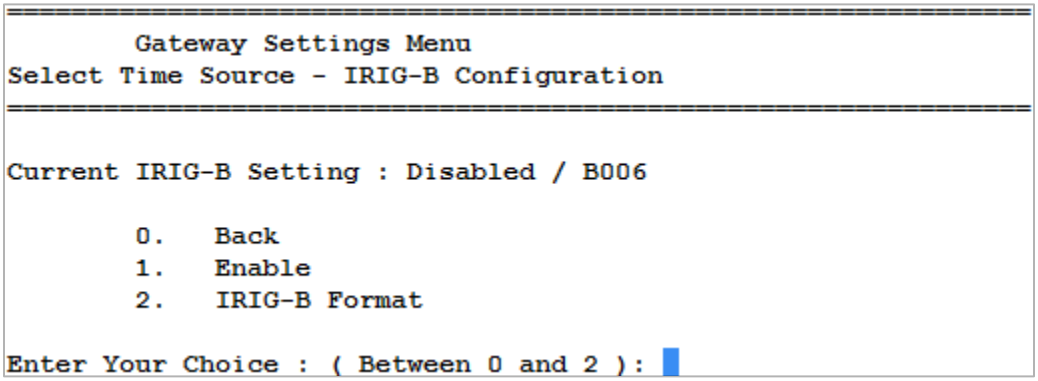
Configure IRIG-B IN

Configures the MCP to use IRIB-B as time synchronization source.

Step 1: In the "**Time & Time Sync - Select Time Source**" menu, select option **2 → IRIG-B**:



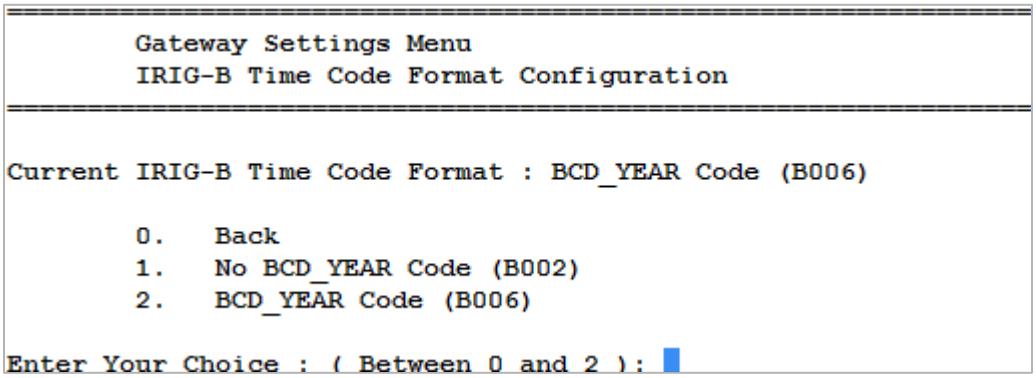
The following "**Select Time Source – IRIG-B Configuration**" screen will be launched on the selection:



Step 2: User can disable/enable IRIG-B time source and change the IRIG-B time code format by selecting the individual options.

Option	Name	Description
1	Enable/Disable	Enable or Disable the IRIG-B input. Default Value: 0 (disabled)
2	IRIG-B Format	Choose IRIG-B time code format: B002 or B006. Default Value: B006

Step 3: When user select the option **2** → **IRIG-B Format**, the "**IRIG-B Time Code Format Configuration**" screen will be launched as below:



The details about the two IRIG-B time code formats that MCP supports are as the below table presents:

Option	Name	Description
1	No BCD_YEAR Code (B002)	Binary Coded Decimal, coding of time and day of year (HH, MM, SS, and DDD); doesn't consider year.
2	BCD_YEAR Code (B006)	Binary Coded Decimal, coding of time, day of year, and year (HH, MM, SS, DDD, and YY).

NOTE Any IRIG-B setting changes require device reboot to take effect. This rule applies to both IRIG-B IN and OUT.

NOTE If IRIG-B IN is enabled, the system time will be synced to the configured and enabled IRIG-B source only after seeing valid and good IRIG-B signal once. Here "good" means:

- For B006, only when its OOSYNC is false.
- For B002, it is always treated as good.

Configure NTP IN

Configures the MCP to use NTP to calibrate the system clock (only IPv4 is supported).

Step 1: In the "**Time & Time Sync - Select Time Source**" menu, select option **3** → **NTP:**

```
================================================================================
        Gateway Settings Menu
        Time & Time Sync - Select Time Source
================================================================================

Current Time Source      : PTP

        0.    Back
        1.    PTP
        2.    IRIG-B
        3.    NTP

Enter Your Choice : ( Between 0 and 3 ):
```

The "**Select Time Source - NTP Configuration**" screen will be launched as below:

```
================================================================================
        Gateway Settings Menu
Select Time Source - NTP Configuration
================================================================================

Current NTP Setting   : Disabled / 0.0.0.0          / None

        0.    Back
        1.    Enable
        2.    Primary Server IP Address
        3.    Backup  Server IP Address

Enter Your Choice : ( Between 0 and 3 ):
```

The user can use this submenu to configure the Primary/backup NTP server IP Addresses and then enable/disable the NTP client in MCP.

Step 2: In the "**Select Time Source - NTP Configuration**" menu, select option **2** → **Primary Server IP Address** to configure the IP Address of the preferred NTP server.

Below is an example for the Primary NTP server IP Address configuration steps:

```
================================================================
        Gateway Settings Menu
Select Time Source - NTP Configuration
================================================================

Current NTP Setting  : Disabled / 0.0.0.0         / None

        0.   Back
        1.   Enable
        2.   Primary Server IP Address
        3.   Backup  Server IP Address

Enter Your Choice : ( Between 0 and 3 ): 2


Enter Primary Server IP Address[0.0.0.0]: 192.168.168.100

Do you want to save the change [Y/N]?: y


Primary Server IP address is saved.

Press ENTER Key to continue....
```

The user can select option **3** → **Backup Server IP Address** to configure the IP Address of a backup NTP Server if needed. It is the same as the Primary server IP Address configuration.

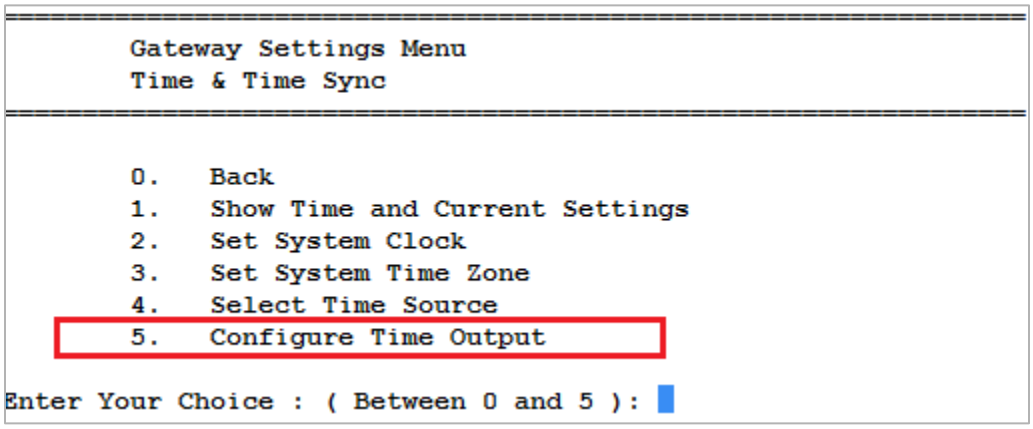
Step 3: After the NTP server(s) are configured, the user can select option **1** → **Enable/Disable** to enable or disable the NTP input in MCP. The option 1 depends on the current status of the NTP input. If it's already enabled, then the option 1 will be "**Disable**". Otherwise, it will show "**Enable**".

NOTE The Primary NTP server is the preferred server. The MCP will try to sync from this preferred server first. If not available, it will try the backup NTP server.

NOTE To change the NTP settings, it is not necessary to reboot the system. The user must re-enable NTP to put the new settings into effect. But after changing the NTP settings, it is necessary to restart the MCP to update the NTP time synchronization related HAMA points.

Configure Time Output

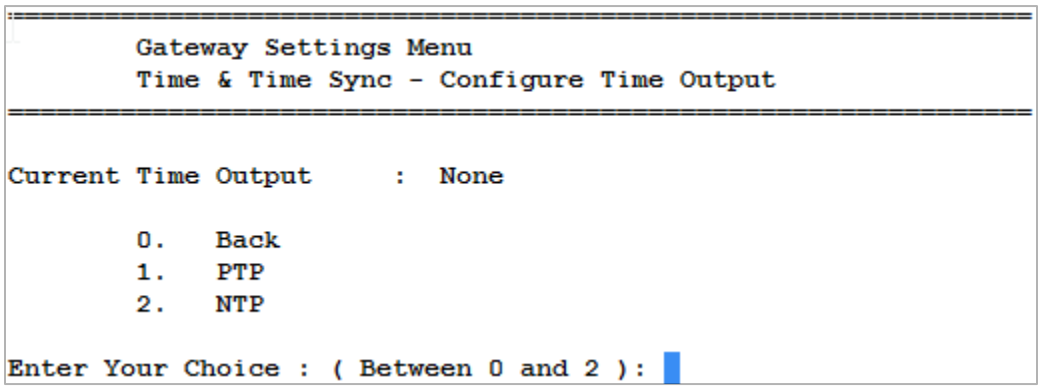
To configure the time synchronization services for time output, select the option **5 → Configure Time Output** in the "**Time & Time Sync**" menu as below:



And the "**Time & Time Sync - Configure Time Output**" screen will be launched.

NOTE

Below is an example of the "**Time & Time Sync - Configure Time Output**" screen when PTP IN is enabled:



NOTE

The PTP Output is available only when the PTP Input is configured and enabled from "**Configure Time & Time Sync - Select Time Source**" menu. And the IRIG-B Output is available only when the IRIG-B Input is configured and enabled from "**Configure Time & Time Sync - Select Time Source**" menu. NTP Output doesn't have such restriction and is available all the time.

Configure PTP OUT

The "PTP" will be available in the "**Time & Time Sync - Configure Time Output**" menu only when the PTP input is configured and enabled.

Step 1: Select option **1→ PTP** in the "**Time & Time Sync - Configure Time Output**" menu:

```
================================================================================
        Gateway Settings Menu
        Time & Time Sync - Configure Time Output
================================================================================

Current Time Output      :  None

        0.    Back
        1.    PTP
        2.    NTP

Enter Your Choice : ( Between 0 and 2 ): 1
```

And then the below "**Configure Time Output - PTP Configuration**" screen will be launched on the selection:

```
================================================================================
        Gateway Settings Menu
        Configure Time Output - PTP Configuration
================================================================================

Current PTP OUT Setting : Disabled

        0.    Back
        1.    Enable

Enter Your Choice : ( Between 0 and 1 ):
```

Step 2: Select option **1->Enable/Disable** to enable/disable the PTP Output:

```
================================================================================
        Gateway Settings Menu
        Configure Time Output - PTP Configuration
================================================================================

Current PTP OUT Setting : Disabled

        0.    Back
        1.    Enable

Enter Your Choice : ( Between 0 and 1 ): 1
```

NOTE If the Current PTP Output is disabled, option 1 in the "**Configure Time Output – PTP Configuration**" will be "Enable". Otherwise, it will be "Disable".

The PTP Output will share same settings configured in the PTP Input, such as domain, priorities and so on.

Configure IRIG-B OUT

The "IRIG-B" will be available in the "**Time & Time Sync - Configure Time Output**" menu only when the IRIG-B input is configured and enabled.

Step 1: Select option **1-> IRIG-B** in the "**Time & Time Sync - Configure Time Output**" menu:

```
================================================================================
        Gateway Settings Menu
        Time & Time Sync - Configure Time Output
================================================================================

Current Time Output      :  None

        0.    Back
        1.    IRIG-B
        2.    NTP

Enter Your Choice : ( Between 0 and 2 ): 1
```

And then the below "**Configure Time Output – IRIG-B Configuration**" screen will be launched:

```
================================================================================
        Gateway Settings Menu
Conigure Time Output - IRIG-B Configuration
================================================================================

Current IRIG-B Output Setting : Disabled /  Out When OOSYNC

        0.    Back
        1.    Enable
        2.    No Signal Out When Out Of Sync (OOSYNC)

Enter Your Choice : ( Between 0 and 2 ):
```

Step 2: Select option **1->Enable/Disable** to enable/disable the IRIG-B Output:

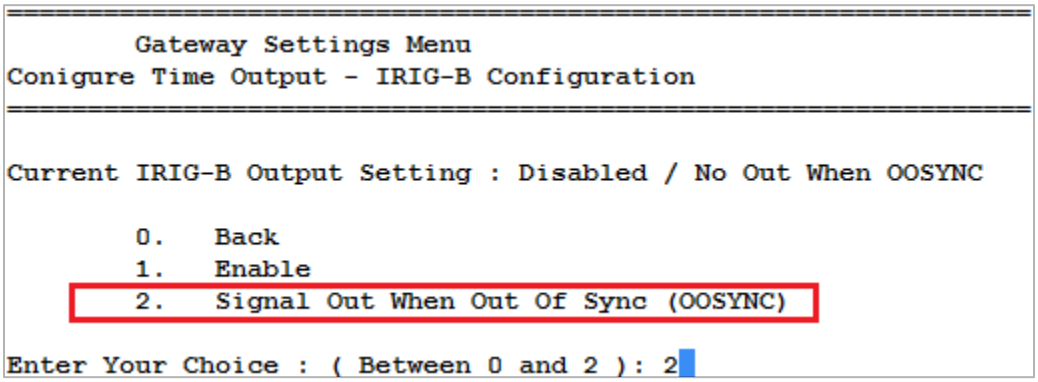
```
================================================================================
        Gateway Settings Menu
Conigure Time Output - IRIG-B Configuration
================================================================================

Current IRIG-B Output Setting : Disabled /  Out When OOSYNC

        0.    Back
        1.    Enable
        2.    No Signal Out When Out Of Sync (OOSYNC)

Enter Your Choice : ( Between 0 and 2 ): 1
```

NOTE If the Current IRIG-B Output is disabled, option 1 in the "**Configure Time Output – IRIG-B Configuration**" will be "Enable". Otherwise, it will be "Disable".

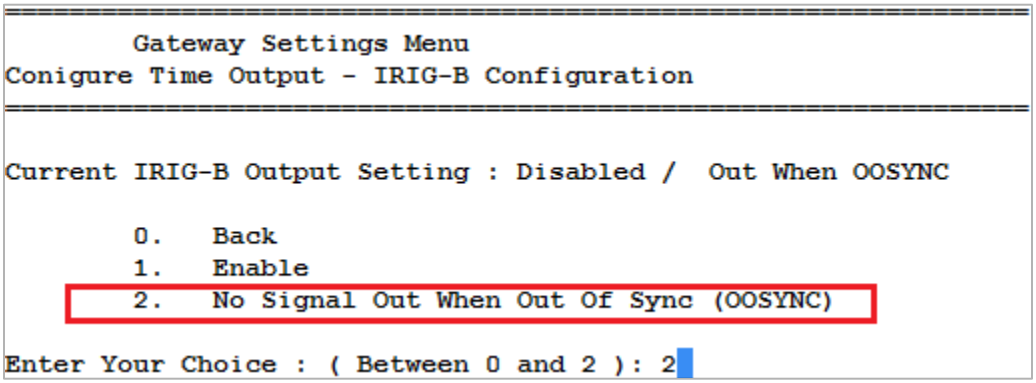
NOTE The IRIG-B output will share same IRIG-B time code format as configured in the IRIG-B Input.

Step 3: Select option **2->(No) Signal Out When Out Of Sync (OOSYNC)** to control whether to allow/suppress the IRIG-B Output when the IRIG-B Input signal is out of sync.

By default, the IRIG-B output signal is suppressed when the IRIG-B input signal is out of sync. In order to allow the IRIG-B output signal when the IRIG-B input signal is out of sync, select option **2 -> Signal Out When Out of Sync (OOSYNC)** in the "**Configure Time Output – IRIG-B Configuration**" menu:



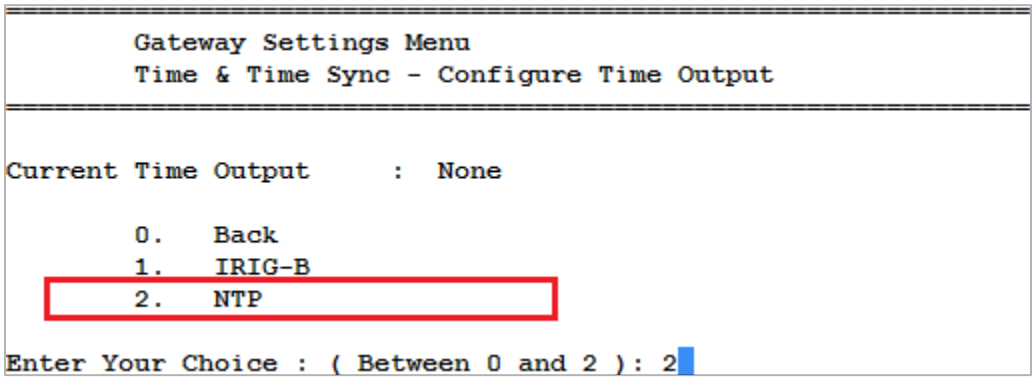
If the IRIG-B output signal is not suppressed when the IRIG-B input signal is out of sync, the user can select the option **2 -> No Signal Out Of Sync (OOSYNC)** in the "**Configure Time Output – IRIG-B Configuration**" menu to suppress it:



Configure NTP OUT

The "NTP" will be always available in the "**Time & Time Sync - Configure Time Output**" menu no matter the NTP input is enabled or not.

Step 1: Select option **2-> NTP** in the "**Time & Time Sync - Configure Time Output**" menu:



NOTE: If there is no PTP or IRIG-B input enabled, the option for NTP will be 1 as below:

```
================================================================================
        Gateway Settings Menu
        Time & Time Sync - Configure Time Output
================================================================================

Current Time Output      :  None

        0.    Back
        1.    NTP

Enter Your Choice : ( Between 0 and 1 ): 1
```

After selecting the NTP option, the below "**Configure Time Output – NTP Configuration**" screen will be launched:

```
================================================================================
        Gateway Settings Menu
Conigure Time Output - NTP Configuration
================================================================================

Current NTP Output Setting : Disabled

        0.    Back
        1.    Enable

Enter Your Choice : ( Between 0 and 1 ):
```

Step 2: Select option **1->Enable/Disable** to enable/disable the NTP Output:

```
================================================================================
        Gateway Settings Menu
Conigure Time Output - NTP Configuration
================================================================================

Current NTP Output Setting : Disabled

        0.    Back
        1.    Enable

Enter Your Choice : ( Between 0 and 1 ): 1
```

NOTE If the Current NTP output is disabled, option 1 in the "**Configure Time Output – NTP Configuration**" will be "Enable". Otherwise, it will be "Disable".

Timestamps and Time Zones on MCP

All timestamps on the MCP are stored in UTC (coordinated universal time). The below table explains how time zones are handled by various components of the MCP and how this behavior can be configured.

Component	Time zone handling	Configuration Method
MCP system clock	For all the time zone features described in this document to work properly, the MCP hardware clock must be set to UTC using the appropriate MCP UEFI setting.	Configured using the *mcpcfg* utility.
Device and master station internal clocks	Can be set to local time or UTC, as desired.	Refer to the user documentation provided with the device or master station. If the device's clock is offset from UTC, the same offset should be configured in the corresponding client map file (see below).
Time-stamped data communicated to the MCP	The timestamp is converted to UTC from the configured offset or is left unmodified if no offset is configured.	Defined by the Time Offset field in the client map files. Refer to MCP Online Help > DNP3 Client topic, IEC 60870-5-103 with MCP Master Application topic, or IEC 60870-5-101+104 with MCP Master Application topic, See notes below table).
Time-stamped data communicated from the MCP	The timestamp is converted from UTC to the configured offset or is left at UTC if no offset is configured.	Defined by the *Time Offset* field. See the MCP Online Help > DNP Server topic.
Local console (including local HMI) and command line via SSH	All time-stamped data is shown to you using the configured MCP time zone setting.	Configured using the *mcpcfg* utility. > "Set System Time Zone"
MCP Runtime HMI	All time-stamped data is shown to you using the time zone configured on the remote PC.	For more details refer to the user documentation provided with the operating system installed on the remote PC.

NOTE

The IEC 60870-5-101+104 application uses a slightly different concept for local to UTC time conversion to be consistent with the D2x product family. If the master is in a different time zone, you should set the Time Mode field to set local/use local time. When the master time synchronizes the application, the application calculates the difference between the internal MCP UTC clock and the master's time. The application then applies this difference to the UTC timestamps it reports to the master. In effect, it automatically calculates the time offset.

Example System Configuration

Table 4.1 shows an example system configuration.

Table 4.1: Sample system configuration

Remote access via Runtime HMI	Local access to command line via RS232 port	Even though the MCP device is in the local time zone of UTC -7, the MCP system clock is set to UTC time.	Local device with clock set to UTC -7	Remote client with clock set to UTC -5
PC clock is set to local time zone (**-8**)	No configuration necessary	*mcpcfg System Clock:* **UTC time** *mcpcfg Time Zone:* **-7**	DNP Client Map File *Time Offset*: **-7**†	DNP Server Application Parameters *Time Offset*: **-5**†
If an event occurs at 13:00 UTC...				
Event timestamp is displayed as **05:00**	Event timestamp is displayed as **06:00**	The MCP system database records the event timestamp as **13:00**	Local device reports the event at **06:00**	Remote client receives the event timestamp as **08:00**

NOTE †This field is configured in minutes, so the value entered in the configuration tool would be -420 and -300 respectively. However, hours are shown in Table 4.1 for clarity.

Time Sync Settings and Runtime Functionality

Current Time Sync Settings

On the Main Time Synch Menu, Option 1 → "Show Time and Current Settings" gives a summary of the Time Sync configuration.

```
================================================================
        Gateway Settings Menu
        Time & Time Sync - Current Time Sync Settings
================================================================


The current Date and Time        : Fri Feb 4,2000 22:28:05

Time Zone                        : UTC

PTP IN                           : Disabled

PTP OUT                          : Disabled

IRIG-B IN                        : Enabled

IRIG-B IN Format                 : BCD_YEAR Code (B006)

IRIG-B OUT                       : Disabled

NTP IN                           : Disabled

NTP OUT                          : Disabled

Press ENTER Key to continue....
```

NOTE: The above example is with IRIG-B B006 Input enabled and all other inputs and all outputs are disabled.

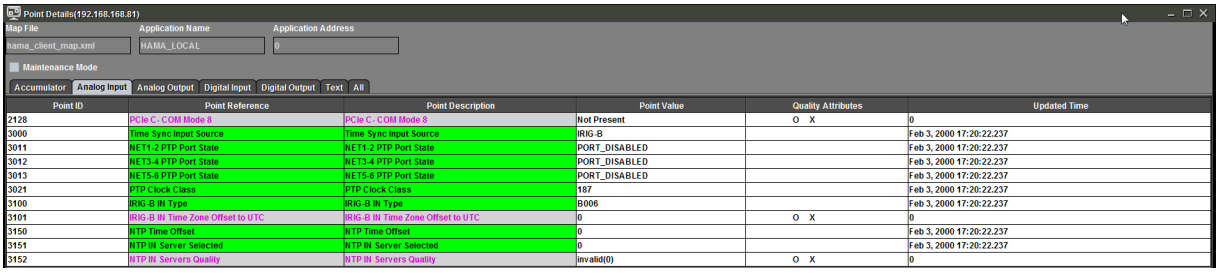
Time Sync Runtime Functionality

The runtime status of Time Sync can be viewed from the Local/ Remote HMI in

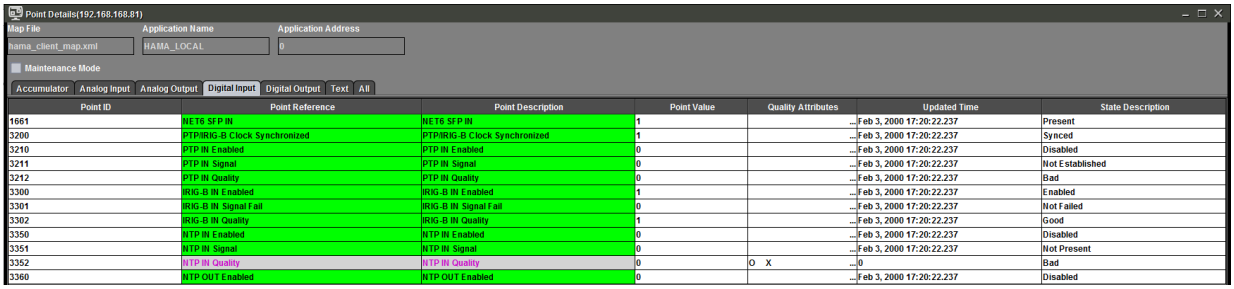
Point Details → Application → "HAMA_LOCAL"

NOTE This menu can take up to 10 seconds to refresh/ update HAMA point values. Refer to HAMA page to get detailed description of the HAMA points and their runtime values.

The following two snapshots are showing an example for the Analog Input/Digital Input displays about the Time Sync when only IRIG-B input is enabled and active.

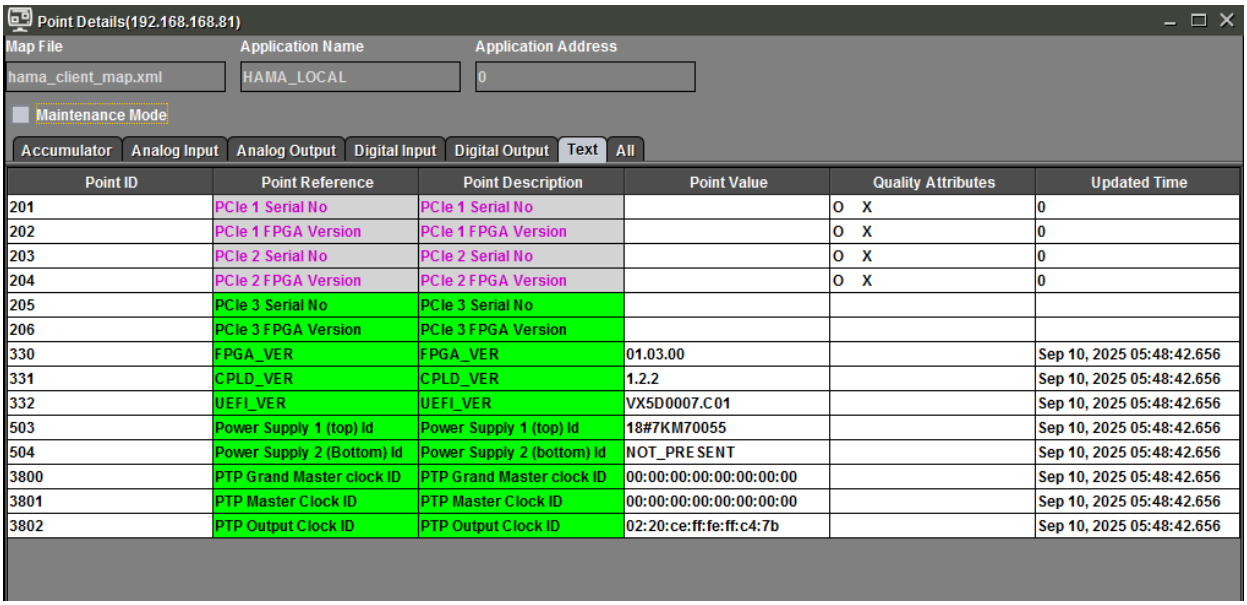


Point ID	Point Reference	Point Description	Point Value	Quality Attributes	Updated Time
2128	PCIe C - COM Mode 8	PCIe C - COM Mode 8	Not Present	O X	0
3000	Time Sync Input Source	Time Sync Input Source	IRIG-B		Feb 3, 2000 17:20:22.237
3011	NET1-2 PTP Port State	NET1-2 PTP Port State	PORT_DISABLED		Feb 3, 2000 17:20:22.237
3012	NET3-4 PTP Port State	NET3-4 PTP Port State	PORT_DISABLED		Feb 3, 2000 17:20:22.237
3013	NET5-6 PTP Port State	NET5-6 PTP Port State	PORT_DISABLED		Feb 3, 2000 17:20:22.237
3021	PTP Clock Class	PTP Clock Class	187		Feb 3, 2000 17:20:22.237
3100	IRIG-B IN Type	IRIG-B IN Type	B006		Feb 3, 2000 17:20:22.237
3101	IRIG-B IN Time Zone Offset to UTC	IRIG-B IN Time Zone Offset to UTC	0	O X	0
3150	NTP Time Offset	NTP Time Offset	0		Feb 3, 2000 17:20:22.237
3151	NTP IN Server Selected	NTP IN Server Selected	0		Feb 3, 2000 17:20:22.237
3152	NTP IN Servers Quality	NTP IN Servers Quality	invalid(0)	O X	0



Point ID	Point Reference	Point Description	Point Value	Quality Attributes	Updated Time	State Description
1661	NET6 SFP IN	NET6 SFP IN	1		Feb 3, 2000 17:20:22.237	Present
3200	PTP/IRIG-B Clock Synchronized	PTP/IRIG-B Clock Synchronized	1		Feb 3, 2000 17:20:22.237	Synced
3210	PTP IN Enabled	PTP IN Enabled	0		Feb 3, 2000 17:20:22.237	Disabled
3211	PTP IN Signal	PTP IN Signal	0		Feb 3, 2000 17:20:22.237	Not Established
3212	PTP IN Quality	PTP IN Quality	0		Feb 3, 2000 17:20:22.237	Bad
3300	IRIG-B IN Enabled	IRIG-B IN Enabled	1		Feb 3, 2000 17:20:22.237	Enabled
3301	IRIG-B IN Signal Fail	IRIG-B IN Signal Fail	0		Feb 3, 2000 17:20:22.237	Not Failed
3302	IRIG-B IN Quality	IRIG-B IN Quality	1		Feb 3, 2000 17:20:22.237	Good
3350	NTP IN Enabled	NTP IN Enabled	0		Feb 3, 2000 17:20:22.237	Disabled
3351	NTP IN Signal	NTP IN Signal	0		Feb 3, 2000 17:20:22.237	Not Present
3352	NTP IN Quality	NTP IN Quality	0	O X	0	Bad
3360	NTP OUT Enabled	NTP OUT Enabled	0		Feb 3, 2000 17:20:22.237	Disabled

The following snapshot shows the Text info about PTP related clock ID information:



Point ID	Point Reference	Point Description	Point Value	Quality Attributes	Updated Time
201	PCIe 1 Serial No	PCIe 1 Serial No		O X	0
202	PCIe 1 FPGA Version	PCIe 1 FPGA Version		O X	0
203	PCIe 2 Serial No	PCIe 2 Serial No		O X	0
204	PCIe 2 FPGA Version	PCIe 2 FPGA Version		O X	0
205	PCIe 3 Serial No	PCIe 3 Serial No			
206	PCIe 3 FPGA Version	PCIe 3 FPGA Version			
330	FPGA_VER	FPGA_VER	01.03.00		Sep 10, 2025 05:48:42.656
331	CPLD_VER	CPLD_VER	1.2.2		Sep 10, 2025 05:48:42.656
332	UEFI_VER	UEFI_VER	VX5D0007.C01		Sep 10, 2025 05:48:42.656
503	Power Supply 1 (top) Id	Power Supply 1 (top) Id	18#7KM70055		Sep 10, 2025 05:48:42.656
504	Power Supply 2 (Bottom) Id	Power Supply 2 (bottom) Id	NOT_PRESENT		Sep 10, 2025 05:48:42.656
3800	PTP Grand Master clock ID	PTP Grand Master clock ID	00:00:00:00:00:00:00:00		Sep 10, 2025 05:48:42.656
3801	PTP Master Clock ID	PTP Master Clock ID	00:00:00:00:00:00:00:00		Sep 10, 2025 05:48:42.656
3802	PTP Output Clock ID	PTP Output Clock ID	02:20:ce:ff:fe:ff:c4:7b		Sep 10, 2025 05:48:42.656

PTP Use Case Scenarios

NOTE: PTP is not supported in G100.

Below are a few commonly used PTP use cases that have been derived to give the user an overview on how PTP can be configured and used in the MCP context.

NOTE User must be cautious while configuring the network interfaces as the PTP functionality is tightly coupled with the mode of the network interfaces.

NOTE PTP functionality is available only on the 6 rear network interfaces (G500).

NOTE In every Configuration Type listed below, NTP OUT can be enabled and used to synch other devices.

MCP can act as a Master Clock, Slave Clock or both based on the Network port configuration and the PTP devices connected.

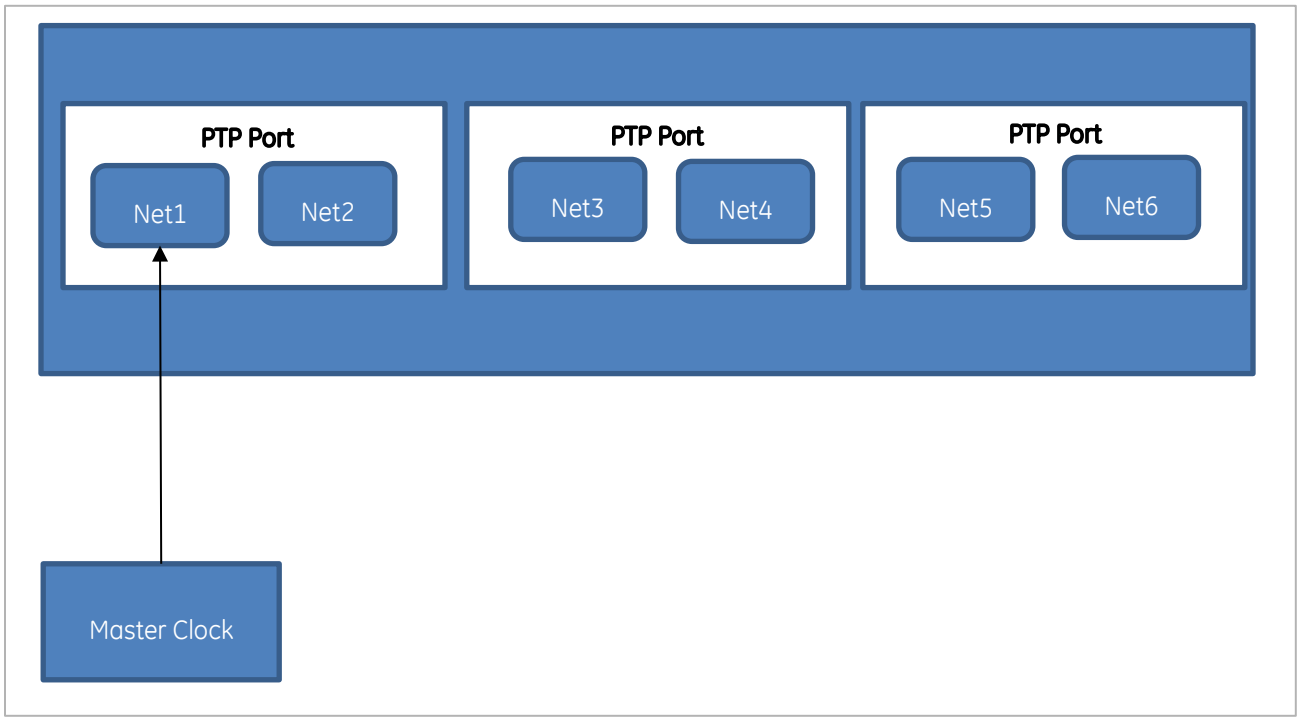
There are different states available for the PTP ports and are described in HAMA - Hardware Asset Management Application.

Configuration Type 1 – Slave Clock

PTP IN is enabled, PTP OUT is disabled, and at least one pair of network ports is configured as independent (SINGLE mode, port 1 and port 2 in this example). The MCP is connected to a valid PTP signal (a clock that is connected to a valid GPS signal).

Figure 4.1 represents a scenario in which the MCP operates as a slave clock.

Figure 4.1: MCP operates as a slave clock



In this state, the MCP will sync to the connected master clock and cannot sync any downstream devices. All ports are in listening or slave mode.

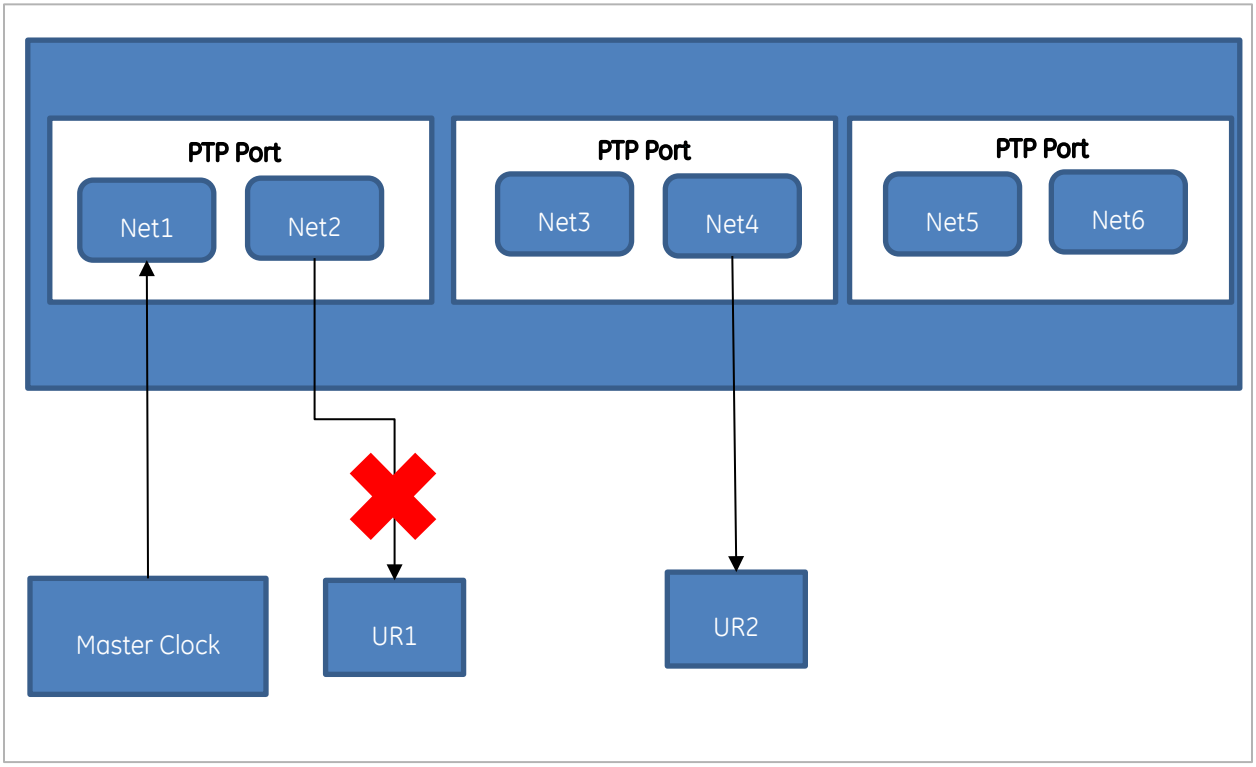
NOTE PTP operates independently of the configured network mode.

It is not possible for one Ethernet port of the PTP port pair to be a master and the other to be a slave.

Configuration Type 2 – Boundary Clock

The MCP has PTP IN and PTP OUT enabled. The following diagram represents a scenario where the MCP acts as a boundary clock:

Figure 4.2: MCP operates as a boundary clock



In Figure 4.2, MCP rear Ethernet port pair Net1-Net2 are connected to a master clock. The MCP synchronizes with the master clock and the port pair connected to the clock becomes a slave and the remaining 2 pairs become Masters. Note here that UR1 will not synchronize to the MCP because the Net1-Net2 pair is in slave mode.

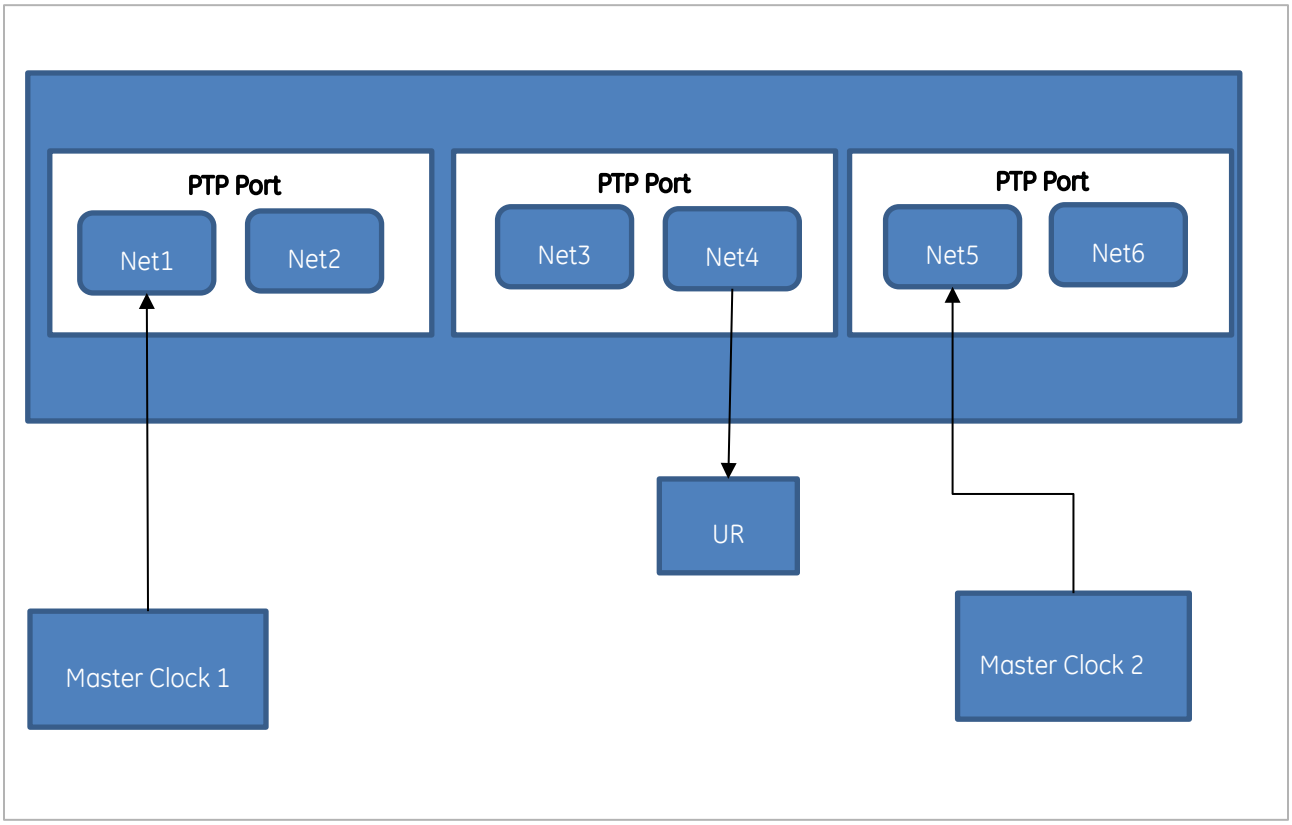
Since UR2 is connected to the Net3-Net4 pair, the MCP acts as Master and synchronizes time to UR2.

The MCP Grandmaster Clock ID, MCP Master Clock ID, and the MCP Output Clock ID are updated in the Text Points section of HAMA_LOCAL application as part of the runtime GUI, refer HAMA - Hardware Asset Management Application.

Configuration Type 3 – Best Master Clock Scenario

The MCP has PTP IN and PTP OUT enabled. The Figure 4.3 gives an example of a MCP connected to multiple time sources which requires the Best Master Clock (BMC) algorithm.

Figure 4.3: Best Master Clock Scenario



From the above, assume that:

- **Clock 1** : Connected to GPS with priority 120
- **Clock 2** : Connected to GPS with priority 128
- **UR** : Slave Only Device

Since clock 1 is a better clock, MCP synchronizes with clock 1 and the Net1-Net2 pair becomes slave.

MCP acts as master and synchronizes the UR connected to Net4.

Networking

This section contains the following topics:

Background

Network Modes

Single Mode

Redundant Mode

PRP Mode

Substation LAN IED Types

Single LAN IED

Dual LAN IED

Redundant LAN IED
PRP LAN IED
Network Configuration
Network Interfaces
IP Configuration
Gateway Configuration
VLANS
Configure Network Interfaces
Run Time Statistics
Network LAN Scenarios
Legacy Single and Dual LAN Scenario
Legacy Single, Dual LAN + PRP Scenario
Legacy Single, Redundant and Dual LAN Scenario (Mixed System)
PRP Only Scenario
Mixed: Legacy + PRP LAN Scenario
Subnet Overlapping Rules
Custom Routing
Custom Routing Example
Configure Custom Routes in the MCP
Display Custom Routes
Delete Custom Routes
Network Summary

Background

Refer to the G500 Substation Gateway Instruction Manual (994-0152) or G100 Substation Gateway Instruction Manual (994-0155) for details on the MCP Network ports and their supported connection types.

Network Modes

G500 supports three modes of network operation. At FPGA level, six rear ports are grouped together in to three pairs. Front port cannot be grouped with rear ports.

In G100 the four ports are all independent, but presented in the settings in pairs to be consistent with G500.

Supported network modes are classified as:

- **Single Mode**
- **Redundant Mode**
- **PRP Mode**

NOTE: G100 does not support Redundant or PRP modes.

Single Mode

In this mode, ports in the pair would be independent to each other. Both network interfaces in that pair are available for network configuration.

This type of mode can also be used to communicate with Dual LAN IEDs.

For e.g.: Say you have an IED with dual LAN communication. Dual LAN IED would have two IP (172.12.232.18 & 192.168.4.16). MCP Net1 can be configured with 172.x network & Net2 can be configured in 192.x network. Now in DCA, while configuring this IED, 172.12.232.18 can be configured as Primary IP & 192.168.4.16 as Secondary IP.

NOTES:

1. It is **not** recommended to use Net0 (G500) for IED communication.
2. By default, Net0 (G500) is in single mode & cannot be configured in PRP or Redundant mode.
3. Subnet overlap is not allowed in MCP. If same subnets are configured warning would be displayed.

For e.g.: Suppose say Net1 is configured with 172.12.232.56/16. Net2 IP cannot be 172.12.232.128/16.

Redundant Mode

Not supported in G100

In this mode, each pair can be configured as redundant and available for network configuration. This type of mode is used to communicate with Redundant LAN IEDs. In this type of communication, one port would be active at a time. If communication lost on one port, then Secondary port would become active.

For e.g.: Say configured Net1 – Net2 in this mode. Connect a Redundant LAN IED with MCP. In this topology Net1 & Net2 must be part of two different LAN switches. If network failure occurred on Net1 then communication would switch to Net2 port. If communication restored on Net1, then communication will switch back to Net1 & Net2 would become inactive.

PRP Mode

Not supported in G100.

In this mode, each pair can be configured for PRP and available for network configuration. This type of mode is used to communicate with PRP LAN IEDs. In this type of communication, both ports would be active all the times. If communication lost on one Network, then communication would continue another Network.

Substation LAN IED Types

IEDs connected to the substation LAN can be classified as:

- **Single LAN IED**
- **Dual LAN IED**
- **Redundant LAN IED**
- **PRP LAN IED**
  MCP supports only Single LAN IED's

Single LAN IED

This type of IED only has one physical LAN port (connection) and communicates only on one single LAN.

Two sample connection scenarios are:

- Two IEDs may be deployed in IED redundant mode, with each Single LAN IED using a single LAN connection on separate substation LAN sides. The LAN sides may (but are not required to) be connected, since redundancy between the multiple (x2) IEDs is provided at the application layer.
- The MCP may be monitoring non-essential IEDs that are not redundant and do not contain multiple LAN ports (for example, Meters, LAN printer).

Network Configuration

This section describes how to configure IP, selecting type of mode & viewing stats of configured ports. This section is divided in to:

- **Network Interfaces**
- **IP Configuration**
- **Gateway Configuration**
- **VLANS**
- **Configure Network Interfaces**
- **Run Time Statistics**

Network Interfaces

The Network Interface workflow allows you to configure the settings for the MCP's network connections.

Default enabled network interface is configured with IP: **192.168.168.81/24** and is enabled as:

- Net0 in G500
- Net1 in G100

Due to hardware differences, Net0, Net5, Net6 are present only in G500.

NOTES: The MCP must be rebooted to activate any changed network settings.

The first time the MCP is started, you must configure the network interface locally through the default enabled network port.

IP Configuration

The Internet Protocol (IP) can be configured as a:

- Static IP Address: Maintenance, Active, or Alias IP Addresses
- Dynamic IP Address: Static or DHCP

SFP Configuration (G100 only)

The SFP types are detected automatically in G500, after startup / reboot.

G100 does not have hardware support to detect automatically the inserted SFP type in Net3 or Net4; these must be set by the user using the Local configuration utility (mcpcfg) or MCP Settings GUI.

The selection of the SFP type is performed only for Net3 and Net4, and is consistent with the order code options:

1. Option C: 10/100BASE-TX
2. Option T: 1000BASE-TX
3. Option F: 100BASE-FX
4. Option S: 1000BASE-SX
5. Option L: 1000BASE-LX

6. Option U: Not Installed

Gateway Configuration

The Default Gateways can be configured for the Maintenance and Active Interfaces.

NOTE Provide the Active Default Gateway Address if the MCP is configured to be operating in Redundant mode (either Warm or Hot Standby).

VLANS

MCP supports VLAN configuration. VLAN IP can be created with IDs from 2-4094. These IDs are common to all interfaces i.e. say a VLAN ID 2 created one network port cannot be used in other network port.

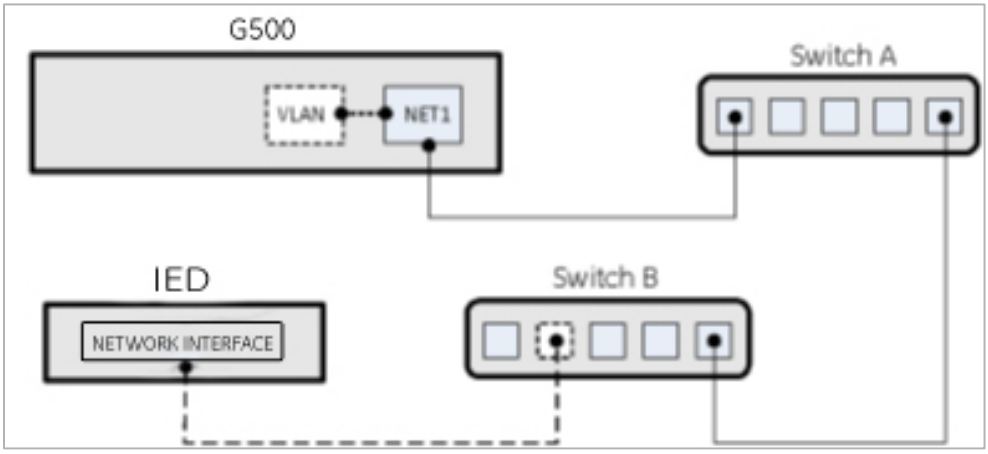
Configure Network Interfaces

The Configure Network Interfaces menu in MCP Local Command Line Utility (**mcpcfg**) includes settings for the MCP's network connections. The Network Interface settings are described in Table 4.2.

NOTE The MCP must be rebooted to activate any changed network settings. The first time the MCP is started up, user must configure the network interface locally through the maintenance Net port, maintenance serial port or local HMI terminal.

Table 4.2: Network Interface Settings

Setting	Description
Net0 (only G500) Net1 – Net2 Net3 – Net4 Net5 – Net6 (only G500)	**Network Interface Settings Edit** **Current Configuration** Use this function to view the current state of the available MCP network interfaces. **Static IP Address** Use this function to configure the MCP to use manually defined network parameters. Configurable addresses include: • ***Maintenance***: Also referred to as the static address, this is the Primary IP Address, subnet mask, and default gateway for use by this MCP. **Note**: In a non-redundant system, the maintenance address is used as the network address of the device. • ***Active***: Used for MCP system redundancy. Whichever redundant MCP is active at the time assumes this IP Address; the standby unit reverts to its own maintenance IP Address. The active address settings should be the same on both redundant units. • ***Alias***: An alternate address that can be configured to allow a Secondary communications link with the MCP. This is typically used for redundant LAN D25s. When used within a redundant MCP system setup, the alias address settings should be the same on both redundant units. The alias addresses must be on a different subnet mask than the maintenance and active addresses. **Dynamic Address** Configure the MCP to use network parameters that are provided by a DHCP server. This requires a DHCP server to be on the same network as the MCP. **Note**: Dynamic addressing is not compatible with MCP system redundancy as the active and alias addresses are not provided by DHCP. **Network Zone** By default, all network interfaces except initial enabled maintenance ones are set to the External firewall mode, which restricts the type of traffic permitted. You can change the selected network interface to the Internal or External modes with this option. For more information on the MCP firewall, refer to section Configure firewall settings. **VLAN**

	It is possible to use a VLAN when connecting MCP and VLAN supported device over a network. By assigning your VLAN supported device to a VLAN, you can ensure a higher priority for data transmitted from it and you can reduce the amount of extraneous information the VLAN supported device receives from other devices on the network. **Figure 4.4: Sample VLAN configuration of Net1**  In Figure 4.4 a VLAN has been created on the NET1 interface on the MCP. NET1 is connected to a third-party switch, which is also connected to another third-party switch. These connections are called the trunks since they carry the VLAN data as well as all other data transmitted on the interface. The switch B is also configured to support a VLAN on a certain network port, which is connected to an IED. Since this port is dedicated to the VLAN, only information flagged for the VLAN is transmitted to that IED. As well, information sent on this VLAN from the IED to device can be classified with a higher priority, which ensures a higher likelihood of transmission during times of network congestion. You can configure the following options on each VLAN you create: • IP Address, subnet mask, and default gateway: You can assign static IP Address / dynamic IP Address. Once you have configured these values, you can use them to access your VLAN. • Network zone: Assign the VLAN to either the internal or external network zone. For more information on network zones, refer to section Configure firewall settings. **Note**: You can always assign a VLAN to the external network zone. However, you cannot assign it to the internal zone when the associated physical interface is configured to the external zone. • EGRESS priority mapping: Set the QoS priority level for data transmitted on this VLAN. Priority levels range from 0 to 7 with 7 being the highest priority. If a QoS-enabled device receives packets transmitted on this VLAN, it should apply a priority based on the level you specify. • Ethernet reorder flag header: This option is reserved for use by MCP staff for Technical Support tasks. **Remove Configuration** Use this command to remove the current Network Interface settings. All configured Maintenance IP Addresses, , Alias IP Addresses, Network Zones and VLANs are removed. This command also allows you to back up the current configuration.
Net1 (only G500) Net2 (G100, G500) Net3 – Net4 (only G100) Net5 – Net6	**EdgeManager Connectivity Configuration** Refer to *Chapter 8 - EdgeManager and PETC* for port availability and additional information. This option is used to enable EdgeManager connectivity on that port. **Current EdgeManager Configuration:** To view the configuration **Configure EdgeManager Static IP Address:** Option to configure Static IP Address , which will be used to enable connectivity to EdgeManager in the cloud/EdgeManager App.

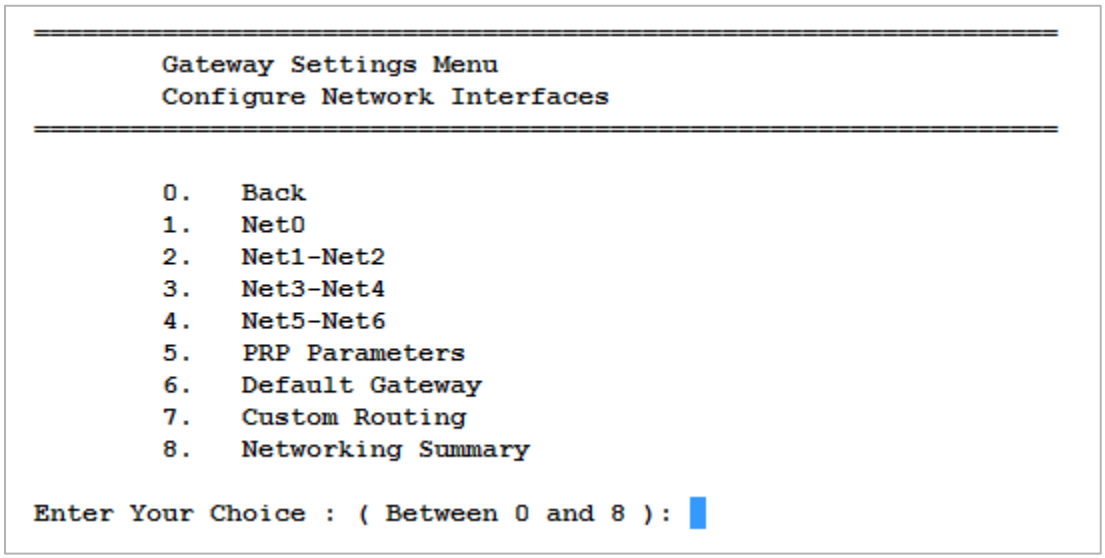
(only G500)	**Configure EdgeManager Dynamic IP Address:** Option to configure Dynamic IP Address , which will be used to enable connectivity to EdgeManager in the cloud / EdgeManager App. **EdgeManager Remove Configuration:** Option to remove the configuration
Net1 – Net2 Net3 – Net4 Net5 – Net6 (only G500)	**Network port mode** **Single** Use this option to configure the network pair in single mode. This mode is useful to communicate LAN devices. **Redundant (only G500)** Use this option to configure a network pair in Redundant mode. This mode is useful to communicate with Redundant IEDs. • This will remove existing Secondary port configuration. • If configuration not removed, then Redundant communication will not be enabled Disable Redundant mode: go to that pair & select single mode for that pair. This would update the setting of that pair to single mode from redundant mode. **PRP (only G500)** Use this option configure a network pair in PRP mode. This mode is useful to communicate with PRP IEDs • This will remove existing Secondary port configuration. • If configuration not removed, then PRP will not be enabled Disable PRP mode: go to that pair & select single mode for that pair. This would update the setting of that pair to single mode from PRP mode. **Current/Edit Configuration** This option is used to view the current configuration of a pair or to edit the configuration of the pair.
Net3 – Net4 (only G100)	**SFP Configuration** Use this option to configure the SFP type inserted in Net3 and Net4: 1. Option C: 10/100BASE-TX 2. Option T: 1000BASE-TX 3. Option F: 100BASE-FX 4. Option S: 1000BASE-SX 5. Option L: 1000BASE-LX 6. Option U: Not Installed
PRP Parameters	Use this command to enable or disable the PRP on the MCP network ports. Enabling PRP: • Removes the existing Network Interface settings. • Uses the PRP LANID and PRP Supervision Frame Interval. Moves the network interface to internal zone of the firewall.
Default Gateway	Use this command to set the Default Gateway IP Address (optional). The IP Address of the Gateway can be configured for all Network Interfaces. If redundancy is configured, you are advised to configure the Active Gateway IP Address. **NOTE:** Gateway address must be re-entered after editing the sub-net mask.
Custom Routing	Use this command to display, enable and disable custom routes in the MCP. For addition of custom routes in the MCP, you may need to provide the following: • Destination IP Address, • Destination subnet mask • Next Gateway IP Address (optional)

	• Network interface of MCP that needs to be used.
Networking Summary	Use this command to display a summary of all the configured network interfaces in the MCP.

To configure the network interface

1. To navigate to this menu in Figure 4.6, type mcpcfg in MCP command prompt and Select option **3. Configure Network Interfaces**

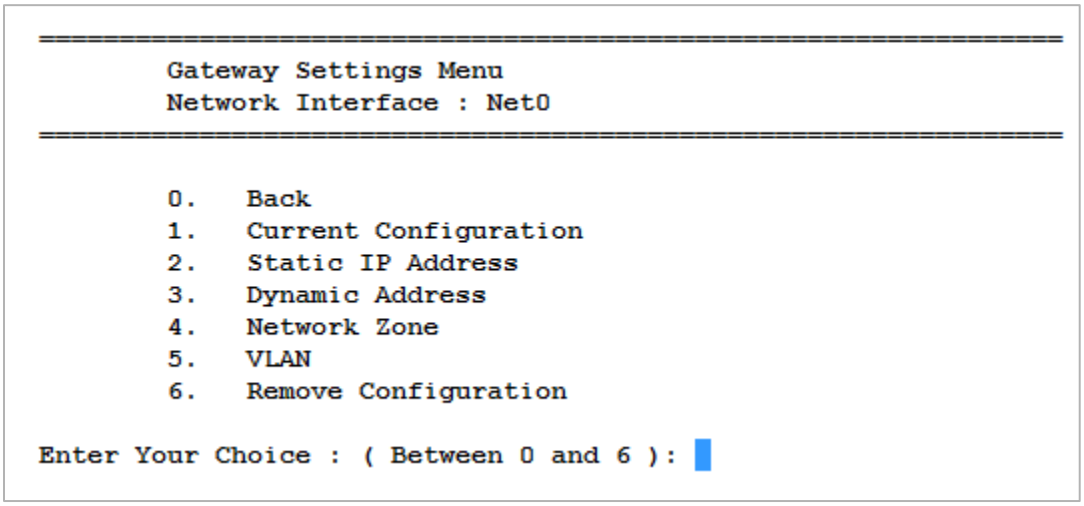
Figure 4.5: Configure Network Interfaces



2. In the sub-menu, select Option **1. Net0**.
   a. In this option 1. Current configuration is used to see the configure IP details.
   b. MCP can be configured with static or dynamic networks.
   c. To configure static network, select option **2. Static IP Address**.
   d. In the static network, maintenance IP, Active IP & Alias IP can be configured.
   e. Dynamic Address can be configured on any port, by with option **3. Dynamic Address**
   f. Option **4. Network Zone** is used to select configure that port to an Internal or External zone. Used for firewall communication
   g. Option **5. VLAN**, is used to create VLANs on that port. VLANs can be created in MCP with ID ranging from 2-4094. This ID is common to all ports.
      For e.g. A VLAN with ID 3 is created on Net0. Now VLAN with ID 2 cannot be created on another port
   h. Select option **0. Back** to return to previous menu.

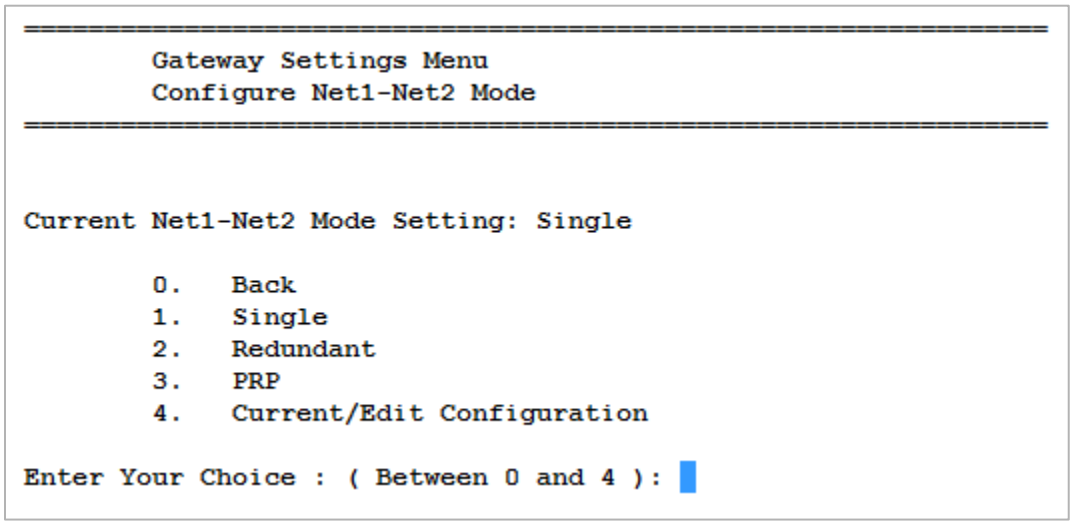
   Note: Dynamic IP & Static cannot be configured together

Figure 4.6: Configure Net0 Interface



3. To configure Net1-Net2, select option **2. Net1-Net2.** Below sub menu (Figure 4.8) would appear.
   a. Select Option **1. Single** to enable Single Mode.
   b. Select option **2. Redundant** to enable Redundant Mode.
   c. Select option **3. PRP** to enable PRP Mode.
   d. Select **4. Current/Edit Configuration** to update configuration

Figure 4.7: Configure Net1 - Net2



4. If Single mode is selected in Figure 4.8, Net1 & Net2 can be configured separately as described in step 2.

Enable and disable Redundant mode

This mode is not supported in G100.

1. Select option **2. Redundant** then, below message (Figure 4.9) would appear.
   a. Select **Y(yes),** to change mode.
   b. Select Yes, to remove the Net2 configuration.
   c. If second port configuration is not removed when asked, redundant mode will not be enabled. Only Net2 configuration is removed & Net1 configuration is retained (if present).
   d. Press Enter, a submenu like show in **Figure 4.9** would appear.

e. As Net1 – Net2 is combined as a single network interface (Redundant 1), this interface can be configured as in step 2 and reboot the device.
f. Reboot of device is required, for Network related changes.
g. To disable Redundant mode, enter to menu shown in Figure 4.8, select option **1. Single** and follow step 4 and reboot device.

Figure 4.8: Enable Redundant mode

```
==========================================================================
        Gateway Settings Menu
        Configure Net1-Net2 Mode
==========================================================================


Current Net1-Net2 Mode Setting: Single

        0.   Back
        1.   Single
        2.   Redundant
        3.   PRP
        4.   Current/Edit Configuration

Enter Your Choice : ( Between 0 and 4 ): 2

Are you sure you want to change the mode for Net1-Net2? [Y/N]:  y

The following settings will be removed for Net2:
Maintenance IP Address
Active IP Address
Alias IP Address
Network Zone
VLANs

Are you sure you want to remove the configuration for Net2? [Y/N]:      y

Net2 successfully assigned to the Internal network zone.

Net1-Net2 Mode is updated to Redundant

Reboot for changes to take effect

Press ENTER Key to continue....
```

Enable and disable PRP mode

This mode is not supported in G100.

1. Select Option **3.PRP** in Figure 4.8 to enable PRP.
   a. Select **Y (yes),** to change mode.
   b. Select Yes, to remove the Net2 configuration.
   c. If second port configuration is not removed when asked, PRP mode will not be enabled. Only Net2 configuration is removed & Net1 configuration is retained (if present).

d. Press Enter, in Figure 4.8, a submenu like **in Figure 4.10** would appear.
e. As Net1 – Net2 is combined as a single network interface (PRP 1), this interface can be configured as in step 2 and reboot device
f. To disable PRP, enter to menu shown in Figure 4.8, select option **1. Single** and follow step 4 and reboot device**.**

2. Similarly, configuration can be done for Net3- Net4 & Net5 -Net6
3. Select Option 5. PRP Parameters
   a. In this option PRP Life Check Interval can be configured.
   b. PRP Life Check Interval can be between a range of 2sec to 10sec
   c. This parameter is common to all Interfaces configured in PRP.

Figure 4.9: Enable PRP Mode

```
=================================================================
        Gateway Settings Menu
        Configure Net1-Net2 Mode
=================================================================


Current Net1-Net2 Mode Setting: Redundant

        0.   Back
        1.   Single
        2.   Redundant
        3.   PRP
        4.   Current/Edit Configuration

Enter Your Choice : ( Between 0 and 4 ): 3

Are you sure you want to change the mode for Net1-Net2? [Y/N]:  y

The following settings will be removed for Net2:
Maintenance IP Address
Active IP Address
Alias IP Address
Network Zone
VLANs

Are you sure you want to remove the configuration for Net2? [Y/N]:      y

Net2 successfully assigned to the Internal network zone.

Net1-Net2 Mode is updated to PRP

Reboot for changes to take effect

Press ENTER Key to continue....
```

4. Select option **6. Default Gateway,** to configure default gateway.
5. Select option **7. Custom Routing** to enable custom routing.
6. Select option **8. Networking Summary** to display IP configuration done on all ports**.**

Run Time Statistics

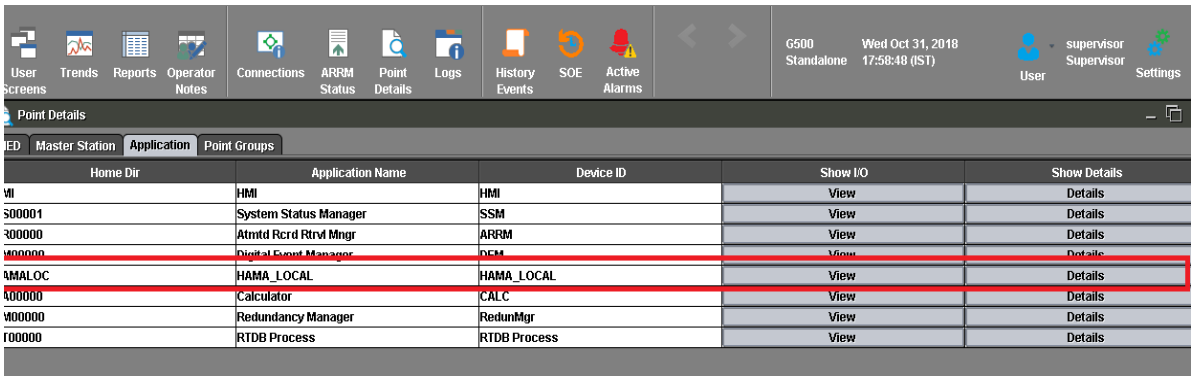
The runtime status of PRP points & can be viewed from the Local/ Remote HMI in

Point Details → Application → "HAMA_LOCAL"

Not available in G100.

Refer to HAMA page to get detailed description of the HAMA points and their runtime values.

Figure 4.10: HAMA Points



Network LAN Scenarios

PRP is not supported in G100.

This section describes network LAN scenarios when enabling PRP in the G500 for operation in substations containing various IED types.

The following scenarios are provided:

- **Legacy Single and Dual LAN Scenario**
- **Legacy Single, Dual LAN + PRP Scenario**
- **Legacy Single, Redundant and Dual LAN Scenario (Mixed System)**
- **PRP Only Scenario**
- **Mixed: Legacy Single/Redundant/Dual LAN + PRP Scenario**

Legacy Single and Dual LAN Scenario

G500 operation within a current substation LAN containing only legacy Single and/or Dual LAN IEDs (see Figure 4.12).

- All network ports must be configured in single mode. Both FX & Copper are supported.
- In single mode, one FX & one copper each is supported per pair.
- SFP 1 – FX.
- SFP 2, 3, 4, 5, 6 – Copper.

NOTE: The VLAN ID must be explicitly configured on switch ports (all others are blocked. Dual LAN is achieved in the G500 using a network pair in Single mode.

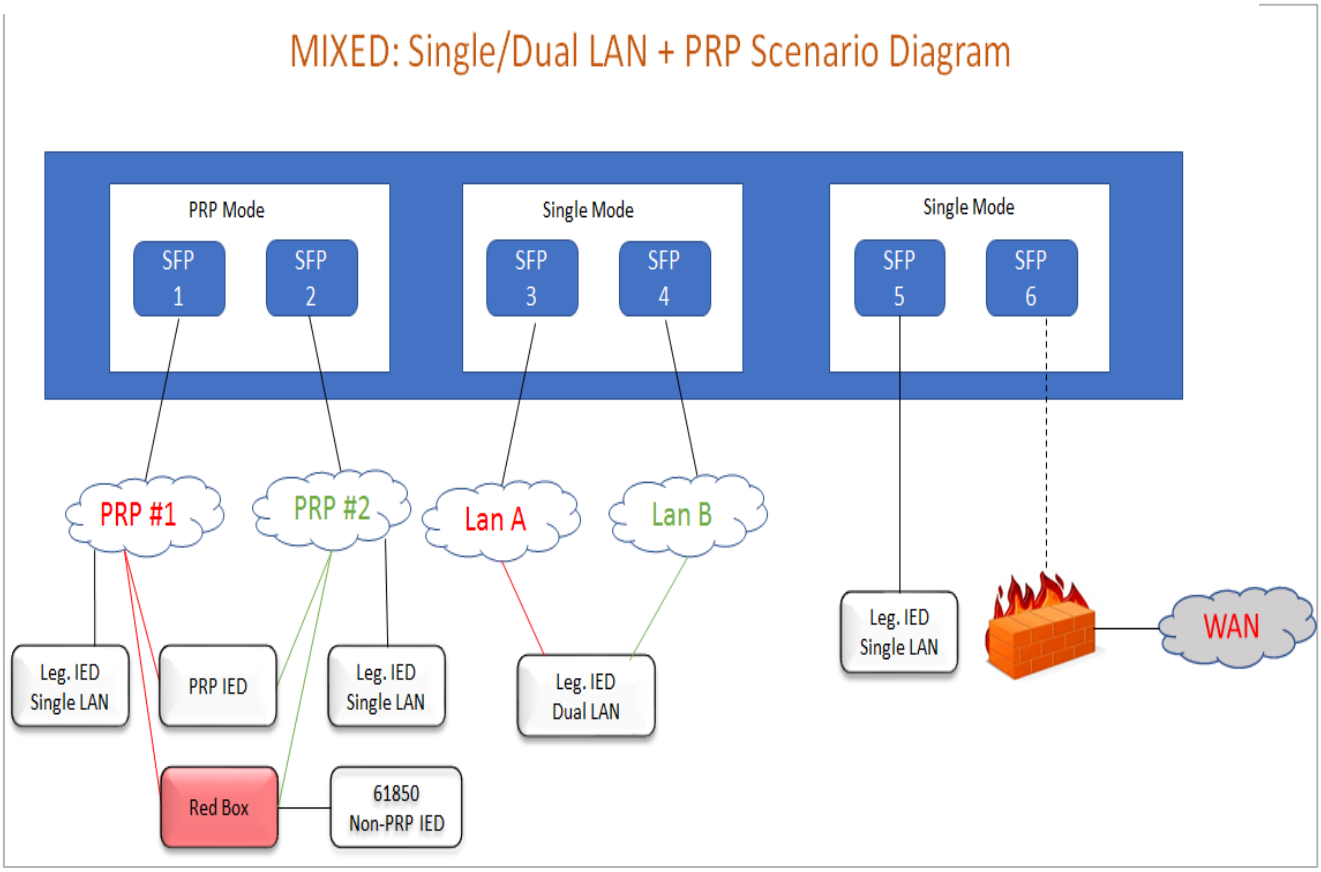
Figure 4.13 shows the one possible method for this scenario with MCP in the current network.

Legacy Single, Dual LAN + PRP Scenario

G500 operation within a current substation LAN containing only legacy Single and/or Dual LAN IEDs (see Figure 4.14):

- SFP 1, 2 – FX
- SFP 3, 4, 5, 6 – Copper
- VLAN tagging is optional for all traffic
- G500 must be configured as Trunk port or PRP/Redundant mode both SFP must be of same type.

Figure 4.11: MIXED: Single/Dual LAN + PRP Scenario Diagram



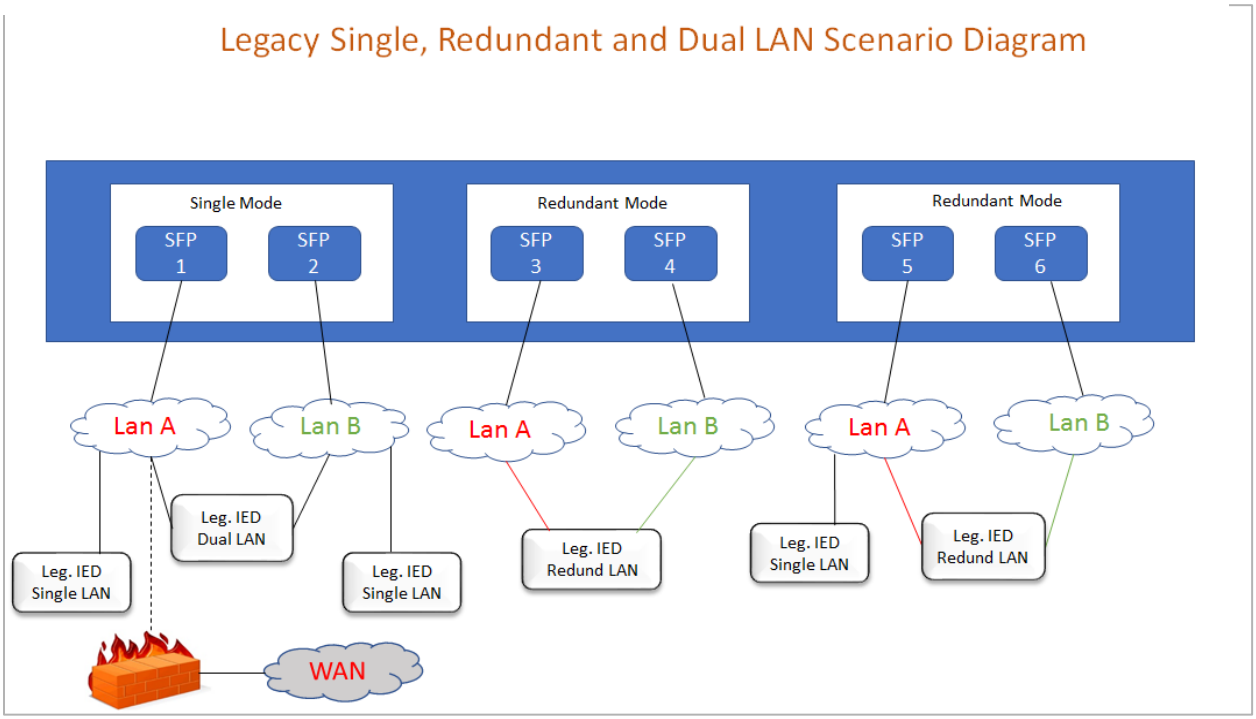
Legacy Single, Redundant and Dual LAN Scenario (Mixed System)

G500 operation within a current substation LAN containing only legacy Single and/or Dual, and Redundant LAN IEDs (see Figure 4.15):

- SFP 1 – FX
- SFP 2, 3, 4, 5, 6 – Copper
- The VLAN ID must be explicitly configured on switch ports (all others are blocked).

- At least one pair must be configured in Redundant mode & other as single mode.

Figure 4.12: Legacy Single, Redundant and Dual LAN Scenario Diagram

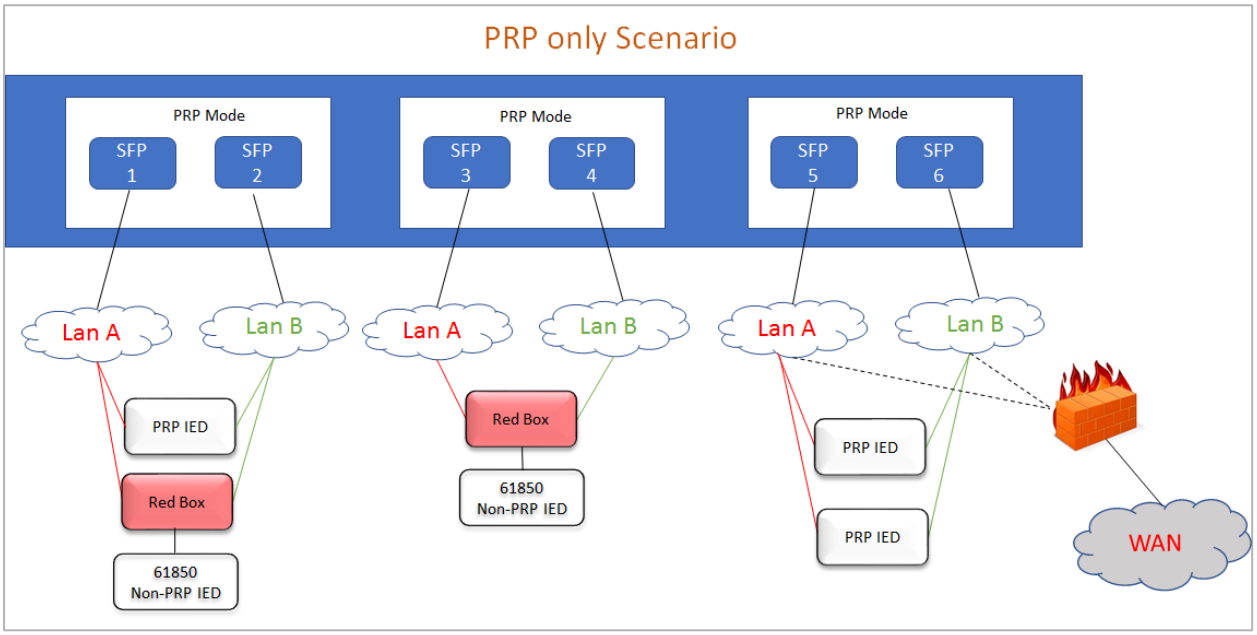


PRP Only Scenario

G500 operation within a current substation LAN containing only PRP IEDs (see Figure 4.16):

- All port pairs must be configured in PRP mode.
- The VLAN ID must be explicitly configured on switch ports (all others are blocked.
- VLAN tagging is optional for all traffic.

Figure 4.13: PRP only Scenario



Mixed: Legacy + PRP LAN Scenario

G500 operation within a substation LAN containing legacy Single and/or Dual, Redundant LAN, and PRP IEDs:

- Supported SFPs must be inserted in G500 rear ports.
- One port pair must be configured in Redundant mode, one in PRP mode and one in single mode.
- Figure 4.16 shows a possible configuration of this scenario network that contains legacy single, redundant and Dual LAN IEDs.

Figure 4.14: Mixed: Legacy Single/Redundant/Dual LAN + PRP Scenario

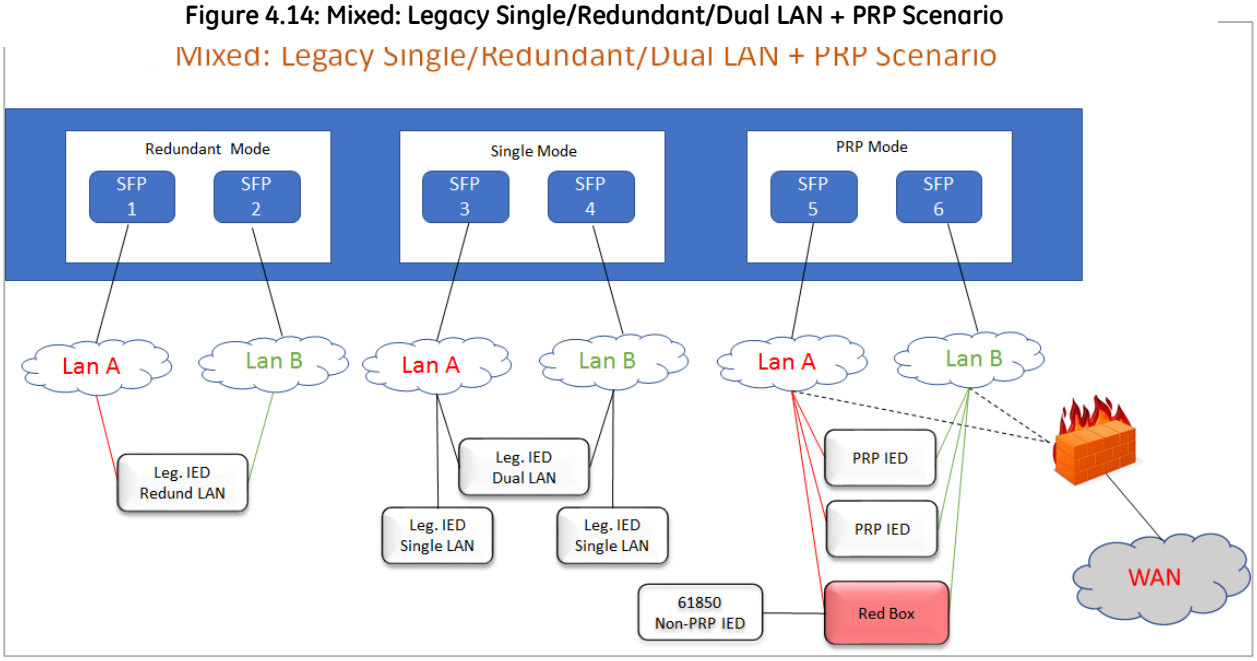
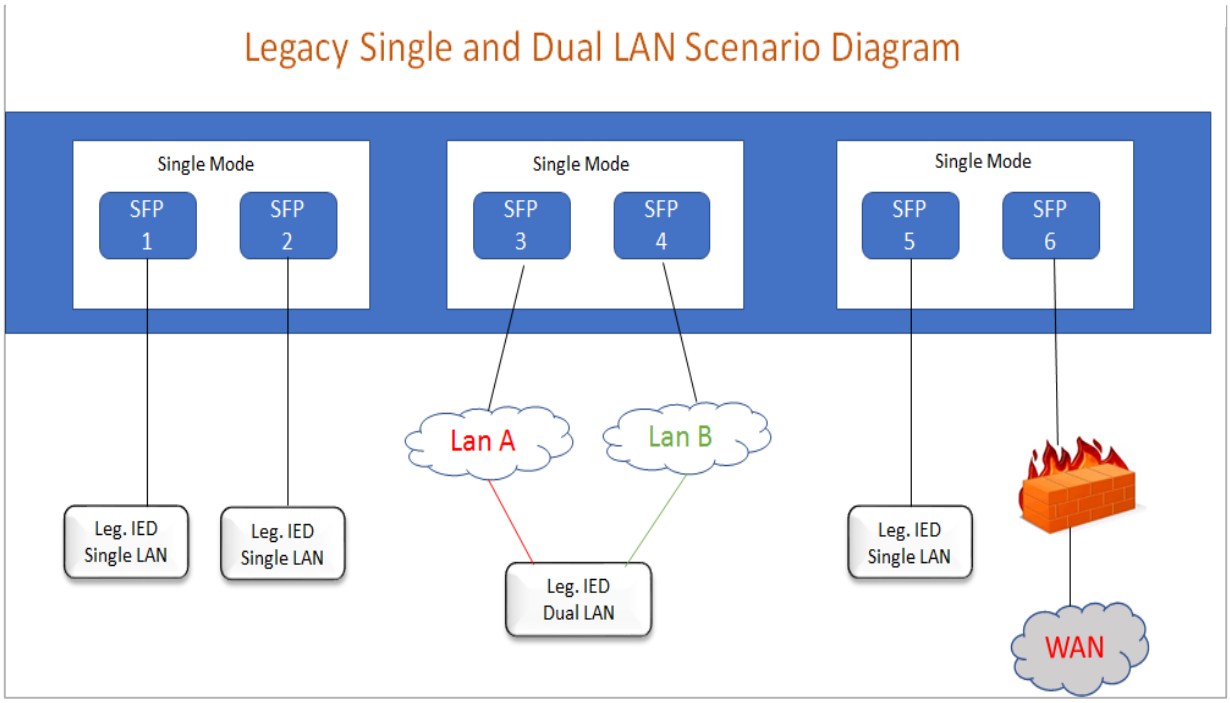


Figure 4.15: Legacy Single and Dual LAN Scenario Diagram



Subnet Overlapping Rules

In MCP, overlapping of subnet validations are done across all the physical and logical interfaces (Net0-Net6). Validations are done for Host, Container as well as VLAN IP configurations.

Below are the IP configurations in MCP which are considered for subnet overlapping validations.

All Network Interfaces in firmware container (Maintenance, Alias).

- Net1 interface in Host.
- EdgeManager.
- VLAN (Can be in any of/all the interfaces).

Subnet Overlapping Rules for same Interface

The Subnet Overlapping Rules for the same Interface are given below.

Table 4.3: Subnet Overlapping Rules for same Interface

	Net1-Net6 Subnet Overlapping same Interface			
	Maintenance	**Alias**	**EdgeManager**	**VLAN**
Maintenance	NA	Allowed	Allowed	Not Allowed
Alias	Allowed	NA	Allowed	Not Allowed
EdgeManager	Allowed	Allowed	Not Allowed	Not Allowed
VLAN	Not Allowed	Not Allowed	Not Allowed	Not Allowed

Subnet Overlapping Rules for two different Interface

The Subnet Overlapping Rules for the two different Interfaces are given below.

Table 4.4: Subnet Overlapping Rules for two different Interface

Interface 1		Interface 2			
		Maintenance	**Alias**	**EdgeManager**	**VLAN**
	Maintenance	Not Allowed	Not Allowed	Not Allowed	Not Allowed
	Alias	Not Allowed	Not Allowed	Not Allowed	Not Allowed
	EdgeManager	Not Allowed	Not Allowed	Not Allowed	Not Allowed
	VLAN	Not Allowed	Not Allowed	Not Allowed	Not Allowed

1. Overlapping of subnet across Maintenance, Alias, Host / EdgeManager IPs **within same network interface are ALLOWED**.
   Net1 Maintenance : 192.168.72.140/24
   Net1 Alias : 192.168.72.142/16
   Net1 host : 192.168.72.145/8
   Net2 Maintenance : 172.169.73.11/8
   Net2 Alias : 172.169.73.13/8
   Net2 EdgeManager : 172.169.73.15/8
2. Overlapping of subnet for VLAN IP configurations within same or different network interfaces are **NOT ALLOWED**.
   Net1/VLAN2 : 192.168.72.151/24 is not ALLOWED as it overlap with Net1 subnet configurations.
   Net1/VLAN2 : 172.169.73.25/24 is not ALLOWED as it overlap with Net2 subnet configurations.
   Net1/VLAN2 : 10.168.8.101/24 is ALLOWED as there is no overlap.
   Net1/VLAN3 : 10.168.8.102/24 is not ALLOWED as it overlap with Net1/VLAN2 subnet.
   Net2/VLAN3 : 10.168.8.102/24 is not ALLOWED as it overlap with Net1/VLAN2 subnet.
3. Overlapping of subnets across the interfaces are **NOT ALLOWED**.

   Net2 Maintenance : 192.168.72.147/24 is not ALLOWED as it overlap with Net1 subnet configurations.

   Net3 Maintenance : 172.169.73.18/24 is not ALLOWED as it overlap with Net2 subnet configurations.

   Net2 EdgeManager : 10.8.5.115/8 is ALLOWED as there is no overlap with any other interfaces

   Net1 host : 101.121.172.25/8 is ALLOWED as there is no overlap with any other interfaces.

   Net3 Maintenance : 101.121.172.101/24 is not ALLOWED as it overlap with Net0 Host subnet configurations.

   Net4 Maintenance : 10.8.5.11/24 is not ALLOWED as it overlap with Net2 EdgeManager subnet configurations.
4. IP conflict checks between Maintenance, Alias, Host / EdgeManager IPs within same interface are done.

Custom Routing

The MCP provides the user with an option to define custom routes through which the network traffic may be forwarded.

The default gateway of the MCP is used to forward the packets to the destination IP if the destination IP is not directly connected to the MCP. The assumption is that the default gateway will know how to reach any network that the MCP itself cannot reach through one of its own interfaces.

Custom routing, on the other hand, defines static rules which specify the route through which the packet is forwarded to reach the pre-defined destination subnet when MCP cannot reach it through one of its own interfaces.

For the addition of custom routes in the MCP, the user may have to provide the following inputs:

- Destination IP Address,
- Destination subnet mask
- Next Gateway IP Address (optional)
- Network interface of MCP that needs to be used.

The IP Address of the Next Gateway should be in the same subnet as the network chosen for the MCP, or else an error is displayed. For the addition of an individual IP Address on destination subnet, you need to set the subnet mask to 255.255.255.255 or define the destination as single host.

If redundancy is configured, the user may have to cautiously configure the static routes in both MCPs.

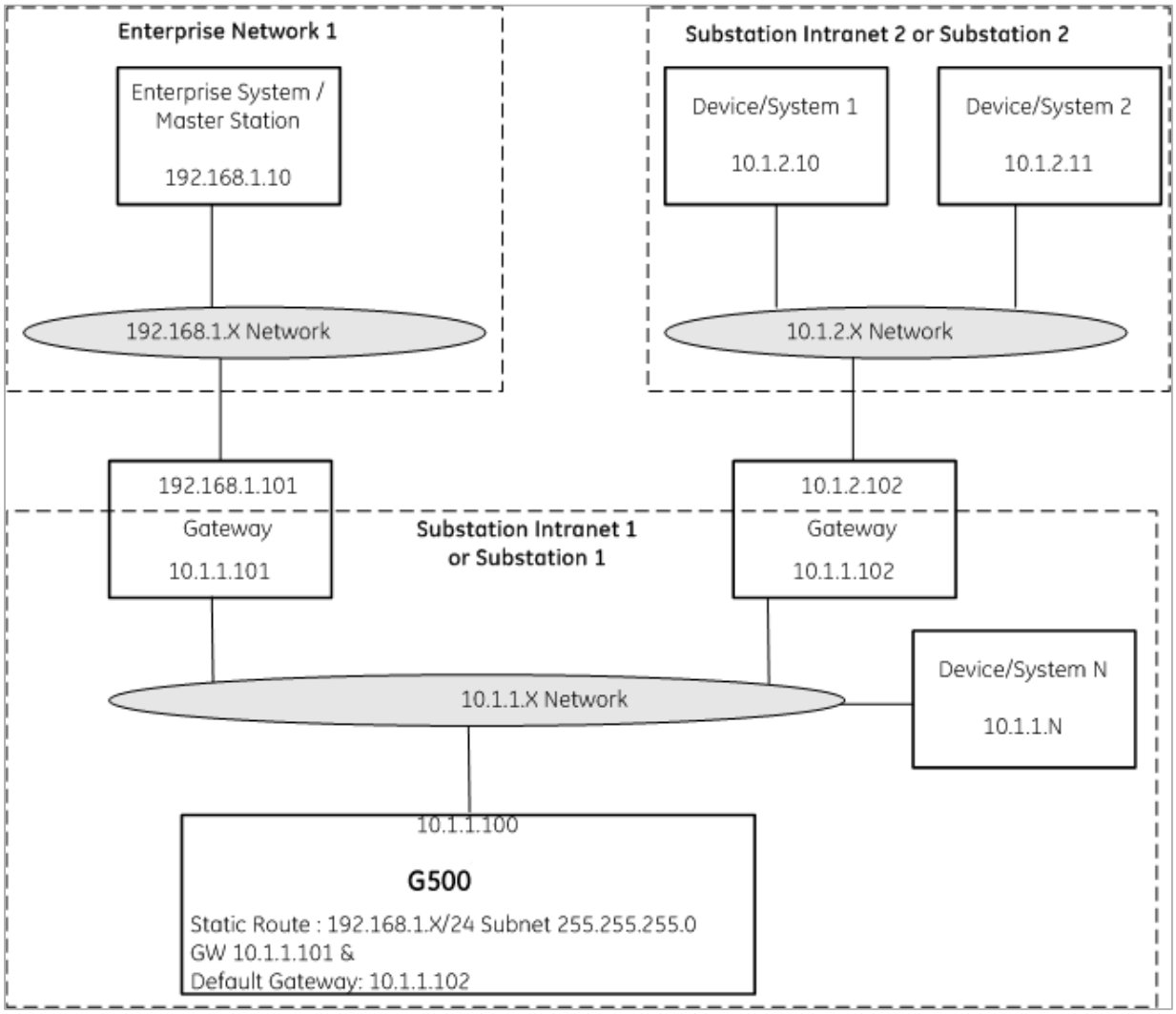
The user may define multiple static routes in the MCP using the custom routing option for each of the available network interfaces including VLAN and PRP.

Custom Routing Example

An example of a configuration that requires custom routing in the MCP is an intranet that has two private Substation Intranets, 10.1.1.X Subnet Mask 255.255.255.0, 10.1.2.X Subnet Mask 255.255.255.0 and Enterprise Network 192.168.1.X Subnet Mask 255.255.255.0. The configuration has one default gateway 10.1.1.102 that forwards traffic between the Substation Intranets 1 and Substation Intranets 2 and one custom route with destination address 192.168.1.X Subnet Mask 255.255.255.0 4 though the gateway 10.1.1.101 that forwards the traffic between Substation IntraNet1 and Enterprise Network.

Note: IP Addresses shown in the diagram below are provided for example purposes only.

Figure 4.16 Custom Routing Example - Block Diagram



Configure Custom Routes in the MCP

When configuring custom routs in the MCP, you can:

- Display Custom Route
- Add Custom Route
- Delete Custom Route
- Add Custom Route

A custom route in the MCP is enabled using the Gateway Configuration Utility (mcpcfg).

NOTE: If an IP Address of an available network interface is changed or deleted, the custom routes for that interface are automatically deleted.

» To add Custom Routes:

1. Log into the MCP **Utilities** page.
   Result: The MCP #>> prompt appears.

2. Type **mcpcfg** and press **Enter**.
   Result: The Gateway Configuration Utility menu appears.
3. Select option **3. Configure Network Interfaces**.
   Result: The Available Network Interfaces sub-menu appears.
4. Select option **7. Custom Routing**.
   Result: The Custom Routes Configuration Settings sub-menu appears.
5. Select option **2. Add Custom Route**.
6. Enter the **Destination IP Address** and press **Enter**.
   Result: You are prompted: **Is Destination IP an individual host: [Y/N]?**
7. Type **Y** or **N** and press **Enter**.
8. If you enter **Y**, the destination is added as a single host.
9. If you enter **N**, you will then enter the destination subnet mask and press Enter
   Result: You are prompted: Do you want to add this route to an interface: [Y/N].
10. Type **Y** or **N** and press **Enter**.
11. If you select **Y**, the list of available subnets to the MCP appears.
12. If you select **N**, you add the gateway IP Address and press Enter.
    Result: The list of subnets available in MCP appears. You then select the destination subnet.
    Note: The IP Address of the Next hop router must be in the same subnet as the network of MCP that will be chosen; otherwise an error occurs.
13. Reboot the MCP. Result: The custom routing settings take effect.

Display Custom Routes

» To display custom routes:

1. Log into the MCP Utilities page.
   Result: The MCP #>> prompt appears.
2. Type **mcpcfg** and press **Enter**.
   Result: The Gateway Configuration Utility menu appears.
3. Select option **3. Configure Network Interfaces**.
   Result: The Available Network Interface sub-menu appears.
4. Select option **7. Custom Routing**.
   Result: The Custom Routes Configuration Settings sub-menu appears.
5. Select option **1. Display Custom routes**
   Result: The list of custom routes available in the MCP are displayed in tabular format.

Delete Custom Routes

» To delete Custom Routes:

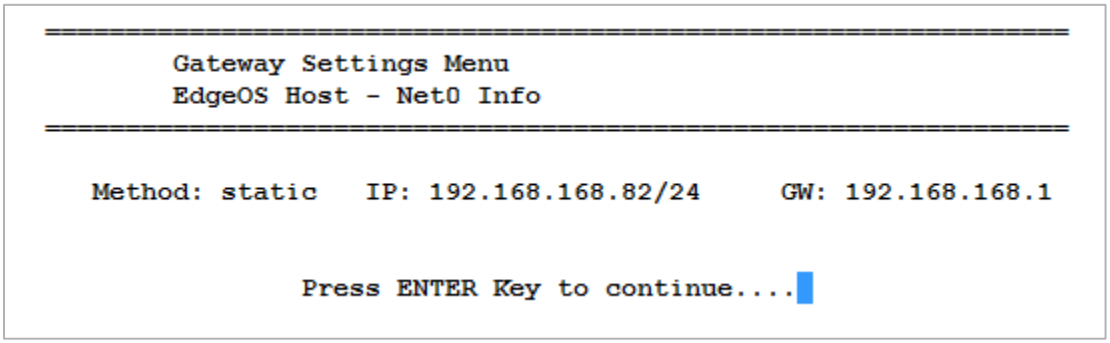
1. Log into the MCP Utilities page.
   Result: The MCP #>> prompt appears.
2. Type **mcpcfg** and press **Enter**.
   Result: The Gateway Configuration Utility menu appears.
3. Select option **3. Configure Network Interfaces.**
4. Select option **7. Custom Routing**.
   Result: The Custom Routes Configuration Settings sub-menu appears.
5. Select option **3. Delete Custom routes**.
   Result: The list of static routes configured in the MCP appears.

6. Select the static route to be deleted, e.g., **Select the Static route to delete [1-1]:**
7. Select the Subnet number of the route to be deleted and press **Enter**.
   Result: The selected static route is deleted.
8. Reboot the MCP. Result: The custom routing settings take effect.

Network Summary

The user can view a summary of all configured network interfaces in the MCP along with the type of interface.

Use MCP local configuration utility (mcpcfg) to access this feature.



Administrators User Management

The MCP from the factory has two default users.

1. Default Root User – **root** (root has all permissions to the MCP but only available via the serial maintenance port).
2. Default Administrator user – **defadmin** (restricted permissions - used for initial setup)

Note: There are no other default HMI users on a from factory MCP.

Default Users

defadmin

MCP supports a default administrator defadmin that is used to connect to MCP from SSH client and from the command line interface of Local HMI. The default password of default administrator user is **defadmin**. When user logins using defadmin, only minimal configuration (adding new administrator group user, adding new emergency group users, configuring network interface settings, rebooting the unit, restore snapshots using DSAS) will only be available. Using this Default Administrator User would need to configure a nominated/custom administrator-level user(s) to login and configure MCP.

- User: **defadmin**
- Password: **defadmin**

Steps to create New user:

1. After success login with defadmin/defadmin
2. Launch **sudo mcpcfg** => user will be prompted with the below message

```
defadmin@G500:~$ sudo mcpcfg
[sudo] password for defadmin:

                Please create an Administrator account in order to access the full mcpcfg menu.

                Press ENTER Key to continue....
```

Result: On Entering, configuration screen with below options will be displayed

```
================================================================================
        Gateway Settings Menu
================================================================================

        0.    Back
        1.    Configure Authentication
        2.    Configure Network Interfaces
        3.    Reboot Device

Enter Your Choice : ( Between 0 and 3 ):
```

3. Enter option 1, to create New user.

```
================================================================================
        Gateway Settings Menu
        Authentication
================================================================================

        Current AuthMode Status          : Local

        0.    Back
        1.    Administrator Group Users
        2.    Emergency Group Users

Enter Your Choice : ( Between 0 and 2 ):
```

4. Enter option 1, to see List Users.

```
================================================================================
        Gateway Settings Menu
        Authentication - Admin Group Users
================================================================================

        0.    Back
        1.    List Users
        2.    Add User
        3.    Change Password
        4.    Remove User

Enter Your Choice : ( Between 0 and 4 ):
```

5. Now **Enter 2** option to Add New user => here user is prompted provide the username and the password with which it must be created. Once done it will prompt with a note:

The defadmin user will be removed automatically once

1. *The defadmin user is logged out and*
2. *Logs in successfully with the newly added administrator user*

```
================================================================================
        Gateway Settings Menu
        Admin Group Users - Add user in Admin group
================================================================================


Enter user name : admin

Enter user's full name : admin

Enter the password for admin:
Re-enter the password :

You entered:
User Name      : admin
User Full Name : admin

Confirm that you want to add this user ? <Y/N> :        y


Successfully added user : admin


Note:
The defadmin user will be removed automatically once
1. The defadmin user is logged out and
2. Logs in successfully with the newly added administrator user

Press ENTER Key to continue....
```

Note: This happens when the device is logged in for the first time and trying to create the User.

7. Press Enter and option '0' to go back to previous menu screen.
8. Login with any of the newly added User. On successful Login the defadmin credentials will be deleted.

root

MCP supports a default **root** user that is used to connect to MCP from serial maintenance port. The default password for the **root** user is **geroot**.

> **NOTICE** **The root account password must be changed by end users, using MCP Local Configuration Utility (sudo mcpcfg).**

To configure users, go to the Configure Authentication option in mcpcfg, and select the authentication mode and change the system access settings. The Authentication settings are described in Table 4.6.

Table 4.5: Authentication setting descriptions

Setting	Description

Root Administrator Settings	Use this function to change the password associated with the system root user account.
Pass-Through Password Authentication	Use this function to enable or disable pass-through password authentication. When authentication is enabled, a valid username and password is required to access client applications through pass-through ports. Enabled by default.
Administrator Group Users	Use this function to create administrator-level users (if you are using local authentication mode) and to change details associated with existing administrator user accounts.
Emergency Group Users	This function allows user to add/delete/modify emergency administrator users for MCP. Adding emergency user is mandatory before changing the authentication from Local to Remote (LDAP /TACACS) Authentication. An emergency user can be used only when remote authentication has been enabled and only if the remote authentication server is not available. In this case emergency user will be allowed to login MCP and perform two key functions: 1. Change the mode authentication from remote to local mode 2. Generate emergency code to login HMI without changing authentication from remote to local mode. User can perform above two functions by using **"sudo emergcfg"** command after login emergency user on any of the below three interfaces: 1. SSH session to MCP (Port-922) 2. Maintenance serial port connection to MCP (Baud Rate- 115200) 3. MCP Emergency option in local console

Administrator Group Users

1. An Administrator Group user is created using the following menu. Enter option **1 Configure Authentication.**

```
================================================================
        Gateway Settings Menu
================================================================

        0.   Back
        1.   Configure Authentication
        2.   Configure Network Settings
        3.   Configure Network Interfaces
        4.   Configure Secure Access
        5.   Configure Firewall
        6.   Configure Host Names
        7.   Configure Time & Time Sync
        8.   Reset System Logs
        9.   Reset Database Tables
        10.  Reset File Persistence Data
        11.  Local HMI
        12.  Configure Sync Manager
        13.  Redundancy
        14.  ARRM
        15.  Suppress Forced Qualities To Masters
        16.  Emulate D20 RTU IEC101 DPA Unbalanced Mode Functionality
        17.  Configure IEC101+104 DPA Startup Quality Event Suppress Interval
        18.  Configure Serial Ports
        19.  Configure D.20 Port Settings
        20.  EdgeOS Host
        21.  Clear Chassis Intrusion State
        22.  Restore Clone Snapshot
        23.  Restore Factory Default
        24.  Reboot Device

Enter Your Choice : ( Between 0 and 24 ):
```

2. Enter option **3 Administrator Group User.**

```
================================================================
        Gateway Settings Menu   Authentication
================================================================

        Current AuthMode Status : Local

        0.   Back
        1.   Root Administrator Settings
        2.   Pass-Through Password Authentication
        3.   Administrator Group Users
        4.   Emergency Group Users

Enter Your Choice : ( Between 0 and 4 ):
```

3. Enter option **2 Add User.**

```
================================================================
        Gateway Settings Menu
        Authentication - Admin Group Users
================================================================

        0.   Back
        1.   List Users
        2.   Add User
        3.   Change Password
        4.   Remove User

Enter Your Choice : ( Between 0 and 4 ):
```

Emergency Group Users

The purpose of the emergency access is to allow user(s) to login to the MCP HMI in case of failure to connect to Remote Authentication servers when using LDAP and TACACS authentication mechanisms.

1. By using emergency group users, we can change from remote authentication mode to local authentication mode. Then user(s) are able to use local authentication mode user credentials to login into the runtime HMI (Local and Remote)
2. By using emergency group users, we can generate emergency access code, this generated emergency access code can be used to login into the runtime HMI (Local and Remote) as operator user role only.

NOTE:

1. At least one user must be present in the "Emergency Group users" to change the mode from local authentication to Remote Authentication. A dialog "Please add Emergency User before switching to LDAP/TACACS Authentication "will be present if this condition is not met.
2. The emergency group users are not allowed sudo ***su*** command from SSH port 922 and maintenance serial port to avoid root permissions to the MCP.
3. The emergency group users are not allowed to connect to SSH port 22 unless mapped in both administrator group users and emergency group users.
4. The logon for emergency group users will be allowed only when Remote Authentication is configured, and server(s) are not available.

An Emergency group User is created using the following menu. Enter option **1 Configure Authentication** and then option **4 Emergency Group Users.**

1. Enter 1 option to see the **List Users**

```
================================================================
        Gateway Settings Menu
        Authentication - Emergency Admin Group Users
================================================================

        0.   Back
        1.   List Users
        2.   Add User
        3.   Change Password
        4.   Remove User

Enter Your Choice : ( Between 0 and 4 ):
```

2. The list of users in Emergency group are displayed.

```
================================================================
        Gateway Settings Menu
        Emergency Group Users - List of users in Emergency group
================================================================

   User Name                          UID    Full Name
=====================================================================

1. emadmin                            1005   emergency administrator

            Press ENTER Key to continue....
```

3. Enter 2 option to **Add User**

```
================================================================
        Gateway Settings Menu
        Emergency Group Users - Add user in Emergency group
================================================================


Enter user name : emadmin1

Enter user's full name : Emergency Administartor

Enter the password for emadmin1:
Re-enter the password :

You entered:
User Name      : emadmin1
User Full Name : Emergency Administartor

Confirm that you want to add this user ? <Y/N> :        y


Successfully added user : emadmin1

Press ENTER Key to continue....
```

4. Enter 3 option to **Change Password**

```
================================================================
        Gateway Settings Menu
        Emergency Group Users - Change Password
================================================================


Enter user name : emadmin1
```

Next need to enter new password for the user

```
================================================================
        Gateway Settings Menu
        Setting password for emadmin1
================================================================


Enter the password for emadmin1:
Re-enter the password :

Successfully changed the password of emadmin1

Press ENTER Key to continue....
```

5. Enter 4 option to **Remove User**

```
================================================================
        Gateway Settings Menu
        Emergency Group Users - Delete user in Emergency group
================================================================


Enter user name to be deleted : admin1


Confirm that you want to delete user admin1 ? <Y/N> : [Y]y


Successfully deleted user : admin1

Press ENTER Key to continue....
```

Emergency Access User Configuration and Privileges:

Emergency Group Users can connect to MCP by using below three interfaces, only when remote authentication has been enabled and only if the remote authentication server is not available:

1. SSH session to MCP (Port-922)
2. Maintenance serial port connection to MCP
3. MCP Emergency option in local HMI console

After selecting any one interface then Emergency user can login in to MCP. After login got successful need use command **" sudo emergcfg"** .User can perform below two key functions.

1. Change the Authentication mode from remote to local mode
2. Generate Emergency Access code to login HMI without changing authentication from remote to local mode.

```
emadmin@G500:~$ sudo emergcfg
```

3. Below menu will come after " sudo emergcfg" command.

```
================================================
        Gateway Settings Menu
================================================

        0.   Back
        1.   Configure Authentication
        2.   Configure Emergency Access

Enter Your Choice : ( Between 0 and 2 ):
```

4. Change the Authentication mode from remote to local mode.

a. For Change the Authentication mode from remote to local mode enter option **1 Configure Authentication**.

```
=======================================================
        Gateway Settings Menu   Authentication
=======================================================

        Current AuthMode Status : Remote(TACACS+)

        0.   Back
        1.   Local Authentication mode

Enter Your Choice : ( Between 0 and 1 ):
```

b. Enter option 1 for **Local Authentication mode**

```
=======================================================
        Gateway Settings Menu   Authentication
=======================================================

 Gateway Emergency Local Authentication Menu
 ------------------------------------------

        0.  Back
        1.  Enable Local Authentication

Enter Your Choice : ( Between 0 and 1 ): 1
```

c. Enter option 1 to **Enable Local Authentication** and enter **Y (yes).**

```
=================================================
       Gateway Settings Menu   Authentication
=================================================

 Gateway Emergency Local Authentication Menu
 ------------------------------------------

       0.  Back
       1.  Enable Local Authentication

Enter Your Choice : ( Between 0 and 1 ): 1


All Emergency Users will be logged off automatically after local authentication is enabled

Are you sure you want to enable local authentication [Y/N]?:    y

Moved to Local Authentication Mode.
Please use Local Authentication credentials to login
All Emergency Users will now be logged off..
```

d. Here Authentication mode is change from Remote to Local. We can use Local authentication Users to login in to DSAS, HMI.

5. To generate Emergency Access code. Enter option **2 Configure Emergency Access** from main menu.

```
================================================================
        Gateway Settings Menu
        Configure Secure Access
================================================================

        0.   Back
        1.   Generate Emergency Access Code

Enter Your Choice : ( Between 0 and 1 ):
```

6. Enter option **1 Generate Emergency Access Code**.

```
Generating Emergency Access Code
Access code : A8DD41XEOFV4C28605HW
Status      : Valid


Press ENTER Key to continue....
```

7. Run the Runtime HMI and use the above access code to login HMI when Remote Authentication servers are not available/not reachable. Here we need to reopen the HMI enter the Host IP details then it will open window like below:

8. Here we need to enter emergency access code then HMI will open in emergency operator.

NOTE: Generated emergency access code will be valid for 5 minutes and once we used in HMI login then code will be cleared.

9. If code is generated and not used and again trying to generate new code within 5 min duration. Then message will be shown as "Emergency access code is already generated" like below:

```
================================================================
        Gateway Settings Menu
        Configure Secure Access
================================================================

        0.   Back
        1.   Generate Emergency Access Code

Enter Your Choice : ( Between 0 and 1 ): 1

        Emergency access code is already generated
        Access code : YT5E9D168IDBHO5PB923
        Status      : Valid


Do you want to re-generate emergency access code [Y/N]?:
```

User Management Overview

The User Management tab on the **Configuration** page in MCP Runtime HMI allows you to set up accounts for MCP users, including user names, passwords and access level.

Add a User

» To add a user:

1. Click **Add** to create a new user account.
   Result: The Add User window appears.
2. Enter the user information.

3. Click **OK**.
   Result: The User Management table is saved.

Change a User Account

» To change a user account:

1. Click on the user record from the list in the User Management table.
   Result: The Update User window appears.
2. Change the user information as required.
3. Click **OK**.
   Result: The User Management table is saved.

Delete a User

» To delete a user:

1. Click on a user record from the list in the User Management table.
   Result: The Update User window appears.
2. Click **Delete**.
   Result: The Delete confirmation popup appears.
3. Click **Yes** to confirm the deletion.

Configure User HMI Home Page

» To configure the User Homepage:

1. Click on the user record from the list in the User Management table.
   Result: The Update User window appears.
2. Update the user information as required.
3. Select the user Home Page from the dropdown list.
4. Click **OK**. Result: The User Management table is saved.

NOTE:

1. For existing configured users, the User Home Page can be changed from the dropdown list directly. There are no "Save" or "Commit" actions required. The changes take effect when navigating away from the page.
2. The successful login and display of the intended page depend on the configured user's access rights. i.e. When attempting to access a page, which requires higher user right level than the one used in the session – a message of "Access Forbidden" is displayed.
3. If the "User Defined Screens" is selected, users can specify additional parameters for example: dra=<dra filename>

Auto Login

The MCP allows users to view a custom UI page both for Local and Remote HMIs sessions after a successful login; for example: when choosing a one-line drawing (.dra file) or ActiveAlarmViewer.

The User Home Page field is available under the **Access/User Management** tab, allowing users to select a home page for each configured user. See the User Management section for configuring a custom UI page per user.

Log in to Specific Custom UI Page in Remote HMI when Auto Login is DISABLED

Logging into a Specific Custom UI Page in Remote HMI mode upon successful login follows the below priority when Remote UI Auto Login is disabled (to disable Remote UI Auto Login refer to section: >> Access > Automatic Login) in the DS Agile MCP Studio:

1. User Home Page configured in the User Management tab.
2. **RemoteUIMainPage** is configured in the **Systemwide**-> Runtime GUI-> Global configuration settings when User Home Page is not selected.

   Default Home Page when above (1) and (2) are not configured.

Log in to Specific Custom UI Page in Remote HMI when Auto Login is ENABLED

Logging into a Specific Custom UI Page in Remote HMI upon successful login follows the priority below when Remote UI Auto Login is enabled. (To enable Remote UI Auto Login, refer to section: >> Access -> Automatic Login) in the DS Agile MCP Studio.

1. **RemoteUIMainPage** is configured in the Systemwide-> Runtime GUI -> Global configuration settings.
2. User Home Page configured in the User Management tab settings when **RemoteUIMainPage** is not selected.
3. Default Home Page when above (1) and (2) are not configured

NOTE: When Remote UI Auto Login is enabled – remote users can still logout from the default auto login account and log back with different credentials, within the "Remote UI Automatic Login Wait Time"; in this case, the Specific Custom UI Page will be associated with the User Home Page as a priority, if configured.

Log in to Specific Custom UI Page in Local HMI when Auto Login is DISABLED

Logging into a Specific Custom UI Page in Local HMI follows upon successful login the below priority when Auto Login is disabled. (To disable Local UI Auto Login, refer to section: >> Access -> Automatic Login) in the DS Agile MCP Studio.

1. User Home Page configured in the User Management tab.
2. If User Home Page is not configured, then
   a. If MCP redundancy is not configured, then **LocalUIMainPage** configured in the Systemwide -> Runtime GUI -> Global configuration settings.
   b. Or, if MCP redundancy is configured and the designation of MCP is Gateway A, then **LocalUIMainPageA** configured in the Systemwide -> Runtime GUI -> Global configuration settings.
   c. Or, if MCP redundancy is configured and the designation of MCP is Gateway B, then LocalUIMainPageB configured in the Systemwide -> Runtime GUI -> Global configuration settings.
3. Default Home Page when above (1) and (2) are not configured.

Log in to Specific Custom UI Page in Local HMI when Auto Login is ENABLED

Logging into a Specific Custom UI Page in Local HMI upon successful login follows the below priority when Auto Login is enabled. (To enable Local UI Auto Login; refer to section: >> Access -> Automatic Login in the DS Agile MCP Studio

1. If MCP redundancy is not configured, then
   a. **LocalUIMainPage** configured in the Systemwide -> Runtime GUI -> Global configuration settings.
   b. User Home Page if **LocalUIMainPage** is not configured.
   c. Default Home Page when above (a) and (b) are not configured.
2. Or, if MCP redundancy is configured and the designation of MCP is Gateway A, then

   a. **LocalUIMainPageA** configured in the Systemwide -> Runtime GUI -> Global configuration settings.
   b. User Home Page if **LocalUIMainPageA** is not configured.
   c. Default Home Page when above (a) and (b) are not configured.
3. Or, if MCP redundancy is configured and designation of MCP is Gateway B, then
   a. **LocalUIMainPageB** configured in the Systemwide -> Runtime GUI -> Global configuration settings.
   b. User Home Page if **LocalUIMainPageB** is not configured.
   c. Default Home Page when above (a) and (b) are not configured.

NOTE: When Local UI Auto Login is enabled – local users can still logout from the default auto login account and log back with different credentials, within the "Local UI Automatic Login Wait Time"; in this case, the Specific Custom UI Page will be associated with the User Home Page as a priority, if configured.

Other Services/Settings

Configure Remote HMI Non-Observer Privileges

This feature prevents users with MCP operator and supervisor role (class) credentials from logging into the MCP from the Remote HMI and consequently prevents them from executing commands and other controllable actions (force, ACK alarms, etc.), or from changing configurations.

When this feature is enabled, all Remote HMI users are granted the observer role (class) after successful login. There is no impact on users logged in through Local HMI.

This feature is enabled or disabled using the Gateway Configuration Utility (mcpcfg). For security reasons, only a super user or users with elevated admin class privileges in Linux mcpcfg can update the configuration of this feature.

NOTE: When Redundancy is configured, this parameter must be enabled or disabled both in the Active MCP and the Standby MCP for proper operation.

Disable controls from Remote HMI procedure

To disable controls from Remote HMI:

1. Log into the MCP through serial maintenance port or KVM.
   Result: The **MCP#>>** command prompt appears.
2. Type **mcpcfg** and press **Enter**.
   Result: The Gateway Configuration Utility Menu appears.
3. Select option 4. Configure Secure Access.
   Result: The **Secure Access** sub-menu appears.
4. Select option 4. Configure Remote HMI Non-Observer Privileges.
   Result: The following message appears:

Currently Remote HMI Non-Observer privileges are Enabled.

IMPORTANT!!!

Disabling Remote HMI Non-Observer privileges will log off all Non-Observer remote HMI sessions.

Do you want to disable Remote HMI Non Observer privileges [Y/N]?

```
=====================================================================
        Gateway Settings Menu
        Secure Access - Configure Remote HMI Non Observer Privileges
=====================================================================


Currently Remote HMI Non Observer privileges are Enabled.


IMPORTANT !!!
Disabling Remote HMI Non Observer privileges will log off all
Non Observer remote HMI sessions.

Do you want to disable Remote HMI Non Observer privileges [Y/N]?:
```

5. If you enter **Y**, then the controls from the Remote HMI are disabled.

   If you enter **N**, then the controls from the Remote HMI are not disabled.

   Result: The settings take effect.

```
=====================================================================
        Gateway Settings Menu
        Secure Access - Configure Remote HMI Non Observer Privileges
=====================================================================


Currently Remote HMI Non Observer privileges are Enabled.


IMPORTANT !!!
Disabling Remote HMI Non Observer privileges will log off all
Non Observer remote HMI sessions.

Do you want to disable Remote HMI Non Observer privileges [Y/N]?:       y


Settings have been saved and applied

Press ENTER Key to continue...
```

Enable controls from Remote HMI procedure

To enable controls back from Remote HMI:

1. Log into the MCP through serial maintenance port or KVM.
   Result: The **MCP#>>** command prompt appears.
2. Type **mcpcfg** and press **Enter**.
   Result: The Gateway Configuration Utility Menu appears.
3. Select option 4. Configure Secure Access.
   Result: The Secure Access sub-menu appears.
4. Select option 4. Configure Remote HMI Non-Observer Privileges.
   Result: The following message appears:

Currently Remote HMI Non Observer privileges are Disabled.
Do you want to enable Remote HMI Non Observer privileges [Y/N]?
If you enter **Y**, then the controls from the Remote HMI are enabled.
If you enter **N**, then the controls from the Remote HMI is not enabled.

5. Result: The settings take effect.

Configure Rsyslog service

The MCP can be configured to accept system logs from an IED or any substation equipment that can support the syslog remote logging feature. The MCP supports both TCP- and UDP-based remote connections to the IEDs on the standard port numbers.

When configuring Rsyslog service in a redundant MCP setup:

1. Start configuring Rsyslog service in the Active MCP (see section: Rsyslog service configuration procedure).
2. Reboot the device. Rebooting the device initializes Rsyslog with the newly committed configuration.
3. Once Active MCP is back online, sync the configuration to the Standby MCP and reboot the Standby MCP as well. This ensures that both Active MCP and Standby MCP configurations and firewall settings are in sync.

NOTICE

The MCP Rsyslog service changes the firewall settings to allow messages/logs on the configured port numbers for UDP/TCP based connections. These rules update the Firewall rulesets once configured and rebooted.

While choosing a different port number configured for either TCP/UDP based connections, ensure that no other application is using/running with the same port number in the MCP.

In the firewall configuration, it is the user's responsibility to connect Internal zone interfaces to networks that are protected from unauthorized use.

Rsyslog service configuration procedure

To configure Rsyslog Service:

1. Navigate to the Rsyslog Service configuration menu.

   Choose option 4. Configure Secure Access > 5. Configure Rsyslog Service.

   Result: The **Configure Rsyslog Service** menu appears.

2. Choose option **1. Current Settings** to view the current settings configured.
3. Return to the Configure Rsyslog Service menu.
4. Choose option 2. Configure Rx via UDP.

   Result: Receiving Messages via UDP - Settings menu appears.

```
================================================================================
        Gateway Settings Menu
        Secure Access - Configure Rsyslog service
================================================================================

        0.   Back
        1.   Current Settings
        2.   Configure Rx via UDP
        3.   Configure Rx via TCP
        4.   Configure Hosts/Subnets filters

Enter Your Choice : ( Between 0 and 4 ):
```

5. Choose option 1. Enable/Disable Rsyslog Logging service

   By default, syslog UDP uses the 514-port number. If this is to be changed, choose option **2. Edit UDP Port Number**.

```
================================================================================
        Gateway Settings Menu
        Configure Rsyslog service - Receiving Messages via UDP - Settings
================================================================================

        0.   Back
        1.   Enable/Disable Rsyslog Logging service
             (Reception of Messages via UDP)
        2.   Edit UDP Port Number

Enter Your Choice : ( Between 0 and 2 ):
```

NOTE: Before proceeding with this step, ensure that no other MCP applications/services are using the same port number. You can do this by manually checking the Connections tab of the MCP web/local HMI.

6. Return to the Configure Rsyslog Service menu.
7. Choose option 3. Configure Rx via TCP.

   Result: The Receiving Messages via TCP - Settings menu appears.

```
================================================================================
        Gateway Settings Menu
        Secure Access - Configure Rsyslog service
================================================================================

        0.   Back
        1.   Current Settings
        2.   Configure Rx via UDP
        3.   Configure Rx via TCP
        4.   Configure Hosts/Subnets filters

Enter Your Choice : ( Between 0 and 4 ):
```

   The configuration options are like UDP.

```
================================================================
        Gateway Settings Menu
        Configure Rsyslog service - Receiving Messages via TCP - Settings
================================================================

        0.    Back
        1.    Enable/Disable Rsyslog Logging service
              (Reception of Messages via TCP)

        2.    Edit TCP Port Number

Enter Your Choice : ( Between 0 and 2 ):
```

8. Return to the Configure Rsyslog Service menu.
9. Choose option 4. Configure Hosts/Subnets filters.

   Result: The Configure Hosts/Subnets filters menu appears.

```
================================================================
        Gateway Settings Menu
        Secure Access - Configure Rsyslog service
================================================================

        0.    Back
        1.    Current Settings
        2.    Configure Rx via UDP
        3.    Configure Rx via TCP
        4.    Configure Hosts/Subnets filters

Enter Your Choice : ( Between 0 and 4 ):
```

   This setting allows the MCP Rsyslog service to bind to the subnet/Host address. By default, no binding filter rules are applied. That is, the MCP syslog application logs messages being pushed IEDs connected through all available MCP's network interfaces.

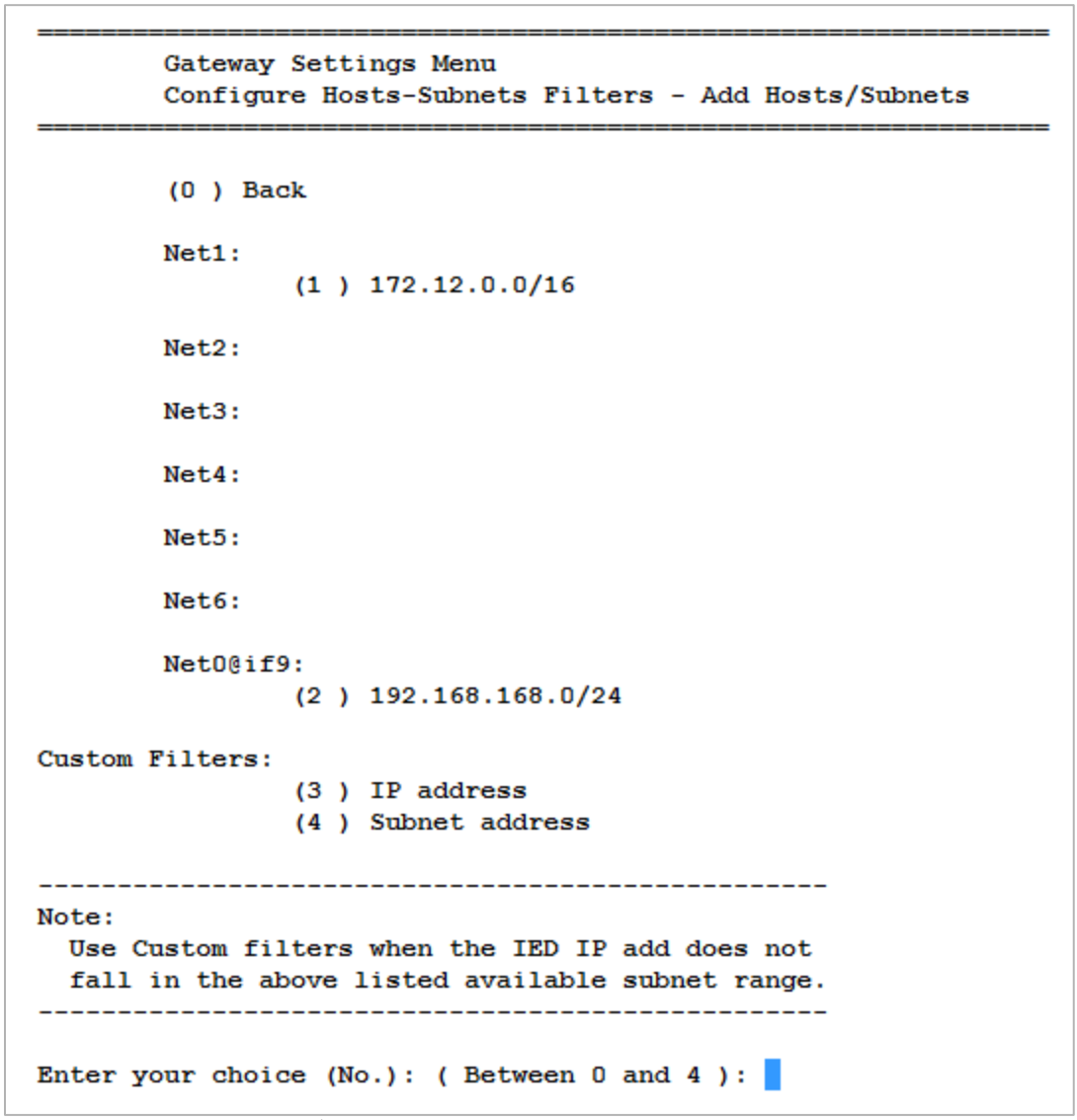
10. Choose option 2. Add Hosts/Subnets to add Subnets and IP Address of the Hosts/IEDs.

```
================================================================
        Gateway Settings Menu
        Configure Rsyslog service - Configure Hosts-Subnets Filters
================================================================

        0.    Back
        1.    Current Settings
        2.    Add Hosts/Subnets
        3.    Delete Hosts/Subnets

Enter Your Choice : ( Between 0 and 3 ):
```

11. Select the applicable interface from the list of available interfaces in the MCP.

    If the subnet is missing in the list, choose one of the Custom Filters options.

    Adding a subnet configures the MCP Rsyslog to log messages only being sent from the IED-IP Addresses which are in range of the configured subnet.



12. Choose option 3. Delete Hosts/Subnets to delete any of the added addresses.
13. Choose option 1. Current Settings to view the current settings configured.

Configure Secure Access

SECURITY NOTICE: HTTPS, SFTP, and SSH services are automatically configured in MCP by default.

The **Configure Secure Access** menu allows you to configure the modes through which users can access the MCP.

Table 4.6: Secure access setting descriptions

Setting	Description
Current Configuration	Use this function to view the current state of the MCP secure access settings.
Configure SSH Service	Use this function to enable or disable access to the MCP through the SSH protocol for Pass Through and Terminal Server Connections
Configure SFTP Service	Use this function to enable or disable access to the MCP through the Secure FTP protocol **Note**: When transferring files to and from the MCP, you may receive file permission errors. Disable "permission change error reporting" in your file transfer utility to prevent these messages from appearing.
Configure Emergency Access ports	Use this function to configure Access ports: • Display and serial maintenance port • Display port only • Serial maintenance port only
Configure Remote HMI Non-Observer Privileges	Use this command to enable or disable privileges for the Non-Observer users from the Remote HMI. It is necessary to reboot the MCP after configuring this parameter. If redundancy is configured, this parameter must also be configured in the Standby MCP.
Configure Rsyslog Service	Use this command to enable or disable Remote Syslog service in the MCP. Rsyslog service supports the following features: • Receiving of Syslog Messages through UDP. • Receiving of Syslog Messages through TCP. • Add or Delete Subnets/Hosts for receiving Syslog Messages. **Note**: The MCP Rsyslog service changes the firewall settings to allow messages/logs on the configured port numbers for UDP/TCP based connections. These rules update the Firewall rulesets once configured and rebooted. While choosing a different port number configured for either TCP/UDP based connections, ensure that no other application is using/running with the same port number in the MCP. In the firewall configuration, it is the user's responsibility to connect Internal zone interfaces to networks that are protected from unauthorized use.

```
================================================================================
        Gateway Settings Menu
        Configure Secure Access
================================================================================

        0.   Back
        1.   Current Configuration
        2.   Configure SSH Service
        3.   Configure SFTP Service
        4.   Configure Emergency Access Ports
        5.   Configure Remote HMI Non Observer Privileges
        6.   Configure Rsyslog Service

Enter Your Choice : ( Between 0 and 6 ):
```

Configure Firewall

The MCP contains a firewall capable of stateful packet inspection to protect your device from unauthorized access. By default, network interfaces on the MCP drop packets that are determined to be invalidly routed or unsolicited.

SECURITY NOTICE: The MCP firewall is intended only to protect itself and does not extend protection to other devices on the network. As such, it does not replace the need for a network firewall which offers deep packet inspection and detailed configuration capabilities.

The MCP firewall is automatically configured by default to its most secure setting. The user assumes all responsibility for associated security risks if the firewall configuration is manually changed.

It is the user's responsibility to connect Internal zone interfaces to networks that are protected from unauthorized use.

Also, if the firewall is disabled then all the ports that are internal to the MCP will be visible/available to the external scanner tools.

Network interfaces can operate in one of two modes:

Internal : The Internal mode permits traffic from known protocols and should only be enabled on interfaces connected to known devices only. The Internal mode is typically used when the interface is connected to the substation LAN.

External : The External mode offers a stricter set of rules and is the default mode for all interfaces except Net0 and Net1. The External mode would typically be used when the interface is connected to a WAN.

By default, the firewall allows outbound traffic on internal interfaces and blocks all outbound traffic except outbound SSH on external interfaces. If you want the firewall to allow outbound traffic for a protocol on an external interface, you must create a "custom" rule. See section: Add/Edit/Remove Custom Rules.

By default, the firewall blocks inbound traffic on both internal and external interfaces. The MCP automatically generates rules allowing inbound traffic on internal interfaces for all configured services. If you want the firewall to allow inbound traffic on an external interface, you may modify the associated "generated" rule to allow the traffic on ALL interfaces rather than only the "Internal" interface. See section: Add/Edit/Remove Custom Rules.

Table 4.7: Service traffic defaults through the firewall

Service Name	Notes	External Mode	Internal Mode
Modbus/TCP Server (Inbound)		Deny	Allow

DNP/UDP Server (Inbound)		Deny	Allow
DNP/TCP Server (Inbound)		Deny	Allow
DNP/TCP Client (Inbound)	Dual Endpoint Enabled	Deny	Allow
DNP/UDP Client (Inbound)			
IEC 60870-5-104 Server (Inbound)		Deny	Allow
Terminal Server (Inbound)	TLS Disabled	Deny	Allow
DCA Pass-Through (Inbound)	TLS Disabled	Deny	Allow
Secure Connection Relay (Inbound)		Allow	Allow
Secure DCA Pass-Through (Inbound)	TLS Enabled	Allow	Allow
Secure Terminal Server (Inbound)	TLS Enabled	Allow	Allow
SNMP Client (Inbound)		Deny	Allow
LogicLinx Executor (Inbound)		Deny	Allow
HTTPS (Inbound)	When enabled in mcpcfg, see note below	Deny	Allow
DHCP Client (Inbound)	When enabled in mcpcfg	Deny	Allow
NTP Client (Inbound)	When enabled in mcp	Deny	Allow
NTP Server (Inbound)	When enabled in mcpcfg	Deny	Allow
SSH/SFTP/SCP (Outbound)	When enabled in mcpcfg for SCP/SFTP.	Allow	Allow
Secure Tunnel -Redundancy (Inbound)	When enabled in mcpcfg	Deny	Allow
Standby Local HMI Redirection to Active (Inbound)	When enabled in mcpcfg	Deny	Allow
Settings GUI(Inbound)		Deny	Allow
Emergency SSH Server (Inbound)		Deny	Allow
Emergency SSH Serve (Outbound)		Allow	Allow
LDAP Client (Outbound)		Allow	Deny
Modbus/TCP Server (Inbound)		Deny	Allow
DNP/UDP Server (Inbound)		Deny	Allow
DNP/TCP Server (Inbound)		Deny	Allow
Note: By default, HTTPS and SSH do not provide strong client authentication since only a password is required to access the system. Therefore, these protocols are not considered secure enough for use over external interfaces. They can be considered secure if you employ a remote authentication server that provides two-factor authentication. In that case, you may opt to modify the firewall rule and allow HTTPS and SSH on external interfaces.			

The default firewall rules should be enough for most users. However, you may create a set of custom rules if you desire more granular permissions for the protocols you are accessing.

These firewall rules in the table are used for whitelisting the IP connections and ports on the Network Interfaces.

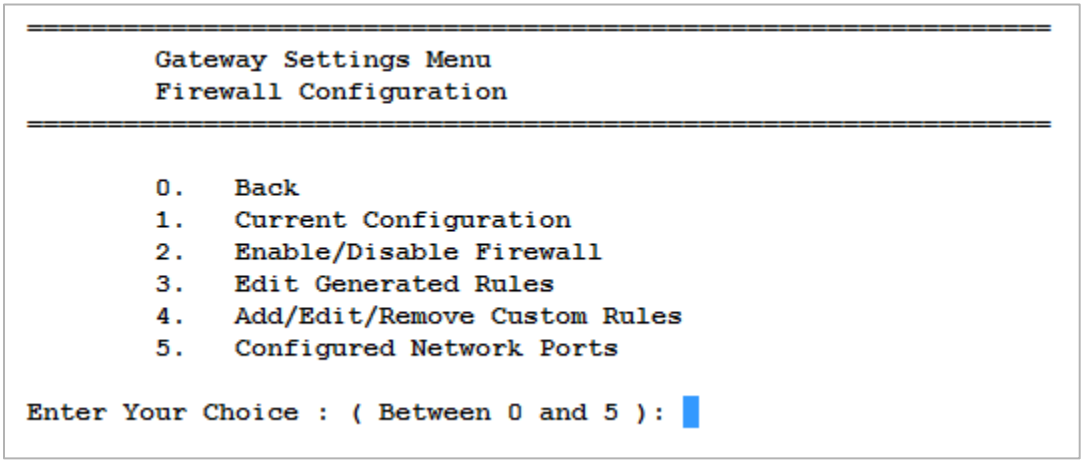
Additional notes on the MCP firewall:

- In a redundant setup, the same firewall rules above apply to both the active and standby device.
- When the firewall is active, you cannot perform IP routing between an external and internal interface. The only way to pass through the firewall is by using a secure TLS connection or the proxy.

Configure the settings of the firewall through the **Firewall** menu. The Secure Access settings are described in Table 4.9.

Table 4.8: Firewall setting descriptions

<table>
<tr><th>Setting</th><th>Description</th></tr>
<tr><td>Current Configuration</td><td>Use this function to view the status of the firewall and the rules currently being enforced.</td></tr>
<tr><td>Enable/Disable Firewall</td><td>Use this function to turn the firewall feature on or off. By default, the firewall is enabled when the MCP is received from the factory. If you disable the firewall, incoming traffic is not filtered.</td></tr>
<tr><td>Edit Generated Rules</td><td>When the firewall is active, rules are generated for the services in use on your MCP based on the parameters specified in the table above. Use this option to modify these generated rules.</td></tr>
<tr><td>Add/Edit/Remove Custom Rules</td><td>Use this option to create a custom firewall rule that is applied in addition to the system generated rules.</td></tr>
<tr><td>Configure Network Ports</td><td>List of Network ports listening on TCP:
<table>
<tr><th>Service</th><th>Port</th><th>Interfaces</th></tr>
<tr><td>SNMP</td><td>162</td><td>Internal</td></tr>
<tr><td>Modbus/TCP_Server</td><td>502</td><td>Internal</td></tr>
<tr><td>DNP/TCP_Server</td><td>20001</td><td>Internal</td></tr>
<tr><td>IEC_60870-5-104</td><td>2404</td><td>Internal</td></tr>
<tr><td>Web Server (Remote_HMI)</td><td>443</td><td>Internal</td></tr>
<tr><td>SSH_Inbound</td><td>22</td><td>Internal</td></tr>
<tr><td>SSH_Outbound</td><td>22</td><td>All</td></tr>
<tr><td>SSH_HOST_Inbound</td><td>922</td><td>Internal</td></tr>
<tr><td>SSH_HOST_Outbound</td><td>922</td><td>All</td></tr>
<tr><td>HotStandby</td><td>51000, 51001</td><td>Internal</td></tr>
<tr><td>SSH Tunnel WStdby IN</td><td>51003</td><td>Internal</td></tr>
<tr><td>SSH Tunnel WStdby OUT</td><td>51003</td><td>Internal</td></tr>
<tr><td>MCP Settings_Inbound</td><td>8081</td><td>Internal</td></tr>
<tr><td>SSH (EdgeOS_Shell)</td><td>22</td><td>Internal</td></tr>
<tr><td>Synch_to_and_from (DSAS)</td><td>22</td><td>Internal</td></tr>
<tr><td>Web_Server (PETC/EdgeManager)</td><td>443</td><td>Internal</td></tr>
</table>
Based on the configuration this list will be updated accordingly.</td></tr>
</table>



Configure Host Names

The **Configure Host Names** menu allows you to assign a host name to your MCP and to view, add, and delete entries in the hosts file. The Host Name settings are described in Table 4.10.

NOTE: The MCP only allows you to enter IPV4 addresses.

Table 4.9: Host name setting descriptions

Setting	Description
Add a New Host	Use this function to add a host name and IP Address to the host's file.
Delete a Host	Use this function to view a list of configured hosts. Select an item number to delete the associated host entry.
Modify a Host	Use this function to view a list of configured hosts. Select an item number to modify the associated host name and IP Address. Press Enter to use the previously entered value.
Delete All Hosts	Use this function to remove all entries from the hosts file.
View All Hosts	Use this function to view a list of configured hosts.

Configure Time & Time Sync

Refer to the section *Date and Time* for configuring Time & Time Sync

Reset System Logs

Use the **Reset System Logs** menu to clear various system logs that are stored in the MCP. The Reset System Log settings are described in Table 4.11.

Table 4.10: Reset System Log setting descriptions

Setting	Description
Check Size of Archived Logs	Active system logs are automatically archived when they reach a size of 256 KB. Up to 10 archives are kept within the MCP, with newer logs overwriting older stored logs. Check Size of Archived Logs lets you view the amount of disk space occupied by these archived log files. The value is shown in KB.
Check Size of Current Application Logs	Use this function to view the amount of disk space occupied by the current application logs. The value is shown in KB.
Delete Archived Logs	Use this function to permanently delete archived logs from the MCP.
Delete Current Logs	Use this function to permanently delete current application logs from the MCP.

Reset Database Tables

Modify tables in the SQL database through the **Reset Database Tables** menu. The Reset System Log settings are described in Table 4.12.

Use the DB Exporter tool on the Utilities page of the MCP HMI to save a backup of the SQL database tables before deleting them.

Table 4.11: Reset database table setting descriptions

Setting	Description
Delete Digital Event Data: SOE and Alarm records	Use this command to clear or delete the Digital Event Data from the SQL database of the MCP. • This action stops all running applications and permanently deletes entries from the digital events database. • If NVRAM based persistence is configured for SOE and Alarm records, also reset NVRAM using mcpcfg.
Delete Quality Records	Use this command to clear or delete the Quality Data from the SQL database of the MCP. The quality status and quality attributes (also referred to as the quality flags) are stored in the MCP SQL database along with the point or object and are updated as the status or value of the point or object changes.
Delete PRF Event Records	Use this command to clear or delete the Protective Relay Faults (PRF) stored in the SQL database of the MCP. All PRF fields including the Event ID, Trip Description, Fault code etc. are deleted permanently from the SQL database of the MCP.
Delete Operator Records	Use this command to delete the operator notes that have been entered by users and stored in the SQL database of the MCP. Each Operator Note record entered in the SQL database of the MCP contains a custom Note/Text message entered by an operator. This record also contains the last modified record date and time details.
Delete Accumulator Records	Use this command to clear or delete the Accumulator records from the SQL database of the MCP.

```
================================================================================
        Gateway Settings Menu
        mSQL Tables
================================================================================


WARNING: The Gateway applications will be stopped during
 delete operations and restarted!!!

        0.   Back
        1.   Delete Digital Event Data : SOE and Alarm records
        2.   Delete Quality records
        3.   Delete PRF Event records
        4.   Delete Operator Note records
        5.   Delete Accumulator records

Enter Your Choice : ( Between 0 and 5 ):
```

NOTE: If redundancy is configured, it is required to perform same operations on PEER gateway as well.

```
================================================================
        Gateway Settings Menu
        mSQL Tables
================================================================


WARNING: The Gateway applications will be stopped during
 delete operations and restarted!!!

        0.   Back
        1.   Delete Digital Event Data : SOE and Alarm records
        2.   Delete Quality records
        3.   Delete PRF Event records
        4.   Delete Operator Note records
        5.   Delete Accumulator records

Enter Your Choice : ( Between 0 and 5 ): 1

This will stop all applications and permanently delete
entries from the digital events database

Are you sure you want to do this? <Y/N> ?       y

Stopping all applications on Gateway...

Note:Redundancy is configured.It is required to perform same operations on peer Gateway as well.

Are you sure you want to restart applications now? <Y/N> ?      y

Restarting all applications on Gateway...

Press ENTER Key to continue...
```

Reset File Persistence Data

You can reset the data being held in the MCP's database with the File Based Persistence setting provided through the Reset File Persistence Data menu. Reset File Persistence Data Settings

Use this command to reset the data being stored by the File Based Persistence application in the MCP. This command permanently deletes data stored in the Persistence Files of the MCP.

After you have reset the data stored in the Persistence Files, you must restart the MCP. It is advised to restart the File Based Persistence application when the **mcpcfg** prompts for user action.

Local HMI

You can configure the settings of the monitor connected to display port of the MCP output through the **Local HMI** menu. The Local HMI settings are described in Table 4.13.

Table 4.12: Local HMI setting descriptions

Setting	Description
Current Settings	Use this command to view the existing Local HMI Settings.
DPMS	Use this function to enable or disable DPMS (Display Power Management Signaling). These settings determine how much time must pass without user interaction before your monitor is put into a reduced power mode. A setting of "00" prevents the MCP from triggering the power mode. The following modes are available: • **Stand-by:** Monitor blanks but power supply remains on; screen restores in

	approximately one second when reactivated by keyboard or mouse input by user. • **Suspend:** Monitor power supply shuts off; screen restores in approximately 2-3 seconds. • **Turned off:** Monitor is fully powered down except for an auxiliary circuit to detect a wake-up signal; screen restores in approximately 8-10 seconds **Note**: Refer to the manual that came with your monitor for more information on how it receives and responds to DPMS signals.
Standby Local HMI (Redundancy)	Use this command to enable or disable Standby Local HMI redirects to the Active MCP feature. **Note**: This parameter must be configured in both MCPs for proper operation. This feature is not available in G100.

```
================================================================================
        Gateway Settings Menu
        Local HMI
================================================================================

        0.   Back
        1.   Current Settings
        2.   DPMS
        3.   Standby Local HMI (Redundancy)

Enter Your Choice : ( Between 0 and 3 ):
```

Standby local HMI redirects to the active MCP

This feature applies to redundant MCP units, where both MCPs are equipped with a Local HMI. When this feature is enabled, it is recommended to enable auto-login in both the redundant MCP units.

If the MCP units are configured in non-redundant configuration, this feature is not applicable.

This feature allows a user to interact with the Local HMI of the active MCP of both units at the same time, allowing two separate Local HMIs to show data from the same active MCP.

When auto-login is enabled, the Local HMI screens of redundant MCPs display default pages as per their designation (Gateway_A or Gateway_B) and the configured Local UI Main Page for Gateway_A / Gateway_B. This allows the Local HMI screen of a MCP to display same UI page, regardless of its active or standby state.

Table 4.13: Redundant MCP display default pages

MCP Designation	Default UI Page as per Parameter
GatewayA	Local UI Main Page for GatewayA (MCP)
GatewayB	Local UI Main Page for GatewayB (MCP)

These parameters can be configured using **MCP** Configuration **GUI > Systemwide > Runtime GUI > Global configuration** tab in DS Agile MCP Studio.

NOTES:

- The Standby HMI redirects to Active MCP parameter must be enabled or disabled both in Active and Standby MCPs for proper operation.
- When auto-login is not enabled, the Local HMI screens of redundant MCPs display the configured User Home page in the User Management Tab. Refer to the MCP Software Configuration Guide for details.
- Standby Local HMI redirecting to Active MCP depends on the configured PEER MCP IP Addresses and Keys transferred to the PEER MCP but is independent of the Heart Beat communications options.

- The Local HMI on the Standby MCP behaves same as Local HMI on the Active MCP for all access purposes. As a result, the Configure Remote HMI Non-Observer Privileges feature does not take effect on the StandbyMCP.
- The Utilities Login feature to login to the Standby MCP only though the Local HMI is redirected to the Active MCP.
- The Export Database feature in MCP Utilities downloads the database into the USB mounted on the Standby MCP.
- The Export Database CSV Files feature in MCP Utilities stores the files on the Standby MCP.
- If Serial Only heart-beat option is configured in Warm Standby Redundancy, then both PEER User and IP Address needs to be configured in both the MCPs using mcpcfg to make Standby Redirects to Active functional.

To enable Standby Local HMI redirects to Active MCP:

1. Log into the MCP Utilities page.

   Result: The **MCP#>>** command prompt appears.

2. Type **mcpcfg** and press **Enter**.

   Result: The Gateway Configuration Utility Menu appears.

3. Select option **11. Local HMI**.

   Result: The **Local HMI** sub-menu appears.

4. Select option 3. Standby Local HMI (Redundancy).

   Result: The following prompt appears:

   IMPORTANT!

   *** Currently Redundancy configuration is Disabled.**

   *** Active Gateway Access from Standby Local HMI configuration is applicable only when Redundancy is Enabled.**

   *** Number of simultaneous users must be a minimum of 2 for the configured user role in both Gateways, which can be configured from HMI (Configuration > Systemwide > AccessManager) menu.**

   Currently Active Gateway Access from Standby Local HMI is Disabled.
   Are you sure you want to Enable Active Gateway Access from Standby Local HMI [Y/N]?

5. If you enter **Y**, then this feature is enabled.

   If you enter **N**, then this feature is not enabled.

```
============================================================
        Gateway Settings Menu
        Standby Local HMI (Redundancy)
============================================================


IMPORTANT !
* Currently Redundancy configuration is Disabled.

* Active Gateway Access from Standby Local HMI configuration
  is applicable only when Redundancy is Enabled.

* Number of simultaneous users must be minimum 2 for the
  configured user role in both Gateways which can be configured
  from HMI(Configuration->Systemwide->AccessManager) menu.



Currently Active Gateway Access from Standby Local HMI is Disabled

Are you sure you want to Enable Active Gateway Access from Standby Local HMI [Y/N]?:y


Settings have been saved and applied

Press ENTER Key to continue...
```

To disable Standby Local HMI redirects to Active MCP:

1. Log into the MCP Utilities page.

   Result: The **MCP#>>** command prompt appears.

2. Type **mcpcfg** and press **Enter**.

   Result: The Gateway Configuration Utility Menu appears.

3. Select option **11. Local HMI**.

   Result: The Local HMI sub-menu appears.

4. Select option 3. Standby Local HMI (Redundancy).

   Result: The following prompt appears:

   Currently Active Gateway Access from Standby Local HMI is Enabled.
   Are you sure you want to Disable Active MCP Access from Standby Local HMI [Y/N]?

5. If you enter **Y**, then this feature is disabled.
6. If you enter **N**, then this feature is not disabled.

Configure Sync Manager

The Configure Sync Manager utility can be used to securely copy files from a location on your MCP device to a specified directory on a remote device. The utility monitors the specified local directory for changed or added files. To reduce bandwidth demands on your network, only files found to have been changed or created since the last synchronization are transferred. This utility employs the Linux-based rsnyc/ftp/sftp command to perform this function.

You can configure the settings of the Sync Manager through the **Sync Manager** menu. The Sync Manager settings are described in Table 4.15.

Reboot the MCP after the Sync manager configuration is complete.

Table 4.14: Sync Manager setting descriptions

Setting	Description
Enable Sync Manager	Use this command to enable the Sync Manager application. This command deletes the old pair of Public-Private Keys and generates a new pair of Public-Private Keys. The existing/newly generated keys are available at: /mnt/datalog/SSHKeys/SyncMgr/id_rsa. This command provides an option to configure the "sync set" through the rsnyc, ftp, and sftp features. Rsync is a software utility and network protocol for Unix-like systems (with a port to Microsoft Windows) that synchronizes files and directories between one location and another location while minimizing data transfer. It also includes the option to provide encrypted transfer by using the SSH. FTP (File Transfer Protocol) is a popular method of transferring files between two remote systems. SFTP (Secure File Transfer Protocol) is a separate protocol packaged with SSH that works in a similar way over a secure connection.
Generate SSH Authentication Keys	Files from the MCP are securely copied to the remote device over an SSH connection. To facilitate authentication on this link, a private/public key pair must be generated and transferred to the remote device. When a key set is generated, the files are stored in **/mnt/datalog/SSHKeys/SyncMgr/**. You should copy the public key file (id_rsa.pub) from this location and store it in the appropriate location on the remote device. Refer to the user documentation provided with your remote device to determine where this location is. Do not remove the private key from this location since the Sync Manager will not be able to establish a secure connection. You must copy the public key (or host fingerprint) from any remote device you are connecting to into the **/mnt/datalog/SSHKeys/SyncMgr/known_hosts/** folder on your MCP. This file likely has a ".pub" extension; refer to the user documentation provided with your remote device to determine where the key can be obtained. These keys are used with either rsync or sftp server for authentication. **NOTE:** In case if you are not able to access the folder, enter **sudo chmod ug+x /mnt/datalog/SSHKeys/SyncMgr** from the command prompt as an **administrator user.**
Configure Sync Sets	Up to 8 sync sets can be created at any time. Table 4.16 lists the settings can be configured for each set:

Table 4.15: Settings for each sync set

Setting	Description	Range
Configure Server	File transfer to Enterprise server from MCP occurs on selected Protocol	Rsync, ftp, or sftp

Sync Set ID	A unique number used by the system to identify the sync set. Not editable; automatically assigned.	Auto-incremented from 1. Once a number has been assigned, it is never reused.
Destination IP Address	The IP Address of the remote device where the files are to be copied.	Valid IPv4 address
Destination Username	The username used for SSH authentication on the remote system.	1 to 128 ASCII characters
Password	The password required for establishing a session on FTP. This is not applicable to rsync and sftp protocols.	Text string; 1 to 22 characters Alphabetic letters, numbers 0 to 9, and special characters are allowed
Source Path Name	The absolute directory pathname that is synched to the remote device.	2 to 120 ASCII characters pointing to a valid location on the MCP file system
Destination Path Name	The absolute directory pathname that the files are to be copied to	2 to 120 ASCII characters pointing to a valid location on the remote device's file system
Check and sync Interval	The amount of time, in seconds, that the Sync Manager waits before checking the source path for changes. If changed or created files are detected, an rsync/ftp/sftp operation is triggered.	60 to 86400 seconds
Forced sync Interval	The amount of time, in seconds, that the Sync Manager waits before a forced sync operation is triggered, regardless of detected changes. If rsync is configured, then forced sync recreates files that have been deleted from the remote device as well as forcing the transfer of files whose changes may not have been detected due to MD5 collision, an extremely rare occurrence.	60 to 86400 seconds

Table 4.16: Sync Set Example 1

Field	Value
Configure Server	rsync
Sync Set ID	1
Destination IP Address	192.168.1.1
Destination User Name	admin
Password	xxxxxx
Source Path Name	/mnt/datalog/arrm
Destination Path Name	/cygdrive/c/Stations_Data
Check and sync Interval	60
Forced sync Interval	60

Table 4.17: Sync Set Example 2

Field	Value
Configure Server	rsync
Sync Set ID	2
Destination IP Address	192.168.1.2
Destination Username	admin
Password	xxxxxx
Source Path Name	/mnt/datalog/arrm
Destination Path Name	/cygdrive/c/Stations_Data/GW/Station_1/MCP_Name_1
Check and sync Interval	60
Forced sync Interval	60

Table 4.18: Sync Set Example 3

Field	Value
Configure Server	rsync
Sync Set ID	3
Destination IP Address	192.168.1.3
Destination Username	admin
Password	xxxxxx
Source Path Name	/mnt/datalog/arrm
Destination Path Name	/cygdrive/c/Stations_Data/GW/[Station_1,Station_2,Station_3]/MCP_Name_1
Check and sync Interval	60
Forced sync Interval	60

NOTE: The Sync Manager only copies files to the remote device. Files are not deleted from the remote device if they are deleted from the MCP after synchronization. Instead, they are recreated during the next sync operation.

A forced sync is performed upon each startup of your MCP device.

The MCP Designation Place holder %MCP_DESIGNATION is only to be used with redundant MCPs.

In the configured Syncset, ensure that the total text string length does not exceed 200 characters for the Source Path and Destination Path fields.

Redundancy

This feature is not available in G100.

If you are configuring your MCP for use within a redundant setup, you can configure redundancy application settings through the **Redundancy** menu. The Redundancy settings are described in Table 4.19.

Table 4.19: Redundancy setting descriptions

Setting	Description
Current Configuration	Use this command to view the current redundancy configuration.

Enable/Disable Redundancy	Use this function to enable or disable redundancy functionality within the MCP. **Redundancy Type** The available types of redundancy that can be configured are: • Warm Standby • Hot Standby (Default) **Note**: This configuration parameter must be set to the same value on both MCPs.
Heart Beat Configuration	**Configure Heart Beat Timeout** The interval within which the MCP must receive at least one message or Heart Beat from the other MCP. The valid range is 100 to 1000 msec; the default is 300 msec. **Note**: This configuration parameter must be set to the same value on both MCPs. **Configure Heart Beat retries** Use this function to set the number of times the MCP re-transmits a Heart Beat message before assuming that the other MCP has failed. The valid range is 1 to 10; the default is 3. **Note**: This configuration parameter must be set to the same value on both MCPs. **Configure Heart Beat Communication Mechanism through Hot standby** Select the Heart Beat communication option: 1. Single LAN (Default) 2. LAN1 and LAN2 3. LAN and Serial 4. LAN1, LAN2 and Serial **Configure Heart Beat Communication Mechanism through Warm standby** Select the Heart Beat communication option: 1. Serial Only 2. Single LAN 3. LAN1 and LAN2 4. LAN and Serial 5. LAN1, LAN2 and Serial In both Hot Standby and Warm Standby redundancy, the Heart Beat communication option includes serial and LAN. **Note**: This configuration parameter must be set to the same value on both MCPs **Note**: If the Heart Beat communication option includes a serial link, then a Primary and an optional backup serial port must be configured on the Connection configuration page of online HMI.
Configure IP Address of PEER Gateway	Use this function to set the unique IP Address of the other MCP device configured within the redundant system. If the PEER MCP has a second Ethernet interface, you can configure it as well. The maintenance IP Addresses of the PEER MCP must be entered here (see the *Ethernet Connections* topic in the MCP online help.

Username of PEER Gateway	Use this function to enter the username of an administrator user account on the PEER MCP unit (see Administrator Group Users). This parameter value should be the same on both MCP units. This setting is used in conjunction with the authentication mechanism defined in section: To configure users, go to. **Note**: Both MCPs must be configured with the same authentication mode (i.e., either Local or Remote). The PEER username should be reconfigured when the authentication mode changes from local to remote and vice versa.
Configure Time Sync with Standby	Use this function to enable or disable time synchronization of the standby MCP from the active MCP. This option should be enabled only if the standby MCP does not have an IRIG-B or NTP/SNTP based time synchronization mechanism. **Note**: This configuration parameter must be set to the same value on both MCPs.
Configure Enable/disable DTAs in Standby	Use this function to enable DTA applications to run normally on the standby MCP. If set to False, DTA applications suspend processing on the standby MCP. This setting is applicable to LogicLinx, Calculator, and Load Shed DTAs only. **Note**: This configuration parameter must be set to the same value on both MCPs.
Configure Gateway A/B Designation	Use this function to configure the A/B designation of the MCP. This parameter is only used if a switch panel is not configured. If a switch panel is configured, the Gateway A/B Designation is read from the switch panel and this parameter is not used.
Configure Switch Panel Type	Use this function to configure the type of switch panel: • **MASTER:** A change-over can be initiated from the switch panel. The switch panel is also used to route serial connections to the active unit. • **SLAVE:** The switch panel is only used to route serial connections to the active unit. **Note**: This parameter is only applicable to Hot Standby Redundancy. This parameter is only used if switch panel is configured (see section Redundancy Switch Panel). In Warm Standby redundancy mode, this parameter is ignored since the switch panel is always MASTER. **Note:** This configuration parameter must be set to the same value on both MCPs.
Enable/Disable Non-Sync Mode	If Non-Sync mode is disabled, then the standby MCP does not enter non-sync mode at startup, even if the firmware or configurations are not the same on both MCPs (see the Non-Sync Mode topic in the MCP online help). **Note**: This configuration parameter must be set to the same value on both MCPs.

```
================================================================
        Gateway Settings Menu
        Redundancy
================================================================

        0.   Back
        1.   Current Configuration
        2.   Enable/Disable Redundancy
        3.   Heart Beat Configuration
        4.   Configure IP Address of PEER Gateway
        5.   UserName of PEER Gateway
        6.   Configure Time Sync with Standby
        7.   Configure Enable/Disable DTAs in Standby
        8.   Configure Gateway A/B Designation
        9.   Setup Public Key Authentication with Peer Gateway
        10.  Configure Switch Panel Type
        11.  Enable/Disable Non-Sync mode

Enter Your Choice : ( Between 0 and 11 ):
```

ARRM - Automatic Record Retrieval Manager

From the **ARRM** menu, you can configure the Automated Record Retrieval Manager (ARRM) which retrieves and stores record files from devices connected to the MCP. For example, the SEL Binary DCA application retrieves and archives the Event Log files from the SEL IEDs/numerical relays.

The Automated Record Retrieval Manager settings are described in Table 4.21.

ARRM uses the Distributed Network Protocol (DNP), MODBUS, SELBIN, GENASCII and the IEC 61850 protocol to communicate with a variety of devices and uses the Trivial File Transfer Protocol (TFTP), File Transfer Protocol (FTP), Secure File Transport Protocol (SFTP), MMS or ASCII (for SEL devices) to archive the files from the IED to the device over a local area network (LAN) or serial connection.

Retrieved files are stored on the MCP file system in the folder /mnt/datalog/arrm/ with the structure Company > Station > Device.

Table 4.20: Automated Record Retrieval Manager setting descriptions

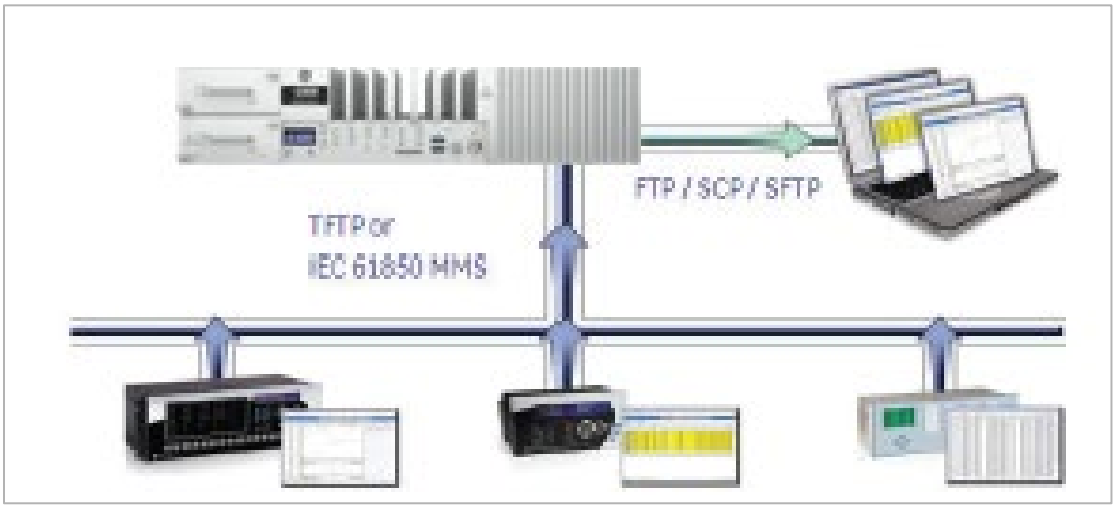
Setting	Description
Delete Records	You can use the ARRM menu to delete the contents of these folder structures, as well as temp and cache files, while leaving the directory structure intact for future downloads. You can also retrieve downloaded records from the MCP using any FTP/SCP/SFTP client as needed or on a scheduled basis

```
================================================================================
        Gateway Settings Menu
        ARRM Configuration
================================================================================

        0.    Back
        1.    Delete Records

Enter Your Choice : ( Between 0 and 1 ):
```

Select option **1. Delete Records**

```
================================================================================
        Gateway Settings Menu
        ARRM Configuration(Delete)
================================================================================

        0.    Back
        1.    Delete all Records
        2.    Delete Storage Directory Specific Records
        3.    Delete Station Specific Records
        4.    Delete Device Specific Records
        5.    Delete Temp
        6.    Delete Cache

Enter Your Choice : ( Between 0 and 6 ):
```

Figure 4.17: ARRM Connections



Suppress Forced Qualities To Masters

From the **Suppress Forced Qualities To Masters** menu, you can suppress forced qualities being reported to the IEC101-104 Master for a configured duration of time.

When a master is configured in this mode:

- All the values with Forced/Substituted flags are communicated to the Master as value changes only.
- All other flags are still communicated normally.

Only elevated users (that is, administrator users with root access privileges) can execute this functionality.

Re-starting the processes has no impact on the functionality.

This functionality is canceled (and the forced qualities are reported back to the master):

- Upon time expiration, or
- When the MCP is rebooted.

```
=====================================================================
        Gateway Settings Menu
        Suppress Local & Remote Forced Qualities
=====================================================================

When Enabled for a Master:
For a Configured Duration,Values with Forced/Substituted
Flags are communicated to Master as value changes only.
-No Forced/Substituted Flags are seen
-All other flags will still be communicated normally

Note:
1.On Expiration of Configured Suppression Time (OR)
  On Disabling this Mode,Normal Processing will be Resumed
2.Currently this Feature implies only for IEC101-104 Masters

        0.   Back
        1.   Suppression Mode Timer Stats
        2.   Enable/Disable Mode for all Masters
        3.   Enable/Disable Mode for only Specified Masters

Enter Your Choice : ( Between 0 and 3 ):
```

Option 1 => Suppression Mode Timer Stats.

```
=====================================================================
        Gateway Settings Menu
        Suppress Qualities Stats
=====================================================================

At any point of time this stats shows the remaining time
for which the qualities will be suppressed to IEC101-104 master

DISPLAY FORMAT:
Serial->  Port No.     Time duration
Network-> Instance No. Time duration

        0.   Back
        1.   Serial IEC-60870-101 Master
        2.   Network IEC-60870-104 Master

Enter Your Choice : ( Between 0 and 2 ):
```

Option 2=> Enable/Disable Mode for only Specified Masters.

```
=================================================================
        Gateway Settings Menu
        Suppress Local & Remote Forced Qualities
=================================================================

When Enabled for a Master:
For a Configured Duration,Values with Forced/Substituted
Flags are communicated to Master as value changes only.
-No Forced/Substituted Flags are seen
-All other flags will still be communicated normally

Note:
1.On Expiration of Configured Suppression Time (OR)
  On Disabling this Mode,Normal Processing will be Resumed
2.Currently this Feature implies only for IEC101-104 Masters

        0.   Back
        1.   Suppression Mode Timer Stats
        2.   Enable/Disable Mode for all Masters
        3.   Enable/Disable Mode for only Specified Masters

Enter Your Choice : ( Between 0 and 3 ): 2

Quality Suppression Mode is Disabled

Enabling this mode will Restart all Applications

Do you want to Enable it[Y/N]: y

Enter the Quality suppression period in hours[1-120]: 20

Restarting All applications for changes to take into effect
Changes Accepeted: Press ENTER Key to continue...
```

Option 3 => Enable/Disable Mode for only Specified Masters.

```
=================================================================
        Gateway Settings Menu
        Suppress Local & Remote Forced Qualities
=================================================================

        0.   Back
        1.   Serial IEC-60870-101 Master
        2.   Network IEC-60870-104 Master

Enter Your Choice : ( Between 0 and 2 ):
```

Emulate D20 RTU IEC101 DPA Unbalanced Mode Functionality

1. Log into the MCP firmware container through SSH/KVM/Serial maintenance port.
2. At the MCP# command prompt, enter **mcpcfg.**
3. Enter **16. Emulate D20 RTU IEC101 DPA Unbalanced Mode Functionality**

```
================================================================
        Gateway Settings Menu
================================================================

        0.   Back
        1.   Configure Authentication
        2.   Configure Network Settings
        3.   Configure Network Interfaces
        4.   Configure Secure Access
        5.   Configure Firewall
        6.   Configure Host Names
        7.   Configure Time & Time Sync
        8.   Reset System Logs
        9.   Reset Database Tables
        10.  Reset File Persistence Data
        11.  Local HMI
        12.  Configure Sync Manager
        13.  Redundancy
        14.  ARRM
        15.  Suppress Forced Qualities To Masters
        16.  Emulate D20 RTU IEC101 DPA Unbalanced Mode Functionality
        17.  Configure IEC101+104 DPA Startup Quality Event Suppress Interval
        18.  Configure Serial Ports
        19.  Configure D.20 Port Settings
        20.  EdgeOS Host
        21.  Clear Chassis Intrusion State
        22.  Restore Clone Snapshot
        23.  Restore Factory Default
        24.  Reboot Device

Enter Your Choice : ( Between 0 and 24 ):
```

4. Enter **1. Set Emulate D20 RTU IEC101 DPA Unbalanced Mode Functionality to TRUE/FALSE** based on the current status.

```
================================================================
        Gateway Settings Menu
        Emulate D20 RTU IEC101 DPA  Unbalanced Mode Functionality
================================================================


Emulate D20 RTU IEC101 DPA  Unbalanced Mode Functionality  is set to FALSE
        0.   Back
        1.   Set Emulate D20 RTU IEC101 DPA  Unbalanced Mode Functionality  to TRUE

Enter Your Choice : ( Between 0 and 1 ):
```

5. Enter **Y** to confirm or **N** to abort.

```
============================================================
        Gateway Settings Menu
        Emulate D20 RTU IEC101 DPA  Unbalanced Mode Functionality
============================================================


Emulate D20 RTU IEC101 DPA  Unbalanced Mode Functionality  is set to FALSE
        0.   Back
        1.   Set Emulate D20 RTU IEC101 DPA  Unbalanced Mode Functionality  to TRUE

Enter Your Choice : ( Between 0 and 1 ): 1


Are you sure you want to set Emulate D20 RTU IEC101 DPA Unbalanced Mode Functionality to TRUE [Y/N]?:
```

Configure IEC101+104 DPA Startup Quality Event Suppress Interval

1. Log into the MCP firmware container through SSH/KVM/Serial maintenance port.
2. At the MCP# command prompt, enter **mcpcfg.**
3. Enter **17. Configure IEC101+104 DPA Startup Quality Event Suppress Interval**

```
============================================================
        Gateway Settings Menu
============================================================

        0.   Back
        1.   Configure Authentication
        2.   Configure Network Settings
        3.   Configure Network Interfaces
        4.   Configure Secure Access
        5.   Configure Firewall
        6.   Configure Host Names
        7.   Configure Time & Time Sync
        8.   Reset System Logs
        9.   Reset Database Tables
        10.  Reset File Persistence Data
        11.  Local HMI
        12.  Configure Sync Manager
        13.  Redundancy
        14.  ARRM
        15.  Suppress Forced Qualities To Masters
        16.  Emulate D20 RTU IEC101 DPA Unbalanced Mode Functionality
        17.  Configure IEC101+104 DPA Startup Quality Event Suppress Interval
        18.  Configure Serial Ports
        19.  Configure D.20 Port Settings
        20.  EdgeOS Host
        21.  Clear Chassis Intrusion State
        22.  Restore Clone Snapshot
        23.  Restore Factory Default
        24.  Reboot Device

Enter Your Choice : ( Between 0 and 24 ):
```

4. Enter Startup Quality Event Suppress Interval in Seconds (0 to 600).

```
================================================================
        Gateway Settings Menu
        Configure IEC101+104 DPA Startup Quality Event Suppress Interval
================================================================


Current Value of Startup Quality Event Suppress Interval  is 0 Seconds

Note!!!Set the Value of Startup Quality Event Suppress Interval  to 0 Seconds to disable this functionality

Enter Startup Quality Event Suppress Interval in Seconds[0 to 600]:
```

NOTE: Set the value of Startup Quality Event Suppress Interval to 0(zero) seconds to disable this functionality.

Configure Serial Port Modes (RS-232/485)

1. Log into the MCP firmware container through SSH/KVM/Serial maintenance port.
2. At the MCP# command prompt, enter **mcpcfg.**
3. Enter **18. Configure Serial Ports**

```
================================================================
        Gateway Settings Menu
================================================================

        0.   Back
        1.   Configure Authentication
        2.   Configure Network Settings
        3.   Configure Network Interfaces
        4.   Configure Secure Access
        5.   Configure Firewall
        6.   Configure Host Names
        7.   Configure Time & Time Sync
        8.   Reset System Logs
        9.   Reset Database Tables
        10.  Reset File Persistence Data
        11.  Local HMI
        12.  Configure Sync Manager
        13.  Redundancy
        14.  ARRM
        15.  Suppress Forced Qualities To Masters
        16.  Emulate D20 RTU IEC101 DPA Unbalanced Mode Functionality
        17.  Configure IEC101+104 DPA Startup Quality Event Suppress Interval
        18.  Configure Serial Ports
        19.  Configure D.20 Port Settings
        20.  EdgeOS Host
        21.  Clear Chassis Intrusion State
        22.  Restore Clone Snapshot
        23.  Restore Factory Default
        24.  Reboot Device

Enter Your Choice : ( Between 0 and 24 ):
```

4. The Serial Ports Settings menu appears:

```
================================================================================
        Gateway Settings Menu
        Serial Ports Settings Menu
================================================================================

        0.   Back
        1.   Ports 1 2 3 4
        2.   Ports 5 6 7 8

Enter Your Choice : ( Between 0 and 2 ):
```

5. Enter your choice:
   - Enter **1** for configuring Ports 1, 2, 3, 4
   - Enter **2** for configuring Ports 5, 6, 7, 8 (only in G500)
   - For e.g.: Enter **2.**

```
================================================================================
        Gateway Settings Menu
        Serial Ports Settings Menu
================================================================================

        0.   Back
        1.   Ports 1 2 3 4
        2.   Ports 5 6 7 8

Enter Your Choice : ( Between 0 and 2 ): 2

Enter Serial port number(5 to 8):
```

6. Enter Serial port number which needs to be configured. For e.g.: Enter **6.**

```
================================================================================
        Gateway Settings Menu
        Serial Ports Settings Menu
================================================================================

        0.   Back
        1.   Ports 1 2 3 4
        2.   Ports 5 6 7 8

Enter Your Choice : ( Between 0 and 2 ): 2

Enter Serial port number(5 to 8): 6


Current Settings for Port 6:
        Mode: RS232
        Termination: Disable

Do you want to change these settings[Y/N]:
```

7. The current settings for selected port are displayed, for change the settings enter **Y** or enter **N** to navigate back to Serial Ports Settings menu.

- If "**Y**" :

```
================================================================================
        Gateway Settings Menu
        Serial Ports Mode Configuration
================================================================================

        0.   Back
        1.   RS232
        2.   RS422
        3.   RS4852W
        4.   RS4854W

Enter Your Choice : ( Between 0 and 4 ):
```

- Enter your choice from the list to change the mode and restart the device for the changes to take into effect.

Configure D.20 Port Hardware Settings

1. Log into the MCP firmware container through SSH/KVM/Serial maintenance port.
2. At the MCP# command prompt, enter **mcpcfg.**
3. Enter **19. Configure D.20 Port Settings**
4. If the D.20 HDLC cards are not installed, then the below message appears:

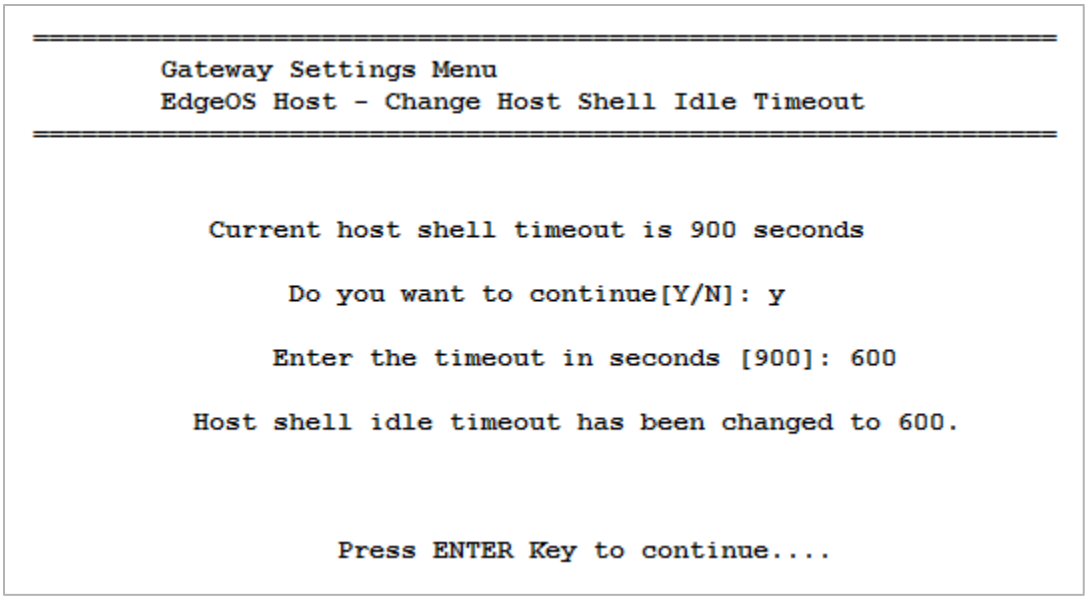
```
================================================================================
        Gateway Settings Menu
        D.20 Port Settings Menu
================================================================================


There are no D.20 HDLC cards installed.

        0.   Back

Enter Your Choice : ( 0 ):
```

EdgeOS Host Access

In MCP, normally users do not need to access the Predix EdgeOS host shell. In case there is a need to access the Predix EdgeOS host shell under some special circumstance, PETC provides a way for users to enable the Predix EdgeOS host SSH/SCP service temporally. Refer to section Chapter 8 - EdgeManager and PETC for how to access the PETC online documentation. The session timeout for the host shell access can be set in mcpcfg as described in this section.

To change the Host Shell Idle Timeout:

1. In the EdgeOS Host menu, enter 3**. Change Host Shell Idle Timeout**.
2. It will show the current timeout value. Then follow the instructions to change the timeout value. Its valid range is [60, 1800] seconds.



Clear Chassis Intrusion State

This feature is not available in G100.

Use the **Clear Chassis Intrusion State** menu to clear Chassis Intrusion state.

Step 1: Connect to MCP SSH (Secure Terminal Emulator from DS Agile MCP Studio) and login using Root user.

Step 2: Execute the command "**mcpcfg**" to launch the configuration Menu.

Step 3: Select option **21 – Clear Chassis Intrusion State**

```
================================================================
        Gateway Settings Menu
================================================================

         0.   Back
         1.   Configure Authentication
         2.   Configure Network Settings
         3.   Configure Network Interfaces
         4.   Configure Secure Access
         5.   Configure Firewall
         6.   Configure Host Names
         7.   Configure Time & Time Sync
         8.   Reset System Logs
         9.   Reset Database Tables
         10.  Reset File Persistence Data
         11.  Local HMI
         12.  Configure Sync Manager
         13.  Redundancy
         14.  ARRM
         15.  Suppress Forced Qualities To Masters
         16.  Emulate D20 RTU IEC101 DPA Unbalanced Mode Functionality
         17.  Configure IEC101+104 DPA Startup Quality Event Suppress Interval
         18.  Configure Serial Ports
         19.  Configure D.20 Port Settings
         20.  EdgeOS Host
         21.  Clear Chassis Intrusion State
         22.  Restore Clone Snapshot
         23.  Restore Factory Default
         24.  Reboot Device

Enter Your Choice : ( Between 0 and 24 ):
```

Step 4: The following screen will be launched on selection option **21.**

```
================================================================
        Gateway Settings Menu
        Clear Chasis Intrusion State
================================================================


Do you want to clear Chassis Intrusion state [Y/N]:
```

- Enter **Y,** to clear Chassis Intrusion state.

  Result: Successfully cleared Chassis intrusion state.

```
================================================================
        Gateway Settings Menu
        Clear Chasis Intrusion State
================================================================


Do you want to clear Chassis Intrusion state [Y/N]: y

Successfully cleared Chassis Intrusion state.

Press ENTER Key to continue...
```

- Enter **N,** to abort clear Chassis Intrusion state.
  Result: Chassis Intrusion state clear aborted.

```
================================================================
        Gateway Settings Menu
        Clear Chasis Intrusion State
================================================================


Do you want to clear Chassis Intrusion state [Y/N]: n

Chassis Intrusion state clear aborted.

Press ENTER Key to continue...
```

Restore Clone Snapshot

A root user or a super ("sudo") user can restore a Clone Snapshot, and the existing configuration will be replaced with the snapshot configuration.

Below are the ways to proceed with the restore:

1) In this scenario, user needs to connect a FAT32 formatted USB device containing clone snapshot file(s) with extension *. MCPClonesnapshot.DS7zip (taken using DSAS).
   GE doesn't recommend using more than one USB connected at a time for this operation.
2) Below two cases are applicable:
   If USB is not mounted: User will be prompted with 'Automatic mount of USB'
   - On Failure: Possible reasons for USB mount failure will be displayed:
     a. No USB drive inserted into one of the available slots.
     b. The inserted USB drive is malfunctioning.
     c. The inserted USB drive is not compatible with MCP drivers (only FAT32 is supported in this release).
     d. Device(s) busy (some other process is using the device(s)).

```
================================================================
        Gateway Settings Menu
        Restore Clone Snapshot
================================================================


WARNING!!! This action needs REBOOT of the device.

Do you want to Restore Clone Snapshot[Y/N]: y

USB not mounted. Insert USB device and select Yes to initiate auto-mounting [Y/N]: y

Initiating auto-mounting. Please wait...

Could not auto-mount USB.

Possible reasons:

        1. No USB drive inserted into one of the available slots.

        2. The inserted USB drive is malfunctioning.

        3. The inserted USB drive is not compatible with G500 drivers.

        4. Device(s) busy (some other process is using the device(s)).

Press ENTER Key to continue...
```

- On Success:
  - If Single USB is Present, then the list of Clone Snapshots will be listed or If no snapshots are present, then folder EMPTY message will be displayed.
  - If More than one USB is detected, then the list of detected USBs will be listed. On Selection of the USB, the list of Clone Snapshots present in the USB will be listed. If no snapshots are present, then folder EMPTY message will be displayed.

If USB is already mounted successfully:

- If Single USB is Present, then the list of Clone Snapshots will be listed or If no snapshots are present, then folder EMPTY message will be displayed.
- If More than one USB is detected, then the list of detected USBs will be listed. On Selection of the USB, the list of Clone Snapshots present in the USB will be listed. If no snapshots are present, then folder EMPTY message will be displayed.

3) Once the snapshot is selected, user checks the below conditions and once met will copy the file to /mnt/usr/SnapShotTransfer folder for restore on to the device.
   - Checks for *. MCPCloneSnapshot.DS7zip extension
   - Clone snapshots are password protected; it will provide 3 attempts for user to enter the correct password
   - Checks for schema version of the clone snapshot matches with the device schema version
   - Replace the existing configuration and settings with the new ones from the selected clone snapshot
4) Automatic reboot of the device takes place to make the changes effective.

Restore Clone Snapshot with correct password

In this scenario, User connects a USB to device with file/files with extension *.MCPClonesnapshot.DS7zip and enters correct password.

```
================================================================
        Gateway Settings Menu
        Restore Clone Snapshot
================================================================


WARNING! This action will REBOOT the device.

Do you want to Restore Clone Snapshot[Y/N]: y

USB not mounted. Insert USB device and select Yes to initiate auto-mounting [Y/N]: y

Initiating auto-mounting. Please wait...

Successfully mounted USB. It will be unmounted once the restoration is complete.

----------------------------------------
List of Snapshots present in the USB.
----------------------------------------
        0.   Back
        1.   106_CloneSnapshot.MCPCloneSnapshot.DS7zip
        2.   G500A_V110_106_v200.MCPCloneSnapshot.DS7zip
        3.   LDAP_GroupMapping_Build90.MCPCloneSnapshot.DS7zip
        4.   TIMESYNC.MCPCloneSnapshot.DS7zip

Enter Your Choice : ( Between 0 and 4 ): 1

Enter Password for 106_CloneSnapshot.MCPCloneSnapshot.DS7zip:

Re-enter the password for 106_CloneSnapshot.MCPCloneSnapshot.DS7zip:

System will now reboot to apply the snapshot.

Gateway is going to reboot....
```

Once the command is initiated, user will copy **MCPCloneSnapshot.DS7zip** file from the USB mount paths to /mnt/usr/SnapShotTransfer/ folder for restore on to the device.

Automatic reboot of the device takes place to make the changes effective.

Restore Clone Snapshot with Incorrect Password

In this scenario, User connects a USB to device with file/files with extension *. MCPClonesnapshot.DS7zip and enters incorrect password.

User will be provided 3 attempts to provide correct password. Failing which will result in return to main menu.

```
================================================================
        Gateway Settings Menu
        Restore Clone Snapshot
================================================================

WARNING!!! This action needs REBOOT of the device.

Do you want to Restore Clone Snapshot[Y/N]: y

USB not mounted. Insert USB device and select Yes to initiate auto-mounting [Y/N]: y

Initiating auto-mounting. Please wait...

Successfully mounted USB. It will be unmounted once the restoration is complete.

----------------------------------------
List of Snapshots present in the USB.
----------------------------------------
        0.   Back
        1.   106_CloneSnapshot.MCPCloneSnapshot.DS7zip
        2.   G500A_V110_106_v200.MCPCloneSnapshot.DS7zip
        3.   LDAP_GroupMapping_Build90.MCPCloneSnapshot.DS7zip
        4.   TIMESYNC.MCPCloneSnapshot.DS7zip

Enter Your Choice : ( Between 0 and 4 ): 1

Enter Password for 106_CloneSnapshot.MCPCloneSnapshot.DS7zip:

Re-enter the password for 106_CloneSnapshot.MCPCloneSnapshot.DS7zip:

Error : Unable to extract with the password provided. Retry entering valid Password.

Enter Password for 106_CloneSnapshot.MCPCloneSnapshot.DS7zip:

Re-enter the password for 106_CloneSnapshot.MCPCloneSnapshot.DS7zip:

Error : Unable to extract with the password provided. Retry entering valid Password.

Enter Password for 106_CloneSnapshot.MCPCloneSnapshot.DS7zip:

Re-enter the password for 106_CloneSnapshot.MCPCloneSnapshot.DS7zip:

Entered Passwords do not match!!!

Error : Max retries reached.

Press ENTER Key to continue...
```

Restore Clone Snapshot with snapshot already present in Snapshot Transfer folder

In this scenario, User has already performed MCPCloneSnapshot operation once and tries to re-perform the operation again.

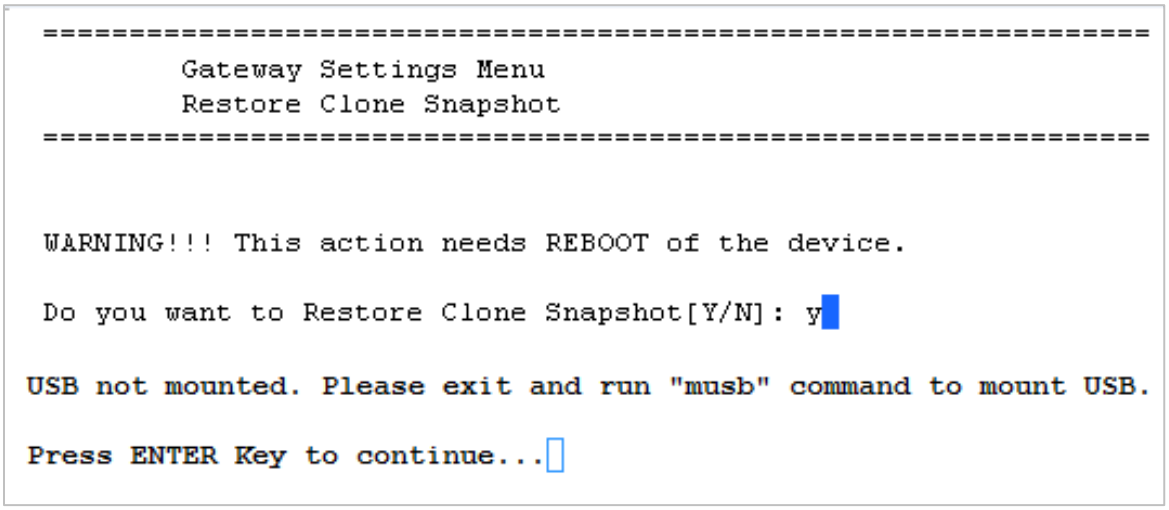
Snapshot Replace Scenario:

User will be prompted with the message to delete the existing snapshot in the Transfer Folder and replace with the new selected clone snapshot from the USB. On confirmation the old/existing snapshot and respective content i.e., reason.txt file and SnapshotPwd.txt file will be deleted from the SnapshotTransfer folder and new Clone snapshot and it's corresponding files will be copied to respective folder.

```
================================================================
        Gateway Settings Menu
        Restore Clone Snapshot
================================================================


WARNING!!! This action needs REBOOT of the device.

Do you want to Restore Clone Snapshot[Y/N]: y

USB not mounted. Insert USB device and select Yes to initiate auto-mounting [Y/N]: y

Initiating auto-mounting. Please wait...

Successfully mounted USB. It will be unmounted once the restoration is complete.

---------------------------------------
List of Snapshots present in the USB.
---------------------------------------
        0.   Back
        1.   106_CloneSnapshot.MCPCloneSnapshot.DS7zip
        2.   G500A_V110_106_v200.MCPCloneSnapshot.DS7zip
        3.   LDAP_GroupMapping_Build90.MCPCloneSnapshot.DS7zip
        4.   TIMESYNC.MCPCloneSnapshot.DS7zip

Enter Your Choice : ( Between 0 and 4 ): 1

Enter Password for 106_CloneSnapshot.MCPCloneSnapshot.DS7zip:

Re-enter the password for 106_CloneSnapshot.MCPCloneSnapshot.DS7zip:

A snapshot file already exists in the /mnt/usr/SnapShotTransfer/ folder

with filename:  106_CloneSnapshot.MCPCloneSnapshot.DS7zip

Do you want to remove the old snapshot and copy new snapshot [Y/N]: y

Snapshot will be applied only on Reboot.

Press ENTER Key to continue...
```

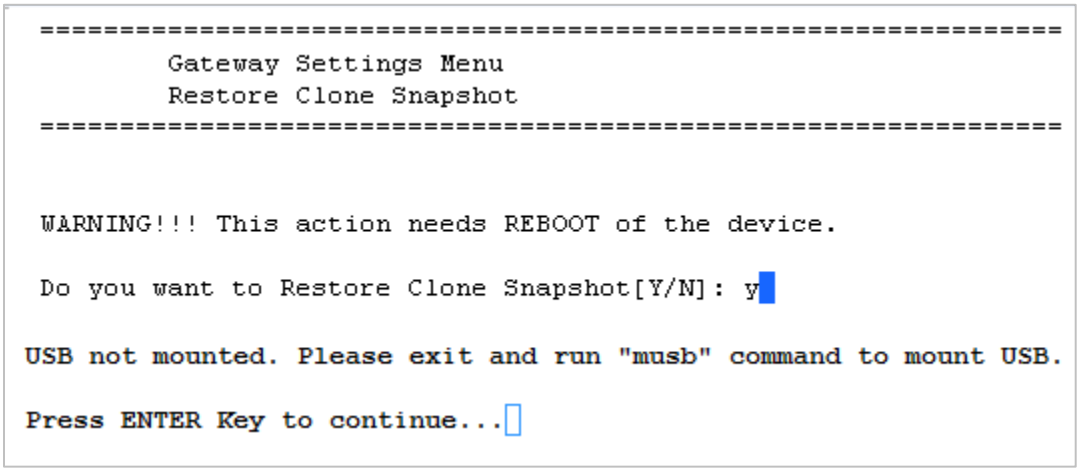
Snapshot Replace Abort Scenario:

User will be prompted with the message to delete the existing snapshot and replace with the new snapshot. Here user says No, on confirmation message to delete the old/existing snapshot and respective content i.e., reason.txt file and SnapshotPwd.txt file from the SnapshotTransfer folder. The old snapshot remains, and current Clone snapshot operation will be aborted.



Restore Clone Snapshot with Schema mismatch

In this scenario, User connects a USB to device with file/files with extension *. MCPClonesnapshot.DS7zip and selects the snapshot whose schema version is less than the device schema version i.e., user cannot restore Clone Snapshot of 1.0 and 1.1 directly to 2.0 device. User must use DSAS firmware upgrade procedure to upgrade the snapshot to current device version and copy the upgraded snapshots to the USB.



Restore to Factory Default

A root user or a super (“sudo”) user can restore a MCP to the factory default (or “clean”) configuration.

When restored to default factory settings, all user configuration files, and system settings will be lost.

In case all root / administrator user credentials have been lost, and the MCP cannot be accessed with these roles – the MCP can be restored to a clean and defaulted state using an external USB workflow; for detailed steps please refer to the technical note: *TN0116 MCP Firmware Upgrade and Restore to Defaults Workflows.*

Factory default of current configuration

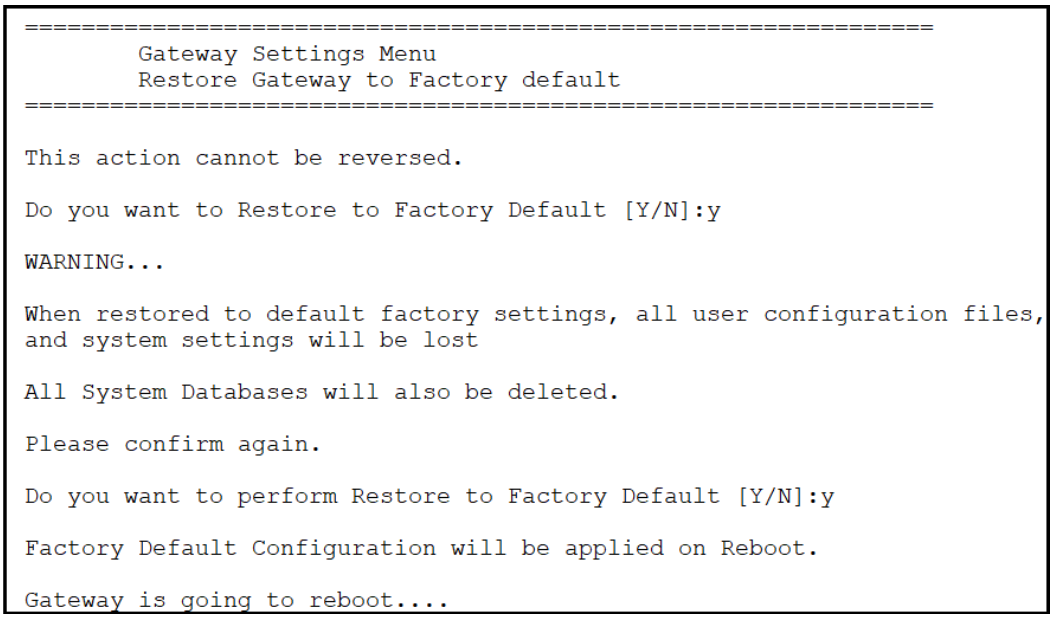
Once the command is initiated, user will be prompted with confirmation message whether to proceed with Restore Operation or not.

On confirmation, Warning message prompts with the information of that is going to be lost by user during restore process and Re-confirmation will be prompted.

Here the user still has the possibility of exiting the current operation and go back to the Gateway Main Settings Menu.

- On yes, the following operations will be performed in background:
  - All the content and container's will be cleaned up.
  - Reboot will be triggered automatically.
  - On Reboot, the system will be set to factory default settings.

Below screenshot refers to the "Restore to factory default settings screen that is been explained above:



- On No, the user will be return to Main Gateway Settings Menu.

  Below screenshot refers to the "Exit Restore to factory default settings and return to Gateway Main Menu" screen that is been explained above:

```
============================================================
        Gateway Settings Menu
        Restore Gateway to Factory default
============================================================

This action cannot be reversed.

Do you want to Restore to Factory Default [Y/N]:y

WARNING...

When restored to default factory settings, all user configuration files,
and system settings will be lost

All System Databases will also be deleted.

Please confirm again.

Do you want to perform Restore to Factory Default [Y/N]:n

Aborted Restore to Factory Default operation.

Press ENTER Key to continue...
```

Exit to Main Gateway Menu without factory Default

In this scenario, the user will exit the current Restore Gateway to Factory default menu and return to the Gateway Settings Menu without performing any operation.

This will result the user displayed with an information message stating, "Aborted Configuring to Factory Default operation." and asked to press enter to go back to Gateway Settings Menu.

Below screenshot refers to the "No configuration-Exit to Main Gateway Settings Menu" screen that is been explained above.

```
============================================================
        Gateway Settings Menu
        Restore Gateway to Factory default
============================================================

This action cannot be reversed.

Do you want to Restore to Factory Default [Y/N]:N

Aborted Configuring to Factory Default operation.

Press ENTER Key to continue...
```

Reboot device

This option allows user to reboot the MCP unit.

To reboot the MCP unit:

1. Log into the MCP Utilities page.
   Result: The **MCP#>>** command prompt appears.
2. Type mcpcfg and press **Enter**.

Result: The **Gateway Configuration Utility Menu** appears.

3. Select option 24. **Reboot Device**
   Result: The following prompt appears: **Do you want to reboot Gateway? [Y/N]:**
   If you enter **Y, then MCP unit will start rebooting**
   If you enter N, then it navigates back to earlier menu.

The user can reboot the unit using the following command “mcpreboot” at the command prompt.

Chapter 5 - MCP Settings GUI

Introduction

This chapter provides settings instructions to users of **MCP Settings GUI Web Interface**.

This interface is the Web based equivalent of the *Chapter 4 - MCP Local Configuration Utility (mcpcfg).*

The functionality of the system is identical as when settings are performed via MCP Local Configuration Utility (mcpcfg). The difference is only this is a Web based GUI.

How to access/logout

- Login – Local MCP
- Login – Remote MCP
- Initial Setup
- Logout

MCP Settings Workflows

- Configure Authentication
- Configure Network Settings
- Configure Network Interfaces
- Configure Secure Access
- Configure Firewall
- Configure Host Names
- Configure Time & Time Sync
- Reset System Logs
- Reset Database Tables
- Reset File Persistence Data
- Local HMI
- Configure Sync Manager
- Redundancy
- ARRM
- Suppress Forced Qualities To Masters
- Emulate D20 RTU IEC101 DPA Unbalanced Mode Functionality
- Configure IEC101+104 DPA Startup Quality Event Suppress Interval
- Configure Serial Port Modes (RS-232/485)
- EdgeOS Host Access
- Configure D.20 Port Settings
- Clear Chassis Intrusion State
- Restore Clone Snapshot
- Restore to Factory Default
- Reboot Device

How to access/logout

Users can access MCP Settings Web Interface through Local or Remote MCP connection. Remote access must be completed using a supported web browser (Internet Explorer, Microsoft Edge, Mozilla Firefox, Google Chrome). This section provides information on the following:

- Login – Local MCP
- Login – Remote MCP
- Initial Setup
- Logout

Login – Local MCP

1. Connect an available mouse/keyboard/monitor to the MCP.
2. Once the MCP device is powered up and has a valid license installed, click on the **MCP** name via the taskbar.
3. Click **System Settings**.
4. A default web browser will be opened showing **MCP Settings** Login screen.

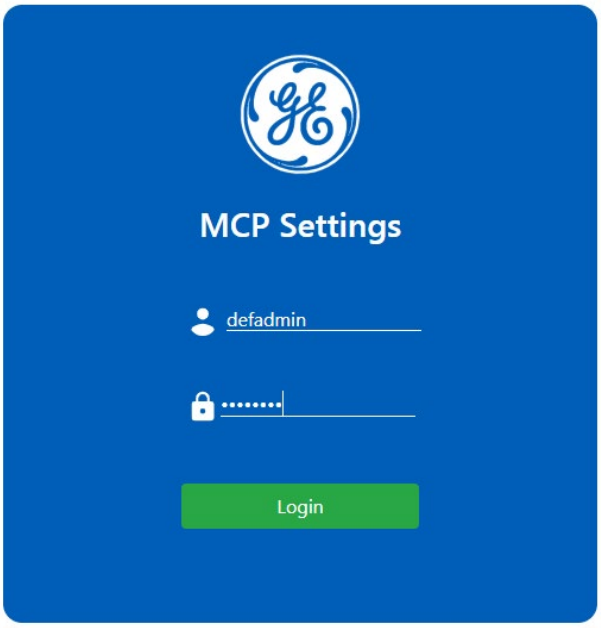
Login – Remote MCP

1. Using a supported web browser, disable proxy and type the default IP 192.168.168.81 with port 8081 into the address bar and press the 'Enter key'. i.e., https://192.168.168.81: :8081
2. User is required to **confirm security certificate** exception.
3. The **MCP Settings** Login screen is displayed.

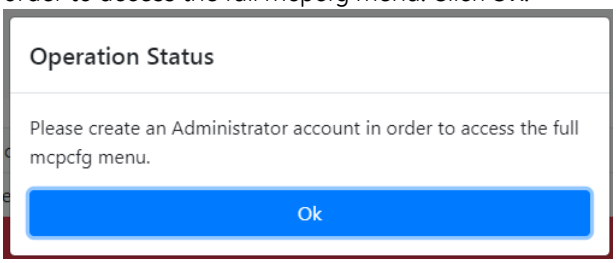
Initial Setup

NOTE: Initial Setup section is identical between Local/Remote access.

1. Enter the default **Username** (defadmin), default **Password** (defadmin) and click **Login**.



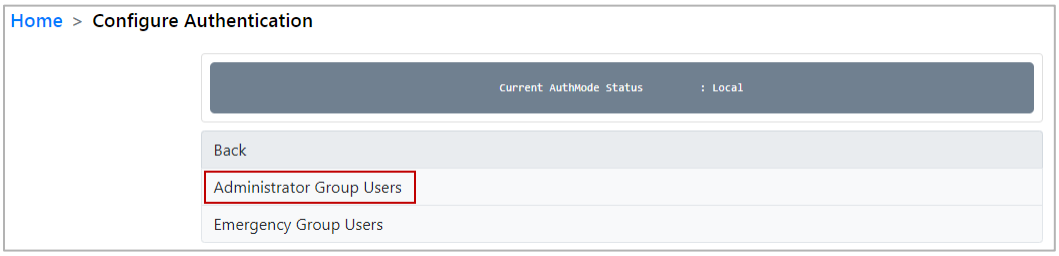
2. If the defadmin account is used to login, you will be prompted to create an Administrator account in order to access the full mcpcfg menu. Click **OK**.



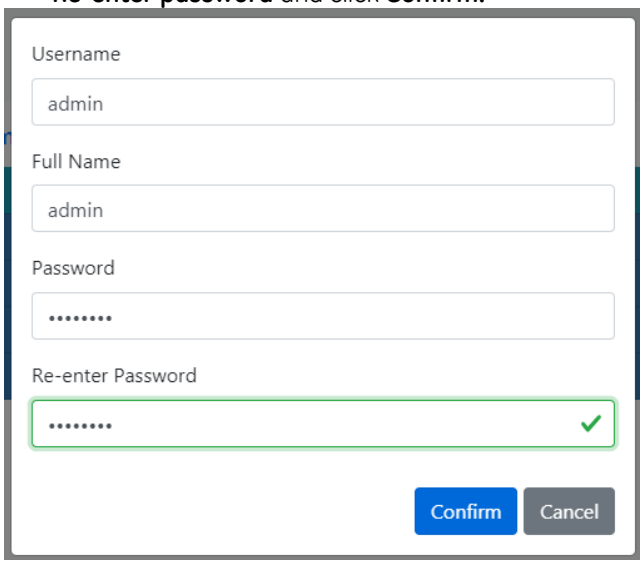
3. The Gateway Settings main menu appears:

4. Select **Configure Authentication** tab from main menu.

5. Select **Administrator Group Users** tab from Configure Authentication menu.

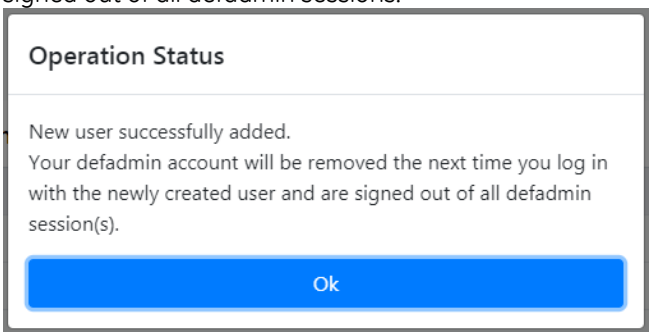


6. This function is used to perform the following actions:
   - List Users
   - Add User
   - Change Password
   - Remove User
7. Select **Add User** tab to create administrator-level users.
   - Enter the desired **Username**, conforming to the username rules as listed below:
     - Username must be between 2 and 31 characters.
     - Username must start with a lowercase alphabetical character.
     - Username must only contain [a-z][0-9][-,_] characters.
   - Enter the **Full Name** of the user.
   - Enter the **Password**, conforming to the password security rules as listed below:
     - Password must be between 8 and 199 characters in length
     - Password must contain:
       - 1 character from [a-z]
       - 1 character from [A-Z]
       - 1 digit from [0-9]
       - 1 special character from the set [$%@!&]
   - **Re-enter password** and click **Confirm.**

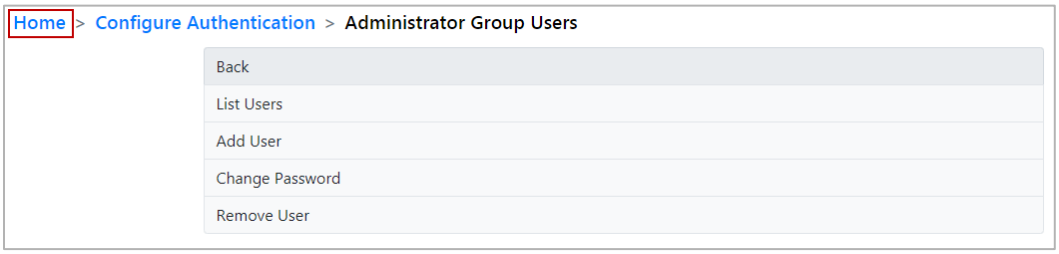


8. **RESULT:** Pop-up window appears showing the Operation Status, click **OK.**
   NOTE: defadmin account will be removed the next time you log in with the newly-created user and are

signed out of all defadmin sessions.



9. Navigate back to the main menu by clicking on the **HOME** link located at the upper left corner of the page.

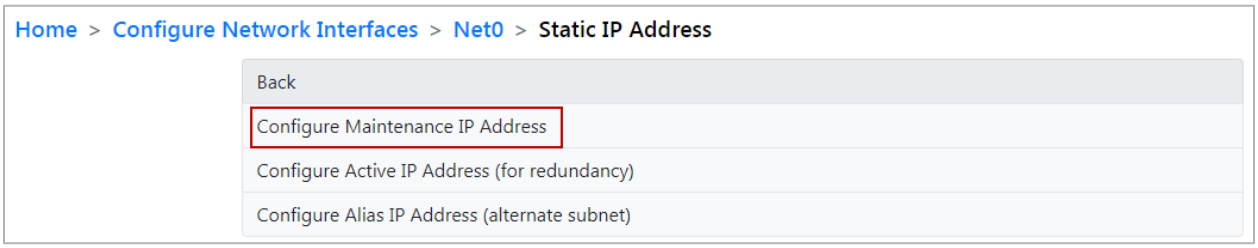


10. Select **Configure Network Interfaces** tab from main menu.

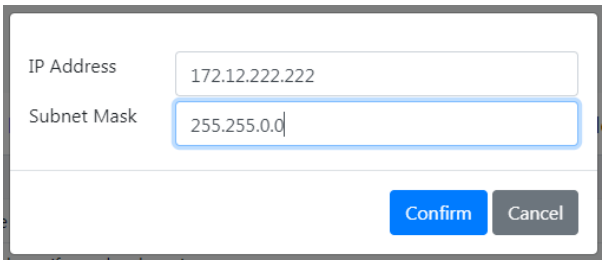
11. Select the desired Network port (default 192.168.168.81) which is connected to MCP device from the list.

12. Select **Static IP Address** tab.

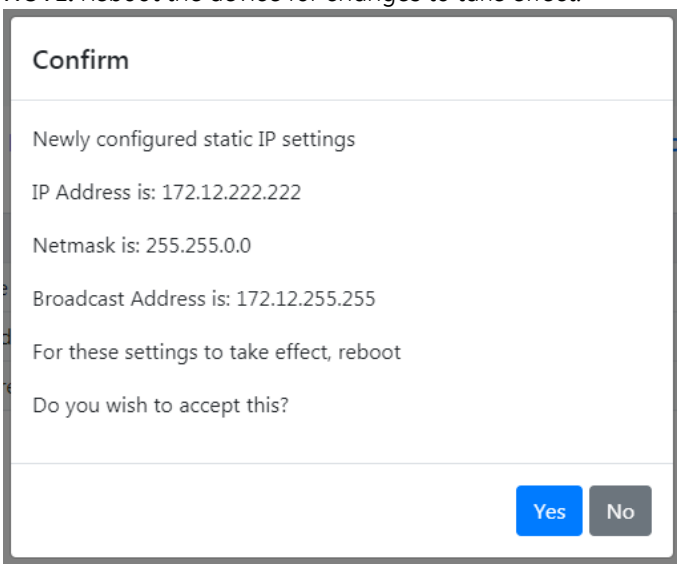
13. Select **Configure Maintenance IP Address** tab.



14. Enter **IP Address** and **Subnet Mask**. Click **Confirm**.

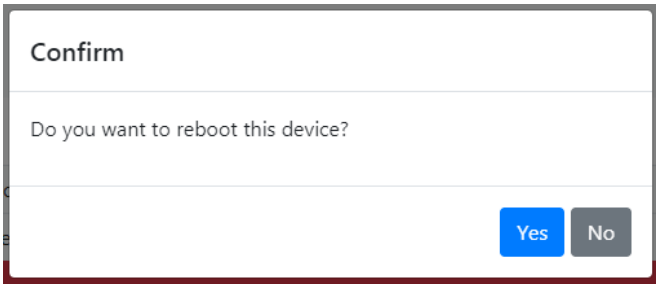


15. Click **Yes** to confirm the newly-configured static IP settings.
NOTE: Reboot the device for changes to take effect.

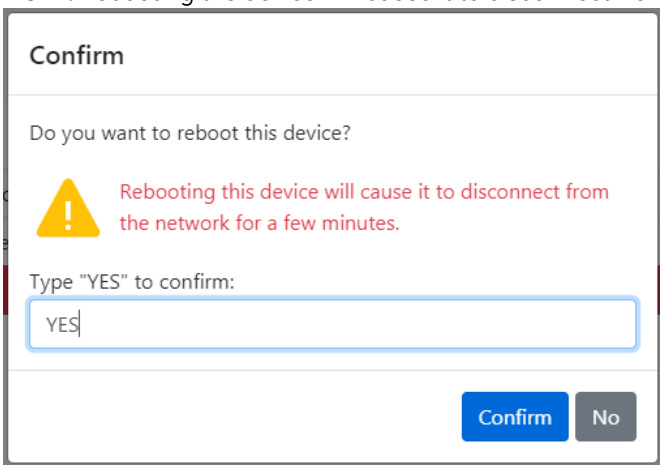


16. Navigate back to main menu and select **Reboot Device** tab.

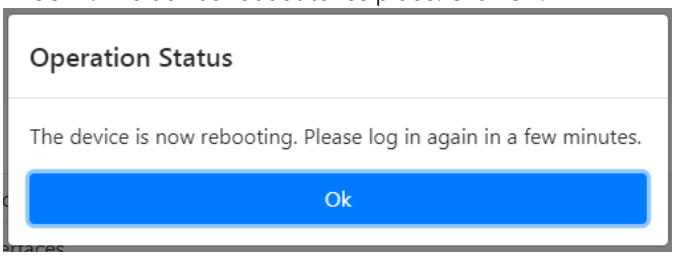
17. Click **Yes** to confirm Reboot the device.



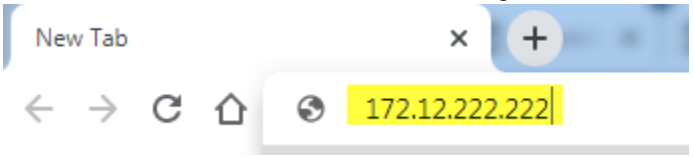
18. Type "**YES**" and click **Confirm**.
NOTE: Rebooting the device will cause it to disconnect from the network for a few minutes.



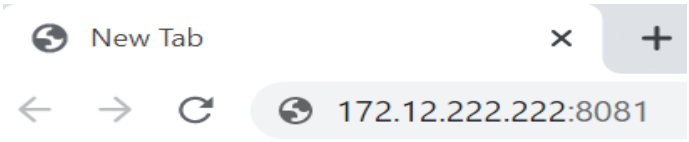
RESULT: The device reboot takes place. Click **OK**.



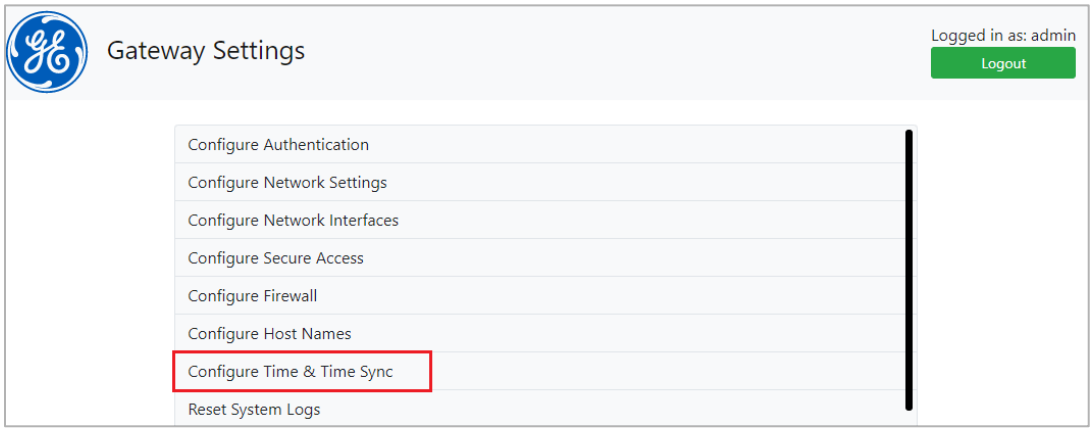
19. Upon MCP reconnect, users can access MCP Web Interface remotely via the newly-configured IP Address and a supported web browser. In the supported browser address bar, type in the new MCP device IP (ex.: **172.12.222.222**) as shown in figure below.



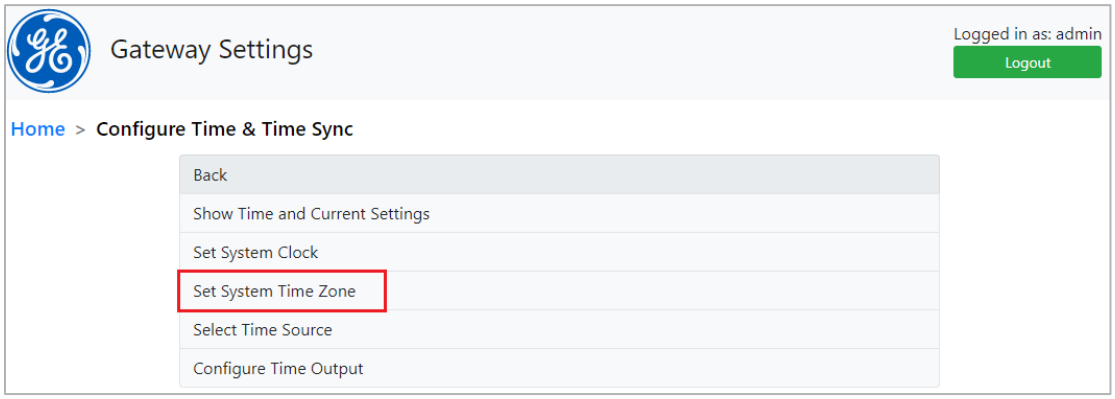
or



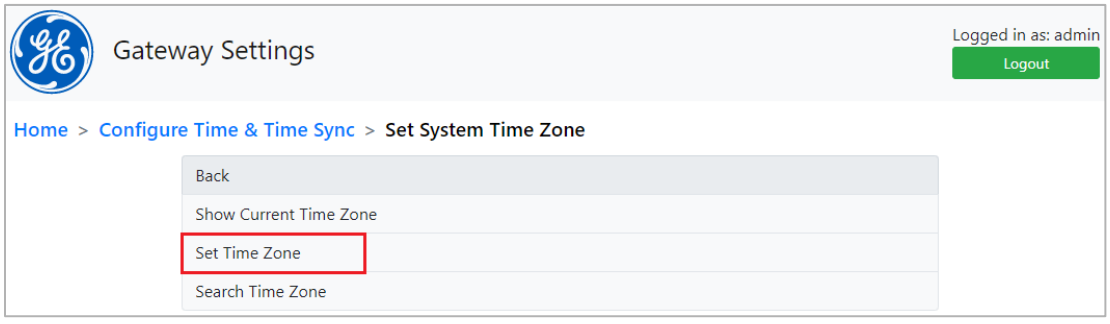
20. Press the 'Enter key' and the MCP Settings Login page appears.
21. Login using the newly-created admin username/password and click on the "Login" button.
22. Select **Configure Time & Time Sync** tab.



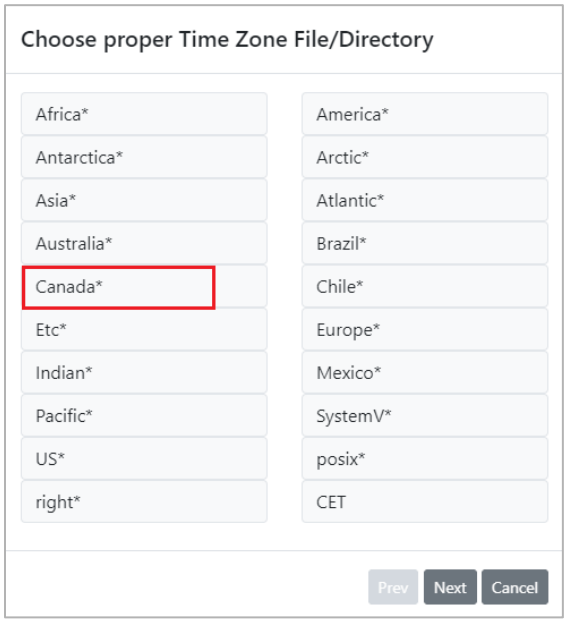
23. Select **Set System Time Zone** tab.



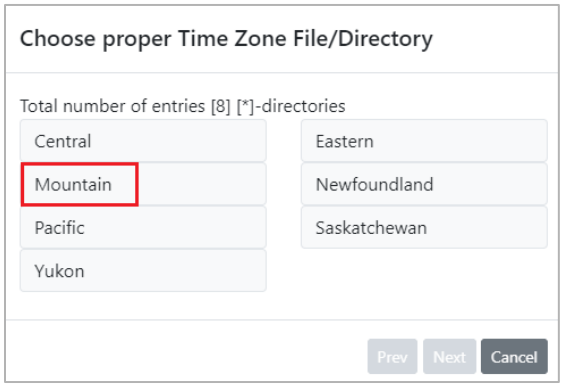
24. Select **Set Time Zone** tab. Configure the MCP to the same time zone as remote PC.



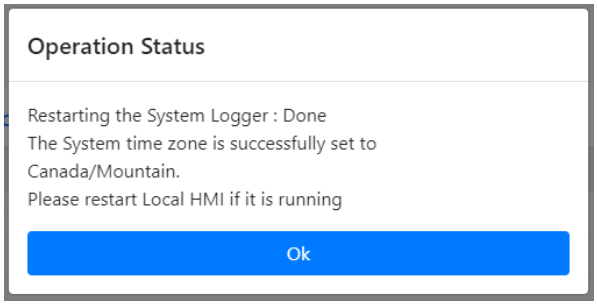
25. Select applicable time zone. User can navigate the menu using Prev/Next buttons.



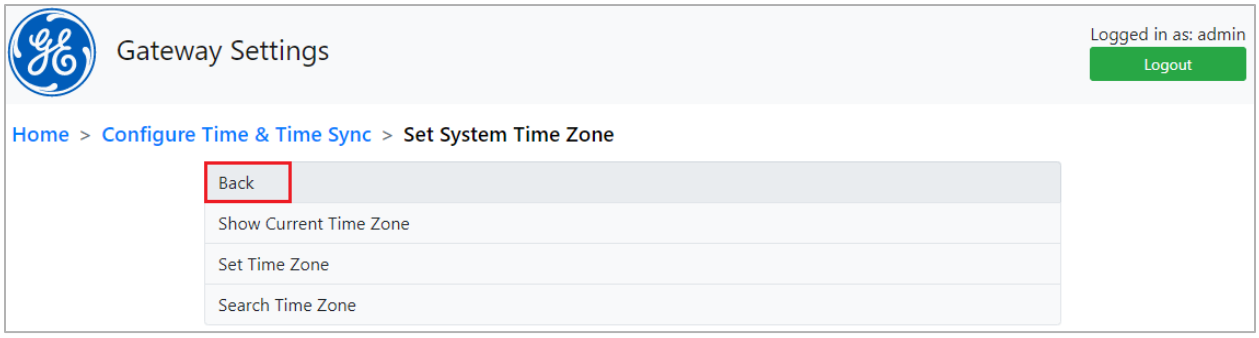
26. Select applicable region within the selected time zone.



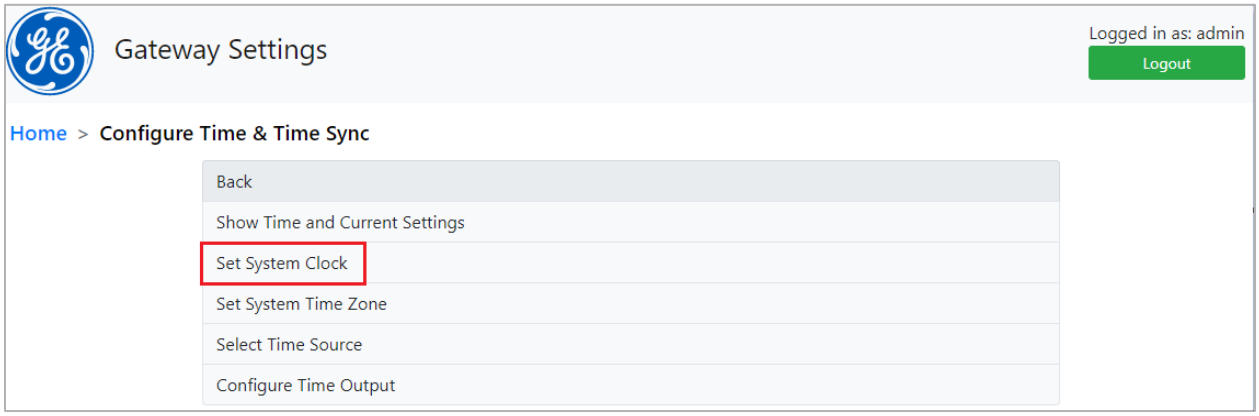
RESULT: The Operation Status dialog shows success message. Click **OK**.



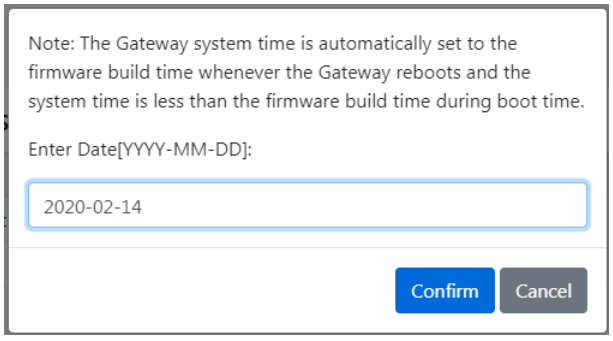
27. Select the **Back** tab.



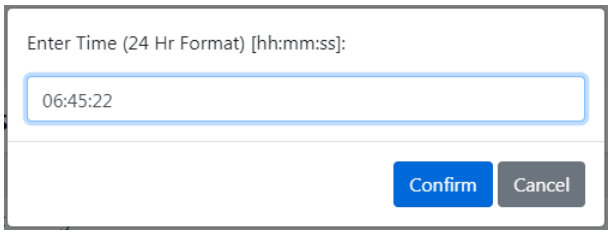
28. Select the **Set System Clock** tab.



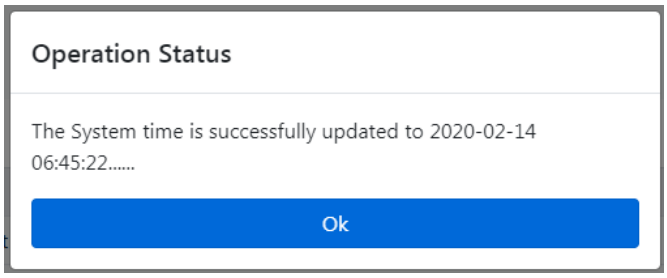
29. A dialog is displayed informing the user to enter a date using the format **YYYY-MM-DD**. Enter **today's date** and select the **Confirm** button



30. A dialog is displayed informing the user to enter time, using the **24 Hr Format hh:mm:ss**. Enter **remote PC time** and select the **Confirm** button

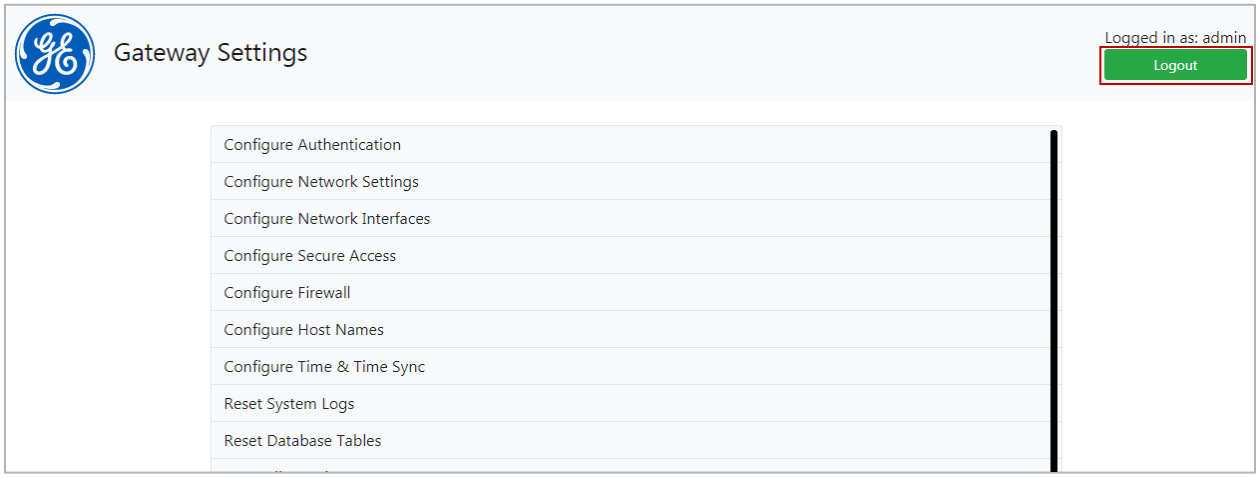


RESULT: The Operation Status dialog shows success message. Click **OK**.

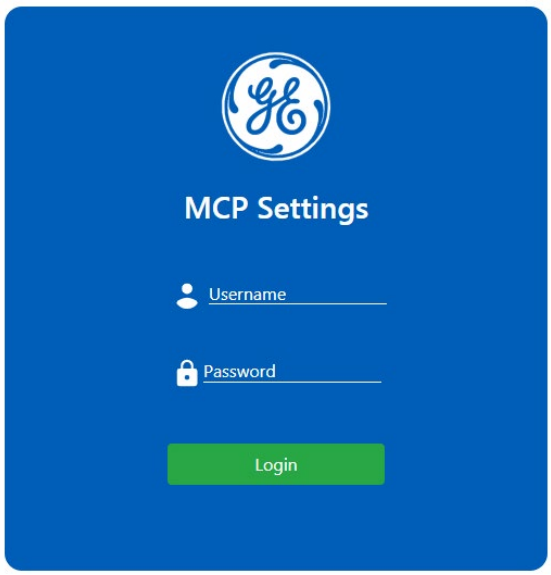


Logout

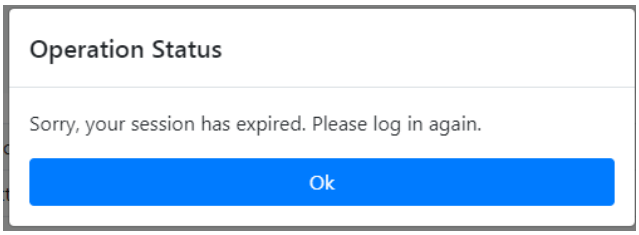
To logout, click on the link to "Logout" located at the upper right corner of the page as shown in figure below.



When you have successfully logged-out of the system, the screen below will be displayed.

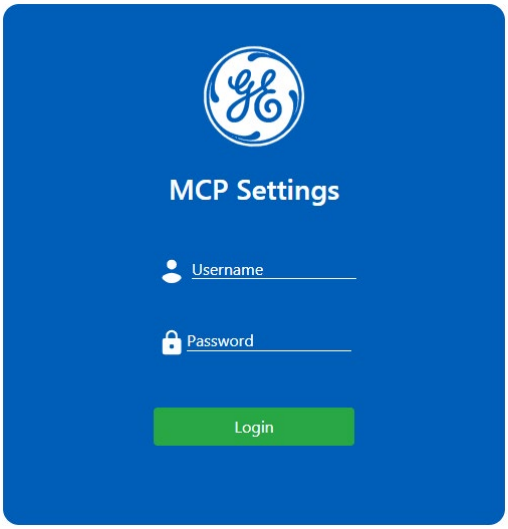


Note that after 20 minutes of inactivity, the session is automatically timed out and a message will be displayed as shown in below figure. In such cases, either click on "OK" and login again or click on any of the links to be redirected to the log in page.

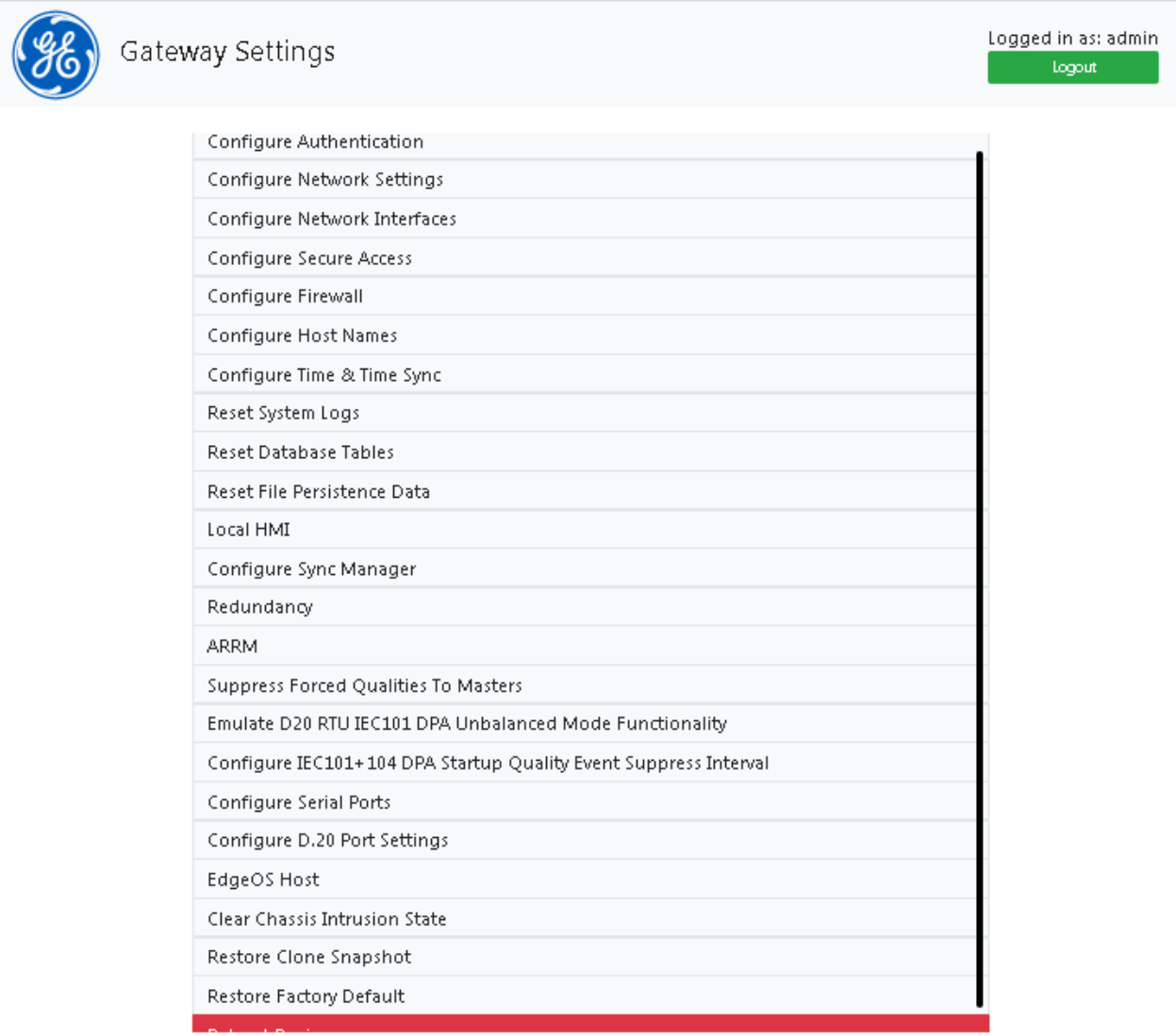


MCP Settings Workflows

1. Users who have previously configured MCP device IP must login by:
   - Entering their User Name.
   - Entering their Password.
   - Selecting Login to advance to the next screen and begin using the application.

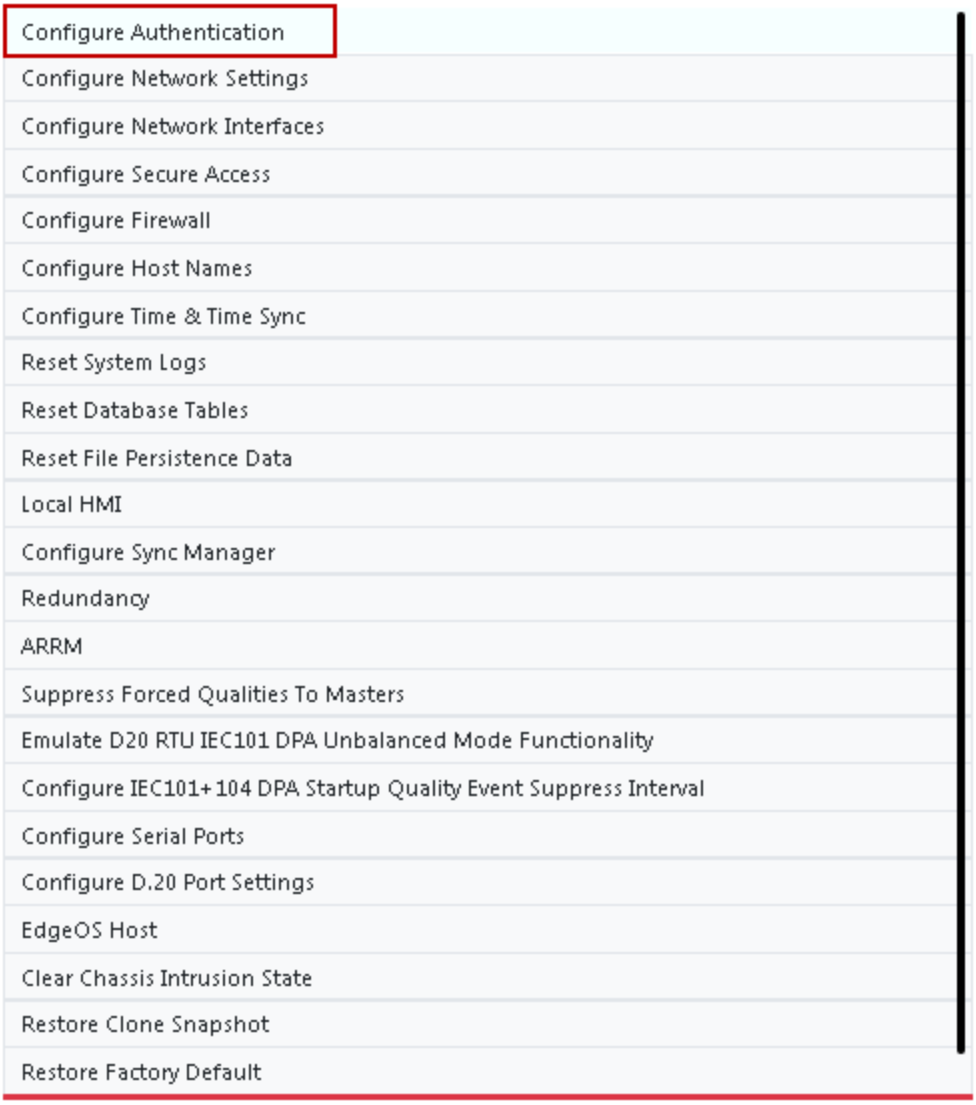


2. Once you have logged in to the MCP Settings, you can see a menu on the center and Logout option on the top right of the screen. To explore the MCP settings use the menu options shown on the home page:

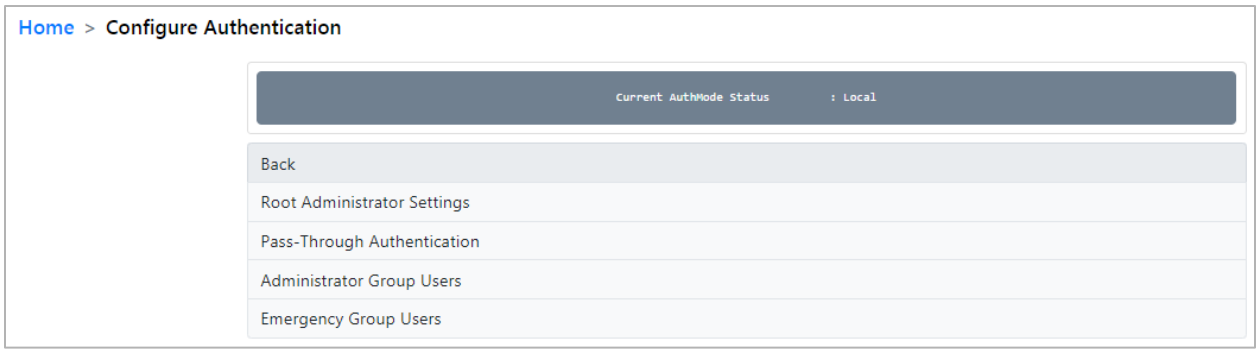


Configure Authentication

1. Click **Configure Authentication** from the main menu.

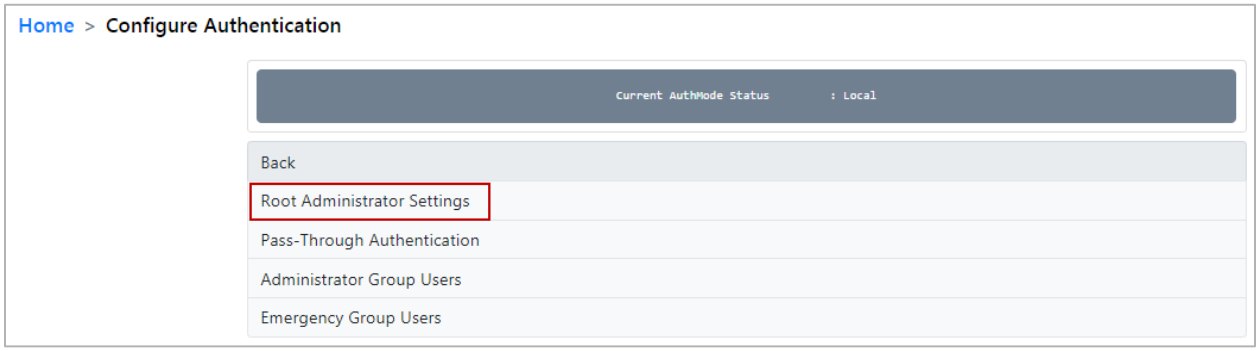


2. Click **Back** to return to the **Main Menu.**



Root Administrator Settings

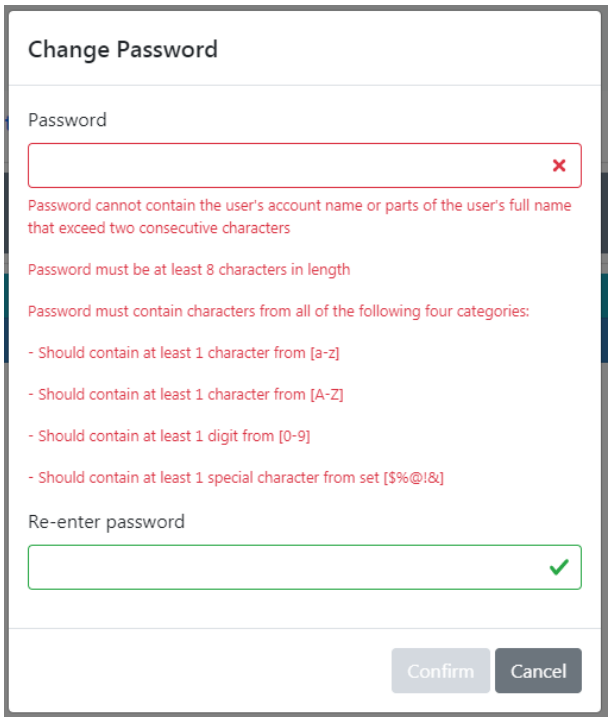
1. Click **Root Administrator Settings** tab.



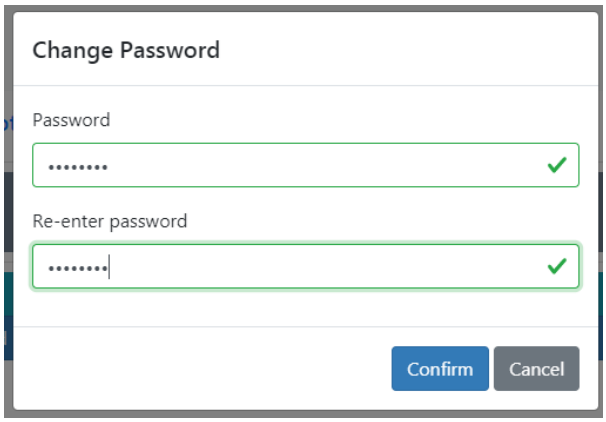
2. Click Change Root Password to change the password associated with the system root user account.

3. Change Password:
    - Password cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters.
    - Password must be at least 8 characters in length.
    - Password must contain characters from all the following four categories:
        - Should contain at least 1 character from [a-z]
        - Should contain at least 1 character from [A-Z]
        - Should contain at least 1 digit from [0-9]
        - Should contain at least 1 special character from set [$%@!&]

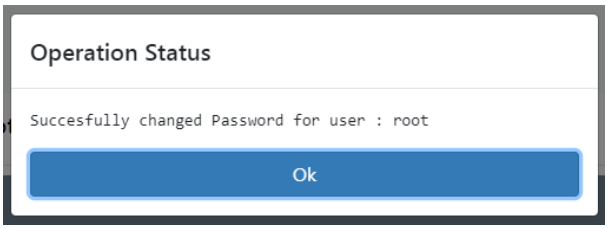
- Re-enter password.



4. Click **Confirm.**



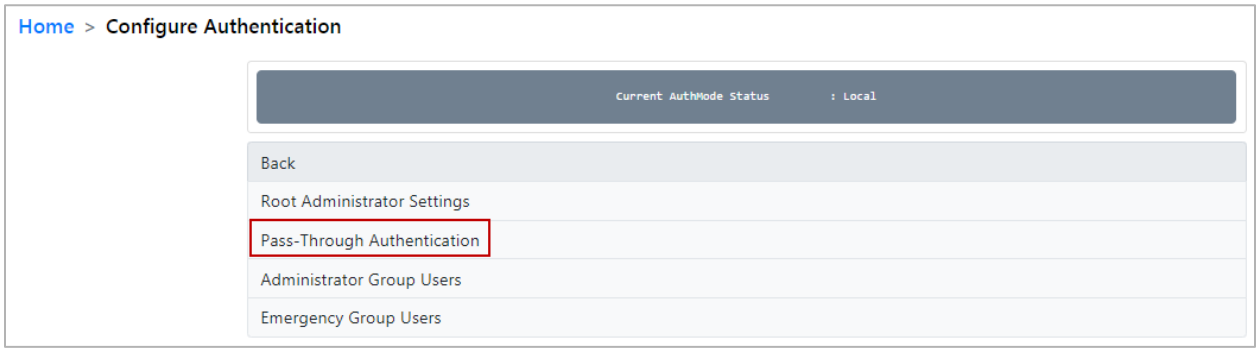
5. **RESULT**: Pop-up window appears showing the Operation Status, click **OK.**



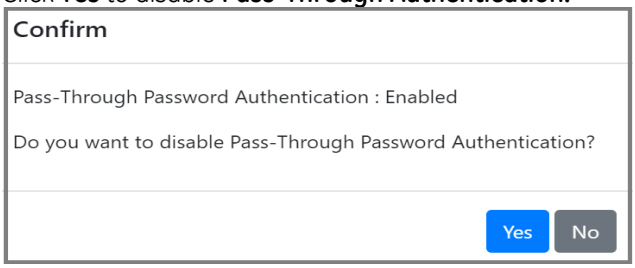
6. Click **Back** to return to the **Configure Authentication** menu.

Pass-Through Authentication

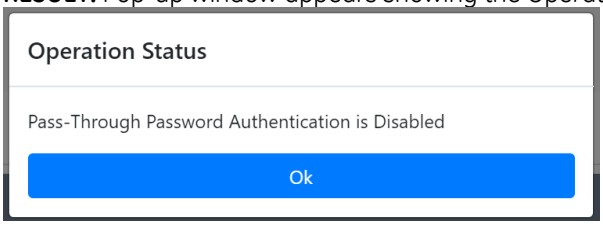
1. Click **Pass-Through Authentication** tab.



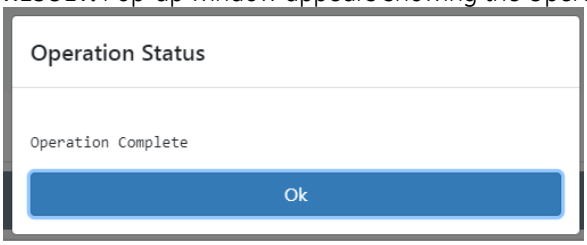
2. Use this function to enable or disable **Pass-Through Authentication**.
   - When authentication is enabled, a valid username and password is required to access client applications through pass-through ports. Enabled by default.
   - Click **Yes** to disable **Pass-Through Authentication.**



   - **RESULT:** Pop-up window appears showing the Operation Status, click **OK.**



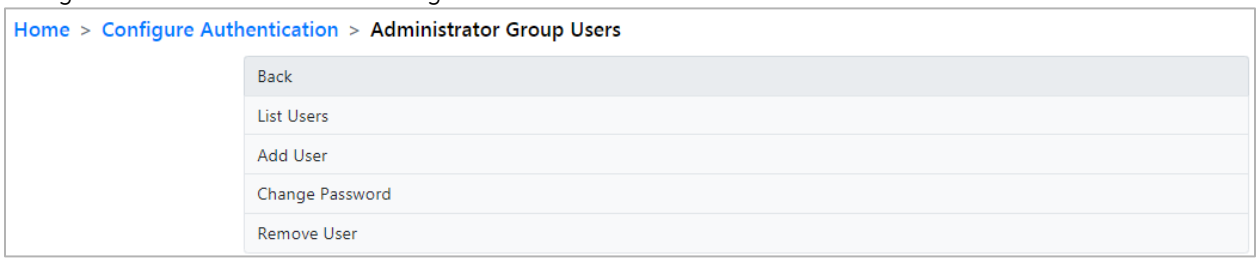
- Click **No** to keep service enabled.
  - **RESULT:** Pop-up window appears showing the Operation Status, click **OK.**



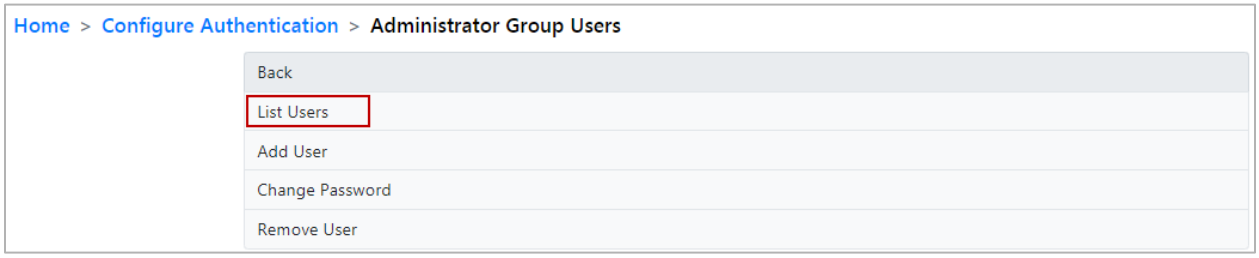
Administrator Group Users

1. Click **Administrator Group Users** tab.

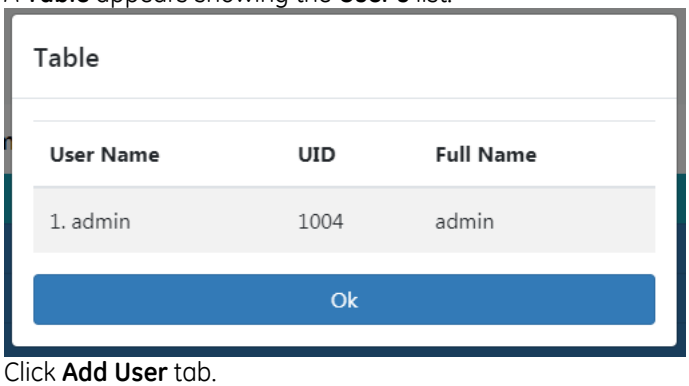
2. Use this function to create administrator-level users (if you are using local authentication mode) and to change details associated with existing administrator user accounts.



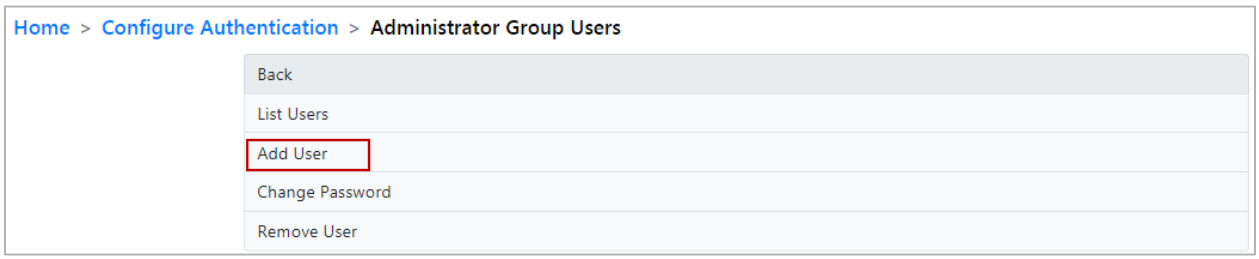
3. Click **List Users** tab.



4. A **Table** appears showing the **User's** list.

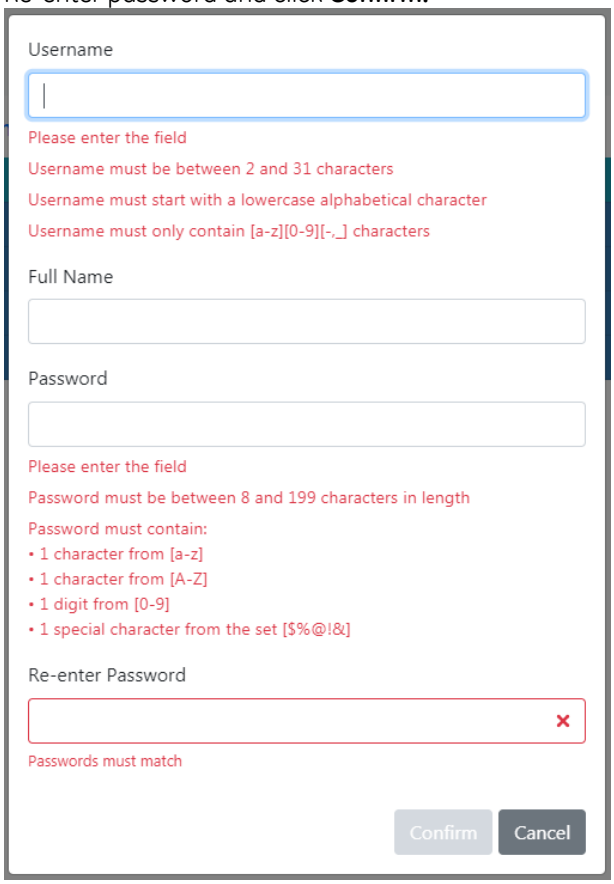


5. Click **Add User** tab.

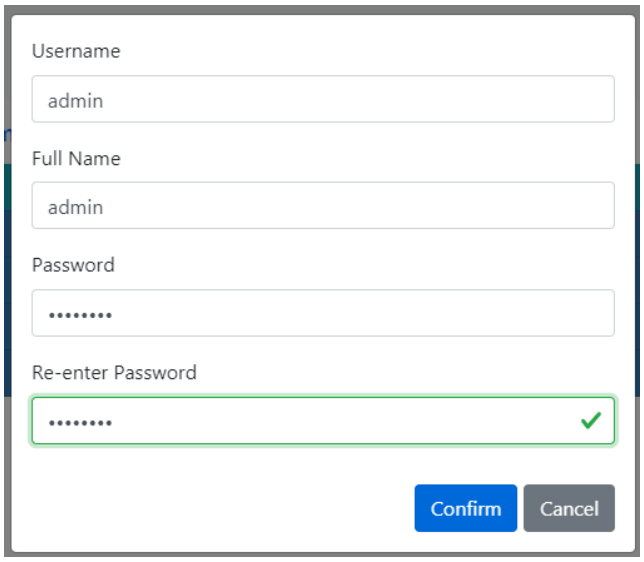


6. Enter the desired **Username**, conforming to the username rules as listed below:
   - Username must be between 2 and 31 characters.
   - Username must start with a lowercase alphabetical character.
   - Username must only contain [a-z][0-9][-,_] characters.
7. Enter the **Full Name** of the user.
8. Enter the **Password**, conforming to the password security rules as listed below:
   - Password must be between 8 and 199 characters in length
   - Password must contain:
     - 1 character from [a-z]
     - 1 character from [A-Z]
     - 1 digit from [0-9]
     - 1 special character from the set [$%@!&]

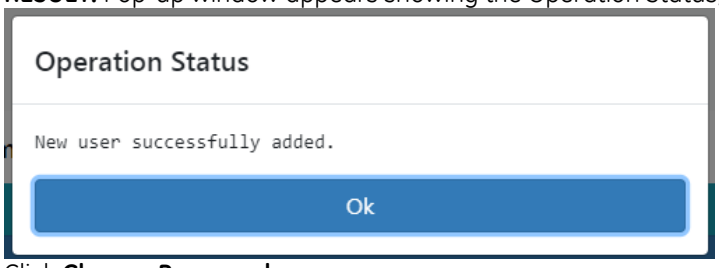
- Re-enter password and click **Confirm.**



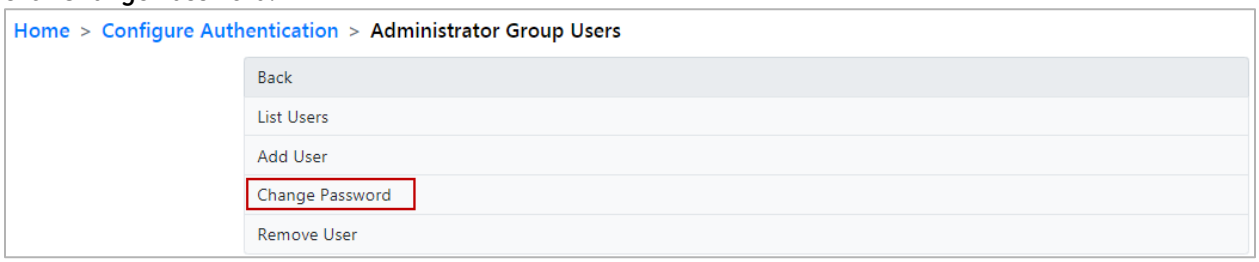
9. Click **Confirm.**



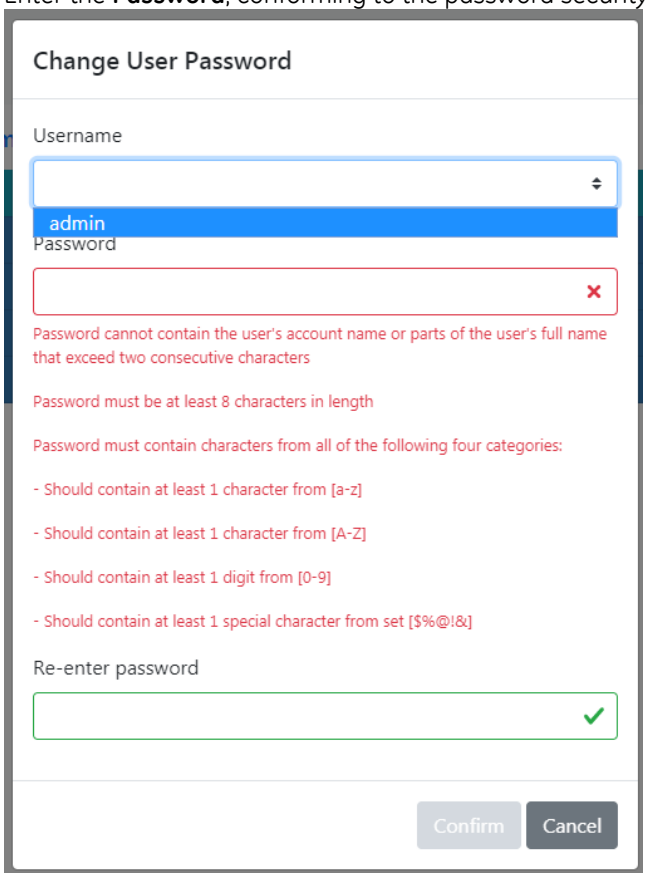
10. **RESULT:** Pop-up window appears showing the Operation Status, click **OK.**



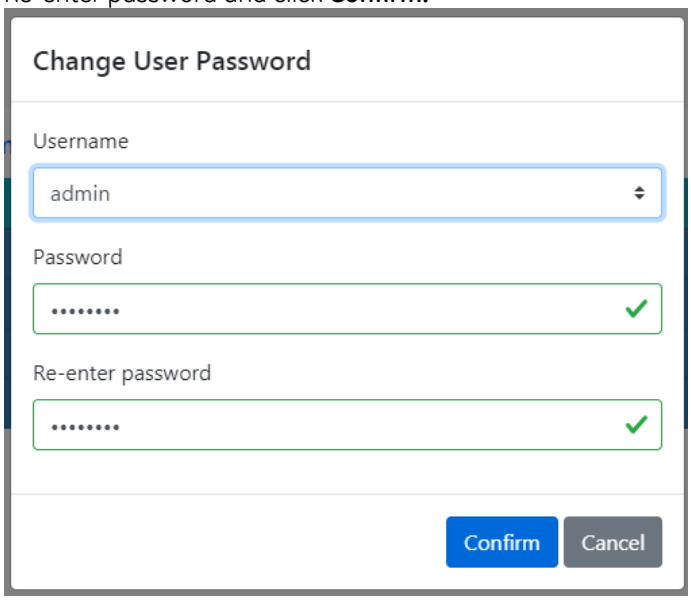
11. Click **Change Password.**



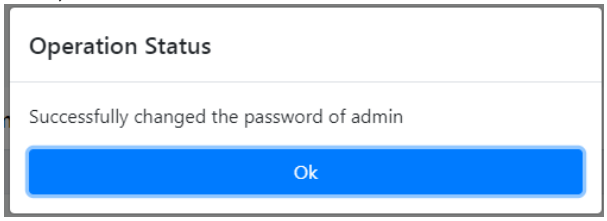
12. Select **Username** from the drop-down list.
13. Enter the **Password**, conforming to the password security rules.



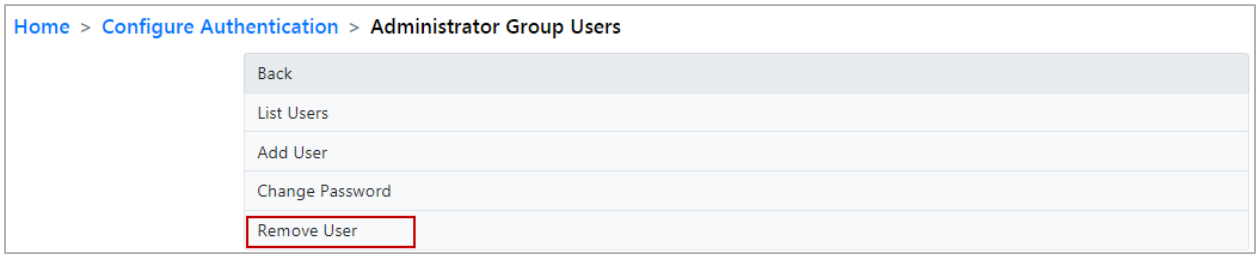
14. Re-enter password and click **Confirm.**



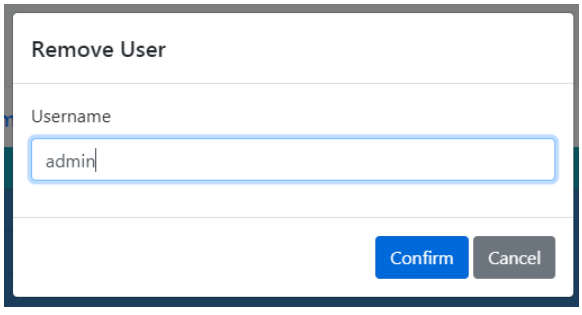
15. **RESULT:** Pop-up window appears showing the Operation Status: **Successfully changed the Password of User**, click **OK.**



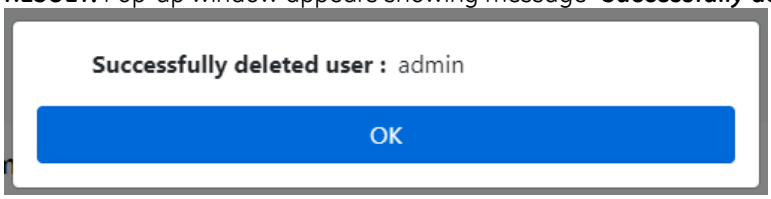
16. Click **Remove User** tab.



17. Enter the Username which needs to be removed and click **Confirm.**



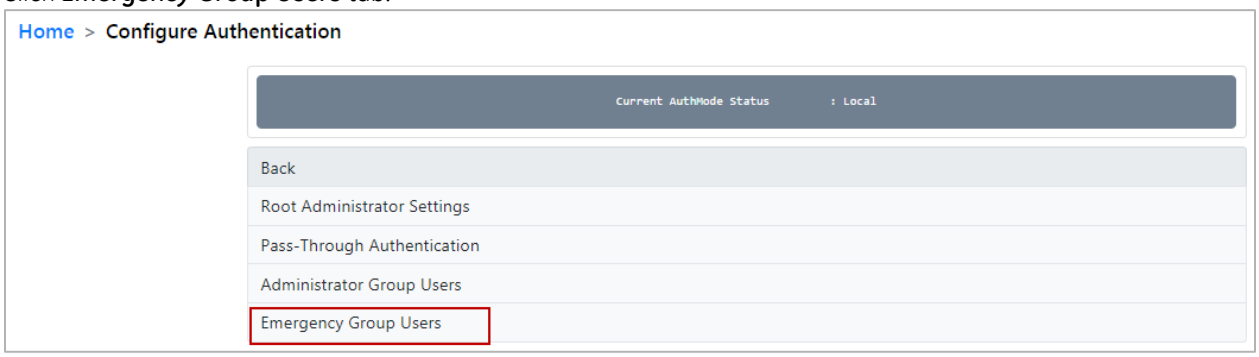
18. **RESULT:** Pop-up window appears showing message "**Successfully deleted user : <Username>"**



19. Click **OK.**

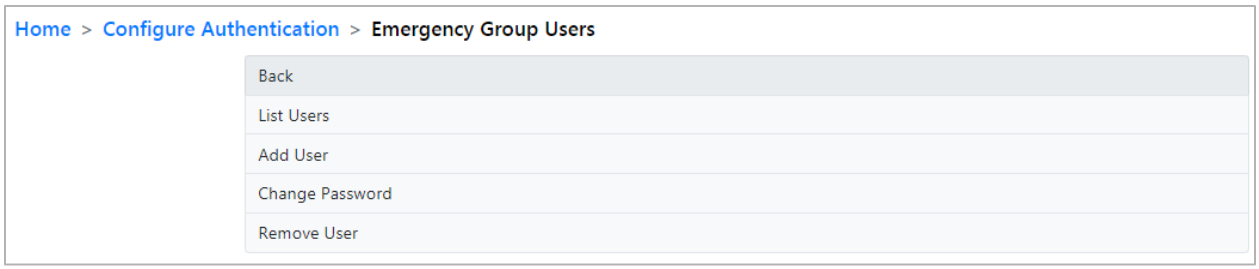
Emergency Group Users

1. Click **Emergency Group Users** tab.

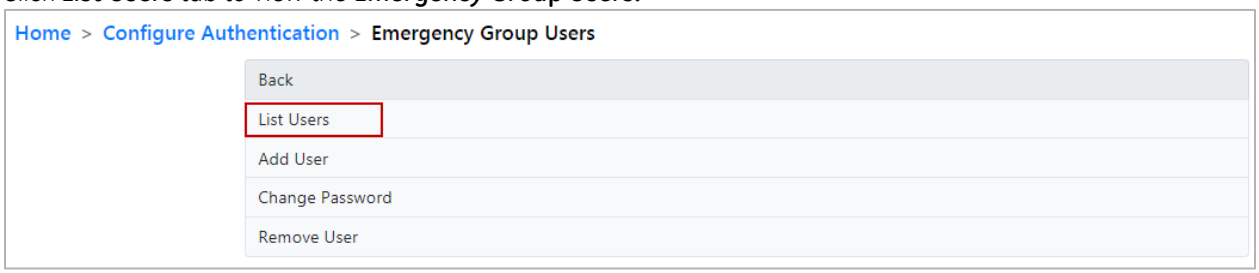


2. This function allows user to add/delete/modify emergency users for MCP. Adding emergency user is mandatory before changing the authentication from Local to Remote (LDAP /TACACS) Authentication. This emergency user can be used when remote authentication server is not available, and user is not able to access MCP with remote authentication. In this case emergency administrator user will be allowed to login MCP and perform two key functions:
3. Change the mode authentication from remote to local mode.
4. Generate emergency code to login HMI without changing authentication from remote to local mode.

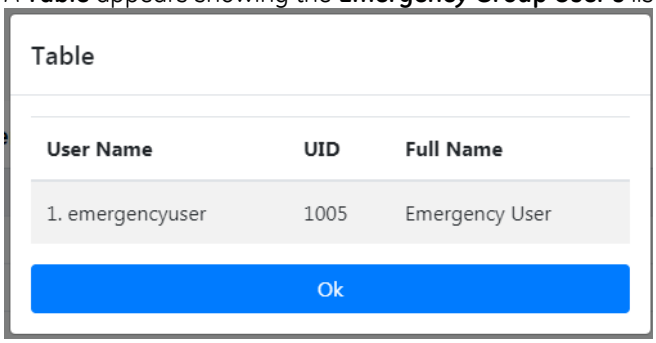
   User can perform above two functions by using **"emergcfg"** command after login emergency user on any of the below three interfaces:
   1. SSH session to MCP (Port-922)
   2. Serial maintenance port connection to MCP (Baud Rate- 115200)
   3. MCP Emergency option in local console (KVM)



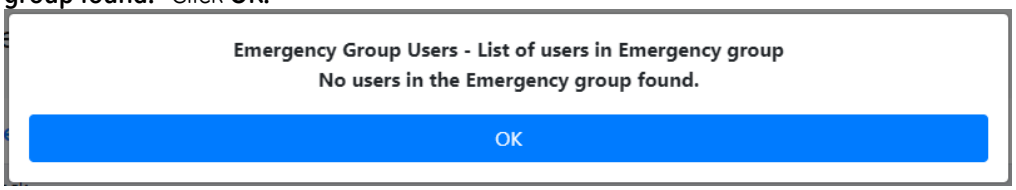
5. Click **List Users** tab to view the **Emergency Group Users.**



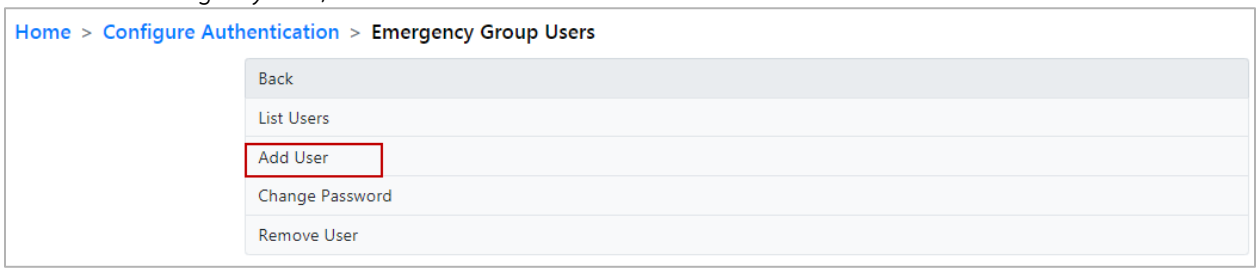
6. A **Table** appears showing the **Emergency Group User's** list.



7. If no users are added, then a pop-up window appears showing a message **"No users in the Emergency group found."** Click **OK.**

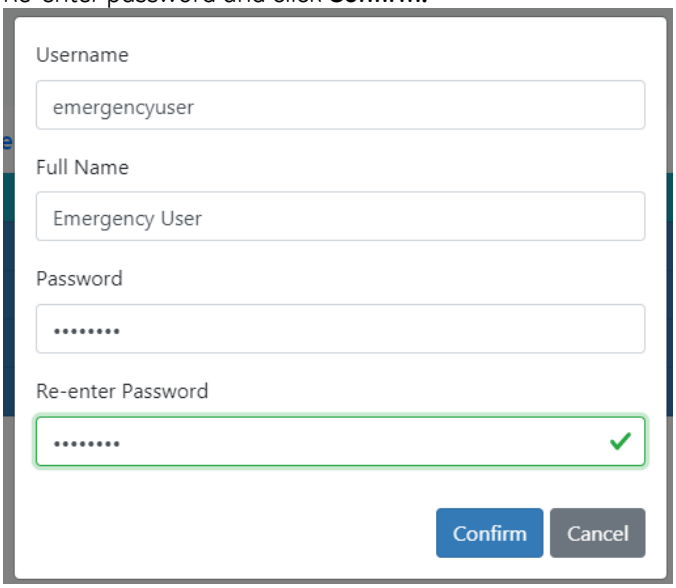


8. To add new emergency user, click **Add User** tab.

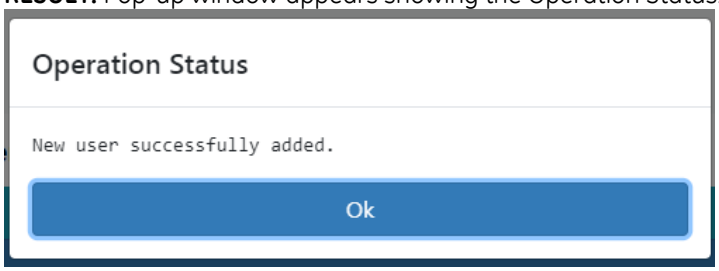


9. Enter the desired Emergency Group **Username**, conforming to the emergency group username rules as listed below:
    - Emergency Group Username must be between 2 and 31 characters.
    - Emergency Group Username must start with a lowercase alphabetical character.
    - Emergency Group Username must only contain [a-z][0-9][-,_] characters.
10. Enter the **Full Name** of the emergency group user.
11. Enter the **Password**, conforming to the password security rules as listed below:
    - Password must be between 8 and 199 characters in length
    - Password must contain:
        - 1 character from [a-z]
        - 1 character from [A-Z]
        - 1 digit from [0-9]
        - 1 special character from the set [$%@!&]

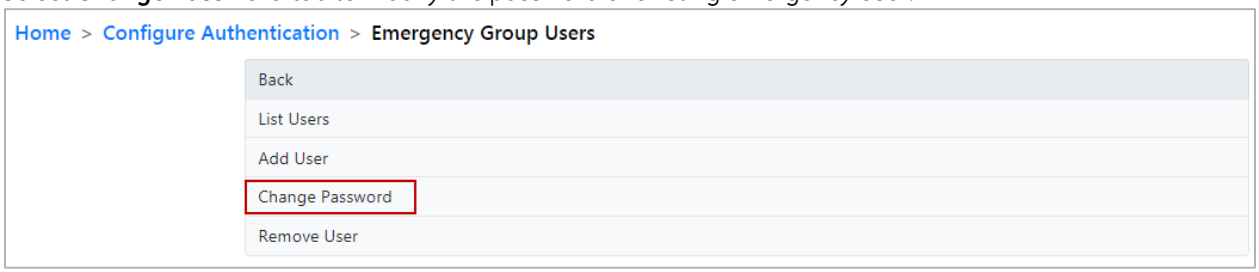
- Re-enter password and click **Confirm.**



12. **RESULT:** Pop-up window appears showing the Operation Status: **New user successfully added**, click **OK.**

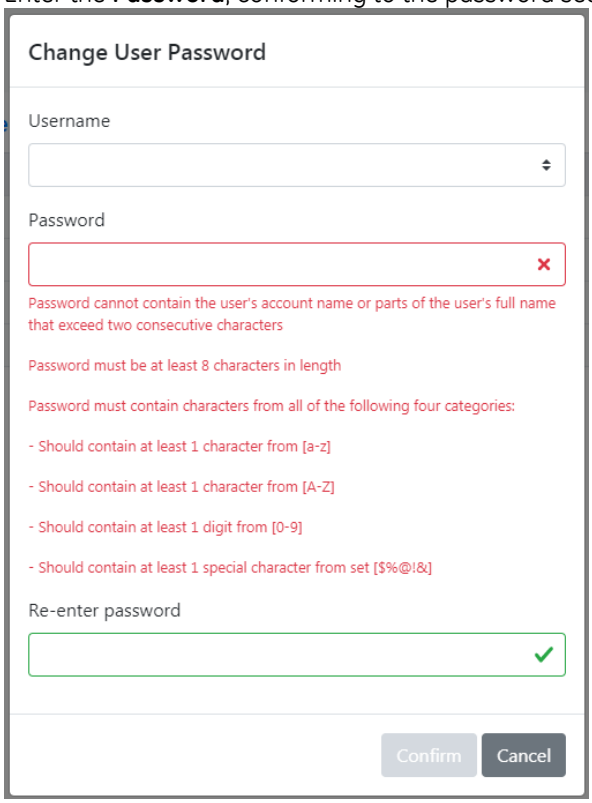


13. Select **Change Password** tab to modify the password of existing emergency user.

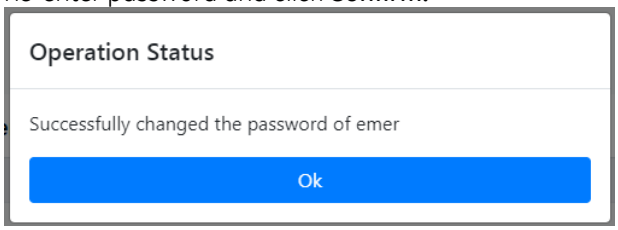


14. Select the **Emergency Group Username** from the drop-down list.

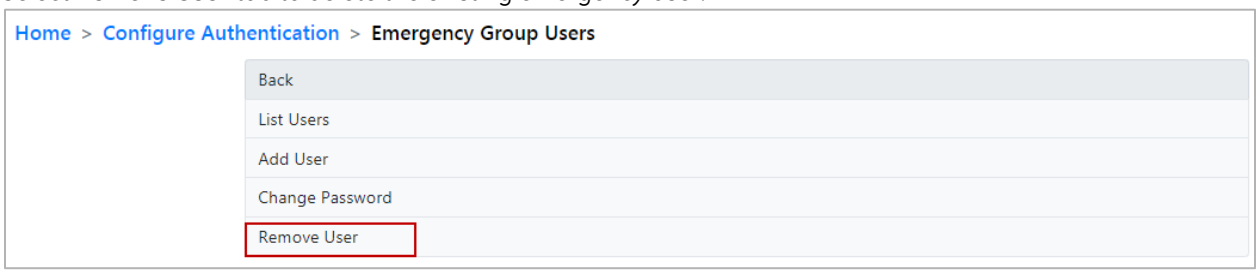
15. Enter the **Password**, conforming to the password security rules.



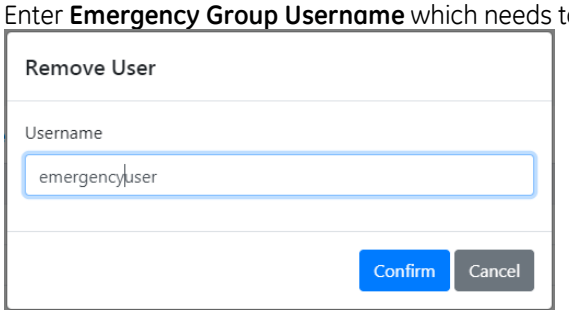
16. Re-enter password and click **Confirm.**



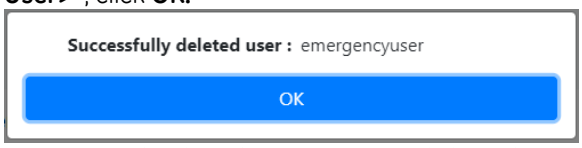
17. Click **OK.**
18. Select **Remove User** tab to delete the existing emergency user.



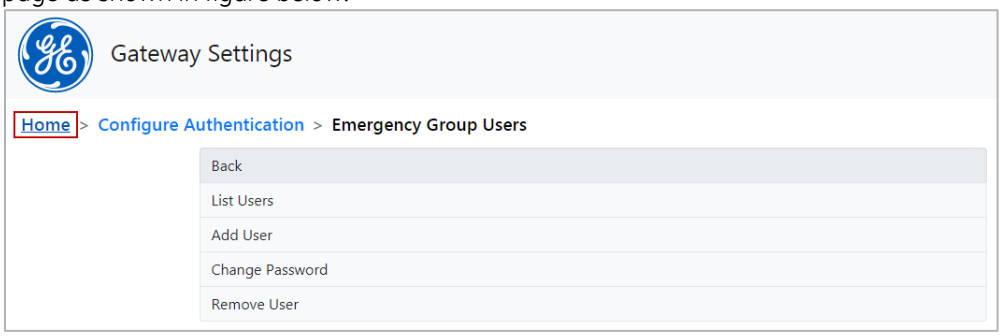
19. Enter **Emergency Group Username** which needs to be removed and click **Confirm.**



20. **RESULT:** A pop-up window appears showing a message **"Successfully deleted user : <Emergency Group User>"**, click **OK.**

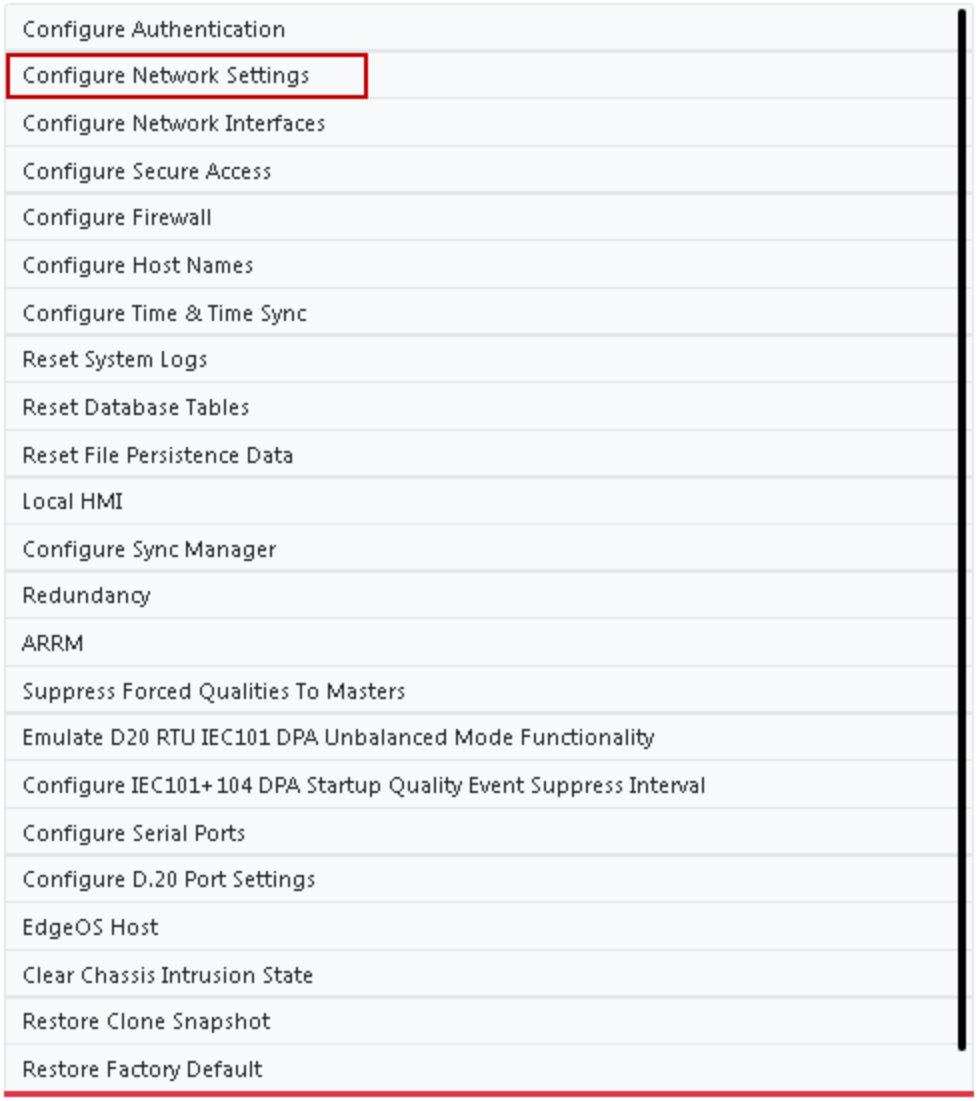


21. To navigate back to the **Main Menu**, click on the **Home** link which is located at the upper left corner of the page as shown in figure below.

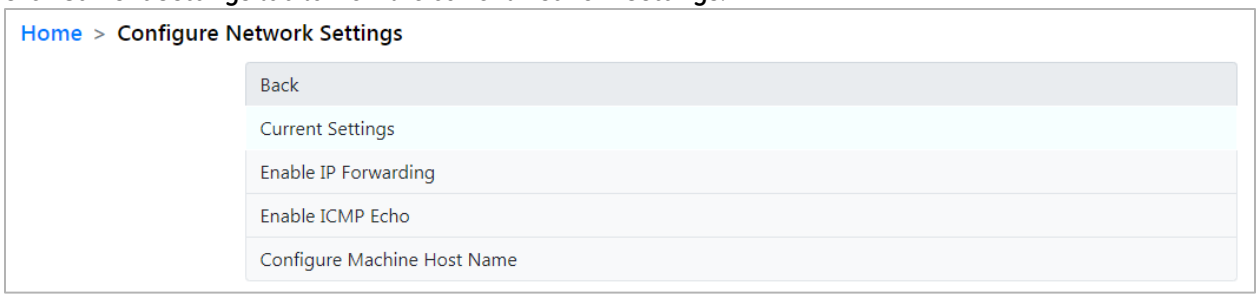


Configure Network Settings

1. Click **Configure Network Settings** tab from the main menu.

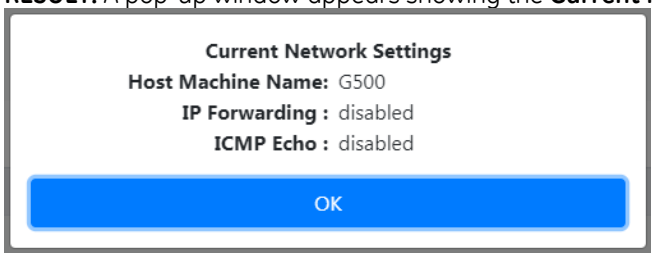


2. Click **Current Settings** tab to view the current **Network Settings**.



Current Settings

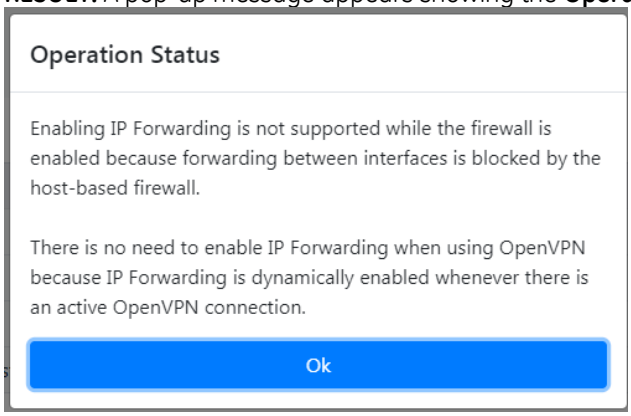
1. **RESULT:** A pop-up window appears showing the **Current Network Settings.** Click **OK.**



Enable IP Forwarding

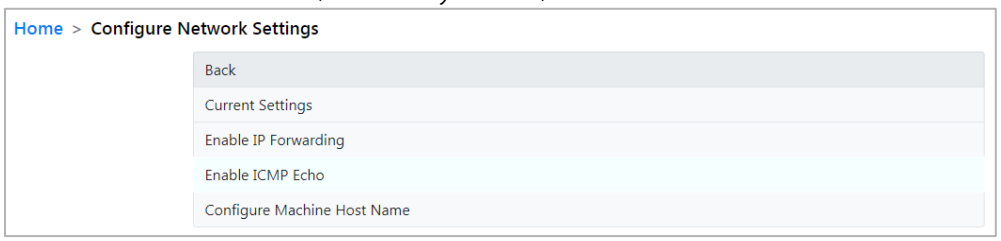
1. Click **Enable IP Forwarding** tab.

2. **RESULT:** A pop-up message appears showing the **Operation Status**. Click **OK.**

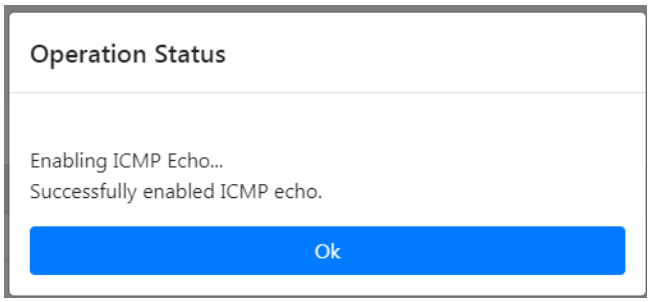


Enable ICMP Echo

1. Click **Enable ICMP Echo** tab (Disabled by Default).

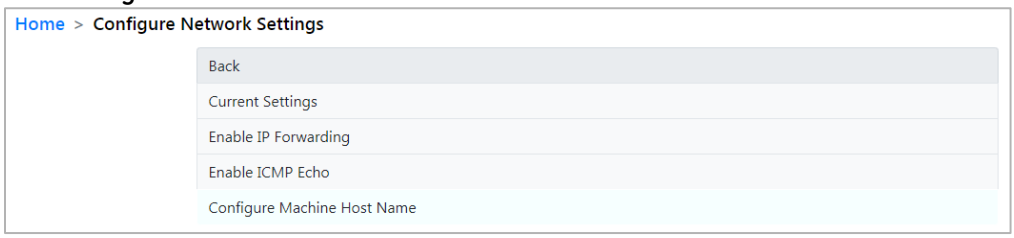


2. **RESULT:** A pop-up message appears showing the **Operation Status: Successfully enabled ICMP echo**, click **OK.**



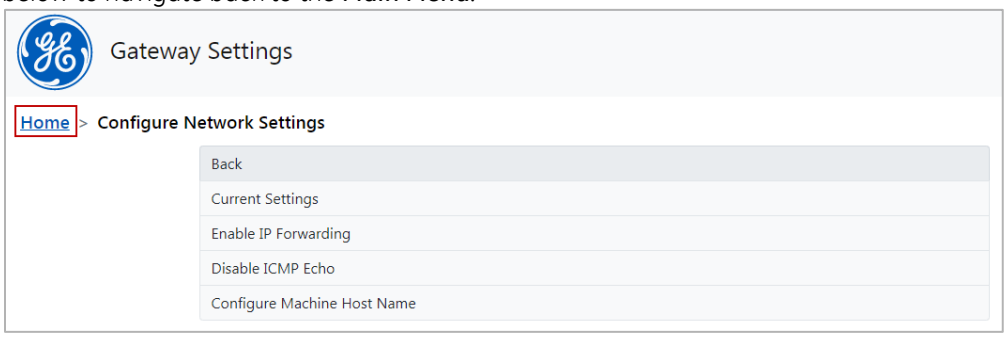
Configure Machine Host Name

1. Click **Configure Machine Host Name** tab.



2. Enter new Machine Name [MCP] : **<new machine name>** and click **Confirm.**

3. **RESULT:** A pop-up message appears showing the **Operation Status**, click **OK** and reboot for changes to take effect.
4. Click **Back** or click on the **Home** link which is located at the upper left corner of the page as shown in figure below to navigate back to the **Main Menu**.

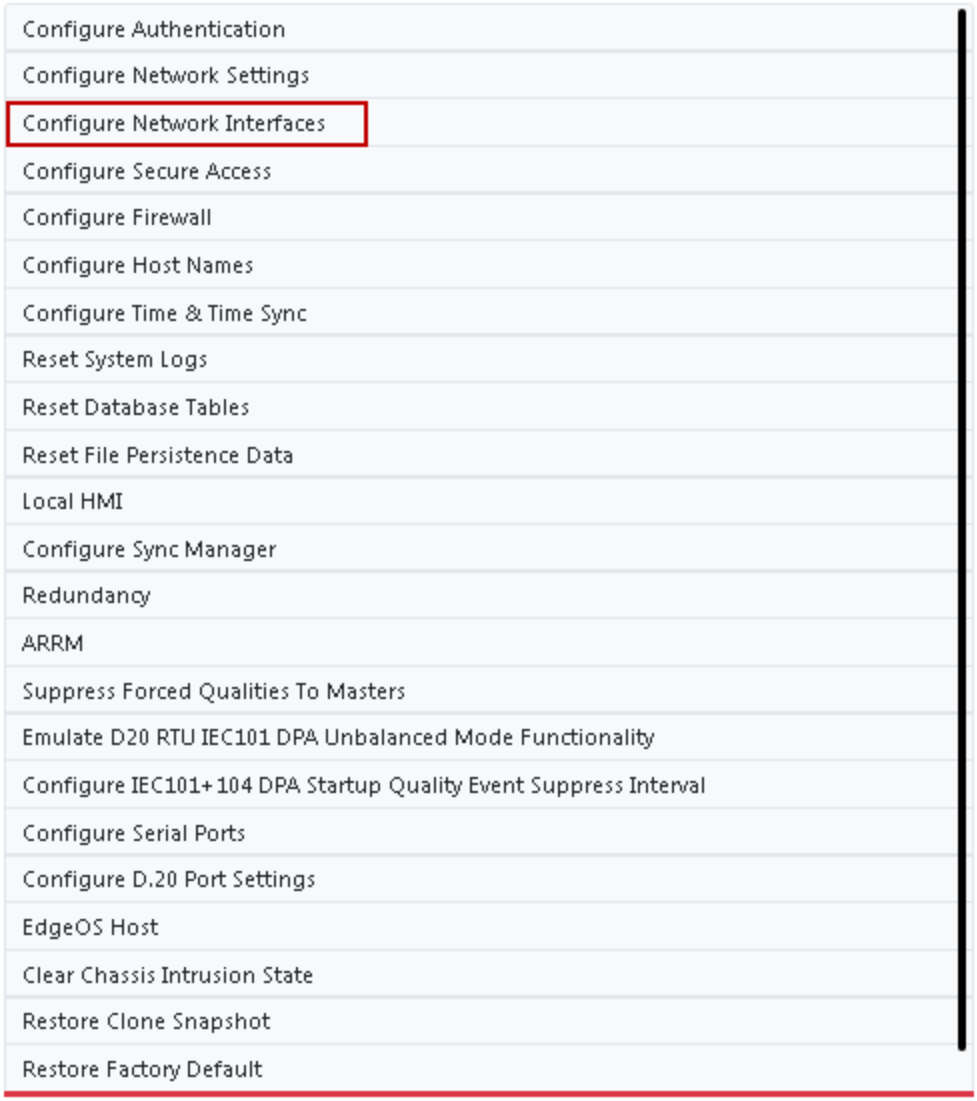


Configure Network Interfaces

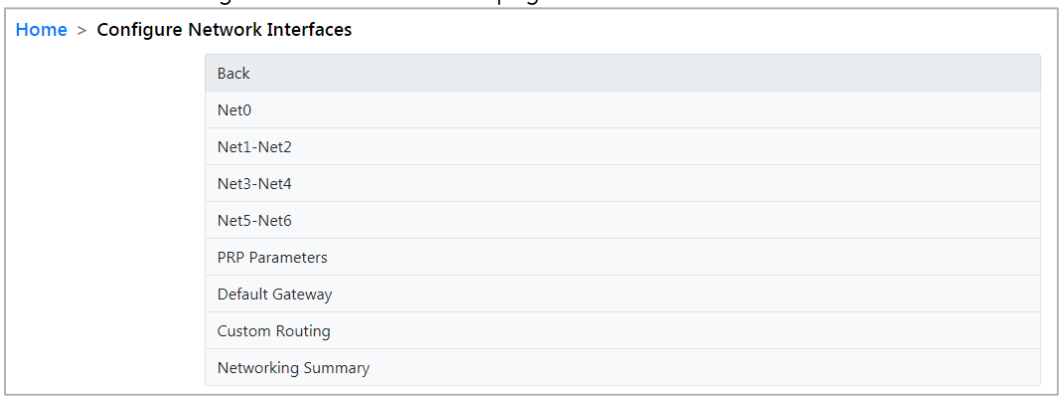
The Network Interface allows you to configure the settings for the MCP's network connections.

NOTE: The MCP must be rebooted to activate any changed network settings.
On first time use of MCP, user can login to web interface using default enabled network interface (G100 Net1 / G500 Net0 with IP: 192.168.168.81) with defadmin credentials. The user will then be prompted to create an admin user; who can then login later and continue to setup the MCP.

1. Click **Configure Network Interfaces** tab from the main menu.

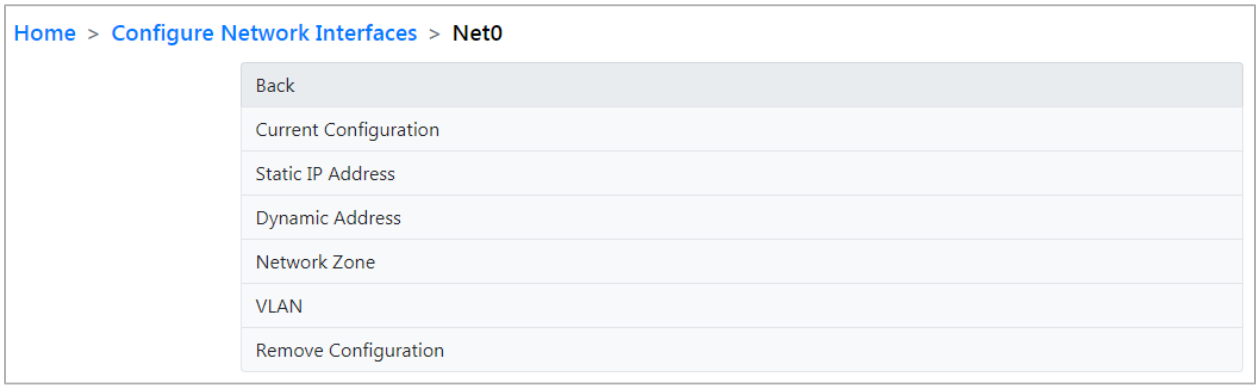


2. You can see a menu showing the Network Interfaces on the screen. To explore them use the menu options shown on the Configure Network Interfaces page as shown below:

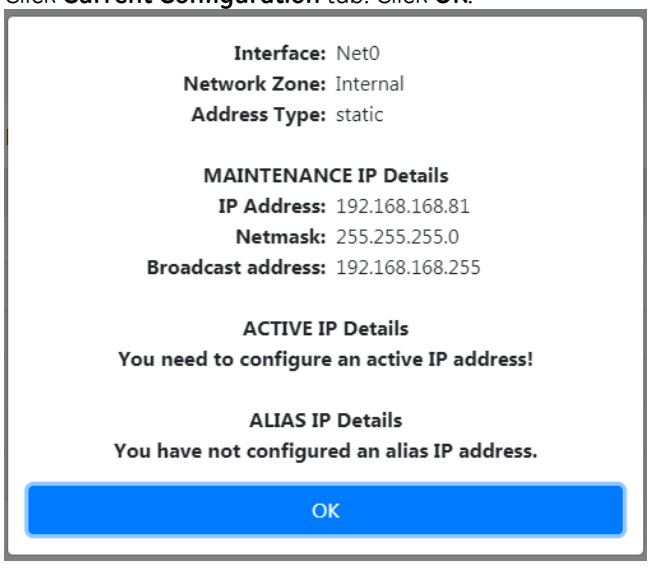


Net0 (G500 only)

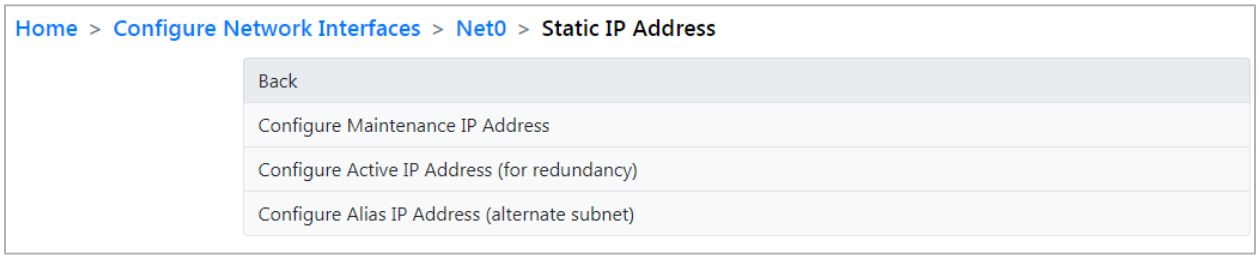
1. Click **Net0** tab.



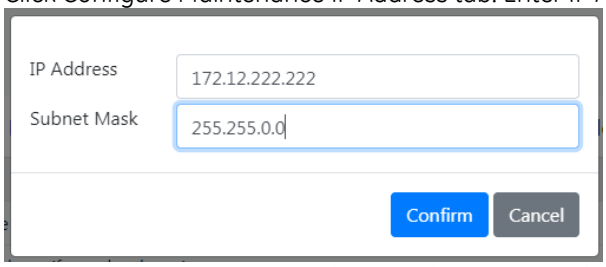
2. Click **Current Configuration** tab. Click **OK**.



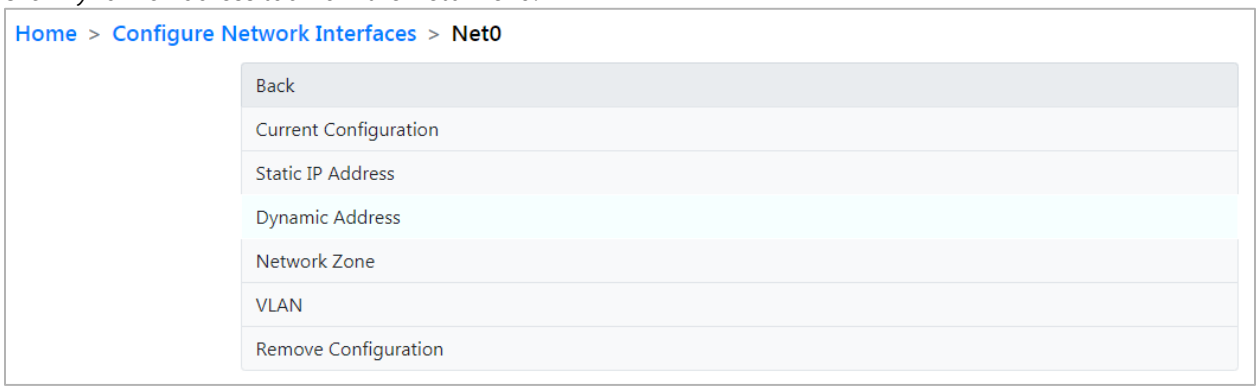
3. Click Static IP Address tab.



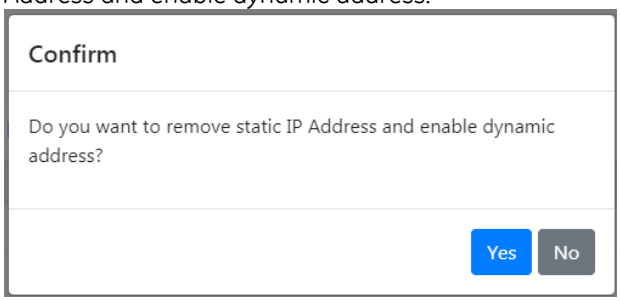
4. Click Configure Maintenance IP Address tab. Enter IP Address and Subnet Mask. Click Confirm.



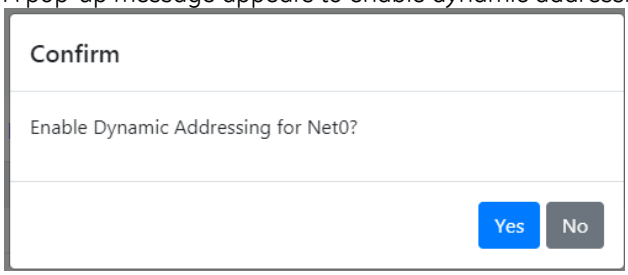
5. A pop-up message appears showing the newly-configured static IP settings, click Yes to accept it and reboot the device for changes to take effect or click No to abort the changes.
6. Click Configure Active IP Address (for redundancy) tab from the Net0 > Static IP Address menu.
7. Enter IP Address, Subnet Mask and click Confirm.
8. A pop-up message appears showing the newly-configured static IP settings, click Yes to accept the settings or No to abort the settings.
9. Click Configure Alias IP Address (alternate subnet) tab from the Net0 > Static IP Address menu.
10. Enter IP Address, Subnet Mask and click Confirm.
11. A pop-up message appears showing the newly-configured static IP settings, click Yes to accept the settings or No to abort the settings.
12. Click Back to navigate to Net0 menu.
13. Click Dynamic Address tab from the Net0 menu.



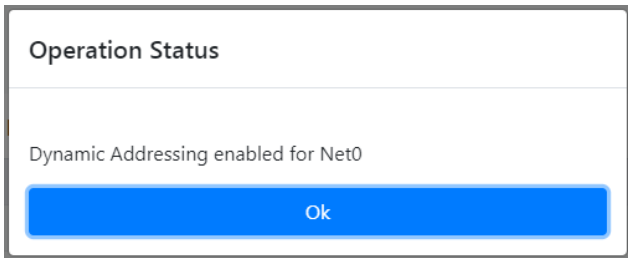
14. A pop-up message appears if the Static IP Address is already configured, click Yes to remove static IP Address and enable dynamic address.



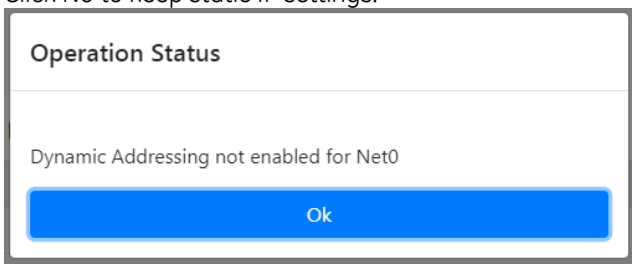
15. A pop-up message appears to enable dynamic addressing for Net0.



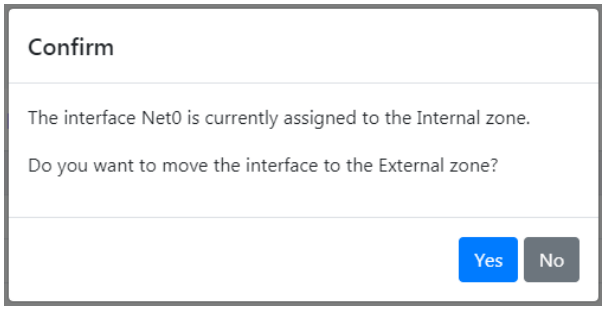
- Click Yes to enable.



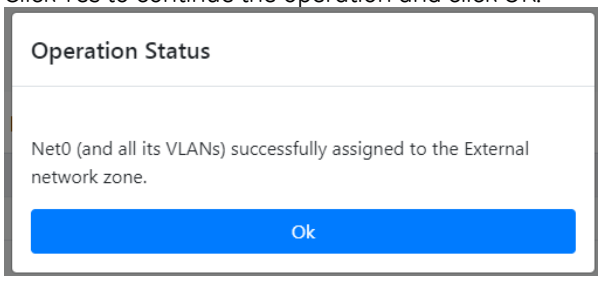
- Click No to keep static IP settings.



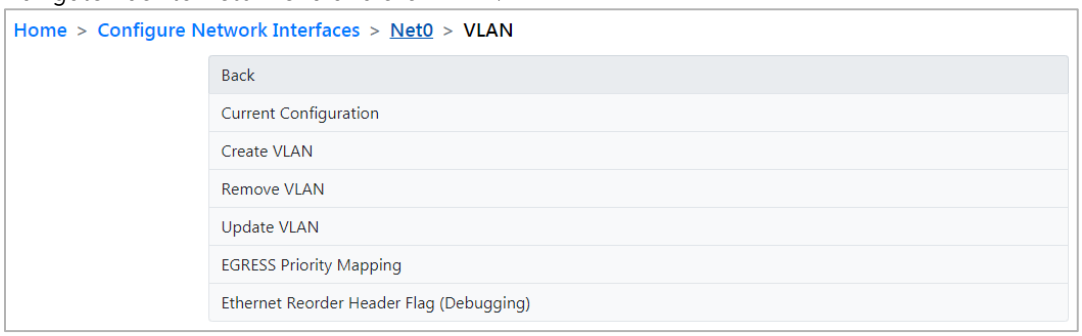
16. Click Network Zone tab from the Net0 menu.
17. Click Yes to move the Net0 interface from Internal to External zone.



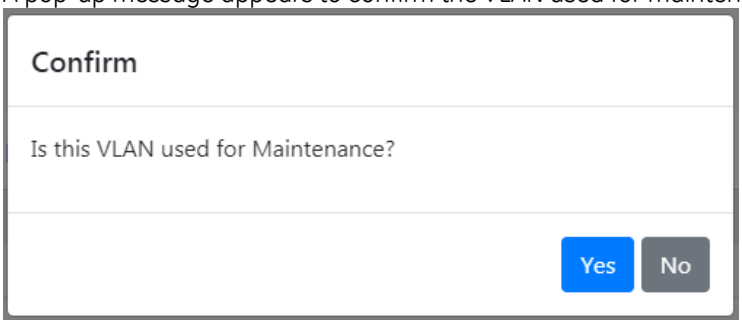
18. A WARNING message appears stating that all the interfaces VLANs will be assigned to the External zone.
    - Click No to abort the operation.
    - Click Yes to continue the operation and click OK.



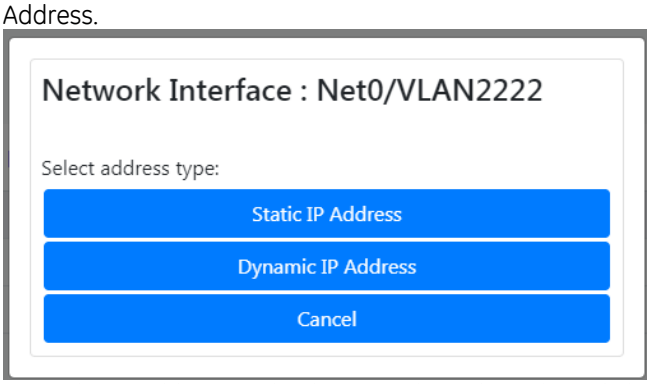
19. Navigate Back to Net0 menu and click VLAN.



20. Click Create VLAN tab.
    - Enter new VLAN ID (2-4094).
    - A pop-up message appears to confirm the VLAN used for maintenance.



      - Network Interface message appears, select address type: Static or Dynamic IP Address.

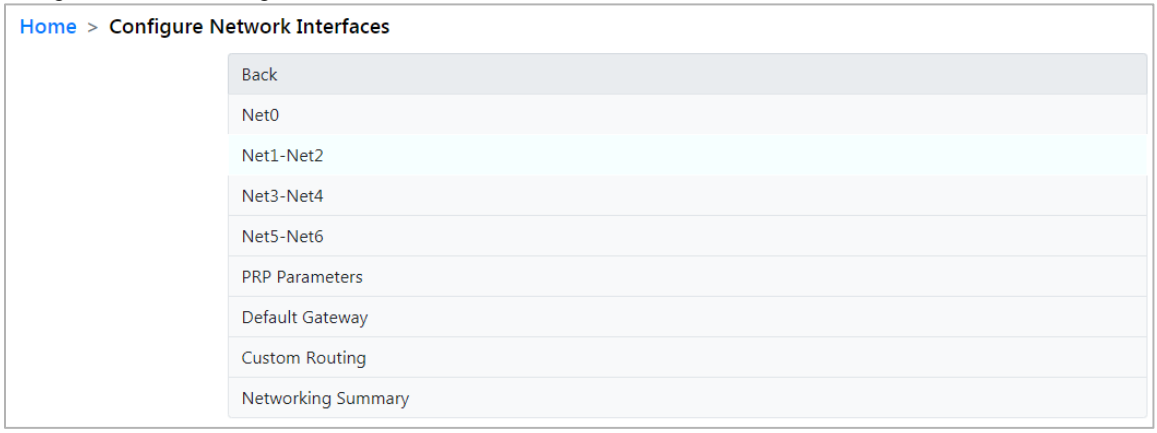


      - Enter the IP Address and Subnet Mask credentials and click Confirm.
      - A confirmation message appears showing the newly-configured IP settings, click Yes to accept it and reboot the device for changes to take effect or click No to abort the changes.
      - RESULT: VLAN ID created, click OK.
21. Navigate back to VLAN menu and click Remove VLAN.
22. Select the VLAN ID which needs to be removed from the list shown on the screen.
23. Click Yes to confirm or No to abort.
24. RESULT: Operation Status appears on the screen based on your action.
25. Navigate back to VLAN menu and click Update VLAN.
26. For updating the VLAN IP Address, click Update IP Address and select address type: Static or Dynamic IP Address.
27. Enter the IP Address and Subnet Mask credentials and click Confirm.
28. A confirmation message appears showing the newly-configured IP settings, click Yes to accept it and reboot the device for changes to take effect or click No to abort the changes.
29. RESULT: VLAN ID created, click OK.

30. Click Network Zone to check the current status of VLAN and select Yes or No to move the interface from External zone to Internal zone and vice-versa.
31. Navigate back to VLAN menu and click Remove VLAN.
32. Select EGRESS Priority Mapping and select the VLAN ID from the list.
33. Select Current Configuration to view the socket priority.
34. Select Set Priority Mapping and enter the value based upon the credentials listed below and click Confirm.
    - 7 (Highest) - Network management
    - 6 - Voice
    - 5 - Video
    - 4 - Controlled load
    - 3 - Excellent effort
    - 2 - Undefined
    - 1 (Lowest) - Background
    - 0 (Routine) - Best effort
35. Navigate back to VLAN menu and click Remove VLAN.
36. Select Ethernet Reorder Header Flag (Debugging) and select the VLAN ID.
37. Click Yes to set VLAN Ethernet reorder header flag or No to abort.
38. Navigate Back to Net0 menu and select Remove Configuration.
39. Click Yes to take Net0 Settings Backup or No to continue.
40. A confirmation message appears showing the Backup file location and the settings which will be removed for Net0. Click Yes to confirm or No to abort.
41. RESULT; A message appears showing the Operation Status: Net0 successfully assigned into its default network zone.
42. Click OK and reboot the device for changes to take effect.

Other Network Interfaces

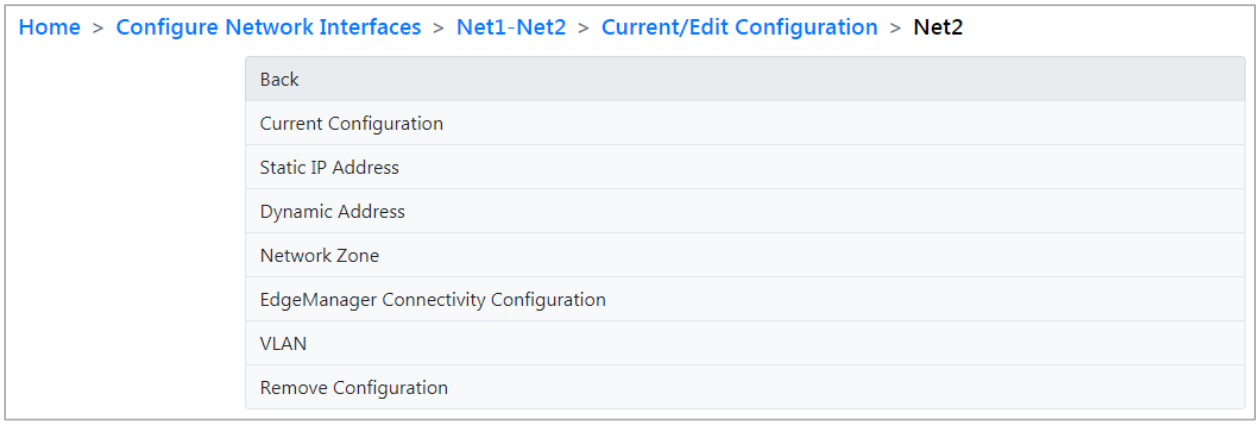
1. Navigate Back to Configure Network Interfaces menu and select Net1-Net2.



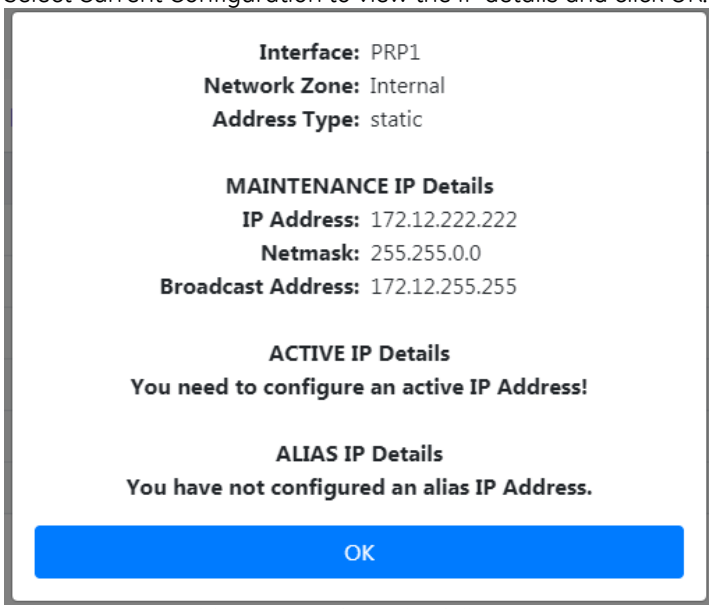
2. Select Single tab and click Yes to change the mode for Net1-Net2.
3. RESULT: Operation Status – Net1Net2 Mode is updated to Single. Click OK.
4. Select Redundant tab you will see a message that this is not supported in the device.
5. Select PRP tab from Net1-Net2 menu
    - PRP is supported only in G500, is not supported in G100.

Select Current/Edit Configuration and select specified network interface.

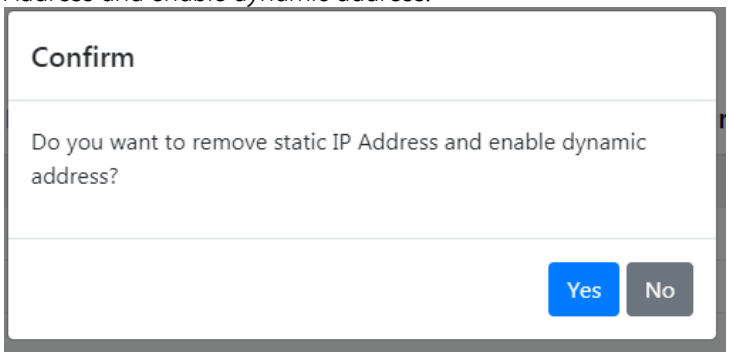
Note: Refer to Chapter 8 - EdgeManager and PETC for port availability and additional information.

6. 

7. Select Current Configuration to view the IP details and click OK.



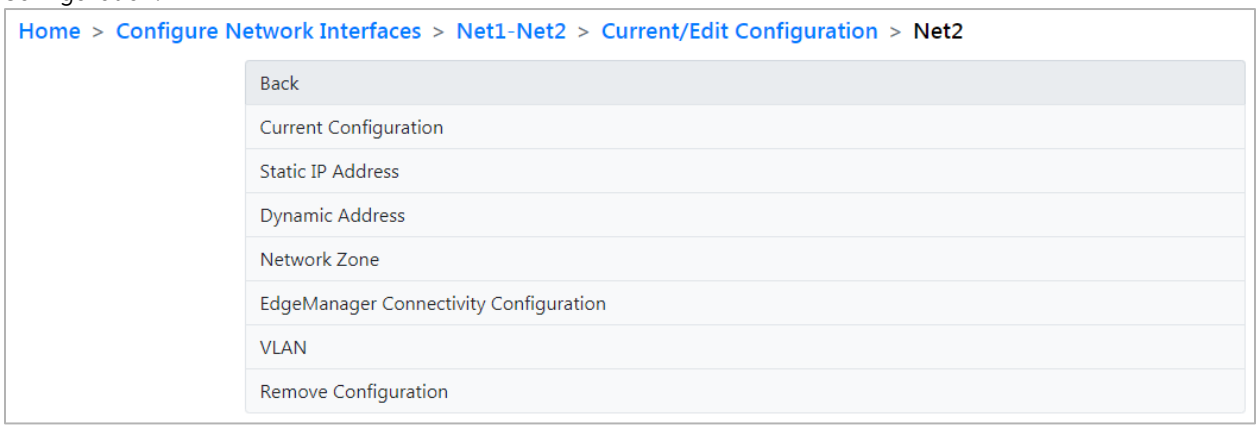
8. Select Static IP Address to perform the following operations:
   - Configure Maintenance IP Address
   - Configure Active IP Address (for redundancy) – Not available in G100
   - Configure Alias IP Address (alternate subnet)
9. Select the specified option as per your requirement and enter the IP Address and Subnet Mask credentials and select Confirm to proceed.
10. Navigate back to Current/Edit Configuration menu and select Dynamic Address.
11. If the static IP Address is already configured, then a confirmation message appears to remove static IP Address and enable dynamic address.



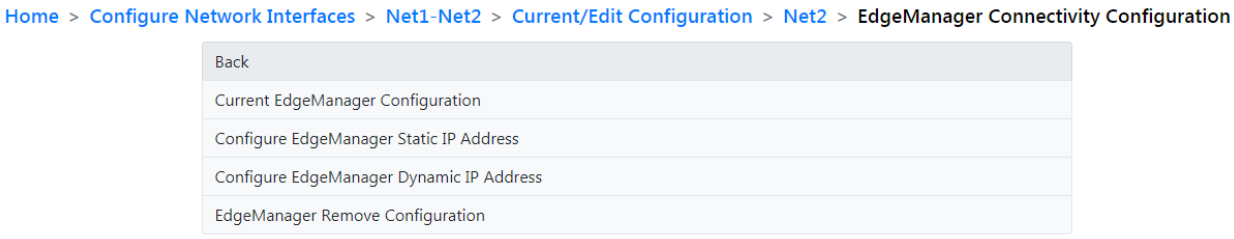
   - Click No to abort.

- Click Yes to Enable Dynamic Addressing for a specific Network Interface Mode.
- Click Yes to confirm.
- RESULT: Operation Status – Dynamic Addressing enabled for a specific Network Interface mode.

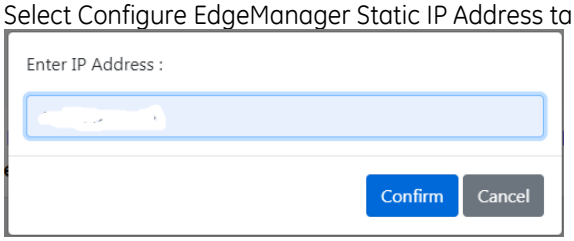
12. Click Network Zone to check the current status of Network Interface and select Yes or No to move the Interface from External zone to Internal zone and vice-versa.
13. Navigate Back to Net1-Net2 > Current/Edit Configuration menu and click EdgeManager Connectivity Configuration.



14. This function enables you to configure:

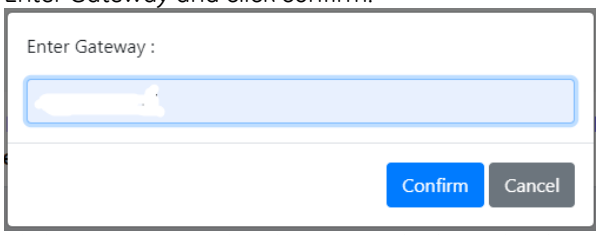


15. Select Current EdgeManager Configuration tab to view available configuration for EdgeManager Connectivity.
16. Select Configure EdgeManager Static IP Address tab and enter IP Address and click confirm:

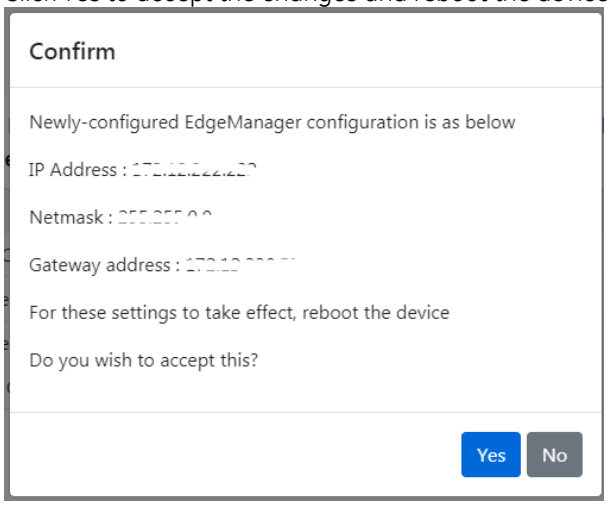


17. Enter Netmask and click confirm:

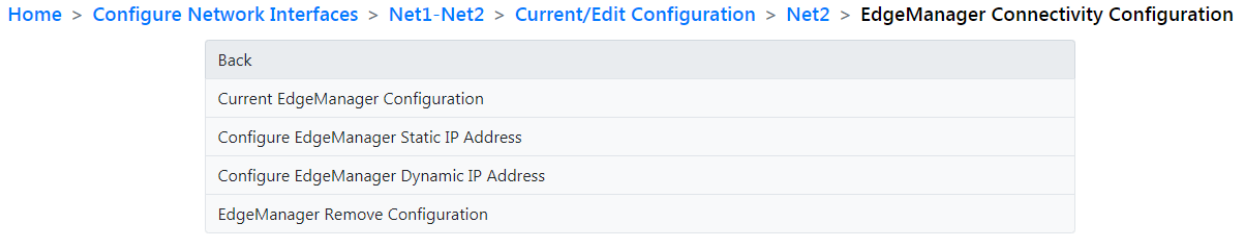
18. Enter Gateway and click confirm:



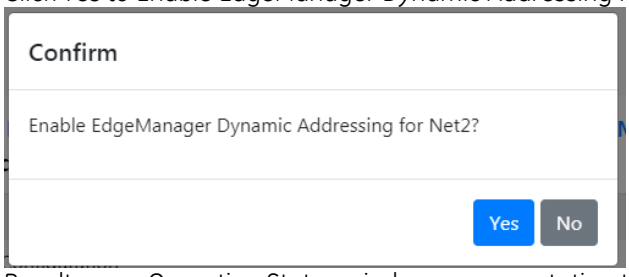
19. Click Yes to accept the changes and reboot the device for the settings to take effect or No to abort:



20. Select Configure EdgeManager Dynamic IP Address tab from EdgeManager Connectivity Configuration menu:



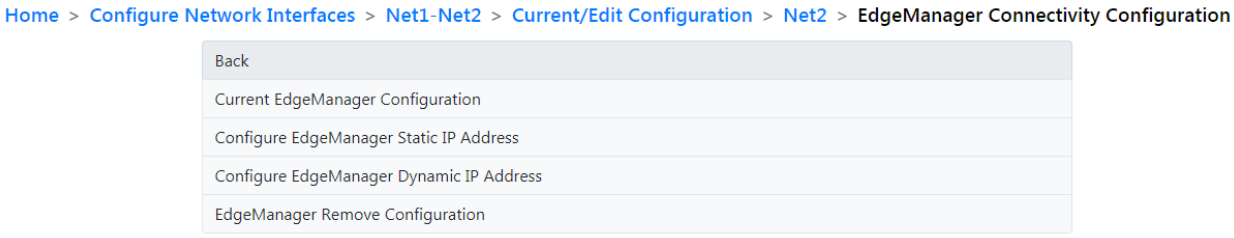
21. Click Yes to Enable EdgeManager Dynamic Addressing for selected port, or No to abort:



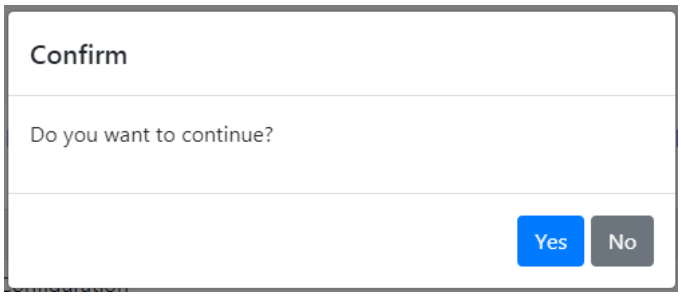
Result: Operation Status window appears stating the Dynamic Addressing enabled for EdgeManager Interface for the selected port.

Note: Reboot the device for the settings to take effect.

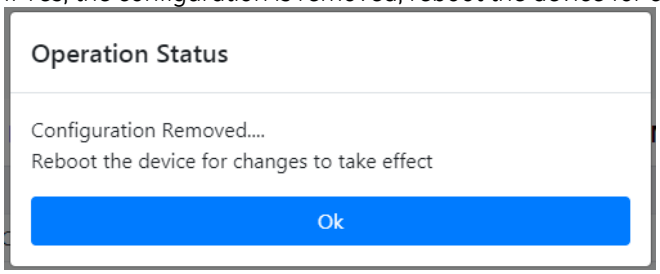
22. Select EdgeManager Remove Configuration tab from EdgeManager Connectivity Configuration menu:



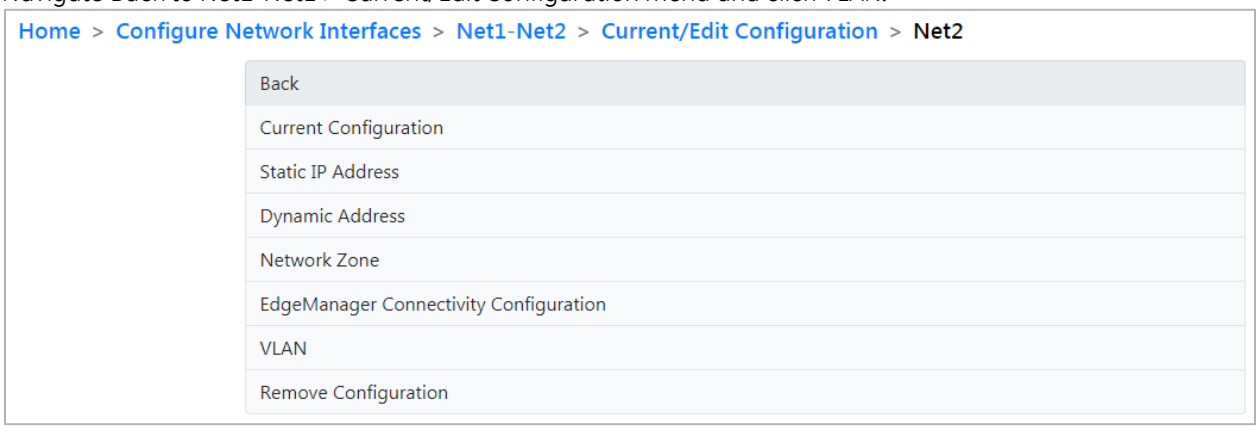
23. Click Yes to continue or No to abort:



- If Yes, the configuration is removed, reboot the device for changes to take effect. Click Ok.

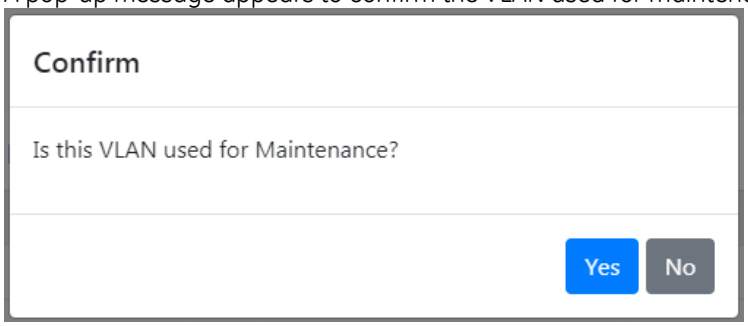


24. Navigate Back to Net1-Net2 > Current/Edit Configuration menu and click VLAN.

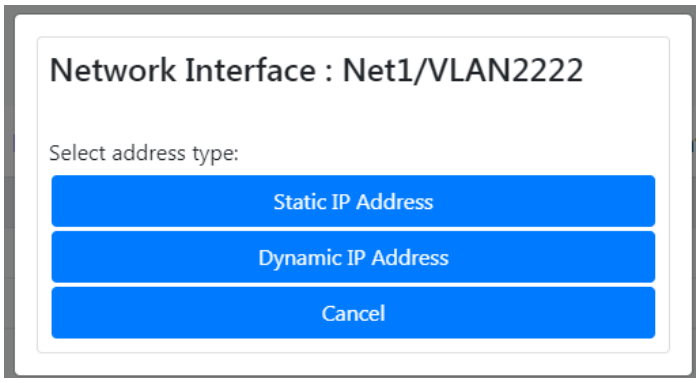


25. Click Create VLAN tab.
    - Enter new VLAN ID (2-4094).

- A pop-up message appears to confirm the VLAN used for maintenance.



  - Network Interface message appears, select address type: Static or Dynamic IP Address.



  - Enter the IP Address and Subnet Mask credentials and click Confirm.
  - A confirmation message appears showing the newly-configured IP settings, click Yes to accept it and reboot the device for changes to take effect or click No to abort the changes.
  - RESULT: VLAN ID created, click OK.

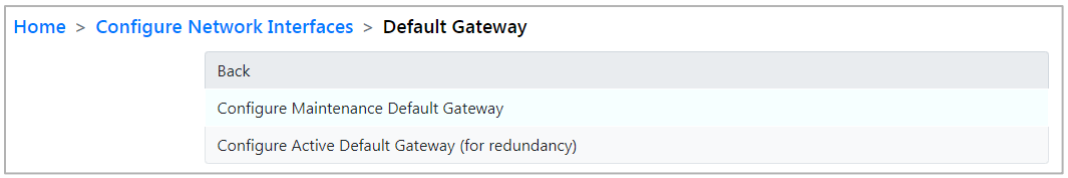
26. Navigate back to VLAN menu and click Remove VLAN.
27. Select the VLAN ID which needs to be removed from the list shown on the screen.
28. Click Yes to confirm or No to abort.
29. RESULT: Operation Status appears on the screen based on your action.
30. Navigate back to VLAN menu and click Update VLAN.
31. Select the VLAN ID which needs to be removed from the list shown on the screen.
32. For updating the VLAN IP Address, click Update IP Address and select address type: Static or Dynamic IP Address.
33. Enter the IP Address and Subnet Mask credentials and click Confirm.
34. A confirmation message appears showing the newly-configured IP settings, click Yes to accept it and reboot the device for changes to take effect or click No to abort the changes.
35. RESULT: VLAN ID created, click OK.
36. Click Network Zone to check the current status of VLAN and select Yes or No to move the interface from External zone to Internal zone and vice-versa.
37. Navigate back to VLAN menu and click Remove VLAN.
38. Select EGRESS Priority Mapping and select the VLAN ID from the list.
39. Select Current Configuration to view the socket priority.
40. Select Set Priority Mapping and enter the value based upon the credentials listed below and click Confirm.
    - 7 (Highest) - Network management
    - 6 - Voice
    - 5 - Video
    - 4 - Controlled load
    - 3 - Excellent effort
    - 2 - Undefined

- 1 (Lowest) - Background
- 0 (Routine) - Best effort

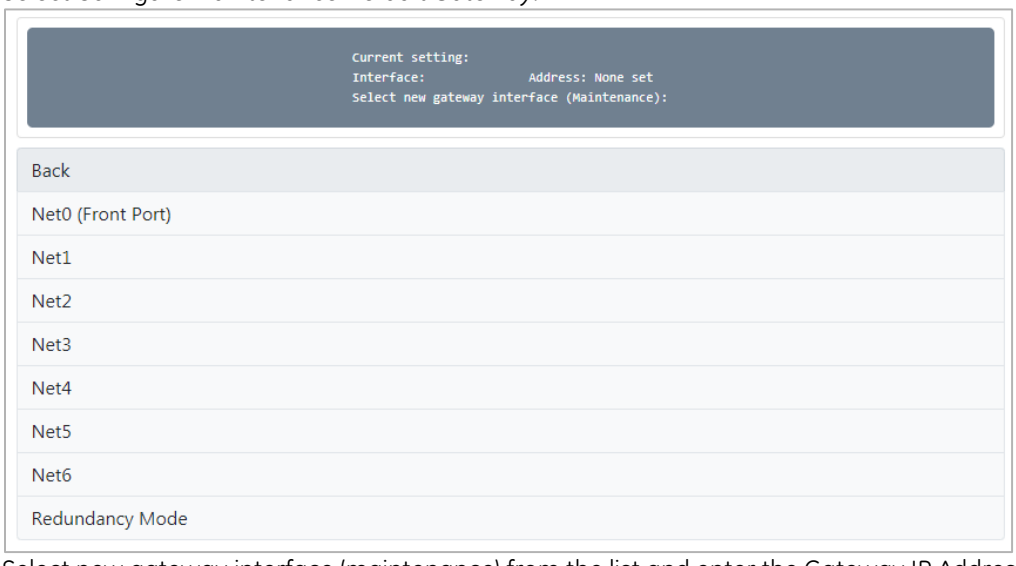
41. Navigate back to VLAN menu and click Remove VLAN.
42. Select Ethernet Reorder Header Flag (Debugging) and select the VLAN ID.
43. Click Yes to set VLAN Ethernet reorder header flag or No to abort.
44. Navigate back to Net1-Net2 > Current/Edit Configuration and select Remove Configuration.
45. Click Yes to take Network Interface Mode Settings Backup or No to continue.
46. A confirmation message appears showing the Backup file location and the settings which will be removed for that Network Interface. Click Yes to confirm or No to abort.
47. RESULT; A message appears showing the Operation Status: Net1 successfully assigned into its default network zone.
48. Click OK and reboot the device for changes to take effect.
49. Navigate back to Configure Network Interfaces menu and follow the same Net1-Net2 procedure for configuring Net3-Net4 Default Gateway

Default Gateway

1. Navigate back to Configure Network Interfaces menu and select Default Gateway tab.

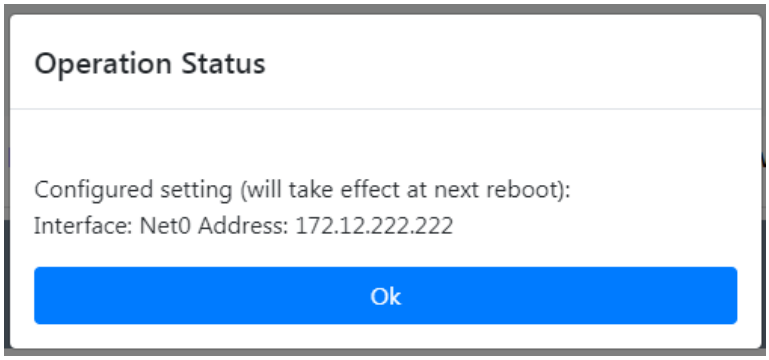


2. Select Configure Maintenance Default Gateway.



3. Select new gateway interface (maintenance) from the list and enter the Gateway IP Address and click Confirm.
   NOTE: Create a Maintenance configuration for Network Interface mode before adding a gateway for it.

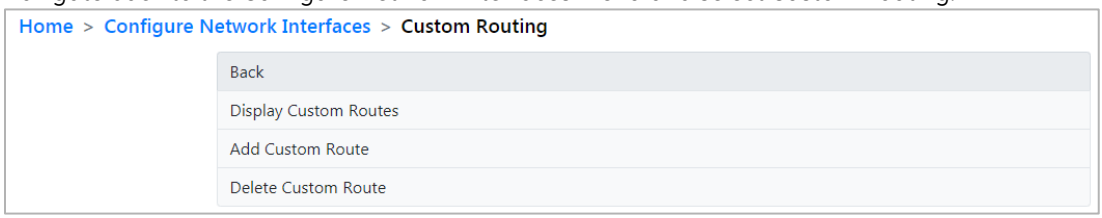
4. RESULT:



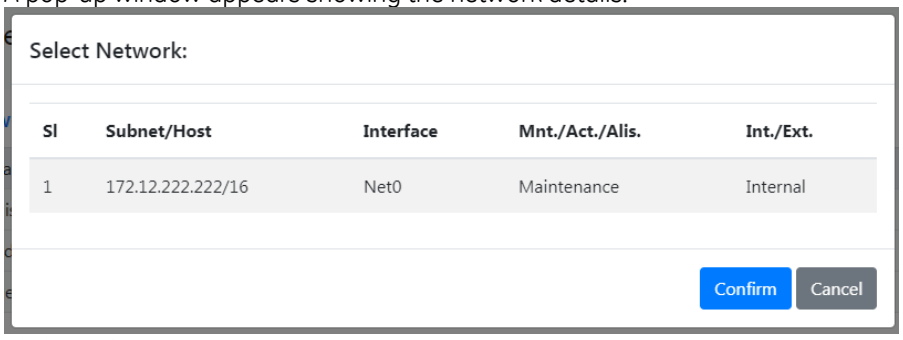
5. Click OK and reboot the device for changes to take effect.

Custom Routing

1. Navigate back to the Configure Network Interfaces menu and select Custom Routing.



2. Select Add Custom Route and enter destination IP Address and click Confirm.
3. A message appears to confirm the destination IP and individual host.
    - Click No and enter the Subnet mask and click confirm or click Yes to continue.
    - Click Yes to add the specified route to an interface.
    - A pop-up window appears showing the network details.

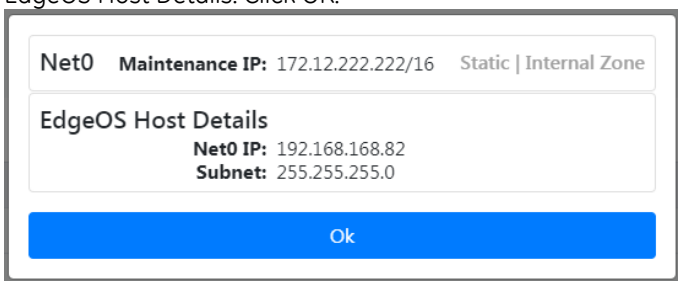


    - Click Confirm
4. Navigate back to Custom Routing menu and select Delete Custom Route.
5. Select the Network Interface which needs to be deleted and click Confirm.

Network Summary

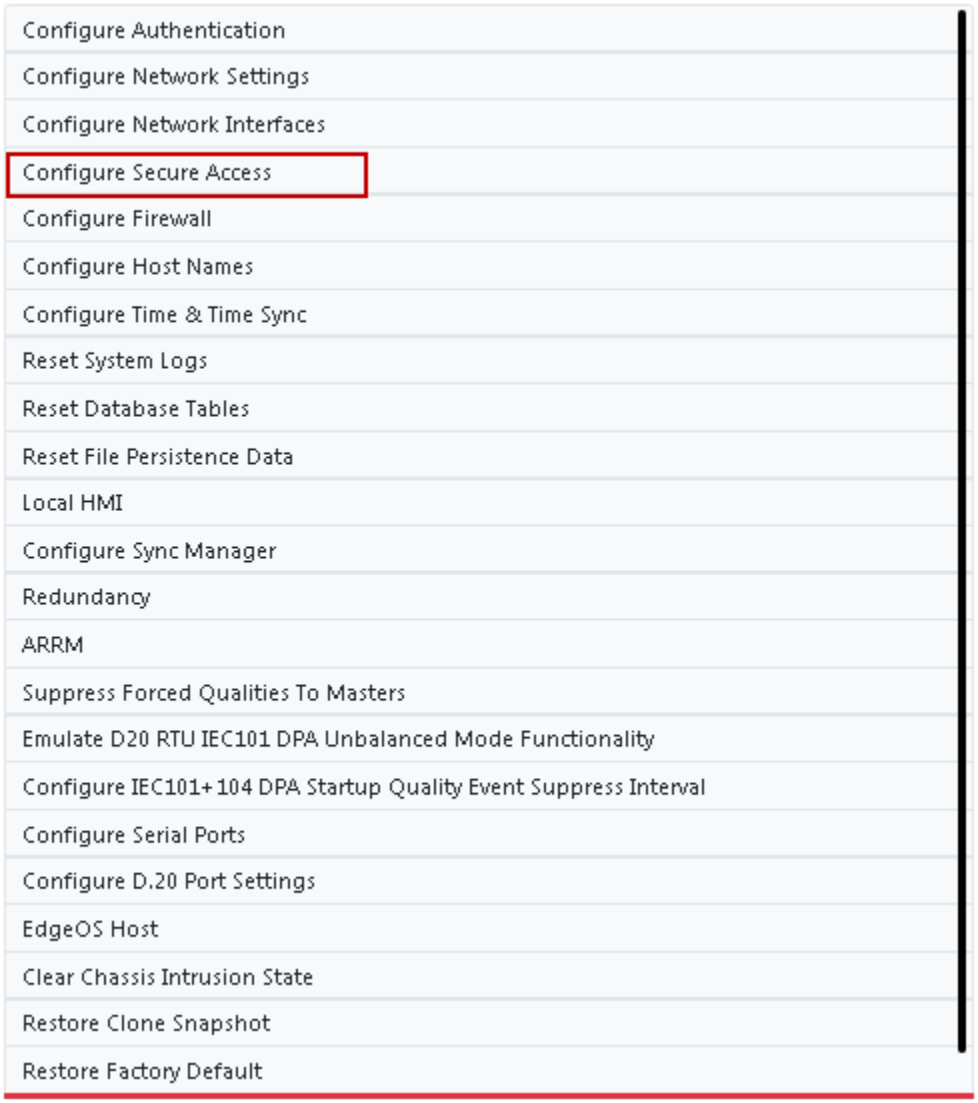
1. Navigate back to Configure Network Interfaces and select Network Summary.

2. A message appears showing the Network Interface Maintenance IP, Address type, Network Zone and EdgeOS Host Details. Click OK.



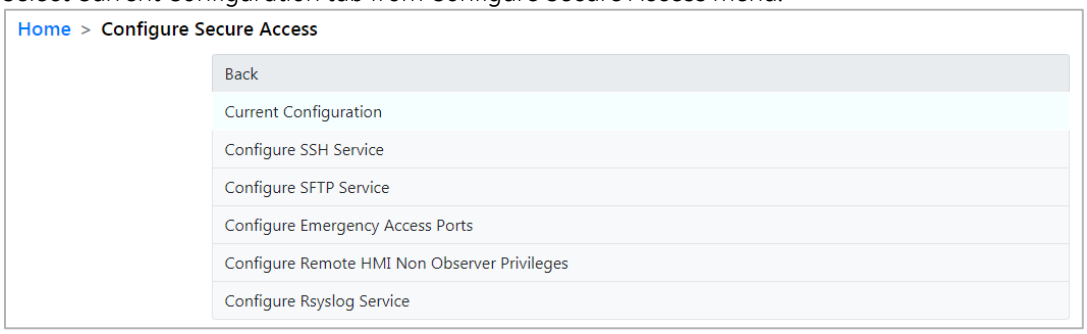
Configure Secure Access

1. Select Configure Secure Access tab from main menu.

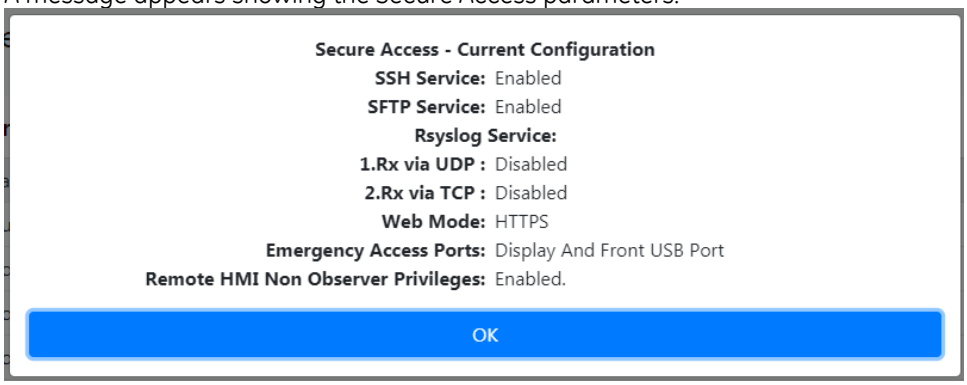


Current Configuration

1. Select Current Configuration tab from Configure Secure Access menu.



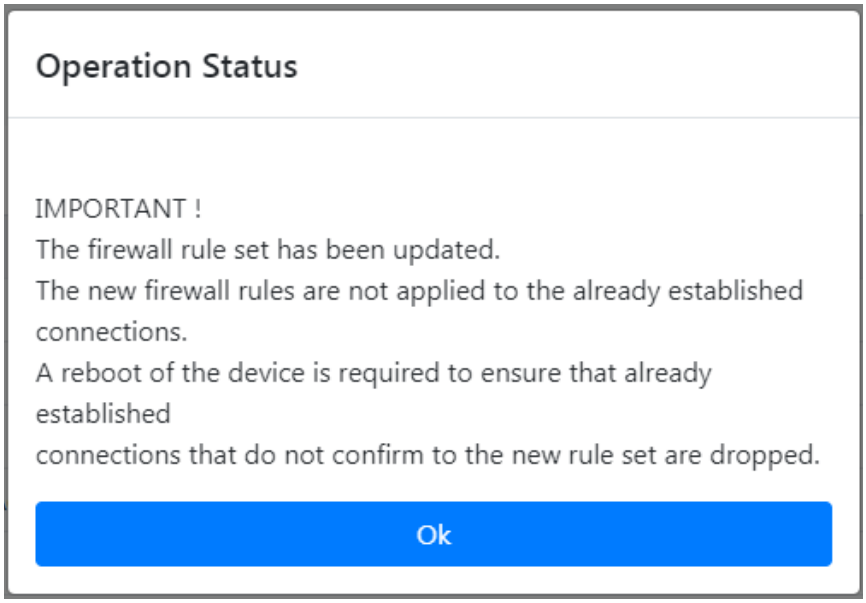
2. A message appears showing the Secure Access parameters:



3. Click OK.

Configure SSH Service

1. Select Configure SSH Service from Configure Secure Access menu.
   - Select Yes to close the current SSH session and disable SSH:



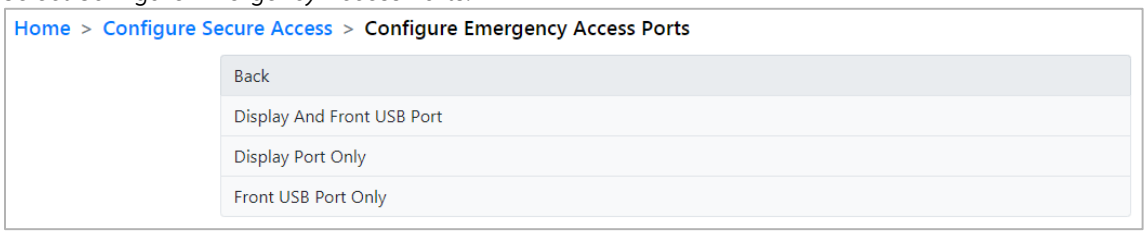
   - Select No to abort.

Configure SFTP Service

1. Select Configure SFTP Service tab from Configure Secure Access menu.
   NOTE: The SSH service must be Enabled to change SFTP configuration.
   - Select Yes to close current SSH session and Enable SFTP.
   - RESULT; Operation Status – Completed.

Configure Emergency Access Ports

1. Select Configure Emergency Access Ports.



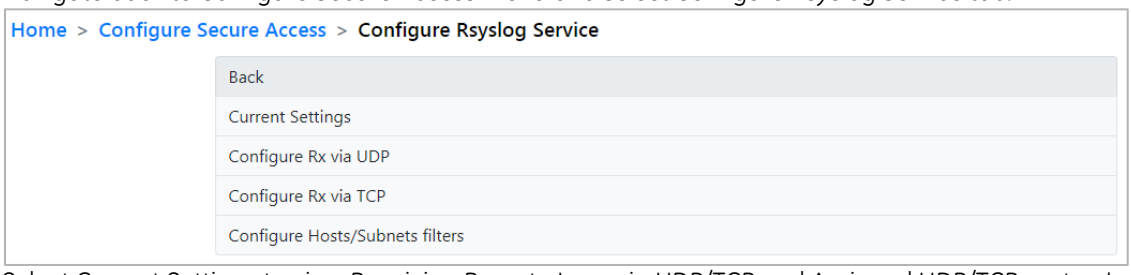
2. Select access ports from the list to configure and click OK once updated successfully.

Configure Remote HMI Non Observer Privileges

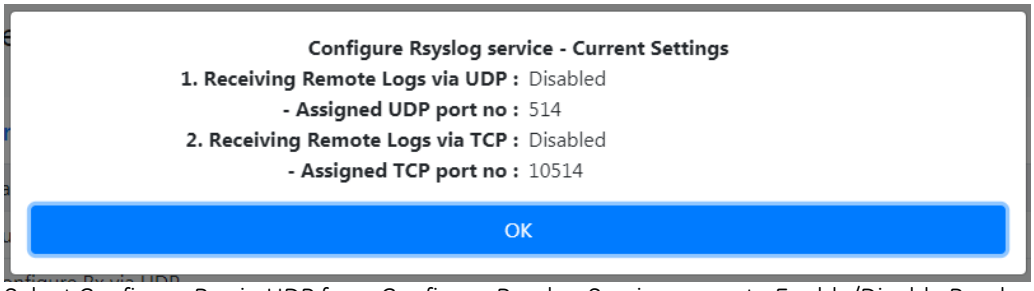
1. Navigate back to Configure Secure Access menu and select Configure Remote HMI Non Observer Privileges tab.
2. A message appears showing the current status of Remote HMI Non Observer privileges whether Enabled or Disabled. Select Yes to change the mode from one state to another or No to abort.
   - RESULT: If Yes, Operation Status – Settings have been saved and applied. Click OK.

Configure Rsyslog Service

1. Navigate back to Configure Secure Access menu and select Configure Rsyslog Service tab.



2. Select Current Settings to view Receiving Remote Logs via UDP/TCP and Assigned UDP/TCP port no's. Click OK.

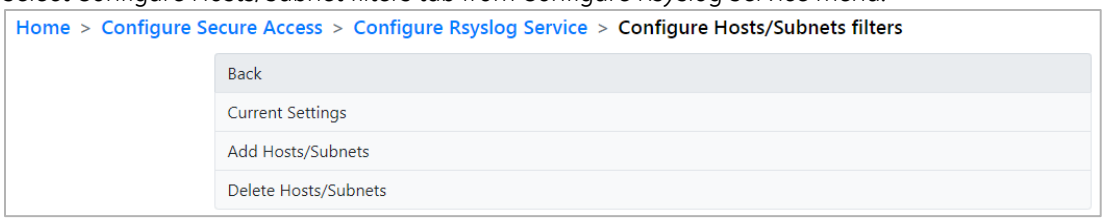


3. Select Configure Rx via UDP from Configure Rsyslog Service menu to Enable/Disable Rsyslog Logging service and Edit UDP Port number.
4. Select Enable/Disable Rsyslog Service to view the current Rsyslog remote-host message reception service via UDP status (Enable/Disable) and select Yes to change its state accordingly or select No to abort.

5. Select Edit UDP Port number to view the current port number configured and select Yes to configure different port or No to continue with same port.
   NOTE:
   - It is recommended to use the Default 514 port.
   - In case you really need to assign a new port number, ensure that no other Gateway applications/services are using the same port number.

   Click Yes to assign new port number and enter the new port number and click Confirm.
6. Select Configure Rx via TCP from Configure Rsyslog Service menu to Enable/Disable Rsyslog Logging service and Edit TCP Port Number.
7. Select Enable/Disable Rsyslog Service to view the current Rsyslog remote logging service via TCP status (Enable/Disable) and select Yes to change its state accordingly or select No to abort.
8. Select Edit TCP Port number to view the current port number configured and select Yes to configure different port or No to continue with same port.
   NOTE:
   - It is recommended to use the Default 10514 port.
   - In case you really need to assign a new port number, ensure that no other Gateway applications/services are using the same port number.

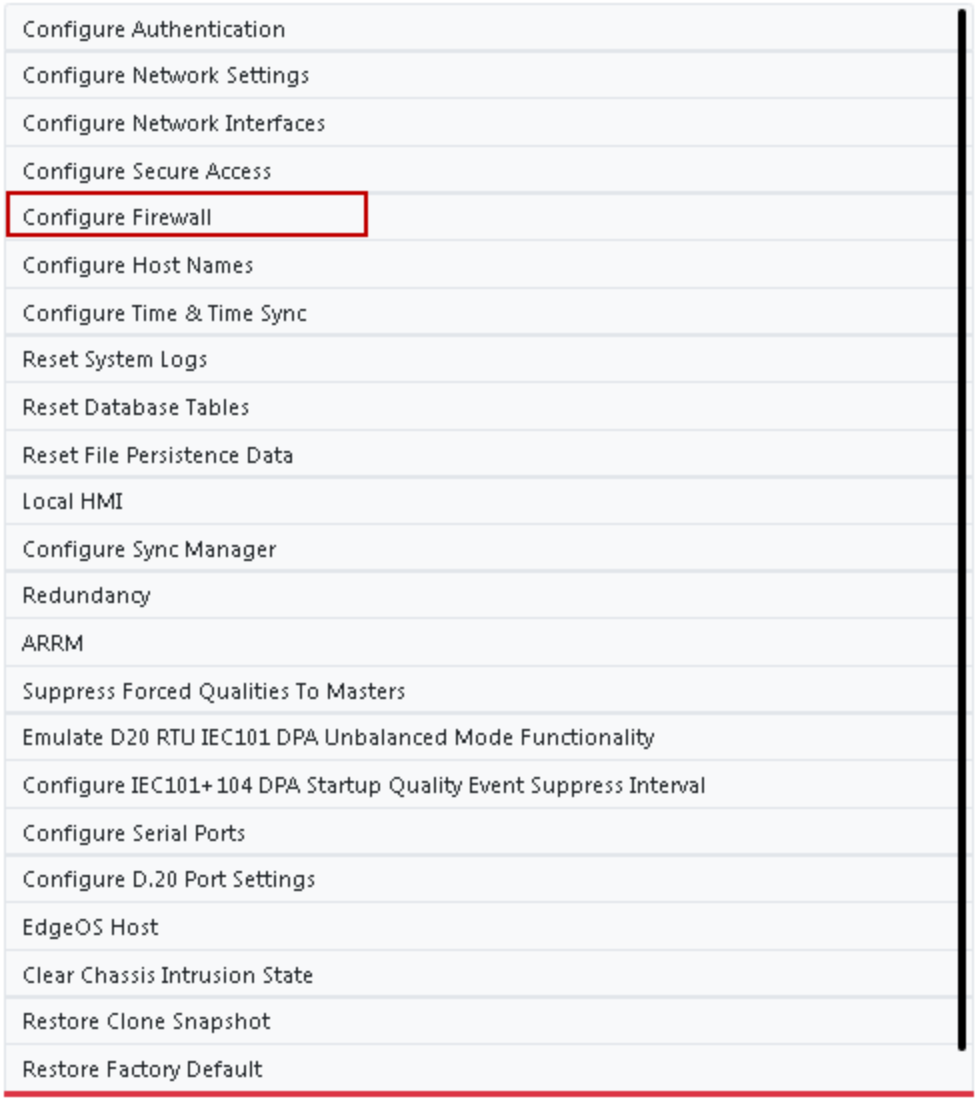
   Click Yes to assign new port number and enter the new port number and click Confirm.
9. Select Configure Hosts/Subnet filters tab from Configure Rsyslog Service menu.



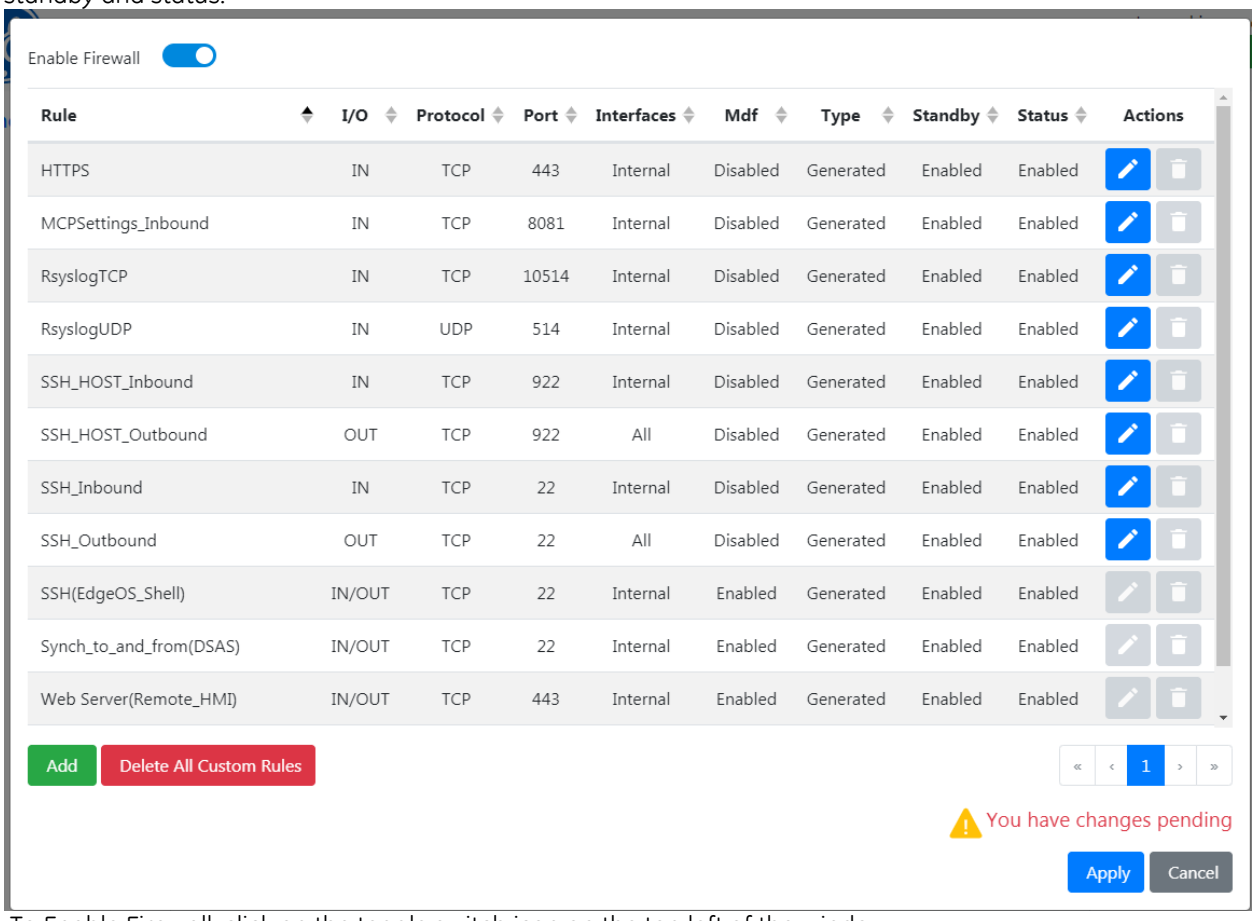
10. Select Current Settings to view Hosts/Subnets configured in allowed senders list.
11. Select Add Hosts/Subnets, select the listed Network Interfaces and enter Custom Filters by selecting IP Address and Subnet address.
    NOTE: Use Custom filters when the IED IP add does not fall in the Configure Hosts-Subnets Filters listed available subnet range.
12. Select Delete Hosts/Subnets tab from Configure Hosts/Subnets filters menu and select the Hosts/Subnets from the list and select Yes to confirm.

Configure Firewall

1. Select Configure Firewall tab from main menu.

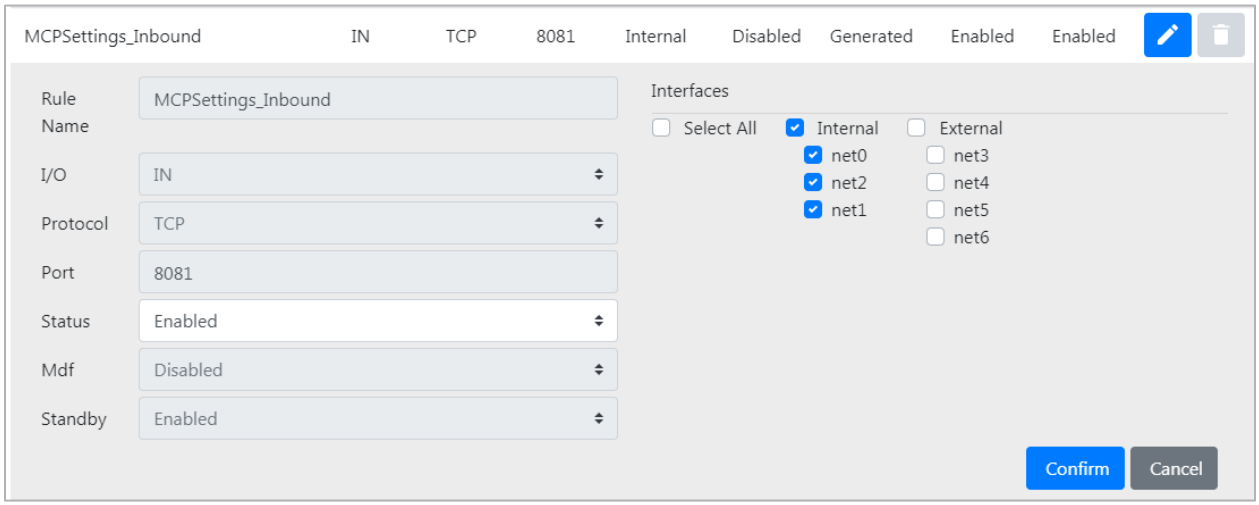


2. A list of Firewall Rules appears on screen displaying Input/Output, protocol, port, interfaces, Mdf, type standby and status.



3. To Enable Firewall, click on the toggle switch icon on the top left of the window.

4. To Edit the firewall rule, click on the icon on the Actions column of a rule.



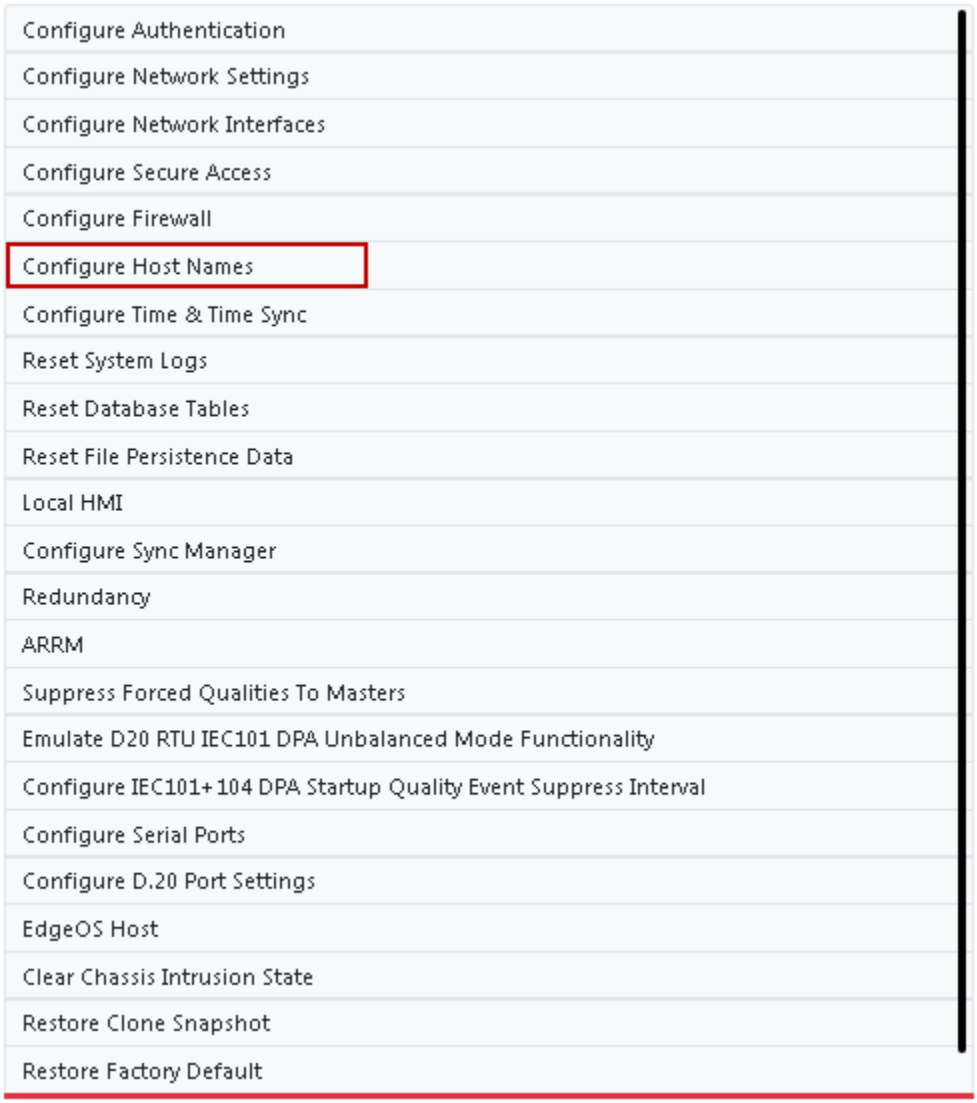
5. Select the Status of firewall rule from the dropdown list (Enable/Disable) and check in/out the Interfaces required and click Confirm.
6. To Add a New rule, select Add button on the bottom left

- Select I/O,
- Select Protocol type
    - UDP – 0 to 65535
    - TCP – 0 to 65535
    - ICMP – 0 to 255
- Select Status (Enabled/Disabled)
- Check in the Interfaces required and click Confirm to add.

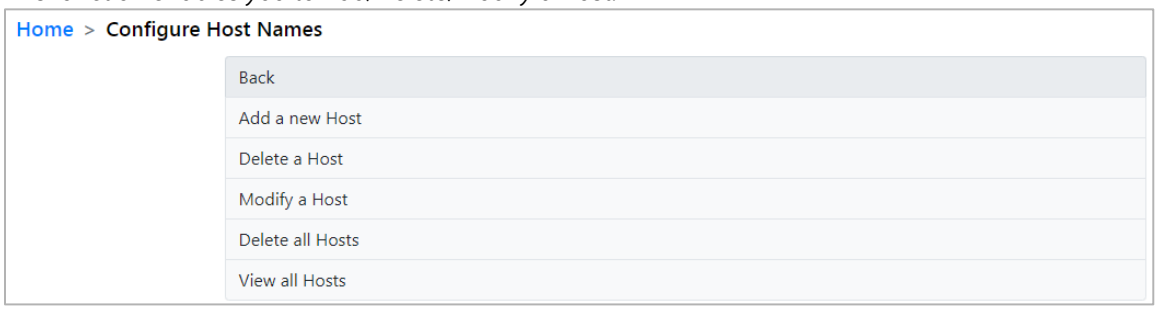
7. Only the Custom rules can be deleted. To Delete rules, click on the icon on the respective rule. By default, the generated rules cannot be deleted.
8. Once all the changes are done, click Apply button on the bottom right of the page and restart the device for the changes to take effect.
9. Select Delete All Custom Rules to delete all custom rules except Generated Rules, select Apply and restart the device for the changes to take effect.

Configure Host Names

1. Select Configure Host Names from the Main menu.



2. This function enables you to Add/Delete/Modify a Host.



Add a new Host

1. Select Add a new Host tab from the Configure Host Names.
2. Enter Hostname, IP Address and click Confirm.
   RESULT: Operation Status – Host <Hostname> added successfully. Click OK.

Delete a Host

1. Select Delete a Host and click on the host which needs to be removed.
   RESULT: Deleted the selected host successfully. Click OK.

Modify a Host

1. Select Modify a Host tab from the Configure Host Names menu.
2. Select the Host which needs to be modified.
   NOTE: Change in Host name will change Machine host name also.
   - Click No to abort.
   - Click Yes to continue and enter Host name, IP Address and click Confirm to save changes.
   - Reboot the device for changes to take effect.

Delete all Hosts

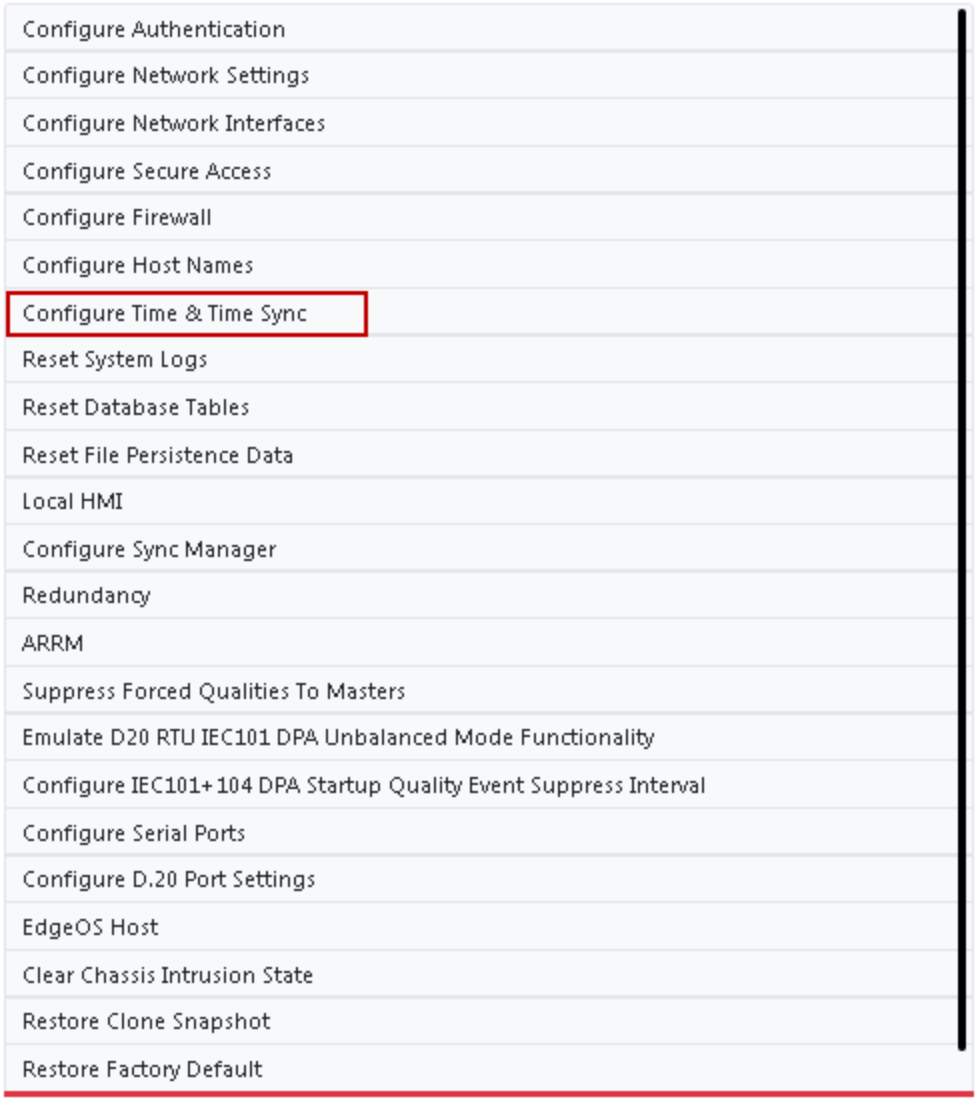
1. Select Delete all Hosts tab from the Configure Host Names menu.
2. Click No to abort or Yes to delete all hosts.
   RESULT: If Yes, all hosts deleted successfully, click OK.

View all Hosts

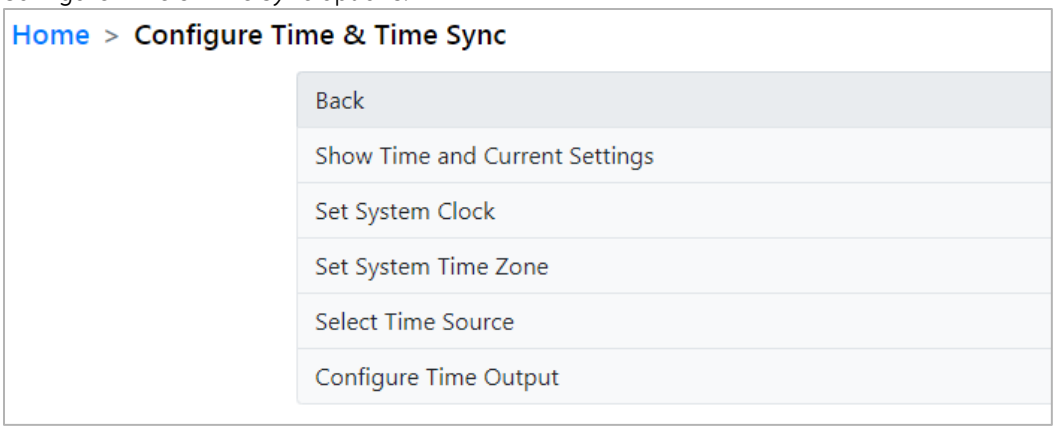
1. Select View all Hosts tab from the Configure Host Names menu.
   RESULT: List of Hosts configured are displayed. Click OK.

Configure Time & Time Sync

1. Select Configure Time & Time Sync tab from the Main menu.

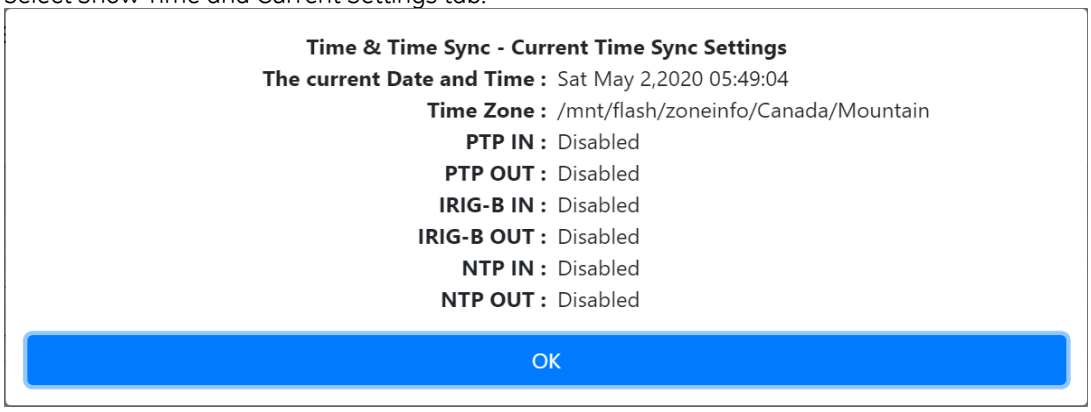


2. Configure Time & Time Sync options:



Show Time and Current Settings

1. Select Show Time and Current Settings tab.

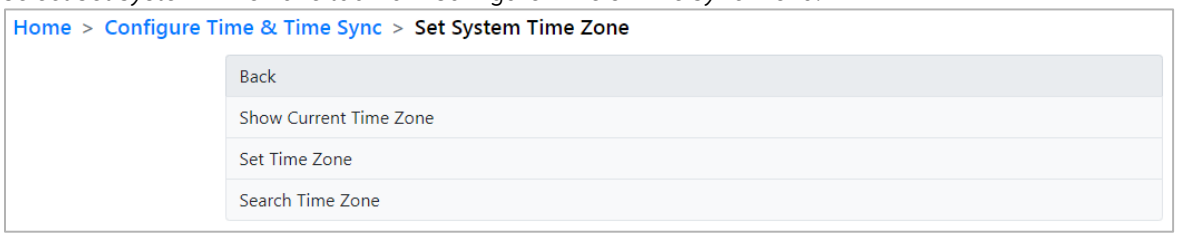


Set System Clock

1. Select Set System Clock tab.
   NOTE: The Gateway system time is automatically set to the firmware build time whenever the Gateway reboots and the system time is less than the firmware build time during boot time.
2. Enter Date in YYYY-MM-DD format and click Confirm.
3. Enter Time (24 Hr Format) in hh:mm:ss format and click Confirm.
   RESULT: The System time is successfully updated according to the input credentials. Click OK.

Set System Time Zone

1. Select Set System Time Zone tab from Configure Time & Time Sync menu.



2. Select Show Current Time Zone to view current date, time and time zone.
3. Select Set Time Zone and choose proper Time Zone File/Directory from the list. Choose Previous, Next options to view all the available time zones.
   RESULT: System Logger restarted; the time zone is successfully set to predefined zone.
   NOTE: Restart Local HMI if it is running.
4. Select Search Time Zone and enter your specified time zone and click search to view the available time zones and select it accordingly.
   RESULT: System Logger restarted, the time zone is successfully set to predefined zone.
   NOTE: Restart Local HMI if it is running.

Select Time Source

This function enables you to configure which time source is active:

- PTP - not available in G100
- IRIG-B
- NTP

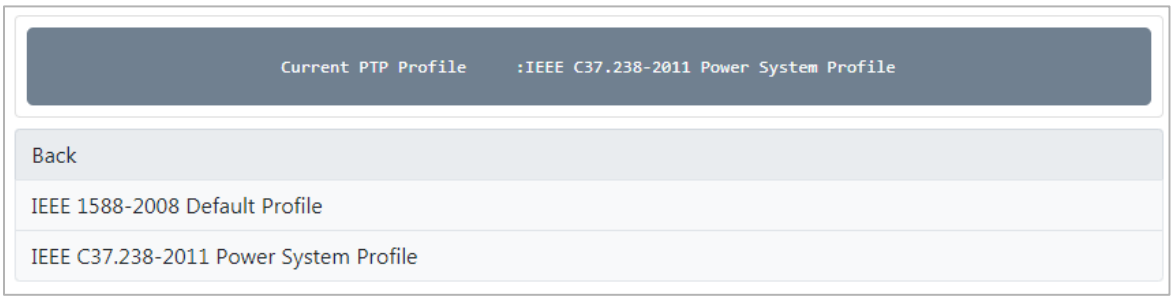
Only one time source can be enabled at a time.

PTP IN

NOTE: This feature is not supported in G100.

1. Select PTP tab to perform the following functions.
   - Enable/Disable
   - Domain
   - Priority 1
   - Priority 2
   - Profile

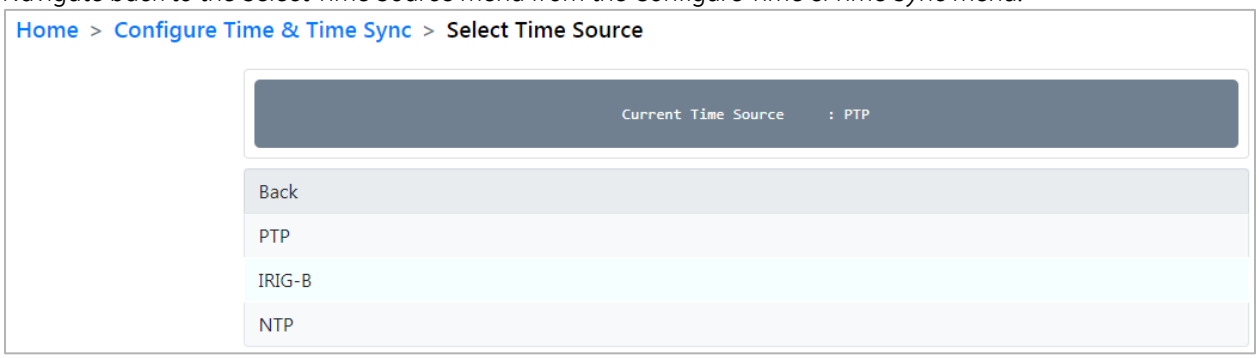
2. Select Enable/Disable tab to switch the mode accordingly.
3. Select Domain tab and enter configure PTP Domain value (0 - 255) and click Confirm.
4. Select Priority 1 and enter configure Priority 1 value (0-255) and click Confirm.
5. Select Priority 2 and enter configure Priority 2 value (0-255) and click Confirm.
6. Select Profile tab to view the current PTP Profile:



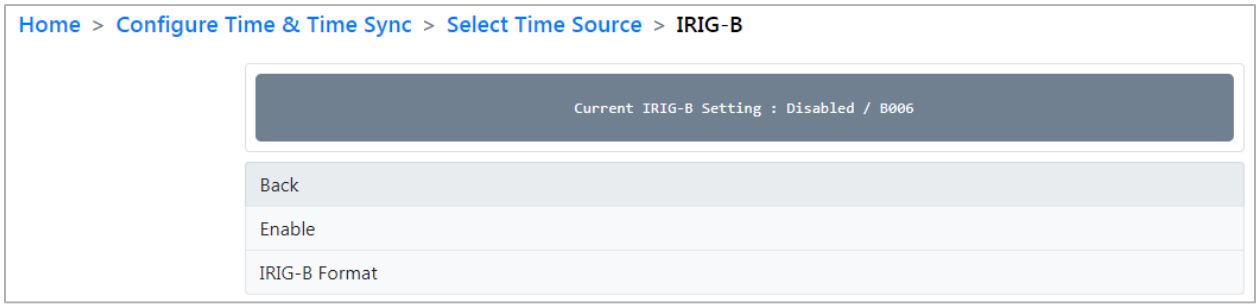
   - Select required profiles available from the list to activate them and reboot the device for the changes to take effect.

IRIG-B IN

1. Navigate back to the Select Time Source menu from the Configure Time & Time Sync menu.

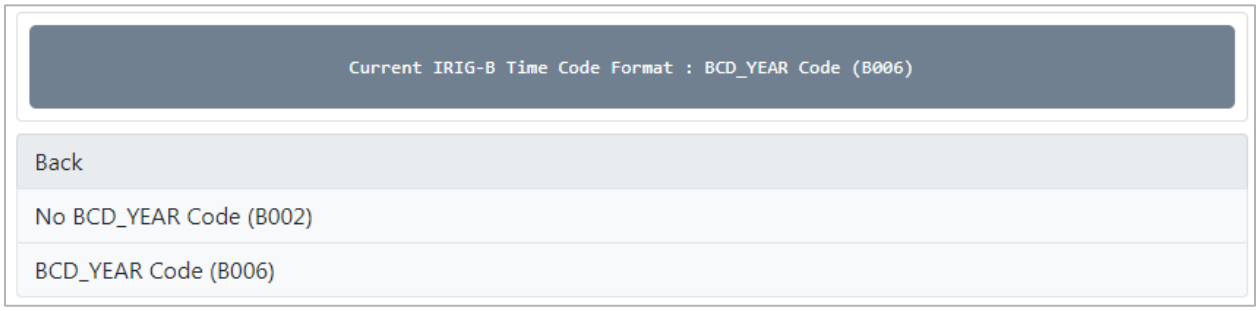


2. Select IRIG-B tab.



3. Select Enable/Disable tab to switch the mode accordingly.

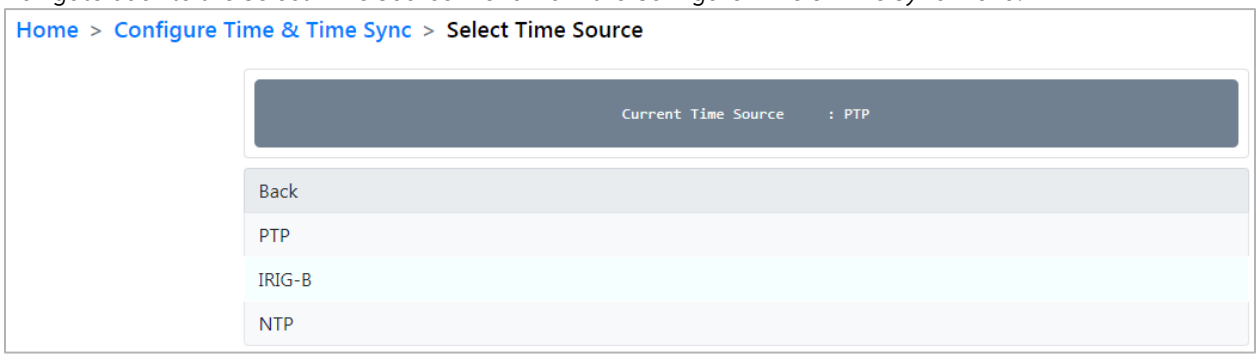
4. Select IRIG-B Format to view the status.



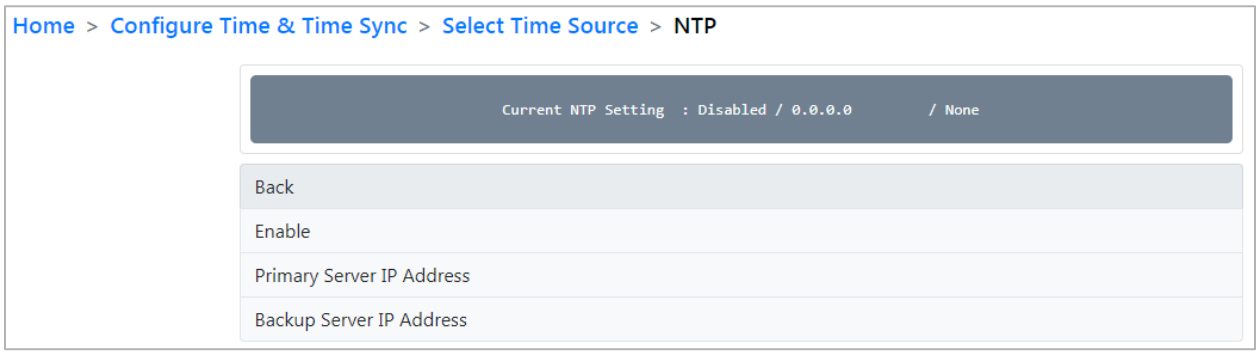
5. Select required Format available from the list to activate them and reboot the device for the changes to take effect.

NTP IN

1. Navigate back to the Select Time Source menu from the Configure Time & Time Sync menu.



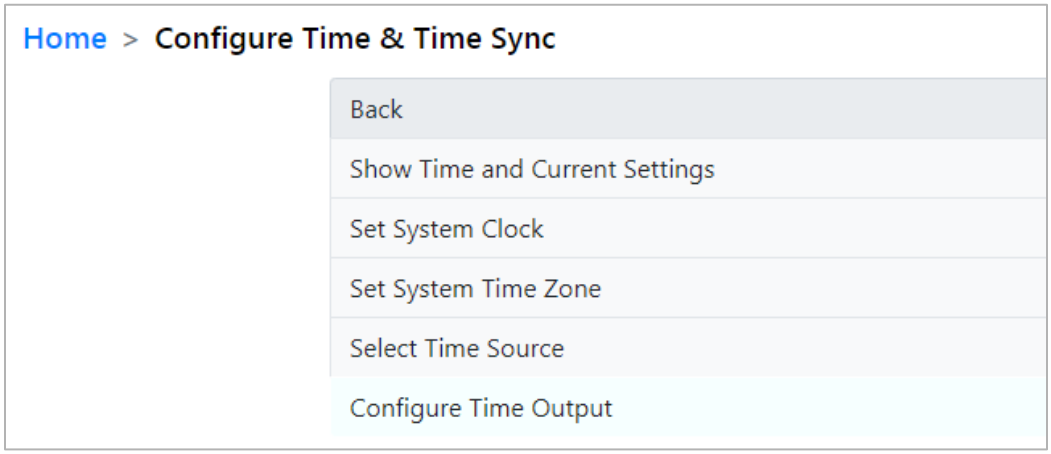
2. Select NTP tab.



3. Select Enable/Disable tab to switch the mode accordingly.
4. Select Primary Server IP Address tab and enter Primary Server IP Address [0.0.0.0] and click Confirm. Click Yes to save changes.
   RESULT: Primary Server IP Address is saved. Click Ok.
5. Select Backup Server IP Address tab and enter Backup Server IP Address [None] field with appropriate either of the following values.
   a. Enter 'None' to delete the Secondary configuration
   b. Enter Secondary Server IP Address [0.0.0.0]
6. Click Confirm. Click Yes to save changes.

Configure Time Output

1. Select **Configure Time Output** tab from **Configure Time & Time Sync** menu.



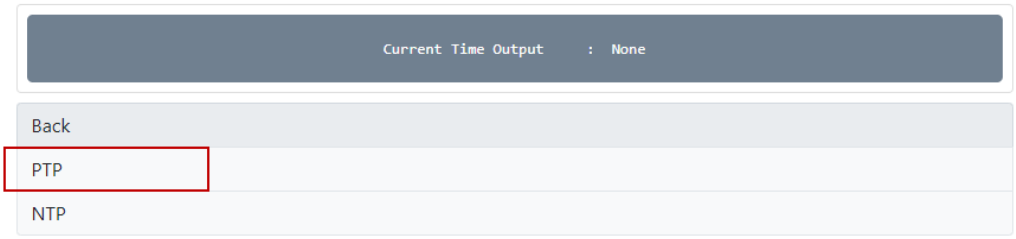
Configure PTP OUT

NOTE: Not supported in G100.

The "PTP" will be available in the "**Configure Time & Time Sync - Configure Time Output**" menu only when the PTP input is configured and enabled.

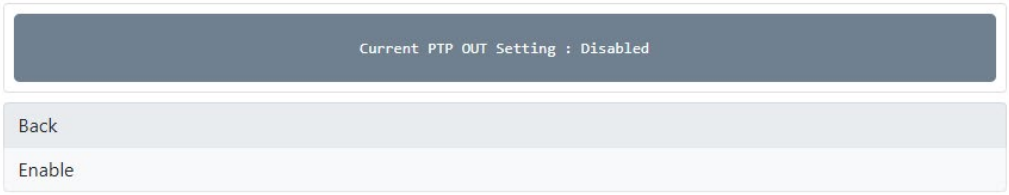
1. Select **PTP** from Configure Time Output menu:

Home > Configure Time & Time Sync > **Configure Time Output**



2. Current status of PTP OUT Settings is displayed on the screen, Select **Enable/Disable** tab to change the status accordingly and reboot the device for the changes to take effect.

Home > Configure Time & Time Sync > Configure Time Output > **PTP**



NOTE: If the Current PTP Output is disabled, "Enable" option is displayed on the "**Configure Time Output – PTP**" menu. Otherwise, it will be "Disable".

NOTE: The PTP Output will share same settings configured in the PTP Input, such as domain, priorities and so on.

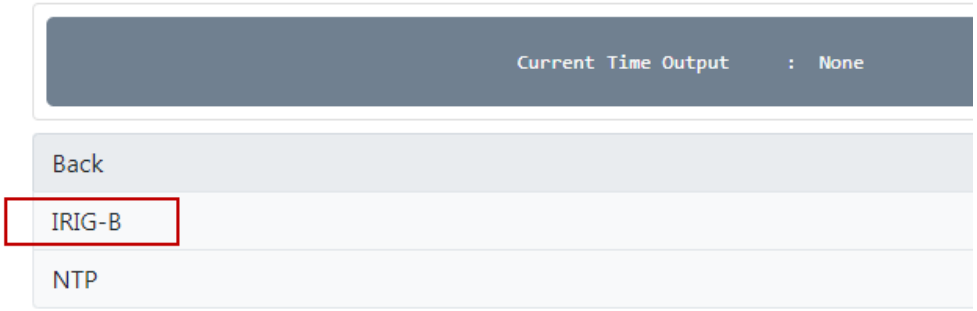
Configure IRIG-B OUT

NOTE: Not supported in G100.

The "IRIG-B" will be available in the "**Configure Time & Time Sync - Configure Time Output**" menu only when the IRIG-B input is configured and enabled.

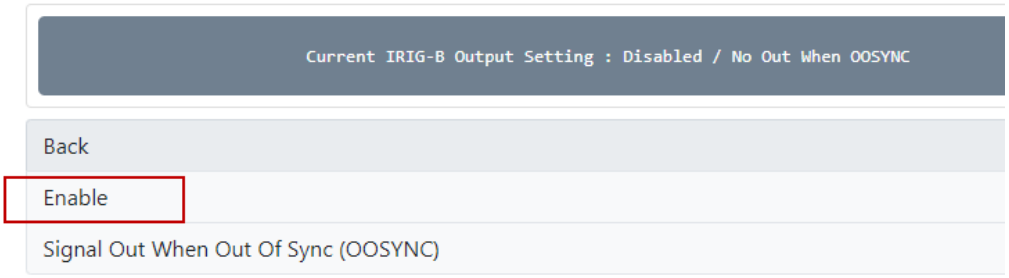
1. Select **IRIG-B** from Configure Time Output menu:

   Home > Configure Time & Time Sync > **Configure Time Output**



2. Current status of IRIG-B OUT Settings is displayed on the screen, select **Enable/Disable** tab to change the status accordingly and reboot the device for the changes to take effect.

   Home > Configure Time & Time Sync > Configure Time Output > **IRIG-B**

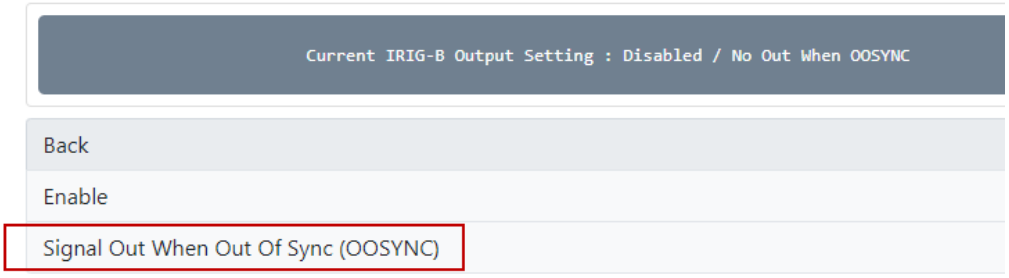


   NOTE: If the Current IRIG-B Output is disabled, "Enable" option is displayed on the "**Configure Time Output – IRIG-B**" menu. Otherwise, it will be "Disable".

   NOTE: The IRIG-B output will share same IRIG-B time code format as configured in the IRIG-B Input.

3. Select **Signal Out/No Signal Out - When Out OF Sync (OOSYNC)** tab to allow/suppress IRIG-B output when the IRIG-B input signal is out of sync.
   By default, the IRIG-B output signal is suppressed when the IRIG-B input signal is out of sync.

   Home > Configure Time & Time Sync > Configure Time Output > **IRIG-B**

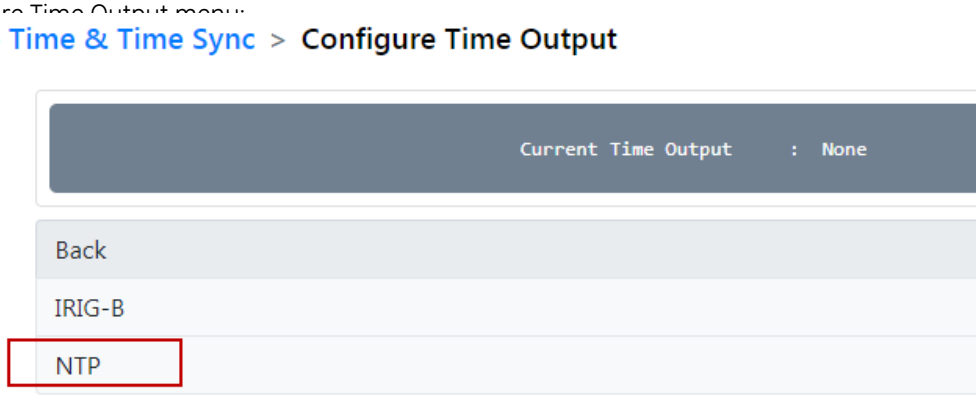


   - Click Yes to confirm or No to abort.

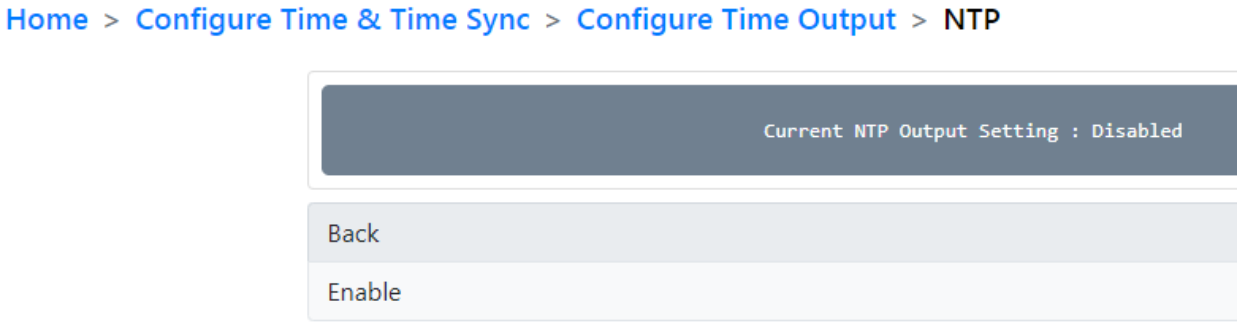
Configure NTP OUT

The "NTP" will be always available in the "**Configure Time & Time Sync - Configure Time Output**" menu no matter the NTP input is enabled or not.

1. Select **NTP** from Configure Time Output menu.



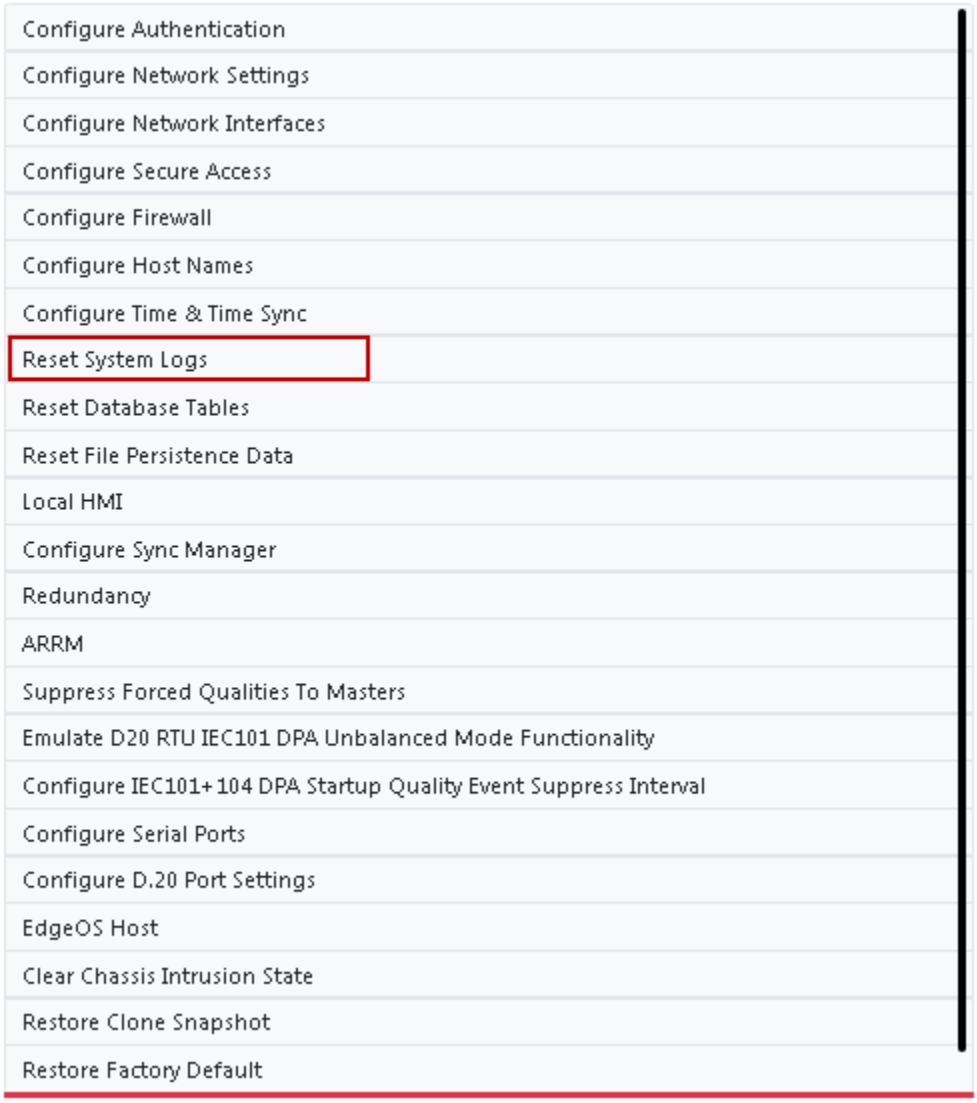
2. Current status of NTP OUT Settings is displayed on the screen, Select **Enable/Disable** tab to change the status accordingly and restart the applications for proper update of HAMA Pseudo points.



NOTE: If the Current NTP Output is disabled, "Enable" option is displayed on the "**Configure Time Output – NTP**" menu. Otherwise, it will be "Disable".

Reset System Logs

1. Select Reset System Logs tab form main menu.



2. This function is used to perform the following actions:
   - Check Size of Archived Logs
   - Check size of current Application Logs
   - Delete Archived Logs
   - Delete current Logs

Check Size of Archived Logs

1. Select Check Size of Archived Logs.
   RESULT: Operation Status: The size of the Archived Gateway logs is displayed. Click OK.

Check size of current Application Logs

1. Select Check size of current Application Logs.
   RESULT: Operation Status: The size of the Archived Gateway logs is displayed. Click OK.

Delete Archived Logs

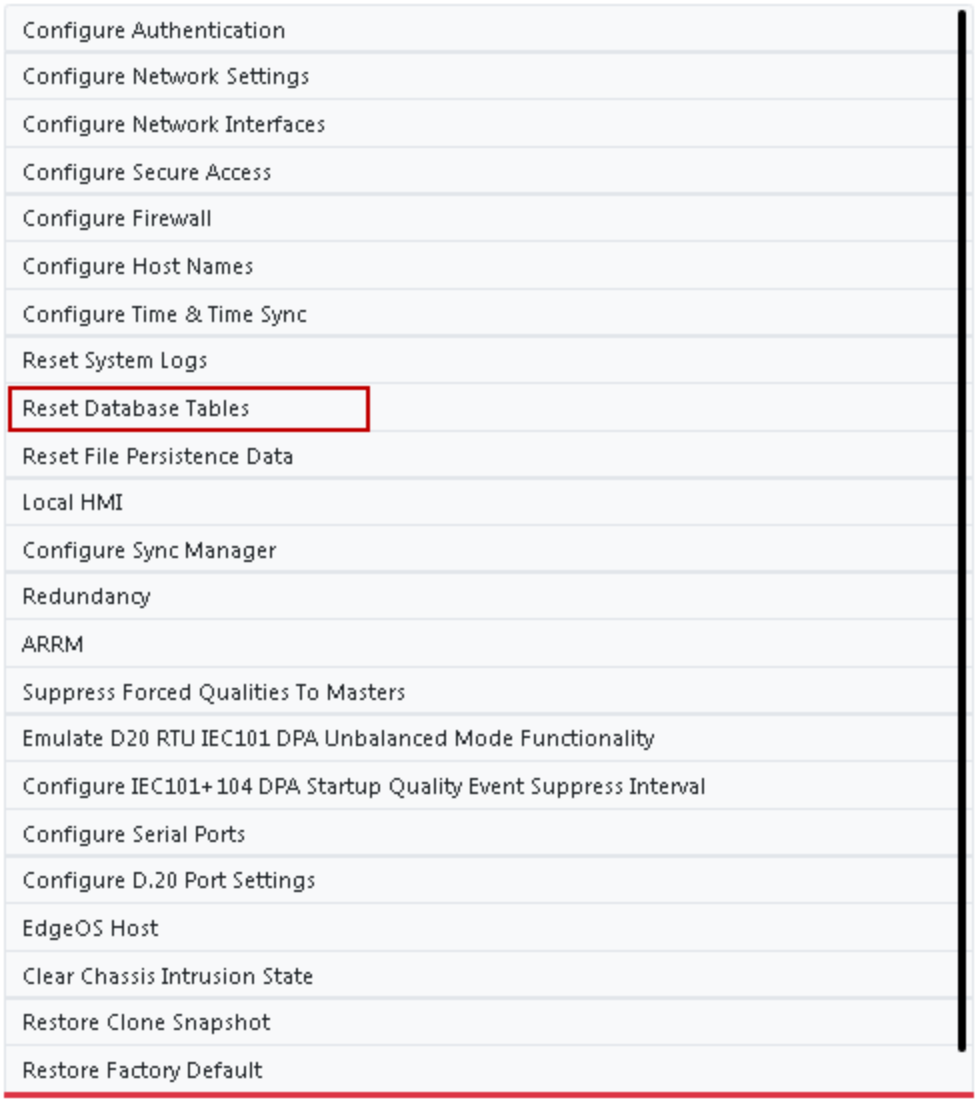
1. Select Delete Archived Logs tab and click Yes to confirm or No to abort.
   RESULT: If Yes, the Archived log files are Deleted. If No, the archived log files are not deleted. Click OK.

Delete current Logs

1. Select Delete current Logs tab and click Yes to confirm or No to abort.
   RESULT: If Yes, the Current log files are Deleted, and System Logger is restarted. If No, the Current log files are not deleted. Click OK.

Reset Database Tables

1. Select Reset Database Tables from Main menu.



2. The function is used to perform the following actions:
   - Delete Digital Event Data: SOE and Alarm records
   - Delete Quality records
   - Delete PRF Event records

- Delete Operator Note records
- Delete Accumulator records

Delete Digital Event Data: SOE and Alarm records

1. Select Delete Digital Event Data: SOE and Alarm records tab.
   NOTE: This will stop all applications and permanently delete entries from the digital events database.
2. Click Yes to confirm or No to Abort.
   - If No, no records deleted from the database. Click OK.
   - If Yes, a message appears confirming to stop all applications on Gateway and to restart applications. Click Yes.
     RESULT: Restarting all applications on Gateway. Click OK.

Delete Quality records

1. Select Delete Quality records tab from Reset Database Tables menu.
2. Click Yes to confirm or No to abort.
   - If No, no records deleted from the database. Click OK.
   - If Yes, a message appears confirming to stop all applications on Gateway, Quality Tag Records - Deleting and to restart applications. Click Yes.
     RESULT: Restarting all applications on Gateway. Click OK.

Delete PRF Event records

1. Select Delete PRF Event records tab from Reset Database Tables menu.
2. Click Yes to confirm or No to abort.
   - If No, no records deleted from the database. Click OK.
   - If Yes, a message appears confirming to stop all applications on Gateway, PRF Records - Deleting and to restart applications. Click Yes.
     RESULT: Restarting all applications on Gateway. Click OK.

Delete Operator Note records

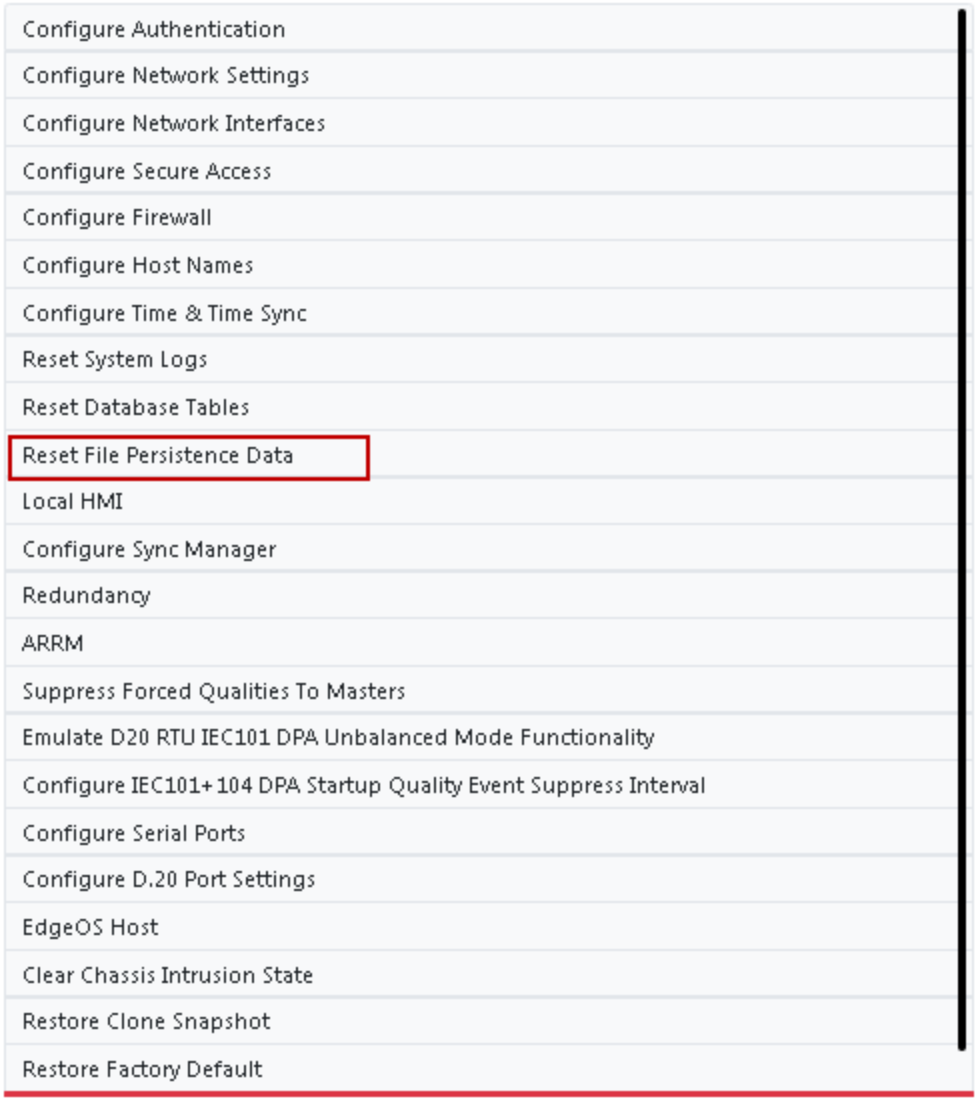
1. Select Delete Operator Note records tab from Reset Database Tables menu.
2. Click Yes to confirm or No to abort.
   - If No, no records deleted from the database. Click OK.
   - If Yes, a message appears confirming to stop all applications on Gateway, Operator Note Records - Deleting and to restart applications. Click Yes.
     RESULT: Restarting all applications on Gateway. Click OK.

Delete Accumulator records

1. Select Delete Accumulator records tab from Reset Database Tables menu.
2. Click Yes to confirm or No to abort.
   - If No, no records deleted from the database. Click OK.
   - If Yes, a message appears confirming to stop all applications on Gateway, Accumulator Records - Deleting and to restart applications. Click Yes.
     RESULT: Restarting all applications on Gateway. Click OK.

Reset File Persistence Data

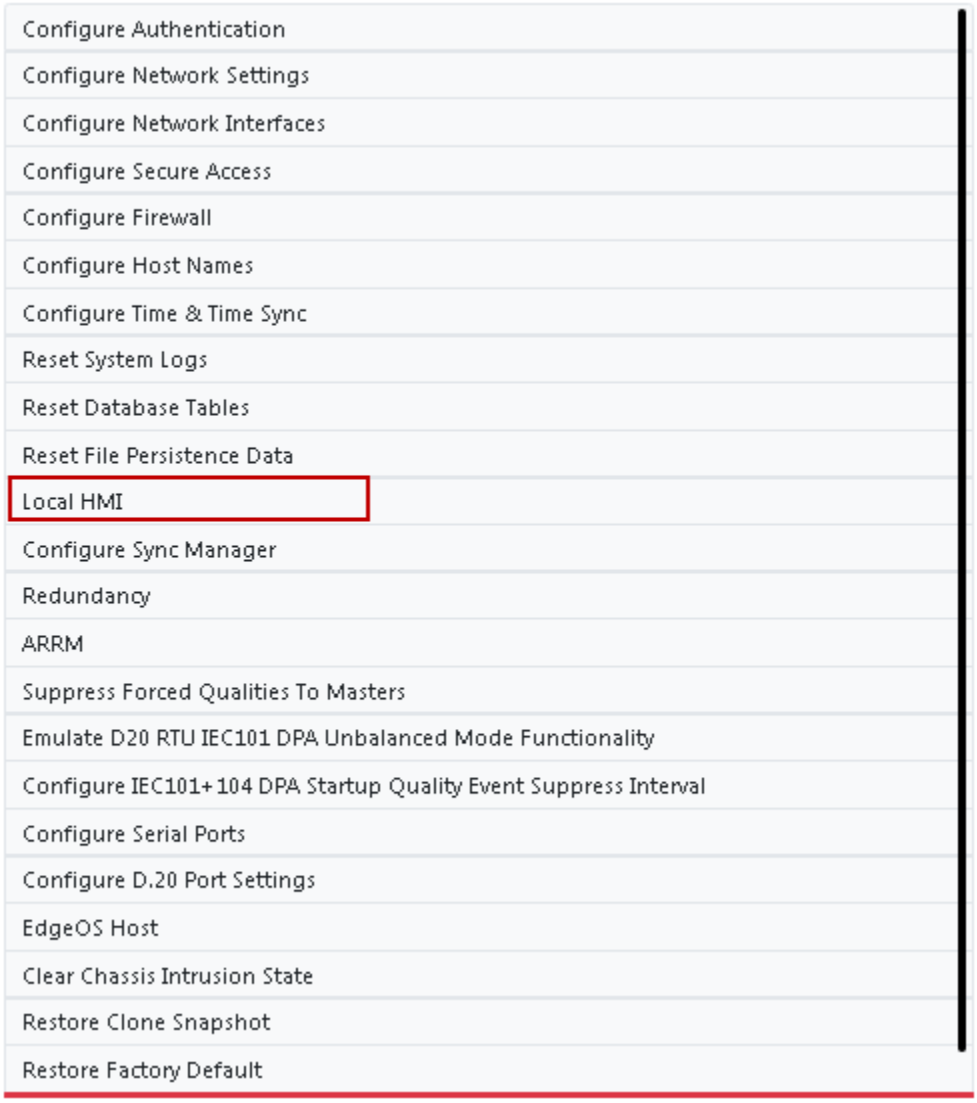
1. Select Reset File Persistence Data form the Main menu.



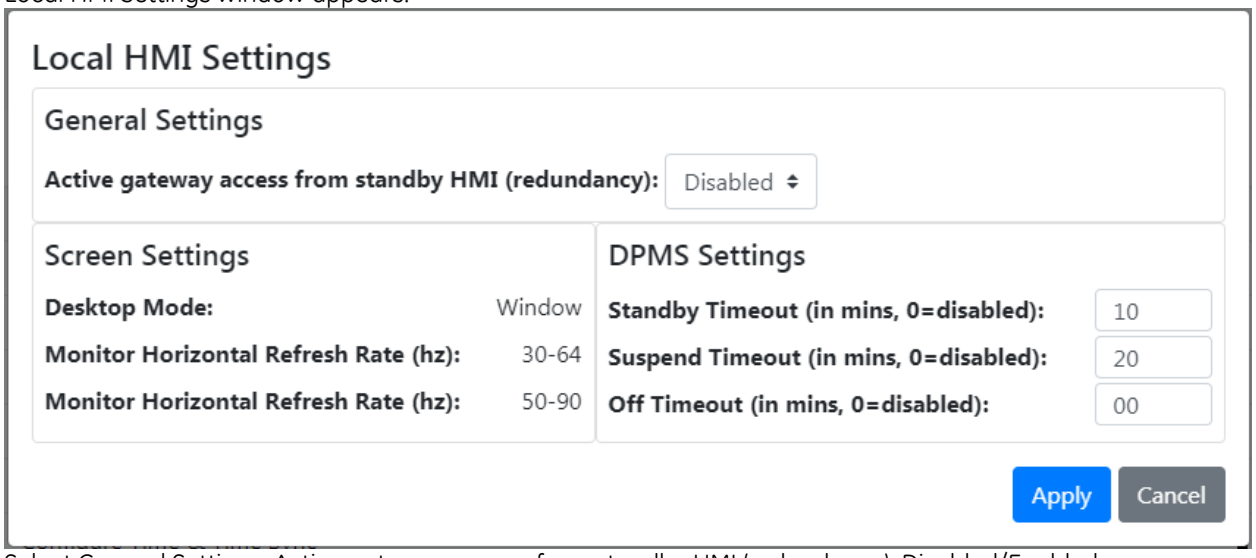
2. Select Reset File Persistence Data, click Yes to confirm or No to abort.
   - If No, Operation Status – No application restarts and commit operation from HMI.
   - If Yes,
     NOTE: "Last Fault number" saved in persistent memory for "Fault Number File retrieval" method in ARRM is also cleared.
     Click Yes to confirm.
   - RESULT: Restarting all applications on Gateway. Click OK.

Local HMI

1. Select Local HMI from the main menu.



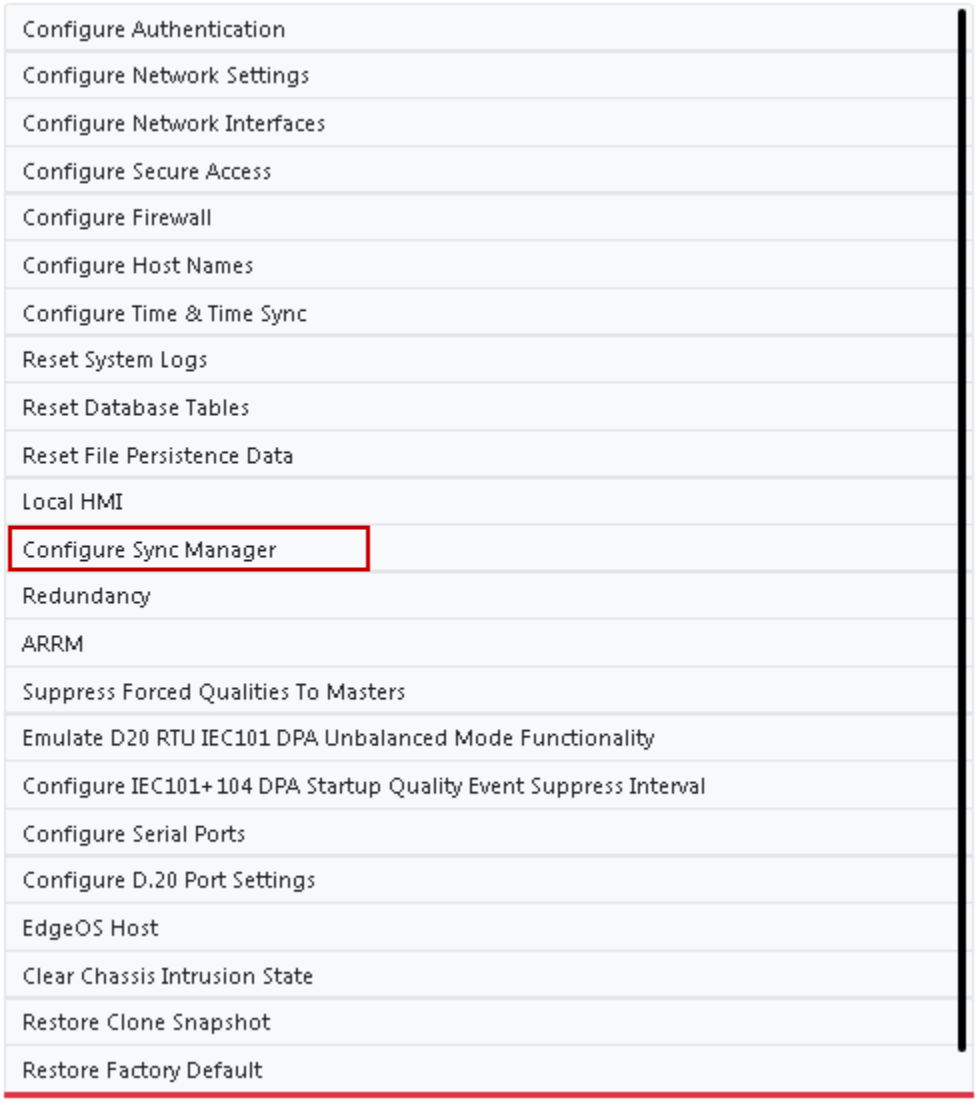
2. Local HMI Settings window appears:



3. Select General Settings: Active gateway access from standby HMI (redundancy): Disabled/Enabled.
   NOTE: This is not supported in G100.
4. Screen Settings are displayed on the Local HMI Settings window:
   - Desktop Mode: Window
   - Monitor Horizontal Refresh Rate (hz): 30-64
   - Monitor Horizontal Refresh Rate (hz): 50-90
5. DPMS Settings are displayed on the Local HMI Settings window:
   - Standby Time (in mins, 0=disabled): 10
   - Suspend Timeout (in mins, 0=disabled): 20
   - Off Timeout (in mins, 0=disabled): 00
6. Click Apply to apply settings successfully.
7. Click Close.

Configure Sync Manager

1. Select Configure Sync Manager from the main Menu.



2. The function is used to perform the following actions:
    - Enable/Disable Sync Manager
    - Generate SSH Authentication Keys
    - Configure Sync Sets

Enable/Disable Sync Manager

1. Select Enable/Disable Sync Manager tab from the Configure Sync Manager menu.
2. A message appears showing the current Sync Manager mode whether Enabled/Disabled.
3. Click Yes to confirm or No to abort.
    - If Yes, Operation Status – Sync Manager status is changed, click OK.

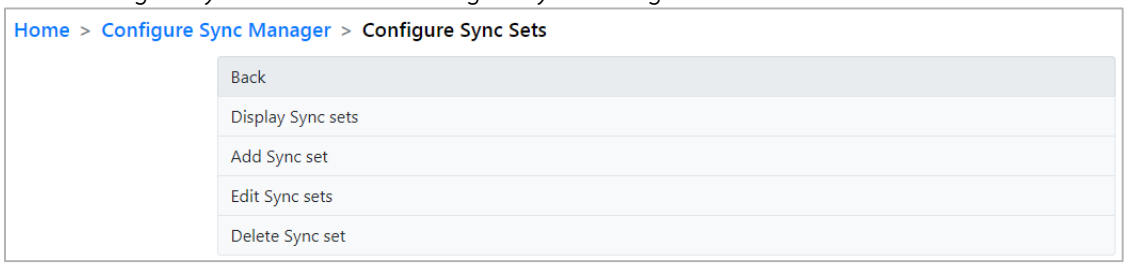
Generate SSH Authentication Keys

1. Select Generate SSH Authentication Keys tab from the Configure Sync Manager menu.

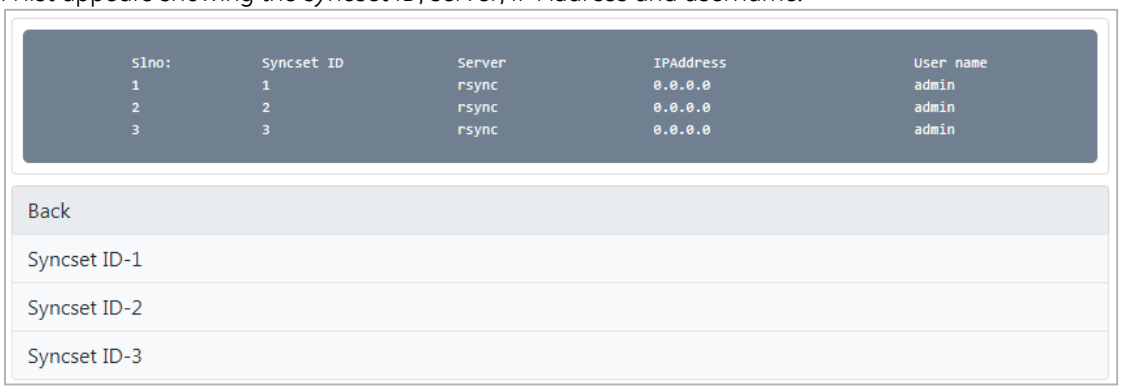
2. Click Yes to generate new keys or No to abort.
   NOTE: New keys will overwrite any existing keys in /mnt/datalog/SSHKeys/SyncMgr?!
   - If No.
     RESULT; No New keys are generated.
   - If Yes.
     RESULT:
     - Generating SSH Public/Private key pair
     - Removing old keys, if any.
     - Key location is /mnt/datalog/SSHKeys/SyncMgr/id_rsa
     - New keys are generated.
   - Click OK.

Configure Sync Sets

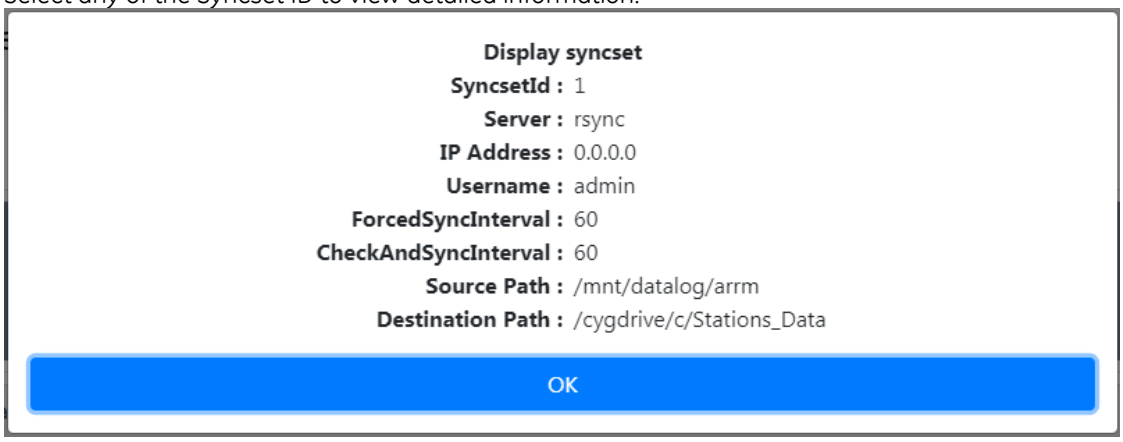
1. Select Configure Sync Sets tab from Configure Sync Manager menu.



2. Select Display Sync sets tab.
3. A list appears showing the syncset ID, server, IP Address and username.



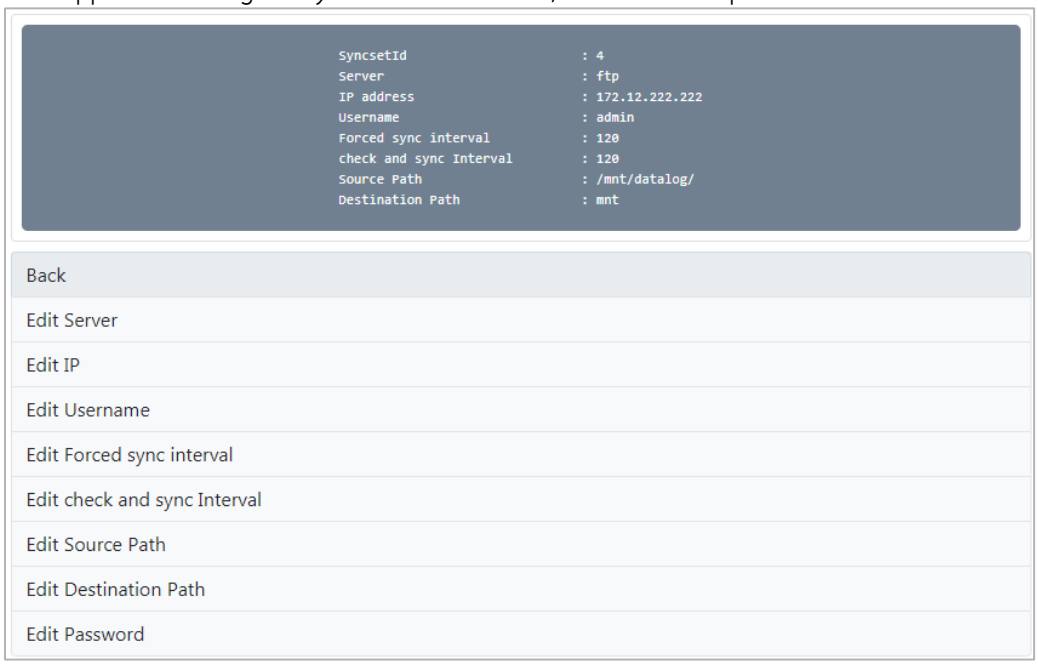
4. Select any of the Syncset ID to view detailed information:



5. Navigate back to Configure Sync Sets and select Add Sync set tab.
6. Select Configure Server type:
   - rsync

- ftp
- sftp

7. Enter Destination IP Address and click Confirm.
8. Enter Destination User name and click Confirm.
9. Enter Password credentials (shown only for ftp) and click Confirm.
10. Enter Forced sync Interval (60 to 86400 or 0 seconds) and click Confirm.
11. Enter Check and sync Interval (60 to 86400 or 0 seconds) and click Confirm.
12. Enter Source Path Name and click confirm
13. Enter Destination Path Name and click Confirm.
14. RESULT: Operation Status – Complete, click OK.
15. Select Edit Sync sets tab from Configure Sync Sets menu.
16. A list appears showing the syncset ID, server, IP Address and user name. Select one of the Syncset ID which needs to be Edited.
17. A list appears showing the Syncset ID credentials, click on the respective tab to edit it.

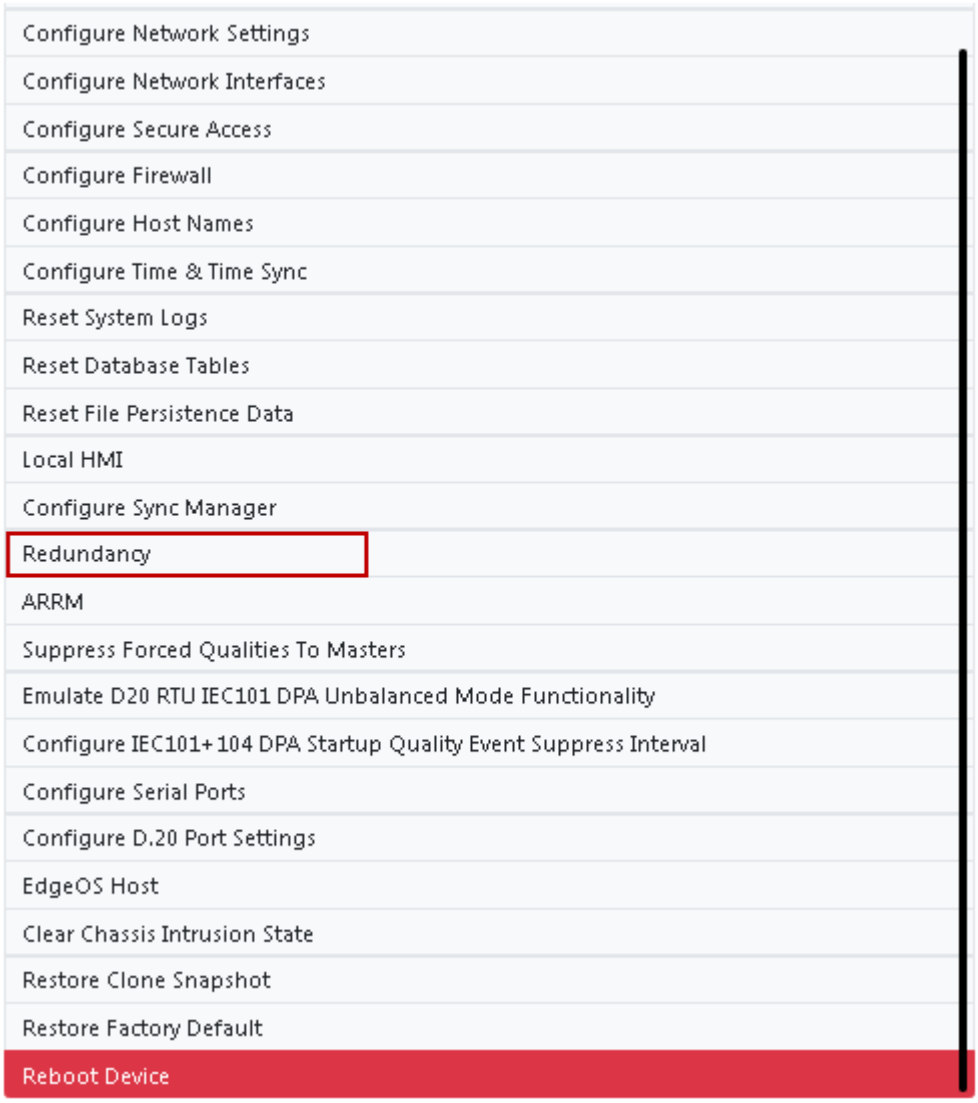


18. Select Edit Server to modify the existing server and select:
    - rsync
    - ftp
    - sftp
19. Select Edit IP and enter Destination IP Address and click Confirm.
20. Select Edit Username and enter Destination User name and click Confirm.
21. Select Edit Forced sync Interval and enter Forced sync Interval (60 to 86400 or 0 seconds) and click Confirm.
22. Select Edit check and sync Interval and enter Check and sync Interval (60 to 86400 or 0 seconds) and click Confirm.
23. Select Edit Source Path and enter Source Path Name and click confirm
24. Select Edit Destination Path and enter Destination Path Name and click Confirm.
25. Navigate back to Configure Sync Sets and select Delete Sync set.
26. Select the Syncset ID which needs to be removed from the list and click Confirm to delete Syncset or cancel to abort.

Redundancy

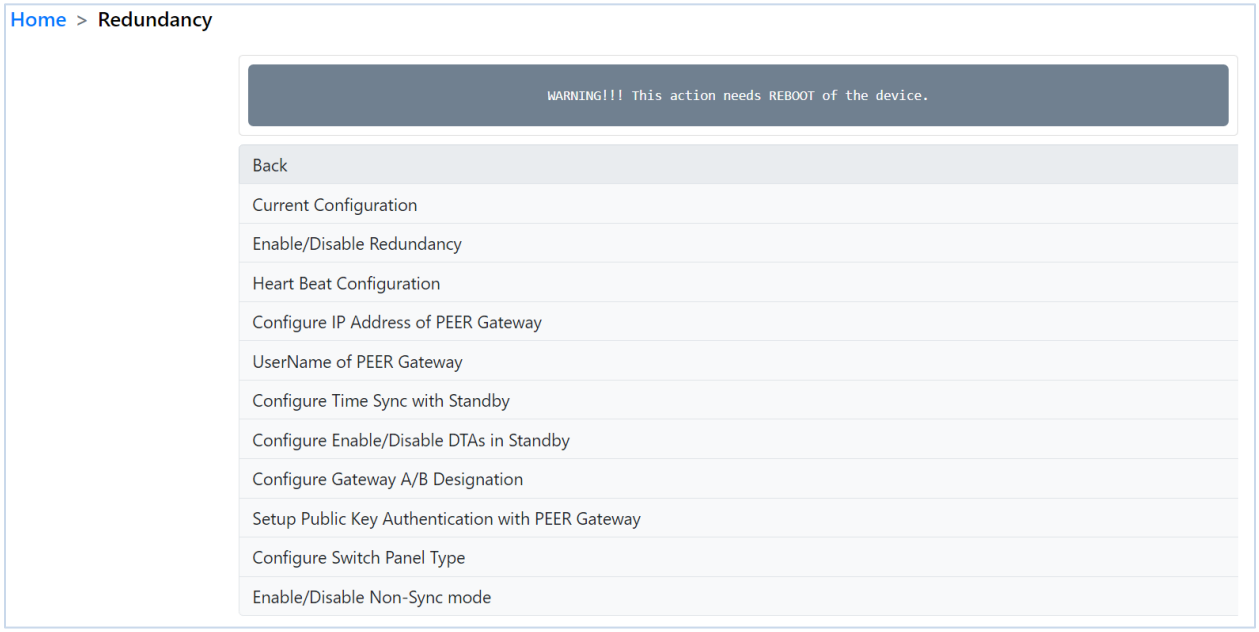
NOTE: Not supported in G100.

1. Select Redundancy tab from the Main menu.



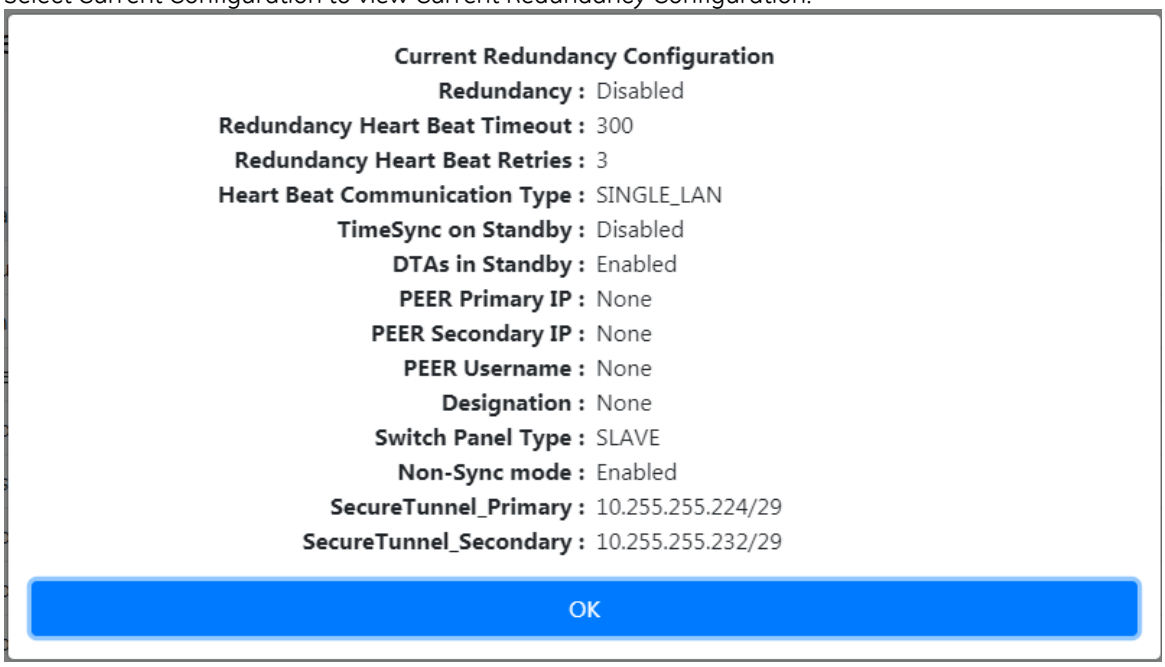
2. The function is used to perform the following actions:
   - Current Configuration
   - Enable/Disable Redundancy
   - Heart Beat Configuration
   - Configure IP Address of PEER Gateway
   - Username of PEER Gateway
   - Configure Time Sync with Standby
   - Configure Enable/Disable DTAs in Standby
   - Configure Gateway A/B Designation
   - Setup Public Key Authentication with PEER Gateway
   - Configure Switch Panel Type
   - Enable/Disable Non-Sync mode

Note: Any operation in this need a Device Reboot.



Current Configuration

1. Select Current Configuration to view Current Redundancy Configuration:



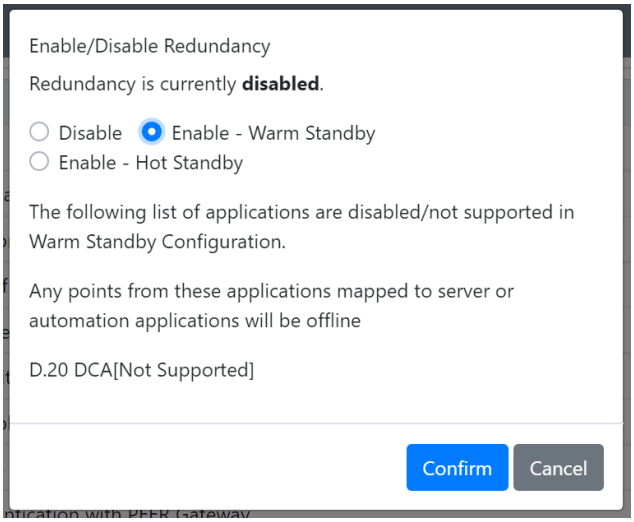
Click OK.

Enable/Disable Redundancy

1. Select Enable/Disable Redundancy to view the current Redundancy status and to switch to different modes:
    - Enable/Disable

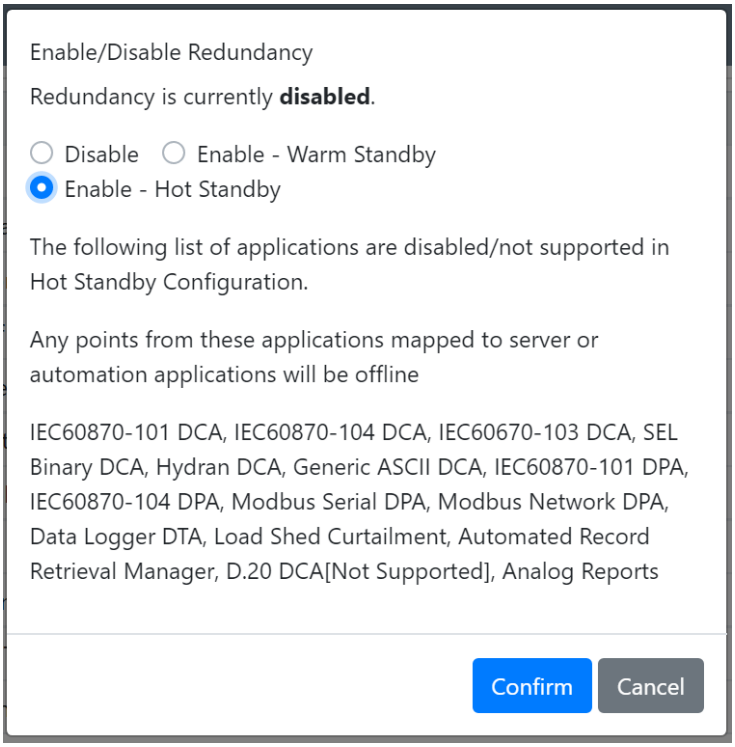
- A message appears showing the current Enabled Redundancy Type: Hot/Warm Standby. Click Yes to Disable Redundancy.
- RESULT: Deleting all active HMI Sessions, changes saved successfully.
- Click OK.

- Enable – Warm Standby
  - D.20 Client/DCA will be disabled/not supported in Warm Standby Configuration
  - Click Confirm.
  - RESULT:
    - Deleting all active HMI sessions.
    - Redundancy is Enabled, generating SSH Public/Private key pair.
    - Removing old Public/Private keys, if any.
    - Key location is /mnt/datalog/SSHKeys/id_rsa
  - Click OK.



- Enable – Hot Standby
  - The following list of applications are disabled in Hot Standby Configuration:
    - IEC60870-101 DCA
    - IEC60870-104 DCA
    - IEC60670-103 DCA
    - SEL Binary DCA
    - Hydran DCA
    - Generic ASCII DCA
    - D.20 DCA
    - IEC60870-101 DPA
    - IEC60870-104 DPA
    - Modbus Serial DPA
    - Modbus Network DPA
    - Data Logger DTA
    - Load Shed Curtailment
    - D.20 DCA [Not supported]
    - Automated Record Retrieval Manager
    - Analog Reports
  - Click Confirm.
  - RESULT:
    - Deleting all active HMI Sessions.
    - Redundancy is Enabled, generating SSH Public/Private key pair.
    - Removing old Public/Private keys, if any.
    - Key location is /mnt/datalog/SSHKeys/id_rsa

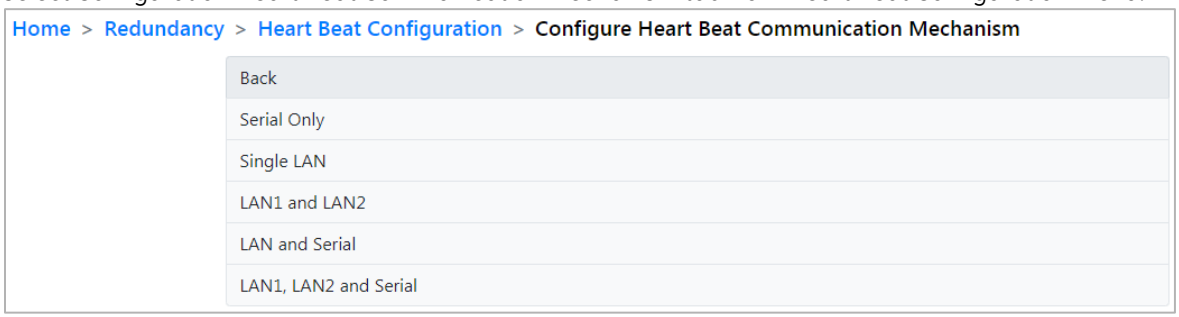
- Click OK.



Heart Beat Configuration

1. Select Heart Beat Configuration tab from Redundancy menu.
   NOTE:
   - A very low Heart Beat timeout should not be used for a network-based Heart Beat Communication Mechanism.
   - If you are not using serial Heart Beat Communication Mechanism, then Heart Beat Timeout and Heart Beat Retries parameters should not be less than 300ms and 3 respectively (default).
2. The function is used to perform the following actions:
   - Configure Heart Beat Timeout
   - Configure Heart Beat Retries
   - Configure Heart Beat Communication Mechanism
3. Select Configure Heart Beat Timeout tab from Heart Beat Configuration menu.
4. Enter Heart Beat timeout in Milliseconds [100 to 1000] is which the interval before which the Gateway Redundancy Manager expects at least one message or Heart Beat from the other Gateway. Click Confirm.
5. Click Yes to save the settings or No to abort.
6. Select Configure Heart Beat Retries tab from Heart Beat Configuration menu.
7. Enter Heart Beat retries [1 to 10] is which the number of retries Gateway Redundancy Manager transmits Heart Beat message before assuming that the other Gateway has failed. Click Confirm.
8. Click Yes to save the settings or No to abort.

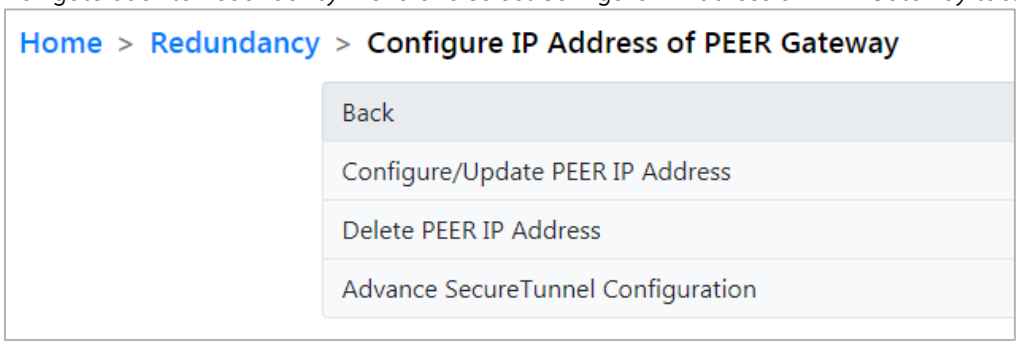
9. Select Configuration Heart Beat Communication Mechanism tab from Heart Beat Configuration menu.



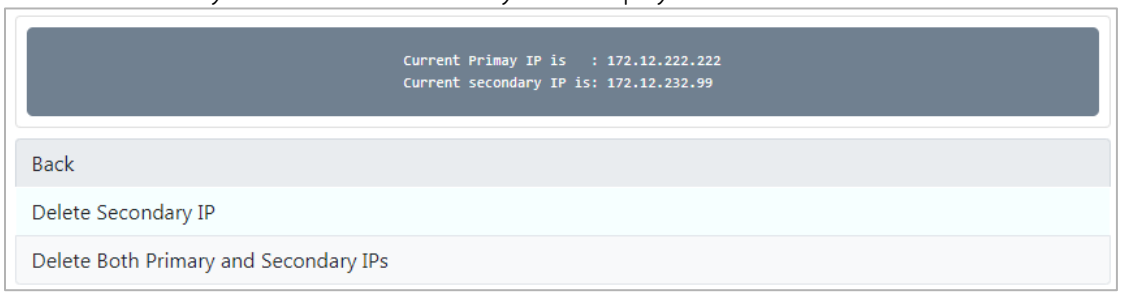
10. Select any of the Heart Beat Communication Mechanism from the list and click Yes to confirm.
RESULT: Settings have been saved, click OK.

Configure IP Address of PEER Gateway

1. Navigate back to Redundancy menu and select Configure IP Address of PEER Gateway tab.



2. Select Configure/Update PEER IP Address tab.
   - Enter new Primary IP Address and click Confirm.
   - Enter new Secondary IP Address and click Confirm.
     NOTE: Firewall does not allow Redundancy LAN Communication on External zones
   - Click Yes to confirm changes to take effect or No to abort.
     RESULT: Saving PEER IP Address, click OK.
3. Select Delete PEER IP Address tab.
4. The current Primary IP and current Secondary IP are displayed on the window:



5. Select Delete Secondary IP to delete it and click OK.
6. Select Delete Both Primary and Secondary IPs to delete both and click OK.
7. Select Advance Secure Tunnel Configuration tab.
8. Current Primary Secure Tunnel and current Secondary Secure Tunnel are displayed on the window.
   - Enter the new Primary Secure Tunnel address and click Confirm.
   - Enter new Secondary Secure Tunnel address and click Confirm.
     NOTE: Firewall does not allow Redundancy LAN Communication on External zones
   - Click Yes to confirm changes to take effect or No to abort.
     RESULT: Saving PEER IP Address, click OK.

Username of PEER Gateway

1. Select Username of PEER Gateway tab from Redundancy menu.
    - Enter New Username and click Confirm.
    - Click Yes to confirm.
    - RESULT: Successfully saved Username.

Configure Time Sync with Standby

1. Select Configure Time Sync with Standby tab from Redundancy menu.
    - If enabled, click Yes to disable Time Synchronization between Active and Standby Gateway.
      RESULT: Disabled Time Synchronization between Active and Standby. Click OK.
    - If disabled, click Yes to Enable Time Sync Gateway or No to abort.
        - Current Time Synchronization between Active and Standby Gateway is displayed.
        - NOTE: This option should be enabled only if Standby Gateway does not have a non-SCADA time synchronization mechanism (IRIG-B or NTP).

      RESULT: Enabled Time Synchronization between Active and Standby. Click OK.

Configure Enable/Disable DTAs in Standby

1. Select Configure Enable/Disable DTAs in Standby tab from Redundancy menu.
   NOTE:
    - This parameter is only applicable to hot standby mode. In case of warm standby, this parameter is ignored.
    - DTA's (LOGICLINX, Calculator and Enhanced Automation applications) on Standby Gateway are Enabled.
        - If Enabled, these DTAs will run normally on the standby Gateway.
        - If Disabled, these DTAs will suspend processing on standby Gateway.
    - Click Yes to Confirm.
    - RESULT: Enabled/Disabled DTA's on Standby Gateway. Click OK.

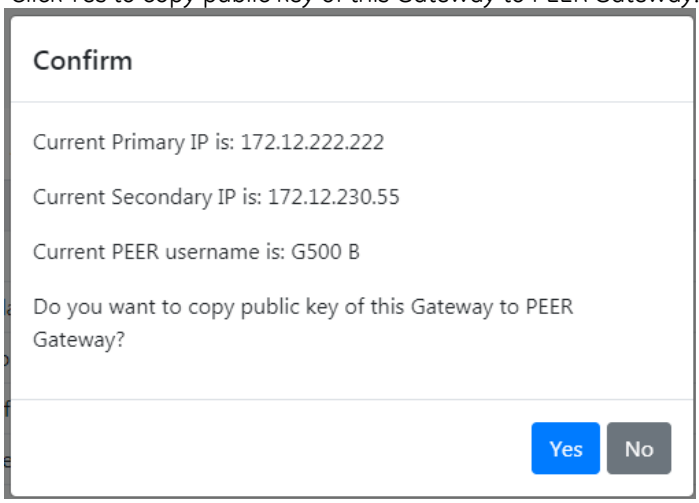
Configure Gateway A/B Designation

1. Select Configure Gateway A/B Designation tab from Redundancy menu.
2. A message showing the current Gateway Designation status is displayed.
   NOTE: Gateway A/B Designation:
    - This parameter is only applicable if Switch Panel is optional.
        - If Switch panel is not configured, this parameter is used.
        - If Switch Panel is configured, Gateway A/B Designation is read from the switch panel.
3. Select Gateway_A or Gateway_B.
   RESULT: Gateway A/B Designation changed to selected Gateway. Click OK.

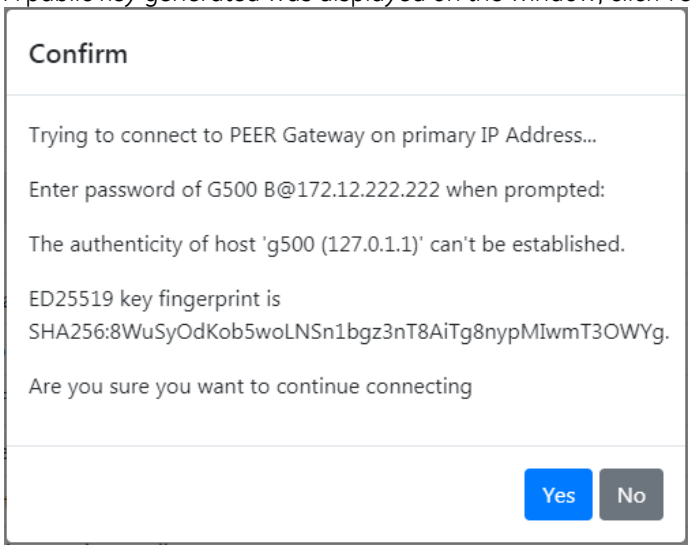
Setup Public Key Authentication with PEER Gateway

1. Select Setup Public Key Authentication with PEER Gateway tab from Redundancy menu.

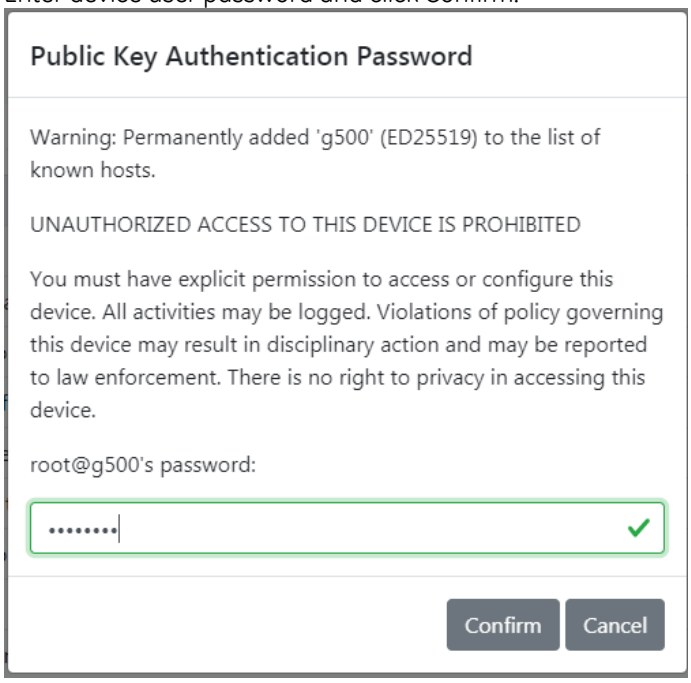
2. Click Yes to copy public key of this Gateway to PEER Gateway.



3. A public key generated was displayed on the window, click Yes to continue connecting.



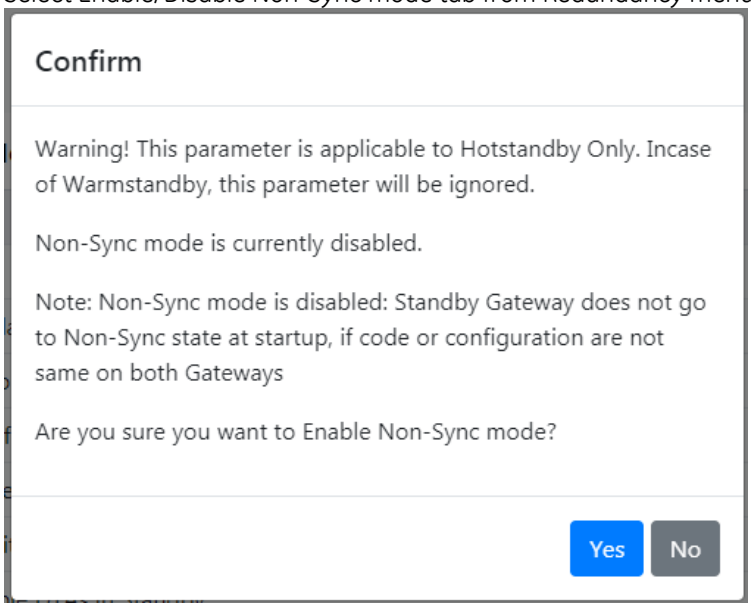
4. Enter device user password and click Confirm.



5. RESULT:
    - Successfully setup public Key Authentication with PEER Gateway.
    - You need to perform this operation on PEER Gateway as well
    - Click OK.
6. Select Configure Switch Panel Type tab from Redundancy menu.
7. Select switch panel type;
    - MASTER
    - SLAVE
8. RESULT; Switch Panel Type changed to selected. Click OK.

Enable/Disable Non-Sync mode

1. Select Enable/Disable Non-Sync mode tab from Redundancy menu.

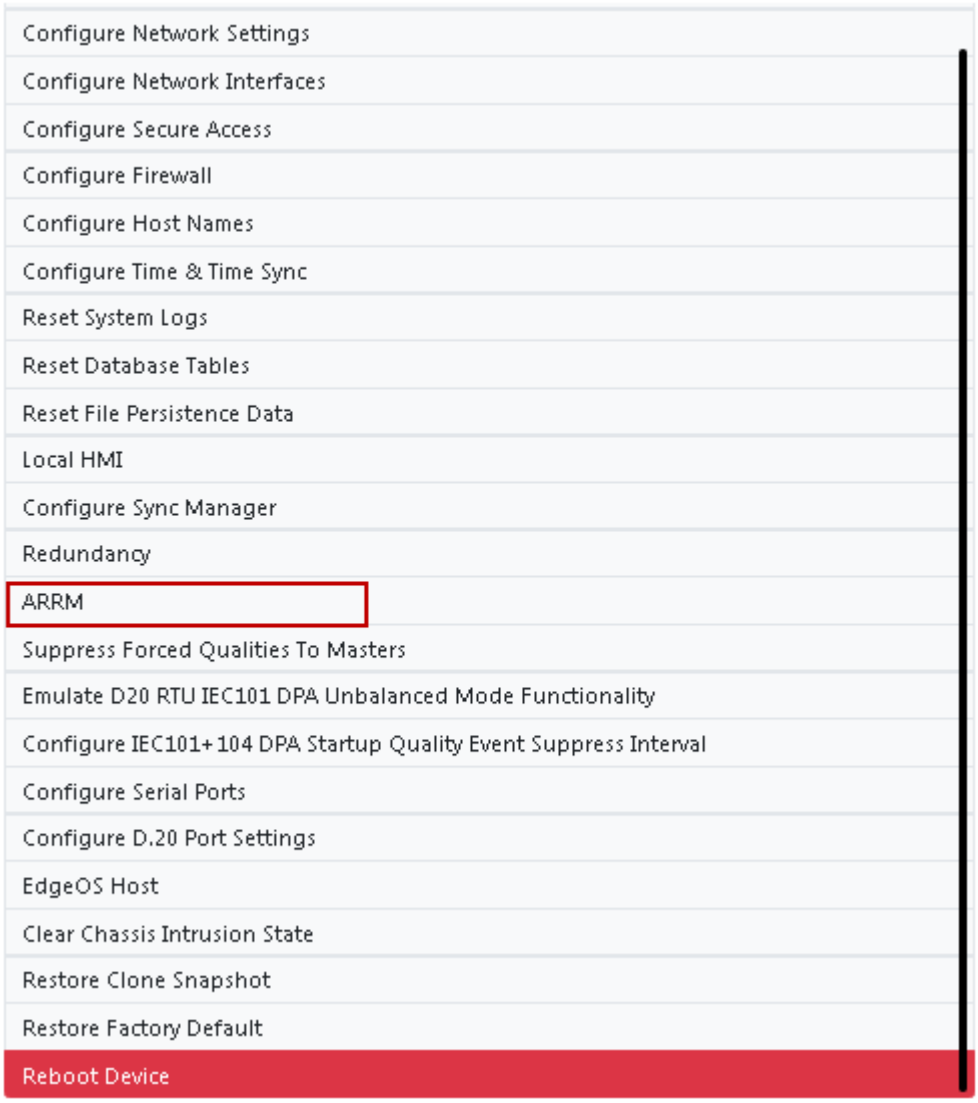


NOTE:

- This parameter is applicable to hot standby only. In case of warm standby, this parameter will be ignored.
- Non-Sync mode is enabled
    - Standby Gateway goes to Non-Sync state at startup, if code or configuration are not same on both Gateways.
- Non-Sync mode is disabled
    - Standby Gateway does not go to Non-Sync state at startup, if code or configuration are not same on both Gateways.
- Click Yes to Enable/Disable Non-Sync mode.

ARRM

1. Select ARRM tab from the main menu.



Delete Records

The function is used to perform the following actions:

- Delete all Records
- Delete Storage Directory Specific Records
- Delete Station Specific Records
- Delete Device Specific Records
- Delete Temp
- Delete Cache

Delete all Records

1. Select Delete all Records tab.
   NOTE: A WARNING message appears stating that the "Directory Delta records will not be retrieved again once deleted. Delete Cache Files to retrieve the old records.

2. Select Confirm to continue or Back to navigate back to Delete Records menu.
    - Select No to abort or
    - Select Yes to continue.
      RESULT: Restarts ARRM application. Details of files deleted are updated in log file.

Delete Storage Directory Specific Records

1. Select Delete Storage Directory Specific Records tab.
   NOTE: Directory Delta records will not be retrieved again once deleted. Delete Cache Files to retrieve the old records.
2. Click on the files that need to be deleted and click Yes to confirm or No to abort.
   NOTE: Deleting these files will restart ARRM application.

Delete Station Specific Records

1. Select Delete Station Specific Records tab.
   NOTE: Directory Delta records will not be retrieved again once deleted. Delete Cache Files to retrieve the old records.
2. Click on the files that need to be deleted and click Yes to confirm or No to abort.
   NOTE: Deleting these files will restart ARRM application.

Delete Device Specific Records

1. Select Delete Device Specific Records tab.
   NOTE: Directory Delta records will not be retrieved again once deleted. Delete Cache Files to retrieve the old records.
2. Click on the files that need to be deleted and click Yes to confirm or No to abort.
   NOTE: Deleting these files will restart ARRM application.

Delete Temp

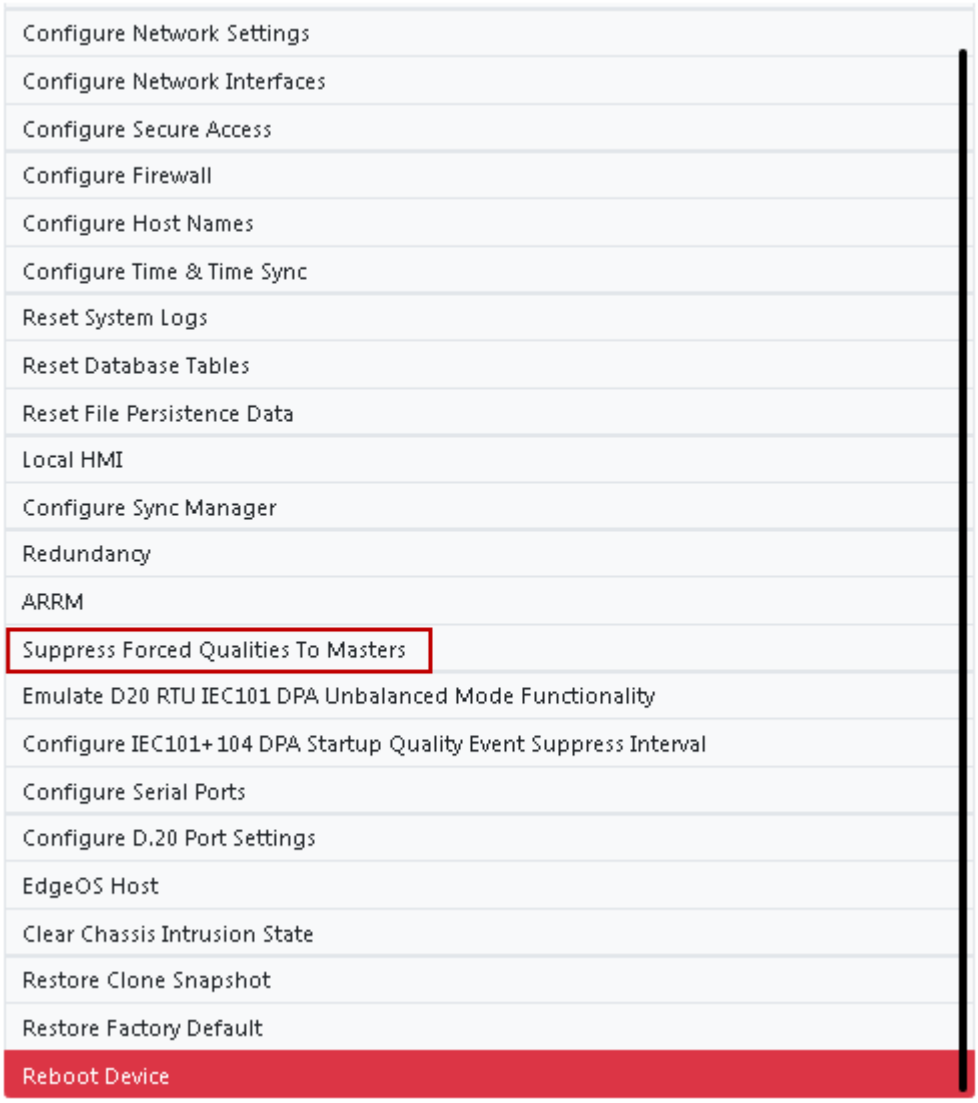
1. Select Delete Temp tab and select Confirm.
2. Select Yes to confirm or No to abort.
   RESULT: ARRM application will be restarted and the details of Files deleted are updated in log file. Click OK.

Delete Cache

1. Select Delete Cache tab to:
    - Delete All Cache Files
    - Delete Station Specific Cache Files
    - Delete Device Specific Cache Files
2. Select Delete All Cache Files tab and click Yes to confirm or No to abort.
   If Yes, RESULT; Restarts ARRM application.
3. Select Delete Station Specific Cache Files tab and click Yes to confirm or No to abort.
    - If Yes, enter Station Name and click Confirm.
      RESULT: ARRM application will be restarted and the details of Files deleted are updated in log file. Click OK.
4. Select Delete Device Specific Cache Files tab and click Yes to confirm or No to abort.
    - If Yes, enter Station Name and click Confirm.
    - Enter Device name and click Confirm.
      RESULT: ARRM application will be restarted and the details of Files deleted are updated in log file. Click OK.

Suppress Forced Qualities To Masters

1. Select Suppress Forced Qualities To Masters tab from the Main menu.



2. When Enabled for a Master:
   - For a configured duration, values with Forced/Substituted Flags are communicated to Master as value changes only.
     - No Forced/Substituted Flags are seen.
     - All other flags will still be communicated normally.
   - NOTE:
     - On expiration of configured suppression time or on disabling this mode, normal processing will be resumed.
     - Currently this feature implies only for IEC101-104 masters.
3. This function is used to perform the following actions:
   - Suppression Mode Timer Stats
   - Enable/Disable Mode for all Masters
   - Enable/Disable Mode for only specified Masters

Suppression Mode Timer Stats

1. Select Suppression Mode Timer Stats tab.
   NOTE: At any point of time this stat shows the remaining time for which the qualities will be suppressed to IEC101-104 master.
2. Select Serial IEC-60870-101 Master or Network IEC-60870-104 Master tab from Suppression Mode Timer Stats menu to view Suppressed Values Summary.

Enable/Disable Mode for all Masters

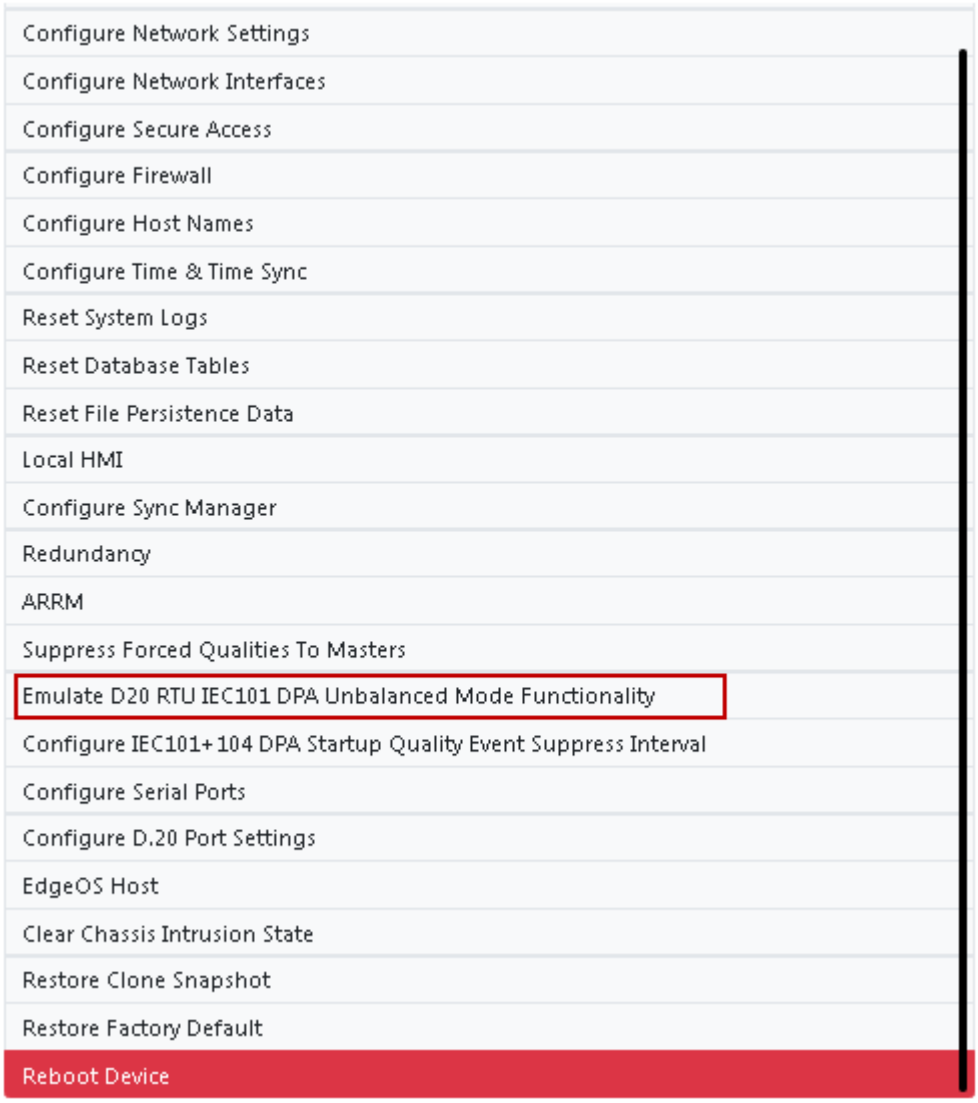
1. Select Enable/Disable Mode for all Masters tab from Suppress Forced Qualities to Masters menu.
2. Click Yes to change the Quality Suppression Mode and enter the Quality suppression period in hours [1-120].
   RESULT: Restarting all applications for changes to take into effect, click OK.

Enable/Disable Mode for only specified Masters

1. Select Enable/Disable Mode for only Specified Masters tab from Suppress Forced Qualities to Masters menu.
   - Serial IEC-60870-101 Master
   - Network IEC-60870-104 Master
2. Select Serial IEC-60870-101 Master tab and select any of the configured Serial port number of IEC Master and click on the toggle switch at the bottom of the window to change the mode and click Yes to configure suppression mode for any other masters before restarting all applications.
3. Select Network IEC-60870-104 Master tab and select any of the configured Network Instance number of IEC Master and click on the toggle switch at the bottom of the window to change the mode and click Yes to configure suppression mode for any other masters before restarting all applications.

Emulate D20 RTU IEC101 DPA Unbalanced Mode Functionality

1. Select Emulate D20 RTU IEC101 DPA Unbalanced Mode Functionality tab from Main Menu.

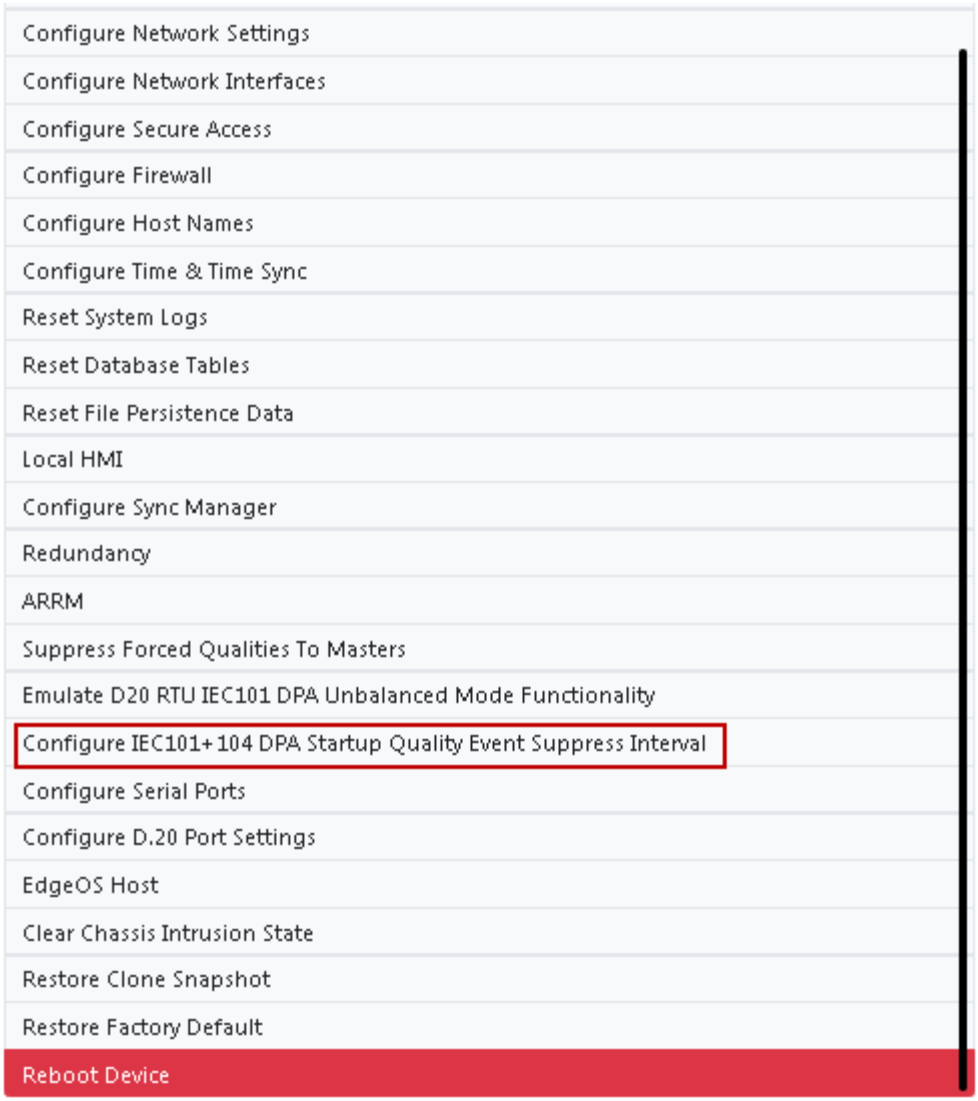


Set Emulate D20 RTU IEC101 DPA Unbalanced Mode Functionality to TRUE/FALSE

1. Set Emulate D20 RTU IEC101 DPA Unbalanced Mode Functionality to TRUE/FALSE, click Yes to confirm.
   RESULT: Emulate D20 RTU IEC101 DPA Unbalanced Mode Functionality is set to selected., Click OK.

Configure IEC101+104 DPA Startup Quality Event Suppress Interval

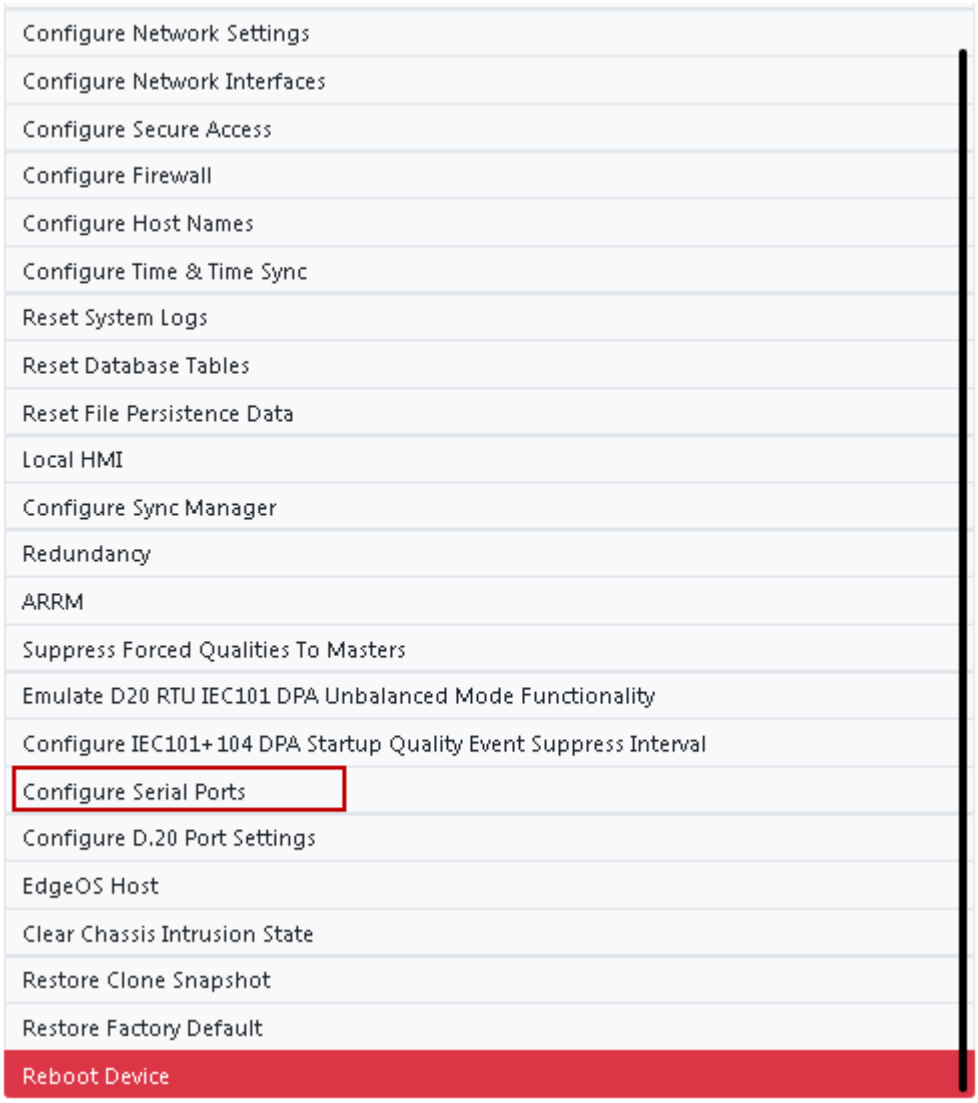
1. Select Configure IEC101+104 DPA Startup Quality Event Suppress Interval tab from the Main menu.



2. Current Value of Startup Quality Event Suppress Interval (in seconds) is displayed.
   NOTE: Set the value of startup quality event suppress interval to 0 seconds to disable this functionality.
3. Enter Startup Quality Event Suppress Interval in Seconds [0 to 600] and click Confirm.

Configure Serial Port Modes (RS-232/485)

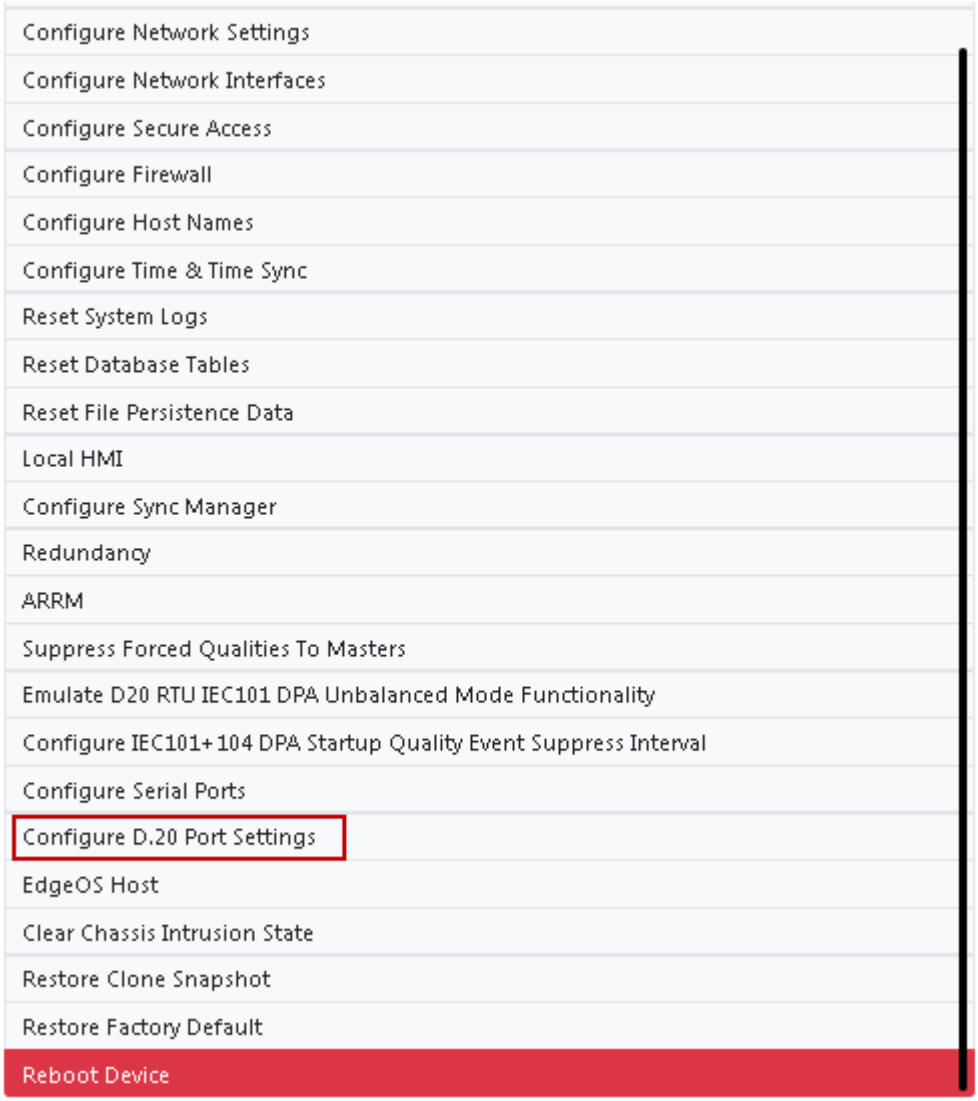
1. Select Configure Serial Ports tab from Main menu.



2. Select the desired port, mode and its termination if applicable (Disabled/Enabled). Click Apply.

Configure D.20 Port Settings

1. Select Configure D.20 Port Settings tab from Main menu.



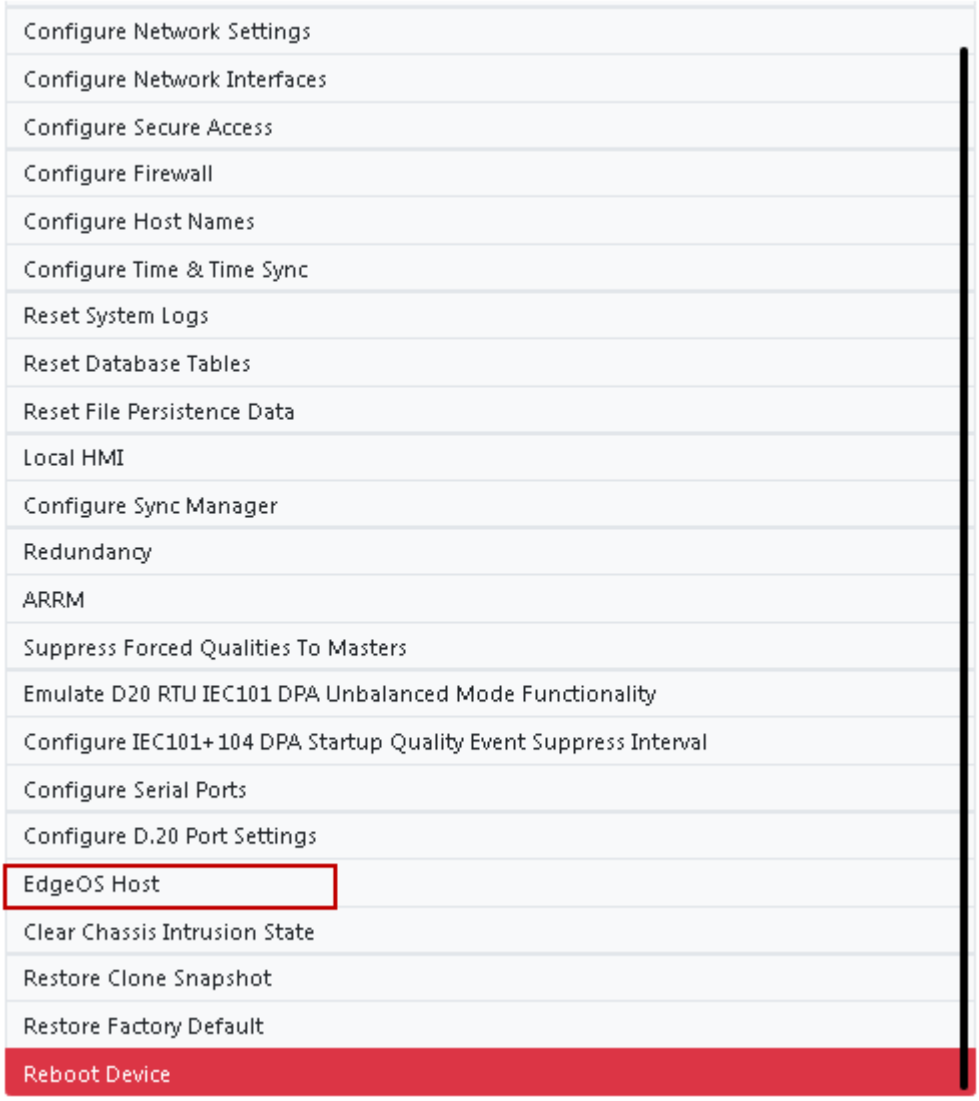
2. The below message appears if no D.20 HDLC cards installed.

3. Install D.20 HDLC card and select D.20 HDLC PCIe 3 tab.
4. Select D.20 Channel 1/2 tab to perform:
   - End of Link Termination
   - D.20 Port B Connection
5. Select End of Link Termination tab.
   - Click No to abort
   - Click Yes to change the status (Enable/Disable)

6. Select D.20 Port B Connection tab.
    - Click No to abort
    - Click Yes to change the status (Enable/Disable)

EdgeOS Host Access

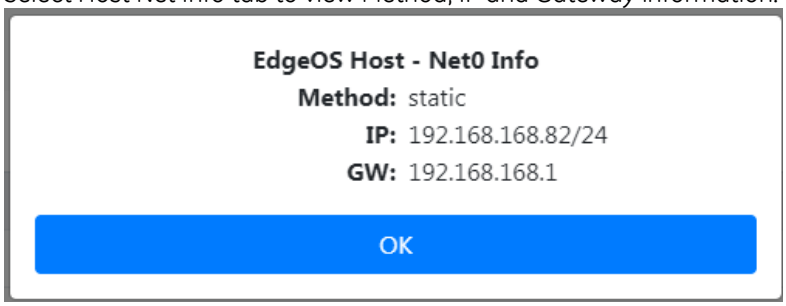
1. Select EdgeOS Host from Main menu.



2. The function is used to perform the following actions:
    - Host Net Info (in G100 is Net1, in G500 is Net0)
    - Host Version Info
    - Enable Host SSH/SCP Service
    - Disable Host SSH/SCP Service
    - Change Host Shell Idle Timeout
    - Host Logoff

Host Net Info

1. Select Host Net Info tab to view Method, IP and Gateway information. Click OK.



Host Version Info

1. Select Host Version Info tab to view EdgeOS Host release information. Click OK.

Enable Host SSH/SCP Service

1. Select Enable Host SSH/SCP Service tab.
   - Enter the timeout in minutes [5 to 240] and click Confirm.

   RESULT:

   - Host SSH/SCP service has been enabled and will expire as per timeout.
   - Please make a note of the root password for the host SSH/SCP access: (_____)
   - Once the timer expires, Active SSH user session will not be automatically logged off. User must log them off using the "Host Logoff" option or reboot the MCP.

   - Click OK.

Disable Host SSH/SCP Service

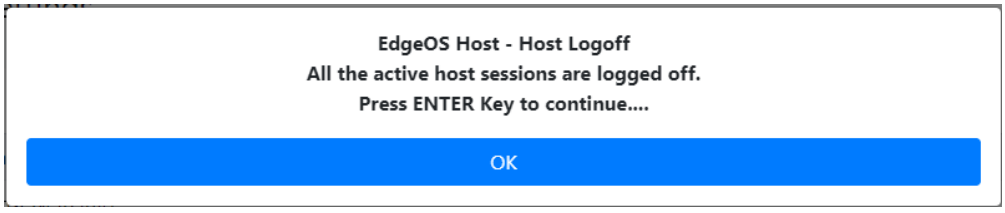
1. Select Disable Host SSH/SCP Service tab to disable SSH/SCP service.
   RESULT: Host SSH/SCP service has been disabled. Click OK.

Change Host Shell Idle Timeout

1. Select Change Host Shell Idle Timeout tab.
   - Current host shell idle timeout is displayed in seconds, click Yes to continue and enter the timeout in seconds [60 to 1800]. Click OK.

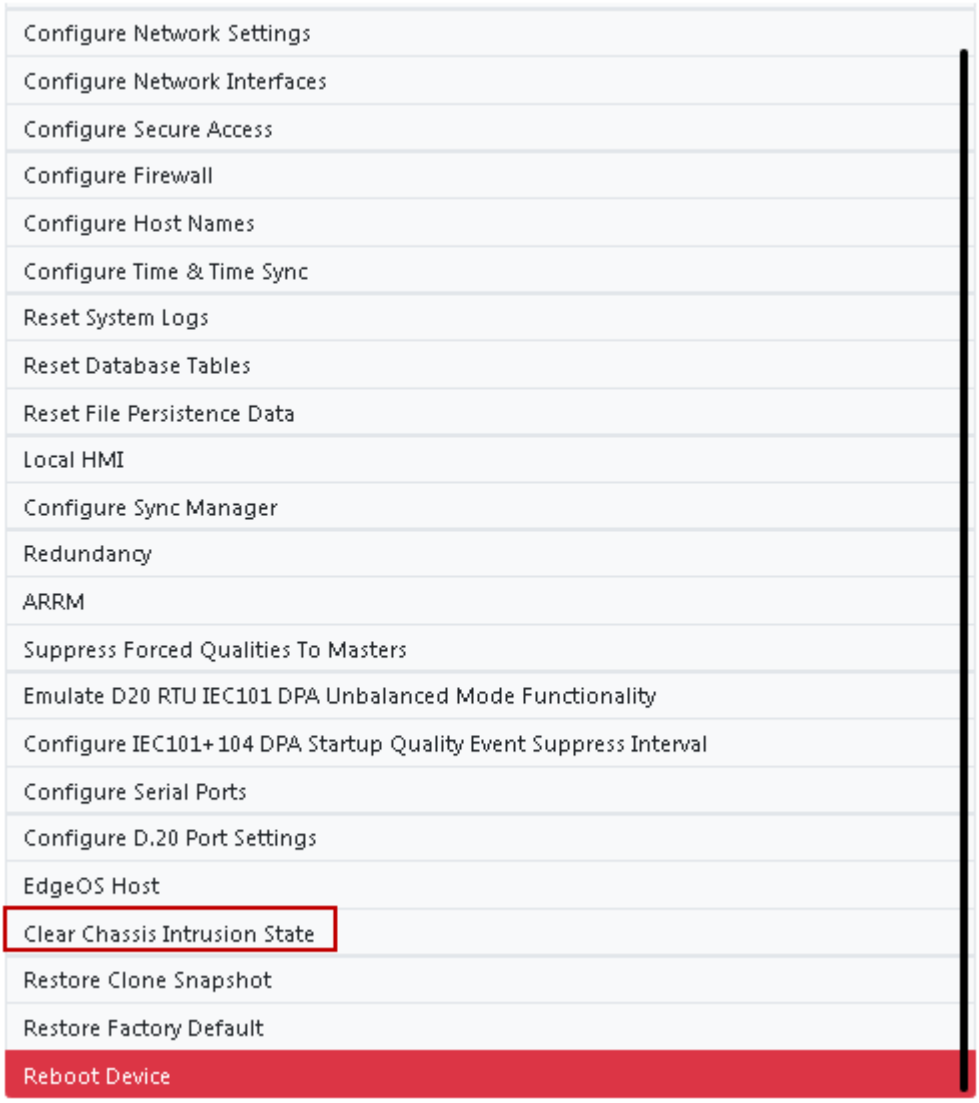
Host Logoff

1. Select Host Logoff tab.
   RESULT:



Clear Chassis Intrusion State

1. Select Clear Chassis Intrusion State tab from Main menu.



2. Click Yes to confirm or No to abort.
   RESULT:
   - If No, no action performed.
   - If Yes, successfully cleared Chassis Intrusion State. Click OK.

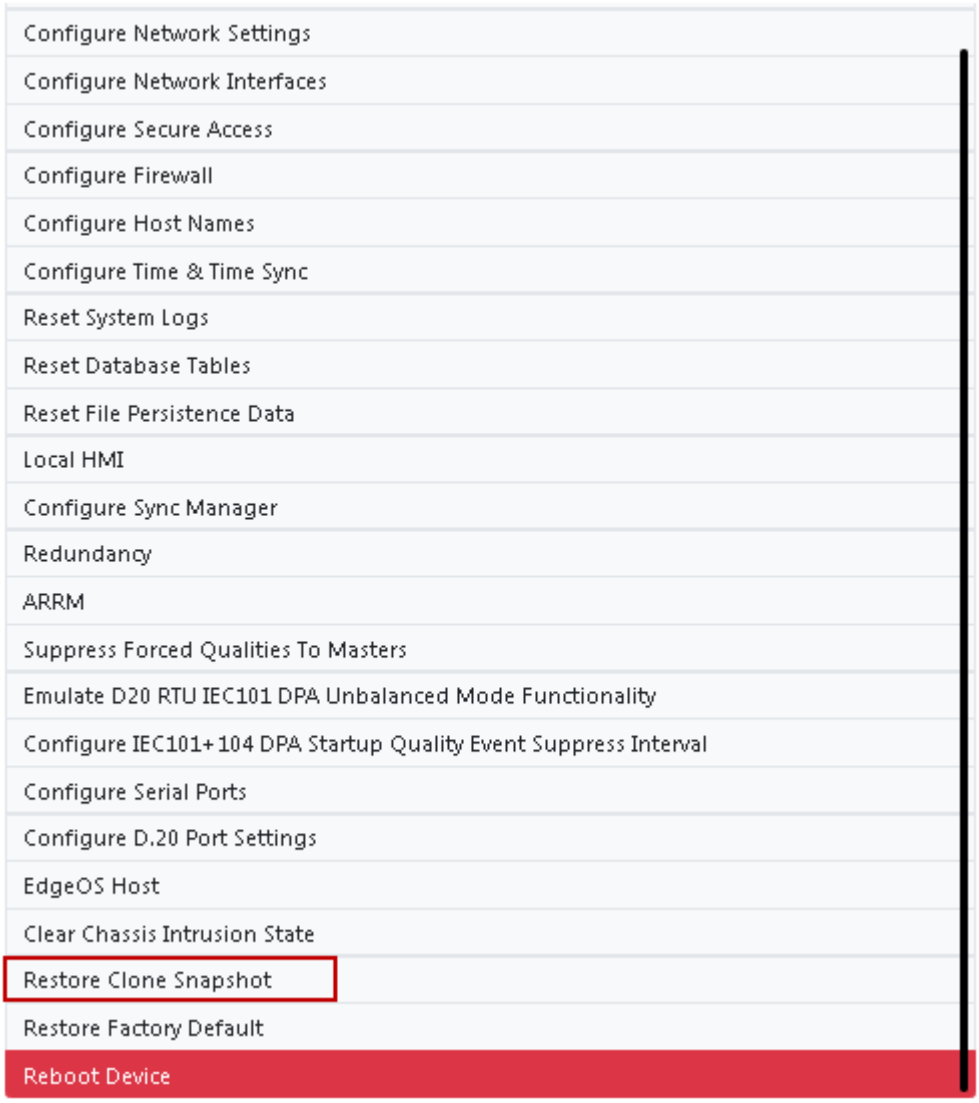
Restore Clone Snapshot

Precondition: In order to perform this operation, user needs to connect a FAT32 formatted USB device containing clone snapshot file(s) with extension *. MCPClonesnapshot.DS7zip (taken using DSAS).

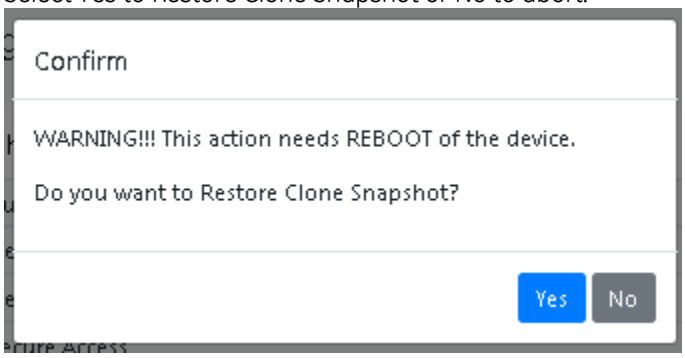
GE doesn't recommend using more than one USB connected at a time for this operation.

NOTE: Automatic reboot of the device takes place to make the changes effective.

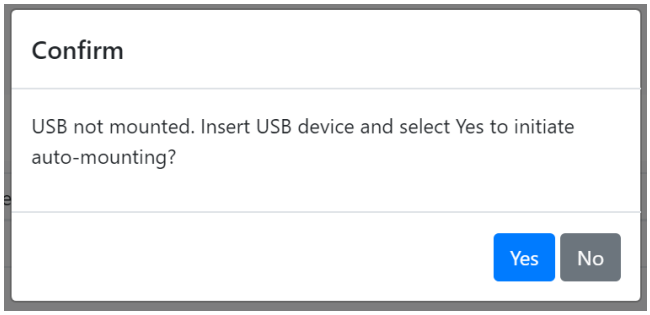
1. Select Restore Clone Snapshot tab from Main menu.



2. Select Yes to Restore Clone Snapshot or No to abort.

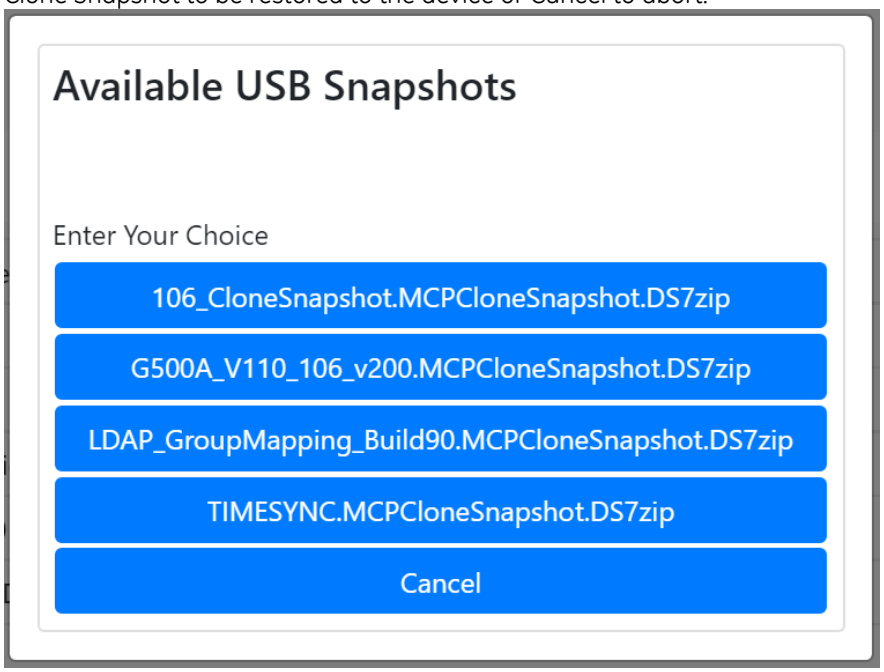


3. Select Yes to Auto Mount the USB or No to abort.

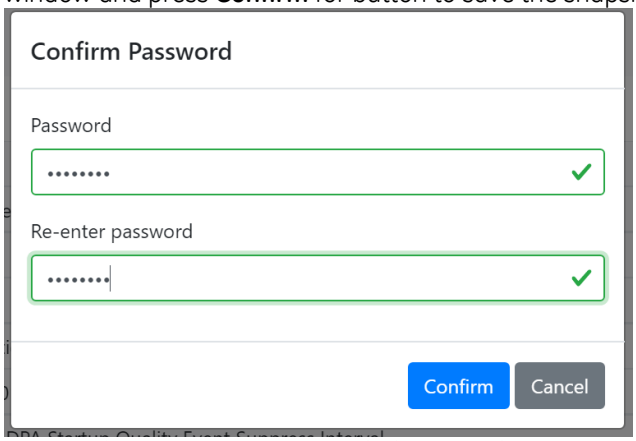


If more than one USB is connected to device, then the list of USBs will be displayed, and the User need to select the USB from which the Clone snapshot need to be restored.

4. If Single USB is connected to device, then the list of clone snapshot snapshots will be displayed. Select the Clone Snapshot to be restored to the device or Cancel to abort.



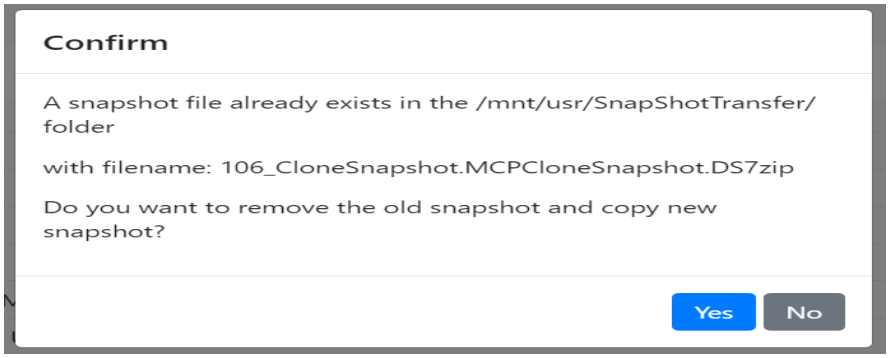
5. If the selected Clone Snapshot is a password protected, then enter the password in the confirm password window and press **Confirm** for button to save the snapshot or **Cancel** to abort the operation.



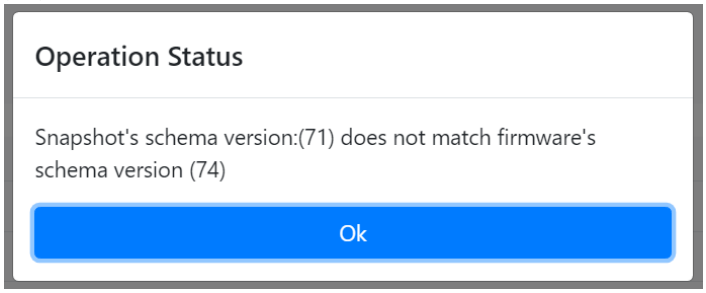
Note: Only 3 attempts are provided to provide correct password, failing will display message 'Error: Unable

to extract with the password provided. Retry entering valid Password. Error: Max retries reached.' OK to return to main Menu.

6. On Selection of Confirm
    a. If the Clone snapshot schema version match with device schema version, then snapshot copy is successful with message 'Snapshot will be applied after Reboot'.
    b. If snapshot folder already contains snapshot, the Confirm operation popups to delete old clone snapshot and copy the new one. Yes, to overwrite and proceed to save the snapshot- '`Snapshot will be applied after Reboot 'or No to abort replace the operation.



    c. If the Clone snapshot schema version doesn't match with device schema version, then snapshot will fail with message 'Snapshot's schema version:(XX) does not match firmware's schema version (XX)'.



7. Automatic reboot of the device takes place to make the changes effective.

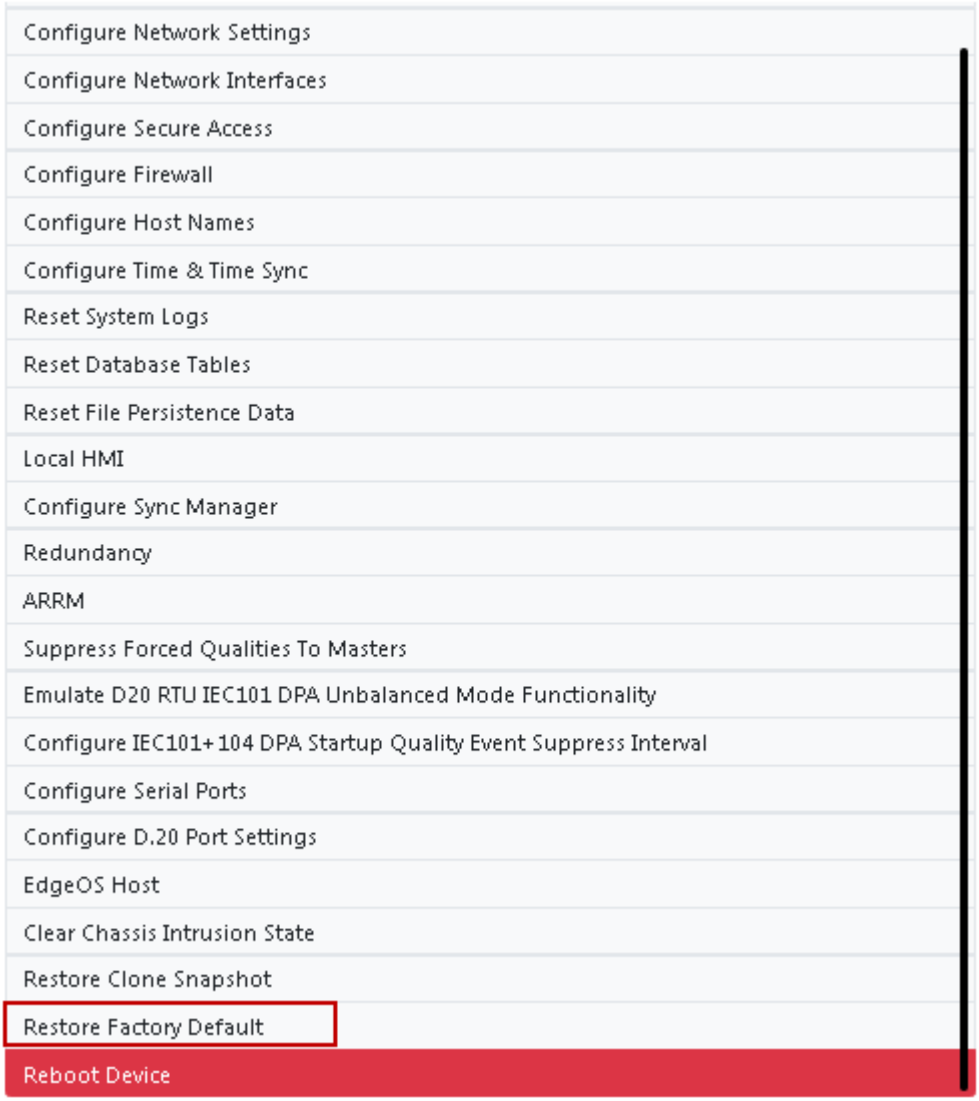
Restore to Factory Default

User can restore a MCP to the factory default (or "clean") configuration.

When restored to default factory settings, all user configuration files, and system settings will be lost.

In case all root / administrator user credentials have been lost, and the MCP cannot be accessed with these roles – the MCP can be restored to a clean and defaulted state using an external USB workflow; for detailed steps please refer to the technical note: *TN0116 MCP Firmware Upgrade and Restore to Defaults Workflows.*

1. Select Restore Factory Default tab from Main menu



2. Click Yes to restore to Factory Default or No to abort.
   NOTE: Ensure you have a full snapshot of the current configuration.
3. If Yes,
   NOTE: When restored to default factory settings, all user configuration files, and system settings will be lost. All System Databases will also be deleted.
4. Click Yes to confirm.

Reboot Device

1. Select Reboot tab from Main menu.

2. Click Yes to reboot the device or No to abort.

Chapter 6 - DS Agile Studio Configuration

This chapter consists of the following sections:

Steps to Configure MCP
- Configuration file format

Configure System Wide Options
- Systemwide tab
- AI Text Enumeration Tab

Build Client Map Files
- GPIO Configuration steps
- D.20 Peripheral Client
- Client Map
- DNP3 Client
- Modbus Client
- SEL Binary Client
- IEC 60870-5-103 Client
- IEC 60870-5-101+104 Client
- Generic ASCII Client
- SNMP Client Properties
- IEC 61850 Client

MCP Redundancy
- About Redundancy
- Redundancy Summary
- Operational States
- MCP Redundancy Configuration Combinations
- Configure the MCP for Redundancy
- System Points
- Non-Sync Mode
- Validating the Redundant Connections
- Changeover during Standby Start-up
- Data Synchronization
- Ethernet Connections
- Sync Config Operation
- HMI User Access Privileges on Redundant System
- Redundancy Setup Checklist
- Error Messages and Troubleshooting

Communications
- Connection

Configuring Client Applications
- Client Configuration Overview
- DNP3 Multi-drop
- DNP IED Block
- IEC 60870-5-101 Multi-drop
- IEC 60870-5-103 Multi-drop
- IEC 60870-5-104 IED Block
- Modbus Multi-drop
- Modbus TCP or TCP/SSH IED Block
- Generic ASCII
- SEL Binary
- LogicLinx Device
- SNMP Block

Configure to acquire files(ARRM)
- Automated Record Retrieval Manager Overview
- ARRM Configuration
- ARRM Viewer
- ARRM Pseudo Points
- Enterprise Synchronization
- Applications - ARRM
- File Set Template - Standard
- File Set Template – Sel ASCII
- About Oscillography files and IEEE File
- Connection Polling
- Sample File Set Templates for Relay Models
- ARRM ASCII Directory Delta Support

Configure Automation Features
- Configuration Overview
- System Point Manager
- Accumulator Freeze
- Alarm
- Calculator
- Input Point Suppression
- Remote Logging (Rsyslog)

Configure Serial Communications
Configure Network Communications

Configure Datalogger
Report Types
Storage Allocation
Save Report
Load Report
Manage Reports
Select Points
Change Scaling

HAMA - Hardware Asset Management Application
Analog Inputs
Digital Inputs
Accumulator Points
Text Points

Build Server Map Files
Server Maps
DNP3 Server
MODBUS Server
IEC 60870-5-101+104 Server

Configuring Server Applications
Server Configuration Overview
DNP3 Serial Master Stations
IEC 60870-5-101 Master Station
Modbus Serial Master Station
DNP3 Network Master Stations
IEC 60870-5-104 Master Station
Modbus TCP Master

Build HMI One-Line Diagrams
One-Line Viewer
View One-Line Diagrams
Executing One-Line Diagram Commands

Create Analog Reports
Analog Report Generation - Overview
Analog Report - Viewing
Analog Report Generation - Configuration

Configure System Security
Security Features
System Security
Password Complexity
Connection Security
User Accounts and Authentication
Setting Up a User Account
Secure Access
Software Licensing Tools
Firewall Settings
Automatic logout

System Utilities
Utilities
Utilities Log In
Certificate Import
Certificate Management
Export Database
Generate Gateway Key Pair
Exporting VPN Client Configuration File
Upload SSL server Certificate/Server Key

Miscellaneous Utilities
Utilities Overview
Setting up a Terminal Session
Pass-Through Connections
Direct Connect (mcpconnect)
MCP Configuration Manager

DS Agile Studio MCP Configuration steps

Once basic settings are configured using MCP Gateway Local Configuration Utility settings (mcpcfg) or MCP Settings GUI , use DS Agile MCP studio's online & offline configuration tool to configure the MCP's gateway/SCADA configuration. The typical sequence of steps involved in configuring MCP from DS Agile MCP Studio are as follows:

1. Create the configuration of MCP device using an administrator level user or supervisor level user. Refer to DS Agile MCP Studio's Online Help or User Manual for more details.
2. Use "Sync From" option from the DS Agile MCP Studio's offline editor/configuration tool and get the current settings from the MCP device. This would need connecting to MCP once through the IP Address of the MCP. The default connection mode is HTTPS.
3. Once the MCP's device settings are synced to DS Agile MCP Studio, Use the offline editor/ configuration utility and configure system settings for the MCP first.
4. Configure the MCP Device Redundancy if MCPs need to be configured for redundancy or else skip this step.
5. Create and edit Client (device) maps.
6. Set up device serial and network connections, including protocol-specific parameters.
7. If IEC61850 client needs to be configured, then using Loader utility in the DS Agile Studio and configure the IEC61850 client configuration.
8. If Automatic Record Retrieval Manager (ARRM) needs to be configured, then use the ARRM configuration from the offline configuration utility and configure ARRM to acquire files from the IEDs.
9. If Passthrough, Terminal Server, Secure Scada or OpenVPN needs to be configured then configure the same from the offline configuration tool. Note that OpenVPN configuration is configured using administrator level users only.
10. Configure Automation applications, including the Digital Event Management (alarms), Calculator, Logiclinx and the System Point Manager etc using the offline configuration tool.
11. Configure Datalogger and Analog Reports.
12. Create and edit Server (master station) map.
13. Set up master station connections, including protocol-specific parameters.
14. Create substation one-line diagrams using the One-Line Designer utility from the offline configuration tool.
15. Configure System Security settings (e.g. creation of HMI users, HMI Auto Login settings, importing/installing of certificates, exporting of Open VPN client configuration files etc.) using online editor/configuration utility of DS Agile MCP Studio.
16. Save the configuration file by applying commit changes button from the online configuration utility DS Agile MCP Studio.
17. Apply "Sync To" from the DS Agile MCP Studio's offline editor/configuration utility to transfer that applies configuration changes to the MCP.

The DS Agile MCP Studio configuration tool validates the changes and reports any errors. Once a configuration is validated and committed to MCP through "Sync To" option in the Offline configuration tool, the previous configuration files are replaced with the new file and all the MCP applications are re-started to reflect with the new configuration changes.

The Help section in the DS Agile MCP Studio Offline Configuration Tool describes how to configure the MCP for various substation applications

Configuration file format

All Gateway/SCADA Configuration information for an individual MCP is stored as a set of configuration files. The configuration files are saved into the Solid-State Drive on the MCP. The configuration files are stored as XML files.

The configuration files contain the following information:

- Device and master point maps
- Application settings
- HMI settings

Configuration information for each application, is also contained in the individual configuration files which includes configuration settings, default application settings and saved or custom user settings.

All MCP Device specific and System configuration information that is modified using the MCP's Gateway Local configuration utility (mcpcfg) or MCP Settings GUI is stored in separate set of configuration files on the MCP. These configuration files are updated each time changes are made through mcpcfg. The configuration file is stored in non-XML files.

Configure System Wide Options

This chapter contains the following sections and sub-sections:

Systemwide tab
Point Groups
Security
Email configuration
Storage
RTDB Configuration
Event Logger
Locale
Access Manager
Runtime GUI

User Management
Overview
Add a User
Change a User Account
Delete a User
Configure User HMI Home Page
Auto Login

AI Text Enumeration
Enumeration Values
Analog Input Mappings

Systemwide tab

The **Systemwide** tab in the **DSAS MCP Studio Configuration Tool** provides access to a wide range of options for the general operation of the MCP, including:

- System
  - Point Groups
  - Security
  - Email
  - Storage
- Real-time Database (RTDB)
- Event Logger
- HMI
  - Locale
- Access Manager
  - Authentication
- Runtime GUI
  - Global

To access any of these configuration areas, select the appropriate item from the left pane.

Point Groups

The **Point Groups** option under the **Systemwide** tab->System allows you to configure the names of point groups to appear on the **Point Summary** pages.

» To modify the point groups:

1. Open the DSAS MCP Studio Configuration Tool.
2. Click the **Systemwide** tab.
3. In the left pane, click **System** > **Point Groups** and modify the settings, if desired.
   - Click **Add** to create a new group. Double-click a field to modify the settings.
   - Select a row and click **Delete** to remove an application from the list.
4. Click **Save** to save your changes.
5. Click **Commit Changes** to apply the changes to the MCP.

NOTE: The point group assigned to ID number 0 will be used as the default point group. Newly created points are automatically assigned to this group. You should not delete this point group.

Security

The **Security** options on the **Systemwide** tab -> system allows you to configure the general security features of the MCP.

» To change security settings:

1. Open the DSAS MCP Studio Configuration tool.
2. Click the **Systemwide** tab.
3. In the left pane, click **System** > **Security** and change the security settings, if desired.
4. Click **Save** to save your changes.
5. Click **Commit Changes** to apply the changes to the MCP.

Security settings

Table 6.1: Security Settings

Point Name	Description
Pass-through Access	If set to **From command line only**, you must initiate connections to devices manually from the MCP command line using the *mcpconnect* utility. Note that only SEL Binary and Generic ASCII clients support command line access. If set to **Allow network connections**, the MCP makes the pass-through connections accessible over the network on port *<8000 plus the configured com port number>*. For more information on the *mcpconnect* utility and pass-through connections, refer to Direct Connect. Default is **From command line only**.
Passthrough Idle Timeout	Specify the time duration that Pass Through enabled DCA/Terminal Server waits for the data to be available from the user in SSH Secure Tunnel Mode before closing the connection. This parameter is not applicable to Telnet or TLS Security Types.
Local Commands Only	If set to true, only commands issued from the Local HMI (accessed from the USB KVM card) are accepted. If set to false, both local and remote commands are accepted. Applies to controls, set points, local force, inhibits and tagging commands. Default is false.
SSH Security Banner	A block of text that appears on the local HMI command prompt/Login with Secure Terminal Emulator from DS Agile MCP Studio.
Login Security Banner	A message appears on the login page of the MCP local HMI or remote HMI.
CRL Check Interval (Hours)	The interval that the Secure SCADA module checks whether certificates currently in use have been revoked. If the value of CRL Check Interval is 0, the Secure SCADA module will not perform a periodic check of whether certificates currently in used have been revoked. The range is from 0 to 720.

Email configuration

The MCP can send logs produced by the Digital Event Manager by email to a defined distribution list to notify users of configured system exceptions.

Using the **Server** settings on the **Systemwide** tab **-> System**, you can update the email server information and email address list. The MCP supports network and dial-up (PPP) connections to email servers.

» To set up email Server

1. Open the DSAS MCP Studio Configuration tool.
2. Click the **Systemwide** tab.
3. In the left pane, click **System** > **Server** and enter the settings for the email server.
4. In the left pane, click **System** > **Recipients** and add the email recipients.
   - Click **Add** to create a new entry. Double-click a field to modify the settings.
   - Select a row and click **Delete** to remove an email address from the list.
5. Click **Save** to save your changes.

Email Server settings

Table 6.2: Email Server Settings

Field	Description
Enable Dial Out	Select to enable PPP dial-up: **True** or **False**.
Dial Out Username	Enter a username, if required by the email server.
Dial Out Password	Enter a password, if required by the email server.

Field	Description
Enable Dial Out	Select to enable PPP dial-up: **True** or **False**.
Server Type	Select the type of authentication protocol (handshaking) configured on the PPP server: **Script based**, **PAP/CHAP** or **NT Based MSCHAP**.
Primary Phone # (dial-up only)	Enter the phone number.
Secondary Phone # (dial-up only)	Enter a phone number if the Primary phone line is unavailable.
Idle Time Before Hanging Up (dial-up only)	Enter the amount of time (in seconds) the MCP waits before closing an idle connection. Range is 0 to 240.
Enable Log Session	Select to activate a session log of the PPP dialer: **True** or **False**. The messages are stored in the MCP system log.
Email Server Address	Enter the IP Address of the email server in ipv4 format (*123.x.y.z*) or the fully qualified domain name. To disable email notification, set to 127.0.0.1.
Email Server Username	Enter the username of the email server. Default value is temp.
Email Server Password	Password to be used when accessing the PPP server. Default password is temp123$.
Sender Email Address	Enter the email address of the MCP. Default is gateway@ge.com.

Email Recipient settings

Table 6.3: Email Recipient Settings

Field	Description
Send Email	Select to include the recipient on the email distribution list.
Email	Enter the recipient's email address in the format *name@domain.tld*.
Name	Enter the name of the email recipient.

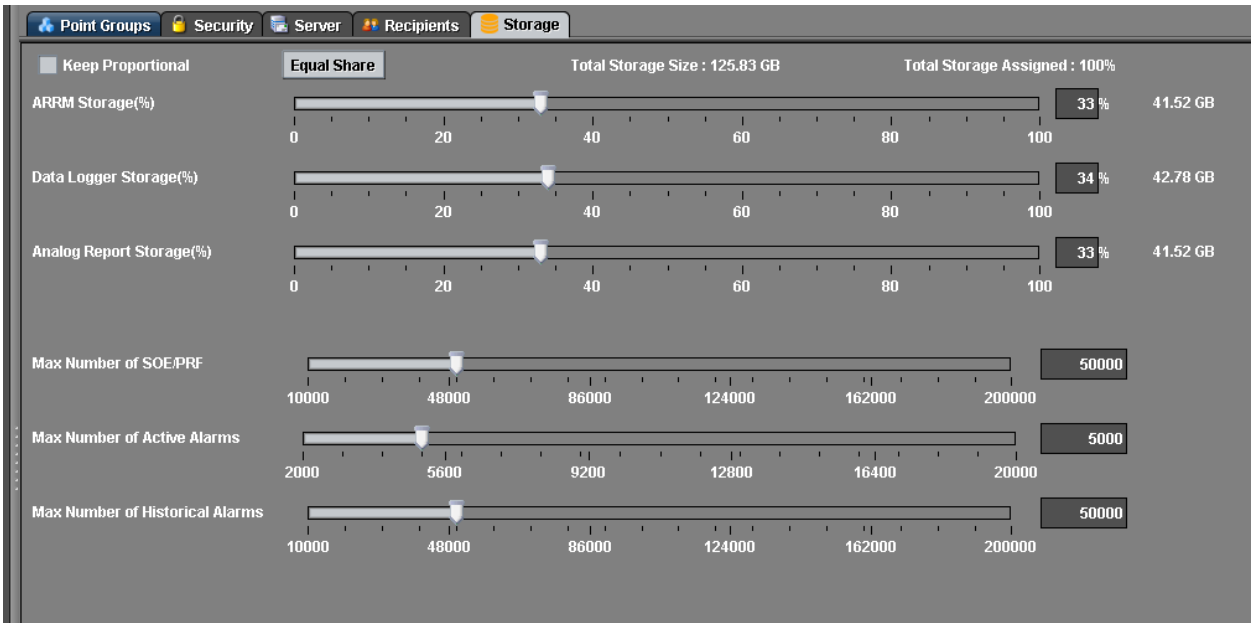
Storage

Using the storage option, you will be able to allocate storage areas for the various subsystems, and this will be done exclusively with the sliders as shown;

» To change storage settings:

1. Open the **DSAS MCP Studio Configuration Tool**.
2. Click the **Systemwide** tab.
3. In the left pane, click **System** > **Storage** and change the storage settings, if desired.
4. Click **Save** to save your changes.
5. Click **Commit Changes** to apply the changes to the MCP.

Figure 6.1: Storage



The following subsystems storage space is allocated with this storage option

- ARRM
- Data Logger
- Analog Reports

The maximum number of SOE, active alarms and historical alarms that can be present in the MCP database are configurable and this configuration is done from **storage** option on the **Systemwide** tab.

RTDB Configuration

Using the **RTDB** option on the **Systemwide** tab you can change general settings for how data is handled by the real-time database (RTDB).

» To change RTDB settings:

1. Open the **DSAS MCP Studio Configuration** tool.
2. Click the **Systemwide** tab.
3. In the left pane, click **RTDB** and change the settings, if desired.
4. Click **Save** to save your changes.
5. Click **Commit Changes** to apply the changes to the MCP.

RTDB settings

Table 6.4: RTDB Settings

Field	Description
AI Persistence	Select the type of analog input persistence: **RAM**. The default value is RAM.
AO Persistence	Select the type of analog output persistence: **RAM**. The default value is RAM.
DI Persistence	Select the type of digital input persistence: **RAM**. The default value is RAM.

DO Persistence	Select the type of digital output persistence: **RAM**. The default value is RAM.
ACC Persistence	Select the type of accumulator persistence: **RAM**. The default value is RAM.
Text Persistence	Select the type of text persistence: **RAM**. The default value is RAM.
Output Command Time To Live	Enter the amount of time, in seconds, that passes before a control request is cancelled. Range is 0 to 65535. Default is 5.
Max Startup Sync	Enter the maximum start-up synchronization period (in seconds) for MCP applications to register all events generated at start-up. If set to 0, there is no limit on the duration. Range is 0 to 65535. Default is 0.
Event Queue Full Action	Select how events are handled if the event queue is full: **Do not lose events** or **Lose newest events**.
Event Distribution Priority	Select the distribution priority of events: **High** or **Normal**.
HMI Status Queue	Enter the directory path and file name where the command status queue is stored. This field is not editable.
Global Control Disable Home Directory	Indicates the directory path and name of the application that owns the Global Controls Disable point. This field is not editable.
Global Control Disable PointName	Indicates the Global Controls Disable point reference ID number. This field is not editable. **NOTE:** This point is owned by System Status Manager and is available for display in the System Status Manager Point Details page.
Reject Control Request on Offline Points	Select to reject control requests for data points that are currently marked offline: **Yes** or **No**. If set to No, control requests are sent to the device. Default is Yes. This setting takes effect only after closing and reopening the Point Details window.
Report Offline Points if Comm Lost	Report IED data points as OFFLINE if COMM LOST quality attribute is set. Default is Yes.
Display 61850 Object Reference	The 61850 Object Reference is displayed if attribute is set to Yes. Default is Yes.

Event Logger

Using the **Event Logger** option on the **Systemwide** tab you can change general settings for how data is handled by the Event Logger.

» To change Event Logger settings:

1. Open **DSAS MCP Studio Configuration** Tool.
2. Click the **Systemwide** tab.
3. In the left pane, click **Event Logger** and change the settings, if desired.
4. Click **Save** to save your changes.

Event Logger settings

Table 6.5: Event Logger Settings

Field	Description
PRF NVRAM Size	Enter the amount of space to allocate for the table containing the protective relay fault (PRF) records. Default value is 1000 and is not editable.
Quality NVRAM Size	Enter the amount of space to allocate for the table containing the quality records. Range is 1000 to 10000, default is 1000.
NVRAM	Select whether event records are stored in NVRAM: Default value is false and is not editable.
Number of PRF Records	Enter the maximum number of protective relay fault (PRF) records to store in the real-time database. Range is 1000 to 10000, default is 5000.
Number of Quality Force Records	Enter the maximum number of quality records to store in the real-time database. Range is 1000 to 10000, default is 5000.
Notification Delay	Enter the amount of time (in seconds) the Event Logger waits to buffer additional events before sending a notification. Range is 30 to 3600. Default is 30.
Notification Threshold	Enter the number of events that are buffered before a notification is sent. Range is 0 to 65535. Default is 100.
PRF Notification	Select the method to report PRF events. Range is **Not Used**, **Email**. Default is Not Used.

Locale

The MCP HMI can be localized to reflect regional languages, number formats, and date/time formats. Any changes on the **Locale** page require a restart of your browser to take effect.

» To set up your locale:

1. Open **DSAS MCP studio configuration** Tool.
2. Click the **Systemwide** tab.
3. In the left pane, click **Locale** and edit the fields as required.
4. Click **Save** to save your changes.
5. Click **Commit Changes** to apply the changes to the MCP.
   NOTE: Your changes do not take effect until you log out of the MCP HMI.

Table 6.6: Locale

Field	Description
HMI Language	A list of languages available based on the language packs that have been installed on your device.
Decimal Separator	Select whether to use a comma or period to denote a decimal place. Selecting **Locale Symbol** reverts to the default defined in the selected HMI Language.
Grouping Separator	Select whether to use a comma, period, or space to denote hundreds of groupings. If **None** is selected, no grouping is shown. Selecting **Locale Separator** reverts to the default defined in the selected HMI Language.
Date Format	Select the format to use when showing dates. Refer to the table below for an explanation of string values. Selecting **Locale Format** reverts to the default defined in the selected HMI Language.

<table>
<tr><td>Time Format</td><td>Select the format to use when showing times. Refer to the table below for an explanation of string values. Selecting Locale Format reverts to the default defined in the selected HMI Language.
<table>
<tr><th>String</th><th>Definition</th></tr>
<tr><td>dd</td><td>Day of the month with leading zero</td></tr>
<tr><td>MM</td><td>Month of the year with leading zero</td></tr>
<tr><td>yy</td><td>Date of the year truncated to the last 2 digits</td></tr>
<tr><td>yyyy</td><td>Date of the year</td></tr>
<tr><td>h</td><td>Hour of the day in 12-hour format without leading zero</td></tr>
<tr><td>hh</td><td>Hour of the day in 12-hour format with leading zero</td></tr>
<tr><td>H</td><td>Hour of the day in 24-hour format without leading zero</td></tr>
<tr><td>HH</td><td>Hour of the day in 24-hour format with leading zero</td></tr>
<tr><td>mm</td><td>Minute of the hour with leading zero</td></tr>
<tr><td>ss</td><td>Second of the hour with leading zero</td></tr>
<tr><td>SSS</td><td>Microseconds of the hour with leading zeros</td></tr>
<tr><td>a</td><td>AM/PM in the format a or p</td></tr>
</table></td></tr>
<tr><td>Time Zone</td><td>Select the time zone mode that should be used when the HMI displays time values. Selecting Local Timezone displays events using the timezone that is configured on your computer. Selecting UTC displays event timestamps as they have been recorded in the MCP without modification.</td></tr>
</table>

Access Manager

The **Access Manager** is a utility in the MCP that controls access, authentication, and authorization to the MCP. It allows or denies users access to specific features of the system at the point of log in, authentication or log out.

» To change system access settings:

1. Open **DSAS MCP studio configuration** Tool.
2. Click the **Systemwide** tab.
3. In the left pane, click **Access Manager**.
4. Modify the settings as required.
5. Click **Save** to save your changes.
6. Click **Commit Changes** to apply the changes to the MCP.

System access settings

Table 6.7: System Access Settings

Field	Description
Max. Simultaneous Observers	Enter the maximum number of Observer-level users who can be logged in concurrently. Range is 0 to 255. Default is 8.
Max. Simultaneous Operators	Enter the maximum number of Operator-level users who can be logged in concurrently. Range is 0 to 255. Default is 4.
Max. Simultaneous Supervisors	Enter the maximum number of Supervisor-level users who can be logged in concurrently. Range is 1 to 255. Default is 1.

Inactivity Timeout for Local HMI	Enter the amount of time (in minutes) that the MCP waits before automatically logging out an inactive user logged in locally. Range is 0 to 1440. Lower number offers more security while higher number offers more convenience. Default is 15. A value of 0 disables auto logoff. **NOTE:** It is required to logoff all Local HMI sessions and re-login again for this parameter to take effect.
Inactivity Timeout for Remote HMI	Enter the amount of time (in minutes) that the MCP waits before automatically logging out an inactive user logged in remotely. Range is 0 to 1440. Lower number offers more security while higher number offers more convenience. Default is 15. A value of 0 disables auto logoff. **NOTE:** It is required to logoff all Remote HMI sessions and re-login again for this parameter to take effect.
Inactivity Timeout for command line operations	Enter the amount of time (in minutes) that the MCP waits before automatically logging out an inactive user when using the command line utility. This setting applies to TELNET, SSH, and serial sessions. Range is 10 to 60. Lower number offers more security while higher number offers more convenience. Default is 15.
Lockout Count	Enter the number of times a password can be incorrectly entered before the user account is locked out. Range is 1 to 32. Default is 3.
Lockout Duration	Enter the amount of time (in minutes) that a user must wait before attempting to log in after being locked out. Range is 1 to 30. Default is 1.

Secret Signature	The text string that the HMI Access Manager uses to authenticate a user at login. Range is between 64 and 128 characters. The default secret signature should be replaced with a secure signature chosen by your security administrator. Also, the root password must be changed from the local serial communications port using the mcpcfg local configuration utility. The Secret Signature is a Cyber Security feature facilitating a user managed layer of protection on the Session Cookie for the HMI Interface. The MCP creates its own session cookie based on hashing a configurable sentence, called "Secret Signature". In order to ensure session cookie uniqueness users should change the Secret Signature. To change the Secret Signature: 1. Launch DS Agile MCP Studio and connect to MCP using a nominated administrator user. 2. With the Offline or Online Editor, navigate to Systemwide > Access Manager tab. 3. Change the Secret Signature from the default to user defined and select"Save" button. 4. Apply "Sync To" in the case of Offline Editor to apply these changes to MCP. In the case of Online Editor, these changes will be reflected automatically when User applies "Save" button. 5. Re-Login from the MCP Runtime HMI or MCP Command Line to check the updated Secret Signature. **NOTE:** The default secret signature should be replaced with a secure signature chosen by your security administrator. This needs to be done after successful creation of nominated administrator level user.

Auto Login

Automatic Login' related settings can be configured from HMI, Settings → Automatic Login tab, as shown below:

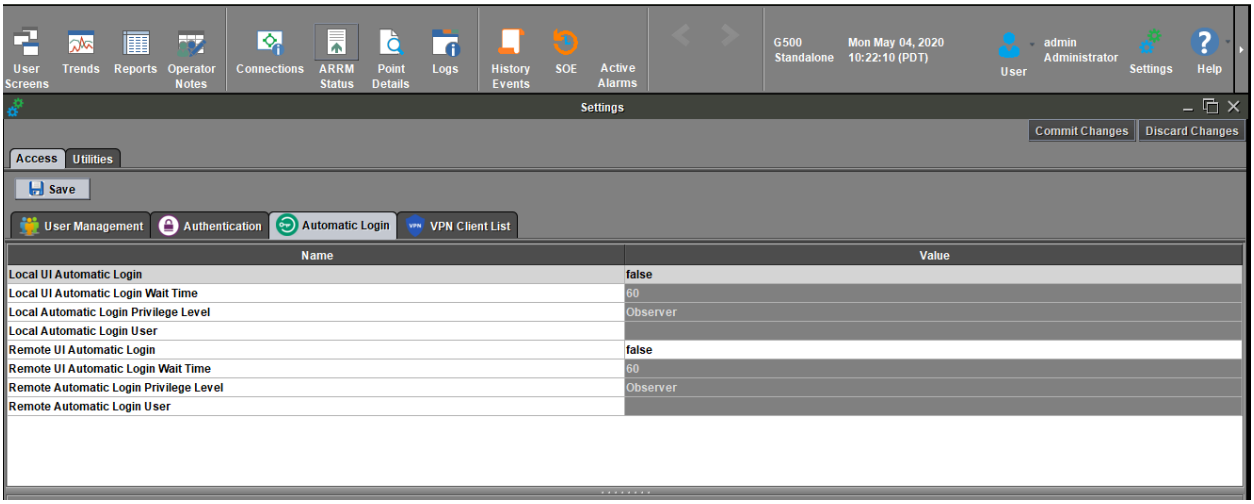


Table 6.8: Auto Login

Local UI Automatic Login	Select to skip the Local HMI log in when a user logs into the MCP through the local substation computer setup (KVM card) and go directly to the Local HMI main page (home page). Default is False. **NOTE:** This feature is disabled for Cisco, TACACS+, and LDAP Remote Authentication. **SECURITY NOTICE:** If Local UI Auto Login is set to true, the Local HMI will perform an automatic login using the selected user privilege level and name, without additional human authentication required. It is up to the system's Engineer / Operations to assess the effect and application of this behavior at runtime.
Local UI Automatic Login Wait Time	This parameter can only be configured if "Local UI Automatic Login" is set to true. The Local UI Automatic Login Wait Time parameter represents the wait time (in seconds) that is available for the user to interrupt the system from entering the Local Graphical UI's Main Page from the Command Line Interface.
Local Automatic Login Privilege Level	This parameter can only be configured if the Local UI Automatic Login parameter is set to true. The Local Automatic Login Privilege Level parameter provides the user with the option to configure the Default Privilege Level when navigating to the Local Graphical UI.
Local Automatic Login User	This parameter can only be configured if the Local UI Automatic Login parameter is set to true. The Local Automatic Login User parameter allows the user to choose the default user from the list of users configured under each Privilege Level (Supervisor/Operator/Observer).
Remote UI Automatic Login	Select to skip the Remote HMI log in when a user logs into the MCP through the Remote substation computer and go directly to the Remote HMI main page (home page). Default is False. **NOTE:** This feature is disabled for Cisco, TACACS+, and LDAP Remote Authentication. **SECURITY NOTICE:** If Remote UI Auto Login is set to true, the Remote HMI will perform an automatic login using the selected user privilege level and name, without additional human authentication required. It is up to the system's Engineer / Operations to assess the effect and application of this behavior at runtime.
Remote UI Automatic Login Wait Time	This parameter can only be configured if "Remote UI Automatic Login" is set to true. The Remote UI Automatic Login Wait Time parameter represents the wait time (in seconds) that is available for the user to interrupt the system from entering the Remote UI's Main Page from the Command Line Interface.
Remote Automatic Login Privilege Level	This parameter can only be configured if the Remote UI Automatic Login parameter is set to true. The Remote Automatic Login Privilege Level parameter provides the user with the option to configure the Default Privilege Level when navigating to the Remote Graphical UI.
Remote Automatic Login User	This parameter can only be configured if the Remote UI Automatic Login parameter is set to true. The Remote Automatic Login User parameter allows the user to choose the default user from the list of users configured under each Privilege Level (Supervisor/Operator/Observer).

GUI (Runtime GUI)

Using the **Global** option on the **Systemwide** tab, you can change general settings for how commands and data appear in the HMI.

» To change global settings:

1. Open **DSAS MCP studio configuration** Tool.
2. Click the **Systemwide** tab.
3. In the left pane, click **Runtime GUI** > **Global** and modify the settings, if desired.
4. Click **Save** to save your changes.
5. Click **Commit Changes** to apply the changes to the MCP.

Global configuration settings

Table 6.9: Global Configuration Settings

Field	Description
Device Identity	This parameter is used to identify the current device. It appears on HMI Powerbar. **NOTE**: • If not specified, the hostname appears on the HMI Powerbar by default. • It is necessary to re-login to the HMI to view the new identity on the HMI Powerbar after the device identity has been changed. If a device is running in Redundant mode, the suffix '-A' or '-B' is appended to the end of specified value on the HMI Powerbar; for example: if the specified text is 'This is my device', the text 'This is my device-A' appears on the HMI Powerbar when connecting to Gateway_A. The appended suffix '-A' or '-B' is determined by the device configured as Gateway_A or Gateway_B in the mcpcfg.
Tag/Inhibit Interface Inactivity Timeout	Enter the amount of time, in seconds, that a tag/inhibit interface window remains open before it automatically closes and cancels the operation. Range is 10 to 65535.
Local Force Interface Inactivity Timeout	Enter the amount of time, in seconds, that a local force interface window remains open before it automatically closes and cancels the operation. Range is 10 to 65535.
Execute Control Interface Inactivity Timeout	Enter the amount of time, in seconds, that an execute control interface window remains open before it automatically closes and cancels the operation. Range is 10 to 65535.
Confirmation Inactivity Timeout	Enter the amount of time, in seconds, that a confirmation window remains open before it automatically closes and cancels the operation. Range is 10 to 65535.
Normal Quality Foreground Color	Select the text color to be used when showing normal power quality records. Color choices available in **Color** palette window.
Normal Quality Background Color	Select the background color to be used when showing normal power quality records. Color choices available in **Color** palette window.
Invalid Quality Foreground Color	Select the text color to be used when showing invalid power quality records. Color choices available in **Color** palette window.
Invalid Quality Background Color	Select the background color to be used when showing invalid power quality records. Color choices available in Color palette window.
Questionable Quality Foreground Color	Select the text color to be used when showing questionable power quality records. Color choices available in **Color** palette window.

Questionable Quality Background Color	Select the background color to be used when showing questionable power quality records. Color choices available in **Color** palette window.
Engaged Quality Foreground Color	Select the text color to be used when showing engaged power quality records. Color choices available in **Color** palette window.
Engaged Quality Background Color	Select the background color to be used when showing engaged power quality records. Color choices available in **Color** palette window.
Zombie Quality Foreground Color	Select the text color to be used when showing zombie power quality records. Color choices available in **Color** palette window.
Zombie Quality Background Color	Select the background color to be used when showing zombie power quality records. Color choices available in **Color** palette window.
Conditional Formatting Text Color for Errors	Select the text color to be used when showing errors (Conditional formatting). Color choices available in **Color** palette window.
Conditional Formatting Background Color for Errors	Select the background color to be used when showing errors (Conditional formatting). Color choices available in **Color** palette window.
Conditional Formatting Text Color for Unavailable items	Select the text color to be used when showing Unavailable items (Conditional formatting). Color choices available in **Color** palette window.
Conditional Formatting Background Color for Unavailable items	Select the background color to be used when showing Unavailable items (Conditional formatting). Color choices available in **Color** palette window.
Conditional Formatting Font Style for Unavailable items	Select the Font style to be used when showing Unavailable items (Conditional formatting). Color choices available in **Color** palette window.
Record Block Size	Enter the number of rows that appear per page on the **Point Details** and **Point Groups** pages. Range is 10 to 100. Default is 20.
Viewer Initial Drawing	Enter the filename of the default drawing to display in the One-Line Viewer. Drawings are created and saved using the One-Line Designer. Default is *main.dra*.
Local UI Main Page	Select a home page from the dropdown list to display after login to the Local HMI. This parameter is applicable for Local HMI when Redundancy is not configured.
Local UI Main Page for this GatewayA	This parameter is only applicable when Redundancy (Warm Redundancy/Hot Redundancy) is configured. Select a home page from the dropdown list to display after login to the Local HMI of the MCP with the designation Gateway_A. This is not supported in G100
Local UI Main Page for this GatewayB	This parameter is only applicable when Redundancy (Warm Redundancy/Hot Redundancy) is configured. Select a home page from the dropdown list to display after login to the Local HMI of the MCP with the designation Gateway_B.This is not supported for G100
Remote UI Main Page	Select a home page from the dropdown list to display after login to the Remote HMI. This parameter is applicable to the Remote HMI, both when Redundancy is not configured or not configured.

CGI request time-to-live	Enter the amount of time, in seconds, that passes before a CGI request is cancelled. Range is 0 to 65535. Default is 5.

AI Text Enumeration Tab

The **AI Text Enumeration** feature allows you to assign text strings to integer values of analog input points. This can be used to provide user-friendly definitions to SNMP codes. Though the underlying data reported remains intact (that is, the actual reported integer value of the point is still recorded in the database), the point details page shows the associated text enumeration to users.

Enumeration Values

An **Enumeration** is a set of value/text pairs that can be used by one or more analog input mappings. Your first step in configuring AI Text Enumeration is to create one or more enumerations.

NOTE:

There are predefined.

Click the **Add** button to insert a new row in the table. Select one or more rows and click **Delete** to remove them.

Table 6.10: Enumeration Values

Value Name	Description
Name	A unique ASCII text description of the enumeration.
Invalid Value Text	If an analog input value is not defined in the enumeration, this text string is shown to users.
Value	The analog value returned by the analog input. You can enter any signed 32-bit integer.
Text	The text string associated with the selected value. Valid range is up to 64 Unicode characters.

Analog Input Mappings

Point Selection Area

You can select system points using the system point tree. Click the checkbox to the left of a point or group name to add a point or a group of points to the group. Points included in the group are shown at the right-hand side of the point selection area. To remove a point, uncheck the appropriate box in the system point tree or highlight the point and click the **Delete** button. Click the **Delete NE** to remove any points that are not valid (that is, points that have been deleted from the system database after they were included in analog input mappings list.

Enumeration

Select one of the available enumerations to be associated with the analog input.

Build Client Map Files

This chapter contains the following sections and sub-sections:

D.20 Peripheral Client

Client Map

DNP3 Client

Modbus Client

SEL Binary Client

IEC 60870-5-103 Client

IEC 60870-5-101+104 Client

Generic ASCII Client

SNMP Client Properties

IEC 61850 Client

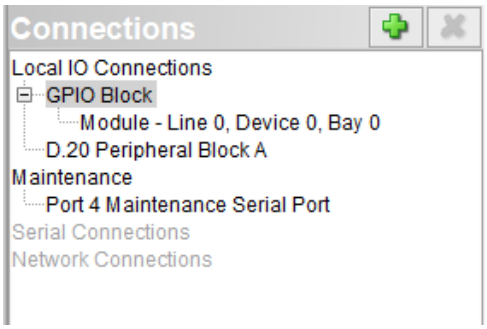
GPIO Configuration steps (G100 only)

G100 device has a built in **General Purpose IO module (*GPIO*)** providing 8xDI, 4x DC AI and 4x DO. For additional details about GPIO please refer to *G100 Instruction Manual* (GE part number 994-0155).

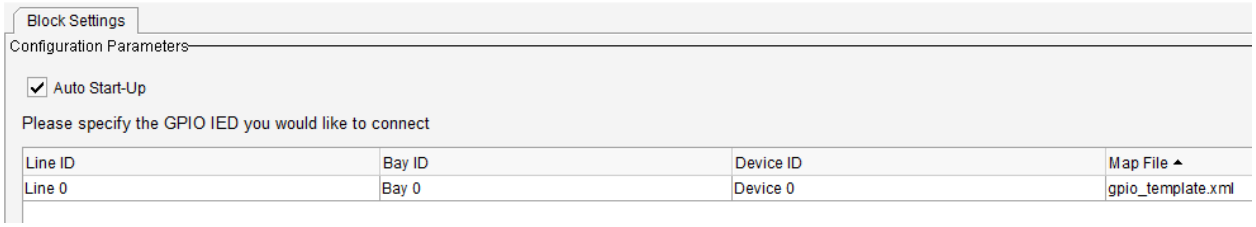
The DO operation types on the internal G100 relays are PULSE, LATCH_ON and LATCH_OFF. At runtime, commands received as CLOSE are translated to LATCH_ON, and commands received as TRIP are translated to LATCH_OFF. The PULSE command types are executed as PULSE, according to their associated repeat and duration parameters.

Use DS Agile MCP studio's Online & Offline configuration tool to configure the G100 GPIO configuration. The typical sequence of steps involved in configuring G100 GPIO from DS Agile MCP Studio are as follows:

1. Access the Online or Offline editor for the G100 device:
    - Online Editor – Accessed via the option 'Connect' under the 'Communications' ribbon menu category, or 'Communications' via right-click menu on the G100 device
        - Login to Online Editor using administrative credentials
    - Offline Editor – Accessed via the option 'Editor' under the 'Configuration' ribbon menu category, or 'Configuration' via right-click menu on the G100 device
2. Left click on 'GPIO Block' located under 'Local IO Connections' in the 'Connections' tree



3. The block settings window on the right will display the default Line ID / Bay ID / Device ID for the GPIO, along with the default 'gpio_template.xml'



4. The 'Auto Start-Up' checkbox is enabled by default, this setting automatically starts the GPIO application (Local/Remote HMI indicates the application is running under Connections/Point Details), otherwise the application must be manually started
5. The **Line/Bay/Device ID** fields can be populated with unique names, the constraints on naming convention are the same as existing applications in DSAS
6. The 'Map File' column shows the default 'gpio_template.xml', which can be edited, detailed below in step #7
7. Select 'Edit' the 'Edit – gpio_template.xml' window will be displayed; the window contains three tabs for editing (Analog Input / Digital Input / Digital Output)
    - **Analog Input**
        - **Point ID** cannot be modified and indicates the internal point ID for the respective Analog Input
        - **Point Reference/Description** shows default values, the columns can be populated with unique names, the constraints on naming convention are the same as existing applications in DSAS
        - **Multiplier** default value of '1', the injected current/voltage on the specific Analog Input value is multiplied by the configured multiplier amount, and represented accordingly in the local/remote HMI
        - **Offset** default value of '0', the offset configured for the specific Analog Input will be added to the injected current/voltage on the respective Analog Input, and represented accordingly in the local/remote HMI
        - **Range Selection** default setting '+/- 5V' can be set to '20mA', the local/remote HMI displays the value according to the range selected.
            - Note: To obtain proper values, there are internal jumpers on the MCP that need to be set to configure each Analog Input individually as a current or voltage input. Please refer to *G100 Instruction Manual* (GE part number 994-0155).
        - **Report Deadband** default value of '0.1', in % of FS. Can be set to a maximum value of '100', and is used to define the reporting threshold for the individual Analog Inputs
            - Voltage Input Deadband calculation = 5 * configured_deadband_value / 100 (in V)
            - Current Input Deadband calculation = 20 * configured_deadband_value / 100 (in mA)
        - **Point Group** default value of 'PVal' can be used to set the point group for the individual Analog Inputs, adding a new group can be completed via Systemwide → Point Groups tab
    - **Digital Input**
        - **Point ID** cannot be modified and indicates the internal point ID for the respective Digital Input
        - **Point Reference/Description** shows default values, the columns can be populated with unique names, the constraints on naming convention are the same as existing applications in DSAS
        - **Debounce Filter** (ms) default value of '0', can be set to a maximum value of '1000', the filter is used to eliminate unwanted noise on the Digital Input; indicating the signal on the Digital Input must be valid for 0-1000ms before the Digital Input value is changed/reported

- **ON State** represents the unique name which is displayed in the local/remote HMI when the respective Digital Input is in the ON state, the constraints on naming convention are the same as existing applications in DSAS
- **OFF State** represents the unique name which is displayed in the local/remote HMI when the respective Digital Input is in the OFF state, the constraints on naming convention are the same as existing applications in DSAS
- **Point Group** default value of 'PVal' can be used to set the point group for the individual Digital Inputs, adding a new group can be completed via Systemwide → Point Groups tab

- **Digital Output**
  - **Point ID** cannot be modified and indicates the internal point ID for the respective Digital Output
  - **Point Reference/Description** shows default values, the columns can be populated with unique names, the constraints on naming convention are the same as existing applications in DSAS
  - **OFF State** represents the unique name which is displayed in the local/remote HMI when the respective Digital Output is in the OFF state, the constraints on naming convention are the same as existing applications in DSAS
  - **ON State** represents the unique name which is displayed in the local/remote HMI when the respective Digital Output is in the ON state, the constraints on naming convention are the same as existing applications in DSAS
  - **Pulse Count** default value '1', can be set to a maximum of '100,000', the amount configured determines how many operations are applied on the respective Digital Output when a PULSE control type is operated
    - The 'Pulse Count' is overwritten by the value entered in the 'Digital Output Interface' window when operating controls using local/remote HMI
  - **Pulse On Duration** (ms) default value '1,000', can be set to a maximum of '100,000', the amount configured determines the duration the relay remains in the 'On' position for the respective Digital Output when a PULSE control is operated
    - The 'Pulse On Duration (ms)' is overwritten by the value entered in the 'Digital Output Interface' window when operating controls using local/remote HMI
  - **Pulse Off Duration** (ms) default value '1,000', can be set to a maximum of '100,000', the amount configured determines the duration the relay remains in the 'Off' position for the respective Digital Output when a PULSE control is operated
    - The 'Pulse Off Duration (ms)' is overwritten by the value entered in the 'Digital Output Interface' window when operating controls using local/remote HMI
  - **Point Group** default value of 'PVal' can be used to set the point group for the individual Digital Outputs, adding a new group can be completed via Systemwide → Point Groups tab

8. Once changes to the default 'gpio_template.xml' have been performed, the changes need to be synchronized to the MCP
   - Using the Online Editor, simply select 'Save', enter a new name for the template, select 'Save' again, followed by 'Commit Changes'
   - Using the Offline Editor, select 'Save', enter a new name for the template, select 'Save' again, followed by 'Commit Changes', then 'Save Session', finally selecting 'Sync to Device'

   NOTE: The default 'gpio_template.xml' can be modified but not deleted, in the case an edited template has been saved; the dropdown menu allows using the default template again along with any modified templates

D.20 Peripheral Client

D.20 Peripheral Mapfiles

About the D.20 Peripheral Mapfiles

The D.20 Peripheral map defines how the MCP is configured to poll the data from D.20 peripherals. The MCP supports communications to D.20 peripherals over a standard D.20 link using the D.20 Peripheral Link Client application.

On the **Client Map** tab on the **Configuration** page you configure point maps for the D20 peripheral modules you are connecting to.

The D.20 Peripheral Link Client polls for and retrieves information from peripheral modules according to a client map file. The map file contains information on how polling is scheduled for a device based on the device's capabilities, frequency of polling, selected data points, etc.

To facilitate the collection of data, the MCP comes pre-loaded with map files for all D.20 peripheral modules. Once you create a client map file, it becomes available to select on the Configuration page when assigning device connections.

NOTE: Additional D.20 client configuration settings are available for device communications when configuring D.20 connections on the **D.20** Connection tab.

D.20 Client Peripheral Properties

The Client map settings are available on the **Client Map** tab when a D.20 protocol device type is selected. The below table lists the poll-specific settings for the D.20 peripherals.

The MCP supports the following configurable D.20 data types:

D.20 data types	Supported by card	Description
Analog inputs	D20 – A, C1, C2	Measured or computed values by the device
Analog outputs	D20 – C2	Physical or computed analog quantities
Digital inputs	D20 – C0, C1, C2, S	States of physical or logical Boolean devices
Digital outputs	D20 – K, C0, C1, C2	Physical or logical ON-OFF, raise-lower, and trip-close points

Types of D.20 Peripherals

Below table lists the D.20 Peripherals and its supported Point Types and count of points in each Type.

Peripheral Board Type	Available Point Type(s) on Board	
D20 A (analog Input board)	32 analog input points	
D20 S (digital input or status board)	64 digital (status) inputs up to 64 Form A counters up to 32 Form C counters up to 32 Double points	
D20 K (digital output or control board)	32 digital (control) outputs (always configured in groups of 8, e.g.:8 raise/lower and 24 trip/close, 16 raise/lower and 16 trip/close, etc.)	
D20 C (combination boards) D20 C0	**C0**	16 digital (status) inputs 8 digital (control) outputs (always configured in groups of 2)

D20 C1 D20 C2	**C1**	16 digital (status) inputs 8 digital (control) outputs (always configured in groups of 2) 16 analog inputs
	C2	16 digital (status) inputs 8 digital (control) outputs (always configured in groups of 2) 8 analog inputs 8 analog outputs

Configuring Peripheral Map files

This section describes how to configure D.20 peripheral map files for D.20 application.

For each peripheral configured following option are available in DSAS.

Configure a D20 A Peripheral (Analog Input Points)

A D20 A peripheral board, also known as the analog board, has 32 analog input points, and can be terminated by a D20 A or a D20 AD termination board.

For D20 A card there are certain sets of fields supported and are given below:

Table 6.11: D20 A card - Peripheral level

Parameter	Description	Range	Default
Termination Board	D20 A Analog Input Peripheral (32 AI)	WESTERM D20 A WESTERM D20 AD WESTERM D20 0AD WESTERM D20 AZ WESTERM D20 AB WESTERM D20 AX WESTERM D10 A	WESTERM D20 A
Description	D20 A Analog Input Peripheral (32 AI), It supports up to 32 ASCII user defined characters	N/A	N/A
Reference Check	Specifies how often the software updates the on-board analog input references, in terms of analog input references.	20 to 255	100
Reference Dead band	Specifies how often the software updates the on-board analog input references, in terms of analog input references.	0 to 32767	256
Input Setting time (microseconds)	Difference between running reference and EEPROM references before peripheral shutdown.	0 to 32767	500
Line Frequency (Hz)	Frequency of the system being monitored by the device.	50 and 60	60

For each point, fill in the fields as outlined in the table below:

Table 6.12: D20 A card – Point level

Parameter	Description	Default	Action required
Point Reference	Some general information about the point. This information will be displayed in MCP Point Details.	N/A	Type a brief description of the point. Maximum length 64 ASCII Characters
Point Description	Some general information about the point. This information will be displayed in MCP Point Details.	N/A	Type a brief description of the point. Maximum length 64 ASCII Characters

Point Group	Refence for defined point group	Pval	Pval/Demand/Peak Demand
Scan Enable	Enables or disables a point from being scanned and having its value returned to the RTU.	YES	Select either YES or NO.
Range Select	The maximum positive and negative full-scale voltage to be applied to the input point. NOTE: The appropriate input adapter module must be present on the termination board.	0±5 volts	Select either 0±1 volt, 0±5 volts, or 0±10 volts.
Report Deadband	The least significant bits of the analog value that must change before the application reports the value to the system point database. Use this option to control the number of data change events generated.	4	Type in a suitable value for your system.
Client High Scale	The maximum value that is to be returned to the system point database, as a percentage of 32767.	100 %	Use 100% unless you have non-standard analog input scaling modules.
Client Low Scale	The minimum value that is to be returned to the system point database, as a percentage of 32767.	-100 %	Use -100% unless you have non-standard analog input scaling modules.
Peripheral High Scale	The maximum value that is expected from the analog input peripheral, as a percentage of 32767.	100 %	Use 100% unless you have non-standard analog input scaling modules.
Peripheral Low Scale	The minimum value that is expected from the analog input peripheral, as a percentage of 32767.	-100 %	Use -100% unless you have non-standard analog input scaling modules.

Configure a D20 S Peripheral (Digital Input Points)

A D20 S peripheral board, also known as the status (or digital input) peripheral, has 64 digital input points, up to 64 Form A counters, or up to 32 Form C counters and 32 Double points.

Digital inputs monitor and report changes of state, either ON or OFF.
If they are accumulator input points (known as single-point or double point accumulators), they ***count*** those changes.

For D20 S card there are certain sets of fields supported and are given below:

Table 6.13: D20 S card - Peripheral Level

Parameter	Description	Range	Default
Termination Board	D20 S Digital Input Peripheral (64 DI)	WESTERM D20 S WESTERM D20 SD WESTERM D20 0SD WESTERM D20 SZ WESTERM D20 SZ2 WESTERM D20 SB WESTERM D20 SI WESTERM D20 SX WESTERM D20 SDI WESTERM D10 SI	WESTERM D20 S
Description	D20 S Digital Input Peripheral (64 DI), Supports max 32 ASCII Characters	N/A	N/A

Filter Period (ms)	Length of time used as the sample time window for chatter filtering.	100 to 65535	0

For each point, fill in the fields as outlined in the table below:

Table 6.14: D20 S card - Point Level

Parameter	Description	Default	Action required
Point Reference	Some general information about the point	N/A	Type a brief point reference of the point. Maximum length 64 ASCII Characters
Point Description	Some general information about the point. This information will be displayed in MCP Point Details	Spare	Type a brief description of the point. Maximum length 64 ASCII Characters
Point Group	Refence for defined point group	Pval	Pval/Demand/Peak Demand
Point Type	The type of point.	Status Input	Select from *Single-point State*, *Double-point state*, *Form A Counter*, or *Form C Counter*.
Report Limit	Specify the size of change in the new counter value from the previous value before the application reports the new value to the system point database. This is only valid if the user has selected "Transition Counter" or "Form C Counter" as the point type.	0 times	Type in the maximum number of counts that can occur before being reported to the MCP. 0 to 255
Tolerant Phase	A period of time during which contact bounce is "acceptable." Having a tolerant period allows you to monitor and time-stamp the initial state of change, while ignoring any subsequent contact bounce.	0 ms	Type in a value between 0 and 255 milliseconds.
Intolerant Phase	A period of time following the tolerant phase during which contact bounce is not "acceptable." It ensures that contact bounce is not mistaken for a valid change of state.	6 ms	Type in a value between 0 and 255 milliseconds.
Valid Period	**For a single-point state/Form A counter:** Defines the period of time (in 256 ms increments) during which the point state must be ON. **For a double-point state/Form C counter:** Defines the period of time (in multiples of 10 ms) during which both points must be in a "valid" state (i.e. either 1-0 or 0-1).	0	Type in a value between 0 and 255 increments.
Invalid Period	**For a single-point state/Form A counter:** Defines the period of time (in 256 ms increments) during which the point state must be OFF. **For a double-point state/Form C counter:** Defines the period of time (in multiples of 256 ms) during which both points must be in an "invalid" state (i.e. either 0-0 or 1-1).	0	Type in a value between 0 and 255 increments.

Chatter Transitions	The maximum allowable number of state transitions that can occur within a filter base period. If the number of state transitions during a filter period equals or exceeds the maximum allowable number of state transitions, the chatter filter will turn ON, and any further transitions will be ignored for the duration of the "lock-out" period.	0 transitions	Type in a value between 0 and 255 transitions. If the transition value is 0 (zero), the chatter filter is disabled for the associated digital input.
Lock-out Period	If one, the minimum number of filter base periods during which the chatter filter will remain ON. The chatter filter can proceed from ON to OFF only if no state transitions are detected for an entire lock-out period. If zero, the chatter filter can proceed from ON to OFF only if there are less transitions than the maximum expected number of transitions.	0 filter base periods	Type in a value between 0 and 65535 filter base periods.

Configure a D20 K Peripheral (Digital Output Points)

A D20 K peripheral board, also known as the digital output (or control) peripheral, has 32 digital (control) output points, or 16 raise/lower pairs, or a combination of these. It can be terminated by a D20 K or D20 KR termination board. In addition, interposer relay (or KI) expansion boards can be used to provide additional functionality.

For D20 K card there are certain sets of fields supported and are given below:

Table 6.15: D20 K card - Peripheral Level

Parameter	Description	Range	Default
Termination Board	WESTERM D20 K	WESTERM D20 K WESTERM D20 KR WESTERM D20 0KR WESTERM D20 K4Z WESTERM D20 KX WESTERM D10 K WESTERM D10 KR	WESTERM D20 K
Description	User defined string to identify peripheral, Supports up to 32 ASCII User Defined characters	N/A	N/A
Select Time (ms)	Length of time the select relay operates before the master relay.	1 to 255	10
Clear time (ms)	Length of time select relay continues operating after master relay.	1 to 255	10
Control arm Time-outs (ms)	Length of time between the arm and executes request for a digital output point before the control is disarmed.	100 to 255	100
Retry time (s)	Length of time peripherals wait to start after shutting down.	1 to 255	10
Retry attempts	No of time peripherals tries to restart after it fails.	0 to 255	0
Comm fail time out (ms)	Length of time peripheral wait for communication on HDLC link before shutting down all relays.	0 to 65535	0

For each point to be modified, fill in the fields as outlined in the table below:

Table 6.16: D20 K card - Point Level

Parameter	Description	Default	Action required
Point Reference	Some general information about the point This information will be displayed in Point details for individual point.		Type a brief point reference of the point. Maximum length 64 ASCII Characters
Point Description	Some general information about the point. This information will be displayed in Point details for individual point.	Spare	Some general information about the point. Maximum length 64 ASCII Characters
Point Group	Refence for defined point group	Pval	Pval/Demand/Peak Demand
Termination Type	Defines the configuration of the termination board, i.e. the way each group of 8 outputs are configured according to jumper settings.	Trip/Close	WESTERM K-board: select either: Trip/Close, Raise/Lower, Form C outputs, or Open Collector. WESTERM KR-board: select Trip/Close or Raise/Lower.
Reset on Startup	Determines if a latched relay is automatically reset when the MCP starts up.	No	Set "Yes" to reset the relay to a known (clear) state at startup of MCP.

Configure a D20 C Peripheral (Combination of Points)

There are three types of D20 C peripheral boards.

Each one has a different combination of point types shown below. C1 and C2 peripherals have a module also support analog functionality.

Details of each C type peripherals and the input/output support is given below.

Peripheral Board Type	Available Point Type(s) on Board	
D20 C (combination boards) D20 C0 D20 C1 D20 C2	**C0**	16 digital (status) inputs 8 digital (control) outputs (always configured in groups of 2)
	C1	16 digital (status) inputs 8 digital (control) outputs (always configured in groups of 2) 16 analog inputs
	C2	16 digital (status) inputs 8 digital (control) outputs (always configured in groups of 2) 8 analog inputs 8 analog outputs

For D20 C0 card there are certain sets of fields supported and are given below:

Table 6.17: D20 C card - Peripheral Level

Parameter	Description	Range	Default

Termination Board	Standard combo termination board	WESTERM D20 C WESTERM D20 CD WESTERM D20 C4Z WESTERM D20 C4Z2 WESTERM D20 CB WESTERM D20 CDI WESTERM D20 C (DB25) WESTERM D20 CX WESTERM D10 C	WESTERM D20 C
Description	User defined string to identify peripheral. Supports up to 32 ASCII User Defined characters	N/A	N/A
Filter Period (ms)	Length of time used as the sample time window for chatter filtering.	100 to 65535	0
Select Time (ms)	Length of time the select relay operates before the master relay.	1 to 255	10
Clear time (ms)	Length of time select relay continues operating after master relay.	1 to 255	10
Control arm Time-outs (ms)	Length of time between the arm and executes request for a digital output point before the control is disarmed.	100 to 255	100
Retry time (s)	Length of time peripherals wait to start after shutting down.	1 to 255	10
Retry attempts	No of time peripherals tries to restart after it fails.	0 to 255	0
Comm fail time out (ms)	Length of time peripheral wait for communication on HDLC link before shutting down all relays.	0 to 65535	0

For each point to be modified, fill in the fields as outlined in the table below.

Configure D20 C Digital Input Points

To configure digital input points on D20 C0, C1, or C2 peripheral boards:

1. Click points (near the top of the window).
   For each point to be modified, fill in the fields as shown in the table in **Configure a D20 S Peripheral (Digital Input Points)** earlier in this chapter.
2. If you enter a value that is out of range, *DSAS* will show a warning and automatically insert the lowest or highest value that it can accept, as appropriate.

Configure D20 C Digital Output Points

To configure digital output (control) points for D20 C0, D20 C1, or D20 C2 peripheral boards:

1. For each point to be modified, fill in the fields as outlined in the table in **Configure a D20 K Peripheral (Digital Output Points)** earlier in this chapter.
2. If you enter a value that is out of range, *DSAS* will show a waring and automatically insert the lowest or highest value that it can accept, as appropriate.

Configure D20 C Analog Input Points

To configure analog input points for D20 C1 or D20 C2 peripheral boards:

1. For each point to be modified, fill in the fields as outlined in the table in **Configure a D20 A Peripheral (Analog Input Points)** earlier in this chapter.

2. If you enter a value that is out of range, *DSAS* will show a waring and automatically insert the lowest or highest value that it can accept, as appropriate.

Configure D20 C Analog Output Points

Parameter	Description	Default	Action required
Point Reference	Some general information about the point. This information will be displayed with each point in MCP Point Details.	Spare	Type a brief description of the Point Reference. Maximum length Supports up to 32 ASCII characters.
Point Description	Some general information about the point. This information will be displayed with each point in MCP Point Details.	Spare	Type a brief description of the point. Maximum length Supports up to 32 ASCII characters.
Initial Value	The initial voltage/current setting (in counts) for the device wired to the analog output. The range of this point is -4095 to 4095	Zero (0).	If you are in unipolar current mode and the range of the device reading the outputs is 4-20 mA, it is very important to set the initial value to 819. In all other modes (or in unipolar current mode when device range is 0-20 mA), the default value of zero (0) is fine.
Output Mode	The polarity of the output.	Unipolar 5V	Choose mode range setting for each analog output point from the available choices: Bipolar 5V, Bipolar 10V, Unipolar 5V, Unipolar 10V, Unipolar current.

Client Map

The client map file is based on a specific protocol. Each Client Map specifies what information or data to be gathered from a device. The MCP polls for and retrieves information from a device according to a client map file. The map file contains information on how polling is scheduled for a device based on the device's capabilities, frequency of polling, selected data points, etc.

The MCP has the following default client maps:

- DNP3
- SEL Binary
- Modbus

You can use these default client maps or customize them for your system requirements. Once you create a client map file, it becomes available to select on the Configuration page when assigning device connections.

NOTE: If you are running a LogicLinx program on your MCP and you change the point mapping, you must synchronize the configuration within MCP Utilities to ensure that your LogicLinx mappings are still valid.

The MCP communicates with devices connected to your power network. These devices monitor and record several types of information. The information can be generally classified in the following point groups, defined by default in the MCP:

- Present values (PVal) that reflect the current state of the power system at an instance in time.
- Peak demand that reflects the minimum and maximum power flow conditions encountered.

- Demand

Point groups can be modified on the **Systemwide** tab in the MCP Online Configuration Tool.

The devices store all the information in a "map". Refer to the device manufacturer's manual for a list and description of all the data points available from a device.

Creating Client Maps

» To create or edit a client map:

1. On the **Configuration** page, select the **Client Map** tab.
2. Click **New** to create a new client map or **Open** to edit an existing client map.
3. Select the device protocol type and then create or select the device map file.
4. Edit the data type and device protocol settings as desired.
5. Click **Save** and enter a name for your map file.

Tips

- To add points to the point map, in the **Number of rows to insert** box, type the number of rows you want to add and click **Insert**.
- To delete a point from the point map, select the row and click **Delete**.
- Keep the default map files as basic templates. To create custom templates, modify the default map files, click **Save** and then enter a new template name.

Device properties

Device properties are available on the **Device Properties** pane of Client **Map** tab on the **Configuration** page. These settings shown vary based on the protocol selected.

The **Device Properties** pane allows you to view and modify the protocol settings for a specific client application. These protocol specific settings of a device will also store in the client map file.

» To configure device properties:

1. On the **Client Map** tab, open a map file.
2. In the **Device Properties** pane, to modify a parameter, double-click the associated value and enter a new value or select from the drop-down list.
3. Click **Save** to save your changes.

Protocols

You can create map files for devices using the following protocols.

- D.20 Peripheral Client
- DNP3 Client
- Modbus Client
- SEL Binary Client
- IEC 60870-5-103 Client
- IEC 60870-5-101+104 Client
- Generic ASCII Client
- IEC 61850 Client
- Genascii Client
- SNMP

DNP3 Client

About the DNP3 Client

The DNP3 Client map defines how the MCP is configured to poll data from DNP3 devices. The MCP supports the following configurable DNP3 data types:

- Analog inputs - measured or computed values by the device
- Analog outputs - physical or computed analog quantities
- Digital inputs - states of physical or logical Boolean devices
- Digital outputs - physical or logical ON-OFF, raise-lower, and trip-close points
- Accumulators - counter values
- Device properties – device-level settings

The DNP3 Client map settings are available on the **Client Map** tab when a DNP3 protocol device type is selected.

NOTE: Additional DNP3 client configuration settings are available for device communications when configuring DNP3 serial connections on the **Serial** tab.

DNP3 Client Device Properties

Settings are available in the **Device Properties** pane on the **Client Map** tab. The following table lists the poll-specific settings for the DNP3 device.

DNP3 Device Properties

Table 6.18: DNP3 Device Properties

Setting	Description	Range	Default
Request Data Link Confirm	Enables request Data Link Confirmations from the device.	True False	False
Request Data Link Confirm for Direct Operate Controls	Enables request Data Link confirms for direct operate control (no SBO controls)	True False	False
Data Link Retry	How many times to retry a failed data link layer message before giving up. Increase the value for unreliable connections, noisy environment, modem communication, etc.	0 to 300	1
Data Link Timeout	Time (in milliseconds) to wait for a data link layer response before deciding it has failed. Set the value much higher for a modem connection, i.e. 600000.	1 to 3600000	1000 (i.e. 1 second)
Enable Unsolicited	True: Send Enable Unsolicited at startup, and in response to a NULL UR. False: Never send Enable Unsolicited.	True False	False
Disable Unsolicited	True: Send Disable Unsolicited at startup, and in response to ANY UR. False: Never send Disable Unsolicited.	True False	False
Feedback Poll AO	When the LOCAL IIN bit is asserted in the device, poll for Analog Outputs.	True False	False
Feedback Poll DO	When the LOCAL IIN bit is asserted in the device, poll for Digital Outputs.	True False	True
Feedback Poll Events	When the LOCAL IIN bit is asserted in the device, poll for Class 1, 2, 3 data.	True False	False

Setting	Description	Range	Default
Override Control Type	When an Override is configured, ignore the Control Type propagated by the system point database. That is, always send the control type configured for this setting.	None Direct Operate Direct Operate No ACK SBO	None
Remote Accumulators	True: Send Accumulator commands to the device. False: Perform accumulator operations in the system point database.	True False	True
Connection Check Enable	True: Periodically send Link Status messages to the device to check connection.	True False	True
Connection Check Timeout	If Connection Check is enabled, send a Link Status message to the device after this time out interval (in seconds) has elapsed since a message was last received from the device	30 to 36000	30
Enable Extended Feedback Polling	True: Send the Extended Digital/Analog Feedback poll to the device when a Digital/Analog control is sent to the device.	True False	True
Feedback Poll Delay	Interval to wait (in seconds) after the control is requested, before issuing the Feedback Poll.	1 to 3600	1
Counter Feedback Poll Delay	Interval to wait (in seconds) after the counter command is requested before issuing the counter poll.	1 to 3600	1
IED Persists Counters	True: Device retains counters across restarts. False: Device clears counters on startup. This setting affects accumulator processing.	True False	True
Freeze Command	Freeze command used by the application: Freeze (and Clear) Running Counters or Freeze (and Clear) Frozen Counters.	Running Counters Frozen Counters	Running Counters
Integrity Poll	The MCP requests integrity poll data at this interval (in seconds). If set to 0, the request is never transmitted.	0 to 360000	300
Class1 Poll	The MCP requests class 1 data at this interval (in seconds). If set to 0, the request is never transmitted.	0 to 36000	1
Class2 Poll	The MCP requests class 2 data at this interval (in seconds). If set to 0, the request is never transmitted.	0 to 36000	1
Class3 Poll	The MCP requests class 3 data at this interval (in seconds). If set to 0, the request is never transmitted.	0 to 36000	1
DI Poll	The MCP requests digital input data at this interval (in seconds). If set to 0, the request is never transmitted.	0 to 36000	0
DI Change Poll	The MCP requests digital input event data at this interval (in seconds). If set to 0, the request is never transmitted.	0 to 36000	0
DO Poll	The MCP requests digital output data at this interval (in seconds). If set to 0, the request is never transmitted.	0 to 36000	0

Setting	Description	Range	Default
AI Poll	The MCP requests analog input data at this interval (in seconds). If set to 0, the request is never transmitted.	0 to 36000	0
AI Change Poll	The MCP requests analog input event data at this interval (in seconds). If set to 0, the request is never transmitted.	0 to 36000	0
Frozen AI Poll	The MCP requests single-precision frozen analog input with flag at this interval (in seconds). If set to 0, the request is never transmitted.	0 to 36000	0
Frozen AI Change Poll	The MCP requests frozen analog input data at this interval (in seconds). If set to 0, the request is never transmitted.	0 to 36000	0
Bit 16 AI Poll	The MCP requests 16-bit analog input with flag data at this interval (in seconds). If set to 0, the request is never transmitted.	0 to 36000	0
Bit 32 AI Poll	The MCP requests 32-bit analog input with flag data at this interval (in seconds). If set to 0, the request is never transmitted.	0 to 36000	0
Float AI Poll	The MCP requests single-precision analog input with flag at this interval (in seconds). If set to 0, the request is never transmitted.	0 to 36000	0
AO Poll	The MCP requests analog output status data at this interval (in seconds). If set to 0, the request is never transmitted.	0 to 36000	0
16-Bit AO Poll (sec)	The MCP requests 16-bit analog output status data at this interval (in seconds). If set to 0, the request is never transmitted.	0 to 36000	0
32-Bit AO Poll (sec)	The MCP requests 32-bit analog output status data at this interval (in seconds). If set to 0, the request is never transmitted.	0 to 36000	0
Acc Poll	The MCP requests static counter data at this interval (in seconds). If set to 0, the request is never transmitted.	0 to 36000	0
Acc Change Poll	The MCP requests counter event data at this interval (in seconds). If set to 0, the request is never transmitted.	0 to 36000	0
Frozen Acc Poll	The MCP requests frozen counter data at this interval (in seconds). If set to 0, the request is never transmitted.	0 to 36000	0
Frozen Acc Change Poll	The MCP requests frozen counter event data at this interval (in seconds). If set to 0, the request is never transmitted.	0 to 36000	0
Freeze Acc Poll	Freeze the MCP Accumulator poll	0 to 36000	0
Alternate channel health check interval	The frequency (in seconds) at which the DCA schedules a health check message to the IED. A value of zero disables the health check message.	0 to 3600	60

DNP3 Client Analog Inputs

Settings are available on the **Analog Input** tab on the **Client Map** tab. The MCP provides the mapping settings for analog inputs as shown below.

Analog Input Mapping Settings

Table 6.19: Analog Input Mapping Settings

Setting	Description	Range	Default
Address	Number of the point in the device Analog Input Map.	0 to 65535	Incremented from 0
Point Reference	A short identifier for the point in the map file.	Up to 66 ASCII characters	AI X
Point Description	A detailed and localized description for the point in the map file.	Up to 128 Unicode characters	Analog Input X
Multiplier	Scale factor of the point (**m** of formula **mx +b**).	Full range of 64-bit Float	1.0
Offset	Scale factor of the point (**b** of formula **mx +b**).	Full range of 64-bit Float	0.0
Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0

DNP3 Client Analog Outputs

Settings are available on the **Analog Output** tab on the **Client Map** tab. The MCP provides the mapping settings for analog outputs as shown below.

Analog Output Mapping Settings

Table 6.20: Analog Output Mapping Settings

Setting	Description	Range	Default
Address	Number of the point in the Analog Output Map.	0 to 65535	Incremented from 0
Point Reference	A short identifier for the point in the map file.	Up to 66 ASCII characters	AO X
Point Description	A detailed and localized description for the point in the map file.	Up to 128 Unicode characters	Analog Output X
Multiplier	Scale Factor of a point (**m** of formula **mx +b**).	Full range of 64-bit Float	1.0
Offset	Scale Factor of a point (**b** of formula **mx +b**).	Full range of 64-bit Float	0.0
AO Variation	How the point values should be reported.	16-bit, 32-bit	16-bit
Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0

DNP3 Client Digital Inputs

Settings are available on the **Digital Input** tab on the **Client Map** tab. The MCP provides the mapping settings for digital inputs as shown below.

Digital Input Mapping Settings

Table 6.21: Digital Input Mapping Settings

Setting	Description	Range	Default
Address	The DNP3 Point Index of this point as reported from the device.	0 to 65535	Incremented from 0
Point Reference	A short identifier for the point in the map file.	Up to 66 ASCII characters	DI X
Point Description	A detailed and localized description for the point in the map file.	Up to 128 Unicode characters	Digital Input X
ON State Name	Text description of the 1 state.	Up to 32 characters	ON
OFF State Name	Text description of the 0 state.	Up to 32 characters	OFF
Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0

DNP3 Client Digital Outputs

Settings are available on the **Digital Output** tab on the **Client Map** tab. The MCP provides the mapping settings for digital outputs as shown below.

Digital Output Mapping Settings

Table 6.22: Digital Output Mapping Settings

Setting	Description	Range	Default
Address	Number of the point in the Digital Output Map.	0 to 65535	Incremented
Point Reference	A short identifier for the point in the map file.	Up to 66 ASCII characters	DO X
Point Description	A detailed and localized description for the point in the map file.	Up to 128 Unicode characters	Digital Output X
ON State Name	Text description of the 1 state.	Up to 32 characters	OFF
OFF State Name	Text description of the 0 state.	Up to 32 characters	ON
Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0

DNP3 Client Accumulators

Settings are available on the **Accumulators** tab on the **Client Map** tab. The MCP provides the mapping settings for accumulators as shown below.

Accumulator Mapping Settings

Table 6.23: Accumulator Mapping Settings

Setting	Description	Range	Default
Address	Number of the point in the Accumulator Map.	0 to 65535	Incremented from 0
Point Reference	A short identifier for the point in the map file.	Up to 66 ASCII characters	ACC X
Point Description	A detailed and localized description for the point in the map file.	Up to 128 Unicode characters	Accumulator X

Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0

Modbus Client

The Modbus Client map defines how the MCP is configured to poll data from Modbus devices. The MCP supports the following configurable Modbus data types:

- Read Coil Status – status of coils
- Read Input Status – digital input data
- Read Holding Register – holding registers of the device
- Read Input Register – input registers of the device
- Write Single Coil – set a single output to either ON or OFF in the device
- Write Single Register 6A – set a single holding register in the device (value required)
- Write Single Register 6B – set a single holding register in the device (value optional)
- Device properties

Modbus Client map settings are available on the **Client Map** tab when a Modbus protocol device type is selected.

Common Table

Supported Poll Types for Modbus Client

Table 6.24: Supported Poll Types for Modbus Client

Poll Type	Description
Fast	The application schedules requests to retrieve the values of Registers/Coils as quickly as possible, subject to the configured Inter-Poll Delay.
Slow	The application schedules requests to retrieve the values of Registers/Coils at a slower rate; requests occur once a Fast Poll Cycle Count cycle has been completed.
Once	The application schedules requests to retrieve the values of Registers/Coils once upon startup and subsequently whenever the device returns to an online state after communications failure.

Supported Data Types for Modbus Client Points

Table 6.25: Supported Data Types for Modbus Client Points

Data Type	Description
INT8	8-bit signed integer. Range: -128 to 127.
UINT8	8-bit unsigned integer. Range: 0 to 255.
INT16	16-bit signed integer. Range: -32768 to +32767.
INT16_FC16	16-bit signed integer. Range: -32768 to +32767. (Supports both Big Endian and Little-Endian Formats with function code 16)
UINT16	16-bit unsigned integer. Range: 0 to 65535.
UINT16_FC16	16-bit unsigned integer. Range: 0 to 65535. (Supports both Big Endian and Little-Endian Formats with function code 16)
INT32	32-bit signed integer. Range: -2147483648 to +2147483647.
UINT32	32-bit unsigned integer. Range: 0 to 4294967295.
FLOAT32	IEEE® single-precision floating point value, MSB-LSB or little endian.
FLOAT32_MODICON	Single-precision floating point value, LSB-MSB or big endian.
DATE	Date in the format of DD-MMM-YYYY.

Data Type	Description
TIME	24 hour time in the format of HH:MM:SS.
ASCII	A string of ASCII data. Range as specified in ASCII Size.
BITSTRING 16	A bitstring of 16- bit binary input data. See the bitstring Mapping Settings table.
BITSTRING 32	A bitstring of 32- bit binary input data. See the bitstring Mapping Settings table.

Bitstring Mapping Settings

The Bitstring mapping settings are available for the Data Type BITSTRING 16 and BITSTRING 32 in the Read Holding Registers and Read Input Registers tabs.

Table 6.26: Bitstring Mapping Settings

Setting	Description	Range	Default
Bit Position	Position of the Bit in the Bitstring.	1 to 32	Incremented from 1
Point reference	The short user-defined identifier for the point corresponding to the bit position.	0 to 66 alphanumeric characters plus space, underscore, and dash	DI X
Point description	The user-defined block of text that provides a detailed and localized description of the point corresponding to the bit position.	1 to 128 Unicode characters	Digital input X
ON State	A text string that is associated with the 1 state. This string is recorded in the MCP database and is displayed with the point corresponding to the bit position.	0 to 64 characters	ON
OFF State	A text string that is associated with the 0 state. This string is recorded in the MCP database and is displayed with the point corresponding to the bit position.	0 to 64 characters	OFF

Read Coil Status

Settings are available on the **Read Coil Status** tab on the **Client Map** tab.

Table 6.27: Read Coil Status Settings

Setting	Description	Range	Default
Address	A unique identifying number in the register map	0 to 65535	x
Point Name	A short identifier for the point in the map file.	Up to 66 ASCII characters	Coil X
Point Description	A detailed and localized description for the point in the map file.	Up to 128 Unicode characters	Coil X
OFF State Name	Text description of the 0 state.	Up to 32 Unicode characters	OFF
ON State Name	Text description of the 1 state.	Up to 32 Unicode characters	ON
Poll Type	The type of poll to be taken of the point	See Support Poll Types table	Fast

Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0

Read Status Input

Settings are available on the **Read Status Input** tab on the **Client Map** tab.

Table 6.28: Read Status Input Settings

Setting	Description	Range	Default
Address	A unique identifying number in the register map.	0 to 65535	x
Point Name	A short identifier for the point in the map file.	Up to 66 ASCII characters	Input X
Point Description	A detailed and localized description for the point in the map file.	Up to 128 Unicode characters	Input X
OFF State Name	Text description of the 0 state.	Up to 32 Unicode characters	OFF
ON State Name	Text description of the 1 state.	Up to 32 Unicode characters	ON
Poll Type	The type of poll to be taken of the point.	See Support Poll Types table	Fast
Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0

Read Holding Register

Settings are available on the **Read Holding Register** tab on the **Client Map** tab.

Table 6.29: Read Holding Register Settings

Setting	Description	Range	Default
Address	A unique identifying number in the register map.	0 to 65535	x
Point Name	A short identifier for the point in the map file.	Up to 66 ASCII characters	Holding Register X
Point Description	A detailed and localized description for the point in the map file.	Up to 128 Unicode characters	Holding Register X
Multiplier	Scale factor of the point (**m** of formula **mx +b**).	Full range of 64-bit Float	1.0
Offset	Scale factor of the point (**b** of formula **mx +b**).	Full range of 64-bit Float	0.0
Poll Type	The type of poll to be taken of the point.	See Support Poll Types table	Fast
Data Type	The type of data polled.	See Support Data Types table	UINT16
ASCII Size	ASCII size, in bits, when a text string is being retrieved from the device. If this field is set to 0, the register does not contain ASCII data.	0 to 99	0
Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0

Read Input Register

Settings are available on the **Read Input Register** tab on the **Client Map** tab.

Table 6.30: Read Input Register Settings

Setting	Description	Range	Default
Address	A unique identifying number in the register map.	0 to 65535	x
Point Name	A short identifier for the point in the map file.	Up to 66 ASCII characters	Input Register X
Point Description	A detailed and localized description for the point in the map file.	Up to 128 Unicode characters	Input Register X
Multiplier	Scale factor of the point (**m** of formula **mx +b**).	Full range of 64-bit Float	1.0
Offset	Scale factor of the point (**b** of formula **mx +b**).	Full range of 64-bit Float	0.0
Poll Type	The type of poll to be taken of the point.	See Support Poll Types table	Fast
Data Type	The type of data polled.	See Support Data Types table	UINT16
ASCII Size	ASCII size, in bits, when a text string is being retrieved from the device. If this field is set to 0, the register does not contain ASCII data.	0 to 99	0
Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0

Write Single Coil

Settings are available on the **Write Single Coil** tab on the **Client Map** tab.

Table 6.31: Write Single Coil Settings

Setting	Description	Range	Default
Address	A unique identifying number in the register map.	0 to 65535	x
Point Name	A short identifier for the point in the map file.	Up to 66 ASCII characters	Single Coil X
Point Description	A detailed and localized description for the point in the map file.	Up to 128 Unicode characters	Single Coil X
OFF State Name	Text description of the 0 state.	Up to 32 Unicode characters	OFF
ON State Name	Text description of the 1 state.	Up to 32 Unicode characters	ON
Data Value	The value to be written to the point.	0000, FF00, NONE	FF00
Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0

Write Single Register 6A

Settings are available on the **Write Single Register 6A** tab on the **Client Map** tab.

Table 6.32: Write Single Register 6A Settings

Setting	Description	Range	Default
Address	A unique identifying number in the register map.	0 to 65535	x
Point Name	A short identifier for the point in the map file.	Up to 66 ASCII characters	Single 6A Register X
Point Description	A detailed and localized description for the point in the map file.	Up to 128 Unicode characters	Single 6A Register X

OFF State Name	Text description of the 0 state.	Up to 32 Unicode characters	OFF
ON State Name	Text description of the 1 state.	Up to 32 Unicode characters	ON
Data Value	The value to be written to the point.	0000, FF00, NONE	FF00
Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0

Write Single Register 6B

Settings are available on the **Write Single Register 6B** tab on the **Client Map** tab.

Table 6.33: Write Single Register 6B Settings

Setting	Description	Range	Default
Address	A unique identifying number in the register map.	0 to 65535	x
Point Name	A short identifier for the point in the map file.	Up to 66 ASCII characters	Single 6B Register X
Point Description	A detailed and localized description for the point in the map file.	Up to 128 Unicode characters	Single 6B Register X
Multiplier	Scale factor of the point (**m** of formula **mx +b**).	Full range of 64-bit Float	1.0
Offset	Scale factor of the point (**b** of formula **mx +b**).	Full range of 64-bit Float	0.0
Data Type	The type of data polled.	See Support Data Types table	UINT16
Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0

Device Properties

The MCP provides mapping settings for the Modbus Client settings on the right side of the **Client** Map tab.

Table 6.34: Modbus Device Properties

Setting	Description	Range	Default
Inter Poll Delay	Delay, in seconds, between polls.	0 to 60	0.1
Reconnect Interval	Time, in seconds, between attempts by the MCP to bring an offline device online.	1 to 3600	60
Endian Type	Endian data interpretation in the map file.	Little, Big	Big
Max Block Size	The maximum block size, in bits, of Modbus requests.	8 to 255	255
Request Retry Count	The number of retries for each request.	1 to 255	2
Fast to Slow Poll Cycle Frequency	Number of fast poll cycles before a slow poll cycle is initiated.	0 to 255	10
Fault Reset Time	Time, in seconds, for which the fault parameter pseudo points retain values from the latest fault.	1 to 3600	5
Restrike Interval	Once the first fault has occurred, the time to wait (in seconds) before updating the Fault Pseudo points with information if subsequent faults occur before this interval has elapsed.	1 to 3600	30

PRF Processing Type	The PRF processing type to use.	Pre-defined list of types	None
Response Timeout	Time in seconds after which the request is timed out.	0.1 to 300	2

SEL Binary Client

The SEL Binary Client map defines how the MCP is configured to poll data from SEL Fast Meter devices. The SEL client application uses ASCII messages to extract Protective Relay Fault (PRF) information from the SEL device. The MCP supports the following configurable SEL Binary data types:

- Fast Meter analog channel
- Demand analog channel
- Peak demand analog channel
- SER digital channel
- Device properties

The SEL Binary Client map settings are available on the **Client Map** tab when a SEL Binary protocol device type is selected.

NOTE: Additional SEL Binary configuration settings are available for device communications when configuring SEL serial connections on the **Serial** tab.

Pseudo points are available for the SEL Binary Client application.

Auto-discovery

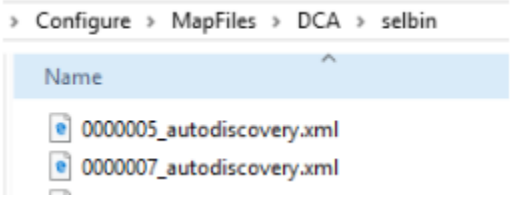
Most SEL devices support auto-discovery, also known as self-description. This feature allows you to use point mappings automatically provided by the device rather than creating a custom mapping.

Point mappings provided via auto-discovery always override those specified in the selected map file. However, if the remote device refuses an auto-discovery request, the MCP falls back to the mappings specified in the configured map file.

The path for the auto discovery file is: /mnt/usr/Configure/MapFiles/DCA/selbin/<homedir>_autodiscovery.xml

NOTE: <homedir> is the Home Directory of the SEL Binary Client Connection which can be seen through either **Connections** Tab or **Point Details** Tab in the Runtime GUI.

e.g.: /mnt/usr/Configure/MapFiles/DCA/selbin/0000007_autodiscovery.xml



Tip: It is recommended that you create a specific placeholder map file for devices that use auto-discovery; this map file should be given a distinctive name that indicates to system operators that the selected map file is being overridden.

To configure Auto-Discovery map files in SEL Binary Client configuration:

1. Go to DSAS Offline Editor and add a SEL Binary Client connection under "Connections → New Connection" tab.
2. Select an existing SEL relay mapfile **e.g.:** SEL-351.xml from the drop-down list of Map files.
   NOTE: Choose a mapfile from the list which matches to the type of the relay.

3. Save the configuration and apply "Sync To" to upload the configuration to MCP.
4. SEL Binary Client applications starts communicating with the relay and creates an auto-discovery map file from the list of point mappings provided by the relay.
5. Use Secure File Browser from DSAS, connect to the MCP using administrator credentials.
6. Navigate to /mnt/usr/Configure/Mapfiles/DCA/selbin path in the MCP.
7. Due to auto-discovery, a new mapfile is generated in the above folder with the name starting with the 'Home Directory' of the SEL Binary Connection.
   e.g.: 0000007_autodiscovery.xml. Here, 0000007 is the Home Directory of the SEL Binary Connection that can be seen in the Connection XML file.
8. Now, Open the DSAS Online Editor and go the same SEL Binary Client connection that is configured earlier using DSAS Offline Editor.
9. Go the SEL Binary Client Mapfile drop-down list and select the auto-discovery mapfile 0000007_autodiscovery.xml that is created by the SEL Binary Client application.
10. Save the configuration and Commit the changes to the MCP.
11. After commit changes the SEL Binary Client application starts using the 0000007_autodiscovery.xml to communicate to the SEL relay.

Fast Meter Analog Channel

Settings available on the **Fast Meter Analog Channel** tab on the **Client Map** tab. The MCP provides the mapping settings for fast meter analog outputs (Function code 1) as shown below.

Table 6.35: Fast Meter Analog Outputs

Setting	Description	Range	Default
Name	Text description of the point in the Fast Meter Analog Channel Map.	Up to 128 characters	FMA_xxx
Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0
Multiplier	Scale factor of the point (**m** of formula **mx +b**).	Full range of 64-bit Float	1.0
Offset	Scale factor of the point (**b** of formula **mx +b**).	Full range of 64-bit Float	0.0

Demand Analog Channel

Settings available on the **Demand Analog Channel** tab on the **Client Map** tab. The MCP provides the mapping settings for demand analog outputs (Function code 2) as shown below.

Table 6.36: Demand Analog Outputs

Setting	Description	Range	Default
Name	Text description of the point in the Demand Analog Channel Map.	Up to 128 characters	DAC_xxx
Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0
Multiplier	Scale factor of the point (**m** of formula **mx +b**).	Full range of 64-bit Float	1.0
Offset	Scale factor of the point (**b** of formula **mx +b**).	Full range of 64-bit Float	0.0

Peak Demand Analog Channel

Settings available on the **Peak Demand Analog Channel** tab on the **Client Map** tab. The MCP provides the mapping settings for peak demand analog outputs (Function code 3) as shown below.

Table 6.37: Peak Demand Analog Outputs

Setting	Description	Range	Default

Name	Text description of the point in the Peak Demand Analog Channel Map.	Up to 128 characters	PDA_xxx
Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0
Multiplier	Scale factor of the point (**m** of formula **mx +b**).	Full range of 64-bit Float	1.0
Offset	Scale factor of the point (**b** of formula **mx +b**).	Full range of 64-bit Float	0.0

SER Digital Channel

Settings are available on the **SER Digital Channel** tab on the **Client Map** tab. The MCP provides the mapping settings for SER digital inputs (Function code 5) as shown below.

Table 6.38: SER Digital Input Settings

Setting	Description	Range	Default
Point Name	A short identifier for the point in the map file.	Up to 66 ASCII characters	SER X
Point Description	A detailed and localized description for the point in the map file.	Up to 128 Unicode characters	SER Digital Channel X
Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0
OFF State Name	Text description of the 0 state.	Up to 32 characters	OFF
ON State Name	Text description of the 1 state.	Up to 32 characters	ON

Device Properties

Settings are available in the **Device Properties** pane on the **Client Map** tab. The following table lists the poll-specific settings for the SEL Fast Meter device.

Table 6.39: SEL Binary Device Properties

Setting	Description	Range	Default
Name	Name of the device map file.	Up to 8 characters	<File name>
No. of Targets	Number of Target Rows returned by the device in the Fast Meter command	0 to 255	0
No. of Breakers	Number of Breakers supported by the Fast Operate message	0 to 255	0
No. of Remote Bits	Number of Remote Bits supported by the Fast Operate message	0 to 255	0
Pulse Remote Bits	If Pulsing of remote bits is supported by the Fast Operate message	Yes No	No
No. of Calculation Blocks	Number of Calculation blocks returned by the Fast Meter Definition Block	0 to 6	0

IEC 60870-5-103 Client

IEC 60870-5-103 Client Device Properties

The IEC 60870-5-103 Client map defines how the MCP is configured to poll data from IEC 60870-5-103 compliant devices. Map settings are available on the **Client Map** tab when an IEC 60870-5-103 protocol type is selected.

Settings are available in the **Device Properties** pane. The following table lists the device-specific protocol settings.

Table 6.40: IEC 60870-5-103 Device Properties

Setting	Description	Range	Default
Data Link Confirm	Specifies whether the application requests data link confirmation when transmitting data.	Enabled Disabled	Enabled
General Interrogation Interval	The General Interrogation interval (in minutes). A value of 0.0 disables General Interrogations to the remote device, except on application startup.	0.0 to 1440.0	30.0
General Interrogation Timeout	The time (in seconds) after which a General Interrogation is assumed to have completed if no Termination of General Interrogation message has been received from the remote device.	0.01 to 3600.0	30.0
Command Timeout	The time (in seconds) after which a General Command is assumed to have completed if the appropriate ASDU Type 6 (COT=ACK or NACK) message has not been received from the remote device.	0.01 to 3600.0	10.0
Auto Time Sync	Specifies whether the application performs a time sync to the remote device when the application detects a change in the local system time and at application startup.	Enabled Disabled	Enabled
Time Sync Interval	The time synchronization interval (in minutes). A value of 0.0 disables scheduled Time Synchronizations to the remote device.	0.0 to 1440.0	10.0
Time Sync Timeout	The time (in seconds) after which a time sync is assumed to have completed if the appropriate ASDU Type 6 (COT=Time Sync) message has not been received from the remote device.	0.01 to 3600.0	5.0
IEC 103 Compliant Device	Specifies whether the IED of the client mapfile is compliant to IEC 60870-103 Standard.	True False	True

IEC 60870-5-103 Client Info Objects

An information object consists of a set of data elements. You can create the following types of information objects:

- Input
  - Measurand Time Tag Relative
  - Measurand Type 1
  - Measurand Type 2
  - Measurand User Defined
  - Time Tagged Message
- Output
  - General Command

» To create an Information Object:

1. Click Add Info Object.
2. On the **New Info Object** window, enter values for the fields as described in Table 70 and click **OK**.
3. Enter the number of rows and click **Add** to create and configure elements within the information object.

Table 6.41: Info Object Settings

Setting	Description	Range
Info Object Type	The type of information object being created.	General Command Measurand Time Tag Relative Measurand Type 1 Measurand Type 2 Measurand User Defined Time Tagged Message
Info Object Name	An identifier used within the configuration interface.	1 to 128 ASCII characters
Function Type	The IEC 60870-5-103 function type corresponding to this information object type reported by the remote device.	0 to 255
Info Number	Starting address for this object.	0 to 255

The table directly below the Info Object type drop-down menu shows the configured Info Object Name and either the Function Type and Info Number or the Default Function Type and Initial Info Number of the selected information object.

When General Command or Time Tagged Message types are selected, the Default Function Type value indicates the default function type that is used when a new information object element is added. The Initial Info Number value is incremented for each new information object element that is added.

NOTE: Additional info-object level settings are available for *Time Tagged Message* objects. These are described in the table below.

For all other info object types, values entered for Function Type and Info Number are used for all information object elements that are created.

General Command

Table 6.42: General Command Element Settings

Setting	Description	Range	Default
Function Type	The IEC 60870-5-103 function type corresponding to this information object type reported by the remote device.	0 to 255	0
Info Number	Address for this object.	0 to 255	Incremented by 1 from starting address
Point Reference	A short identifier for the point in the map file.	Up to 66 ASCII characters	<Info object name> X
Point Description	A detailed and localized description for the point in the map file.	Up to 128 Unicode characters	<Info object name> X
ON State	Text description of the 1 state.	Up to 32 Unicode characters	ON
OFF State	Text description of the 0 state.	Up to 32 Unicode characters	OFF
Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0

Measurand Time Tag Relative Time

Table 6.43: Measurand Time Tag Relative Time Element Settings

Setting	Description	Range	Default
Point Reference	A short identifier for the point in the map file.	Up to 66 ASCII characters	<Info object name> X

Point Description	A detailed and localized description for the point in the map file.	Up to 128 Unicode characters	<Info object name> X
Multiplier	Scale factor of the point (**m** of formula **mx +b**).	Full range of 64-bit Float	1.0
Offset	Scale factor of the point (**b** of formula **mx +b**).	Full range of 64-bit Float	0.0
Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0

Measurand Type 1

Table 6.44: Measurand Type 1 Element Settings

Setting	Description	Range	Default
Point Reference	A short identifier for the point in the map file.	Up to 66 ASCII characters	<Info object name> X
Point Description	A detailed and localized description for the point in the map file.	Up to 128 Unicode characters	<Info object name> X
Multiplier	Scale factor of the point (**m** of formula **mx +b**).	Full range of 64-bit Float	1.0
Offset	Scale factor of the point (**b** of formula **mx +b**).	Full range of 64-bit Float	0.0
Element Name	Specifies the name of each element.	current L2 or I.N, voltage L1-L2 or V.EN, active power P, reactive power Q	current L2 or I.N
Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0

Measurand Type 2

Table 6.45: Measurand Type 2 Element Settings

Setting	Description	Range	Default
Point Reference	A short identifier for the point in the map file.	Up to 66 ASCII characters	<Info object name> X
Point Description	A detailed and localized description for the point in the map file.	Up to 128 Unicode characters	<Info object name> X
Multiplier	Scale factor of the point (**m** of formula **mx +b**).	Full range of 64-bit Float	1.0
Offset	Scale factor of the point (**b** of formula **mx +b**).	Full range of 64-bit Float	0.0
Element Name	Specifies the name of each element.	current L1 current L2 current L3 voltage L1-E voltage L2-E voltage L3-E active power P reactive power Q frequency f	current L1
Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0

Measurand User Defined

Table 6.46: Measurand Type 1 User Defined Element Settings

Setting	Description	Range	Default
Measurand Position	You can define up to 255 elements within the Measurand 1 User Defined info object type. The Measurand Position setting specifies the element position that this value is assigned to.	1 to 255	Incremented from 1
Point Reference	A short identifier for the point in the map file.	Up to 66 ASCII characters	<Info object name> X
Point Description	A detailed and localized description for the point in the map file.	Up to 128 Unicode characters	<Info object name> X
Multiplier	Scale factor of the point (**m** of formula **mx +b**).	Full range of 64-bit Float	1.0
Offset	Scale factor of the point (**b** of formula **mx +b**).	Full range of 64-bit Float	0.0
Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0

Table 6.47: Measurand Type 2 User Defined Element Settings

Setting	Description	Range	Default
Measurand Position	You can define up to 255 elements within the Measurand 2 User Defined info object type. The Measurand Position setting specifies the element position that this value is assigned to.	1 to 255	Incremented from 1
Point Reference	A short identifier for the point in the map file.	Up to 66 ASCII characters	<Info object name> X
Point Description	A detailed and localized description for the point in the map file.	Up to 128 Unicode characters	<Info object name> X
Multiplier	Scale factor of the point (**m** of formula **mx +b**).	Full range of 64-bit Float	1.0
Offset	Scale factor of the point (**b** of formula **mx +b**).	Full range of 64-bit Float	0.0
Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0

Time Tagged Message

Table 6.48: Time Tagged Message Info Object Settings

Setting	Description	Range	Default
Relative Time	Specifies whether the time tagged message is returned using relative times.	Yes No	No
In General Interrogation	Specifies whether the points in this object are returned in response to a General Interrogation.	In General Interrogation Not In General Interrogation	In General Interrogation

Fleeting Points	Specifies whether the points in this object are fleeting points. Update of the Not Fleeting Point database only occurs when the reported value is different from the previous reported value in the database. For Fleeting points, the **Fleeting Point Reporting** setting determines how fleeting points are sent to the Database.	Fleeting Points Not Fleeting Points	Not Fleeting Points
Fleeting Points Reporting	This setting is only applicable to fleeting point objects. It specifies how fleeting point values are sent to the database. The options are: • The Two Events option sends two successive events to the Database, one with the reported value and one with the opposite value to set the point back to its previous state. • The Send Always option sends the reported value to the RTDB as a data change event even if the value is the same as that already in the database.	Two Events Send Always	Not Applicable

Table 6.49: Time Tagged Message Element Settings

Setting	Description	Range	Default
Function Type	The IEC 60870-5-103 function type corresponding to this information object type reported by the remote device.	0 to 255	0
Info Number	Starting address for this object.	0 to 255	Incremented by 1 from starting address
P1 Ref	A short identifier for the first point in the map file for this double point object.	Up to 66 ASCII characters	<Info object name> X
P1 Desc	Text description of the first point in the map file for this double point object.	Up to 128 Unicode characters	See note
P1 ON State	Text description of the 1 state for the first point.	Up to 32 Unicode characters	ON
P1 OFF State	Text description of the 0 state for the first point.	Up to 32 Unicode characters	OFF
P1 Group	Point group to which the first point belongs.	List of defined point groups	Group assigned to ID number 0
P2 Ref	A short identifier for the second point in the map file for this double point object.	Up to 66 ASCII characters	<Info object name> X
P2 Desc	Text description of the second point in the map file for this double point object.	Up to 128 Unicode characters	See note
P2 ON State	Text description of the 1 state for the second point.	Up to 32 Unicode characters	ON
P2 OFF State	Text description of the 0 state for the second point.	Up to 32 Unicode characters	OFF
P2 Group	Point group to which the second point belongs.	List of defined point groups	Group assigned to ID number 0

NOTE: The format for the default value is **X/Y Z**, where X is the function type, Y is the info number, and Z is either *Point 1* or *Point 2*.

IEC 60870-5-101+104 Client

IEC 60870-5-101+104 Client Common Properties

The IEC 60870-5-101+104 Client map defines how the MCP is configured to poll data from IEC 60870-5-101+104 compliant devices. Map settings are available on the **Client Map** tab when an IEC 60870-5-101+104 protocol type is selected.

Settings are available in the **Device Properties** pane of the IEC 60870-5-101+104 protocol type **Client Map** tab. The following table lists the device-specific protocol settings.

Table 6.50: IEC 60870-5-101+104 Client Common Properties

Setting	Description	Range	Default
Buffer Overflow DI	The information object address of the DI point where the ON (1) state indicates that the event buffer on the device has overflowed. A value of 0 disables this feature.	0 to 1	0
Command Timeout	The time (in seconds) after which a Command is assumed to have completed if the Termination message has not been received from the remote device.	0.01 to 3600.0	10.0
General Interrogation Timeout	The time (in seconds) after which a General Interrogation is assumed to have completed if no Termination of General Interrogation message has been received from the remote device.	0.01 to 3600.0	30.0
Counter Interrogation Timeout	The time (in seconds) after which a Counter Interrogation is assumed to have completed if no Termination of Counter Interrogation message has been received from the remote device.	0.01 to 3600.0	30.0
Time Sync Timeout	The time (in seconds) after which a Delay Acquisition Request or a Time Sync request is assumed to have completed if the ACTCON PDU has not been received from the remote device	0.01 to 3600.0	5.0
ACTCON Expected	Specifies whether an ACTCON PDU is expected from the remote device after the application sends an ACT PDU request.	Yes No	Yes
ACTCON Timeout	The time (in milliseconds) after which an ACTCON PDU is assumed to come back after sending out a request of ACT PDU (only applicable to control requests, general interrogation requests, and counter interrogation requests).	1 to 65535	1000
ACTTERM Expected	Specifies whether an ACTTERM PDU is expected to indicate the completion of a transaction.	Yes No	Yes
Control Override	Specifies whether the application is to override the Control Type sent in an RTDB control request, to use in the actual Binary Output request to the remote device.	None DirectOperate SBO	None
Time Sync Interval	The time synchronization interval (in minutes). A value of 0.0 disables scheduled time synchronization to the remote device.	0.0 to 1440.0	10.0
Global Counter Interrogation Interval	The Global Counter Interrogation interval (in minutes). A value of 0.0 disables Global Counter Interrogations to the remote device, except on application startup.	0.0 to 1440.0	0.0

Setting	Description	Range	Default
Group *X* Counter Interrogation Interval	The Group *X* Counter Interrogation interval (in minutes). A value of 0.0 disables Group *X* Counter Interrogations to the remote device, except on application startup.	0.0 to 1440.0	0.0
Global Interrogation Interval	The Global General Interrogation Interval (in minutes). A value of 0.0 disables Global General Interrogations to the device, except on application startup.	0.0 to 1440.0	30.0
Group *X* Interrogation Interval	The Group *X* General Interrogation Interval (in minutes). A value of 0.0 disables Group *X* General Interrogations to the device, except on application startup.	0.0 to 1440.0	0.0

IEC 60870-5-101 Client

Settings are available in the **IEC 60870-5-101** pane. The following table lists the device-specific protocol settings.

Table 6.51: IEC 60870-5-101 Client Properties

Setting	Description	Range	Default
Information Object Address Length	The number of octets used in the information object address field.	1 to 3	1
Cause of Transmission Length	The number of octets used in the Cause of Transmission field.	1 to 2	1
Data Link Confirm	Specifies whether the application requests data link confirmation when transmitting data	Enabled Disabled	Enabled
TX Delay Acquisition	Specifies whether the application performs a TX Delay Acquisition command to the device prior to performing the Clock Synchronization	Enabled Disabled	Enabled
Default TX Delay	The default transmission delay (in milliseconds) that is used by the application to perform a Clock Sync of the remote device when the TX Delay Acquisition is disabled	0 to 60000	0
Load Tx Delay	Specifies whether or not the DCA shall transmit the acquired transmission delay to the remote device if Tx Delay Acquisition is Enabled.	Enabled Disabled	Enabled

IEC 60870-5-104 Client

Settings are available in the **IEC 60870-5-104** pane. The following table lists the device-specific protocol settings.

Table 6.52: IEC 60870-5-104 Client Properties

Setting	Description	Range	Default
Information Object Address Length	The number of octets used in the information object address field.	Not editable	3
Cause of Transmission Length	The number of octets used in the Cause of Transmission field.	Not editable	2
Default TX Delay	The transmission delay (in milliseconds) that is used by the application to perform a Clock Sync of the remote device.	Not editable	0
Controls with Time Tag	Specify if the application is to include a time tag with control requests.	Enabled Disabled	Disabled
Max TX Frames Before Ack	The maximum number of information frames that the application transmits before it must receive an acknowledgement message (value of **w**).	1 to 32,767	8

Setting	Description	Range	Default
Max RX Frames Before Ack	The maximum number of information frames that the application receives before it must send an acknowledgement message (value of **k**).	1 to 32,767	12
Connect Timeout	The maximum time (in seconds) that the application waits for the TCP transport layer to establish a connection (value of **t0**).	1 to 255	30
Send Timeout	The maximum time (in seconds) that the application waits for an acknowledgement after sending a frame (value of **t1**).	1 to 255	15
No Data Timeout	The maximum time (in seconds) that the application waits before sending a supervisory acknowledgement (S) frame (value of **t2**).	1 to 255	10
Idle Timeout	The period during which no messages are received, in seconds, that the application allows pass before sending a test frame (value of **t3**).	1 to 255	20

IEC 60870-5-101+104 Client Info Objects

An information object consists of a set of data elements. You can create the following types of information objects:

- Input
  - Bitstring
  - Double Point
  - Integrated Total
  - Measurand
  - Packed Single Point
  - Single Point
  - Step Position
- Output
  - Double Command
  - Regulating Step Command
  - Setpoint Command
  - Single Command

» To create an Information Object:

1. Click Add Info Object.
2. On the **New Info Object** window, enter values for the fields as described in the Infor Object Settings table and click **OK**.
3. Enter the number of rows and click **Add** to create and configure elements within the information object.

Table 6.53: IEC 60870-5-101+104 Client Info Objects

Setting	Description	Range
Info Object Type	The type of information object being created.	Bitstring Double Point Integrated Total Measurand Packed Single Point Single Point Step Position Double Command Regulating Step Command Setpoint Command Single Command
Info Object Name	An identifier used within the configuration interface. This is a view-only field.	1 to 128 ASCII characters
Address	The assigned address for BitString and Packed Single Point types; the starting default address for all other types.	1 to 16777215

The table directly below the Info Object type drop-down menu shows the configured Info Object Name and either the Address or Starting Address of the selected information object. When Bitstring or Packed Single Point types are selected, the Address value indicates the actual information object address. If any other Info Object type is selected, the Starting Address value indicates the default starting address that is used when a new information object element is added.

Bitstring

Table 6.54: Bitstring Element Settings

Setting	Description	Range	Default
Bit Position	The bit position within the DI point	1 to 32	Incremented from 1
Point Reference	A short identifier for the point in the map file.	Up to 66 ASCII characters	<Info object name> X
Point Description	A detailed and localized description for the point in the map file.	Up to 128 Unicode characters	<Info object name> X
ON State	Text description of the 1 state.	Up to 32 characters	ON
OFF State	Text description of the 0 state.	Up to 32 characters	OFF
Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0

Double Command

Table 6.55: Double Command Element Settings

Setting	Description	Range	Default
Address	The address of this information object element	1 to 16777215	Incremented by 1 from starting address
Point Reference	A short identifier for the point in the map file.	Up to 66 ASCII characters	<Info object name> X

Point Description	A detailed and localized description for the point in the map file.	Up to 128 Unicode characters	<Info object name> X
Command Qualifier	An attribute that specifies in greater detail the type of control action requested.	No Additional Definition Short Pulse Duration Long Pulse Duration Persistent	Persistent
ON State	Text description of the 1 state.	Up to 32 characters	ON
OFF State	Text description of the 0 state.	Up to 32 characters	OFF
Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0

Double Point

Table 6.56: Double Point Element Settings

Setting	Description	Range	Default
Address	The address of this information object element	1 to 16777215	Incremented by 1 from starting address
P1 Name	Text description of the first point in the map file for this double point object.	Up to 128 characters	DP *X*A
P1 ON State	Text description of the 1 state for the first point.	Up to 32 characters	ON
P1 OFF State	Text description of the 0 state for the first point.	Up to 32 characters	OFF
P1 Group	Point group to which the first point belongs.	List of defined point groups	Group assigned to ID number 0
P2 Name	Text description of the second point in the map file for this double point object.	Up to 128 characters	DP *X*B
P2 ON State	Text description of the 1 state for the second point.	Up to 32 characters	ON
P2 OFF State	Text description of the 0 state for the second point.	Up to 32 characters	OFF
P2 Group	Point group to which the second point belongs.	List of defined point groups	Group assigned to ID number 0

Integrated Total

Table 6.57: Integrated Total Element Settings

Setting	Description	Range	Default
Address	The address of this information object element	1 to 16777215	Incremented by 1 from starting address
Point Reference	A short identifier for the point in the map file.	Up to 66 ASCII characters	<Info object name> X
Point Description	A detailed and localized description for the point in the map file.	Up to 128 Unicode characters	<Info object name> X
Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0

Measurand

Table 6.58: Measurand Element Settings

Setting	Description	Range	Default
Address	The address of this information object element	1 to 16777215	Incremented by 1 from starting address
Point Reference	Text description of the point in the map file.	Up to 128 characters	M *X*
Multiplier	Scale factor of the point (**m** of formula **mx +b**).	Full range of 64-bit Float	1.0
Offset	Scale factor of the point (**b** of formula **mx +b**).	Full range of 64-bit Float	0.0
Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0

Packed Single Point

Table 6.59: Packed Single Point Element Settings

Setting	Description	Range	Default
Setting	Description	Range	Default
Bit Position	The bit position within the DI point	1 to 32	Incremented from 1
Point Reference	A short identifier for the point in the map file.	Up to 66 ASCII characters	<Info object name> X
Point Description	A detailed and localized description for the point in the map file.	Up to 128 Unicode characters	<Info object name> X
ON State	Text description of the 1 state.	Up to 32 characters	ON
OFF State	Text description of the 0 state.	Up to 32 characters	OFF
Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0

Regulating Step Command

Table 6.60: Regulating Step Command Element Settings

Setting	Description	Range	Default
Address	The address of this information object element	1 to 16777215	Incremented by 1 from starting address
Point Reference	A short identifier for the point in the map file.	Up to 66 ASCII characters	<Info object name> X
Point Description	A detailed and localized description for the point in the map file.	Up to 128 Unicode characters	<Info object name> X
Regulating Command State	The relative position that the step controller is commanded to move to.	Lower Higher	Lower

Command Qualifier	An attribute that specifies in greater detail the type of control action requested.	No Additional Definition Short Pulse Duration Long Pulse Duration Persistent	Persistent
ON State	Text description of the 1 state.	Up to 32 characters	ON
OFF State	Text description of the 0 state.	Up to 32 characters	OFF
Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0

Setpoint Command

Table 6.61: Setpoint Command Type 2 Element Settings

Setting	Description	Range	Default
Address	The address of this information object element	1 to 16777215	Incremented by 1 from starting address
Point Reference	A short identifier for the point in the map file.	Up to 66 ASCII characters	<Info object name> X
Point Description	A detailed and localized description for the point in the map file.	Up to 128 Unicode characters	<Info object name> X
Conversion	The type of setpoint command. There are 3 possible types: Normalized - value is between -1 and +1 -2^-15 Scaled - value is scaled using multiplier and offset to -2^15 to +2^15 – 1 Short Floating Point - value is a 32-bit floating point.	Normalized Scaled ShortFP	Normalized
Multiplier	Scale factor of the point (**m** of formula **mx +b**).	Full range of 64-bit Float	1.0
Offset	Scale factor of the point (**b** of formula **mx +b**).	Full range of 64-bit Float	0.0
Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0

Single Command

Table 6.62: Single Command Element Settings

Setting	Description	Range	Default
Address	The address of this information object element	1 to 16777215	Incremented by 1 from starting address
Point Reference	A short identifier for the point in the map file.	Up to 66 ASCII characters	<Info object name> X
Point Description	A detailed and localized description for the point in the map file.	Up to 128 Unicode characters	<Info object name> X

Command Qualifier	An attribute that specifies in greater detail the type of control action requested.	No Additional Definition Short Pulse Duration Long Pulse Duration Persistent	Persistent
ON State	Text description of the 1 state.	Up to 32 characters	ON
OFF State	Text description of the 0 state.	Up to 32 characters	OFF
Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0

Single Point

Table 6.63: Single Point Element Settings

Setting	Description	Range	Default
Address	The address of this information object element	1 to 16777215	Incremented by 1 from starting address
Point Reference	A short identifier for the point in the map file.	Up to 66 ASCII characters	<Info object name> X
Point Description	A detailed and localized description for the point in the map file.	Up to 128 Unicode characters	<Info object name> X
ON State	Text description of the 1 state.	Up to 32 characters	ON
OFF State	Text description of the 0 state.	Up to 32 characters	OFF
Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0

Step Position

Table 6.64: Step Position Element Settings

Setting	Description	Range	Default
Address	The address of this information object element	1 to 16777215	Incremented by 1 from starting address
Point Reference	A short identifier for the point in the map file.	Up to 66 ASCII characters	<Info object name> X
Point Description	A detailed and localized description for the point in the map file.	Up to 128 Unicode characters	<Info object name> X
Multiplier	Scale factor of the point (**m** of formula **mx +b**).	Full range of 64-bit Float	1.0
Offset	Scale factor of the point (**b** of formula **mx +b**).	Full range of 64-bit Float	0.0
Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0

Generic ASCII Client

About the Generic ASCII Client

The Generic ASCII client can be used to extract data from devices that use an ASCII-based communications protocol over a serial connection. Information that can be collected through this protocol includes:

- Metering data (present values, demand meter data, peak demand data).
- System status and self-test status.
- Status of digital inputs.

There are three configurable components of Generic ASCII client map: common properties, which define device-specific parameters; parsing policies, which define how messages are handled when they are received; and transactions, which define how messages are collected from the remote device.

Generic ASCII Client Common Properties

Settings are available in the pane at the right of the window. The following table lists the device-specific protocol settings.

Table 6.65: Generic ASCII Client Common Properties

Setting	Description	Range	Default
Device family name	The name of the device manufacturer or the product series (for example, SEL or GE DFP).	1 to 65 characters	none
Login required	Specify if a valid username and password is required when accessing the remote device.	True False	True
Enable logging	If set to true, all traffic to and from this device is logged to an IO Traffic window on the MCP HMI.	True False	True
Enable unsolicited processing	If set to *true*, the MCP accepts unsolicited data from the remote device. If set to *false*, unsolicited data is ignored.	True False	False
User comments	General comments or information about the client map file.	0 to 1024 characters	none
Fault reset time (sec)	Whenever a fault occurs, the fault information is provided in a pseudo point. After the configured period of time passes, the value of the pseudo point is reset to 0. All faults are recorded in the event log regardless of the amount of time the pseudo point is active.	0 to 3600 seconds	5
Restrike interval (sec)	The amount of time, in seconds, that must pass after a fault is reported before subsequent fault reports are considered valid. If a subsequent fault report occurs within this time period, it is recorded in the event log but is not reported as the value of the pseudo point.	0 to 3600 seconds	30
Login prompt	If login is required, the MCP monitors incoming data from the remote device for the configured login prompt. When encountered, the MCP begins the login sequence. If neither the login prompt or the successful login prompt appears, the MCP sends the configured break sequence.	0 to 64 characters	=
User name	The user name to use when logging into the remote device.	0 to 64 characters	ACCESS

Setting	Description	Range	Default
Successful login prompt	The MCP monitors the incoming data from the remote device for the configured successful login prompt. Once detected, the MCP begins the next protocol transactions with the remote device. This parameter is mandatory.	0 to 64 characters	=>
Login retries	The maximum number of times the MCP attempts the login sequence.	0 to 255	0
SOM	The start of message character sequence is defined in hex-decimal format. When this sequence is encountered, the MCP considers it to be the start of the message. If the SOM is not defined, any valid ASCII character received is considered as the SOM. If a multiple character sequence is required as the start of message, use + as a delimiter between each character. For example, to define 123 as the SOM, define these characters as 0x31+0x32+0x33.	0 to 64 characters.	0x02
EOM	The end of message character sequence is defined in hex-decimal format. When this sequence is encountered, the MCP considers the message to be complete. If the EOM is not defined, the message is assumed to be complete when the response timeout passes.	0 to 64 characters	0x03
Break	This character sequence is transmitted to the remote device when the MCP requires a prompt.	0 to 64 characters	0x0D
Stop transmission	This character sequence is transmitted to the remote device by the MCP to request that data transmission be stopped. It is used when the amount of incoming data exceeds the capacity of the MCP to process it.	0 to 64 characters	0x13
Resume transmission	This character sequence is transmitted to the remote device by the MCP to resume a stopped data transmission.	0 to 64 characters	0x11
Default line ends	This character sequence is transmitted to the remote device by the MCP to indicate the end of a command transmission.	0 to 64 characters	Nil (no characters transmitted)
Default retries	The maximum number of times the MCP retries a transaction when it does not receive a response from the remote device.	0 to 300	0
Transaction timeout	The amount of time, in milliseconds, that must pass before the MCP retries a transaction.	20 to 65000 milliseconds	100
Device Response Timeout	The maximum duration in seconds that the DCA is to wait for a response when the **Allow Delayed Message Processing** property is enabled in application parameters. If the **Allow Delayed Message Processing** property is disabled, this parameter is not applicable.	0 to 300	5
Reconnect Interval	The **Device Offline Reconnect Interval** property duration in seconds. Once the MCP detects any device in the offline state, the MCP is to resume polling of transactions only after this Reconnect Interval timer has expired.	10 to 3600	60

Setting	Description	Range	Default
Wait Time Between Polls	The minimum time in seconds to wait between polls; that is by measuring the time between receiving the response of one poll and the beginning of the next poll.	0 to 3600	0.001
Max Offline Fail Count	The number of consecutive failed requests to an IED before the points are marked offline.	1 to 300	2

Generic ASCII Client Parsing Policies

Parsing policies define how incoming generic ASCII messages are processed by the MCP. To add a parsing policy to the client map file, click the **Add Parsing Policy** button and configure the options in the popup window. To remove an existing policy, select it in the drop-down list and click **Remove Parsing Policy**.

The following table lists the options that can be configured for each parsing policy.

Table 6.66: Generic ASCII Client Parsing Policies Options

Setting	Description	Range	Default
Policy name	A user-supplied name to identify the parsing policy.	1 to 64 characters	none
Type of policy	The type of method that the MCP uses to interpret incoming messages. *Token*: the message is divided into tokens based on a defined separator pattern. *Position*: The contents of the message are provided in a fixed data position.	Token Position	Token
Invalid Pattern	If this string is returned in response to a request, the MCP assumes that a configuration error has occurred. The data points associated with this message are placed OFFLINE and the Config Errors pseudo point is incremented.	0 to 64 characters	Invalid Command
Separators	The character sequence to be used when tokenizing the incoming message. This field is only applicable when **Token** is selected as the **Type of Policy**.	0 to 64 characters	0x09+0x0B+ 0x0D+0x20
Override line end	If this parsing policy is required to interpret line endings differently than as configured on the common properties pane, it can be defined here. Since a parsing policy may be used by different transactions, you should only apply an override here if it applies to all transactions that are configured to use the policy.	0 to 64 characters	Nil (no characters transmitted)

Generic ASCII Client Transactions

Transactions are used to configure message exchange between the MCP and the remote device.

To add a transaction to the client map file, click the **Add Transaction** button and configure the options in the popup window.

To remove an existing transaction, select it in the drop-down list and click **Remove Transaction**.

Once a transaction has been created, you can define the analog input points, digital input points, and text data points to be made available based on data received from the remote device.

The data points under each transaction are specific to that transaction; that is, the data point values are only updated with the response received during that transaction execution. Even if multiple transactions are defined to provide the same response, the data points are unique for each transaction; that is, the data point values are updated for each specific transaction execution.

Transaction options

The following table lists the options that can be configured for each transaction.

Table 6.67: Generic ASCII Client Transactions Options

Setting	Description	Range	Default
Transaction name	A user-supplied name to identify the transaction.	1 to 64 characters	none
Parsing policy name	Select a parsing policy to be used by this transaction.	List of configured parsing policies	none
Trigger	Select how message requests are made by this transaction: • **Cyclic:** The remote device is polled for information relative to other transactions based on the number of cycles per poll. • **Periodic:** The remote device is polled for information at the configured time frequency. **NOTE**: When multiple transactions are defined, the MCP verifies each transaction for scheduling based on round robin mode. If the cycle time to verify all transactions exceeds the Periodic interval (Msec per poll), the MCP schedules the transaction only when it completes the scan cycle and detects the expiry of the Periodic interval for any transaction. • Unsolicited: The MCP accepts messages from the remote device as they are made available. Support for the Trigger mode setting is available for the SEL family of devices.	Cyclic Periodic Unsolicited	Cyclic
Timestamp parsing	Specifies whether timestamp information should be parsed from information on the transaction level or on the individual point level. Select *None* if a timestamp should be assigned based on the MCP system clock.	None TransacLevel PointLevel	None
Timestamp definition	Specify how timestamps are to be parsed from incoming messages. Only available if the timestamp parsing field is set to *TransacLevel*.	See Timestamp Definition.	
Message out	This character sequence is transmitted to the remote device when requesting a message. The MCP supports predefined variable syntax {$ADDR$}. This setting contains the IED Address configured in the Connection page for the respective device. This setting can also be referenced whenever an IED Address is required while configuring the Message out setting. For example: If the required Message Out setting is 123<IED Address>,I0<IED Address>, then configure the Message Out setting as 123{$ADDR$},I0{$ADDR$}.	0 to 64 characters	Meter

Setting	Description	Range	Default
Override retries	The maximum number of retry requests for this transaction. If this value is defined, it overrides the default retry limit specified in the common properties pane. Select *0* to use the default retry limit.	0 to 300	0
Override line end	If this transaction is required to interpret line endings differently than as configured on the common properties pane, it can be defined here.	0 to 64 characters	Nil (no characters transmitted)
Msec per poll	The frequency at which the poll request is transmitted to the remote device. If set to 0, the poll is only performed once. This setting is only used if the trigger is set to *Periodic*.	0 to 86400000	30000
Cycles per poll	The number of times the poll request is transmitted to the remote device per batch. If set to 0, the poll is only performed once. This setting is only used if the trigger is set to *Cyclic*.	0 to 5000	2
Valid Response Pattern	The valid pattern which is to be available in the received response. When set to **Nil**, this setting is not applicable and the MCP accepts any response as a valid response. If this setting is defined with a value other than **Nil**, the MCP assumes the response for Message Out is to contain the valid response string defined and if this valid response string is not available in the response received, the MCP considers the response as an invalid or unrecognized response and discards the response. All the responses received from devices are logged in the global IO traffic window and the valid responses are logged in the respective device IO traffic window.	1 to 255 Printable ASCII Characters	Nil

Valid Response Pattern Definition

For devices which are expected to provide delayed responses, the MCP is configured with a valid response pattern.

Supported characters from MCP HMI comprise all printable ASCII characters. If predefined variables are used, they must match with the syntax definition of predefined variables otherwise they will be considered as regular sub strings in the matching criteria.

Predefined variables supported by the Valid Response Pattern are:

- ADDR – IED Address defined in connection page
- CHKSUM16 – Checksums supported by the device.

The IED Address can be specified using the following pattern: {$ADDR$}.

For example: When the response expected from a device is IFF12414F# where the IED Address is 1241 then the valid pattern definition is to be:

- I..{$ADDR$}
  where I is the starting character
  The IED Address defined in Connection Page is available after 2 characters from I.
- I*{$ADDR$}

where I is the starting character
The response contains the IED Address defined in the Connection page.

If the predefined variables do not match with the required syntax, the MCP considers this response to be the expected regular string.

For example: When the response is IFF12414F# where IED Address is 1241 and if the valid pattern definition is configured incorrectly as I*{%s$ADDR@}, the MCP uses {%s$ADDR@} as one of the substrings it expects in the response which can lead to responses mismatching with any of the configured requests. Consequently, the requests which do not get a matching response are considered as TIMEOUT and are retried based on the configured number of retries.

Examples of incorrect configurations are:

- {ADDR}
- {$ADDR}
- {ADDR$}
- {$addr$}

An example of a correct configuration is:

- {$ADDR$}

If devices support the checksum field in the response, the checksum can be configured using the predefined variables to validate the data received.

The XOR-based 16-bit CHKSUM must be defined using the predefined variable {$CHKSUM16$}.

The syntax rules are:

{$CHKSUM16$} or {$CHKSUM16$^n} or {$CHKSUM16$#n}

Where:

- n specifies the zero-based position of checksum in the response.
- ^ specifies the position from beginning of the response received
- # specifies the position from end of response received

The default definition of {$CHKSUM16$} expects the checksum be available in the 2nd and 3rd byte from the end of response.

If there is any misconfiguration of the checksum definition as per the supported syntax checksum definition is considered by the MCP as a regular substring to be used in the matching criteria.

Examples of incorrect configurations are:

- {$CHKSUM16$^0}
- {$CHKSUM16$^999999999999}
- {$CHKSUM16@^5}

As an example of a correct configuration, consider a response as IFF12414F#; then the valid Pattern Definition is to be:

- I..{$ADDR$}{$CHKSUM16$}
- I..{$ADDR$}{$CHKSUM16$^7}
- I..{$*ADDR*$}{$CHKSUM16$#2}
- I*{$ADDR$}*{$CHKSUM16$}
- I*{$ADDR$}*{$CHKSUM16$^7}
- I*{$ADDR$}*{$CHKSUM16$#2}

The incorrect configuration of predefined variables can lead to mismatching requests which results in TIMEOUT for the requests.

Timestamp definition

The **Timestamp** window allows you to define a custom timestamp parsing policy for use in a transaction. The following table lists the options that can be configured for each timestamp definition.

Table 6.68: Timestamp Options

Setting	Description	Range	Default
Date format	The format that the remote device reports the date in.	MM/DD/YY MM/DD/YYYY DD/MM/YYYY	MM/DD/YY
Date parsing type	The type of method that the MCP uses to interpret the data to determine the date. *Token*: the data is divided into tokens based on a defined separator pattern. *Position*: The contents of the timestamp are provided in a fixed data position.	Token Position	Position
Date parsing start position	The starting position of the date information within the data. *Token* date parsing type only.	Numeric value	0
Date parsing length	The length of the date information within the data. *Token* date parsing type only.	Numeric value	0
Date parsing index	The array index that contains the date.	Numeric value	0
Date parsing initial string	If the date token contains a prefix (for example, "*Date:* ") it can be specified here. The MCP removes this string from the token. Enter *None* to disable parsing.	0 to 20 printable ASCII characters	None
Date Parsing Encoding Format	The encoded data format for the date fields in the received response from the device.	Hex Ascii Binary Packed BCD Decimal	Decimal
Time format	The format that the remote device reports the time in.	hh:mm:ss [AM/PM] hh:mm:ss [24 hour] hh:mm [AM/PM] hh:mm hh:mm:ss.msec [AM/PM] hh:mm:ss.msec [24 hour]	Hh:mm:ss [AM/PM]
Time parsing type	The type of method that the MCP uses to interpret the data to determine the time. *Token*: the data is divided into tokens based on a defined separator pattern. *Position*: The contents of the timestamp are provided in a fixed data position.	Token Position	Position
Time parsing start location	The starting position of the time information within the data. *Token* time parsing type only.	Numeric value	0
Time parsing length	The length of the time information within the data. *Token* time parsing type only.	Numeric value	0
Time parsing index	The array index that contains the time.	Numeric value	0

Setting	Description	Range	Default
Time parsing initial string	If the time token contains a prefix (for example, "*Time:* ") it can be specified here. The MCP removes this string from the token. Enter *None* to disable parsing.	0 to 20 printable ASCII characters	None
Time Parsing Encoding Format	The encoded data format for the time fields in the received response from the device.	Hex Ascii Binary Packed BCD Decimal	Decimal

Add Analog Input Points, Digital Input Points and Text Data Points

Once you have created a transaction, you can add Analog Input points, Digital Input points, and Text Data points based on messages received by the MCP. To add one or more points, select the number of points you wish to add and click the **Add** button. To remove points, select them and click the **Delete** button.

The following three tables list the options that can be configured for each point type:

- Analog Input Points
- Digital Input Points
- Text Data Points

Analog Input Points

Table 6.69: Analog Input Points

Setting	Description	Range	Default
Point reference	The short user-defined identifier for the point.	0 to 66 alphanumeric characters plus space, underscore, and dash	none
Point description	The user-defined block of text that provides a detailed and localized description of the point.	1 to 128 Unicode characters	Analog input *n*
Multiplier	Scale Factor of a point (**m** of formula **mx +b**).	Full range of 64-bit Float	1
Offset	Scale Factor of a point (**b** of formula **mx +b**).	Full range of 64-bit Float	0
Parsing location	If the type of parsing policy selected in the transaction is *Token*, you can specify the array index and initial string for this point. If the type of parsing policy is *Position*, you can specify the length of the data for this point. The starting position is automatically calculated based on the previous configured points.	Index: Numeric value Initial string: 0 to 20 printable ASCII characters Position: Numeric Value	Index: 0 Initial string: None Position: 0
	Encoding Format: Specify the encoding data format for the Analog Point fields in the response received. The MCP decodes the response packets based on the encoding format selected. If the data is not valid as per the selected encoded format, respective points are put offline and the quality property is set to "Old Data".	Hex Ascii Binary Packed BCD Decimal	Decimal

Setting	Description	Range	Default
Timestamp parsing	Specify how timestamps are to be parsed from incoming messages. Only available if the timestamp parsing field is set to *PointLevel*.	See Timestamp Definition.	
Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0

Digital Input Points

Table 6.70: Digital Input Points

Setting	Description	Range	Default
Point reference	The short user-defined identifier for the point.	0 to 66 alphanumeric characters plus space, underscore, and dash	none
Point description	The user-defined block of text that provides a detailed and localized description of the point.	1 to 128 Unicode characters	Digital input *n*
ON state	A text string that is associated with the 1 state. This string is recorded in the MCP database and is displayed with the point.	0 to 64 characters	ON
OFF state	A text string that is associated with the 0 state. This string is recorded in the MCP database and is displayed with the point.	0 to 64 characters	OFF
Parsing location	If the type of parsing policy selected in the transaction is *Token*, you can specify the array index and initial string for this point. If the type of parsing policy is *Position*, you can specify the length of the data for this point. The starting position is automatically calculated based on the previous configured points.	Index: Numeric value Initial string: 0 to 64 characters Position: Numeric Value	Index: 0 Initial string: None Position: 0
	Encoding Format: Specify the encoding data format for the Digital Point fields in the response received. The MCP decodes the response packets based on the encoding format selected. If the data is not valid as per the selected encoding format selected, respective points are put offline and the quality property is set to "Old Data".	Hex Ascii Binary Decimal	Hex
	Bit Position: This defines the bit position to be considered in the response token for updating the DI Point.	0 to 31	0
Timestamp parsing	Specify how timestamps are to be parsed from incoming messages. Only available if the timestamp parsing field is set to *PointLevel*.	See Timestamp Definition.	
Enumeration 0	The string returned by the device that should be interpreted as the 0 state. This parameter is applicable only when the encoding format selected is ASCII. For other encoding formats, the point data is decoded as per the selected encoding format and bit position defined.	0 to 64 characters	0

Setting	Description	Range	Default
Enumeration 1	The string returned by the device that should be interpreted as the 1 state. This parameter is applicable only when the encoding format selected is ASCII. For other encoding formats, the point data is decoded as per the selected encoding format and bit position defined	0 to 64 characters	1
Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0

Text Data Points

Table 6.71: Text Data Points

Setting	Description	Range	Default
Point reference	The short user-defined identifier for the point.	0 to 66 alphanumeric characters plus space, underscore, and dash	none
Point description	The user-defined block of text that provides a detailed and localized description of the point.	1 to 128 Unicode characters	Analog input *n*
Parsing location	If the type of parsing policy selected in the transaction is *Token*, you can specify the array index and initial string for this point. If the type of parsing policy is *Position*, you can specify the length of the data for this point. The starting position is automatically calculated based on the previous configured points.	Index: Numeric value Initial string: Position: Numeric Value	Index: 0 Initial string: None Position: 0
	Encoding Format: Specify the encoding data format for the Digital Point fields in the response received. The MCP decodes the response packets based on the encoding format selected. If the data is not valid as per the selected encoding format selected, respective points are put offline and the quality property is set to "Old Data".	Ascii Binary Decimal	Ascii
Timestamp parsing	Specify how timestamps are to be parsed from incoming messages. Only available if the timestamp parsing field is set to *PointLevel*.	See Timestamp Definition.	
Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0

NOTE: The data points under each transaction are specific to that transaction; that is, the data point values are only updated with the response received during that transaction execution. Even if multiple transactions are defined to provide the same response, the data points are unique for each transaction; that is, the data point values are updated for each specific transaction execution.

Generic ASCII Client Application Settings

Generic ASCII client application settings are available under the Application Parameters field.

Application Tab

Table 6.72: Generic ASCII Client Application Tab

Setting	Description	Range	Default
Allow Delayed Message Processing	This parameter enables support for processing delayed responses from the devices. With this configuration, distinct "Valid Response Patterns" must be defined for transactions.	Disabled Enabled	Enabled
Passthrough response timeout	This parameter is the same as the pass-through *timeout* setting, except that it applies to those times when the pass*through connection is idle while awaiting a response from the remote device. In some cases, this time period is configured to be longer than the default timeout below because of the additional time required to process responses to operator commands.	0 to 3600 seconds	10
XON_XOFF flow control	Enable or disable XON/XOFF flow control.	True False	False
RTS_CTS flow control	Enable or disable RTS/CTS flow control.	True False	False
DTR_DSR handshaking	Enable or disable DTR/DSR handshaking.	True False	False
Inter Device Delay	This parameter specifies the delay time in seconds to wait between consecutive device polls. (measured from receiving the response for the last request of one device to the beginning of first poll of next device)	0 to 3600	0.01

SNMP Client Properties

An SNMP client map is used to determine how information is retrieved from SNMP-enabled devices.

Settings are available in the **Device Properties** pane. The following table lists the device-specific protocol settings.

Table 6.73: SNMP Client Common Properties

Setting	Description	Range	Default
Version name	Select the SNMP protocol version to use when communicating with the remote device. The MCP currently supports versions 1 and 2 of the protocol.	V1 V2	V1
Comm name	The name of the community that the SNMP device belongs to. This helps define where information is sent. Default community names are public and private.	2 to 255 ASCII characters	public
Poll frequency	The amount of time, in seconds, that the MCP waits before polling the remote device for new SNMP messages.	5 to 300	60
Session timeout	The amount of time, in seconds, to wait for a response from the remote device before the MCP assumes that a poll has failed.	1 to 10	5

Retry count	The number of session timeouts that must occur before the MCP attempts to contact the remote device on an alternate port.	0 to 100	3
Reconnect time	The amount of time, in seconds, that the MCP waits before attempting to retry polling a remote device after a session timeout.	10 to 3600	60

Table 6.74: Digital Input Sub Tab

Setting	Description	Range	Default
Point reference	The short user-defined identifier for the point.	0 to 66 alphanumeric characters plus space, underscore, and dash	DI X
Point description	The user-defined block of text that provides a detailed and localized description of the point.	1 to 128 Unicode characters	Digital input X
OID	The identifier of the SNMP object to be retrieved as the point value. You can open the SNMP Agent Browser and enter an IP Address and port number to retrieve a listing of all available OIDs from the remote device.	Valid OID from the remote SNMP device.	None
Poll type	The type of poll to be performed for the point. Selecting: • POLL causes the MCP to periodically check for new SNMP messages at the configured poll interval. • TRAP causes the MCP to wait for unsolicited SNMP messages. • BOTH configures the MCP to both poll and accept unsolicited messages from the remote device.	POLL TRAP BOTH	POLL
ON state	A text string that is associated with the 1 state. This string is recorded in the MCP database and is displayed with the point.	0 to 64 characters	ON
OFF state	A text string that is associated with the 0 state. This string is recorded in the MCP database and is displayed with the point.	0 to 64 characters	OFF
Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0

Table 6.75: Analog Input Sub Tab

Setting	Description	Range	Default
Point reference	The short user-defined identifier for the point.	0 to 66 alphanumeric characters plus space, underscore, and dash	AI X
Point description	The user-defined block of text that provides a detailed and localized description of the point.	1 to 128 Unicode characters	Analog input X

OID	The identifier of the SNMP object to be retrieved as the point value. You can open the SNMP Agent Browser and enter an IP Address and port number to retrieve a listing of all available OIDs from the remote device.	Valid OID from the remote SNMP device.	None
Poll type	The type of poll to be performed for the point. Selecting: • POLL causes the MCP to periodically check for new SNMP messages at the configured poll interval. • TRAP causes the MCP to wait for unsolicited SNMP messages. • BOTH configures the MCP to both poll and accept unsolicited messages from the remote device.	POLL TRAP BOTH	POLL
Multiplier	Scale factor of the point (**m** of formula **mx +b**).	Full range of 64-bit Float	1.0
Offset	Scale factor of the point (**b** of formula **mx +b**).	Full range of 64-bit Float	0.0
Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0

Table 6.76: Accumulator and Text Sub Tabs

Setting	Description	Range	Default
Point reference	The short user-defined identifier for the point.	0 to 66 alphanumeric characters plus space, underscore, and dash	ACC X or TEXT X
Point description	The user-defined block of text that provides a detailed and localized description of the point.	1 to 128 Unicode characters	Accumulator X or Text X
OID	The identifier of the SNMP object to be retrieved as the point value. You can open the SNMP Agent Browser and enter an IP Address and port number to retrieve a listing of all available OIDs from the remote device.	Valid OID from the remote SNMP device.	None
Poll type	The type of poll to be performed for the point. Selecting: • POLL causes the MCP to periodically check for new SNMP messages at the configured poll interval. • TRAP causes the MCP to wait for unsolicited SNMP messages. • BOTH configures the MCP to both poll and accept unsolicited messages from the remote device.	POLL TRAP BOTH	POLL
Point Group	Point group to which the point belongs.	List of defined point groups	Group assigned to ID number 0

IEC 61850 Client

The MCP supports communications to IEC 61850 compliant devices using the IEC 61850 client application. The IEC 61850 Loader is used to configure the IEC 61850 client Map file and application for the MCP Substation Gateway. The IEC 61850 client application allows the MCP to act as a master communications device for IEC 61850 compliant server devices. The master device responsibilities include:

- Initiating data exchanges with devices
- Sending control commands to devices, and
- Processing data autonomously reported by devices

The IEC 61850 Loader is integrated into DS Agile MCP Studio™ Utilities. For information on how to configure the MCP for IEC 61850 communications, refer to the DS Agile MCP Studio™ online help.

Note: The IEC 61850 loader application will be launched only if the MCP device is licensed for the IEC61850 client.

IEC61850 Client and Configuration tool (Loader) are compatible to Ed.1 and Ed.2 as detailed in the Conformance Statements.

MCP Redundancy

This chapter consists of the following sections:

About Redundancy
Redundancy Summary
Operational States
MCP Redundancy Configuration Combinations
Configure the MCP for Redundancy
System Points
Non-Sync Mode
Validating the Redundant Connections
Changeover during Standby Start-up
Data Synchronization
Ethernet Connections
Sync Config Operation
HMI User Access Privileges on Redundant System
Redundancy Setup Checklist
Error Messages and Troubleshooting

NOTE: This feature is not supported in G100

About Redundancy

The MCP redundancy solution uses two MCPs connected through serial and/or network links; one MCP is in active mode and the other MCP is in standby mode. If the active unit fails, the standby unit becomes active and takes over system operation. Redundancy in the MCP is enabled and disabled using the mcpcfg Configuration Utility/Settings GUI.

Three redundancy modes can be configured:

- **Warm Standby Redundancy**

Two MCP units are connected using an RS-232 switch panel and a single dedicated serial link. Data synchronization is minimal, restricted to field Accumulator points, local command quality, and configurations.

Two MCP units can also be connected using a network link only. In this case, connection to an RS-232 switch panel is only required if serial IED or Master(s) are configured.

- **Hot Standby Redundancy**

Two MCP units are connected using network and optional Primary and backup serial links. In Hot standby redundancy, two MCP units are kept in constant synchronization with respect to their real-time databases. Connection to an RS-232 switch panel is optional. Connection to an RS-232 switch panel is required only if serial IED or Master(s) are configured.

- **Stand-Alone** (No Redundancy)

Once configured, redundant systems use the MCP Configuration Manager to synchronize configuration between the two MCP units, ensuring both are configured identically. In addition, the Automated Record Retrieval Manager (ARRM) provides redundancy support.

Serial connections include the redundancy settings listed in the Redundancy Dedicated Link and Redundancy Switch Panel sections.

The Redundancy Manager supervises the operational state and state transitions of the MCP units in redundant mode. See the Operational States and System Points sections for details.

Hybrid Model for MCP Redundancy

The MCP allows the user to select the system redundancy mode; that is, either:

- Hot Standby or
- Warm Standby/Standalone

When system redundancy is set to Hot Standby mode, the user can only configure and run a specific list of applications. The MCP Configuration Tool (mcpcfg/settings GUI) provides an option to select the system redundancy mode as Hot Standby or Warm Standby/Standalone. Accordingly, the MCP Configuration HMI tool only displays the applications that are supported to run in Hot Standby mode.

When system redundancy is set to Warm Standby/Standalone mode, the user can configure and run all the MCP applications in Warm Standby or Standalone mode.

Applications Available with MCP Redundant Operation

This table lists the MCP applications that are available with each redundancy type.

NOTICE Not all protocols are supported in the various Redundancy modes.

Carefully review product documentation and configure Redundancy accordingly.

Table 6.77: MCP Applications - Redundancy

Application Name	Available with this Redundancy Mode		License required
	Warm Standby	Hot Standby	
Client Application (DCA)			
DNP3	✓	✓	
Generic ASCII	✓	✗ Not Available	
IEC® 60870-5-101+104	✓	✗ Not Available	
IEC 60870-5-103	✓	✗ Not Available	

Application Name	Available with this Redundancy Mode		License required
	Warm Standby	Hot Standby	
IEC 61850	✓	✓	Yes
SEL Binary	✓	✗ Not Available	
MODBUS Multi-drop®	✓	✓	
MODBUS TCP/SSMODBUS TCP®	✓	✓	
SSMODBUS TCP/SSH®	✓	✓	
D.20 (available only in non redundant mode in this release)	✗ Not Available	✗ Not Available	
SNMP	✓	✗ Not Available	
Server Application (DPA)			
IEC 60870-5-101+104	✓	✗ Not Available	
DNP3	✓	✓	
MODBUS®	✓	✗ Not Available	
Automation Application (DTA)			
Alarm	✓	✓	
Calculator	✓	✓	
Data Logger	✓	✗ Not Available	
System Point Manager	✓	✓	
LogicLinx®	✓	✓	Yes
ARRM (Automated Record Retrieval Manager)	✓	✗Not Available	Yes
Load Shed and Curtailment	✓	✗ Not Available	
Tools/Utilities			
Runtime HMI	✓	✓	
Online Configuration Tool	✓	✓	
Offline Configuration Tool	✓	✓	
System Utilities	✓	✓	
System Point Database	✓	✓	
HMI Access Manager	✓	✓	
User Management	✓	✓	
One-Line Designer & Viewer	✓	✓	Yes
IEC 61850 Loader	✓	✓	Yes
Secure Enterprise Connectivity	✓	✓	
HAMA	✓	✗ Not Available	

For details, see the following sections:

Operational States
System Points
Redundancy Manager Pseudo Points
Non-Sync Mode
Validating the Redundant Connections
Changeover during Standby Start-up
Data Synchronization
Ethernet Connections
Sync Config Operation
HMI User Access Privileges on Redundant System
Error Messages and Troubleshooting
Configure the MCP for Redundancy
Redundancy Dedicated Link
Redundancy Switch Panel
MCP Configuration Manager

Redundancy Summary

Table 6.78: Redundancy Summary

Component	Warn Standby Redundancy	Hot Standby Redundancy
MCP Redundancy Manager	The MCP Redundancy Manager is responsible for managing communications between the two MCP units and the RS232 Redundancy Switch Panel. It also controls data synchronization and state changes.	The MCP Redundancy Manager is responsible for managing Heart Beat communications between the two MCP units, and the RS232 switch panel. It also controls system state changes. The MCP Redundancy Manager does not perform data synchronization from active unit to standby. Each application on an active unit directly communicates to its standby counterpart for data synchronization.
Redundancy Serial Port Settings	Two serial ports on each MCP are dedicated to redundancy-related communications: **Redundancy Dedicated Link** - Links the two MCP units together through the ping cable. This is optional in Warm Standby redundancy. **Redundancy Switch Panel** – Connects each MCP unit to the RS232 switch panel through the watchdog cable. This is optional in Warm Standby redundancy.	Up to three serial ports on each MCP are dedicated to redundancy-related communications: **Redundancy Dedicated Link** - Links the two MCP units together through the ping cable (Primary and backup serial link). This is optional in Hot Standby redundancy. **Redundancy Switch Panel** – Connects each MCP unit to the RS232 switch panel through the watchdog cable. This is optional in the Hot Standby redundancy.
MCP Configuration Manager	The MCP Configuration Manager allows you to synchronize configurations between two MCP units. The MCP redundancy application uses this tool to manage the synchronization of configuration files between the active and standby units to ensure both units are configured identically.	
Gateway Configuration Utility – Redundancy	The Gateway Configuration Utility is a tool accessed through the command line/settings GUI of the MCP. The Redundancy section of this utility is used to configure the parameters of the redundancy application.	

Operational States

The MCP Redundancy Manager supervises the operational state and state transitions of the MCP units in redundant mode. The following states are possible:

MCP Redundancy Manager Operational States

Table 6.79: MCP Redundancy Manager Operational States

Field	Description
Active	The unit is active and performing all the standard functions of a MCP.
Standby	The unit is connected to another MCP unit that is in active mode and is ready to assume active mode in the event of a failure of the other MCP unit or a manual change over request.
Non-redundant	The MCP is placed in this mode when redundancy is disabled through the *mcpcfg* utility/settings GUI or when a configuration error is detected. In this state, the MCP ignores the RS232 switch panel and the other MCP unit. All redundancy related system points and functions are disabled.
Failed	The MCP has entered an unrecoverable state and all software functions have been suspended. The unit must be serviced or restarted to restore functionality.
Service	While in service mode, MCP units do not accept change-over requests. The standby unit enters the Service mode during Sync Config operation and re-initialization.
Non-Sync	If the firmware or configuration of the Standby unit is not the same as that of the active unit, the standby unit enters Non-Sync mode. In non-sync mode, no application is started on the standby unit. The Redundancy Manager on both units maintains communications and responds to user commands initiated on the active unit normally (Configuration Sync, Switch-over, Reboot, etc.). See Non-Sync Mode for more details.

MCP Redundancy Configuration Combinations

The MCP can be configured to operate in Warm Standby or Hot Standby redundancy mode. The table below summarizes the various configuration combinations that are possible.

Table 6.80: MCP Redundancy Configuration Combinations

Scenario Number	Behavior	Required configurations			
		"mcpcfg" (13>10) /Settings GUI Switch Panel Type	"mcpcfg" (13>3>3) /Settings GUI Heart Beat Mechanism	"Connections" Redundancy Switch Panel	"Connections" Redundancy Serial Dedicated Link ("PING")
1	Switch panel must be present and powered up; it dictates Active/Standby. "PING" link is serial and must be present.	MASTER	Only Serial	YES	YES
2	Switch panel must be present and powered up; it dictates Active/Standby. "PING" link is LAN and must be present.	MASTER	Only LAN	YES	NO
3	Switch panel must be present and powered up; it dictates Active/Standby. "PING" link is serial plus LAN and at least one must be present.	MASTER	Combinations of Serial and LAN	YES	YES
4	Switch panel is present but does NOT dictate Active/Standby and Switch panel button is not operational. Active/Standby is set in software via communications between MCPs. "PING" link is serial and must be present.	SLAVE	Only Serial	YES	YES
5	Switch panel is present but does NOT dictate Active/Standby and Switch panel button is not operational. Active/Standby is set in software via communications between MCPs. "PING" link is LAN and must be present.	SLAVE	Only LAN	YES	NO
6	Switch panel is present but does NOT dictate Active/Standby and Switch panel button is not operational. Active/Standby is set in software via communications between MCPs. "PING" link is serial plus LAN and at least one must be present.	SLAVE	Combinations of Serial and LAN	YES	YES
7	Switch panel is not present. Active / Standby is set in software via communications between MCPs. "PING" link is serial and must be present. Serial IED or Master(s) are not configured.	SLAVE	Only Serial	NO	YES
8	Switch panel is not present. Active / Standby is set in software via communications between MCPs. "PING" link is LAN and must be present. Serial IED or Master(s) are not configured.	SLAVE	Only LAN	NO	NO
9	Switch panel is not present. Active / Standby is set in software via communications between MCPs. "PING" link is serial plus LAN and at least one must be present. Serial IED or Master(s) are not configured.	SLAVE	Combinations of Serial and LAN	NO	YES

10	Switch panel is not present. Active / Standby is set in software via communications between MCPs. "PING" link is serial and must be present. Serial IED or Master(s) are configured.	SLAVE	Only Serial	YES	YES
11	Switch panel is not present. Active / Standby is set in software via communications between MCPs. "PING" link is LAN and must be present. Serial IED or Master(s) are configured.	SLAVE	Only LAN	YES	NO
12	Switch panel is not present. Active / Standby is set in software via communications between MCPs. "PING" link is serial plus LAN and at least one must be present. Serial IED or Master(s) are configured.	SLAVE	Combinations of Serial and LAN	YES	YES

Expected results of above combinations

» **For scenarios numbered 1, 2, and 3:**

- Removal of the switch panel (with PING communications still valid) leaves the ACTIVE unit as ACTIVE, and the STANDBY unit never becomes ACTIVE (It may go to Fail / Service Mode, but never becomes Active).
- Removal of all PING comms (with switch panel still connected) leaves the ACTIVE unit as ACTIVE, and the STANDBY unit never becomes ACTIVE (It may go to Fail / Service Mode, but never becomes Active).

» **For scenarios numbered 4, 5, and 6:**

- Removal l of the switch panel (with PING communications still valid) does not matter. ACTIVE unit remains as ACTIVE, and the STANDBY unit remains as STANDBY.
- Removal of all PING communications (with switch panel being irrelevant if it is left connected or right connected) leaves the ACTIVE unit as ACTIVE, and the STANDBY unit is in the FAILED state.

  NOTE: For scenarios 4, 5, and 6 – the switch panel must be energized and connected at the time of MCP switchover, because the "position" of it may become out of synch if the switch panel is not present while the MCPs are switching.

» **For scenarios numbered 7, 8, and 9:**

- Removal of the switch panel (with PING communications still valid) does not matter. ACTIVE unit remains as ACTIVE, and the STANDBY unit remains as STANDBY.
- Removal of all PING communications (with switch panel being irrelevant if it is left connected or right connected) leaves the ACTIVE unit as ACTIVE, and the STANDBY unit becomes ACTIVE as well. This is because in absence of any external ACTIVE/STANDBY arbitrator (that was the Switch Panel in Master Mode in scenarios 1 to 3) and in absence of any communications between them – the two MCP units are not aware of each other's status and will be ACTIVE for the sake of delivering service.

» **For scenarios numbered 10, 11, and 12:**

- Removal of the switch panel (with PING communications still valid) does not matter. The ACTIVE unit remains as ACTIVE, and the STANDBY unit remains as STANDBY. However, the ACTIVE unit is not able to connect to Serial IED or Master(s).
- Removal of all PING communications (with the RS232 switch panel being irrelevant if it is left-connected or right-connected) leaves the ACTIVE unit as ACTIVE, and the STANDBY unit becomes ACTIVE as well. This is due to in absence of any external ACTIVE/STANDBY arbitrator (that was the Switch Panel in Master Mode in scenarios 1 to 3) and in absence of any communications between them – the two MCP units are not aware of each other's status and will be ACTIVE for the sake of delivering service.

NOTE: Customers can configure up to 3x PING separate channels, to provide multiple PING link availability; this impacts scenario 6 and 9.

Important Notes

- If a customer wants to control ACTIVE/STANDBY from the mechanical toggle button on the switch panel, then the configuration must be 1, 2, 3 (MASTER switch panel in mcpcfg/Settings GUI). And in this case, the arbitration ACTIVE/STANDBY is done by the switch panel.
- When the switch panel is configured as SLAVE, from the toggle mechanical button on the switch panel doesn't do anything. This is because in the case SLAVE Mode either ACTIVE/STANDBY doesn't get any control from the mechanical toggle button on the switch panel and the switch panel in this case should not be used as an arbitrator (SLAVE).
- If redundancy is configured as Master, it is mandatory to configure the switch panel through the **Configuration** > **Connection** tab in the DS Agile Studio.
- It is strongly recommended to use redundant Heart Beat links when the Switch panel is present in SLAVE mode or not present at all. This means that scenarios 4, 5, 7, 8, 10 and 11 are NOT recommended.
- It is strongly recommended that LAN Heart Beat links be configured on the Net interface that is connected to the substation LAN. This means that a dedicated Net interface for the Heart Beat link is NOT recommended. This will ensure that one MCP will be isolated from the substation LAN if the Heart Beat link fails.

Configure the MCP for Redundancy

The MCP can be configured to operate in Warm Standby or Hot Standby redundancy mode.

NOTICE Do not share the root user's password and do not forget it; this is crucial information.

No method is available to regenerate a lost password.

NOTE: Depending upon the users usability the options of enter or select can be varied from mcpcfg/Setting GUI.

Prerequisites

To set up two MCPs for redundant operation, the following is required:

- Two MCPs running same Firmware Production Build
- An SSH client: Secure Terminal Emulator from DS Agile MCP Studio
- KVM set connected to the MCPs

Configure Warm-Standby redundancy

» Task 1: Warm standby - Configure the MCPs for operation:

Set up both MCPs for operation. Refer to section: "Connecting to the MCP for the first time" of the MCP Substation Gateway Instruction Manual (994-0152).

» Task 2: Warm standby - Connect the MCPs:

1. Connect to the MCPs (Gateway A and Gateway B) through a secure shell client.
2. Enter the admin login credentials.
3. Login to and start the mcpcfg local MCP configuration utility. You can also use the Local HMI available to login to and start mcpcfg.

» Task 3: Warm standby - Create user accounts:

To configure redundancy, both MCPs are required to have a user account. Skip this task if a user account has already been created.

Tip: In the following procedures, the term "enter" indicates that the menu item number is typed in and then the **Enter** key is pressed.

1. At the MCP#>> prompt, enter **mcpcfg** if you are a root user. Otherwise, enter **sudo mcpcfg** and give login admin user password.
   Result: The Gateway Configuration Utility Menu appears.
2. Enter **1. Configure Authentication**.
   Result: The Gateway Configuration Utility Menu - Authentication menu appears.
3. Enter **3. Administrator Group Users**.
   Result: The Gateway Configuration Utility Menu - Admin Group Users menu appears.
4. Enter **2. Add User**.
   Result: The Gateway Configuration Utility Menu - Admin Group Users - Add User in Group command details appear.
5. Enter the desired user name.
6. Enter the password, conforming to the password security rules.
7. Repeat this task to add a new user in the second MCP.

» Task 4: Warm standby - Configure the Primary MCP for redundancy:

1. Navigate back to the main mcpcfg menu.
   Result: The Gateway Configuration Utility Menu appears.
2. Enter **13. Redundancy**.
   Result: The Gateway Configuration Utility Menu - Redundancy menu appears.
3. Enter **1. Current Configuration** to view the Current Redundancy Configuration.
4. Enter **2. Enable/Disable Redundancy**.
   - Enter **Y** to enable Redundancy.
     Result: You are prompted for the redundancy type.
   - Enter **1. Warm Standby** to configure the MCPs in Warm-Standby mode.
   - Enter **Y** to confirm your selection.
5. Enter **3. Heart Beat Configuration**.
   Result: The Gateway Redundancy Configuration Menu - Heart Beat Configuration Parameters menu appears.
   - Enter **1. Configure Heart Beat Timeout**.
     - Enter a value for the **Heart Beat Timeout** (in milliseconds) within the suggested range (100 to 1000 milliseconds).
     - Enter **Y.** To save the changes.
   - Enter **2. Configure Heart Beat Retries**.
     - Enter the number of **Heart Beat Retries** within the suggested range (1 to 10).
     - Enter **Y.** To save the changes.
   - Enter **3. Configure Heart Beat Communication Mechanism**.
     Result: The Gateway Redundancy Configuration Menu - Heart Beat Mechanism menu appears.
     - Select the required Heart Beat Mechanism by selecting one of the options from the below menu:
       1. **Serial Only**

2. **Single LAN**
3. **LAN1 and LAN2**
4. **LAN and Serial**
5. **LAN1, LAN2 and Serial**

- If the option is either **1 or 4 or 5,** select the required **Heart Beat Mechanism,** then follow the below steps to configure the Serial Ports:
  1. Navigate to **DS Agile MCP Studio -> Connections -> Serial Connections**.
  2. Add a **New connection**.
  3. Select the **Serial Connection.**
  4. Select the **Redundancy Dedicated Link** type.
  5. Select the **Primary** and **Backup Port** settings.
  6. Enable the **Auto Start** configuration parameters.
  7. **Save** and **Commit Changes.**
- If the option is either **2 or 3 or 4 or 5,** select the required **Heart Beat Mechanism.**
  1. Enter **Y** to save the settings.

6. Navigate back to the Redundancy menu.
7. Enter **4. Configure IP Address of PEER MCP**.
   - Enter **1. Configure/Update PEER IP Address**.
     - Enter the new Primary address of the PEER MCP.
     - If a Secondary IP for the PEER MCP is available, enter the new Secondary IP Address.
     - Confirm the Primary and Secondary IP Address changes by entering **Y**.
   - Enter **2. Delete PEER IP Address**
     - Enter **1** to **Delete Secondary IP**
     - Enter **2** to **Delete Both Primary and Secondary IPs**
8. Enter **5. UserName of PEER MCP**.
   - Enter the username defined by you earlier in the PEER MCP.
9. Navigate back to the Gateway Configuration Utility Menu - Redundancy menu.
10. Enter **6. Configure Time Sync with Standby**. (Optional)
    - Skip this option if both MCPs are already in time-sync through other means (for example, IRIG-B or NTP).
11. Enter **7. Configure Enable/Disable DTAs in Standby**

    NOTE: This parameter is not applicable for Warm Stand Redundancy.
12. Enter **8. Configure Gateway A/B Designation**.
    - If Switch Panel is configured (master), Gateway A/B Designation is read from the Switch Panel (i.e. user configuration is disabled).
    - If Switch Panel is not configured (slave), enter **1. Gateway_A** to select the Gateway Designation.

    Result: Gateway A/B Designation changed to **Gateway_A**.
13. Enter **9. Setup Public Key Authentication with PEER MCP**.

    NOTE: LAN based Heart Beat Mechanism is not applicable for **"Serial Only" Heart Beat Mechanism.**
    - Enter **Y** to copy the public key of this MCP to PEER the MCP.
    - Enter the password of the user defined in the PEER MCP. This option exchanges the public and private keys.

14. Enter **10. Configure Switch Panel Type**.

    NOTE: This option is not applicable if switch panel is not configured.

    - Select Switch Panel Type Configuration:
      1. **MASTER**
      2. **SLAVE**
    - Enter **1 or 2.**
    - Navigate to **DS Agile MCP Studio -> Connections -> Serial Connections**.
    - Add a **New connection**.
    - Select the **Serial Connection.**
    - Select the **Redundancy Switch Panel** type.
    - Select the **Primary Port** settings.
    - Enable the **Auto Start** configuration parameters.
    - **Save** and **Commit Changes.**
15. Navigate back to the Gateway Configuration Utility Menu – Redundancy menu.
16. Enter **11. Enable/Disable Non-Sync mode**

    NOTE: This parameter is not applicable for Warm Stand Redundancy.
17. Navigate back to the Gateway Configuration Utility Menu.
18. Enter **24. Reboot Device** and wait for a minute.
    Result: This command:
    - Restarts all the applications and runs them in Warm-Standby mode.
    - Starts the ACTIVE MCP in Warm Standby Mode.

    Result: After the first MCP is configured, it enters the Active mode.
19. Login to the PEER MCP and execute **mcpcfg**.
20. Repeat the steps of this task to configure the PEER MCP.

» Task 5: Warm standby - Configure the Secondary MCP for redundancy:

1. Navigate back to the main mcpcfg menu.
   Result: The Gateway Configuration Utility Menu appears.
2. Enter **13. Redundancy**.
   Result: The Gateway Configuration Utility Menu - Redundancy menu appears.
3. Enter the remaining configuration settings to be identical to the Primary MCP. See **Task 4: Warm standby - Configure the Primary MCP for redundancy**.
4. Enter **8. Gateway A/B Designation**.
   - If Switch Panel is configured (master), Gateway A/B Designation is read from the Switch Panel (i.e. user configuration is disabled).
   - If Switch Panel is not configured (slave), enter **2. Gateway_B** to select the Gateway Designation.

   Result: Gateway A/B Designation changed to **Gateway_B**.
5. Enter **24. Reboot Device** and wait for a minute.
   Result: All the MCP applications are restarted and run in Warm-Standby mode.

This MCP (Gateway_B) communicates to the PEER MCP (Gateway_A) and declares itself to be the Standby MCP since the PEER MCP is already in Active mode.

» Task 6: Warm standby - Verify configuration:

1. At the command prompt of the Primary MCP, enter **mcpcfg**.
2. Enter **13. Redundancy**.
3. Enter **1. Current Configuration**.
4. Repeat the steps of this task for the Secondary MCP.
5. Compare the Primary and Secondary configurations.

» Task 7: Warm standby - Verify redundant MCP operation:

1. Login to MCP remote-HMI and enter credentials.
2. Click **Point Details** button.
3. Click the **Application** tab.
4. Click **Redundancy Manager Details**.
5. Repeat the steps of this task for the Secondary MCP.
6. Compare the configurations.
7. Confirm that the State of PEER MCP pseudo point is Standby.

Configure Hot-Standby redundancy

Before configuring the MCPs for Warm-Standby redundancy, ensure that the listed Prerequisites on page 419 are on-hand.

» Task 1: Hot standby - Configure the MCPs for operation:

Set up both MCPs for operation. Refer to section: “Connecting to the MCP for the first time” of the G500 Substation Gateway Instruction Manual (994-0152) or G100 Substation Gateway Instruction Manual (994-0155).

» Task 2: Hot standby - Connect the MCPs:

1. Connect to the MCPs (Gateway A (MCP) and Gateway B (MCP)) through a secure shell client.
2. Enter the admin login credentials.
3. Login to and start the mcpcfg local MCP configuration utility. You can also use the Local HMI available to login to and start mcpcfg.

» Task 3: Hot standby - Create user accounts:

Creation of user accounts follows the same procedure whether it is for hot standby or warm standby redundancy. See the procedure in section: **Task 3: Warm standby - Create user accounts**.

» Task 4: Hot standby - Configure the Primary MCP for redundancy:

1. Navigate back to the main mcpcfg menu.
   Result: The Gateway Configuration Utility Menu appears.
2. Enter **13. Redundancy**.
   Result: The Gateway Configuration Utility Menu - Redundancy menu appears.
3. Enter **1. Current Configuration** to view the Current Redundancy Configuration.
4. Enter **2. Enable/Disable Redundancy**.
   - Enter **Y** to enable Redundancy.
     Result: You are prompted for the redundancy type.
   - Enter **2. Hot Standby** to configure the MCPs in Hot-Standby mode.
   - Enter **Y** to confirm your selection.

5. Enter **3. Heart Beat Configuration**.
   Result: The Gateway Redundancy Configuration Menu - Heart Beat Configuration Parameters menu appears.
   - Enter **1. Configure Heart Beat Timeout**.
     - Enter a value for the **Heart Beat Timeout** (in milliseconds) within the suggested range (100 to 1000 milliseconds).
     - Enter **Y.** To save the changes.
   - Enter **2. Configure Heart Beat Retries**.
     - Enter the number of **Heart Beat Retries** within the suggested range (1 to 10).
     - Enter **Y.** To save the changes.
   - Enter **3. Configure Heart Beat Communication Mechanism**.
     Result: The Gateway Redundancy Configuration Menu - Heart Beat Mechanism menu appears.
     - Select the required Heart Beat Mechanism by selecting one of the options from the below menu:
       1. **Single LAN**
       2. **LAN1 and LAN2**
       3. **LAN and Serial**
       4. **LAN1, LAN2 and Serial**
     - Enter **1. Single LAN** (the default value).
       1. Enter **Y** to save the settings.
     - If the option is either **3 or 4,** select the required **Heart Beat Mechanism,** then follow the below steps to configure the Serial Ports:
       1. Navigate to **DS Agile MCP Studio -> Connections -> Serial Connections**.
       2. Add a **New connection**.
       3. Select the **Serial Connection.**
       4. Select the **Redundancy Dedicated Link** type.
       5. Select the **Primary** and **Backup Port** settings.
       6. Enable the **Auto Start** configuration parameters.
       7. **Save** and **Commit Changes.**
6. Navigate back to the Redundancy menu.
7. Enter **4. Configure IP Address of PEER MCP**.
   - Enter **1. Configure/Update PEER IP Address**.
     - Enter the new Primary IP Address of the PEER MCP.
     - If a Secondary IP for the PEER MCP is available, enter the new Secondary IP Address.
     - Confirm the Primary and Secondary IP Address changes by entering **Y**.
8. Enter **5. UserName of PEER MCP**.
   - Enter the username defined by you earlier in the PEER MCP.
9. Enter **6. Configure Time Sync with Standby**. (Optional)
   - Skip this option if both MCPs are already in time-sync through other means (for example, IRIG-B or NTP).
10. Enter **7. Configure Enable/Disable DTAs in Standby**.
    Result: The Gateway Redundancy Configuration Menu - Enable/Disable DTAs on Standby menu appears.
    - If the "Enable/Disable DTAs in Standby" parameter is set to Enabled, the LogicLinx, Calculator and Enhanced Automation DTAs run normally on the standby MCP. If this parameter is set to

Disabled, these applications suspend processing on the standby MCP and resume normal operations when the MCP state becomes active.

- Skip this option if DTA applications (that is, automation applications such as LogicLinx, Calculator, Enhanced Automation) on the Standby MCP are to run (default option).

11. Enter **8. Configure Gateway A/B Designation**.
    - If Switch Panel is configured (master), Gateway A/B Designation is read from the Switch Panel (i.e. user configuration is disabled).
    - If Switch Panel is not configured, enter **1. Gateway_A** to select the Gateway Designation.

    Result: Gateway A/B Designation changed to **Gateway_A**.
12. Enter **9**. Setup Public Key Authentication with PEER MCP.
    - Enter **Y** to copy the public key of this MCP to PEER the MCP.
    - Enter the password of the user defined in the PEER MCP. This option exchanges the public and private keys.
13. Enter **10. Configure Switch Panel Type**.
    NOTE: This option is not applicable if switch panel is not configured.
    - Select Switch Panel Type Configuration:
      1. **MASTER**
      2. **SLAVE**
    - Enter **1 or 2.**
    - Navigate to **DS Agile MCP Studio -> Connections -> Serial Connections**.
    - Add a **New connection**.
    - Select the **Serial Connection.**
    - Select the **Redundancy Switch Panel** type.
    - Select the **Primary Port** settings.
    - Enable the **Auto Start** configuration parameters.
    - **Save** and **Commit Changes.**
14. Enter **11. Enable/Disable Non-Sync mode.**
    - Default option: The MCP in Hot-Standby mode runs with Non-Sync Mode Enabled. You can disable this mode.
      Enter either:
      - **Y** to disable Non-Sync Mode.
      - **N** to continue operation with the default option (Non-Sync mode enabled).
15. Navigate back to the main menu.
16. Enter **24. Reboot Device** and wait for a minute.
    - Restarts all the applications and runs them in Hot-Standby mode.
    - Starts the ACTIVE MCP in Hot Standby Mode.

    Result: After the first MCP is configured, it enters the Active mode.
17. Login to the PEER MCP and execute **mcpcfg**.
18. Repeat the steps of **Task 4: Hot standby - Configure the Primary MCP for redundancy** to configure the PEER MCP.

» Task 5: Hot standby - Configure the Secondary MCP for redundancy:

1. Navigate back to the main mcpcfg menu.
   Result: The Gateway Configuration Utility Menu appears.
2. Enter **13. Redundancy**.
   Result: The Gateway Configuration Utility Menu - Redundancy menu appears.

3. Enter the remainder of the configuration settings identical to the Primary MCP. See **Task 4: Hot standby - Configure the Primary MCP for redundancy**.
4. Enter **8. Gateway A/B Designation**.
   - If Switch Panel is configured (master), Gateway A/B Designation is read from the Switch Panel (i.e. user configuration is disabled).
   - If Switch Panel is not configured (slave), enter **2. Gateway_B** to select the Gateway Designation.

   Result: Gateway A/B Designation changed to **Gateway_B**.
5. Enter **24. Reboot Device** and wait for a minute.
   Result: All the MCP applications are restarted and run in Hot-Standby mode.

This MCP (Gateway_B) communicates to the PEER MCP (Gateway_A) and declares itself to be the Standby Gateway since the PEER MCP is already in Active mode.

» Task 6: Hot standby - Verify configuration:

1. At the command prompt of the Primary MCP, enter **mcpcfg**.
2. Enter **13. Redundancy**.
3. Enter **1. Current Configuration**.
4. Repeat the steps of this task for the Secondary MCP.
5. Compare the Primary and Secondary configurations.

» Task 7: Hot standby - Verify redundant MCP operation:

1. Login to MCP remote-HMI and enter credentials.
2. Click **Point Details** button.
3. Click the **Application** tab.
4. Click **Redundancy Manager Details**.
5. Repeat the steps of this task for the Secondary MCP.
   If the State of PEER MCP point is Non-Sync, then synchronize the configuration by entering the DirectOperate -> PulseOn command on the SyncConfig point.
6. Compare the configurations.
7. Confirm that the State of PEER MCP pseudo point is Standby.

System Points

When running in active mode, the application provides indications through the following digital input system points:

MCP Redundancy Manager Digital Input Points

Table 6.81: MCP Redundancy Manager Digital Input Points

Field	Description
SystemRedundant	TRUE if the MCP is configured to be redundant FALSE if the MCP is not redundant
StandbyGatewayCommFail	TRUE if communications with the redundant MCP unit have failed FALSE if communications with the redundant MCP unit have not failed OFFLINE and INVALID if the MCP is in non-redundant mode

Field	Description
StandbyGatewayinServiceMode	TRUE if the standby MCP is in service mode FALSE if the standby MCP is not in-service mode OFFLINE and INVALID if the MCP is in non-redundant mode
StandbyGatewayNotAvailable	TRUE if the standby MCP is in failed mode False if the standby MCP is not in failed mode OFFLINE and INVALID if the MCP is in non-redundant mode
GatewayAActive	TRUE if the MCP has been designated as unit "A" (See note) OFFLINE and INVALID if the MCP is in non-redundant mode
GatewayBActive	TRUE if the MCP has been designated as unit "B" OFFLINE and INVALID if the MCP is in non-redundant mode
Config Sync in Progress	TRUE if configuration synchronization is currently in progress FALSE if configuration synchronization is not currently in progress OFFLINE and INVALID if the MCP is in non-redundant mode
Standby Config Out of Sync	TRUE if the configurations on the active and standby MCPs do not match FALSE if the configurations on the active and standby MCPs do match OFFLINE and INVALID if the MCP is in non-redundant mode
HotstandbyDisabled	TRUE if Hot Standby redundancy is disabled, i.e., Warm Standby redundancy is enabled. FALSE if Hot Standby redundancy is enabled OFFLINE and INVALID if the MCP is in non-redundant mode
Standby Code Out of Sync	FALSE when the firmware on the Primary device is the same as that on the backup device TRUE when the firmware on the Primary device is not the same as that on the backup device OFFLINE and INVALID if the MCP is in non-redundant mode

NOTE: If a RS232 switch panel is configured, the MCP is designated as unit A or B depending on the input block it is wired to on the RS232 switch panel. If RS232 switch panel is not configured, designation of both units must be configured using local Gateway Config Utility (See Redundancy).

The state of both units in redundant configuration is provided through the following analog input system points:

MCP Redundancy Manager Analog Input Points

Table 6.82: MCP Redundancy Manager Analog Input Points

Field	Description
State of This Gateway	State of unit where point summary is open. State is one of the Operational States (see Operational States). State is presented in enumerated text.
State of PEER Gateway	State of another unit. State is one of the Operational States (see Operational States). State is presented in enumerated text.
A/B Designation of the Gateway	Designation of the current Gateway

In addition to these indications, the following control points are available as digital outputs:

MCP Redundancy Manager Digital Output Points

Table 6.83: MCP Redundancy Manager Digital Output Points

Field	Description
StartChangeOver	Triggers a change-over – the active MCP moves to standby mode while the standby MCP takes over the active mode. If you are logged into the online GUI of the active MCP when a changeover occurs, the browser window closes, and you are required to log in again. OFFLINE and INVALID if the MCP is in non-redundant mode.
RestartActive	Requests a restart of all software on the active MCP. **NOTE**: This operation does not cause fail-over. The active MCP comes back as active after restart of all applications.
RestartStandby	Requests a restart of all software on the standby MCP. OFFLINE and INVALID if the MCP is in non-redundant mode.
RebootActive	Requests a reboot of the active MCP. **NOTE**: This operation causes fail-over. The active MCP comes back as standby after reboot operation.
RebootStandby	Requests a reboot of the standby MCP. OFFLINE and INVALID if the MCP is in non-redundant mode.
SyncConfig	Requests that the configuration of the standby MCP be synchronized with that of the active unit. OFFLINE and INVALID if the MCP is in non-redundant mode. NOTE: This operation automatically restarts software (applications) on the standby MCP to allow applications to take new configuration. If a change to system configuration is synchronized to the standby MCP, a manual reboot of standby unit is required. This operation can be performed using the "RebootStandby" point after SyncConfig operation is over. (See Changeover during Standby Start-up.) Standby takes time to initialize and sync initialized data either during start-up or after changeover. During this time, changeover is not allowed, and a message is logged when a changeover command is issued. Changeover can be issued only after 180 seconds in case of standby start-up. A second changeover can be issued only after 30 seconds of the first changeover.
ShutdownActive	Requests shutdown of active MCP. **NOTE**: This DO should be used to shutdown active MCP gracefully before powering it off. This prevents data corruption on SSD.
ShutdownStandby	Requests shutdown of standby MCP. OFFLINE and INVALID if the MCP is in non-redundant mode. **NOTE**: This DO should be used to shutdown standby MCP gracefully before powering it off. This prevents data corruption on SSD.

You may issue any control operation on these points to initiate the request associated with the point. Upon receiving a control operation, the Redundancy Manager momentarily changes the state of the digital output to ON then OFF.

All local commands on indication and control points are rejected.

Non-Sync Mode

If the firmware or configuration of the standby unit is not the same as that of the active unit, the standby unit enters non-sync mode at start up.

Non-Sync Mode is only applicable to Hot-Standby Redundancy.

The **Standby Config Out of Sync** digital input point indicates if the configuration on the standby unit does not match with the active unit.

The **Code Out of Sync** digital input point indicates if the firmware on the standby unit does not match with the active unit.

In non-sync mode, no application is started on the standby unit. The Redundancy Manager on both units maintains communications and responds to user commands initiated on the active unit normally (Sync Config, Change-over, Reboot Active, Reboot Standby, Restart Active, Restart Standby, Shutdown Active, and Shutdown Standby).

The non-sync mode of standby unit can be disabled using MCP Config Utility (see Enable/Disable Non-Sync mode).

NOTICE If change-over operation is performed while the standby unit is in non-sync mode, the standby unit changes to active, and the active unit enters non-sync mode.

Validating the Redundant Connections

Once you have configured your redundant setup, you should test the system to ensure that redundancy has been properly configured.

» **To validate a redundant system:**

1. Log into the online HMI of the active MCP unit.
2. Click the **Point Details** button on the toolbar.
3. Under the **Application** tab, click the **Details** button for **RedunMgr**.
4. Select the **Analog Input** tab and verify that the points are in the following states:

Point Name	Quality	Value
State of This Gateway	Online	Active
State of PEER Gateway	Online	Standby
A/B Designation of the Gateway	Online	Gateway_A

NOTE: If the state of this Gateway is Active Non-Redundant, check diagnostic logs for the "B034" application for any configuration issues.

NOTE: If the state of PEER Gateway is non-sync, see Non-Sync Mode.

5. Select the **Digital Input** tab and verify that the points are in the following states:

Point Name	Quality	Value
SystemRedundant	Online	1 if both MCP's are Redundant 0 if Both MCP's are non Redundant
StandbyGatewayCommFail	Online	0 if Communication between both MCP's is ok 1 If communication between both MCP's is not OK
StandbyGatewayinService Mode	Online	0 Standby MCP is not in service mode 1 Standby MCP is in Service mode
StandbyGatewayNotAvailable	Online	0 Standby MCP Available 1 Standby MCP Failed
GatewayAActive	Online	1 if you are connected to Gateway A (MCP) 0 if you are connected to Gateway B (MCP) (See note)
GatewayBActive	Online	1 if you are connected to Gateway A (MCP)

Point Name	Quality	Value
		0 if you are connected to Gateway B (MCP) (See note)
Config Sync in Progress	Online	0 Configuration sync to peer MCP not in Progress 1 Configuration sync to peer MCP is in Progress
Standby Config Out of Sync	Online	0 if both MCPs have the same configuration 1 if both MCPs have a different configuration
Hot Standby Disabled	Online	0 in case of Hot Standby 1 in case of Warm Standby
Standby Code Out of Sync	Online	0 if both MCPs have the same code 1 if both MCPs have a different code

NOTE: If a switch panel is used, and if *MCPA Active* and *MCPB Active* remain fixed at 0 or 1 regardless of the position of the A/B switch on the RS232 panel, ensure that the RS232 adapter cards containing the redundancy control ports are set to the **DTE** position. Refer to *Switch SW1/SW2 Configuration* and *Switch SW3/SW4 Configuration* in the *G500 Substation Gateway Instruction Manual (994-0152) or G100 Substation Gateway Instruction Manual (994-0155)* for more information.

6. Select the **Digital Output** tab and verify that all points are online and have a value of zero.

Changeover during Standby Start-up

Standby takes time to initialize and sync initialized data either during start-up or after changeover. During this time, changeover is not allowed, and a message is logged when a changeover command is issued. Changeover can be issued only after 180 seconds in case of standby start-up. A second changeover can be issued only after 30 seconds of the first changeover.

Data Synchronization

Hot Standby

In Hot Standby redundancy, two MCP devices are kept in constant synchronization with respect to their real-time databases. The following data is automatically synchronized to the standby MCP:

Real time databases

Events from IEDs

Alarm and SOE databases

Local commands that have been applied to individual system points (control inhibit, scan inhibit, local force, etc.)

Acknowledgements from the Master station to server application, to delete an event from event queues

Application internal data to start an application from the same state in the event of change-over

This data is synchronized between the units through the network connection.

Warm Standby

In Warm standby redundancy, only the following data is automatically synchronized from the active to the standby MCP:

Accumulator running values.

ARRM files (Files which MCP extracted from IED's).

Local commands that have been applied to individual system points (control inhibit, scan inhibit, local force, etc.).

Data is synchronized between the units through the dedicated serial link. Initial states are synchronized when the active unit first begins to communicate with the standby unit. Once this initial synchronization is complete, individual events are transferred from the active unit to the standby unit as they occur in real-time.

Ethernet Connections

When you configure a pair of MCPs for redundancy, you need a total of 3 IP Addresses for the two MCPs:

One unique IP Address for each MCP

One "active" IP Address to be used by the active MCP.

The same "active" IP Address is configured in both MCPs. When a MCP is in active mode, it uses the configured "active" IP Address. In any other state, it uses its own unique IP Address. This allows external devices and master stations to use only one IP Address to access the pair of MCPs. The following table describes the possible combinations.

IP Address Combinations

Table 6.84: IP Address Combinations

Gateway A (MCP)		**Gateway B (MCP)**	
State	**IP Address**	**State**	**IP Address**
Active State	Active	Inactive State	Unique for Gateway B (MCP)
Inactive State	Unique for Gateway A (MCP)	Active State	Active
Inactive State	Unique for Gateway A (MCP)	Inactive State	Unique for Gateway B (MCP)
Active State	Active (See note)	Active State	Active (See note)

NOTE: Having both MCPs active at the same time can only be achieved if the two units are not reachable to each other via configured Heart Beat communication links. In any other scenario, the two units successfully arbitrate so that only one MCP claims the active IP Address.

This scheme requires static IP Address configuration. The MCP Redundancy solution does not support use of a DHCP server to assign dynamic IP Addresses.

If the MCPs have a Secondary Ethernet interface installed, a second set of 3 IP Addresses is assigned to that interface, using the same rules.

The MCP Hot Standby service uses 50000 and 50001 TCP ports for Heart Beat communication, data and configuration synchronization. If the two MCPs are connected through an external firewall, then inbound and outbound traffic should be allowed for 50000 and 50001 TCP ports in the external firewall.

Sync Config Operation

The active unit indicates if the configuration on the standby unit does not match with itself via the **Standby Config Out of Sync** digital input.

A Sync Config operation can be initiated from the **SyncConfig** digital output point. As part of Sync Config operation, the following configurations are synchronized:

Application configurations (for example, DNP server mappings, LogicLinx programs, etc.).

NOTE: This operation automatically resets software on the standby MCP to allow applications to take new configuration (this is, only a software restart, not a reboot of the entire device).

System configurations: System configuration refers to any configuration done through the Gateway Configuration Utility (mcpcfg/settings GUI) or User Management of online HMI (for example, time sync inputs, user logins and passwords, etc.).

NOTE: If a change to system configuration is synchronized with the standby MCP, a manual reboot of the standby unit is required. This operation can be performed using **RebootStandby** point after the SyncConfig operation is complete.

While a configuration transfer is in process, the standby unit does not accept any commands from the active unit. The active unit indicates via the **Config Sync in Progress** digital input when configuration synchronization is occurring.

During the software reset of the standby MCP, the active unit may briefly indicate that the standby unit has failed. If the standby unit remains in failed mode, or if the **Standby Config Out of Sync** digital input does not turn off after the standby unit completes the restart, then the configuration synchronization has likely failed. Check the system and diagnostic logs in both the active and standby units for details on why the synchronization did not complete.

The following parameters are not synchronized as part of Sync Config operation:

IP Addresses: They must be independently configured for each unit (see Ethernet Connections).

Redundancy Configuration: (see Redundancy)

No other data is synchronized between the two MCPs, including software licenses, or firmware images.

NOTICE Do not change the configuration of the active MCP while configuration synchronization is in progress. Changing the configuration of the active MCP may result in a configuration mismatch or configuration corruption.

HMI User Access Privileges on Redundant System

Only observer privilege level is granted to any user logging into the standby MCP. When a supervisor, admin or operator user logs into the standby MCP, his privilege level is demoted to observer.

Upon change-over from:

Active to standby, all users are forcefully logged off.

Standby to active, supervisor and operator users are forcefully logged off.

Redundancy Setup Checklist

The following checklists can be used when preparing a redundant MCP system:

Warm Standby Setup Checklist

Hot Standby Setup Checklist

Warm Standby Setup Checklist

Table 6.85: Warm Standby Setup Checklist

Task	Reference
1. Prepare two MCP units and ensure they are running the same firmware version.	*G500 Substation Gateway Instruction Manual* (GE part no. 994-0152) or G100 *Substation Gateway Instruction* Manual (994-0155)
2. Connect the MCP units to each other and to remote devices as shown in the redundancy wiring diagrams.	
3. Configure Authentication mode, Admin users and maintenance IP Address of the MCP units using mcpcfg/Settings GUI. Ensure that the maintenance IP Address is reachable over the network. User must reboot MCPs after completing this step.	Configure Authentication *Configure Network Interfaces*

4. Configure the redundancy settings on both MCP units using mcpcfg/Settings GUI. This includes configuring the Active IP Address for redundancy and type of redundancy, PEER MCP IP Address and PEER MCP username. Ensure that the active IP Address is reachable over the network.	*Configure Network Interfaces* Redundancy
5. Setup Public Key Authentication with PEER MCP. **NOTE**: This step must be performed after steps 1 to 4 are completed on both MCPs.	Redundancy > Setup public Key Authentication with PEER MCP
6. Configure the Redundancy Dedicated Link and the Redundancy Switch Panel serial connections on the Connection configuration page of the MCP's online HMI. **NOTE**: The user must reboot the MCP units after completing steps 1 to 6.	Redundancy Dedicated Link Redundancy Switch Panel
7. Validate the redundant connection to ensure that the system has been fully configured.	To validate a redundant system
8. If the *Standby Config Out of Sync* point has a value of 1, initiate configuration sync from the active unit by executing a control command on the *SyncConfig* pseudo output point of the Redundancy Manager application. After the sync operation, verify that the *Standby Config Out of Sync* point has a value of 0.	*MCP Redundancy Manager* Changeover during Standby Start-up Standby takes time to initialize and sync initialized data either during start-up or after changeover. During this time, changeover is not allowed, and a message is logged when a changeover command is issued. Changeover can be issued only after 180 seconds in case of standby start-up. A second changeover can be issued only after 30 seconds of the first changeover. Sync Config Operation

Hot Standby Setup Checklist

Table 6.86: Hot Standby Setup Checklist

Task	Reference
1. Prepare two MCP units and ensure they are running the same firmware version.	*G500 Substation Gateway Instruction Manual* (GE part no. 994-0152) or G100 *Substation Gateway Instruction* Manual (994-0155)
2. Connect the MCP units to each other and to remote devices as shown in the redundancy wiring diagrams.	
3. Configure Authentication mode, Admin users and maintenance IP Address of the MCP units using mcpcfg/Settings GUI. Ensure that the maintenance IP Address is reachable over the network. You must reboot the MCPs after completing this step.	Configure Authentication *Configure Network Interfaces*

Task	Reference
4. Configure the redundancy settings on both MCP units using mcpcfg/Settings GUI. This includes configuring Active IP Address for redundancy and type of redundancy, PEER MCP IP Address and PEER MCP username. Ensure that the active IP Address is reachable over the network.	*Configure Network Interfaces* Redundancy
5. Configure Heart Beat communication option from the available options. Ensure that both MCP units are connected, based on this parameter.	Redundancy
6. Setup Public Key Authentication with PEER MCP. **NOTE**: This step must be performed after steps 1 to 4 are completed on both MCPs.	Redundancy > Setup public Key Authentication with PEER MCP
7. If the Heart Beat communication option includes Serial link as well, configure the Redundancy Dedicated Link on the Configuration > Connection page of the DSAS Configuration. The Primary and an optional backup serial links can be configured.	Redundancy Dedicated Link
8. If a switch panel is configured, configure the Redundancy Switch Panel serial connections on the Configuration > Connection page of the DSAS Configuration. If a switch panel is not configured, designate one MCP as "A", and other as "B" using *mcpcfg/Settings GUI*. **NOTE**: The user must reboot the MCP units after completing steps 1 to 8.	Redundancy Switch Panel Redundancy *G500 Substation Gateway Instruction Manual* (GE part no. 994-0152) or G100 *Substation Gateway Instruction* Manual (994-0155) > Configure Gateway A/B Designation
9. Validate the redundant connection to ensure that the system has been fully configured.	To validate a redundant system
10. If the *Standby Config Out of Sync* point has a value of 1, initiate configuration sync from the active unit by executing a control command on the *SyncConfig* pseudo output point of the Redundancy Manager application. After the sync operation, verify that the *Standby Config Out of Sync* point has a value of 0.	*MCP Redundancy Manager* Changeover during Standby Start-up Standby takes time to initialize and sync initialized data either during start-up or after changeover. During this time, changeover is not allowed, and a message is logged when a changeover command is issued. Changeover can be issued only after 180 seconds in case of standby start-up. A second changeover can be issued only after 30 seconds of the first changeover. Sync Config Operation

Error Messages and Troubleshooting

The table below describes the possible error messages displayed by the MCP Redundancy Manager. These messages are entered in the diagnostic log of the MCP.

Common Tables

Configuration Manager Error Codes

Table 6.87: Configuration Manager Error Codes

Error Number	Cause
-1	The two MCP units are not already in sync
0	Success
1	Md5sum.txt / tar-zipped file missing in local/tar modes
2	Command line arguments are not proper
3	IP Address or target unit not provided in correct format
4	Validation of transferred configuration files failed
5	Authentication is not set or remote MCP is not accessible
6	Insufficient permissions to read from file
8	Copying of new configuration to /mnt/usr has failed.

Redundancy Manager Reason Codes

Table 6.88: Redundancy Manager Reason Codes

Technical Number	Reason Code	Description
1	B034_NACK_CHECKSUM_ERROR	corrupted message received
2	B034_NACK_HW_ERROR	some hardware problem
3	B034_NACK_SERVICE_MODE	Service mode
4	B034_NACK_SWITCH_PULL_FAIL	Switch panel hardware problem
5	B034_NACK_TOOL_TASK_TIMEOUT	System was busy or software failure
6	B034_NACK_TOOL_TASK_FAILED	Software failure

MCP Redundancy Diagnostic Error Messages

Table 6.89: MCP Redundancy Diagnostic Error Messages

Serial Number	Diagnostic Log Messages	Details
1	b034_active_proc_db_sync failed with error <error code>	Initial mSQL database synchronization failed. Quality or accumulator records may not have been transferred correctly.
2	Active: failed to pull switch towards	The active unit failed to pull the switch. The RS232 switch panel may not be powered correctly or the connection from the switch panel to the MCP may not be correct.
3	Active: Health CHK failed: Terminating Child	A software error in the MCP Redundancy Manager has occurred.
4	[ACTIVE]: Rejecting command <command type #> because other MCP is in Service Mode	The user issued a command that is not valid when the standby is in Service Mode.
5	[ACTIVE]: Rejecting command <command type #> because activity <activity type> is in progress	The user issued a command that was rejected because another activity was already in progress.

Serial Number	Diagnostic Log Messages	Details
6	[ACTIVE]: Rejecting command <command type> because other MCP is not available	The user issued a command that was rejected since the active cannot communicate with the other MCP. The other MCP may have failed or the HB communication link between the two may be disconnected.
7	[ACTIVE]: CONFIG SYNC activity response timeout waiting for response from standby	Configuration synchronization failed because the standby unit failed to respond to the active. The standby unit may have failed or the HB communication link between the two may be disconnected.
8	[ACTIVE]: Standby MCP rejected the Config Sync request with reason <reason code>	Configuration synchronization failed because the standby unit issued an error.
9	[ACTIVE]: Standby MCP failed in Config Sync using network mode	Configuration synchronization in network (Ethernet) mode has failed. The network connection between the MCPs may be disconnected, or the public/private authentication keys may not be correctly configured.
10	[ACTIVE]: Tool task failed with error = <error code>	Configuration synchronization failed because the standby unit issued an error. Review the <error code> in the table of Configuration Manager error codes.
11	[ACTIVE]: CONFIG SYNC failed due to tool task timeout	Configuration synchronization failed because the Configuration Manager software failed to respond.
12	[ACTIVE]: Standby MCP rejected the DB Sync start request with reason <reason code>	The standby unit rejected a request to synchronize either quality or accumulator data. The <reason code> is identified by a technical number. See Redundancy_Manager_Reason_Codes for the technical number (reason code) descriptions. The most common cause is that the standby unit is in service mode or has failed.
13	[ACTIVE]: Standby MCP failed in DB sync in network mode	Synchronization of either quality or accumulator tables failed to complete. The most common cause is that either communications with the standby unit have been interrupted, or the standby is in service mode or has failed.
14	[ACTIVE]: Response timeout for activity <activity type> subactivity <subactivity type>	The standby unit failed to send a response to the active unit. The numeric codes define the activity that timed out. This is a diagnostic message that only needs to be considered if there are messages indicating that something has failed.
15	Configuration read failed: Entering Active Non-Redundant mode	Check Redundancy serial ports or switch panel are not configured in the connection configuration of the MCP.
16	Redundancy is DISABLED: Entering Active Non-Redundant mode	Diagnostic message only. Redundancy is disabled in the configuration.
17	Failed to open switch panel port: Entering Active Non-Redundant mode	This message indicates a software failure of the MCP. Either the configuration files of the MCP have been corrupted or the MCP has not started properly.
18	Failed to open Heart Beat port: Entering Active Non-Redundant mode	This message indicates a software failure of the MCP. Either the configuration files of the MCP have been corrupted or the MCP has not started properly.

Serial Number	Diagnostic Log Messages	Details
19	Error in reading switch panel: Entering Active Non-Redundant mode	This message indicates a software failure of the MCP. Either the configuration files of the MCP have been corrupted or the MCP has not started properly.
20	Failed to receive initial HB from PEER MCP: Entering Active mode	The active MCP never sent a Heart Beat message to the standby, causing the standby unit to become active. Check that the active unit is functional and that the HB communication link between the two units is properly installed.
21	STATE CONFLICT: This MCP = ACTIVE and A, PEER MCP = ACTIVE and A Failing this MCP	Check the wiring of the MCP units to the switch panel
22	STATE CONFLICT: This MCP = ACTIVE and A, PEER MCP = ACTIVE and B PEER MCP should fail	Check the wiring of the MCP units to the switch panel
23	STATE CONFLICT: This MCP = ACTIVE and B, PEER MCP = ACTIVE Failing this (B) MCP	Check the wiring of the MCP units to the switch panel
24	STATE CONFLICT: This MCP = STANDBY and A, PEER MCP = STANDBY and A Failing this (B) MCP	Check the wiring of the MCP units to the switch panel
25	STATE CONFLICT: This MCP = STANDBY and B, PEER MCP = STANDBY Failing this (B) MCP	Check the wiring of the MCP units to the switch panel. This could also be loss of power to the switch panel, as a powered-down switch panel reads as “standby” and “B” to the MCP.
26	[STANDBY]: Failed to pull the switch, Rejecting Change Over request	The MCP could not pull the switch. Check the wiring of the MCP units to the switch panel. This could also be loss of power to the switch panel.
27	[STANDBY]: Config Sync failed in network mode while copying configuration to /mnt/usr/	The standby MCP unit failed to commit its transferred configuration into the flash card. The flash card may be full, or someone may have changed the write permissions on the card. The standby configuration may be partially copied and unusable.
28	[STANDBY]: Config Sync failed in local mode due to tool task failure	Configuration synchronization failed while transferring configuration data. The standby unit uses its original configuration.
29	[STANDBY]: Config Sync failed in local mode while copying configuration to /mnt/usr/	The standby MCP unit failed to commit its transferred configuration into the flash card. The flash card may be full, or someone may have changed the write permissions on the card. The standby configuration may be partially copied and unusable.
30	[STANDBY]: CONFIG SYNC Activity: Tool task timeout in mode <tool task mode>	Configuration synchronization failed while transferring configuration data. The standby unit uses its original configuration.

Serial Number	Diagnostic Log Messages	Details
31	[STANDBY]: CONFIG SYNC Activity: Response timeout	The active unit failed to send a response during configuration sync activity. The active unit may be experiencing problems, or the communication link between the two units may be disconnected. The standby configuration may be partially copied and unusable.
32	Response timeout in DB SYNC Activity	The standby unit failed to send a response while synchronizing quality or accumulator data. The data on the standby unit may not be up to date. The standby unit may be experiencing problems or the communication link between the two units may be disconnected.
33	[ACTIVE]: Config check completed: Configuration is same	The configuration is the same on both active and standby units.
34	[STANDBY]: Response timeout for activity <activity type> subactivity <subactivity type>	The standby unit failed to send a response to the active unit. The numeric codes define the activity that timed out. This is a diagnostic message that only needs to be considered if there are messages indicating that something has failed.
35	[ACTIVE]: Switch pulled away: PEER MCP is failed, Failing this MCP	Switch pulled manually when the standby unit is not available. The standby unit may have failed or the communication link between the two units may be disconnected.
36	[ACTIVE]: Switch pulled away: Rejecting CHANGE OVER since Other MCP is in Service Mode	Switch pulled manually when the standby unit is in service mode. The active unit rejects the command to switch over.
37	[ACTIVE]: RACE Condition for switch: Failing this (B) MCP	Switch was pulled in the last 1000 ms.
38	[ACTIVE]: Standby MCP rejected the code config request with reason <reason code>	The standby unit rejected a request to update code and config check values. The <reason code> is identified by a technical number. See the Redundancy_Manager_Reason_Codes for the technical number (reason code) descriptions. The most common cause is that the standby unit is in service mode or has failed.
39	[ACTIVE]: No Change Over Event Resp from <no of applications> applications. Change Over Timeout	The active redundancy manager does not receive a change-over event response from the indicated number of applications.
40	failed to open code_config_check file	A MCP has failed due to a software failure. Either the ssh keys are not synced, or the MCP has not started properly.
41	failed to read code_config_check file	A MCP has failed due to a software failure. The MCP has not started properly.
42	failed to update code config info <file name>	A MCP has failed due to a software failure. The MCP has not started properly.
43	redun manager update fifo creation failed with reason <error code>	A MCP has failed due to a software failure. The MCP has not started properly.
44	Failed to write active->standby trigger message to main thread fifo	A MCP has failed due to a software failure. The MCP has not started properly.

Serial Number	Diagnostic Log Messages	Details
45	Failed to read message from redun manager update FIFO	A MCP has failed due to a software failure. The MCP has not started properly.
46	[ACTIVE] Failed to read state of switch panel (master), Failing MCP	Check the: ☐ Switch panel port configuration. ☐ Wiring of the MCP units to the switch panel. ☐ Availability of power to the switch panel.
47	[Active] Failed to read state of switch panel (slave), Ignoring error	Check the: ☐ Switch panel port configuration. ☐ Wiring of the MCP units to the switch panel. ☐ Availability of power to the switch panel.
48	[Active] failed to pull master switch panel towards itself, Failing MCP	Check the: ☐ Switch panel port configuration. ☐ Wiring of the MCP units to the switch panel. ☐ Availability of power to the switch panel.
49	[Active] failed to pull slave switch panel towards itself, Ignoring	Check the: ☐ Switch panel port configuration. ☐ Wiring of the MCP units to the switch panel. ☐ Availability of power to the switch panel.
50	[PRP] Failed to recv msg from PEER MCP on Channel <channel no>	Possibly a partial message has been received on channel <channel no>
51	Failed to write standby->active trigger message to main thread fifo	A MCP has failed due to a software failure. The MCP has not started properly.
52	bind () call failed. Error [<error code>], Restarting applications on this MCP	There could be more than one instance of Redundancy manager running at the same time.
53	MCP DESIGNATION CONFLICT. BOTH MCPs are <gateway name>. Failing this MCP.	Both MCPs have either Gateway_A or Gateway_B designation. Check mcpcfg for the MCP designation or switch panel configuration on both MCPs.
54	STATE CONFLICT. BOTH MCPs are ACTIVE	Both MCPs are in the active state. This could be due to either: ☐ Heart beat communication link is available after a brief failure or ☐ Switch panel configuration mismatch
55	STATE CONFLICT. BOTH MCPs are ACTIVE. Restarting this MCP	Both MCPs are in the active state. This could be due to either: ☐ Heart beat communication link is available after a brief failure or ☐ Switch panel configuration mismatch
56	STATE CONFLICT. BOTH MCPs are STANDBY. Restarting this MCP	Both MCPs are in the active state. This could be due to a switch panel configuration mismatch.

Serial Number	Diagnostic Log Messages	Details
57	TCP client connection from <IP Address> is not matching with configured PEER ip. Rejecting connection	This indicates a third MCP or another device, which is not configured as PEER, is attempting to connect to this MCP. Subsequently, the connection is closed. Check the configuration using mcpcfg/Settings GUI configuration tool.
58	Failed to get pseudo points from pseudo map file Err:-98	The RTDB Pseudo points file became corrupted. To recover from this situation, issue the following command from the MCP console and then reboot: 'cp /home/Configure/SystemConfig/RTDBPseudoPoints.xml.default /home/Configure/SystemConfig/RTDBPseudoPoints.xml'

The following table describes the possible system event messages displayed by the MCP Redundancy Manager. These messages are entered in the system event log of the MCP. These are notifications of significant events, not necessarily errors. If it indicates an error or failure, consult the diagnostic log for details.

MCP Redundancy System Log Messages

Table 6.90: MCP Redundancy System Log Messages

Serial Number	System Event Log Messages	Details
1	MCP Started in Active Mode	
2	Switching to standby mode	The change-over operation is initiated - switching to standby mode.
3	Switching to Non-sync mode	There is a mismatch between the firmware code and/or configuration on two MCPs entering non-sync mode.
4	Sent message to SWWatchdog to restart all apps	
5	Sent message to SWWatchdog to stop all apps	The MCP is being placed in failed mode.
6	Received HB from standby	A lost connection with the standby has been restored.
7	Child starts	Redundancy Manager child started
8	Appl starts	Redundancy Manager application started
9	MCP Started in Non-Redundant Mode	
10	Heart Beat(s) missed from Standby system : Declaring PEER MCP as Failed	The standby MCP has stopped responding to communications.
11	Heart Beat(s) missed from Active system : Declaring PEER MCP as Failed	The active MCP has stopped responding to communications.
12	MCP Started in Standby Mode	
13	Switching to Active mode	The change-over operation is initiated - switching to active mode.

The table below describes the possible diagnostic log messages that can come during initialization, configuration parsing, startup, runtime operations when applications are running in Hot Standby mode, by using services of MCP Synchronization Service Library (NTEK-L011-0).

MCP Hot Standby Synchronization Service Diagnostic Log Messages

Table 6.91: MCP Hot Standby Synchronization Service Diagnostic Log Messages

Serial Number	System Event Log Messages	Details
1	ERROR: Config Parsing Failed	MCP Sync Service Configuration file parsing failed. Applications run with default parameters.
2	HotStandbySleep Failed with RetVal: (errorCode)	Error in identifying System State.
3	State Returned is neither Active/Standby: (SystemState), Waiting for State from RM	Redundancy Manager System State was not identified or an Invalid System State Received message occurred.
4	ERROR: State Returned is ActiveNonRedundant, Not Starting SyncService Thread	Hot Redundancy is configured but System State is ActiveNonRedundant. Sync operation with standby unit is not performed.
5	Shared Memory Creation Failed with Error (errorCode)	A software failure has occurred on the MCP. Either the MCP is running out of memory or the MCP has not started properly.
6	Shared Memory Registration Failed with Error (errorCode)	A software failure has occurred on the MCP. Either the MCP is running out of memory or the MCP has not started properly.
7	RingBuffer Creation Failed	A software failure has occurred on the MCP. Either the MCP is running out of memory or the MCP has not started properly.
8	SyncService RingBuffer OverFlow, Setting OverFlow Flag	The application buffer has overflowed. The Standby unit may lose some events.
9	Detected RingBuffer OverFlow, Starting Complete Init	Starting Initial Synchronization with Standby unit.
10	DeleteDataPacket: Invalid EntryID passed: (Packet entryID)	Duplicate data has been received from Standby MCP. This can occur during channel switching or change-over. Does not affect normal operation.
11	Starting UDS Server Channel Failed with RetVal: (errorCode)	A software failure has occurred on the MCP. Either the MCP is running out of memory or the MCP has not started properly.
12	Connection Timeout, Closing Current Active Channel: (activeChannel)	The Heart Beat is missing from the Active MCP. Check the TCP communication between the MCPs.
13	Applications Restart on Active/Standby, Doing Complete INIT newPPID: (standby parent process ID), oldPPID: (Standby Old parent process ID)	Applications start on Active/Standby. Starting initial synchronization with Standby unit.

14	Child Restart on Standby	Standby Application child was restarted.
15	No OverFlow: Skipping INIT upon channel reconnection, Last acked EntryID: (entryID)	Channel Reconnection, no buffer overflow observed on Active unit. Does not affect normal operation.
16	ERROR: StartFileTransfer: File Stat Failed	A software failure has occurred on the MCP. Either the MCP is running out of memory or the MCP has not started properly.

Communications

This chapter contains the following sections and sub-sections:

Connection

Configure Serial Communications
- Types of Serial Connections
- Add a Serial Connection
- Modify a Serial Connection
- Delete a Serial Connection
- Connection Application Parameters
- Port Settings
- Virtual Serial Ports
- Connection Security
- Redundancy Dedicated Link
- Redundancy Switch Panels
- Terminal Server

Configure Network Communications
- Types of Network Connections
- Add a Network Connection
- Modify a Network Connection
- Delete a Network Connection
- Connection Application Parameters
- SSH TCP Tunnel
- Secure Connection Relay
- VPN Server

Configure D.20
- **Error! Reference source not found.**
- D.20 Peripheral Mapfiles
- Configuring Peripheral Map files
- D.20 Peripheral Link Client Pseudo Points

Connection

You can configure serial and network communication connections in the MCP on the **Connection** tab of the **Configuration** page.

The following related actions can be performed:
- Add a serial connection

Modify a serial connection
Delete a serial connection
Add a network connection
Modify a network connection
Delete a network connection

Configure Serial Communications

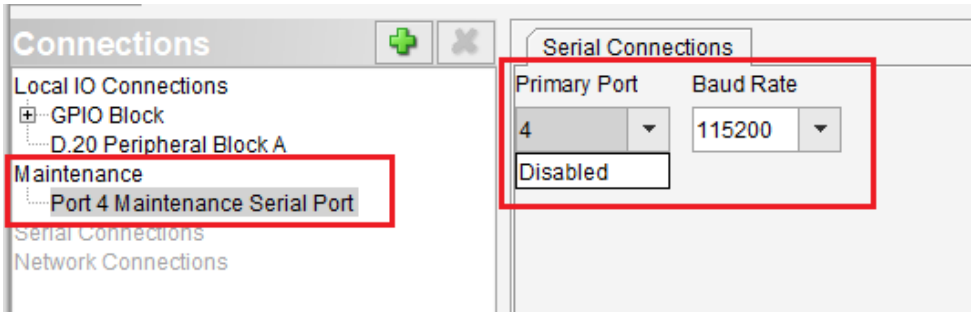
Serial Maintenance Port

MCP devices have a dedicated serial port reserved for settings and maintenance operations.

For G500 this is the front USB type B port (see *G500 Substation Gateway Instruction Manual (994-0152)*. This serial port cannot be used for other purposes in G500.

For G100, this is by default serial port # 4, enabled in the default configuration. When enabled, serial port #4 cannot be used for other purposes in G100. The serial maintenance port in G100 can be disabled and made available to other applications using the MCP Studio Editor (online or offline). When enabled, this is always serial port #4.

Figure 6.2 G100 Serial Maintenance Port control



Types of Serial Connections

Refer to *G500 Substation Gateway Instruction Manual (994-0152) or G100 Substation Gateway Instruction Manual (994-0155)* for more details about the serial port modes and characteristics. Each serial port can be assigned a single host protocol (server application) for master station communications using a standard serial connection. Each serial port can be assigned ONLY a single device protocol (client application) for device communications.

The MCP supports the following types of serial connections:

- Point-to-point
- Multi-drop
- Serial master station

Redundancy

Communications that take place over a serial connection can be configured for redundancy by setting up two serial ports – a Primary port and a Secondary (back up) port. Communications normally take place over the Primary port. In the event of a loss of communication with the device over the Primary port, the MCP tries to re-establish communication over the Secondary port. If the MCP cannot re-establish communication over the backup port it reports the device status as off line.

Multi-Drop

Some devices support a daisy-chain connection in which multiple devices are wired together from one to the other. A multi-drop configuration requires additional configuration to set up each individual device on a multi-drop connection.

SCADA Communications

The MCP supports serial connections to SCADA masters through up to eight serial ports. Each serial port can be assigned a single SCADA protocol (server application) for master station communications. The MCP currently supports serial master communications using the following server protocols:

- DNP server
- Modbus
- IEC 60870-5-101

Protocols

Serial connections can be configured using the following protocols.

- DNP3 Master Stations
- DNP3 Multi-drop
- IEC 60870-5-101 Master Station
- IEC 60870-5-101 Multi-drop
- IEC 60870-5-103 Multi-drop
- LogicLinx Device
- Modbus Master Stations
- Modbus Multi-drop
- Redundancy Dedicated Link – not supported in G100
- Redundancy Switch Panel – not supported in G100
- Generic ASCII
- SEL Binary with MCP as Master
- Terminal Server

Add a Serial Connection

You manage the serial connections on the MCP on the **Connection** tab on the **Configuration** page.

A client map file must be available in the MCP before a protocol type is available for configuration. The MCP includes several default client maps. If you require a custom map, create it first before setting up the serial connection. See Client Maps.

» To add a serial connection:

1. On the Connections tab, click Add Connection (+).
2. On the New Connection window, select Serial Connection and select the Serial Configuration Type from the list. A new serial connection sub-item is added.
3. Modify the settings for the new connection. Double-click a cell, to modify a value.
4. The fields under Configuration Settings are specific to the connection type. (See the protocols listed below.)
5. Click Save Configuration to save your changes.

Each row under the **Serial** heading of the Connections pane represents one connection through a serial port.

The serial ports are indicated by numbers or combination of letters and numbers, as below:

- Ports 1 to 4 apply to G100 and G500, and correspond to the numbered physical ports on each device
- Ports 5 to 8 apply to G500, and correspond to the numbered physical ports on the G500 device
- Ports A1 to A4 apply to G500, and correspond to serial ports 1-4 installed in the PCIe slot #1
- Ports B1 to B4 apply to G500, and correspond to serial ports 1-4 installed in the PCIe slot #2
- Ports C1 to C4 apply to G500, and correspond to serial ports 1-4 installed in the PCIe slot #3

Depending on the configured model in the order code in MCP Studio / Device Properties – the ports which are not available in the order code are shown grayed out. They are still available to configure, to allow porting configurations across differently serial ports equipped devices, and without causing configuration errors. However, please note that in absence of the serial port in hardware, configured ports will naturally not operate.

When converting G500 configurations to G100 configurations – the port assignments will be retained, as the system cannot automatically determine what to do with the extra serial ports. Because this conversion is from a device with more serial ports, this operation will require user decision and re-assignment of serial ports in the lesser equipped G100.

The mode of each serial port (RS-232/RS-422/RS-485 2w/RS-485 4w) is configured using online *MCP Local Configuration Utility (mcpcfg)* or *MCP Settings GUI* (default is RS-232).

Each serial connection can be configured for device (client) or master station (server) communications using a selected protocol. The type of connection and the protocol you select determine the client or server application and related settings that are used for the communications on that serial port. See the Port Settings section.

Modify a Serial Connection

» To modify a connection:

1. Select the connection in the **Connections** pane.
2. Double-click or select a configuration parameter field
3. Enter a new value in the parameter field.
4. Click **Save Configuration** to save your changes.

NOTE: If you select a different map file for an existing connection, all point mappings related to the connection becomes invalid. This includes points selected within applications like the Calculator, the Alarms configuration page, and the System Point Manager. Mappings affected by this are referred to as being "non-existent". Editing an existing map file does not invalidate mappings.

Delete a Serial Connection

» To delete a connection:

1. Select the connection you wish to delete in the **Connections** pane.
2. Click **Delete Connection**.
3. Click **Yes** to confirm deletion.
   Result: The item is removed from the connections list.
4. Click **Save Configuration** to save your changes.

Connection Application Parameters

The **Application Parameters** window allows you to view and modify the protocol settings for a specific client or server connection. Application parameters are available on the **Connection** tab on the **Configuration** page. The settings shown vary based on the connection type and protocol selected.

» To create a custom application parameter profile:

1. On the **Connection** tab, select or add a connection.
2. Under **Application Parameters**, select **Use Custom** and click **Create**. The **Application Parameters** window opens.

3. To modify a parameter, double-click the associated value and enter a new value or select from the drop-down list. More advanced parameters may be available on the **Advanced** sub-tab.
4. When you are done, click **Save**.
5. On the **Save As** window, enter a filename and click **Save**.
6. Click **Save Configuration** to save your changes.

» To modify application parameters:

1. On the **Connection** tab, select or add a connection.
2. Under **Application Parameters**, select **Use Custom** and click **Edit**.
   Result: Either the **Application Parameters** window opens (go to step 4), or the **Choose Version** popup appears (if you created a profile and have not committed it yet).
3. Select the version of the application parameters profile to be edited from the **Choose Version** popup:
   - **COMMITTED:** The most recently committed version.
   - **UNCOMMITTED:** The version created, but not committed yet.
4. Click **OK**.
   Result: The **Application Parameters** window opens.
5. To modify a parameter, double-click the associated value and enter a new value or select from the drop-down list. More advanced parameters may be available on the **Advanced** sub-tab.
6. When you are done, click **Save**.
7. On the **Save As** window, enter a filename and click **Save**.
8. Click **Save Configuration** to save your changes.

» To view application parameters:

1. Go to the **Connection** tab.
2. Under **Application Parameters.** select **Use Default** and then click **Show**.
   Result: The **Application Parameters** window opens.

Port Settings

The following settings are required for each connection; they define how the MCP communicates over the serial link. Some settings may not be available for all connection types.

Table 6.92: Port Settings

Setting	Description	Range	Default
Primary Port	**For G500:** Primary serial port for device communications with the MCP. Ports 1-8, A1-A4, B1-B4 and C1-C4 refer to Physical Serial Ports and ports VP1 through VP150 refer to Virtual Serial Ports. **For G100:** Primary serial port for device communications with the G100. Ports 1-4 refer to Physical Serial Ports and ports VP1 through VP150 refer to Virtual Serial Ports.	**For G500:** 1-8, A1-A4, B1-B4 and C1-C4 Physical Serial Ports VP1 -VP150 – Virtual Serial Ports **For G100:** 1-4 - Physical Serial Ports VP1 - VP150 – Virtual Serial Ports	Increment from 1 – Physical Serial Ports Incremented from VP1 – Virtual Serial Ports
Backup Port	**For G500:**	**For G500:**	NA

	Secondary port for device communications if the Primary port fails. The Backup port automatically takes on the settings of the associated Primary port. Ports 1-8, A1-A4, B1-B4 and C1-C4 refer to Physical Serial Ports and ports VP1 through VP150 refer to Virtual Serial Ports. **For G100:** Secondary port for device communications if the Primary port fails. The Backup port automatically takes on the settings of the associated Primary port. Ports 1-4 refer to Physical Serial Ports and ports VP1 through VP150 refer to Virtual Serial Ports.	1-8, A1-A4, B1-B4 and C1-C4 Physical Serial Ports VP1 -VP150 – Virtual Serial Ports **For G100:** 1-4 - Physical Serial Ports VP1 - VP150 – Virtual Serial Ports	
Baud Rate	The speed of information being transmitted across the serial connection, in bits per second (bps).	List of baud rates (110 to 115200)	9600
Parity	A bit added to a group of bits to detect the presence of an error.	Even None Odd	None
Data Bits	Number of bits used for each character.	7, 8	8
Stop Bits	Number of bits used to indicate the end of each character as it is transmitted.	1, 2	1

RTS, CTS and DCD Values

Some protocols may require these parameters to be configured.

Table 6.93: RTS Values

Setting	Description	Range	Default
Flow Control	Specifies whether or not RTS Flow Control is enabled	Enabled Disabled	Disabled
Pre-Trans Delay	Specifies the time (in milliseconds) that RTS is asserted before data is transmitted. Also known as the RTS preamble.	1 to 65535	15
Post-Trans Delay	Specifies the time (in milliseconds) after data is transmitted that RTS is held asserted. Also known as the RTS post amble.	1 to 65535	15

Table 6.94: CTS Values

Setting	Description	Range	Default
Flow Control	Specifies whether or not CTS Flow Control is enabled	Enabled Disabled	Disabled

Table 6.95: DCD Values

Setting	Description	Range	Default
Flow Control	Specifies whether or not DCD Flow Control is enabled	Enabled Disabled	Disabled
Receive Inhibit Delay	Specifies the Receive Inhibit Delay, in milliseconds.	1 to 65535	15

Dial-up Modem Settings

The following settings are required when configuring a Dial-up Modem link.

Table 6.96: Dial-up Modem Settings

Setting	Description	Range	Default
Init String	The data string sent to the modem when the application starts.	1 to 64 ASCII characters, no spaces	ATZ*
Attention String	The data string sent to the modem to place it into command mode.	1 to 32 ASCII characters, no spaces	+++
Hang Up String	The data string sent to the modem to cause it to hang up the phone connection.	1 to 32 ASCII characters, no spaces	ATH
Retry Count	How many times to retry a failed connection before giving up. Increase the value for unreliable connections.	0 to 30	3
Retry Delay (sec)	The amount of time to wait (in seconds) between retry attempts.	0 to 3600	3 (Client) 30 (Server)
Idle Wait Time (sec)	The amount of time (in seconds) that must elapse without data transmission before the connection is terminated.	0 to 3600	10 (Client) 15 (Server)
Auto Answer	Enable the modem to automatically answer incoming calls.	Enabled Disabled	Enabled

***NOTE**: Init String depends on Modem make.

Physical Serial Ports

Table identifies the port names used to identify physical serial ports.

Port Range	Physical Serial Ports
1 to 4	Base Serial Ports on G100 and G500
5 to 8	G500 only: Base Serial Ports
A1 to A4	G500 only: Port 1 to 4 on Serial Expansion card in PCIe slot 1
B1 to B4	G500 only: Port 1 to 4 on Serial Expansion card in PCIe slot 2
C1 to C4	G500 only: Port 1 to 4 on Serial Expansion card in PCIe slot 3

Virtual Serial Ports

The Virtual Serial Ports feature allows you to communicate with devices through an Ethernet connection even though they appear to be connected through a physical serial port. You can use virtual serial ports for any connection except for system redundancy and modem links, and you can create up to 150 virtual ports.

The Terminal Server and Pass-Through Connections features provide additional options for connecting to devices through the MCP.

» To create a virtual serial port:

1. Access the **Connections** tab of the **Configuration** page. If there are no serial connections on this page, you must create one.
2. Click the **Virtual Serial Ports** tab. This tab is available on all serial connections.
3. Click the **Add** button and configure the newly created row.

4. You can now select this virtual serial port as the Primary or backup port on the **Serial Connection** tab.

Table 6.97: Virtual Serial Port Settings

Setting	Description	Range	Default
Virtual Serial Port #	The port number assigned to the virtual serial port. VP1 to VP150 are reserved for virtual serial ports	VP1 – VP150	Lowest unused virtual port number. Default VP1.
IP Address	The IP Address to use to connect to the device.	Valid IPV4 address	127.0.0.1
Network Port	The network port to connect to on the remote IP Address	0 to 65535	10000 plus the pre-assigned virtual serial port number

NOTE: Do not configure any hardware handshaking options on serial connections that use virtual serial ports. Doing this prevents the virtual serial port from initializing and the server or client application configured for the port fail to start.

Connection Security

The MCP supports Transport Layer Security (TLS) which is cryptographic protocol that provide security for communications over networks such as the Internet. TLS encrypt the segments of network connections at the Application Layer to ensure secure end-to-end transit at the Transport Layer.

This security feature is available on the following types of connections:

- IEC 60870-5-103 Multi-drop
- Modbus Multi-drop
- Generic ASCII
- SEL Binary with MCP as Master
- Terminal Server

NOTICE

- SECURITY NOTICE

The following services are considered unsecure:

- IEC 60870-5-103 Multi-drop (Passthrough - Telnet)
- Modbus Multi-drop (Passthrough - Telnet)
- Generic ASCII (Passthrough - Telnet)
- SEL Binary with MCP as Master (Passthrough - Telnet)
- Terminal Server (Telnet)

It is strongly recommended that TLS tunnels or SSH Tunnels are used for sessions across unprotected / external networks.

The user assumes all responsibility for the system design and associated security risks when unsecured sessions are used, for e.g. Telnet.

The following parameters can be configured on any security-enabled connection.

Secure Application Parameters

Table 6.98: Secure Application Parameters

Setting	Description	Range	Default
Parameters			

Setting	Description	Range	Default
Enable insecure authentication	When enabled, connection security features are not enforced. You should only enable this setting if alternate security features are available for the connection.	Disabled Enabled	Disabled
Session key renegotiation interval	The maximum amount of time, in seconds, that can pass before the connection session key is renegotiated. Frequently renegotiating the session key increases the security of the connection.	600 to 7200	900
Session key renegotiation count	The amount of data, in bytes, that can be transmitted between devices before the connection session key is renegotiated.	10000 to 1000000	100000
Session key renegotiation timeout	The amount of time, in milliseconds, that the MCP waits for a response to a renegotiation request before the connection is considered timed out and is disconnected.	500 to 120000	2000
Issuers			
PEER	The text string that must match the common name as provided on the certificate provided by the remote device.	Free text entry	N/A
Issuer	The name of the issuer that generated the certificate provided by the remote device.	List of installed issuer certificates	N/A
Enable PEER identity validation	If enabled, connections are only permitted to devices that provide a certificate that contains a common name included in the list above and that was provided by the associated issuer. If disabled, PEER identity validation is not performed.	Disabled Enabled	Enabled
Ciphers			
Cipher name	A list of ciphers supported by the MCP. When a connection is established with a remote device, a list of enabled ciphers is exchanged, and the most secure cipher is selected to secure the connection.	N/A	N/A
Enable	Select whether or not to enable the associated cipher. If the remote device does not support at least one of the enabled ciphers, the connection is not established. List Of Supported Ciphers: EDH-DSS-DES-CBC3-SHA:DHE-DSS-AES128-SHA:DHE-DSS-AES256-SHA:EDH-RSA-DES-CBC3-SHA:DHE-RSA-AES128-SHA:DES-CBC3-SHA:@STRENGTH	Disabled Enabled	Disabled
Permit null encryption	If checked, null encryption ciphers are permitted. If a null encryption cipher is used, the connection itself is unencrypted and is vulnerable to interception attacks.	Disabled Enabled	Disabled
Secure protocol	Select the protocol used to secure the connection.	TLS 1.1 TLS 1.0	TLS 1.0

Redundancy Dedicated Link

NOTE: This is not supported in G100.

The following settings are used when configuring MCP system redundancy. A Redundancy Dedicated Link is configured on the ports that MCP ping cables are connected to.

In Warm Standby redundancy, only a single serial port is used as a Redundancy Dedicated Link. In Hot Standby redundancy, an optional backup port can also be configured.

Table 6.99: Redundancy Dedicated Link Settings

Setting	Description	Range	Default
Device Name	Text description to identify the redundancy connection.	1 to 32 ASCII characters	RLINKx
Auto Start	Not Used.	NA	NA

Ensure that both MCP units in the redundant setup have connected the ping cable to the same serial port number. In a redundant setup, the MCP Configuration Manager synchronizes configurations between the MCP units; this setting is lost if there is a difference between the two configurations.

Redundancy Switch Panels

NOTE: This is not supported in G100.

The following settings are used when configuring MCP system redundancy. A Redundancy Switch Panel connection is configured on the port that the RS232 watchdog cable is connected to.

Table 6.100: Redundancy Switch Panel Settings

Setting	Description	Range	Default
Device Name	Text description to identify the redundancy connection.	1 to 32 ASCII characters	RSWITCH
Auto Start	Not used.	NA	NA

Ensure that both MCP units in the redundant setup have connected the watchdog cable to the same serial port number. In a redundant setup, the MCP Configuration Manager synchronizes configurations between the MCP units and this setting are lost if there is a difference between the two.

Terminal Server

The MCP can be configured to provide transparent access (also known as pass-through) to connected devices using vendor-supplied PC programs. This is done by configuring the port the device is connected to as a Terminal Server.

Refer to *Pass-Through Connections* for more information.

The following settings are used when configuring a Terminal Server.

Table 6.101: Terminal Server Settings

Setting	Description	Range	Default
Device Name	Text description to identify the terminal server.	1 to 32 ASCII characters	N/A
Auto Start	Indicates if the client application automatically starts when the configuration is changed and reloaded or when the MCP re-boots.	Disabled Enabled	Disabled
Secure Type	Select a security feature to be enabled on the connection. For more information, refer to *Connection Security*.	Disabled Telnet TLS Security SSH Secure Tunnel	Disabled

Setting	Description	Range	Default
TLS port	Enter the port number that can be used to access the secure connection.	1 to 65535	50000 + X
File	Select the security parameters defining this connection. After a configuration can be created, it can be saved and reused on other connections. Refer to *Secure Application Parameters*.	List of saved security settings	N/A

Terminal Server Application Parameters

Terminal Server application settings are available under the **Application Parameters** field.

Terminal Server Application Parameters

Table 6.102: Terminal Server Application Parameters

Setting	Description	Range	Default
Base network port	By default, the terminal server listens for incoming connections on port 8000. However, a custom port can be specified instead	Use Default Use Custom	Use Default
Custom network port	The network port where the terminal server listens for incoming connections	0 to 65535	Not enabled
Password authentication	If set to Yes, the terminal server application requires a valid username and password before a connection is opened. See note below.	Yes No	Yes
Minimum privilege level	The minimum user privilege level required for the user account providing login credentials.	Supervisor Operator	Supervisor

NOTE: If you configure one MCP to act as a terminal server for another MCP that is using virtual serial ports, the password authentication option must be disabled on the terminal server port.

Configure Network Communications

Types of Network Connections

The MCP supports network connections to up to 8 master stations. Each network interface can be assigned a single host protocol (server application) for master station communications.

Network connections to the MCP are shown as sub-items under the **Network Connections** heading of the **Connections** pane. Each network connection can be configured for either:

- Master station (server) communications using a selected protocol.
- IEDs (client) communications using a selected protocol.

Network Blocks

To improve the efficiency of communications, the MCP supports network capable device and master connections using "blocks" that can process communications concurrently. Each network block is an instance of a designated protocol (client or server application).

Each network block can be configured for the number of device (client) or master station (server) connections and instance-specific protocol settings that are used for the network communications. Network blocks appear under the **Network Connections** heading of the **Connection** tab as *<Protocol Name> Blocks*.

Tip: Each additional instance uses additional system resources yet increases system throughput.

Network Devices

Network capable devices can be connected to one or more data collection blocks and polled according to the instance-specific protocol settings.

Master Connections

The MCP can support communications to multiple (up to eight) master stations. The data presented to each master station may be identical or unique as defined by a server map. Although the MCP accepts data requests from only one master station at a time, it can support requests from any master station. A single Master block defines the master station connections.

The **Master Block** tab on the **Network** tab includes a tab for each configured server application. Each row on the **Master Connection** page represents one master connection.

A master station represents a single instance of a server application. Each configured master station application is shown as a sub-item underneath the **Network Master Stations** item on the **Connection** tab.

Protocols

You can configure network connections using the following protocols:

- DNP IED Block
- DNP3 Master
- IEC 60870-5-104 IED Block
- IEC 60870-5-104 Master Station
- Modbus TCP or TCP/SSH IED Block
- Modbus TCP Master
- Secure connection relay
- SNMP Block
- VPN Server

NOTE: IEC 61850 device connections are available for viewing only and cannot be edited on the Network page. To change the IEC 61850 client configuration, you must use the IEC 61850 Loader tool and re-load the configuration into the MCP. Refer to the IEC 61850 Loader online Help for more information.

Add a Network Connection

You manage the network connections on the MCP on the **Connection** tab on the **Configuration** page.

A map file must be available in the MCP before a protocol type can be added. The MCP includes several default maps. If you require a custom map, create it first before setting up the network connection. See *Client Maps* or *Server Maps*.

» To add a network connection:

1. On the Connection tab, click Add Connection.
2. On the New Connection window, select Network Connection and select the configuration type. Result: A new network connection item or master station sub-item is added.
3. Modify the settings for the new connection. Double-click a cell to modify a value.
4. Select whether the server application automatically starts (Auto-Start) when the configuration is loaded and when the MCP re-boots. Range is Automatic and Disabled.
5. Enter the fields under Configuration Settings are specific to the connection type. (See the protocols listed below.)
6. Click Save Configuration to save your changes.

Modify a Network Connection

» To modify a connection:

1. Select the connection in the **Connections** pane.
2. Double-click or select a configuration parameter field and enter a new value.
3. Click **Save Configuration** to save your changes.

NOTE: If you select a different map file for an existing connection, all point mappings related to the connection become invalid. This includes points selected within applications like the Calculator, the Alarms configuration page, and the System Point Manager. Mappings affected by this are referred to as being "non-existent". Editing an existing map file does not invalidate mappings.

Delete a Network Connection

» To delete a connection:

1. Select the connection you wish to delete in the **Connections** pane.
2. Click **Delete Connection**.
3. Click **Yes** to confirm deletion.
   Result: The item is removed from the connections list.
4. Click **Save Configuration** to save your changes.

Connection Application Parameters

The **Application Parameters** window allows you to view and modify the protocol settings for a specific client or server connection. Application parameters are available on the **Connection** tab on the **Configuration** page. The settings shown vary based on the connection type and protocol selected.

» To create a custom application parameter profile:

1. On the **Connection** tab, select or add a connection.
2. Under **Application Parameters**, select **Use Custom** and click **Create**. The **Application Parameters** window opens.
3. To modify a parameter, double-click the associated value and enter a new value or select from the drop-down list. More advanced parameters may be available on the **Advanced** sub-tab.
4. When you are done, click **Save**.
5. On the **Save As** window, enter a filename and click **Save**.
6. Click **Save Configuration** to save your changes.

» To modify application parameters:

1. On the **Connection** tab, select or add a connection.
2. Under **Application Parameters**, select **Use Custom** and click **Edit**.
   Result: Either the **Application Parameters** window opens (go to step 4), or the **Choose Version** popup appears (if you created a profile and have not committed it yet).
3. Select the version of the application parameters profile to be edited from the **Choose Version** popup:
   - **COMMITTED:** The most recently committed version.
   - **UNCOMMITTED:** The version created, but not committed yet.
4. Click **OK**.
   Result: The **Application Parameters** window opens.
5. To modify a parameter, double-click the associated value and enter a new value or select from the drop-down list. More advanced parameters may be available on the **Advanced** sub-tab.
6. When you are done, click **Save**.

7. On the **Save As** window, enter a filename and click **Save**.
8. Click **Save Configuration** to save your changes.

» To view application parameters:

1. Go to the **Connection** tab.
2. Under **Application Parameters.** select **Use Default** and then click **Show**.
   Result: The **Application Parameters** window opens.

Modbus TCP/SSH Tunnel

The following settings are used when configuring a Modbus IED block with TCP/SSH Protocol.

Modbus TCP/SSH Tunnel Configuration Parameters

Table 6.103: SSH TCP Tunnel Configuration Parameters

Setting	Description	Range	Default
SSH Server Port	The port number on which Modbus TCP/SSH is to communicate with the IED.	0 to 65535	22
M2M User Name	Name of the User to authenticate for TCP/SSH communication.	Not Available	m2m_user
SSH Key Rotation Period(days)	Key Rotation Period in days after which new SSH keys are generated, transferred to IED and then the session will be reestablished with new SSH Keys.	0 to 365	1

Secure Connection Relay

A secure connection relay can be used to apply security features to any existing Ethernet connection.

NOTICE

- SECURITY NOTICE

It is strongly recommended that the user employ TLS tunnels to protect the following services:

- DNP3 Master
- IEC 60870-5-104 Master Station
- Modbus TCP Master

The user assumes all responsibility for associated security risks when enabling unsecured services onto an unprotected network.

The following settings are used when configuring a secure connection relay.

Table 6.104: Secure Connection Relay settings

Setting	Description	Range	Default
Secure Relay Name	Text description to identify the connection.	1 to 32 ASCII characters	N/A
Auto Start	Indicates if the application automatically starts when the configuration is changed and reloaded or when the MCP re-boots.	Disabled Enabled	Enabled
Remote IP Address	The IP Address of the remote device that the secure connection is established with.	Valid IPv4 address	0.0.0.0
LAN port	The IP port number to use when connecting to the remote device.	1 to 65535	20001

Setting	Description	Range	Default
TLS port	Enter the port number that can be used to access the secure connection.	1 to 65535	50000 + X
Max Conn	The maximum number of concurrent connections permitted to access the secure connection relay at one time.	1 to 32768	1
File	Select the security parameters defining this connection. After a configuration can be created, it can be saved and reused on other connections. Refer to *Secure Application Parameters*.	List of saved security settings	N/A

VPN Server

The following settings are used when configuring a VPN Server through DS Agile MCP Studio.

NOTE: Refer to the Integration of MCP with open VPN (Virtual Private Network) Client - Configuration Guide (SWM0103) for the detailed procedures used to:

- Implement a simple Certification Authority using XCA Certification Authority (Open Source tool).
- Install certificates on the MCP and Windows PC running open VPN client.
- Configure open VPN client to communicate to the MCP over virtual private network.

Table 6.105: VPN Server settings

Setting	Description	Range	Default
Name	Unique name for the VPN Server.	Text string 32 characters are allowed	VPN Server
Auto Start	Indicates if the application automatically starts when the configuration is changed and reloaded or when the MCP re-boots.	Disabled Enabled	Enabled
Network IP Address	IP Address of the device. Must be unique from other configured devices.	Valid IPv4 address	10.200.0.0 /24
Port	The port number on which the device communicates.	0 to 65535	1,194
Concurrent Connections	The number of allowed concurrent connections.	1, 2, 3	1
Transport Layer	The transport layer protocol; either: • Transmission Control Protocol (TCP), or • User Datagram Protocol (UDP)	TCP UDP	UDP

Setting	Description	Range	Default
Encryption Algorithm	Mathematical formula used in encryption and decryption of the VPN communication.	List of encryption algorithms. AES-256-CBC AES-256-CFB1 AES-256-CFB8 AES-256-OFB AES-192-CBC AES-192-CFB1 AES-192-CFB8 AES-192-OFB CAMELLIA-256-CBC CAMELLIA-256-CFB CAMELLIA-256-CFB1 CAMELLIA-256-CFB8 CAMELLIA-256-OFB CAMELLIA-192-CBC CAMELLIA-192-CFB CAMELLIA-192-CFB1 CAMELLIA-192-CFB8 CAMELLIA-192-OFB	AES-256-CBC
Authentication Algorithm	Authentication is the process of verifying the encrypted data was sent by the sender and was not altered.	List of authentication algorithms. SHA1-160 SHA-160 RSA-SHA1-160 RSA-SHA2-160 RSA-SHA-160 DSA-SHA1-160 DSA-SHA1-old-160 DSA-SHA-160 DSA-160 RIPEDMD160-160 RSA-RIPEDMD160-160 ecdsa-with-SHA1 SHA-224 RSA-SHA-224 SHA-256 RSA-SHA-256 SHA-384 RSA-SHA-384 SHA-512 RSA-SHA-512 whirlpool-512	SHA-256

Setting	Description	Range	Default
Custom Option	Enter any options to be added to the VPN Server Configuration. Custom options that overlap the standard options take precedence. All options appear in this field, separated by semicolons. For example: reneg-sec 900; keepalive 90 To edit this field: 1. Click the **Edit** button. Result: The Configure Custom Option window appears. 2. Click the **Add** button. Result: A line appears as a Custom Option. 3. Type in the option text. 4. Click **Save**. **NOTICE** Custom Options are advanced options and take precedence over the standard configuration options. The standard options are secure by default. Implementing custom options can impact the security strength (e.g. using weak ciphers such as DES*, RC2-*, and BF-*). The customer assumes risk of weakened security when implementing custom options. Consult the online OpenVPN literature for guidance.	Text string For example: • reneg-sec • tun-mtu 1500; mssfix 1300 • fragment 1400; • mssfix • tls-cipher TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA • socket-flags TCP_NODELAY • push "socket-flags TCP_NODELAY"	blank

NOTE: VPN Client Configuration (Client Name, Routing and White List) needs to be done by VPN Client.

Configure D.20

The D.20 Subsystem is responsible for:

- Monitor and maintain the code and configuration of every D.20 peripheral in the connected network.
- Present all hardware inputs and outputs provided by the D.20 peripherals as discrete system points of the appropriate data type in the Real Time Database (RTDB) of MCP.
- Send output commands on analog and digital output system points received via the RTDB to the peripheral output associated with the affect system point.
- Monitor the health of each D.20 peripheral in the network and report any issues to the user.

Add a D.20 Peripheral

You manage the D.20 Peripheral connections on the MCP on the **Connection** tab on the **Configuration** page.

D.20 client can use the default peripheral map files or can create the custom peripherals. The MCP includes all supported peripherals default client maps. If you require a custom mapfile, create it first before setting up the connection. See Client Maps.

» To add a D.20 peripheral:

1. On the Connections tab, select D.20 peripheral Block A under D20 connections.
2. Select **Add** option from right button corner of the window to add peripherals, the fields under block settings.

3. Type in the number of peripherals to be connected.
4. Click **Add** to create the new D.20 peripheral connections.
   Result: A new peripheral connection appears as a row in the table at the bottom of the pane.
5. In the **D20 Address Hex** column, select the peripheral address.
   Result: The peripheral's D.20 Number is computed based on the selected peripheral address with parity setting (see D20 Address settings).
6. In The peripheral type column select the peripheral type.
7. In the **Map File** column, select the appropriate Map File for that peripheral.
   Result: The selected Map File is assigned to that peripheral.
8. Update the **Line ID**, **Device ID**, **Cabinet No**, and **Rack Position** as required. Use a unique identifier for the Line ID.
9. Click **Save.**
   Result: The changes are saved. Before continuing, wait for the dialog box announcing that the configuration has been saved.
10. Click **Commit Changes**.
    Result: The changes are applied to the MCP device.

Modify Peripheral Connections

On the **Connections** tab in the **Configuration** pane you can modify the settings of configured peripheral connections.

» To modify a peripheral connection

1. Select a connection row in the peripheral connections table.
2. Double-click or select a peripheral connection table field and enter a new value.
3. Click **Save.**
   Result: The changes are saved.
4. Click **Commit Changes**.
   Result: The changes are applied to your MCP device.

Delete Peripheral Connections

On the **Connections** tab in the **Configuration** pane you can delete configured peripheral connections.

» To delete a peripheral connection

1. Select a connection row in the peripheral connections table.
2. Click **Delete**.
   Result: The item is removed from the connections table.
3. Click **Save.**
   Result: The changes are saved.
4. Click **Commit Changes**.
   Result: The changes are applied to your MCP device.

Import D20 Peripheral Link

The D.20 IO (B003) part of a D20/200/MX RTU configuration of can be automatically imported into the MCP. This process will configure the entire D.20 Client with identical parameters as the D20 RTU (D.20 communication settings, IO points and associated settings).

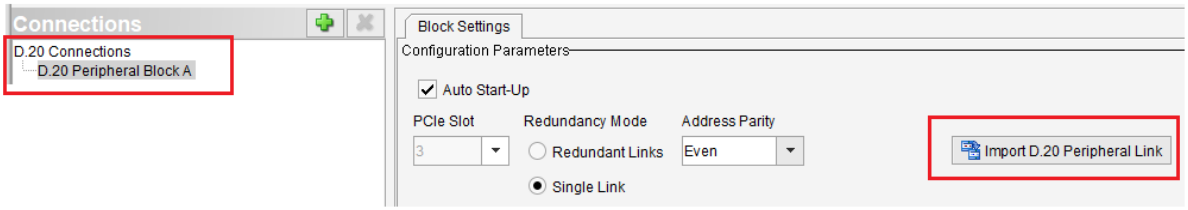
Only one instance of D.20 (B003) can be imported to MCP in this release.

Pre-requisites:

Computer with DSAS and both MCP Studio and D2X Studio installed.

D20 RTU archive / device configuration.

1. Enable D2X Studio if launched DSAS MCP.
2. Ensure the D20 RTU configuration is present in the DSAS repository, in same computer as the one used to configure the MCP (can be different project).
3. Perform a Generate Configuration on the D20 RTU (this is required to identify and correct potential errors). If this cannot be done because the RTU configuration is considered to be "master" – then please make a copy of it and generate the copy.
4. Open MCP offline editor, in Connections, select the D.20 branch on the left side and then click on the button "Import D.20 Peripheral Link" on the right:



5. Follow the prompts and select the D20 RTU from Step 3. Click Next, and on next page click Finish.
6. Result: the D.20 configuration has been copied into the MCP.
7. Click Save / Commit. The MCP device can now talk to the D.20 IO modules same as the D20 RTU was able to do.

Note:

The imported data will be automatically named based on the source D20 RTU configuration, as following:

Line ID	Bay ID	Device ID	Peripheral Number	D.20 Address Hex	Peripheral Type	Map File	Cabinet Number	Rack Position
{RTU_Name} {Processor#}	PCIe 3	D.20 IO {# from D20 RTU}	1	0x03 (0000 0011)	WesdacD20C1	Block_A/D20C1_P1_x03.xml Edit	{From D20RTU}	{From D20RTU}

Line ID is composed of:

- {*RTU_Name*} = name of the D20 RTU device in Step 3
- {*Processor #*} = number of the processor (for single node D20 is always "Proc1"

Bay ID is always the PCIe slot of the MCP, cannot be changed

Device ID is the D.20 IO # coming from the D20 RTU

Peripheral Number comes from the D20 RTU

Peripheral Address comes from the D20 RTU

Peripheral Type comes from the D20 RTU

Cabinet Number comes from the D20 RTU

Rack Position comes from the D20 RTU

Each imported D.20 IO module will have its own D.20 client map file, automatically named based on the following naming convention, to be easily cross referenced with the original D20 RTU IO configuration, based on imported data from D20 RTU:

Block_A is always present and associates with the D20 block of IO imported in the MCP; this is a.

{type}_Peripheral #}_{Peripheral Hex Address}

Map File
Block_A/D20C1_P1_x03.xml
Block_A/D20C1_P2_x05.xml
Block_A/D20S_P3_x06.xml

Application Parameters

The **Application Parameters** tab allows you to view and modify the protocol settings for a specific client connection. Application parameters are available on the **Connection** tab on the **Configuration** page.

» To create a custom application parameter profile

1. On the **Connection** tab, select D.20 Peripheral BlockA under D.20 Connections
2. Under **Application Parameters**, select **Use Custom** and click **Create**. The **Application Parameters** window opens.
3. To modify a parameter, double-click the associated value and enter a new value or select from the drop-down list.
4. When you are done, click **Save**.
5. On the **Save As** window, enter a filename and click **Save**.
6. Click **Save Configuration** to save your changes.

» To modify application parameters

1. On the **Connection** tab, select D.20 Peripheral BlockA under D.20 Connections
2. Under **Application Parameters**, select **Use Custom** and click **Edit**.
3. Change the required settings and click **OK**
   Result: The **Application Parameters** window opens.
4. To modify a parameter, double-click the associated value and enter a new value or select from the drop-down list.
5. When you are done, click **Save**.
6. On the **Save As** window, enter a filename and click **Save**.
7. Click **Save Configuration** to save your changes.

» To view application parameters

1. Go to the **Connection** tab, select D.20 Peripheral BlockA under D.20 Connections.
2. Under **Application Parameters.** select **Use Default** and then click **Show**.
   Result: The **Application Parameters** window opens.

Configuration Parameters

Setting	Description	Range	Default
Auto Start	Indicates if the client application automatically starts when the configuration is changed and reloaded or when the MCP re-boots.	Disabled Enabled	Disabled
Redundancy	This option differs in the way the peripherals are connected physically to MCP.	"Single Link" “Redundant Links”	Single Link
Address Parity	The automatically generated peripheral address, which is based upon the jumpers settings on peripherals, where the top jumper setting is for the parity bit and can be configured based on the DSAS address configuration. The address is equal to the peripheral number with the parity bit appended as the least significant bit. (for example, the address	Even / Odd	Even

	of peripheral 3 is 00000110 (0x06) with even parity, or 00000111 (0x07) with odd parity).		
Import D.20 Peripheral Link	This feature allows user to import existing D.20 configurations from D20MX projects into MCP. Refer Import D20 Peripheral Link.	N/A	N/A

Peripheral connection parameters table

Parameter	Description	Range	Default
Line ID	Text description to identify the electrical transmission line associated with this peripheral.	1 to 64 ASCII characters	Line ID
Device ID	Text description to identify the device associated with this peripheral.	1 to 64 ASCII characters	Device ID
D20 Address	The automatically generated peripheral address which is based upon the peripheral number and the configured address parity. The address is equal to the peripheral number with the parity bit appended as the least significant bit (for example, the address of peripheral 3 is 00000110 (0x06) with even parity, or 00000111 (0x07) with odd parity).	0x3 (0000 0011) to 0xF0 (1111 0000)	Not applicable
Peripheral Type	Select the type of peripheral to be configure	WesdacD20A, WesdacD20S, WesdacD20K, WesdacD20C0, WesdacD20C1, WesdacD20C2,	Not applicable
Map File	Either a standard or custom-created client map file defining the points available from the peripheral.	Select the Mapfile	WesdacD20S_template
Cabinet Number	Text description to identify the cabinet associated with this peripheral. This parameter is provided for informational purposes only and may be used in a report-generation capability in a future release.	1 to 32 ASCII characters	Cabinet ID
Rack Position	The customer or manufacturing reference number for the location of the peripheral in the rack.	1 to 32 ASCII characters	Rack ID

D.20 Application Configuration parameters

The D.20 Client map defines how the MCP is configured to poll data from D.20 peripherals. D.20 application supports two types of configuration parameters options.

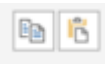
Table 6.106: D.20 Link Configuration parameters

Parameter	Description	Range	Default
Global Delay	Length of time between the transmission of a global message and the polling of the first peripherals (milliseconds)	0 to 65535	10ms

Wait Time	Length of time the D.20 Peripheral Link Client waits before trying to communicate with the peripheral board after a serious error (milliseconds)	0 to 65535	5
Network Retries	Maximum number of times the D.20 Peripheral Link Client tries to consecutively poll the peripheral after it detects a failure.	0 to 65535	3
Scan Interval	How often the D.20 Peripheral Link Client will scan all the D.20 Peripherals for data (milliseconds)	10 to 1000	50
Analog Input Scan Rate	Rate that the D.20 peripheral link client polls the peripherals for analog input information. The integrity scan interleaving option overrides the analog input scan rate (milliseconds)	1 to 65535	4000
Analog Ref Scan Rate	Rate that the D.20 Peripherals Link Client performs the scheduled scan of the peripheral for the on-board analog input reference. The integrity scan interleaving option overrides the analog reference scan rate (milliseconds)	1 to 65535	60000
Binary Scan Rate	Rate that the D.20 peripheral link client polls the peripherals for digital input information. The integrity scan interleaving option overrides the digital input scan rate (milliseconds)	1 to 65535	2000
SOE Buffer size	The maximum number of SOE events that a peripheral can report at one time. Typically, 10.	1 to 255	10
Control Output Pattern Generation	Enable or Disable the capability of the client to operate several control points simultaneously.	Enable/Disable	Enabled
Integrity Scan Type	Selected interleaved or scheduled integrity scan	Scheduled/ Interleaved	Interleaved
Standby Accumulator	Specify if the standby device in a warm redundant system maintains the current accumulator counts for the peripherals. In a hot standby redundant system, the standby device always maintains the current accumulator counts.	Yes/No	Yes
Max Polls	Specify the number of consecutive successful polls to turn the health pseudo point on D.20 communication parameter. Advanced max polls.	1 to 65535	1
Max Retries	Specify the number of consecutive retried polls to turn the health pseudo point OFF. Advanced max polls.	5 to 65535	5

Additional configuration feature

DSAS supports easy way of configuration for each and every point detail in client map files. With this feature user can copy point details of map file into excel and after modification all points will be copied in the map file.

Use the Copy and Paste  options to copy the point details into the Excel sheet. Select the point details which needs to be copied and click copy icon and copy them into the excel sheet. Modify the point details in the excel sheet and copy them from the excel sheet and click paste icon to import the point details content from Excel.

NOTE: If you enter a value that is out of range, *DSAS* will show a warning and automatically insert the lowest or highest value that it can accept as appropriate.

Configuring Client Applications

This chapter contains the following sections and sub-sections:

Connection

Configure Serial Applications

DNP3 Multi-drop

IEC 60870-5-101 Multi-drop

IEC 60870-5-103 Multi-drop

Modbus Multi-drop

Generic ASCII Client

SEL Binary

LogicLinx Device

Terminal Server

Configure Network Clients

DNP IED Block

IEC 60870-5-104 IED Block

Modbus TCP or TCP/SSH IED Block

SNMP Block

Note: IEC61850 Client Configuration will be done using IEC61850 Loader in the DS Agile MCP Studio.

Client Configuration Overview

You can customize the MCP to poll, receive and store the necessary data from connected Intelligent Electronic Devices (IEDs). Client applications in the MCP allow the MCP to collect event and/or static data from devices through different communication protocols and store the data in the system point database.

The MCP configuration tool supports configuration of protocol-specific object references, scaling factors, and user-defined names for various objects configured for collection. Where applicable, you can also configure additional device-level settings (for the same protocol) at the same time.

» To configure the MCP to communicate with devices, perform the following typical tasks:

1. Create MCP client map file for each device and protocol type.
2. Define the data points list and set point properties.
3. Set protocol-specific properties.
4. Set up serial and network device connections.
5. Configure protocol-specific settings for each device connection.
6. Save the configuration file.
7. Run the configuration file in the MCP by committing the changes.

DNP3 Multi-drop

The following settings are used when configuring a DNP3 Multi-drop connection. If a Modem connection is used, refer to the additional settings defined in Dial-up Modem Settings.

DNP3 Multi-Drop Settings

Table 6.107: DNP3 Multi-Drop Settings

Setting	Description	Range	Default
Auto Start	Indicates if the client application automatically starts when the configuration is changed and reloaded or when the MCP re-boots.	Disabled Enabled	Disabled
Line ID	Text description to identify the electrical transmission line associated with this serial connection.	1 to 64 ASCII characters	Line X
Device ID	Text description to identify the device associated with this serial connection.	1 to 64 ASCII characters	Device X
Bay ID	Text description to identify the bay area associated with this serial connection.	1 to 256 ASCII characters	Bay X
IED Address	Protocol address of the device (i.e. DNP3 device address)	0 to 65519	X
Map File	Name of the Client map file to be used with the specific device.	List of users configured client map files.	N/A
Enable on Start Up	Indicates if communication to the device automatically starts when the configuration is changed and reloaded or when the MCP re-boots.	Disabled Enabled	Disabled

DNP3 Client Application Parameters

DNP3 client settings are available under the **Application Parameters** field and these settings will apply to all multi-dropped devices in a connection.

Tip: If the configured number of DNP IEDs is more than 80, then it is recommended to use higher values for the settings:

- Response Timeout, such as 5 seconds
- Max Offline Fail Count, such as 3

DNP3 Client Application Settings

Table 6.108: DNP3 Client Application Settings

Setting	Description	Range	Default
Master Address	Address of the DNP3 client application. Must be different from all configured devices on this port.	0 to 65519	100
IIN Class 1 Action	True: Master polls Class 1 data when IIN Class 1 available data is received. False: Ignore "Class 1" IIN. Class 1 Data events are typically very important and should be retrieved from the target device as soon as the indication is received	True False	True

Setting	Description	Range	Default
IIN Class 2 Action	True: Master polls Class 2 data when IIN Class 2 available data is received. False: Ignore "Class 2" IIN. Class 2 Data events are typically very reasonably important and should be retrieved from target device as soon as the indication is received	True False	True
IIN Class 3 Action	True: Master polls Class 3 data when IIN Class 3 available data is received. False: Ignore "Class 3" IIN. Some target devices generate large numbers of insignificant Class 3 events. To minimize I/O traffic, set to False.	True False	True
IIN Time Sync Action	True: Master performs time sync when IIN Time Synchronization Required message is received. False: Ignore IIN Time Synchronization Required message. If a target device requests a time sync, it should be given one, unless the target device has access to another clock than the MCP	True False	True
Time Sync Every Integrity Poll	True: Send out a "Time Sync" message to a target device each time an "Integrity Poll" message is sent to that device. False: Do not send out a "Time Sync" message to a target device each time an "Integrity Poll" message is sent to that device. In general, if a target device needs a time sync, it requests one. This setting should be used only if there is a known problem with the target device's clock.	True False	True
Enable Stagger Integrity Poll	Specifies whether Staggered Integrity polling is enabled or not. True: The DNP3 client ignores the Integrity Poll Interval configured for the devices and utilizes an internal scheduling mechanism to determine when the next integrity poll should be transmitted. False: Do not enable staggered integrity polling. Use the configured settings.	True False	False
Stagger Integrity Interval	If Staggered Integrity polling is enabled, the DNP3 client schedules Integrity polls to devices based on the interval (in seconds) specified here.	30 to 36000	600
Max Switch Fail Count	Maximum number of consecutive failed requests the DNP3 client must see before it attempts to establish communications on the Backup Port.	1 to 300	1
Max Offline Fail Count	Maximum number of consecutive failed requests to a device before the RTDB points is marked offline.	1 to 300	2
Wait Between Messages	Time (in seconds) to wait between two consecutive messages sent on the serial port	0 to 60	0.0
Confirmation Delay	Time in seconds to delay application layer acknowledgment on single fragment solicited or unsolicited responses.	0 to 2	2

Setting	Description	Range	Default
Response Timeout	Time (in seconds) to wait for an application layer response before deciding it has failed. Set the value higher for a dial-up modem connection, i.e. 40.	0 to 60	2.0
Time Zone	This option allows you to configure a custom time zone offset which is applied to messages received through this application. By default, the timestamps of messages received through the DNPDPA are in UTC time.	One of listed Time Zones and geographic locations	UTC
Enable/Disable DNPDCA Post TCP Delay	This feature is enabled or Disabled per DNPDCA instance and is applicable to TCP-based DNP IEDs. Use this command to enable or disable the first DNP poll request after TCP connection since the configured DNPDCA instance is delayed by data link time-out.	True False	False

DNP IED Block

The following settings are used when configuring a DNP3 IED block.

NOTE: It is recommended that the total number of IEDs configured in one IED block be limited to 10 IEDs. If more than 10 IEDs are configured in a single multi-drop connection, data connection performance degrades.

DNP3 IED Block connection settings

Table 6.109: DNP3 IED Block connection settings

Setting	Description	Range	Default
Auto Start	Indicates if the application automatically starts when the configuration is changed and reloaded or when the MCP re-boots.	Disabled Enabled	Disabled
Enable Dual Endpoint	Enable or disable TCP dual end point. A dual end point enables the MCP to listen for connection requests from remote devices. If enabled, either side may initiate the connection; the master to send controls, integrity polls, and so on, and the remote device to report unsolicited data. If a remote device establishes a connection, the connection is closed after the period of time specified in the Auto-Disconnect setting. If both sides simultaneously initiate the connection, the connection initiated by the MCP is maintained while the other is dropped. This feature is not supported for devices using the UDP transport layer.	Disabled Enabled	Disabled
Port	The MCP port configured to receive data from remote devices.	1 to 65535	N/A
Auto Disconnect	The amount of time, in seconds, that the MCP allows to pass with no received transmissions before the connection to the remote device is closed. If set to 0, auto disconnect is disabled.	0 to 65535	10

Setting	Description	Range	Default
Application Parameters	Select the application parameters defining this connection. The default parameters can be used, or a custom configuration can be created. Refer to *DNP3 Application Parameters*.	Use Default Use Custom	Use Default
Line ID	Text description to identify the electrical transmission line associated with this connection.	1 to 64 ASCII characters	Line X
Device ID	Text description to identify the device associated with this connection.	1 to 64 ASCII characters	Device X
Bay ID	Text description to identify the bay area associated with this connection.	1 to 256 ASCII characters	Bay X
IED Address	DNP3 address of the device.	0 to 65519	N/A
Map File	Name of the client map file to be used with the specific device.	List of users configured map files.	N/A
IP Address	IP Address of the device. Must be unique from other configured devices.	Valid IPv4 address	0.0.0.0
Backup IP Address	Redundant backup IP Address of the device.	Valid IPv4 address	0.0.0.0
Network Port Number	The port number on which the device communicates.	0 to 65535	20000
Transport Layer	Transport mode for IED communication.	TCP or UDP	TCP
Enable on Start Up	Indicates if communication to the device automatically starts when the configuration is changed and reloaded or when the MCP re-boots.	Enabled Disabled	Disabled

DNP3 application specific settings are available under the **Application Parameters** field.

DNP3 Application Parameters

Tip: If the configured number of DNP IEDs is more than 80, then it is recommended to use higher values for the settings:

- Response Timeout, such as 5 seconds
- Max Offline Fail Count, such as 3

Table 6.110: DNP3 Application Parameters

Setting	Description	Range	Default
Master Address	DNP3 address of the MCP. Must be different from all configured devices on this port.	0 to 65519	100
IIN React Class1	True: Respond to "Class 1" IIN in a message by requesting class 1 event data. False: Ignore "Class1" IIN Class 1 Data events are typically very important and should be retrieved from the target device as soon as the indication is received	True False	True

Setting	Description	Range	Default
IIN React Class2	True: Respond to "Class 2" IIN in a message by requesting class 2 event data. False: Ignore "Class2" IIN Class 2 Data events are typically very reasonably important and should be retrieved from target device as soon as the indication is received	True False	True
IIN React Class3	True: Respond to "Class 3" IIN in a message by requesting class 3 event data. False: Ignore "Class3" IIN Some target devices generate large numbers of insignificant Class 3 events. To minimize I/O traffic, set to False.	True False	True
IIN React Time Sync	True: Respond to "Need Time Sync" IIN in a message by sending a "Time Sync" message. False: Ignore "Need Time Sync" message If a target device requests a time sync, it should be given one, unless the target device has access to another clock than the MCP	True False	True
Integrity Time Sync	True: Send out a "Time Sync" message to a target device each time an "Integrity Poll" message is sent to that device. False: Do not send out a "Time Sync" message to a target device each time an "Integrity Poll" message is sent to that device. In general, if a target device needs a time sync, it requests one. This setting should be used only if there is a known problem with the target device's clock.	True False	False
Stagger Integrity Enable	Specifies whether Staggered Integrity polling is enabled or not. True: The DNP3 client ignores the Integrity Poll Interval configured for the devices and utilizes an internal scheduling mechanism to determine when the next integrity poll should be transmitted. False: Do not enable staggered integrity polling. Use the configured settings.	True False	False
Stagger Integrity Interval	If Staggered Integrity polling is enabled, the DNP3 client schedules Integrity polls to devices based on the interval (in seconds) specified here.	30 to 36000	600
Max Switch Fail Count	Maximum number of consecutive failed requests the DNP3 client must see before it attempts to establish communications on the Backup Port.	1 to 300	1
Device Offline Fail Count	Number of consecutive failed requests to a device before the RTDB points is marked offline.	1 to 300	2
Wait Between Messages	Time (in seconds) to wait between two consecutive messages sent on the serial port or network connection.	0 to 60	0.0
Confirmation Delay	Time in seconds to delay application layer acknowledgment on single fragment solicited or unsolicited responses.	0 to 2	0
Response Timeout	Time (in seconds) to wait for an application layer response before deciding it has failed.	0 to 60	2.0

Setting	Description	Range	Default
Time Zone	This option allows you to configure a custom time zone offset which is applied to messages received through this application. By default, the timestamps of messages received through the DNPDPA are in UTC time.	One of listed Time Zones and geographic locations	UTC
DelayFirstReqPostTCPConn	This feature is enabled or Disabled per DNPDCA instance and is applicable to TCP-based DNP IEDs. Use this command to enable or disable the first DNP poll request after TCP connection since the configured DNPDCA instance is delayed by data link time out.	false or true	false

IEC 60870-5-101 Multi-drop

The following settings are used when configuring an IEC 60870-5-101 Multi-drop connection.

IEC 60870-5-101 Multi-drop Settings

Table 6.111: IEC 60870-5-101 Multi-drop Settings

Setting	Description	Range	Default
Link Address Size	The number of octets used for the link address of the device.	1 or 2	1
Auto Start	Indicates if the client application automatically starts when the configuration is changed and reloaded or when the MCP re-boots.	Disabled Enabled	Disabled
Application Parameters	Select the application parameters defining this connection. The default parameters can be used, or a custom configuration can be created. Refer to *IEC 60870-5-101 Multi-drop Application* Settings.	Use Default Use Custom	Use Default
Line ID	Text description to identify the electrical transmission line associated with this serial connection.	1 to 64 ASCII characters	Line X
Device ID	Text description to identify the device associated with this serial connection.	1 to 64 ASCII characters	Device X
Bay ID	Text description to identify the bay area associated with this serial connection.	1 to 256 ASCII characters	Bay X
Common Address of ASDU	The device's common address of ASDU.	1 to 65534	1
Link Address	The link address of the device.	0 to 65535	1
Map File	Name of the Client map file to be used with the specific device.	List of users configured client map files.	N/A
Enable on Start Up	Indicates if communication to the device automatically starts when the configuration is changed and reloaded or when the MCP re-boots.	Disabled Enabled	Disabled

IEC 60870-5-101 Multi-drop Application

IEC 60870-5-101 client specific settings are available under the **Application Parameters** field.

Table 6.112: IEC 60870-5-101 Multi-drop Application Settings

Setting	Description	Range	Default
Application Tab			
Number of Message Buffers	The number of message buffers allocated by the application used to receive messages and to transmit requests to the remote devices.	1 to 65535	5
Device Restart Delay	The delay (in seconds) between each device restart sequence at application start-up.	0.0 to 3600.0	0.0
Stagger General Interrogation	Specifies whether or not GI polls performed by the application are staggered.	Enabled Disabled	Disabled
GI Qualifier	The Qualifier to use for the General Interrogation poll.	Global, Group 1 through Group 16	Global
GI Stagger Interval	The staggered GI poll interval (in minutes).	0.0 to 1440.0	30.0
Time Zone	The Time Zone of the timestamps exchanged between this instance of the Client and all IEDs it communicates with. **NOTE**: If a different time zone is required for a IED, you need to create a new instance of the Client.	One of listed Time Zones and geographic locations	UTC
Backoff Time	The time (in seconds) to wait before the application tries to re-contact a device after a communication failure.	0 to 65535	30
Minimum Inter Poll Delay	The minimum time delay (in minutes) between any two consecutive application level polls.	0.0 to 1440.0	0.0
Ignore Unrequested GI Data	Specifies if the DCA will ignore data reported with a cause of transmission of one of the interrogation types (i.e. 20-36) when there is no GI pending.	Enabled or Disabled	Disabled
Max ADSU Frame Length	The maximum value for the length (in octets) of non-background messages (excluding framing overhead).	24 to 255	255
Extra Frame Timeout	The time (in milliseconds) that the application adds to the frame timeout calculation.	0 to 65535	150
Max Confirm Idle Time	The maximum communication idle time (in milliseconds) before the application must receive a confirm message.	1 to 65535	100
Max Respond Idle Time	The maximum communication idle time (in milliseconds) before the application must receive a respond message.	1 to 65535	100
Max Transmit Retries	The maximum number of transmissions retries before declaring that communication with a remote device has failed.	1 to 255	1
Wait Between Messages	The minimum time (in seconds) to wait between polls (measured from receiving the response of one poll to the beginning of the next poll).	0.0 to 60.0	0.0
Link Transmission Mode	The link transmission mode used by the application. **NOTE**: Backup ports are not supported on *Balanced* mode.	Unbalanced Balanced	Unbalanced
Unbalanced Serial Link Tab			

Setting	Description	Range	Default
Background Polling Interval	The interval (in seconds) of background autonomous polling that happens at the data link layer.	0.0 to 86400.0	3.0
Reply Poll Count	The Maximum number of times to poll a device for Class 2 and 1 data, after receiving a positive acknowledgement at the link layer (CONFIRM:ACK), in response to a "SEND/CONF user data" request at the link layer, that was sent due to an application level request.	0 to 255	10
Max Poll Count	The maximum number of times to poll a device for Class 1 data before changing to poll the next device, while performing background autonomous polling.	1 to 255	3
Balanced Serial Link Tab			
Extra Response Timeout	The time (in milliseconds) to add to the frame timeout calculation.	0 to 65535	200
Inter Frame Gap	The minimum idle time (in milliseconds) between frames transmitted by the application.	0 to 1000	0
Single Char Acknowledgement	Specifies if the application replies to the remote device with a single character acknowledgement.	Enabled Disabled	Disabled

IEC 60870-5-103 Multi-drop

The following settings are used when configuring an IEC 60870-5-103 Multi-drop connection.

Table 6.113: IEC 60870-5-103 Multi-drop Settings

Setting	Description	Range	Default
Auto Start	Indicates if the client application automatically starts when the configuration is changed and reloaded or when the MCP re-boots.	Disabled Enabled	Disabled
Secure Type	Select a security feature to be enabled on the connection. For more information, refer to *Connection Security*.	Disabled Telnet TLS Security SSH Secure Tunnel	Disabled
TLS port	Enter the port number that can be used to access the secure connection.	1 to 65535	50000 + X
File	Select the security parameters defining this connection. After a configuration can be created, it can be saved and reused on other connections. Refer to *Secure Application Parameters*.	List of saved security settings	N/A
Application Parameters	Select the application parameters defining this connection. The default parameters can be used, or a custom configuration can be created. Refer to *IEC 60870-5-103 Multi-drop Application Settings*.	Use Default Use Custom	Use Default
Line ID	Text description to identify the electrical transmission line associated with this serial connection.	1 to 64 ASCII characters	Line X

Device ID	Text description to identify the device associated with this serial connection.	1 to 64 ASCII characters	Device X
Bay ID	Text description to identify the bay area associated with this serial connection.	1 to 256 ASCII characters	Bay X
Common Address of ASDU	The device's common address of ASDU.	0 to 254	1
Link Address	The link address of the device.	0 to 254	1
Map File	Name of the Client map file to be used with the specific device.	List of users configured client map files.	N/A
Enable on Start Up	Indicates if communication to the device automatically starts when the configuration is changed and reloaded or when the MCP re-boots.	Disabled Enabled	Disabled

IEC 60870-5-103 Multi-drop Application Settings

IEC 60870-5-103 settings are available under the **Application Parameters** field.

Tip: It is recommended to configure both the Max Confirm Time and Max Response Time values to be less than the configured Back off Time value.

Table 6.114: IEC 60870-5-103 Application Parameters

Setting	Description	Range	Default
Number of Message Buffers	The number of message buffers allocated by the application used to receive messages and to transmit requests to the remote devices.	1 to 65535	5
TCP Pass Through Port	The TCP port number used by the application to listen for a pass-through service connection from an IED vendor PC program. A port number of 0 disables the Pass-Through connection service.	0 to 65535	0
Passthrough Response Timeout	The duration (in seconds) of silence on the serial interface before the application closes the pass-through connection	1.00 to 300.00	120.0
Max Confirm Idle Time	The maximum communication idle time (in milliseconds) before the application must receive a confirm message.	1 to 65535	100
Max Respond Idle Time	The maximum communication idle time (in milliseconds) before the application must receive a respond message.	1 to 65535	100
Max Transmit Retries	The maximum number of transmission retries before declaring that communication with a remote device has failed.	1 to 255	1
Backoff Time	The time (in seconds) to wait before the application tries to re-contact a device after a communication failure.	0 to 65535	30
Background Polling Interval	The interval (in seconds) of background autonomous polling that happens at the data link layer.	0.0 to 86400.0	3.0

Wait Between Messages	The minimum time (in seconds) to wait between polls (measured from receiving the response of one poll to the beginning of the next poll).	0.0 to 60.0	0.0
Quick Check	Specifies whether or not quick check is performed between standard polling for class data	Enabled Disabled	Enabled
Reply Poll Count	The Maximum number of times to poll a device for Class 2 and 1 data, after receiving a positive acknowledgement at the link layer (CONFIRM:ACK), in response to a "SEND/CONF user data" request at the link layer, that was sent due to an application level request.	0 to 255	10
Max Poll Count	The maximum number of times to poll a device for Class 1 data before changing to poll the next device, while performing background autonomous polling.	1 to 255	3
Reset Link Function Code	The function code for the reset link request	RESET_CU RESET_FCB	RESET_FCB
Time Zone	The time zone for this instance of the DCA or DPA.	One of listed Time Zones and geographic locations	UTC

IEC 60870-5-104 IED Block

The following settings are used when configuring an IEC 60870-5-104 IED block.

Table 6.115: IEC 60870-5-104 IED Block

Setting	Description	Range	Default
Auto Start	Indicates if the client application automatically starts when the configuration is changed and reloaded or when the MCP re-boots.	Disabled Enabled	Disabled
Application Parameters	Select the application parameters defining this connection. The default parameters can be used, or a custom configuration can be created. Refer to *IEC 60870-5-104 IED Block Application Settings*.	Use Default Use Custom	Use Default
Line ID	Text description to identify the electrical transmission line associated with this serial connection.	1 to 64 Unicode characters	Line X
Device ID	Text description to identify the device associated with this serial connection.	1 to 64 Unicode characters	Device X
Bay ID	Text description to identify the bay area associated with this serial connection.	1 to 256 Unicode characters	Bay X
Common Address of ASDU	The device's common address of ASDU.	0 to 254	1
Map File	Name of the Client map file to be used with the specific device.	List of users configured client map files.	N/A
IP Address	IP Address of the device.	Single IP Address	0.0.0.0

Backup IP Address	Redundant backup IP Address of the device.	Single IP Address	Blank
Network Port #	The port number on which the device communicates.	0 to 65535	2404
Transport Layer	Whether to use TCP or UDP network protocol.	Non-editable	TCP
Enable on Start Up	Indicates if communication to the device automatically starts when the configuration is changed and reloaded or when the MCP re-boots.	Enabled Disabled	Disabled

IEC 60870-5-104 IED Block Application Settings

IEC 60870-5-104 settings are available under the Application Parameters field.

Table 6.116: IEC 60870-5-104 IED Block Application Parameters

Setting	Description	Range	Default
Application Tab			
Number of Message Buffers	The number of message buffers allocated by the application used to receive messages and to transmit requests to the remote devices.	1 to 65535	5
Device Restart Delay	The delay (in seconds) between each device restart sequence at application start-up.	0.0 to 3600.0	0.0
Stagger General Interrogation	Specifies whether or not General Interrogation (GI) polls performed by the application are staggered.	Enabled Disabled	Disabled
GI Qualifier	The Qualifier to use for the General Interrogation poll.	Not editable	Blank
GI Stagger Interval	The staggered General Interrogation poll interval (in minutes).	Not editable	Blank
Time Zone	The Time Zone of the timestamps exchanged between this instance of the Client and all IEDs it communicates with. **NOTE**: If a different time zone is required for a IED, you need to create a new instance of the Client.	One of listed Time Zones and geographic locations	UTC
Backoff Time	The time (in seconds) to wait before the application tries to re-contact a device after a communication failure.	0 to 65535	30
Minimum Inter Poll Delay	The minimum time delay (in minutes) between any two consecutive application level polls.	0.0 to 1440.0	0.0
Network Tab			
Max Length APDU Frame	The maximum length (in octets) of APDU frames.	253	Not editable

Modbus Multi-drop

The following settings are used when configuring a Modbus Multi-drop connection.

Table 6.117: Modbus Multi-drop Settings

Setting	Description	Range	Default
Auto Start	Indicates if the client application automatically starts when the configuration is changed and reloaded or when the MCP re-boots.	Disabled Enabled	Disabled

Secure Type	Select a security feature to be enabled on the connection. For more information, refer to *Connection Security*.	Disabled Telnet TLS Security SSH Secure Tunnel	Disabled
TLS port	Enter the port number that can be used to access the secure connection.	1 to 65535	50000 + X
File	Select the security parameters defining this connection. After a configuration can be created, it can be saved and reused on other connections. Refer to *Secure Application Parameters*.	List of saved security settings	N/A
Line ID	Text description to identify the electrical transmission line associated with this serial connection.	1 to 64 ASCII characters	Line X
Device ID	Text description to identify the device associated with this serial connection.	1 to 64 ASCII characters	Device X
Bay ID	Text description to identify the bay area associated with this serial connection.	1 to 256 ASCII characters	Bay X
IED Address	Protocol address of the device (i.e. Modbus device address)	1 to 254	X
Map File	Name of the Client map file to be used with the specific device.	List of users configured client map files.	N/A
Enable on Start Up	Indicates if communication to the device automatically starts when the configuration is changed and reloaded or when the MCP re-boots.	Disabled Enabled	Disabled

Modbus TCP or TCP/SSH IED Block

The following settings are used when configuring a Modbus TCP or TCP/SSH IED block.

Table 6.118: Modbus TCP or TCP/SSH IED Block connection settings

Setting	Description	Range	Default
Auto Start	Indicates if the application automatically starts when the configuration is changed and reloaded or when the MCP re-boots.	Disabled Enabled	Disabled
Line ID	Text description to identify the electrical transmission line associated with this connection.	1 to 64 ASCII characters	Line X
Device ID	Text description to identify the device associated with this connection.	1 to 64 ASCII characters	Device X
Bay ID	Text description to identify the bay area associated with this connection.	1 to 256 ASCII characters	Bay X
IED Address	Address of the device.	1 to 254	N/A
Map File	Name of the client map file to be used with the specific device.	List of users configured map files.	N/A
IP Address	IP Address of the device. Must be unique from other configured devices.	Valid IPv4 address	0.0.0.0

Setting	Description	Range	Default
Network Port Number	The port number on which the device communicates.	0 to 65535	502
Protocol	Indicates which protocol (TCP or TCP/SSH) is to be used for Modbus IED Communication. Double click on this field to select TCP or TCP/SSH. Currently this feature is only available for UR IEDs.	TCP or TCP/SSH	TCP
SSH Parameters	Configure the SSH parameters required for this connection if Protocol configured as TCP/SSH; otherwise this field is greyed out. The default parameters can be used, or a custom configuration can be created. Refer to Modbus TCP or TCP/SSH IED Block configuration parameters for more information.	Use Default Use Custom	Use Default
Enable on Start Up	Indicates if communication to the device automatically starts when the configuration is changed and reloaded or when the MCP re-boots.	Enabled Disabled	Disabled

Generic ASCII Client

The Generic ASCII application is designed to extract data from devices using an ASCII-based communications protocol over a serial port. The information collected from these devices is stored in the internal system database of the MCP.

Fault and Event Information is collected from connected devices, as well as Protective Relay Fault Information to facilitate user notification of faults. This support is available for the SEL family of devices.

The Generic ASCII application supports multi-drop device configuration and multi-encoding formats; that is, Hex, Decimal, Binary, Packed BCD and ASCII.

NOTE: The Generic ASCII application does not support operation of controls on external devices.

The following settings are used when configuring a Generic ASCII connection.

Table 6.119: Generic ASCII Settings

Setting	Description	Range	Default
Auto Start	Indicates if the client application automatically starts when the configuration is changed and reloaded or when the MCP re-boots.	Disabled Enabled	Disabled
Support Multi-Drop	Indicates if the client application supports Multi-Drop serial devices. If selected, you can add multiple ASCII IED blocks in the client application.	Disabled Enabled	Enabled
Application Parameters	Select the application parameters defining this connection. The default parameters can be used, or a custom configuration can be created. Refer to Generic ASCII Client Application Settings.	Use Default Use Custom	Use Default
Secure Type	Select a security feature to be enabled on the connection. For more information, refer to *Connection Security*.	Disabled Telnet TLS Security SSH Secure Tunnel	Disabled

Setting	Description	Range	Default
TLS port	Enter the port number that can be used to access the secure connection.	1 to 65535	50000 + X
File	Select the security parameters defining this connection. After a configuration can be created, it can be saved and reused on other connections. Refer to *Secure Application Parameters*.	List of saved security settings	N/A
Line ID	Text description to identify the electrical transmission line associated with this serial connection.	1 to 64 ASCII characters	Line X
Device ID	Text description to identify the device associated with this serial connection.	1 to 64 ASCII characters	Device X
Bay ID	Text description to identify the bay area associated with this serial connection.	1 to 256 ASCII characters	Bay X
Map File	Name of the Client map file to be used with the specific device.	List of users configured client map files.	N/A
IED Address	Address to identify the specific device in the multi-drop device configuration. The IED Address defined can be referenced during a Transaction definition in the Client Map File using variable {$ADDR$}. Refer to IED Address Configuration.	0 to 99999	X
Enable on Start Up	Indicates if communication to the device automatically starts when the configuration is changed and reloaded or when the MCP re-boots.	Disabled Enabled	Disabled
Password	For devices that require a password to access information. The provided password will be stored in encrypted format.	1 to 32 ASCII characters	N/A

IED Address Configuration

The IED Address identifies the specific device in the multi-drop device configuration.

The IED Address defined in the Connection page is available as a variable {$ADDR$} for further use while configuring Transaction Messages and Valid Response Pattern parameters in the Client Map File.

For example:

To define a Transaction Message to be sent to a device which contains the IED Address:

Device 1 : IED Address: 1241

Transaction Message: 1231241,I01241

Device 2 : IED Address: 1242

Transaction Message: 1231242,I01242

The required Transaction Message is to be configured using one of the following methods:

Method 1 : Define a single Client Map file for both the devices with Message Out as 123{$ADDR$},I0{$ADDR$} and assign the same Client Map File for both devices in the Connection page.

At runtime, the MCP frames the required Transaction Message as 1231241,I01241 for Device 1 and 1231242,I01242 for Device 2.

Method 2 : Define multiple Client Map files with Message Out as 1231241,I01241 and the other file with Message Out as 1231242,I01242 and assign respective Client Map File for both the devices in the Connection page.

Refer to the Time Sequence Diagrams and Sample Configuration for a more detailed explanation.

SEL Binary

The Schweitzer Engineering Laboratories (SEL) Binary protocol supports the exchange of information with SEL Fast Meter metering and relay devices over a serial link. It also supports pass through connection to the device.

SEL Binary Client Application Parameters

SEL Binary Client application settings are available under the **Application Parameters** field.

Table 6.120: SEL Binary Client Application Parameters

Setting	Description	Range	Default
Wait Between Messages	Duration, in seconds, to wait to transmit a new message after a response to the previous message has been received	0 to 60.00	0.1
Wait Between Cycles	Duration, in seconds, to wait to begin a new cycle of collecting data points after the previous one was complete	0 to 60.00	0
Response Timeout	Maximum duration, in seconds, to wait for a response from the device	0.100 to 300.00	1
Comm Retries	Number of retries on the communications channel before the device is determined offline	0 to 100	2
Passthrough Response Timeout	Duration, in seconds, for which the device waits on the Serial Interface to obtain a response to a communication message received on the Pass-Through socket	1.00 to 300.00	5
Demand Data Poll Cycle	How many times the Fast Meter Data must be retrieved before Demand Data can be polled. 0 disables Demand Data polling.	0 to 36000	600
Peak Demand Data Poll Cycle	How many times the Fast Meter Data must be retrieved before Peak Demand Data can be polled. 0 disables Peak Demand Data polling.	0 to 36000	600
History Poll Cycle	How many times the Fast Meter Data must be retrieved before the History command can be sent to the SEL device. 0 disables the History command.	0 to 36000	3600
Fault Reset Time	Time, in seconds, for which the fault parameter pseudo points retain values from the latest fault.	0 to 3600	5
Restrike Interval	Once the first fault has occurred, the time to wait (in seconds) before updating the Fault Pseudo points with information if subsequent faults occur before this interval has elapsed.	0 to 3600	30

SEL Binary

The following settings are used when configuring a SEL Binary connection.

Terminal emulation settings should be set to CR (carriage return) for <ENTER>.

For example:

- Secure Terminal Emulator from DS Agile MCP Studio, by default sends/receives LF (linefeed) on <ENTER>
- Secure Terminal Emulator serial mode by default sends/receives CR on <ENTER>
- Hyper Terminal, by default sends/receives LF on <ENTER>

Table 6.121: SEL Binary Settings

Setting	Description	Range	Default
Auto Start	Indicates if the client application automatically starts when the configuration is changed and reloaded or when the MCP re-boots.	Disabled Enabled	Disabled
Secure Type	Select a security feature to be enabled on the connection. For more information, refer to *Connection Security*.	Disabled Telnet TLS Security SSH Secure Tunnel	Disabled
TLS port	Enter the port number that can be used to access the secure connection.	1 to 65535	50000 + X
File	Select the security parameters defining this connection. After a configuration can be created, it can be saved and reused on other connections. Refer to *Secure Application Parameters*.	List of saved security settings	N/A
Line ID	Text description to identify the electrical transmission line associated with this serial connection.	1 to 64 ASCII characters	Line X
Device ID	Text description to identify the device associated with this serial connection.	1 to 64 ASCII characters	Device X
Bay ID	Text description to identify the bay area associated with this serial connection.	1 to 256 ASCII characters	Bay X
Map File	Name of the Client map file to be used with the specific device.	List of users configured client map files.	N/A
Enable on Start Up	Indicates if communication to the device automatically starts when the configuration is changed and reloaded or when the MCP re-boots.	Disabled Enabled	Disabled
Password	For devices that require a password to access information.	1 to 32 ASCII characters	N/A

LogicLinx Device

A LogicLinx Device connection is used to define a communications link between the LogicLinx application running on the MCP and a PC running the LogicLinx Editor.

Once assigned, the connection appears with port details.

SNMP Block

SNMP, or Simple Network Management Protocol, is primarily used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. The MCP can be configured to receive SNMP messages on a polled or unsolicited basis.

The following settings are used when configuring an SNMP block.

Table 6.122: SNMP Block connection settings

Setting	Description	Range	Default
Auto Start	Indicates if the application automatically starts when the configuration is changed and reloaded or when the MCP re-boots.	Disabled Enabled	Disabled
Line ID	Text description to identify the electrical transmission line associated with this connection.	1 to 64 ASCII characters	Line X
Device ID	Text description to identify the device associated with this connection.	1 to 64 ASCII characters	Device X
Bay ID	Text description to identify the bay area associated with this connection.	1 to 256 ASCII characters	Bay X
Map File	Name of the client map file to be used with the specific device.	List of users configured map files.	N/A
IP Address	IP Address of the device. Must be unique from other configured devices.	Valid IPv4 address	0.0.0.0
Backup IP Address	Redundant backup IP Address of the device.	Valid IPv4 address	0.0.0.0
Enable on Start Up	Indicates if communication to the device automatically starts when the configuration is changed and reloaded or when the MCP re-boots.	Enabled Disabled	Disabled

Configure to acquire files (ARRM)

Automated Record Retrieval Manager Overview

The Automated Record Retrieval Manager retrieves and stores record files from devices connected to your MCP. The ARRM Viewer can be used to view the status of this application and to initiate manual transfers.

You can retrieve downloaded records from the MCP using any FTP/SCP/SFTP/TFTP/MMS/SEL Binary/Generic ASCII (supports SEL ASCII protocol) client as needed or on a scheduled basis.

You can also configure the MCP to automatically push files to a remote location using the Sync Manager utility. For more information refer to Sync Manager. Also, this application requires additional license (see Software Licensing Tools for more details).

ARRM uses the Trivial File Transfer Protocol (TFTP) or File Transfer Protocol (FTP) or Secure File Transfer Protocol (SFTP) or MMS to retrieve the files from the IED to the device over a local area network (LAN). It is not recommended to perform TFTP or MMS file transfers over WAN systems subject to long and variable packet latencies.

Depending on the IED types and schema used, file retrievals are triggered by:

- The transition of the *RcdMade* digital input point from 0 to 1
- A change in the *FaultNumber* analog input or accumulator point
- Operation of the file retrieval pseudo point, or
- Manual activation through the ARRM application.

The ARRM has the following Primary features and functions:

- Automatic, manual, or connection poll-based retrieval of records from devices
- File naming based on configurable parameters or the IEEE C37.232-2007 File Naming Convention for Time Sequence Data
- File storage organized by device and/or station
- Clearing the file available status on the GE D25 IED
- Easy to use interface accessible through the Online HMI
- Visual indication of device online/offline status
- A simple configuration interfaces
- Pseudo points to trigger file retrievals and to view application status
- Support for MCP system redundancy

ARRM and MCP System Redundancy

In a redundant system setup, the active unit is responsible for retrieving records from devices. Redundancy is supported by mirroring retrieved files on both the active and standby units. The MCP redundancy manager is notified of file or directory changes by the active unit and automatically synchronizes them on the standby unit. This is done as soon as possible but notifications are not made more than every 10 seconds to reduce network traffic.

This is not supported in G100.

ARRM Configuration

The Automated Record Retrieval Manager retrieves and stores from devices connected to your MCP. Examples of files are: Oscillography COMTRADE, SOE logs, Events, Generic data, Information about the IED, IEC 61850 SCL files (IID). The **ARRM** configuration page allows you to configure the ARRM application.

The configuration page is split into two tabs: **Applications** (stations, devices, and file sets), and **File Set Template** (parameters for retrieving files from different types of devices).

ARRM Viewer

The **ARRM Viewer** page is divided into several areas.

Screen Areas

The ARRM Viewer window is comprised of several areas.

Table 6.123: ARRM Viewer - Screen Area

Screen Area	Description
Left pane - Tree view	The left pane provides a hierarchical overview of the stations and devices in your network.

Upper right pane - Device view	The upper right pane shows a tabular listing of devices in your network, including device status and file retrieval status. Selecting a station or device in the left pane filters the grid to only show the selected entries.
Lower right pane - Message log	The lower right pane contains a listing of all communication events (transfer attempts, file downloads, error reports) that have occurred since polling was started. Entries are ordered as they are received, and not necessarily chronologically by their timestamp.
Status Icon	The icon in the bottom right of the window indicates the current connection status of the application.

» To perform actions on devices:

1. Select the station containing the desired device. A listing of devices and file sets within the station is shown.
2. Right-click the row containing the desired file set.
3. On the popup menu, select:
   - **Trigger File Set Retrieval** to manually initiate a file set download. If you select this option, the **Status** field changes to show the progress of the transfer. Status definitions are shown on definition for the Retrieval State pseudo-point.
   - **Clear Recorder Memory** to trigger ARRM to operate the configured digital output point that is mapped to the *MemRs* command. In addition, if the control is successful and the file retrieval method is set to *Fault Number*, ARRM clears the last reported fault number.
   - **Download Files** to save retrieved records from the MCP to your local computer.

ARRM Pseudo Points

The ARRM application makes the following pseudo points available.

Per-Application

Table 6.124: ARRM Pseudo Points - Per Application

Pseudo Point Name	Description
Current Disk Use of ARRM as a Percentage of Total	This analog input pseudo point reports the current disk usage of ARRM on the MCP as a percentage of the total disk space available in the */mnt/datalog/* partition.

Per-File Set

Table 6.125: ARRM Pseudo Points - Per File Set

Pseudo Point Name	Description
Automatic Retrieval Disabled	This digital input pseudo point is set to 1 when automatic retrieval is disabled and is set to 0 when automatic retrieval is enabled. Automatic retrieval can be enabled or disabled using the *Disable Automatic Retrieval* digital output pseudo point.
Clear Recorder Memory	This control triggers ARRM to operate the configured digital output point that is mapped to the *MemRs* command. In addition, if the control is successful and the file retrieval method is set to *Fault Number*, ARRM clears the last reported fault number.
Disable Automatic Retrieval	This digital output pseudo point can be used to disable or enable automatic retrieval of the associated file set. Latch On, Pulse On, or Close to disable automatic retrieval and Latch Off, Pulse Off, or Trip to enable automatic retrieval. The status of automatic retrieval is reported with the *Automatic Retrieval Disabled* digital input pseudo point.

Retrieval State	This analog input pseudo point reports the status of the associated file set with the following status numbers: ➢ **0** - Not Available. This is the initial state of a file set after creation. ➢ **1 -** Available. This is the state reported when ARRM detects the file set is available for retrieval, but automated file set retrieval is disabled. ➢ **2** - Queued. File retrieval has been postponed. This may occur if ARRM is at the maximum number of configured retrievals. ➢ **3** - In Progress. ARRM is in the process of retrieving the associated file set. ➢ **4** - Complete. The last file transfer has been completed successfully. ➢ **5** - Failed. The last file retrieval operation has failed and a retry attempt has been scheduled.
Retrieve File Set	Any control on this digital output point triggers a manual retrieval of the associated file set.
Enable Connection Polling	The digital output pseudo point can be used to disable or enable inclusion of the file set into connection polling. The Latch On, Pulse On, or Close states enable inclusion of file set into connection polling. The Latch Off, Pulse Off, or Trip states disable inclusion of file set into connection polling. The status of file set inclusion into connection polling is reported with the Connection Polling Enabled digital input pseudo point.
Connection Polling Enabled	This digital input pseudo point is set to: ➢ **1** when file set inclusion into connection polling is enabled ➢ **0** when file set inclusion into connection polling is disabled. File set inclusion into connection polling can be enabled or disabled using the Enable Connection Polling digital output pseudo point.

Enterprise Synchronization

See the following sections for details:

ARRM Overview
Configure ARRM
Configure Applications
Configure File Set Templates
ARRM Viewer
ARRM Pseudo Points
About Oscillography Files and IEEE File Naming Convention for Time Sequence Data

Applications - ARRM

The **Applications** tab of the ARRM configuration window allows you to configure stations, devices, and file sets to be retrieved by the ARRM application.

Click the button to create...

- A new station when the company is selected
- A new device when a station is selected
- A new file set when a device is selected.

Click the button to delete the selected station, device, or file set.

Company > General sub-tab

Click the highest item in the tree to access **Company** settings.

Table 6.126: ARRM - General Sub-Tab

Field	Description
Company Name	The name of the company that is saved to the oscillography data filename. Range is 1 to 32 alphanumeric characters.
MCP Gateway Name	The name of the MCP Gateway that is included in the ARRM Connection Status File. Range is 1 to 32 alphanumeric characters. Refer to the Connection Polling section for more details.
Maximum Num of Concurrent Retrievals	Enter the number of files that can be retrieved at the same time. This setting is useful in reducing the load that ARRM places on poor networks or networks with many devices. Range is 1 to 256, default is 10. NOTE: Queued file retrievals are initiated at the TFTP/FTP/SFTP retry interval. For example, if you have set the TFTP/FTP/SFTP retry interval to five minutes and have set the number of concurrent file retrievals to 10, ARRM attempts to download 10 files every five minutes. Considering that retrieved files will likely not be examined in real time, it is not recommended to exceed 20 concurrent file retrieval sessions to accelerate the transfers.
File Deletion Threshold	The amount of space, in MB, allocated for use by ARRM. When this limit is reached, ARRM deletes older files as needed. Range is 1 to 65535, default is 512.
Default Time Tag Reference	Select whether stations belonging to this company apply a time tag based on first sample or time trigger. Stations can be configured to override this setting on a case-by-case basis.
Create Station Subdirectories	Select whether to create a separate folder within the storage folders for each station. If this setting is not enabled, all device directories are stored within the root folder.
Create Device Subdirectories	Select whether to create a separate folder within the storage folders (and, if selected, the station subfolder) for each device.

NOTE: It is recommended that the creation of Station and Device Subdirectories be enabled when using non-IEEE file naming, to prevent mixing different Substations and IEDs files in the same folder. This is also required for correct file structuring when pushing the files to Enterprise systems.

Company > Global TFTP sub-tab

Table 6.127: ARRM - Global TFTP Sub-Tab

Field	Description
Retries	The number of times ARRM is to retry a file transfer that has timed-out. Valid range is 0 to 10 times. Default is 2 times.
Retry Interval	If there is a network error, ARRM retries the file retrieval at a configured interval. Enter the amount of time, in seconds, that ARRM must wait before retrying a file transfer that has failed. Valid range is 1 to 86400. Default is 5.

Station

Table 6.128: ARRM - Station

Field	Description
Station Name	**T**he name of the station that is saved to the oscillography data filename. Valid range is a name that is between 1 and 6 characters in length and must be unique from any other configured station name. Default text is in the format “St x” where x is a system-generated number.
Use Default Time Tag Reference	If set to **true**, the default time tag reference defined on the *Company* level is used for this station. If set to **false**, an override can be specified. Default value is true.
Time Tag Reference	Select whether the station applies a time tag based on first sample or time trigger. This field is disabled when *Use Default Time Tag Reference* is set to *true*. Default value is disabled.
Default Time Zone	The default time zone for devices within the selected station. Devices can be configured to override this setting on a case-by-case basis. Default value is UTC.
Devices Adjust for DST	Specify whether devices within this station automatically adjust for daylight saving time. Default value is false.
Global Connection Polling Interval	Specify the Global Connection Polling Interval of the Station in minutes. Range is 1 to 1440 minutes. Default value is 5 minutes.

Device > Device sub-tab

Table 6.129: ARRM - Device Sub-Tab

Field	Description
Device Name	**T**he name of the device saved to the oscillography data filename. Valid range is a name that is between 1 and 14 characters in length and must be unique from any other device within the station. Default text is in the format “Device x” where x is a system-generated number. Refer to the ARRM FTP Directory Delta Support for Different ftp ls Formats section for the Device Name Suffix.
Use Default Time Zone	Specify if the selected device should use the time zone configured on the station level. Default value is true.
Time Zone	Select the time zone that the device is located in. Disabled when *Use Default Time Zone* is set to *true*. *Default is* disabled.
Device Adjusts for DST	Specify whether the device automatically adjusts for daylight saving time. *Default is* disabled.
Logical Device Name	The device name that the ARRM application uses to replace the "%s" format specifier in the file set template configuration, during the file set retrieval operation. Valid range is a name that is 32 characters or less in length. Default value is Empty.

Field	Description
Use Global Station Connection Polling Interval	Specify if the Global Connection Polling Interval configured for the station allows for poll-based File set retrieval. Default value is True.
Device Connection Polling Interval	Specify if the Device Level Polling Interval (in minutes) allows for poll-based File set retrieval. This parameter is enabled when *Use Global Station Connection Polling Interval* is set to False. Range is 1 to 1440 minutes. Default value is 5 minutes.

Device > File Server sub-tab

Table 6.130: ARRM - File Server Sub-Tab

Field	Description
Server Type	Select the type of server to use when connecting to the device. MMS is only available if an IEC 61850 configuration is loaded on the MCP and UR/SFTP is only available if Modbus TCP IED is configured with protocol TCP/SSH. Default value is TFTP. **NOTE:** File Set Templates with File retrieval mode as Directory Delta cannot work when server is configured as TFTP.
Retrieval Retry Interval (seconds)	If there is a communications error, ARRM retries the file retrieval at a configured interval. Enter the amount of time ARRM waits before retrying a file transfer that has failed. Valid range is 1 to 60000, default is 60.
FileSet Trigger Delay (seconds)	The amount of time (in seconds) after which the ARRM application starts processing file set retrieval, after receiving a file set trigger request.
TFTP Primary Server IP Address	The IP Address of the Primary TFTP server. Not available if the server type is not TFTP. Default value is Empty.
TFTP Secondary Server IP Address	The IP Address of the Secondary TFTP server. Not available if the server type is not TFTP. Default value is 0.0.0.0.
TFTP Timeout	The amount of time ARRM waits for each block in a TFTP transfer. Not available if server type is not TFTP. Valid range is 1 to 60000. Default is 500.
MMS Device	Select the IEC 61850 device that is used as the file server. Not available if TFTP/FTP/SFTP is selected as the server type.
FTP Primary Server IP Address	The IP Address of the Primary FTP server. Not available if server type is not FTP. Default value is Empty.
FTP Secondary Server IP Address	The IP Address of the Secondary FTP server. Not available if server type is not FTP. Enabled when FTP is selected as the server type. Default value is 0.0.0.0.
FTP Server TCP Port	FTP Server TCP port. Enabled when FTP is selected as the server type. Not available if server type is not FTP. Default value is 21.

Field	Description
FTP Timeout (ms)	Timeout for the FTP connection. Not available if server type is not FTP. Valid range is 1 to 60000, default is 2000.
FTP Allow Anonymous Login	Allow Anonymous Login to FTP Server. Not available if server type is not FTP. Enabled when FTP is selected as the server type. Default value is false.
FTP Anonymous Login Password	Password for Anonymous Login to FTP Server. Not available if server type is not FTP. This field is enabled when “FTP Allow Anonymous Login” is set to true. Default value is empty.
FTP Login Name	Login ID for FTP connection. Not available if server type is not FTP. This field is enabled when “FTP Allow Anonymous Login” is set to false. Default value is empty.
FTP Password	Password for FTP connection. Not available if server type is not FTP. This field is enabled when the FTP Allow Anonymous Login field is set to false. Default value is empty.
FTP Connection Mode	FTP Data Connection Mode (Active/Passive). Not available if server type is not FTP. Enabled when FTP is selected as the server type. Default value is Active.
FTP Data Representation Mode	Mode in which data must be retrieved from FTP Server (ASCII/Binary). Not available if server type is not FTP. Enabled when FTP is selected as the server type. Default value is Binary.
SFTP Primary Server IP Address	The IP Address of the Primary SFTP server. Not available if server type is not SFTP. Enabled when SFTP is selected as the server type. Default value is empty.
SFTP Secondary Server IP Address	The IP Address of the Secondary SFTP server. Not available if server type is not SFTP. Enabled when SFTP is selected as the server type. Default value is 0.0.0.0.
SFTP Server TCP Port	SFTP Server TCP port. Not available if server type is not SFTP. Default value is 22.
SFTP Timeout (ms)	Timeout for the SFTP connection. Not available if server type is not SFTP. Valid range is 1 to 60000, default is 2000.

Field	Description
SFTP Authentication Mode	Authentication Mode for SFTP Connection (Password/Public Key). The user needs to configure SFTP Login name and Password if Password mode is selected. For Public Key Authentication mode, you need to generate and copy the ssh public key to the location in IED specified by the vendor (click the **Utilities** powerbar button in the MCP HMI to **Generate Gateway Key Pair**). Not available if server type is not SFTP.
SFTP Login Name	Login ID for SFTP Connection. Not available if server type is not SFTP. This field is enabled when "SFTP Authentication Mode" is set to Password. Default is empty.
SFTP Password	Password for SFTP Connection. Not available if server type is not SFTP. This field is enabled when "SFTP Authentication Mode" is set to Password. Default is empty.
UR/SFTP Device	Select the UR SFTP device that is used as the file server. Not available if server type is not UR/SFTP.
UR/SFTP Timeout(ms)	Timeout for the UR SFTP connection. Valid range is 1 to 60000, default is 30000. Not available if server type is not UR/SFTP.

File Set

Table 6.131: ARRM - File Set

Field	Description
File Set Name	A unique identifier for the file set. Range is 1 to 32 ASCII characters. Default value is in the format "File Set x" where x is a system-generated number.
File Set Template	Select one of the available file set templates.
Include in Connection Polling	Specifies whether polling is enabled or disabled. If this parameter is enabled (True), File Set retrieval occurs through connection polling. Default value is False. **NOTE:** If this parameter is true, it is recommended to use the **Overwrite** option in the Fileset Template to avoid High Disk Usage. In the case of COMTRADE files, use the "New file with IEEE naming" option. **NOTE:** Users should include for connection polling only files which are always available in the end device, otherwise the connection poll may result in a failed file transfer, due to the file(s) no longer being available in the end device. **NOTE:** User shall not be able to configure file sets that have no means to be retrieved i.e. at least one retrieval trigger (RcdMade Mapped DI Point) or Connection Polling must be "True". **NOTE:** File Retrieval using Static Name in the File Set Template requires either "Include in Connection Polling" or a mapped "RcdMade Mapped DI Point" configured.

Field	Description
Use File Trigger Event Timestamp	If set to true, event time that triggers file retrieval operation is used as a timestamp for creation of files in New File with Timestamp File Storage method. Otherwise file retrieved time is used. This is only applicable to New File with Timestamp File Storage method. Default value is false.
Recording Made (RcdMade) Enable	If enabled, ARRM monitors a configured digital input point mapped to the *Recording Made* indication of the device. When a specific File Set Template - Standard is selected, this field is enabled. Default is disabled.
RcdMade Mapped DI Point	If the *Recording Made (RcdMade)* setting is enabled, select a system point to monitor for RcdMade indications. When the Recording Made (RcdMade) Enable field is set to true, this field is enabled. Default is disabled. **NOTE**: To avoid duplication, the RcdMade DI point must be in OFF state and turn ON momentarily to signal that a new file is available or remain ON until the file is read by ARRM. This is only required if the File Set Templates File Type is General.
Fault Number Point Enable	If enabled, ARRM monitors a configured analog input or accumulator point mapped to the *Fault Number* indication of the device. When a specific File Set Template is selected, this field is enabled. Default is disabled.
Fault Number Point	If the *Fault Number* Point Enable setting is enabled, select a system point to monitor for fault number indications. **NOTE:** File retrieval using Fault Number requires %u in the "File Set Template→ Retrieved file Absolute Path Name" field(eg:Osc%u) and mapping an AI point under "Fault Number Point", regardless of "Include in Connection Polling" being True or False
Reset Recorder Memory (MemRs) Enable	If enabled, ARRM operates the MemRs command after the file set is retrieved. This command may also be used to clear the file trigger point in D25 devices. Default value is false.
DO MemRs Point	If the *Reset Recorder Memory* setting is enabled, select a system point to operate after a file retrieval operation is completed.

For a list of pseudo points created for this file set by the ARRM application, refer to ARRM Pseudo Points. Each pseudo point has a reference and a description, as defined below.

Table 6.132: ARRM Pseudo Points - File Set

Field	Description
Reference	A user-defined name that can be used for quick indexing and filtering. Maximum 66 characters, ASCII only.
Description	A user-defined block of text that provides a detailed and localized description of the group. Maximum 128 characters.

File Set Template - Standard

The **File Set Template** sub-tab of the ARRM configuration window allows you to configure file set templates to be used by ARRM when retrieving records. Several predefined templates are provided for some popular IED models. Users have the flexibility to create and save new custom templates for other devices by entering specific file types, locations, and naming parameters.

>> To create a new standard File Set Template:

1. Click the button to create a new file set template.
2. Choose the **Standard** option:
   Select this option to support for File Archival using TFTP, MMS, FTP, or SFTP protocol.
3. Click **OK** to create a New Template.
   Or, click **Cancel** to exit.

>> To delete the selected template:

- Click the button.

Table 6.133: Delete - File Set Template - Standard

Setting	Description
Template ID	A unique identifier for the file set template.
Storage Directory	This is the location on the MCP that records are stored in. This directory is located within */mnt/datalog/arrm/*. The "&" character is used as a placeholder in the Storage Directory to specify a Local File Extension for retrieved files. For example, if you want to save retrieved files with extension "abc" then the Storage Directory is to be configured as "xyz&abc", where "xyz" represents Storage Directory and "abc" represents the local extension. This is applicable to files other than the COMTRADE file type. The valid value for Storage Directory has a minimum length of 2 characters (that is, cannot be blank) and must not start or end with special characters.
File Extension	Files with this file extension are retrieved by the ARRM from the IED. The downloaded files are saved with the same file extension if the local file extension is not configured in the Storage Directory setting. This field is not used if the File Type is set to COMTRADE.
Delete Files Automatically	If enabled, ARRM automatically deletes files in the *Storage Directory* created based on this template when the storage quota is exceeded.

File Type	Select the type of file being downloaded.
	• For COMTRADE-based Templates, select **COMTRADE**-format data only
	• For SELBIN-based Templates:
	  ○ Select **EVE** for Event files; e.g., EVE_10009.TXT
	  ○ Select **CEV** for Compressed Event Files; e.g., CEV_10009.TXT
	  ○ Select **BOTH** for EVE and CEV Event Files

Setting	Description

File Retrieval	Select a value:
	• **Static Name**: Select this option if the data to be retrieved is stored in a fixed location on the target device.
	  • **Retrieved File Absolute Path**: Enter the path to the data file on the remote device. Do not enter a file extension.
	  Add a logical device placeholder into the filename to create dynamic filenames that change based on which Device is using the template.
	  The logical device placeholder "%s" is replaced with the Logical Device Name from the Device that is using this template. For example, /SOE/event%s.
	  • **Enable Record Number**: If enabled, you can enter a number to be appended to the filename of retrieved records. This can be used for D25 SOE logs which have a record number as part of the filename (for example, enter **1** for A027_DISOE_LOG**1**.CSV).
	  • **Enable FileName to Save**: If enabled, the retrieved remote data file is saved locally using the specified file name.
	• **Fault Number**: Select this option if a new record is created on the device each time a fault occurs.
	  Retrieved File Absolute Path: Enter the path to the data file on the remote device. Do not enter a file extension.
	  Add placeholders into the filename to create dynamic filenames that change based on which fault number is being retrieved and which Device is using the template.
	  The logical device placeholder "%s" is replaced with the Logical Device Name from the Device that is using this template.
	  The fault number placeholder "%[fw]u" is replaced with the fault number currently being retrieved. In place of [fw], specify either no number or a number between 1 and 20 to give the field width. For example, %3u is replaced with 003 if the retrieved fault number is 3.
	  Specify at least 1 fault number placeholder but no more than 4.
	  Specify 1 or no logical device placeholders.
	  • **Max Number of Files**: The maximum number of files that can exist in the remote device before older files are deleted to make room for new ones. This setting prevents the MCP from attempting to retrieve files that no longer exist.
	  • **Fault Number Rollover**: This is the highest fault number that the device uses before the internal fault number counter rolls over specified as "n" in 2^n-1. Range is 8, 16 or 32. Default is 16.
	• **Directory Delta**: This option monitors a fixed location on the target device and downloads any new files as they are created.
	• **Directory Name**: Enter the path to the data file on the remote device. Do not enter a file extension.
	• **File Retrieval Expression Type**: This is a Unix shell-style wildcard that is used to specify the files within a directory that are considered for retrieval. Default is *, which specifies all files in the directory. The specific pattern matching symbols are as follows:
	  * matches everything
	  ? matches any single character
	  [seq] matches any character in seq
	  [!seq] matches any character not in seq

Setting	Description
File Storage	For Standard Templates, select a value: • **Append**: If the file does not exist, ARRM creates it. If the file exists and it is not larger than the specified maximum size, ARRM appends the contents of the retrieved file to the existing one. ARRM appends an incrementing number to the filename to distinguish between different files (for example, *dfr_**001**.txt*). Available for general file type only. *Max File Size:* Enter the file size, in bytes, that the download is limited to. Range is 1 to 4^{32}-1, default is 65535. • **New file with IEEE naming**: A new file is created whenever information is downloaded. The file name is defined using the IEEE naming convention. Available for COMTRADE file type only. *User Type:* Specify the type of data being retrieved. This information is then appended to the file name using the IEEE naming convention. For example, you can enter *DFR*, *PQ*, or *ADCP*. Range is 1 to 4 ASCII characters. • **New file with timestamp**: A new file is created whenever information is downloaded. Enter both a file name (to which the timestamp is appended) and a valid extension. For example, *adcp_090416082335.txt* was created on April 16, 2009, at 08:23:35. Available for general file type only. • **Overwrite**: When the parameter Include in Connection Polling is set to True, it is recommended to use this option for retrieval of fixed files from IEDs to avoid high disk usage in the MCP due to connection polling of file sets. Available for the GENREAL file type only.

File Set Template – Sel ASCII

The **File Set Template** sub-tab of the ARRM configuration window allows you to configure file set templates to be used by ARRM when retrieving records from SEL IEDs using automated ASCII commands.

You can also create and save new custom templates for other devices by entering specific file type, location and naming parameters.

NOTE: You can determine if the SEL device supports the EVE and CEV commands by observing pseudo points status provided in the GENASCII application's point summary page.

NOTE: Ensure that the options configured in the File Type setting are supported by the SEL relay before configuring the Template. If a configured option is not supported, this is indicated by the Transaction Failure flags on the ARRM viewer.

>> To create a new Sel ASCII File Set Template:

1. Click the button to create a new file set template.
2. Choose the Sel ASCII option:
   Select this option to generate a New File Template to support Sel Binary protocol.
3. Click **OK** to create a New Template.
   Or, click **Cancel** to exit.

To delete the selected template:

- Click the button.

Table 6.134: Delete - File Set Template - Sel ASCII

Setting	Description
SELB Device	Select the SEL Binary device (supports SEL Fast Meter Protocol) that is used as the file server. Not available if TFTP/FTP/SFTP/UR SFTP/MMS/GENA is selected as the server type.
GENA Device	Select the Generic ASCII device (supports SEL ASCII Protocol) that is used as the file server. Not available if TFTP/FTP/SFTP/UR SFTP/MMS/SELB is selected as the server type.
Template ID	A unique identifier for the file set template.
Storage Directory	This is the location on the MCP that records are stored in. This directory is located within /mnt/datalog/arrm/. The valid value for Storage Directory has a minimum length of 2 characters (that is, cannot be blank) and must not start or end with special characters.
File Extension	The extension to append to any files downloaded using this template. This field is not used if the File Type is set to COMTRADE.
Delete Files Automatically	If enabled, ARRM automatically deletes files in the Storage Directory created based on this template when the storage quota is exceeded
File Type	Select the Fault file type to be retrieved. ARRM supports file archival of EVE and CEV files from the SEL IEDs. The default value in the "Options" field is None. The "Options" configuration allows you to choose the frequently used command options used with EVE and CEV commands such as C, L and Lyyy. The template also allows you to choose "other" supported command options with EVE and CEV where you can enter the command extensions supported in the Additional Option field.
File Storage	For Selbin Templates, select a value: • **FileName with timestamp**: A new file is created whenever information is downloaded. This option saves the event files in the format: EVE_YYMMDDHHMMSS_Msec.EVE/CEV_YYMMDDHHMMSS_Msec.CEV. For example, EVE_090416082335_123.EVE will be created for a file that was generated on April(MM) 16(DD), 2009(YYYY), at 08(HH):23(MM):35(SS).123(mSec) • **FileName with Event Number**: A new file is created whenever information is downloaded. This option saves the event files in the format: EVE_EventNumber.EVE/CEV_EventNumber.CEV. For example, EVE_100009.EVE will be created when the end device sends a command response when this specific file is queried.

About Oscillography files and IEEE File

Oscillography files are saved in COMTRADE format. The COMTRADE standard defines a file format that contains transient waveform and event data collected from power systems. Each oscillography file consists of a three-file set. The files have the same file name but different extensions: .hdr, .cfg, and .dat for header, configuration, and data files respectively. ARRM downloads oscillography files directly from IEDs and automatically generates a new file name for each COMTRADE file set based on the IEEE File Naming Convention for Time Sequence Data.

IEEE File Naming Convention for Time Sequence Data

<Start Date>, <Start Time>, <Time Code>, <Station>, <Device>, <Company>, <Type>. <Extension>

Where:

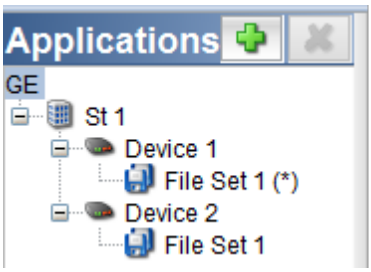
- <Start Date> has the following format: yymmdd
- <Start Time> has the following format: hhmmssmmmmmm, where hh is hours, mm is minutes, ss is seconds, mmm is milliseconds, and mmm is microseconds.
- <Time Code> is the difference between the time used for start time and Universal Time (or Greenwich Mean Time). The time code ends with an "s" if the device always reports standard time, or an "a" if the device adjusts for daylight savings time. If the device is using Universal Time, neither character is appended.
- <Station> is the configured station name
- <Device> is the configured device name
- <Company> is the configured company name
- <Type> is DFR, PQ, or ADCP
- <Extension> is DAT, CFG, or HDR

Connection Polling

The ARRM Connection Polls are required because, in absence of any events, there are no potential ARRM file transfers for days or weeks at a time; consequently, ARRM files will not appear with an up-to-date status.

The file sets configured for polling will be triggered by the Configured Polling interval (either *Global Connection Polling Interval* or *Device Connection Polling Interval*) in addition to their configured event trigger. The ARRM configuration will not impose any restrictions on files to be included in connection polling – none, one, more or all files can be configured for connection polling, as required.

An asterisk (*) is appended to each file set that is supported by periodic polling.



NOTE: In the case of fault number-based file sets which are included in connection polling, ARRM always retrieve files with the last fault number value. Consideration must be given to the files included in connection polling so redundant files are not created un-necessarily.

ARRM Connection Status File

The ARRM Connection Status file is constantly updated whenever ARRM performed and finalized an action on a file, either because of a trigger or by periodic polls.

The name of the ARRM Connection Status file is *ARRM_Conn_Status.txt,* and is *stored* in the /mnt/datalog/Logs folder in the MCP. In case of Warm Standby Redundancy, this file is mirrored to the standby unit to a temporary location, and whenever the Standby unit becomes Active it is copied to /mnt/datalog/Logs folder.

The file name convention is based on IEEE C37.232 with additional data fields as required for this functionality (i.e., Delimiters, FileSetName, and FileTransferResult)

File Name Format

<Start Date>, <Start Time>, <Time Code>, <Station>, <Device>, <Company>, <Type>|<FileSetName>:<FileTransferResult>

Table 6.135: File Name Format

File Name Element	Description
Start Date	The Start Date in the first row always shows the value when the "ARRM_Conn_Status" file was last updated, for whatever reason. The date has the format: YYMMDD (6 characters) according to IEEE C37.232 standard. In subsequent rows, it shows the date when the row-specific file was updated.
Start Time	The Start Time in the first row always shows the value when the "ARRM_Conn_Status" file was last updated, for whatever reason. The time has the format HHMMSSMMMMMM (12 characters) according to IEEE C37.232 standard, where "H" = hour," M" = minute, "S" = seconds and the remaining 6 "M"s refer to milliseconds and micro seconds. In subsequent rows, it shows the time when the row-specific file was updated.
Time Code	The Time Code contains from 1 to 7 formatted characters. The Time code indicates the time zone offset for the start date and time fields. The offset is specified as the offset East of GMT time (e.g., +5h30 for IST). The first character is "+", except if the offset is GMT. If the offset is GMT, then there is no "+" sign character, and the offset appears simply as 0. The character "t" is appended to each offset. **NOTE:** Enterprise systems should ignore the character "t" while parsing the ARRM Connection Status File All time code (zone) values in this file are driven by the MCP Local Time as configured in mcpcfg (independent from any time zone settings in ARRM). The rationale is the indicated times in this file reflect the moment when the MCP ARRM performed a check; these are not times received from IEDs or other files.
Station	The first line is always set to "ARRM" to reflect a generic / virtual "station name" associated with the MCP Gateway. The station name has no meaning in the first line since this first line represents the collector status, and a single collector (i.e. MCP) can have multiple stations. For remaining lines, this is the configured station name.
Device	For the first row, this is the name of the MCP Gateway executing the ARRM. For all other rows, this is the device name as configured in ARRM.
Company	This is the configured company name.
Type	For this file, the type is always "stat" (status) for the Gateway (i.e., for the first line). The other entries (remaining rows in this file) have the file type: • As configured in ARRM under "User Type" where the file was configured as COMTRADE. • As "genr" (generic) for the files not configured as COMTRADE.
Storage Directory	This setting is not applicable to the first row. For subsequent rows, the identifier is the local "Storage Directory" configured in the ARRM File Set Template.
FileSetName	For the first row, the identifier is always: Application (i.e. the ARRM application). For subsequent rows, the identifier is the "File Set Name" configured in ARRM.

File Name Element	Description
FileTransferResult	The <*FileTransferResult*> value in the first row is associated with the ARRM application status. This value is always 1, even if all IEDs have their file transfers disabled or offline. The timestamp (START DATE, START TIME and TIMECODE) in the first row is always updated with the latest file retrieval's timestamp. The remaining rows indicate the last known transfer state of those specific files as follows: • 0 = FAILED; this is the file transfer result due to manual file trigger/automatic file trigger/connection poll file trigger. • 1 = SUCCESSFUL; this is the file transfer result due to manual file trigger/automatic file trigger/periodic poll file trigger. • -1 = DISABLED; this is the case when automatic file trigger is disabled. Example: ARRM_Conn_Status File 150529, 161918353582,-7ht, ARRM, MCP_GW, GE, stat|Application:1 150529, 161918353582,-7ht, St 1, Device 1, GE, comt,storagedir1 |File Set 1:0 150529, 111110414615,-7ht, St 1, Device 2, GE, test,storagedir2 |File Set 1:0

ARRM FTP Directory Delta Support for Different ftp ls Formats

>> To determine the ftp ls format:

1. Log in to the mcpcfg local configuration utility using admin credentials.
2. From mcpcfg, connect to the device using ftp.
3. Log in through ftp.
4. Enter a **ls** command.
5. Observe the format of the response from the device as shown in below screen capture.

```
D400#>> ftp 192.168.4.128
Connected to 192.168.4.128.
220 VxWorks (VxWorks5.5.1) FTP server ready
Name (192.168.4.128:admin): Administrator
331 Password required
Password:
230 User logged in
ftp> ls
200 Port set okay
150 Opening ASCII mode data connection
  size          date       time       name
--------       ------     ------    --------
    2048    Aug-11-2009  09:42:56   boot              <DIR>
    2048    Feb-25-2012  08:07:20   reg               <DIR>
    2048    Aug-11-2009  09:39:24   install           <DIR>
```

The following table lists the ftp **ls** formats which the MCP ARRM supports in directory delta mode. You must provide the suffix listed in the below table for each format in the device name configuration.

Table 6.136: ftp ls formats

S. No.	ftp ls format	Suffix in ARRM device name	Example devices
1	-rwxrwxrwx 1 0 0 3 Dec 30 1969 RAM drwxrwxrwx 2 0 0 0 Jan 1 00:00 code	No suffix required	SEL 451,F650
2	drwxrwxrwx 4 root 4096 Feb 20 00:05 .. -rw-rw-rw- 1 root 150984 Jun 19 15:22 558433B70004	__LS1	Tesla4000
3	size date time name -------- ------ ------ -------- 2048 Aug-11-2009 09:39:24 install <DIR> 5668 Aug-11-2009 09:39:28 latin2.csf	__LS2	ABB-REL670
4	04-28-11 10:00PM 734477 1TXT.DAT 07-10-15 04:00PM <DIR> COMTRADE	__LS3	Window xp

Sample File Set Templates for Relay Models

The table below provides some sample File Set Templates for popular IED Models.

Table 6.137: Sample File Set Templates for IED Models

Template Name	Use this template to . . .
MULTILIN_UR_OSC_TFTP	Retrieve oscillography files using TFTP from GE Grid Solutions Multilin Universal Relays.
MULTILIN_UR_OSC_MMS	Retrieve oscillography files using MMS (IEC 61850) from GE Grid Solutions Multilin Universal Relays.
MULTILIN_F650_OSC_MMS	Retrieve oscillography files using MMS (IEC 61850) from GE Grid Solutions Multilin F650 relays.
7SJ_DFR	Retrieve oscillography files using MMS (IEC 61850) from Siemens 7SJ64 relay. Though this template was only tested with a Siemens 7SJ64 relay, it will likely work for other Siemens 7SJ models.
ABB_REL_670	Retrieve oscillography files using MMS (IEC 61850) from ABB REL670 relay. Though this template was only tested with an ABB REL670 relay, it can likely work with other ABB relay models in the same family.
MICOM	Retrieve oscillography files using MMS (IEC 61850) from MICOM P143 relay. Though this template was only tested with a MICOM P143 relay, it can likely work with other MICOM relays in the same family.
D25_PQ_MMS	Retrieve power quality oscillography files using MMS (IEC 61850) from GE Grid Solutions Multilin D25 IEDs.
D25_PQ_TFTP	Retrieve power quality oscillography files using TFTP from GE Grid Solutions Multilin D25 IEDs.
D25_ACDP_MMS	Retrieve AC Data Profiling oscillography files using MMS (IEC 61850) from GE Grid Solutions Multilin D25 IEDs.
D25_ACDP_TFTP	Retrieve AC Data Profiling oscillography files using TFTP from GE Grid Solutions Multilin D25 IEDs.

Template Name	Use this template to . . .
D25_DFR_MMS	Retrieve Digital Fault Recording oscillography files using MMS (IEC 61850) from GE Grid Solutions Multilin D25 IEDs.
D25_DFR_TFTP	Retrieve Digital Fault Recording oscillography files using TFTP from GE Grid Solutions Multilin D25 IEDs.
D2X_1_DISOE	Retrieve SOE files for Digital Input Logging Record 1 from GE Grid Solutions Multilin D2X devices.
D2X_1_AISOE	Retrieve SOE files for Analog Input Logging Record 1 from GE Grid Solutions Multilin D2X devices.
D2X_2_DISOE	Retrieve SOE files for Digital Input Logging Record 2 from GE Grid Solutions Multilin D2x devices.
D2X_2_AISOE	Retrieve SOE files for Analog Input Logging Record 2 from GE Grid Solutions Multilin D2x devices.
MULTILIN_UR_EVT_TFTP	Retrieve Event files using TFTP from GE Grid Solutions Multilin Universal Relays.
MULTILIN_UR_PRODINFO_TFTP	Retrieve Product Information files using TFTP from GE Grid Solutions Multilin Universal Relays.
MULTILIN_UR_DATALOGTXT_TFTP	Retrieve Datalog files using TFTP from GE Grid Solutions Multilin Universal Relays.
MULTILIN_UR_FLTREP_TFTP	Retrieve Fault Report files using TFTP from GE Grid Solutions Multilin Universal Relays.
MULTILIN_UR_SECEVT_TFTP	Retrieve Security Event files using TFTP from GE Grid Solutions Multilin Universal Relays (This file will be available for UR Relays having Cybersentry Lvl 1 option).
MULTILIN_UR_DATALOGA_TFTP	Retrieve COMTRADE Datalogger files using TFTP from GE Grid Solutions Multilin Universal Relays.
MULTILIN_UR_URINFO_TFTP	Retrieve UR Information files using TFTP from GE Grid Solutions Multilin Universal Relays.
MULTILIN_UR_USER_FLTRESP_TFTP	Retrieve User Fault Report files using TFTP from GE Grid Solutions Multilin Universal Relays.
MULTILIN_UR_ICD_TFTP	Retrieve ICD files using TFTP from GE Grid Solutions Multilin Universal Relays.
MULTILIN_UR_CID_TFTP	Retrieve CID files using TFTP from GE Grid Solutions Multilin Universal Relays.
MULTILIN_UR_IID_TFTP	Retrieve IID files using TFTP from GE Grid Solutions Multilin Universal Relays.
SEL 451	Retrieve COMTRADE files from SEL 451 Relays. A trigger DI (indicates file generation in relay) must be configured to the file set. If DI is not available, it is recommended that the "Include in Connection Polling" option to be enabled.
8Series_EVT_TFTP	Retrieve Event files using TFTP from 8 series Relays.
URPlus_EVT_TFTP	Retrieve Event files using TFTP from GE Grid Solutions Multilin UR+ Relays.

ARRM ASCII Directory Delta Support

ARRM provides an interface to the SELBinary DCA and the GENASCII DCA applications to retrieve and archive the Event Log files from the SEL IEDs/numerical relays.

The SELBinary and GENASCII DCA applications use ASCII commands to retrieve two types of fault/event log files:

- EVE (Event Report Files) and
- CEV (Compressed Event Report Files).

The ARRM application automatically tabulates the number of files present in the SEL IEDs and periodically directs the DCA applications connected to the SEL IEDs to retrieve the event files one after another, sequentially.

The ARRM application also provides configurable user-friendly Templates, custom-designed specifically for file archival from SEL relays.

The Template provides you with an option to choose the type of the Fault records/Event log files to retrieve:

- EVE
- CEV
- Both

The event files retrieved by ARRM from Soleras can be stored with two different naming formats:

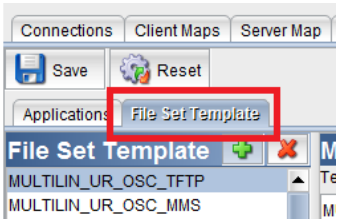
- FileName with Event Number
  The FileName with EventName option saves the event files in the format: EVE_EventNumber.EVE/CEV_EventNumber.CEV

  or

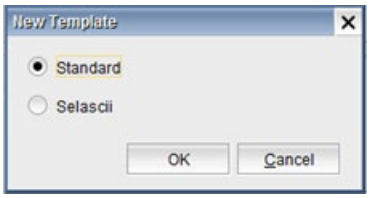
- FileName with TimeStamp.
  The FileName with TimeStamp option saves the event files in the format EVE_YYMMDDHHMMSS_Msec.EVE/CEV_YYMMDDHHMMSS_Msec.CEV

» To create a new file set template:

1. Click **File Set Template**.



Result: Two options are available.



2. Select the appropriate option.

Configure Automation Features

This section contains the following sub-sections:

Configuration Overview

Accumulator Freeze

Alarm
- Digital Event Management
- Alarm Types
- Creating Alarms

Analog Report Generation
- Overview
- Viewing
- Configuration

Automated Record Retrieval
- ARRM Overview
- ARRM Configuration
- ARRM Viewer
- ARRM Pseudo Points
- Enterprise Synchronization
- Applications - ARRM
- File Set Template
- About Oscillography Files and IEEE File
- Connection Polling
- ARRM FTP Directory Delta Support for Different ftp ls Formats
- ARRM ASCII Directory Delta Support

Calculator
- Mapped Points
- Expressions
- Points
- Application Parameters
- Basic Syntax Rules

Data Logger
- Configure the Data Logger
- Report Types
- Storage Allocation

Input Point Suppression

Load Shed and Curtailment

LogicLinx (optional)

System Point Manager
- System Point Manager
- Accumulator Freeze
- Analog Value Selection
- Control Lockout
- Double Point
- Input Point Suppression
- Redundant I/O

Configuration Overview

The MCP Automation applications retrieve data from the real-time database, manipulate the data and store the results in the real-time database. The type of data supported by the automation applications varies depending on the application. The MCP currently supports the following automation applications:

- System Point Manager
- Accumulator Freeze
- Alarm
- Analog Report Generation
- Calculator
- Automated Record Retrieval
- Calculator
- Data Logger
- Input Point Suppression
- Load Shed and Curtailment
- Redundancy Manager
- Remote Logging (Rsyslog)

Automation Applications

Some features are implemented through automation applications which retrieve data from the real-time database, manipulate the data and store the results in the real-time database. The type of data supported by the automation applications varies depending on the application.

» To configure automation applications for use on the MCP you typically:

1. Select data points.
2. Define application points.
3. Set up the point manipulations and associated settings.
4. Save and run the configuration file by committing the changes.

System Point Manager

System Point Manager - Overview

The **System Point Manager** enables you to configure a variety of advanced automation functions on your device. These functions include:

- Accumulator Freeze: Groups of accumulator points whose values are frozen periodically or on demand.
- Analog Value Selection: Define a group of prioritized analog input points with the highest priority, valid input being reported to a single analog input point.
- Control Lockout: Ensure that only a single master station can access a group of controls at one time and lock out groups of local controls for maintenance purposes.

  ⚠WARNING **The MCP Control Lockout feature is not a replacement or equivalent of LOTO (Lockout – Tagout). Use standard safety procedures to implement Lockout - Tagout and to perform maintenance operations.**

- Double Point: Associate two digital input points to form a double point indication. Also known as 4-state points.
- Input Point Suppression: Suppress reporting of input points while they are unavailable during maintenance.

- Redundant I/O: Specify a Secondary data point for any point that is used to report the value and quality when the associated Primary point is invalid or questionable.
- Control In-Progress: The Control In-Progress feature of system point manager allows you to trace if a control command on digital output point is in progress or not. This feature also provides the information about the application that has issued the command and the control command type.

Accumulator Freeze

The **Accumulator Freeze** feature of the System Point Manager allows you to create groups of accumulators that are frozen periodically or on demand.

Table 6.138: Accumulator Freeze

Field	Description
Group Name	A short text description that is assigned to the group. Maximum of 66 ASCII characters comprising alphanumeric characters, space, underscore and dash.
Group ID	Non-editable. A unique reference identifier for the group.
Group Description	A description of the group. Maximum 128 characters.
Configure Freeze Time	Opens the **Freeze Time Point** window, which contains the following two fields. The system point created for this group is available under the System Point Manager application.
Freeze Time Acc Name	A user-defined name that can be used for quick indexing and filtering. Maximum 66 characters, ASCII only.
Freeze Time Acc Description	A user-defined block of text that provides a detailed and localized description of the group. Maximum 128 Unicode characters.
Copy Value Policy	Determines the action performed on all members of the group if an accumulator freeze is triggered. If *Absolute* is selected, the frozen value of the mapped point is applied to the corresponding frozen value point. If *Delta* is selected, the value of the frozen value point is updated by the amount of difference between the new frozen value and the previous frozen value. Note regarding the *Delta* setting: If the current frozen value is smaller than the previous frozen value, the delta value calculated would be calculated as a rollover number, causing the frozen value accumulator points to be extremely large. For example, if the current frozen value is 3 and the previous frozen value is 258, the resulting frozen value accumulator point is shown as 9.22e+18.
Freeze Interval (min)	Specifies the frequency, in minutes, at which freeze commands are automatically issued to the group. The range is 0 to 14400 minutes (i.e., 10 days). Enter 0 to disable.
Time of Hour Alignment Offset	The time of day to align the freeze interval to. For example, if the alignment offset is set to xx:15, the freeze operation is aligned to begin at 15 minutes past the hour. The freeze interval setting must divide evenly into an hour to facilitate the offset. Disabled if the Freeze Interval is set to 0.
Freeze Trigger Point	Define a system point (digital input) that can be used to trigger freeze commands to the group. The trigger state (ON or OFF) is configurable. Disabled if a Freeze Report Point is enabled.

Freeze Report Point	Define a system point (digital output) that is triggered when a freeze operation is initiated. The control type (close, trip, latch ON, latch OFF, pulse ON, or pulse OFF) and pulse duration (in milliseconds, not available for latch controls) are configurable. Disabled if a Freeze Trigger Point is enabled. When you check the digital output box in the accumulator freeze, the Freeze Interval and Freeze trigger point are both disabled. If you want a DO to be triggered whenever a Freeze command is sent on an accumulator, you must make configuration changes in two different Accumulator Groups. In one group, you should be able to configure the Freeze parameters on a point and in other group the DO point triggering can be configured for the same point of the earlier group. **Point Selection Area** You can select system points to add to the accumulator freeze group using the system point tree. System points can be used in multiple accumulator freeze groups. Click the checkbox to the left of a point or group name to add a point or a group of points to the group. Points included in the group are shown at the right-hand side of the point selection area. To remove a point, uncheck the appropriate box in the system point tree or highlight the point and click the **Delete** button. Click the **Delete NE** to remove any points that are not valid (that is, points that have been deleted from the system database after they were included in the accumulator freeze group). The *Frozen Value Reference* and *Frozen Value Description* fields define the accumulator point that is created for the selected point. The value of this accumulator points changes based on the *Copy Value Policy* defined above.

Analog Value Selection

The **Analog Value Selection** feature of the System Point Manager allows you to define a group of prioritized analog inputs with lower and upper limits; the highest priority valid input from the group is reported as the value of a configured analog input point.

Table 6.139: Analog Value Selection

Field	Description
Group Name	A short text description that is assigned to the group. Maximum of 66 ASCII characters comprising alphanumeric characters, space, underscore and dash.
Group ID	Non-editable. A unique reference identifier for the group.
Group Description	A description of the group. Maximum 128 Unicode characters.
Configure Group Point...	Opens the **Group Point** window, which contains the following two fields. The system point created for this group is available under the System Point Manager application. **Group Point Reference** A user-defined name that can be used for quick indexing and filtering. Maximum 66 characters, ASCII only. **Group Point Description** A user-defined block of text that provides a detailed and localized description of the group. Maximum 128 Unicode characters.
Lower Limit	The minimum value that must be met by at least one of the points within the group. If this limit is not met by any points in the group, the value and quality of the lowest-priority point is reported as the value and quality for the group. Note that the limit value itself is considered within range (that is, a value of -1000 is considered valid for an analog selection group with a lower limit of -1000). If all the points are below the defined lower limit, the value of the lowest priority point is reported.

Upper Limit	The maximum value that can be reported by any of the points within the group. If this limit is exceeded by all the points in the group, the value and quality of the lowest-priority point is reported as the value and quality for the group. Note that the limit value itself is considered within range (that is, a value of 1000 is considered valid for an analog selection group with an upper limit of 1000). If all the points are above the defined upper limit, the value of the lowest priority point is reported.
Point Selection Area	You can select system points to add to the analog value selection group using the system point tree. Click the checkbox to the left of a point or group name to add a point or a group of points to the group. Points included in the group are shown at the right-hand side of the point selection area. To remove a point, uncheck the appropriate box in the system point tree or highlight the point and click the **Delete** button. Click the **Delete NE** to remove any points that are not valid (that is, points that have been deleted from the system database after they were included in the analog value selection group). **Priority** Use a numeric value to set the priority of each point within the group, with 0 being the lowest priority.

Control Lockout

The **Control Lockout** feature of the System Point Manager allows you to ensure that only a single master station can access a group of controls at one time and can lock out groups of controls to allow for safer local maintenance. You can create up to 8 remote control groups and up to 1000 local control groups. Any digital output (except for those owned by the System Point Manager application) can be included in one remote and one local group.

The **Control Lockout** feature of the System Point Manager allows users to implement two types of control lockout groups:

- Remote Groups
- Local Groups

⚠WARNING **The MCP Control Lockout feature is not a replacement or equivalent of LOTO (Lockout – Tagout). Use standard safety procedures to implement Lockout - Tagout and to perform maintenance operations.**

Remote Groups

Remote Groups ensure that only a single master station can access a group of controls at one time. Up to 8 remote control groups can be created; i.e., up to 8 control sources can be inter-locked.

A remote group is locked when a control is issued on any member point. For the duration of the control plus 100 milliseconds, no other commands are accepted on controls in the group unless they originate from the application or device that issued the first control operation. After this period has passed, the controls are available to all participating ("candidate") applications and devices again.

NOTE: Reboot of the MCP resets the locked groups.

Local Groups

Lock out groups of controls to allow for safer local maintenance, or any other applications where a group of controls need to be blocked. Up to 1000 local control groups can be created.

Normally, control lockout is manually initiated by an operator and commands are not accepted until the lockout has been released. Control lockout can also be achieved using applications such as Calculator or LogicLinx to issue the lockout commands.

A local group is locked by turning ON (latch) the associated *Local Group Lockout DO* and is unlocked by turning it OFF (latch).

Any of the candidate application included in the local lockout group can remove the lockout by sending the OFF command through the Local Control Group Lockout feature.

NOTE: Reboot of the MCP resets the locked groups.

NOTICE Applications not included in a local group (i.e., the box under *included candidates* is **NOT checked**) – are unrestricted. This means that they are not affected by local group lockouts and can still operate controls on all points even when a local group lockout is in effect.

In addition, the application which turned on the local group lockout (i.e., issued the latch ON for *Group Lockout DO reference*) can still operate controls on all points part of that specific local group, as "owner", and all other applications which have the *include* box **checked** are not able to operate the controls in this locked local group.

Examples

In each configuration, the following candidates are present, included as shown:

- HMI (the MCP HMI)
- Master1 (a first DNP3 Master)
- Master2 (a second DNP3 Master)
- Master3 (a third MODBUS Master)
- Calculator (via the configured expressions in Calculator)

Use case A

At run time, an operator uses the HMI to lock this local group by turning ON the Local Group Lockout DO, directly from the HMI.

Controls to the local group DO points, issued from the HMI still operate, since the HMI was the issuer of the lockout command and is now the current owner of the locked group; this allows users to still execute commands from the HMI for testing purposes.

Controls from Master1, Master2 and Calculator do not operate because the local group is locked, and these candidate applications are included.

Controls from Master3 operate even with the local group being locked because this candidate application was not included.

When finished, the operator uses the HMI to remove the group lockout by turning OFF the Local Group Lockout DO, directly from the HMI.

Use case B

Here the system is configured with a *Digital Assignment* calculator expression which controls the *Local Group Lockout DO*, based on simple conversion logic. Assume the HMI has the capability to change the state of the input of this calculator expression; this allows an operator to perform an HMI action which has the final effect of controlling the *Local Group Lockout DO*, but now indirectly via Calculator.

The operator uses the HMI to turn ON the calculator input, which in turn locks the local group.

Controls to the local group DO points, issued from the HMI do not operate, since the HMI was not the issuer of the lockout command, but – technically – Calculator is the issuer of the lockout command and Calculator is now the current owner of the locked group; this does not allow users to execute any commands from the HMI, even though – from a human operator perspective – the lockout order was done from the HMI.

Controls from Master1 and Master2 do not operate because the local group is locked, and these candidate applications are included.

Controls from Master3 operate even with the local group being locked because this candidate application was **not** *included*.

If Calculator has other expressions which are mapped to the DO points in the locked local group, those execute because Calculator is seen as the owner of the group in this moment.

When finished, the operator uses the HMI to remove the group lockout by changing the state of the input calculator expression which controls the group lockout. Turning OFF the *Local Group Lockout DO* directly from the HMI cannot be done since the issuer of the lock is – technically – not the HMI).

A implementation of this use case is to have a throw switch position acquired via any application as a DI which then is used as calculator input to the assignment expression controlling the group lockout. Multiple local groups can be controlled by the same DI using multiple calculator assignment expressions, or by individual DI points.

Common functionality between Remote and Local Groups

Each defined Remote or Local Group has associated Status and Command Points, which at run time indicate and control the operational state of the group; see Configure Indication Points.

Any digital output (except for those owned by the System Point Manager application) can be included in **one remote** and **one local** group.

Digital output points mapped into a group (remote or local) accept only transient commands at run time; e.g., PULSE, TRIP, CLOSE.

Latched commands (ON, OFF) are rejected because the group allows for only one command at a time and latched requests indefinitely lock the group.

NOTE: For many MCP applications, pseudo (logical) points can still be controlled using CLOSE or PULSE_ON to attain an ON action, and, respectively – TRIP or PULSE_OFF to attain an OFF action.

Field	Description
Group Name	A short text description that is assigned to the group. Maximum of 66 ASCII characters comprising alphanumeric characters, space, underscore and dash.
Group ID	View-only field: A unique reference identifier for the group.
Group Description	A description of the group. Maximum 128 Unicode characters.
Configure Indication Points...	Opens the **Group Status Indication Points** window, which contains the following eight fields. The system points created for this group are available under the System Point Manager application. **<Point> Reference** A user-defined name that can be used for quick indexing and filtering. Maximum 66 characters, ASCII only. **<Point> Description** A user-defined block of text that provides a detailed and localized description of the point. Maximum 128 characters. **Locked DI** The digital input point that is ON when the group is locked out. **Active DI** The digital input point that is ON when a control in the group is in operation. **Group Owner AI** The analog input that contains the ID number of the application that has locked the group. You can use the AI Text Enumeration feature to display a user-friendly text string instead of the identification number. **Group Lockout DO** The digital output point that must be operated to initiate the control lockout.

Control Lockout Candidates selection area	Select the applications that are candidates of the lockout group. **NOTICE** Applications not included in a local group are unrestricted. This means that they are not affected by local control lockouts and can operate controls on all points even when a lockout is in effect.
Point Selection Area	You can select digital output system points to add to the control lockout group using the system point tree. Click the checkbox to the left of a point or group name to add a point or a group of points to the group. Points included in the group are shown at the right-hand side of the point selection area. To remove a point, uncheck the appropriate box in the system point tree or highlight the point and click the **Delete** button. Click the **Delete NE** to remove any points that are not valid (that is, points that have been deleted from the system database after they were included in the group.

Remote Control Groups – Manual Ownership

Each Defined Remote Control Group has associated with the Manual Ownership option to select the list of the applications that needs to lockout the group explicitly. The lock out of the Remote Group Lockout DO can be done by turning ON (latch) the associated Remote Group Control Lockout DO and unlocked by turning it OFF(Latch).

NOTE: This Option is available only for Remote Control Lockout Groups.

Double Point

The **Double Point** feature of the System Point Manager allows you to associate two digital input points to form a double point indication.

» To create a double point:

1. Select a device or application in the left pane. The **Close Point Reference** and the **Open Point Reference** fields must refer to points from the same application or device, so selecting a device or application in this pane limits both fields accordingly.
2. Click the **Add** button at the top right of the screen.
3. Configure the double point using the fields below.
4. Click the **Save** button.

Table 6.140: Double Point

Field	Description
Reference	A user-defined name that can be used for quick indexing and filtering. Maximum 66 characters, ASCII only.
Description	A user-defined block of text that provides a detailed and localized description of the group. Maximum 128 characters.
Close Point Reference	A point selection tree that allows you to choose the point to be used as the Secondary source. Only points of the same data type that have not already been selected as a Primary source are available.
Open Point Reference	A point selection tree that allows you to choose the point to be used as the Secondary source. Only points of the same data type that have not already been selected as a Primary source are available.
State	Text labels to be used for each of the four states of the double point. Maximum 32 characters.
Invalid State Qualification	The amount of time, in milliseconds, that the two source points must remain in the 1 state before the double point is reported as invalid. Range is from 0 to 65535.

Output Type/Output Status	You can specify up to two digital output points that can be used to operate the double point. If you choose *Single Output*, you can select one point via the **Output Status** field to receive Trip and Close commands. If you choose *Dual Outputs*, you can select two points via the **Output Status** field; one to receive Trip commands and another to receive Close commands. Both the *Single Output* and *Dual Outputs* modes allow you to enable or disable inclusion of the status of the output in the double point's quality flag.

NOTE: Double Point functionality is only for Alarms, thereafter it can be used for One Line Data Sources.

Input Point Suppression

The **Input Point Suppression** feature of the System Point Manager allows you to disable groups of analog and digital input points by ignoring their actual data and quality changes within selected applications. While points are suppressed, a predefined suppression value or the last reported value (before applying suppression) and the **Point Suppressed** quality flag are provided instead. This can be useful during maintenance operations to prevent spurious OFFLINE alarms and false readings while devices are powered off or disconnected.

You can add any number of input points to a point suppression group, but any input may only be included in a maximum of one group at any time. Local commands can be executed on suppressed points; however, you do not see the effects of the local command until suppression is removed.

Please review this note if you are using input point suppression in conjunction with redundant I/O.

Table 6.141: Input Point Suppression

Field	Description
Group Name	A short text description that is assigned to the group. Maximum of 66 ASCII characters comprising alphanumeric characters, space, underscore and dash.
Group ID	Non-editable. A unique reference identifier for the group.
Group Description	A description of the group. Maximum 128 Unicode characters. Up to 10000 Input Point Suppression Groups can be created.
Configure Group Quality Point...	Opens the **Group Quality Point** window, which contains the following two fields. **Point Reference** A user-defined name that can be used for quick indexing and filtering. Maximum 66 characters, ASCII only. **Point Description** A user-defined block of text that provides a detailed and localized description of the group. Maximum 128 characters. This digital output point activates the suppression group upon receipt of a latch ON, close, or pulse ON control. Suppression can be disabled through a latch OFF, trip, or pulse OFF control.

Input suppression candidate selection area	Select the applications that are candidates of the suppression group. When the input point suppression group is active, the applications selected here do not receive information from the points selected below. **Candidate Reference** A user-defined name that can be used for quick indexing and filtering. Maximum 66 characters, ASCII only. **Candidate Description** A user-defined block of text that provides a detailed and localized description of the group. Maximum 128 characters. **Point Suffix** A unique identifier that is added to the end of the input point suppression pseudo point generated for this point. Maximum 60 characters, ASCII only. **NOTE**: The applications selected as candidates of the suppression group are common to all groups.
Point Selection Area	You can select system points to add to the input point suppression group using the system point tree. Click the checkbox to the left of a point or group name to add a point or a group of points to the group. Points included in the group are shown at the right-hand side of the point selection area. To remove a point, uncheck the appropriate box in the system point tree or highlight the point and click the **Delete** button. Click the **Delete NE** to remove any points that are not valid (that is, points that have been deleted from the system database after they were included in the group. **Suppression State** Select whether the application provides the last reported value or a pre-configured suppression value to candidate applications when suppression is enabled. **Override Value** Choose the value to supply to candidate applications when suppression is enabled. ON or OFF for DI points, or a value entry for AI points. This field is disabled and ignored when **Last Reported** is selected as the point's suppression state.

Redundant I/O

The **Redundant I/O** feature of the System Point Manager allows you to specify a Secondary data source for any point that is used to report the value and quality of the Primary point in the event the Primary point becomes invalid or questionable.

Controls sent to a Primary point while a Secondary data source is in effect automatically routed to the Secondary data source instead. Acknowledgement messages are handled by the MCP to appear as though they were routed from the Primary point. A virtual quality flag, **Secondary Source**, is applied to the Primary point and is visible within certain system applications, however, this flag is not stored as an actual quality flag.

Please review this note if you are using input point suppression in conjunction with redundant I/O.

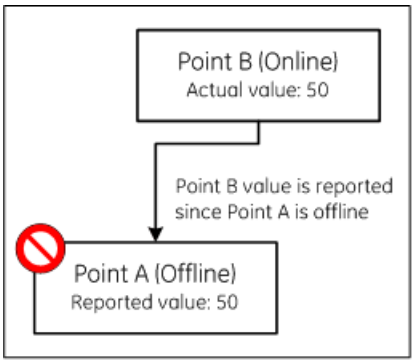
Table 6.142: Redundant I/O

Field	Description
Point Selection Area	You can select the system points that you would like to have a Secondary data source. Click the checkbox to the left of a point or group name to add a point or a group of points to the group. Points included in the group are shown at the right-hand side of the point selection area. To remove a point, uncheck the appropriate box in the system point tree or highlight the point and click the **Delete** button. Click the **Delete NE** to remove any points that are not valid (that is, points that have been deleted from the system database after they were included in this list.

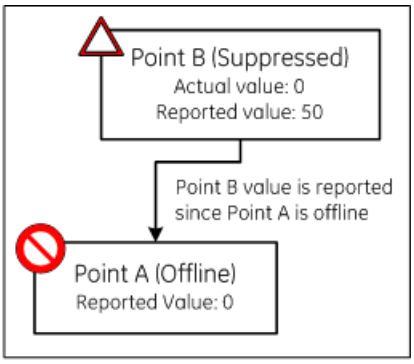
Secondary Source	A point selection tree that allows you to choose the point to be used as the Secondary source. Only points of the same data type that have not already been selected as a Primary source are available.
IO Group	Opens the **Redundant I/O Group** window, which contains the following six fields. Redundant I/O groups can be reused for multiple points. Up to 10000 Redundant IO Groups can be created. **Group Name** A short text description that is assigned to the group. Maximum of 66 ASCII characters comprising alphanumeric characters, space, underscore and dash. **Group Description** A user-defined block of text that provides a detailed and localized description of the group. Maximum 128 Unicode characters. **Secondary Source DI** This digital input point is set to ON if any point within the I/O group is relying on a Secondary source. This field is a user-defined name that can be used for quick indexing and filtering. Maximum 66 characters, ASCII only. **Secondary Source DI Description** A user-defined block of text that provides a detailed and localized description of the Secondary source DI point. Maximum 128 characters. **Secondary Source DO** This digital output point transfers all Primary points within the group to their respective Secondary sources upon receipt of a latch ON, close, or pulse ON control. The points can be returned to their own reported values through a latch OFF, trip, or pulse OFF control. This field is a user-defined name that can be used for quick indexing and filtering. Maximum 66 characters, ASCII only. **Secondary Source DO Description** A user-defined block of text that provides a detailed and localized description of the Secondary source DO point. Maximum 128 characters.

NOTE: Input point suppression and redundant I/O

Redundant I/O processing occurs before input point suppression. Therefore, suppressing the Secondary source of a redundant pair does not cause the suppressed value to appear as the value of the Primary point. Instead, the Primary point continues to receive the live value of the Secondary source. You must suppress the Primary point directly for the suppressed value to appear.



Redundant I/O without input suppression



Redundant I/O with input suppression

Control In-Progress

The Control In-Progress feature of system point manager allows you to trace if a control command on digital output point is in progress or not. This feature also provides information about the application that has issued the command and the control command type.

You can add any number of digital output points to a control in-progress group, but any digital output point may only be included in a maximum of one group at a time. The Apply and Remove tag and alarm local HMI commands are only supported by points generated by this feature.

Table 6.143: Control In-Progress

Field	Description
Group Name	A short text description that is assigned to the group. Maximum of 66 ASCII characters comprising alphanumeric characters, space, underscore and dash.
Group ID	Non-editable. A unique reference identifier for the group.
Group Description	A description of the group. Maximum 128 Unicode characters.
Point Selection Area	You can select system points to add to the control in progress group using the system point tree. Click the checkbox to the left of a point or group name to add a point or a group of points to the group. Points included in the group are shown at the right-hand side of the point selection area. To remove a point, uncheck the appropriate box in the system point tree or highlight the point and click the Delete button. Click the Delete NE to remove any points that are not valid (that is, points that have been deleted from the system database after they were included in the group. **In Progress Point** Opens the **In-Progress Point Details** window, which contains the following two fields. **Point Reference** A user-defined name that can be used for quick indexing and filtering. Maximum 66 characters, ASCII only. **Point Description** A user-defined block of text that provides a detailed and localized description of the group. Maximum 128 Unicode characters. This digital input point is set, when control command on the Digital Output point is in progress and is reset when the control command is complete. Control command is complete either on receiving a command response or expiry of maximum control time. In case of no command response, the maximum time for which the point is in set state depends on type of control command issued. The maximum time is calculated as per the below formulae. **Pulse On / Pulse Off**: (Pulse-On Duration + Pulse-Off Duration) * Number of Pulses + 100ms **Trip / Close:** (Pulse-On Duration) * Number of Pulses + 100ms **Latch-On / Latch-Off**: 100ms **Last Issued Control Type** Opens the **Last Issued Control Point Details** widow, which contains following two fields. **Point Reference** A user-defined name that can be used for quick indexing and filtering. Maximum 66 characters, ASCII only. **Point Description** A user-defined block of text that provides a detailed and localized description of the group. Maximum 128 Unicode characters. This analog input point provides the information about the last control command type that was issued. The possible values of this analog input point are: -1 - Digital Output point is offline 0 - Digital Output Point is online 1 - Last issued control command on Digital Output point is Trip 2 - Last issued control command on Digital Output point is Close 3 - Last issued control command on Digital Output point is Pulse On 4 - Last issued control command on Digital Output point is Pulse Off

	5 - Last issued control command on Digital Output point is Latch On 6 - Last issued control command on Digital Output point is Latch Off **Last Issued Application** Opens the **Last Issued Application Point Details** widow, which contains following two fields. This analog input point gives the application ID of the application that has issued the command in the digital output point. **Point Reference** A user-defined name that can be used for quick indexing and filtering. Maximum 66 characters, ASCII only. **Point Description** A user-defined block of text that provides a detailed and localized description of the group. Maximum 128 Unicode characters. If the control command issuer application is an automation application, then the value is one from the below list. If the application is not an automation application, the application ID is provided as a pseudo point in the issuer application. -1 - HMI -2 - Calculator -3 - Data Logger -4 - LogicLinx -6 - Redundancy Manager (not supported in G100) -7 - System Status Manager -9 - System Point Manager Control Lockout -10 - System Point Manager Input Point Suppression -11 - System Point Manager Accumulator Freeze -12 - System Point Manager Analog Value Selection -13 - System Point Manager RIO -14 - Load Shed Curtailment -15 - Digital Event Manager -23 - Analog Reports

Alarm

In the substation-monitoring environment, alarms are used to indicate the occurrence of an event that requires attention, for example, the opening of a breaker due to an over-current condition.

The MCP monitors a given set of digital input points for alarm conditions. Each configured alarm by default has no associated pseudo points. However, if the "individual digital input indications" parameter is set in an alarm group, then a single digital input pseudo point is created for each alarm in the group.

Upon detecting an alarm condition on a source point or a group of points, the MCP creates a record in the database and presents the alarm to the operator on the MCP Active Alarms page for further action. Once an alarm is acknowledged it is archived by moving it from the **Active Alarms** page to the **Historical Alarms** page.

You can:

- View active alarms
- View historical alarms
- Acknowledge an alarm
- Configure alarms, including double-point alarms, alarm points, and alarm settings
- Enable/mute an audible alarm

Alarm Types

The following alarms types are configurable:

- **Deviation Alarms** (2-state): Generates an active alarm when the point state changes from normal to alarmable and archives the alarm only when the point state returns to normal and the alarm is acknowledged.
- **On Update Alarms** (2-state): Generates an active alarm when the alarm state changes from one state to another and archives the alarm when the alarm is acknowledged. In effect, two alarms are created: the first alarm is generated when the source point changes from ON to OFF, and a second alarm is generated when the source point changes from OFF to ON.
- **Double Point Alarms** (4-state): Two alarm types are generated – an **On-Update Alarm** and a **Deviation Alarm**.

  NOTE: You can only select pre-configured double points for this type of alarm.

  - An **On Update Alarm** is generated when the double point is in the transit state (both points = 0) or in the invalid state (both points = 1) and the state persists longer than the configured invalid period of time. The On Update alarm is archived when it is acknowledged.
  - A **Deviation Alarm** is generated when the double point is in the open state (open point = 1, close point = 0) and is put in the reset state when the double point returns to the close state (open point = 0, close point = 1). The Deviation alarm is archived when the alarm state is reset, *and* it is acknowledged.

NOTE: The Digital Event Manager does not support the "," (comma) character in the Point, Point State, Alarm and Alarm State field descriptions. If the user has used commas in these field descriptions during configuration, the commas are automatically replaced with spaces during runtime processing.

NOTE: The MCP does not raise alarms on points that are offline.

Configure Alarms

On the **Alarm** tab on the **Configuration** page you can configure alarms and modify how alarms are processed and reported by the MCP. The maximum number of SOE, active alarms and historical alarms that can be present in the MCP database are configurable and this configuration is done from **storage** option on the Systemwide tab.

NOTES:

- Alarms must be configured to activate the Active Alarms page in the MCP HMI.
- Digital points must already be configured in map files before they can be selected as alarmable points.

Alarm Points tab

On the **Alarm Points** tab, you configure digital input points for alarm-capable conditions. The MCP supports three alarm types:

- Deviation (2 state)
- On Update (2 state)
- Double Point (4 state)

The **Point Picker** pane lists the digital input points in the database available for configuration as alarm points. Each alarm type tab lists the selected alarm points and the current configuration settings.

NOTES:

- Alarms must be configured to activate the Active Alarms page in the MCP HMI.
- Digital points must already be configured in map files before they can be selected as alarmable points.
- You must select a pre-configured double point for double point alarms.

» To configure alarm points:

1. Click the **Configuration** Power bar button.
2. Click the **Alarm** tab > **Alarm Points** tab.
3. Click the tab for the type of alarm to be configured: **Deviation Alarms**, **On Update Alarms**, or **Double Point Alarms**.
4. In the tree-view pane, expand the folders and click to select digital input points to add to the alarm list.
5. To modify the default settings for an alarm point, in the alarm list, double-click a setting and enter a new value.
6. Click **Save** to save your changes.

» To configure alarm settings:

1. Click the **Configuration** Power bar button.
2. Click the **Alarm** tab > **Settings** tab.
3. Select **Global Settings** or **Alarm Group Settings**.
4. To modify the default settings, double-click a setting and enter a new value.
5. Click **Save** to save your changes.

Tip: To remove a point from the Alarms list, select the row and click **Delete**. Click **Delete NE** to remove points that have been deleted from the system database after they were selected as alarmable points.

Alarm Points configuration settings

Deviation Alarms

Table 6.144: Deviation Alarms

Setting	Description
Connection	The name of the application or device that the point belongs to. This field is not editable.
Source Point	DI source point selected from the Point Picker. This field is not editable.
Source Description	A detailed and localized description of the point. This field is not editable.
Alarm Reference	A user-defined name that can be used for quick indexing and filtering. Maximum 66 characters, ASCII only.
Alarm Description	A user-defined block of text that provides a detailed and localized description of the group. Maximum 128 characters.
Text State 0	Enter text to display to represent the point state when the associated digital input point value becomes 0, typically the Normal state. Range is 1 to 32 alphanumeric characters.
Text State 1	Enter text to display to represent the point state when the associated digital input point value becomes 1, typically the Alarm state. Range is 1 to 32 alphanumeric characters.
Invalid State Description	Select the state to be reported in the event the point is INVALID.
Alarmable State	Select to indicate when the point value is in the alarmable state: OFF (0) or ON (1).
Group	Select the single alarm group to which the point's alarm is to be associated with. All configuration information for the alarm group (for example, color and sound) is applied to every point associated with the alarm group. Alarm groups are configured on the Settings tab.
Originator	Select the specific originators that trigger an alarm. Available for IEC 61850 points only.
Source	Indicates the selected source Home Directory and the Point ID of the Source Point.
Alarm ID	Unique Alarm Identification number which is auto-assigned by the Alarm application for each of the newly configured Alarms.

On Update Alarms

Table 6.145: On Update Alarms

Setting	Description
Connection	The name of the application or device that the point belongs to. This field is not editable.
Source Point	DI source point selected from the Point Picker. This field is not editable.
Source Description	A detailed and localized description of the point. This field is not editable.
Alarm Reference	A user-defined name that can be used for quick indexing and filtering. Maximum 66 characters, ASCII only.
Alarm Description	A user-defined block of text that provides a detailed and localized description of the group. Maximum 128 characters.
Text State 0	Enter text to display to represent the point state when the associated digital input point value becomes 0, typically the Normal state. Range is 1 to 32 alphanumeric characters.
Text State 1	Enter text to display to represent the point state when the associated digital input point value becomes 1, typically the Alarm state. Range is 1 to 32 alphanumeric characters.
Invalid State Description	Select the state to be reported in the event the point is INVALID.
ACK Method	Select the method to acknowledge the alarm: manually by the user or automatically by the MCP when generated (and then immediately archived.)
Group	Select the single alarm group to which the point's alarm is to be associated with. All configuration information for the alarm group (for example, color and sound) is applied to every point associated with the alarm group. Alarm groups are configured on the Settings tab.
Originator	Select the specific originator that triggers an alarm. Available for IEC 61850 points only.
Source	Indicates the selected source Home Directory and the Point ID of the Source Point.
Alarm ID	Unique Alarm Identification number which is auto-assigned by the Alarm application for each of the newly configured Alarms.

Double Point Alarms

Double points must be configured using the System Point Manager before they can be selected for alarming.

Table 6.146: Double Point Alarms

Setting	Description
Source Point	DI source point selected from the Point Picker. This field is not editable.
Source Description	A detailed and localized description of the point. This field is not editable.
Alarm Reference	A user-defined name that can be used for quick indexing and filtering. Maximum 66 characters, ASCII only.
Alarm Description	A user-defined block of text that provides a detailed and localized description of the group. Maximum 128 characters.
Text States	Text labels to be used for each of the four states of the double point. Maximum 32 characters.
Invalid ACK Method	Select the method to acknowledge the alarm: manually by the user or automatically by the MCP when generated (and then immediately archived.)
Invalid State Value	Select the state to be reported in the event the point is INVALID.
Group	Select the single alarm group to which the point's alarm is to be associated with. All configuration information for the alarm group (for example, color and sound) is applied to every point associated with the alarm group. Alarm groups are configured on the Settings tab.
Originator	Select the specific originator that triggers an alarm. Available for IEC 61850 points only.

Alarm ID	Unique Alarm Identification number which is auto-assigned by the Alarm application for each of the newly configured Alarms.

Alarm Settings tab

On the Alarm **Settings** tab, you configure the way that alarms are grouped and presented on the **Active Alarms** page. The MCP supports the configuration of global alarm settings and alarm groups, including the information columns to display on the Active Alarms page.

NOTE: Some changes on the **Alarm Settings** tab require a restart of your browser to take effect.

Global settings

Table 6.147: Alarm Settings - Global

Setting	Description
Alarm On Startup	Set which points generate alarms when the MCP is started or restarted. This value can be set to: • **Disable**: No points are generated at startup • **All Points**: All points mapped to alarms are generated at startup. • **Only Pseudo Points**: Only pseudo points mapped to alarms are generated at startup.
DB Commit Time (sec)	The interval, in seconds, at which data is committed to the database by the digital event manager. Range is 10 to 60, default is 30.
SOE Notification Method	Select the method to report SOE events. Range is **None**, **Email**. Default is None.
Alarm Notification Method	Select the method to report SOE events. Range is **None**, **Email**. Default is None.
Email Notification Delay	The amount of time, in seconds, that the digital event manager waits to buffer additional events before sending an email notification. Range is 30 to 3600. Default is 30.
Notification Time Format	The timezone to use when printing or sending email notifications. Localtime uses the time zone configured on the MCP using mcpcfg and UTC uses the MCP system clock without any modification.
Log Pseudo Points	Select whether or not to report alarms from pseudo digital inputs. You can override this setting by manually configuring alarms on pseudo digital input points.
Alarm Sound File	The audio file to be played by the MCP HMI when an alarm occurs.
Alarm Blinking Rate	The speed at which the Active Alarms icon in the powerbar flashes when acknowledged or unacknowledged alarms are present.
LOCAL HMI Alarm Buzzer ON	The alarm buzzer ON in seconds. The buzzer is disabled when ON=0
LOCAL HMI Alarm Buzzer OFF	The alarm buzzer OFF in seconds. Continuous steady tone is when OFF=0 and ON>0

Number of SOE and Alarms

The maximum number of SOE's, historical and SOE alarms that can be present in system are configurable. This configuration is present in S**ystemwide** tab under **System ->Storage** section. The slider options allow the User to configure maximum under of SOE/PRF, historical and active alarms that can be present in the system.

Table 6.148: Number of SOE and Alarms

Setting	Description
Max Number of SOE/PRF	The Maximum number of SOE/PRF records that can be stored in the Database. Range is 10,000 to 2,00,000, default is 50,000
Max Number of Active Alarms	The Maximum number of Active alarm records that can be stored in the Database. Range is 2000 to 20,000, default is 5,000
Max Number of Historical Alarms	The Maximum number of Historical alarms records that can be stored in the Database. Range is 10,000 to 2,00,000, default is 50,000

Alarm Groups settings

Click the **Add** button to create a new alarm group. Select a group and click the **Delete** button to remove it. Any alarms assigned to a group that is deleted become unassigned and must be manually re-assigned to a different group.

Table 6.149: Alarm Groups Settings

Setting	Description
Group Reference	A user-defined name that can be used for quick indexing and filtering. Maximum 66 characters, ASCII only.
Group Description	A user-defined block of text that provides a detailed and localized description of the group. Maximum 128 characters.
Individual Alarm Indication	If this setting is enabled, one digital input pseudo point is created for each alarm in the group. The pseudo point for the group is set to ON if the alarm is active. **NOTE**: Redundant pseudo points are created if alarms are assigned to multiple groups.
Display Scheme	Select a pre-configured alarm display scheme or create a new one. The settings below are configurable for each display scheme.
Display Name	A user-defined name that can be used for quick indexing and filtering. Maximum 66 characters, ASCII only.
Display Description	A user-defined block of text that provides a detailed and localized description of the group. Maximum 128 characters.
In Alarm Blink Rate	The rate at which the active alarm text blinks when it is in the alarm state.
Reset Alarm Blink Rate	The rate at which the active alarm text blinks when it is in the normal alarm state.
Acked Alarm Blink Rate	The rate at which the active alarm text blinks when it is in the acknowledged state.
Foreground Colors (4x)	Select the color of the text that appears when a point belonging to the alarm group is in one of the following alarm conditions: • On Update In Alarm, • Deviation in Alarm, • Deviation Reset, or • Deviation Acked (acknowledged) Click a color Value cell to see the color palette window. The color can be chosen from **Swatch**, **HSV**, **HSL**, **RGB**, or **CMYK** palettes.

Setting	Description	
Background Colors (4x)	Select the background (BG) color of the text that appears when a point belonging to the alarm group is in one of the following alarm conditions: • On Update In Alarm, • Deviation in Alarm, • Deviation Reset, or • Deviation Acked (acknowledged) Click a color Value cell to see the color palette window. The color can be chosen from **Swatch**, **HSV**, **HSL**, **RGB**, or **CMYK** palettes.	
Group Alarm Reflash Time (ms)	The amount of time (in milliseconds) that the group alarm re-flash DI point continues to indicate to the master station that a new alarm has occurred.	
Pseudo Points	Opens the **Group Pseudo Point Properties** window, which contains the following fields which are available under the System Point Manager application.	
Group Unacknowledged Reference	This point specifies whether there are alarm records for any alarm in this group that are not in the reset or not acknowledged state.	These pseudo points created for this group evaluate to TRUE when any points in the group are in the conditions listed (unacknowledged, in alarm, or acknowledged).
Group Unacknowledged Description	This is a user-defined block of text that provides a description of the Group Unacknowledged Reference point. Maximum 128 characters.	
Group In Alarm Reference	This specifies whether there are alarm records for any alarm in this group that are not in the reset state.	
Group In Alarm Description	This is a user-defined block of text that provides a description of the Group In Alarm Reference point. Maximum 128 characters.	
Acknowledge Group Reference	A latch ON, close, or pulse on operation for this point acknowledges all alarms in this group.	
Acknowledge Group Description	This is a user-defined block of text that provides a description of the Acknowledge Group Reference point. Maximum 128 characters.	
<State> Reference	A user-defined name that can be used for quick indexing and filtering. Maximum 66 characters, ASCII only.	
<State> Description	A user-defined block of text that provides a detailed and localized description of the point. Maximum 128 characters.	
Total Alarms Reference	A user-defined name that can be used for quick indexing and filtering. Maximum 66 characters, ASCII only.	These two pseudo points refer to an analog output point that contains the number of alarms contained within the group.
Total Alarms Description	A user-defined block of text that provides a detailed and localized description of the point. Maximum 128 characters.	
Alarm Indication Point Reference	These DI points are reset whenever one or more of the alarms belonging to the group are active.	
Alarm Indication Point Description	This is the description field for the Alarm Indication Point Reference setting.	
Group In Alarm Reflash Reference	This DI point is momentarily de-asserted and re-asserted after a short duration of time to alert that a new alarm has occurred in a group that is already in an alarmable state.	

Setting	Description	
Group In Alarm Reflash Description	This is the description field for the Group In Alarm Reflash Point Reference setting.	

Originators

The MCP documents the sources of control commands and reports this information on the Active Alarms, Historical Alarms, and SOE List pages under the **Originator** field.

The Originator is only available for points mapped from IEC 61850 devices that support enhanced security controls, such as the GE D25 Multifunction IED. It corresponds to the orCat value in IEC 61850-7-3 Table 8. For all other points, it appears as *not supported*.

Table 6.150: Originators example from D25

Originator	Description
not-supported	The control command did not contain originator information.
bay-control	Operator using a client located at bay level. For example, a graphical display panel on a bay controller.
station-control	MCP web interface or local HMI.
remote-control	Remote operator outside the substation. For example, master station via MCP server applications, like DNP3 or Modbus.
automatic-bay	Automation logic, like Calculator or LogicLinx, through a bay controller.
automatic-station	Automation logic, like Calculator or LogicLinx, on the MCP.
automatic-remote	Automation logic, like Calculator or LogicLinx, through a master station.
maintenance	Actions initiated through the WESMAINT connection.
process	Status change occurred without control action. For example, the trip of a circuit breaker or failure inside the breaker.

Calculator

On the **Calculator** tab on the **Configuration** page you configure the Calculator automation application by:

- Selecting data points referenced in expressions (called mapped points)
- Building expressions

The Calculator creates new points in the MCP system point database based on the results of the configured expressions. Once you have defined calculated points, they are available for selection when creating server maps, configuring alarms, and creating additional Calculator expressions. During runtime, calculated point values are presented to the operator on the **Application** tab on the **Point Details** page.

NOTE: Data points must already be configured in the MCP before they can be selected as mapped points in the Calculator.

The Calculator application is typically used in the MCP to carry out the following functions:

- Perform Mathematical, Logical, or Timer based operations on selected system data points
- Automatically operate one or more digital or analog outputs when certain conditions are met

The Calculator creates new points in the MCP system point database based on the results of configured expressions. All Calculator-owned points are referred to in the expressions by a configurable alias name. The values of the data points generated by the Calculator are evaluated each time a change event is received on one of the data points referenced in a defined expression.

The following data types are supported for use in expressions.

- Analog Input (AI)
- Digital (binary) Input (DI)
- Analog Output (AO)
- Digital (binary) Output (DO)
- Accumulators
- Text

The Calculator supports the following types of point calculations:

- Evaluations
- Timers
- Analog Assignments
- Digital Assignments
- Quality conversion
- Type conversion
- Averages
- Output to Input conversions

One you have defined calculated points; they are available for selection when creating client and server maps and configuring alarms. During runtime, calculated point values are presented to the operator on the **Automation** tab on the **Point Details** page.

Mapped Points

The **Mapped Points** tab on the **Calculator** page is used to select system points to be used as variables within Calculator expressions.

The left pane displays a tree view listing of the data points available in the MCP system point database from which you can select as mapped points. Mapped points are organized under the data type sub-tabs: Analog Input, Analog Output, Digital Input, Digital Output, Accumulator, and Text.

Mapped points that are selected in the tree view are added to the list in the center of the screen. Double-click the **Alias** field within this list to change the Calculator alias for the point (the alias is only used within the Calculator application). The alias field can be 1 to 126 ASCII characters.

To delete a point, select the point and click the **Delete** button. Click the **Delete NE** button to remove all non-existent points that are referenced. Non-existent points may occur if a device containing the referenced data points is deleted from the MCP.

Expressions

Expressions

The **Expressions** tab on the **Calculator** page is used to create, modify and delete calculated expressions. Up to 10000 Calculator Expressions can be created.

You construct expressions by combining operands and operators to produce a resulting point. You can use any defined reference points in expressions. Operands can include constants, system data points and Quality attributes. Operators include mathematical, logical, and bit-wise operators. The expressions also define the Point Names and Data Types that are used to represent the resulting evaluation.

» To create an expression:

1. Click the button.
2. On the **New Expression** window, select the type of expression you want to create and click **OK**.
3. The new expression is added to the left pane. Select it to display the configuration window.

» To delete an expression:

1. Select the expression in the left pane.
2. Click the button. The expression is deleted.

The following related actions can be performed to configure:

- Evaluations
- Timers
- Analog assignments
- Digital assignments
- Quality conversions
- Type conversions
- Averages
- Output to Input conversions

Evaluations

Evaluation expressions perform operations on referenced points and store the result in a Calculator-owned input point.

The following operations are supported in evaluation expressions:

- Math operations
- Logical operations
- Bit-wise operations
- Request Type operations
- If-Then-Else construct

Evaluation expressions are re-evaluated whenever a data change event is issued on a point referenced by the expression. Quality changes on referenced points only cause re-evaluation if the expression is converting the changed quality flag into a digital input, or if the quality change indicates that the referenced point is coming online or has had communications restored. The Calculator monitors the quality of referenced points for changes in the Questionable and Invalid quality flags. If any referenced point becomes Invalid or Questionable, the resulting point for any expression that includes that referenced point becomes Invalid.

Table 6.151: Evaluation Fields

Field	Description
Name	A system name to describe this expression within the Calculator application. Range is up to 128 alphanumeric characters.
Target Point Type	The type of point that is returned as the output of the expression.
Target Point	The name of the point that is returned as the output of the expression. This name must be unique across all data types.
Target Alias	Enter a short name to reference the output point within Calculator. Must be unique across all data types. Used as point description in Available Points list. Supported characters are: any combination of up to 126 characters using "a" through "z", "0" through "9", "_" (underscore) and "-" (hyphen), followed by a suffix indicating the data type of the referenced point (ai, ao, di, do, acc, or txt). Spaces are not allowed. Suggested format is <a to z><1 to 9999><datatype>. For example, scada43di. Range is up to 126 alphanumeric characters. Default is Xai or Xdi, depending on the Target Point Type, where X is incremented from 1.
Result Point Description	A user-defined description of the expression.
Expression Notes	Internal notes regarding the expression.
Expression	The formula used to calculate the expression. To insert a mapped point, calculator point, or expression, expand the tree menu and double-click the entry.

Example Field Settings

Table 6.152: Field Settings - Example 1

Field	Example Settings
Name	Evaluation 1
Target Point Type	Analog Input
Target Point	AI 11
Target Alias	11ai
Result Point Description	Analog Input 11
Expression Notes	Sum of AI 1, AI 2 and AI 3.
Expression	1ai + 2ai + 3ai

Table 6.153: Field Settings - Example 2

Field	Example Settings
Name	Evaluation 2
Target Point Type	Analog Input
Target Point	AI 12
Target Alias	12ai
Result Point Description	Analog Input 12
Expression Notes	Multiplication of AI 1 and AI 11.
Expression	1ai * 11ai

Table 6.154: Field Settings - Example 3

Field	Example Settings
Name	Evaluation 3
Target Point Type	Digital Input
Target Point	DI 10
Target Alias	10di
Result Point Description	Digital Input 10
Expression Notes	Logical AND of DI 1 and DI2.
Expression	1di && 2di

Example Expressions

Table 6.155: Expressions - Example

Expression	Description
3di && (4di || 5di)	If DI3 is 1 and either DI 4 or DI 5 is 1 then the result of the expression is set to 1. Otherwise, if DI 3 is 0 or both DI 4 and DI 5 are 0 then the result of the expression is set 0. Where, DI 3, DI 4 and DI 5 are the mapped/referenced points.
(RT (10do) == TR)? 0 : 1	When a trip command is received on calculator digital output point DO 10, set the result of the expression to 0. For any other commands, set to 1.
(6di | 7di | 8di) ?(4ai + 1000) : 0	If any of DI 6, DI 7, or DI 8 are 1, set the result of the expression to (4ai + 1000). If all are zero, set the result of the expression to zero.
(RT (11do) == PU)? 5ai	Whenever a pulse on operation is received on calculator digital output point DO 11, set the result of the expression to 5ai. Otherwise, no operation.
(6ai > 5000)? 1: (RT (12do) == ANY)? 0	If AI 6 is greater than 5000, set the result of the expression to 1. Otherwise, if AI 6 is less than or equal to 5000 and when any command is issued on calculator digital output point DO 12, set the result of the expression to 0.

Math Operations

The Calculator handles mathematical operations as follows:

- A mathematical operation is always evaluated using floating-point arithmetic.
- If binary values are used as operands for a math operation, then TRUE is interpreted as 1 and FALSE as zero.
- Mathematical operators are evaluated left to right only. Order of precedence is not enforced on mathematical expressions unless parentheses are used.

The Calculator supports the following math operators:

Table 6.156: Math Operations

Symbol	Operation	Example
+	Addition	B1 + B2
-	Subtraction	B1 - B2
*	Multiplication	B1 * B2
/	Division	B1 / B2
%	Modulo	B1 % B2
^^	Exponent	B1 ^^ B2
loge	Natural logarithm	loge(B1)
log10	Logarithm base	10 log10(B1)

Logical Operations

The Calculator handles logical operations as follows:

- All operands are evaluated as binary values before performing the logical operation.
- A logical operation evaluates to TRUE or FALSE.
- All non-zero values are interpreted as TRUE and zero values as FALSE.
- If the output is later used in a mathematical operation, TRUE is interpreted as 1 and FALSE as zero.

The Calculator supports the following logical operators:

Table 6.157: Logical Operations

Symbol	Operation	Example
==	Equal	B1 == B2; Result is true if B1 and B2 are equal, false otherwise
>	Greater Than	B1 > B2; Result is true if B1 is greater than B2, false otherwise
<	Less Than	B1 < B2; Result is true if B1 is less than B2, false otherwise
>=	Greater Than or Equal To	B1 >= B2; Result is true if B1 is greater than or equal to B2, false otherwise
<=	Less Than or Equal To	B1 <= B2; Result is true if B1 is less than or equal to B2, false otherwise
!=	Not Equal	B1 != B2
&&	Logical AND	B1 && B2; Result is true if B1 and B2 are true, false otherwise.
||	Logical OR	B1 || B2; Result is true if either of B1 or B2 is true, false otherwise.
!	Logical NOT	!B1; Result is true if B1 is false and vice versa.

Logical operators and mathematical operators can be combined to create if/then/else-style statements.

For example, the simple construct *if a then b else c*, where a is a logical operation, could be expressed as *((a) * b) + ((!a) * c)* in the Calculator. Since logical operations always evaluate to 1 or 0, the multiplication effectively 'cancels' the result for the logical operation that is not true.

NOTE: The weakness of this approach is that the "else" case must always be defined. It is not possible to define a simple "if/then" construct with this method.

Bit-Wise Operations

The Calculator handles bit-wise operations as follows:

- The output of a bit-wise operation is always a 32-bit integer value.

- A floating-point value is converted to a 32-bit integer by dropping all data after the decimal before performing a bit-wise operation.
- If the expression stores the final value in a digital input, then a non-zero value is interpreted as TRUE, while a zero value is interpreted as FALSE, unless a specific bit position is specified in the result to be selected as the DI state.

The Calculator supports the following bit-wise operators:

Table 6.158: Bit-Wise Operations

Symbol	Operation	Example
>>	Bit Shift Right	B1 >>3
<<	Bit Shift Left	B1<<3
&	AND	B1&B2
|	OR	B1|B2
~	1's complement	~ B1
^	Exclusive OR	B1^B2

Request Type Operations

The Calculator handles request type operations as follows:

- The request type operator references the type of command received by a Calculator-owned digital output point and evaluates to one of the request types listed below. As such, the operator can only be used in conjunction with the logical operators *equal* and *not equal* (for example, *RT (d05) == TR*).
- The syntax *RT(<alias>) == <request type>* is used, where *alias* is the alias of any Calculator-owned digital output point and *request type* is one of the nine request types listed below.
- The operator is only evaluated now a command is received on the Calculator-owned digital output point. At that moment, all expressions that reference the digital output are evaluated. Immediately after all evaluations are complete, the operator evaluates to NO when processing a change in any other point in the expression.

The request type operator evaluates to one of the following values:

Table 6.159: Request Type Operations

Operation	Request Type
Latch On	ON
Latch Off	OFF
Pulse On	PU
Pulse Off	PO
Close	CL
Trip	TR
Don't Care (see note)	ANY
No Operation	NO

NOTE: If the request type is tested against ANY, then any control operation except NO evaluates to 1

If-Then-Else Construct

The Calculator supports the **If-Then-Else** construct *<condition> ? <value if true> : <value if false>*. The construct evaluates to *value if true* if the *condition* results in a non-zero value, or to *value if false* if the *condition* results in zero.

You may leave either of the value fields empty. If this is done and the *condition* selects the empty value, the construct is considered not to have changed and no further evaluation is carried out. The syntax of the construct is either <*condition*> *?* <*value if true*> or <*condition*> *? :* <*value if false*>

Timers

The Calculator provides timer functionality to a resolution of 1 second. A timer operation is defined by two hold times: rising edge (FALSE to TRUE) and falling edge (TRUE to FALSE). Hold times can be positive or zero. When the result of a binary expression changes, Calculator starts a timer based on the defined hold times. If the value of the binary expression stays constant for the entire timer duration, then the value of the timer expression evaluates to TRUE.

For example, if you want a Calculator digital input to turn ON when digital inputs DI22 and DI54 are the same value for more than 10 seconds, use the following settings:

- Output point type is *Digital Input*
- The timer expression is *(DI22 == DI54)*
- The Rising Edge Time is *10* and the Falling Edge Time is *0*.

Result: The output of Calculator digital input will turn ON after 10 seconds.

Table 6.160: Timer Operations

Field	Example Settings
Name	A system name to describe this expression within the Calculator application. Range is up to 128 alphanumeric characters.
Target Point Type	The type of point that is returned as the output of the expression.
Target Point	The name of the point that is returned as the output of the expression. This name must be unique across all data types.
Target Alias	Enter a short name to reference the output point within Calculator. Must be unique across all data types. Used as point description in Available Points list. Supported characters are: any combination of up to 126 characters using "a" through "z", "0" through "9", "_" (underscore) and "-" (hyphen), followed by a suffix indicating the data type of the referenced point (ai, ao, di, do, acc, or txt). Spaces are not allowed. Suggested format is <a to z><1 to 9999><datatype>. For example, scada43di. Range is up to 126 alphanumeric characters. Default is Xai or Xdi depending on the Target Point Type, where X is incremented from 1.
Result Point Description	A user-defined description of the expression.
Expression Notes	Internal notes regarding the expression.
Rising Edge Time (s)	The amount of time, in seconds, that the expression must remain in the TRUE state before the timer expression evaluates to TRUE.
Falling Edge Time (s)	The amount of time, in seconds, that the expression must remain in the FALSE state before the timer expression evaluates to FALSE.
Expression	The formula used to calculate the expression. To insert a mapped point, calculator point, or expression, expand the tree menu and double-click the entry.

Example Field Settings

Table 6.161: Timer Operations - Example 1

Field	Example Settings
Name	**Timer 1**
Target Point Type	Digital Input
Target Point	DI 11
Target Alias	11di
Result Point Description	Digital Input 11
Rising Edge Time (s)	10
Falling Edge Time (s)	5
Expression Notes	(DI 7 == DI 8) (T10 L5)
Expression	(7di == 8di)

Table 6.162: Timer Operations - Example 2

Field	Example Settings
Name	**Timer 2**
Target Point Type	Digital Input
Target Point	DI 12
Target Alias	12di
Result Point Description	Digital Input 12
Rising Edge Time (s)	5
Falling Edge Time (s	10
Expression Notes	(DI 9 == 1) (T5 L10)
Expression	(9di == 1)

Analog Assignments

Analog Assignment expressions receive commands on Calculator-owned analog output and input points and translate these into operations on mapped analog data output points. Quality changes on the Calculator and referenced points are monitored in case the change in quality impacts the Calculator expression. Assignment expressions support the same syntax as evaluation expressions on the right-hand side of the expression.

Fields

Table 6.163: Analog Assignments

Field	Example Settings
Name	A system name to describe this expression within the Calculator application. Range is up to 128 alphanumeric characters.
Target Point	The source analog output point that receives output command generated by Calculator.
Expression Notes	Internal notes regarding the expression
Expression	The formula used to calculate the expression. To insert a mapped point, calculator point, or expression, expand the tree menu and double-click the entry.

Example Field Settings

Table 6.164: Analog Assignments - Example 1

Field	Example Settings
Name	**Analog Assignment 1**
Target Point	0ao
Expression Notes	Send the SetPoint command on the mapped point AO 0 if an event comes on the mapped point AI 1.
Expression	1ai

Table 6.165: Analog Assignments - Example 2

Field	Example Settings
Name	**Analog Assignment 2**
Target Point	1ao
Expression Notes	Route SetPoint command on the mapped point AO1 if a SetPoint command receives on calculator AO 10.
Expression	10ao

Table 6.166: Analog Assignments - Example 3

Field	Example Settings
Name	**Analog Assignment 3**
Target Point	2ao
Expression Notes	Assign AO 2 with 1234 if TRIP is received on calculator DO 10, OR Assign AO2 with -1234 if CLOSE is received on calculator DO 10.
Expression	(RT (10do) ==TR)? 1234: ((RT (10do) == CL)? (-1234))

NOTE: It is recommended to use braces around negative numbers in the expressions. e.g., (-1234).

Digital Assignments

Digital Assignment expressions receive commands on Calculator-owned digital output and input points and translate these into operations on referenced system digital output points. Quality changes on the Calculator and referenced points are monitored in case the change in quality impacts the Calculator expression. Assignment expressions support the same syntax as evaluation expressions on the right-hand side of the expression.

Control type (specification)

You can declare the parameters of output commands in line with the rest of an assignment expression, instead of (or in addition to) using the control type. If provided, the in-line declaration overrides any configured operation for the point. The digital output parameter syntax is *{<command type>, <on duration>,<off duration>,*<number of operations>*}* where:

- *command type* is a valid request type
- *on duration* is the length of time, in milliseconds, that the control remains in the ON state
- off duration is the length of time, in milliseconds, that the control remains in the OFF state
- number of operations is a numerical value

The alias of any mapped analog input or Calculator-owned analog output point can be used for the *on duration*, *off duration*, and number of operations variables. If aliases are used, the current value of the point associated with the alias is used as the value of the parameter (refer to the Example Expressions).

» To insert a control output parameter:

- Click the **Ctrl Spec** button on the Expression Builder.

Table 6.167: Digital Assignments - Control Type

Field	Description
Name	A system name to describe this expression within the Calculator application. Range is up to 128 alphanumeric characters.
Control Routing	The possible options are: • **None**: The functionality of the Digital assignment expression types is the same as Analog assignment. So, a command will be issued to the target DO point based on the result of the expression and according to control type and other configuration parameters. • **On Target Point**: Only "ON" type commands are routed to another DO. "OFF" type commands are not routed. • **Off Target Point**: Only "OFF" type commands are routed to another DO. "ON" type commands are not routed. • **Both Target Points**: Both "ON" and "OFF" type commands are routed to different targets. The default value selected for Control Routing is None - i.e. Digital assignment will perform no routing.
Target Point	This point receives all operation commands when the Control Routing parameter is set to None.
ON Target Point (When Control Routing Parameter is set to ON Target Point / Both Target Points)	This receives 'Close/Latch ON/Pulse ON' commands if the result of the Expression is TRUE. No command is received if the result of the Expression is FALSE.
OFF Target Point (When Control Routing Parameter is set to OFF Target Point/Both Target Points)	This point receives 'Trip/Latch OFF/Pulse ON' commands if the result of the Expression is FALSE. No command is received if the result of the Expression is TRUE. Pulse OFF commands can be issued only when Control Routing is not set to None.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Control Type
(When Control Routing Parameter is set to None)</td><td>Control type is used if your assignment expression:
• Evaluates to a true or false value
In this case, the control type instructs Calculator how to interpret the expression result based on the following criteria:
<table>
<tr><th rowspan="2">Control Type</th><th colspan="2">Control Type Issued</th></tr>
<tr><th>When expression changes to True</th><th>When expression changes to False</th></tr>
<tr><td>Inverted Latch</td><td>Latch OFF</td><td>Latch ON</td></tr>
<tr><td>Latch</td><td>Latch ON</td><td>Latch OFF</td></tr>
<tr><td>Pulse</td><td>Pulse ON</td><td>No operation</td></tr>
<tr><td>Trip/Close</td><td>Close</td><td>Trip</td></tr>
</table>
The default Control Type is Trip-Close.
• This is meant to translate a control operation from a Calculator-owned digital output into another type and pass it on to a mapped digital output if you aren't using inline control specifications. As noted above, if you use an inline control specification, the command defined inline overrides the configured control type.
In this case, the control received on the Calculator is evaluated as being a True or False type of command, and the same logic as above is applied. Control types are evaluated as follows:
• True commands: Latch ON, Pulse ON, Close
• False commands: Latch OFF, Pulse OFF, Trip
<table>
<tr><th rowspan="2">Control Type Received Calculator Owned DO Point</th><th colspan="4">Control Type Issued to Target DO Point</th></tr>
<tr><th>Control Type is Latch</th><th>Control Type is Pulse</th><th>Control Type is Trip/Close</th><th>Control Type is Inverted Latch</th></tr>
<tr><td>Latch ON</td><td>Latch ON</td><td>Pulse ON</td><td>Close</td><td>Latch OFF</td></tr>
<tr><td>Pulse ON</td><td>Latch ON</td><td>Pulse ON</td><td>Close</td><td>Latch OFF</td></tr>
<tr><td>Close</td><td>Latch ON</td><td>Pulse ON</td><td>Close</td><td>Latch OFF</td></tr>
<tr><td>Latch OFF</td><td>Latch OFF</td><td>Pulse OFF</td><td>Trip</td><td>Latch ON</td></tr>
<tr><td>Pulse OFF</td><td>Latch OFF</td><td>Pulse OFF</td><td>Trip</td><td>Latch ON</td></tr>
<tr><td>Trip</td><td>Latch OFF</td><td>Pulse OFF</td><td>Trip</td><td>Latch ON</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Control Type
(When Control Routing Parameter is set to On Target Point)</td><td>
On Target Point Control type is used if your assignment expression:
Is meant to translate a control operation from a Calculator-owned digital output into another type and pass it on to a mapped digital output if you are not using inline control specifications. As noted above, if you use an inline control specification, the command defined inline overrides the configured control type.
The On Target Point Control Type instructs Calculator on how to interpret the expression result based on the following criteria:
<table>
<tr><th rowspan="2">On Target Point Control Type</th><th colspan="2">On Target Point Control Type Issued</th></tr>
<tr><th>When expression changes to True</th><th>When expression changes to False</th></tr>
<tr><td>Inverted Latch</td><td>Latch OFF</td><td>No operation</td></tr>
<tr><td>Latch</td><td>Latch ON</td><td>No operation</td></tr>
<tr><td>Pulse</td><td>Pulse ON</td><td>No operation</td></tr>
<tr><td>Trip/Close</td><td>Close</td><td>No operation</td></tr>
</table>
The default Control Type is Trip-Close.
The On Target Point Control Types are evaluated as follows:
<table>
<tr><th rowspan="2">Control Type Received for Owned DO Point (i.e. the single mapped in the Expression field)</th><th colspan="4">Control Type Issued to On Target DO Point</th></tr>
<tr><th>Control Type is Latch</th><th>Control Type is Pulse</th><th>Control Type is Trip/Close</th><th>Control Type is Inverted Latch</th></tr>
<tr><td>Latch ON</td><td>Latch ON</td><td>Pulse ON</td><td>Close</td><td>Latch OFF</td></tr>
<tr><td>Pulse ON</td><td>Latch ON</td><td>Pulse ON</td><td>Close</td><td>Latch OFF</td></tr>
<tr><td>Close</td><td>Latch ON</td><td>Pulse ON</td><td>Close</td><td>Latch OFF</td></tr>
<tr><td>Latch OFF</td><td>No operation</td><td>No operation</td><td>No operation</td><td>No operation</td></tr>
<tr><td>Pulse OFF</td><td>No operation</td><td>No operation</td><td>No operation</td><td>No operation</td></tr>
<tr><td>Trip</td><td>No operation</td><td>No operation</td><td>No operation</td><td>No operation</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Control Type
(When Control Routing Parameter is set to Off Target Point)</td><td>Off Target Point Control type is used if:
• Your assignment expression is meant to translate a control operation from a Calculator-owned digital output into another type and pass it on to a mapped digital output if you aren't using inline control specifications. As noted above, if you use an inline control specification, the command defined inline overrides the configured control type.
The Off-Target Point Control Type instructs Calculator on how to interpret the expression result based on the following criteria:
<table>
<tr><th rowspan="2">Off Target Point Control Type</th><th colspan="2">Off Target Point Control Type Issued</th></tr>
<tr><th>When expression changes to True</th><th>When expression changes to False</th></tr>
<tr><td>Inverted Latch</td><td>No operation</td><td>Latch OFF</td></tr>
<tr><td>Latch</td><td>No operation</td><td>Latch ON</td></tr>
<tr><td>Pulse</td><td>No operation</td><td>Pulse ON</td></tr>
<tr><td>Trip/Close</td><td>No operation</td><td>Trip</td></tr>
</table>
The default Control Type is Trip-Close.
The Off-Target Point Control Types are evaluated as follows:
<table>
<tr><th rowspan="2">Control Type Received for Owned DO Point (i.e. the single mapped in the Expression field)</th><th colspan="4">Control Type Issued to Off Target DO Point</th></tr>
<tr><th>Control Type is Latch</th><th>Control Type is Pulse</th><th>Control Type is Trip/Close</th><th>Control Type is Inverted Latch</th></tr>
<tr><td>Latch On</td><td>No operation</td><td>No operation</td><td>No operation</td><td>No operation</td></tr>
<tr><td>Pulse On</td><td>No operation</td><td>No operation</td><td>No operation</td><td>No operation</td></tr>
<tr><td>Close</td><td>No operation</td><td>No operation</td><td>No operation</td><td>No operation</td></tr>
<tr><td>Latch OFF</td><td>Latch ON</td><td>Pulse ON</td><td>Trip</td><td>Latch OFF</td></tr>
<tr><td>Pulse OFF</td><td>Latch ON</td><td>Pulse ON</td><td>Trip</td><td>Latch OFF</td></tr>
<tr><td>Trip</td><td>Latch ON</td><td>Pulse ON</td><td>Trip</td><td>Latch OFF</td></tr>
</table>
</td></tr>
</table>

Control Type (When Control Routing Parameter is set to Both Target Points)

Both Target Points Control type is used if your assignment expression:

- Is meant to translate a control operation from a Calculator-owned digital output into another type and pass it on to two mapped digital outputs (either same DOs or different Dos), if you are not using inline control specifications. As noted above, if you use an inline control specification, the command defined inline overrides the configured control type.

The Both Target Points Control Type instructs Calculator on how to interpret the expression result based on the following criteria:

On Target Point Control Type	On Target Point Control Type Issued	
	When expression changes to True	When expression changes to False
Inverted Latch	Latch OFF	No operation
Latch	Latch ON	No operation
Pulse	Pulse ON	No operation
Trip/Close	Close	No operation

Off Target Point Control Type	Off Target Point Control Type Issued	
	When expression changes to True	When expression changes to False
Inverted Latch	No operation	Latch OFF
Latch	No operation	Latch ON
Pulse	No operation	Pulse ON
Trip/Close	No operation	Trip

The resulting actions will be a combination of configuration On Target Point Control Type and Off Point Target Control Types.

Control Type Received for Owned DO Point (i.e. the single mapped in the Expression field)	Control Type Issued to On Target DO Point			
	Control Type is Latch	Control Type is Pulse	Control Type is Trip/Close	Control Type is Inverted Latch
Latch ON	Latch ON	Pulse ON	Close	Latch OFF
Pulse ON	Latch ON	Pulse ON	Close	Latch OFF
Close	Latch ON	Pulse ON	Close	Latch OFF
Latch OFF	No operation	No operation	No operation	No operation
Pulse OFF	No operation	No operation	No operation	No operation
Trip	No operation	No operation	No operation	No operation
Latch ON	No operation	No operation	No operation	No operation
Pulse ON	No operation	No operation	No operation	No operation
Close	No operation	No operation	No operation	No operation
Latch OFF	Latch ON	Pulse ON	Trip	Latch OFF
Pulse OFF	Latch ON	Pulse ON	Trip	Latch OFF
Trip	Latch ON	Pulse ON	Trip	Latch OFF

The default type is Trip-Close.

Field	Description
Expression Notes	Internal notes regarding the expression.
Expression	The formula used to calculate the expression. To insert a mapped point, calculator point, or expression, expand the tree menu and double-click the entry.

Example Field Settings

Table 6.168: Digital Assignments - Example 1

Field	Example Settings
Name	Digital Assignment 1
Control Routing	None
Target Point	3do
Control Type	Pulse
Pulse On Duration	1000
Pulse Off Duration	100
Number of Operations	1
Override Operation	None
Expression	(RT(13do) ==PU) ?{CL,1000,0,1} :{TR,100,0,1}
Expression Notes	If a Pulse ON command is received on calculator DO 13, send a 1000ms CLOSE command on mapped point DO 3. Otherwise, send a 100ms TRIP command to DO 3.

Table 6.169: Digital Assignments - Example 2

Field	Example Settings
Name	Digital Assignment 2
Enable Control Routing	Both Target Points
Close/Latch/Pulse ON Target Point	1do
Control Type (ON Target Point)	Pulse
Pulse On Duration (ON Target Point)	1000
Pulse Off Duration (ON Target Point)	100
Number of Operations (ON Target Point)	1
Trip/Latch/Pulse OFF Target Point	2do
Control Type (OFF Target Point)	Trip-Close
Pulse On Duration (OFF Target Point)	1000
Pulse Off Duration (OFF Target Point)	0
Number of Operations (OFF Target Point)	1

Override Operation	Select Before Operate
Expression	(RT(13do) ==PU) ?{CL,1000,0,1} :{TR,100,0,1}
Expression Notes	If a Pulse ON command is received on calculator DO 13, send a 1000ms CLOSE command on mapped point DO 1. Otherwise, send a 100ms TRIP command to DO 2.

Table 6.170: Digital Assignments - Example 3

Field	Example Settings
Name	Digital Assignment 3
Enable Control Routing	On Target Point
Close/Latch/Pulse ON Target	0do
Control Type (ON Target Point)	Trip-Close
Pulse On Duration (ON Target Point)	1000
Pulse Off Duration (ON Target Point)	0
Number of Operations (ON Target Point)	1
Override Operation	None
Expression	0di
Expression Notes	Send the Trip/Close command on DO 0 if an ON event is received on 1di.

Table 6.171: Digital Assignments - Example 4

Field	Example Settings
Name	Digital Assignment 4
Enable Control Routing	OFF Target Point
Trip/Latch/Pulse OFF Target Point	3do
Control Type (OFF Target Point)	Trip-Close
Pulse On Duration (OFF Target Point)	1000
Pulse Off Duration (OFF Target Point)	
Number of Operations (OFF Target Point)	1
Override Operation	None
Expression	3do
Expression Notes	When the 1di value is 0 then the Trip command is sent to 3do. When the 1di value is 1, then no command is sent to 3do.

Example Expressions

Table 6.172: Expressions - Example

Expression	Description
!14do	Any command on the calculator owned point DO 14 is inverted and passed on to the configured mapped DO point according to the control type and other configuration parameters.
(RT (15do) != CL) ? 1 : 0	Any command on the calculator owned point DO 15 except CLOSE is passed through to configured mapped DO point according to the control type and other configuration parameters.
(0di) ? {TR, 100, 0 ,1} : 1di	When DI 0 is true, a 100-millisecond trip command will be sent to the configured mapped DO point. And, when DI 0 is false the value of 1di will be translated according to the control type and other configuration parameters.
(1ai< 1000) ? 16do	When AI 1 is less than 1000, any command calculator owned point DO 16 is passed through to the configured mapped DO point according to the control type and other configuration parameters. And, If AI 1 is greater than or equal to 1000, any command on DO 16 is ignored.
(4di) ? {PU, 1ai, 2ai, 3ai}	When mapped point DI 4 goes from false to true, send a Pulse ON command to configured mapped DO with On Duration equal to the current value of AI 1, an OFF Duration equal to the current value of AI 2, and a number of operations are equal to the current value of AI 3.

Quality Conversions

Converted points are a special class of pseudo points that are created based on an actual system point. Quality conversions take a system point and report a binary TRUE or FALSE based on a certain quality flag within that point. For example, if you create an OFFLINE quality point conversion based on analog point called *AI_000*, whenever *AI_000* is off line, the quality conversion points you created is TRUE. When *AI_000* is online, the quality conversion point is FALSE.

Quality conversion types

The MCP provides the following quality conversion flags:

- ALARM_INHIBIT
- CHATTER
- COMM_LOST
- LOCAL_CONTROL_ACTIVE
- LOCAL_FORCE – Commonly used to test expressions
- OFFLINE
- OLD_DATA
- OUTPUT_INHIBIT
- OVER_RANGE
- OVERFLOW
- QUESTIONABLE - Ceases evaluating the expression while Questionable is asserted
- REF_CHECK
- REMOTE_CONTROL_ACTIVE
- REMOTE_FORCE
- RESTART
- SCAN_INHIBIT – Asserts Questionable and Old Data flags

- SECONDARY_SOURCE
- SECONDARY_SOURCE_OFFLINE
- TAGGED
- TEST
- TIME_SYNC
- ZOMBIE - Asserts when the Zombie quality attribute of the mapped point is set

Table 6.173: Quality Conversions

Field	Description
Name	Enter a text description of the converted point in the Calculator map. Appears as the Point Description on the Point Details page. Range is up to 128 alphanumeric characters.
Quality Attribute	Selected quality flag to which the reference point is forced.
Source Point	The input point for the expression.
Target Point	The name of the point that is returned as the output of the expression. This name must be unique across all data types.
Target Alias	Enter a short name to reference the conversion point in the Calculator expression. Must be unique across all data types. Used as point description in Available Points list. Supported characters are: any combination of up to 126 characters using "a" through "z", "0" through "9", "_" (underscore) and "-" (hyphen), followed by a suffix indicating the data type of the referenced point (ai, ao, di, do, acc, or txt). Spaces are not allowed. Suggested format is <a to z><1 to 9999><datatype>. For example, scada43di. Range is up to 126 alphanumeric characters. Default is Xdi, where X is incremented from 1.
Result Point Description	A user-defined description of the expression.
Expression Notes	Internal notes regarding the expression.

Example Field Settings

Table 6.174: Quality Conversions - Example 1

Field	Example Settings
Name	Quality Conversion 1
Quality Attribute	OFFLINE
Source Point	0ai
Target Point	DI 13
Target Alias	13di
Result Point Description	Digital Input 13
Expression Notes	Set DI 13 to 1, if the quality of mapped point AI 0 is OFFLINE

Table 6.175: Quality Conversions - Example 2

Field	Example Settings
Name	Quality Conversion 2

Quality Attribute	ALARM_INHIBIT
Source Point	0di
Target Point	DI 14
Target Alias	14di
Result Point Description	Digital Input 14
Expression Notes	Set DI 14 to 1, if the quality of mapped point DI 0 is ALARM_INHIBIT

Type Conversions

Converted points are a special class of pseudo points that are created based on an actual system point. Type conversion points change points from binary to analog format, or from analog to binary. For example, if you create a binary input type conversion from an analog input, a new point is created where the value of the analog input value is converted to a binary TRUE or FALSE. The MCP provides the following type conversions:

Table 6.176: Type Conversions

Field	Description
Analog input to digital input	Floating-point values are truncated to integers. The bit position specifies which resulting integer is used to determine the state of the digital input.
Digital input to analog input	The digital input state is converted to the value 1 (TRUE) or 0 (FALSE)
Analog output to analog input	Value of the analog input reflects the current Set Point Value of the analog output
Digital output to digital input	State of the digital input reflects the current state of the digital output
Accumulator to analog input	The value type of the references point specifies whether the running or frozen value of the accumulator is used in the expression
Accumulator to digital input	The value type of the referenced points specifies whether the running or frozen value of the accumulator is used in the expression. The bit position specifies which resulting integer is used to determine the state of the digital input.
Text to analog input	ASCII text is converted into a floating-point value

Field	Description
Name	Enter a text description of the conversion point in the Calculator map. Appears as Point Description on Point Details page. Range is up to 128 alphanumeric characters. Default is tcX, where X is incremented from 1.
Source Point	The input point for the expression.
Target Point Type	The type of point that is returned as the output of the expression.
Target Point	The name of the point that is returned as the output of the expression. This name must be unique across all data types.
Target Alias	Enter a short name to reference the conversion point in the Calculator expression. Must be unique across all data types. Used as point description in Available Points list. Supported characters are: any combination of up to 126 characters using "a" through "z", "0" through "9", "_" (underscore) and "-" (hyphen), followed by a suffix indicating the data type of the referenced point (ai, ao, di, do, acc, or txt). Spaces are not allowed. Suggested format is <a to z><1 to 9999><datatype>. For example, scada43di.

	Range is up to 126 alphanumeric characters. Default is Xai or Xdi depending on the Target Point Type, where X is incremented from 1.
Value Type (ACC to AI, ACC to DI only)	The type of accumulator points to use in the expression.
Bit Position (AI to DI, ACC to DI only)	The integer within the value returned from the source point used to determine the state of the digital input.
Result Point Description	A user-defined description of the expression.
Expression Notes	Internal notes regarding the expression.

Example Field Settings

Table 6.177: Type Conversions - Example 1

Field	Example Settings
Name	Type Conversion 1
Source Point	1ai
Target Point Type	Digital Input
Target Point	DI 15
Target Alias	15di
Bit Position (AI to DI, ACC to DI only)	0
Result Point Description	Digital Input 15
Expression Notes	AI to DI Conversion

Table 6.178: Type Conversions - Example 2

Field	Example Settings
Name	Type Conversion 2
Source Point	0di
Target Point Type	Analog l Input
Target Point	AI 13
Target Alias	13ai
Result Point Description	Analog Input 13
Expression Notes	DI to AI Conversion

Table 6.179: Type Conversions - Example 3

Field	Example Settings
Name	Type Conversion 3
Source Point	0acc
Target Point Type	Digital Input

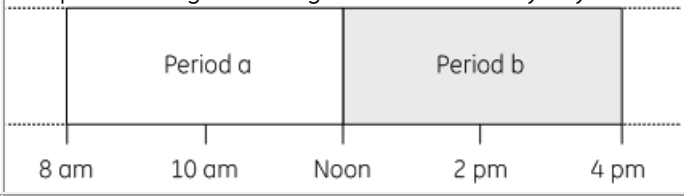
Target Point	DI 16
Target Alias	16di
Bit Position (AI to DI, ACC to DI only)	1
Value Type (ACC to AI, ACC to DI only)	RUNNING
Result Point Description	Digital Input 16
Expression Notes	ACC to DI Conversion

Calculator Averages

Calculator supports both standard and time-weighted averaging on selected analog inputs.

Fields

Table 6.180: Calculator Averages

Field	Description
Name	A system name to describe this expression within the Calculator application. Range is up to 128 alphanumeric characters.
Average Type	Select the type of averaging to perform: • *Block* averaging is a basic arithmetic average. • *Time-Weighted gives an average that considers the amount of time the point stayed at each value. Time-Weighted average is used to reduce the influence of infrequent outliers.*
Source Point	The analog input to be averaged.
Target Point	The name of the source point that is created for this expression. This name must be unique across all data types.
Target Alias	Enter a short name to reference the output point within Calculator. Must be unique across all data types. Used as point description in Available Points list. Supported characters are: any combination of up to 126 characters using "a" through "z", "0" through "9", "_" (underscore) and "-" (hyphen), followed by a suffix indicating the data type of the referenced point (ai). Spaces are not allowed. Suggested format is <a to z><1 to 9999><datatype>. For example, scada43ai. Range is up to 120 alphanumeric characters. Default is Xai, where X is incremented from 1.
Alignment	The time of day to align the period to. Periods are positioned such that a new period begins each day at the alignment time. For example, if the alignment time is set to 12:00 pm, a new period is aligned to begin at this time every day. 
Sub Block Divisor	How many segments to divide the period into. The minimum value is 1. If a value greater than 1 is provided, Calculator averages the analog input over the segment instead of the full averaging period. Calculator reports the average of the last *n* fractional averages, where *n* is the sub-block divisor.

Sliding	Select if a sliding window should be used. If not selected, Calculator reports the average at every full averaging interval. For example, if you specify an averaging interval of 1 hour and a sub-block divisor of 4, Calculator calculates the average of the analog input every 15 minutes; it reports this average every 15 minutes if a sliding window is used, or every hour if set to use a non-sliding window.
Value Exclusion	An enable/disable flag for excluding or not excluding the range of sample values for the averaging.
Value Exclusion: Min	A Floating-point minimum value for the value exclusion. Default is -0.5.
Value Exclusion: Max	A Floating-point maximum value for the value exclusion. Default is +0.5.
Result Point Description	A user-defined description of the expression.
Period	Enter the size of the averaging interval. The size of the period must divide evenly into the alignment interval, defined above. For example, in the figure above, the period is set to 4 hours. Since the alignment period is 12:00 pm, there are 6 periods in a full day. For this reason, a period size of 5 hours would not be accepted since this would divide into 2.4 periods per day and would not coincide with the *Alignment* value.
Expression Notes	Internal notes regarding the expression.

Example Field Settings

Table 6.181: Calculator Average - Example 1

Field	Example Settings
Name	Average 1
Average Type	Block
Source Point	0ai
Target Point	AI 14
Target Alias	14ai
Alignment	00:00:00
Sub Block Divisor	1
Sliding	Not Selected
Value Exclusion	Not Selected
Value Exclusion: Min	-0.5
Value Exclusion: Max	0.5
Result Point Description	Analog Input 14
Period: Days	0
Period: Hours	1
Period: Minutes	0
Period: Seconds	0
Expression Notes	Calculate and Report Block Average for every 1 hour.

Table 6.182: Calculator Average - Example 2

Field	Example Settings
Name	Average 2
Average Type	Block
Source Point	0ai
Target Point	AI 15
Target Alias	15ai
Alignment	00:00:00
Sub Block Divisor	4
Sliding	Selected
Value Exclusion	Not Selected
Value Exclusion: Min	-0.5
Value Exclusion: Max	0.5
Result Point Description	Analog Input 15
Period: Days	0
Period: Hours	1
Period: Minutes	0
Period: Seconds	0
Expression Notes	Calculate and Report Block Average for every 15 minutes.

Table 6.183: Calculator Average - Example 3

Field	Example Settings
Name	Average 3
Average Type	Time-Weighted
Source Point	0ai
Target Point	AI 16
Target Alias	16ai
Alignment	00:00:00
Sub Block Divisor	1
Sliding	Not Selected
Value Exclusion	Selected
Value Exclusion: Min	-0.9
Value Exclusion: Max	0.9
Result Point Description	Analog Input 16
Period: Days	0
Period: Hours	0
Period: Minutes	1

Period: Seconds	0
Expression Notes	Calculate and Report Time Weighted Average for every 1 minute (Excluding the samples from -0.9 to +0.9).

Output to Input Conversion

Output to input conversion expressions enable master stations to communicate with each other by converting two types of calculator-owned points:

- digital output to digital input
- analog output to digital input, accumulator, or analog input

This feature replicates the functionality of the Mailbox DTA (B009). To convert inputs belonging to external applications and devices, use calculator's type conversion feature.

Table 6.184: Output to Input Conversion

Field	Description
Name	Enter a text description of the conversion point in the Calculator map. Appears as Point Description on the Point Details page. Range is up to 128 alphanumeric characters.
Source Point Type	The type of point that is returned as the output of the expression, either Analog Output or Digital Output.
Source Point	A user-defined name that can be used for quick indexing and filtering. Maximum 66 characters, ASCII only. The default value is the next available system point reference.
Source Alias	Enter a short name to reference the conversion point in the Calculator expression. Must be unique across all data types. Used as point description in Available Points list. Supported characters are: any combination of up to 126 characters using "a" through "z", "0" through "9", "_" (underscore) and "-" (hyphen), followed by a suffix indicating the data type of the referenced point (ai or do). Spaces are not allowed. Suggested format is <a to z><1 to 9999><datatype>. For example, scada43do. Range is up to 126 alphanumeric characters. Default is the next available auto-generated alias, Xao or Xdo depending on the selected Source Point Type, where X is incremented from 1.
Source Point Description	A user-defined description of the expression.
Expression Notes	Internal notes regarding the expression.
Target Point Type	The type of point that is used as the input of the expression, *Digital Input* (if digital output is selected as the result point type) or *Accumulator*, *Analog Input*, or *Digital Input* (if analog output is selected as the result point type).
Target Point	A user-defined name that can be used for quick indexing and filtering. Maximum 66 characters, ASCII only.
Target Alias	The alias of the point that is used as the input of the expression.
Input Point Reference	The input point to be used by the expression.
Bits to Map (AO to DI only)	The number of input points to concatenate as the expression's digital input.
Result Point Description	A user-defined description of the expression.

Example Field Settings

Table 6.185: Output to Input Conversion - Example 1

Field	Example Settings
Name	Output To Input Conversion 1
Source Point Type	Digital Output
Source Point	DO 17
Source Alias	17do
Source Point Description	Digital Output 17
Expression Notes	DO 17 into DI 17 Output to Input Conversion
Target Point Type	Digital Input
Target Point	DI 17
Target Alias	17di
Result Point Description	Digital Input 17

Table 6.186: Output to Input Conversion - Example 2

Field	Example Settings
Name	Output To Input Conversion 2
Source Point Type	Analog Output
Source Point	AO 3
Source Alias	3ao
Source Point Description	Analog Output 3
Expression Notes	AO 3 into DI 18 and DI19 Output to Input Conversion
Target Point Type	Digital Input
Bits Position	0
Target Point	DI 18
Result Point Description	Digital Input 18
Target Alias	18di
Bits Position	1
Target Point	DI 19
Result Point Description	Digital Input 19
Target Alias	19di

Calculator Points

Calculator points can be used to provide input into one or more expressions. Once defined on the **Calculator Points** page, these analog output and digital output points are shown within the point picker tree on the Expression Builder.

Table 6.187: Calculator Points

Field	Description

Analog Output and Digital Output tabs	The type of output point to be made available.
Source Reference	The unique name of the source point. This field is automatically assigned and cannot be edited.
Alias	Enter a short name to reference the output point within Calculator. Must be unique across all data types. Used as point description in Available Points list. Supported characters are: any combination of up to 126 characters using "a" through "z", "0" through "9", "_" (underscore) and "-" (hyphen), followed by a suffix indicating the data type of the referenced point (ai, ao, di, do, acc, or txt). Spaces are not allowed. Suggested format is <a to z><1 to 9999><datatype>. For example, scada43di. Range is up to 126 alphanumeric characters. Default is Xai, Xdi, Xdo, Xacc, Xtxt, where X is incremented from 1.
Source Description	A user-defined description of the expression.

Calculator Application Parameters

The **Application Parameters** tab allows you to change the way that time stamps are recorded by the Calculator application.

Table 6.188: Calculator Application Parameters

Field	Description
Data Change Time Tag	Can be set to: • Use evaluation time When this option is selected, Calculator uses the time stamp of the trigger event to time stamp the resulting point from an expression (if the expression evaluation results in a changed point value). • Use trigger event When this option is selected, Calculator time stamps the resulting point with the time reported by the system clock after the expression has been evaluated. The default setting is *Use trigger event*.
Allow Controls At Startup	Can be set to: • Only Pseudo Points **When this option is selected, Calculator at startup allows the controls to the mapped pseudo points only.** • All Points **When this option is selected, Calculator at startup allows the controls to all the mapped points.** • Disabled When this option is selected, Calculator does not allow the controls at startup. The default value is Only Pseudo Points.

Basic Syntax Rules

To create a valid expression, the following syntax rules of the Calculator must be followed (in addition to the format of the specific operation types).

Order of precedence

No special precedence is enforced on any Calculator expression, except where parentheses have been used. The Calculator evaluates parts of any expression that are within parentheses first, and then evaluate the rest of the expression in a left to right manner. The Calculator allows up to 10 levels of nested parentheses. Evaluation of

nested statements occurs in an inward-to-outward manner where the more deeply nested parts of the expression are evaluated first.

For example, in the expression x = Part_1(Part_2)Part_3(Part_4(Part_5(Part_6))Part_7)Part_8((Part_9)Part_10)

the correct order of evaluation is Part_2; Part_6; Part_5; Part_4; Part_7; Part_9; Part_10; Part_1; Part_3; Part_8.

White space

You may insert any number of spaces between operators and operands; the Calculator ignores these spaces.

Input Point Suppression

The Input Point Suppression feature of the System Point Manager allows you to disable groups of analog and digital input points by ignoring their actual data and quality changes within selected applications. While points are suppressed, a predefined suppression value or the last reported value (before applying suppression) and the Point Suppressed quality flag are provided instead. This can be useful during maintenance operations to prevent spurious OFFLINE alarms and false readings while devices are powered off or disconnected.

You can add any number of input points to a point suppression group, but any input may only be included in a maximum of one group at any time. Local commands can be executed on suppressed points. However, you do not see the effects of the local command until suppression is removed.

Load Shed and Curtailment

The **Load Shed** application allows you to configure sets of feeders and load shed zones. Inputs to the MCP can be used to trigger the opening of feeders to shed load on the system. Load shedding can also be referred to as Demand Side Management or Load Management.

You can create up to 50 zones and select up to 100 feeders.

Feeders tab

Table 6.189: Feeder Tab

Field	Description
Feeder Name	A user-defined name that can be used for quick indexing and filtering. Maximum 66 characters, ASCII only.
Zone Assignment	The Load Shed zone that the feeder is assigned to. Zones can be created on the **Zones** sub-tab.
Description	A user-defined block of text that provides a detailed and localized description of the group. Maximum 128 characters.
Point Selection Area	You can select digital output system points to add to the feeder group using the system point tree. Click the checkbox to the left of a point or group name to add a point or a group of points to the group. Points included in the group are shown at the right-hand side of the point selection area. To remove a point, uncheck the appropriate box in the system point tree or highlight the point and click the **Delete** button. Click the **Delete NE** to remove any points that are not valid (that is, points that have been deleted from the system database after they were included in the group.

In the event a load shed command is issued to the zone that this feeder is a member of, all the digital outputs selected here receive a TRIP control command.

Zones tab

Table 6.190: Zones Tab

Field	Description
Zone Name	A user-defined name that can be used for quick indexing and filtering. Maximum 66 characters, ASCII only.
Zone Description	A user-defined block of text that provides a detailed and localized description of the group. Maximum 128 characters.
Load Shed Trigger Point	A point selection tree that allows you to choose the digital input point to be used as the load shed trigger point. The feeders associated with this group are tripped when this point transitions to the configured Trigger state.
Trigger Point Description	A detailed and localized description of the trigger point. This field is not editable.
Trigger State	The binary state used to trigger the load shed point selected.

Remote Logging (Rsyslog)

RemoteLogs

File : RemoteLogs.txt

Location on MCP : /mnt/datalog/Logs

Log Format : <ID>|< DATE_SHORT > <TIME_SHORT >|< TIMESTAMP>|< SOURCE_IP >|< SOURCE_NAME>|< FACILITY>|< FACILITY_NUM>|< SEVERITY>|< SEVERITY_NUM >|< TAG>|<MESSAGE >

Delimiter : Pipe

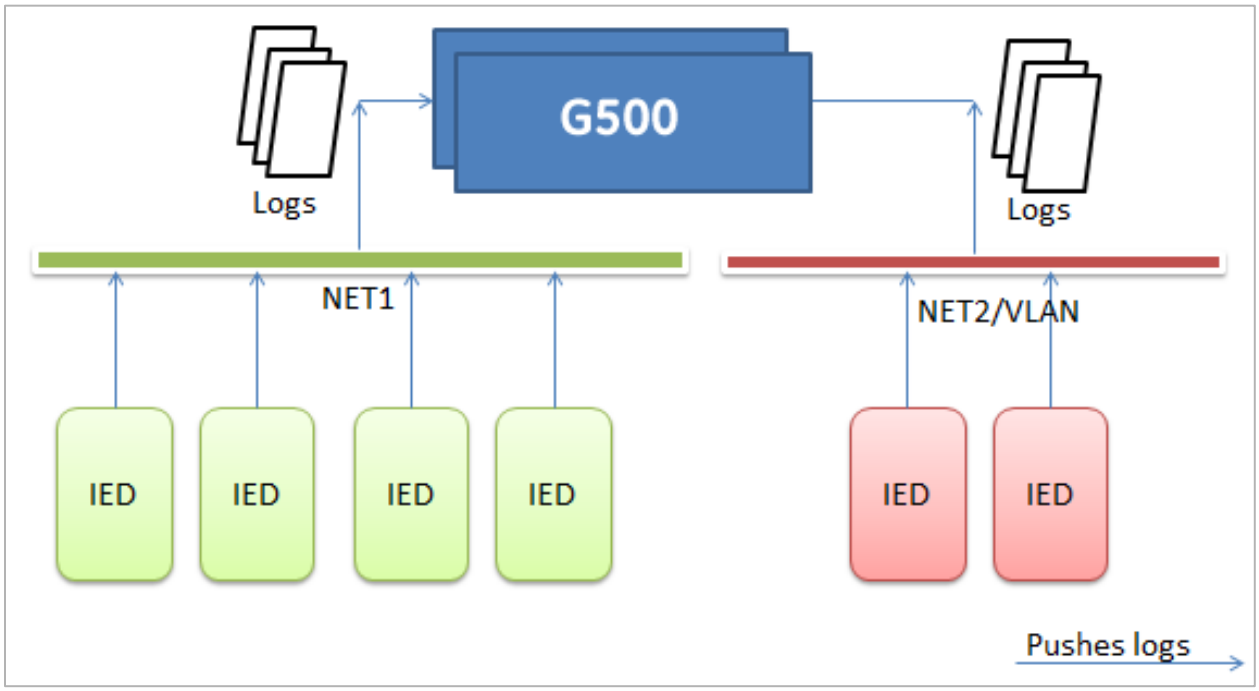
Example Log Format : -|03/03/2020 22:29|March 7 02:01:58|10.1.1.80|localhost|local6|22|info|6|HMI_Access_Mngr:| HMI_Access_Mngr;2020-5-7 2:2:7:634 UTC;1430964118;634;observer_remote;3.185.89.75;3.185.89.75;observer;Logout of HMI user session for user: observer_remote at 3.185.89.75

To configure Remote System Log through mcpcfg, refer Configure Rsyslog service and from Settings GUI, refer Configure Rsyslog Service.

Receiving Remote System Logs

The MCP can be configured to accept system logs from an IED or any substation equipment that can support the syslog remote logging feature. The MCP supports both TCP- and UDP-based remote connections to the IEDs on the standard port numbers. All the logs received are saved in a default file under a set path. The current version is configured to conform to RFC5424 standard.

Figure 6.3: System Log Retrieval



Configure UDP- and TCP-based logging

Both the UDP- and TCP-based connection ports can be simultaneously opened to listen for the incoming remote syslog messages being pushed from the IEDs or another substation equipment. A dedicated port is opened in listen mode and is classified operate under internal interface (see Firewall settings for more details).

Configure Hosts-Subnets Filters

By default, the MCP saves all incoming logs being pushed from any of the IEDs connected to the network and configured with the MCP IP Address and syslog port).

The MCP also allows you to configure the:

- **Subnets-based binding filter**: By selecting a subnet from the displayed list or by specifying a subnet from the Custom Filters options, the MCP starts logging messages from IEDs whose IP Addresses fall under the subnet's range)
- **Host-based binding filter:** By Specifying a Host's IP Address, the MCP starts logging messages being pushed from the specified host.

Configuring Subnet address and Host IP Address is beneficial when:

- An IED or substation equipment's IP Address is not under any of the subnets available in the MCP.
- The MCP is in redundant mode and the Standby's Ethernet Interface (Alias IP/Gateways etc...) are configured to be in different subnets from that of the Active's Ethernet Interface.

For details on enabling and editing Rsyslog services, refer to the online help topic: Configure Secure Access.

Configure Datalogger

Configure the Data Logger

The Data Logger application allows you to graphically monitor and record data from devices connected to the MCP. You can also save and review historical reports created by the application.

Choose between three different report types:

- Continuous Reports
- Periodic Reports
- Out of Range Reports

Report Types

Continuous Reports

Continuous reports record all events on the selected points.

» To select a point to log:

1. Expand the point tree by clicking the +.
2. Click the checkbox next to the point name. If a folder is selected, all points that fall under that group are added to the report.
3. Enter the deadband setting by double clicking the **Deadband** cell and entering the desired value.

Table 6.191: Continuous Reports

Field	Description
Name	User-defined name to refer to the report.
Log Full Action	When the maximum number of records is reached, define how incoming records are to be handled. *Overwrite Oldest Data* replaces the oldest entries in the log with the new incoming records; *Reject Newest Data* ceases recording incoming records until space is made available (through the Manage Reports window of the Data Logger).
Max Number of Records	Enter the maximum number of records that should be recorded within this report. Note that the number of records is divided among the selected points. Refer to Storage Allocation for information on configuring MCP storage space available for reports.
Enable Trigger Point	When selected, the Data Logger monitors a defined digital input point for status changes. When a status change occurs, log recording begins; it ends when the status changes back.
Trigger Point	Select a digital input to trigger recording of the report.
Go State	If *Enable Trigger Point* is selected, select the state that the point must enter to begin recording.

Periodic Reports

Periodic reports record current value, minimum value, or maximum value for the selected points within a defined interval:

» To select a point to log:

1. Expand the point tree by clicking the +.

2. Click the checkbox next to the point name. If a folder is selected, all points that fall under that group are added to the report.
3. Enter the deadband setting by double clicking the **Deadband** cell and entering the desired value.

Table 6.192: Periodic Reports

Field	Description
Name	User-defined name to refer to the report.
Log Full Action	When the maximum number of records is reached, define how incoming records are handled. *Overwrite Oldest Data* replaces the oldest entries in the log with the new incoming records; *Reject Newest Data* ceases recording incoming records until space is made available (through the Manage Reports window of the Data Logger).
Max Number of Records	Enter the maximum number of records that should be recorded within this report. Note that the number of records is divided among the selected points. Refer to Storage Allocation for information on configuring MCP storage space available for reports.
Periodic Value	Select if you would like to record the current, minimum, or maximum values for selected points at each interval.
Log Interval	Select the type of interval. This value is combined with the Alignment value below to define the interval length.
Interval	The length of interval. For example, if the selected log interval is *hours* and the interval is *2*, the length of the interval is 2 hours.
Alignment	The time of day to align the period to. Intervals are positioned to meet at the alignment value. For example, if an *Hours* interval is selected and the alignment is set to *xx:15*, a new interval begins at 15 minutes past each hour. If a *Days* interval is selected and the alignment is set to *8*, a new interval begins at 8:00 am each day.
Enable Trigger Point	When selected, the Data Logger monitors a defined digital input point for status changes. When a status change occurs, log recording begins; it ends when the status changes back.
Trigger Point	Select a digital input to trigger recording of the report.
Go State	If *Enable Trigger Point* is selected, select the state that the point must enter to begin recording.

Out of Range Reports

Out of Range reports record events on the selected points that fall outside of a configured range.

» To select a point to log:

1. Expand the point tree by clicking the +.
2. Click the checkbox next to the point name. If a folder is selected, all points that fall under that group are added to the report.
3. Enter the deadband setting by double clicking the **Deadband** cell and entering the desired value.
4. Enter the validation time. A value of 0 disables this feature. See below for an explanation of this setting.
5. Enter the lower and upper limits of the configured range.

Table 6.193: Out of Range Reports

Field	Description
Name	User-defined name to refer to the report.

Log Full Action	When the maximum number of records is reached, define how incoming records are to be handled. *Overwrite Oldest Data* replaces the oldest entries in the log with the new incoming records; *Reject Newest Data* ceases recording incoming records until space is made available (through the Manage Reports window of the Data Logger).
Max Number of Records	Enter the maximum number of records that should be recorded within this report. Note that the number of records is divided among the selected points. Refer to Storage Allocation for information on configuring MCP storage space available for reports.
Enable Trigger Point	When selected, the Data Logger monitors a defined digital input point for status changes. When a status change occurs, log recording begins; it =ends when the status changes back.
Trigger Point	Select a digital input to trigger recording of the report.
Go State	If *Enable Trigger Point* is selected, select the state that the point must enter to begin recording.

Validation Time

Out of range logging allows for an optional validation period. This is used to account for instances where a reading may be incorrect for one scan before the device corrects itself. If this feature is enabled, the following occurs:

1. If a new event is in the *same* reporting range as the previously reported value, the new event is accepted and recorded.
2. If a new event is in a *different* reporting range than the previously reported value, the validation timer is started:
   a) If the validation timer expires with no new events being reported, the event being validated is accepted and recorded
   b) If a new event is reported before the timer expires, and it falls within the same range as the event being validated, both are accepted and recorded, and the validation timer is reset
   c) If a new event is reported before the timer expires, and it falls outside the range of the event being validated, the event being validated is discarded, the validation timer is reset, and the new event starts at step 2.

Storage Allocation

Global Memory allocated to Data Logger

The percentage of memory allocated to datalogger is present under Storage section of Systemwide Tab. By default, it is equally divided between 3 applications i.e. ARRM, Data Logger and Analog reports.

» To change the Data Logger storage allocation:

1. On the storage section under Systemwide the storage space allocated to datalogger can be changed
2. Move the slider left or right to change the allocation. You cannot decrease the amount of storage space to less than that currently allocated to records.
3. Save the selected allocation in system wide storage and these changes will be reflected in Storage section under datalogger Tab

Memory allocated to Data Logger

Tip: Each record uses 0.06 KB of memory space.

Save Report

The **Save Report** window allows you to export a .csv (comma separated values) file from the Data Logger. The CSV file contains point attributes and values for the entire timeframe shown in the Summary Area.

» To save a report:

1. Click Save Report.
2. On the CSV Report Options window, enable or disable saving vertex data in the report. Click OK.
3. Browse to the location you want to store the report file.
4. Enter a file name ending in .csv and click Save.

NOTES:

- Historic records loaded from other reports are not saved within the new report file.
- If no records exist within the selected timeframe, the exported file will contain one entry that shows the first available value before the selected start time.

Vertex Data

When saving reports, Data Logger gives you the option of including or excluding vertex data from the file. Vertex data is the collection of x and y coordinates that comprise a plotted trend. When a report is saved without vertex data, only the properties of the report (configured trends, scales, pen colors, axis settings, etc.) are saved, not the data within the report itself.

Load Report

The **Load Report** window allows you to import a .csv (comma separated values) file previously exported from the Data Logger.

» To load a report:

1. Click Load Report.
2. If vertex data has been saved to the report:
   a) On the CSV Report Options window, enable or disable loading of vertex data from the report.
   b) Click OK.
3. Browse to the report file you want to display and click Open.

Vertex Data

When loading reports, Data Logger gives you the option of importing or ignoring vertex data within the file. Vertex data is the collection of x and y coordinates that comprise a plotted trend. When a report is loaded containing vertex data, the trends appear on the chart area as they appeared when the file was saved.

NOTE: When a historic report is loaded, **No End Date** is automatically unchecked, and auto-trending is disabled.

When a report is loaded without vertex data, only the properties of the trend (scales, pen color, axis settings, etc.) are restored that is, not the data within the trend itself. Data Logger attempts to reestablish a connection to the live trends as defined in the report.

Manage Reports

The **Manage Reports** window allows you to view the amount of disk space consumed by report data as well as pause and restart logging.

Table 6.194: Manage Reports

Field	Description
#	A non-editable row number to identify the trend.
Report ID	The ID number of the report. Non-editable field that can be configured in the Data Logger tab of the Configuration Tool.
Name	The system name of the report. Non-editable field that can be configured in the Data Logger tab of the Configuration Tool.
Historic?	If a report is no longer configured within Data Logger but is loaded from a saved file, the checkbox is selected to indicate this.
Active?	Indicates if logging is currently enabled for the report type. Use the *Activate* and *Deactivate* buttons to change this setting.
Activate	Sends a command to the MCP to resume logging for this report type. The *Active?* field indicates logging status.
Deactivate	Sends a command to the MCP to pause logging for this report type. The *Active?* field indicates logging status.
Capacity (B)	The amount of disk space allocated to the report type, in bytes. Non-editable field that can be configured in the Data Logger tab of the Configuration Tool.
Size (B)	The amount of disk space currently consumed by the report, in bytes, including cache data.
Size (%)	A percent-representation of the amount of capacity currently being consumed by the report type.
Empty	Sends a command to the MCP to delete all records for this report type. Trend data already cached and displayed within Data Logger is not deleted.

Select Points

The **Select Points for Trending** window lists the points that can be selected for graphing within the Data Logger.

» To select points for graphing:

1. Select the **Start Date** for the graph timeframe. If **Earliest Record** is selected, the timeframe of the graph resizes to show the first recorded point.
2. Select the **End Date** for the graph timeframe. If **No End Date** is selected, Data Logger continually polls the MCP for new data values on a regular basis and extends the graph as new data is received. **No End Date** must be selected to enable Auto-Trend.
3. Select up to 10 points to graph by clicking the ☐ icon. When a point is selected, it is marked by a ☑ icon. The ☐ icon indicates some child points of the item have been selected.
4. Click **OK**.
   Result: Data Logger creates a graph of the selected points.

Data Logger supports the following record types:

- **Periodic** – Records one or more of the following for the selected analog input:
  - Current value
  - Minimum value
  - Maximum value
- **Continuous** – Records all events on the selected analog input
- **Ranged** – Records events on the selected analog input that fall outside of a configured range

Change Scaling

The **Change Scales and Axes** window allows you to change the way graphs are shown within the Data Logger.

Table 6.195: Change Scaling

Field	Description
#	A non-editable row number to identify the trend.
Color	The color of line used when graphing the trend.
Report	The system name of the report the trend belongs to. Non-editable field that can be configured in the Data Logger tab of the Configuration Tool.
Point	The system name of the point. Non-editable field that can be configured in the Data Logger tab of the Configuration Tool.
Axis Label	The user-configurable name shown when referencing the trend.
Unit	A user-configurable label shown to indicate the type of data being graphed. This field is for display only and does not affect the graphing of the point.
Auto-Range	When enabled, the *Min* and *Max* fields are disabled, and the Y-axis on the Summary Area automatically scales vertically to contain the trend's data.
Min	The minimum Y-axis limit to be displayed. Enabling Auto-Range will override this setting.
Max	The maximum Y-axis limit to be displayed. Enabling Auto-Range will override this setting.
Axis	Display or hide the Y-axis scale for the trend. This affects the scales in both the Summary Area and the Viewing Area.
Historic	Shows whether the trend is live or has been loaded from a saved report.
Axis Sets	• Individual: One axis per point in each report. • Per Point Name: One axis per point. Each axis is shared between reports. • Single: One shared axis for all points. This axis is shared between reports.

HAMA - Hardware Asset Management Application

This chapter contains the following sections and sub-sections:

Hardware Asset Management Application (HAMA)

Analog Inputs

Digital Inputs

Accumulator Points

Text Points

Hardware Asset Management Application (HAMA)

Hardware Asset Management Application (HAMA) is a Data Translation application in MCP. HAMA DTA gathers the live or dynamic data (e.g. network modes, serial port settings, temperatures, real time utilizations of various resources, etc.) and presents to RTDB by means of Analog/Digital/Accumulator/Text Points but not in the above report.

The below are list of RTDB points supported by HAMA DTA application. All these points present to RTDB as field points (i.e. Point IDs greater than 1).

Analog Inputs

Table 6.196: Analog Inputs

Point ID	Point Reference	Point Description	Values
300	Last Reset Cause	Last Reset Cause	**Not supported in G100** Gets the Last Reset Cause of the Main Board. **Options (INT from 1 to 9):** • Reset Power Other, 1 • Reset Power Main, 2 • Reset Temp Module, 3 • Reset Temp Carrier, 4 • Reset WDT Module, 5 • Reset WDT Carrier, 6 • Reset System, 7 • Reset Carrier, 8 • Reset Power Button, 9 **Note:** value 0 is present only while initializing.
310	Chassis Intrusion Status	Chassis Intrusion Status	**Not supported in G100** Gets the Chassis Intrusion Status of the Board. **Options:** • Intrusion Safe (1), • Intrusion Unsafe (2), or • Intrusion Undefined (-1) **Note:** value 0 is present only while initializing or point is invalid.
400	Front Display State	Front Display State	**Not supported in G100** State of the Display in BIT ENCODED values: **Options:** • Bit 0 = Display State OFF (bit = 0) / ON (bit = 1) - this is the actual state, is not driven by the saver setting • Bit 1 = Display State OverTemp Warn (bit =1) • Bit 2 = Display State OverTemp Alarm (bit =1)
501	Power Supply 1 (top) Status	Power Supply 1 (top) Status	**Not supported in G100** Bit encoded value: • Bit 0 = INSERTED (1) / NOT PRESENT (0) • Bit 1 = ENERGIZED (1) / NOT ENERGIZED (0) • Bit 2 = OK (1) / Not OK (0) - this sets also the GOOD DI • Bit 3 = LV (1) / HV (0)
502	Power Supply 2 (bottom) Status	Power Supply 2 (bottom) Status	**Not supported in G100** Bit encoded value:

			• Bit 0 = INSERTED (1) / NOT PRESENT (0) • Bit 1 = ENERGIZED (1) / NOT ENERGIZED (0) • Bit 2 = OK (1) / Not OK (0) - this sets also the GOOD DI • Bit 3 = LV (1) / HV (0)
601	Temperature Power Supply 1 (top)	Temperature Power Supply 1 (top) in Deg C	**Not supported in G100** Deg C
602	Temperature Power Supply 2 (bottom)	Temperature Power Supply 2 (bottom) in Deg C	**Not supported in G100** Deg C
610	Temperature CPU	Temperature CPU in Deg C	**Not supported in G100** Deg C
611	Temperature Memory (RAM)	Temperature Memory (RAM) in Deg C	**Not supported in G100** Deg C
615	Temperature FPGA LAN	Temperature FPGA LAN in Deg C	**Not supported in G100** Deg C
621	Temperature storage SSD	Temperature storage (SSD) in Deg C	**Not supported in G100** Deg C
624	Slot 1 (UART exten card) Temperature	Slot1(UART exten card) Temperature in Deg C	**Not supported in G100** Deg C
625	Slot 2(UART exten card) Temperature	Slot2(UART exten card) Temperature in Deg C	**Not supported in G100** Deg C
626	Temperature Display	Temperature Display in Deg C	**Not supported in G100** Deg C
1100	ETH1-2 Redundancy Mode	ETH1-ETH2 Redundancy Mode	**Not supported in G100** 0 = not redundant 1 = redundant same MAC/Same IP 2 = PRP 3 = HSR
1110	ETH1-2 PRP/HSR lreInterfaceStatsIndex	Unique value for each LRE	**Not supported in G100** lreInterfaceStatsIndex Unsigned32, This value should always be 1
1111	ETH1-2 PRP/HSR lreCntNodes	number of nodes in the Nodes Table	**Not supported in G100** lreCntNodes Integer32,
1112	ETH1-2 PRP/HSR lreCntProxyNodes	number of nodes in the Proxy Node Table. Only applicable to RedBox.	**Not supported in G100** lreCntProxyNodes Integer32,
1300	ETH3-4 Redundancy Mode	ETH3-ETH4 Redundancy Mode	**Not supported in G100** 0 = not redundant 1 = redundant same MAC/Same IP

			2 = PRP 3 = HSR
1310	ETH3-4 PRP/HSR lreInterfaceStatsIndex	Unique value for each LRE	**Not supported in G100** lreInterfaceStatsIndex Unsigned32, This value should always be 2
1311	ETH3-4 PRP/HSR lreCntNodes	number of nodes in the Nodes Table	**Not supported in G100** lreCntNodes Integer32,
1312	ETH3-4 PRP/HSR lreCntProxyNodes	number of nodes in the Proxy Node Table. Only applicable to RedBox.	**Not supported in G100** lreCntProxyNodes Integer32,
1500	ETH5-6 Redundancy Mode	ETH5-ETH6 Redundancy Mode	**Not supported in G100** 0 = not redundant 1 = redundant same MAC/Same IP 2 = PRP
1510	ETH5-6 PRP/HSR lreInterfaceStatsIndex	Unique value for each LRE	**Not supported in G100** lreInterfaceStatsIndex Unsigned32, This value should always be 3
1511	ETH5-6 PRP/HSR lreCntNodes	number of nodes in the Nodes Table	**Not supported in G100** lreCntNodes Integer32,
1512	ETH5-6 PRP/HSR lreCntProxyNodes	number of nodes in the Proxy Node Table. Only applicable to RedBox.	**Not supported in G100** lreCntProxyNodes Integer32,
1521	PCIe 1 Module type	Integer	**Not supported in G100** Integer: 0 = Not present -1 = Unknown 1 = Serial 4 ports
1522	PCIe 2 Module type	Integer	**Not supported in G100** Integer: 0 = Not present -1 = Unknown 1 = Serial 4 ports
1523	PCIe 3 Module type	Integer	**Not supported in G100** Integer: 0 = Not present -1 = Unknown 1 = Serial 4 ports 2 = Serial 8 ports (Not supported in MCP) 3 = D.20 HDLC

2010	COM1 Mode	COM1 Mode (RS232,485 2w,485 4w,Term_In,V_Out_OL)	**Not supported in G100** Bit encoded value, an overall value of 0 means not initialized or error: • Bit 0 ON= RS232 • Bit 1 ON = RS422 • Bit 2 ON = RS485 2W • Bit 3 ON = RS485 4W • Bit 4 ON = Termination IN
2020	COM2 Mode	COM2 Mode (RS232,485 2w,485 4w,Term_In,V_Out_OL)	**Not supported in G100** Bit encoded value, an overall value of 0 means not initialized or error: • Bit 0 ON= RS232 • Bit 1 ON = RS422 • Bit 2 ON = RS485 2W • Bit 3 ON = RS485 4W • Bit 4 ON = Termination IN
2030	COM3 Mode	COM3 Mode (RS232,485 2w,485 4w,Term_In,V_Out_OL)	**Not supported in G100** Bit encoded value, an overall value of 0 means not initialized or error: • Bit 0 ON= RS232 • Bit 1 ON = RS422 • Bit 2 ON = RS485 2W • Bit 3 ON = RS485 4W • Bit 4 ON = Termination IN
2040	COM4 Mode	COM4 Mode (RS232,485 2w,485 4w,Term_In,V_Out_OL)	**Not supported in G100** Bit encoded value, an overall value of 0 means not initialized or error: • Bit 0 ON= RS232 • Bit 1 ON = RS422 • Bit 2 ON = RS485 2W • Bit 3 ON = RS485 4W • Bit 4 ON = Termination IN
2050	COM5 Mode	COM51 Mode (RS232,485 2w,485 4w,Term_In,V_Out_OL)	**Not supported in G100** Bit encoded value, an overall value of 0 means not initialized or error: • Bit 0 ON= RS232 • Bit 1 ON = RS422 • Bit 2 ON = RS485 2W • Bit 3 ON = RS485 4W • Bit 4 ON = Termination IN
2060	COM6 Mode	COM6 Mode (RS232,485 2w,485 4w,Term_In,V_Out_OL)	**Not supported in G100** Bit encoded value, an overall value of 0 means not initialized or error: • Bit 0 ON= RS232

			• Bit 1 ON = RS422 • Bit 2 ON = RS485 2W • Bit 3 ON = RS485 4W • Bit 4 ON = Termination IN
2070	COM7 Mode	COM7 Mode (RS232,485 2w,485 4w,Term_In,V_Out_OL)	**Not supported in G100** Bit encoded value, an overall value of 0 means not initialized or error: • Bit 0 ON= RS232 • Bit 1 ON = RS422 • Bit 2 ON = RS485 2W • Bit 3 ON = RS485 4W • Bit 4 ON = Termination IN
2080	COM8 Mode	COM8 Mode (RS232,485 2w,485 4w,Term_In,V_Out_OL)	**Not supported in G100** Bit encoded value, an overall value of 0 means not initialized or error: • Bit 0 ON= RS232 • Bit 1 ON = RS422 • Bit 2 ON = RS485 2W • Bit 3 ON = RS485 4W • Bit 4 ON = Termination IN
2101	PCIe A – COM Mode 1	COM8 Mode (RS232,485 2w,485 4w,Term_In,V_Out_OL)	**Not supported in G100** Same as COM1
2102	PCIe A – COM Mode 2	COM8 Mode (RS232,485 2w,485 4w,Term_In,V_Out_OL)	**Not supported in G100** Same as COM1
2103	PCIe A – COM Mode 3	COM8 Mode (RS232,485 2w,485 4w,Term_In,V_Out_OL)	**Not supported in G100** Same as COM1
2104	PCIe A – COM Mode 4	COM8 Mode (RS232,485 2w,485 4w,Term_In,V_Out_OL)	**Not supported in G100** Same as COM1
2105	PCIe A – COM Mode 5	COM mode is always RS232, indicate with 0 if not installed	**Not supported in G100** Forced to Bit 0 ON (RS232) when present
2106	PCIe A – COM Mode 6	COM mode is always RS232, indicate with 0 if not installed	**Not supported in G100** Forced to Bit 0 ON (RS232) when present
2107	PCIe A – COM Mode 7	COM mode is always RS232, indicate with 0 if not installed	**Not supported in G100** Forced to Bit 0 ON (RS232) when present

2108	PCIe A – COM Mode 8	COM mode is always RS232, indicate with 0 if not installed	**Not supported in G100** Forced to Bit 0 ON (RS232) when present
2111	PCIe B – COM Mode 1	COM8 Mode (RS232,485 2w,485 4w,Term_In,V_Out_OL)	**Not supported in G100** Same as COM1
2112	PCIe B – COM Mode 2	COM8 Mode (RS232,485 2w,485 4w,Term_In,V_Out_OL)	**Not supported in G100** Same as COM1
2113	PCIe B – COM Mode 3	COM8 Mode (RS232,485 2w,485 4w,Term_In,V_Out_OL)	**Not supported in G100** Same as COM1
2114	PCIe B – COM Mode 4	COM8 Mode (RS232,485 2w,485 4w,Term_In,V_Out_OL)	**Not supported in G100** Same as COM1
2115	PCIe B – COM Mode 5	COM mode is always RS232, indicate with 0 if not installed	**Not supported in G100** Forced to Bit 0 ON (RS232) when present
2116	PCIe B – COM Mode 6	COM mode is always RS232, indicate with 0 if not installed	**Not supported in G100** Forced to Bit 0 ON (RS232) when present
2117	PCIe B – COM Mode 7	COM mode is always RS232, indicate with 0 if not installed	**Not supported in G100** Forced to Bit 0 ON (RS232) when present
2118	PCIe B – COM Mode 8	COM mode is always RS232, indicate with 0 if not installed	**Not supported in G100** Forced to Bit 0 ON (RS232) when present
2121	PCIe C – COM Mode 1	COM8 Mode (RS232,485 2w,485 4w,Term_In,V_Out_OL)	**Not supported in G100** Same as COM1
2122	PCIe C – COM Mode 2	COM8 Mode (RS232,485 2w,485 4w,Term_In,V_Out_OL)	**Not supported in G100** Same as COM1
2123	PCIe C – COM Mode 3	COM8 Mode (RS232,485 2w,485 4w,Term_In,V_Out_OL)	**Not supported in G100** Same as COM1
2124	PCIe C – COM Mode 4	COM8 Mode (RS232,485 2w,485 4w,Term_In,V_Out_OL)	**Not supported in G100** Same as COM1
2125	PCIe C – COM Mode 5	COM mode is always RS232, indicate with 0 if not installed	**Not supported in G100** Forced to Bit 0 ON (RS232) when present
2126	PCIe C – COM Mode 6	COM mode is always RS232, indicate with 0 if not installed	**Not supported in G100** Forced to Bit 0 ON (RS232) when present

2127	PCIe C – COM Mode 7	COM mode is always RS232, indicate with 0 if not installed	**Not supported in G100** Forced to Bit 0 ON (RS232) when present
2128	PCIe C – COM Mode 8	COM mode is always RS232, indicate with 0 if not installed	**Not supported in G100** Forced to Bit 0 ON (RS232) when present
3000	Time Sync Input Source	Time Sync Input Source (None-SCADA, PTP, IRIG-B, NTP, SNTP)	Indicates at runtime the Time Sync Input for the MCP in real time. Values: • Local/Not synch'ed/SCADA, • PTP • IRIG-B • NTP SCADA time synch is set in SSM points because HAMA cannot access this type of information.
3011	NET1-2 PTP Port State	NET1-2 PTP Port State	**Not supported in G100** port state: • PORT_MASTER • PORT_SLAVE • PORT_PASSIVE • PORT_LISTENING • PORT_PRE_MASTER • PORT_UNCALIBRATED • PORT_FAULTY • PORT_DISABLED • PORT_INITIALIZING
3012	NET3-4 PTP Port State	NET3-4 PTP Port State	**Not supported in G100** port state: • PORT_MASTER • PORT_SLAVE • PORT_PASSIVE • PORT_LISTENING • PORT_PRE_MASTER • PORT_UNCALIBRATED • PORT_FAULTY • PORT_DISABLED • PORT_INITIALIZING
3013	NET5-6 PTP Port State	NET5-6 PTP Port State	**Not supported in G100** port state: • PORT_MASTER • PORT_SLAVE • PORT_PASSIVE • PORT_LISTENING

			• PORT_PRE_MASTER • PORT_UNCALIBRATED • PORT_FAULTY • PORT_DISABLED • PORT_INITIALIZING
3021	PTP Clock Class	PTP Clock Class	**Not supported in G100** Indicates the grandmaster's clock class if synced. Otherwise, shows its default clock class (187).
3100	IRIG-B IN Type	IRIG-B IN Type (B002, B006)	Indicates the configured IRIG-B input signal type: • B002 • B006 • Absent
3101	IRIG-B IN Time Zone Offset to UTC	IRIG-B IN Time Zone Offset to UTC	Not currently supported.
3150	NTP Time Offset	NTP Time Offset	NTP Time Offset
3151	NTP IN Server Selected	NTP IN Server Selected	Bit encoded AI to indicate communication with all configured NTP time sources. • Bit 0 = ON for NTP Source 1 • Bit 1 = ON for NTP Source 2
3152	NTP IN Servers Quality	NTP IN Servers Quality	Bit encoded AI to indicate quality with all configured NTP time sources. • Bit 0 = ON for NTP Source 1 good quality • Bit 1 = OK for NTP Source 2 good quality, etc

Digital Inputs

Table 6.197: Digital Inputs

Point ID	Point Reference	Point Description	Values
311	Chassis Intrusion State	Chassis Intrusion State	**Not supported in G100** Gets the Chassis Intrusion State of the Board 1 - Intrusion Unsafe and 0 – Intrusion Safe
333	Needs System Reboot	Needs System Reboot	**Not supported in G100** Shows the MCP needs cold reboot 1 - for needs for cold reboot 0 - for otherwise
420	Front Display Always ON	Front Display Always ON	**Not supported in G100**

			1 - Front Display light saver is disabled; display is always on
531	Power Supply 1 (top) Good	Power Supply 1 (top) Good	**Not supported in G100** Alarm = 0, for e.g. over temp, bad output (if available in HW) 1 - if all is OK
532	Power Supply 2 (bottom) Good	Power Supply 2 (bottom) Good	**Not supported in G100** Alarm = 0, for e.g. over temp, bad output (if available in HW) 1 - if all is OK
1524	PCIe 1 Card Status	Available if D.20 PCIe Card is present or else it will be Offline/Greyed Out	**Not supported in G100** "0 - if D.20 PCIe Card is Not Healthy (the absence of card is indicated by quality and a value set to 0) 1 - if D.20 PCIe Card is available and healthy (as a card)"
1525	PCIe 2 Card Status	Available if D.20 PCIe Card is present or else it will be Offline/Greyed Out	**Not supported in G100** "0 - if D.20 PCIe Card is Not Healthy (the absence of card is indicated by quality and a value set to 0) 1 - if D.20 PCIe Card is available and healthy (as a card)"
1526	PCIe 3 Card Status	Available if D.20 PCIe Card is present or else it will be Offline/Greyed Out	**Not supported in G100** "0 - if D.20 PCIe Card is Not Healthy (the absence of card is indicated by quality and a value set to 0) 1 - if D.20 PCIe Card is available and healthy (as a card)"
1600	ETH_FRONT Link Good	NET0/ETH_FRONT Link Good	**Not supported in G100** 1 - Link is UP / '0' Link is down
1610	ETH1 Link Good	NET1/ETH1 Link Good	**Not supported in G100** 1 - Link is UP / '0' Link is down
1611	ETH1 SFP IN	NET1/ETH1 SFP IN	**Not supported in G100** 1 - SFP is IN (present) / '0' SFP is OUT (not present)
1620	ETH2 Link Good	NET2/ETH2 Link Good	**Not supported in G100** 1 - Link is UP / '0' Link is down
1621	ETH2 SFP IN	NET2/ETH2 SFP IN	**Not supported in G100** 1 - SFP is IN (present) / '0' SFP is OUT (not present)
1630	ETH3 Link Good	NET3/ETH3 Link Good	**Not supported in G100** 1 - Link is UP / '0' Link is down
1631	ETH3 SFP IN	NET3/ETH3 SFP IN	**Not supported in G100** 1 - SFP is IN (present) / '0' SFP is OUT (not present)
1640	ETH4 Link Good	NET4/ETH4 Link Good	**Not supported in G100**

			Not supported in G100 1 - Link is UP / '0' Link is down
1641	ETH4 SFP IN	NET4/ETH4 SFP IN	**Not supported in G100** 1 - SFP is IN (present) / '0' SFP is OUT (not present)
1650	ETH5 Link Good	NET5/ETH5 Link Good	**Not supported in G100** 1 - Link is UP / '0' Link is down
1651	ETH5 SFP IN	NET5/ETH5 SFP IN	**Not supported in G100** 1 - SFP is IN (present) / '0' SFP is OUT (not present)
1660	ETH6 Link Good	NET6/ETH6 Link Good	**Not supported in G100** 1 - Link is UP / '0' Link is down
1661	ETH6 SFP IN	NET6/ETH6 SFP IN	**Not supported in G100** 1 - SFP is IN (present) / '0' SFP is OUT (not present)
3200	PTP/IRIG-B Clock Synchronized	PTP/IRIG-B Clock Synchronized	**Not supported in G100** Indicates 1 if the MCP is in time sync with the configured PTP or IRIG-B Input. Indicates 0 if the MCP has never synchronized with a PTP or IRIG-B input source. Note: if the configured time source signal exists but its quality has never been good, this DI will be 0.
3210	PTP IN Enabled	PTP IN Enabled	**Not supported in G100** Set to – 1, if PTP Client enabled in the configuration. Default is 0.
3211	PTP IN Signal	PTP IN Signal	**Not supported in G100** Indicates 1 if PTP time sync communication is established. Indicates 0 if PTP time sync communication is not established.
3212	PTP IN Quality	PTP IN Quality	**Not supported in G100** Indicates 1 if PTP time sync communication is established and the grandmaster's clock class is 6 or 7, and its UtcOffsetValid is true. Otherwise, the value will be 0.
3300	IRIG-B Enabled	IRIG-B Enabled	Set to 1 if IRIG-B input is enabled in the configuration. Default is 0.
3301	IRIG-B IN Signal Fail	IRIG-B IN Signal Fail	Set to 0 when IRIG-B signal is present (regardless of quality). Set to 1 if IRIG-B Input Watchdog is expired, meaning the input signal is not present. Inverted compared to other time sources, need to stay inverted for MCP legacy compatibility

3302	IRIG-B IN Quality	IRIG-B IN Quality	Set to 1 if the IRIG-B Input has good quality (this is not about the signal being present). 0 otherwise.
3350	NTP IN Enabled	NTP IN Enabled	Set to 1 if NTP time sync client is enabled in the configuration. Default is 0.
3351	NTP IN Signal	NTP IN Signal	Indicates 1 if NTP time sync communication is established. Indicates 0 if NTP time sync communication is not established.
3352	NTP IN Quality	NTP IN Quality	Set to 1 if the NTP Input signal has good quality (this is not about the signal being present). 0 otherwise.
3360	NTP OUT Enabled	NTP OUT Enabled	Set to 1 if NTP time sync server is enabled in the configuration. Default is 0.

Accumulator Points

Table 6.198: Accumulator Points

Point ID	Point Reference	Description
1701	ETH1-2 PRP/HSR lreCntTxA	**Not supported in G100** PRP/HSR frames sent over port A
1702	ETH1-2 PRP/HSR lreCntTxB	**Not supported in G100** PRP/HSR frames sent over port B
1703	ETH1-2 PRP/HSR lreCntTxC	**Not supported in G100** number of frames sent towards the application interface
1704	ETH1-2 PRP/HSR lreCntErrWrongLanA	**Not supported in G100** number of frames with the wrong LAN identifier received on port A
1705	ETH1-2 PRP/HSR lreCntErrWrongLanB	**Not supported in G100** number of frames with the wrong LAN identifier received on port B
1706	ETH1-2 PRP/HSR lreCntErrWrongLanC	**Not supported in G100** number of frames with the wrong LAN identifier received on the RedBox interlink
1707	ETH1-2 PRP/HSR lreCntRxA	**Not supported in G100** number of PRP/HSR frames received on port A
1708	ETH1-2 PRP/HSR lreCntRxB	**Not supported in G100** number of PRP/HSR frames received on port B
1709	ETH1-2 PRP/HSR lreCntRxC	**Not supported in G100** number of frames received from the application interface of a DANP or DANH or the number of number of frames received on the interlink of a RedBox

1710	ETH1-2 PRP/HSR lreCntErrorsA	**Not supported in G100** number of frames with errors received on port A
1711	ETH1-2 PRP/HSR lreCntErrorsB	**Not supported in G100** number of frames with errors received on port B
1712	ETH1-2 PRP/HSR lreCntErrorsC	**Not supported in G100** number of frames with errors received on the application interface of a DANP or DANH or on the interlink of a RedBox
1716	ETH1-2 PRP/HSR lreCntDuplicateA	**Not supported in G100** number of entries in the duplicate detection mechanism on port A for which one single duplicate was received
1717	ETH1-2 PRP/HSR lreCntDuplicateB	**Not supported in G100** number of entries in the duplicate detection mechanism on port B for which one single duplicate was received
1718	ETH1-2 PRP/HSR lreCntDuplicateC	**Not supported in G100** number of entries in the duplicate detection mechanism on the application interface of the DAN or the interlink of the RedBox for which one single duplicate was received
1731	ETH3-4 PRP/HSR lreCntTxA	**Not supported in G100** PRP/HSR frames sent over port A
1732	ETH3-4 PRP/HSR lreCntTxB	**Not supported in G100** PRP/HSR frames sent over port B
1733	ETH3-4 PRP/HSR lreCntTxC	**Not supported in G100** number of frames sent towards the application interface
1734	ETH3-4 PRP/HSR lreCntErrWrongLanA	**Not supported in G100** number of frames with the wrong LAN identifier received on port A
1735	ETH3-4 PRP/HSR lreCntErrWrongLanB	**Not supported in G100** number of frames with the wrong LAN identifier received on port B
1736	ETH3-4 PRP/HSR lreCntErrWrongLanC	**Not supported in G100** number of frames with the wrong LAN identifier received on the RedBox interlink
1737	ETH3-4 PRP/HSR lreCntRxA	**Not supported in G100** number of PRP/HSR frames received on port A
1738	ETH3-4 PRP/HSR lreCntRxB	**Not supported in G100** number of PRP/HSR frames received on port B
1739	ETH3-4 PRP/HSR lreCntRxC	**Not supported in G100** number of frames received from the application interface of a DANP or DANH or the number of number of frames received on the interlink of a RedBox

1740	ETH3-4 PRP/HSR lreCntErrorsA	**Not supported in G100** number of frames with errors received on port A
1741	ETH3-4 PRP/HSR lreCntErrorsB	**Not supported in G100** number of frames with errors received on port B
1742	ETH3-4 PRP/HSR lreCntErrorsC	**Not supported in G100** number of frames with errors received on the application interface of a DANP or DANH or on the interlink of a RedBox
1746	ETH3-4 PRP/HSR lreCntDuplicateA	**Not supported in G100** number of entries in the duplicate detection mechanism on port A for which one single duplicate was received
1747	ETH3-4 PRP/HSR lreCntDuplicateB	**Not supported in G100** number of entries in the duplicate detection mechanism on port B for which one single duplicate was received
1748	ETH3-4 PRP/HSR lreCntDuplicateC	**Not supported in G100** number of entries in the duplicate detection mechanism on the application interface of the DAN or the interlink of the RedBox for which one single duplicate was received
1761	ETH5-6 PRP/HSR lreCntTxA	**Not supported in G100** PRP/HSR frames sent over port A
1762	ETH5-6 PRP/HSR lreCntTxB	**Not supported in G100** PRP/HSR frames sent over port B
1763	ETH5-6 PRP/HSR lreCntTxC	**Not supported in G100** number of frames sent towards the application interface
1764	ETH5-6 PRP/HSR lreCntErrWrongLanA	**Not supported in G100** number of frames with the wrong LAN identifier received on port A
1765	ETH5-6 PRP/HSR lreCntErrWrongLanB	**Not supported in G100** number of frames with the wrong LAN identifier received on port B
1766	ETH5-6 PRP/HSR lreCntErrWrongLanC	**Not supported in G100** number of frames with the wrong LAN identifier received on the RedBox interlink
1767	ETH5-6 PRP/HSR lreCntRxA	**Not supported in G100** number of PRP/HSR frames received on port A
1768	ETH5-6 PRP/HSR lreCntRxB	**Not supported in G100** number of PRP/HSR frames received on port B
1769	ETH5-6 PRP/HSR lreCntRxC	**Not supported in G100** number of frames received from the application interface of a DANP or DANH or the number of number of frames received on the interlink of a RedBox

1770	ETH5-6 PRP/HSR lreCntErrorsA	**Not supported in G100** number of frames with errors received on port A
1771	ETH5-6 PRP/HSR lreCntErrorsB	**Not supported in G100** number of frames with errors received on port B
1772	ETH5-6 PRP/HSR lreCntErrorsC	**Not supported in G100** number of frames with errors received on the application interface of a DANP or DANH or on the interlink of a RedBox
1776	ETH5-6 PRP/HSR lreCntDuplicateA	**Not supported in G100** number of entries in the duplicate detection mechanism on port A for which one single duplicate was received
1777	ETH5-6 PRP/HSR lreCntDuplicateB	**Not supported in G100** number of entries in the duplicate detection mechanism on port B for which one single duplicate was received
1778	ETH5-6 PRP/HSR lreCntDuplicateC	**Not supported in G100** number of entries in the duplicate detection mechanism on the application interface of the DAN or the interlink of the RedBox for which one single duplicate was received

Text Points

Table 6.199: Text Points

Point ID	Point Reference	Point Description
205	PCIe 3 Serial No.	**Not supported in G100** Serial No. of HDLC Card
206	PCIe 3 FPGA Version	**Not supported in G100** FPGA Version of HDLC Card
330	FPGA_VER	**Not supported in G100** FPGA Version details
331	CPLD_VER	**Not supported in G100** CPLD Version details
332	UEFI_VER	**Not supported in G100** UEFI Version details
503	Power Supply 1 (top) Id	**Not supported in G100** Power supply 1 (top) ID details
504	Power Supply 2 (Bottom) Id	**Not supported in G100** Power Supply 2 (Bottom) ID details
3800	PTP Grand Master clock ID	**Not supported in G100**

		PTP Grand Master clock ID
3801	PTP Master Clock ID	**Not supported in G100** PTP Master Clock ID
3802	PTP Output Clock ID	**Not supported in G100** PTP Output Clock ID

Build Server Map Files

This chapter contains the following sections and sub-sections:

Server Maps

- Server Configuration Overview
- Creating Server Maps
- Server Protocol Settings
- Logical Remote Units
- Communication Statistics

IEC 60870-5-101+104 Server

- Info Object Settings
- Bitstring Mapping Settings
- Double Command Mapping Settings
- Double Point Mapping Settings
- Integrated Total Mapping Settings
- Measurand Mapping Settings
- Packed Single Point Mapping Settings
- Regulating Command Mapping Settings
- Root Directory Mapping Settings
- Setpoint Command Mapping Settings
- Single Command Mapping Settings
- Single Point Mapping Settings
- Step Position Mapping Settings

DNP3 Server

- About the DNP3 Server
- Analog Inputs
- Digital Inputs
- Analog Outputs
- Digital Outputs
- Accumulators

Modbus Server
About the Modbus Server
Coils
Read Only Registers
Read Write Registers
Input Status

Server Maps

SCADA master stations monitor many remote terminal units and gateway devices for certain critical information. The MCP forms an integral part of a SCADA system by collecting data from devices and then transmitting selected information to the master station as required. The MCP stores all the desired information for a master station in a "map" that lists and describes the selected data points from selected devices

The server map file is based on a specific protocol and specifies what information to present to a master. The map file contains information on how and when data is transmitted to a master station.

Once you create a server map file, it becomes available to select on the Configuration page when assigning master connections.

Creating Server Maps

» To create or edit a server map:

1. On the **Configuration** page, select the **Server Map** tab.
2. Click **New** to create a new client map or **Open** to edit an existing server map.
3. Select the SCADA protocol type and then create or select the master map file.
4. Edit the data type and protocol settings as desired.
5. Click **Save** and enter a name for your map file.

Tips

- To create a custom mapping template, create a map file, click "Save" and enter a template name.
- To add a full level of points for a device or point group, select the checkbox in the points tree view.
- To delete a point from the point map, select the row and click **Delete**.
- To create custom templates, create a default map file, click **Save** and then enter a new template name.

Server Protocol Settings

Server applications are available for the following protocols:

- DNP3 Server
- Modbus Server
- IEC 60870-5+104 Server

Logical Remote Units

The MCP can be configured to function as several distinct instances. Each instance is called a Logical Remote Unit (LRU). It appears as a single, physical server to any master station communicating with the LRU.

The MCP can be configured to represent multiple Logical Remote Units (LRUs) to multiple master stations. The data presented to each master station may be identical or unique and can be achieved using multiple protocols simultaneously.

For example, the MCP can maintain a separate event queue for every master station configured in the system. If a data point is configured for presentation to eight master stations, an event on the point causes eight events to be reported – one event to each master station.

Communication Statistics

Server applications maintain communication statistics and other status information in the real-time database as pseudo points.

DNP3 Server

About the DNP3 Server

The DNP3 Server application allows a remote master station to retrieve and/or modify the information in the database of the MCP using the DNP3 protocol. Because the DNP3 server application supports device-level addressing, it can access the full range of addresses supported by the protocol. For example, for DNP3, all master station addresses are user configurable per the DNP3 address range of 0 to 65519.

The DNP3 Server map defines how the MCP is configured to present data to DNP3 masters. The MCP supports the following configurable DNP3 data types:

- Analog inputs - measured or computed values by the device
- Digital inputs - states of physical or logical Boolean devices
- Analog outputs - physical or computed analog quantities
- Digital outputs - physical or logical ON-OFF, raise-lower, and trip-close points
- Accumulators - counter values

The DNP3 Server map settings are available on the **Server Map** tab when a DNP3 SCADA protocol type is selected.

DNP3 Server Analog Inputs

Settings are available on the **Analog Inputs** tab. The default property values are defined in the lower pane. The MCP provides the mapping settings for analog inputs as shown below.

Analog Input Mapping Settings

Table 6.200: Analog Input Mapping Settings

Setting	Description	Range	Default
Index	Point Index (0 Based). Each point index number must be unique.	0 to 65535	Incremented from 0.
Home Directory	Home directory of the IED AI point selected from the Point Picker. Read only.	N/A	System Assigned Identifier
Point Description	Point description of the AI point selected from the Point Picker. Read only.	N/A	System Assigned Identifier.
Point Reference	Point reference of the AI point selected from the Point Picker. Read only	N/A	System Assigned Identifier

Setting	Description	Range	Default
Point ID	Point ID of the AI point selected from the Point Picker. Read only.	N/A	System Assigned Identifier
Multiplier	Scale factor of the point (**m** of formula **mx + b**)	Full range of 64-bit Float	1.0
Offset	Scale factor of the point (**b** of formula **mx + b**)	Full range of 64-bit Float	0.0
Buffer Events	Specify whether to buffer analog input events.	Buffered Not Buffered	
Processing Options	When Buffer Events is set to Not Buffered, this setting determines whether to send the event with the: • Current value and time or • First value and Time, (in the case of multiple changes on the same point before the DPA can report a change)	Current Value and Time First Value and Time	Current Value and Time
Dead Band	Minimum change in the AI point value that constitutes an event. A value of 0 disables event generation for the point.	0 to 65535	User selected Default
Static Variation	How the point values should be reported.	32-Bit 16-Bit 32-Bit w/o flag 16-Bit w/o flag 32-Bit Float	User selected Default
Event Variation	Indicates how an event on this point should be reported.	32-Bit with Time 32-Bit without Time 16 Bit with Time 16 Bit without Time 32-Bit Float with Time 32-Bit Float without Time	User selected Default
Class	Default Class for change events on the point.	None 3 2 1	User selected Default

Settings are available in the lower pane of the **Analog Inputs** tab. The configuration settings defined below are used to configure the default values for all analog input points defined in the DNP3 server map.

Analog Input Properties

Table 6.201: Analog Input Properties

Setting	Description	Range	Default
Default Class Assignment	All AI events belong to this class by default.	None 3 2 1	2

Default Static Variation	Type to report when the master does not request any specific type.	32-Bit 16-Bit 32-Bit w/o flag 16-Bit w/o flag 32-Bit Float	32-Bit
Default Event Variation	Type to report when the master does not request any specific type. l	32-Bit with Time 32-Bit without Time 16 Bit with Time 16 Bit without Time 32-Bit Float with Time 32-Bit Float without Time	32-Bit with Time
Default Dead Band	Minimum change in the AI point value that constitutes an event. A value of 0 disables event generation for the point.	0-65535	5

DNP3 Server Digital Inputs

Settings are available on the **Digital Inputs** tab. The default property values are defined in the lower pane. The MCP provides the mapping settings for digital inputs as shown below.

Digital Input Mapping Settings

Table 6.202: Digital Input Mapping Settings

Setting	Description	Range	Default
Index	Point Index (0 Based). Each point index number must be unique.	0 to 65535	Incremented from 0.
Point Description	Point description of the DI point selected from the Point Picker. Read only	N/A	System Assigned Identifier
Point Reference	Point reference of the DI point selected from the Point Picker. Read only	N/A	System Assigned Identifier
Point ID	Point ID of the DI point selected from the Point Picker. Read only.	N/A	System Assigned Identifier
Home Directory	Home Directory of the IED DI point selected from the Point Picker. Read only.	N/A	System Assigned Identifier
Invert	Select if the value of the mapped points should be inverted.	True or False	False
Static Variation	How the point values should be reported.	32-Bit 16-Bit 32-Bit w/o flag 16-Bit w/o flag 32-Bit Float	User selected Default

Setting	Description	Range	Default
Event Variation	Indicates how an event on this point should be reported.	32-Bit with Time 32-Bit without Time 16 Bit with Time 16 Bit without Time 32-Bit Float with Time 32-Bit Float without Time	User selected Default
Class	Default Class for change events on the point.	None 3 2 1	User selected Default

Settings are available in the lower pane of the **Digital Inputs** tab. The configuration settings defined below are used to configure the default values for all digital input points defined in the DNP3 server map.

Digital Input Properties

Table 6.203: Digital Input Properties

Setting	Description	Range	Default
Default Class Assignment	All DI events belong to this class by default.	None 3 2 1	1
Default Invert	Indicates whether Digital Input (DI) point values are to be inverted.	True or False	False
Default Static Variation	Type to report when the master does not request any specific type.	With Status Without Status	With Status
Default Event Variation	Type to report when the master does not request any specific type.	With Time Without Time	With Time

DNP3 Server Analog Outputs

Settings are available on the **Analog Outputs** tab. The default property values are defined in the lower pane. The MCP provides the mapping settings for analog outputs as shown below.

Analog Output Mapping Settings

Table 6.204: Analog Output Mapping Settings

Setting	Description	Range	Default
Index	Point Index (0 Based). Each point index number must be unique.	0 to 65535	Incremented from 0.
Home Directory	Home Directory of the IED of AO point selected from the Point Picker. Read only.	N/A	System Assigned Identifier
Point Description	Point Description of the AO point selected from the Point Picker. Read only.	N/A	System Assigned Identifier
Point Reference	Point Reference of the AO point selected from the Point Picker. Read only	N/A	System Assigned Identifier

Point ID	Point ID of the AO point selected from the Point Picker. Read only.	N/A	System Assigned Identifier
Multiplier	Scale factor of the point (**m** of formula **mx + b**)	Full range of 64-bit Float	1.0
Offset	Scale factor of the point (**b** of formula **mx + b**)	Full range of 64-bit Float	0.0
Static Variation	How the point values should be reported.	32-Bit 16-Bit 32-Bit w/o flag 16-Bit w/o flag 32-Bit Float	User selected Default

Settings are available in the lower pane of the **Analog Outputs** tab. The configuration settings defined below are used to configure the default values for all analog output points defined in the DNP3 server map.

Analog Output Properties

Table 6.205: Analog Output Properties

Setting	Description	Range	Default
Default Static Variation	Type to report when the master does not request any specific type.	32-Bit 16-Bit	32-Bit

DNP3 Server Digital Outputs

Settings are available on the **Digital Outputs** tab. The default property values are defined in the lower pane. The MCP provides the mapping settings for digital outputs as shown below.

Digital Output Mapping Settings

Table 6.206: Digital Output Mapping Settings

Setting	Description	Range	Default
Index	Point Index (0 Based). Each point index number must be unique.	0 to 65535	Incremented from 0.
Home Directory	Home Directory of the IED of DO point selected from the Point Picker. Read only.	N/A	System Assigned Identifier
Point Description	Point Description of the DO point selected from the Point Picker. Read only.	N/A	System Assigned Identifier
Point Reference	Point Reference of the DO point selected from the Point Picker. Read only	N/A	System Assigned Identifier
Point ID	Point ID of the DO point selected from the Point Picker. Read only.	N/A	System Assigned Identifier
Supported Command	Command the DNP3 server should expect. If the DNP3 server receives a command that is not configured, it rejects the command.	All operations SBO Only	User selected Default

Settings are available in the lower pane of the **Digital Outputs** tab. The configuration settings defined below are used to configure the default values for all digital output points defined in the DNP3 server map.

Digital Output Properties

Table 6.207: Digital Output Properties

Setting	Description	Range	Default
Default Command Supported	The DNP3 server uses this as the default command to support when the master does not request any specific type.	All operations SBO Only	SBO Only

DNP3 Server Accumulators

The accumulators are used for reporting running values, frozen values, and events. This means that the same DNP3 point index is used for both the running and frozen value. The DNP3 server returns the running value when data points for Static Variation (Object 20) are requested by the master station. The DNP3 server returns the frozen value when data points for Static Variation (Object 21) is requested by the Master station. The Threshold configured is used to qualify events for running accumulators only Event Variation (Object22). Frozen accumulator events (Object 23) are generated whenever a configured accumulator is frozen.

Settings are available on the **Accumulators** tab. The default property values are defined in the lower pane. The MCP provides the mapping settings for accumulators (counters) as shown below.

Accumulator Mapping Settings

Table 6.208: Accumulator Mapping Settings

Setting	Description	Range	Default
Index	Point Index (0 Based). Each point index number must be unique.	0 to 65535	Incremented from 0.
Home Directory	Home directory of the IED Accumulator point selected from the Point Picker. Read only.	N/A	System Assigned Identifier
Point Description	Point description of the Accumulator point selected from the Point Picker. Read only.	N/A	System Assigned Identifier
Point Reference	Point reference of the Accumulator point selected from the Point Picker. Read only	N/A	System Assigned Identifier
Point ID	Point ID of the Accumulator point selected from the Point Picker. Read only.	N/A	System Assigned Identifier
Threshold	Minimum change required in the Running Accumulator count to cause an event to be generated. 0 disables generation of Running Accumulator Events.	0 to 5000	User selected Default
Static Variation	How the point values should be reported. Applies to Running value.	32-Bit 16-Bit	User selected Default
Event Variation	Indicates how an event on this point should be reported. Applies to Running value.	32-Bit with Time 32-Bit without Time 16 Bit with Time 16 Bit without Time	User selected Default

Setting	Description	Range	Default
Frozen Static Variation	How the point values should be reported. Applies to Frozen value.	32-Bit with Time 32-Bit without Time 16 Bit with Time 16 Bit without Time	User selected Default
Frozen Event Variation	Indicates how an event on this point should be reported. Applies to Frozen value.	32-Bit with Time 32-Bit without Time 16 Bit with Time 16 Bit without Time	User selected Default
Class	Default Class for change events on the point.	None 3 2 1	User selected Default

Settings available in the lower pane on the **Accumulators** tab. The configuration settings defined below are used to configure the default values for all accumulator points defined in the DNP3 server.

Accumulator Properties

Table 6.209: Accumulator Properties

Setting	Description	Range	Default
Default Class Assignment	All ACC Events belong to this class by default	None 3 2 1	3
Default Static Variation (Object 20 and 21)	Type to report, when the master does not request any specific type.	32-Bit 16-Bit	32-Bit
Default Event Variation (Object 22 and 23)	Type to report, when the master does not request any specific type.	32-Bit with Time 32-Bit without Time 16 Bit with Time 16 Bit without Time	32-Bit with Time
Frozen Static Variation	Type to report, when the master does not request any specific type.	32-Bit with Time 32-Bit without Time 16 Bit with Time 16 Bit without Time	32-Bit with Time
Frozen Event Variation	Type to report, when the master does not request any specific type.	32-Bit with Time 32-Bit without Time 16 Bit with Time 16 Bit without Time	32-Bit with Time
Default Threshold	Minimum change in the ACC point value that constitutes an event.	0 to 5000	0

MODBUS Server

About the Modbus Server

The Modbus Server application allows a remote master station to retrieve and/or modify the information in the database of the MCP using the Modbus protocol.

The Modbus Server map defines how the MCP is configured to present data to Modbus masters. The MCP supports the following configurable Modbus data types:

- Coils
- Read Only Registers
- Read Write Registers
- Input Status

The Modbus Server map settings are available on the **Server Map** tab when a Modbus protocol type is selected.

Modbus Server Coils

Mapping settings are available in the upper pane of the **Coils** tab as shown below.

Table 6.210: Coil Mapping Settings

Setting	Description	Range	Default
Address	The Modbus address assigned to the point	0 to 65535	X
IED	System Point Identifier. Consists of Home Directory and Point Name. Based on selected DO point from the Point Picker. Read only.	N/A	System Assigned Identifier
Point Description	A detailed and localized description of the point in the Digital Output/ Digital Input map. Based on the selected DO/DI point. Read only.	Up to 128 Unicode characters	Assigned IED point description
Point Reference	Based on selected DO/DI point, it is the short identifier of the point in the map. Read Only	Up to 66 ASCII characters	Assigned point name
Point ID	Consists of Point ID of the selected DI point from the Digital Input Point map. Read only.	Not editable	System Generated Point Identifier
Type	The point type. Read only.	DI, DO	Assigned type
Control Spec	See the Control Specification Properties table. Only enabled for DO type points.		
Feedback Opt	If set to *Self*, the values of the DO points are returned. If set to *Digital Inputs*, the value of the Digital Input point is returned. Only enabled for DO type points.	Self DigitalInput	Self
Feedback Point	If Feedback Opt is set to *Digital Input*, the point selected is returned.	List of points based on configured DIs	N/A
Invert	Select if the value of the mapped points should be inverted. Only enabled for DI points.	True or False	False

Table 6.211: Control Specification Properties

Setting	Description	Range	Default
Control Code	The control commands that the IED accepts.	Latch ON/OFF Pulse ON/OFF TRIP/CLOSE	Latch ON/OFF
Function Code	The protocol function code to pass as part of the digital control command sent to a device.	Select Before Operate Direct Operate	Select Before Operate
Count	Number of times to consecutively repeat a control code, applying the pulse on and pulse off times to each control pulse repetition (applies only to Control Codes of type Pulse On, Pulse Off, Trip, or Close).	1 to 255	1
On Time	Duration, in milliseconds, of an ON pulse	0 to 65535	0
Off Time	Duration, in milliseconds, of an OFF pulse	0 to 65535	0

Property settings are available in the lower pane of the **Coils** tab. The configuration settings defined in the table below are used to configure the default values for all coils defined in the Modbus server map.

Table 6.212: Coil Properties

Setting	Description	Range	Default
Default Control Spec	See the Default Control Specification Properties table.		
Default Feedback Opt	If set to *Self*, the values of the DO points are returned. If set to *Digital Inputs*, the value of the Digital Input point is returned.	Self DigitalInput	Self
Default Invert	Select if the value of the mapped points should be inverted by default	True or False	False

Table 6.213: Default Control Specification Properties

Setting	Description	Range	Default
Default Control Code	The control commands that the IED accepts by default.	Latch ON/OFF Pulse ON/OFF TRIP/CLOSE	Latch ON/OFF
Default Function Code	The default protocol function code to pass as part of the digital control command sent to a device.	Select Before Operate Direct Operate	Select Before Operate
Default Count	Number of times to consecutively repeat a control code, applying the pulse on and pulse off times to each control pulse repetition (applies only to Control Codes of type Pulse On, Pulse Off, Trip, or Close).	1 to 255	1
Default On Time	Default duration, in milliseconds, of an ON pulse	0 to 65535	0
Default Off Time	Default duration, in milliseconds, of an OFF pulse	0 to 65535	0

Modbus Server Read Only Registers

Mapping settings are available on the **Read Only Registers** tab as shown below.

Table 6.214: Read Only Register Mapping Settings

Setting	Description	Range	Default
Address	The Modbus address assigned to the point	0 to 65535	X
IED	System Point Identifier. Consists of Home Directory and Point Name. Based on selected DO point from the Point Picker. Read only.	N/A	System Assigned Identifier
Point Description	A detailed and localized description of the selected point in the map. Based on the selected AI/DI/ACC point. Read only.	Up to 128 Unicode characters	Assigned IED point description
Point Reference	Based on selected AI/DI/ACC point, it is the short identifier of the point in the map. Read only.	Up to 66 ASCII characters	Assigned point name
Point ID	Consists of Point ID of the selected DI point from the Digital Input Point map. Read only.	Not editable	System Generated Point Identifier
Type	The point type. Read only.	DI, AI, AO, ACC	Assigned type
Data Format	The type of data polled	See the Modbus Client Supported Data Types table.	INT16
Point Value to Use	The attribute of the point to be polled	Value Frozen Value Date and Time Freeze Date and Time	Value
Multiplier	Scale factor of the point (**m** of formula **mx + b**)	Full range of 64-bit Float	1.0
Offset	Scale factor of the point (**b** of formula **mx + b**)	Full range of 64-bit Float	0.0

Property settings are available in the lower pane of the **Read Only Registers** tab. The configuration settings defined in the table below are used to configure the default values for all read only registers defined in the Modbus server map.

Table 6.215: Read Only Register Properties

Setting	Description	Range	Default
Default Point Value To Use	The attribute of the point that should be polled by default	Value Frozen Value Date and Time Freeze Date and Time	Value
Default Multiplier	Default scale factor of the point (**m** of formula **mx + b**)	Full range of 64-bit Float	1.0
Default Offset	Default scale factor of the point (**b** of formula **mx + b**)	Full range of 64-bit Float	0.0

Modbus Server Read Write Registers

Mapping settings are available on the upper pane of the **Read Write Registers** tab as shown below.

Table 6.216: Read Write Register Mapping Settings

Setting	Description	Range	Default
Address	The Modbus address assigned to the point	0 to 65535	X
IED	System Point Identifier. Consists of Home Directory and Point Name. Based on selected DO point from the Point Picker. Read only.	N/A	System Assigned Identifier
Point Description	A detailed and localized description of the point in the Analog Input map. Based on the selected AI point. Read only.	Up to 128 Unicode characters	Assigned IED point description
Point Reference	Based on selected AI point, it is the short identifier of the point in the map. Read Only.	Up to 66 ASCII characters	Assigned point name
Point ID	Consists of Point ID of the selected DI point from the Digital Input Point map. Read only.	Not editable	System Generated Point Identifier
Type	The point type. Read only.	DI, AI, AO, ACC	Assigned type
Data Format	The type of data polled	See the Modbus Client Supported Data Types table.	INT16
Point Value to Use	The attribute of the point to be polled	Value Frozen Value Date and Time Freeze Date and Time	Value
Multiplier	Scale factor of the point (**m** of formula **mx + b**)	Full range of 64-bit Float	1.0
Offset	Scale factor of the point (**b** of formula **mx + b**)	Full range of 64-bit Float	0.0

Property settings are available in the lower pane of the **Read Write Registers** tab. The configuration settings defined in the table below are used to configure the default values for all read write registers defined in the Modbus server map.

Table 6.217: Read Write Register Properties

Setting	Description	Range	Default
Default Point Value To Use	The attribute of the point that should be polled by default	Value Frozen Value Date and Time Freeze Date and Time	Value
Default Multiplier	Default scale factor of the point (**m** of formula **mx + b**)	Full range of 64-bit Float	1.0
Default Offset	Default scale factor of the point (**b** of formula **mx + b**)	Full range of 64-bit Float	0.0

Modbus Server Input Status

Mapping settings are available on the upper pane of the **Input Status** tab as shown below.

Table 6.218: Input Status Mapping Settings

Setting	Description	Range	Default
Address	The Modbus address assigned to the point	0 to 65535	X
IED	System Point Identifier. Consists of Home Directory and Point Name. Based on selected DO point from the Point Picker. Read only.	N/A	System Assigned Identifier
Point Description	A detailed and localized description of the point in the Digital Input map. Based on selected DI point. Read only.	Up to 128 Unicode characters	Assigned IED point name
Point Reference	Based on selected DI point, it is the short identifier of the point in the map. Read Only.	Up to 66 ASCII characters	Assigned point name
Type	The point type. Read only.	DI, AI, AO, ACC	Assigned type
Invert	Select if the value of the mapped points should be inverted	True or False	False

Property settings are available in the lower pane of the **Input Status Mapping** tab. The configuration settings defined in the table below are used to configure the default values for all read write registers defined in the Modbus server map.

Table 6.219: Input Status Properties

Setting	Description	Range	Default
Default Invert	Select if the value of the mapped points should be inverted by default	True or False	False

IEC 60870-5-101+104 Server

The IEC 60870-5-101 and IEC 60870-5-104 Server applications allow remote master stations to retrieve and/or modify the information in the database of the MCP using the IEC 60870-5 protocol.

The IEC 60870-5-101+104 Server map defines how the MCP is configured to present data to IEC 60870-5 masters. User can create the following types of information objects:

User can configure the IEC 60870 Server Time Zone offset using the **mcpcfg** command line utility. Refer to Configure Time Synchronization.

» **To create an Information Object:**

1. Click **Add Info Object**.
2. On the **New Info Object** window, enter values for the fields as described in the table below and click **OK**.
3. Configure each info object and add points to present to the master station.

Info Object Settings

Table 6.220: Info Object Settings

Setting	Description	Range
Info Object Type	The type of information object being created.	Bitstring Double Command Double Point Integrated Total Measurand Packed Single Point Regulating Command Root Directory Setpoint Command Single Command Single Point Step Position
Info Object Name	An identifier used within the configuration interface.	1 to 128 ASCII characters
Starting Info Object Address	Starting address for this object.	1 to 16777215

The table directly below the Info Object type drop-down menu shows the configured values for the selected Info Object. Info Object Name cannot be edited in this table.

Bitstring Mapping Settings

Table 6.221: Bitstring Mapping Settings

Setting	Description	Range	Default
Info Object Settings			
Info Object Name	The name of the information object as entered on the New Info Object window. Read only.	N/A	N/A
Address	The address of this entry.	1 to 16777215	
Interrogation Group	The interrogation group used for reporting this information object.	Not Used Group 1 ... Group 16	Not Used
Interrogation Response	Specify whether to include this information object in a general interrogation response.	Include Exclude	Include
Report Class	Specify if spontaneous events for this object are reported as class 1 or class 2 messages. Applies to unbalanced mode and spontaneous events only.	Class 1 Class 2	Class 1
Periodic Update Mode	The type of periodic updating	Not Used Background Scan	Not Used
Periodic Update Interval	The time (in seconds) between periodic reports. Used only if Periodic Update Mode is not set to *Not Used*.	0 to 65535	0
Periodic Report On Power Up	Specify if periodic reporting (if enabled) should begin immediately upon startup.	Disabled Enabled	Disabled
Time Tag	The type of time tag to use.	None With Time Tag With CP56 Time Tag	None

Per-Point Settings			
Bit Position		1 to 32	Incremented from 1
IED	System Point Identifier. Consists of Home Directory of the selected DI point from the Point Picker. Read only.	Not editable	System Assigned Identifier
Point ID	Shows the Point ID of the selected DI point from the Digital Input Point map. Read only.	Not editable	System Generated Point Identifier
Point Reference	A short identifier for the selected DI point from the Point Picker. Read Only.	Up to 66 ASCII Characters Not editable	Assigned point name
Point Description	A detailed and localized description of the selected point in the Binary Input map. Read only.	Up to 128 characters Not editable	Assigned IED point description
Invert	Select if the value of the mapped points should be inverted.	True or False	False

Double Command Mapping Settings

Table 6.222: Bitstring Mapping Settings

Setting	Description	Range	Default
Info Object Settings			
Info Object Name	The name of the information object as entered on the New Info Object window. Read only.	N/A	N/A
Starting Address	The starting address of this entry.	1 to 16777215	
Time Tag	The type of time tag to use.	None With Time Tag With CP56 Time Tag	None
Per-Point Settings			
Address	The address of this entry. Read only.	N/A	N/A
Control Type	The type of control to operate.	Trip/Close Regulating Persistent	Persistent
Short Pulse Duration	The control duration (in milliseconds) of the short pulse output.	1 to 2147483647	1000
Long Pulse Duration	The control duration (in milliseconds) of the long pulse output.	1 to 2147483647	2000
Transmission Type	The type of transmission used for control command execution; either a select and execute command sequence or direct execute command sequence.	Select and Execute Direct Execute	Select and Execute

Source Point One	First of two digital output source points selected from the Point Picker to comprise the 4-state point being monitored. Based on the user-selected DO point, the point ID of Source Point One is prefixed with the home directory of that point.	List of points based on configured DOs	System assigned identifier
Point 1 Description	A detailed and localized description of the selected Source Point One. Read Only	Not editable	Assigned IED point Description
Source Point Two	Second of two digital output source points selected to comprise the 4-state point being monitored.	List of points based on configured DOs	N/A
Point 2 Description	A detailed and localized description of the selected Source Point Two. Read Only	Not editable	Assigned IED point Description

Double Point Mapping Settings

Table 6.223: Double Point Mapping Settings

Setting	Description	Range	Default
Info Object Settings			
Info Object Name	The name of the information object as entered on the New Info Object window. Read only.	N/A	N/A
Starting Address	The starting address of this entry.	1 to 16777215	
Interrogation Group	The interrogation group used for reporting this information object.	Not Used Group 1 ... Group 16	Not Used
Interrogation Response	Specify whether to include this information object in a general interrogation response.	Include Exclude	Include
Report Class	Specify if spontaneous events for this object are reported as class 1 or class 2 messages. Applies to unbalanced mode and spontaneous events only.	Class 1 Class 2	Class 1
Periodic Update Mode	The type of periodic updating	Not Used Background Scan	Not Used
Periodic Update Interval	The time (in seconds) between periodic reports. Used only if Periodic Update Mode is not set to *Not Used*.	0 to 65535	0
Periodic Report On Power Up	Specify if periodic reporting (if enabled) should begin immediately upon startup.	Disabled Enabled	Disabled
Time Tag	The type of time tag to use.	None With Time Tag With CP56 Time Tag	None
Valid Time	The minimum amount of time (in milliseconds) that both digital input points must be stable before an ON or OFF state is reported. –1 disables this setting.	-1 to 65535	-1
Suppress Time	The minimum amount of time (in milliseconds) that both digital input points must be stable before an indeterminate state is reported. –1 disables this setting.	-1 to 65535	-1

Setting	Description	Range	Default
Per-Point Settings			
Address	The address of the entry. Read only.	N/A	N/A
Off Point Source	First of two digital input source points selected from the Point Picker to comprise the 4-state point being monitored. Based on user configured DI point, the home directory of the point is post fixed with system assigned identifier (Point ID).	Not Editable List of points based on configured DIs	System assigned identifier
Point 1Description	A detailed and localized description of the selected Off Point Source. Read Only	List of points based on configured DIs.	Assigned IED point Description.
On Point Source	Second of two digital input source points selected to comprise the 4-state point being monitored.	List of points based on configured DIs.	N/A
Point 2 Description	A detailed and localized description of the selected-On Point Source. Read Only	Not editable	Assigned IED point Description
Invert	Select if the value of the mapped points should be inverted.	True or False	False

Integrated Total Mapping Settings

Table 6.224: Integrated Total Mapping Settings

Setting	Description	Range	Default
Info Object Settings			
Info Object Name	The name of the information object as entered on the New Info Object window. Read only.	N/A	N/A
Starting Address	The starting address of this entry.	1 to 16777215	
Interrogation Group	The interrogation group used for reporting this information object.	Not Used Group 1 ... Group 4	Not Used
Interrogation Response	Specify whether to include or exclude this information object in a general interrogation response.	Include Exclude	Include
Report Class	Specify if spontaneous events for this object are reported as class 1 or class 2 messages. Applies to unbalanced mode and spontaneous events only.	Class 1 Class 2	Class 1
Time Tag	The type of time tag to use.	None With Time Tag With CP56 Time Tag	None
Periodic Update Mode	The type of periodic updating	Not Used Background Scan	Not Used
Periodic Update Interval	The time (in seconds) between periodic reports. Used only if Periodic Update Mode is not set to *Not Used*.	0 to 65535	0
Periodic Report On Power Up	Specify if periodic reporting (if enabled) should begin immediately upon startup.	Disabled Enabled	Disabled

Setting	Description	Range	Default
Per-Point Settings			
Address	Read only.	N/A	N/A
IED	System Point Identifier. Consists of Home Directory of the selected ACC point from the Point Picker. Read only.	N/A	System Assigned Identifier
Point Description	A detailed and localized text description of the selected point in the Accumulator point map. Read only.	Up to 128 Unicode characters	Assigned IED point Description
Point Reference	A short identifier for the selected ACC point from the Point Picker. Read Only.	Up to 66 ASCII Characters Not editable	Assigned point name
Accumulator Type	Specifies whether every change (transition) or every pair of changes (pulse) in the monitored accumulator point value increments the reported count.	Pulse Transition	Pulse
Accumulator Return Type	Specifies whether the running or frozen accumulator value is reported.	Running Frozen	Running
Accumulator Freeze	Specifies whether the master station can freeze the monitored accumulator point.	Enabled Disabled	Disabled
Accumulator Clear	Specifies whether or not the master station is allowed to clear the monitored accumulator point.	Enabled Disabled	Disabled
Threshold	Specifies the minimum change in accumulator value required to produce a spontaneous report or event. Only used when the Accumulator Return Type is *Running*.	0 to 1000000	1

Measurand Mapping Settings

Table 6.225: Measurand Mapping Settings

Setting	Description	Range	Default
Info Object Settings			
Info Object Name	The name of the information object as entered on the New Info Object window. Read only.	N/A	N/A
Starting Address	The starting address of this entry.	1 to 16777215	
Interrogation Group	The interrogation group used for reporting this information object.	Not Used Group 1 ... Group 16	Not Used
Interrogation Response	Specify whether to include this information object in a general interrogation response.	Include Exclude	Include
Report Class	Specify if spontaneous events for this object are reported as class 1 or class 2 messages. Applies to unbalanced mode and spontaneous events only.	Class 1 Class 2	Class 1

Setting	Description	Range	Default
Periodic Update Mode	The type of periodic updating	Not Used Background Scan Periodic/Cyclic	Not Used
Periodic Update Interval	The time (in seconds) between periodic reports. Used only if Periodic Update Mode is not set to *Not Used*.	0 to 65535	0
Periodic Report On Power Up	Specify if periodic reporting (if enabled) should begin immediately upon startup.	Disabled Enabled	Disabled
Time Tag	The type of time tag to use.	None With Time Tag With CP56 Time Tag	None
Conversion	The type of setpoint command. There are 3 possible types: • Normalized - value is between -1 and +1 - 2^-15 • Scaled - value is scaled using multiplier and offset to -2^15 to +2^15 – 1 • Short Floating Point - value is a 32-bit floating point.	Normalized Scaled ShortFP	Normalized
Quality	Whether quality information is included with this entity.	With Quality Descriptor Without Quality Descriptor	With Quality Descriptor
Per-Point Settings			
Address	The address of this entity. Read only.	N/A	N/A
IED	System Point Identifier. Consists of Home Directory of the selected AI point from the Point Picker. Read only.	N/A	System Assigned Identifier
Point Reference	A short identifier for the selected AI point from the Point Picker. Read Only.	Up to 66 ASCII Characters Not editable	Assigned point name
Point Description	A detailed and localized text description of the selected point in the Analog Input map. Read only.	Up to 128 Unicode characters. Non-Editable	Assigned IED point description
Multiplier	Scale factor of the point (**m** of formula **mx + b**)	Full range of 64-bit Float	1.0
Offset	Scale factor of the point (**b** of formula **mx + b**)	Full range of 64-bit Float	0.0
Polarity	Specifies whether a negative analog value is valid.	Bipolar Value Unipolar Value	Bipolar Value
Threshold	The initial minimum change in the analog input value that is required to produce a spontaneous report or event.	0 to 1,000,000,000	5
High Limit	The initial high limit that is required for an analog input value to exceed to produce an event.	-1.0E+12 to 1.0E+12	1.0E+12

Setting	Description	Range	Default
Low Limit	The initial low limit that is required for an analog input value to exceed to produce an event.	-1.0E+12 to 1.0E+12	-1.0E+12

Packed Single Point Mapping Settings

Table 6.226: Packed Single Point Mapping Settings

Setting	Description	Range	Default
Info Object Settings			
Info Object Name	The name of the information object as entered on the New Info Object window. Read only.	N/A	N/A
Address	The address of this entry.	N/A	N/A
Interrogation Group	The interrogation group used for reporting this information object.	Not Used Group 1 ... Group 16	Not Used
Interrogation Response	Specify whether to include this information object in a general interrogation response.	Include Exclude	Include
Report Class	Specify if spontaneous events for this object are reported as class 1 or class 2 messages. Applies to unbalanced mode and spontaneous events only.	Class 1 Class 2	Class 1
Periodic Update Mode	The type of periodic updating	Not Used Background Scan	Not Used
Periodic Update Interval	The time (in seconds) between periodic reports. Used only if Periodic Update Mode is not set to *Not Used*.	0 to 65535	0
Periodic Report On Power Up	Specify if periodic reporting (if enabled) should begin immediately upon startup.	Disabled Enabled	Disabled
Per-Point Settings			
Bit Position	Specifies the bit position within the information object element.	1 to 16	Incremented from 1
IED	System Point Identifier. Identifies the Home Directory of the selected DI point from the Point Picker. Read only.	N/A	System Assigned Identifier
Point ID	Consists of Point ID of the selected DI point from the Digital Input Point map. Read only.	Not editable	System Generated Point Identifier
Point Description	A detailed and localized text description of the selected DI point in the Binary Input map. Read only.	Up to 128 Unicode characters Not editable	Assigned IED point description
Invert	Select if the value of the mapped points should be inverted.	True or False	False

Regulating Command Mapping Settings

Table 6.227: Regulating Command Mapping Settings

Setting	Description	Range	Default
Info Object Settings			
Info Object Name	The name of the information object as entered on the New Info Object window. Read only.	N/A	N/A
Starting Address	The starting address of this entry.	1 to 16777215	
Time Tag	The type of time tag to use.	None With Time Tag With CP56 Time Tag	None
Per-Point Settings			
Address	The address of this entry. Read only.	N/A	N/A
Control Type	The type of control to operate.	Trip/Close Regulating Persistent	Persistent
Short Pulse Duration	The control duration (in milliseconds) of the short pulse output.	1 to 2147483647	1000
Long Pulse Duration	The control duration (in milliseconds) of the long pulse output.	1 to 2147483647	2000
Transmission Type	The type of transmission used for command control execution; either a select and execute command sequence or direct execute command sequence.	Select and Execute Direct Execute	Select and Execute
Source Point One	First of two digital input source points selected from the Point Picker to comprise the 4-state point being monitored. Based on user configured DI point name post fixed with system assigned identifier (Point ID).	Not editable	System assigned identifier
Point 1 Description	A detailed and localized description of the selected Source Point One. Read Only	Not editable	Assigned IED point Description
Source Point Two	Second of two digital input source points selected to comprise the 4-state point being monitored.	List of points based on configured DIs.	N/A
Point 2 Description	A detailed and localized description of the selected Source Point Two. Read Only	Not editable	Assigned IED point Description

Root Directory Mapping Settings

Table 6.228: Root Directory Mapping Settings

Setting	Description	Range	Default
Info Object Settings			
Info Object Name	The name of the information object as entered on the New Info Object window. Read only.	N/A	N/A
Address	The address of this entry.	1 to 16777215	none

Setpoint Command Mapping Settings

Table 6.229: Setpoint Command Mapping Settings

Setting	Description	Range	Default
Info Object Settings			
Info Object Name	The name of the information object as entered on the New Info Object window. Read only.	N/A	N/A
Starting Address	The starting address of this entry.	1 to 16777215	none
Time Tag	The type of time tag to use.	None With Time Tag With CP56 Time Tag	None
Conversion	The type of setpoint command. There are 3 possible types: • Normalized - value is between -1 and +1 - 2^-15 • Scaled - value is scaled using multiplier and offset to -2^15 to +2^15 – 1 • Short Floating Point - value is a 32-bit floating point.	Normalized Scaled ShortFP	Normalized
Per-Point Settings			
Address	The address of this entry. Read only.	N/A	N/A
IED	System Point Identifier. Identifies the Home Directory of the selected AO point from the Point Picker. Read only.	N/A	System Assigned Identifier
Point ID	Shows the Point ID of the selected AO point from the Digital Input Point map. Read only.	Not editable	System Generated Point Identifier
Point Reference	A short identifier of the selected AO point from the Point Picker. Read Only.	Up to 66 ASCII Characters Not editable	Assigned point name
Point Description	A detailed and localized text description of the point in the selected AO point map. Read only.	Up to 128 Unicode characters Not editable	Assigned IED point description
Multiplier	Scale factor of the point (**m** of formula **mx + b**)	Full range of 64-bit Float	1.0
Offset	Scale factor of the point (**b** of formula **mx + b**)	Full range of 64-bit Float	0.0
Polarity	Specifies whether a negative analog value is valid.	Bipolar Value Unipolar Value	Bipolar Value
Transmission Type	The type of transmission used for control command execution; either a select and execute command sequence or only an execute command sequence.	Select and Execute Direct Execute	Select and Execute
Send Ackterm	Specifies whether the application sends an ACTTERM response to the master station when a C_SE setpoint command completes	No Yes	No

Single Command Mapping Settings

Table 6.230: Single Command Mapping Settings

Setting	Description	Range	Default
Info Object Settings			
Info Object Name	The name of the information object as entered on the New Info Object window. Read only.	N/A	N/A
Starting Address	The starting address of this entry.	1 to 16777215	
Time Tag	The type of time tag to use.	None With Time Tag With CP56 Time Tag	None
Per-Point Settings			
Address	The address of this entry. Read only.	N/A	N/A
Control Type	The type of control to operate.	Trip/Close Regulating Persistent	Persistent
Short Pulse Duration	The control duration (in milliseconds) of the short pulse output.	1 to 2147483647	1000
Long Pulse Duration	The control duration (in milliseconds) of the long pulse output.	1 to 2147483647	2000
Transmission Type	The type of transmission; either a select and execute command sequence or only an execute command sequence.	Select and Execute Direct Execute	Select and Execute
Source Point One	First of two digital input source points selected from the Point Picker to comprise the 4-state point being monitored. Based on user configured DO point name post fixed with system assigned identifier (Point ID).	Not editable	System assigned identifier
Point 1 Description	A detailed and localized description of the selected Source Point One. Read Only	Not editable	Assigned IED point Description
Source Point Two	Second of two digital input source points selected to comprise the 4-state point being monitored.	List of points based on configured DIs.	N/A
Point 2 Description	A detailed and localized description of the selected Source Point Two. Read Only	Not editable	Assigned IED point Description

Single Point Mapping Settings

Table 6.231: Single Point Mapping Settings

Setting	Description	Range	Default
Info Object Settings			
Info Object Name	The name of the information object as entered on the New Info Object window. Read only.	N/A	N/A
Starting Address	The starting address of this entry.	1 to 16777215	none
Interrogation Group	The interrogation group used for reporting this information object.	Not Used Group 1 ... Group 16	Not Used
Interrogation Response	Specify whether to include this information object in a general interrogation response.	Include Exclude	Include
Report Class	Specify if spontaneous events for this object are reported as class 1 or class 2 messages. Applies to unbalanced mode and spontaneous events only.	Class 1 Class 2	Class 1
Periodic Update Mode	The type of periodic updating	Not Used Background Scan	Not Used
Periodic Update Interval	The time (in seconds) between periodic reports. Used only if Periodic Update Mode is not set to *Not Used*.	0 to 65535	0
Periodic Report On Power Up	Specify if periodic reporting (if enabled) should begin immediately upon startup.	Disabled Enabled	Disabled
Time Tag	The type of time tag to use.	None With Time Tag With CP56 Time Tag	None
Per-Point Settings			
Address	The address of the entity.	1 to 16777215	none
IED	System Point Identifier. Consists of Home Directory of the selected DI point from the Point Picker. Read only.	N/A	System Assigned Identifier
Point Description	A detailed and localized text description of the selected point in the Binary Input map. Read only.	Up to 128 Unicode characters Not editable	Assigned IED point description
Point Reference	A short identifier of the selected DI point from the Point Picker. Read Only.	Up to 66 ASCII Characters Not editable	Assigned point name
Invert	Select if the value of the mapped points should be inverted.	True or False	False

Step Position Mapping Settings

Table 6.232: Step Position Mapping Settings

Setting	Description	Range	Default
Info Object Settings			
Info Object Name	The name of the information object as entered on the New Info Object window. Read only.	N/A	N/A
Starting Address	The starting address of this entry.	1 to 16777215	none
Interrogation Group	The interrogation group used for reporting this information object.	Not Used Group 1 ... Group 16	Not Used
Interrogation Response	Specify whether to include this information object in a general interrogation response.	Include Exclude	Include
Report Class	Specify if spontaneous events for this object are reported as class 1 or class 2 messages. Applies to unbalanced mode and spontaneous events only.	Class 1 Class 2	Class 1
Periodic Update Mode	The type of periodic updating	Not Used Background Scan	Not Used
Periodic Update Interval	The time (in seconds) between periodic reports. Used only if Periodic Update Mode is not set to *Not Used*.	1 to 255	60
Periodic Report On Power Up	Specify if periodic reporting (if enabled) should begin immediately upon startup.	Disabled Enabled	Disabled
Time Tag	The type of time tag to use.	None With Time Tag With CP56 Time Tag	None
Per-Point Settings			
Address	The address of the entity.	1 to 16777215	none
IED	System Point Identifier. Indicates the Home Directory of the selected AI point from the Point Picker. Read only.	N/A	System Assigned Identifier
Point ID	Shows the Point ID of the selected AI point from the Digital Input Point map. Read only.	Not editable	System Generated Point Identifier
Point Reference	A short identifier of the selected AI point from the Point Picker. Read Only.	Up to 66 ASCII Characters Not editable	Assigned point name
Point Description	A detailed and localized text description of the selected point in the Analog Input map. Read only.	Up to 128 characters Not editable	Assigned IED point description
Multiplier	Scale factor of the point (**m** of formula **mx + b**)	Full range of 64-bit Float	1.0
Offset	Scale factor of the point (**b** of formula **mx + b**)	Full range of 64-bit Float	0.0

Setting	Description	Range	Default
Polarity	Specifies whether a negative analog value is valid.	Bipolar Value Unipolar Value	Bipolar Value
Threshold	The initial minimum change in the analog input value that is required to produce a spontaneous report or event.	0 to 100,000,000	5
High Limit	The initial high limit that is required for an analog input value to exceed to produce an event.	-1.0E+12 to 1.0E+12	1.0E+12
Low Limit	The initial low limit that is required for an analog input value to exceed to produce an event.	-1.0E+12 to 1.0E+12	-1.0E+12

- IEC 60870-5+104 Server

Configuring Server Applications

Server Configuration Overview

User can customize the MCP to transmit the necessary data from Intelligent Electronic Devices (IEDs) to master stations. Server applications in the MCP allow the MCP to retrieve selected data from event queues and the real-time database and send the data to the master station according to the how the SCADA protocol is defined.

The MCP configuration tool supports configuration of protocol-specific object references, scaling factors, and user-defined names for various objects configured for transmission. Where applicable, user can also configure additional device-level settings (for the same protocol) at the same time.

» To configure server applications for use on the MCP, perform the following typical tasks:

1. Create MCP server map file for each master station and protocol type.
2. Select data points and assign point indices.
3. Configure protocol-specific settings.
4. Configure scaling and enable reverse scaling (reverse effect of scaling applied by a client application).
5. Set up serial and network master connections.
6. Configure protocol-specific settings for each master connection.
7. Save the configuration file.
8. Run the configuration file in the MCP by committing the changes.

DNP3 Serial Master Stations

The Distributed Network Protocol (DNP3) supports communication with one or more devices over dedicated serial links, as well as over Ethernet. The MCP supports communications to DNP3 devices using the DNP3 client application. It collects the point values from the devices based on the protocol and device settings and stores them in the system point database.

The DNP3 protocol is highly configurable. You have the option of configuring the way the DNP3 client application on the MCP behaves by modifying the DNP3 protocol settings or use the default configuration settings.

The following settings are used when configuring a DNP3 Master Station. If a Modem connection is used, refer to the additional settings defined in Dial-up Modem Settings.

DNP3 Master Stations

Table 6.233: DNP3 Master Stations

Setting	Description	Range	Default
Name	Text description to identify the master station being connected to.	1 to 32 ASCII characters	MASTER*X*
MCP Address	Unique DNP3 address of the server application instance.	0 to 65519	*X*
Map File	Name of the Client map file to be used with the specific device.	List of users configured client map files.	N/A
Application Parameters	Select the application parameters defining this connection. The default parameters can be used, or a custom configuration can be created. Refer to DNP3 Server Application Parameters and the DNP3 Master Stations Application Parameters.	Use Default Create New...	Use Default
Auto Start	Indicates if the client application automatically starts when the configuration is changed and reloaded or when the MCP re-boots.	Disabled Enabled	Enabled

DNP3 Master Stations Application Parameters

Table 6.234: DNP3 Master Stations Application Parameters

Setting	Description	Range	Default
Basic			
Max Application Retry	Number of times to resend an unconfirmed application message before taking a degraded timeout.	0 to 300	2
Application Timeout	Number of milliseconds the DNP server waits for the remote station to confirm an application message before resending it.	1 to 120,000	6,000
Datalink Confirmation Bitmask	Defines when the slave should request remote station confirmation of a data link message.	0 - Never 1 - Multi-fragment only 2 - Event only 3 - Event or Multi-fragment 4 - IIN only 5 - IIN or Multi-fragment 6 - Event or IIN 7 - Event, IIN or Multi-fragment 8 - Always	0 - Never
Datalink Max Retry	Maximum number of times to send an unconfirmed datalink message before taking a degraded timeout.	0 to 300	2
Datalink Timeout	Number of milliseconds to wait for a remote-station datalink confirmation before resending it.	1 to 120,000	1,000

Setting	Description	Range	Default
Primary Address	DNP3 Master Station address.	0 to 65,519	1
Degraded Timeout	Number of milliseconds the application delays between retry cycles when seeking confirmation of an application message.	1 to 7,200,000	5,000
Transmission Fragment Size	Maximum size of an unsolicited application message or response message fragment, minimum of 249 bytes.	249 to 2,048	2, 048
Communication Timeout	This timeout (in seconds) is used with the CommStatus Indication pseudo point. A value of zero disables the CommStatus Indication feature. Enter Value > { [Application Timeout + (Application Timeout * Max Application Retry)] + [Data-Link Timeout + (Data-Link Timeout * Data-Link Max Retry)] }/1000, otherwise minimum value will be used. The CommStatus pseudo point changes to zero if it does not receive any message from the master station within the configured timeout.	0 to 86,400 seconds (1 day)	0 to 86,400 seconds (1 day)
Unsolicited Class 1 Mode	Enable/disable unsolicited message support from class 1 events: True = Enable unsolicited message support False = Disable unsolicited message support	True False	
Unsolicited Class 2 Mode	Enable/disable unsolicited message support from class 2 events: True = Enable unsolicited message support False = Disable unsolicited message support	True False	
Unsolicited Class 3 Mode	Enable/disable unsolicited message support from class 3 events: True = Enable unsolicited message support False = Disable unsolicited message support	True False	
Unsolicited Poll Frequency	Frequency in milliseconds at which the application checks for unreported data.	1 to 120,000 milliseconds	1 to 120,000 milliseconds
Select Timeout	Number of seconds to wait for an operate request before cancelling the select operation.	0.01 to 65,535 seconds	0.01 to 65,535 seconds
Time Zone	This option allows you to configure a custom time zone offset which is applied to messages received through this application. By default, the timestamps of messages received through the DNPDPA are in UTC time.	One of listed Time Zones and geographic locations	UTC
Startup Event Suppress Interval	Duration for which DNP DPA does not report quality events to Master Station.	0 to 600 seconds	20 seconds

Setting	Description	Range	Default
IIN Time Sync Frequency	The Frequency (in minutes) at which Need Time Sync IIn is sent to the master station. A configured value of: -1 Never sends "Need Time Sync IIN"; Rejects Time Sync Requests sent from Master. 0 Sends the "Need Time Sync IIN" only during Stat-up; Accepts Time Sync Requests sent from Master. 1 to 1446 Sends the "Need Time Sync IIN" every configured interval; Accepts Time Sync Requests send from Master	-1 0 1 to 1446	0
Advanced			
Application Confirmation Bitmask	Defines when the slave should request remote-station confirmation of an application message.	0 - Never 1 - Multi-fragment only 2 - Event only 3 - Event or Multi-fragment 4 - IIN only 5 - IIN or Multi-fragment 6 - Event or IIN 7 - Event, IIN or Multi-fragment 8 - Always	7 - Event, IIN or Multi-fragment
Internal Indication Confirm	Define whether local-station indications require confirmation on change in status.	None Buffer Overflow	Buffer Overflow
Reboot On Cold Start	Reboot the MCP when a cold restart is received from the master: True = Enable cold restart False = Disable cold restart	True False	False
Response Fragment Size	Maximum size of a solicited application message fragment.	249 to 2,048 bytes	2,048 bytes
Report Comm Failure As Offline	Report MCP data points as Offline if MCP COMM FAILED quality attribute is set. True = Report communications failure False = Do not report communications failure	True False	True
Unsolicited Data	Define what type of unsolicited message is reported to the remote station.	Indications Only Events and Indications	Events and Indications
Unsolicited Startup	Define the unsolicited startup message.	Indications Only Events and Indications	Events and Indications
Buffer Overflow Policy	Policy on how to handle buffer overflow.	Discard Newest Discard Oldest	Discard Newest

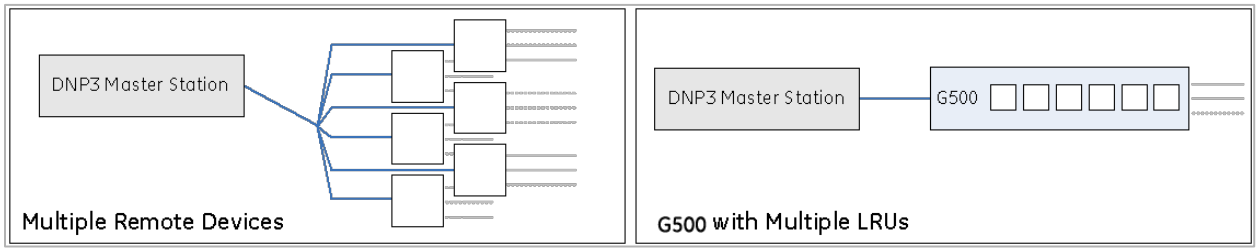
Setting	Description	Range	Default
Internal Buffer Location	Location of unreported events collected from Event Queues. **NOTE**: The MCP NVRAM only supports one instance of a DPA in an entire system configured to use NVRAM. However, additional DPAs can be configured with the Internal Buffer Location parameter set to RAM.	RAM NVRAM	RAM
Internal Event Buffer Capacity	Maximum number of events that can be stored in the internal buffer.	512 to 16384 events (in increments of 256)	16384 events
Max Class 1 Events	Maximum number of class 1 events that can be buffered.	512 to 16384 events (in increments of 256) Up to Capacity	Up to Capacity
Max Class 2 Events	Maximum number of class 2 events that can be buffered.	512 to 16384 events (in increments of 256) Up to Capacity	Up to Capacity
Max Class 3 Events	Maximum number of class 3 events that can be buffered.	512 to 16384 events (in increments of 256) Up to Capacity	Up to Capacity
Broadcast on Both Ports	Indicates whether to either: True = broadcast on both Primary and backup ports False = not to broadcast.	True False	False
Disable Online/Offline Quality Change Event	Enable or disable the reporting of DNPDPA Quality Change Events to the Master station when the point quality changes from Online to Offline or from Offline to Online: True = DNPDPA Quality Change Events are reported. False = DNPDPA Quality Change Events are not reported.	True False	False
Default Binary Input Event Time Type	Indicates which time type (absolute or relative) the DPA reports in response to an event poll with variation 0 or a Class poll.	Relative Absolute	Relative Absolute

Multiple Logical Remote Units (LRU)

You can configure multiple logical remote units on a single or redundant serial connection. This allows a remote DNP3 master station to communicate with multiple logical remote units within a physical MCP unit using a single serial link. You can use multiple LRU functionality to test a system configuration without needing to connect to multiple physical devices.

Multiple LRU Overview

Figure 6.4: Multiple LRU Overview

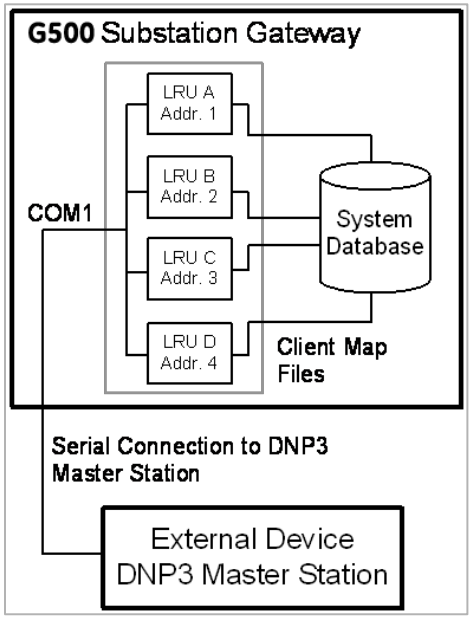


To add an LRU to communicate over a serial link with a DNP3 Master Station, click the **Add** button under *Configuration Parameters* and configure the row.

In the example below, a DNP3 Master Station is configured on serial port 1 of the MCP. Under *Configuration Parameters*, four rows are added and configured as follows:

Name	MCP Address	Map File	Application Parameters	Auto Start
LRU A	1	LRUA.xml	Use Default	☐
LRU B	2	LRUB.xml	Use Default	☐
LRU C	3	LRUC.xml	Use Default	☐
LRU D	4	LRUD.xml	Use Default	☐

Figure 6.5 Example Remote LRU Configuration



In this example, the DNP3 master station can connect to each of the four LRUs through the serial connection (COM1). Each LRU has a unique DNP address so that they can be communicated with independently. Each LRU can reference the same or different server map file. If the same server map file is referenced by multiple LRUs, each of these LRUs will serve the same data to the remote DNP3 master station.

DNP3 Server Application Parameters

Regular and advanced DNP3 server settings are available under the **Application Parameters** field.

DNP3 Server Communication Settings - Regular

Table 6.235: DNP3 Server Communication Settings - Regular

Setting	Description	Range	Default
Application Retry	Number of times the DNP3 resends an unconfirmed application message before taking a degraded timeout.	0 to 300	2
Application Timeout	Time (in milliseconds) the DNP3 waits for the remote station to confirm an application message before re-sending it. Set the value much higher for a dial-up modem connection, i.e. 60000.	1 to 120000	6000
Data Link Confirm	Defines when the DNP3 requests remote-station confirmation of a data link message.	0 - Never 1 - Multi-fragment only 2 - Event only 3 - Event or Multi-fragment 4 - IIN only 5 - IIN or Multi-fragment 6 - Event or IIN 7 - Event, IIN or Multi-fragment 8 - Always	Never
Data Link Retry	Number of times the DNP3 Server resends an unconfirmed data link message before taking a degraded timeout.	0 to 300	2
Data Link Timeout	Time (in milliseconds) the DNP3 Server waits for remote-station confirmation of a data link message before re-sending it. Set the value higher for a dial-up modem connection, i.e. 60000.	1 to 120000	1000
Initial Master Address	DNP3 Server master station address	0 to 65519	100
Degraded Timeout	Time (in milliseconds) the DNP3 Server delays between retry cycles when seeking confirmation of an application message.	1 to 7200000	5000
EventTimeType	Indicates which time type (absolute or relative) the DPA reports in response to an event poll with variation 0 or a Class poll.	Absolute Relative	Absolute
Transmission Fragment Size	Maximum size (in bytes) of an unsolicited application message or response message fragment (minimum is 249 bytes).	249 to 2048	2048
IIN Time Sync Frequency	The Frequency (in minutes) at which Need Time Sync IIn is sent to the master station. A configured value of: -1 Never sends "Need Time Sync IIN"; Rejects Time Sync Requests sent from Master. 0 Sends the "Need Time Sync IIN" only during Stat-up; Accepts Time Sync Requests sent from Master. 1 to 1446 Sends the "Need Time Sync IIN" every configured interval; Accepts Time Sync Requests send from Master	-1 0 1 to 1446	0

Setting	Description	Range	Default
Communication Timeout	This timeout (in seconds) is used with the CommStatus Indication pseudo point. A value of zero disables the CommStatus Indication feature. Enter Value > { [Application Timeout + (Application Timeout * Max Application Retry)] + [Data-Link Timeout + (Data-Link Timeout * Data-Link Max Retry)] }/1000, otherwise minimum value will be used. The CommStatus pseudo point value changes to zero if it does not receive a message from the master station within the configured timeout.		
Unsolicited Mode Class 1	Flag that enables or disables DNP3 Server unsolicited message support for class 1 events		
Unsolicited Mode Class 2	Flag that enables or disables DNP3 Server unsolicited message support for class 2 events		
Unsolicited Mode Class 3	Flag that enables or disables DNP3 Server unsolicited message support for class 3 events		
Unsolicited Poll Frequency	Frequency (in milliseconds) at which the DNP3 Server checks for unreported data.		
Select Timeout	Time (in seconds) the DNP3 Server waits for an operate request before canceling the select.		
Time Offset	Time offset (in minutes) from UTC. For example, for Eastern Standard Time, specify *–300*, which means UTC minus 5 hours. Specify only if the Master Station does not use UTC within DNP3 messages. DNP3 requires the time base to be UTC, but non-compliant Master Stations may use local time.		
Accept Any Master	If set to True, the DNP3 sever responds to any master that connects it. The Master address in this case is used only for sending a destination address in the initial unsolicited messages. If set to false, the DNP3 server only responds to the configured DNP3 Master.	True False	False

The advanced settings listed in the table below are for adjustment by experienced system engineering personnel and project engineers deploying the product in a specified configuration. Typically, these settings should not require modification.

DNP3 Server Communication Settings - Advanced

Table 6.236: DNP3 Server Communication Settings - Advanced

Setting	Description	Range	Default
Application Confirm	Defines when the DNP3 Server requests remote-station confirmation of an application message.	0 - Never 1 - Multi-fragment only 2 - Event only 3 - Event or Multi-fragment 4 - IIN only 5 - IIN or Multi-fragment 6 - Event or IIN 7 - Event, IIN or Multi-fragment 8 - Always	Event, IIN or Multi-fragment
Internal Indication Confirm	Indicates whether local-station indications require confirmation on change in status.	Buffer Overflow None	Buffer Overflow
Reboot On Cold Start	Reboot the MCP upon receiving a cold restart from the Master Station.	True False	True
Response Fragment Size	Maximum size of a solicited application message fragment (minimum is 249 bytes).	249 to 2048	2048
Report Comm-Failed As Offline	Determines if a MCP Data Point must be reported as Offline to the Master Station when the MCP COMM-FAILED quality attribute is set.	True False	True
Unsolicited Data	What information the DNP3 Server sends to the remote station in unsolicited messages.	Events and indications Indications only	Events and indications
Unsolicited Startup	Defines what data the DNP3 Server sends in the initial unsolicited startup message.	Events and indications Indications only	Indications only
Buffer Overflow Policy	Indicates whether the DNP3 Server discards newest or oldest event when a class event queue overflow occurs.	Discard Newest Discard Oldest	Discard Oldest
Internal Buffer Location	Specifies how to store the unreported events collected from Event Queues. **NOTE**: The MCP NVRAM only supports one instance of a DPA in an entire system configured to use NVRAM. However, additional DPAs can be configured with the Internal Buffer Location parameter set to RAM.	RAM NVRAM	RAM
Internal Event Buffer Capacity	Number of events that can be contained in the Internal buffer of the DNP3 Server.	512, 1024, 2048, 4096, 8192, 16384	2048
Max Class 1 Events	Maximum number of Class 1 Events that can be buffered. This can either be "Up to Capacity", or a Number. If a Number is entered, the sum Max. Lengths for all Class Queues cannot exceed the Internal Event Buffer Capacity.	512, 1024, 2048, 4096, 8192, 16384, Up to Capacity	Up to Capacity

Setting	Description	Range	Default
Max Class 2 Events	Maximum number of Class 2 Events that can be buffered. This can either be "Up to Capacity", or a Number. If a Number is entered, the sum Max. Lengths for all Class Queues cannot exceed the Internal Event Buffer Capacity.	512, 1024, 2048, 4096, 8192, 16384, Up to Capacity	Up to Capacity
Max Class 3 Events	Maximum number of Class 3 Events that can be buffered. This can either be "Up to Capacity", or a Number. If a Number is entered, the sum Max. Lengths for all Class Queues cannot exceed the Internal Event Buffer Capacity.	512, 1024, 2048, 4096, 8192, 16384, Up to Capacity	Up to Capacity
Broadcast on both ports	When enabled, all unsolicited events and poll responses are sent simultaneously on both the Primary and backup serial ports.	True False	False
Disable Online/Offline Quality Change Event	If this parameter is set to True, DNPDPA disables Quality change events being reported to the Master station when quality of the mapped points changes from Online to Offline and Vice-Versa.	False True	False

IEC 60870-5-101 Master Station

The following settings are used when configuring an IEC 60870-5-101 Master Station connection.

IEC 60870-5-101 Master Station Settings

Table 6.237: IEC 60870-5-101 Master Station Settings

Setting	Description	Range	Default
Transmission Mode	The link transmission mode used by the application. **NOTE**: Backup ports are not supported on *Balanced* mode.	Balanced Unbalanced	Unbalanced
Link Address Size	The number of octets used for the link address of the LRU.	1 or 2	1
LRU Name	The name of the LRU/master station connection	1 to 32 ASCII characters	MASTER*x*
Common Address of ASDU Size	The number of octets used for the common address of ASDU for the LRU.	1 or 2	1
Common Address of ASDU	The Common Address of ASDU for the LRU.	1 to 254 [1 octet size] 1 to 65534 [2 octet size]	1
Link Address	The Primary link address of the LRU.	0 to 65535	1
Backup Port Link Address	This is Backup port link address of the LRU, which is available when the Backup port is configured.	0 to 65535	Not Used (-1)
Map File	Name of the server map file to be used with the specific LRU.	List of users configured server map files.	N/A

Application Parameters	Select the application parameters defining this connection. The default parameters can be used, or a custom configuration can be created. Refer to *IEC 60870-5-101 Master Station Application Settings*.	Use Default List of user-customized application configuration files	Use Default
Auto Start	Indicates if the server application automatically starts when the configuration is changed and reloaded or when the MCP re-boots.	Disabled Enabled	Disabled

IEC 60870-5-101 Master Station Application

IEC 60870-5-101 settings are available under the **Application Parameters** field for Master Stations.

IEC 60870-5-101 Master Station Application Settings

Table 6.238: IEC 60870-5-101 Master Station Application Settings

Setting	Description	Range	Default
Application Tab			
Info Object Address Length	The number of octets used by the LRU for information object addresses. **NOTE**: For multiple LRUs on the same serial channel, only the first LRU's setting is used for this parameter.	1, 2, or 3	2
Time Mode	Specifies if the master station can set or use the main MCP and/or local LRU time.	Set main/use main time Set local/use local time Set local/use main time	Set main/use main time
Time Sync Timeout	The maximum allowed time (in seconds) between time synchronization attempts from the IEC 60870-5-101/104 master station or other time source before time tagged data is reported as invalid by the LRU. Set to "0" for the time tags to never reported as invalid by the LRU, except the mapped points quality flags indicate time invalid.	0 to 86400	900
Control Select Timeout	The maximum allowed time (in seconds) between the control select and the control execute commands (for digital and analog output points) from the IEC 60870-5-101/104 master station.	0.01 to 60.0	5.0
Double Point Valid Time	The minimum time (in seconds) that both digital input points must be stable before an ON/OFF state is reported. **NOTE:** The value of this property only applies when the corresponding parameters of a double point information object are specified as undefined. Not used when set to 0.	0 to 65535	500

Setting	Description	Range	Default
Double Point Suppress Time	The minimum time (in seconds) that both digital input points must be stable before an indeterminate state is reported. NOTE: The value of this property only applies when the corresponding parameters of a double point information object are specified as undefined. Not used when set to 0.	0 to 65535	1000
LRU Event Buffer Size	The number of events (non-time-tagged, time-tagged, and hour update objects) that are buffered by this LRU.	50 to 65535	255
LRU Event Buffer Location	The location where unreported events that are collected from event queues are stored. **NOTE**: The MCP NVRAM only supports one instance of a DPA in an entire system configured to use NVRAM. However, additional DPAs can be configured with the LRU Event Buffer Location parameter set to RAM.	RAM NVRAM	RAM
Event Buffer Overflow Policy	Specify whether the newest or oldest events are discarded when the server event buffer is filled.	Discard Newest Discard Oldest	Discard Newest
Event Buffer Low Threshold	A percent value of the total event buffer. When the amount of available buffer space drops below this threshold, a server event buffer low indication is reported by the application.	10 to 100	20
DI Cancels Select	Specify whether digital output select requests are automatically cancelled when any digital input changes are detected.	Enabled Disabled	Disabled
Buffer AI	Specify whether analog input changes (spontaneous, periodic, background scan) are buffered for reporting. When this is enabled, the LRU reports each analog change separately. For example, if an analog input point exceeds the threshold 3 times before the LRU is polled for data in unbalanced mode, the LRU reports all 3 value changes. If this feature is disabled, the LRU reports only the most recent value.	Enabled Disabled	Disabled
Zero Threshold Reporting	Specify how the LRU should treat a zero value for the Threshold configuration parameter for an analog input. If this setting is enabled, setting the threshold configuration parameter of an analog input point to zero (i.e. 0.0) spontaneously reports all changes for the point. If disabled, setting the Threshold configuration parameter of an analog input point to zero disables spontaneous reporting for the point.	Enabled Disabled	Disabled

Setting	Description	Range	Default
Time Tagging	When to report time-tag data. If configured as *Not on Interrogations*, the LRU reports a time tag only for spontaneous, periodic/cyclic, or background scan causes of transmission (that is, the LRU suppresses time tag for interrogated data). If configured as Always, the LRU reports time tag for all causes of transmission.	Not on Interrogations Always	Not on Interrogations
Clear Statistics	Specify if the application should reset all LRU statistics to zero at startup.	Enabled Disabled	Disabled
Comm Log Mode	The logging mode for all I/O communications traffic with the LRU.	Disabled ASCII Hex ASCII and Hex	Hex
Number of Files Supported	The number of information object addresses reserved for file transfer. Not used when set to 0.	0 to 128	0
Time to Live	The time (in seconds) a queued control command is to be treated as active in the system. If the configured value is 0, the RTDB setting is used.	0.0 to 60.0	0.0
Cause of TX Length	The number of octets used for the Cause of Transmission field. **NOTE**: For multiple LRUs on the same serial channel, only the first LRU's setting is used for this parameter.	1 or 2	1
Broadcast on both ports	When enabled, all unsolicited events and poll responses are sent simultaneously on both the Primary and backup serial ports. **NOTE**: For multiple LRUs on the same serial channel, only the first LRU's setting is used for this parameter.	True False	False
Time Zone	This option allows you to configure a custom time zone offset which is applied to messages received through this application. By default, the timestamps of messages received through the IEC 60870-101 server applications are in UTC time. **NOTE**: For multiple LRUs on the same serial channel, only the first LRU's Time Zone is used for this parameter.	One of listed Time Zones and geographic locations	UTC
Unbalanced Serial Link Tab			
Max ASDU Frame Length	The maximum length (in octets) of non-background messages (excluding framing overhead). **NOTE**: For multiple LRUs on the same serial channel, only the first LRU's setting is used for this parameter.	24 to 255	255

Setting	Description	Range	Default
Extra Frame Timeout	The time (in milliseconds) that the application adds to the frame timeout calculation. **NOTE**: For multiple LRUs on the same serial channel, only the first LRU's setting is used for this parameter.	0 to 65535	150
Single Char Acknowledge	Specify if the application should respond to the master station with a single character acknowledgement message. **NOTE**: For multiple LRUs on the same serial channel, only the first LRU's setting is used for this parameter.	Enabled Disabled	Disabled
Comm Fail Timeout	The maximum allowed time (in seconds) for when there is no available connection in the STARTDT state (that is, no communication from the master station) before the application assumes communications have failed. Not used when set to 0. **NOTE**: For multiple LRUs on the same serial channel, only the first LRU's setting is used for this parameter.	0 to 86400	30
File Transfer Report Class	The report class to use when sending file transfer related PDU. Used in unbalanced mode only. **NOTE**: For multiple LRUs on the same serial channel, only the first LRU's setting is used for this parameter.	Class 1 Class 2	Class 2
Balanced Serial Link Tab			
Max ASDU Frame Length	The maximum length (in octets) of non-background messages (excluding framing overhead). **NOTE**: For multiple LRUs on the same serial channel, only the first LRU's setting is used for this parameter.	24 to 255	255
Extra Frame Timeout	The time (in milliseconds) that the application adds to the frame timeout calculation. **NOTE**: For multiple LRUs on the same serial channel, only the first LRU's setting is used for this parameter.	0 to 65535	150
Single Char Acknowledgement	Specify if the application should respond to the master station with a single character acknowledgement message. **NOTE**: For multiple LRUs on the same serial channel, only the first LRU's setting is used for this parameter.	Enabled Disabled	Disabled
Transmit Retries	The maximum number of transmission retries when no acknowledgement is received from the master station before the application assumes communications has failed. **NOTE**: For multiple LRUs on the same serial channel, only the first LRU's setting is used for this parameter.	0 to 255	1

Setting	Description	Range	Default
Extra Response Timeout	The time (in milliseconds) that the application adds to the frame timeout calculation. **NOTE**: For multiple LRUs on the same serial channel, only the first LRU's setting is used for this parameter.	0 to 65535	200
Inter Frame Gap	The minimum idle time (in milliseconds) between frames transmitted by the application. **NOTE**: For multiple LRUs on the same serial channel, only the first LRU's setting is used for this parameter.	0 to 1000	0
Holding Time	The maximum delay (in milliseconds) of reporting spontaneous data changes to the master station after the data is available for transmission.	0.1 to 500000.0	0.2
Retry Time	The interval (in seconds) between LRU attempts to resend messages held in its buffer after previous failed transmissions. **NOTE**: For multiple LRUs on the same serial channel, only the first LRU's setting is used for this parameter.	0.1 to 86400.0	5.0

Modbus Serial Master Station

The following settings are used when configuring a Modbus Master Station.

Modbus Master Station Settings

Table 6.239: Modbus Master Station Settings

Setting	Description	Range	Default
Name	Text description to identify the master station being connected to.	1 to 32 ASCII characters	MASTER*X*
MCP Address	DNP3 address of the server application instance.	0 to 65519	X
Map File	Name of the Client map file to be used with the specific device.	List of users configured client map files.	N/A
Application Parameters	Select the application parameters defining this connection. The default parameters can be used, or a custom configuration can be created. Refer to *Modbus Server Application Settings*.	Use Default Create New...	Use Default
Auto Start	Indicates if the client application automatically starts when the configuration is changed and reloaded or when the MCP re-boots.	Disabled Enabled	Disabled

Modbus Server Application Settings

Modbus Server settings are available under the **Application Parameters** field.

Modbus Server Application Parameters

Table 6.240: Modbus Server Application Parameters

Setting	Description	Range	Default
NACK Offline Digitals	If enabled, the MCP is to NACK the offline coils upon receiving the *Force Single Coil* or *Force Multiple Coils* command with an Exception code 4 in the response. If disabled, the MCP reports the offline coil with the value OFF.	Yes No	No
NACK Offline Analogs	If enabled, the MCP is to NACK the offline registers upon receiving the *Preset Single Register* or *Preset Multiple Register* command with an Exception code 4 in the response. If disabled, the MCP reports the value of the offline registers as 0.	Yes No	No
Offline analog value	The value reported by points that are offline.	-32768 to 32767	0
Broadcast on both ports	When enabled, all unsolicited events and poll responses are sent simultaneously on both the Primary and backup serial ports.	True False	False

DNP3 Network Master Stations

The following settings are used when configuring a DNP3 master station connection.

DNP3 Master connection settings

Table 6.241: DNP3 Master Connection Settings

Setting	Description	Range	Default
Remote Connection Name	Text description to identify the master station associated with this serial connection.	1 to 32 ASCII characters	N/A
Map File	Name of the server map file to be used with the specific master.	List of users configured map files.	N/A
Auto Start	Indicates if the application automatically starts when the configuration is changed and reloaded or when the MCP re-boots.	Automatic Disabled	Automatic
MCP Address	DNP3 address of the server application instance.	0 to 65519	0
Transport Layer	Whether to use TCP or UDP network protocol.	TCP UDP	TCP
Network Port	The MCP port number on which the master station communicates.	0 to 65535	20001
Application Parameters	Select the application parameters defining this connection. The default parameters can be used, or a custom configuration can be created. Refer to *DNP3 Server Communication Settings - Regular* and *DNP3 Server Communication Settings - Advanced*.	Use Default Use Custom	Use Default
Permitted Remote Hosts	IP Addresses of master stations permitted to connect to the MCP. If all are set to *0.0.0.0*, all hosts can connect.	Up to 8 IP Addresses	0.0.0.0
Accept All Hosts	If checked, all hosts can connect.	Disabled Enabled	Disabled

IEC 60870-5-104 Master Station

The following settings are used when configuring an IEC 60870-5-104 Master Station connection.

IEC 60870-5-104 Master Station

Table 6.242: IEC 60870-5-104 Master Station

Setting	Description	Range	Default
Remote Connection Name	Text description to identify the master station associated with this serial connection.	1 to 32 ASCII characters	N/A
Map File	Name of the Server map file to be used with the specific master.	List of users configured client map files.	N/A
Auto Start	Indicates if the client application automatically starts when the configuration is changed and reloaded or when the MCP re-boots.	Automatic Disabled	Disabled
Common Address of ASDU	The device's common address of ASDU.	1 to 65534	1
Transport Layer	Whether to use TCP or UDP network protocol.	Non-editable	TCP
Network Port	The MCP port number on which the master station communicates.	0 to 65535	2404
Application Parameters	Select the application parameters defining this connection. The default parameters can be used, or a custom configuration can be created. Refer to *IEC 60870-5-104 Master Station Application Settings*.	Use Default Use Custom	Use Default
Accept All Hosts	If enabled, all remote hosts can connect.	Enabled Disabled	Disabled
Permitted Remote Hosts	IP Addresses of master stations permitted to connect to the MCP. If *Accept All Hosts* is enabled, these fields are disabled and ignored.	Up to 8 IP Addresses	0.0.0.0
Accept All Hosts	If checked, all hosts can connect.	Disabled Enabled	Disabled

IEC 60870-5-104 Master Station Application Settings

IEC 60870-5-104 settings are available under the Application Parameters field for Master Stations.

IEC 60870-5-104 Master Station Application Parameters

Table 6.243: IEC 60870-5-104 Master Station Application Parameters

Setting	Description	Range	Default
Application Tab			
Time Mode	Specifies if the master station can set or use the main MCP and/or local LRU time.	Set main/use main time Set local/use local time Set local/use main time	Set main/use main time

Setting	Description	Range	Default
Time Sync Timeout	The maximum allowed time (in seconds) between time synchronization attempts from the IEC 60870-5-101/104 master station or other time source before time tagged data is reported as invalid by the LRU. Set to "0" for the time tags to never reported as invalid by the LRU, except the mapped points quality flags indicate time invalid.	0 to 86400	900
Control Select Timeout	The maximum allowed time (in seconds) between the control select and the control execute commands (for digital and analog output points) from the IEC 60870-5-101/104 master station.	0.01 to 60.0	5.0
Double Point Valid Time	The minimum time (in seconds) that both digital input points must be stable before an ON/OFF state is reported. **NOTE**: The value of this property only applies when the corresponding parameters of a double point information object are specified as undefined. Not used when set to 0.	0 to 65535	500
Double Point Suppress Time	The minimum time (in seconds) that both digital input points must be stable before an indeterminate state is reported. **NOTE**: The value of this property only applies when the corresponding parameters of a double point information object are specified as undefined. Not used when set to 0.	0 to 65535	1000
LRU Event Buffer Size	The number of events (non-time-tagged, time-tagged, and hour update objects) that are buffered by this LRU.	50 to 65535	255
LRU Event Buffer Location	The location where unreported events that are collected from event queues are stored. **NOTE**: The MCP NVRAM only supports one instance of a DPA in an entire system configured to use NVRAM. However, additional DPAs can be configured with the LRU Event Buffer Location parameter set to RAM.	RAM NVRAM	RAM
Event Buffer Overflow Policy	Specify whether the newest or oldest events are discarded when the server event buffer is filled.	Discard Newest Discard Oldest	Discard Newest
Event Buffer Low Threshold	A percent value of the total event buffer. When the amount of available buffer space drops below this threshold, a server event buffer low indication is reported by the application.	10 to 100	20
DI Cancels Select	Specify whether digital output select requests are automatically cancelled when any digital input changes are detected.	Enabled Disabled	Disabled

Setting	Description	Range	Default
Buffer AI	Specify whether analog input changes (spontaneous, periodic, background scan) are buffered for reporting. When this is enabled, the LRU reports each analog change separately. For example, if an analog input point exceeds the threshold 3 times before the LRU is polled for data in unbalanced mode, the LRU reports all 3 value changes. If this feature is disabled, the LRU reports only the most recent value.	Enabled Disabled	Disabled
Zero Threshold Reporting	Specify how the LRU should treat a zero value for the Threshold configuration parameter for an analog input. If this setting is enabled, setting the threshold configuration parameter of an analog input point to zero (i.e. 0.0) spontaneously reports all changes for the point. If disabled, setting the Threshold configuration parameter of an analog input point to zero disables spontaneous reporting for the point.	Enabled Disabled	Disabled
Time Tagging	When to report time-tag data. If configured as *Not on Interrogations*, the LRU reports a time tag only for spontaneous, periodic/cyclic, or background scan causes of transmission (that is, the LRU suppresses time tag for interrogated data). If configured as Always, the LRU reports time tag for all causes of transmission.	Not on Interrogations Always	Not on Interrogations
Clear Statistics	Specify if the application should reset all LRU statistics to zero at startup.	Enabled Disabled	Disabled
Comm Log Mode	The logging mode for all I/O communications traffic with the LRU.	Disabled ASCII Hex ASCII and Hex	Hex
Number of Files Supported	The number of information object addresses reserved for file transfer. Not used when set to 0.	0 to 128	0
Time to Live	The time (in seconds) a queued control command is to be treated as active in the system. If the configured value is 0, the RTDB setting is used.	0.0 to 60.0	0.0
Holding Time	The maximum delay (in milliseconds) of reporting spontaneous data changes to the master station after the data is available for transmission.	0.1 to 500000.0	0.2
Control Time Window	The time range (in seconds) used to qualify a time-tagged request.	0.001 to 86400.0	1
Time Zone	This option allows you to configure a custom time zone offset which is applied to messages received through this application. By default, the timestamps of messages received through the IEC 60870-104 server applications are in UTC time.	One of listed Time Zones and geographic locations	UTC

Setting	Description	Range	Default
Network Tab			
Comm Fail Timeout	The maximum allowed time (in seconds) for when there is no available connection in the STARTDT state (that is, no communication from the master station) before the application assumes communications have failed. Not used when set to 0.	0 to 86400	30
Max TX Frames Before Ack	The maximum number of information frames that the application transmits before it must receive an acknowledgement message (value of **w**).	1 to 32,767	8
Max RX Frames Before Ack	The maximum number of information frames that the application receives before it must send an acknowledgement message (value of **k**).	1 to 32,767	12
Connect Timeout	The maximum time (in seconds) that the application waits for the TCP transport layer to establish a connection (value of **t0**).	1 to 255	30
Send Timeout	The maximum time (in seconds) that the application waits for an acknowledgement after sending a frame (value of **t1**).	1 to 255	15
No Data Timeout	The maximum time (in seconds) that the application waits before sending a supervisory acknowledgement (S) frame (value of **t2**).	1 to 255	10
Idle Timeout	The period during which no messages are received, in seconds, that the application allows pass before sending a test frame (value of **t3**).	1 to 255	20
Max APDU Frame Length	The maximum length (in octets) of APDU frames.	253	Not editable

Modbus TCP Master

The following settings are used when configuring a Modbus TCP master connection.

Modbus TCP Master connection settings

Table 6.244: Modbus TCP Master connection settings

Setting	Description	Range	Default
Remote Connection Name	Text description to identify the master station associated with this connection.	1 to 32 ASCII characters	N/A
Map File	Name of the Server map file to be used with the specific master.	List of users configured map files.	N/A
Auto Start	Indicates if the application automatically starts when the configuration is changed and reloaded or when the MCP re-boots.	Automatic Disabled	N/A
Gateway Address	Address of the server application instance.	0 to 65519	0
Transport Layer	Whether to use TCP or UDP network protocol. Only TCP is supported at this time.	TCP	TCP

Setting	Description	Range	Default
Network Port	The MCP port number on which the master station communicates.	0 to 65535	20001
Application Parameters	Select the application parameters defining this connection. The default parameters can be used, or a custom configuration can be created. Refer to *Modbus TCP Master Application Parameters*.	Use Default Use Custom	Use Default
Permitted Remote Hosts	IP Addresses of master stations permitted to connect to the MCP. If all are set to *0.0.0.0*, all hosts can connect.	Up to 8 IP Addresses	0.0.0.0
Accept All Hosts	If checked, all hosts can connect.	Disabled Enabled	Disabled

Modbus TCP Master Application Parameters

Modbus TCP master settings are available under the **Application Parameters** field.

Modbus TCP Master application parameters

Table 6.245: Modbus TCP Master application parameters

Setting	Description	Range	Default
NACK Offline Digitals	If enabled, the MCP is to NACK offline digital points upon receiving a command with an Exception code 4 in the response. If disabled, the MCP reports the offline point with the value OFF.	Yes No	No
NACK Offline Analogs	If enabled, the MCP is to NACK offline analog points upon receiving a command with an Exception code 4 in the response. If disabled, the MCP reports the offline point with the value OFF.	Yes No	No
Offline analog value	The value reported by points that are offline.	-32768 to 32767	0
Broadcast on both ports	When enabled, all unsolicited events and poll responses are sent simultaneously on both the Primary and backup ports.	True False	False

Build HMI One-Line Diagrams

This chapter contains the following sections and sub sections:

One-Line Viewer

View One Line Diagrams

One-Line Designer

One-Line Designer - Overview
Standard Toolbar
Stencil Panel
Designer Canvas
Property Panel

Object Configuration Settings

Data Source Configuration Settings

Executing One-Line Diagram Commands

One-Line Viewer

The One-Line (also referred to as the Single Line Diagram - SLD) Viewer displays:

- The main drawing (main.dra) by default.
- Simplified schematic diagrams during runtime that represent the interconnections in a substation, including devices and the real-time values and/or state of selected ports and points.

These custom-built diagrams are built using the following two types of objects from the MCP HMI library:

- Static objects that do not change during runtime. Examples of static objects are buttons, labels, lines and other shapes used to lay out the drawing.
- Dynamic objects that represent a data source and are updated continually as new information becomes available. Examples of dynamic objects are circuit breakers, switches, and value boxes. The source of the data can be the Real-Time Database, the Active Alarms (Digital Event Manager) application or other MCP resources.

The **One-Line Viewer** diagrams are designed and configured using the One-Line Designer.

The following related action can be performed: Issue a command

View One-Line Diagrams

The **One-Line Viewer** displays configured one-line diagrams.

» To view one-line diagrams:

- Click the **One-Line Viewer** button on the Power bar.

The pre-defined main one-line drawing displays.

One-Line Viewer toolbar

Table 6.246: One-Line Viewer Toolbar

Button	Name	Action	Keyboard Shortcut
	Home Screen	Return to the default diagram (*main.dra*)	CTRL + H
	Previous Screen	View the previous diagram (if navigation history is available)	CTRL + B
	Next Screen	View the next diagram (if navigation history is available)	CTRL + F
	Browse Screen	Open a diagram stored on the MCP	CTRL + O
	Animation (Play)	Refresh the currently displayed diagram and start (or restart) the continuous update of dynamic objects	*none*
	Animation (Stop)	Stop redrawing the diagram and stop the continuous updating of dynamic objects	*none*

Drawing tasks

» To display the current data quality status:

- Point to a dynamic object.

» To open the linked diagram (replaces page currently displayed):

- Click the diagram buttons.

» To open the Command Interface window for the object:

- Double-click a dynamic object with control/set-point functionality (for example, Circuit Breaker, Transformer, Button, Value Box).

» To access other functions:

- Right-click a dynamic object, if available, for the selected object:
  - Execute Control,
  - Execute Set Point,
  - Tag/Inhibit,
  - Local Force,
  - Acknowledge Alarm,
  - Acknowledge Alarm Group, or
  - Navigate to Active Alarm Page (according to alarm group or point group).

Executing One-Line Diagram Commands

You can execute the following commands from a One-Line Diagram:

- Acknowledge an Alarm
- Acknowledge an Alarm Group
- Analog Output Interface
- Analog Set-point Interface
- Digital Control Interface
- Digital Output Interface
- Local (Point) Force Interface
- Navigate to Active Alarm Page
- Raise/Lower Control Interface
- Tag/Inhibit Interface

One-Line Designer - Overview

The **One-Line Designer** is a specialized drawing tool for creating substation one-line diagrams and forms, such as a Digital Event Manager panel. The One-Line Designer is accessed from within the MCP Offline Configuration Tool (DS Agile Studio).

To start the one-line configuration tool:

- From DS Agile Studio, click the Configuration button on the Power bar.

You must have Supervisor or Administrator privileges to access the runtime configuration tool. Only one Supervisor user at a time can be logged in to perform configuration functions.

The **One-Line Designer** allows you to create a two-dimensional diagram of your electrical grid, which can be accessed by MCP users through the **One-Line Viewer**.

The One-Line Designer screen contains a toolbar and three windows:

Standard Toolbar	-	Save and open diagrams, modify the placement of objects, and change the way the Drawing Area appears.
Stencil Panel	-	Select from this list to create a new object
Designer Canvas	-	The window containing the one-line drawing. All drawing elements are created within this area.
Property Panel	-	This screen gives you access to all the parameters and configuration options for the currently selected object.

» To save a drawing:

- Click the **Save** button.
- Enter a filename.

» To open an existing drawing:

- Click the **Open** button.
- Select a file from the list.

» To clear the designer canvas to create a new drawing:

- Click the **New** button.

Tip: To make a drawing the default drawing that opens in the One-Line Viewer name it *main.dra*. This setting can be changed on the Global section of the Configuration > Systemwide page.

Standard Toolbar

The One-Line Designer is a tool that enables you to create specialized diagrams and forms, customized to your substation environment and viewable via the **One-Line Viewer**.

In addition to creating a diagram or schematic of your network, you can display real time readouts of the values of selected ports and points.

The standard toolbar provides tools to save and open diagrams, modify the placement of objects, and change the way the Drawing Area appears.

If you forget the function of a toolbar button, hover the mouse pointer over the button and a short description of the button's function is provided in the upper right of the display. A shortcut key combination is also shown that you can use to invoke the command.

Table 6.247: Standard Toolbar

Toolbar Button	Command	Keyboard Shortcut	Description
	New	Ctrl + N	Create a new OneLine Designer drawing.
	Open	Ctrl + O	Open an existing OneLine Designer drawing. Retrieve and edit any drawing that has been previously saved. When the Open a Diagram window appears, select the desired file name from the list and click the **Open** button.

Toolbar Button	Command	Keyboard Shortcut	Description
	Save	Ctrl + S	As with any application, it is imperative that you save your data in a regular and ongoing fashion. Click the **Save** Toolbar button. When the Save a Diagram window appears, enter a file name or select a file name, and then click the **Save** button. **NOTE:** If you want the drawing to be the default diagram (the one that is loaded when you use the One Line Viewer), then the filename must be *main.dra*. You can also set the default diagram on the **Systemwide** > **Runtime GUI** > **Global** configuration tab on the **Configuration** window.
	Refresh Symbols		Refresh a symbol imported into a drawing. **NOTE**: Refreshing taking effect only when the selected symbol file has same filename as the symbol imported into the drawing.
	Open Symbol		Open an existing symbol (drawing) file to edit. A symbol is useful when you have designed a drawing with a group of objects and want to reuse this drawing as a common symbol in multiple drawings.
	Save Symbol		Save opened drawing as a symbol or save opened symbol file. The saved symbol file can then be imported into drawings or other symbol files.
	Cut	Ctrl + X	Cut the currently selected object(s) from the screen to the clipboard.
	Copy	Ctrl + C	Copy the currently selected object(s) to the clipboard.
	Paste	Ctrl + V	Paste objects from the clipboard to the screen.
	Undo	Ctrl + U	Undo recently made changes to the workspace.
	Redo	Ctrl + D	Redo recently undone changes to the workspace.
	Align Left	Ctrl + L	Multiple objects may be aligned so that any of their four edges or two axes are in alignment and level along the grid no matter what their size. Buttons for each of the four edges and two axes are provided on the upper toolbar.
	Align Horizontal Center		
	Align Right	Ctrl + R	
	Align Top	Ctrl + T	
	Align Vertical Center		
	Align Bottom	Ctrl + B	
	Distribute Horizontally		Multiple objects may be distributed horizontally; the selected objects that are furthest to the left and right remain in place while the remaining selected objects are distributed evenly based on their centers.
	Distribute Vertically		Multiple objects may be distributed vertically, the top and bottom selected objects remain in place while the remaining selected objects are distributed evenly based on their centers.
	Make Width Same Size	Ctrl + W	Make multiple objects the same size on the horizontal plane.

Toolbar Button	Command	Keyboard Shortcut	Description
	Make Height Same Size	Ctrl + H	Make multiple objects the same size on the vertical plane.
	Make Both Same Size	Ctrl + E	Make multiple objects the same size on the horizontal and vertical planes.
	Bring to Front	Ctrl + F	Bring the selected object to appear in front of the other objects.
	Send to Back	Ctrl + K	Send the selected object to appear behind the other objects.
	Snap to Grid		Indicates that Snap To Grid is enabled. When enabled, a dragged and dropped object size snaps to the grid. Click to disable Snap to Grid.
			Indicates that Snap To Grid is disabled. When disabled, a dragged and dropped object size does not snap to the grid, the grid. Click to enable Snap to Grid.
			The grid size is selected, in the number pixels.

Stencil Panel

The **Stencil Panel** on the **One-Line Designer** page allows you to create drawing objects from a list of pre-defined object types.

To add an object to a drawing, click on an object from the Stencil Panel. Then, click and hold your left mouse button down on the Designer Canvas as you drag the cursor diagonally across the screen. When you release the mouse button, an object is drawn to fill the selected area.

Objects can be re-sized and customized according to their corresponding Property Panel attributes.

You cannot add new dynamic objects or change the runtime shapes of existing dynamic objects.

Drawing Objects

A general listing of the object types available is shown below. The shortcuts are activated once the Designer Canvas window has the focus.

Table 6.248: Drawing Objects

Icon	Name / Detailed Settings	Shortcut	Description
	Pointer	Alt + P	Click the Pointer tool, then click the cursor on an object to make it the active object. Confirm that the object is selected by observing a series of eight (8) boxes surrounding the object, located one to each corner and one to the middle of each edge. **NOTE:** Even in the case of rounded objects, such as circles, the highlight boxes are in a square configuration. Since a line is one-dimensional, there is space only for two highlight boxes, one on each end of the chosen line.
	Label / settings	Alt + B	The Label tool allows you to create a box designed specifically to insert text.
	Button / settings	Alt + Z	The Button tool allows you to create a button that performs an action when clicked.

Icon	Name / Detailed Settings	Shortcut	Description
	Alarm Box / settings	Alt + Y	Use this tool to create a box that changes color depending on the alarm status of a polled data source.
	Line / settings	Alt + L	Use this tool to create a one-dimensional line.
	Rectangle / settings	Alt + R	Use this tool to create a four-sided box of any size. You can modify the color of the border and the fill, the border type and thickness, and the URL Anchor for linking to another drawing.
	Polygon / settings	Alt + P	Use this tool to create a circle or a three-sided to ten-sided polygon of any size. You can modify the color of the border and the fill, the border type and thickness,
	Circle / settings	Alt + C	Use this tool to create a round object of any dimension. You can modify the color of the border and the fill, the border type and thickness, and the URL Anchor for linking to another drawing.
	Image / settings	Alt + I	This tool allows you to place an image on the drawing area, such as a scanned image of a piece of equipment or another specialized element not provided for in the default object types.
	Value Box / settings	Alt + V	A Value Box can contain any IED value that is being polled by the MCP.
	Circuit Breaker Box / settings	Alt + X	The CBBox object is designed to schematically represent a power system circuit breaker. The CBBox object accepts status inputs from 2 digital points (BitStrings).
	Transformer / settings	Alt + T	This object is a basic graphic representation of a transformer and has the same Property Value characteristics as a standard rectangle (except for the fill choice), including border color and type, and rotation. The URL Anchor is also available for linking to another drawing.
	Ground / settings	Alt + G	This object is a basic graphic representation of a ground and is limited to the same Property Value characteristics as a standard line, including border color and type. The URL Anchor is also available for linking to another drawing.
	Switch / settings	Alt + S	This object represents a switch in the substation configuration. As such, it has Property Values that can be drawn from existing equipment. You must assign the appropriate IEDname and the PointName for the switch. You also need to identify the correct Property Value for when the switch is closed (0 or 1) and apply the opposite value for the open position; note that the graphic configuration changes its appearance relative to the switch's condition.
	Capacitor / settings	Alt + A	This object is a basic graphic representation of a capacitor and has the same Property Value characteristics as a standard rectangle (except for the fill choice), including border color and type, and rotation. The URL Anchor is also available for linking to another drawing.
	Reactor / settings	Alt + E	This object is a basic graphic representation of a reactor and has the same Property Value characteristics as a standard rectangle (except for the fill choice), including border color and type, and rotation. The URL Anchor is also available for linking to another drawing.
	Range-Aware Line / settings	Alt + N	Use this tool to create a line that changes color depending on the value of a polled data source.

Icon	Name / Detailed Settings	Shortcut	Description
	Range-Aware Value Box / settings	Alt + O	Use this tool to create a value box that contains the value of that polled data source that changes color depending on the value.
	Range-Aware Chart / settings	Alt + H	Use this tool to create a bar chart that contains the value of a polled data source that changes color depending on the value.
	Data-Source Wizard	Alt + 0	Click this button to run the Data-Source Wizard. This wizard helps manage the data sources objects. If Create a new DataSource option is selected, the supported DataSource Types appear. Select the required DataSource Type and click **Next**. The wizard displays respective configuration window to create the DataSource object. If Modify existing DataSource option is selected, the supported DataSource Types appear. Upon Selecting the required DataSource Type, the existing DataSource objects under the selected DataSource Type appear. Select the required DataSource object to reconfigure its settings. If Delete existing DataSource option is selected, the supported DataSource Types appear. Upon selecting the required DataSource Type, the existing DataSource objects under the selected DataSource Type appear. Select the required DataSource object and click **Finish** to delete the selected DataSource object. **NOTE**: if a DataSource is referenced by one or more element(s), and DataSource is removed, the reference to DataSource from element(s) is automatically removed.
	Import Symbol	Alt + 1	Add the selected symbol file into the drawing or symbol currently being edited.

Designer Canvas

The **Designer Canvas** on the **One Line Designer** page is the workspace in which you can create and edit one-line drawings.

To build a drawing, click on an object from the **Stencil Panel**. Then, click and hold your left mouse button down as you drag the cursor diagonally across the Designer Canvas window. When you release the mouse button, an object is drawn to fill the selected area.

Drawing Tasks

Table 6.249: Drawing Tasks

To...	Do this...
Select item(s)	Click on the item with your left mouse button *or* click and hold your left mouse button down on an empty area of the screen and drag the cursor to encompass the items you want to select.
Select additional items	Click and drag across multiple objects. OR 1. Click on an object. 2. Right-click on additional objects.
Move an object	Select it and drag it to the desired location. A dotted outline of the object is shown as you move it to assist you in positioning.
To delete an object from the canvas	Select it and click your Delete key

To...	Do this...
To cut an object	Select it and press CTRL + X *or* Select it and press the **Cut** button.
To copy an object	Select it and press CTRL + C *or* Select it and press the **Copy** button.
To paste an object	Select it and press CTRL + V *or* Select it and press the **Paste** button.
To undo an action	Press CTRL + U *or* Click the **Undo** button.
To redo an action	Press CTRL + D *or* Click the **Redo** button.

Positioning and Sizing Objects

Table 6.250: Positioning and Sizing Objects

Icon	Description	Shortcut
	Align all selected objects to the left edge of the object that was selected first.	ALT + L
	Align all selected objects vertically to the center of the object that was selected first.	
	Align all selected objects to the right edge of the object that was selected first.	ALT + R
	Align all selected objects to the top edge of the object that was selected first.	ALT + T
	Align all selected objects horizontally to the center of the object that was selected first.	
	Align all selected objects to the bottom edge of the object that was selected first.	ALT + B
	The selected objects that are furthest to the left and right remain in place while the remaining selected objects are distributed evenly based on their centers.	
	The top and bottom selected objects remain in place while the remaining selected objects are distributed evenly based on their centers.	
	Set the width of all selected objects to the largest width from all selected objects.	ALT + W
	Set the height of all selected objects to the largest height from all selected objects.	ALT + H
	Set the height and width of all selected objects to the largest height and width from all selected objects.	ALT + E
	Move the selected object in front of all other objects.	ALT + F
	Move the selected object behind of all other objects.	ALT + K

Quality Attribute Symbols

Table 6.251: Quality Attribute Symbols

Symbol	Description
O	OFFLINE
Restart	RESTART
CX	COMM_LOST
R	REM_FORCE
CK	REF_CHECK
OR	CHATTER_OVERRANGE
OD	OLD_DATA
Test	TEST
Time Invalid	TIME_INVALID
?	QUESTIONABLE
X	INVALID
Remote Scan Inhibit	REM_SCAN_INHIBIT
OF	OVERFLOW
Remote Time	REMOTE_TIME

C	CONTROL_INHIBIT
A	ALARM_INHIBIT
S	SCAN_INHIBIT
T	TAG_FORCE
M	LOCAL_FORCE
2	SECONDARY_SRC
2x	SECONDARY_SRC_INVALID
2F	SECONDARY_SRC_FORCED
LC	LOCAL_CTRL_ACTIVE
RC	REMOTE_CTRL_ACTIVE
P	SUPPRESSED
Z	ZOMBIE

For more details regarding the Quality Attributes, please refer to the Quality Attributes section on page no. 116.

Property Panel

The **Property Panel** on the **One Line Designer** page displays all parameters associated with the object currently selected on the **Designer Canvas**. When multiple elements are selected, all common parameters are shown so that you can edit them at one time. By modifying the values shown in this window you can alter the behavior and appearance of the objects in your diagram.

» To modify object properties:

1. Select an object on the **Designer Canvas**.
2. On the **Property Panel**, double-click the **Value** field of the **Property Name** you want to modify.
3. Enter the new value, or if you see a drop-down list, select a pre-defined option.
4. Click anywhere outside of the field to activate your changes.

Object Configuration Settings

Property Panel - Object Tables

The Property Panel displays the properties associated with the currently selected object.

The One Line Designer Object types are:

- Alarm Box Object Settings
- Button Object Settings
- Capacitor Object Settings
- Circle Object Settings
- Circuit Breaker Box Object Settings
- Ground Object Settings
- Image Object Settings
- Label Object Settings
- Line Object Settings
- Range Aware Bar Chart Object Settings
- Range Aware Line Object Settings
- Range Aware Value Box Object Settings
- Reactor Object Settings
- Rectangle Object Settings

- Polygon Object Settings
- Switch Object Settings
- Transformer Object Settings
- Value Box Object Settings

Alarm Box Object Settings

The Alarm Box Object:

- Is a Dynamic Object that is associated with a single Alarm or Alarm Group Object.
- Appears with a color and text that indicates whether the alarm is in active or normal state.

Table 6.252: Alarm Box Object Settings

Setting	Description	Range	Default
Name	Name of the One Line Designer object.	Text	Alarmbox
X	X (horizontal) pixel position from the top left corner of the screen to the top left corner of the area used to display the object	0 to the Draw Panel width less the object width	0
Y	Y (vertical) pixel position from the top left corner of the screen to the top left corner of the area used to display the object	0 to the Draw Panel height less the object height	0
Border Type	Defines the type of border to display	One of No border, Symmetric borders, raised borders, Sunken borders, Outdent borders, Indent borders, Picture borders, Double raised, Double sunken, Bottom right borders, Top left borders	No border
Border Color	Defines the color to apply to the border around the perimeter of the display area of the object	Any 24-bit RGB color	Gray
Border Variant	Defines the width of the border to display	0 to 9	0
Border Multiplier	Defines the thickness of the border to display	One of None (x1), x2, x3, x4, x5, x6, x7, x8	None (x1)
Width	Pixel width of the rectangular area used to display the object	1 to the Draw Panel width	None
Height	Pixel height of the rectangular area used to display the object	1 to the Draw Panel height	None
Font Type	The type of font used to display text	One of SansSerif, Serif, Monospaced, DialogInput	SansSerif
Font Style	The font style to apply to the display of text	One of normal, bold, or italic	Normal
Font Size	The size of the font used to display text	1 to 100	11
Alignment	The horizontal alignment of the text within the object's display area	One of Left, Center, or Right	Left

Setting	Description	Range	Default
Vertical Alignment	The vertical alignment of the text within the object's display area	One of Bottom or Top	Top
Alternate Blink Color	The alternate color to apply to blinking element	Any 24-bit RGB color	White
Offline	An Offline alarm can be set to blink.	No Blink, Blink Text, Blink Border, Blink Background	No Blink
- Text	The text displayed for this alarm condition.	Any ASCII text.	Offline
- Text Color	The color of the alarm text.	See color selection window.	Black
- BG Color	The background color of the alarm text.	See color selection window.	Pink
Neutral	A Neutral alarm can be set to blink.	No Blink, Blink Text, Blink Border, Blink Background	No Blink
- Text	The text displayed for this alarm condition.	Any ASCII text.	Neutral
- Text Color	The color of the alarm text.	See color selection window.	Black
- BG Color	The background color of the alarm text.	See color selection window.	Green
Ack'd Alarm	An Acknowledged alarm can be set to blink.	No Blink, Blink Text, Blink Border, Blink Background	No Blink
- Text	The text displayed for this alarm condition.	Any ASCII text.	Ack'd Alarm
- Text Color	The color of the alarm text.	See color selection window.	Black
- BG Color	The background color of the alarm text.	See color selection window.	Pink
Alarm,No Ack	An alarm that has not been acknowledged can be set to blink.	No Blink, Blink Text, Blink Border, Blink Background	No Blink
- Text	The text displayed for this alarm condition.	Any ASCII text.	Alarm
- Text Color	The color of the alarm text.	See color selection window.	Black
- BG Color	The background color of the alarm text.	See color selection window.	Pink
Reset,No Ack	An alarm that has been reset, but has not been acknowledged, can be set to blink.	No Blink, Blink Text, Blink Border, Blink Background	No Blink
- Text	The text displayed for this alarm condition.	Any ASCII texts.	Reset
- Text Color	The color of the alarm text.	See color selection window.	Black
- BG Color	The background color of the alarm text.	See color selection window.	Green
Acknowledgement Action	Defines the user mouse action required to acknowledge an alarm box	One of Single Left Click, Double Left Click, Single Right Click, Double Right Click, or No Mouse Click	Double Left Click

Setting	Description	Range	Default
Navigation Action	Defines the user mouse action required to navigate to the active alarm page. If the alarm datasource mapped to an alarm group, the navigation action displays the mapped alarm group on the active alarm page; if a point is selected in the alarm datasource, navigation action displays the alarm group of the selected point on the active alarm page.	One of Single Left Click, Double Left Click, Single Right Click, Double Right Click, No Mouse Click	No Mouse Click
Data Source	Unique identifier for the data source required for the Alarm Box.	Select a data source	None
Quality Horizontal Alignment	The horizontal alignment of the quality display within the object's display area	One of Left, Center, Right	Center
Quality Vertical Alignment	The vertical alignment of the quality display within the object's display area	One of Bottom, Top	Bottom

Button Object Settings

The Button Object:

- Is a Static Object that displays text centered within a rectangular area.
- Performs the configured action when you left click the object.

Table 6.253: Alarm Box Object Settings

Setting	Description	Range	Default
Name	Name of the One Line Designer object.	Text	Button
X	X (horizontal) pixel position from the top left corner of the screen to the top left corner of the area used to display the object	0 to the Draw Panel width less the object width	0
Y	Y (vertical) pixel position from the top left corner of the screen to the top left corner of the area used to display the object	0 to the Draw Panel height less the object height	0
Border Type	Defines the type of border to display	One of No border, Symmetric borders, raised borders, Sunken borders, Outdent borders, Indent borders, Picture borders, double raised, Double sunken, Bottom right borders, Top left borders	0
Border Color	Defines the color to apply to the border around the perimeter of the display area of the object	Any 24-bit RGB Color	Grey

Setting	Description	Range	Default
Border Variant	Defines the width of the border to display	0 to 9	0
Border Multiplier	Defines the thickness of the border to display	One of None (x1), x2, x3, x4, x5, x6, x7, x8	None (x1)
Width	Pixel width of the rectangular area used to display the object	1 to the Draw Panel width	40
Height	Pixel height of the rectangular area used to display the object	1 to the Draw Panel height	20
Caption	Text for the object to display	Text	Button
Font Type	The type of font used to display text	One of SansSerif, Serif, Monospaced, DialogInput	SansSerif
Font Style	The font style to apply to the display of text	One of normal, bold, or italic	Normal
Font Size	The size of the font used to display text	1 to 100	11
Fore Color	The color to apply to text	Any 24-bit RGB Color	Black
Back Color	The color to apply to the background	Any 24-bit RGB Color	Grey
Action Type	Defines the action to occur when the user selects the button	One of: Open Analog Set Point Interface Open Digital Control Interface Open Raise/Lower Control Interface User Specified URL	None
Data Source	Unique identifier for the data source required for the Button object.	Select a data source	None
URL Action	Specifies whether to load the URL Address into the same window, or a new window.	Same or New	Same
URL Address	Specify a link from this object, to either a: URL address, or Oneline Designer drawing	Any valid URL address, or existing Oneline Designer drawing	None

Capacitor Object Settings

The Capacitor Object is a Static Object that displays a single vector image of a capacitor.

Table 6.254: Capacitor Object Settings

Setting	Description	Range	Default
Name	Name of the One Line Designer object.	Text	Capacitor
X	X (horizontal) pixel position from the top left corner of the screen to the top left corner of the area used to display the object	0 to the Draw Panel width less the object width	0

Setting	Description	Range	Default
Y	Y (vertical) pixel position from the top left corner of the screen to the top left corner of the area used to display the object	0 to the Draw Panel height less the object height	0
Border Type	Defines the type of border to display	One of No border, Symmetric borders, raised borders, Sunken borders, Outdent borders, Indent borders, Picture borders, double raised, Double sunken, Bottom right borders, Top left borders	0
Border Color	Defines the color to apply to the border around the perimeter of the display area of the object	Any 24-bit RGB Color	Gray
Border Variant	Defines the width of the border to display	0 to 9	0
Border Multiplier	Defines the thickness of the border to display	One of None (x1), x2, x3, x4, x5, x6, x7, x8	None (x1)
Width	Pixel width of the rectangular area used to display the object	1 to the Draw Panel width	32
Height	Pixel height of the rectangular area used to display the object	1 to the Draw Panel height	32
Back Color	The color to apply to the background	Any 24-bit RGB Color	Gray
Fore Color	The color to apply to text	Any 24-bit RGB Color	Black
Rotation	Angle of clockwise rotation (in degrees) to apply to the object	0,90,180,270	0
File Path	File path of alternate (non-default) image to display	Any existing server-side image file	None
URL Action	Specifies whether to load the URL Address into the same window, or a new window.	Same or New	Same
URL Address	Specify a link from this object, to either a: URL address, or Oneline Designer drawing	Any valid URL address, or existing Oneline Designer drawing	None

Circle Object Settings

The Circle Object is a Static Object that displays a single vector-based circle or ellipse.

Table 6.255: Circle Object Settings

Setting	Description	Range	Default
Name	Name of the One Line Designer object.	Text	Circle
X	X (horizontal) pixel position from the top left corner of the screen to the top left corner of the area used to display the object	0 to the Draw Panel width less the object width	0

Setting	Description	Range	Default
Y	Y (vertical) pixel position from the top left corner of the screen to the top left corner of the area used to display the object	0 to the Draw Panel height less the object height	0
Border Type	Defines the type of border to display	One of No border, Symmetric borders, raised borders, Sunken borders, Outdent borders, Indent borders, Picture borders, double raised, Double sunken, Bottom right borders, Top left borders	0
Border Color	Defines the color to apply to the border around the perimeter of the display area of the object	Any 24-bit RGB Color	Grey
Border Variant	Defines the width of the border to display	0 to 9	0
Border Multiplier	Defines the thickness of the border to display	One of None (x1), x2, x3, x4, x5, x6, x7, x8	None (x1)
Fill Color	Defines the color to apply to the inside of the object shape.	Any 24-bit RGB Color	Red
Width	Pixel width of the rectangular area used to display the object	1 to the Draw Panel width	12
Height	Pixel height of the rectangular area used to display the object	1 to the Draw Panel height	12
Back Color	The background color with which to fill the object	Any 24-bit RGB Color	Grey
URL Action	Specifies whether to load the URL Address into the same window, or a new window.	Same or New	Same
URL Address	Specify a link from this object, to either a: URL address, or Oneline Designer drawing	Any valid URL address, or existing Oneline Designer drawing	None

Circuit Breaker Box Object Settings

The Circuit Breaker Box Object is:

- A Dynamic Object that displays a single rectangular vector image.
- Color-coded to indicate the current state value from a Digital Status Object or Digital Control Object.

You can program the fill-colors of the breaker object, by setting colors to the following properties:

- FT_Color
- FF_Color
- TT_Color
- TF_Color

Based on the logic levels of the Digital Points selected, the fill color of the CBBox changes appropriately in the Run_Mode.

In the design mode, you can set the properties of Digital Input Value1 True State and Digital Input Value2 True State to 0 or 1 and verify that the fill color settings are satisfactory.

Table 6.256: Circuit Breaker Box Object Settings

Setting	Description	Range	Default
Name	Name of the One Line Designer object.	Text	Circuitbreakerbox
X	X (horizontal) pixel position from the top left corner of the screen to the top left corner of the area used to display the object	0 to the Draw Panel width less the object width	0
Y	Y (vertical) pixel position from the top left corner of the screen to the top left corner of the area used to display the object	0 to the Draw Panel height less the object height	0
Border Type	Defines the type of border to display	One of No border, Symmetric borders, raised borders, Sunken borders, Outdent borders, Indent borders, Picture borders, double raised, Double sunken, Bottom right borders, Top left borders	No border
Border Color	Defines the color to apply to the border around the perimeter of the display area of the object	Any 24-bit RGB Color	Gray
Border Variant	Defines the width of the border to display	0 to 9	0
Border Multiplier	Defines the thickness of the border to display	One of None (x1), x2, x3, x4, x5, x6, x7, x8	None (x1)
Width	Pixel width of the rectangular area used to display the object	1 to the Draw Panel width	12
Height	Pixel height of the rectangular area used to display the object	1 to the Draw Panel height	12
Digital Input Value 1 True State	Digital input 1 value to associate with a “true” state	0 or 1	1
Digital Input Value 2 True State	Digital input 2 value to associate with a “true” state	0 or 1	1
FF_Color	The background color to display when the digital input 1 value (high or leftmost bit) corresponds to the false state, and the digital input 2 value (low or rightmost bit) corresponds to the false state.	Any 24-bit RGB Color	Gray
FT_Color	The background color to display when the digital input 1 value (high or leftmost bit) corresponds to the false state, and the digital input 2 value (low or rightmost bit) corresponds to the true state.	Any 24-bit RGB Color	Gray

Setting	Description	Range	Default
TF Color	The background color to display when the digital input 1 value (high or leftmost bit) corresponds to the true state, and the digital input 2 value (low or rightmost bit) corresponds to the false state.	Any 24-bit RGB Color	Gray
TT_Color	The background color to display when the digital input 1 value (high or leftmost bit) corresponds to the true state, and the digital input 2 value (low or rightmost bit) corresponds to the true state.	Any 24-bit RGB Color	Gray
Data Source	Unique identifier for the data source required for the Circuit Breaker Box object. When the Digital Control datasource type is selected and Feedback Enabled is set to True, then the displayed Circuit Breaker background color changes, based upon feedback from Digital Input points. When the Digital Control datasource type is selected and Feedback Enabled is set to False, then the displayed Circuit Breaker background color does not change when the Digital Output point value changes.	Select a data source	None
Quality Horizontal Alignment	The horizontal alignment of the quality display within the object's display area	One of Left, Center, Right	Center
Quality Vertical Alignment	The vertical alignment of the quality display within the object's display area	One of Bottom, Top	Bottom

Ground Object Settings

The Ground Object is a Static Object that displays a single vector image of an electrical ground.

Table 6.257: Ground Object Settings

Setting	Description	Range	Default
Name	Name of the One Line Designer object.	Text	Ground
X	X (horizontal) pixel position from the top left corner of the screen to the top left corner of the area used to display the object	0 to the Draw Panel width less the object width	0
Y	Y (vertical) pixel position from the top left corner of the screen to the top left corner of the area used to display the object	0 to the Draw Panel height less the object height	0

Setting	Description	Range	Default
Border Type	Defines the type of border to display	One of No border, Symmetric borders, raised borders, Sunken borders, Outdent borders, Indent borders, Picture borders, double raised, Double sunken, Bottom right borders, Top left borders	No border
Border Color	Defines the color to apply to the border around the perimeter of the display area of the object	Any 24-bit RGB Color	Gray
Border Variant	Defines the width of the border to display	0 to 9	0
Border Multiplier	Defines the thickness of the border to display	One of None (x1), x2, x3, x4, x5, x6, x7, x8	None (x1)
Width	Pixel width of the rectangular area used to display the object	1 to the Draw Panel width	20
Height	Pixel height of the rectangular area used to display the object	1 to the Draw Panel height	20
Back Color	The color to apply to the background	Any 24-bit RGB Color	Gray
Fore Color	The color to apply to text	Any 24-bit RGB Color	Black
Rotation	Angle of clockwise rotation (in degrees) to apply to the image	0,90,180,270	0
URL Action	Specifies whether to load the URL Address into the same window, or a new window.	Same or New	Same
URL Address	Specify a link from this object, to either a: URL address, or Oneline Designer drawing	Any valid URL address, or existing Oneline Designer drawing	None

Image Object Settings

The Image Object is a Static Object that displays a single image.

When an image object is initially added, the image field is empty.

» To assign an image:

1. Double-click the value box for the property labeled File Path.
   Result: A list of all images contained in the MCP's mnt/usr/Configure/Images directory appears.
2. Select the desired Image File and click **OK**.
3. If required, change the border color, border type, and URL Anchor for linking to another drawing.
4. If required, the image can be rotated 90 or 180 degrees.

Table 6.258: Image Object Settings

Setting	Description	Range	Default
Name	Name of the One Line Designer object.	Text	Image
X	X (horizontal) pixel position from the top left corner of the screen to the top left corner of the area used to display the object	0 to the Draw Panel width less the object width	0

Setting	Description	Range	Default
Y	Y (vertical) pixel position from the top left corner of the screen to the top left corner of the area used to display the object	0 to the Draw Panel height less the object height	0
Border Type	Defines the type of border to display	One of No border, Symmetric borders, raised borders, Sunken borders, Outdent borders, Indent borders, Picture borders, double raised, Double sunken, Bottom right borders, Top left borders	No border
Border Color	Defines the color to apply to the border around the perimeter of the display area of the object	Any 24-bit RGB Color	Gray
Border Variant	Defines the width of the border to display	0 to 9	0
Border Multiplier	Defines the thickness of the border to display	One of None (x1), x2, x3, x4, x5, x6, x7, x8	None (x1)
Width	Pixel width of the rectangular area used to display the object	1 to the Draw Panel width	12
Height	Pixel height of the rectangular area used to display the object	1 to the Draw Panel height	12
Rotation	Angle of clockwise rotation (in degrees) to apply to the image	0,90,180,270	0
File Path	File path of image to display	Any existing server-side image file	Built In
URL Action	Specifies whether to load the URL Address into the same window, or a new window.	Same or New	Same
URL Address	Specify a link from this object, to either a: URL address, or Oneline Designer drawing	Any valid URL address, or existing Oneline Designer drawing	None
Data Source	Unique identifier for the data source required for the image. If no datasource is specified, the image is still shown.	Select a data source	None
Data Source Attribute	Attribute for the data source. See Quality Attributes.	One of: Value, Offline, Restart, Communications Lost, Remotely Forced, Reference Check, Chatter/Over-range, Old Data, Test, Time Invalid, Questionable, Invalid, Remote Scan Inhibit, Overflow, Remote Time, Control Inhibit, Alarm Inhibit, Scan Inhibit, Tagged, Manually Forced, Secondary Source, Secondary Invalid, Secondary Forced, Local Control Active, Remote Control Active, Suppressed	Value

Setting	Description	Range	Default
Show Image When	If data source is mapped, the image is shown/hidden in the following circumstances. If Value is selected in Data Source Attribute, mapped Digital Status Data Source Feedback Size 2 State: • Only show the image when the specified Data Source Value (0 or 1) is equal to 2 states 0 or 1(00, 01). • Data Source Feedback Size 4 State: • Only show image when the specified Data Source Value (0,1,2,3) is equal to 4 states 0, 1, 2 or 3(00, 01, 10, 11) If any quality attribute is selected, except Value in Data Source Attribute: • Show image when the select quality attribute is set. • Show image when the select quality attribute is not set	If Value is selected for Data Source Attribute: • Digital Status Data Source with Feedback Size 2 State: 2 State: 00 2 State: 01 • Digital Status Data Source with Feedback Size 4 State: 4 State: 00 4 State: 01 4 State: 10 4 State: 11 If Value is not selected for Data Source Attribute: Selected Quality Set Selected Quality Not Set	1

Label Object Settings

The Label Object is a Static Object that displays a caption within a rectangular area.

In the One Line Designer, the user first creates the box; text is added or altered by using the **Properties** display located on the right side of the screen. Clicking into the Values entry labeled *Caption* allows you to enter the desired text. Other properties that may be changed include the alignment of the text inside the box (limited to left-aligned or centered), the color of the text (*Foreground*), the box's background color (*Background*) and the box's border color. Double-clicking in the *Font* value enables you to change both the font type and size.

The Label object, as well as other objects, contains the capability to link to another drawing created by the One-Line Designer and stored on the MCP In the **Property Pane** box, click the mouse into the value column associated with the URL Anchor choice. To link to another drawing, type in the correct file name (note that all One-Line Designer files are saved with a dot extension of .dra, which must be typed as part of the filename). Likewise, to link to a web page, type in the full web address. In this manner, you may create complex interlinked drawings. This enables someone viewing a file to go to a different diagram that may provide further detail. Should a user want to know more readings associated with a device, clicking on that device image launches him or her into another diagram that has been created to provide such magnified detail.

Table 6.259: Label Object Settings

Setting	Description	Range	Default
Name	Name of the One Line Designer object.	Text	Label
X	X (horizontal) pixel position from the top left corner of the screen to the top left corner of the area used to display the object	0 to the Draw Panel width less the object width	0

Setting	Description	Range	Default
Y	Y (vertical) pixel position from the top left corner of the screen to the top left corner of the area used to display the object	0 to the Draw Panel height less the object height	0
Border Type	Defines the type of border to display	One of No border, Symmetric borders, raised borders, Sunken borders, Outdent borders, Indent borders, Picture borders, double raised, Double sunken, Bottom right borders, Top left borders	No border
Border Color	Defines the color to apply to the border around the perimeter of the display area of the object	Any 24-bit RGB Color	Gray
Border Variant	Defines the width of the border to display	0 to 9	0
Border Multiplier	Defines the thickness of the border to display	One of None (x1), x2, x3, x4, x5, x6, x7, x8	None (x1)
Caption	Text for the object to display	Text	Label
Width	Pixel width of the rectangular area used to display the object	1 to the Draw Panel width	32
Height	Pixel height of the rectangular area used to display the object	1 to the Draw Panel height	12
Foreground	The color to apply to text	Any 24-bit RGB Color	Black
Background	The color to apply to the background	Any 24-bit RGB Color	White
Text Horizontal Alignment	The horizontal alignment of the text within the object's display area	One of Left, Center, or Right	Left
Font Type	The type of font used to display text	One of SansSerif, Serif, Monospaced, DialogInput	SansSerif
Font Style	The font style to apply to the display of text	One of normal, bold, or italic	Normal
Font Size	The size of the font used to display text	1 to 100	9
URL Action	Specifies whether to load the URL Address into the same window, or a new window.	Same or New	Same
URL Address	Specify a link from this object, to either a: URL address, or Oneline Designer drawing	Any valid URL address, or existing Oneline Designer drawing	None

Line Object Settings

The Line Object is a Static Object that displays a single line.

Table 6.260: Line Object Settings

Setting	Description	Range	Default
Name	Name of the One Line Designer object.	Text	Line
X1	X (horizontal) pixel position from the top left corner of the screen to the top left corner of the start point of the line	0 to the Draw Panel width	0

Setting	Description	Range	Default
Y1	Y (vertical) pixel position from the top left corner of the screen to the top left corner of the start point of the line	0 to the Draw Panel height	0
X2	X (horizontal) pixel position from the top left corner of the screen to the top left corner of the end point of the line	0 to the Draw Panel width	0
Y2	Y (vertical) pixel position from the top left corner of the screen to the top left corner of the end point of the line	0 to the Draw Panel height	0
Width	Defines the pixel width of the line	1 to 100	1
Color	Defines the color to apply to the line	Any 24-bit RGB color	Black
Line Type	Defines the type of line to draw	One of Solid, Dotted, or Dashed	Solid
Arrow	Defines the type of arrowhead to apply to the line at the X1, Y2 position (start of line) and/or the X2, Y2 position (end of line)	One of No Arrow, Start Arrow, End Arrow, or Both Start and End Arrows	No Arrow
Data Source	Unique identifier for the data source required for the Line.	Select a data source	None

Range Aware Bar Chart Object Settings

The Range Aware Bar Object is a Dynamic Object that highlights a percentage of a rectangular area based on the:

- Real time value of the configured Analog Status or
- Accumulator Status Object divided by the configured Bar Scaling Value.

Table 6.261: Range Aware Bar Chart Object Settings

Setting	Description	Range	Default
Name	Name of the One Line Designer object.	Text	Rangeawarebar
X	X (horizontal) pixel position from the top left corner of the screen to the top left corner of the area used to display the object	0 to the Draw Panel width less the object width	0
Y	Y (vertical) pixel position from the top left corner of the screen to the top left corner of the area used to display the object	0 to the Draw Panel height less the object height	0
Border Type	Defines the type of border to display	One of No border, Symmetric borders, raised borders, Sunken borders, Outdent borders, Indent borders, Picture borders, double raised, Double sunken, Bottom right borders, Top left borders	No border

Setting	Description	Range	Default
Border Color	Defines the color to apply to the border around the perimeter of the display area of the object	Any 24-bit RGB Color	Gray
Border Variant	Defines the width of the border to display	0 to 9	0
Border Multiplier	Defines the thickness of the border to display	One of None (x1), x2, x3, x4, x5, x6, x7, x8	None (x1)
Width	Pixel width of the rectangular area used to display the object	1 to the Draw Panel width	32
Height	Pixel height of the rectangular area used to display the object	1 to the Draw Panel height	32
Font Type	The type of font used to display the scaling value as text	One of SansSerif, Serif, Monospaced, DialogInput	SansSerif
Font Style	The font style to apply to the display of the scaling value as text	One of normal, bold, or italic	Normal
Font Size	The size of the font used to display the scaling value as text	1 to 100	11
Foreground Color	The color to apply to scaling value displayed as text	Any 24-bit RGB Color	Black
Background Color	The color to apply to the background, non-highlighted area of the bar chart.	Any 24-bit RGB Color	Red
High Color	The color to apply to the highlighted area, but only when the real-time value exceeds the configured High Value.	Any 24-bit RGB Color	Red
Low Color	The color to apply to the highlighted area, but only when the real-time value is less than or equal to the configured High Value.	Any 24-bit RGB Color	Red
High Value	The value, which when exceeded by the real-time value, results the highlighted area of the bar chart being displayed in the High Color, and which when the real-time value is less than or equal to, results in the highlighted area of the bar chart being displayed in the Low Color.	Any 64-bit floating point value	0.0
Scale Value	The value by which the real-time values are divided to calculate a full-scale percentage that determines the height of the bar during run-time.	Any 64-bit floating point value	1.0

Setting	Description	Range	Default
Fill Direction	Fill direction defines the way the highlighted area is drawn: If set to bottom, the highlighted area rises vertically upwards, being filled from its bottom edge upwards ending at a horizontal line that corresponds to the percentage of the real-time value as compared to the configured bar scaling value. If set to top, the highlighted area rises vertically downwards, being filled from its top edge downwards ending at a horizontal line that corresponds to the percentage of the real-time value as compared to the configured bar scaling value. If set to left, the highlighted area rises horizontally to the right, being filled from its left edge to the right ending at a vertical line that corresponds to the percentage of the real-time value as compared to the configured bar scaling value. If set to right, the highlighted area rises horizontally to the left, being filled from its right edge to the left ending at a vertical line that corresponds to the percentage of the real-time value as compared to the configured bar scaling value.	One of Top, Bottom, Left, or Right	Bottom
Data Source	Unique identifier for the data source required for the Range Aware Bar Chart.	Select a data source	None
URL Action	Specifies whether to load the URL Address into the same window, or a new window.	Same or New	Same
URL Address	Specify a link from this object, to either a: URL address, or Oneline Designer drawing	Any valid URL address, or existing Oneline Designer drawing	None
Quality Horizontal Alignment	The horizontal alignment of the quality display within the object's display area	One of Left, Center, Right	Center
Quality Vertical Alignment	The vertical alignment of the quality display within the object's display area	One of Bottom, Top	Bottom

Range Aware Line Object Settings

The Range Aware Line Object is a Dynamic Object that displays a color representing the summation of run-time values from three configured Analog Status Objects.

Table 6.262: Range Aware Line Object Settings

Setting	Description	Range	Default
Name	Name of the One Line Designer object.	Text	Rangeawareline
X1	X (horizontal) pixel position from the top left corner of the screen to the top left corner of the start point of the line	0 to the Draw Panel width	0
Y1	Y (vertical) pixel position from the top left corner of the screen to the top left corner of the start point of the line	0 to the Draw Panel height	0
X2	X (horizontal) pixel position from the top left corner of the screen to the top left corner of the end point of the line	0 to the Draw Panel width	0
Y2	Y (vertical) pixel position from the top left corner of the screen to the top left corner of the end point of the line	0 to the Draw Panel height	0
Width	Defines the pixel width of the line	1 to 100	1
Line Type	Defines the type of line to draw	One of Solid, Dotted, or Dashed	Solid
Arrow	Defines the type of arrowhead to apply to the line at the X1, Y2 position (start of line) and/or the X2, Y2 position (end of line)	One of No Arrow, Start Arrow, End Arrow, or Both Start and End Arrows	No Arrow
Very Low Value	The value, which when the real-time value is lower, results in the line being drawn with the Very Low Color. **NOTE**: Very Low Value <= Low Value < High Value <= Very High Value.	Any 64-bit floating point value	0.0
Low Value	The value, which when the real-time value is lower, but higher than or equal to the Very Low Value, results in the line being drawn with the Low Color. **NOTE**: Very Low Value <= Low Value < High Value <= Very High Value.	Any 64-bit floating point value	0.0
High Value	The value, which when the real-time value is the same or lower, but higher than or equal to the Low Value, results in the line being drawn with the Normal Color. Also, the value, which when the real-time value is higher, but less than or equal to the Very High Value, results in the line being drawn with the High Color. **NOTE**: Very Low Value <= Low Value < High Value <= Very High Value.	Any 64-bit floating point value	0.0
Very High Value	The value, which when the real-time value is the higher, results in the line being drawn with the Very High Color. **NOTE**: Very Low Value <= Low Value < High Value <= Very High Value.	Any 64-bit floating point value	0.0

Setting	Description	Range	Default
Low Color	The color to apply to the line, but only when the summation of the three Analog Status values exceeds the configured Very Low Value and is less than the Low Value.	Any 24-bit RGB Color	Black
Very Low Color	The color to apply to the line, but only when the summation of the three Analog Status values is less than or equal to the Very Low Value.	Any 24-bit RGB Color	Black
Normal Color	The color to apply to the line, but only when the summation of the three Analog Status values is greater than or equal to the configured Low Value and is less than or equal to the High Value.	Any 24-bit RGB Color	Black
High Color	The color to apply to the line, but only when the summation of the three Analog Status values exceeds the configured High Value and is less than or equal to the Very High Value.	Any 24-bit RGB Color	Black
Very High Color	The color to apply to the line, but only when the summation of the three Analog Status values exceeds the configured Very High Value.	Any 24-bit RGB Color	Black
Data Source 1	Unique identifier for the data source required for the Range Aware Line.	Select a data source	None
Data Source 2	Unique identifier for the data source required for the Range Aware Line.	Select a data source	None
Data Source 3	Unique identifier for the data source required for the Range Aware Line.	Select a data source	None
Quality Horizontal Alignment	The horizontal alignment of the quality display within the object's display area	One of Left, Center, Right	Center
Quality Vertical Alignment	The vertical alignment of the quality display within the object's display area	One of Bottom, Top	Bottom

Range Aware Value Box Object Settings

The Range Aware Value Box Object is a Dynamic Object that displays the current value and Quality Attributes of an Analog Status Object or Accumulator Status Object.

Table 6.263: Range Aware Value Box Object Settings

Setting	Description	Range	Default
Name	Name of the One Line Designer object.	Text	Rangeawarevaluebox
X	X (horizontal) pixel position from the top left corner of the screen to the top left corner of the area used to display the object	0 to the Draw Panel width less the object width	0
Y	Y (vertical) pixel position from the top left corner of the screen to the top left corner of the area used to display the object	0 to the Draw Panel height less the object height	0

Setting	Description	Range	Default
Border Type	Defines the type of border to display	One of No border, Symmetric borders, raised borders, Sunken borders, Outdent borders, Indent borders, Picture borders, double raised, Double sunken, Bottom right borders, Top left borders	No border
Border Color	Defines the color to apply to the border around the perimeter of the display area of the object	Any 24-bit RGB Color	Gray
Border Variant	Defines the width of the border to display	0 to 9	0
Border Multiplier	Defines the thickness of the border to display	One of None (x1), x2, x3, x4, x5, x6, x7, x8	None (x1)
Width	Pixel width of the rectangular area used to display the object	1 to the Draw Panel width	32
Height	Pixel height of the rectangular area used to display the object	1 to the Draw Panel height	12
Alignment	The horizontal alignment of the value displayed as text within the object's display area	One of Left, Center, or Right	Left
Font Type	The type of font used to display value as text	One of SansSerif, Serif, Monospaced, DialogInput	SansSerif
Font Style	The font style to apply to the display of the value as text	One of normal, bold, or italic	Normal
Font Size	The size of the font used to display value as text	1 to 100	11
Fore Color	The color to apply to the value displayed as text	Any 24-bit RGB Color	Black
High Value	The value, which when the real-time value is higher, results in the background being displayed with the High Color.	Any 64-bit floating point value	0.0
Low Value	The value, which when the real-time value is lower, results in the background being displayed with the Low Color.	Any 64-bit floating point value	0.0
High Color	The color to apply to the background, but only when the real-time value exceeds the configured High Value.	Any 24-bit RGB Color	Red
Low Color	The color to apply to the background, but only when the real-time value is less than the configured Low Value.	Any 24-bit RGB Color	Red

Setting	Description	Range	Default
Mid Color	The color to apply to the background, but only when the real-time value is greater than or equal to the configured Low Value and is less than or equal to the configured High Value.	Any 24-bit RGB Color	Red
Data Source	Unique identifier for the data source required for the Range Aware Value Box.	Select a data source	None
Quality Horizontal Alignment	The horizontal alignment of the quality display within the object's display area	One of Left, Center, Right	Center
Quality Vertical Alignment	The vertical alignment of the quality display within the object's display area	One of Bottom, Top	Bottom

Reactor Object Settings

The Reactor Object is a Static Object that displays a single vector image of a reactor, as positioned by the One Line Designer.

Table 6.264: Reactor Object Settings

Setting	Description	Range	Default
Name	Name of the One Line Designer object.	Text	Reactor
X	X (horizontal) pixel position from the top left corner of the screen to the top left corner of the area used to display the object	0 to the Draw Panel width less the object width	0
Y	Y (vertical) pixel position from the top left corner of the screen to the top left corner of the area used to display the object	0 to the Draw Panel height less the object height	0
Border Type	Defines the type of border to display	One of No border, Symmetric borders, raised borders, Sunken borders, Outdent borders, Indent borders, Picture borders, double raised, Double sunken, Bottom right borders, Top left borders	No border
Border Color	Defines the color to apply to the border around the perimeter of the display area of the object	Any 24-bit RGB Color	Gray
Border Variant	Defines the width of the border to display	0 to 9	0
Border Multiplier	Defines the thickness of the border to display	One of None (x1), x2, x3, x4, x5, x6, x7, x8	None (x1)
Width	Pixel width of the rectangular area used to display the object	1 to the Draw Panel width	32
Height	Pixel height of the rectangular area used to display the object	1 to the Draw Panel height	32
Back Color	The color to apply to the background	Any 24-bit RGB Color	Gray
Fore Color	The color to apply to the value displayed as text	Any 24-bit RGB Color	Black

Rotation	Angle of clockwise rotation (in degrees) to apply to the image	0,90,180,270	0
URL Action	Specifies whether to load the URL Address into the same window, or a new window.	Same or New	Same
URL Address	Specify a link from this object, to either a: URL address, or Oneline Designer drawing	Any valid URL address, or existing Oneline Designer drawing	None

Rectangle Object Settings

The Rectangle Object is a Static Object that displays a single rectangle, as positioned by the One Line Designer.

Table 6.265: Rectangle Object Settings

Setting	Description	Range	Default
Name	Name of the One Line Designer object.	Text	Rectangle
X	X (horizontal) pixel position from the top left corner of the screen to the top left corner of the area used to display the object	0 to the Draw Panel width less the object width	0
Y	Y (vertical) pixel position from the top left corner of the screen to the top left corner of the area used to display the object	0 to the Draw Panel height less the object height	0
Border Type	Defines the type of border to display	One of No border, Symmetric borders, raised borders, Sunken borders, Outdent borders, Indent borders, Picture borders, double raised, Double sunken, Bottom right borders, Top left borders	No border
Border Color	Defines the color to apply to the border around the perimeter of the display area of the object	Any 24-bit RGB Color	Gray
Border Variant	Defines the width of the border to display	0 to 9	0
Border Multiplier	Defines the thickness of the border to display	One of None (x1), x2, x3, x4, x5, x6, x7, x8	None (x1)
Fill Color	Defines the color to apply to the inside of the object shape.	Any 24-bit RGB Color	Red
Width	Pixel width of the rectangular area used to display the object	1 to the Draw Panel width	12
Height	Pixel height of the rectangular area used to display the object	1 to the Draw Panel height	12
URL Action	Specifies whether to load the URL Address into the same window, or a new window.	Same or New	Same
URL Address	Specify a link from this object, to either a: URL address, or One line Designer drawing	Any valid URL address, or existing Oneline Designer drawing	None

Polygon Object Settings

The Polygon Object is a Static Object that displays a circle or a 3- to 10-sided polygon, as positioned by the One Line Designer.

Table 6.266: Polygon Object Settings

Setting	Description	Range	Default
Name	Name of the One Line Designer object.	Text	Polygon
X	X (horizontal) pixel position from the top left corner of the screen to the top left corner of the area used to display the object.	0 to the Draw Panel width less the object width	0
Y	Y (vertical) pixel position from the top left corner of the screen to the top left corner of the area used to display the object.	0 to the Draw Panel height less the object height	0
Border Type	Specify the type of border to display.	One of No border, Symmetric borders, raised borders, Sunken borders, Outdent borders, Indent borders, Picture borders, double raised, Double sunken, Bottom right borders, Top left borders	No border
Border Color	Specify the color to apply to the border around the perimeter of the screen area of the object.	Any 24-bit RGB Color	Gray
Border Variant	Specify the width of the border to display.	0 to 9	0
Border Multiplier	Specify the thickness of the border to appear.	One of None (x1), x2, x3, x4, x5, x6, x7, x8	None (x1)
Width	Pixel width of the rectangular area used to show the object.	1 to the Draw Panel width	12
Height	Pixel height of the rectangular area used to show the object.	1 to the Draw Panel height	12
Polygon Type	Specify the shape of the object; that is, a circle or a polygon.	0 = Circle 3 = Triangle 4 = Tetragon 5 = Pentagon 6 = Hexagon 7 = Heptagon 8 = Octagon 9 = Enneagon 10 = Decagon	Triangle (3)
Rotation	Angle of clockwise rotation (in degrees) to apply to the object	0,90,180,270	0
Digital Input Value1 True State	Digital input 1 value to associate with a “true” state	0 or 1	1
Digital Input Value2 True State	Digital input 2 value to associate with a “true” state	0 or 1	1

Setting	Description	Range	Default
FT_Color	The background color to display when the digital input 1 value (high or left-most bit) corresponds to the false state, and the digital input 2 value (low or right-most bit) corresponds to the true state.	Any 24-bit RGB Color	Dark pink
Data Source	Unique identifier for the data source required for the Polygon.	Select a data source	None
Data Source Attribute	Attribute for the data source. See Quality Attributes.	One of: Value, Offline, Restart, Communications Lost, Remotely Forced, Reference Check, Chatter/Over-range, Old Data, Test, Time Invalid, Questionable, Invalid, Remote Scan Inhibit, Overflow, Remote Time, Control Inhibit, Alarm Inhibit, Scan Inhibit, Tagged, Manually Forced, Secondary Source, Secondary Invalid, Secondary Forced, Local Control Active, Remote Control Active, Suppressed	Value
Quality Horizontal Alignment	The horizontal alignment of the quality display within the object's display area	One of: Left, Center, Right	Center
Quality Vertical Alignment	The vertical alignment of the quality display within the object's display area	One of: Bottom, Top	Bottom
Line Width	Line width in pixels	1 to 100	0
Line Data Source	Unique identifier for the data source required for the Line.	Select a data source	None
Line FT Color	The color to display when the digital input 1 value (high or left-most bit) corresponds to the false state, and the digital input 2 value (low or right-most bit) corresponds to the true state.	Any 24-bit RGB Color	Dark pink

Switch Object Settings

The Switch Object:

- Is a Dynamic Object that visually represents (with vector images) the real-time status of a substation switch.
- Monitors the values of one or two digital input points it is configured to reference from a Digital Status Object.
  For Digital Status Objects configured to reference:
  a) Two digital input points, the Switch Object is in one of four states at any given time: open, in transit, closed, or invalid.
  b) Only one digital input point, the Switch Object is in one of two states at any given time: open or closed.

The available switch object states are:

Table 6.267: Switch Object States

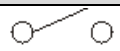
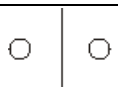
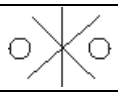
Setting	Description
Open	
Closed	
In Transit	
Invalid	

Table 6.268: Switch Object Settings

Setting	Description	Range	Default
Name	Name of the One Line Designer object.	Text	Switch
X	X (horizontal) pixel position from the top left corner of the screen to the top left corner of the area used to display the object	0 to the Draw Panel width less the object width	0
Y	Y (vertical) pixel position from the top left corner of the screen to the top left corner of the area used to display the object	0 to the Draw Panel height less the object height	0
Border Type	Defines the type of border to display	One of No border, Symmetric borders, raised borders, Sunken borders, Outdent borders, Indent borders, Picture borders, double raised, Double sunken, Bottom right borders, Top left borders	No border
Border Color	Defines the color to apply to the border around the perimeter of the display area of the object	Any 24-bit RGB Color	Gray
Border Variant	Defines the width of the border to display	0 to 9	0
Border Multiplier	Defines the thickness of the border to display	One of None (x1), x2, x3, x4, x5, x6, x7, x8	None (x1)
Width	Pixel width of the rectangular area used to display the object	1 to the Draw Panel width	32
Height	Pixel height of the rectangular area used to display the object	1 to the Draw Panel height	32
Back Color	The color to apply to the background	Any 24-bit RGB Color	Grey
Orientation	Whether to draw the switch state representations in a horizontal or vertical orientation	Horizontal or Vertical	Horizontal
Line Color	Defines the color with which to draw the lines that comprise the switch display	Any 24-bit RGB Color	Black
Line Width	Line width in pixels	1 to 100	1

Setting	Description	Range	Default
00 Switch State	If the Digital Status Object is a 4-State Digital Switch: The switch state to display when the digital input 1 value (high or leftmost bit) corresponds to the 0 state, and the digital input 2 value (low or rightmost bit) corresponds to the 0 state.	One of Open, Closed, In Transit, or Invalid	Open
01 Switch State	If the Digital Status Object is a 4-State Digital Switch: The switch state to display when the digital input 1 value (high or leftmost bit) corresponds to the 0 state, and the digital input 2 value (low or rightmost bit) corresponds to the 1 state.	One of Open, Closed, In Transit, or Invalid	Closed
10 Switch State	If the Digital Status Object is a 4-State Digital Switch: The switch state to display when the digital input 1 value (high or leftmost bit) corresponds to the 1 state, and the digital input 2 value (low or rightmost bit) corresponds to the 0 state.	One of Open, Closed, In Transit, or Invalid	Invalid
11 Switch State	If the Digital Status Object is a 4-State Digital Switch: The switch state to display when the digital input 1 value (high or leftmost bit) corresponds to the 1 state, and the digital input 2 value (low or rightmost bit) corresponds to the 1 state.	One of Open, Closed, In Transit, or Invalid	Invalid
URL Action	Specifies whether to load the URL Address into the same window, or a new window.	Same or New	Same
URL Address	Specify a link from this object, to either a: URL address, or Oneline Designer drawing	Any valid URL address, or existing Oneline Designer drawing	None
Data Source	Unique identifier for the data source required for the Switch Box. When a Digital Control datasource type is selected and Feedback Enabled is set to True, then the displayed switch state changes, based upon feedback from Digital Input points. When a Digital Control datasource type is selected and Feedback Enabled is set to False, then the displayed switch state does not change when the Digital Output point value changes.	Select a data source	None
Quality Horizontal Alignment	The horizontal alignment of the quality display within the object's display area	One of Left, Center, Right	Center
Quality Vertical Alignment	The vertical alignment of the quality display within the object's display area	One of Bottom, Top	Bottom

Transformer Object Settings

The Transformer Object is a Dynamic Object that displays a single vector image of a 2 winding or 3 winding transformers, as positioned by the One Line Designer.

Table 6.269: Transformer Object Settings

Setting	Description	Range	Default
Name	Name of the One Line Designer object.	Text	Transformer
X	X (horizontal) pixel position from the top left corner of the screen to the top left corner of the area used to display the object	0 to the Draw Panel width less the object width	0
Y	Y (vertical) pixel position from the top left corner of the screen to the top left corner of the area used to display the object	0 to the Draw Panel height less the object height	0
Border Type	Defines the type of border to display	One of No border, Symmetric borders, raised borders, Sunken borders, Outdent borders, Indent borders, Picture borders, double raised, Double sunken, Bottom right borders, Top left borders	No border
Border Color	Defines the color to apply to the border around the perimeter of the display area of the object	Any 24-bit RGB Color	Gray
Border Variant	Defines the width of the border to display	0 to 9	0
Border Multiplier	Defines the thickness of the border to display	One of None (x1), x2, x3, x4, x5, x6, x7, x8	None (x1)
Width	Pixel width of the rectangular area used to display the object	1 to the Draw Panel width	32
Height	Pixel height of the rectangular area used to display the object	1 to the Draw Panel height	32
Back Color	The color to apply to the background	Any 24-bit RGB Color	Gray
Orientation	Whether to draw the object transformer windings in a horizontal or vertical orientation	Horizontal or Vertical	Horizontal
Number of Windings	Defines the number of transformer windings to include in the object	2 or 3	2
Winding 1 Line Width	Line width of the first winding in pixels	1 to 100	1
Winding 1 Line Color	Line color of the first winding	Any 24-bit RGB Color	Black
Winding 2 Line Width	Line width of the second winding in pixels	1 to 100	1
Winding 2 Line Color	Line color of the second winding	Any 24-bit RGB Color	Black
Winding 3 Line Width	If Number of Windings are Configured as 3: Line width of the third winding in pixels	1 to 100	1

Setting	Description	Range	Default
Winding 3 Line Color	If Number of Windings are Configured as 3: Line color of the third winding	Any 24-bit RGB Color	Black
Load Tap Changer Line Width	Line width of the load tap changer arrow	1 to 100	1
Load Tap Changer Line Color	Line color of the load tap changer arrow	Any 24-bit RGB Color	Black
Load Tap Changer Winding #	Defines which winding to draw the load tap changer arrow over top of (with 0 indicating to not draw a load tap changer arrow)	0, 1, 2, or 3	0
URL Action	Specifies whether to load the URL Address into the same window, or a new window.	Same or New	Same
URL Address	Specify a link from this object, to either a: • URL address, or • Oneline Designer drawing	Any valid URL address, or existing Oneline Designer drawing	None
Data Source	Unique identifier for the data source required for the Value Box.	Select a data source	None
Quality Horizontal Alignment	The horizontal alignment of the quality display within the object's display area	One of Left, Center, Right	Center
Quality Vertical Alignment	The vertical alignment of the quality display within the object's display area	One of Bottom, Top	Bottom

Value Box Object Settings

The Value Box Object is a Dynamic Object that displays the current run-time value of an Analog Set Point, Analog Status, Accumulator Status, Digital Status Object, or Text Object

Table 6.270: Value Box Object Settings

Setting	Description	Range	Default
Name	Name of the One Line Designer object.	Text	Valuebox
X	X (horizontal) pixel position from the top left corner of the screen to the top left corner of the area used to display the object	0 to the Draw Panel width less the object width	0
Y	Y (vertical) pixel position from the top left corner of the screen to the top left corner of the area used to display the object	0 to the Draw Panel height less the object height	0
Border Type	Defines the type of border to display	One of No border, Symmetric borders, raised borders, Sunken borders, Outdent borders, Indent borders, Picture borders, double raised, Double sunken, Bottom right borders, Top left borders	No border
Border Color	Defines the color to apply to the border around the perimeter of the display area of the object	Any 24-bit RGB Color	Gray
Border Variant	Defines the width of the border to display	0 to 9	0
Border Multiplier	Defines the thickness of the border to display	One of None (x1), x2, x3, x4, x5, x6, x7, x8	None (x1)

Setting	Description	Range	Default
Width	Pixel width of the rectangular area used to display the object	1 to the Draw Panel width	45
Height	Pixel height of the rectangular area used to display the object	1 to the Draw Panel height	16
Alignment	The horizontal alignment of the value displayed as text within the object's display area	One of Left, Center, or Right	Right
Font Type	The type of font used to display value as text	One of SansSerif, Serif, Monospaced, DialogInput	SansSerif
Font Style	The font style to apply to the display of the value as text	One of normal, bold, or italic	Normal
Font Size	The size of the font used to display value as text	1 to 100	9
Fore Color	The color to apply to the value displayed as text	Any 24-bit RGB Color	Black
Back Color	The color to apply to the background	Any 24-bit RGB Color	White
Data Source	Unique identifier for the data source required for the Value Box.	Select a data source	None
Quality Horizontal Alignment	The horizontal alignment of the quality display within the object's display area	One of Left, Center, Right	Center
Quality Vertical Alignment	The vertical alignment of the quality display within the object's display area	One of Bottom, Top	Bottom

Data Source Configuration Settings

Property Panel - Data Source Tables

The Property Panel displays the properties associated with the currently selected data source type. Based on the type of data source selected, the properties window shows different options.

The Data Source types are:

- Accumulator Status Data Source Settings
- Alarm Data Source Settings
- Analog Set Point Data Source Settings
- Analog Status Data Source Settings
- Digital Control Data Source Settings
- Digital Status Data Source Settings
- Raise/Lower Control Data Source Settings
- Text Data Source Settings

Accumulator Status Data Source Settings

Table 6.271: Accumulator Status Data Source Settings

Setting	Description	Range	Default
Name	Name of the Accumulator data source.	Text	Accumulator Status
IED Name	Name of the IED.	Existing IED name	None

Point Name	Name of the single alarm accumulator point.	Existing accumulator point identifier	None
Accumulator Type	Whether to monitor status on frozen or running value	One of Frozen or Running	Running

Alarm Data Source Settings

Table 6.272: Alarm Data Source Settings

Setting	Description	Range	Default
Name	Name of the Alarm data source.	Text	Alarm
Point Name	Name of the single alarm indicator point or alarm group If alarm group is selected, acknowledgement action in oneline viewer acknowledges all alarms belonging to this alarm group.	Existing alarm indicator point identifier or existing alarm group	None

Analog Set Point Data Source Settings

Table 6.273: Analog Set Point Data Source Settings

Setting	Description	Range	Default
Name	Name of the Analog Set Point data source.	Text	Analog Set Point
Primary IED Name	IED identifier where the identifier consists of the device name.	Existing IED name	None
Primary Point Name	Point identifier for a single analog output point on which to operate a set point command.	Existing point name	None
Minimum Value	Minimum permitted set point value	Any 64-bit floating point value	0.0
Maximum Value	Maximum permitted set point value	Any 64-bit floating point value	0.0
Function Code	The type of protocol request to send as part of the set point command	One of Direct Operate, or Direct Operate with No Acknowledgement	Direct Operate
Feedback Enabled	Whether to enable a feedback analog input point to receive status on a set point command **NOTE:** In a distributed system, the only reliable way to determine the success of a control operation is through a hardwired digital input or analog input point providing the feedback of the process state being controlled.	True or False	False
Feedback IED Name	If Feedback Enabled is True: IED name for Analog feedback.	Existing IED name	None
Feedback Point Name	If Feedback Enabled is True: Point identifier for a single analog input point on which to receive the feedback value in response to a set point command.	Existing analog input point name	None

Setting	Description	Range	Default
Timeout (sec)	If Enable Feedback is True: the timeout period (in seconds) during which the feedback point value must change to correspond to the set point value to indicate successful completion of the set point command. A value of 0 indicates there is no timeout.	0 to 65535	120
Deadband	If Enable Feedback is True: the feedback value maximum percentage variation from the set point value by which the feedback value is still considered to be equal to the set point value.	0 to 65535	0
Require Confirmation	Defines whether the GUI is to display a confirmation dialog immediately prior to executing a set point	True or False	True

Analog Status Data Source Settings

Table 6.274: Analog Status Data Source Settings

Setting	Description	Range	Default
Name	Name of the Analog Status data source.	Text	Analog Status
IED Name	Name of the IED.	Existing IED name	None
Point Name	Name for a single analog input point.	Existing analog input point identifier	None
Deadband	The percentage variation from the last value that exceeded deadband, which once exceeded becomes reported, and becomes the new last value for future reporting	0 to 65535	0

Digital Control Data Source Settings

Table 6.275: Digital Control Data Source Settings

Setting	Description	Range	Default
Name	Name of the Digital Control datasource.	Text	Digital Control
Secondary Output Enabled	Whether to enable a Secondary output point or not. When a Primary output exists but a Secondary is not enabled, both an on and off control state are associated with the Primary output point. Setting a control state to on or off has the result of executing the configured control code on the Primary output point. When a Primary output and a Secondary output is enabled, then the on-control state must be assigned to only one of them, and the off-control state must be assigned to the other output. Setting a control state to on or off in this case has the result of executing the configured control code on either the Primary or Secondary output point, but never both.	True or False	False

Setting	Description	Range	Default
Secondary Control State	If Secondary Output Enabled set to True: whether to associate the Secondary output point with the On State or Off State. The Primary outpoint point is associated with whichever state the Secondary is not associated with.	On or Off	Off
Primary IED Name	IED identifier where the identifier consists of the device name.	Existing IED name	None
Primary Point Name	Point identifier of a digital output point where the identifier consists of the device point descriptor. If size is 4-state, this maps to the left-most bit.	Existing point name	None
Function Code	The protocol function code to pass as part of the digital control command sent to a device.	One of Direct Operate, Direct Operate with No Acknowledgement, Select Before Operate, Select, Operate	Direct Operate
Primary Pulse On Time	Primary control pulse on time in milliseconds (applies only to Control Codes of type Pulse On, Pulse Off, Trip, or Close).	0 to 65535	0
Primary Pulse Off Time	Primary control pulse off time in milliseconds (applies only to Control Codes of type Pulse On, Pulse Off, Trip, or Close).	0 to 65535	0
On State Control Code	Protocol control code to send as part of the digital control command, when the user requests to send an On state.	One of Latch On, Latch Off, Pulse On, Pulse Off, Trip, or Close	Latch On
Off State Control Code	Protocol control code to send as part of the digital control command when the user requests to send an Off state.	One of Latch On, Latch Off, Pulse On, Pulse Off, Trip, or Close	Latch Off
On State Control Text	The user defined text used to describe the operation to turn the digital control to “on”	Any text	Textual representation of the configured control code
Off State Control Text	The user defined text used to describe the operation to turn the digital control to “off”	Any text	Textual representation of the configured control code
Num Operations	Number of times to consecutively repeat a control code, applying the pulse on and pulse off times to each control pulse repetition. A value of 1 specifies that the control code is issued once (i.e., no repetition).	1 to 255	1
Secondary IED Name	If Secondary Output Enabled set to True: IED identifier where the identifier consists of the device name.	Existing IED name	None

Setting	Description	Range	Default
Secondary Point Name	If Secondary Output Enabled set to True: point identifier of a digital output point where the identifier consists of the point descriptor. If size is 4-state, this maps to the right-most bit.	Existing point name	None
Secondary Pulse On Time	If Secondary Output Enabled set to True: Secondary control pulse on time in milliseconds (applies only to Control Codes of type Pulse On, Pulse Off, Trip, or Close).	0 to 65535	0
Secondary Pulse Off Time	If Secondary Output Enabled set to True: Secondary control pulse off time in milliseconds (applies only to Control Codes of type Pulse On, Pulse Off, Trip, or Close).	0 to 65535	0
Feedback Enabled	Whether or not to enable feedback status. **NOTE:** In a distributed system, the only reliable way to determine the success of a control operation is through a hardwired digital input or analog input point providing the feedback of the process state being controlled.	True or False	False
Feedback Size	If Feedback Enabled set to True: whether to utilize 2 state feedback or 4-state feedback.	2 State or 4 State	None
Primary Feedback IED Name	If Feedback Enabled set to True: IED identifier where the identifier consists of the device name.	Existing IED name	None
Primary Feedback Point Name	If Feedback Enabled set to True: point identifier for a single two state feedback point consisting of a single digital input point, or of the first of two digital input points required to represent four state status, where the identifier consists of the device point descriptor. If size is 4-state, this maps to the left-most bit.	Existing point name	None
Secondary Feedback IED Name	If Feedback Enabled set to True, and Feedback Size set to 4-state: IED identifier, where the identifier consists of the device name.	Existing IED name	None
Secondary Feedback Point Name	If Feedback Enabled set to True, and Feedback Size set to 4-state: point identifier for the second of two digital input points required to represent four state status, where the identifier consists of the device point descriptor. If size is 4-state, this maps to the right-most bit.	Existing point name	None
Feedback Timeout	If Feedback Enabled set to True: the timeout period after which a digital control is executed that the feedback state must change to correspond to the digital control state. If the digital control state does not correspond within the timeout period, the control is to be aborted. A value of 0 indicates no timeout.	0 to 65535	120
State 00 Text	If Feedback Enabled set to True, and Feedback Size set to 4, the user defined text used to represent a 4-state feedback value of 00.	Any text	Off
State 01 Text	If Feedback Enabled set to True, and Feedback Size set to 4, the user defined text used to represent a 4-state feedback value of 01.	Any text	On

Setting	Description	Range	Default
State 10 Text	If Feedback Enabled set to True, and Feedback Size set to 4, the user defined text used to represent a 4-state feedback value of 10.	Any text	Empty
State 11 Text	If Feedback Enabled set to True, and Feedback Size set to 4, the user defined text used to represent a 4-state feedback value of 11.	Any text	Empty
On Control State Feedback State	The feedback state required to occur in response to an On State sent to a control, for the control to be considered successful.	If 2 State, one of 0 or 1. If 4 State, one of 00, 01, 10, or 11.	None
Off Control State Feedback State	The feedback state required to occur in response to an Off State sent to a control, for the control to be considered successful.	If 2 State, one of 0 or 1. If 4 State, one of 00, 01, 10, or 11.	None
Require Confirmation	Defines whether the GUI is to display a confirmation dialog immediately prior to executing a control	True or False	True

Digital Status Data Source Settings

Table 6.276: Digital Status Data Source Settings

Setting	Description	Range	Default
Name	Name of the Digital Status data source.	Text	Digital Status
Feedback Size	Whether to utilize 2 state status or 4 state status	2 State or 4 State	2 State
Primary IED Name	Name of the Primary IED.	Existing IED name	None
Primary Point Name	Name of the Primary point. If size is 4-state, this maps to the left-most bit.	Existing point name	None
Secondary IED Name	Name of the Secondary IED.	Existing IED name	Empty
Secondary Point Name	Name of the Secondary point. If size is 4-state, this maps to the right-most bit.	Existing point name	Empty
State 00 Text	State 00 text.	Any text	In Transit
State 01 Text	State 01 text.	Any text	Open
State 10 Text	State 10 text.	Any text	Empty
State 11 Text	State 11 text.	Any text	Empty

Raise/Lower Control Data Source Settings

Table 6.277: Raise/Lower Control Data Source Settings

Setting	Description	Range	Default
Name	Name of the Raise/Lower Control data source.	Text	Raise Lower Control
Primary IED Name	Name of the Primary IED.	Existing IED name	None
Primary Point Name	Name of the Primary point. If size is 4-state, this maps to the left-most bit.	Existing point name	None

Setting	Description	Range	Default
Function Code	The protocol function code to pass as part of the digital control command sent to a device.	One of Direct Operate, Direct Operate with No Acknowledgement, Select Before Operate, Select, Operate	Direct Operate
Primary Pulse On Time	Primary control pulse on time in milliseconds	0 to 65535	0
Primary Pulse Off Time	Primary control pulse off time in milliseconds	0 to 65535	0
Raise State Control Code	Protocol control code to send as part of the control command when the user requests to send a Raise.	One of Pulse On, Pulse Off, Trip, or Close	Pulse On
Lower State Control Code	Protocol control code to send as part of the control command when the user requests to send a Lower.	One of Pulse On, Pulse Off, Trip, or Close	Pulse On
Num Operations	Number of operations.	1 to 255	1
Secondary Output Enabled	Whether to enable a Secondary output point or not. When a Primary output exists but a Secondary is not enabled, a raise and lower control state are both associated with the Primary output point. Setting a control state to raise or lower has the result of executing the configured control code on the Primary output point. When a Primary output and a Secondary output is enabled, then the raise control state must be assigned to only one of them, and the lower control state must be assigned to the other output. Setting a control state to raise or lower in this case has the result of executing the configured control code on either the Primary or Secondary output point, but never both.	True or False	False
Secondary IED Name	Name of the Secondary IED.	Existing IED name	Empty
Secondary Point Name	Name of the Secondary point. If size is 4-state, this maps to the right-most bit.	Existing point name	Empty
Secondary Pulse On Time	If Secondary Output Enabled set to True: Secondary control pulse on time in milliseconds	0 to 65535	Empty
Secondary Pulse Off Time	If Secondary Output Enabled set to True: Secondary control pulse off time in milliseconds	0 to 65535	Empty
Secondary Control State	If Secondary Output Enabled set to True: whether to associate the Secondary output point with the Raise State or Lower State. The Primary outpoint point is associated with whichever state the Secondary is not associated with.	On or Off	Empty

Setting	Description	Range	Default
Feedback Enabled	Whether or not to enable feedback status. **NOTE:** In a distributed system, the only reliable way to determine the success of a control operation is through a hardwired digital input or analog input point providing the feedback of the process state being controlled.	True or False	False
Analog Feedback IED Name	Name of the analog feedback IED.	Existing IED name	Empty
Analog Feedback Point Name	Name of the analog feedback point.	Existing point name	Empty
Require Confirmation	Defines whether the GUI is to display a confirmation dialog immediately prior to executing a control	True or False	True

Text Data Source Settings

Table 6.278: Text Data Source Settings

Setting	Description	Range	Default
Name	Name of the Text data source.	Text	Text
IED Name	Name of the IED.	Existing IED name	None
Point Name	Name for a single RTDB text point.	Existing text point name	None

Create Analog Reports

Analog Report Generation - Overview

This feature allows you to generate an Analog Report log.

Each Electric Utility Substation requires that various analog parameters from different bays be logged. Logging of this substation equipment information is required for:

- Records
- Periodic maintenance
- Preventive maintenance

In a substation where no Substation Automation System is available, the shift operator uses a log sheet to manually enter parameters into pre-printed log sheets.

In a substation where a Substation Automation System is available, automated report generation:

- Logs the values of the selected analog parameters.
- Uses logged parameter data in online and offline report formats.
- Creates online reports as per the user-configured tabular formats.
- Creates offline reports as per the existing or user-configured tabular formats (that is, templates created from Reports).
- Provides a view of the online report in a separate window.
- Allows you to list, view, print, and download the offline reports.
- Exports the online report to xls or pdf file formats.

The Analog Report Log is accessed from the System log for information and provides Offline Analog Reports. This log will be updated when a:

- New report is generated.
- Report is automatically deleted by the Analog Report application.
- Report has been manually deleted by a user.
- Report(s) has been downloaded by a user.

Analog Report - Viewing

The Analog Report Viewer allows you to:

- View online reports.
- Save and view offline reports.

NOTE: The Analog Report Viewer is only available in the remote HMI due to limited resources available in the local HMI.

NOTE: A maximum of 50000 updated data values can be viewed in a report at one time with a maximum socket timeout of 30 seconds.

Online Reports

Online Reports are the Periodic Data-logger reports configured in the Data Logger application.

Online Report Fields

Table 6.279: Online Report Fields

Field	Description
Periodic Datalogger Reports	Choose the available Datalogger Reports.
Templates	Choose the available Online Template. Only one Default Online Template can exist in the MCP.
Start Date	Set the start date that data is to start populating the generated Reports. Use the checkbox to enable and disable the start date: • Select the checkbox to enable a start date. • Clear the checkbox to disable a start date. When the Start Date field is enabled, you can either: 1. Click the **Start Date** field. Result: The Select Date/Time window appears. 2. Select the date and time. 3. Click **Select**. or • Use the up-arrow and down-arrow buttons to change the Date/Time.

End Date	Set the end date that data is to stop populating the generated Reports. Use the checkbox to enable and disable the end date: • Select the checkbox to enable an end date. • Clear the checkbox to disable an end date. When the End Date field is enabled, you can either: 1. Click the **End Date** field. Result: The Select Date/Time window appears. 2. Select the date and time 3. Click **Select**. or • Use the up-arrow and down-arrow buttons to change the Date/Time.

Online Report - Top Table

This table lists the Analog Points Mapped in the Online Data Logger Applications**.** The online Report Viewer allows you to generate Online Reports in any of the following file formats:

- HTML
- PDF
- XLS

Table 6.280: Online Report - Top Table

Column	Description	Value determined by ...
Name	Report parameter name: • customer • substation • bay ID • voltageLevel • title	... the Online report templates.
Description	Default description of the report parameter.	
Value	Description of the report parameter.	.... the user.

Online Report - Bottom Table

This table lists the source Analog Points Mapped in the Data Logger Application.

Table 6.281: Online Report - Bottom Table

Column	Description
Selection	Check this box to select the Analog Input Point to generate the Online Report.
Source	The Home Directory and Point ID of Analog Input Point.
Bay ID	The Bay ID of the Analog Input point
Point Description	The Point Description of the Analog Input Point.
Point Reference	The Point Reference of the Analog Input Point.

Online Report Controls

Table 6.282: Online Report Controls

Control	Description

File Type	Select the file format of the periodic data logger reports to be viewed: • html • pdf • xls
Show button	Click to view a Datalogger report.

Offline Reports

Offline reports are generated by the Analog Report Generation application.

This feature allows you to view and download the Analog Reports generated over a period in any of the following file formats:

- html
- pdf
- xls

All available reports are listed in the file tree structure in the left pane.

Report names with:

- Suffix In **Progress:** indicates that the report is still in the process of being logged.
- Prefix **Archived <N>**: indicates that the report is archived on the MCP to avoid logging records having the same record time on the same offline report file before and after the system date/time changed. <N> is sequence number.

Records having the same record time might be found in archived offline report and regular offline report.

Offline Report Fields

Table 6.283: Offline Report Fields

Field	Description
Disk Usage	Indicates disk usage in percent against total disk size configured.
Estimated Days of Disk Full	Estimated number of days that the disk will be full. This approximation is based on the various parameters such as the Number of configured Reports, Size of each Report and the Available Disk Space.
Total Reports	Indicates the total number of reports currently available on disk.
Total Shift Reports	Indicates the total number of shift type reports currently available on disk.
Total Daily Reports	Indicates the total number of daily type reports currently available on disk
Total Weekly Reports	Indicates the total number of weekly type reports currently available on disk
Total Monthly Reports	Indicates the total number of monthly type reports currently available on disk

Offline Report Controls

Allows user to save and delete Reports.

Table 6.284: Offline Report Controls

Control	Description
checkbox	Use the checkbox to select and de-select the Reports • Checkbox to Select a Report • Clear the checkbox to de-select a Report

File Type	Select the file format of the periodic data logger reports to be viewed: • html • pdf • xls
Save button	To save one or more reports: 1. Select the report(s) in the file tree structure in the left pane. Use the checkbox to select and de-select reports. 2. Click **Save**.
Delete button	To delete one or more reports: 1. Select the report(s) in the file tree structure in the left pane. Use the checkbox to select and de-select reports. 2. Click **Delete**.
Filter button	Click the **Filter** down-arrow to view the filter options. Result: The Select Filter window appears. You can either: • Type in a specific Report Name, or • Choose a set of Analog Reports that were generated between the Start and End Dates. Click the **Apply** button to list the reports that match the specified filter conditions. Click the **Show All** button to list all available reports. Click **X** (top-right) to close the Select Filter window.

Analog Report Generation - Configuration

The configuration page provides three tabs:

- Reports
- Templates
- Global Settings

Reports Tab

The Reports tab of the Analog Reports Generation configuration window allows you to configure different sets of reports in the system.

>> To create a new Analog Report:

1. Log into the MCP web HMI.
2. Click the **Configuration** powerbar button.
3. Click the **Analog Report** tab.
4. Click the button to initiate the creation of a new Analog Report.
   Result: A default report name appears in the Reports pane on the left.
   Result: The **Reports** > **Properties** tab fields appear.
5. Enter values in the **Properties** fields.
   Result: The entered **Report Name** appears in the Reports pane.
6. Click the **Reports** > **Points Map** tab.
   Result: A report parameter list appears in a Point Map table. The list of report parameters is determined by which Template Name was selected in the previous step.
7. Click on a report parameter.
   Result: The selected table row appears with a light-blue background.

8. Map a point to the point parameter by double-clicking a point in the file tree structure.
   Result: The mapped point details appear.
9. Click the **Save** icon.
   Result: A confirmation window appears.
   Result: The created report is saved in the HMI.
10. Click **Commit Changes** to apply the changes to the MCP.

Known Issue:

The current Offline Analog Report is created with incorrect start time and end time if the MCP time is manually changed when DST is enabled (Daylight Saving Time). Note that the DST is enabled automatically based on the Time zone configured.

If an Offline Analog Report is in the process of gathering data records when DST is enabled:

- The first Offline Analog Report will contain an extra 1 hour of records; this additional 1-hour of records should have been included with the next report.
- The next report will not contain the first 1 hour of records.

For example:

1. A 4-hour duration shift report starts at 00:00 and is to end at 03:45.
2. DST is enabled at 2 am.
3. The reports are created:
   - The first report contains records gathered from 00:00 to 03:45 and 04:00 to 04:45.
   - The next report contains records gathered from 05:00 to 07:45; that is, it does not contain the 04:00 to 04:45 records.

   Subsequent reports are created and logged correctly.

>> To delete an Analog Report:

1. Log into the MCP web HMI.
2. Click the **Configuration** powerbar button.
3. Click the **Analog Report** tab.
4. Select a report name in the Reports pane.
5. Click the button.
   Result: The Delete Report confirmation window appears.
6. Click **Yes** to delete the report.
7. Click the **Save** icon.
   Result: A confirmation window appears.
   Result: The report is removed from the HMI.
8. Click **Commit Changes** to apply the changes to the MCP.

Reports > Properties Sub-tab Fields

Table 6.285: Reports - Properties

Field	Description
Report ID	Auto-generated unique report identifier number.
Report Name	Type the report name.

Template Name	Select the template: ☐ Battery Chargers ☐ Circuit Breaker ☐ Transformer Reactor Temperature ☐ Meter Readings ☐ EHV Line ☐ EHV_Transformers ☐ Daily Voltage Summary ☐ Polled Data NOTE: The MCP Analog Report Generation Application also allows you to add additional (user-configurable) templates. Refer to the Jasper iReport Configuration Manual.
Report Type	Select the type of report: ☐ Shift ☐ Daily ☐ Weekly ☐ Monthly
Enable Logging	Check this box to enable logging of the configured analog data.
Report Duration	Select the duration period in which data is to be logged before a report is generated: ☐ 4 hours ☐ 6 hours ☐ 8 hours ☐ 12 hours
Log Interval	Select the interval at which a new record is to be logged for the report: ☐ 15 Minutes ☐ 30 Minutes ☐ 60 Minutes
Start Time Alignment (Hour of Day)	Select the hour of the day (on a 24-hour clock) at which a new report will start to log data. The range is 0 to 23 hours.
Logging Alignment (Minute of Hour)	Select the minute of the hour at which every record will be aligned in a report: ☐ xx:00 ☐ xx:15 ☐ xx:30 ☐ xx:45

Reports > Point Map Sub-tab

Table 6.286: Reports - Point Map

Point Map Table		
Column	**Description**	**Value determined by ...**
Name	Report parameter ID.	... the **Template** selected in the Properties fields.
Description	Report parameter description	
Home Dir	Home Directory of the source Analog Point Mapped for logging	... which point has been mapped to this report parameter.
Point ID	Point ID of the source Analog Point Mapped for logging	

Point Description	Point Description of the source Analog Point Mapped for logging	
Point Reference	Point Reference of the source Analog Point Mapped for logging	

Reports > Parameters Map Sub-tab

Table 6.287: Reports - Parameters Map

Parameter Map Table		
Column	**Description**	**Value determined by ...**
Name	Name of Parameter Map.	... the **Template** selected in the Properties fields.
Description	Description of Parameter Map.	
Value	Type the suitable text for each row. The entered text appears as the header and footer of the generated reports. The position of the header and footer in the layout of the generated report can be pre-defined in the Template	... the Template selected in the Properties fields. This field can be edited

Templates Tab

The Templates tab allows you to:

- Upload a user-configured Template to the MCP
- Download available Templates from the MCP
- Preview the available user-configured Templates.

Upload a Template to MCP

Only use this procedure if you have created Templates using Jasper iReports Software. For more details, refer to the iReport Designer manual. This manual is available in the GE Grid Solutions Technical Support Library.

For manuals, login and navigate to: Substation Automation Products > MCP > Manuals

For the template files, login and navigate to:

Substation Automation Products > MCP > Manuals > Analog Reports Templates

>> To upload a template to the MCP:

1. Log into the MCP Web HMI from the PC where the **Templates** are available.
2. Click the **Configuration** powerbar button.
3. Click the **Analog Report** tab.
4. Click the **Templates** sub-tab
5. Either:
   - Select an existing template from the Templates pane.
     or
   - Create a new template by clicking the button.
6. Click the **Upload** button.
   Result: The Open window appears.
7. Navigate to select the required **.rz** file.
8. Click **Open**.
   Result: The .rz file is opened and the Open window closes.

9. Click the **Save** icon.
   Result: A confirmation window appears.
   Result: The created template is saved in the HMI.
10. Click **Commit Changes** to apply the changes to the MCP.

NOTE:

- If a template is uploaded onto an existing template which is being used by a report, you might need to reconfigure the report for mapped points and parameters. This occurs only if parameter list or point list changed in new template; that is, a parameter or point field has been added or removed.
- To ensure that a new template is working well, it is recommended that you preview the report before saving and committing the report.

>> To download a report template from the MCP:

1. Log into the MCP Web HMI.
2. Click the **Configuration** power bar button.
3. Click the **Analog Report** tab.
4. Click the **Templates** sub-tab.
5. Select an existing report template from the Templates pane.
6. Ensure that the report template has been saved and committed.
7. Click the **Download** button.
   Result: The Save window appears.
8. Navigate to the folder which is to contain the. rz file.
9. Click **Save**.
   Result: The Save window closes and the Download Template confirmation window appears.
10. Click **OK**.
    Result: The Download Template confirmation window closes.
11. Click the **Save** icon.
    Result: A confirmation window appears.
    Result: The created template is saved in the HMI.
12. Click **Commit Changes** to apply the changes to the MCP.

>> To preview a report template:

1. Log into the MCP HMI.
2. Click the **Configuration** power bar button.
3. Click the **Analog Report** tab.
4. Click the **Templates** sub-tab.
5. Select an existing report template from the Templates pane.
6. Click the **Preview** button.
   Result: A preview of the report appears.

Templates Tab Fields

Table 6.288: Templates Tab Fields

Field	Description
Template Name	Type the template name.
Jasper File	Displays the name of the Jasper file.
XML File	Displays the name of the .Jrxml file.
Details	

Creation Time	The time that this template was created.
Installation Time	The time that this template was uploaded to this MCP.
Template Description	The description of the template file provided by the Template.

Templates Tab Buttons

Table 6.289: Templates Tab Buttons

Button	Description
Upload	Upload a report template to the MCP. For example, the uploaded report template could have been created using Jasper iReports Software.
Download	Download a report template from the MCP.
Preview	Preview a report template.

Global Settings Tab

The Global Settings tab allows you to configure global settings which affect all reports.

Table 6.290: Global Settings Tab

Field	Description
Storage Full Action	Select an action to occur when the configured Analog Report Generation storage space is full. The options are: • Delete Oldest Reports • Stop New Reports
Threshold (%) for Storage Full	Set the percentage of storage space at which a warning message appears. The valid range is 50% to 95%.
Time Zone	Select a time zone from the list provided. This parameter affects the Start Time Alignment and Logging Alignment of the report.

Configure System Security

This chapter contains the following sections and sub-sections:

Security Features
System Security
Password Complexity
Connection Security
Secure Application Parameters
User Accounts and Authentication
User Management tab
Local Authentication
Setting Up a User Account
Secure Access
Software Licensing Tools
Firewall Settings
Automatic logout

Security Features

The MCP employs several security measures to ensure the safety of the MCP system from unauthorized users, including:

- Log in using password security and authentication
- Secure HMI access using security certificates
- User access levels to limit access to MCP functions
- User authentication before executing control commands
- Secure shell (SSH) log in for terminal session (optional)
- Automatic logout
- TLS based encryption and identity verification on serial and Ethernet connections
- Password Complexity

For information on setting up secure Web access and remote authentication, see the *G500 Substation Gateway Instruction Manual (994-0152) or G100 Substation Gateway Instruction Manual (994-0155).*

System Security

The MCP provides security features to authenticate its identity and to maintain the privacy of information between the MCP and your computer when communicating over the Internet. The MCP makes use of digital signatures and secure Web access to ensure this security.

Secure Web access to the MCP is provided using the Transport Layer Security (TLS) protocol version 1.2 over a 128-bit connection. To support the MCP's secure Web access features, you need to obtain and install a security certificate and a private key on the MCP.

Refer to the G500 Substation Gateway Instruction Manual 994-0152 or G100 Substation Gateway Instruction Manual (994-0155) for details.

Password Complexity

To ensure the strength of user passwords, it is recommended that a specific set of rules be presented to users.

Passwords must contain characters from all the following categories:

- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Base 10 digits (0 through 9)
- Non-alphabetic characters (for example, $, #, %)
- A maximum of 199 characters for a password are allowed.

Connection Security

The MCP supports the below security features for the pass-through supported and terminal server applications. This can be configured using the **Connection** tab > **Secure Type** option. The Secure type options are:

- **Disabled** (default)
- **Telnet** : The MCP supports pass-through and terminal server access to the devices from PC-based configuration tools and, if necessary, COM port redirection software. These connections are accessible through a TCP port on the MCP.
- **TLS Security** : The MCP supports Transport Layer Security (TLS) which is cryptographic protocol that provide security for communications over networks such as the Internet. TLS encrypt the segments of network connections at the Application Layer to ensure secure end-to-end transit at the Transport Layer.
- **SSH Secure Tunnel** : The MCP supports SSH Secure Tunnel to provide secure access to pass through and terminal server connections.

The Telnet, TLS Security, SSH Secure Tunnel features are available on the following types of connections:

- IEC 60870-5-103 Multi-drop
- Modbus Multi-drop
- Generic ASCII
- SEL Binary with MCP as Master
- Terminal Server

NOTICE

SECURITY NOTICE

The following services are considered unsecure:

IEC 60870-5-103 Multi-drop (Passthrough-Telnet)

Modbus Multi-drop (Passthrough-Telnet)

Generic ASCII (Passthrough-Telnet)

SEL Binary with MCP as Master (Passthrough-Telnet)

Terminal Server (Telnet)

It is strongly recommended that TLS tunnels or SSH Tunnels are used for sessions across unprotected / external networks.

The user assumes all responsibility for the system design and associated security risks when unsecured sessions are used, for e.g. Telnet.

The following parameters can be configured on any security-enabled connection.

Secure Application Parameters

Table 6.291: Secure Application Parameters

Setting	Description	Range	Default
Parameters			
Enable insecure authentication	When enabled, connection security features are not enforced. You should only enable this setting if alternate security features are available for the connection.	Disabled Enabled	Disabled
Session key renegotiation interval	The maximum amount of time, in seconds, that can pass before the connection session key is renegotiated. Frequently renegotiating the session key increases the security of the connection.	600 to 7200	900

Session key renegotiation count	The amount of data, in bytes, that can be transmitted between devices before the connection session key is renegotiated.	10000 to 1000000	100000
Session key renegotiation timeout	The amount of time, in milliseconds, that the MCP waits for a response to a renegotiation request before the connection is considered timed out and is disconnected.	500 to 120000	2000
Issuers			
PEER	The text string that must match the common name as provided on the certificate provided by the remote device.	Free text entry	N/A
Issuer	The name of the issuer that generated the certificate provided by the remote device.	List of installed issuer certificates	N/A
Enable PEER identity validation	If enabled, connections are only permitted to devices that provide a certificate that contains a common name included in the list above and that was provided by the associated issuer. If disabled, PEER identity validation is not performed.	Disabled Enabled	Enabled
Ciphers			
Cipher name	A list of ciphers supported by the MCP. When a connection is established with a remote device, a list of enabled ciphers is exchanged, and the most secure cipher is selected to secure the connection.	N/A	N/A
Enable	Select whether to enable the associated cipher. If the remote device does not support at least one of the enabled ciphers, the connection is not established. List Of Supported Ciphers: EDH-DSS-DES-CBC3-SHA:DHE-DSS-AES128-SHA:DHE-DSS-AES256-SHA:EDH-RSA-DES-CBC3-SHA:DHE-RSA-AES128-SHA:DES-CBC3-SHA:@STRENGTH	Disabled Enabled	Disabled
Permit null encryption	If checked, null encryption ciphers are permitted. If a null encryption cipher is used, the connection itself is unencrypted and is vulnerable to interception attacks.	Disabled Enabled	Disabled
Secure protocol	Select the protocol used to secure the connection.	TLS 1.0 TLS 1.1	TLS1.0

User Accounts and Authentication

The User Management, VPN Client Configuration, Authentication Configuration and Automatic Login are available in the Access Tab of DS Agile Configuration tool.

User Management tab

On the **User Management** tab on the **Configuration** page you can set up accounts for MCP users, including usernames, passwords and access level. The settings on this tab are not available if you are using a TACACS+ or LDAP remote authentication server.

User settings

Table 6.292: User Management Tab Settings

Name	Description
Username	Enter a username to identify the user to the MCP. This is the username when logging into the system. Usernames may only contain numbers, lower-case letters, and the dash (-) and underscore (_) characters.
Privilege Level	Select an access level assigned to the user: **Observer**, **Operator**, **Supervisor** or **SSHPassThrough**.
Full Name	Enter the full name of the user.
Password	Enter a password for the user. The password displays as asterisks (*).
Confirm Password	Enter the same password as above.
User Home Page	Select the UI page from the dropdown list. For details see section: Configure User Home Page on page 209.

Local Authentication

Local authentication makes use of files stored locally to control user authentication, as opposed to connecting to a remote server to obtain username and password information. This is the default authentication mode available in the MCP.

The MCP has two types of administrative users.

Default Administrator - Default username is **defadmin** and the default password is **defadmin**. When user logins using defadmin, only minimal configuration (adding new administrator user, configuring LAN and rebooting the unit) will only be available. Using this Default Administrator User would need to configure a nominated/custom administrator-level user(s) to login and configure MCP.

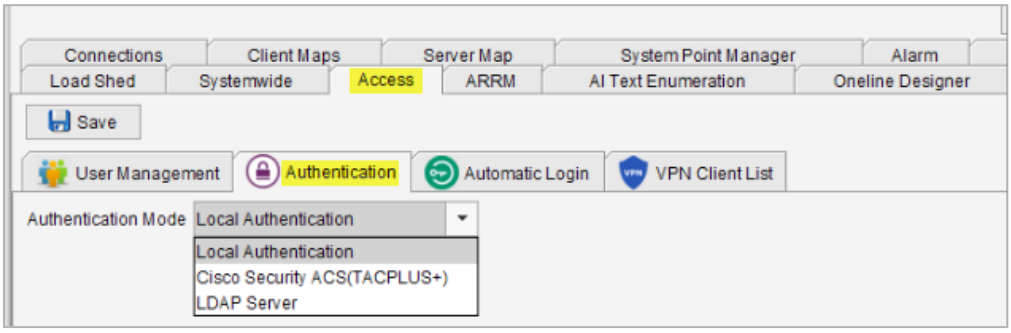
Nominated Administrator - Supervisor-level access to all configuration, runtime, operation, and system administration runtime screens in the Online MCP HMI as well as full access to run commands at the MCP command line interface when the **sudo** command is used (see section Setting up a Terminal Session). OpenVPN configuration and Runtime viewers are only available from Runtime HMI using administrator-level users only.

Remote Authentication

The MCP supports two remote authentication modes:

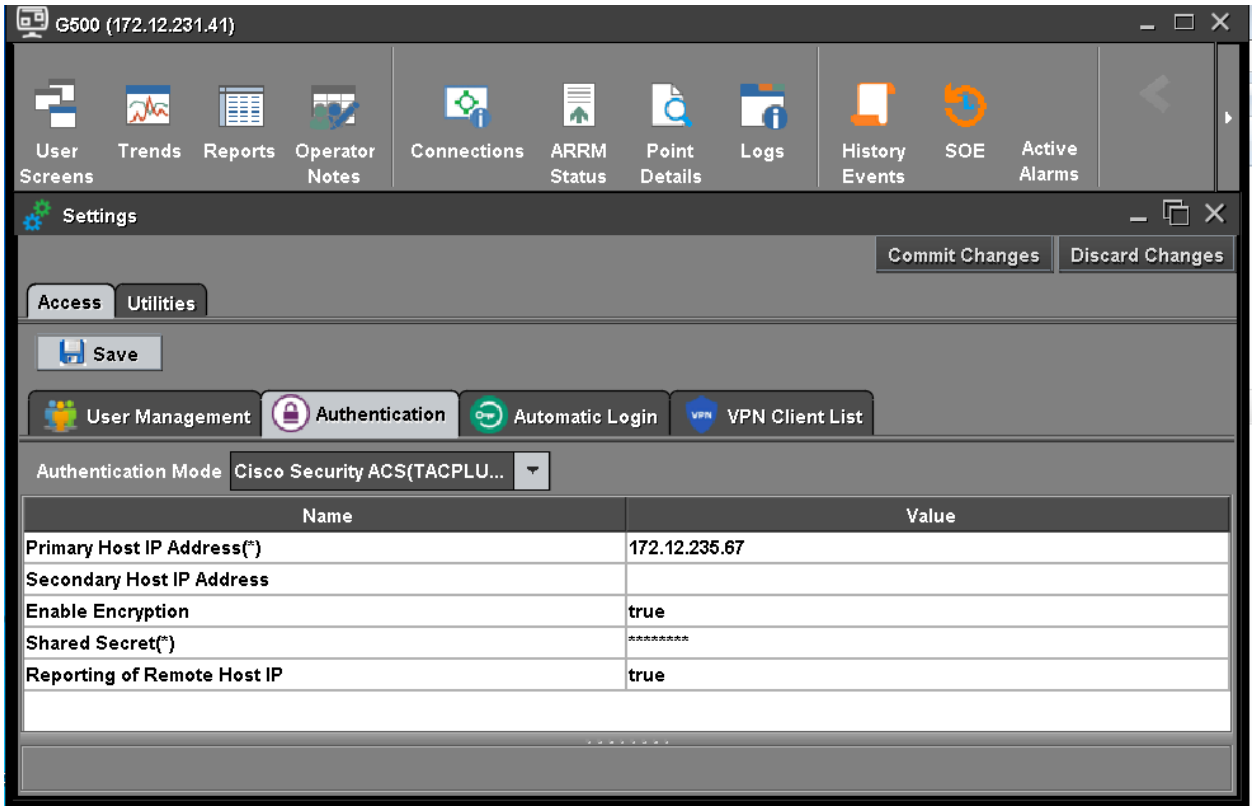
- Cisco® TACACS+
- LDAP

To enable Local, Cisco® TACACS+, LDAP authentication modes, you must login to the MCP HMI as an Administrator User and then click on **Settings > Access > Authentication** tab.



Cisco TACACS+ remote authentication mode requires the following settings:

- TACACS+ server address – valid IPV4 address
- TACACS+ Secondary server address (if enabled) – valid IPV4 address. If the Primary server does not respond, the MCP automatically attempts to connect to the server at this address instead.
- Encryption – select whether to enable or disable encryption for the connection between the MCP and the TACACS+ server
- Shared secret (if enabled) – as provided by TACACS+ server administrator
- Enable reporting of remote host IP Address – if enabled, the MCP reports the IP Address of the MCP to the authentication server. Only enable this if you are using an authentication server that supports this feature.



NOTE: If working in redundancy, above configuration need to be done in both Active and Standby devices.
At least one emergency admin user needs to be configured in Emergency users.
Remote authentication server should be up and running.

Configure IP Address of PEER Gateway: Use this function to set the unique IP Address of the other MCP device configured within the redundant system. If the PEER MCP has a second Ethernet interface, you can configure it as well. The maintenance IP Addresses of the PEER MCP must be entered here (see the *Ethernet Connections* topic in the MCP online help.

Username of PEER Gateway: Use this function to enter the username of an administrator user account on the PEER MCP unit (see Administrator Group Users). This parameter value should be the same on both MCP units.

NOTE: In redundancy, both MCPs must be configured with the same authentication mode (i.e., either Local or Remote). The PEER username should be reconfigured when the authentication mode changes from local to remote and vice versa. Setup Public Key authentication with PEER Gateway.

How Cisco TACACS+ privilege levels are configured has changed slightly to accommodate the "SSHPassThrough" group. Refer to Cisco TACACS+ for information on configuring your TACACS+ server.

The following table provides an example of configuring Cisco TACACS+ including new user privilege level "SSHPassThrough":

User	MCP Group ID	Cisco TACACS+ privilege level
Observer	501	0 -3
Operator	502	4-7
Supervisor	503	8 -11
SSHPassThrough	504	12
Administrator	0	13-15

The **Lightweight Directory Access Protocol (LDAP)** remote authentication mode requires the following settings:

- Full Qualified Domain Name FQDN of LDAP server.
- LDAP server IP Address – valid IPV4 address
- LDAP authentication mechanism (TLS or SSK) and the configured port number. For example, for the Windows Active Directory:
  - Portnumber = 389 for TLS communication
  - Portnumber = 636 for SSL communication
- Bind username (in DN format) & password.
  - For example: Bind User name (in DN format) = cn=MCPadmin,cn=Users,dc=central,dc=home
- LDAP search base directory in DN format. For example: dc=central,dc=home
- LDAP user ID attribute map. For example: sAMAccountName or uid for the Windows Active Directory.
- LDAP homeDirectory attribute map. For example: unixHomeDirectory for the Windows Active Directory.
- Test the LDAP Server to validate the user configured LDAP details and its connectivity. If the LDAP configuration is invalid, an error message displays to correct the configuration details and to avoid the user from locking down to access MCP.
- Enable the LDAP Server Authentication Mode to configure the LDAP certificate with the LDAP server.

Refer to the SWM0108 Configuring the Multilin™ MCP for Centralized LDAP Authentication – Software Configuration Guide for information on configuring your LDAP Server.

NOTE: When the mode is changed from local to remote or vice versa, you need to reconfigure the PEER username and set up public key authentication under the redundancy settings for the PEER MCP again.

Setting Up a User Account

You can manage user accounts by:

- Adding a User
- Changing a User Account
- Deleting a User
- Changing User Access Levels

User assigned access level appears in the top right corner of the title bar of the MCP HMI screen when you log in. User access levels are configured on the **User Management** tab in the **Configuration Tool** -> **Access Tab**

Secure Access

NOTICE

SECURITY NOTICE

The default secure services that MCP employs are HTTPS, SFTP, and SSH.

The SFTP, and SSH services are automatically configured by default.

The HTTPS service is enabled by default. It is the user's responsibility to install a server certificate.

Software Licensing Tools

The MCP contains a set of utilities to manage software licensing for optional applications and features. Licensing is controlled through a single license file stored on your MCP.

» To unlock an application using a license code:

1. Start a terminal session and log into the MCP with an Administrator-level user account.
2. At the prompt, enter the following commands
   cd /home/ MCP_APPS/
   sudo ./swlic-unlock –l <26 digit license code>
   NOTE: The parameter –l above is a lower-case letter "L"
   Result: The feature is unlocked and available for use.

» To update existing MCP licenses using a batch file:

GE Grid Solutions can issue a batch license file, which contains licenses for multiple MCP units. This is useful when licensing features across many MCP units or when licensing several applications on one MCP unit.

1. Start a terminal session and log into the MCP with an Administrator-level user account.
2. Connect a USB drive containing the MCP batch license file.
3. At the prompt, enter the following commands
   cd /home/ MCP_APPS/
   sudo ./swlic-batch
   Result: The tool locates the license file and licenses all applicable features for the current MCP. Repeat steps 1 to 3 for each remaining MCP unit.

» To view detailed information on your MCP license:

1. Start a terminal session and log into the MCP with an Administrator-level user account.
2. At the prompt, enter the following commands
   cd /home/ MCP_APPS/
   sudo ./swlic-report
   Result: The application output shows the MCP ownership information and a list of available features. Each item under Application License represents an application or feature that can be licensed. They are shown in the format: *3-digit application ID number: Description of feature License status*

There are four possible license statuses:

Table 6.293: MCP License Statuses

License Status	Description
Unlocked	The feature has been licensed and is available for use.
Trial Disabled	A trial license is available for this feature. To enable, see the instructions below.

Trial Enabled (Expires YYYY-MM-DD)	The feature is available for use under a temporary trial license. The license expires on the date shown.
Disabled	A trial license was used, and the feature has now been disabled. This feature cannot be re-activated unless a license is purchased.

» To enable a trial license for an application or feature:

A 30-day trial license can be obtained for any application listed as Trial Disabled in the Application License report.

1. Start a terminal session and log into the MCP with an Administrator-level user account.
2. At the prompt, enter the following commands
   cd /home/ MCP_APPS/
   sudo ./swlic-trial –id <3 digit application ID number>
   NOTE: The 3-digit application ID number can be obtained using the swlic-report utility.
   Result: The 30-day trial license is enabled for the feature. Once the 30 days has elapsed, the feature is disabled. A trial license can only be enabled once for each feature.

» To obtain information about your MCP:

Some older MCP units may not contain a license file. In this case, Technical Support can generate a replacement license file for you. To do this, you must provide unique identifying information about your MCP.

1. Start a terminal session and log into the MCP with an Administrator-level user account.
2. At the prompt, enter the following commands
   cd /home/ MCP_APPS/
   sudo ./swlic-info
3. Provide the information shown to Technical Support.

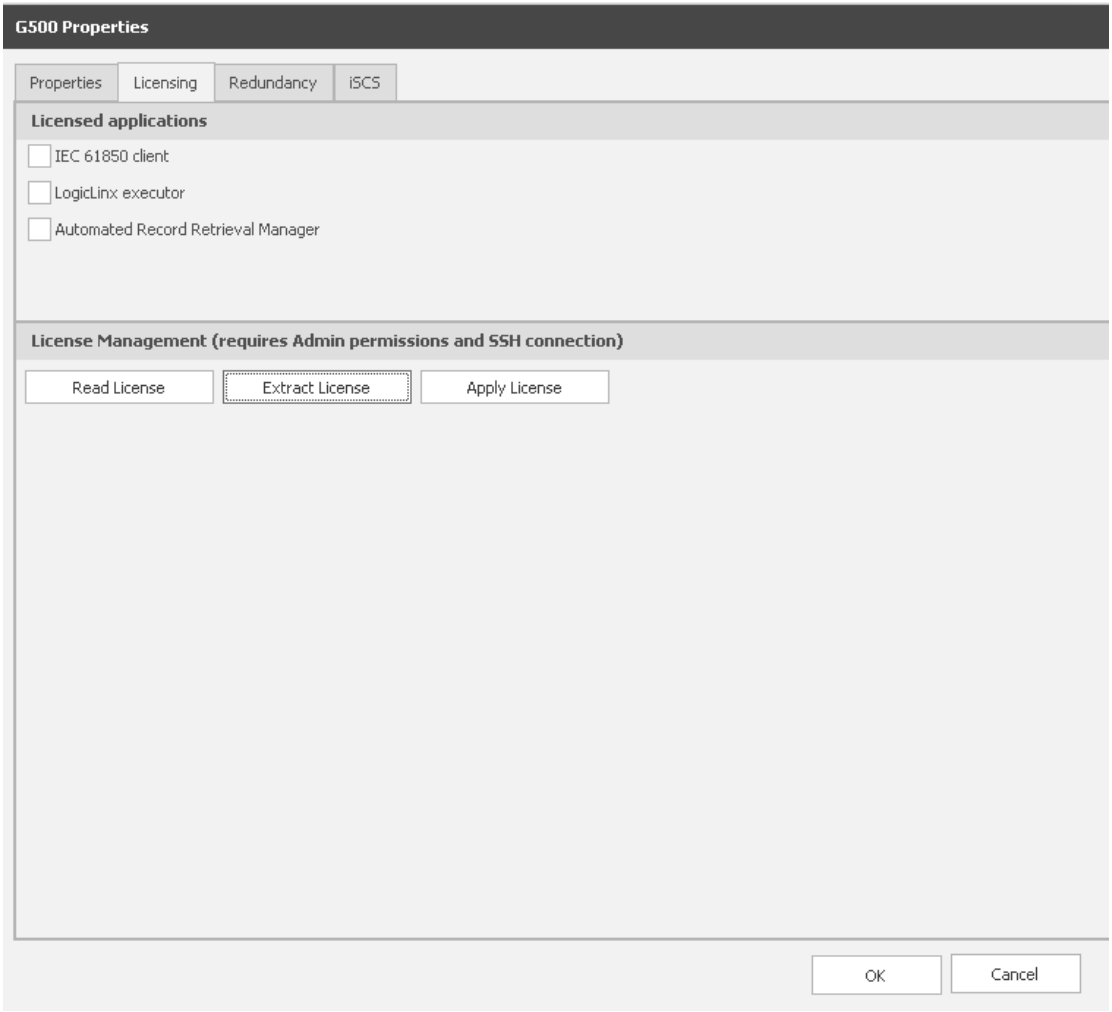
» DSAS based workflow

Users have the possibility to read/extract/apply licenses to MCP using the Licensing option available in the DSAS Configuration Tool.

To access these options:

1. Open Device Properties for your DSAS offline Device in your Project. If one was not created, please follow the normal workflow to create one.

2. Go to the Licensing Tab.

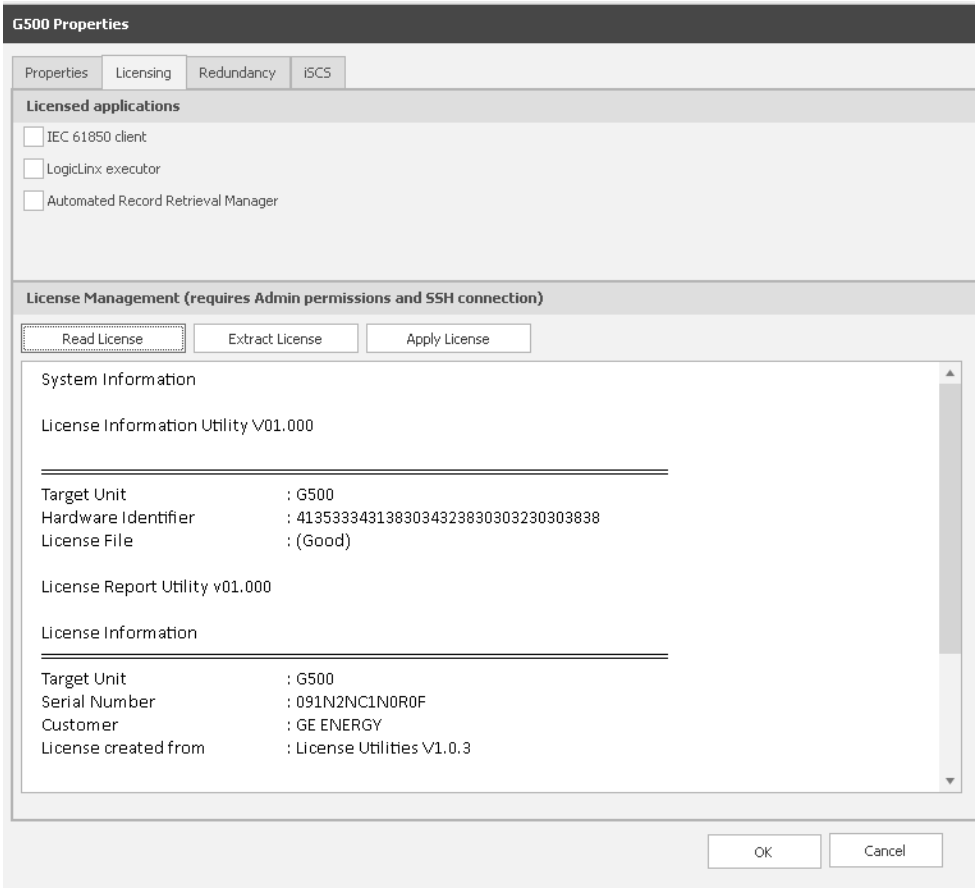


3. Under License Management there are three buttons:
    a. Read License
    b. Extract License
    c. Apply License
4. When user clicks on any of the three buttons, a login dialog is prompted to connect to MCP with Administrator privileges (this role is required to access any of the licensing information).
5. After successful authentication, user is authorized to access the license information. If the user stays within this tab, subsequent button actions will not prompt again to login.

Read License

This option displays the license information of the live target unit (connected MCP device).

Displayed information may be copied to the Windows Clipboard with regular actions (mouse click and drag or CTRL+A to select, right click or CTRL+C to copy).



Extract License

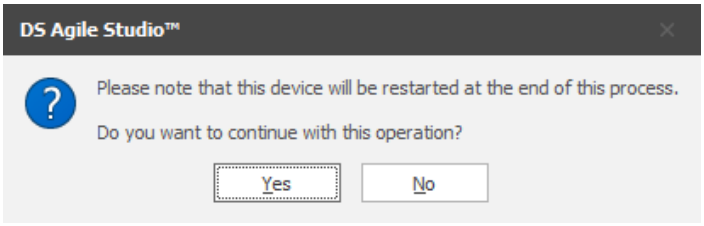
This option allows user to extract the current license file from the live target unit to a specified PC location, for example to archive a copy.

The extracted license file is saved as a *.key file (default name is license but can be changed as desired).

Apply License

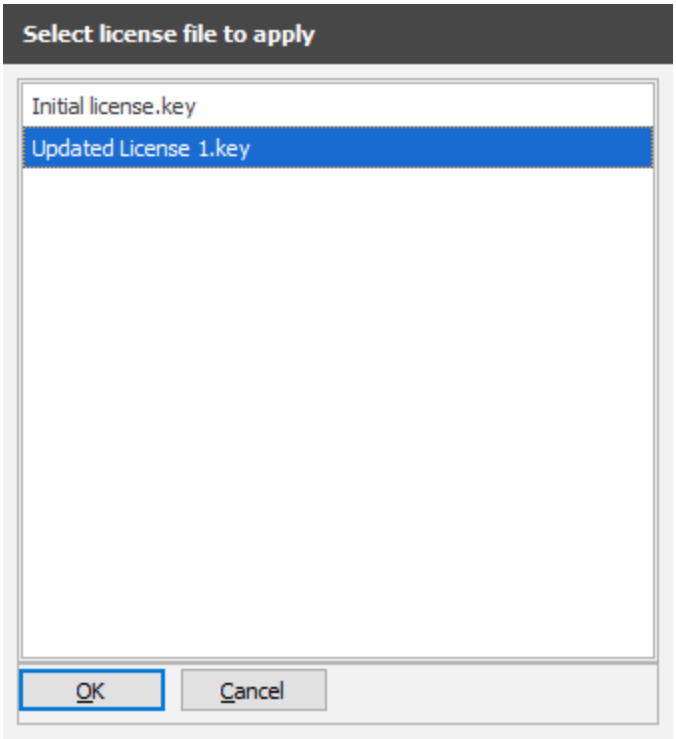
This option allows user to apply a compatible license key, from a location in the PC, to the live target unit.

NOTE: The live target unit is restarted at the end of this process, not immediately, and only if a hardware compatible license file was selected.

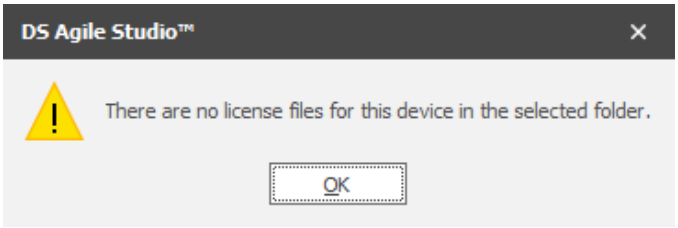


When browsing for license files, user must select the folder containing one or more license files. The action does not include sub-folders of the selection.

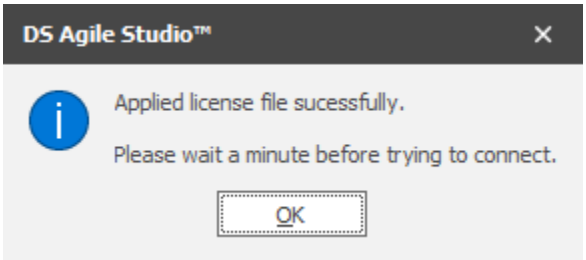
In the resulting dialog only license files (any filename) that match the Hardware Identifier of the live target unit are displayed for selection. This is the reason why users must first login to the live device as Administrators.



If the selected folder has no license compatible with the connected live unit, an information dialog is presented to this effect:



If a valid license file has been selected it will be applied and the device restarts:



The workflow to apply a license can be cancelled at any time before selecting a valid license and click on OK.

Firewall Settings

The MCP contains a firewall capable of stateful packet inspection to protect your device from unauthorized access. By default, network interfaces on the MCP drops packets that are determined to be invalidly routed or unsolicited.

NOTICE

SECURITY NOTICE

The MCP firewall is intended only to protect itself and does not extend protection to other devices on the network. As such, it does not replace the need for a network firewall which offers deep packet inspection and detailed configuration capabilities.

The MCP firewall is automatically configured by default to its most secure setting. The user assumes all responsibility for associated security risks if the firewall configuration is manually changed.

It is the user's responsibility to connect Internal zone interfaces to networks that are protected from unauthorized use.

The MCP firewall is intended only to protect itself and does not extend protection to other devices on the network. As such, it does not replace the need for a network firewall which offers deep packet inspection and detailed configuration capabilities.

Network interfaces can operate in one of two modes:

Internal - The Internal mode permits traffic from known protocols and should only be enabled on interfaces connected to known devices only. The Internal mode is the default mode for Net0, Net1 and would typically be used when the interface is connected to the substation LAN.

External - The External mode offers a stricter set of rules and is the default mode for all interfaces except Net0 and Net1. The External mode would typically be used when the interface is connected to a WAN.

Default modes can be changed by user.

To configure Firewall via mcpcfg, refer Configure Firewall or via Settings GUI, refer Configure Firewall.

Automatic logout

For security, the MCP includes a configurable automatic logout feature. You are automatically logged out of the MCP system when the Inactivity timeout period is reached.

Thirty seconds before the configured inactivity timeout period is to expire, a warning message appears asking you whether you wish to continue. Click **Renew Session** to continue using the HMI.

When an automatic logout occurs, a message appears indicating that you have been disconnected from the MCP and you are prompted to close your Web browser.

» To log back in:

- Re-open your runtime HMI and log in as usual.

System Utilities

This chapter contains the following sections and sub-sections:

Utilities
Utilities Log In
Certificate Import
Diffie Hellman parameter files
Private key file
Certificate Management
Local tab

Issuer tab
CRL tab
Certificate Error Codes
Export Database
Export Database
Export Database .CSV Files
Exporting VPN Client Configuration

Utilities

The **Utilities** page provides access to software tools installed on your MCP device. All available utilities are listed along with a description of the functionality they provide.

NOTE: Except Login to the MCP utility other configuration options are only supported through Local HMI of MCP and not available either in MCP Remote HMI or MCP Offline Configuration Tool.

The following related actions can be performed:

Login to the MCP utility functions	This Utility is used for an SSH (Secure Shell) terminal session to the MCP. To login you must have Administrator access and your username and password.
Import Certificates	Import certificates and Certificate Revocation Lists (CRLs) from an externally mounted filesystem or the local import directories.
Manage Certificates	Manage Local Certificates, Issuer Certificates, and Certificate Revocation Lists.
Export Database utility	Export/Backup Local Database.
Generate Gateway Key Pair	Generate Public/Private key pairs in the MCP for the SSH terminal session. This MCP HMI utility provides an option to: • Save the generated Public key to the host computer • Delete the existing keys.
Exporting VPN Client Configuration File	Export the VPN Client Configuration File into a PC/Shared Location/USB. The VPN Client File is used to configure the VPN Client to establish VPN connection with the VPN server running in the MCP. You must install a Server Certificate prior to exporting the VPN Client File. Go to the Configuration powerbar button > **Communications** tab, and then select **Network Connection** and Network Connection Type: **VPN Server**.

Utilities Log In

For security reasons, some advanced MCP configuration and system administration functions are available only at the MCP command line interface. The **Utilities** page provides a Secure Shell (SSH) login to establish a remote terminal session with the MCP. You must have Supervisor-level access to proceed with Utilities Log In. Access to the command line interface requires an additional Administrator log in.

If the **Utilities** page displays an **SSH** button, the security portal has been configured for a Secure Shell (SSH) login.

» To log in:

1. Click **SSH**.
2. Enter your Administrator username.
3. Click **OK** to verify the MCP unit name.
4. Acknowledge the security message.
5. Enter your administrator password.
   Result: The command line interface appears.

Certificate Import

The **Certificate Import** window allows you to copy local certificates, issuer certificates, and certificate revocation lists (CRLs) from a connected USB drive or from the user CompactFlash card. These certificates and revocation lists are used to facilitate secure connections to remote devices.

Your local certificate may or may not contain Diffie Hellman parameters, the private key, and/or the issuer chain. In the event these are not included within your local certificate, you can install them using the procedures specified below.

Diffie Hellman parameter files

If a cipher that uses the Diffie Hellman key exchange protocol is used (such as those shown in the HMI with a prefix of *dhe*), the associated Diffie Hellman parameters must be available on the MCP. These parameters are either provided as part of the local certificate file or in a separate file. If the parameters are included in the local certificate file, no further action is required after the certificate is installed. If the parameters are in a separate file, it can be stored in the same location as the local certificate (with the same basename) and it will be automatically installed when the local certificate is imported. If multiple files containing Diffie Hellman parameters are found, the one with the largest key size is imported.

Private key file

When a local certificate is installed on a MCP, the associated private key must also be made available. The private key is either provided as part of the local certificate file or in a separate file. If the key is included in the local certificate file, no further action is required after the certificate is installed. If the key is in a separate file, it can be stored in the same location as the local certificate (with the same base name) and it is automatically installed when the local certificate is imported.

» To import certificates:

1. Plug a USB drive containing the certificates, CRLs, Diffie Hellman parameter files, or private key files in a root folder called *SecureScadaTransfer* into one of the USB ports
   or
   Copy the files to the **/mnt/usr/SecureScadaTransfer/** folder using a utility such as Secure File Browser from DS Agile MCP Studio. Note that the local USB method is more secure than transferring the files over an unprotected Ethernet connection.
2. On the **Utilities** page, click the **Import** button that is shown under the *Certificate Import* heading.
3. The **Certificate Import** window opens and displays the progress of the task. Once the files have been imported, a message is shown indicating the number of items that were successfully copied over.
4. Close the **Certificate Import** window.
5. Disconnect the USB drive
   or
   Close the SCP connection to the MCP.

Once the certificate files have been imported to the MCP, they must be installed using the **Certificate Management** window on the **Utilities** page. You must install these files within 96 hours of importing them or else they are automatically deleted. For more details refer to Appendix G – Security Certificates Creation for MCP.

Certificate Management

The **Certificate Management** window allows you to install the local certificates, issuer certificates, and certificate revocation lists (CRLs) that have been copied to the MCP using the Certificate Import utility. Diffie Hellman parameter files and private key files are automatically installed when they are imported using this tool. For more details refer to Appendix G – Security Certificates Creation for MCP.

To enable connection security, you must have:

- A local certificate installed
- An issuer certificate available for all certificate authorities used by remote devices

Certificates belonging to remote devices are transferred automatically when the secure connection is established, so they do not need to be managed using this utility.

Local tab

The **Local** tab contains the certificate that is provided to remote devices to allow them to verify the identity of the MCP unit. The *Staged Local Certificates* area shows all the local certificates that have been copied to the MCP. Select one and click the **Install** button to install it as the local certificate. Though there is no limit on the number of local certificates that can be staged, only one can be installed on the MCP device at any time.

Issuer tab

The **Issuer** tab contains the certification authority certificates that are used by the MCP to verify the integrity of certificates provided by remote devices. Refer to the connection security section for an explanation of how issuer certificates are used. You must install the issuer certificate belonging to the provider of the identity certificate of each remote device you are connecting to. However, multiple devices can refer to the same issuer certificate if the same issuer was used.

The *Staged Issuer Certificates* area shows all the issuer certificates that have been copied to the MCP. Select one and click the **Install** button to install it. Though there is no limit on the number of issuer certificates that can be staged, only one certificate per issuer can be installed at any time (up to a maximum of 32 issuers).

NOTE: You must install all the certificates in the issuer chain. For example, you may be using an intermediate signing certificate provided by a certificate authority to issue your own certificates for remote devices. In this case, you would need to install both the intermediate signing certificate and the issuer's root certificate.

CRL tab

The **CRL** tab contains certificate revocation lists provided by third party certificate issuers. These lists are used to revoke invalid certificates that were previously issued under the authority of the issuer. By maintaining accurate CRLs, you can ensure that revoked certificates are not accepted. The *Staged CRLs* area shows all the CRLs that have been copied to the MCP. Select one and click the **Install** button to install it. Though there is no limit on the number of CRLs that can be staged, only one CRL per issuer can be installed at any time.

Certificate Error Codes

Table 6.294: Certificate Error Codes

Error Number	Message	Description
2	unable to get issuer certificate	The issuer certificate of a looked-up certificate could not be found. This normally means the list of trusted certificates is not complete.
3	unable to get certificate CRL	The CRL of a certificate could not be found.
4	unable to decrypt certificate's signature	The certificate signature could not be decrypted. This means that the actual signature value could not be determined, rather than it did not match the expected value. This only applies to RSA keys.
5	unable to decrypt CRL's signature	The CRL signature could not be decrypted. This means that the actual signature value could not be determined, rather than it did not match the expected value. Not used.

Error Number	Message	Description
6	unable to decode issuer public key	The public key in the certificate SubjectPublicKeyInfo could not be read.
7	certificate signature failure	The signature of the certificate is invalid.
8	CRL signature failure	The signature of the CRL is invalid.
9	certificate is not yet valid	The certificate is not yet valid; that is, the notBefore date is after the current time.
10	certificate has expired	The certificate has expired; that is, the notAfter date is before the current time.
11	CRL is not yet valid	The CRL is not yet valid.
12	CRL has expired	The CRL has expired.
13	format error in certificate's notBefore field	The certificate notBefore field contains an invalid time.
14	format error in certificate's notAfter field	The certificate notAfter field contains an invalid time.
15	format error in CRL's lastUpdate field	The CRL lastUpdate field contains an invalid time.
16	format error in CRL's nextUpdate field	The CRL nextUpdate field contains an invalid time.
17	out of memory	An error occurred trying to allocate memory. This should never happen.
18	self-signed certificate	The passed certificate is self-signed, and the same certificate cannot be found in the list of trusted certificates.
19	self-signed certificate in certificate chain	The certificate chain could be built up using the untrusted certificates, but the root could not be found locally.
20	unable to get local issuer certificate	The issuer certificate could not be found: this occurs if the issuer certificate of an untrusted certificate cannot be found.
21	unable to verify the first certificate	No signatures could be verified because the chain contains only one certificate and it is not self-signed.
22	certificate chain too long	The certificate chain length is greater than the supplied maximum depth. Unused.
23	certificate revoked	The certificate has been revoked.
24	invalid CA certificate	A CA certificate is invalid. Either it is not a CA or its extensions are not consistent with the supplied purpose.
25	path length constraint exceeded	The basicConstraints pathlength parameter has been exceeded.
26	unsupported certificate purpose	The supplied certificate cannot be used for the specified purpose.
27	certificate not trusted	The root CA is not marked as trusted for the specified purpose.
28	certificate rejected	The root CA is marked to reject the specified purpose.
29	subject issuer mismatch	The current candidate issuer certificate was rejected because its subject name did not match the issuer name of the current certificate. Only displayed when the -issuer_checks option is set.

Error Number	Message	Description
30	authority and subject key identifier mismatch	The current candidate issuer certificate was rejected because its subject key identifier was present and did not match the authority key identifier current certificate. Only displayed when the -issuer_checks option is set.
31	authority and issuer serial number mismatch	The current candidate issuer certificate was rejected because its issuer name and serial number was present and did not match the authority key identifier of the current certificate. Only displayed when the -issuer_checks option is set.
32	key usage does not include certificate signing	The current candidate issuer certificate was rejected because its keyUsage extension does not permit certificate signing.
50	application verification failure	An application specific error. Unused.

Export Database

Export Database

The Database Export utility allows you to save sequence of events and analog data logger points from your MCP device to your local computer in comma-separated values (CSV) format.

» To export data using the Export Database utility:

1. Click the **Export Database > Export (button)** on the **Utilities** page.
   Result: The Export Database utility is launched in a new window.
2. Click the ellipsis button (**...**) next to the **Path** field and select the directory where the .csv files is to be stored.
   NOTE: In Local HMI, the logs (.csv files) must be exported to **/home/hmi/logs** or into the USB mounted on the MCP.
3. Enter the **Start Date** using the pattern shown in the field or select **Earliest Record**.
4. Enter the **End Date** using the pattern shown in the field or select **No End Date**.
5. Select the data sources to be exported. If **Sequence of Events** is selected, all SOE data within the configured timeframe is included. If **Analog Datalogger** is selected, a tree view is shown allowing you to select the specific points, reports, or report types to be included.
6. Click the **Extract** button.

The status bar displays the progress of the operation. All downloaded files are stored in a sub-folder within the configured path (the name of the subfolder is the date and time of the export). Once the export task is complete, the status bar shows the message, *<Time and date> Download Complete*.

Refer to Export Database CSV Files for an explanation of the files that may have been exported.

NOTES:

- The Export Database utility does not support simultaneous export by multiple users. You should verify that no other export operations are in progress before beginning a new one.
- If no data logger records exist within the selected timeframe, the exported file contains one entry that shows the first available value before the selected start time. This does not apply to SOE records.
- In Local HMI, the logs (.csv files) must be exported to **/home/hmi/logs** or into the USB mounted on the MCP.

» To download all records that have been created since your last export:

1. Select the path where you stored the files from the previous export. You should select the higher-level directory and not the subfolder containing the CSV files that were downloaded.
2. Click the **Load Settings** button. The options that were previously selected are restored.
3. Ensure that the **Continue from last download** checkbox is enabled. This automatically downloads the new records.
   If the selection of data sources is changed, the **Continue from last download** feature is not available.
4. Click the **Extract** button.

This procedure can be repeated as often as desired to keep the local export files current. As before, all downloaded files are stored in a new subfolder within the configured path (the name of the subfolder is the date and time of the export).

Interrupted Transfers

If an export is cancelled or interrupted before all records are transferred, one of two actions may occur.

- If an SOE export was interrupted, there is no option to resume the export. You can either overwrite the partially downloaded file with new data or you can save the new data file in a different directory.
- If a Data Logger export was interrupted, a warning message appears during the next export operation. If you click **Yes**, the utility completes the download that was interrupted using the previously configured options (any new options selected are ignored). If you click **No**, the utility exports the data from the beginning based on the settings configured. You can choose to overwrite the existing partial data files or to save them in a different directory.

Export Database .CSV Files

The following files are created when the Export Database utility is used to export data from your MCP device.

In Local HMI, the logs (.csv files) must be exported to **/home/hmi/logs** or into the USB mounted on the MCP.

Sequence of Events

SOE data is exported directly from the MCP system database to a single .csv file.

SOEvents.csv

Table 6.295: Sequence of Events

Field	Description
Record ID	A unique numerical identifier for the record.
Source Point ID	The unique numerical identifier of the point referenced in the record.
Source Point Reference	The short user-defined name for the source point.
Source Point Description	The user-defined block of text that provides a detailed and localized description of the source point.
Point Type	The type of point that the source point is, either single or double point.
Event Value	The binary state of the point, either *0* or *1*.
Event Date	The date and time of the record.
Originator	The source of the control command. See Originators for more information. *0* indicates "Not Supported".

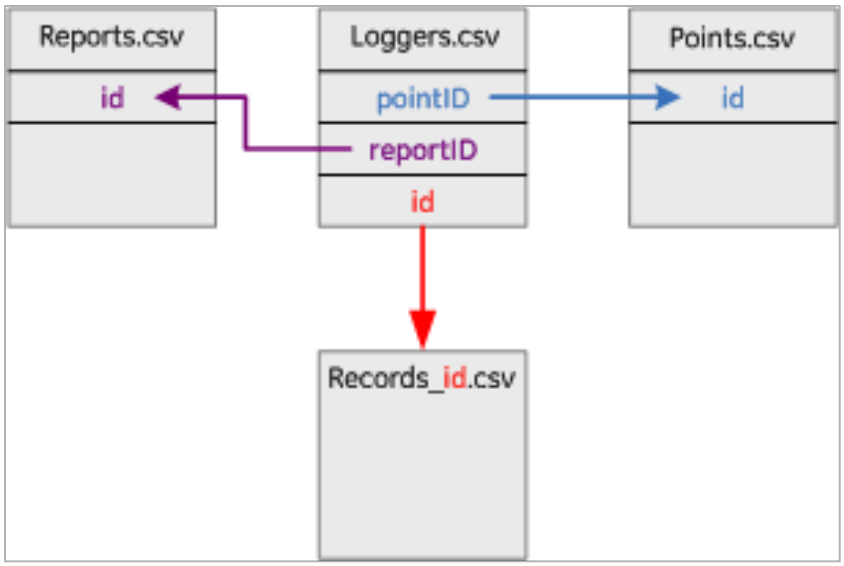
Field	Description
Quality	For most events, this field equals *32768* or *0*. If this field contains *32768*, the time values in the *EventSec*, *EventuSec*, and *EventTimeVal* fields were populated based on the time stamp from the device. If this field contains *0*, the protocol reporting the event does not support time stamps, so the event was time stamped by the MCP when it was received from the device. In some places, quality attributes (flags) are presented as a numeric value instead of a list of discrete flags. To determine which quality flags are set, please refer to the Quality Attributes section on page no. 116.
State Description	The user-defined description for the binary state of the point.
Home Directory	The Home Directory of the device or application that generated the record.
Line ID	The user-defined line ID for the device or application that generated the record.
Device ID	The user-defined ID for the device or application that generated the record.
Bay ID	The user-defined bay ID for the device or application that generated the record.
Device Type	The user-defined map file or device type, as applicable

NOTE: In Local HMI, the logs (.csv files) must be exported to **/home/hmi/logs** or into the USB mounted on the MCP.

Data Logger

Data logger records are exported across several .csv files. These relational tables can be linked together using several fields.

Figure 6.6 Data Logger - Data Flow



The Loggers.csv file contains one row for each trend exported from the Data Logger. Each logger row can be linked to a report using the *Report ID* field (linked to the *ID* field in Reports.csv), to a point in the points table with the *Point ID* field (linked to the *ID* field in Points.csv), and to the dataset itself, which is stored in a file called Records_*n*.csv, where *n* is the ID field in Loggers.csv.

Reports.csv

This csv report file contains information on all exported Data Logger reports.

Table 6.296: Data Logger - Reports

Field	Description
ID	A unique numerical identifier for the report.
Type	The report type, either: • ContinuousReport, • PeriodicReport, or • OutofRangeReport.
Name	The user-defined name for the report.
Active	Whether the report is enabled on the MCP device, either *Active*, or *Deactivated*.
inTriggeredState	Records if the report was in the Triggered state at the time of export, either *TRUE* or *FALSE*.
File Size	The amount of disk space, in bytes, allocated for the report within the Data Logger Configuration Tool on the MCP device.
Usage	The amount of disk space, in bytes, the report is currently consuming.
Percentage	The percentage of disk space used by the report divided by the amount of disk space allocated for it.

Points.csv

This csv report file contains a listing of all unique points referenced in the reports. Though points may be referenced multiple times in different reports, they only appear once in this file.

Table 6.297: Data Logger - Points

Field	Description
ID	A unique numerical identifier for the point.
DataType	The data type of the point, currently only *ANALOG_IN* is supported.
IED	The user-defined name for the device that contains the point.
Point Ref	Point Reference, the short user-defined name for the source point.
PointDescription	The user-defined block of text that provides a detailed and localized description of the source point.
numLoggers	The number of loggers assigned to this point.

Loggers.csv

This csv report file contains a listing of all the trends that were exported. There is one record for each point in each report (that is, points referenced in multiple reports are repeated in this table).

Table 6.298: Loggers

Field	Description
ID	A unique numerical identifier for the logger. The number shown here corresponds to Records_*n*.csv, which contains the dataset for this logger.
ReportID	A numerical reference to the ID field in the *Reports.csv* file.
PointID	A numerical reference to the ID field in the *Points.csv* file.
OldestRecordID	The ID of the oldest record contained in the corresponding *Records_n.csv* file.
OldestTime	The timestamp of when the oldest record was created (based on the MCP device clock).
OldestMSecs	The milliseconds portion of the *oldestTime* timestamp (based on the MCP device clock).
NewestRecordID	The ID of the newest record contained in the corresponding *Records_n.csv* file.
NewestTime	The timestamp of when the newest record was created (based on the MCP device clock).
NewestMSecs	The milliseconds portion of the *newestTime* timestamp (based on the MCP device clock).

Records_n.csv

One .csv file is created for each logger trend above. The *n* in the filename corresponds to the *ID* field shown in the *Loggers.csv* file.

Table 6.299: Records_n

Field	Description
ID	A unique numerical identifier for the row.
Time	The timestamp of when the record was created (based on the MCP device clock).
MSecs	The milliseconds portion of the timestamp (based on the MCP device clock).
Value	The recorded value.
Quality	The recorded quality flag, if available.

Generate Gateway Key Pair

Generate Public/Private key pairs in the Gateway/MCP for the SSH terminal session.

This MCP HMI utility provides an option to:

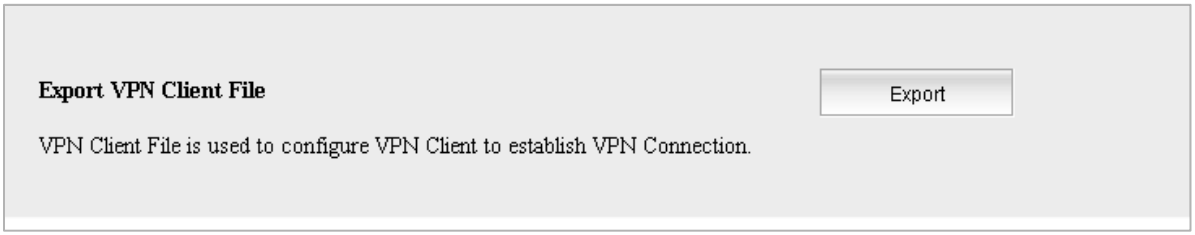
- Save the generated Public key to the host computer
- Delete the existing keys

Exporting VPN Client Configuration File

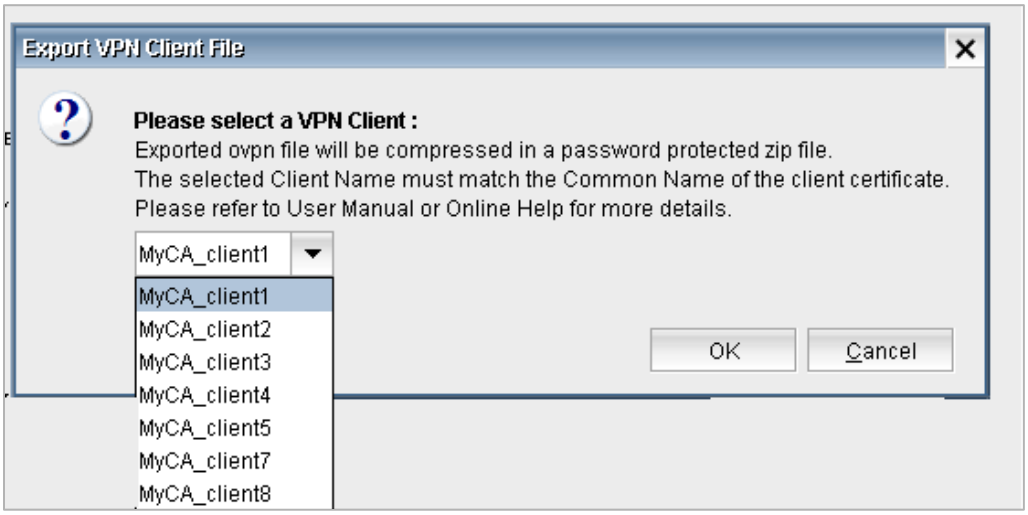
The VPN client configuration file is generated by the MCP. This client configuration is archived with password protection into a file and exported into a PC or a shared location using option Export VPN Client File from the Utilities button .

To export a VPN Client file:

1. Go to Export VPN Client File option and click the **Export** button.

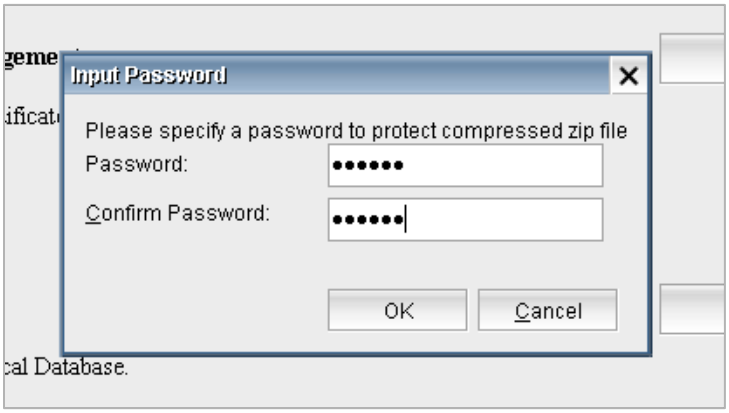


2. Select the Client from configured drop-down list of configured Clients.

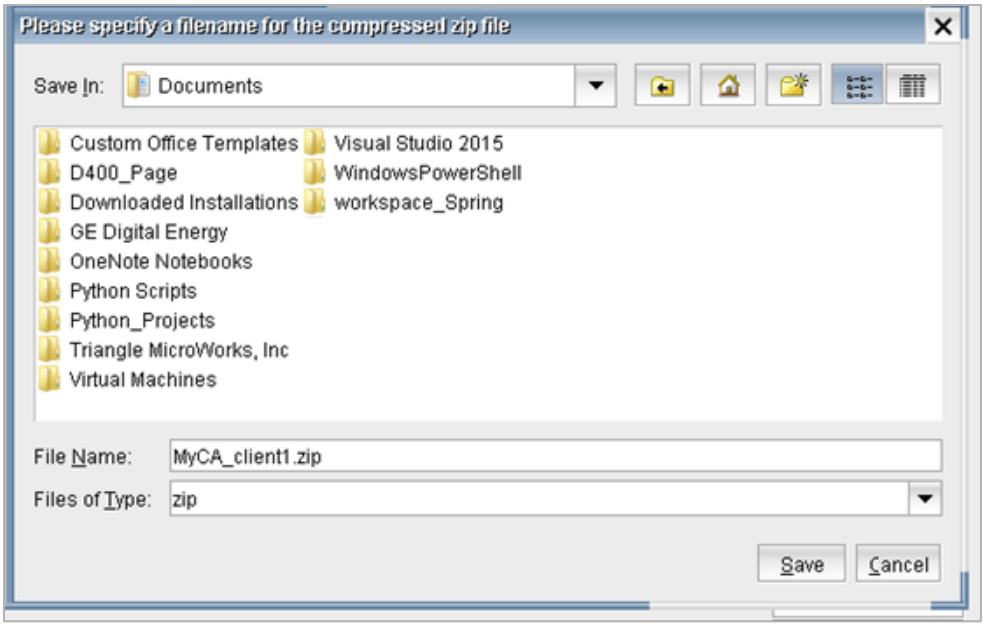


3. Select the Local Gateway IP Address to which the VPN Client will need to connect from the list of Configured IP Address of the MCP.

4. Enter the Password to save the Client Configuration file in protected &compressed format. You need to use the same password to uncompress the Client configuration file using 7Zip or WinRAR software.



5. Securely save the file into a PC/Shared Location/USB.



NOTE: Exporting VPN Client Configuration options is also available through File Explorer functionality in Local HMI. The compressed Client Configuration file is available in the USB.

Upload SSL server Certificate/Server Key

When MCP first time boots up, it will create a default SSL server certificate and server key for HTTPS communication. Alternatively, the MCP allows users with administrator privilege to upload their own SSL server certificate and private key by using DSAS (method 1) or Local HMI Utilities (method 2).

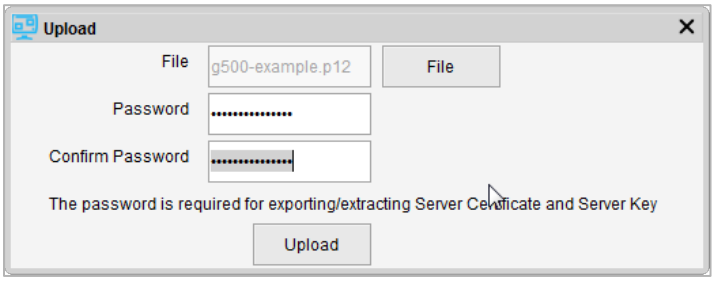
In the MCP, a p12 file (RFC 7292 – PKCS #12: Personal Information Exchange Syntax v1.1) is used for the certificate and private key transfer. Create the p12 file by exporting the server certificate and its private key. The MCP supports the password privacy and password integrity modes defined by PKCS#12, and they must share the same password.

When creating a p12 file you'll be asked to create an export password. You will be prompted for this password later.

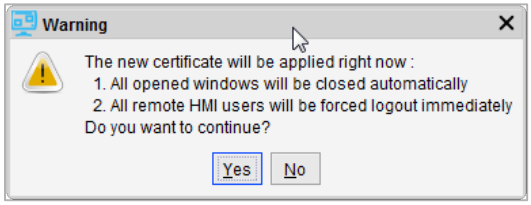
Method 1: To upload SSL Server Certificate/Server Key from DSAS:

1. Go to "Upload SSL Server Certificate/Server Key" option and click the **Upload** button.

2. Select the p12 file by clicking the **File** button and then input/confirm the export password. Then click the "**Upload**" button to start uploading the bundle.



3. Then a warning window will pop up. If you understand and accept, then click "Yes" button to proceed.

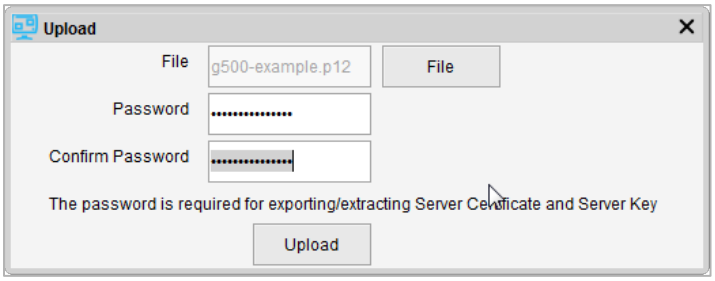


If the upload succeeds, the current online editor will be closed automatically. You will need to reconnect to the MCP due to the new p12 file being applied.

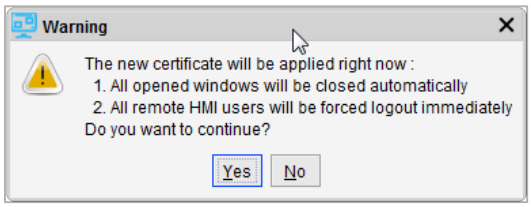
Method 2: To upload SSL Server Certificate/Server Key from the Local HMI:

1. Copy the p12 file to a USB flash drive formatted with FAT32 (must have a partition table).
2. Insert the USB flash drive into a USB slot on the MCP.
3. Open the file explorer from the top Power Bar and select **Mount USB**.
4. Go to "Upload SSL Server Certificate/Server Key" option and click the **Upload** button.

5. Select the p12 file by clicking the **File** button and browse to the USB flash drive. Input/confirm the export password, and then click the "**Upload**" button to start uploading the p12 file.



6. Then a warning window will pop up. If you understand and accept, then click "Yes" button to proceed.



There is no need to restart the local HMI because it uses an internal connection, which doesn't require a certificate.

Miscellaneous Utilities

This chapter contains the following sections:

Utilities Overview
Setting up a Terminal Session
Pass-Through Connections
Direct Connect (mcpconnect)
MCP Configuration Manager

Utilities Overview

Configuration information related to the MCP system is changed using utility programs that are installed on the MCP platform.

The MCP system utilities are typically used during the initial setup of the MCP and for changing the basic configuration of the system, including the network connections, system date and time, and administrator passwords.

The utilities are intended for use by service personnel and application engineers responsible for setting up and maintaining the MCP. Because of the advanced functionality, it is helpful to have basic knowledge of Telnet, ftp and Linux commands to execute the commands for your specific system setup.

The MCP includes the following utility programs:

- MCP Configuration Manager
- Direct Connect (mcpconnect)
- Software licensing tools

These advanced MCP configuration and system administration functions are available at the MCP command line interface.

Setting up a Terminal Session

You can access these system utilities directly at the MCP command prompt through the local maintenance port through the Utilities Power bar button in the MCP HMI. The Utilities page provides a Secure Shell (SSH) login to establish a remote terminal session with the MCP.

Access to the command line interface requires an Administrator or root log in.

NOTE: When accessing the MCP with an Administrator-level user account, you may not have enough security privileges to execute the commands listed in this manual. If this occurs, type **sudo** in front of each command.

SSH Log In

For security reasons, some advanced MCP configuration and system administration functions are available only at the MCP command line interface. The Utilities page provides a Secure Shell (SSH) login to establish a remote terminal session with the MCP.

You must have Supervisor-level access to proceed with SSH Log In. Access to the command line interface requires an additional Administrator log in.

If the Utilities Log In page shows a Utilities Login via SSH button, the security portal has been configured for a Secure Shell (SSH) login.

» To log in:

1. Click Utilities Login > **SSH** button.
2. Enter your Administrator username.
3. Click **OK** to verify the MCP unit name.
4. Enter your Administrator password.
   Result: If your login is successful, the command line interface appears.

Pass-Through Connections

For client applications that support pass-through connections, these connections are accessible through a TCP port on the MCP. You can connect to the device through the MCP using PC-based configuration tools and, if necessary, COM port redirection software.

» To enable client pass-through connections:

1. Click the **Configuration** Power bar button.
2. Click the **Systemwide** tab.
3. Click **System** in the left-hand menu and the select the **Security** tab.
4. For **Pass-Through and Terminal Server Access**, select **Allow Network Connections**.
   Result: The port number is automatically assigned as 8000 plus the serial port number the client is using. For example, if the client is configured to use serial port 1, the pass-through connection port is 8001.

To enable pass-through connections on a serial port without enabling a client application, the port must be configured as an automatic terminal server.

» To enable pass-through connections without a client application:

1. On the **Connection** tab of the MCP Online Configuration Tool, configure the port as **Terminal Server**.
2. Set the Startup parameter to **Automatic**.
3. On the **Systemwide** tab of the MCP Online Configuration Tool, click **System** in the left-hand menu and then select the **Security** tab.
4. Go to the **Connection** tab, click **Secure Type** and select the **Telnet** option from the drop-down list.

For Pass-Through and Terminal Server Access, select Allow Network Connections.

The port number is automatically assigned as 8000 plus the serial port number. For example, if the terminal server is assigned to serial port 2, the pass-through connection port is 8002.

SSH Secure Tunnel Pass-Through Connections

For client applications that supports SSH secure tunnel pass-through connections, you can connect to the device through the MCP using SSH Client (e.g. Secure Terminal Emulator from DS Agile MCP Studio) configuration tools. These connections are accessible through an SSH port on the MCP.

» To enable client supported SSH Secure Tunnel pass-through connections:

1. Click the **Configuration** Power bar button.
2. Click the **Systemwide** tab.
3. Click **System** in the left-hand menu and then select the **Security** tab.
4. For **Pass-Through and Terminal Server Access,** select **Allow Network Connections**.
   Result: The port number is automatically assigned as 8000 plus the serial port number the client is using. For example, if the client is configured to use serial port 1, the pass-through connection port is 8001.
5. Select **SSH Security Tunnel Idle Timeout** under the **Security** tab and change (if you want to change the default value of 120 seconds).
6. Go to the **Connection** tab, click **Secure Type** and select the **SSH Secure Tunnel** option from the drop-down list.

To enable SSH Secure pass-through connections on a serial port without enabling a client application, the port must be configured as an automatic terminal server.

» To enable SSH Secure Tunnel pass-through/Terminal Server connections without a client application:

1. On the **Connection** tab of the MCP Online Configuration Tool, configure the port as **Terminal Server**.
2. Set the Startup parameter to **Automatic**.
3. On the **Systemwide** tab of the MCP Online Configuration Tool, click **System** in the left-hand menu and then select the **Security** tab.
4. Select **Allow Network Connections** for **Pass-Through and Terminal Server Access.**
5. Select **SSH Security Tunnel Idle Timeout** under the **Security** tab and change (if you want to change the default value of 120 seconds).
6. Go to the **Connection** tab, click **Secure Type** and select the **SSH secure tunnel** option from the drop-down list.

For **SSH secure tunnel Pass-Through and SSH secure tunnel Terminal Server Access**, select **Allow Network Connections**.

The port number is automatically assigned as 8000 plus the serial port number. For example, if the terminal server or pass through enabled client connection is assigned to serial port 2, the SSH Secure Tunnel terminal server or client pass-through connection port is 8002.

Use SSH client software (e.g., Secure Terminal Emulator from DS Agile MCP Studio) in a PC and connect to the pass-through server port or terminal server port.

For Security reasons, SSH Secure Tunnel Pass Through and Terminal Server Connections are available only to the Administrator and SSHPassThrough level users only. Refer to User Management Section for details about SSHPassThrough User Role.

Direct Connect (mcpconnect)

Using the mcpconnect utility, you can communicate directly with devices via the MCP. The mcpconnect utility establishes a terminal session with a device connected to one of the MCP serial ports and transfers binary data without modification.

The direct connect utility is set up at the MCP command prompt.

NOTE: You cannot launch the mcpconnect utility on a serial port that already has an automatic terminal server configured.

» To start mcpconnect:

1. Connect and configure devices in the MCP Configuration Tool.
2. Start a terminal session and log into the MCP.
3. At the MCP#>>, enter the following commands:
   cd /home/MCP_APPS/
   ./mcpconnect –d -u <*MCP port number*>
   For example, the command in the format *./mcpconnect –d -u 1* enables communications to a device connected to Serial Port 1 on the MCP.
   The device command prompt appears.
4. Configure or query the connected device as usual.

Tip Type **./mcpconnect –h** to view help information about the tool. Type **./mcpconnect –hx** for documentation on extended options of the tool.

» To exit mcpconnect:

- Press **CTRL** + **C**, and press **Enter**.
  Result: The MCP command prompt appears.

MCP Configuration Manager

The MCP Configuration Manager provides two modes of operation. In redundant systems (not supported by G100), the utility synchronizes configurations between the two MCP units to ensure that both are configured identically. In non-redundant setups, you may launch it manually to copy configurations from the current MCP to another MCP connected over a network or to a location in the MCP's file system, like a connected USB drive.

In redundant systems (not supported by G100), the MCP Configuration Manager can also be activated by operating the *SyncConfig* digital output point, which copies the configuration from the active unit to the standby unit. See MCP Redundancy Manager for more information.

NOTE: The MCP Configuration Manager does not synchronize the configuration parameters defined in the *mcpcfg* utility. You must apply these settings manually.

» To use the MCP Configuration Manager:

1. Start a terminal session and log into the MCP.
2. At the prompt, enter the following command:
   cd /home/MCP_APPS/
   ./configmgr.pl <*command line parameters*>

When executing the application, the following command-line parameters are accepted:

Table 6.300: MCP Configuration Manager - Command Line Parameters

Parameter	Description	Arguments
-m	Mode	*network*, *local*, or *tar*.
-i	IP Address (network mode only)	The IP Address of the remote MCP device.
-l [Lower-case L]	Local Path (local and tar modes only)	The local path to transfer the configuration to. In local mode, the entire directory structure containing the configuration files is copied to a specified location (for example, the path to a USB drive may be */dev/sda1)*. In tar mode, the configuration files are stored in a single compressed archive file. When specifying the path, include a filename ending in **.tar.gz**
-u	Username (network mode only)	Username that is used to access the remote MCP unit.
-p	Password Prompt (network mode only)	*yes*, *no*. If a password is required to access the network MCP device, entering *yes* for this parameter prompts you for a password during the connection. If *no* is entered, SSH key authentication must be enabled to allow communication between the MCP devices. (See Sync Manager for more information about SSH key authentication.) If the –p parameter is not specified, the default action is *yes*.
-f	Reset Flag	*yes, no*. Entering *yes* triggers a restart of all applications running on the remote MCP device once the configuration has been synchronized. If *no* is entered, the applications are not restarted. If the –f parameter is not specified, the default action is *no*.

For example, to trigger a network synchronization followed by a restart of the applications running on the remote unit, you would enter the command:

./configmgr.pl –m network –i <IP Address of remote computer> -u <username of remote MCP unit> -p yes -f yes

If the transfer of the configuration is successful, a confirmation notice appears. If any errors occur, a description of the failure is shown.

Chapter 7 - MCP Pseudo Points

This chapter contains the following sections:

Application Pseudo Points
Analog Reports
Calculator
Data Logger
Digital Event Management
DNP 3.0 Serial with MCP as Master Application
DNP 3.0 Serial with MCP as Slave Application
DNP 3.0 Ethernet with MCP as Master Application
DNP 3.0 Ethernet with MCP as Slave Application
GENASCII Serial with MCP as Master Application
IEC 60870-5-101 with MCP as Master Application
IEC 60870-5-101 with MCP as Slave Application
IEC 60870-5-104 with MCP as Master Application
IEC 60870-5-104 with MCP as Slave Application
IEC 60870-5-103 with MCP as Master Application
IEC 61850 with MCP as Master Application
IEC 61850 Application – Global Points
IEC 61850 Application – Per-Device Points
Load Shed
LogicLinx
Modbus Ethernet with MCP as Master Application
Modbus Ethernet with MCP as Slave Application
Modbus Serial with MCP as Master Application
Modbus Serial with MCP as Slave Application
Redundancy Manager
SEL Binary Serial with MCP as Master Application
System Status Manager
D.20 Peripheral Link Client Pseudo Points
GPIO Client Pseudo Points

Application Pseudo Points

Applications may provide status information and allow functions or operations to be initiated through system and/or device level pseudo points. These points can be accessed through the Point Summary page of the Online HMI.

» **To access device-level and system-level pseudo points:**

1. Log into the online HMI of the MCP unit.
2. Click the **Point Details** button on the toolbar.
3. For device-level pseudo points, click the **IED** tab. A row appears for the IEC 61850 DCA application with a home directory and other details as per the user configuration.
   For system-level pseudo points, click the **Application** tab, and select the **IEC61850Client** application.
4. Click the **Details** button for the selected application.
5. Select the appropriate point type tab to view all points belonging to the group.
6. To send a control request, right-click the point and select **Digital Output Interface**.

Analog Reports

Analog Reports – Analog Input Points

Table 7.1: Analog Reports – Analog Input Points

Pseudo Point Name	Description
Current Percentage Disk Usage	Indicates disk usage in percent against total disk size configured.
Days until Storage Space Available	Estimated number of days that the disk will be full.
Total Report Count	Indicates the total number of reports currently available on disk.
Total Shift Report Count	Indicates the total number of shift type reports currently available on disk.
Total Daily Report Count	Indicates the total number of daily type reports currently available on disk.
Total Weekly Report Count	Indicates the total number of weekly type reports currently available on disk.
Total Monthly Report Count	Indicates the total number of monthly type reports currently available on disk.

Analog Reports – Digital Input Points

Table 7.2: Analog Reports – Digital Input Points

Pseudo Point Name	Description
Storage Space Full	Set to FULL if disk usage exceeds threshold value. Set to AVAILABLE if disk usage does not exceed threshold value.

Calculator

Calculator – Accumulator Points

Table 7.3: Calculator – Accumulator Points

Pseudo Point Name	Description
CommandsReceived	Updated whenever a Control is received
RxdCommandsFailed	Updated whenever a command received by the Calculator DTA fails.
Commands Txd	Updated whenever the Calculator DTA transmits a control request
TxdCommandsFailed	Updated whenever a command transmitted by the Calculator DTA fails.

Calculator – Analog Input Points

Table 7.4: Calculator – Analog Input Points

Pseudo Point Name	Description
TimerCount	Indicates the number of Timers configured.
CalcPointCount	Indicates the number of Calculator Points configured.

Calculator – Digital Input Points

Table 7.5: Calculator – Digital Input Points

Pseudo Point Name	Description
ConfigError	Indicates if errors were detected: • Indicates 0 if no errors were detected. • Indicates 1 if errors were detected.
CalcStatus	Indicates if the Calculator application is functional: • Indicates 1 if the application is functional. • Indicates 0 if application cannot proceed (because of a Config error etc.)
DeviceDisabled	Indicates if the Calculator application is disabled or enabled: • Indicates 1 if the Calculator application is disabled. • Indicates 0 if the Calculator application is running. **NOTE**: The Calculator application can be disabled or enabled through the Disable Device Digital Output pseudo point.

Calculator – Digital Output Points

Table 7.6: Calculator – Digital Output Points

Pseudo Point Name	Description
DisableDevice	Provides an option to disable/enable the Calculator application (DTA): • Set to 1 to disable the Calculator application. • Set to 0 to enable the Calculator application.

Data Logger

Data Logger – Analog Input Points

Table 7.7: Data Logger – Analog Input Points

Pseudo Point Name	Description
Active Report Count	Indicates how many configured Reports are active
Continuous Report (nn): Storage	Analog Input Displays the % of the configured log space that has been used for Continuous Report(nn).
Periodic Report (nn): Storage	Analog Input Displays the % of the configured log space that has been used for Periodic Report(nn).
Out of Range Report (nn): Storage	Analog Input Displays the % of the configured log space that has been used for Out of Range Report(nn).

Data Logger – Digital Input Points

Table 7.8: Data Logger – Digital Input Points

Pseudo Point Name	Description
Application Status	Set when the application is running.
Configuration Error	Set when a configuration error is detected.

Data Logger – Digital Output Points

Table 7.9: Data Logger – Digital Output Points

Pseudo Point Name	Description
Disable Logging	When set to ON, this point disables logging for all Reports.
Reset All Logs	When set to ON, this point clears the log data of all log records.
Continuous Report (nn): Disable	When set to ON, this point disables logging for the associated Continuous Report(nn).
Continuous Report (nn): Reset	When set to ON, this point clears the log data of all log records for the associated Continuous Report(nn).

Digital Event Management

Digital Event Manager – Analog Input Points

Table 7.10: Digital Event Manager – Analog Input Points

Pseudo Point Name	Description
Total Number of Alarms	The total number of alarm records in the database including the uncommitted records.

Total Number of UnAck Alarms	The total number of Unacknowledged alarm records in the database including the uncommitted records.
TotalAlarmsDesc-GrpCritical	The total number of alarm records for alarms in the Critical group.
TotalAlarmsDesc-GrpDefault	The total number of alarm records for alarms in the Default group.

Digital Event Manager – Digital Input Points

Table 7.11: Digital Event Manager – Digital Input Points

Pseudo Point Name	Description
Unacknowledged Alarms	TRUE if there are alarm records that are not in reset and not acknowledged.
Points in Alarm	TRUE if there are alarm records that are not in reset.
Points Suppressed	One or more digital inputs in the MCP are in the forced, alarm inhibited, or scan inhibited state.
GroupUnAckDesc-GrpCritical	TRUE if there are alarm records for any alarm in the Critical group that are not acknowledged.
GroupInAckDesc-GrpCritical	TRUE if there are alarm records for any alarm in the Critical group that are not in reset.
GroupInAlarmReFlashDesc-GrpCritical	TRUE if a new alarm record has occurred for any alarm in the Critical group for the configured Alarm Group Reflash Time.
GroupUnAckDesc-GrpDefault	TRUE if there are alarm records for any alarm in the Default group that are not acknowledged.
GroupInAlarmDesc-GrpDefault	TRUE if there are alarm records for any alarm in the Default group that are not in reset.
GroupInAlarmReFlashDesc-GrpDefault	TRUE if a new alarm record has occurred for any alarm in the Default group for the configured Alarm Group Reflash Time.

Digital Event Manager – Digital Output Points

Table 7.12: Digital Event Manager – Digital Output Points

Pseudo Point Name	Description
AcknowledgeOrphanAlarms	A latch ON, close, or pulse on operation for this point acknowledges all orphan alarms in the MCP.
GrpAckDesc-GrpCritical	A latch ON, close, or pulse on operation for this point acknowledges all alarms in Critical group.
GrpAckDesc-GrpDefault	A latch ON, close, or pulse on operation for this point acknowledges all alarms in the Default group.

DNP 3.0 Serial with MCP as Master Application

DNP 3.0 Serial with MCP as Master – Accumulator Points

Table 7.13: DNP 3.0 Serial with MCP as Master – Accumulator Points

Pseudo Point Name	Description
UpdateCount	Accumulation for the total number of points the RTDB has been updated for this DNP Slave.
MsgSent	Accumulation for the total number of requests sent by the DNP DCA to this DNP Slave.
MsgReceived	Accumulation for the total number of responses received by the DNP DCA from this DNP Slave.
MsgTimeOuts	Accumulation for the number of message timeouts detected by the DNP DCA for this DNP Slave.
MsgError	Accumulation for the total number of responses received in error from this DNP Slave.
OperationsRequested	Accumulations for the number of control requests received by the DNP DCA via the RTDB that was directed to this DNP Slave.
OperationsFailed	Accumulations of the number of operation failures detected for this DNP Slave.

DNP 3.0 Serial with MCP as Master – Digital Input Points

Table 7.14: DNP 3.0 Serial with MCP as Master – Digital Input Points

Pseudo Point Name	Description
Device Online	Indicates if the Configured DNP Slave is Online (1) or Offline (0).
IEDCommDeviceRestart	This status point is set when the DNP DCA receives a Device Restart IIN from the DNP Slave. The status is reset otherwise.
IEDCommBadConfig	This status point is set when the DNP DCA receives a BAD CONFIG IIN from the DNP Slave. The status point is reset when the DNP Slave does not transmit IINs with BAD CONFIG bit set.
IEDCommNeedTime	This status point is set when the DNP DCA receives a NEED TIME IIN from the DNP Slave. The status point is reset when the DNP Slave does not transmit IINs with NEED TIME bit set.
IEDCommLocal	This status point is set when the DNP DCA receives a LOCAL IIN from the DNP Slave. The status point is reset when the DNP Slave does not transmit IINs with LOCAL bit set.
IEDCommDevTroble	This status point is set when the DNP DCA receives a DEVICE TROUBLE IIN from the DNP Slave. The status point is reset by the DNP DCA when the DNP Slave does not transmit IINs with DEVICE TROUBLE bit set
IEDCommBadFunc	This status point is set when the DNP DCA receives a BAD FUNCTION IIN from the DNP Slave. The status point is reset when the DNP Slave does not transmit IINs with BAD FUNCTION bit set
IEDCommObjectUnknown	This status point is set when the DNP DCA receives an OBJECT UNKNOWN IIN from the DNP Slave. The status point is reset when the DNP Slave does not transmit IINs with OBJECT UNKNOWN bit set

IEDCommParamError	This status point is set when the DNP DCA receives a PARAMETER ERROR IIN from the device. The status point is reset when the DNP slave does not transmit IINs with PARAMETER ERROR bit set
IEDCommBufferOverFlow	This status point is set when the DNP DCA receives a BUFFER OVERFLOW IIN from the DNP Slave. The status point is reset when the DNP slave does not transmit IINs with BUFFER OVERFLOW bit set
IEDCommAlreadyExec	This status point is set when the DNP DCA receives an ALREADY EXEC IIN from the DNP Slave. The status point is reset when the DNP slave does not transmit IINs with ALREADY EXEC bit set
IEDCommAllStations	This status point is set when the DNP DCA receives an ALL STATIONS IIN from the DNP Slave. The status point is reset when the DNP Slave does not transmit IINs with ALL STATIONs bit set
DCAStatus	Set if DNP DCA application is enabled.
PrimaryPortActiveStatus	Indicates the status of the Configured Primary Port. Active (1) Inactive (0)
BackupPortActiveStatus	Indicates the status of the Configured Backup Port. Active (1) Inactive (0)
DeviceDisable	Set if DNPDCA application is disabled.
UnsolicitedResponse	Set if a Control (1) is received on the EnableUnsolicited DO Pseudo point.
PollingDisabled	Set if the polling is disabled.

DNP 3.0 Serial with MCP as Master – Digital Output Points

Table 7.15: DNP 3.0 Serial with MCP as Master – Digital Output Points

Pseudo Point Name	Description
DisableDevice	This pseudo control accepts Latch ON/Latch OFF controls. When set (i.e. latched ON), the DNP DCA disables polling to the DNP Slave. Sets all RTDB points belonging to the DNP Slave OFFLINE, and no scheduled data requests are sent to the DNP Slave.
SendTimeSync	This pseudo control accepts Pulse ON/Pulse OFF controls. NTEKA0230FS1.1.10.1.1.2 When pulsed, the DNP DCA transmits a Time Sync message to the DNP Slave
SendRestart	This pseudo control accepts Pulse ON/Pulse OFF controls. When pulsed, the DNP DCA transmits a Cold Restart message to the DNP Slave.
EnableUnsolicited	This pseudo control accepts Latch ON/Latch OFF controls. When set (i.e. latched ON), the DNP DCA enables supporting of Unsolicited Messages sent from DNP Slave.
DisablePolling	This control disables or enables scheduled polling of the device.
IntegrityPoll	When a control request is received from this point, the DCA sends one general interrogation to the device.
ClassPoll	When a control request is received from this point, the DNP DCA sends a Class Poll (Class 1, 2 and 3) to the configured DNP Slave.
SwitchChannel	When a control request is received from this point, the DNP DCA switches to the configured alternate Channel.
ClearStats	When a control request is received from this point, the DNP DCA clears all the values on the Accumulator points.

DNP 3.0 Serial with MCP as Slave Application

DNP 3.0 Serial with MCP as Slave – Accumulator Points

Table 7.16: DNP 3.0 Serial with MCP as Slave – Accumulator Points

Pseudo Point Name	Description
MasterMsgIn	Indicates the number of response messages sent by the DNP Master to the DNPDPA.
MasterMsgOut	Indicates the number of request messages received by the DNP Master to the DNPDPA.
RemMsgAckTimeouts	Indicates number of acknowledgement message time out.
RemOperationRequests	Indicates the number of control operation requests received by DNPDPA from DNP Master.
RemOperationsFailed	Indicates number of control operations failed
BIChangeEventsOut	Indicates the number of binary input change events sent to DNP Master.

DNP 3.0 Serial with MCP as Slave – Analog Input Point

Table 7.17: DNP 3.0 Serial with MCP as Slave – Analog Input Point

Pseudo Point Name	Description
MasterAdd	Indicates DNP Master station address that DNP DPA is communicating with.
DPAProcessID	Indicates DNP DPA child process ID.

DNP 3.0 Serial with MCP as Slave – Digital Input Points

Table 7.18: DNP 3.0 Serial with MCP as Slave – Digital Input Points

Pseudo Point Name	Description
CommStatus	Indicates DNP DPA communication status. Set when communication with DNP Master is Enabled and Unset when Disabled.
DPAStatus	Indicates the DNP DPA Application status. Set when DNP Master application is Enabled and Unset when Disabled.
PriPortStatus	Indicates the health of the configured Primary Port.
BackPortStatus	Indicates the health of the configured Backup Port. Point is Offline mode if not configured.

DNP 3.0 Serial with MCP as Slave – Digital Output Points

Table 7.19: DNP 3.0 Serial with MCP as Slave – Digital Output Points

Pseudo Point Name	Description
ForceControlsLockout	Indicates DNP DPA control disable pseudo point. If set DNP DPA does not accept any control operations from DNP Master, Except the command on same point if same is registered by DNP DPA.

Clear Stats	When a control request is received from this point, the DNP DPA clears all the values on the Accumulator points.

DNP 3.0 Ethernet with MCP as Master Application

DNP 3.0 Ethernet with MCP as Master – Accumulator Points

Table 7.20: DNP 3.0 Ethernet with MCP as Master – Accumulator Points

Pseudo Point Name	Description
UpdateCount	Accumulation for the total number of points the RTDB has been updated for this DNP Slave.
MsgSent	Accumulation for the total number of requests sent by the DNP DCA to this DNP Slave.
MsgReceived	Accumulation for the total number of responses received by the DNP DCA from this DNP Slave.
MsgTimeOuts	Accumulation for the number of message timeouts detected by the DNP DCA for this DNP Slave.
MsgError	Accumulation for the total number of responses received in error from this DNP Slave.
OperationsRequested	Accumulations for the number of control requests received by the DNP DCA via the RTDB that was directed to this DNP Slave.
OperationsFailed	Accumulations of the number of operation failures detected for this DNP Slave.

DNP 3.0 Ethernet with MCP as Master – Digital Input Points

Table 7.21: DNP 3.0 Ethernet with MCP as Master – Digital Input Points

Pseudo Point Name	Description
Device Online	Indicates if the Configured DNP Slave is Online (1) or Offline (0).
IEDCommDeviceRestart	This status point is set when the DNP DCA receives a Device Restart IIN from the DNP Slave. The status is reset otherwise.
IEDCommBadConfig	This status point is set when the DNP DCA receives a BAD CONFIG IIN from the DNP Slave. The status point is reset when the DNP Slave does not transmit IINs with BAD CONFIG bit set.
IEDCommNeedTime	This status point is set when the DNP DCA receives a NEED TIME IIN from the DNP Slave. The status point is reset when the DNP Slave does not transmit IINs with NEED TIME bit set.
IEDCommLocal	This status point is set when the DNP DCA receives a LOCAL IIN from the DNP Slave. The status point is reset when the DNP Slave does not transmit IINs with LOCAL bit set.
IEDCommDevTroble	This status point is set when the DNP DCA receives a DEVICE TROUBLE IIN from the DNP Slave. The status point is reset by the DNP DCA when the DNP Slave does not transmit IINs with DEVICE TROUBLE bit set

IEDCommBadFunc	This status point is set when the DNP DCA receives a BAD FUNCTION IIN from the DNP Slave. The status point is reset when the DNP Slave does not transmit IINs with BAD FUNCTION bit set
IEDCommObjectUnknown	This status point is set when the DNP DCA receives an OBJECT UNKNOWN IIN from the DNP Slave. The status point is reset when the DNP Slave does not transmit IINs with OBJECT UNKNOWN bit set
IEDCommParamError	This status point is set when the DNP DCA receives a PARAMETER ERROR IIN from the device. The status point is reset when the DNP slave does not transmit IINs with PARAMETER ERROR bit set
IEDCommBufferOverFlow	This status point is set when the DNP DCA receives a BUFFER OVERFLOW IIN from the DNP Slave. The status point is reset when the DNP slave does not transmit IINs with BUFFER OVERFLOW bit set
IEDCommAlreadyExec	This status point is set when the DNP DCA receives an ALREADY EXEC IIN from the DNP Slave. The status point is reset when the DNP slave does not transmit IINs with ALREADY EXEC bit set
IEDCommAllStations	This status point is set when the DNP DCA receives an ALL STATIONS IIN from the DNP Slave. The status point is reset when the DNP Slave does not transmit IINs with ALL STATIONs bit set
DCAStatus	Set if DNP DCA application is enabled.
PrimaryPortActiveStatus	Indicates the status of the Configured Primary Port. Active (1) Inactive (0)
BackupPortActiveStatus	Indicates the status of the Configured Backup Port. Active (1) Inactive (0)
DeviceDisable	Set if DNPDCA application is disabled.
UnsolicitedResponse	Set if a Control (1) is received on the EnableUnsolicited DO Pseudo point.
PollingDisabled	Set if the polling is disabled.

DNP 3.0 Ethernet with MCP as Master – Digital Output Points

Table 7.22: DNP 3.0 Ethernet with MCP as Master – Digital Output Points

Pseudo Point Name	Description
DisableDevice	This pseudo control accepts Latch ON/Latch OFF controls. When set (i.e. latched ON), the DNP DCA disables polling to the DNP Slave. Sets all RTDB points belonging to the DNP Slave OFFLINE, and no scheduled data requests are sent to the DNP Slave.
SendTimeSync	This pseudo control accepts Pulse ON/Pulse OFF controls. NTEKA0230FS1.1.10.1.1.2 When pulsed, the DNP DCA transmits a Time Sync message to the DNP Slave
SendRestart	This pseudo control accepts Pulse ON/Pulse OFF controls. When pulsed, the DNP DCA transmits a Cold Restart message to the DNP Slave.
EnableUnsolicited	This pseudo control accepts Latch ON/Latch OFF controls. When set (i.e. latched ON), the DNP DCA enables supporting of Unsolicited Messages sent from DNP Slave.
DisablePolling	This control disables or enables scheduled polling of the device.
IntegrityPoll	When a control request is received from this point, the DCA sends one general interrogation to the device.
ClassPoll	When a control request is received from this point, the DNP DCA sends a Class Poll (Class 1, 2 and 3) to the configured DNP Slave.

SwitchChannel	When a control request is received from this point, the DNP DCA switches to the configured alternate Channel.
ClearStats	When a control request is received from this point, the DNP DCA clears all the values on the Accumulator points.

DNP 3.0 Ethernet with MCP as Slave Application

DNP 3.0 Ethernet with MCP as Slave – Accumulator Points

Table 7.23: DNP 3.0 Ethernet with MCP as Slave – Accumulator Points

Pseudo Point Name	Description
MasterMsgIn	Indicates the number of response messages sent by the DNP Master to the DNPDPA.
MasterMsgOut	Indicates the number of request messages received by the DNP Master to the DNPDPA.
RemMsgAckTimeouts	Indicates number of acknowledgement message time out.
RemOperationRequests	Indicates the number of control operation requests received by DNPDPA from DNP Master.
RemOperationsFailed	Indicates number of control operations failed
BIChangeEventsOut	Indicates the number of binary input change events sent to DNP Master.

DNP 3.0 Ethernet with MCP as Slave – Analog Input Point

Table 7.24: DNP 3.0 Ethernet with MCP as Slave – Analog Input Point

Pseudo Point Name	Description
MasterAdd	Indicates DNP Master station address that DNP DPA is communicating with.
DPAProcessID	Indicates DNP DPA child process ID.

DNP 3.0 Ethernet with MCP as Slave – Digital Input Points

Table 7.25: DNP 3.0 Ethernet with MCP as Slave – Digital Input Points

Pseudo Point Name	Description
CommStatus	Indicates DNP DPA communication status. Set when communication with DNP Master is Enabled and Unset when Disabled.
DPAStatus	Indicates the DNP DPA Application status. Set when DNP Master application is Enabled and Unset when Disabled.
PriPortStatus	Indicates the health of the configured Primary Port.
BackPortStatus	Indicates the health of the configured Backup Port. Point is Offline mode if not configured.

DNP 3.0 Ethernet with MCP as Slave – Digital Output Points

Table 7.26: DNP 3.0 Ethernet with MCP as Slave – Digital Output Points

Pseudo Point Name	Description
ForceControlsLockout	Indicates DNP DPA control disable pseudo point. If set DNP DPA does not accept any control operations from DNP Master, Except the command on same point if same is registered by DNP DPA.
Clear Stats	When a control request is received from this point, the DNP DPA clears all the values on the Accumulator points.

GENASCII Serial with MCP as Master Application

These points comprise:

- DCA Pseudo Points
- IED Pseudo Points

DCA Pseudo Points

Accumulators

Table 7.27: DCA Pseudo Points - Accumulators

Pseudo Point Name	Description
MsgSent	Accumulator for the total number of messages sent to all devices.
MsgReceived	Accumulator for the total number of messages received from all devices.
MsgTimeOuts	Accumulator for the total number of message timeouts detected. It is incremented every time the device has failed to respond to a Request within the allowed timeout.

Digital Input

Table 7.28: DCA Pseudo Points - Digital Input

Pseudo Point Name	Description
DCA Status	Indicates the status of the GenASCII DCA Application. Set to Enabled if DCA Application is initialized correctly. Reset to Disabled if DCA Application failed to initialize correctly.
Enable Polling Of All IEDs Status	Indicates the polling status of all devices. **NOTE**: If "Polling of IED Status" is Enabled for specific device, but "Enable Polling Of All IEDs Status" is Disabled at DCA Level, polling occurs for the respective device. Set to Enabled if polling is Enabled for all devices. Reset to Disabled if polling is Disabled for all devices.

All Devices Disabled	Indicates the disabled status of all devices. **NOTE**: If "DeviceDisable" is Enabled for specific device, but "AllDevicesDisabled" is Disabled at DCA Level, the respective device disabled status is Enabled. Set to Enabled if the status of all devices is Enabled. Reset to Disabled if the status of all devices is Disabled.

Digital Output

Table 7.29: DCA Pseudo Points - Digital Output

Pseudo Point Name	Description
Enable Polling Of All IEDs	This control enables or disables polling status of all devices in multi drop device configuration. If disabled, the polling status of all the individual devices will be disabled. If enabled, the polling status of all the individual devices will be enabled. **NOTE**: If "Enable Polling of IED" DO Pseudo Point is Disabled and if "Enable Polling Of All IEDs" control is Enabled, the polling status of device is given priority. Rest of the devices whose "Enable Polling Of IED" DO Pseudo Point is Enabled will be Enabled.
DisableAllDevices	This control enables or disables the running state of all IEDs. When Set to Enabled, all the individual devices will be enabled unless specific device DO Pseudo Point DisableDevice is in Disabled state. When Reset to Disabled, all the individual devices will be disabled.

IED Pseudo Points

Accumulators

Table 7.30: IED Pseudo Points - Accumulators

Pseudo Point Name	Description
UpdateCount	Accumulator for the total number of points in the RTDB that have been updated for this device.
MsgSent	Accumulator for the total number of messages sent by the Client to the device.
MsgReceived	Accumulator for the total number of messages received by the Client from the device. It is incremented only when the message is received from the device and response is valid.
MsgTimeOuts	Accumulator for the total number of message timeouts detected by the Client for the device. It is incremented every time the device has failed to respond to a Request within the allowed timeout.
MsgError	Accumulator for the total number of frames received in error from the device.

Analog Input

Table 7.31: IED Pseudo Points - Analog Input

Pseudo Point Name	Description
ConfigError	Indicates the number of responses received in error because of misconfiguration. This is detected based on the Invalid Pattern definition of the transaction definition in client map file.

Digital Input

Table 7.32: IED Pseudo Points - Digital Input

Pseudo Point Name	Description
Device Online	Indicates if the Configured device is: • ONLINE (1), or • OFFLINE (0).
Primary Port Active Status	Indicates the usage of configured Primary Port. Set to IN USE if Primary port is in use. Reset to NOT INUSE if not in use.
Backup Port Active Status	Indicates the usage of configured Secondary Port. Set to IN USE if backup port is in use. Reset to NOT INUSE if not configured.
DeviceDisable	Indicates the disabled status of device. **NOTE**: If "DisableAllDevices" control is Disabled, the DeviceDisable DI Pseudo Point will be Disabled. If "DisableAllDevices" control is Enabled, the DeviceDisable DI Pseudo Point will be Enabled only if "DisableDevice" DO Pseudo Point is Enabled. Set to Enabled if the status of device is Enabled. Reset to Disabled if the status of device is Disabled.
Polling Of IED Status	Indicates the polling status of device. **NOTE**: If "Enable Polling Of All IEDs" control is Disabled, the Polling Of IED Status DI Pseudo Point will be Disabled. If "Enable Polling Of All IEDs" control is Enabled, the Polling Of IED Status DI Pseudo Point will be Enabled only if "Enable Polling Of IED" DO Pseudo Point is Enabled. Set to Enabled if polling is Enabled for device. Reset to Disabled if polling is Disabled for device.
His_cmd_support	Indicates support for HIS command for SEL device.
Eve_cmd_support	Indicates support for EVE command for SEL device.
Cev_cmd_support	Indicates support for CEV command for SEL device
File Retrieval In-Progress	Value 1 indicates that file retrieval from the SEL device is in-progress. Value 0 indicates that file retrieval from the SEL device is not in-progress.

Pass Through In-Progress	Value 1 indicates that data transfer through the Pass-Through connection with SEL device is in-progress. Value 0 indicates that data transfer through the Pass-Through connection with SEL device is not in-progress.

Digital Output

Table 7.33: IED Pseudo Points - Digital Output

Pseudo Point Name	Description
DisableDevice	This control enables or disables the running state of the device. When Set to Enabled, the device will be enabled. When Reset to Disabled, the device will be disabled and will be declared as OFFLINE.
ClearStats	This control clears all the communication statistics UpdateCount (MsgSent, MsgReceived, MsgTimeouts and MsgErrors) Pseudo Points of the device.
Enable Polling Of IED	This control disables or enables polling to the device. If set to Disabled, the polling to the device is stopped. If reset to Enabled, the polling to the device will be resumed.

Text Points

Table 7.34: IED Pseudo Points - Text Points

Pseudo Point Name	Description
DEVICEINFO_LINEID	Indicates the Line id of the device.
DEVICEINFO_DEVICEID	Indicates the Device id of the device.
DEVICEINFO_BAYID	Indicates the Bay id of the device.
DEVICEINFO_DEVICETYPE	Indicates the device type.
DEVICEINFO_DEVICEADDRESS	Indicates the device address.
MapFile	Indicates the map file name of the device.

Refer to Time Sequence Diagrams and Sample Configuration for more detailed explanation.

IEC 60870-5-101 with MCP as Master Application

IEC 101 with MCP as Master - Device Level

IEC 101 with MCP as Master – Device Level - Accumulator Points

Table 7.35: IEC 101 with MCP as Master – Device Level - Accumulator Points

Pseudo Point Name	Description
NewEventsReceived	The number of new events received by the IEC 60870-5-104/101 DCA from the device. Incremented immediately after a previously unrecorded event has been reported by the device.
EventsReported	The number of events successfully reported to the RtDB for a Device.
MsgSent	The number of messages sent by the IEC 60870-5-104/101 DCA to the device. It is incremented immediately after a data link frame is sent to the device. The IEC 60870-5-104/101 DCA increments this statistic for each Device that shares the same link addresses.
MsgReceived	The number of messages received by the IEC 60870-5-104/101 DCA from the device. It is incremented immediately after a data link frame has been successfully received from the device. The IEC 60870-5-104/101 DCA increments this statistic for each Device that shares the same link address if the link address of the message is known. If the link address is unknown, this Pseudo point is not incremented.
MsgTimeouts	The number of message timeouts detected by the IEC 60870-5-104/101 DCA for the device. It is incremented every time the device has failed to respond to a confirmed data link frame (i.e. any Primary frame but function code 4 – Send No Reply) within the allowed timeout. The IEC 60870-5-104/101 DCA increments this statistic for each Device that shares the same link address.
MsgError	The number of frames received in error (e.g. checksum failure). Does not include Respond NACK (function code 4) or Confirm NACK (function code 1) frames, as those would be incremented under MsgReceived. The IEC 60870-5-104/101 DCA increments this statistic for each Device that shares the same link address if the link address of the message is known. If the link address is unknown, this pseudo point is not incremented.
UpdateCount	The number of data change events reported to the RtDB for a Device.
CommandsReceived	The number of Output, Local, or Accumulator Commands received from the RtDB.
CommandsFailed	The number of negative command statuses sent to the RtDB.
RxBadTypeID	The number of invalid or unsupported Type Identification messages received from the Device. As a prerequisite to incrementing this statistic, the ASDU address of the message must be known.
UpdateCount	The number of data change events reported to the RtDB for a Device.
MsgSent	The number of messages sent by the IEC 60870-5-104/101 DCA to the device. It is incremented immediately after a data link frame is sent to the device. The IEC 60870-5-104/101 DCA increments this statistic for each Device that shares the same link addresses.

MsgReceived	The number of messages received by the IEC 60870-5-104/101 DCA from the device. It is incremented immediately after a data link frame has been successfully received from the device. The IEC 60870-5-104/101 DCA increments this statistic for each Device that shares the same link address if the link address of the message is known. If the link address is unknown, this Pseudo point is not incremented.
MsgTimeOuts	The number of message timeouts detected by the IEC 60870-5-104/101 DCA for the device. It is incremented every time the device has failed to respond to a confirmed data link frame (i.e. any Primary frame but function code 4 – Send No Reply) within the allowed timeout. The IEC 60870-5-104/101 DCA increments this statistic for each Device that shares the same link address.
MsgError	The number of frames received in error (e.g. checksum failure). Does not include Respond NACK (function code 4) or Confirm NACK (function code 1) frames, as those would be incremented under MsgReceived. The IEC 60870-5-104/101 DCA increments this statistic for each Device that shares the same link address if the link address of the message is known. If the link address is unknown, this pseudo point is not incremented.
NewEventsReceived	The number of new events received by the IEC 60870-5-104/101 DCA from the device. Incremented immediately after a previously unrecorded event has been reported by the device.

IEC 101 with MCP as Master – Device Level – Digital Input Points

Table 7.36: IEC 101 with MCP as Master – Device Level – Digital Input Points

Pseudo Point Name	Description
Device Online	Indicates if the communications with the Device is Active (1) or Inactive (0). The DCA sets this to ON after the initialization procedure with a device completes successfully. The DCA sets this to OFF after communications has been lost with the Device or when the Device is Disabled
DeviceDisable	Indicates if the communications with the Device is disabled. Reflects the status of the DisableDevice Digital Output pseudo point or'ed with the DisableAllDevices Digital Output pseudo point.
PollingDisabled	Indicates if the scheduled polling of the Device is disabled. Reflects the status of the DisablePolling Digital Output pseudo point or'ed with the DisableAllPolling Digital Output pseudo point.
IntegrityPollExecution	Indicates the status of Integrity Poll. In progress (pending: 1) or completed (0). Integrity Poll can be manually triggered either by IntegrityPoll or IntegrityPollAllDevices Digital Output pseudo points
TimeSyncExecution	Indicates the status of the Time synchronization. In progress (pending: 1) or completed (0). Time Synchronization can be triggered by either the TimeSync or the TimeSyncAllDevices Digital Output pseudo point is.
DeviceRestarted	Toggled when Restart or Power On indications are received from the device. Restarted (1) and Running (0) Applicable only to the IEC 60870-5-103 Client.

CounterIntegrityPollExecution	Indicates the status of Counter Integrity Poll. In progress (pending: 1) or completed (0). The Counter Integrity Poll can be triggered by either the CounterIntegrityPoll or CounterIntegrityPollAllDevices Digital Output pseudo points

IEC 101 with MCP as Master – Device Level – Digital Output Points

Table 7.37: IEC 101 with MCP as Master – Device Level – Digital Output Points

Pseudo Point Name	Description
DisableDevice	This control enables or disables communications with the Device.
DisablePolling	When a control request is received from this point, the DCA sends one counter interrogation to the device.
IntegrityPoll	This control disables or enables scheduled polling of the device.
TimeSync	When a control request is received from this point, the DCA issues time synchronization to the device.
CounterIntegrityPoll	When a control request is received from this point, the DCA sends one general interrogation to the device.

IEC 101 with MCP as Master – DCA Level

IEC 101 with MCP as Master – DCA Level - Accumulator Points

Table 7.38: IEC 101 with MCP as Master – DCA Level - Accumulator Points

Pseudo Point Name	Description
MsgSent	Accumulation of the total number of the "MsgSent" accumulator values for all devices managed by the IEC 60870-5-104/101 DCA.
MsgReceived	Accumulation of the total number of the "MsgReceived" accumulator values for all devices managed by the IEC 60870-5-104/101 DCA.
MsgTimeOuts	Accumulation of the total number of the "MsgTimeouts" accumulator values for all devices managed by the IEC 60870-5-104/101 DCA.
RxUnknownASDUAddress	Accumulation of the number of unknown ASDU address messages received on the channel managed by the IEC 60870-5-104/101 DCA.
RxUnknownLinkAddress	Accumulation of the number of unknown link address messages received on the channel managed by the IEC 60870-5-104/101 DCA.
RxFrameErrors	Accumulation of the number of messages with frame errors received on the channel managed by the IEC 60870-5-104/101 DCA.

IEC 101 with MCP as Master – DCA Level - Digital Input Points

Table 7.39: IEC 101 with MCP as Master – DCA Level - Digital Input Points

Pseudo Point Name	Description
DCAStatus	Indicates the status of the IEC 60870-5-104/101 DCA application. Set if IEC 60870-5-104/101 DCA is running. Reset if IEC 60870-5-104/101 DCA is not running.

AllDevicesDisabled	Indicates if all the configured IEC 60870-5-104/101 DCA is disabled. Set if all the IEC 60870-5-104/101 DCA is disabled. Reset if all the IEC 60870-5-104/101 DCA is enabled.
AllPollingDisabled	Indicates if the scheduled polling of all Devices is disabled. Set if polling of all IEC 60870-5-104/101 DCA is disabled. Reset if polling of all IEC 60870-5-104/101 DCA is enabled.

IEC 101 with MCP as Master – DCA Level - Digital Output Points

Table 7.40: IEC 101 with MCP as Master – DCA Level - Digital Output Points

Pseudo Point Name	Description
DisableAllDevices	This control disables or enables communications with all Devices belonging to the IEC 60870-5-104/101 DCA.
IntegrityPollAllDevices	When a control request is received from this point, the IEC 60870-5-104/101 DCA sends one general interrogation to each IEC 60870-5-104/101 slave.
CounterIntegrityPollAllDevices	When a control request is received from this point, the IEC 60870-5-104/101 DCA sends one counter interrogation to each IEC 60870-5-104/101 slave.
TimeSyncAllDevices	When a control request is received from this point, the IEC 60870-5-104/101 DCA issues time synchronization to each IEC 60870-5-104/101 slave.
DisableAllPolling	This control disables or enables scheduled polling of all IEC 60870-5-104/101 slaves.

IEC 60870-5-101 with MCP as Slave Application

IEC 101 with MCP as Slave - Accumulator Points

Table 7.41: IEC 101 with MCP as Slave - Accumulator Points

Pseudo Point Name	Description
MasterMsgIn	Increments immediately after a data link frame has been successfully received from the master. The DPA increments this statistic for each LRU that shares the same link addresses.
MasterMsgOut	Increments immediately after a data link frame is sent to the master, including retries. The DPA increments this statistic for each LRU that shares the same link address.
RemMsgAckTimeouts	For Balanced, number of confirmed frames that did not receive an acknowledgement within the response timeout (calculated as Extra Response Timeout + Timeout from Annex 2 in 870-5-2). The DPA increments this statistic for each LRU that shares the same link address. For Unbalanced, not incremented. For 104, number of unacknowledged frames that were outstanding at the time the connection was dropped due to a timeout.
RemOperationRequests	Number of commands received from the master.
RemOperationsFailed	Number of commands that the Server either rejected or could not execute due to an error.
ASDUDataRequestsReceived	Number of ASDU data requests received

ASDUDataRequestsRejected	Number of ASDU data requests rejected
ASDUDataResponsesSent	Number of ASDU data responses sent
SpontaneousASDUDataMessages Sent	Number of spontaneous ASDU data messages sent
SpontaneousASDUDataMessages NoACK	Number of spontaneous ASDU data messages that did not receive ACK from Master. Not applicable to 101 Unbalanced.
ASDUControlResponsesSent	Number of ASDU control responses sent
ChangeEventsReceivedFromRtDB	Number of RtDB Data, Quality, or Data and Quality change events received.
BufferOverflows	Number of Event buffer overflows detected either in an RtDB FIFO or within the DPA's internal buffers.
RtDBReadRequests	Number of RtDB read requests
RtDBReadFailures	Number of RtDB read failures
RtDBWriteRequests	Number of RtDB write requests
DOAndAOCommandFailures	Number of DO and AO command failures
DOAndAOCommandFailuresDueTo SBOTimeout	Number of DO and AO command failures due to SBO timeout
CommandFailuresDueToControlLo ckout	Number of command failures due to control lockout
AccumulatorCommandsSent	Number of accumulator command requests
AccumulatorCommandsFailed	Number of accumulator command failures
FileTransfersAttempted	Number of file transfers attempted
FileTransfersFailed	Number of file transfers failed

IEC 101 with MCP as Slave – Analog Input Points

Table 7.42: IEC 101 with MCP as Slave – Analog Input Points

Pseudo Point Name	Description
DPAProcessID	Indicates the ID of the DPA Process thread.

IEC 101 with MCP as Slave – Digital Input Points

Table 7.43: IEC 101 with MCP as Slave – Digital Input Points

Pseudo Point Name	Description
CommStatus	Indicates the Communication status of the DPA with the configured Master. Set if the DPA is actively communicating with the Master. Reset if the DPA is not communicating with the Master.
DPAStatus	Indicates the status of the DPA application. Set if the DPA is currently running. Reset is the DPA is not running.
PriPortStatus	Indicates the status of the configured Primary port for communicating with Master. Set while communication is active on the Primary port. Reset while there are no communications on the Primary port.

BackPortStatus	Indicates the status of the configured Backup port for communication. Set while communication is active on the Backup port. Reset while there are no communications on the Backup port.
EventBufferOverFlow	Toggled when the DPA detects an event buffer overflow.
EventBufferLow	Indicates whether an internal DPA event buffer low condition exists.

IEC 101 with MCP as Slave – Digital Output Points

Table 7.44: IEC 101 with MCP as Slave – Digital Output Points

Pseudo Point Name	Description
ForceControlsLockout	Set if the DPA refuses the control requests sent by the configured Master Reset if the DPA accepts the control requests and performs the respective operation.

IEC 60870-5-104 with MCP as Master Application

IEC 104 with MCP as Master - Device Level

IEC 104 with MCP as Master – Device Level - Accumulator Points

Table 7.45: IEC 104 with MCP as Master – Device Level - Accumulator Points

Pseudo Point Name	Description
UpdateCount	The number of data change events reported to the RTDB for a Device.
MsgSent	The number of messages sent by the IEC 60870-5-104/101 DCA to the device. It is incremented immediately after a data link frame is sent to the device. The IEC 60870-5-104/101 DCA increments this statistic for each Device that shares the same link addresses.
MsgReceived	The number of messages received by the IEC 60870-5-104/101 DCA from the device. It is incremented immediately after a data link frame has been successfully received from the device. The IEC 60870-5-104/101 DCA increments this statistic for each Device that shares the same link address if the link address of the message is known. If the link address is unknown, this Pseudo point is not incremented.
MsgTimeOuts	The number of message timeouts detected by the IEC 60870-5-104/101 DCA for the device. It is incremented every time the device has failed to respond to a confirmed data link frame (i.e. any Primary frame but function code 4 – Send No Reply) within the allowed timeout. The IEC 60870-5-104/101 DCA increments this statistic for each Device that shares the same link address.
MsgError	The number of frames received in error (e.g. checksum failure). Does not include Respond NACK (function code 4) or Confirm NACK (function code 1) frames, as those would be incremented under MsgReceived. The IEC 60870-5-104/101 DCA increments this statistic for each Device that shares the same link address if the link address of the message is known. If the link address is unknown, this pseudo point is not incremented.

NewEventsReceived	The number of new events received by the IEC 60870-5-104/101 DCA from the device. Incremented immediately after a previously unrecorded event has been reported by the device.
EventsReported	The number of events successfully reported to the RtDB for a Device.
CommandsReceived	The number of Output, Local, or Accumulator Commands received from the RtDB.
CommandsFailed	The number of negative command statuses sent to the RtDB.
RxBadTypeID	The number of invalid or unsupported Type Identification messages received from the Device. As a prerequisite to incrementing this statistic, the ASDU address of the message must be known.
RxBadQualifier	The number of invalid structure qualifier field messages received from the Device. As a prerequisite to incrementing this statistic, the ASDU address of the message must be known.
RxBadCOT	The number of invalid cause of transmission type field messages received from the Device. As a prerequisite to incrementing this statistic, the ASDU address of the message must be known.
RxBadASDUSize	The number of invalid ASDU size messages received from the Device. As a prerequisite to incrementing this statistic, the ASDU address of the message must be known.
RxBadObjectAddress	The number of invalid information object address messages received from the Device. Note this does not include messages with unknown object addresses since that is very common. An example of a bad object address is a non-zero object address for Type ID 70: End of Initialization. As a prerequisite to incrementing this statistic, the ASDU address of the message must be known.
RaACK	The number of ACK responses received from the Device.
RxNACK	The number of NACK responses received from the Device.

IEC 104 with MCP as Master – Device Level – Digital Input Points

Table 7.46: IEC 104 with MCP as Master – Device Level – Digital Input Points

Pseudo Point Name	Description
Device Online	Indicates if the communications with the Device is Active (1) or Inactive (0). The DCA sets this to ON after the initialization procedure with a device completes successfully. The DCA sets this to OFF after communications has been lost with the Device or when the Device is Disabled.
DeviceDisable	Indicates if the communications with the Device is disabled. Reflects the status of the DisableDevice Digital Output pseudo point or'ed with the DisableAllDevices Digital Output pseudo point.
PollingDisabled	Indicates if the scheduled polling of the Device is disabled. Reflects the status of the DisablePolling Digital Output pseudo point or'ed with the DisableAllPolling Digital Output pseudo point.
IntegrityPollExecution	Indicates the status of Integrity Poll. In progress (pending: 1) or completed (0). Integrity Poll can be manually triggered either by IntegrityPoll or IntegrityPollAllDevices Digital Output pseudo points
TimeSyncExecution	Indicates the status of Counter Integrity Poll. In progress (pending: 1) or completed (0). The Counter Integrity Poll can be triggered by either the CounterIntegrityPoll or CounterIntegrityPollAllDevices Digital Output pseudo points

DeviceRestarted	Toggled when Restart or Power On indications are received from the device. Restarted (1) and Running (0) Applicable only to the IEC 60870-5-103 Client.
PrimaryChannelHealth	Indicates the health of the Primary communication channel. Applicable only to the IEC 60870-5-104 Client.
secondaryChannelHealth	Indicates the health of the Secondary communication channel. Applicable only to the IEC 60870-5-104 Client.
PrimaryChannelStatus	Indicates whether the Primary communication channel is active. Applicable only to the IEC 60870-5-104 Client.
secondaryChannelStatus	Indicates whether the Secondary communication channel is active. Applicable only to the IEC 60870-5-104 Client.
CounterIntegrityPollExecution	Indicates a Counter Integrity Poll that was triggered by either the CounterIntegrityPoll or CounterIntegrityPollAllDevices Digital Output pseudo point, is either in progress (pending) or completed

IEC 104 with MCP as Master – Device Level – Digital Output Points

Table 7.47: IEC 104 with MCP as Master – Device Level – Digital Output Points

Pseudo Point Name	Description
DisableDevice	This control enables or disables communications with the Device.
DisablePolling	This control disables or enables scheduled polling of the device.
IntegrityPoll	When a control request is received from this point, the DCA sends one general interrogation to the device.
TimeSync	When a control request is received from this point, the DCA issues time synchronization to the device.
ForceDeviceToAlternateChannel	When a control request is received from this point, the DCA forces communications for the device to the alternate channel. Applicable only to the IEC 60870-5-104 Client.
CounterIntegrityPoll	When a control request is received from this point, the DCA sends one counter interrogation to the device.

IEC 104 with MCP as Master – DCA Level

IEC 104 with MCP as Master – DCA Level - Accumulator Points

Table 7.48: IEC 104 with MCP as Master – DCA Level - Accumulator Points

Pseudo Point Name	Description
MsgSent	The total of the "MsgSent" accumulator values for all devices managed by the DCA.
MsgReceived	The total of the "MsgReceived" accumulator values for all devices managed by the DCA.
MsgTimeOuts	The total of the "MsgTimeouts" accumulator values for all devices managed by the DCA.
RxUnknownASDUAddress	The number of unknown ASDU address messages received on the channel managed by the DCA.

RxFrameErrors	The number of messages with frame errors received on the channel managed by the DCA.
t1ConfirmTimeOuts	Number of confirm timeouts t1.
NumSequenceErrors	Number of N(S) sequence number errors.
TCPReadFailures	Number of TCP reads failed.
TCPWriteFailures	Number of TCP writes failed.
ECONNRESETErrors	Number of ECONNRESET socket errors.
ETIMEDOUTErrors	Number of ETIMEDOUT socket errors.
ECONNREFUSEDErrors	Number of ECONNREFUSED socket errors.
EHOSTUNREACHErrors	Number of EHOSTUNREACH socket errors.
EADDRUNAVAILErrors	Number of EADDRUNAVAIL socket errors.
ENOBUFSErrors	Number of ENOBUFS socket errors.
T0ConnTimeOuts	Number of outgoing connections failed due to timeout t0.
OtherConnectErrors	Number of outgoing connections failed due to other error.
ConnClosedByLocal	Number of connections closed by the local end.
ConnClosedByRemote	Number of connections closed by the remote end.
InvalidLenghtFieldErrors	Number of invalid length field errors.
InvalidFrameTypeErrors	Number of invalid frame type errors.
ReceivedBufferOverflowErrors	Number of receive buffer overflow errors.
IFrameDiscardedLinkInactive	Number of information frames discarded because the link was inactive.

IEC 104 with MCP as Master – DCA Level - Digital Input Points

Table 7.49: IEC 104 with MCP as Master – DCA Level - Digital Input Points

Pseudo Point Name	Description
DCAStatus	Indicates the status of the IEC 60870-5-104/101 DCA application. Set if IEC 60870-5-104/101 DCA is running. Reset if IEC 60870-5-104/101 DCA is not running.
AllDevicesDisabled	Indicates if all the configured IEC 60870-5-104/101 DCA is disabled. Set if all the IEC 60870-5-104/101 DCA is disabled. Reset if all the IEC 60870-5-104/101 DCA is enabled.
AllPollingDisabled	Indicates if the scheduled polling of all Devices is disabled. Set if polling of all IEC 60870-5-104/101 DCA is disabled. Reset if polling of all IEC 60870-5-104/101 DCA is enabled.

IEC 104 with MCP as Master – DCA Level - Digital Output Points

Table 7.50: IEC 104 with MCP as Master – DCA Level - Digital Output Points

Pseudo Point Name	Description
DisableAllDevices	This control disables or enables communications with all Devices belonging to the IEC 60870-5-104/101 DCA.
IntegrityPollAllDevices	When a control request is received from this point, the IEC 60870-5-104/101 DCA sends one general interrogation to each IEC 60870-5-104/101 slave.
CounterIntegrityPollAllDevices	When a control request is received from this point, the DCA sends one counter interrogation to each device.

TimeSyncAllDevices	When a control request is received from this point, the IEC 60870-5-104/101 DCA issues time synchronization to each IEC 60870-5-104/101 slave.
DisableAllPolling	This control disables or enables scheduled polling of all IEC 60870-5-104/101 slaves.
ForceAllDevicesOffPrimaryChannel	When a control request is received from this point, the IEC 60870-5-104/101 DCA clears ALL IEC 60870-5-104/101 slaves off the requested Primary Channel or Secondary Channel. Applicable only to the IEC 60870-5-104 DCA.

IEC 60870-5-104 with MCP as Slave Application

IEC 104 with MCP as Slave - Accumulator Points

Table 7.51: IEC 104 with MCP as Slave - Accumulator Points

Pseudo Point Name	Description
MasterMsgIn	Increments immediately after a data link frame has been successfully received from the master. The DPA increments this statistic for each LRU that shares the same link addresses.
MasterMsgOut	Increments immediately after a data link frame is sent to the master, including retries. The DPA increments this statistic for each LRU that shares the same link address.
RemMsgAckTimeouts	For Balanced, number of confirmed frames that did not receive an acknowledgement within the response timeout (calculated as Extra Response Timeout + Timeout from Annex 2 in 870-5-2). The DPA increments this statistic for each LRU that shares the same link address. For Unbalanced, not incremented. For 104, number of unacknowledged frames that were outstanding at the time the connection was dropped due to a timeout.
RemOperationRequests	Number of commands received from the master.
RemOperationsFailed	Number of commands that the Server either rejected or could not execute due to an error.
ASDUDataRequestsReceived	Number of ASDU data requests received
ASDUDataRequestsRejected	Number of ASDU data requests rejected
ASDUDataResponsesSent	Number of ASDU data responses sent
SpontaneousASDUDataMessagesSent	Number of spontaneous ASDU data messages sent
SpontaneousASDUDataMessagesNoACK	Number of spontaneous ASDU data messages that did not receive ACK from Master. Not applicable to 101 Unbalanced.
ASDUControlResponsesSent	Number of ASDU control responses sent
ChangeEventsReceivedFromRtDB	Number of RtDB Data, Quality, or Data and Quality change events received.
BufferOverflows	Number of Event buffer overflows detected either in an RtDB FIFO or within the DPA's internal buffers.
RtDBReadRequests	Number of RtDB read requests

RtDBReadFailures	Number of RtDB read failures
RtDBWriteRequests	Number of RtDB write requests
DOAndAOCommandFailures	Number of DO and AO command failures
DOAndAOCommandFailuresDueToSBOTimeout	Number of DO and AO command failures due to SBO timeout
CommandFailuresDueToControlLockout	Number of command failures due to control lockout
AccumulatorCommandsSent	Number of accumulator command requests
AccumulatorCommandsFailed	Number of accumulator command failures
FileTransfersAttempted	Number of file transfers attempted
FileTransfersFailed	Number of file transfers failed

IEC 104 with MCP as Slave – Analog Input Points

Table 7.52: IEC 104 with MCP as Slave – Analog Input Points

Pseudo Point Name	Description
DPAProcessID	Indicates the ID of the DPA Process thread.

IEC 104 with MCP as Slave – Digital Input Points

Pseudo Point Name	Description
CommStatus	Indicates when a master station request has not been received for a configurable period, or transmission failure is detected by the communication transport.
DPAStatus	The Server sets the DPA Status to DISABLED upon creating the pseudo point. The Server sets the DPA Status to ENABLED immediately after all initialization is complete (i.e., after DB Initialized Event is received for all the Server's mapped points).
EventBufferOverFlow	Toggled when the DPA detects an event buffer overflow.
EventBufferLow	Indicates whether an internal DPA event buffer low condition exists.

IEC 104 with MCP as Slave – Digital Output Point

Pseudo Point Name	Description
ForceControlsLockout	This control enables or disables the Server acceptance of digital output or analog output command requests from the master station. Range: • Latch On, Pulse On, and Close for a Disabled (1) point status • Latch off, Pulse Off, and Trip for an Enabled (0) point status Default value: • Value retained in NVRAM if DOs are retained in NVRAM; otherwise Enabled (0)

IEC 60870-5-103 with MCP as Master Application

IEC 103 with MCP as Master - Device Level

IEC 103 with MCP as Master – Device Level - Accumulator Points

Pseudo Point Name	Description
UpdateCount	The number of data change events reported to the RtDB for a Device.
MsgSent	The number of messages sent by the DCA to the device. It is incremented immediately after a data link frame is sent to the device. The DCA increments this statistic for each Device that shares the same link address.
MsgReceived	The number of messages received by the DCA from the device. It is incremented immediately after a data link frame has been successfully received from the device. The DCA increments this statistic for each Device that shares the same link address if the link address of the message is known. If the link address is unknown, the DCA does not increment this statistic for any Device.
MsgTimeOuts	The number of message timeouts detected by the DCA for the device. It is incremented every time the device has failed to respond to a confirmed data link frame (i.e. any Primary frame but function code 4 – Send No Reply) within the allowed timeout. The DCA increments this statistic for each Device that shares the same link address.
MsgError	The number of frames received in error (e.g. checksum failure). Does not include Respond NACK (function code 4) or Confirm NACK (function code 1) frames, as those would be incremented under MsgReceived. The DCA increments this statistic for each Device that shares the same link address if the link address of the message is known. If the link address is unknown, the DCA does not increment this statistic for any Device.
NewEventsReceived	The number of new events received by the DCA from the device. Incremented immediately after a previously unrecorded event has been reported by the device.
EventsReported	The number of events successfully reported to the RtDB for a Device.
CommandsReceived	The number of Output, Local, or Accumulator Commands received from the RtDB.
CommandsFailed	The number of negative command statuses sent to the RtDB.
RxBadTypeID	The number of invalid or unsupported Type Identification messages received from the Device. As a prerequisite to incrementing this statistic, the ASDU address of the message must be known.
RxBadQualifier	The number of invalid structure qualifier field messages received from the Device. As a prerequisite to incrementing this statistic, the ASDU address of the message must be known.
RxBadCOT	The number of invalid causes of transmission type field messages received from the Device. As a prerequisite to incrementing this statistic, the ASDU address of the message must be known.
RxBadASDUSize	The number of invalid ASDU size messages received from the Device. As a prerequisite to incrementing this statistic, the ASDU address of the message must be known.

RxBadObjectAddress	The number of invalid information object address messages received from the Device. Note this does not include messages with unknown object addresses since that is very common. An example of a bad object address is a non-zero object address for Type ID 70: End of Initialization. As a prerequisite to incrementing this statistic, the ASDU address of the message must be known.
RaACK	The number of ACK responses received from the Device. For IEC 60870-5-101/104, this means any response where the P/N bit of the COT is relevant and is set to 0. For IEC 60870-5-103, this means any response where the COT is 20 (positive acknowledgement of command).
RxNACK	The number of NACK responses received from the Device. For IEC 60870-5-101/104, this means any response where the P/N bit of the COT is relevant and is set to 1. For IEC 60870-5-103, this means any response where the COT is 21 (negative acknowledgement of command).

IEC 103 with MCP as Master – Device Level – Digital Input Points

Pseudo Point Name	Description
Device Online	Indicates if the communications with the Device is Active (1) or Inactive (0). The DCA sets this to ON after the initialization procedure with a device completes successfully. The DCA sets this to OFF after communications has been lost with the Device or when the Device is Disabled.
DeviceDisable	Indicates if the communications with the Device is disabled. Reflects the status of the DisableDevice Digital Output pseudo point or'ed with the DisableAllDevices Digital Output pseudo point.
PollingDisabled	Indicates if the scheduled polling of the Device is disabled. Reflects the status of the DisablePolling Digital Output pseudo point or'ed with the DisableAllPolling Digital Output pseudo point.
IntergrityPollExecution	Indicates the status of Integrity Poll. In progress (pending: 1) or completed (0). Integrity Poll can be manually triggered either by IntegrityPoll or IntegrityPollAllDevices Digital Output pseudo points
TimeSyncExecution	Indicates the status of Counter Integrity Poll. In progress (pending: 1) or completed (0). The Counter Integrity Poll can be triggered by either the CounterIntegrityPoll or CounterIntegrityPollAllDevices Digital Output pseudo points
DeviceRestarted	Toggled when Restart or Power On indications are received from the device. Restarted (1) and Running (0) Applicable only to the IEC 60870-5-103 Client.

IEC 103 with MCP as Master – Device Level – Digital Output Points

Pseudo Point Name	Description
DisableDevice	This control enables or disables communications with the Device.
DisablePolling	This control disables or enables scheduled polling of the device.
IntegrityPoll	When a control request is received from this point, the DCA sends one general interrogation to the device.
TimeSync	When a control request is received from this point, the DCA issues time synchronization to the device.

IEC 103 with MCP as Master – DCA Level

IEC 103 with MCP as Master – DCA Level - Accumulator Points

Pseudo Point Name	Description
MsgSent	The total of the "MsgSent" accumulator values for all devices managed by the DCA.
MsgReceived	The total of the "MsgReceived" accumulator values for all devices managed by the DCA.
MsgTimeOuts	The total of the "MsgTimeouts" accumulator values for all devices managed by the DCA.
RxUnknownASDUAddress	The number of unknown ASDU address messages received on the channel managed by the DCA.
RxUnKnownLinkAddress	The number of unknown link address messages received on the channel managed by the DCA.
RxFrameErrors	The number of messages with frame errors received on the channel managed by the DCA.

IEC 103 with MCP as Master – DCA Level - Digital Input Points

Pseudo Point Name	Description
DCAStatus	Indicates the status of the IEC 60870-5-104/101 DCA application. Set if IEC 60870-5-104/101 DCA is running. Reset if IEC 60870-5-104/101 DCA is not running.
AllDevicesDisabled	Indicates if all the configured IEC 60870-5-104/101 DCA is disabled. Set if all the IEC 60870-5-104/101 DCA is disabled. Reset if all the IEC 60870-5-104/101 DCA is enabled.
AllPollingDisabled	Indicates if the scheduled polling of all Devices is disabled. Set if polling of all IEC 60870-5-104/101 DCA is disabled. Reset if polling of all IEC 60870-5-104/101 DCA is enabled.

IEC 103 with MCP as Master – DCA Level - Digital Output Points

Pseudo Point Name	Description
DisableAllDevices	This control disables or enables communications with all Devices belonging to the IEC 60870-5-104/101 DCA.
IntegrityPollAllDevices	When a control request is received from this point, the IEC 60870-5-104/101 DCA sends one general interrogation to each IEC 60870-5-104/101 slave.
TimeSyncAllDevices	When a control request is received from this point, the IEC 60870-5-104/101 DCA issues time synchronization to each IEC 60870-5-104/101 slave.
DisableAllPolling	This control disables or enables scheduled polling of all IEC 60870-5-104/101 slaves.

IEC 61850 with MCP as Master Application

IEC 61850 with MCP as Master - Accumulator Points

Pseudo Point Name	Description
MMS Calling Initiates Req Sent	Number of Initiate requests sent by the DCA. In MMS, the node that initiated the association is the calling node. In addition, the MMS Initiate service is used to establish an association.
MMS Calling Initiates Failed	Number of DCA-initiated Initiate requests that the IED responded to with error.
MMS Concludes Sent	Number of DCA-initiated Conclude requests. Note that the MMS Conclude service is used to gracefully close an association.
MMS Concludes Failed	Number of DCA-initiated Conclude requests that the IED responded to with error.
MMS Concludes Indications	Number of Conclude indications received from the IED.
MMS Concludes Indications Failed	Number of failed Conclude indications received from the IED.
User Abort Indications	Number of non-recoverable errors detected within the DCA (including application, presentation, session, and RFC1006 transport layers) that caused an association to drop. An example of such an error is receiving a malformed packet at the application layer.
Provider Abort Indications	Number of non-recoverable errors detected outside of the DCA that caused an association to drop. This includes IED-initiated rejects and connection drops reported by the Linux TCP/IP stack.
MMS Rejects Sent	Number of MMS Rejects sent by the DCA.
MMS Rejects Received	Number of MMS Rejects received by the DCA.
MMS Requests Sent	Number of MMS requests sent by the DCA.
MMS Requests Failed	Number of DCA-initiated MMS requests that the IED responded to with error.
MMS Request Indications Received	Number of MMS request indications received from the IED.
MMS Request Indications Failed	Number of MMS request indications that the DCA responded to with error.
MMS Information Reports Received	Number of MMS information reports received.
MMS Information Reports Failed	Number of MMS information reports that the DCA discarded due to an error.
TCP Connection Attempts	Number of TCP connections initiated by the DCA.
TCP Connection Attempts Failed	Number of TCP connection attempts that failed.
TCP Connections Closed Locally	Number of TCP connections closed by the DCA.
TCP Connections Closed Remotely	Number of graceful connection closes initiated by the IED.
TCP Connection Drops	Number of TCP connections dropped as reported by the TCP/IP stack
Alternate Channel Checks	Number of alternate channel check operations performed by the DCA.

Alternate Channel Checks Failed	Number of alternate channel check operations that failed.
Current Channel Checks	Number of current channel check operations performed by the DCA
Update Count	Accumulation for the total number of points the RTDB has been updated for this IEC61850 IED.
MsgSent	Accumulation for the total number of requests sent by the DCA to this IEC61850 IED.
MsgReceived	Accumulation for the total number of responses received by the DCA from this IEC61850 IED.
MsgError	Accumulation for the total number of responses received in error from this IEC61850 IED.
MsgTimeOuts	Accumulation for the number of message timeouts detected by the DCA for this IEC61850 IED.
Controls Received	Accumulations for the number of control requests received by the DCA via the RTDB that was directed to this IEC61850 IED.
Controls Failed	Accumulations of the number of control operation failures detected for this IEC61850 IED.

IEC 61850 with MCP as Master– Digital Input Points

Pseudo Point Name	Description
Primary Channel Health	Indicates the health of the Primary Channel configured. Set if healthy.
Secondary Channel Health	Indicates the health of the Secondary Channel configured. Set if healthy.
Primary Channel Status	Indicates the Primary Channel Status. Set if the Configured Primary Channel is being used. Reset if it is not in use.
Secondary Channel Status	Indicates the Secondary Channel Status. Set if the Configured Secondary Channel is being used. Reset if it is not in use.
Report Buffer Overflow	Indicates if IED has reported a buffer overflow condition in one of its buffered report control blocks. Set if IED reports a buffer overflow condition. Reset if No Overflow id observed.
Retrieve All Data Sets From IED Status	Indicates the completion status of all the data set retrieval from the IED. Set if the Retrieval of all Data Sets is Pending. Reset if the Retrieval of all Data Sets is Completed.
DeviceDisable	Set if the communication to the IED is disabled. Unset if disabled.
Polling Of IED Status	Set if data set retrieval from the IED is enabled. Unset if disabled.
Configuration Comparison Status	Indicates whether the most recent configuration comparison for this IED failed. The DCA compares the composition of the IED's Data Sets with what it has configured locally.
Device Online	Indicates if the Configured IEC61850 IED is Online (1) or Offline (0).

IEC 61850 with MCP as Master– Digital Output Points

Pseudo Point Name	Description
Retrieve All Data Sets	This control queues a poll request for every locally configured Data Set on the IED.
DisableDevice	This control disables or enables communications to the IED. If disabled, the DCA does not have an open association with the IED, nor accept user requests for the IED.
Enable Polling Of IED	This control disables or enables data set retrieval from the IED but leaves the association up and does not prevent other controls such as "Retrieve all Data Sets" or "Force to Alternate Channel". The DCA also disables all Report Control Blocks when this control is disabled.
Force IED to Alternate Channel	This control forces the IED to the alternate communications channel.

IEC 61850 Application – Global Points

The following sets of global pseudo points are available for the IEC 61850 application:

IEC 61850 Application - Global, Digital Output Points

Pseudo Point Name	Description	DO state set to
Retrieve All Data Sets from All IEDs	This control queues an integrity request for every data set on every device.	Completed (0)
		Pending (1)
Global "DisableDevice"	This control disables communications to all devices belonging to the application. If disabled, the application does not have an open association with any of its devices or send user requests to any device. When it is set to Enabled, the application sets the device state to its previous state.	Disabled (1)
		Enabled (0)
Enable Polling of All IEDs	This control disables or enables data set retrieval from all devices belonging to the application but leaves the associations up and does not prevent other controls such as "Retrieve All Data Sets from IED" or "Force to Alternate Channel". The application stops polling all devices and disable all Report Control Blocks.	Disabled (0)
		Enabled (1)
Force All IEDs Off Primary Channel	This control clears all devices off the requested channel	Clear Primary Channel (1)
		Clear Secondary Channel (0)

IEC 61850 Application - Global, Digital Input Points

Pseudo Point Name	Description	DO state set to
Global "DeviceDisable"	Communications is disabled to all devices owned by the application. Reflects the status of the Global "DisableDevice" Digital Output pseudo point.	Disabled (1)
		Enabled (0)

Polling of IED Status	Automatic data retrieval from devices is globally disabled. Reflects the status of the "Enable Polling of All IEDs" Digital Output pseudo point.	Disabled (0)
		Enabled (1)
DCA Status	Indicates if the application is running.	Enabled (1)
		Disabled (0)

IEC 61850 Application – Per-Device Points

IEC 61850 Application, Per-Device - Digital Output Points

Pseudo Point Name	Description	DO status set to
Retrieve all Data Sets	This control queues a poll request for every locally configured Data Set on the device.	Completed (0)
		Pending (1)
DisableDevice	This control disables or enables communications to the IED. If disabled, the application does not have an open association with the device, nor accept user requests for the device.	Disabled (1)
		Enabled (0)
Enable Polling of IED	This control disables or enables data set retrieval from the device but leaves the association up and does not prevent other controls such as "Retrieve all Data Sets" or "Force to Alternate Channel". The application also disables all Report Control Blocks when this control is disabled.	Disabled (0)
		Enabled (1)
Force IED to Alternate Channel	This control forces the device to the alternate communications channel.	Completed (0)
		Pending (1)
Enable Test Flag in Controls	This flag enables Test Mode for controls that go to the devices.	Disabled (0)
		Enabled (1)

IEC 61850 Application, Per-Device - Digital Input Points

Pseudo Point Name	Description	DO status set to
Primary Channel Health	Indicates health of Primary communications channel. If Primary channel is in use, Normal health means the association is up. If Primary channel is not in use, Normal health means an association is possible on this channel. Failed health means the last association attempt failed.	Failed (0)
		Normal (1)
Secondary Channel Health	Indicates health of Secondary communications channel. If Secondary channel is in use, Normal health means the association is up. If Secondary channel is not in use, Normal health means an association is possible on this channel. Failed health means the last association attempt failed.	Failed (0)
		Normal (1)
Primary Channel Status	Indicates if Primary channel is In Use or Not In use. In use status means this channel is the active channel and the association is up on this channel.	Not In Use (0)
		In Use (1)
		Not In Use (0)

Secondary Channel Status	Indicates if Secondary channel is In Use or Not In Use. In use status means this channel is the active channel and the association is up on this channel.	In Use (1)
		Overflow (1)
Report Buffer Overflow	Indicates if the device has reported a buffer overflow condition in one of its buffered report control blocks.	No Overflow (0)
		Overflow (1)
Retrieve All Data Sets from IED Status	Operation to retrieve All Data Sets from device that was triggered by either the "Retrieve All Data Sets from All IEDs" or the "Retrieve All Data Sets from IED" pseudo Digital Output is either completed or under way.	Completed (0)
		Pending (1)
DeviceDisable	Device is enabled or disabled as controlled by the DisableDevice Digital Output or the Global "DisableDevice" Digital Output.	Disabled (1)
		Enabled (0)
Polling of IED Status	Polling is enabled or disabled as controlled by the "Enable Polling to IED" Digital Output or the "Enable Polling of All IEDs to IED" Digital Output.	Disabled (0)
		Enabled (1)
Configuration Comparison Status	Indicates whether the most recent configuration comparison for this device failed. The application compares the composition of the device's Data Sets with what it has configured locally.	Failed (0) The DCA logged the discrepancies it detected.
		OK (1) There were no discrepancies in the most recent comparison.
Device Online	Indicates whether communications with the device is Active (Online) or Inactive (Offline)	ON (1)
		OFF (0)

IEC 61850 Application, Per-Device - Analog Input Points

Pseudo Point Name	Description	DO status set to
"AddCause for ..."	This point is created for each field DO and AO point. The name of the pseudo point includes the point name of the associated DO or AO field point.	See note below.

NOTE: The value of this field indicates the result of the last AO or DO operation on an IEC 61850 enhanced security control (see the following table). For IEC 61850 normal security controls, the values are 0 for commands that are successfully sent and –255 for commands that fail to send.

For enhanced security controls, a non-zero value indicates failure; a zero value indicates success. A positive value indicates one of the IEC 61850 Additional Causes was reported by the device. A negative value larger than -255 indicates a low-level MMS error was reported by the device. A value of -255 indicates another error condition not specifically listed has occurred.

Error Class	Error Description	Value of AI
Unknown Error	Unknown error.	-255
DataAccessError	object-non-existent	-10
DataAccessError	object-access-unsupported	-9
DataAccessError	object-attribute-inconsistent	-8
DataAccessError	type-inconsistent	-7

DataAccessError	type-unsupported	-6
DataAccessError	invalid-address	-5
DataAccessError	object-undefined	-4
DataAccessError	object-access-denied	-3
DataAccessError	temporarily-unavailable	-2
DataAccessError	hardware-fault	-1
Success	Success	0
Additional Cause	Blocked-by-switching-hierarchy	2
Additional Cause	Select-failed	3
Additional Cause	Invalid-position	4
Additional Cause	Position-reached	5
Additional Cause	Parameter-change-in-execution	6
Additional Cause	Step-limit	7
Additional Cause	Blocked-by-Mode	8
Additional Cause	Blocked-by-process	9
Additional Cause	Blocked-by-interlocking	10
Additional Cause	Blocked-by-synchrocheck	11
Additional Cause	Command-already-in-execution	12
Additional Cause	Blocked-by-health	13
Additional Cause	1-of-n-control	14
Additional Cause	Abortion-by-cancel	15
Additional Cause	Time-limit-over	16
Additional Cause	Abortion-by-trip	17
Additional Cause	Object-not-selected	18

Load Shed

LoadShed – Accumulator Points

Pseudo Point Name	Description
Controls Received	Indicates the total number of controls received.
Controls Failed	Indicates the total number of controls failed.
Controls Sent	Indicates the total number of controls sent.

LoadShed – Analog Input Points

Pseudo Point Name	Description
Fdr<nnn>	Indicates the zone number to which the configured feeder belongs.

LoadShed – Digital Input Points

Pseudo Point Name	Description
Fdr<nnn>	Provides an option to change the zone of feeder.

LoadShed – Digital Output Points

Pseudo Point Name	Description
DisableDevice	Provides an option to disable/enable the LoadShed application (DTA). • Set to 1 to disable the LoadShed application. • Set to 0 to enable the LoadShed application.
Control Disable	Provides an option to disable all controls.
Zone1	Provides an option to control the zone.

LogicLinx

LogicLinx – Accumulator Points

Pseudo Point Name	Description
Controls Received	Indicates the total number of controls received on the LogicLinx owned Analog Output and Digital Output points.
Controls Failed	Indicates the total number of failed control operations.
Controls Sent	Indicates the total number of the controls sent from the LogicLinx application.

LogicLinx – Analog Input Points

Pseudo Point Name	Description
TotalLLPoint	Indicates the total number of the LogicLinx-owned points configured.

LogicLinx – Digital Input Points

Pseudo Point Name	Description
Device Disable	Indicates if the LogicLInx application is disabled or enabled: • Indicates 1 if the LogicLinx application is disabled. • Indicates 0 if the LogicLinx application is enabled (running). **NOTE**: The LogicLinx application can be disabled or enabled through the "Disable Device" Digital Output pseudo point.

LogicLinx – Digital Output Points

Pseudo Point Name	Description
Device Disable	Provides an option to disable/enable the LogicLInx application (DTA): • Set to 1 to disable the LogicLinx application; that is, to stop executing logical cycles. This sets all the LogicLinx points to the OFFLINE state. • Set to 0 to enable the LogicLinx application; that is, to execute the user-programmed logic. This sets all the LogicLinx points to the ONLINE state.

Modbus Ethernet with MCP as Master Application

Modbus Ethernet with MCP as Master – Accumulator Points

Pseudo Point Name	Description
Update Count	Accumulation for the total number of points the RTDB has been updated by the Modbus DCA for this Modbus Slave.
MsgSent	Accumulation for the total number of requests sent by the Modbus DCA to this Modbus Slave.
MsgReceived	Accumulation for the total number of responses received by the Modbus DCA from this Modbus Slave.
MsgTimeouts	Accumulation for the number of message timeouts detected by the Modbus DCA for this Modbus Slave.
Events Received	Accumulations for the total number of events received by the Modbus DCA for this Modbus Slave.
Events Logged	Accumulations for the total number of events logged to the RTDB by the Modbus DCA for this Modbus Slave.
Controls Received	Accumulations for the number of control requests received by the Modbus DCA via the RTDB that was directed to this Modbus Slave.
Control Failed	Accumulations of the number of control operation failures detected for this Modbus Slave.

Modbus Ethernet with MCP as Master – Digital Input Points

Pseudo Point Name	Description
Primary Port Status	Indicates the usage of configured Primary Port. Set if Primary port is in use. Reset if not in use.
Backup Port Status	Indicates the usage of configured Secondary Port. Set if backup port is in use Reset if not configured.
Device Online	Indicates if the Configured Modbus Slave is Online (1) or Offline (0).
IED COMM Status	Indicates whether the Modbus DCA is actively collecting data from this Modbus IED. Set if communications with the Modbus Slave is Active. Reset if communications with the Modbus Slave is Inactive.

DCA Status	Indicates the status of the Modbus DCA application. Set if Modbus DCA is running. Reset if Modbus DCA is not running.
Device Disable	Indicates if the Modbus DCA Application is disabled. Set if Modbus DCA application is disabled. Reset if Modbus DCA application is enabled.

Modbus Ethernet with MCP as Master – Digital Output Point

Pseudo Point Name	Description
Disable Device	Set if Modbus DCA Application is disabled. Do not set if enabled.

Modbus Ethernet with MCP as Master – Analog Input Point

Pseudo Point Name	Description
Secure Connection State	State of unit when Modbus TCP/SSH Master is configured. This pseudo point state is offline or invalid for ModbusTCP and Modbus Multidrop Master configurations. State is one of the Secure Connection States (see the Secure Connection States table under section: Modbus Serial with MCP as Slave Application. State is presented in enumerated text.

Modbus Ethernet with MCP as Slave Application

Modbus Ethernet with MCP as Slave – Accumulator Points

Pseudo Point Name	Description
UpdateCount	Accumulation of number of times the Modbus DPA Application updated the RTDB.
MasterMsgIn	Accumulation of number of request messages received by the Modbus DPA from the Master.
MasterMsgOut	Accumulation of number of response messages sent by the Modbus DPA to the Master.
RemMsgAckTimeouts	Number of confirmed frames that did not receive an acknowledgement within the response timeout (calculated as Extra Response Timeout + Timeout from Annex 2 in 870-5-2). The DPA increments this statistic for each LRU that shares the same link address.
RemOperationRequests	Accumulation of number of Control requests received by the Modbus DPA from the Master.
RemOperationsFailed	Accumulation of number of failed control operations. Generated once every time an exception is produced by the Modbus DPA.
MissedUpdates	Accumulation of number of failures occurred while updating the RTDB.
LockAtproducerconsumerdpaptrts Failed	Not in use

Modbus Ethernet with MCP as Slave – Analog Input Point

Pseudo Point Name	Description
DPAProcessID	Indicates the ID of the Modbus DPA Process thread.

Modbus Ethernet with MCP as Slave – Digital Input Points

Pseudo Point Name	Description
PrimaryportStatus	Indicates the status of the configured Primary port for communicating with Modbus Master. Set while communication is active on the Primary port. Reset while there are no communications on the Primary port.
BackupPortStatus	Indicates the status of the configured Backup port for comm. Set while communication is active on the Backup port. Reset while there are no communications on the Backup port.
CommStatus	Indicates the Communication status of the Modbus DPA with the configured Modbus Master. Set if the Modbus DPA is actively communicating with the Master. Reset if the Modbus DPA is not communicating with the Master.
DPAStatus	Indicates the status of the Modbus DPA application. Set if the Modbus DPA is currently running. Reset is the Modbus DPA is not running.

Modbus Ethernet with MCP as Slave – Digital Output Points

Pseudo Point Name	Description
ForceControlsLockout	Set if the Modbus DPA refuses the control requests sent by the configured Modbus Master. Reset if the Modbus DPA accepts the control requests and performs the respective operation.

Modbus Serial with MCP as Master Application

Modbus Serial with MCP as Master – Accumulator Points

Pseudo Point Name	Description
UpdateCount	Accumulation for the total number of points the RTDB has been updated by the Modbus DCA for this Modbus Slave.
MsgSent	Accumulation for the total number of requests sent by the Modbus DCA to this Modbus Slave.
MsgReceived	Accumulation for the total number of responses received by the Modbus DCA from this Modbus Slave.
MsgTimeOuts	Accumulation for the number of message timeouts detected by the Modbus DCA for this Modbus Slave.
Controls Received	Accumulations for the number of control requests received by the Modbus DCA via the RTDB that was directed to this Modbus Slave.

Controls Failed	Accumulations of the number of control operation failures detected for this Modbus Slave.
Events Received	Accumulations for the total number of events received by the Modbus DCA for this Modbus Slave.
Events Logged	Accumulations for the total number of events logged to the RTDB by the Modbus DCA for this Modbus Slave.

Modbus Serial with MCP as Master – Digital Input Points

Pseudo Point Name	Description
Device Online	Indicates if the Configured Modbus Slave is Online (1) or Offline (0).
DCA Status	Indicates the status of the Modbus DCA application. Set if Modbus DCA is running. Reset if Modbus DCA is not running.
DeviceDisable	Indicates if the MODBUS DCA Application is disabled. Set if Modbus DCA application is disabled. Reset if Modbus DCA application is enabled.
Primary Port Status	Indicates the usage of configured Primary Port. Set if Primary port is in use. Reset if not in use.
Backup Port Status	Indicates the usage of configured Secondary Port. Set if backup port is in use. Reset if not configured.
IED Comm. Status	Indicates whether the Modbus DCA is actively collecting data from this Modbus IED. Set if communications with the MODBUS Slave is Active. Reset if communications with the MODBUS Slave is Inactive.

Modbus Serial with MCP as Master – Digital Output Point

Pseudo Point Name	Description
DisableDevice	Set if Modbus DCA Application is disabled. Unset if enabled.

Modbus Serial with MCP as Slave Application

Modbus Serial with MCP as Slave – Accumulator Points

Pseudo Point Name	Description
UpdateCount	Accumulation of number of times the Modbus DPA Application updated the RTDB.
MasterMsgIn	Accumulation of number of request messages received by the Modbus DPA from the Master.
MasterMsgOut	Accumulation of number of response messages sent by the Modbus DPA to the Master.

RemMsgAckTimeouts	Number of confirmed frames that did not receive an acknowledgement within the response timeout (calculated as Extra Response Timeout + Timeout from Annex 2 in 870-5-2). The DPA increments this statistic for each LRU that shares the same link address.
RemOperationRequests	Accumulation of number of Control requests received by the Modbus DPA from the Master.
RemOperationsFailed	Accumulation of number of failed control operations. Generated once every time an exception is produced by the Modbus DPA
MissedUpdates	Accumulation of number of failures occurred while updating the RTDB.
LockAtproducerconsumer dpaptrtsFailed	Not in use

Modbus Serial with MCP as Slave – Analog Input Point

Pseudo Point Name	Description
DPAProcessID	Indicates the ID of the Modbus DPA Process thread.

Modbus Serial with MCP as Slave – Digital Input Points

Pseudo Point Name	Description
PrimaryportStatus	Indicates the status of the configured Primary port for communicating with Modbus Master. Set while communication is active on the Primary port. Reset while there are no communications on the Primary port.
BackupPortStatus	Indicates the status of the configured Backup port for comm. Set while communication is active on the Backup port. Reset while there are no communications on the Backup port.
CommStatus	Indicates the Communication status of the Modbus DPA with the configured Modbus Master. Set if the Modbus DPA is actively communicating with the Master. Reset if the Modbus DPA is not communicating with the Master.
DPAStatus	Indicates the status of the Modbus DPA application. Set if the Modbus DPA is currently running. Reset is the Modbus DPA is not running.

Modbus Serial with MCP as Slave – Digital Output Points

Pseudo Point Name	Description
ForceControlsLockout	Set if the Modbus DPA refuses the control requests sent by the configured Modbus Master Reset if the Modbus DPA accepts the control requests and performs the respective operation.

Modbus TCP/SSH Client - SSH Tunnel Interface

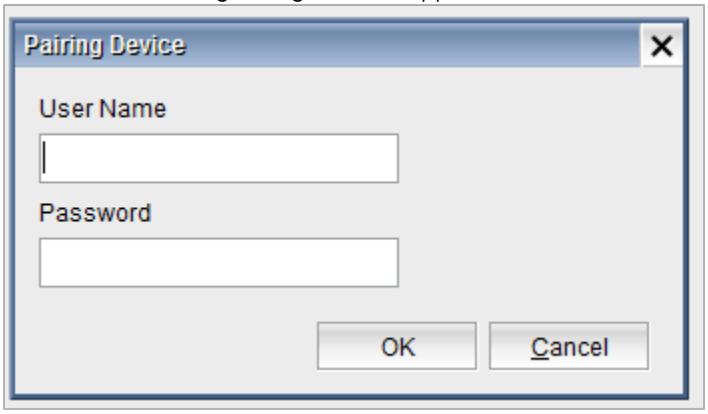
The MCP Modbus Client also supports TCP/SSH mode to establish an SSH secure tunnel with the UR7.6 IEDs that supports SSHv2 protocol through Machine-To-Machine (M2M) access role.

SSH Key Pair

The MCP provides an option in the IED Comm Summary GUI for copying the MCP's public key into a UR 7.6.

» To copy the MCP key into a UR7.6:

1. Log into the MCP with administrator rights.
2. Navigate tot the IED communications summary in the HMI.
3. Select the Modbus TCP/SSH IED that you want to pair from the IED comm summary
4. Click the **Pair** button.
   Result: The following dialog window appears.



5. Enter UR 7.6's Administrator Username & Password to copy the MCP's public key into UR 7.6.

   Result: This file is saved by default as "m2m_user.pk2" and available in the folder "/ata0a/pkey_ssh/" in UR 7.6.

   Result: Upon success, MCP will get one M2M user from UR for all Key based authentications.

   Result: The possible states of the Pair button are described in the Secure Connection States table.

NOTICE The **Pair** button in the HMI is only available to Administrator users. This button is only applicable to Modbus TCP/SSH Clients.

SSH Key Rotate:

The MCP provides an option in the IED Comm Summary HMI for rotating the MCP's public key into UR 7.6 on an on-demand basis.

» To rotate the MCP key into a UR7.6 on an on-demand basis:

1. Log into the MCP with administrator rights.
2. Navigate tot the IED communications summary in the HMI.
3. Select the Modbus TCP/SSH IED from the IED comm summary that you want to pair
4. Click the **Rotate** button.
   Result: The SSHv2 keys are transferred on-demand into the default location in the UR7.6.
   Result: The possible states of the Rotate button are described in the Secure Connection States table.

NOTICE The **Rotate** button in the HMI is only available to Administrator users. This button is only applicable to Modbus TCP/SSH Clients. The **Key Rotate** button is enabled when the IED is paired successfully using SSH Key Pair.

Secure Connection States

State	Description	Status of Pair & Rotate Buttons in IED Comm Summary
-1	This state is not applicable to TCP and Serial connections and only available for Modbus TCP/SSH client connections.	Both Pair & Rotate Buttons are greyed out.
0	Pairing is not done yet.	Pair button is enabled, and Rotate button is greyed out. Pair button state shows "Pair" and Rotate button is disabled.
1	Pairing is failed.	Pair button is enabled, and Rotate button is greyed out. Pair button state shows "Failed" and Rotate button is disabled.
2	Pairing is Successful and Rotate is yet to be done.	Both Pair & Rotate buttons are enabled. Pair button state shows "Paired" and Rotate button shows "Rotate".
3	Pairing and Rotating are successful.	Both Pair & Rotate buttons are enabled. Pair button state shows "Paired" and Rotate button shows "Rotated".
4	Pairing is successful, and Rotating is in-progress.	Pair button is enabled, and Rotate button is greyed out. Pair button state shows "Paired" and Rotate button shows "Rotating".
5	Pairing is successful and previous rotating state is failed.	Pair and Rotate buttons are enabled. Pair button state shows "Paired" and Rotate button shows "Failed".
6	Pairing is in-progress and Rotate is yet to be done.	Pair button is greyed out and Rotate buttons is enabled. Pair button state shows "Pairing" and Rotate button shows "Rotate".
7	Pairing is in-progress and previous rotate state is successful.	Pair button is greyed out and Rotate buttons is enabled. Pair button state shows "Pairing" and Rotate button shows "Rotated".
8	Pairing is in-progress and previous rotate state is failed.	Pair button is greyed out and Rotate buttons is enabled. Pair button state shows "Pairing" and Rotate button shows "Failed".
9	Previous Pairing is Failed and Rotate is yet to be done.	Pair and Rotate buttons are enabled. Pair button state shows "Failed" and Rotate button shows "Rotate".
10	Previous pairing state is failed, and current rotate state is successful.	Pair and Rotate buttons are enabled. Pair button state shows "Failed" and Rotate button shows "Rotated".
11	Previous pairing state is failed, and current rotate state is in-progress.	Pair button is enabled, and Rotate buttons is greyed out. Pair button state shows "Failed" and Rotate button shows "Rotating.
12	Previous pairing state is failed, and current rotate state is failed.	Pair and Rotate buttons are enabled. Pair button state shows "Failed" and Rotate button shows "Failed".
13	Not applicable	Not applicable

Redundancy Manager

Redundancy Manager – Analog Input Points

Pseudo Point Name	Description
State of this Gateway	Indicates the current state of this MCP as given in operational states.
State of PEER Gateway	Indicates the current state of the PEER MCP as given in operational states.
A/B designation of this Gateway	A or B designation of this MCP, obtained from switch panel or through MCP configuration utility.

Redundancy Manager – Digital Input Points

Pseudo Point Name	Description
SystemRedundant	Set to TRUE if the MCP is configured to be redundant. Set to FALSE if the MCP is not redundant.
StandbyGatewayCommFail	Set to TRUE if MCP is configured as redundant and communications with the standby unit have failed. FALSE otherwise. Set to offline in non-redundant mode.
StandbyGatewayInService Mode	Set TRUE if the standby MCP is in Service mode, FALSE otherwise. Set to offline in non-redundant mode.
Standby Gateway Not Available	Set TRUE if the standby MCP is in Failed mode, FALSE otherwise. Set to offline in non-redundant mode.
GatewayA Active	Set to TRUE if the unit is MCP "A". Set to offline in non-redundant mode.
GatewayB Active	Set to TRUE if the unit is MCP "B". Set to offline in non-redundant mode.
Config Sync In Progress	Set to TRUE if currently Configuration Synchronize is in progress. Set to offline in non-redundant mode.
Standby Config Out Of Sync	Set to True if configuration on Standby MCP is out of sync with configuration on Active MCP. Set to offline in non-redundant mode.
HotstandbyDisabled	Set to TRUE when system is configured in warm standby mode. Set to FALSE when system is configured in hot standby mode.
Standby Code Out of Sync	Set to FALSE when code image (Primary CF image) on device is the same as that on the other device. Set to TRUE when the code images are not in sync.

Redundancy Manager – Digital Output Points

Pseudo Point Name	Description
StartChangeOver	Triggers a change-over. Set to offline in non-redundant mode.
RestartActive	Requests a restart of all software on the active MCP.
RestartStandby	Requests a restart of all software on the standby MCP. Set to offline in non-redundant mode.
RebootActive	Requests a reboot of the active MCP.
RebootStandby	Requests a reboot of the standby MCP. Set to offline in non-redundant mode.
SyncConfig	Requests that the standby MCP's configuration be synchronized with that of the active MCP. Set to offline in non-redundant mode.
ShutdownActive	Requests a shutdown of the active MCP.
ShutdownStandby	Requests a shutdown of the standby MCP.

SEL Binary Serial with MCP as Master Application

Accumulators

Pseudo Point Name	Description
UpdateCount	Accumulation for the total number of points in the RTDB that have been updated for this SEL device.
MsgSent	Accumulation for the total number of messages sent by the SEL Binary Client to the SEL device.
MsgReceived	Accumulation for the total number of messages received by the SEL Binary Client from the device. It is incremented immediately after a message has been successfully received from the device.
MsgTimeOuts	Accumulation for the total number of message timeouts detected by the SEL Binary Client for the device. It is incremented every time the device has failed to respond to a Request within the allowed timeout.
MsgError	Accumulation for the total number of frames received in error from this SEL Slave.

Analog Input

Pseudo Point Name	Description
LF_YEAR	Indicates the year of the Last Fault Report.
LF_MONTH	Indicates the month of the Last Fault Report.
LF_DAY	Indicates the day of the Last Fault Report.
LF_HOUR	Indicates the hour of the Last Fault Report.
LF_MIN	Indicates the minute of the Last Fault Report.
LF_SEC	Indicates the second of the Last Fault Report.
LF_MSEC	Indicates the millisecond of the Last Fault Report.

LF_DISTANCE	Indicates the Fault Distance reported in the Latest Fault Report.
LF_CURRENT	Indicates the Fault Current reported in the Latest Fault Report.
LF_DURATION	Indicates the Fault Duration reported in the Latest Fault Report.
LF_FREQUENCY	Indicates the Fault Frequency reported in the Latest Fault Report.
ConfigErrors	Indicates the number of responses received in error because of misconfiguration. This is detected based on the Invalid Pattern definition of the transaction definition in client map file.

Digital Input

Pseudo Point Name	Description
Device Online	Indicates if the Configured SEL device is: • ONLINE (1) or • OFFLINE (0).
DeviceDisable	Indicates the disabled status of SEL Binary Client Application **NOTE**: If "DisableAllDevices" control is Disabled, the DeviceDisable DI Pseudo Point will be Disabled. If "DisableAllDevices" control is Enabled, the DeviceDisable DI Pseudo Point will be Enabled only if "DisableDevice" DO Pseudo Point is Enabled. Set to Enabled if the status of device is Enabled. Reset to Disabled if the status of device is Disabled.
Primary Port Status	Indicates the usage of configured Primary Port. Set to IN USE if Primary port is in use. Reset to NOT IN USE if not in use.
Backup Port Status	Indicates the usage of configured Secondary Port. Set to IN USE if backup port is in use. Reset to NOT IN USE if not configured.
Polling Of IED Status	Indicates the polling status of device. NOTE: If "Enable Polling Of All IEDs" control is Disabled, the Polling Of IED Status DI Pseudo Point will be Disabled. If "Enable Polling Of All IEDs" control is Enabled, the Polling Of IED Status DI Pseudo Point will only be Enabled if "Enable Polling Of IED" DO Pseudo Point is Enabled. Set to Enabled if polling is Enabled for device. Reset to Disabled if polling is Disabled for device.
LoginStatus	Indicates the login status for SEL device.
DIGLF_A	Indicates that phase A was involved in the Last Fault Reported.
DIGLF_B	Indicates that phase B was involved in the Last Fault Reported.
DIGLF_C	Indicates that Phase C was involved in the Last Fault Reported.
DIGLF_G	Indicates that ground was involved in the Last Fault Reported.
His_cmd_support	Indicate s support for HIS command for SEL device.
Eve_cmd_support	Indicates support for EVE command for SEL device.
Cev_cmd_support	Indicates support for CEV command for SEL device
File Retrieval In-Progress	Value '1' indicates that file retrieval from the SEL device is in-progress. Value '0' indicates that file retrieval from the SEL device is not in-progress.

Pass Through In-Progress	Value '1' indicates that data transfer through the Pass-Through connection with SEL device is in-progress. Value '0' indicates that data transfer through the Pass-Through connection with SEL device is not in-progress.

Digital Output

Pseudo Point Name	Description
DisableDevice	This control enables or disables the running state of the device. When Set to Enabled, the device is enabled. When Reset to Disabled, the device is disabled and is declared as OFFLINE.
ClearStats	This control clears all the communication statistics (MsgSent, MsgReceived, MsgTimeouts and MsgErrors) Pseudo Points of the device.
Enable Polling Of IED	This control disables or enables polling to the device. If set to Disabled, the polling to the device is stopped. If reset to Enabled, the polling to the device resumes.

Text Points

Pseudo Point Name	Description
DEVICEINFO_LINEID	Indicates the Line id of the SEL device.
DEVICEINFO_DEVICEID	Indicates the Device id of the SEL device.
DEVICEINFO_BAYID	Indicates the Bay id of the SEL device.
DEVICEINFO_DEVICETYPE	Indicates the map file name of the SEL device
DEVICEINFO_DEVICEADDRESS	Indicates the SEL Device address
PRF_TEXT_POINT	Indicates the Protective Relay Faults (Supported in the SEL relays such as 487, 551, 734 & 651)
MapFile	Indicates the device type.

System Status Manager

System Status Manager – Analog Input Points

Indicates a value read from the NTP or SNTP time offset.

NOTE: This point is offline if the IRIG-B time sync is enabled.

Pseudo Point Name	Description
Session Uptime	Indicates the time in minutes MCP runs after the reboot
Total Uptime	Indicates the time in minutes MCP runs since first power on
Total System Memory	Indicates total system memory in MB available in MCP

Free Memory Available	Indicates the total free memory in MB available in system

System Status Manager – Digital Output Points

Pseudo Point Name	Description
DisableAllControls	If enabled, the MCP rejects all the controls sent to it. If disabled, the MCP accepts all the controls sent to it.
Disable Buzzer	If Enabled, the MCP buzzer functionality is disabled. If disabled, the MCP buzzer functionality is enabled
Buzzer sound ON	If Enabled, the MCP buzzer sound is muted If disabled, the MCP buzzer sound is ON.

System Status Manager – Digital Input Points

Pseudo Point Name	Description
AllControlsDisabled	This point indicates whether Global controls disabled is disabled or enabled
Buzzer Disabled	This point indicates whether the buzzer is enabled or disabled
Buzzer sound is ON	This point indicates whether the buzzer sound is ON or OFF

System Status Manager – Text Points

Pseudo Point Name	Description
Last boot date and time	This time when the system is up after the last reboot in YYYY-MM-DD HH:MM::SS format

D.20 Peripheral Link Client Pseudo Points

D.20 Peripheral Link Client: Per – Peripheral Pseudo Points

Data Type	Name	Description
Digital Input	Peripheral Online	ON when peripheral is restarted and not in TROUBLE state.
	Peripheral Communication Failed	ON when peripheral communication has failed. OFF when peripheral communication is normal.
	Peripheral Trouble Status	OFF when peripheral was successfully started, and peripheral device status word is NOT TROUBLE. ON when peripheral couldn't be started, or it started but reported it was in TROUBLE state.
	Peripheral in Local Mode	ON when digital outputs are in local mode. Set to offline and invalid if the peripheral does not have any digital outputs.

	AI Reference Calibration Required	ON when the peripheral reports that the analog input references need calibration. Set to offline and invalid if the peripheral does not have any analog inputs. OFF / OFFLINE /
	D.20 Channel 1 Retries Alarm Pseudo Point	For Channel 1: Set after consecutive TX failed attempts exceeds configured max retries. Cleared after consecutive successful TX attempts reaches configured max polls.
	D.20 Channel 2 Retries Alarm Pseudo Point	For Channel 2: Set after consecutive TX failed attempts exceeds configured max retries. Cleared after consecutive successful TX attempts reaches configured max polls.
	D.20 Channel 1 Active	ON when the Channel 1 is being used for communications.
	D.20 Channel 2 Active	ON when the Channel 2 is being used for communications.
	D.20 Channel 1 Internal Health	ON when Channel 1 internal hardware is healthy and available.
	D.20 Channel 2 Internal Health	ON when Channel 2 internal hardware is healthy and available.
Accumulator	Total Transactions	Count of transactions on Channel 1 and Channel 2.
	Total Retries	Count of retries on Channel 1 and Channel 2.
	Total Failures	Count of failures on Channel 1 and Channel 2.
	D.20 Channel 1 Transactions	Count of transactions on Channel 1.
	D.20 Channel 2 Transactions	Count of transactions on Channel 2.
	D.20 Channel 1 Retries	Count of retried transactions on Channel 1.
	D.20 Channel 2 Retries	Count of retried transactions on Channel 2.
	D.20 Channel 1 Failures	Count of failed transactions on Channel 1.
	D.20 Channel 2 Failures	Count of failed transactions on Channel 2.

D.20 Peripheral Link Client – Global Pseudo points

Data Type	Name	Description
Analog Input	Alternate Link Devices	Count of number of devices only reachable through the Channel 2 communications path
	Total Number of Peripherals	Indicates the total number of peripherals configured in MCP
Accumulator	Total Number of Message Sent	Total Number of Messages sent on all Peripherals
	Total Number of Message Received	Total Number of Messages received on all Peripherals
	Total Number of Messages Retries	Total Number of Repeat Poll Messages sent on all the Peripherals in case if the answer was received incorrectly or not received on Channel 1 and Channel 2 from the Peripherals.

	Total Number of Message Failures	Total Number of Failure Messages on Peripherals
Digital Output	Disable Device	Disables D.20 Client if set to 1. The default is Enabled.
Digital Input	DCA Status	Set to 1 if the D.20 Client Status is Ok or Reset to 0.
	Device Disabled	Indicates if the D.20 Peripheral Link Application is disabled. Set if application is disabled, Reset if application is enabled.

GPIO Client Pseudo Points

GPIO Client: Pseudo Points

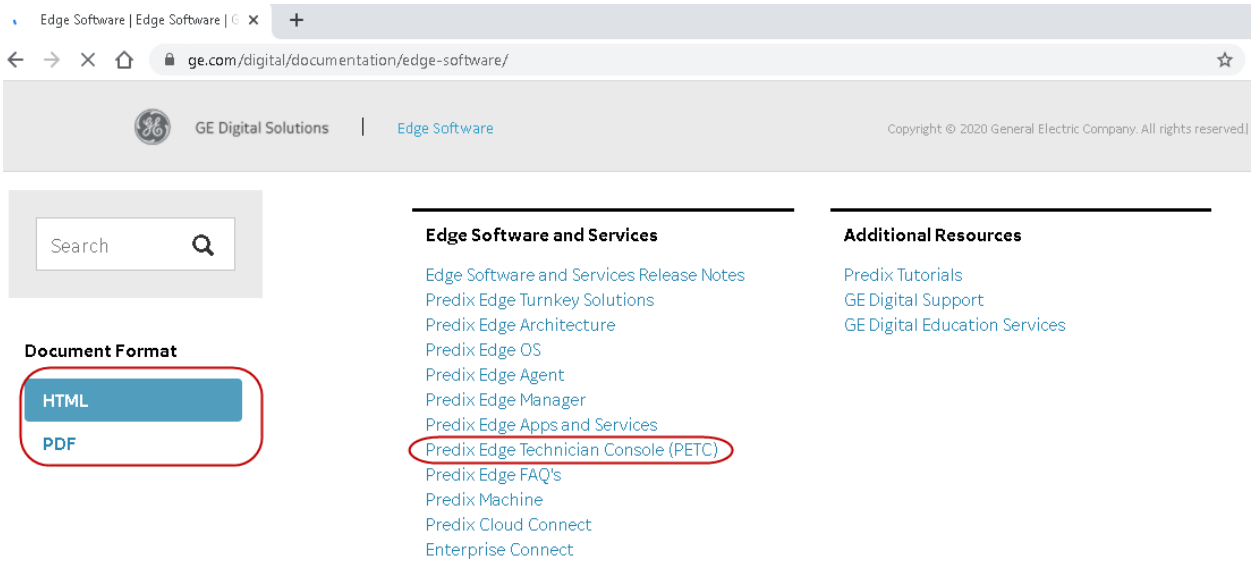
Data Type	Name	Description
Digital Input	Device Online	Indicates if the Configured GPIO Client is Online (1) or Offline (0). **Note**: this is 1 under normal operation, and it exists in current version due to Client standard templates. Users should use the DCA Status below instead.
	DCA Status	Set to 1 if the GPIO Device is running normally.
Accumulator	Controls Received	Accumulations for the number of control requests received by the DCA via the RTDB that was directed to this Application.
	Controls Failed	Accumulations of the number of control operation failures detected for this Application.

Chapter 8 - EdgeManager and PETC

EdgeManager Connectivity is supported only in **single mode** Net settings and in Net ports as below:

- Net1 (G500)
- Net2 (G100, G500)
- Net3 (G100)
- Net4 (G100)
- Net5 (G500)
- Net6 (G500)

Refer to the following website for more details about Predix Edge Technician Console (PETC):
https://www.ge.com/digital/documentation/edge-software/



Select the document format for viewing the content in pdf or HTML.

This document is for a generic Predix Edge device or VM. For the MCP, the following exceptions apply:

- Configuring the Network Time Protocol from PETC is not supported.
- Upload and apply OS updates is not supported.
- Device Reset is not supported.
- SNMP is not supported.
- Configuring the WAN interface from PETC is not supported.

For further exceptions refer to the following sections keyed to the same headings in the Predix documentation.

Downloading and Running Predix Edge Technician Console

In a generic Predix Edge device or VM, the default IP address is configured with DHCP. In an MCP device, the default IP address is static. The default IP address is 192.168.168.82 on Net1 of the G100 and Net0 of the G500.

Device Status

The MCP Edge device has the following additional parameters

Details	• **Memory** – Size of physical RAM • **Storage** – Size of disk drive

Other parameters shown in the generic Predix Edge documentation may not be available in the MCP device due to PETC version differences.

Configuring the Network and Proxy Settings

The following should be appended to the table in this section:

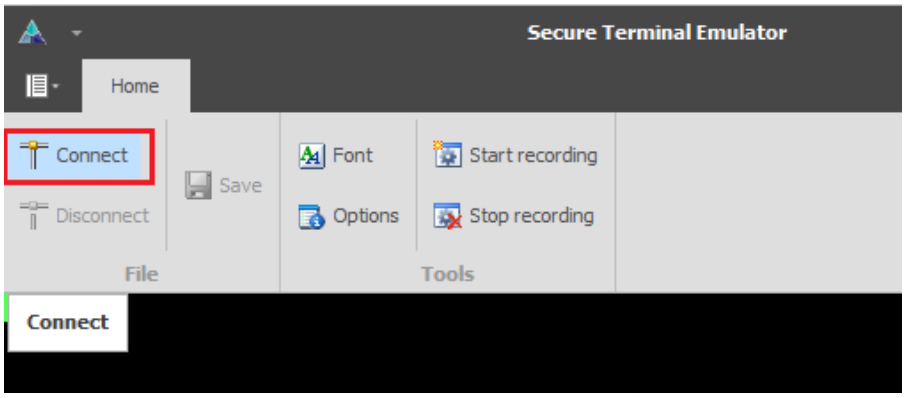
Setting	Description	Configurations
Network Adapters	MCP Specific settings	The interface intended for PETC local access is • For the G100: Net1. • For the G500: Net0. The term "LAN" in the online Predix documentation is taken to describe the interface used for "PETC local access" in an MCP device. The term "WAN" in the online Predix documentation is taken to describe the interface used for "Edge Manager connectivity" in an MCP device. An interface intended for Edge Manager connectivity must be configured using mcpcfg or MCP settings. The current configuration of such an interface can be viewed, but not changed, in PETC. The interface intended for PETC local access must be configured in PETC. The current configuration of such an interface can be viewed, but not changed, in mcpcfg or the MCP settings.

Appendix A – Secure Terminal Emulator

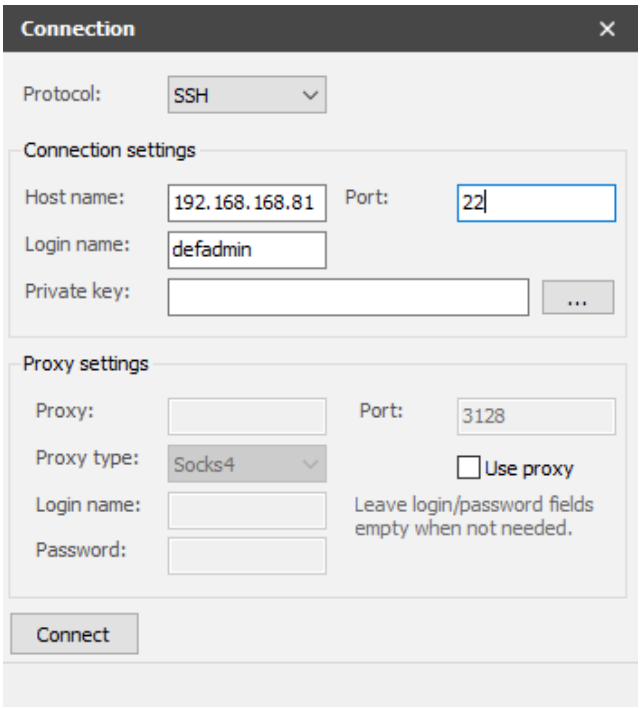
Secure Terminal Emulator (which is used to replace third-party tools like PuTTY®) is launched from the Windows start menu folder of DS Agile Studio.

Connect to MCP Secure Terminal Emulator through SSH

1. Launch the Application: *Windows Start Menu* > *DS Agile Studio x.x* > *Secure Terminal Emulator x.x* and click on *Connect*.

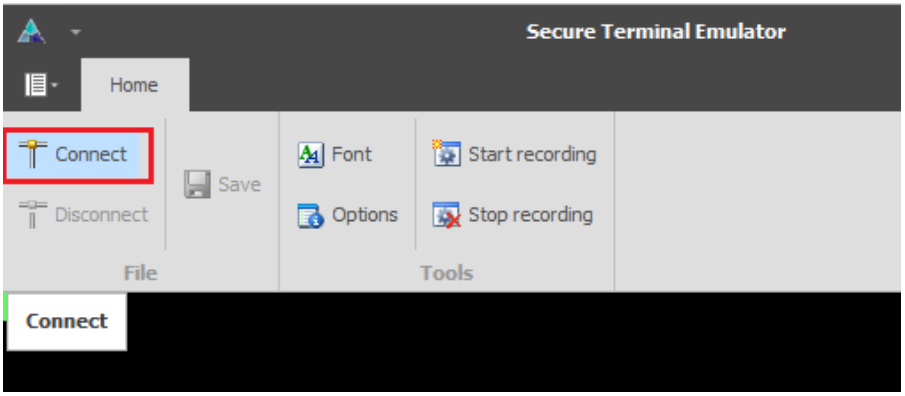


2. Ensure the Protocol is set to SSH and enter the MCP credentials to connect (for example):
   - Host Name: 192.168.168.81
   - Port: 22
   - Login name: **defadmin**
   - Password: **defadmin**



Connect to MCP Secure Terminal Emulator through Serial Port

1. Launch the Application: *Windows Start Menu* > *DS Agile Studio x.x* > *Secure Terminal Emulator x.x* and click on *Connect*.

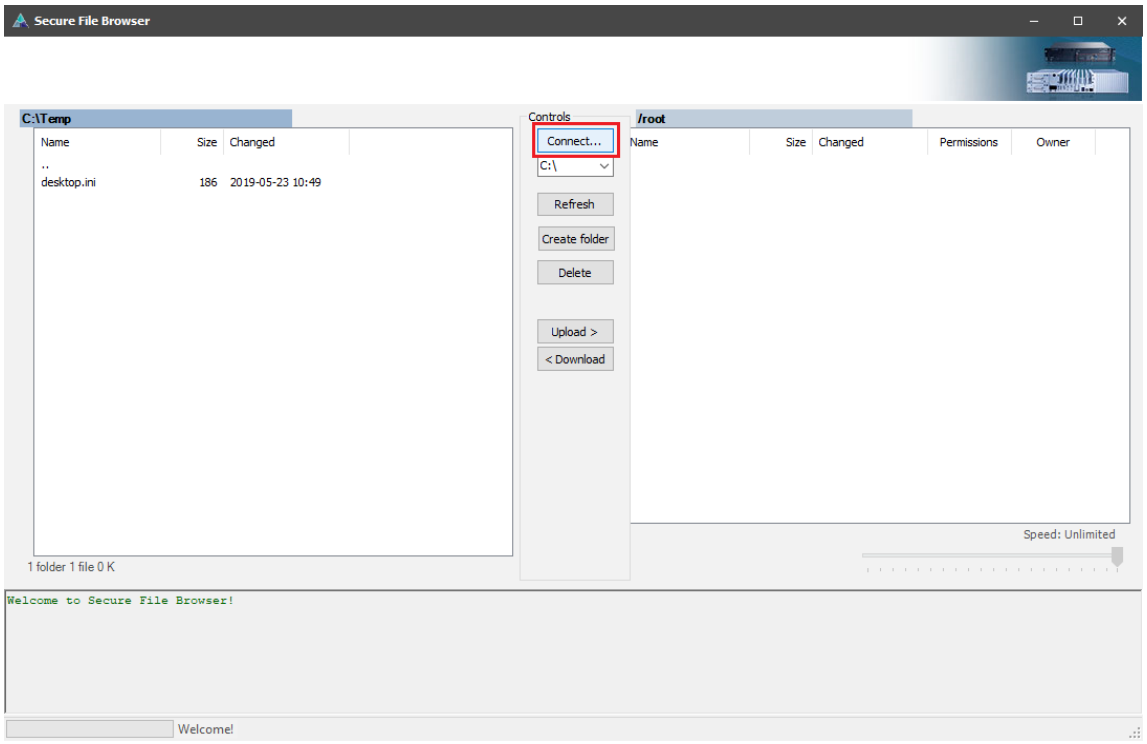


2. Ensure the Protocol is set to Serial Port and confirm the settings before selecting Connect:
    - Serial Port: Select the serial port used by your PC for the MCP serial maintenance connection
    - Baud rate: **115200**
3. At the MCP command shell login prompt, enter the credentials (e.g. defadmin):
    - Username: **defadmin**
    - Password: **defadmin**

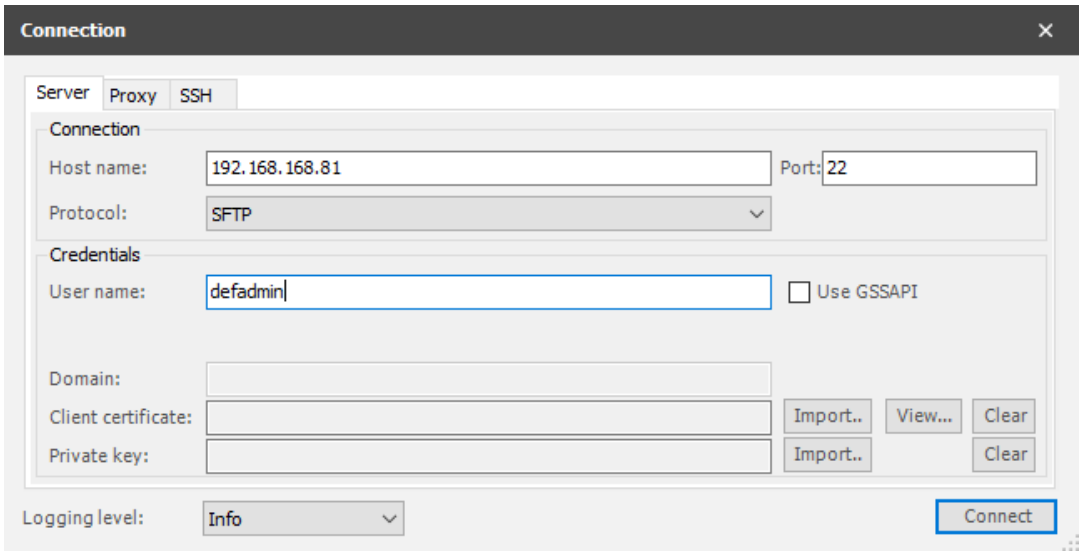
Appendix B – Secure File Browser

Secure File Browser (which is used to replace third-party tools like WINSCP®) is launched from the Windows start menu folder of DS Agile Studio.

1. Launch the Application: *Windows Start Menu* > *DS Agile Studio x.x* > *Secure File Browser x.x* and click on *Connect*.

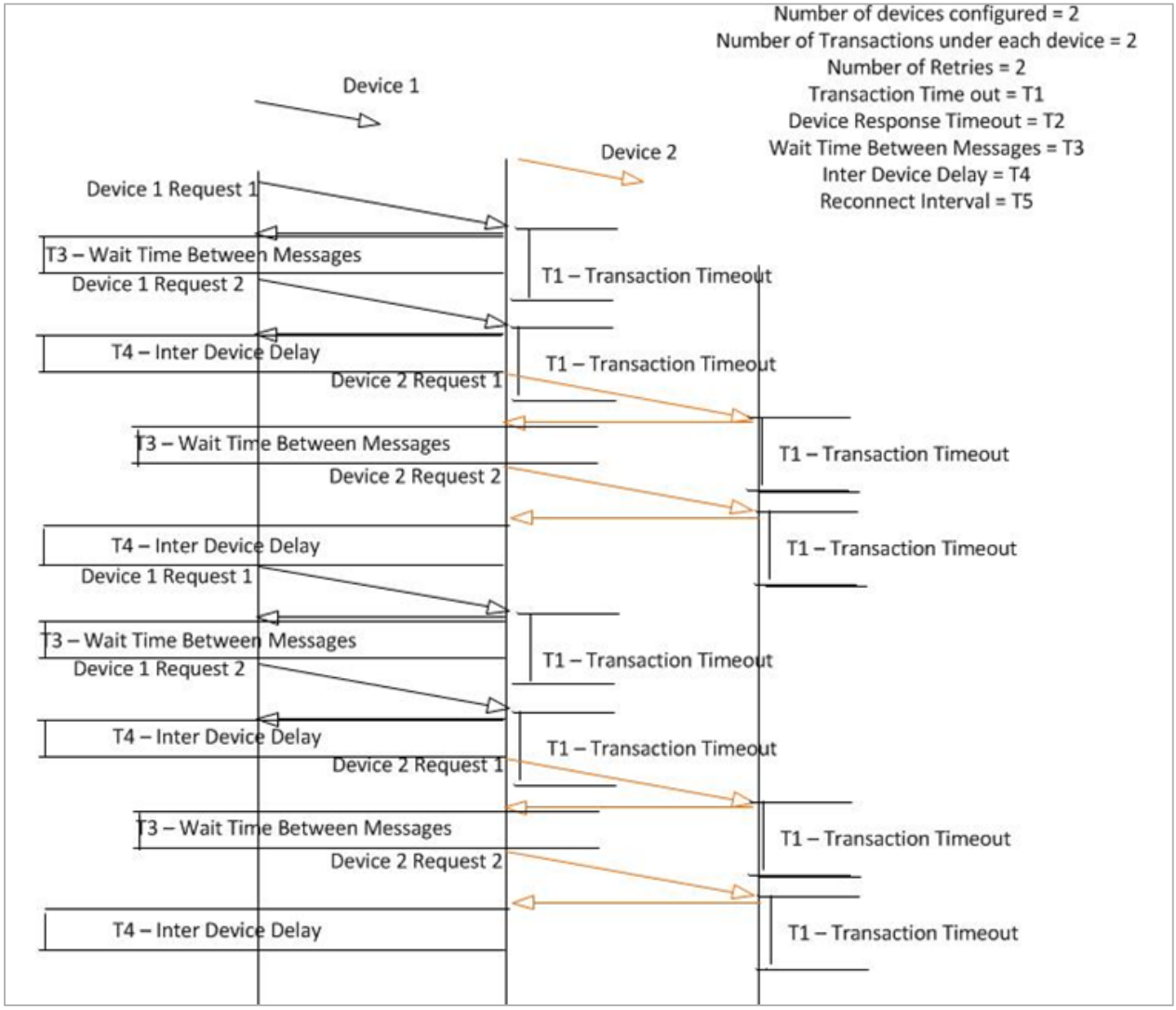


2. Enter the Host name / IP address, port and user/password, for example:



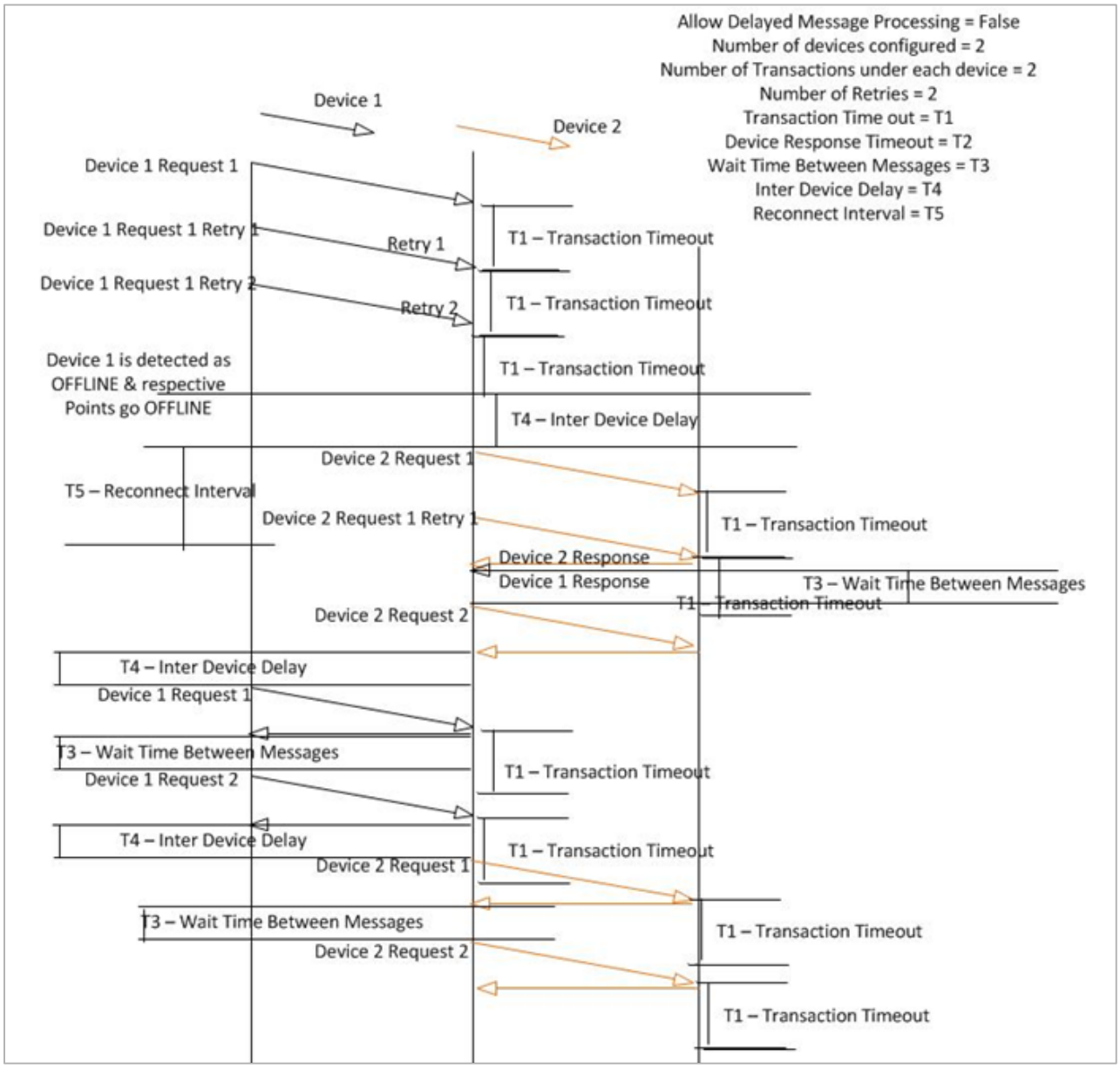
Appendix C - GenASCII Client - Time Sequence Diagrams and Sample Configuration for FEP Devices

Time Sequence of Message Transactions



NOTE: All devices are verified for polling in round robin fashion.

Time Sequence of Message Transaction with Support for delayed message processing as False



NOTE: When a response is not received within the Transaction timeout period for all the configured number of retries, the device is put OFFLINE along with all respective points.

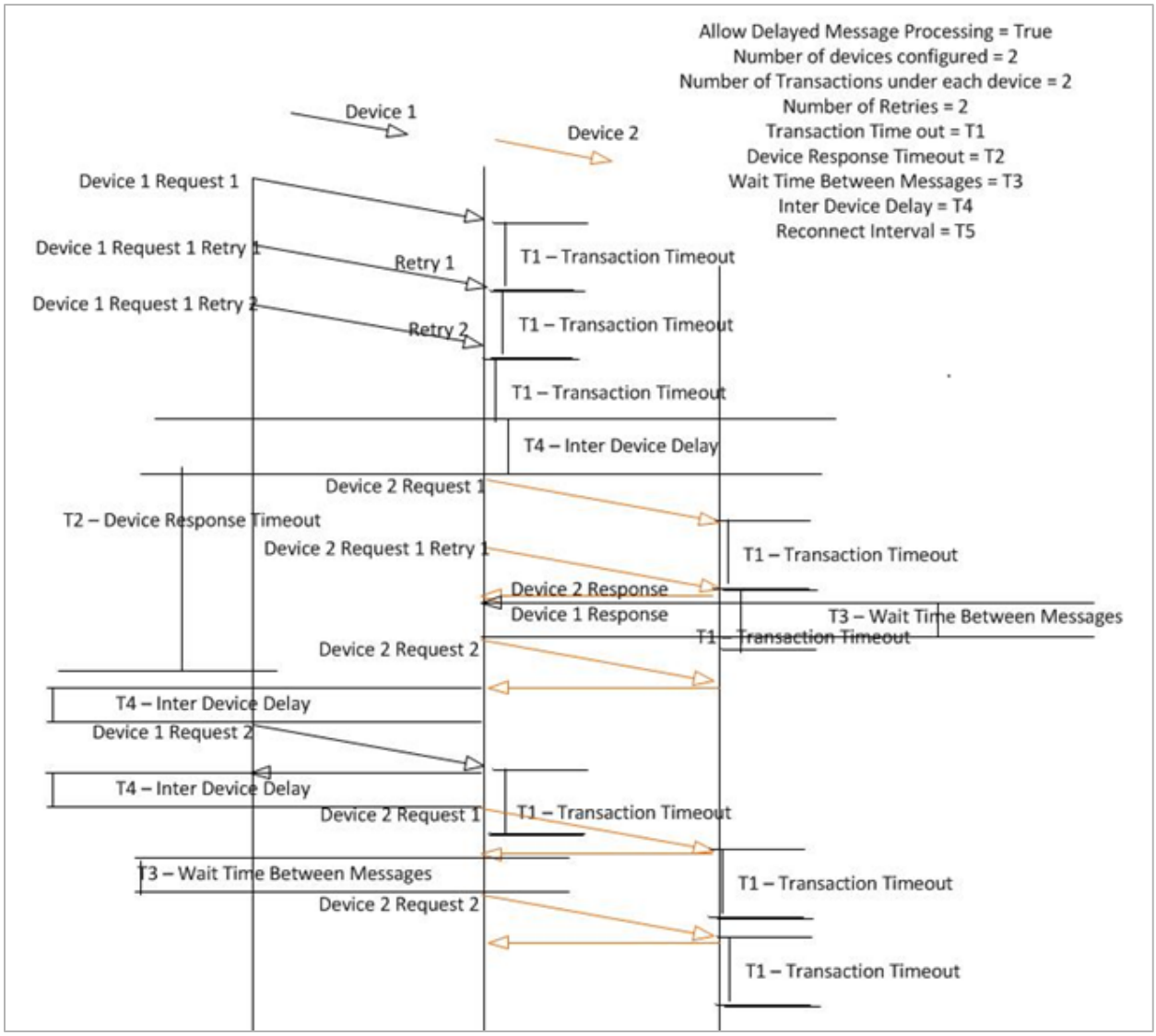
A response received after the device is put OFFLINE is ignored.

An OFFLINE device resumes communication only after the Reconnect Interval duration.

When the OFFLINE device communication resumes, it always resets and starts with the first transaction.

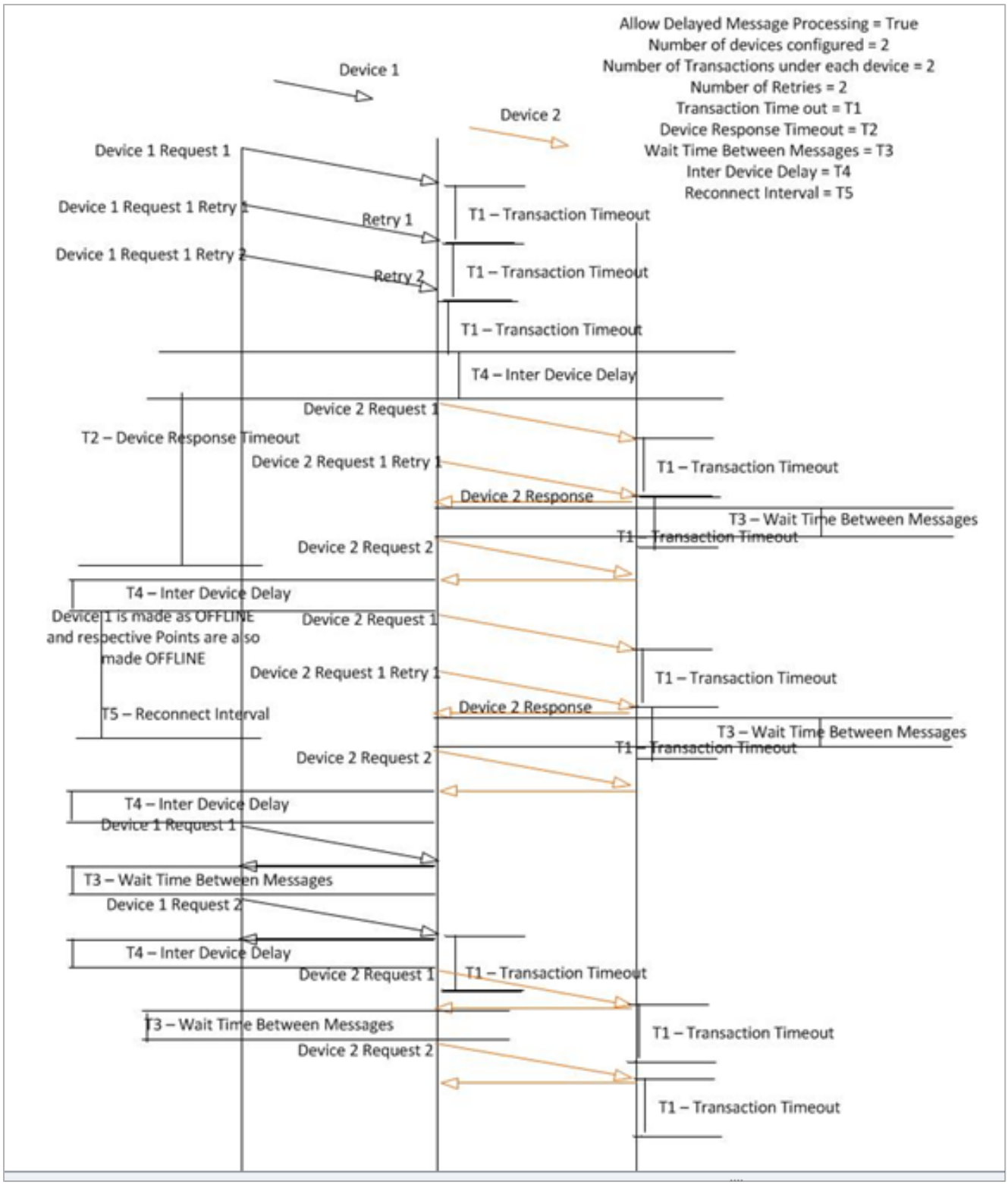
Time Sequence of Message Transaction with Support for delayed message processing as True

Delayed Response received within Device Response Timeout



NOTE: When responses are not received within the transaction timeout period for all the configured number of retries, but are received within the Device response timeout, responses are accepted and processed.

Delayed Response not received within Device Response Timeout:



NOTE: When a response is not received within the transaction timeout period for all the configured number of retries, and within Device response timeout period, the Device is put OFFLINE along with all respective points.

NOTE: An OFFLINE device resumes communication only after the Reconnect Interval duration.

When an OFFLINE device communication resumes, it always resets and starts with the first transaction.

Sample Configuration where response is expected within definite period

Consider configuring an IED with a transaction message having IED Address within transaction message.

IED Device 1:

Message to be sent: 1231241,I01241<CR>

Expected Response: 1FF12414F#

Response is expected within definite period of 100ms

The Message to be sent is to be configured as follows:

Application Parameters:

- Allow Delayed Message Processing: Disabled
- Inter Device Delay: Configure required delay between two consecutive IEDs

Connection Page:

- IED Address: 1241

Client Map File:

- Start of Message: 123
- End of Message: #
- Successful Login Prompt: #
- Transaction Timeout: 100
- Login Required: false (if login is not supported)
- Default Retries: 0 or any required number

Transaction Definition:

- Message OUT: This will be configured in following two ways.

  Method 1: 1241,I01241

  Method 2: {$ADDR$},I0{$ADDR$}

- Invalid Pattern: None

  NOTE: If device supports the detection of an invalid configuration by responding with predefined response for a mis-configuration, the predefined invalid pattern is to be defined for Invalid Pattern field. If the response matches with the Invalid Pattern defined, the Pseudo Point MsgError and ConfigError are incremented.

  Valid Response Pattern:

  - This is to be configured to detect the valid response reliably.

    I..1241 => this signifies that I is the starting character and 1241 is from 4th character position in the response.

I..{$ADDR$} => this signifies that I is the starting character and 1241 is derived at runtime from variable using Address field defined in connection page and expected from 4th character position in the response.

I..{$ADDR$}{$CHKSUM16$} => this signifies that I is the starting character and 1241 is from 4th character position and checksum is available from 3rd character position from end of response.

Depending on the configuration of the valid response pattern, the response is validated and if all the criteria defined in valid response pattern is met, the response is considered valid.

If, except for the checksum, the rest of the defined valid response pattern criteria is met, then the response is considered a MsgError and the Message is resent based on the configured number of retries.

If all defined valid response pattern criteria are met, the response is further processed as per the token / position based parsing policy defined in the transaction definition in the client map file for updating the points. If response fields are not correct (that is, the encoding format selected for processing the data response fields), the points are put offline with the old data quality attribute.

If all defined valid response pattern criteria are met and the data response fields are valid as per encoding format selected, the points are updated in the database.

Appendix D - Configuring a Linux-based Enterprise Server

SSH Server

Almost all Linux distributions typically come with an SSH server pre-installed on them.

Rsync utility

The rsync package is open-source software that enables the rsync utility on a Linux-based computer.

The rsync utility/software synchronizes files and directories from one location to another while minimizing data transfer using delta encoding when appropriate. An important feature of rsync not found in most similar programs/protocols is that the mirroring takes place with only one transmission in each direction. Since rsync does not provide any security while transferring data it is recommended that you use rsync over an SSH session. This allows a secure remote connection.

Installation Steps

Use any one of the following commands to install rsync. If you are using Debian or Ubuntu Linux, type the following command:

 # apt-get install rsync

or

$ sudo apt-get install rsync

If you are using Red Hat Enterprise Linux (RHEL) / CentOS 4.x or older version, type the following command:

 # up2date rsync

If you are a RHEL / CentOS 5.x or newer (or Fedora Linux) user, type the following command:

 # yum install rsync

NOTE: Since rsync does not provide any security while transferring data it is recommended that you use rsync over ssh session. This allows a secure remote connection.

Appendix E - Running Cron Jobs on the MCP

Scheduling background jobs in MCP using Cron utility

Using the MCP Cron utility is an effective way to schedule a routine background job at a specific time and/or day on an on-going basis.

In the MCP the ***/etc/crontab*** configuration file controls the background jobs that are to be scheduled. The format of the file is described in the table below.

```
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file.
# This file also has a username field, that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
42 6    * * *   root    run-parts /etc/cron.daily
47 6    * * 7   root    run-parts /etc/cron.weekly
52 6    1 * *   root    run-parts /etc/cron.monthly
30-59 * * * *   root    /etc/test.sh
```

Field	Description	Allowed Values
Min (m)	Minute field	0 to 59
Hour (h)	Hour Field	0 to 23
DOM	Day of Month	1 to 31
MON	Month of Year	1 to 12
DOW	Day of week	0 to 6
User	MCP user	
Command	Command to run	This can either be a direct shell command or a script.

For example:

In the below line from the ***crontab*** file, the ***test.sh*** script runs every minute on the second half of every hour.

```
30-59 * * * *   root    /etc/test.sh
```

where **30-59** is specified in the Minute field and the remaining fields specified with '*****'.

NOTE 1: The control file **/etc/crontab**:

- Needs to be copied to **/mnt/usr/MCP_SysConfig/etc/** so that the changes done are persisted across reboots.
- Can only be modified by root users or users with elevated root permissions.

NOTE 2: If you are running a script, the script should:

- Have executable permissions.
- Be copied to persistent storage to retain them across reboots.

NOTICE **GE is not responsible for the Cron jobs written by users.**

Appendix F – Shell commands

The customer support bundle tool is developed mainly for customer service team to collect system information when issues happen on customers MCP units. This tool also can be used internally for validation and bug report/analysis purpose.

This tool can only be run from the firmware container and have several conditions:

1. The user who wants to run this tool should be in root group;
2. The MCP unit should already have MCP core license installed;

Once the root group user logs into the firmware container, simply type the "mcpcsb" in the command line and then follow the instructions that the command shows as below:

mcpcsb

```
root@G500:/home/administrators# mcpcsb

CST support information collection request has been sent.

It may take a while to create the CST support information archive file.

Please check the READY file under /mnt/datalog/supportinfo/ directory.

Once the READY file is created, the .tgz archive file under the same diretory is ready.

Please retrieve this file and email it to the person helping with your case.

root@G500:/home/administrators# ls -l /mnt/datalog/supportinfo/
total 19128
-rw-r--r-- 1 root root       20 May 27 08:46 READY
-rw-r--r-- 1 root root 19555478 May 27 08:46 SupportInfo-2019-05-27-08-46-52-10.tgz
root@G500:/home/administrators#
```

The result will be saved as /mnt/datalog/supportinfo/SupportInfo-YYYY-MM-DD-HH-MM-SS-N.tgz, where YYYY-MM-DD-HH-MM-SS is the date/timestamp of the capture, and N is the number of files in the top directory in the archive. For now, N will be less than 10.

If there is already one archive file in the /mnt/datalog/supportinfo before create a new one, the current one will be saved into the /mnt/datalog/supportinfo/.history/. But only the latest old one will be kept in the .history folder and all other old ones will be deleted.

The mcpcsb also supports two command options (--exclude-logs and --exclude-config) to exclude the logs and/or configurations which might include sensitive information.

The full usage for this command is as below:

mcpcsb [--exclude-logs | -l] [--exclude-config | -c]

mcpsi

```
root@G500:/home/administrators# mcpsi

Retrieving the GE Multilin MCP system information, please wait ...

================================================================================
                      GE Multilin MCP System Information
================================================================================

Model Number:
    As-Built:      G500-BHU8-UUUUUU-BUUU-UUU-UUU-S-CAA0022-UUUUUUU
    As-Configured: G500-BHU4-TUUTTU-BUUU-UUU-UUU-S-CAA0022-UUUUUUU

Hardware Version:  V1.1    CPU Core #: 4   RAM Size:  16 GB   SSD Size:  235.7G

CPLD Version:      1.2.2            Date:  2018-11-15

FPGA Version:      01.03.00         Date:  2019-05-14

UEFI Version:      VX5D0007         Date:  2018-05-11

BCOM FPGA Version: 2.3.0

================================================================================

Predix Edge 2.2.1-REL-20190524.015211

Images Information:

    mcppanldisp     latest          2019-05-24      01:29:00      318MB

    mcpwdog         latest          2019-05-24      01:28:53      787MB

    mcphama         latest          2019-05-24      01:28:39      826MB

    mcpcore         latest          2019-05-24      01:28:25      1.44GB

    mcphmi          latest          2019-05-24      01:12:57      1.26GB

    mcpnw           latest          2019-05-07      07:51:09      299MB

================================================================================

GE Multilin MCP Firmware Release 110 Production Build 58 2019-05-24:04:42:03


License Information
================================================================================
Target Unit                     : G500
Serial Number                   : 64726472
Customer                        : ABB INC
License created from            : License Utilities V1.0.3

Application License             Status
================================================================================
001 : 61850                     Unlocked
002 : LogicLinx                 Unlocked
009 : ARRM                      Unlocked
012 : G500 Core                 Unlocked

================================================================================
```

Version info from Firmware container

GE Multilin™ MCP Firmware Release 110 Production Build 58 2019-05-24:04:42:03

Kernel Version:4.14.71-yocto-standard #1 SMP PREEMPT Fri May 24 02:36:28 UTC 2019

```
root@G500:/home/administrators# ver

GE Multilin MCP Firmware Release 110 Production Build 58 2019-05-24:04:42:03
Kernel Version:4.14.71-yocto-standard #1 SMP PREEMPT Fri May 24 02:36:28 UTC 2019
```

get_version from HAMA container

```
root@G500:/opt/ge_mcp/autoupdate# get_version
--------------------------------
--       FW Info V1.2.1       --
--------------------------------

FPGA Information
        Version: 01.02.01
        Type:    0
        Name:    Standard
        Date:    2018-11-26 10:16:52

CPLD Information
        Version: 1.2.2
        Date:    2018-11-15 16:52:47

BCOM FPGA Information
        Version: 2.3.0

BIOS Information
        Vendor: American Megatrends Inc.
        Version: VX5D0007 - Release
        Release Date: 11/05/2018
        Address: 0xF0000
        Runtime Size: 64 kB
        ROM Size: 8192 kB
        Characteristics:
                PCI is supported
                BIOS is upgradeable
                BIOS shadowing is allowed
                Boot from CD is supported
                Selectable boot is supported
                EDD is supported
                5.25"/1.2 MB floppy services are supported (int 13h)
                3.5"/720 kB floppy services are supported (int 13h)
                3.5"/2.88 MB floppy services are supported (int 13h)
                Print screen service is supported (int 5h)
                Serial services are supported (int 14h)
                Printer services are supported (int 17h)
                ACPI is supported
                USB legacy is supported
                BIOS boot specification is supported
                Targeted content distribution is supported
                UEFI is supported
        BIOS Revision: 0.7


MCOM EC Information
         Version: 1.3
         Build:   1
         Date :   2018-07-19 14:09
```

musb: USB Mount command

NOTE The USB must be formatted with FAT32 and must have a partition table.

Good USB

```
root@G500:/home/administrators# musb
         Proceeding with interactive mode...


         Will retry for 15 seconds (in case the USB drive(s) is(are) not yet initialized)
         Press Ctrl+C if you want to exit
                 Retrying...  Please wait .
         Successfully mounted the following USB device(s):
                sdb1  in  /mnt/usb/usb1
```

Corrupted USB

```
root@G500:/home/administrators# musb
         Proceeding with interactive mode...


         Will retry for 15 seconds (in case the USB drive(s) is(are) not yet initialized)
         Press Ctrl+C if you want to exit
                 Retrying...  Please wait .
         Could not mount the following USB device(s):
                sdb1
         Possible reasons:
                 1. No USB drive inserted into one of the available slots.
                 2. The inserted USB drive is malfunctioning.
                 3. The inserted USB drive is not compatible with D400 drivers.
                 4. Device(s) busy (some other process is using the device(s)).
```

No USB

```
root@G500:/home/administrators# musb
         Proceeding with interactive mode...


         Will retry for 15 seconds (in case the USB drive(s) is(are) not yet initialized)
         Press Ctrl+C if you want to exit
                 Retrying...  Please wait .
```

musb unmount: USB unmount command

```
root@G500:/home/administrators# musb unmount
success
root@G500:/home/administrators# ls -l /mnt/usb/
total 0
```

Appendix G – Security Certificates Creation for MCP

Overview

This chapter describes how to create and deploy security certificates for secure communication using HTTPS protocol between the DSAS and MCP Runtime HMI Viewer and MCP web server. The secure channel is implemented using an SSL (Secure Sockets Layer)/TLS (Transport Layer Security) connection and certificate-based server authentication.

Certificates are issued by a Certification Authority (CA). The MCP does not come with a CA so you must make use of an existing CA or create your own. There are many third-party commercial and open source CAs available. This chapter describes one open source CA package: X Certificate and Key Management (XCA).

Setting up a Certification Authority

Before you can configure a secure channel between a client device and the MCP you need a Certification Authority (CA). In case you don't already have a CA, this section describes how to set up the XCA certification authority.

Once your CA is up and running, export the CA certificate so that you can install it on the MCP.

NOTICE

A CA that is planned for field use should be protected with strong security measures. Such measures include dedicating a machine for the CA, physically securing the machine, ensuring the machine is accessible only by authorized users, and not connecting the machine to a network. Such measures are required because a security breach of a CA would impact all devices that used certificates generated by the authority.

Setting up the XCA Certification Authority

XCA runs on Linux or Microsoft Windows. The following steps detail how to setup and initialize an XCA certification authority.

Install XCA

1. Download the latest version of XCA from here: http://sourceforge.net/projects/xca.
2. Run the installation wizard to install XCA.

Create a Database and Initialize the CA

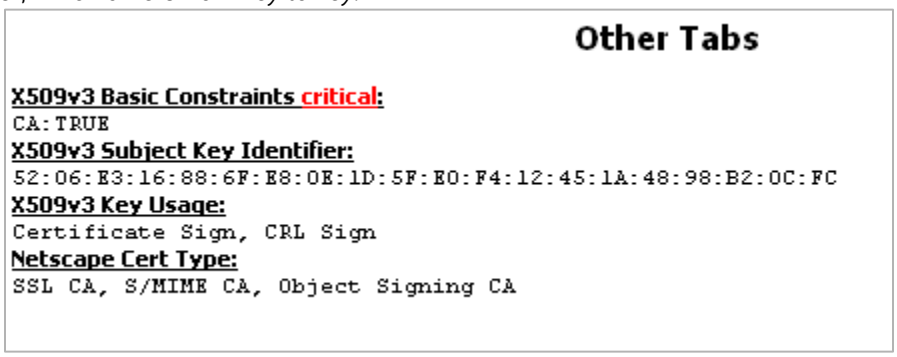
1. From XCA, select **File** > **New Database**.
2. Choose a protected location to save the database and then enter a strong password to encrypt the database.
3. Under the **Certificates** tab, choose **New Certificate**.
4. Under the **Source** tab, select the checkbox next to the label **Create a self-signed certificate with the serial**. Leave the dropdown named **Signature Algorithm** as "SHA 256" and leave the dropdown named **Template for the new certificate** as "[default] CA".

5. Under the **Source** tab, click **Apply All**.
6. Under the **Subject** tab, click the button labeled **Generate a new key**.
7. In the dialog that appears, enter the name of the CA (e.g., "MyCA") in the **Name** field. Choose the **Keytype** as RSA Change the **Keysize** to 2048.
8. Under the **Subject** tab, enter the distinguished name of the CA certificate. The following table provides example distinguished name components.
   Note: You must enter all components of the distinguished name, including the email Address.

Table 0.1: Example Distinguished Name Components

Distinguished Name Component	Example
Internal name	MyCA
countryName	US
stateOrProvinceName	MyState
localityName	MyCity
organizationName	MyCompany
organizationalUnitName	MyDivision
commonName	MyCA
emailAddress	mail@my.domain

9. Under the **Extensions** tab, if necessary, change the **Time Range** that the CA certificate is valid for and click **Apply**. The default is 10 years. Certificates generated with this CA certificate after this period are no longer valid.
10. Under the **Key usage** tab, do not change the defaults.
11. Under the **Netscape** tab, remove the value in the **Comment** field.
12. Under the **Advanced** tab, the following messages are expected except the value of the X509v3 Subject Key Identifier, which differs from key to key:



If above message is not displayed, click **Validate** to see the message.

13. Click **OK**. You now have a CA certificate to sign your MCP web server certificates.
14. Under the **Certificates** tab of the main view of XCA, select the new Certification Authority and click on **Export**.
15. Ensure the **Export Format** is set to PEM.
16. Browse to a protected directory (e.g., My Documents->MyXCAFiles) and click **Save**. Finally click **OK**. The file is named based upon the internal name of your CA with a .crt extension.

Certificate Generation

This section describes how to generate private keys and certificates for the MCP https web server. These certificates allow the MCP to authenticate itself to the Client.

Creating a CA-Signed Server Certificate

1. Click the Certificates tab.
2. Click the **New Certificate** button.
3. Make sure the **Source** tab is showing, clicking it if necessary.
    - At the bottom of the panel, select the template **"[default] HTTPS_server"** (or another suitable template, if you have created your own) and click the **Apply** button. This will fill in appropriate values under the **Extensions**, **Key Usage**, and **Netscape** tabs.
    - In the Signing section, select the certificate that will be used to sign the new certificate. Select the radio button next to the label **Use this Certificate for signing**. On the dropdown to the right of this checkbox, select the CA you created in section Create a Database and Initialize the CA (e.g., MyCA).
4. Click the **Subject** tab.
    - Please enter the Distinguished name of the MCP server certificate.

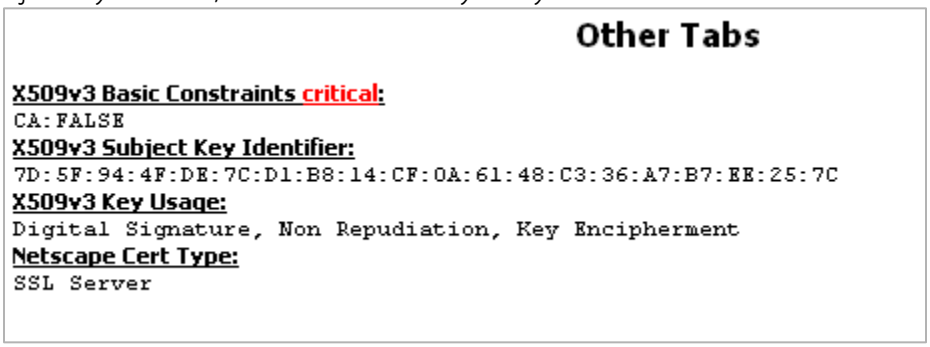
    Note: You must enter all components of the distinguished name, including the email Address.

Table 0.2: Example Distinguished Name Components

Distinguished Name Component	Example
Internal name	MyMCP
countryName	US
stateOrProvinceName	MyState
localityName	MyCity
organizationName	MyCompany
organizationalUnitName	MyDivision
commonName	**MyMCP**
emailAddress	mail@my.domain

5. Under the **Subject** tab, click the **Generate a new key** button.
    - In the dialog that appears, enter a name that uniquely identifies the MCP in your network (for this example, that is "MyMCP"). Choose **Keytype** as RSA and change the **Keysize** to 2048. Click **OK**.
6. Click the **Extensions** tab.
    - Under the **Extensions** tab, if necessary, change the **Time Range** that the server certificate is valid for and click **Apply**. The default is one year. The shorter the Time Range the more secure the certificate. The longer the Time Range, the more often you need to regenerate MCP Server certificates and deploy them into your MCP.
7. Under the **Key usage** tab, leave the defaults.
8. Under the Netscape tab, remove the comment.

9. Under the **Advanced** tab, click **Validate**. The following messages are expected except the value of the X509v3 Subject Key Identifier, which differs from key to key:



   If above message is not displayed, click **Validate** to see the message.
10. Click the OK button at the bottom. You now have a MCP certificate.
11. In the tree view under the **Certificates** tab, open the branch labeled after your Certificate Authority, and select the new Server certificate.
12. Click **Export.**
13. In the dialog that appears, ensure the **Export Format** field is set to "PEM Cert". Browse to a protected location **(e.g., My Documents->MyXCAFiles)** and click **Save**. Finally click **OK.** The certificate will be in a file named with your MCP's Internal Name with the extension .crt (e.g., MyMCP.crt).
14. Now go to **Private Keys** tab and select Private key with Internal name MyMCP.
15. Click **Export**.
16. In the dialog that appears, ensure the **Export Format** field is set to "PEM private". Browse to a protected location **(e.g., My Documents->MyXCAFiles)** and click **Save**. Finally click **OK.** The certificate will be in a file with the extension .pem (e.g., MyMCP.pem).

NOTICE This file is sensitive so keep it protected always. Remove the file after it has been installed on the MCP.

Installing Certificates

This chapter describes how the CA Certificate, Server Certificate, Server key is installed on your Windows PC and MCP respectively. The following table summarizes where to get the files containing the CA certificate, Server certificates and key.

Table 0.3: Location of Files Exported by Certification Authorities

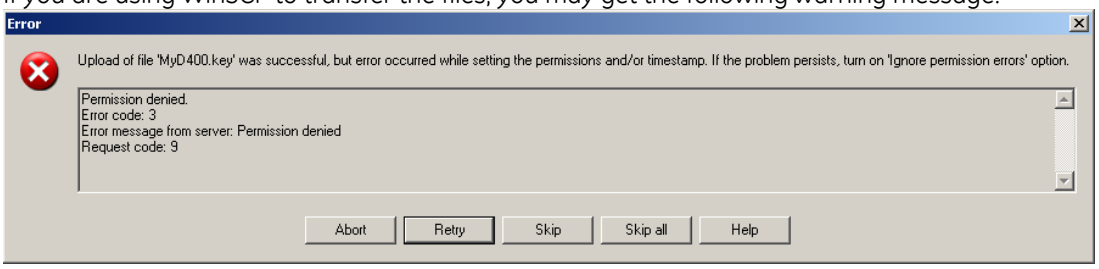
Files	Location
CA Certificate	The CA certificate is in a file downloaded to a location of your choice as described in Section Create a Database and Initialize the CA. The file is named with a .crt extension (e.g., MyCA.crt).
Server Certificate	Server certificate is in the file under the location of your choice as described in Section Creating a CA-Signed Server Certificate. The file is named with a .crt extension (e.g., MyMCP.crt).
Server Private Key	Server private key is in the file under the location of your choice as described in Section Creating a CA-Signed Server Certificate. The file is named with a.pem extension (e.g., MyMCP.pem).

Installing Server Certificate and Private Key on the MCP

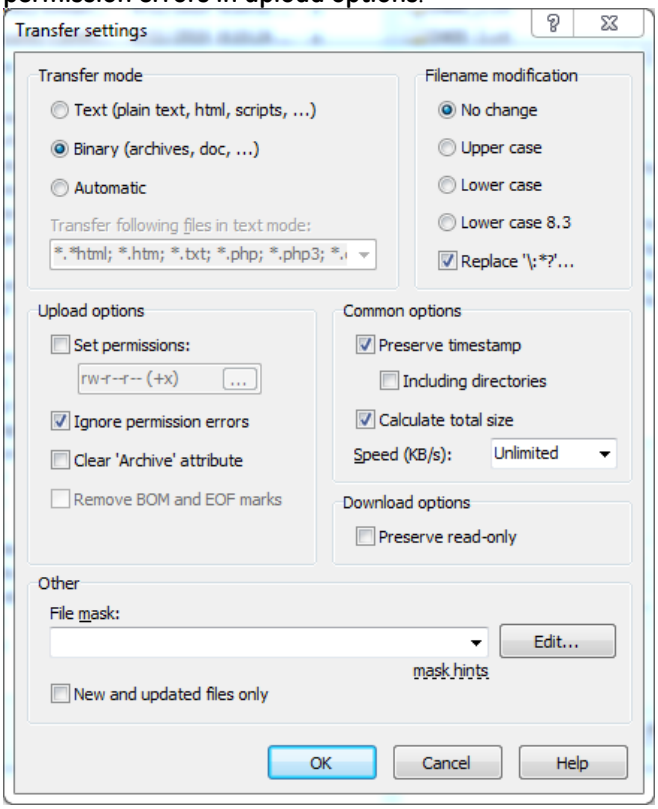
1. Referring to Table 400 for file names and locations, copy the files containing the Server certificate, and server private key to following locations:
   - Copy Server Certificate to the folder /home/MCP_SysConfig/Certificate as **server.crt** on the MCP. In this case, use an SFTP/SCP file transfer program such as WinSCP.
   - Copy Server Private Key to the folder /home/MCP_SysConfig/Certificate as **server.key** on the MCP. In this case, use an SFTP/SCP file transfer program such as WinSCP.

NOTICE Private key file is sensitive so keep it protected always.

2. If you are using WinSCP to transfer the files, you may get the following warning message:



The reason for this warning is that the MCP file system does not support per-file permissions, so when WinSCP tries to set the permissions on a file, it is unable to do so. However, there is no security risk because the file takes on the default permissions of the files system which are correct. Therefore, this warning can be safely ignored by clicking **Skip**. To prevent this warning from appearing in the future, in WinSCP go to **Options** > **Preferences**. Then select **Transfer** and click **Edit** button and select **Ignore permission errors in upload options**.



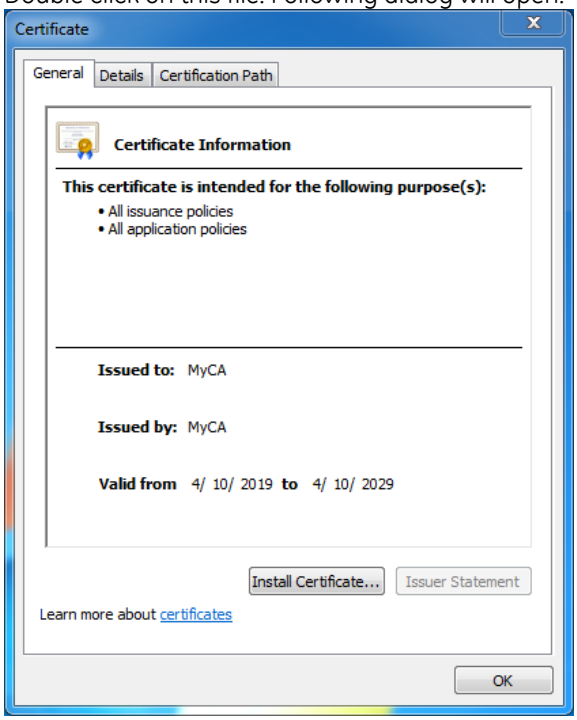
3. Now reboot your MCP so that new certificates can be loaded.
4. Now launch mcpcfg from the MCP console or SSH terminal window.

5. Select **Configure Secure Access** > **Configure Web Mode**. If the current Web Mode is HTTP, please change it to HTTPS.

Installing CA Certificate for use by the MCP Runtime HMI Viewer

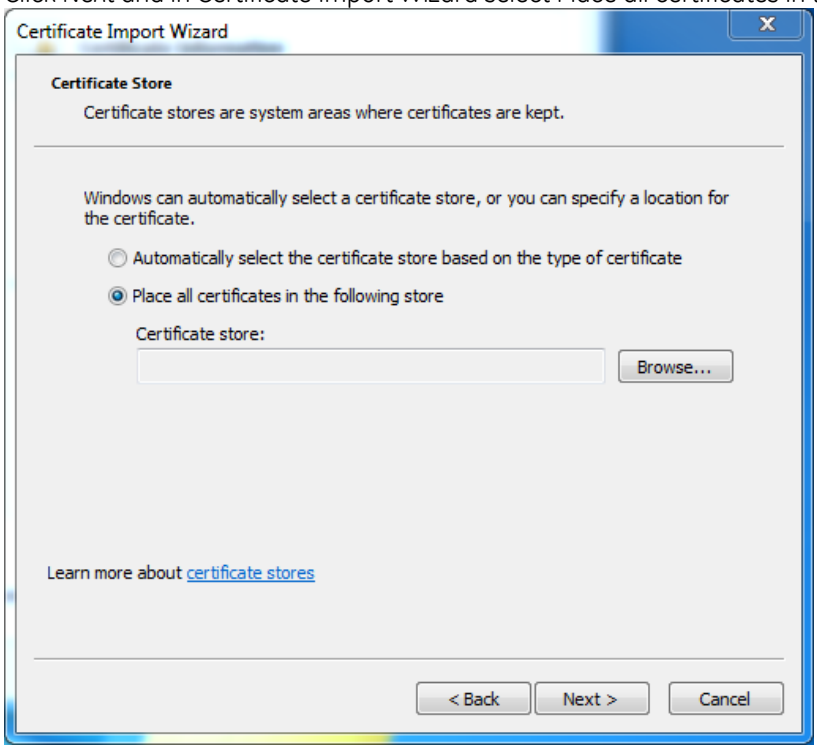
Note: This section is only required for the MCP Runtime HMI Viewer. The DSAS HMI Viewer will prompt you to confirm the server certificate on first connection to the MCP and therefore doesn't use a CA certificate to validate the server certificate.

1. Copy the CA certificate to client Windows PC to a directory of your choice (e.g., CA.crt).
2. Double click on this file. Following dialog will open.

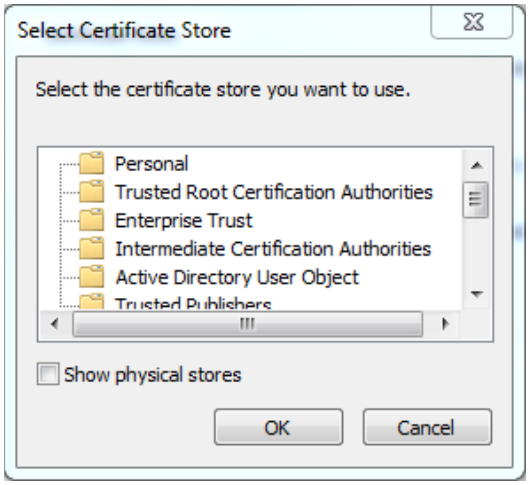


3. Click **Install Certificate** button. Following dialog will open. Click **Next**.

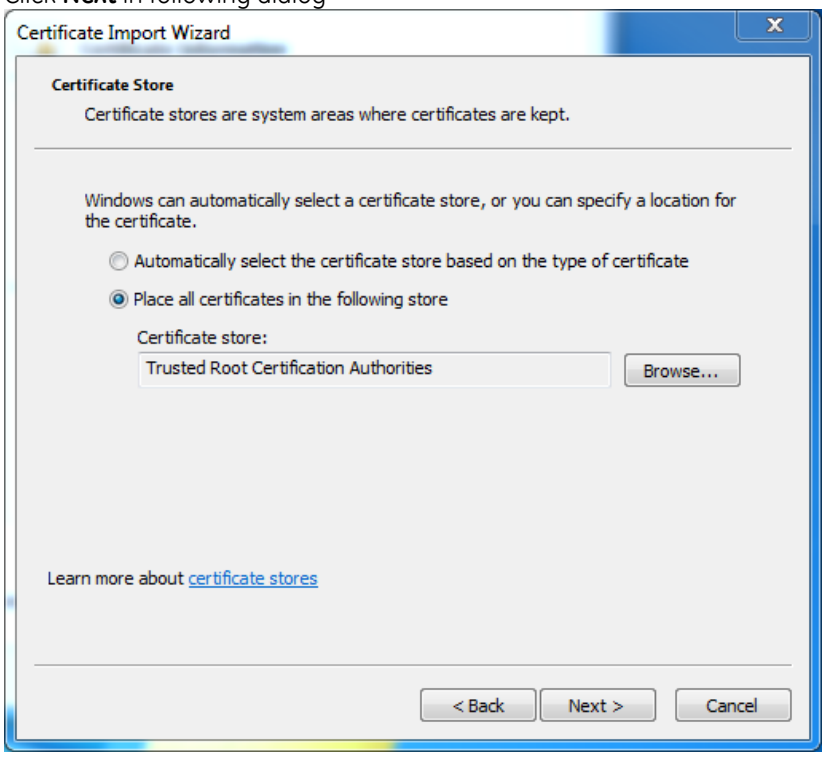
4. Click Next and in Certificate Import Wizard select Place all certificates in the following store option.



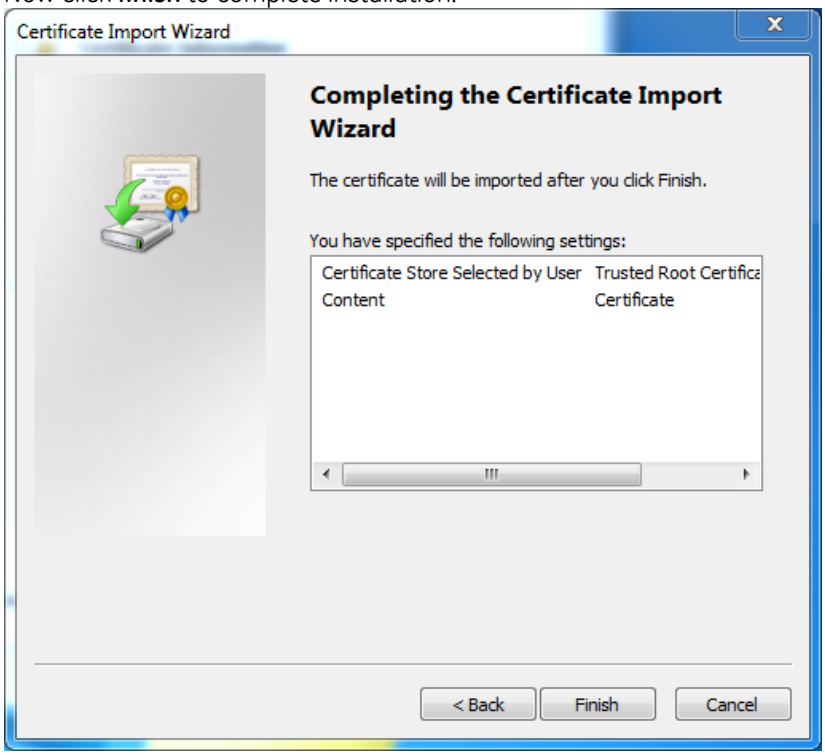
5. Click Browse and in Select Certificate Store Dialog Select Trusted Root Certification Authorities and click OK.



6. Click **Next** in following dialog



7. Now click **finish** to complete installation.



After this step you may use the MCP Runtime HMI Viewer for secure communication with the MCP device.

Appendix H – List of Factory Default open ports (TCP and UDP)

Overview

This chapter describes complete list of ports. Factory default open ports are indicated by "**Yes**" from the "Enabled by default?" column from the below table:

Port Numbers	TCP/UDP	Enabled by default ?	Used for…
443	TCP	Yes	Sync to/from, Online Editor, PETC, Remote runtime HMI.
22	TCP	Yes	Snapshot save/restore, shell access to gateway, file transfer with Gateway.
922	TCP	No	Emergency administrator access, open only when remote authentication configured.
80, 8081	TCP	Yes	Settings GUI.
123	TCP	No	NTP, if configured.
Configurable, default 502	TCP	No	MODBUS, if configured.
Configurable, default 2404	TCP	No	IEC60870-5-104, if configured.
514	UDP	No	Rsyslog, if configured.
10514	TCP	No	Rsyslog, if configured.
Configurable, default 20000	TCP/ UDP	No	DNP, if configured.
Configurable, default 8001 – 8020	TCP	No	Pass-through or terminal server, if configured.
Configurable	TCP	No	TLS tunnel for pass through, terminal server or secure connection relay, if configured.
54000	TCP	No	LogicLinx, if configured.
162	UDP	No	SNMP, if configured.
Configurable, default 1194	UDP	No	OpenVPN, if configured.
51003	TCP	No	Standby pointing to active tunnel, if configured.
51194, 51195	TCP	No	Hot/Warm Standby Tunnel, if Hot/Warm-Standby Configured(not supported in G100)
389	TCP	Yes	LDAP Client Outgoing if Configured.

Appendix I – Modbus Protocol Support

Read Coils Status (Function Code 1)

This function code is used to read the status of the coils, contiguous from 1 to 2000, in an IED. The DCA shall transmit configured READ COILS STATUS Modbus Command to the IED.

The response message contains coils status packed as one coil per bit. Status is indicated as 1=ON and 0=OFF. The DCA shall read multiple coils from the IED.

The Coil status read from the IED shall be represented as a 1 BIT DIGITAL INPUT in the MCP's system points real-time database (RTDB).

Read Input Status (Function Code 2)

This function code is used to read from 1 to 2000 contiguous status of discrete inputs in an IED. The DCA shall transmit configured READ INPUT STATUS Modbus Commands to the IED.

The discrete inputs in the response message are packed as one input per bit of the data field. Status is indicated as 1=ON and 0=OFF. The DCA shall read multiple input status from the IED.

The Input status read from the IED shall be represented as a 1 BIT DIGITAL INPUT in the MCP's system points real-time database (RTDB).

Read Holding Registers (Function Code 3)

This function code is used to read the contents of a contiguous block of 1 to 125 holding registers in an IED. The DCA shall transmit configured READ HOLDING REGISTERS Modbus Commands to the IED.

The register data in the response are packed as two bytes per register. The DCA shall process the received register data by performing the following:

- Apply the byte ordering interpretation as specified by the Endian configuration in the IED MAP FILE
- Parse the values of the registers as specified by the Data Type configured in IED MAP
- Apply a scaling factors as specified in the IED MAP FILE

The DCA shall represent the values calculated from above as an ANALOG INPUT and storing in the MCP's system points real-time database (RTDB).

Read Input Registers (Function Code 4)

This function code is used to read the contents of a contiguous block of 1 to 125 Input registers in an IED. The DCA shall transmit configured READ INPUT REGISTERS Modbus Commands to the IED.

The register data in the response are packed as two bytes per register. The DCA shall process the received register data by performing the following:

- Apply the byte ordering interpretation as specified by the Endian configuration in the IED MAP FILE
- Parse the values of the registers as specified by the Data Type configured in IED MAP
- Apply a scaling factors as specified in the IED MAP FILE

The DCA shall represent the values calculated from above as an ANALOG INPUT and storing in the MCP's system points real-time database (RTDB).

This function code is used to read from 1 to approximately 125 input registers in an IED. The DCA shall transmit configured READ INPUT REGISTERS Modbus Commands to the IED.

Write Single Coil (Function Code 5)

This function code is used to write a single output to either ON or OFF in an IED. The requested state ON/OFF is specified by a constant in the request data field.

As specified in the Modbus Protocol Specifications, a value of 0xFF00 request the output to be ON; a value of 0x0000 requests the output to be OFF. All other values are illegal or invalid. The Modbus DCA shall transmit a Write Single Coil command with a value of 0xFF00 or 0x0000.

The value to be transmitted for the Write Single Coil command is user configurable in the IED MAP FILE. These values are defaulted per the Modbus protocol specification, but the user has the capability of modifying the default values via the Modbus Config Applet. The configurable value allows the Modbus DCA to provide greater flexibility to better interoperate with non-standard MODBUS protocol implementations in third party vendor products.

The configured points in the IED MAP FILE shall be represented as a DIGITAL OUTPUT in the MCP's system point database. When a DIGITAL OUTPUT control is requested on the coil, the DCA shall transmit the WRITE SINGLE COIL command to the IED. The value configured in the IED MAP FILE shall be used in the transmit request command.

As specified in the Modbus Protocol Specifications, a normal response is an echo of the request. The DCA shall utilize this echo message to determine FAILURE or SUCCESS of the DIGITAL OUTPUT control request in the MCP's system point database.

Write Single Register (Function Code 6)

This function code is used to write a single holding register in an IED. As specified in the Modbus Protocol Specifications, the value of 0xFF00 and 0x0000 are permitted to be the transmitted register value. All other values are illegal or invalid. The Modbus DCA shall transmit a Write Single Register command with a value of 0xFF00 or 0x0000 as configured in the IED MAP FILE.

These values are defaulted per the Modbus protocol specification, but the user has the capability of modifying the default values via the Modbus Config Applet. The configurable value allows the Modbus DCA to provide greater flexibility to better interoperate with non-standard MODBUS protocol implementations in third party vendor products.

The configured points in the IED MAP FILE shall be represented as a DIGITAL OUTPUT in the MCP's system point database. When a DIGITAL OUTPUT control is requested on the coil, the DCA shall transmit the WRITE SINGLE COIL command to the IED. The value configured in the IED MAP FILE shall be used in the transmit request command.

As specified in the Modbus Protocol Specifications, a normal response is an echo of the request. The DCA shall utilize this echo message to determine FAILURE or SUCCESS of the DIGITAL OUTPUT control request in the MCP's system point database.

Data Representation for Write Single Register

The WRITE SINGLE REGISTER shall be configured as either 0x6A or 0x6B in the IED MAP FILE. If a register is configured as 6A, the user shall be required to specify a value (0xFF00 or 0x0000) to be sent to the IED. If a register is configured as 6B, the user shall not be required to configure a value.

Registers shall be represented in the MCP's system database as either DIGITAL OUTPUTS or ANALOG OUTPUTS based on its configuration in the IED MAP FILE, as follows:

- Registers mapped as 0x6A are represented as DIGITAL OUTPUTS in the system point database. When a control is queued to the point, the DCA shall transmit a WRITE SINGLE REGISTER command to the IED with the value specified in the IED MAP FILE.
- Registers mapped as 0x6B are represented as ANALOG OUTPUTS in the system point database. When a control is queued to this point, the DCA shall transmit a WRITE SINGLE REGISTER command to the IED with the value specified in the ANALOG OUTPUT REQUEST.

Glossary

A

AD: Active Directory

B

BG: Background

C

CHP: Combined Heat and Power. A CHP unit is a cogeneration system.

CMYK: Cyan/Magenta/Yellow/Black (color palette)

CR: carriage return

CRL: Certificate Revocation Lists

D

DAN: Double Attached Node

DCA: Data Collection Application. Also referred to as client application

DNP: Distributed Network Protocol

DPA: Data Processing Application. Also referred to as server application.

DPMS: Display Power Management Signaling

DST: Daylight Saving Time

DTA: Data Translation Application. Also referred to as automation application.

F

FG: foreground

G

GUI: Graphical User Interface (also called Human Machine Interface – HMI)

GTW / GW: Gateway

H

HMI: Human Machine Interface (also called Graphical User Interface – GUI)

HMI Client: Client-side functionality that resides in the user's browser

HMI Server: Server-side functionality that resides on the MCP and provides services to the client-side browsers

HSL: hue/saturation/lightness (color palette)

HSV: hue/saturation/value (color palette)

HTTP: HyperText Transfer Protocol

HTTPS: Designated the use of HTTP but with a different default port and an additional encryption/authentication layer between HTTP and TCP

I

IED: Intelligent Electronic Device

IP: Internet Protocol

IRIG-B: Inter Range Instrumentation Group (IRIG) - an American standardized network time code format

J

JRE: JAVA Runtime Environment

L

LAN: Local Area Network

LDAP: Lightweight Directory Access Protocol

LF: linefeed

M

MAC: Media Access Control

MCP: Multifunction Controller Platform

MPC: Model predictive control

mSQL: Mini Sequential Query Language - provides fast access to stored data with low memory requirements

N

NIC: Network Interface Card

NTP: Network Time Protocol

NVRAM: Non-Volatile Random Access Memory

O

OLV: One-Line Viewer

P

P: Active Power

PRF: Protective Relay Fault

PRP: Parallel Redundancy Protocol

Q

Q: Reactive Power

R

RBAC: Role Based Access Control

RGB: Red/Green/Blue (color palette)

RGE: ratio for gas-to-electricity

RGH: ratio for gas-to-heat

RTC: Real-time clock

RTDB: Real-time database

S

S: Apparent Power

Secure SCADA: Secure SCADA is a term used to refer to a number of features built into the MCP Substation Gateway to facilitate encrypted communications and identity verification.

sFTP: Secure File Transfer Protocol

SNTP: Simple Network Time Protocol

SOE: Sequence of Events

SSH: Secure Shell

SSL: Secure Socket Layer

T

T: Torque

TFTP: Trivial File Transfer Protocol

TCP: Transmission Control Protocol

U

UR: Universal Relay

URL: Universal Resource Locator

Modification Record

Version	Revision	Date	Change Description
1.00	0	25th March, 2019	Document Created.
1.10	0	14th February, 2020	Updated for G500 v1.1 release.
2.00	0	29th May, 2020	Updated for G500 v2.0 release.
2.10	0	10th December, 2020	Updated for G500 v2.1 release.
	1	27th January, 2021	Updated LDAP Server software configuration guide references (SWM0111/12/13).
3.00	0	18th May, 2021	Updated for MCP family.
	1	26th July, 2021	Updated DN components requirements

GE
Grid Solutions

Multilin™ MCP Substation Gateway Analog Reports

User Guide

SWM0102

Version 2.00 Revision 1

imagination at work

GE Information

Copyright Notice

© 2021, General Electric Company. All rights reserved.

The information contained in this online publication is the exclusive property of General Electric Company, except as otherwise indicated. You may view, copy and print documents and graphics incorporated in this online publication (the "Documents") subject to the following: (1) the Documents may be used solely for personal, informational, non-commercial purposes; (2) the Documents may not be modified or altered in any way; and (3) General Electric Company withholds permission for making the Documents or any portion thereof accessible via the internet. Except as expressly provided herein, you may not use, copy, print, display, reproduce, publish, license, post, transmit or distribute the Documents in whole or in part without the prior written permission of General Electric Company.

The information contained in this online publication is proprietary and subject to change without notice. The software described in this online publication is supplied under license and may be used or copied only in accordance with the terms of such license.

Trademark Notices

GE and are trademarks and service marks of General Electric Company.

* Trademarks of General Electric Company.

Cisco is a registered trademark of Cisco Corporation. Hyperterminal is a registered trademark of Hilgraeve, Incorporated. IEC is a registered trademark of Commission Electrotechnique Internationale. IEEE and POSIX are registered trademarks of the Institute of Electrical and Electronics Engineers, Inc. Internet Explorer, Microsoft, and Windows are registered trademarks of Microsoft Corporation. JAVA is a registered trademark of Sun Microsystems, Inc. MODBUS is a registered trademark of Schneider Automation, Inc. Netscape is a registered trademark of Netscape Communications Corporation. SEL is a registered trademark of Schweitzer Engineering Laboratories, Inc.

Other company or product names mentioned in this document may be trademarks or registered trademarks of their respective companies.

Contents

About this Document **4**

Product Support **6**

GE Grid Solutions Web Site....6
GE Technical Support Library....6
Contact Technical Support....6

1 Creating Template Using iReport Designer **7**

1.1 iReport Designer....7
1.2 Report Template Creation Procedure....7
1.3 Create a Customized Offline Report Template .8
1.4 Create a Customized Online Report Template39

2 Importing Templates **46**

2.1 Create MANIFEST file....46
2.2 Create RZ file....47
2.3 Upload Template....47

3 Offline Report Viewer **49**

3.1 Report Controls....49
3.1 Offline Report Fields....50

4 Online Report Viewer **51**

4.1 Use Filter....52
4.2 Set Report Parameters....52
4.3 Select AI Points....53

5 Analog Report Generation - Configuration **54**

5.1 Reports Tab....54
5.2 Templates Tab....57

About this Document

Purpose

This document describes how to set up Analog Reports in a Multilin™ MCP HMI.

NOTICE This document applies to the MCP family (G100/G500) unless otherwise indicated.

Screen captures may show G500 in some areas, however the workflow applies to products in the MCP family (G100/G500).

Intended Audience

This document provides a reference for systems integrators who wish to set up Analog Reports on the MCP.

Additional Documentation

For further information about Analog Reports, refer to the following documents:

- MCP Substation Gateway, Software Configuration Guide
- MCP HMI Online Help
- iReport Ultimate Guide

http://community.jaspersoft.com//system/files/documentation/ireport-ultimate-guide.pdf

NOTICE It is highly recommended that the iReport Designer tool distributed with the MCP is not to be subjected to a software upgrade. The iReports Designer Software is customized and optimized specifically for the use with the MCP.

Manual Layout

This document outlines and details the procedures regarding:

- Creating a customized report template using iReport Designer
- Importing templates
- Configuring Archived (Offline) Reports
- Configuring Current (Online) Reports
- Report Viewer

Document Conventions

The software-related procedures in this guide are based on using a computer running Windows® XP. Some steps and dialog boxes may vary slightly if you are using another version of Windows.

Safety words and definitions

Before attempting to install or use the device, review all safety indicators in this document to help prevent injury, equipment damage or downtime.

The following safety and equipment symbols are used in this document:

⚠DANGER **Indicates a hazardous situation which, if not avoided, will result in death or serious injury.**

⚠WARNING **Indicates a hazardous situation which, if not avoided, could result in death or serious injury.**

⚠CAUTION **Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.**

NOTICE **Indicates practices that are not related to personal injury.**

Product Support

If you need help with any aspect of your GE Grid Solutions MCP, you can:

- Access the GE Grid Solutions Web site
- Search the GE Technical Support library
- Contact Technical Support

GE Grid Solutions Web Site

The GE Grid Solutions Web site provides fast access to technical information, such as manuals, release notes and knowledge base topics.
Visit us on the Web at: http://www.gegridsolutions.com

GE Technical Support Library

This site serves as a document repository for post-sales requests. To *get* access to the GE Grid Solutions Technical Support Web site, go to: http://sc.ge.com/*SASTechSupport

Contact Technical Support

For help with any aspect of your GE Grid Solutions product, please contact our support team, 24/7, as follows:

Region	E-mail	Telephone
Global Contact Centre	ga.support@ge.com	+44 1785 250070
Central and East Asia andPacific	ga.supportCEAP@ge.com	+61 414 730 964
India	ga.supportIND@ge.com	+91 44 22648000
Middle East, North Africa andTurkey	ga.supportMENAT@ge.com	+971 42929467
Europe, Russia, CIS and Sub-Saharan Africa	ga.supportERCIS@ge.com	+34 94 4858854
North America	ga.supportNAM@ge.com	+1 877 605 6777
Latin America	ga.supportLAM@ge.com	+55 11 36187308

1

Creating Template Using iReport Designer

1.1 iReport Designer

The MCP has implemented some standard report templates. You can also design a customized report template and upload it to the MCP. You can:

- Access your data through XML, CSV.
- Export your reports as HTML, Excel or PDF.

1.2 Report Template Creation Procedure

» **To create a report template using iReport Designer:**

1. Download the **ireport-5.6.0_20201113.zip** file and all related sample templates, sample data xml/csv files from the GE Grid Solutions Technical Support Website.

   Login and navigate to the following folders:

   Substation Automation Products > G500 > Analog Reports Templates

   NOTICE Not all features of the standard iReport Designer are supported in the MCP-customized version of iReport Designer. Do not upgrade the iReport Designer as it may not be compatible with the MCP.

2. Extract to .zip file and choose the destination folder to place the extracting files (e.g.: C:\temp).
3. Navigate to the **..\bin** destination folder and run the **ireport.exe** file (e.g.: **C:\temp\ireport-5.6.0_20201113\ireport-5.6.0\bin\iReport.exe)**.
4. Create a customized:
   - Offline Report Template; see page 8.
   - Online Report Template; see page 39.

1.3 Create a Customized Offline Report Template

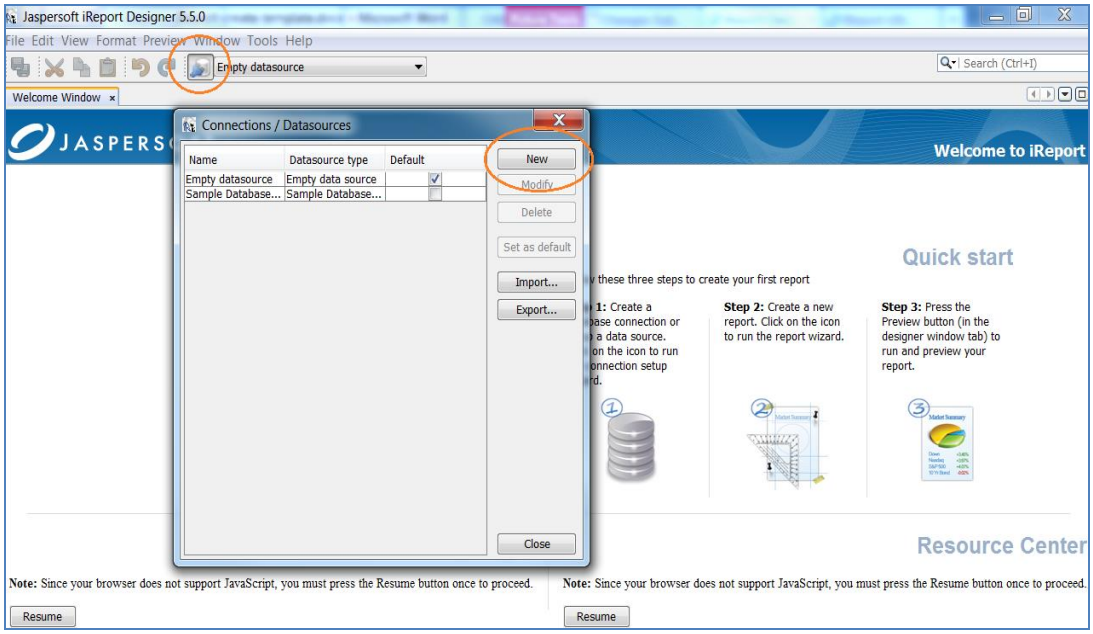
» **To create a customized offline report template:**

1. Create an XML DataSource.

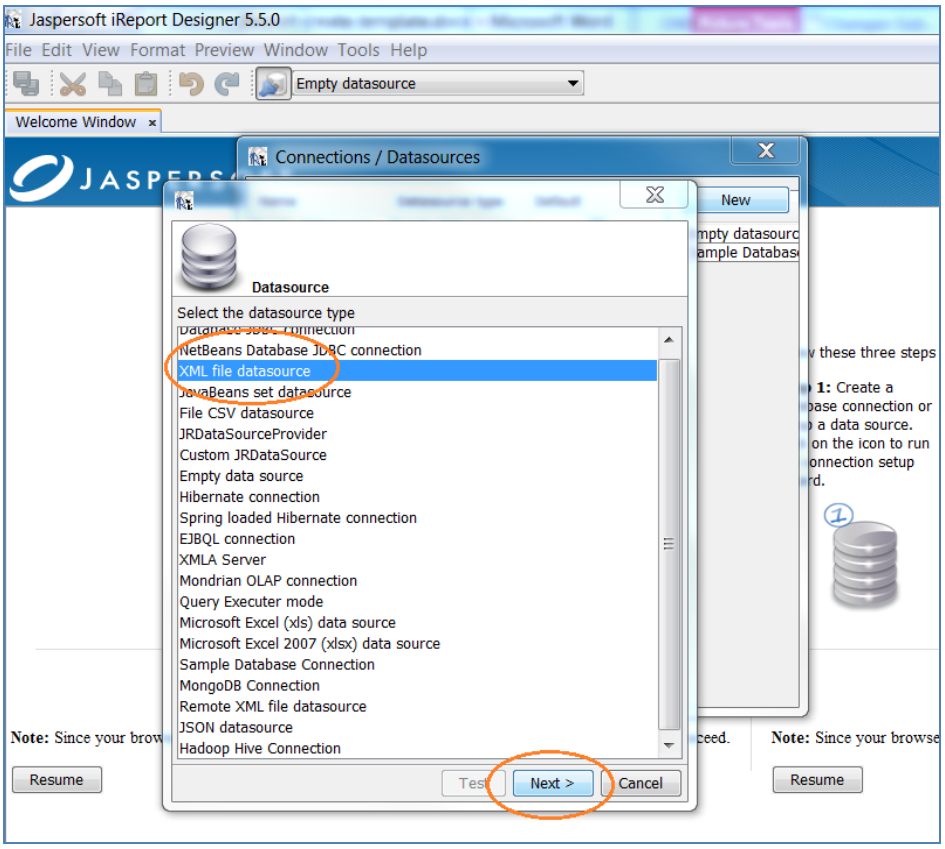
   This action is only required once. Skip this step if it has already been done. The Offline report uses the xml file as the datasource.

   a) Click the **Report Data Sources** button.
   Result: The Connections/Datasources window appears.

   b) Click the **New** button.



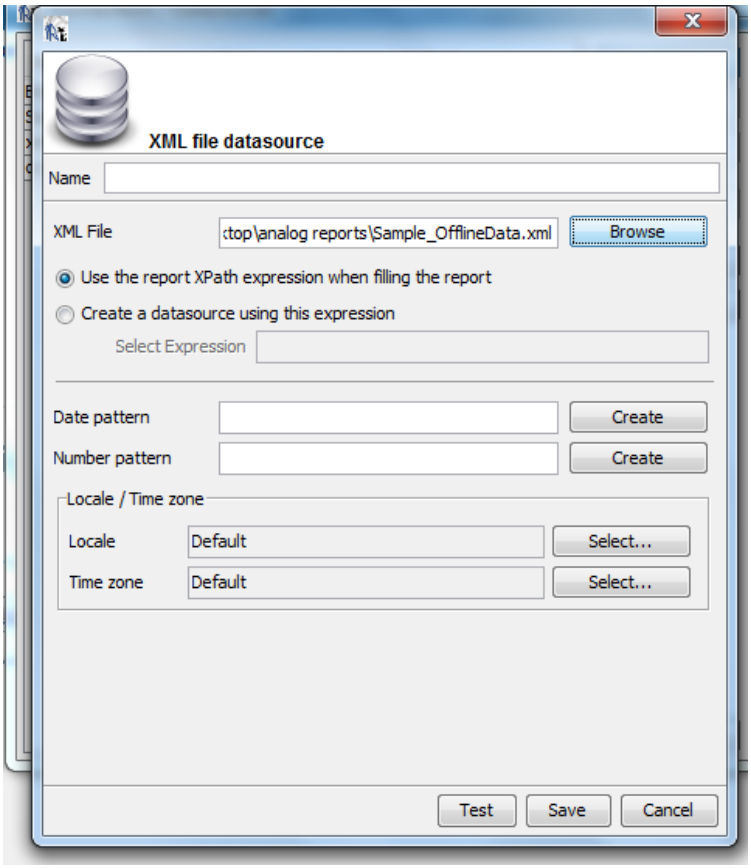
c) Select the database type: **xml file datasource** and click **Next**.
Result: You will be able to preview the file datasource.



d) Type the desired name in the **Name** field (for example, New_Xml_DS).

e) Select the **Use the report XPath expression.**

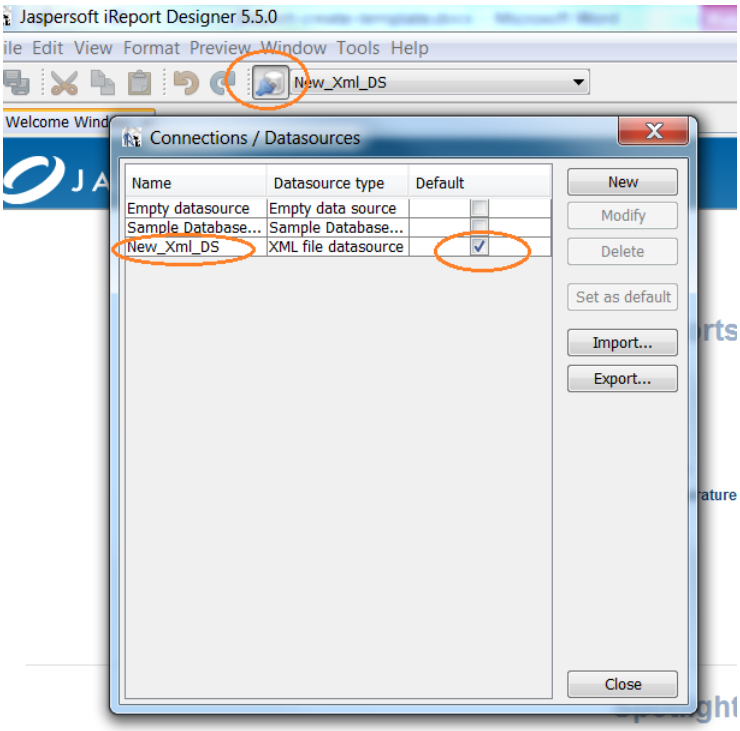
f) Click on **Browse** to **Choose Sample_OfflineData.xml** from the location in local PC**.**



Note: The sample file "Sample_OfflineData.xml" can be found on the GE Grid Solutions Technical Support Website.

g) Click **Test** to check if the correct file is chosen and click **Save**.

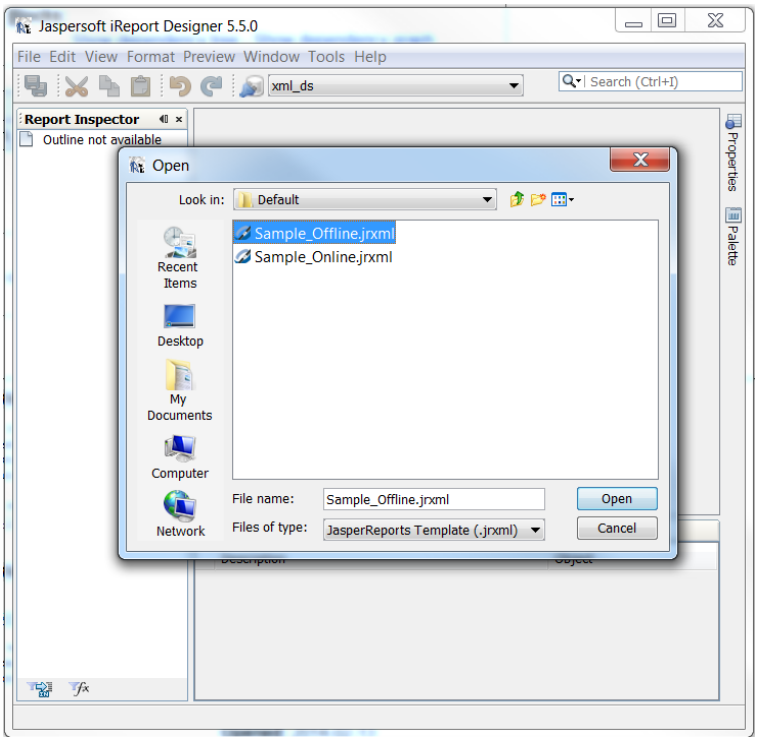
h) Set the default DataSource to **New_Xml_DS** and click **Close**.



2. Create offline template.

a) Click on **File,** select **Open,** navigate to the sample template provided on the GE Grid Solutions Technical Support Website.

Or select **New** to start a new Template (Additional steps required).



Note: It is strongly recommended that using the sample template to create your customized offline template. The sample template 'Sample_Offline.jrxml' is provided on the GE Grid Solutions Technical Support Website.

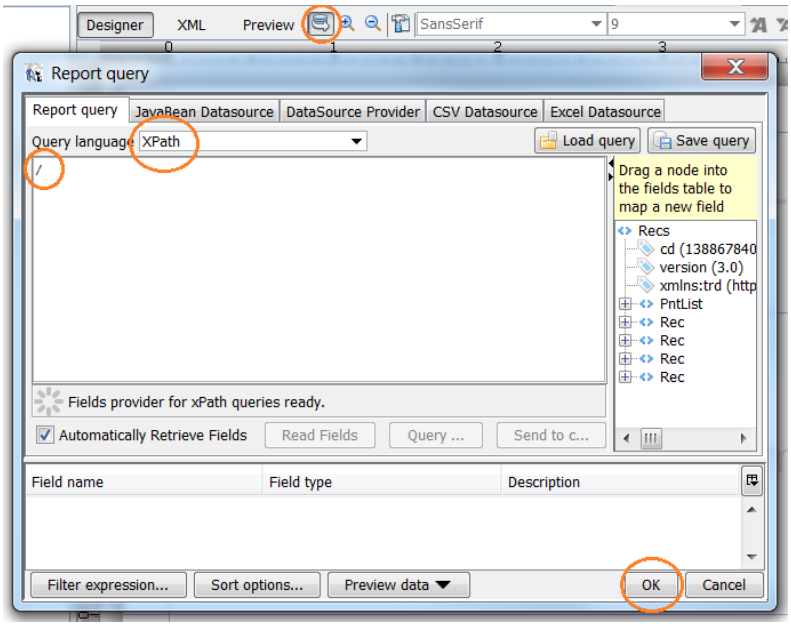
If you choose to create a new template without using the sample template, additional steps are required as below.

i) Click the **Report Query** button, located on the right side of **Preview** button.

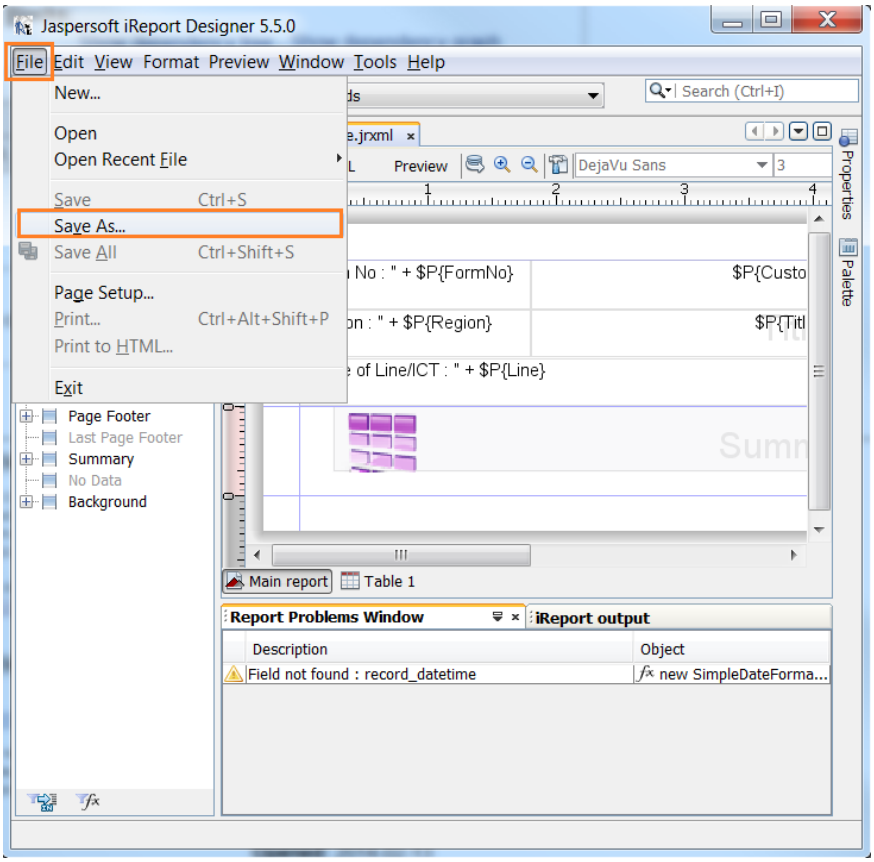
ii) Select **XPath** as query language on the first tab.

iii) Type **/** in the xpath expression textfield.

iv) Click **OK**.



b) Rename the Template by Clicking **File** and select **Save_As** sample template as a new file.



The below report is created in this procedure as a demonstration. You can modify the sample report according to your report requirements.

CORPORATION

Form No:
Region:

Substation:

Daily Log Sheet for EHV Lines

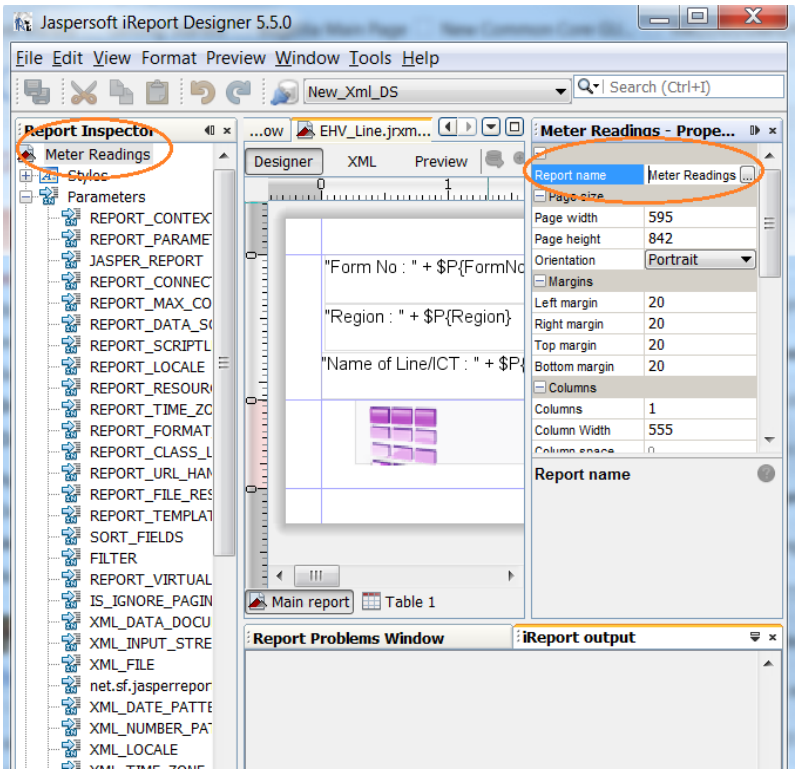
Date		Month		Year	

Time	**Line……..****				**Weather Condition ***	**…….kV *** Bus No……**		**Remarks**
Hrs	**MW**	**MVAR**	**Line Reactor MVAR**	**FSC/TCSC IN/OUT of Service**		**kV**	**Hz**	
0100								
:								
:								
1200								
:								
:								
2400								

* Weather Conditions: Dry/ Cloudy/ Stormy/ Rainy/ Windy – To be recorded once in a shift.
** This format block is to be repeated for each line on the same sheet.
*** This format block is to be repeated for each Bus on the same sheet.
Note: 1. Column spacing to be adjusted as per requirement. Line Reactor & FSC/TCSC IN/OUT of service column to be deleted wherever not applicable.

Shift	**Tech./ JE**	**Shift I/C**
C		
A		
B		
C		

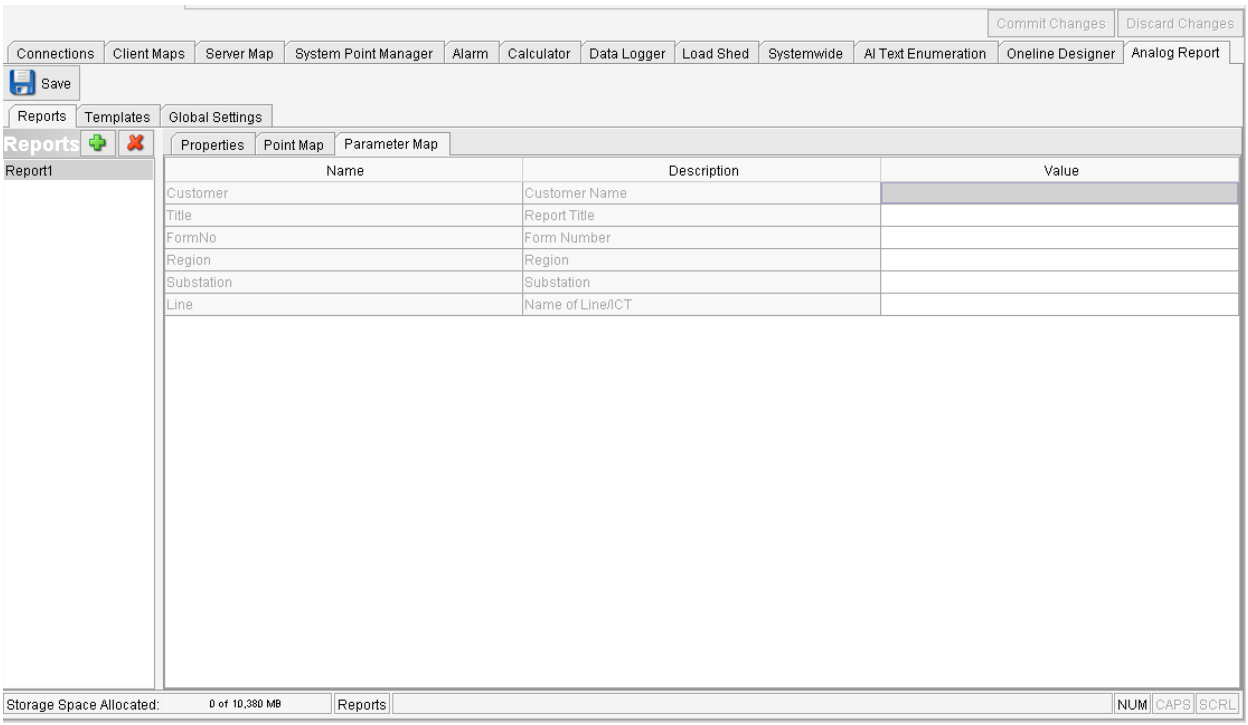
3. Change the **Report Name** as required.



4. Create the report parameters.

   Report parameters defined in the template are used by the MCP Configuration Tool. The below image shows how parameters would appear after creation and importing the template.

   You can specify values for these parameters using the Analog Report Configuration Tool.



Predefined Parameters (Mandatory steps for new templates)

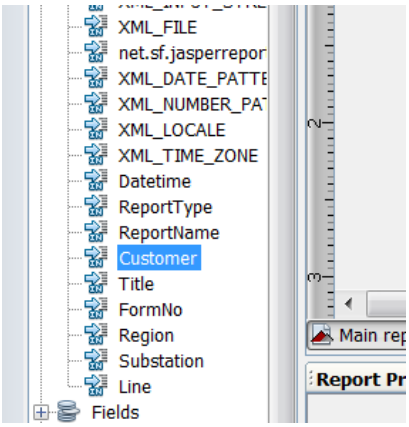
There are three predefined parameters for which values are always transferred.

- Datetime(java.util.Date) – This parameter identifies the starting datetime of current report file logged.
- ReportType (java.lang.String) – This parameter specifies the Report type that you specified in Analog Report Configuration Tool. Possible values are: SHIFT, DAILY, WEEKLY and MONTHLY.
- ReportName(java.lang.String) – This parameter specifies the Report Report name you specified in Analog Report Configuration Tool.

Note: For predefined parameters the **Use as prompt** property must be unchecked. If a new template is not created based upon a sample template, creating predefined parameters is mandatory.

Parameters in Sample Template

The sample template has six parameters in addition to the predefined parameters; for example: Customer, Title, etc.

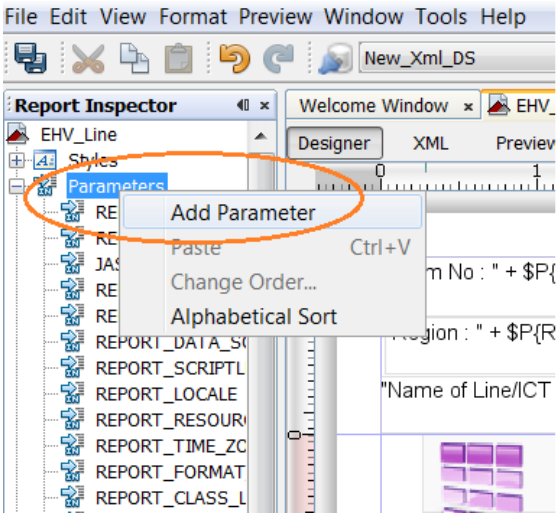


» **To add a new Parameter**:

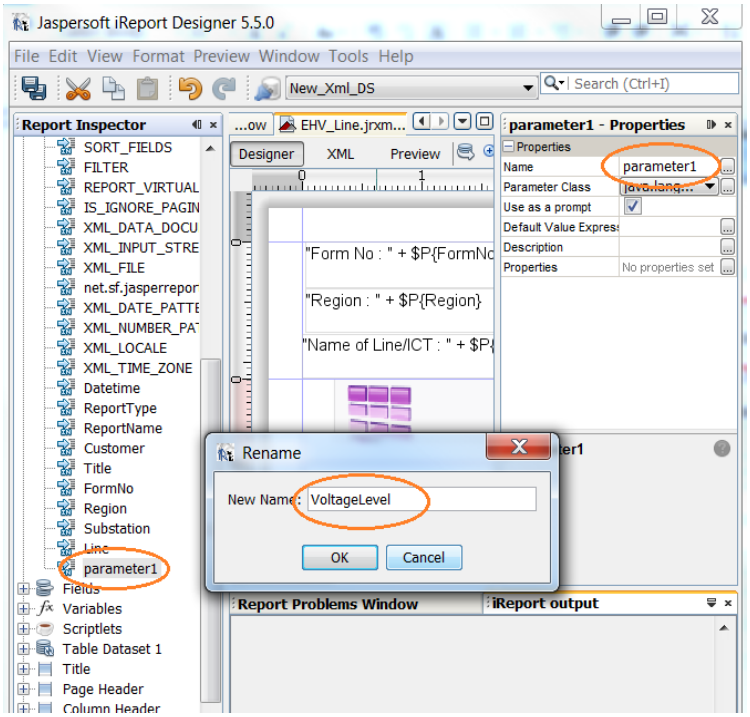
The sample template does not have two other parameters which are required by the report (ignore if already present):

- VoltageLevel (java.lang.String) – Voltage Level is presented in the table column.
- BusNo (java.lang.String) – Bus.No is presented in the table column.

Note: All parameters must be of type: java.lang.String, except the three predefined parameters. You specify the parameter value in the MCP. Text can be used to present values in various types.



5. Use the **Add Parameter** command to add and rename the following paramters:
   - VoltageLevel
   - BusNo



6. Configure the parameters which are to appear in the MCP Analog Report Configuration Tool.

   - The **Use as a prompt** checkbox is used to hide/show the parameters in MCP Analog Report Configuration Tool.

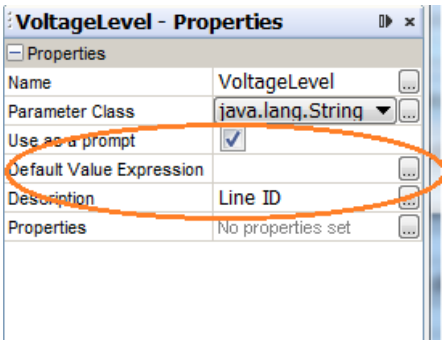
     If this checkbox is selected, the current parameter appears in MCP Analog Report Configuration Tool.

     If this checkbox is not selected, the current parameter does not appear in MCP Analog Report Configuration Tool.

     The predefined parameters are unchecked.

   - The text specified in the **Default Value Expression** field appears by default in the Multilin™ MCP Substation Gateway – Analog Reports. You can override the default value in the MCP.

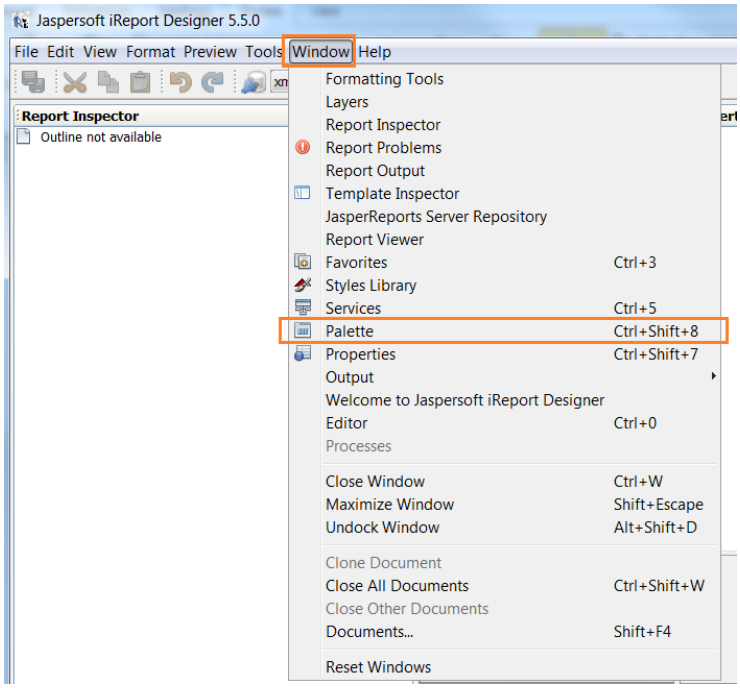
   - The text specified in the **Description** field appears in the parameter map of the Multilin™ MCP Substation Gateway – Analog Reports. Provide any details in the description which will help the user understand the function of the parameter.



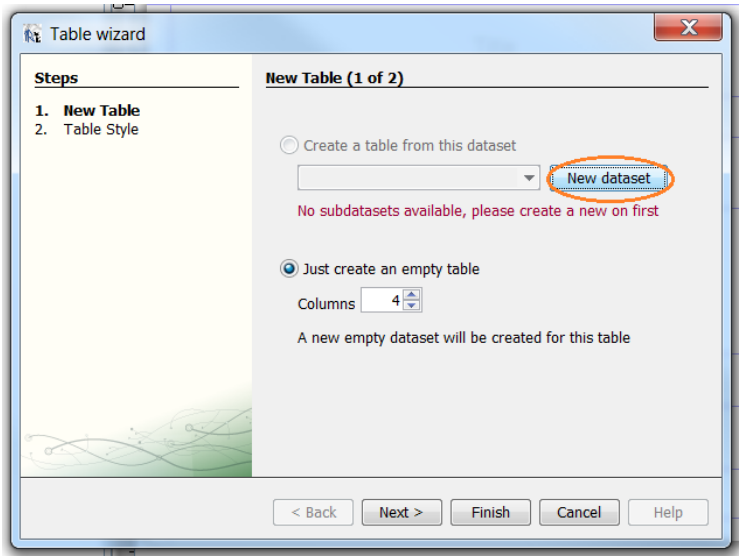
7. Create a table and set the Table DataSource.

   Skip this step if using the sample template.

   a) Drag-and-drop a table from the palette into Designer.
   Result: A Table wizard appears.



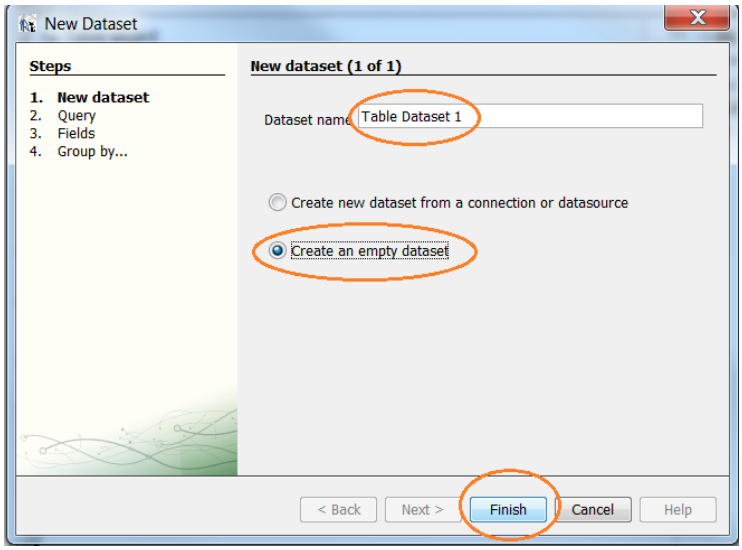
   b) Click **New dataset**.
   Result: The New Dataset wizard appears.



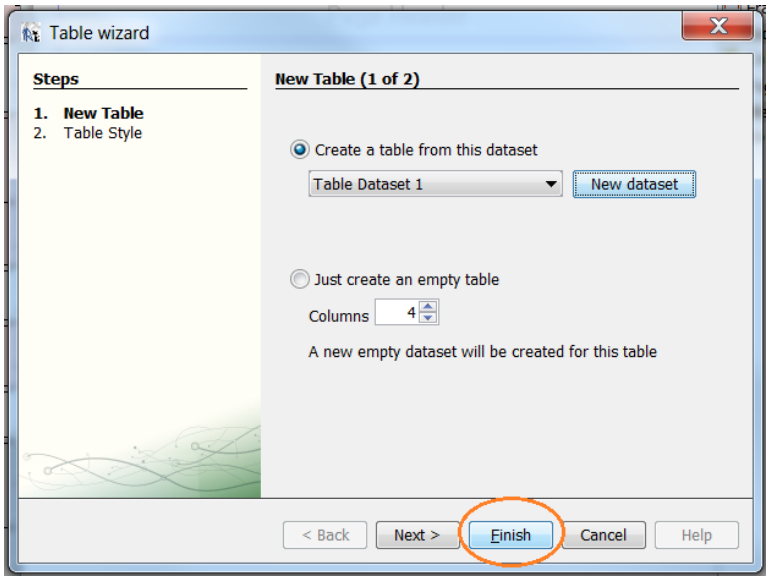
c) Type in a **Dataset name**.

d) Select the **Create an empty dataset** option.

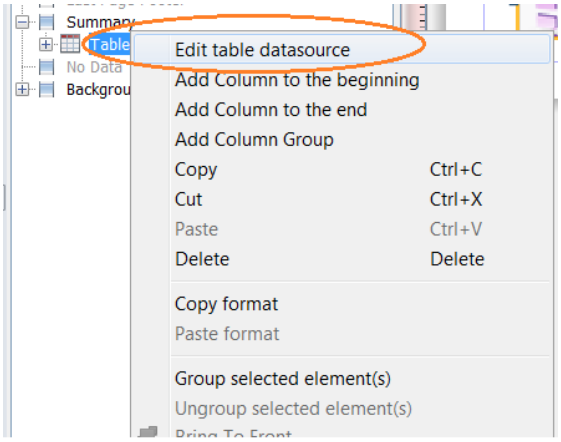
e) Click **Finish**.
Result: The New Dataset wizard closes.



f) Click **Finish**.
Result: The Table wizard closes.



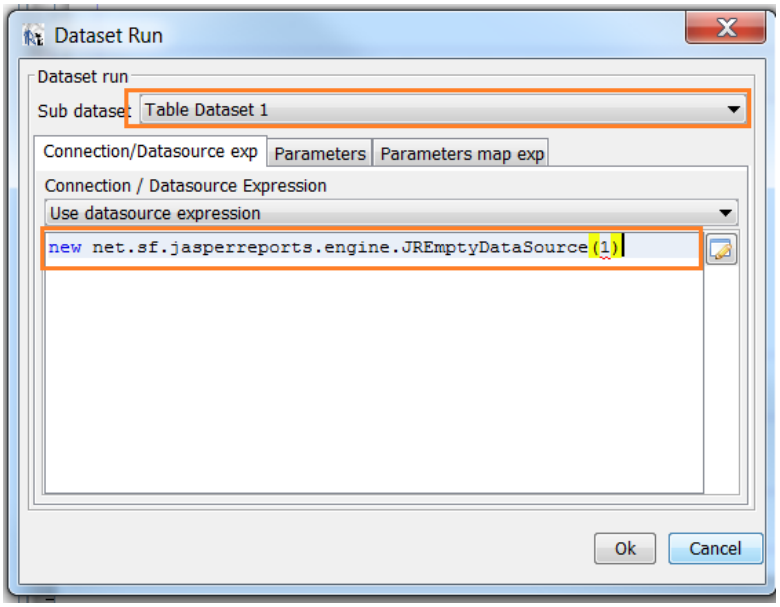
g) Right-click the Table name and select **Edit table datasource**.
Result: The Dataset Run window appears.

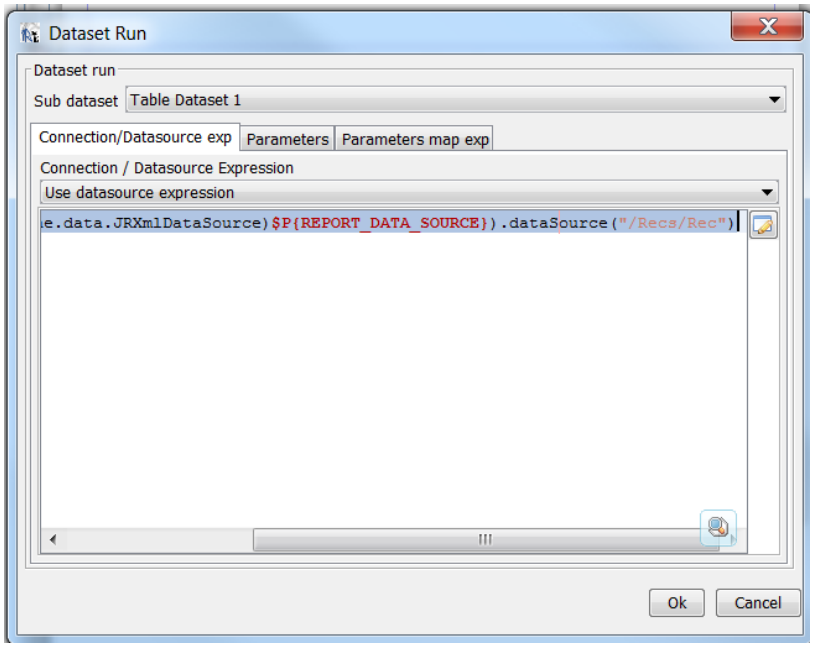


h) Copy and paste the query:

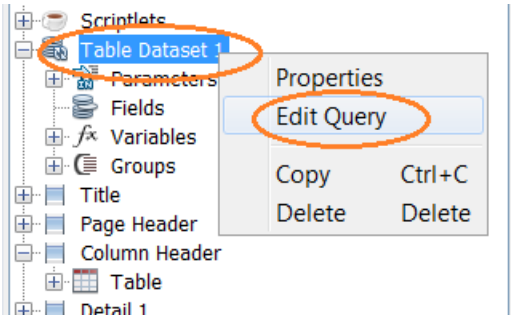
```
((net.sf.jasperreports.engine.data.JRXmlDataSource)$P{REPORT_DATA_SOURCE}).dataSource("/Recs/Rec")
```

to the Connection/Datasource Expression – **Use datasource expression**.

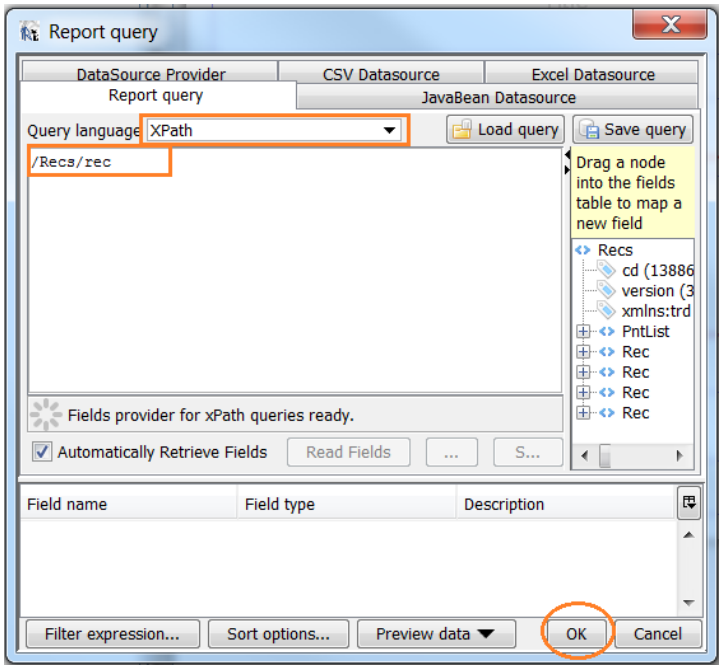




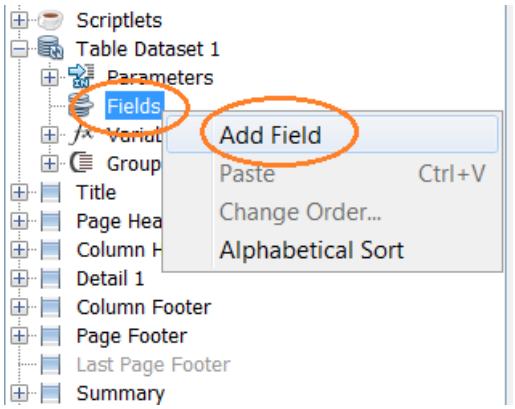
i) Right-click on **Table Dataset 1** and select **Edit Query**.



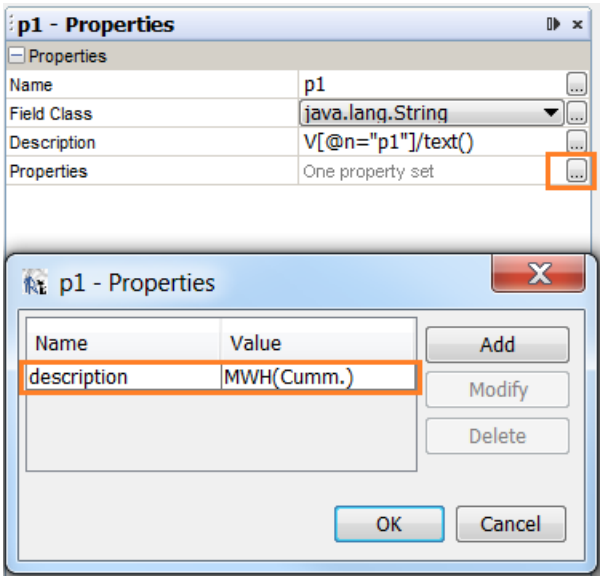
j) Change the Report query to **XPath**, with expression is **/Recs/rec**.



k) Right-click **Fields** and select **Add Field**.



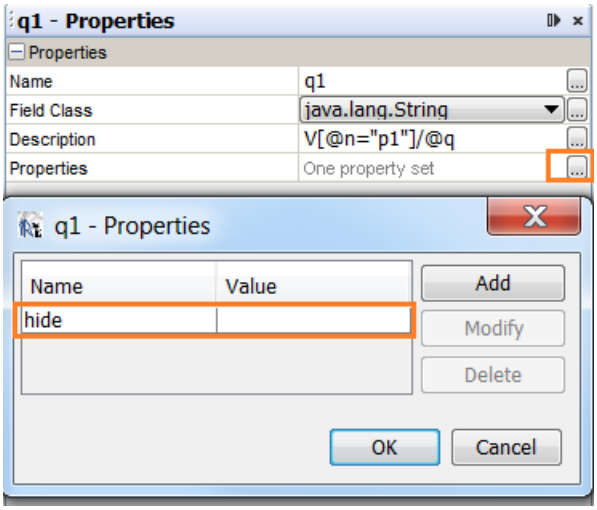
l) Add field **p1**: **AI Point**



Give XPath expression 'V[@n="p1"]/text()' to p1 shown upon.

An additional **description property** is required, which will appear on HMI Analog Report Configuration Tool. User should know which AI Point to be mapped accordingly.

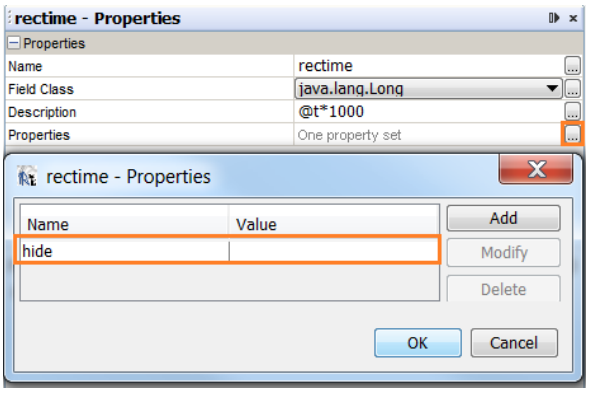
m) Add field **q1: AI Point Quality**.



An additional **hide** property is required, which indicates this is an invisible field in HMI Analog Report Configuration Tool. This field is used to show AI point's quality at runtime.

if multiple analog points are required in the report, repeat sub-steps k) to m) and to create fields for the other analog points.

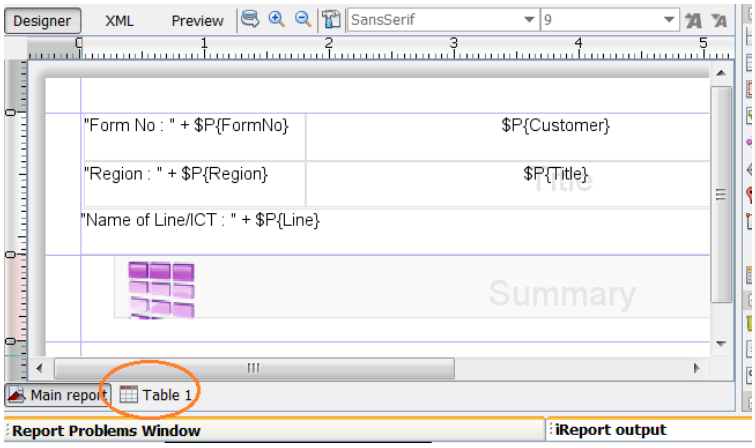
n) Add the **rectime** field: **recording date/time for each logging record**.



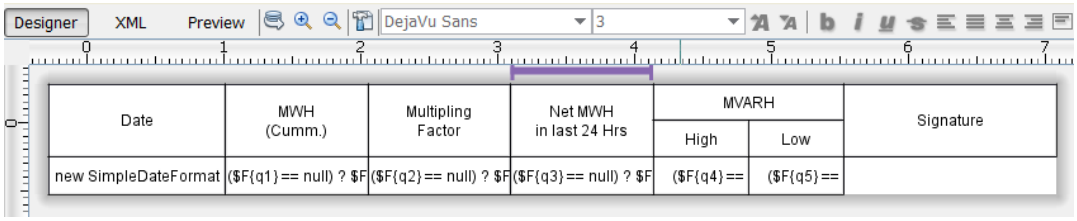
Note: The **rectime** field is the Epoch time in millinsecond. It is not configurable in Analog Report Configuration Tool and should be hidden by adding 'hide' property.

8. Add/Remove Table Column.
Result: if you are using the provided sample template, a table name appears in the Designer summary pane.

a) Click **Table1**.

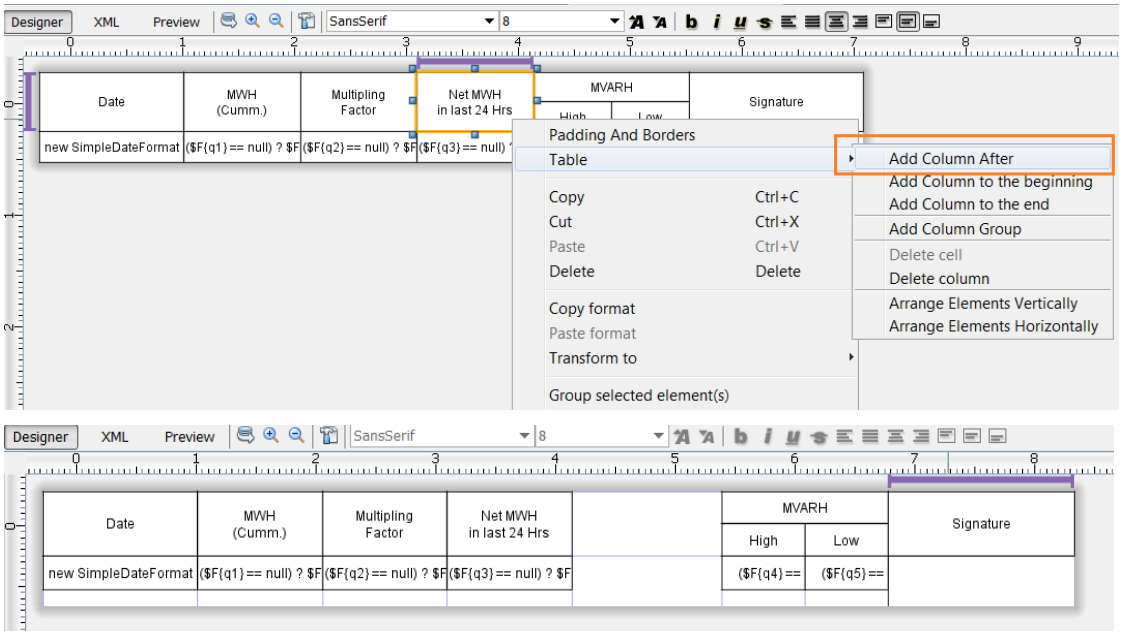


Result: A sample template table appears with 7 columns.

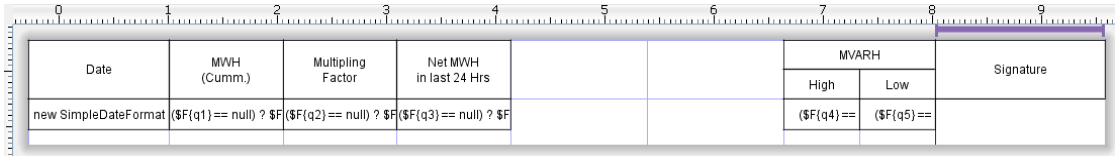


b) Add two additional columns.

Right-click on the fourth column and select **Table** > **Add Column After**.

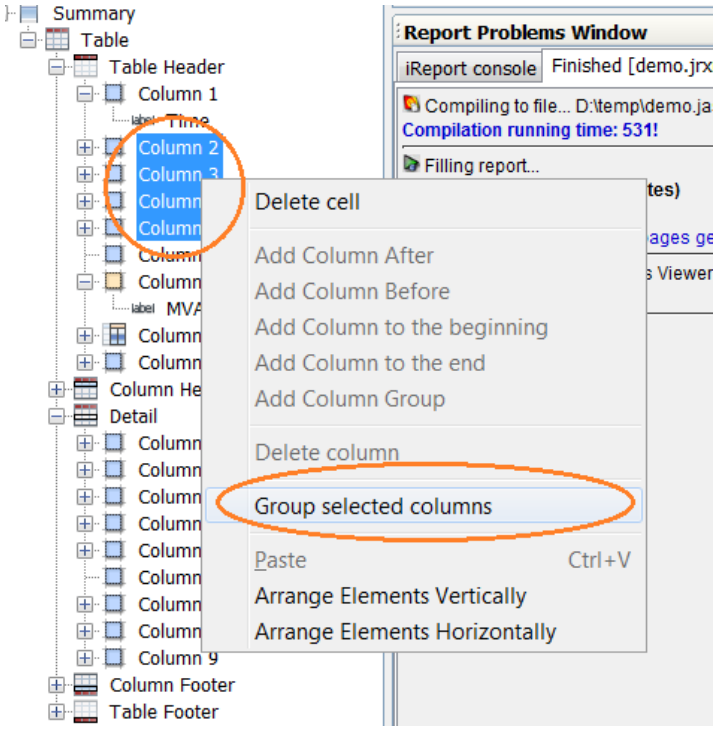


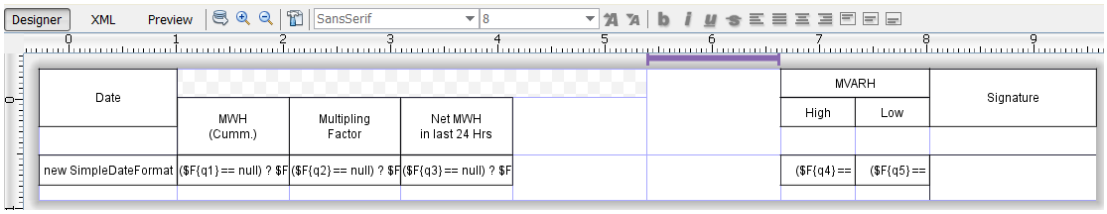
c) Repeat the previous step to add another table column.



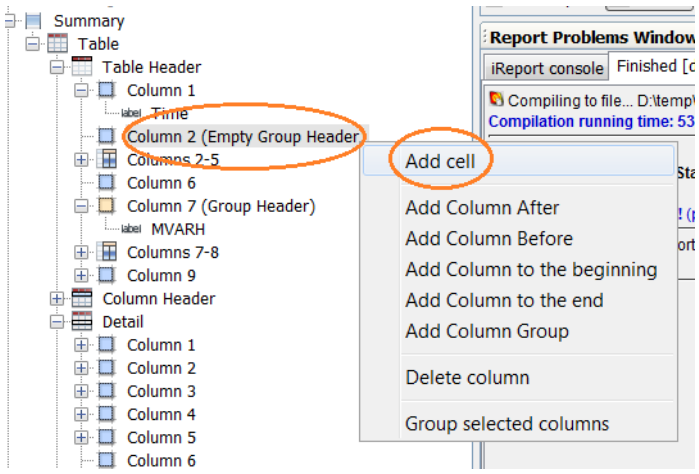
d) Group the table/column header.

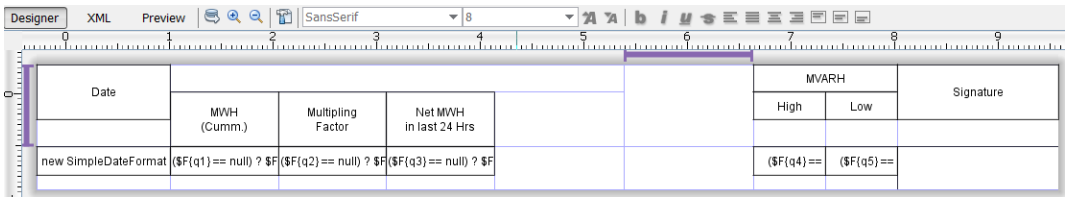
Press and hold the Shift key and select column2 to 5, then right-click and select **Group Selected Columns**.



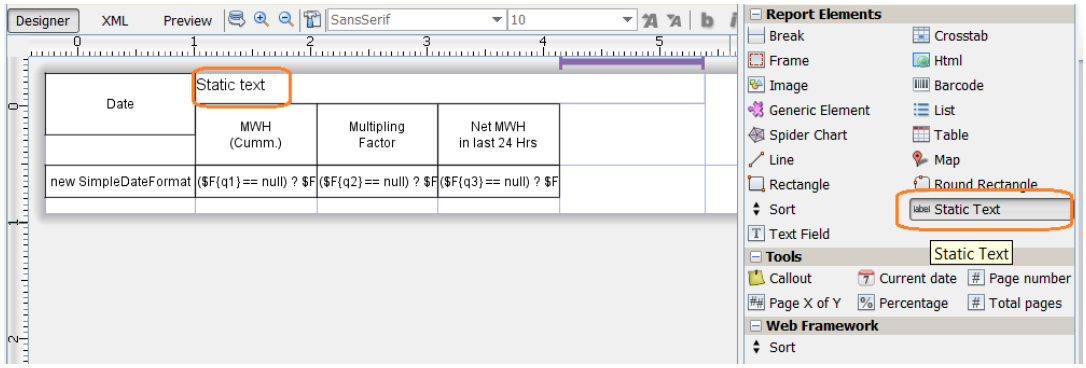


e) Add a cell to the new grouped column.

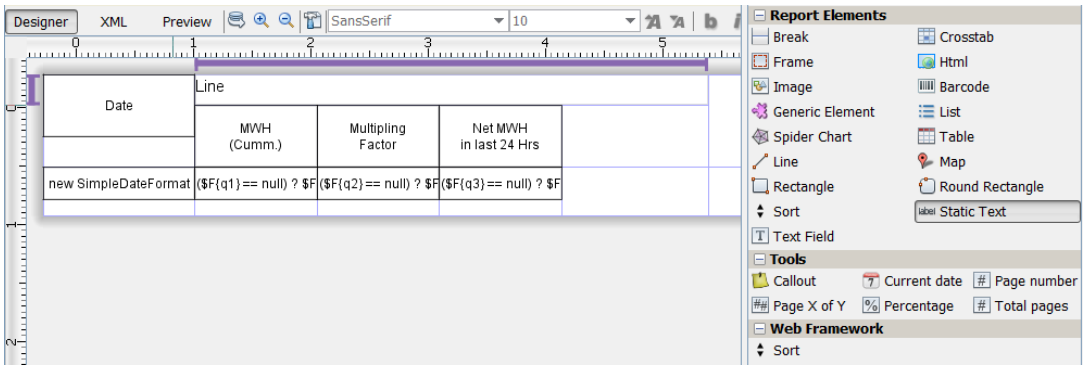




f) Drag-and-drop the Static Text to new grouped column.



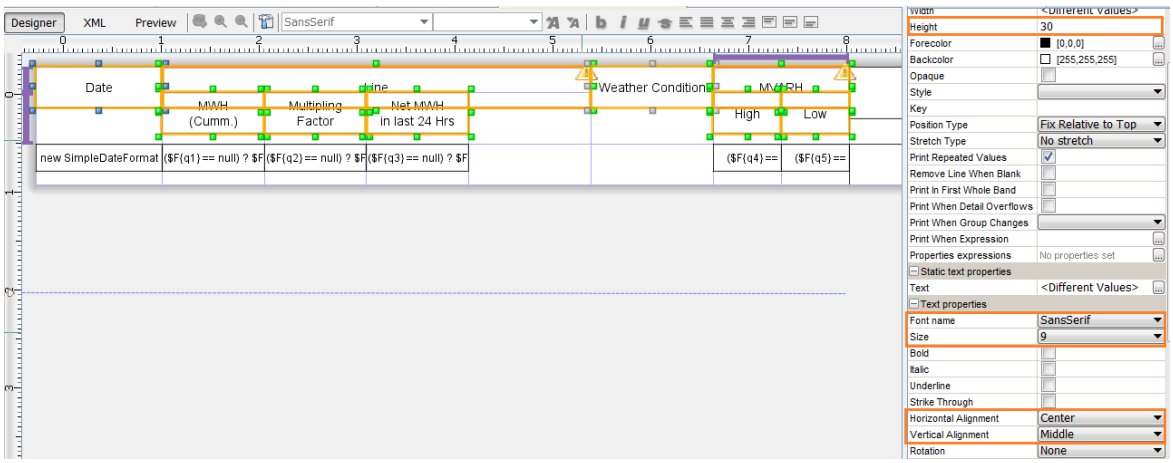
g) Change the static text in table header.



h) Add more static text for **Weather Condition** in the same way.

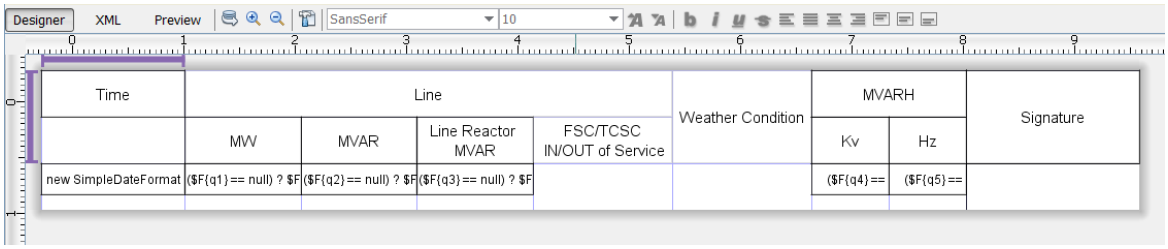
i) Add a column header to the new columns and adjust the column width and height.

You can change the common properties for multiple objects by selecting multiple text fields (by pressing and holding the Ctrl Key).



j) Adjust the height of the **Line** and **MVARH** static text cells. This static text can overflow to its cell height.

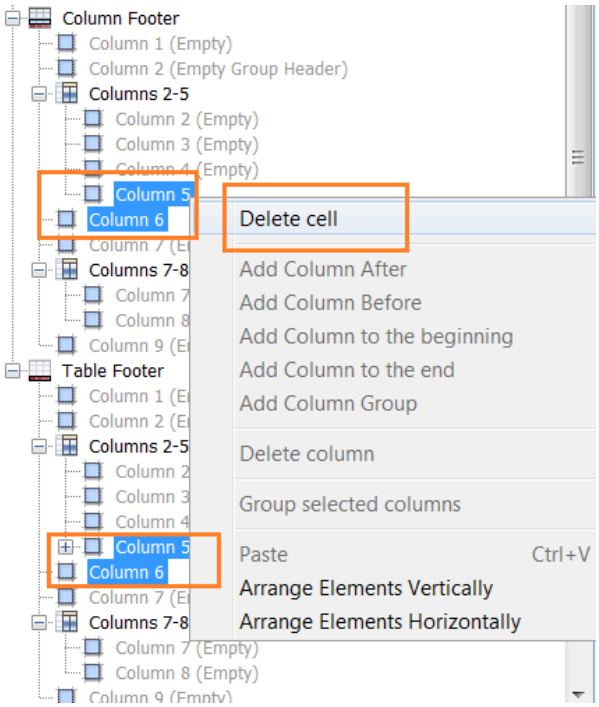
k) Add a column header for each new column, adjust the column width and height, and change static texts to fit the new report.



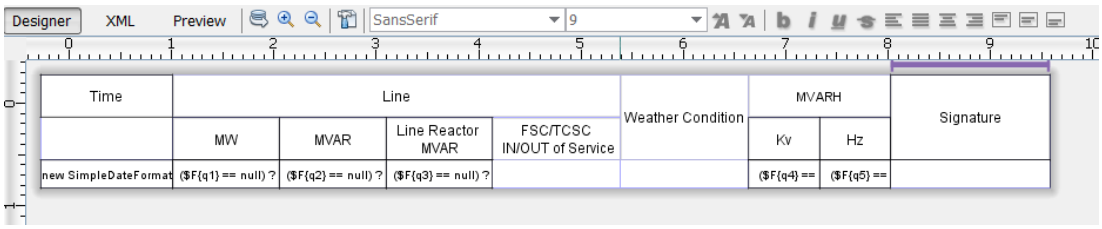
Note: In some cases, column height cannot be decreated after added a new column. To fix this, usually deleting cells from columns in the Table/Column Header/footer is required. This is because a cell is invisible in designer, but it takes space in the table. The height of a red column cannot be decreased since the column footer and table footer have columns with cells.

Result: Column 5 and column 6 have cells in column footer and table footer.

l) Delete these footer cells from columns 5 and 6.



m) Decrease the column height.



In this sample, the report has a column header and does not have a table header.

If you need both a table header and a column header, refer to the “ireport-ultimate-guide.pdf” , Chapter “13.2.2 Table Structure”.

Notes:

- The Table Header is only printed one time; that is, at the beginning of the table. The Table Footer is also only printed one time; that is, at the end of the table.
- The Column Header is only printed one time; that is, at the beginning of each page for the table. The Column Footer is only printed one time; that is, at the end of each page of the table.
  The Table Header and Column Header are typically used to display static text.

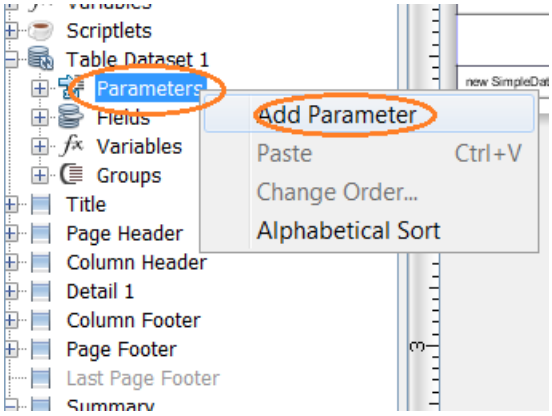
Remove all cells from columns which are not required; otherwise these columns are printed, with unwanted blank spaces. This is also applicable to Table Header, Column Header, Detail, Column Footer and Table Footer.

If your table does not contain a Column Footer, do not put text into any Column Footer cell.

9. Configure the parameter to appear in the table.

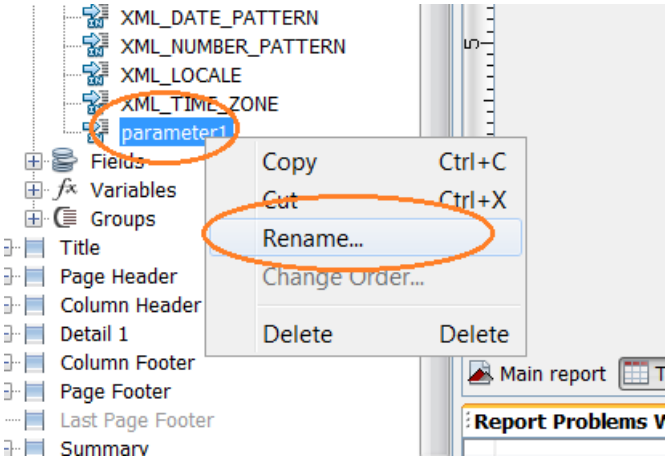
   Skip this step if no parameter is required to be displayed on table. In this demo template, parameters ‘VoltageLevel’ and ‘BusNo’ are required in the table header.

   a) Rightt-click **Parameters** and select **Add Parameter** to add new parameters to the Table Dataset and pass parameter values.



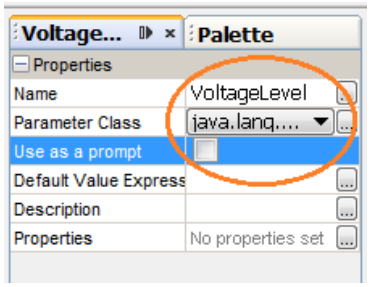
   b) Right-click the paramter name and select **Rename**.

For example, the parameter name **VoltageLevel**, can be renamed for the report. The parameter name can be any legal name. Do not confuse parameter names between the Table Dataset and Report.

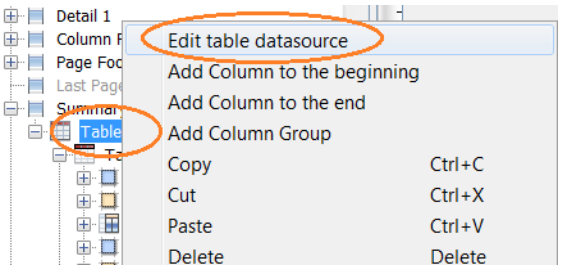


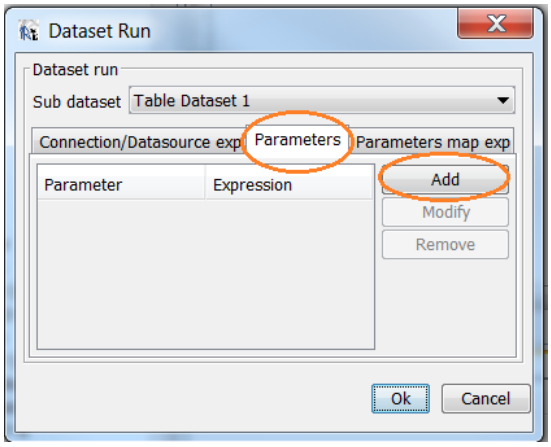
c) Transfer the value of the VoltageLevel parameter into the Report to VoltageLevel parameter in the Table Dataset 1.

d) Set the parameter properties:
- Set Parameter Class to **java.lang.String**.
- Do Not select the checkbox: **Use as a prompt**.



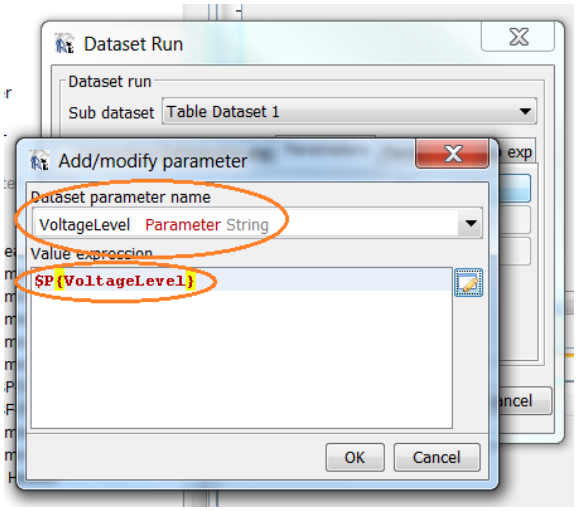
e) Right-click on the table and select **Edit table datasource**.





f) Select the **VoltageLevel** parameter from the Datatset parameter name list.

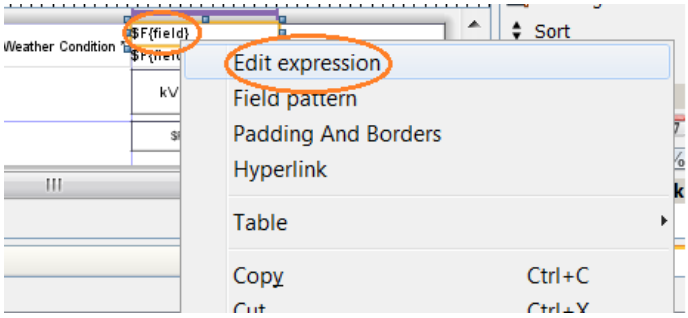
g) Type or select the Value expression: the **$P{**VoltageLevel**}**.

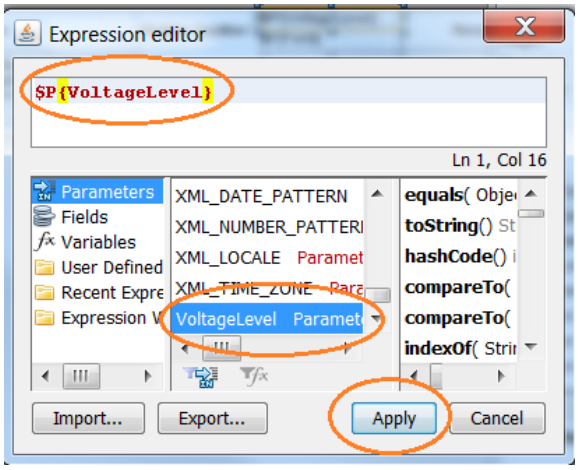


h) Drag-and-drop the **Text Field** element to the table header for Voltage Level and Bus No.

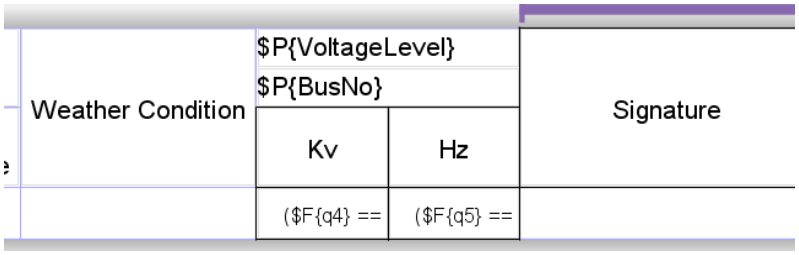
i) Delete the static **MVARH** text.

j) Right-click on the text field and select **Edit expression**.

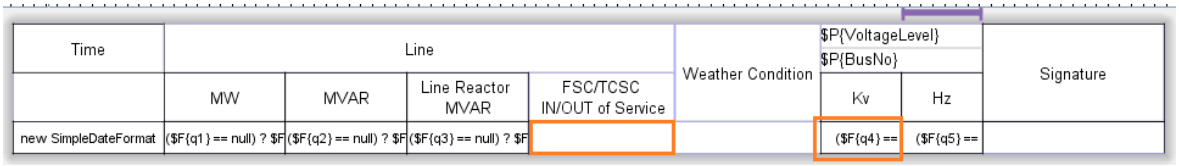




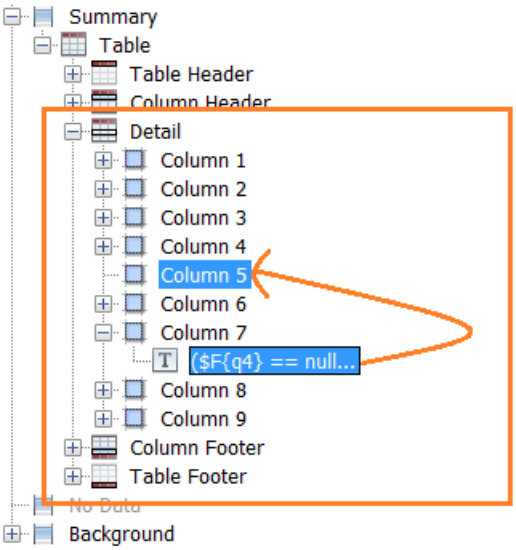
k) Repeat the previous step to create the **BusNo** parameter.



10. Add and move the following fields:
    - Field p4 is to be moved to column 5
    - Field p5 is to be moved to column 6.
    - Two new fields are to be added to the columns where p5 and p6 are located, before moving.



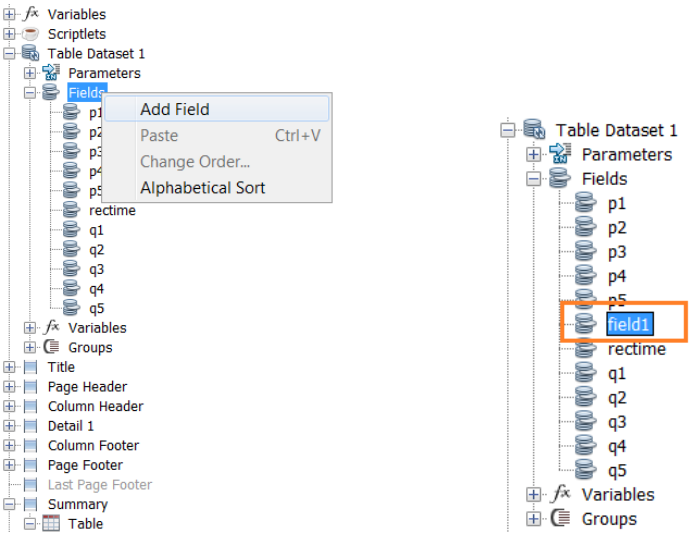
a) Drag-and-drop field p4 to Column 5. Repeat for field p5.



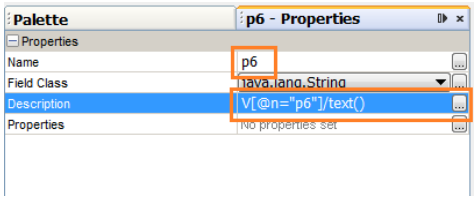
b) Add new fields: **p6**, **q6**, **p7** and **q7**.

c) Add field **p6** for the AI Point value.

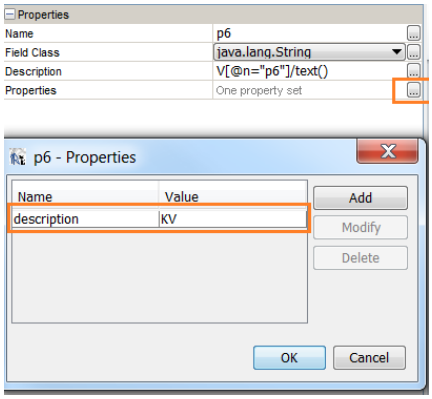
d) Rename the field to specify **XPath V[@n="p6"]/text()** and add properties.



The **Description** property is used to store **XPath V[@n="p6"]/text()**.

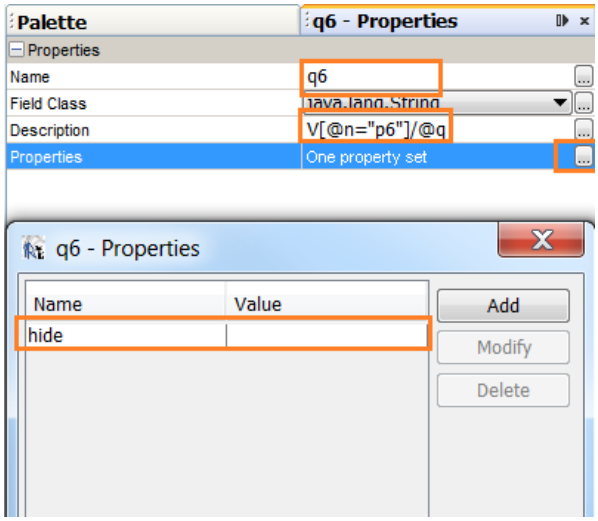


e) Add a **Description** property to be shown on the HMI Analog Report Configuration tool, It is helpful for the HMI user to understand which AI point should be mapped to this field.



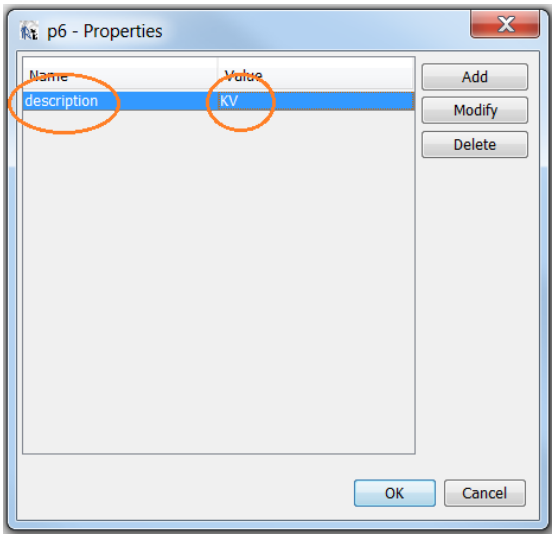
f) Add properties for the **q6** field for the:

- Quality of the AI Point value
- Rename field
- Specify **XPath V[@n="p6"]/@q**
- Add the **hide** property

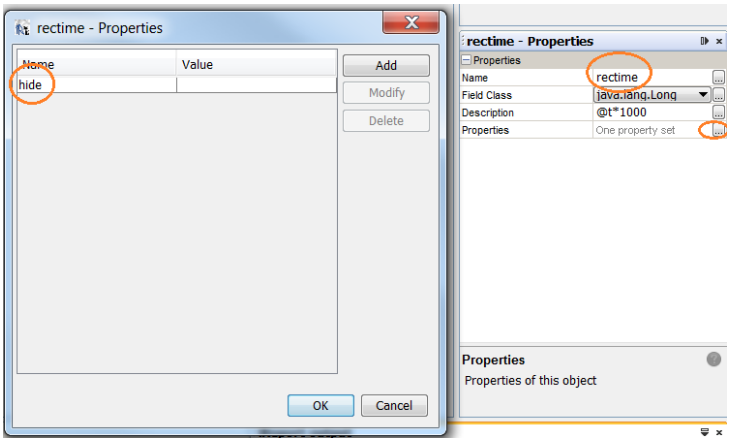


Notes:

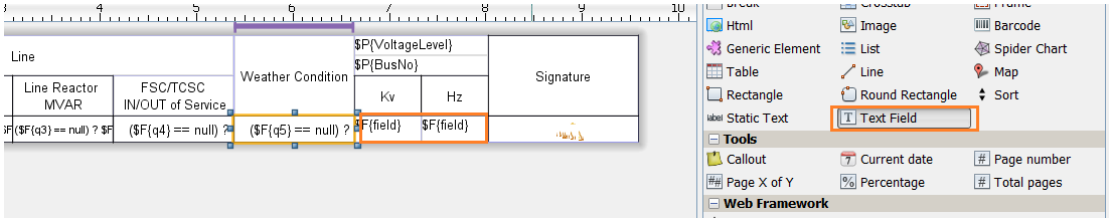
- The field name length cannot exceed 8 characters. The names p[n] and q[n] are recommended, where n is an incremental number, The sample xml file uses field name p[n].
- There are two predefined properties:
  - If specified with a predefined **description** property, this parameter value appears in the MCP Configuration Tool. This description helps the MCP HMI user understand which AI Point should be mapped.



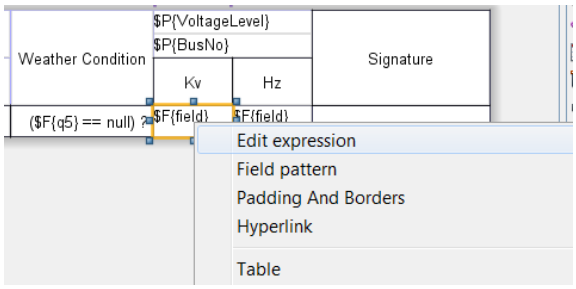
  - The predefined **hide** property is not required to the AI point field. The value in a hidden field does not appear in the MCP Analog Report Configuration Tool. It is very important to **record time** field and **quality** field. For sample : the **rectime** field is the Epoch time in millinseconds, it is not configrable and should be hidden in the MCP Analog Report Configuration Tool.



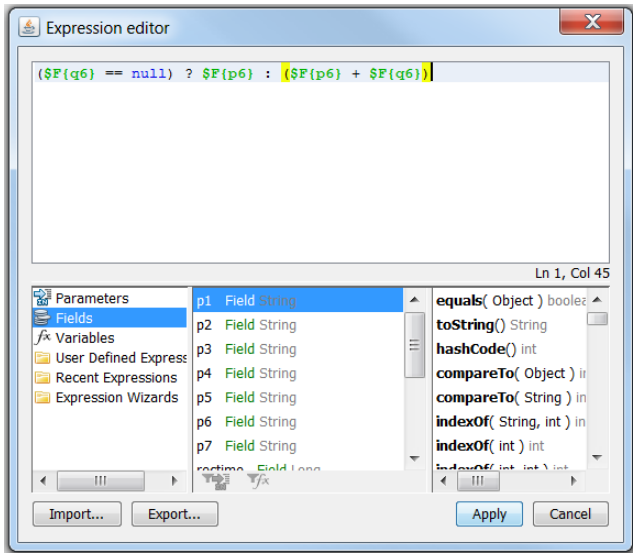
g) Add a field; drag-and-drop a **Text Field** to the table.



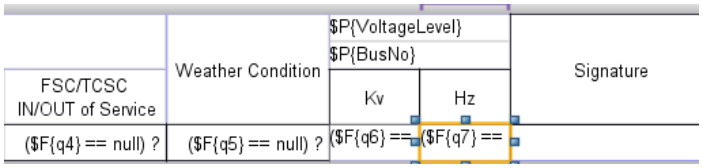
h) Right-click **$F{field}** and select **Edit expression**.



The following expression shows a point value with a quality letter.

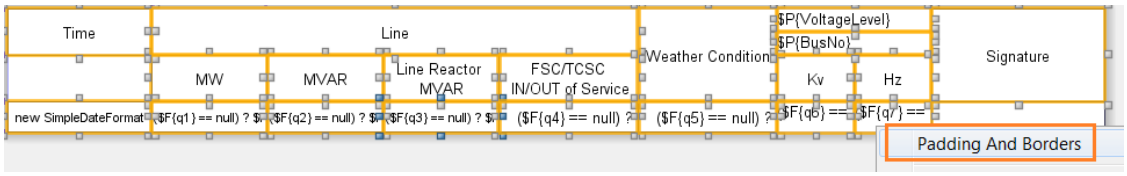


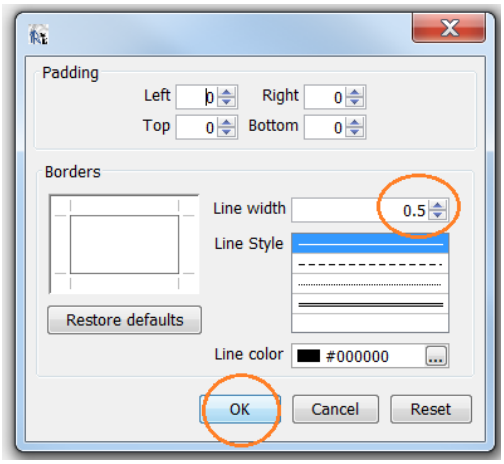
i) Repeat the previous step to add the p7 field.



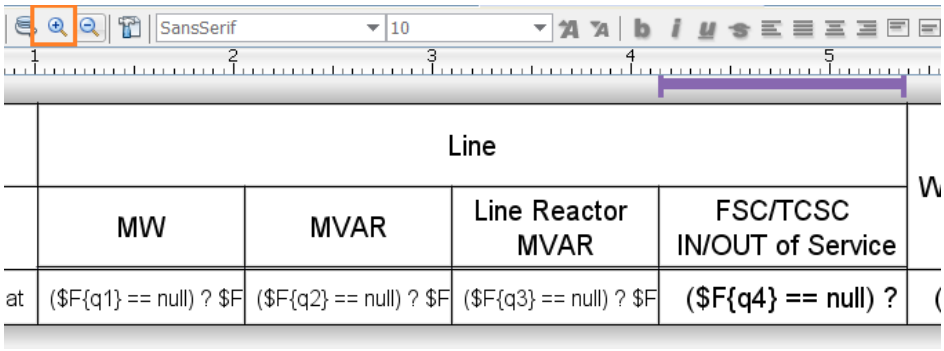
11. Finalize the table.

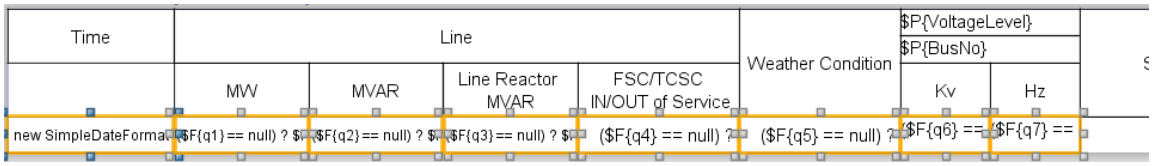
a) Add a table border. Select all text boxes, right-click and select **Padding And Borders**.



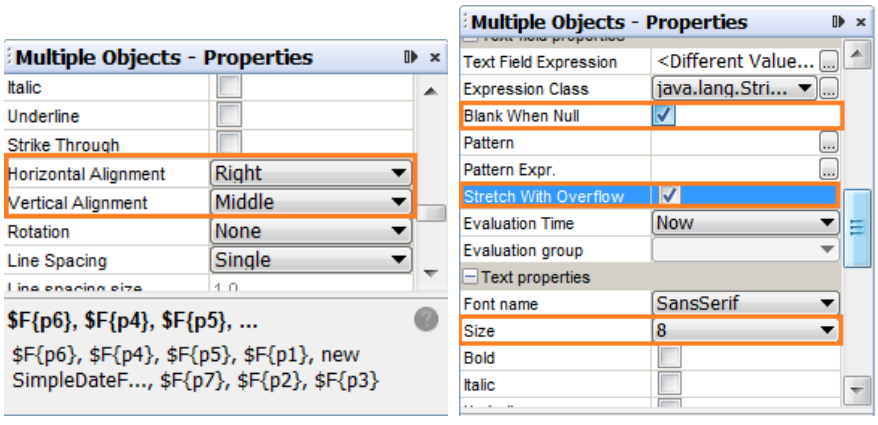


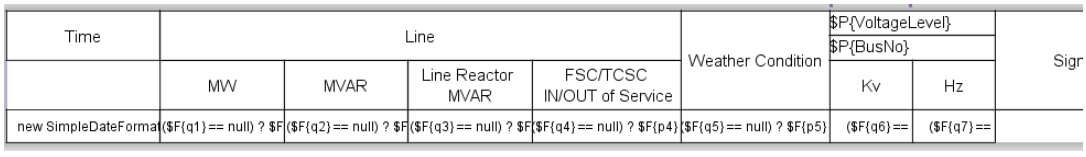
b) Adjust the width and height for column and text field: Zoom-In/Zoom Out.





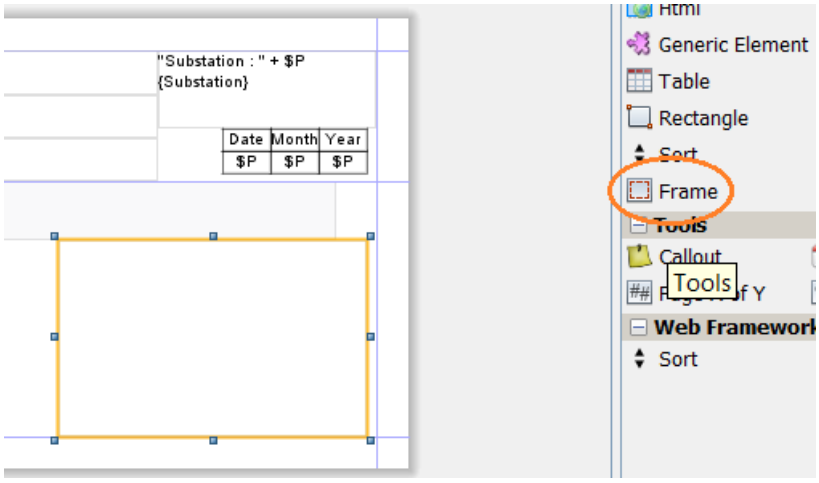
c) Select the **Blank When Null** and **Stretch With Overflow** option, and set the alignment and font size.



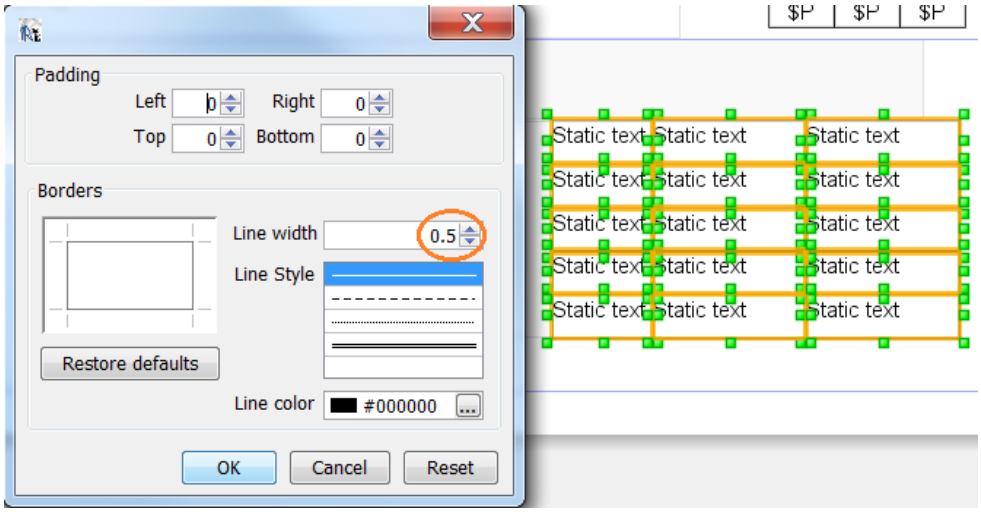


12. Add the report footer.

a) Drag-and-drop the **Frame** to the Designer.



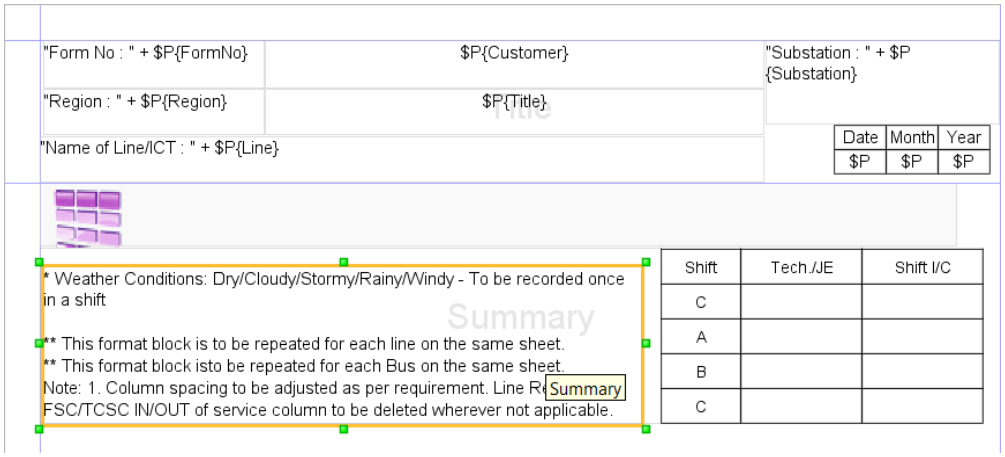
b) Drag-and-drop **Static texts** to the Frame, and set the border parameters.



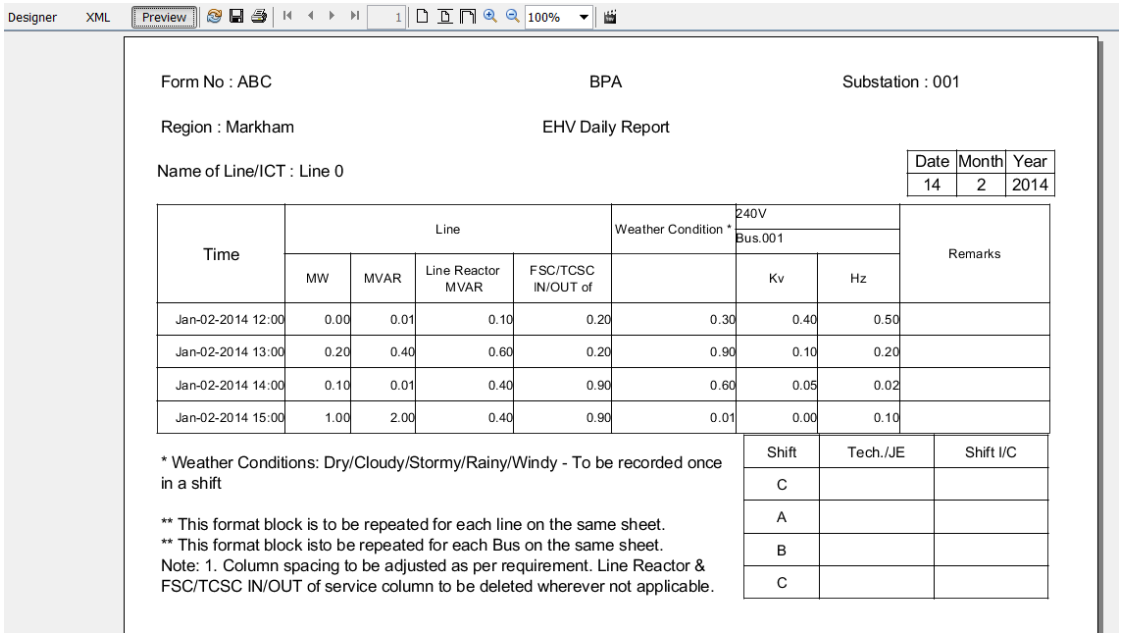
c) Change the text and set the text properties (font size, alignment etc).

Shift	Tech./JE	Shift I/C
C		
A		
B		
C		

d) Add static text on the bottom-left.



e) Preview the report.



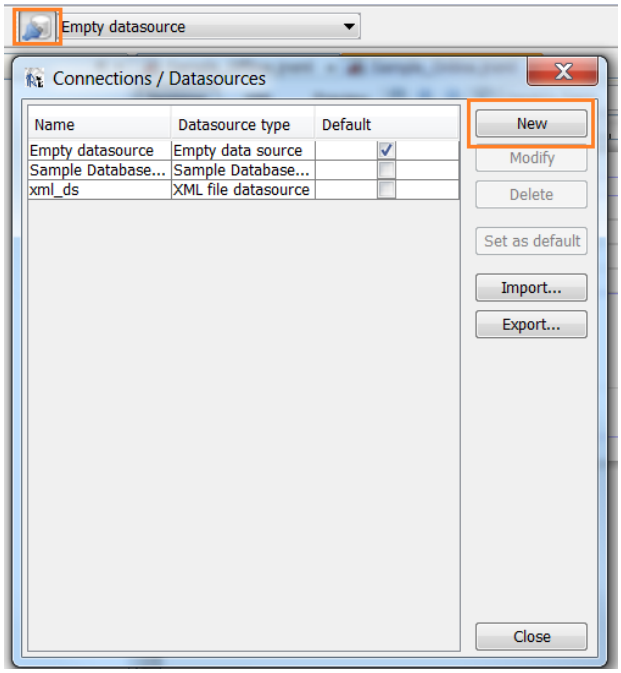
1.4 Create a Customized Online Report Template

The Online Report Template differs from the offline Report template where:

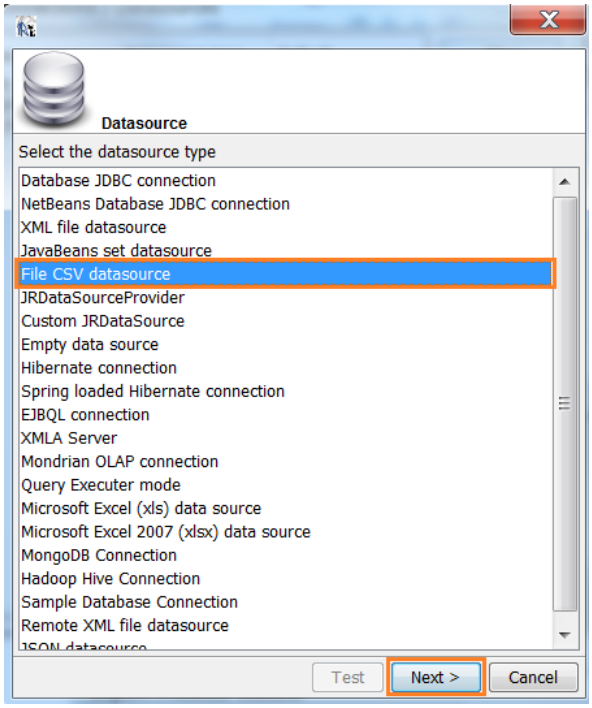
- The online Report Uses a CSV file as the datasource.
- In the online Report the user selects AI Points from 1 to 8 in runtime; that is, the number of AI point is not fixed.

» To create a customized online report template:

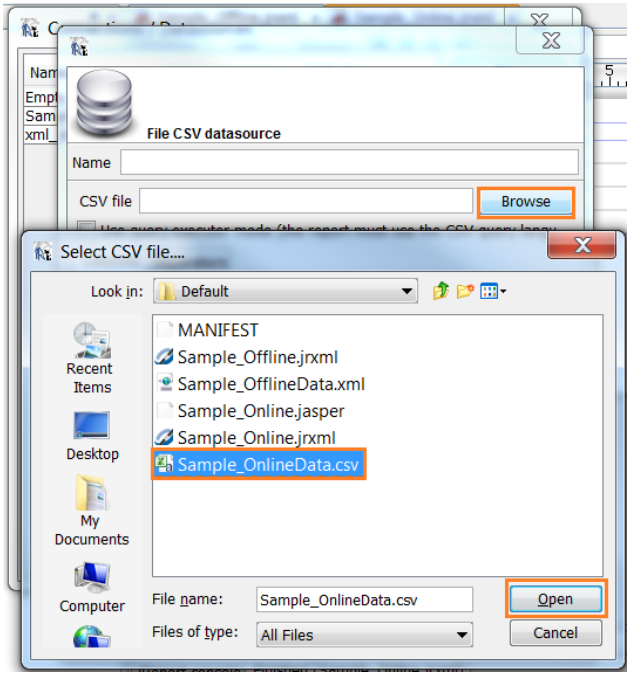
1. Create the CSV DataSource.
   a) Click on **NEW.**



b) Select **File CSV datasource.**



c) Click on **Next.**

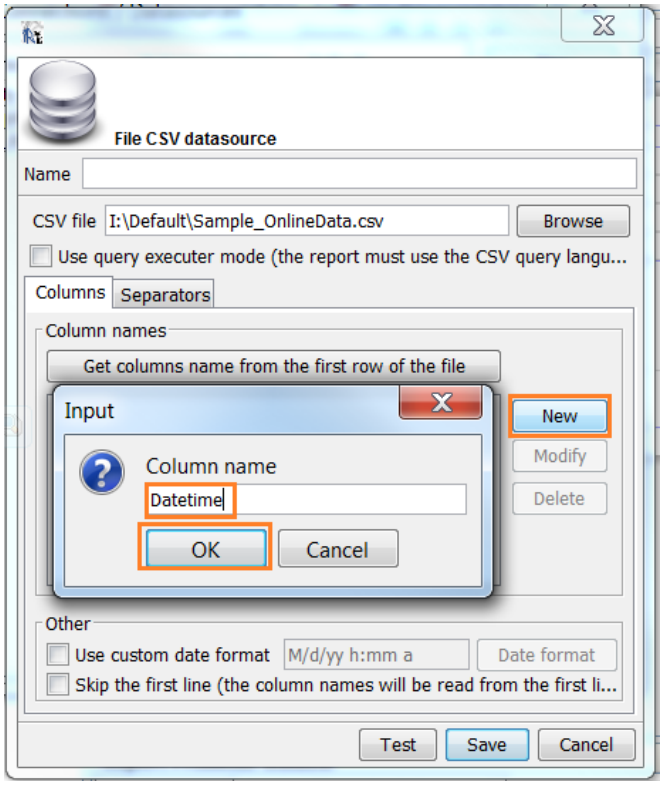


d) Use the GE provided online template named "**Sample_OnlineData.csv**".

e) Navigate to the source file and click **Open**.

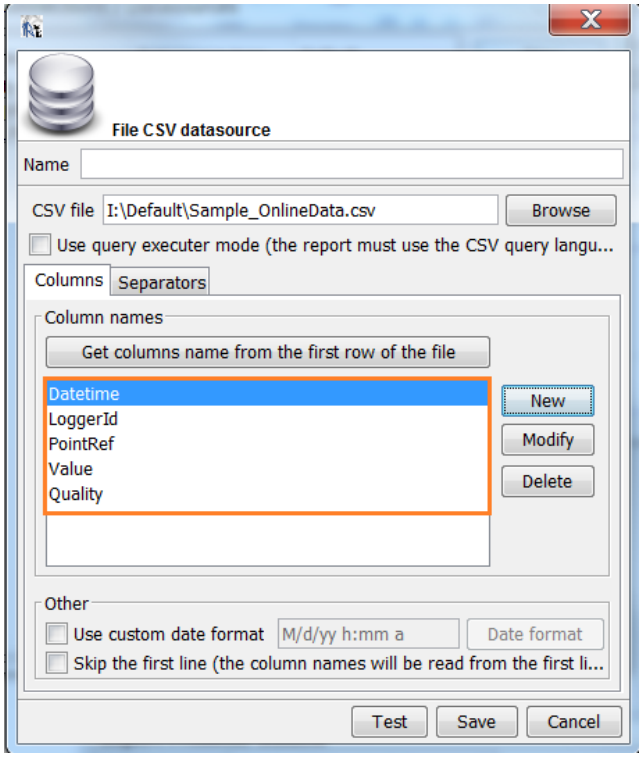
f) Add the required Column name; for example, **Datetime**.

g) Click **OK** and **Save**.



h) Repeat the previous step to add the other four columns: LoggerId, PointRef, Value, Quality.

Note: All of these columns are sequenced as they appear in the CSV file; subsequently, keep the same order.



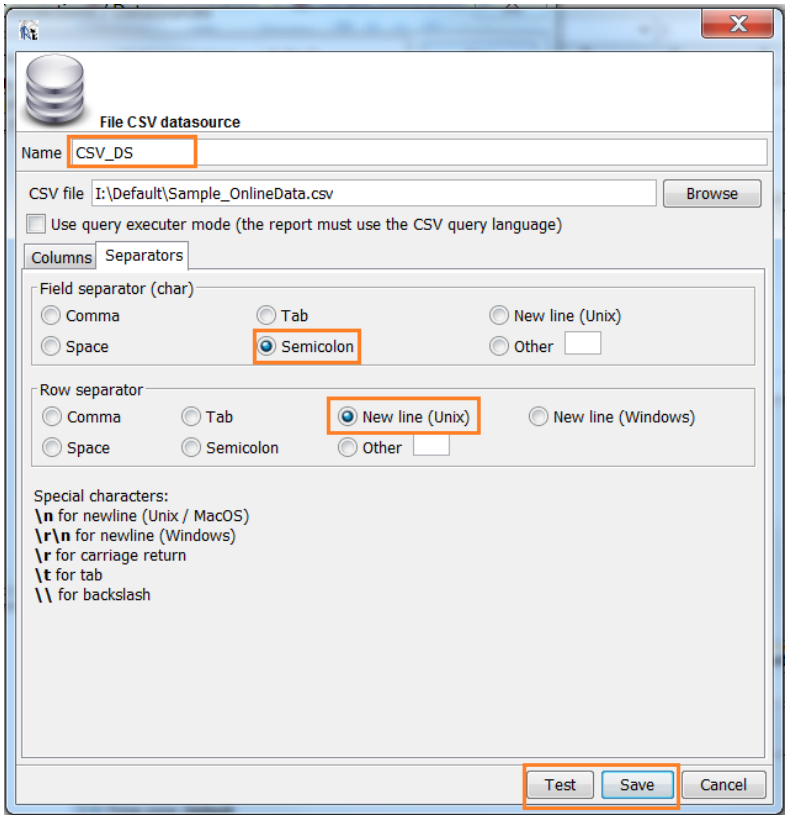
i) Specify the column Separators.

Click the **Separators** tab.

Specify the name of the datasource.

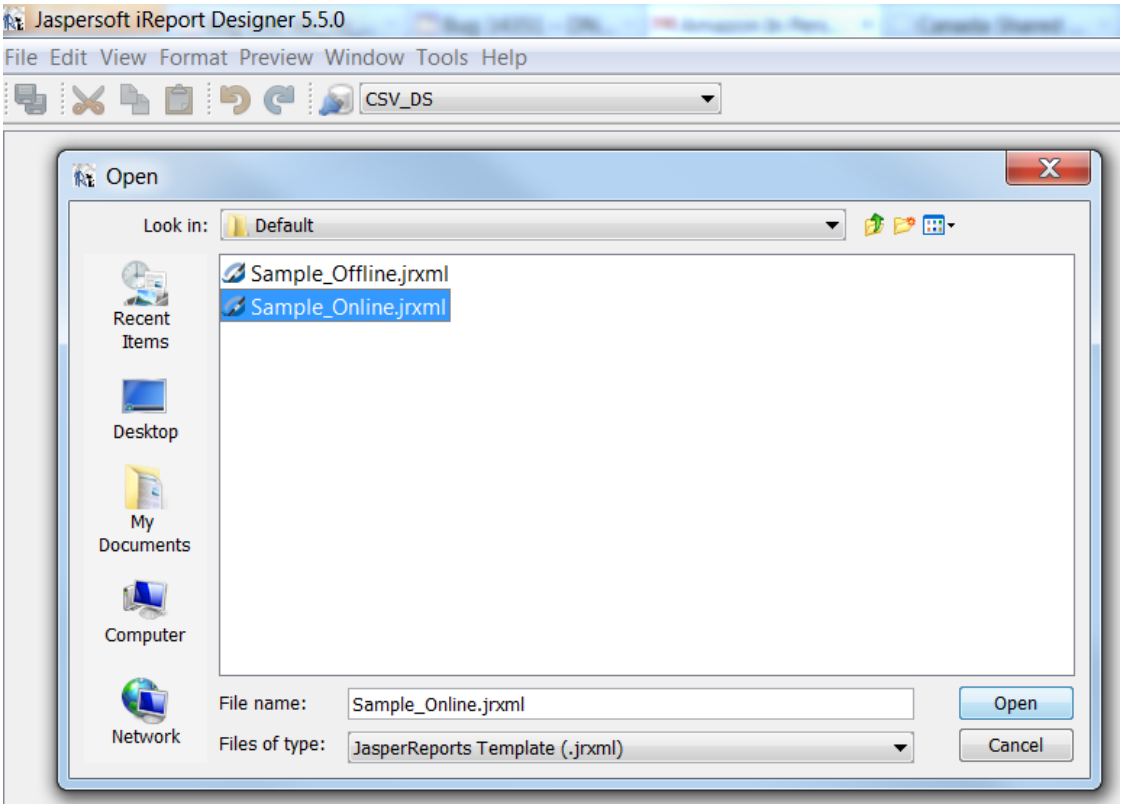
Select a **Semicolon** field separator.

Select a **New line (Unix)** row separator.

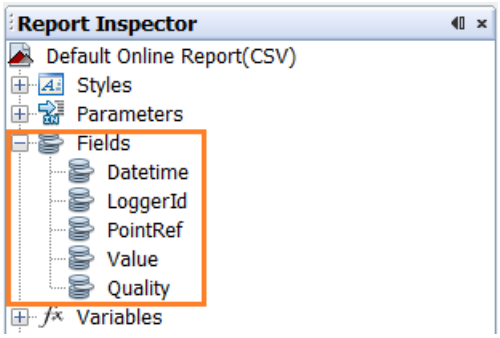


2. Create the Online Report Template using **Sample_Online.jrxml**.

   It is strongly recommended that you use the sample Online Report Template to create your customized template. The sample template can be found at the GE Grid Solutions Technical Support Website.

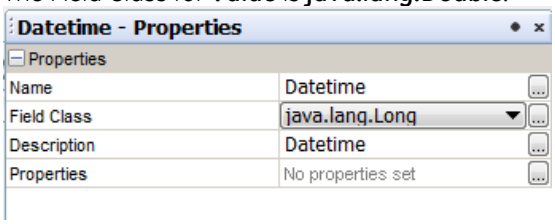


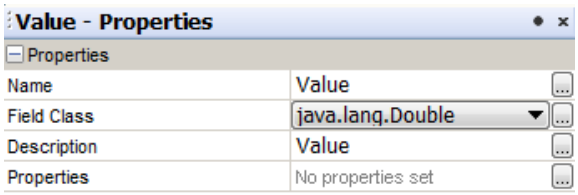
3. All fields are exactly the same as those defined for the **Columns** in the CSV Datasource.



Notes:

- The field Name cannot exceed 8 characters.
- The Field Class for **Datetime** is **java.lang.Long**.
- The Field Class for **Value** is **java.lang.Double**.



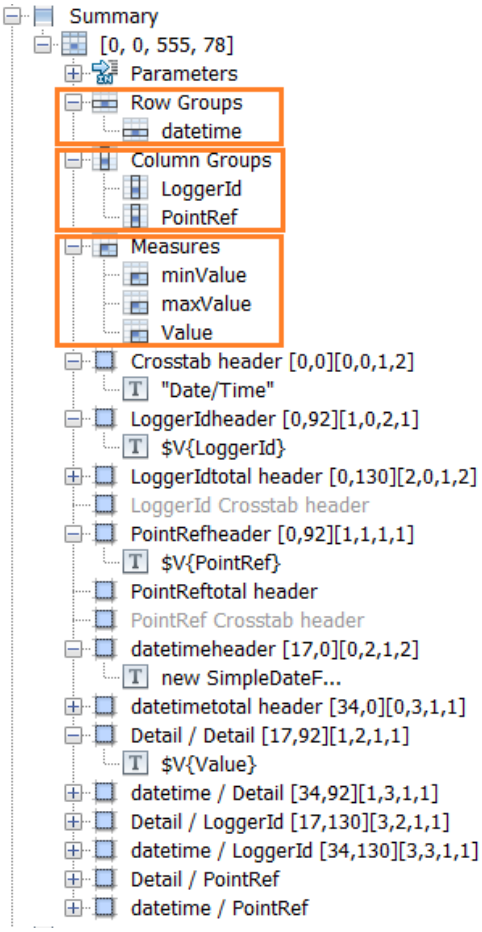


- You can specify the text for the **Description** property, this text appears in Online Report Viewer.
  A field using the CSV Datasource is different from a field using XML Datasource; the **Description** property is used to store XPath in Offline Report Template which is using XML Datasource.

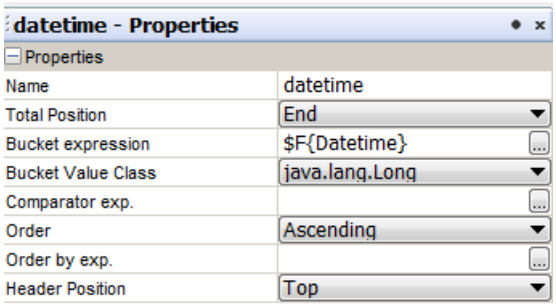
4. Use the **Crosstab** for the Online Report Template.

   The Crosstab component can group records by rows and columns. This is particularly useful when the online report is not aware of the number of AI Points that the user has selected.

   In this sample template the groupings are:

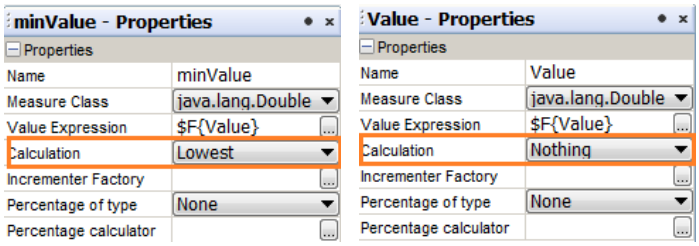


Row Groups: This grouping contains records which have the same value(s) in the field(s); records added to the Row Groups will stay in the same row. The order is specified as, so that newer records always appear below older records.



Column Groups: This grouping contains records with different value(s) in the field(s); records added to Column Groups will stay in a different column. The value of LoggerId is unique for each AI Point.

Measures: Measure labels appear in the crosstab based on their status as a row or column.



The crosstab component is similar to the Table component, but more complex. Refer to the ireport-ultimate-guide.pdf document for more details.

2 Importing Templates

» To import a Report Template into the MCP HMI:

1. Create the MANIFEST file.
2. Create an RZ compressed file.
3. Upload the report template to the MCP by using DS Agile Studio MCP Online Editor or Offline Editor.
4. View the imported report template on the MCP.

2.1 Create MANIFEST file

» To create a MANIFEST file:

1. Navigate to:

   /Sample/MANIFEST

   A sample MANIFEST file is available on the GE Grid Solutions Technical Support Website.

2. Create a new text file or open the sample MANIFEST file using Windows Notepad or another text editor. The sample content is:

   ```
   # template creation datetime in million seconds since 1970-01-01 00:00:00
   creation=1379600831000

   # template's type can be online or any other value. If value is not online, it will be treated as offline. If not specified, default type is offline.

   # template.type=online

   # template description which will be displayed in the report template configuration tool.
   description=This template is a sample, created by the GE Grid Solutions.

   # jasper filename
   file.jasper=demo.jasper

   # jrxml filename
   file.jrxml=demo.jrxml
   ```

3. Change the file.jasper and file.jrxml file names to expected jasper filename and jrxml filename.
4. Save the MANIFEST file to a template directory.

5. Ensure that the both the jasper file, jrxml file and MANIFEST file are saved under the same directory. The jasper file is a binary file compiled by iReport Designer. If you do not have a jasper file:

   a) Run iReport Designer.

   b) Open the jrxml file.

   c) Click Preview.
   Result: iReport Designer creates the jasper file at the same location as the jrxml file by.

2.2 Create RZ file

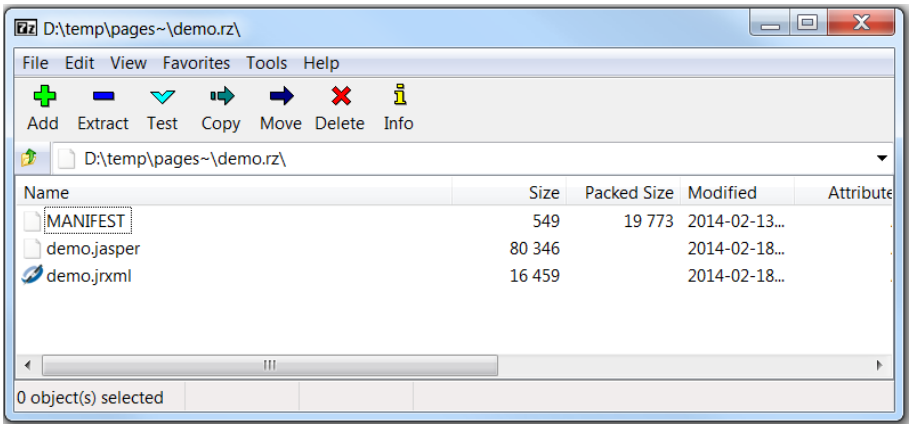
» To create a RZ File:

1. Compress the jrxml file, jasper file and MANIFEST into a zip format file.

   Note: A zip compressing tool is required, i.e. 7zip

2. Change the "zip" file extension to "rz". Only files with an "rz" extension can be uploaded to the MCP. This allows the MCP to distinguish the compressed report template file from other zip files.

   Note: Ensure that the compressed files are located at the top level of the compressed file; therefore, they have no parent folder inside the compressed file. If they are not located at the top level of the compressed file, you will get an "Invalid Template File." error message.



2.3 Upload Template

» To update a template:

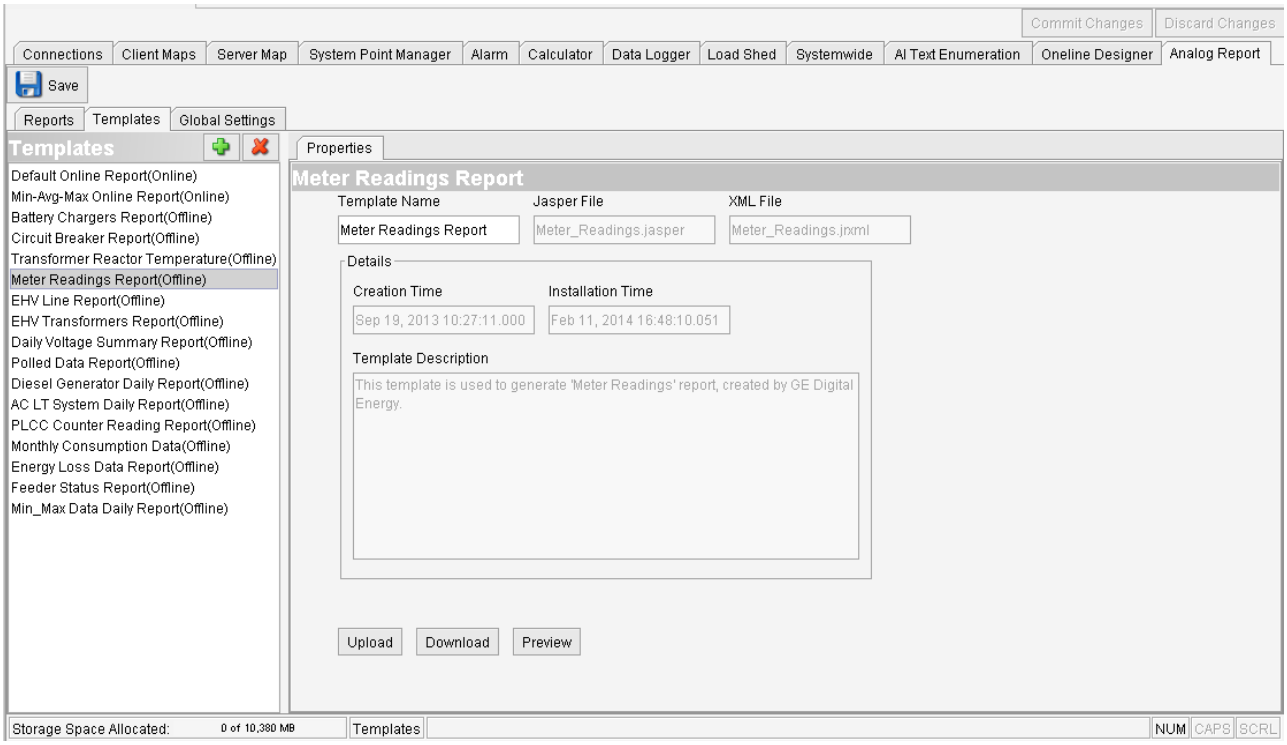
1. Launching MCP Offline from DS Agile Studio and the Configuration needs to be synced to the MCP device later.
2. Select Analog Report tab > Templates.
3. Select an existing template to be changed.
4. If creating a new template, click the button.
5. Click Upload Template and select the "rz" file.

6. If uploading an existing template for a report, you might need to reconfigure the report for the mapped points and parameters. Reformatting is only necessary if the parameter list or point list has changed in the new template; for example, a parameter or point field is added or removed.

   Note: If overwritten template is being used by some reports, all archived offline xml files configured by using this template on MCP might be deleted.

7. Click Preview to ensure proper operation of the new template is providing the expected report.

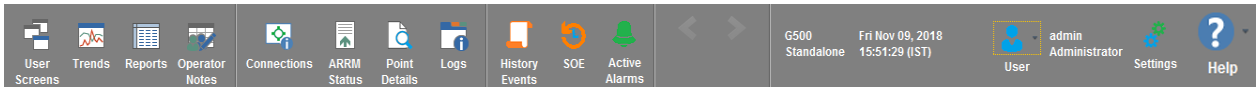
8. Save and Commit.



3 Offline Report Viewer

The offline Reports generated are viewable in the Reports Powerbar Tab in the MCP HMI. The Reports (also known as Offline Report Viewer) allows you to view and download the Analog Reports generated over a period in any of the available file formats like .html, .pdf, .xls.

Refer to MCP Online Help to configure the Analog Report Generation and Data Logger application to generate Offline and Online reports respectively.



All available reports are listed in the file tree structure in the left pane.

Report names with:

- Suffix **In Progress**: indicates that the report is still in the process of being logged.
- Prefix **Archived <N>:** indicates that the report is archived on the MCP to avoid logging records having the same record time on the same offline report file before and after the system date/time changed. <N> is sequence number.

Records having the same record time might be found in archived offline report and regular offline report.

3.1 Report Controls

Report controls allow you save and delete Reports.

Control	Description
check-box	Use the check-box to select and de-select the Reports • Check-box to Select a Report • Clear the check-box to de-select a Report
File Type	Select the file format of the periodic data logger reports to be viewed: • html • pdf • xls

Control	Description
Save button	To save one or more reports: 1. Select the report(s) in the file tree structure in the left pane. Use check-box to select and de-select reports. 2. Click **Save**.
Delete button	To delete one or more reports: 1. Select the report(s) in the file tree structure in the left pane. Use check-box to select and de-select reports. 2. Click **Delete**.
Filter button	Click the **Filter** down-arrow to view the filter options. Result: The Select Filter window appears. You can either: • Type in a specific Report Name, or • Choose a set of Analog Reports that were generated between the Start and End Dates. Click the **Apply** button to list the reports that match the specified filter conditions. Click the **Show All** button to list all available reports. Click **X** (top-right) to close the Select Filter window.

3.1 Offline Report Fields

Field1	Description
Disk Usage	Indicates disk usage in percent against total disk size configured.
Estimated Days of Disk Full	Estimated number of days that the disk will be full. This approximation is based on the various parameters such as the Number of configured Reports, Size of each Report and the Available Disk Space.
Total Reports	Indicates the total number of reports currently available on disk.
Total Shift Reports	Indicates the total number of shift type reports currently available on disk.
Total Daily Reports	Indicates the total number of daily type reports currently available on disk
Total Weekly Reports	Indicates the total number of weekly type reports currently available on disk
Total Monthly Reports	Indicates the total number of monthly type reports currently available on disk

4 Online Report Viewer

The Online Report Viewer is used to show AI Points configured for the Data Logger Periodic Report. To view the Periodic Report, the Periodic Report must be configured properly in the Data Logger.

Two online templates are provided on the GE Grid Solutions Technical Support Website:

- The default online template
- The min avg max template

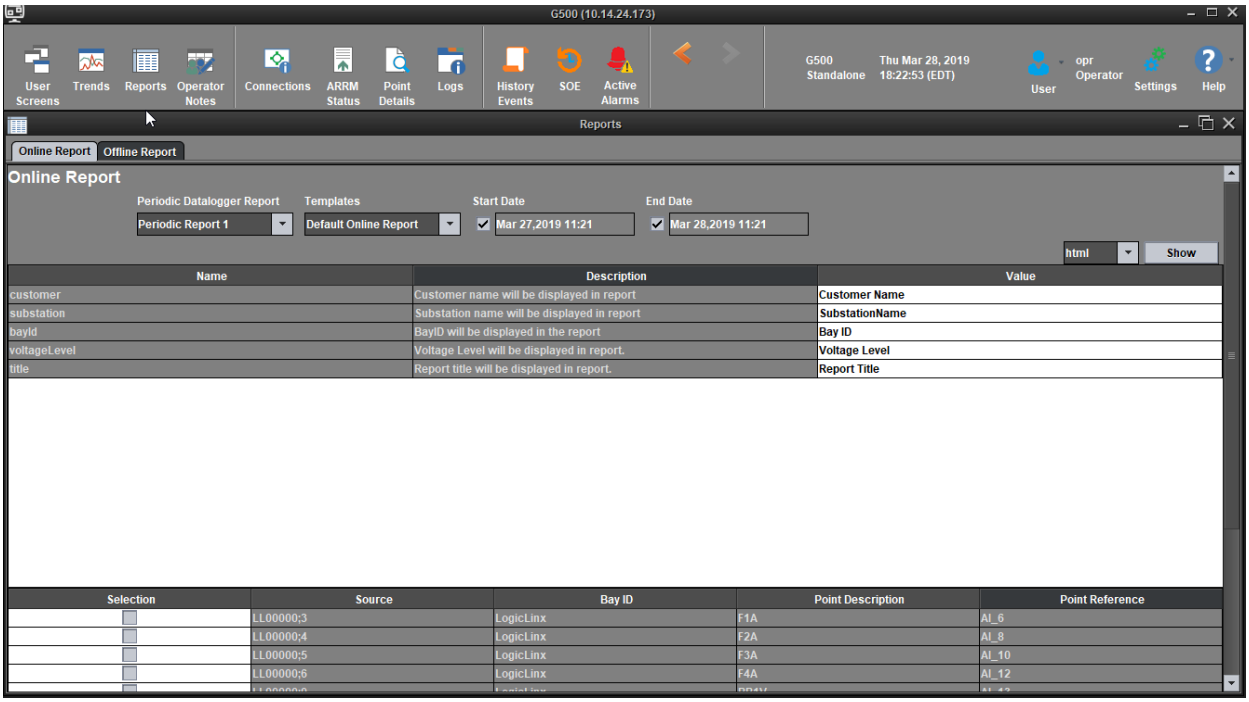
You can overwrite the default online template with another online template.

At any time, one online template should be present in the MCP HMI Analog Report Configuration Tool.

A maximum of 50000 updated data values can be viewed in a report at one time with a maximum socket timeout of 30 seconds.

» **To access the Current (Online) Report Viewer:**

- Click the MCP HMI **Reports** powerbar button.



4.1 Use Filter

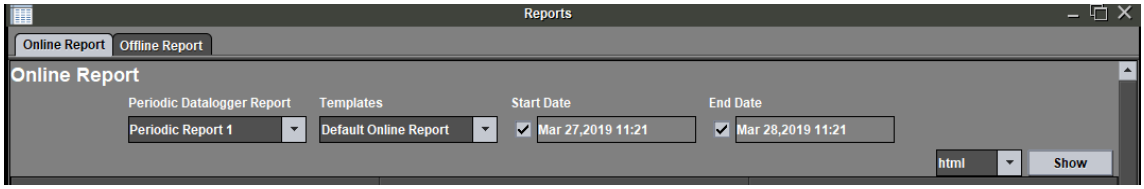
The Use Filter affects the following:

- Generated report only has records which match the selected query criteria.
- Generated report output format (HTML, PDF or MS Excel).

The Use Filter contains the followings:

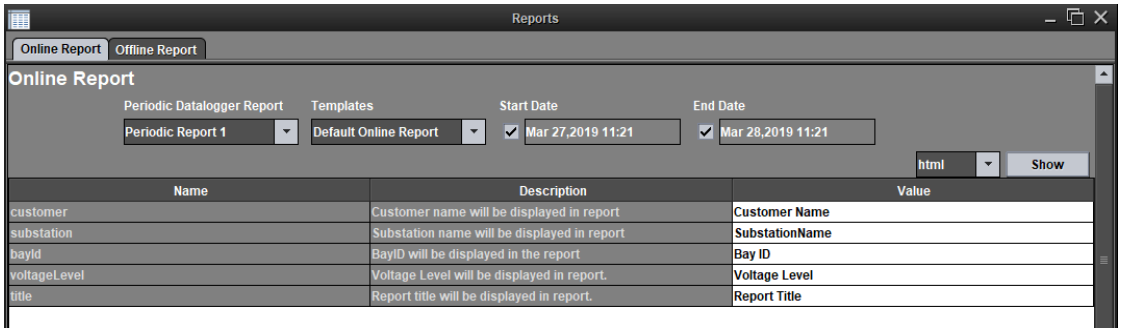
- **Periodic Datalogger Report**: Periodic Reports configured in Data Logger.
- **Templates**: Current (Online) Report Templates configured.
- **Start Date**: If selected, showing records which records' time are newer than specified date/time.
- **End Date**: If selected, showing records which records' time are older than specified date/time.
- **Output Format**: The output format can be html, pdf or MS Excel.

  Note: If both the Start Date and End Date checkboxes are not selected, all records are selected.



4.2 Set Report Parameters

Report parameters are defined in the report template. These parameters will appear in the output report. You can override the default values for these parameters.



4.3 Select AI Points

You can select a maximum of eight AI Points. The created report will show records for the selected AI Points.

Selection	Source	Bay ID	Point Description	Point Reference
☐	0000005;14	Bay 0	LF_SEC	LF_SEC
☑	0000005;13	Bay 0	LF_MONTH	LF_MONTH
☐	0000005;7	Bay 0	FREQ(Present Values)	FREQ(Present Values)(Present Values)
☐	0000005;8	Bay 0	IBX(Present Values)	IBX(Present Values)(Present Values)
☑	0000005;15	Bay 0	ICX(Present Values)	ICX(Present Values)(Present Values)
☐	0000005;9	Bay 0	IBT(Present Values)	IBT(Present Values)(Present Values)
☑	0000005;10	Bay 0	1_Ia_Amps	1_Ia_Amps
☑	0000005;11	Bay 0	1_Ib_Amps	1_Ib_Amps
☑	0000005;12	Bay 0	1_I0_Amps	1_I0_Amps
☐	LL00000;3	LogicLinx	F1A	AI_6
☑	LL00000;4	LogicLinx	F2A	AI_8
☐	LL00000;5	LogicLinx	F3A	AI_10
☑	LL00000;6	LogicLinx	F4A	AI_12
☐	LL00000;0	LogicLinx	BB1V	AI_13
☑	LL00000;1	LogicLinx	BB2V	AI_14
☐	LL00000;2	LogicLinx	FREQ	AI_16

5 Analog Report Generation - Configuration

The configuration page provides three tabs:

- Reports
- Templates
- Global Settings

5.1 Reports Tab

The Reports tab of the Analog Reports Generation configuration window allows you to configure different sets of reports in the system.

» To create a new Analog Report:

1. Launching MCP Offline Editor from DS Agile Studio.

   Note : Configuration needs to be synced to the MCP device if using offline editor.

2. Click the **Analog Report** tab.
3. Click the button to initiate the creation of a new Analog Report.
   Result: A default report name appears in the Reports pane on the left.
   Result: The **Reports** > **Properties** tab fields appear.
4. Enter values in the **Properties** fields.
   Result: The entered **Report Name** appears in the Reports pane.
5. Click the **Reports** > **Points Map** tab.
   Result: A report parameter list appears in a Point Map table. The list of report parameters is determined by which Template Name was selected in the previous step.
6. Click on a report parameter.
   Result: The selected table row appears with a light-blue background.
7. Map a point to the point parameter by double-clicking a point in the file tree structure.
   Result: The mapped point details appear.

8. Click the **Save** icon.
   Result: A confirmation window appears.
   Result: The created report is saved in the HMI.
9. Click **Commit Changes** to apply the changes to the MCP.

NOTICE **Known Issue**	The current Offline Analog Report is created with incorrect start time and end time if the MCP time is manually changed when DST is enabled (Daylight Saving Time). Note that the DST is enabled automatically based on the Time zone configured. If an Offline Analog Report is in the process of gathering data records when DST is enabled: • The first Offline Analog Report will contain an extra 1 hour of records; this additional 1-hour of records should have been included with the next report. • The next report will not contain the first 1 hour of records. For example: 1. A 4-hour duration shift report starts at 00:00 and is to end at 03:45. 2. DST is enabled at 2 am. 3. The reports are created: • The first report contains records gathered from 00:00 to 03:45 and 04:00 to 04:45. • The next report contains records gathered from 05:00 to 07:45; that is, it does not contain the 04:00 to 04:45 records. Subsequent reports are created and logged correctly.

» **To delete an Analog Report:**

1. Launching MCP Offline Editor from DS Agile Studio.
   Note: Configuration needs to be synced to the MCP device if using offline editor.
2. Click the **Analog Report** tab.
3. Select a report name in the Reports pane.
4. Click the button.
   Result: The Delete Report confirmation window appears.
5. Click **Yes** to delete the report.
6. Click the **Save** icon.
   Result: A confirmation window appears.
   Result: The report is removed from the HMI.
7. Click **Commit Changes** to apply the changes to the MCP.

Reports > Properties Sub-tab Fields

Field	Description
Report ID	Auto-generated unique report identifier number.
Report Name	Type the report name.
Template Name	Select the template: • Battery Chargers • Circuit Breaker • Transformer Reactor Temperature • Meter Readings • EHV Line • EHV_Transformers • Daily Voltage Summary • Polled Data **Note**: The MCP Analog Report Generation Application also allows you to add additional (user-configurable) templates. Refer to the Jasper iReport Configuration Manual.
Report Type	Select the type of report: • Shift • Daily • Weekly • Monthly
Enable Logging	Check this box to enable logging of the configured analog data.
Report Duration	Select the duration period in which data is to be logged before a report is generated: • 4 Hours • 6 Hours • 8 Hours • 12 Hours
Log Interval	Select the interval at which a new record is to be logged for the report: • 15 Minutes • 30 Minutes • 60 Minutes
Start Time Alignment (Hour of Day)	Select the hour of the day (on a 24-hour clock) at which a new report will start to log data. The range is 0 to 23 hours.
Logging Alignment (Minute of Hour)	Select the minute of the hour at which every record will be aligned in a report: • xx:00 • xx:15 • xx:30 • xx:45

Reports > Point Map Sub-tab

Point Map Table		
Column	**Description**	**Value determined by ...**
Name	Report parameter ID.	... the **Template** selected in the Properties fields.
Description	Report parameter description.	
Home Dir	Home Directory of the source Analog Point Mapped for logging.	... which point has been mapped to this report parameter.
Point ID	Point ID of the source Analog Point Mapped for logging.	
Point Description	Point Description of the source Analog Point Mapped for logging.	
Point Reference	Point Reference of the source Analog Point Mapped for logging.	

Reports > Parameters Map Sub-tab

Parameter Map Table		
Column	**Description**	**Value determined by ...**
Name	Name of Parameter Map.	... the Template selected in the Properties fields.
Description	Description of Parameter Map.	
Value	Type the suitable text for each row. The entered text appears as the header and footer of the generated reports. The position of the header and footer in the layout of the generated report can be pre-defined in the Template.	... the Template selected in the Properties fields. This field can be edited.

5.2 Templates Tab

The Templates tab allows you to:

- Upload a user-configured Template to the MCP.
- Download available Templates from the MCP.
- Preview the available user-configured Templates.

Upload a Template to a MCP

Only use this procedure if you have created Templates using Jasper iReports Software. For more details, refer to the iReport Designer manual. This manual is available on the GE Grid Solutions Technical Support Website.

For example, to locate the template files, login and navigate to:

Substation Automation Products > G500 > Analog Reports Templates

» **To upload a template to the MCP:**

1. Launching MCP Offline Editor or Online Editor from DS Agile Studio from the PC where the **Templates** are available.
2. Click the **Analog Report** tab.
3. Click the **Templates** sub-tab.
4. Either:

- Select an existing template from the Templates pane.
  or
- Create a new template by clicking the button.

6. Click the **Upload** button.
   Result: The Open window appears.
7. Navigate to select the required **.rz** file.
8. Click **Open**.
   Result: The .rz file is opened and the Open window closes.
9. Click the **Save** icon.
   Result: A confirmation window appears.
   Result: The created template is saved.
10. Click **Commit Changes** to apply the changes to the MCP.

Note:

- If a template is uploaded onto an existing template which is being used by a report, you might need to reconfigure the report for mapped points and parameters. This occurs only if parameter list or point list changed in new template; that is, a parameter or point field has been added or removed.
- To ensure that a new template is working well, it is recommended that you preview the report before saving and committing the report.

» To download a report template from the MCP:

1. Launching MCP Offline Editor or Online Editor from DS Agile Studio.
2. Click the **Analog Report** tab.
3. Click the **Templates** sub-tab.
4. Select an existing report template from the Templates pane.
5. Ensure that the report template has been saved and committed.
6. Click the **Download** button.
   Result: The Save window appears.
7. Navigate to the folder which is to contain the .rz file.
8. Click **Save**.
   Result: The Save window closes and the Download Template confirmation window appears.
9. Click **OK**.
   Result: The Download Template confirmation window closes.
10. Click the **Save** icon.
    Result: A confirmation window appears.
    Result: The created template is saved in the HMI.
11. Click **Commit Changes** to apply the changes to the MCP.

» To preview a report template:

1. Launching MCP Offline Editor or Online Editor from DS Agile Studio.
2. Click the **Analog Report** tab.
3. Click the **Templates** sub-tab.
4. Select an existing report template from the Templates pane.
5. Click the **Preview** button.
   Result: A preview of the report appears.

Templates Tab Fields

Field	Description
Template Name	Type the template name.
Jasper File	Displays the name of the Jasper file.
XML File	Displays the name of the .Jrxml file.
Details	
Creation Time	The time that this template was created.
Installation Time	The time that this template was uploaded to this MCP.
Template Description	The description of the template file provided by the Template.

Templates Tab Buttons

Button	Description
Upload	Upload a report template to the MCP. For example, the uploaded report template could have been created using Jasper iReports Software.
Download	Download a report template from the MCP.
Preview	Preview a report template.

Global Settings Tab

The Global Settings tab allows you to configure global settings which affect all reports.

Field	Description
Storage Full Action	Select an action to occur when the configured Analog Report Generation storage space is full. The options are: • Delete Oldest Reports • Stop New Reports
Threshold (%) for Storage Full	Set the percentage of storage space at which a warning message appears. The valid range is 50% to 95%.
Time Zone	Select a time zone from the list provided. This parameter affects the Start Time Alignment and Logging Alignment of the report.

Modification Record

Version	Revision	Date	Change Description
1.00	0	28th March, 2019	Document created.
	1	22nd April, 2019	Updated the Analog Reports Template download location.
	2	14th October, 2019	Updated the Report Template Creation Procedure.
2.00	0	22nd April, 2021	Updated for MCP family.
	1	23rd April, 2021	Updated Technical Support Contacts.

GE

Grid Solutions

Integration of MCP devices with OpenVPN Client

Installation and Configuration Guide

SWM0103

Version 2.00 Revision 2

Associated Software Release: Version 1.00

imagination at work

GE Information

COPYRIGHT NOTICE

© 2021, General Electric Company. All rights reserved.

The Software Product described in this documentation may only be used in accordance with the applicable License Agreement. The Software Product and Associated Material are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable, and are delivered with Restricted Rights. Such restricted rights are those identified in the License Agreement, and as set forth in the "Restricted Rights Notice" contained in paragraph (g) (3) (Alternate III) of FAR 52.227-14, Rights in Data-General, including Alternate III (June 1987).

If applicable, any use, modification, reproduction release, performance, display or disclosure of the Software Product and Associated Material by the U.S. Government shall be governed solely by the terms of the License Agreement and shall be prohibited except to the extent expressly permitted by the terms of the License Agreement.

The information contained in this online publication is the exclusive property of General Electric Company, except as otherwise indicated. You may view, copy and print documents and graphics incorporated in this online publication (the "Documents") subject to the following: (1) the Documents may be used solely for personal, informational, non-commercial purposes; (2) the Documents may not be modified or altered in any way; and (3) General Electric Company withholds permission for making the Documents or any portion thereof accessible via the internet. Except as expressly provided herein, you may not use, copy, print, display, reproduce, publish, license, post, transmit or distribute the Documents in whole or in part without the prior written permission of General Electric Company. If applicable, any use, modification, reproduction, release, performance, display, or disclosure of the Software Product and Associated Material by the U.S. Government shall be governed solely by the terms of the License Agreement and shall be prohibited except to the extent expressly permitted by the terms of the License Agreement.

The information contained in this online publication is subject to change without notice. The software described in this online publication is supplied under license and may be used or copied only in accordance with the terms of such license.

TRADEMARK NOTICES

GE and are trademarks and service marks of General Electric Company.

* Trademarks of General Electric Company.

Serial/IP is a registered trademark of Tactical Software, LLC.
Tactical Software is a registered trademark of Tactical Software, LLC.

Other company or product names mentioned in this document may be trademarks or registered trademarks of their respective companies.

Contents

About this Document 7

Purpose of this Document 7
Intended Audience 7
Additional Documentation 7
Safety words and definitions 7

Product Support 9

GE Grid Solutions Web Site 9
GE Technical Support Library 9
Contact Technical Support 9

1. Overview 10

1.1 Supported Client Devices 10
1.2 Setup Procedure 10

2. Setting up a Certification Authority 12

2.1 Setting up the XCA Certification Authority 12

3. Server & Client Certificate Generation 16

3.1 Generating Certificates Using XCA 16

4. Installing Certificates 23

4.1 Installing CA Certificate, Server Certificate and Diffie Hellman Parameters on the MCP 23
4.2 Installing Client Certificate in Windows Server 2012 R2 25
4.3 Installing Client Certificate in Windows 7 PC 27
4.4 Installing Chain of CA Certificates on the MCP 31

5. Configuring VPN in MCP 33

5.1 Configuring VPN Server 33
5.2 Configuring VPN Client Parameters 36
5.3 VPN Server Log 38

6. Exporting VPN Client Configuration 39

7. Configuring OpenVPN Client 41

8. Revoking a Client certificate 45

8.1 Revoking the Certificate in XCA 45

8.2 Exporting the CRL in XCA 45
8.3 Installing the CRL in the MCP 46

9. Running OpenVPN Client as Windows Service using NSSM 47

9.1 How to install NSSM 47
9.2 How to Use NSSM..... 47
9.3 Running OpenVPN as Windows Service Using NSSM 48
9.4 Setting Up OpenVPN as a Service..... 48

A. Certificate Error Messages Logged by OpenVPN Configuration HMI 54

B. OpenVPN Server Log Messages.....58

C. VPN Client from Ubuntu PC.....61

D. List of Acronyms.....62

Figures

Figure 1: MCP OpenVPN Configuration & Installation Flow Diagram..... 11

Tables

Table 1 Example Distinguished Name Components 13
Table 2 Example Distinguished Name Components 17
Table 3 Example Distinguished Name Components 19
Table 4 Location of Files Exported by Certification Authorities 23
Table 5 VPN Server Configuration Parameters 33
Table 6 VPN Client Configuration Parameters 36
Table 7 Routing List and White List 37
Table 8 ICMP White List Options 37
Table 9 List of Acronyms 62

About this Document

Purpose of this Document

This document describes how to establish a VPN (Virtual Private Network) channel between a MCP and an OpenVPN client running on a remote computer running Windows® Server 2012 R2 or Windows 7 for accessing one or more protected services in the substation. This document provides the procedures to:

- Implement a simple Certification Authority using XCA Certification Authority (Open-Source tool).
- Install certificates on the MCP and a Windows® Server 2012 running with OpenVPN client software.
- Configure OpenVPN server in MCP to communicate to OpenVPN client.
- Configure OpenVPN client to communicate to the MCP over virtual private network.

NOTE: This document applies to the MCP family (G100/G500) unless otherwise indicated. Screen captures may show G500 in some areas, however the workflow applies to products in the MCP family (G100/G500).

Intended Audience

This document serves as a reference for utility personal and systems integrators who wish to setup a VPN (Virtual Private Network) channel between a client device (Windows® Server 2012 R2 or Windows 7) and a MCP for the purposes of accessing one ore more protected services in the substation.

Additional Documentation

For further information about the Integration of MCP devices with OpenVPN Client, refer to the following documents:

- MCP Substation Gateway Software Configuration Guide, SWM0101/15
- MCP Substation Gateway, HMI Online Help

Safety words and definitions

Before attempting to install or use the device, review all safety indicators in this document to help prevent injury, equipment damage or downtime.

The following safety and equipment symbols are used in this document:

⚠DANGER	**Indicates a hazardous situation which, if not avoided, will result in death or serious injury.**
⚠WARNING	**Indicates a hazardous situation which, if not avoided, could result in death or serious injury.**
⚠CAUTION	**Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.**
NOTICE	**Indicates practices that are not related to personal injury.**

Product Support

If you need help with any aspect of your GE Grid Solutions product, you can:

- Access the GE Grid Solutions Web site
- Search the GE Technical Support library
- Contact Technical Support

GE Grid Solutions Web Site

The GE Grid Solutions Web site provides fast access to technical information, such as manuals, release notes and knowledge base topics.

Visit us on the Web at: http://www.gegridsolutions.com

GE Technical Support Library

This site serves as a document repository for post-sales requests. To *get* access to the Technical Support Web site, go to: http://sc.ge.com/*SASTechSupport

Contact Technical Support

For help with any aspect of your GE Grid Solutions product, please contact our support team, 24/7, as follows:

Region	E-mail	Telephone
Global Contact Centre	ga.support@ge.com	+44 1785 250070
Central and East Asia andPacific	ga.supportCEAP@ge.com	+61 414 730 964
India	ga.supportIND@ge.com	+91 44 22648000
Middle East, North Africa andTurkey	ga.supportMENAT@ge.com	+971 42929467
Europe, Russia, CIS and Sub-Saharan Africa	ga.supportERCIS@ge.com	+34 94 4858854
North America	ga.supportNAM@ge.com	+1 877 605 6777
Latin America	ga.supportLAM@ge.com	+55 11 36187308

1. Overview

A VPN (Virtual Private Network) channel is available between the MCP and an OpenVPN client running on a remote computer running Windows® Server 2012 R2 or Windows 7; this VPN channel allows access to one or more protected services in the substation. The VPN channel is implemented using OpenVPN, which uses a custom protocol based on TLS (Transport Layer Security), and certificate-based mutual authentication.

Certificates are issued by a Certification Authority (CA). Since the MCP is not delivered with a CA, you must make use of an existing CA or create your own. There are many third-party commercial and open-source CAs available. This document describes one open-source CA package:

- X Certificate and Key Management (XCA).

1.1 Supported Client Devices

This document describes how to install and configure the OpenVPN client in the following Devices.

- Windows® Server 2012 R2
- Windows 7

NOTICE This document refers to installation of OpenVPN Client in Windows Server 2012 R2 and Windows 7, but the procedure should be similar for other Windows Operating Systems.

1.2 Setup Procedure

To establish a secure channel between an OpenVPN client and the MCP:

1. Set up your CA; see section 2.1.2 .
2. Generate Diffie Hellman (DH) parameters; see Chapter 2.
3. Generate private key and certificate for your MCP; see section 3.1.1 .
4. Generate client certificate + private key in .pk12 format for OpenVPN client running in Windows® Server 2012 R2 and Windows 7 PC; see section 3.1.2 .
5. Install the CA's Certificate on your MCP; see section 4.1.
6. Install the private keys, certificates and Diffie Hellman parameters on your MCP; see section 4.1.
7. Install .pk12 client certificate + private key into client device (Windows® Server 2012 R2 and Windows 7 PC) -see section 4.2.
8. Using the MCP HMI, configure the parameters for the OpenVPN Server; see section 5.1.
9. Using the "Export VPN Client File" option in the Utilities tab under Settings option, export the OpenVPN client configuration (*. ovpn) into a desired location; see section 5.3.

   Note: Export VPN Client File Option is available in Utilities Tab under Settings option from Local HMI or from the Connected Mode in DS Agile MCP Studio only.
10. Securely copy the OpenVPN client configuration into the client device (Windows® Server 2012 R2 and Windows 7 PC).
11. Run the OpenVPN client software as a service or as a process in the client device (Windows® Server 2012 R2 and Windows 7 PC).
12. Test access to the protected service or device through the MCP OpenVPN server.

Figure 1 shows the sequence of steps involved in setting up an OpenVPN connection between a MCP and OpenVPN Clients. The figure shows G500, but the workflow applies to MCP Family (G500/G100).

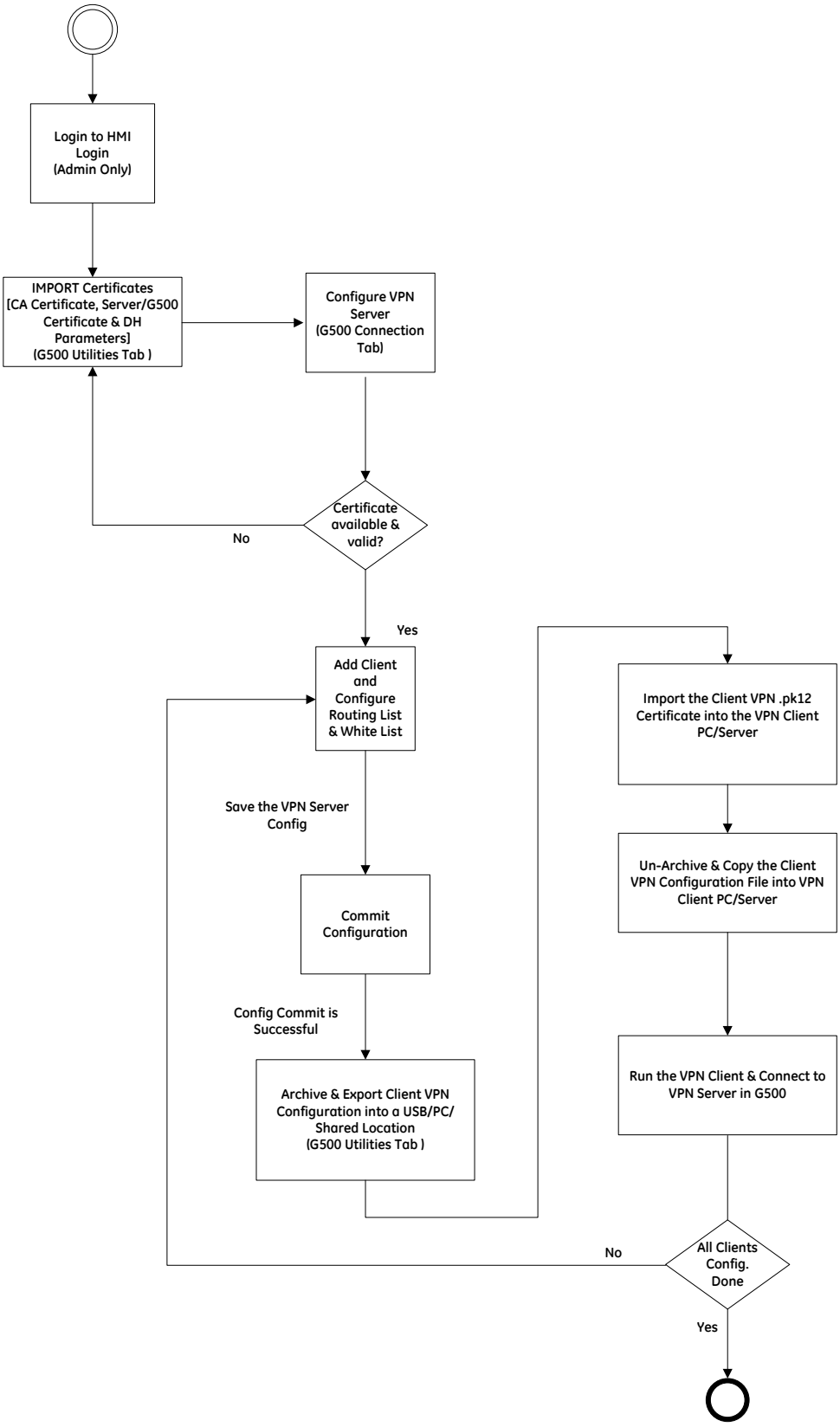


Figure 1: MCP OpenVPN Configuration & Installation Flow Diagram

2. Setting up a Certification Authority

Before you can configure a VPN connection between a client device and the MCP you need a Certification Authority (CA). In case you do not already have a CA, this chapter describes how to set up the XCA certification authority.

Once your CA is up and running, export the CA certificate so that you can install it on the client devices and the MCP.

NOTICE

A CA that is planned for field use should be protected with strong security measures. Such measures include dedicating a computer for the CA, physically securing the computer, ensuring the computer is accessible only by authorized users, and not connecting the computer to a network. Such measures are required because a security breach of a CA would impact all devices that used certificates generated by the CA.

2.1 Setting up the XCA Certification Authority

XCA runs on Linux or Microsoft Windows. Below procedure explains the setting up of XCA Certification Authority for Windows.

The tasks performed to setup and initialize an XCA certification authority are:

1. Install XCA; see section 2.1.1
2. Create a database and initialize the CA; see section 2.1.2 .
3. Generate Diffie Hellman (DH) Parameters; see section 2.1.3 .

2.1.1 Install XCA

1. Download the latest version of XCA from: http://sourceforge.net/projects/xca.
2. Run the installation wizard to install XCA.

2.1.2 Create a Database and Initialize the CA

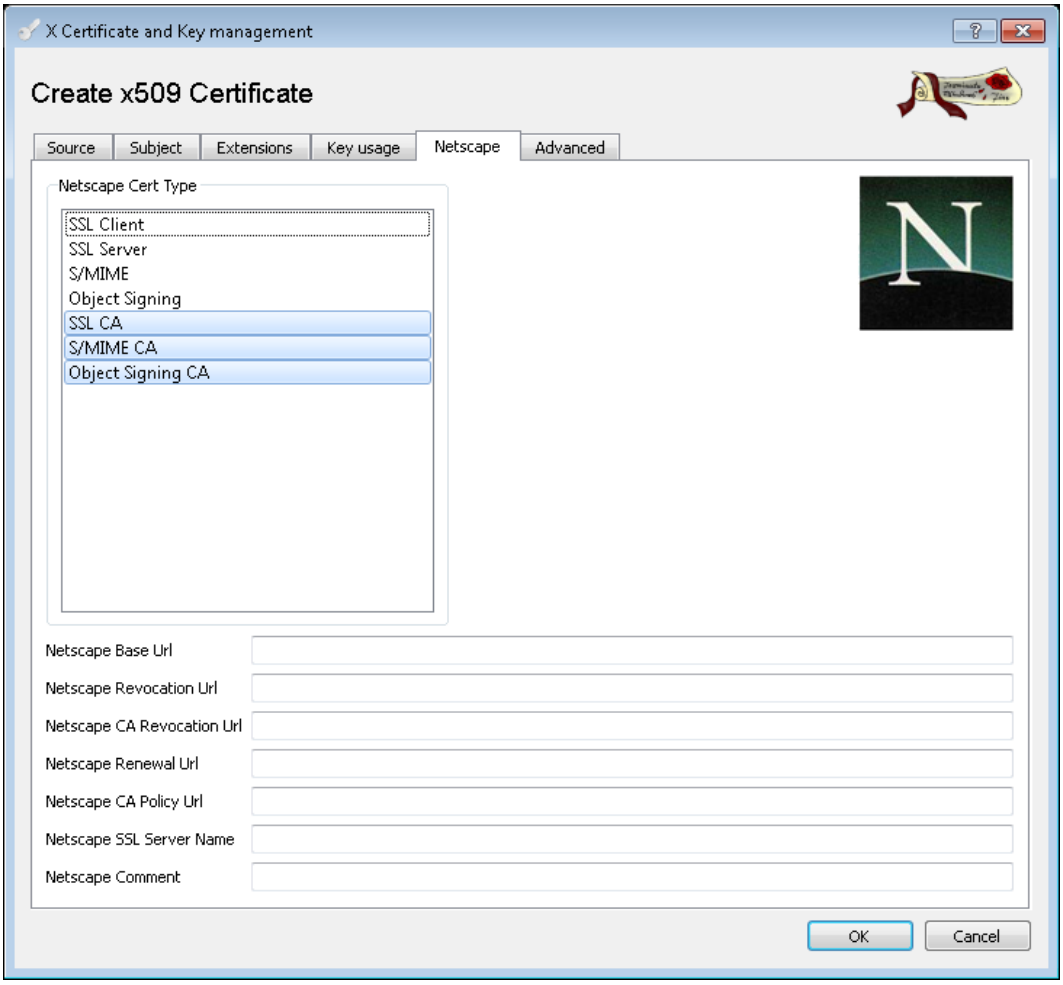
1. From XCA, select **File** > **New Database**.
2. Choose a protected location to save the database and then type in a strong password to encrypt the database.
3. Under the **Certificates** tab, choose **New Certificate**.
4. Under the **Source** tab, select the checkbox next to the label **Create a self signed certificate with the serial**. Change the dropdown named **Signature Algorithm** to “SHA 256” and leave the dropdown named **Template for the new certificate** as “[default] CA”.
5. Under the **Source** tab, click **Apply All**.
6. Under the **Subject** tab, click the **Generate a new key** button.
7. In the dialog that appears, type in the name of the CA (e.g., “MyCA”) in the **Name** field. Choose the **Keytype** as RSA. Change the **Keysize** to 2048.
8. Under the **Subject** tab, type in the distinguished name of the CA certificate. Table 1 provides example distinguished name components.

   Note: You must enter all components of the distinguished name, including the emailAddress.

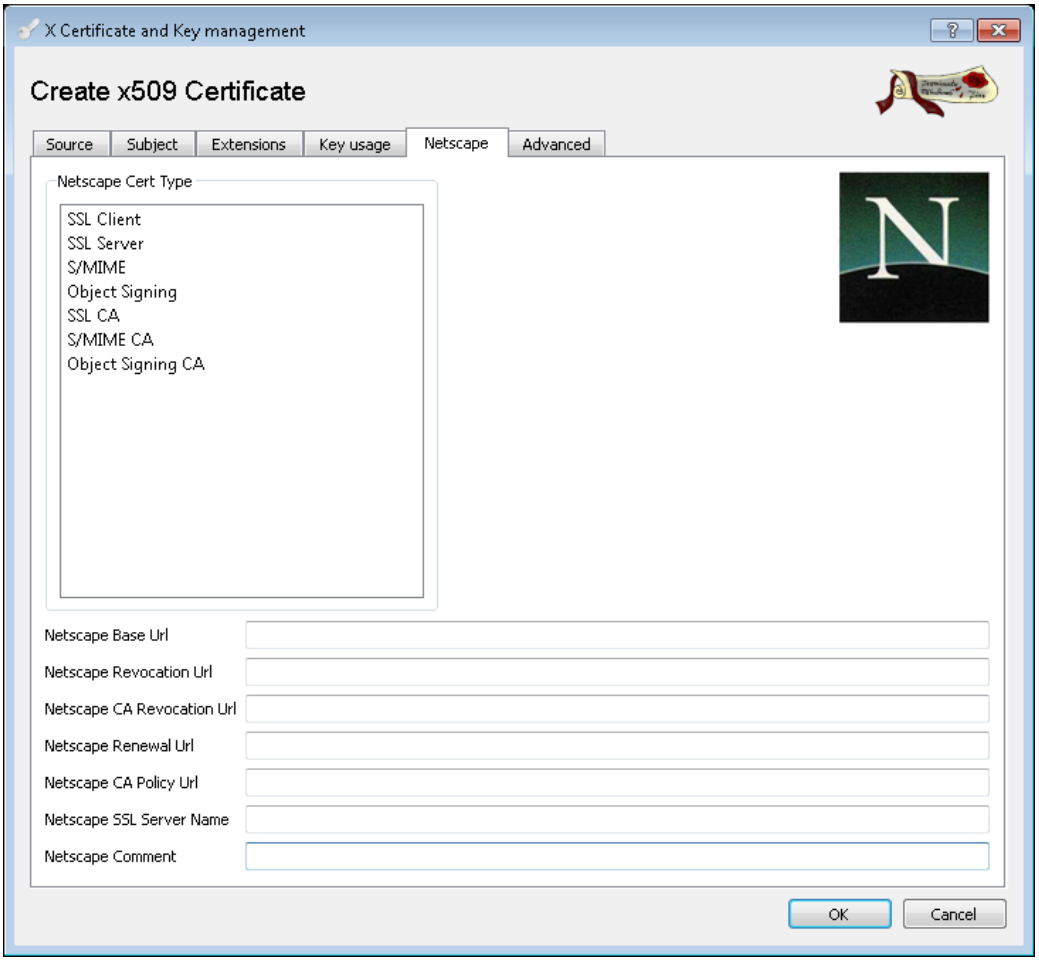
Table 1 Example Distinguished Name Components

Distinguished Name Component	Example
Internal name	MyCA
countryName	US
stateOrProvinceName	MyState
localityName	MyCity
organizationName	MyCompany
organizationalUnitName	MyDivision
commonName	MyCA
emailAddress	mail@my.domain

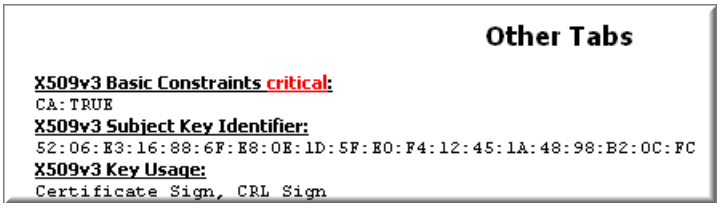
9. Under the **Extensions** tab, if necessary, change the **Time Range** that the CA certificate is valid for and click **Apply**. The default is 10 years. Certificates generated with this CA certificate after this period are no longer valid.
10. Under the **Key usage** tab, do not change the defaults.
11. Under the **Netscape** tab, remove the value in the **Netscape Comment** field.



12. Under the Netscape Cert Type, de-select **SSL CA**, **S/MIME CA**, **Object Signing CA** options.



Result: Under the **Advanced** tab, the following messages appear, except the value of the X509v3 Subject Key Identifier, which differs from key to key:



If above message does not appear, click **Validate** to view the message.

13. Click **OK**.
    Result: You now have a CA certificate to sign your MCP (Server) and Client certificates.
14. Under the **Certificates** tab of the main view of XCA, select the new Certification Authority and click on **Export**.
15. Ensure the **Export Format** is set to **PEM**.
16. Browse to a protected directory (e.g., **My Documents** > **MyXCAFiles**) and click **Save**.
17. Click **OK**.
    Result: The file is named based upon the internal name of your CA with a .crt extension.

2.1.3 Generate Diffie Hellman (DH) Parameters

1. From XCA, select **Extra** > **Generate DH parameter**.
2. Enter a key size of 2048 and click **OK**.
   Result: It may take a few minutes for the parameters to be generated and XCA may appear to be non-responsive. Be patient and allow XCA to complete.
3. When prompted, save the generated DH parameters file in a protected location (e.g., My Documents->MyXCAFiles) and leave the name as dh2048.pem.

3. Server & Client Certificate Generation

This chapter describes how to generate private keys and certificates for both the Client computer and the MCP. These certificates allow the Client to authenticate itself to the MCP and the MCP to authenticate itself to the Client.

There are two types of certificates you can generate:

- The server certificates.
  The server certificate identifies a MCP.
- The client certificate in .pk12 format.
  The client certificate identifies a particular user or a computer that is connected to the MCP.

3.1 Generating Certificates Using XCA

3.1.1 Generating a MCP Server Certificate

A MCP Server certificate allows the MCP to authenticate itself to a Client. The MCP Server certificate contains a **commonName** field. This field should uniquely identify the MCP in your network.

To generate a MCP Server Certificate:

1. Launch XCA from the Windows Programs menu.
2. In the tree view of the **Certificates** tab, select the branch containing your Certification Authority.
3. Under the **Certificates** tab, click the **New Certificate** button.
4. Under the **Source** tab:
   a. Select the checkbox next to the label **Use this Certificate for signing**. On the dropdown to the right of this checkbox, select the CA you created in section 2.1.2 (e.g., MyCA).
   b. Change the dropdown **Signature Algorithm** to **SHA 256**.
   c. Change the dropdown **Template for the new certificate** to "[default] HTTPS_server".
   d. Click **Apply all**.
5. Under the **Subject** tab, click the **Generate a new key** button.
6. In the dialog that appears, type in a name that uniquely identifies the MCP in your network (for this example, "MyMCP"). Choose **Keytype** to RSA. Change the **Keysize** to 2048.
7. Click **OK**.
8. Go back to the **Subject** tab and type in the Distinguished name of the MCP server certificate. The most important component is the ***commonName***. This is the name that your Clients is configured to accept. Any difference between the commonName of the certificate and the name configured in the Client results in a failed connection. Choose other name components that are appropriate for your company. Table 2 provides example distinguished name components.

   Note: You must enter all components of the distinguished name, including the emailAddress.

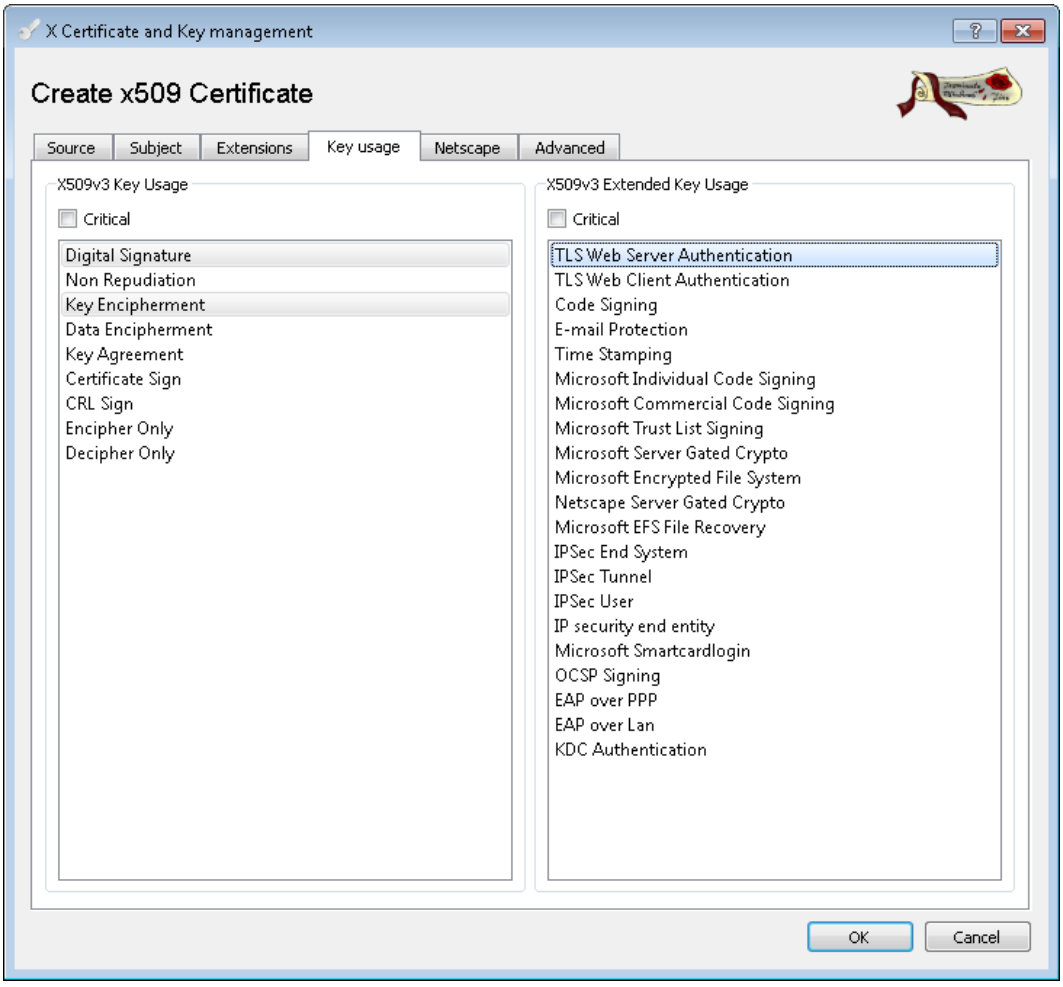
Table 2 Example Distinguished Name Components

Distinguished Name Component	Example
Internal name	MyMCP
countryName	US
stateOrProvinceName	MyState
localityName	MyCity
organizationName	MyCompany
organizationalUnitName	MyDivision
commonName	**MyMCP**
emailAddress	mail@my.domain

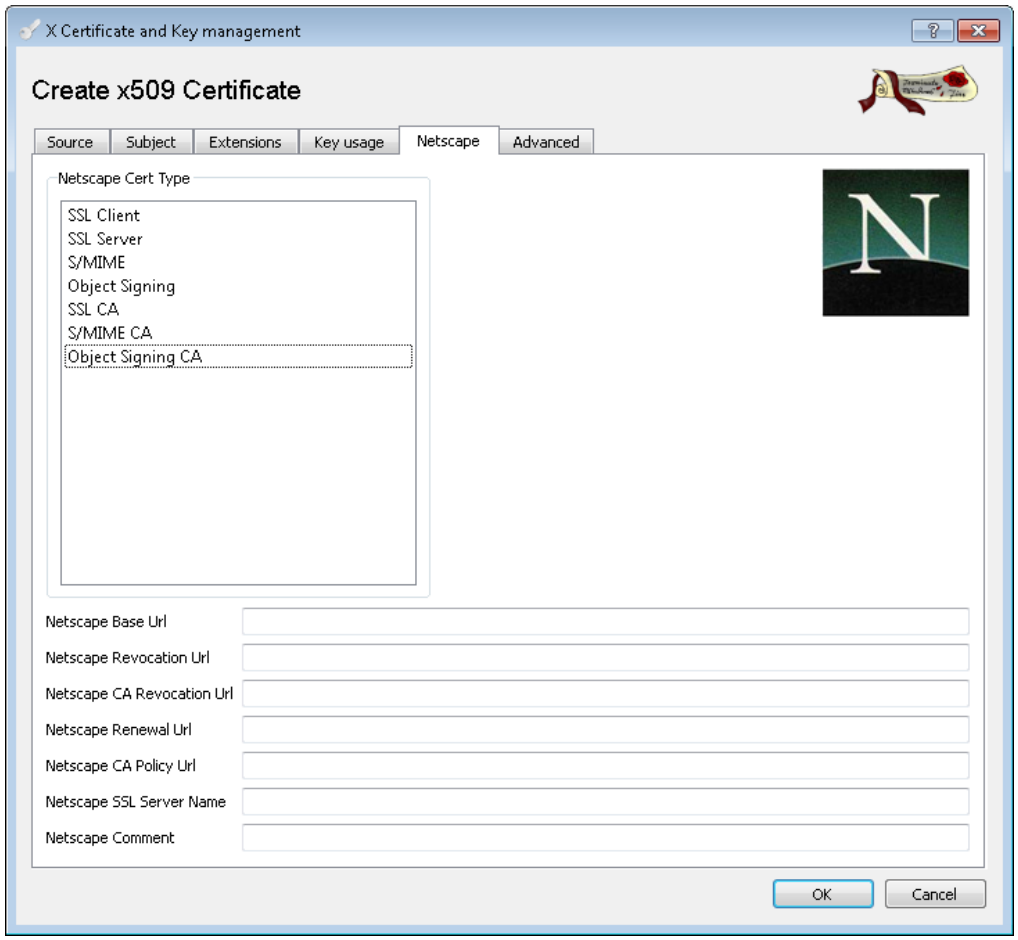
9. Under the **Extensions** tab, if necessary, change the **Time Range** that the CA certificate is valid for and click **Apply**. The default is one year.

   The shorter the Time Range the more secure the certificate, but the more often you need to regenerate MCP Server certificates and deploy them into your MCPs.

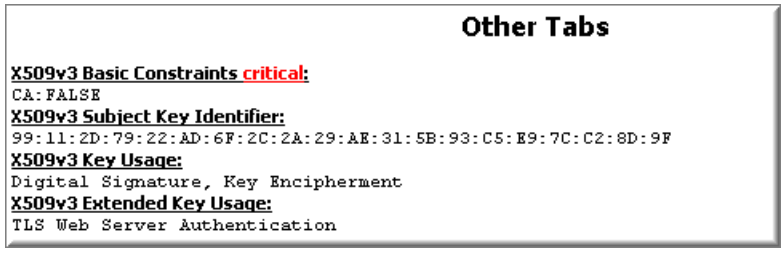
10. Under the **Key usage** tab, under X509v3 Key Usage select **Digital Signature** and **Key Encipherment** and under X509v3 Extended Key Usage select **TLS Web Server Authentication** as shown below.



11. Under the **Netscape** tab, remove the **Netscape comment** and under the **Netscape Cert Type**, if **SSL Server** is selected then deselect it from the list.



12. Under the **Advanced** tab, click **Validate**. The following messages are expected except the value of the X509v3 Subject Key Identifier, which differs from key to key:



If above message is not displayed, click **Validate** to see the message.

13. Click **OK**. You now have a MCP Server certificate.

14. In the tree view under the **Certificates** tab, open the branch labeled according to your Certificate Authority, and select the new Server certificate.

15. Click **Export.**

16. In the dialog that appears, ensure the **Export Format** field is set to "PEM Cert + key". Browse to a protected location (e.g., My Documents->MyXCAFiles) and click **Save**. Finally click **OK.** The certificate and private key will be in a file named with your MCP's Internal Name with the extension .pem (e.g., MyMCP.pem).

NOTICE This file is sensitive so keep it protected at all times. Delete all copies of the file after it has been installed on the MCP. The file can be exported again from XCA if necessary.

3.1.2 Generating a Client Certificate

A Client certificate allows the Client to authenticate itself to a MCP. The Client certificate contains a **commonName** field.

To generate a Client certificate:

1. Launch XCA from the Windows Programs menu.
2. In the tree view of the **Certificates** tab, select the branch containing your Certification Authority.
3. Under the **Certificates** tab, click the **New Certificate** button.
4. Under the **Source** tab,
   a. Select **Use this Certificate for signing** checkbox. On the dropdown to the right of this checkbox, select the CA you created in section 2.1.2 (e.g., MyCA).
   b. Change the dropdown **Signature Algorithm** to **SHA 256**.
   c. Change the dropdown **Template for the new certificate** to "[default] HTTPS_client".
   d. Click **Apply all**.
5. Under the **Subject** tab, click the **Generate a new key** button**.**
6. In the dialog that appears:
   a. Type in a name that uniquely identifies the Client (for this example, that is **MyCA_client1**).
   b. Choose **Keytype** - **RSA**.
   c. Change the **Keysize** to 2048.
   d. Click **OK**.
7. Go back to the **Subject** tab and type in the Distinguished name of the Client certificate. The most important component is the ***commonName***.
   This is the name that the MCP is configured to accept. Any difference between the commonName of the Client certificate and the name configured in the MCP results in a failed connection.
8. Choose other name components that are appropriate for your company. Table 7 provides example distinguished name components.

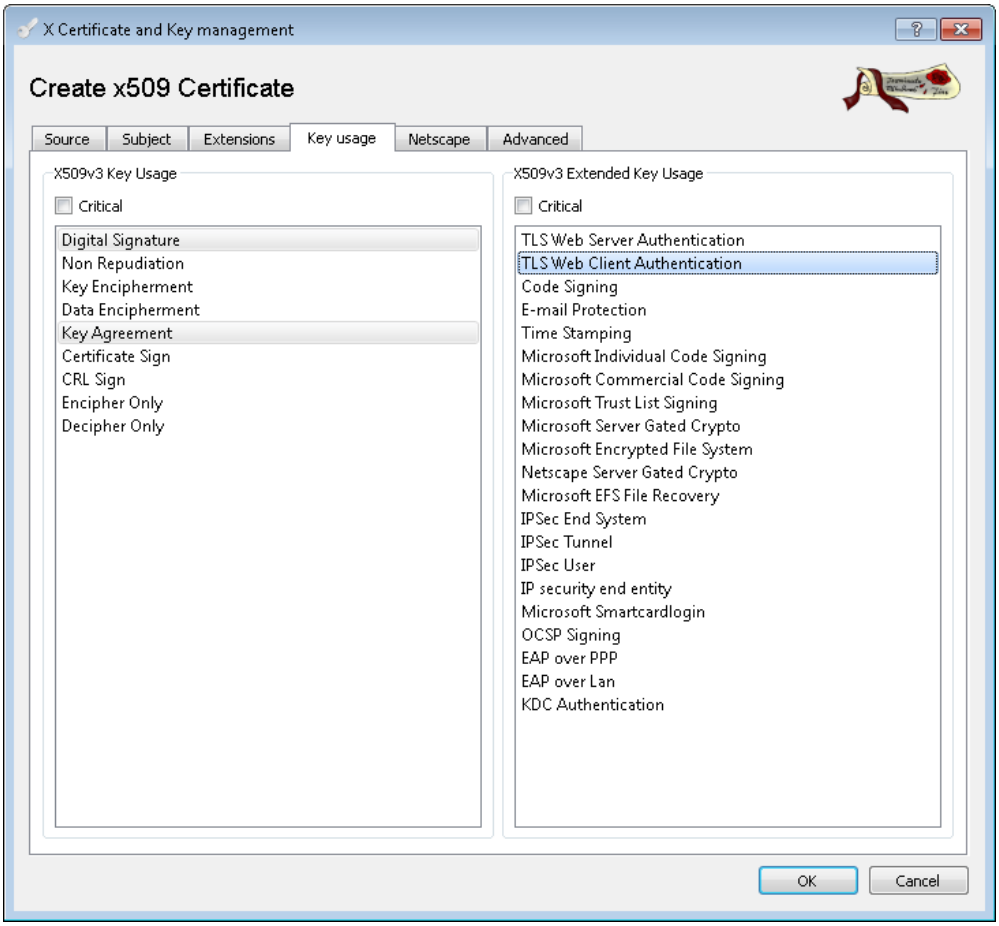
   Note: You must enter all components of the distinguished name, including the emailAddress.

Table 3 Example Distinguished Name Components

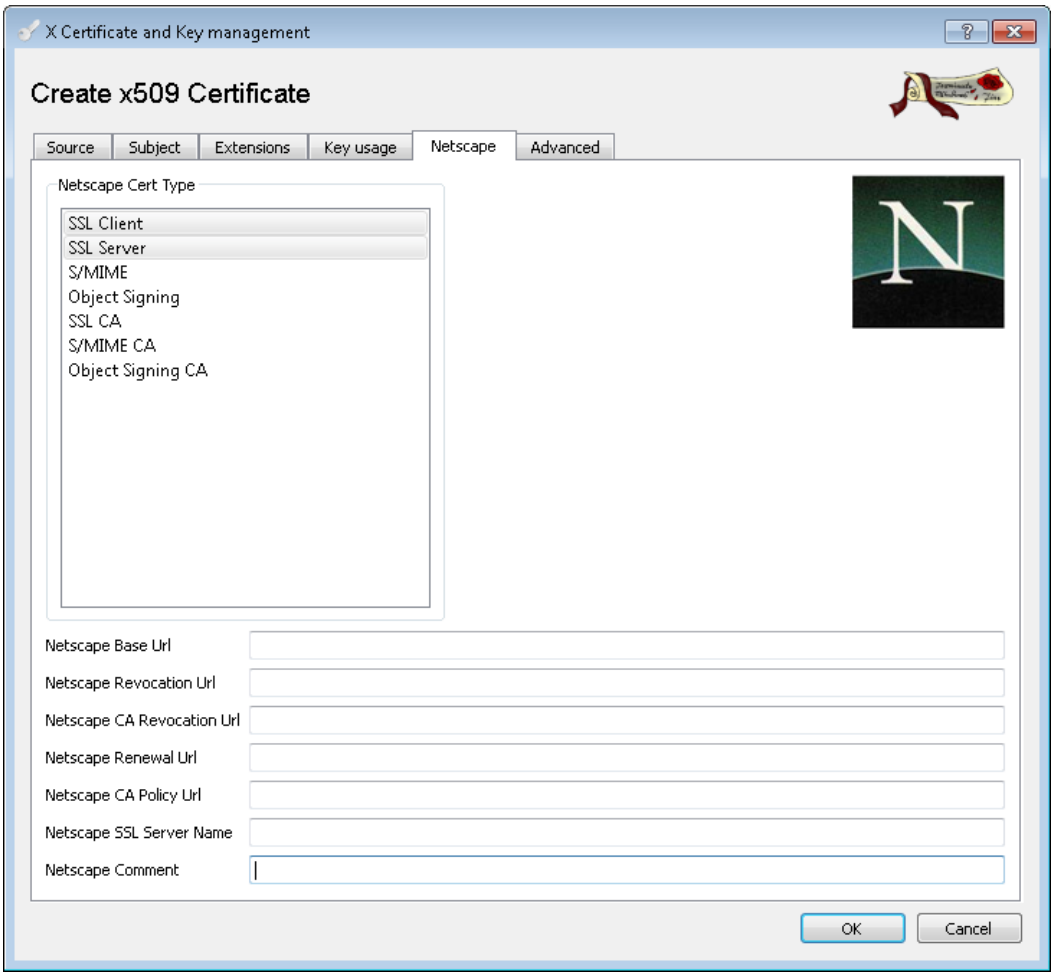
Distinguished Name Component	Example
Internal name	MyCA_client1
countryName	US
stateOrProvinceName	MyState
localityName	MyCity
organizationName	MyCompany
organizationalUnitName	MyDivision
commonName	MyCA_client1
emailAddress	mail@my.domain

9. Under the **Extensions** tab, if necessary, change the **Time Range** that the CA certificate is valid for and click **Apply**. The default is one year. The shorter the Time Range the more secure the certificate, but the more often you need to regenerate Client certificates and deploy them into Clients.

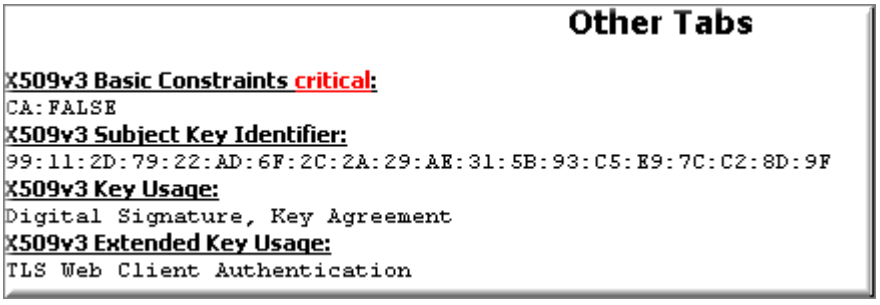
10. Under the **Key usage** tab, under X509v3 Key Usage select **Digital Signature** and **Key Agreement** and under X509v3 Extended Key Usage select **TLS Web Client Authentication** as shown below.



11. Under the **Netscape** tab, remove the **Netscape comment** and under the **Netscape Cert Type**. And, if **SSL Client** and **S/MIME** is selected then deselect them from the list.



12. Under the **Advanced** tab, click **Validate**. The following messages are expected except the value of the X509v3 Subject Key Identifier, which differs from key to key:



If above message does not appear, click **Validate** to view the message.

13. Click **OK**.
Result: You now have a Client certificate.

14. In the tree view of the **Certificates** tab, open the branch labeled with your Certification Authority and select the new Client certificate.

15. Click **Export.**

16. In the dialog that appears, ensure the **Export Format** field is set to "PKCS #12(*. p12)". Browse to a protected location **(e.g., My Documents->MyXCAFiles)** and click **Save**. Finally click **OK. A Password dialog will be prompted to enter the Password to encrypt the PKCS#12 file.** The client certificate and its private key are encrypted and stored in a file named with the Internal Name of your client certificate and the(*.p12) extension (e.g., MyName.p12).

17. The same password will need to be used to import "*. p12" file in the Windows Server/Windows PC in which VPN Client will be running.

NOTICE This file is sensitive so keep it protected at all times. Delete all copies of the file after it has been installed on the client.

4. Installing Certificates

This chapter describes how the CA Certificate, Server Certificate, Client Certificates and DH Parameters are installed. Table 4 summarizes where to get the files containing the CA certificate, Server certificates, Client Certificates and DH parameters.

Table 4 Location of Files Exported by Certification Authorities

Files	Location
CA Certificate	The CA certificate is in a file downloaded to a location of your choice as described in Section 2.1.2 . The file is named with a .crt extension (e.g., MyCA.crt).
Server Certificate and Key	Server certificate and key are in the same file under the location of your choice as described in Section 3.1.1 . The file is named with a. pem extension (e.g., MyMCP.pem).
DH Parameters	DH parameters are in the file named dh2048.pem under the location of your choice as described in Section 2.1.3 .

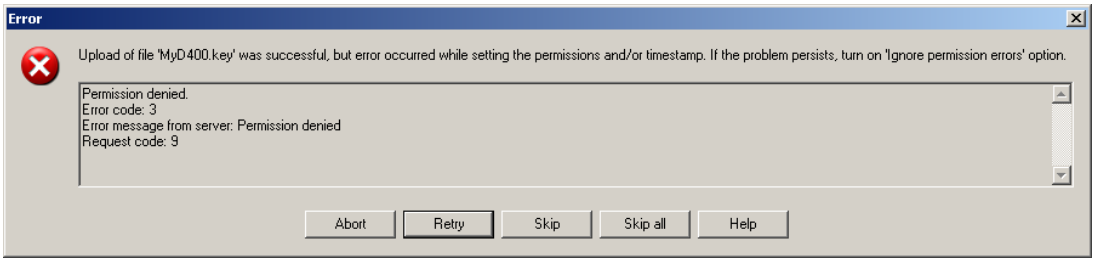
4.1 Installing CA Certificate, Server Certificate and Diffie Hellman Parameters on the MCP

1. Referring to Table 4 for file names and locations, copy the files containing the CA certificate, Server certificate, and DH parameters to one of two locations:
   - The folder /mnt/usr/SecureScadaTransfer on the MCP. In this case, use an SFTP/SCP file transfer program such as WinSCP or Secure File Browser from DS Agile MCP Studio (Refer to Appendix B in SWM0101 for details).
   - The directory \SecureScadaTransfer on a USB drive.

   Note: Do not install client certificates on the MCP.

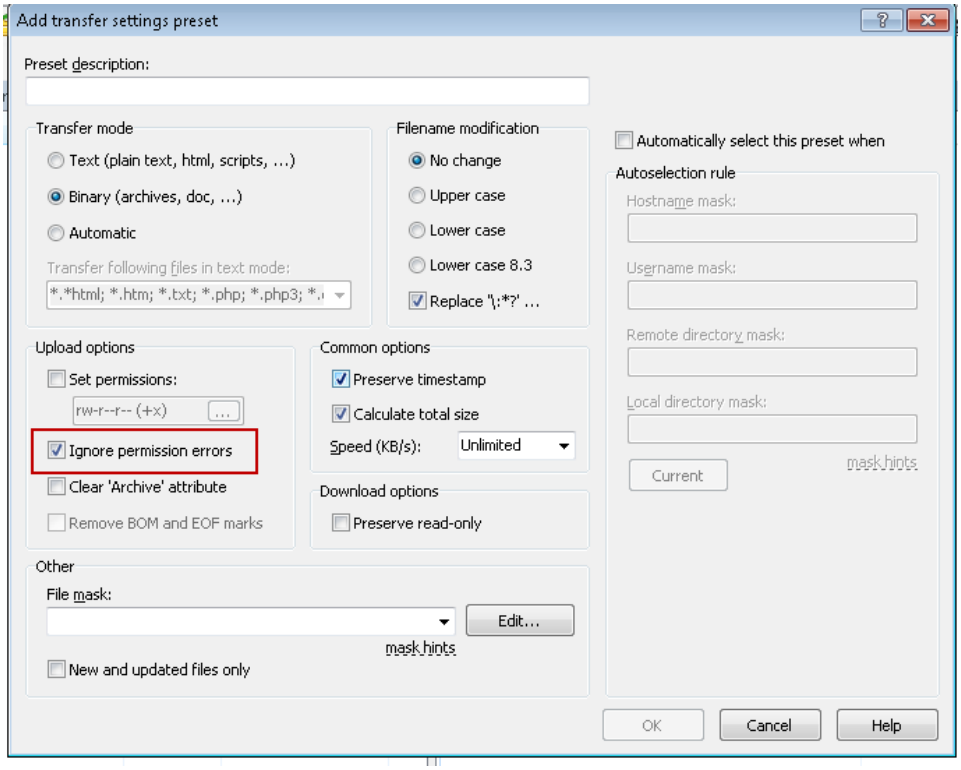
   NOTICE These files are sensitive, so keep them protected at all times. Delete these files from the USB drive after they have been installed on the MCP.

2. If you are using WinSCP or Secure File Browser from DS Agile MCP Studio (Refer to Appendix B in SWM0101 for details) to transfer the files, you may get the following warning message:



   The reason for this warning is that the MCP file system does not support per-file permissions, so when WinSCP or Secure File Browser from DS Agile MCP Studio(Refer to Appendix B in SWM0101/15 for details) tries to set the permissions on a file, it is unable to do so. However, there is no security risk because the file takes on the default permissions of the files system which are correct. Therefore, this warning can be safely ignored by clicking **Skip**.

3. To prevent this warning from appearing in the future, in WinSCP or Secure File Browser from DS Agile MCP Studio (Refer to Appendix B in SWM0101/15 for details) go to **Options** > **Preferences**. Then select **Transfer** and click **Ignore permission errors**.



4. If you are using the USB drive method of transferring the files, insert the drive into any USB slot on the MCP.
5. Connect to the MCP with a browser and click the Utilities tab under Settings option from the power bar.

   Note: This Option is available in Utilities Tab under Settings option from Local HMI or from the Connected Mode in DS Agile MCP Studio only.
6. Click the **Import** button.
   Result: A dialog box appears indicating that 1 Local Certificate and 1 Issuer Certificate was successfully imported. Click **OK** to dismiss the dialog.
7. Click the **Manage** button, and then click the **Local** tab.
   Result: A dialog box appears showing the Local certificate details in the Staged Local Certificates area.
8. Select the certificate and click **Install**.
   Result: The certificate moves into the Installed Local Certificate area. This also installs the DH parameters file.
9. Click the **Issuer** tab.
   Result: The CA certificate appears in the Staged Issuer Certificates area.
10. Select the row containing the CA certificate and click **Install**.
    Result: The certificate moves into the Installed Issuer Certificates area.
11. Close the dialog and log out of the MCP.

Note: If the MCP is part of a redundant system, follow the below steps.

1. Switchover to the Standby MCP.
2. Repeat steps 1 to 11.
3. Switchover back to the Original MCP.

4. Ensure the standby configuration is in sync with the active configuration (i.e., Standby Config Out of Sync DI = Config In Sync)
5. Reboot the standby MCP.

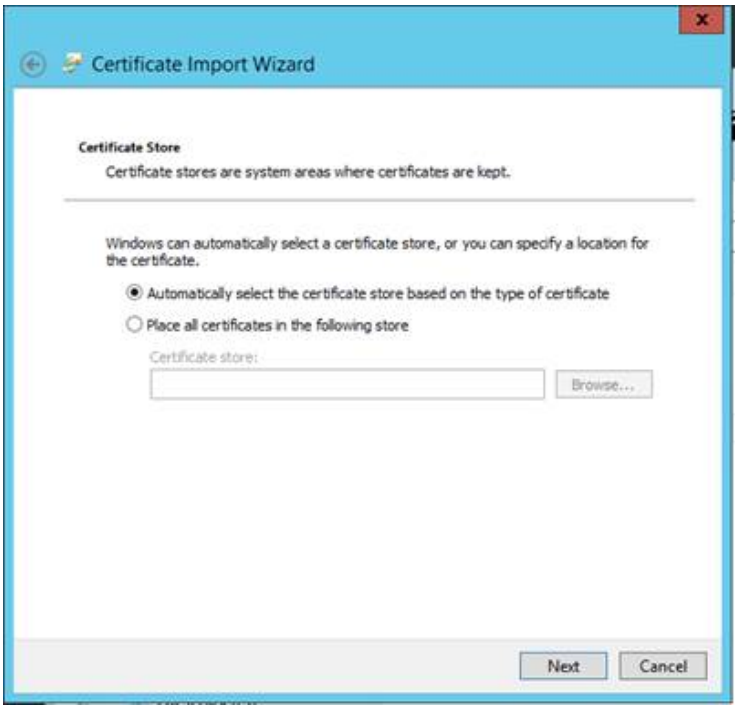
4.2 Installing Client Certificate in Windows Server 2012 R2

To import the "*. p12" file (encrypted PKCS#12 file that has Client Certificate + Private Key) into the Local Machine Store or Current User of Windows 2012 Server:

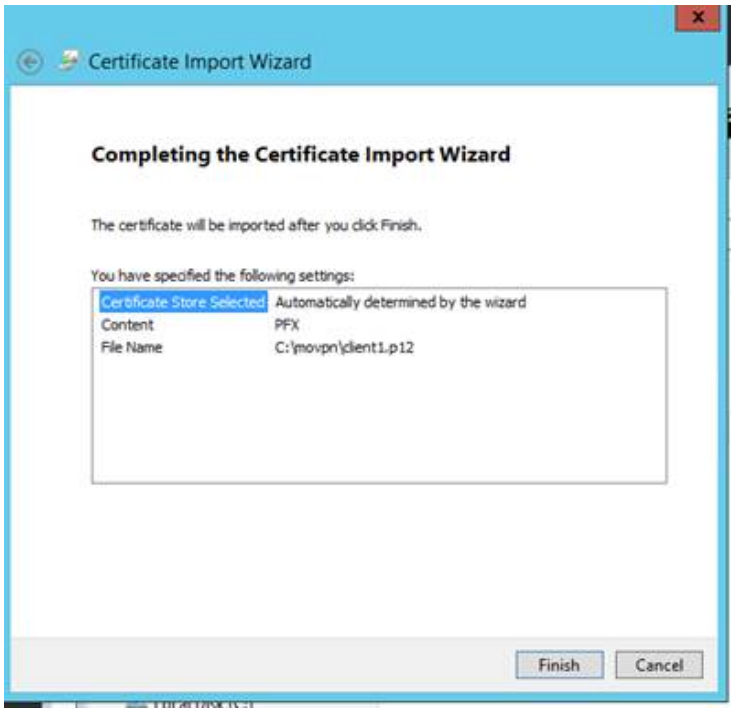
1. Securely Copy the "*. p12" (e.g., MyName.p12) file to the Windows 2012 R2 Server where VPN client will run.
2. Right-click on the" *. p12" file and select option: **Open with -> Crypto Shell Extensions**.
3. If you are running OpenVPN as a service, select **Local Machine**.
   Otherwise, select **Current User**.

4. Click **Next** > **Next**.
5. Enter the same password that was used to encrypt the "*. p12" file as part of Client Certificate + Private Key creation using XCA tool (Refer to Section 3.1.2).
6. It is recommended that you do not select **Mark this key as exportable** as shown below.
7. Select option **Include all extended properties** as shown below.
8. If you are running OpenVPN as a service, the option **Enable strong private key protection** is not available as shown below. If you are running OpenVPN as a user, select option **Enable strong private key protection** for added protection.

9. Click **Next**.
10. Select option: **Automatically select the certificate store based on the type of certificate**.



11. Click **Next**
    Result: An operation summary appears.



12. Click **Finish**.
    Result: A message appears, indicating that the import was successful.
13. Click **OK**.
    Result: The client certificate should now be in the local machine store.

NOTICE Delete the "*. p12" file on the file system because it is sensitive and no longer required to be on the file system.

4.3 Installing Client Certificate in Windows 7 PC

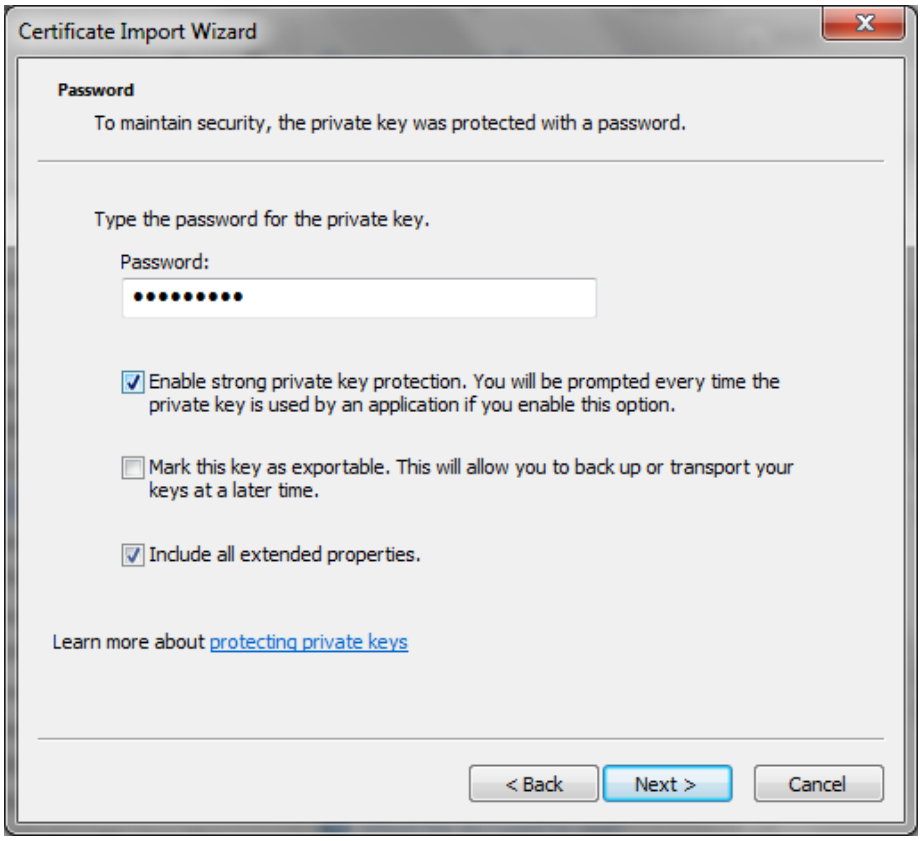
To import the "*. p12" file (encrypted PKCS#12 file that has Client Certificate + Private Key) into a Windows 7 PC:

1. Securely Copy the "*. p12" (e.g., MyName.p12) file using SCP/SFTP or USB into Windows 7 PC where VPN client will run.

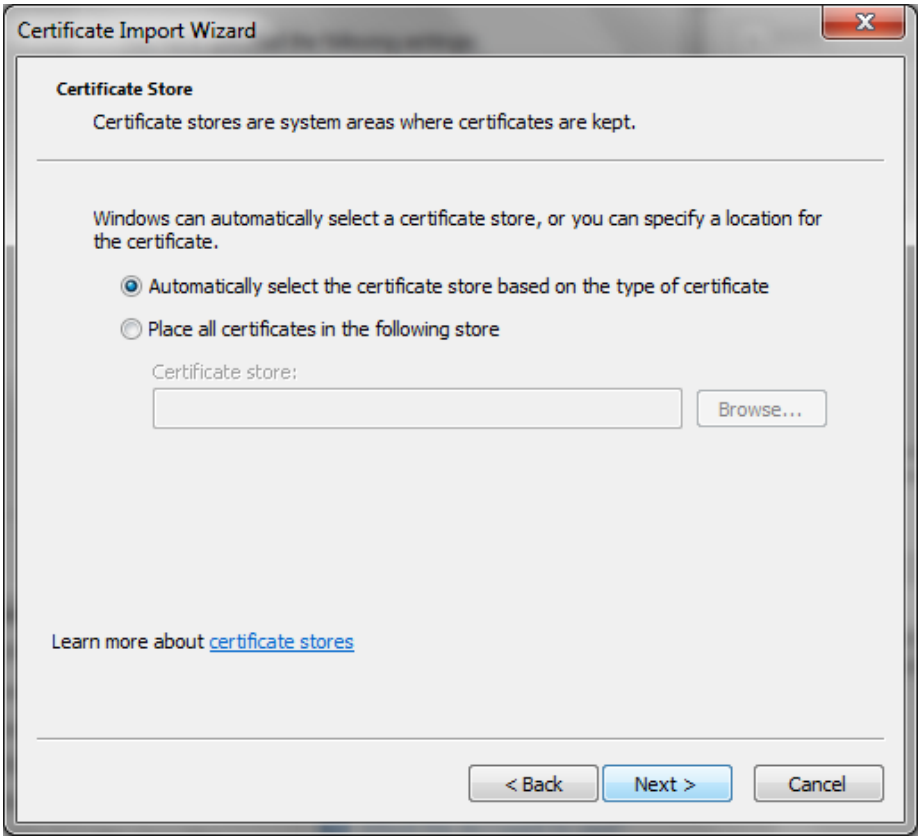
2. Double-click on the" *. p12" file.
   Result: The Certificate Import Wizard window appears.

3. Click **Next** > **Next**.
4. Enter the same password that was used to encrypt the "*. p12" file as part of Client Certificate + Private Key creation using XCA tool (Refer to Section 3.1.2).
5. It is recommended that you do not select option: **Mark this key as exportable** as shown below.
6. Select option: **Include all extended properties**.

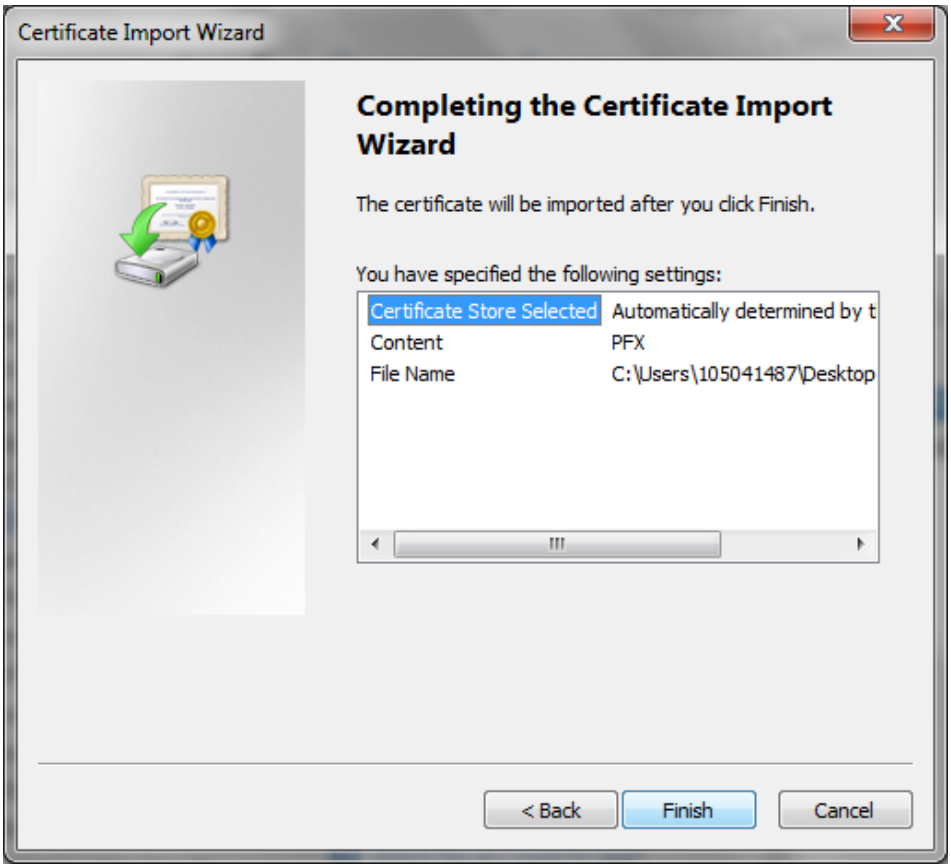
7. Select option: **Enable strong private key protection** for added protection.



8. Click **Next**.
9. Select option: **Automatically select the certificate store based on the type of certificate**.



10. Click **Next**
    Result: A summary of the operation appears.



11. Click **Finish**.

    Result: The following window appears.

12. Click **OK**.

    Result: A message appears, indicating that the import was successful.

13. Click **OK**.
    Result: The client certificate should now be in the local machine store.

NOTICE Delete the "*. p12" file on the file system because it is sensitive and no longer required to be on the file system.

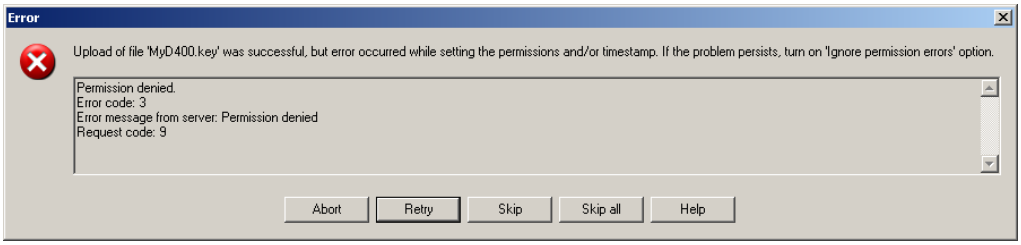
4.4 Installing Chain of CA Certificates on the MCP

1. Referring to Table 4 for file names and locations, copy the files containing the CA certificate, Server certificate, and DH parameters to one of two locations:
   - The folder /mnt/user/SecureScadaTransfer on the MCP. In this case, use an SFTP/SCP file transfer program such as WinSCP or Secure File Browser (Refer to Appendix B in SWM0101 for details).
   - The directory \SecureScadaTransfer on a USB drive.

   Note: Do not install client certificates on the MCP.

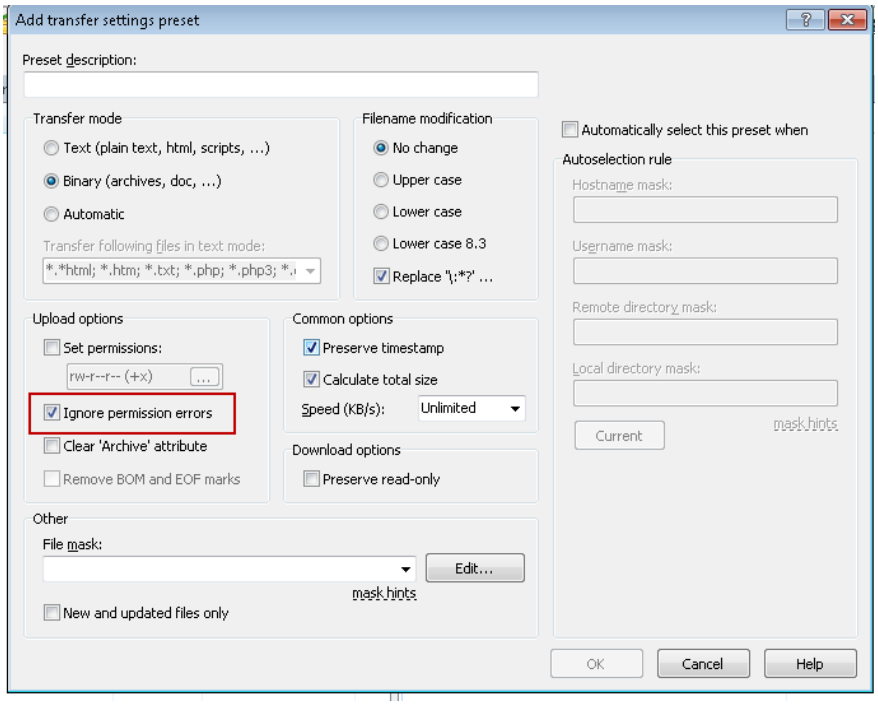
   NOTICE These files are sensitive, so keep them protected at all times. Delete these files from the USB drive after they have been installed on the MCP.

2. If you are using WinSCP or Secure File Browser from DS Agile MCP Studio (Refer to Appendix B in SWM0101 for details) to transfer the files, the following warning message may appear:



The reason for this warning is that the MCP file system does not support per-file permissions, so when WinSCP or Secure File Browser from DS Agile MCP Studio(Refer to Appendix B in SWM0101 for details) tries to set the permissions on a file, it is unable to do so. However, there is no security risk because the file takes on the default permissions of the files system which are correct. Therefore, this warning can be safely ignored by clicking **Skip**.

3. To prevent this warning from appearing in the future, in WinSCP go to **Options** > **Preferences**. Then select **Transfer** and click **Ignore permission errors**.



4. If you are using WinSCP or Secure File Browser from DS Agile MCP Studio (Refer to Appendix B in SWM0101 for details) then copy all the CA certificates files in the chain, Server certificate, and DH parameters to folder "/mnt/usr/SecureScadaTransfer" on the MCP.
5. If you are using the USB drive method of transferring the files, insert the drive into any USB slot on the MCP.
6. Connect to the MCP with a browser and click the Utilities tab under Settings option from the power bar.

   Note: This is available in Utilities Tab under Settings option from Local HMI or from the Connected Mode in DS Agile MCP Studio only.
7. Click the **Import** button.
   Result: A dialog box appears indicating that 1 Local Certificate and a list of all Issuer Certificates in the chain will be successfully imported. Click **OK** to dismiss the dialog.
8. Click the **Manage** button, and then click the **Local** tab.
   Result: A dialog box appears showing the Local certificate details in the Staged Local Certificates area.
9. Select the certificate and click **Install**.
   Result: The certificate moves into the Installed Local Certificate area. This also installs the DH parameters file.
10. Click the **Issuer** tab.
    Result: All the CA certificates in the chain appear in the Staged Issuer Certificates area.
11. Select all the CA certificates in the chain and click **Install**.
    Result: The certificates move into the Installed Issuer Certificates area.
12. Close the dialog box and log out of the MCP.

NOTICE If a chain of certificates is being used, all the certificates in the chain must be installed.

Note:

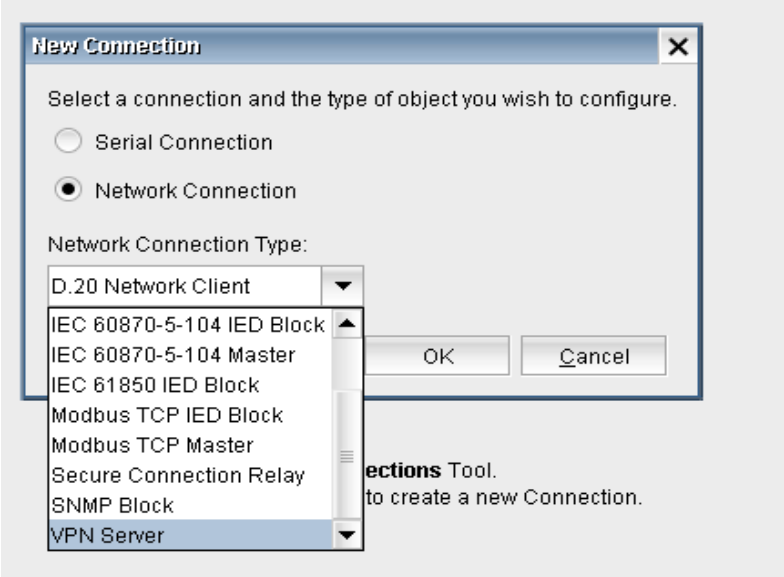
In a redundant system (not supported in MCP) :

1. Switchover to the Standby MCP.
2. Repeat steps 1 to 12.
3. Switchover back to the Original MCP.
4. Ensure the standby configuration is in sync with the active configuration (i.e. Standby Config Out of Sync DI = Config In Sync)
5. Reboot the standby MCP.

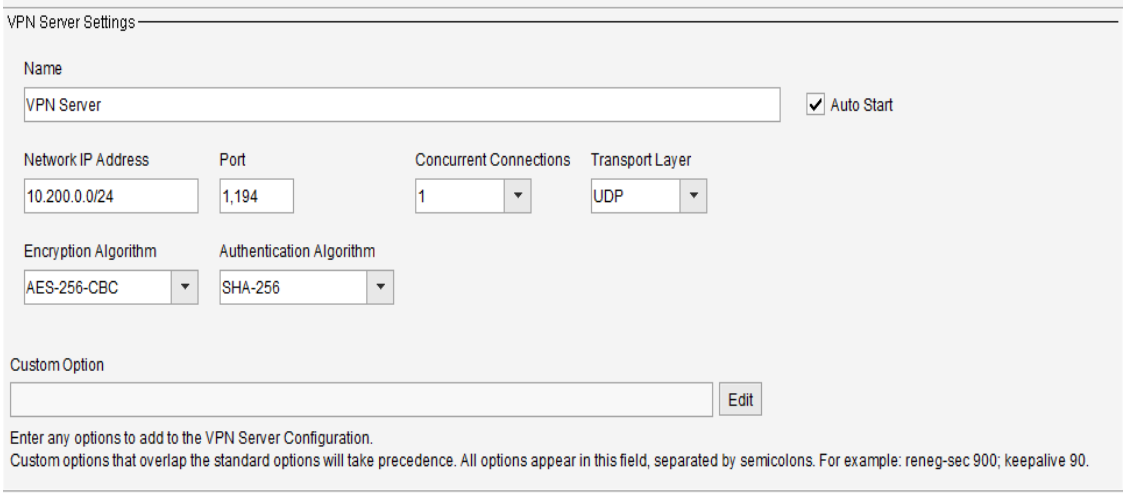
5. Configuring VPN in MCP

5.1 Configuring VPN Server

1. Login to MCP Online GUI as an Administrator user. Only users with administrator rights can configure and view OpenVPN configuration as shown below.
2. Go to Utilities tab under Settings option and install CA and Server Certificates – refer to Section 4.1
3. Go to the **Configuration** tab in DS Agile MCP Studio and then select **Network Connection** and Network Connection Type: **VPN Server**.



4. Configure the VPN Server settings as shown below.



Note: Refer to Table 5 for a description of each setting in the VPN Server configuration.

Table 5 VPN Server Configuration Parameters

Setting	Description	Range	Default
Name	Unique name for the VPN Server.	Text string 32 characters are allowed	VPN Server

Setting	Description	Range	Default
Auto Start	Indicates if the application automatically starts when the configuration is changed and reloaded or when the MCP re-boots.	Disabled Enabled	Enabled
Network IP Address	IP address of the device. Must be unique from other configured devices.	Valid IPv4 address and subnet mask. The supported subnet mask range is from 16 to 31 only.	10.200.0.0 /24
Port	The port number on which the device communicates.	0 to 65535	1,194
Concurrent Connections	The number of allowed concurrent connections.	1, 2, 3	1
Transport Layer	The transport layer protocol; either: • Transmission Control Protocol (TCP), or • User Datagram Protocol (UDP)	TCP UDP	UDP
Encryption Algorithm	Mathematical formula used in encryption and decryption of the VPN communication.	List of encryption algorithms. AES-256-CBC AES-256-CFB1 AES-256-CFB8 AES-256-OFB AES-192-CBC AES-192-CFB1 AES-192-CFB8 AES-192-OFB CAMELLIA-256-CBC CAMELLIA-256-CFB CAMELLIA-256-CFB1 CAMELLIA-256-CFB8 CAMELLIA-256-OFB CAMELLIA-192-CBC CAMELLIA-192-CFB CAMELLIA-192-CFB1 CAMELLIA-192-CFB8 CAMELLIA-192-OFB	AES-256-CBC

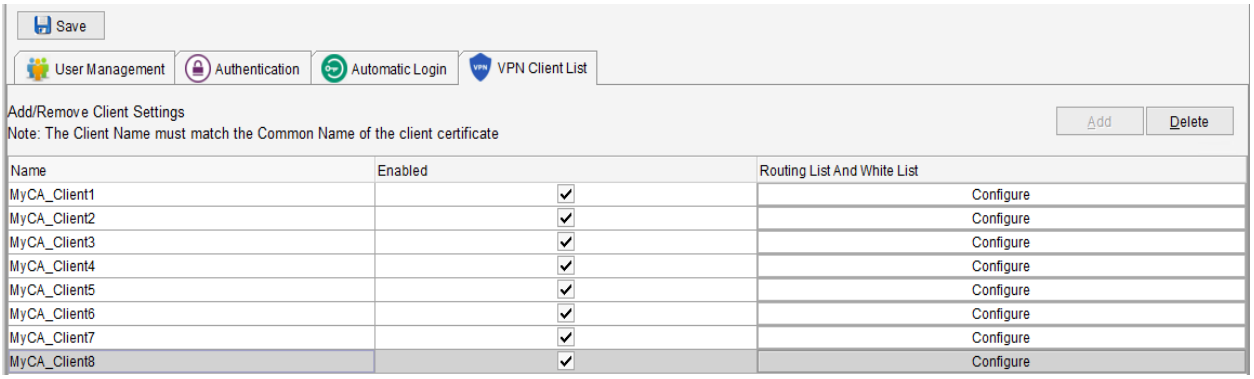
Setting	Description	Range	Default
Authentication Algorithm	Authentication is the process of verifying the encrypted data was sent by the sender and was not altered.	List of authentication algorithms. SHA1-160 SHA-160 RSA-SHA1-160 RSA-SHA2-160 RSA-SHA-160 DSA-SHA1-160 DSA-SHA1-old-160 DSA-SHA-160 DSA-160 RIPEDMD160-160 RSA-RIPEDMD160-160 ecdsa-with-SHA1 SHA-224 RSA-SHA-224 SHA-256 RSA-SHA-256 SHA-384 RSA-SHA-384 SHA-512 RSA-SHA-512 whirlpool-512	SHA-256
Custom Option	Enter any options to be added to the VPN Server Configuration. All options appear in this field, separated by semicolons. To edit this field: 1. Click the **Edit** button. Result: The Configure Custom Option window appears. 2. Click the **Add** button. Result: A line appears as a Custom Option. 3. Type in the option text. 4. Click **Save**. ***NOTICE*** **Custom Options are advanced options and take precedence over the standard configuration options. The standard options are secure by default. Implementing custom options can impact the security strength (e.g. using weak ciphers such as DES*, RC2-*, and BF-*). The customer assumes risk of weakened security when implementing custom options. Consult the online OpenVPN literature for guidance.**	Text string For example: • reneg-sec • tun-mtu 1500 ; mssfix 1300 • fragment 1400; • mssfix • tls-cipher TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA • socket-flags TCP_NODELAY • push "socket-flags TCP_NODELAY	blank

5. Save the VPN Server configuration and apply configuration commit to apply these changes.
   Result: VPN Server files are saved in the directory "/etc/openvpn/".

5.2 Configuring VPN Client Parameters

1. Connect as Administrator to the MCP device through Online Editor (i.e. Connect mode) in DS Agile MCP studio, navigate to the **Access** tab and then select **VPN Client List tab** to configure the VPN client, Routing and White list as shown below.

   Note: VPN Client Configuration can also be done by an Administrator through MCP Runtime HMI (Remote or Local) by navigating to the Access tab and then select the VPN Client Configuration tab.

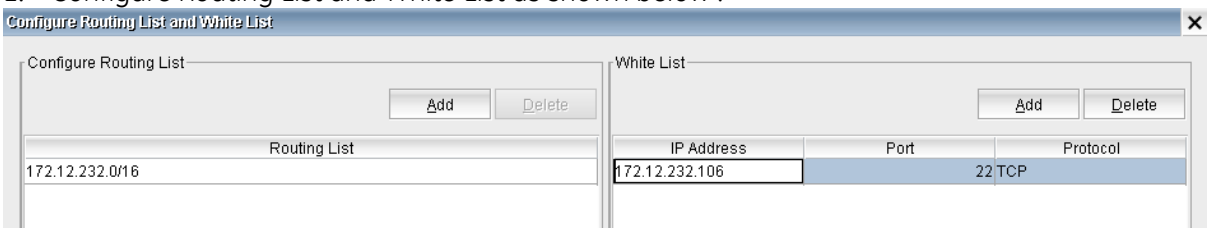


   Note: Refer to Table 6 for a description of each setting in the VPN Client Configuration.

Table 6 VPN Client Configuration Parameters

Setting	Description	Format	Example
Client Name	The client's common name. Note: This name must match the Common Name of the client certificate.	Text string 32 characters are allowed	Client1
Enabled	Selected if the Client is enabled. Not selected if the Client is disabled	Enabled Disabled	Enabled
Routing List and White List:	Click **Configure** to access the Configure Routing List and the White List.		

2. Configure Routing List and White List as shown below :



Note: Refer to the Table 7 for description of each of the Routing List and White List parameters.

Table 7 Routing List and White List

Setting	Description	Format	Example
Routing List	Drop down list of Route IP address &Subnet Mask in CIDR notation. **Note**: Routing List consist of list of configured networks (including VLANs & PRP) in MCP. This list can't be edited by the User.	Valid IP4 Address/Netmask	172.12.232.0/16
White List	"IP/Port/Protocol Whitelist" for each VPN client to allow the incoming connections based on the combination of destination IP address, protocol and Port number through VPN tunnel.	**IP Address:** Valid IP4 Address **Port No:** Valid TCP/UDP Port Number **Protocol:** From the below drop-down list: • TCP • UDP • TCP+UDP • Any ICMP • Useful ICMP • Useful ICMP+ Ping **ICMP Type/Code allowed combinations are described in Table 8 ICMP White List Options.**	IP Address: 172.12.232.106 Port: 22 Protocol: TCP

Note: Port Number is available for TCP, UDP and TCP+UDP protocols only in White List configuration.

Table 8 ICMP White List Options

ICMP White List Option	Type	Code
Any ICMP	All	All
Useful ICMP and Useful ICMP + Ping	3 (Destination Unreachable)	All
	0 (Echo reply)	0
	11 (Time Exceeded)	0 (TTL expired in transit)
	11 (Time Exceeded)	1 (Fragment reassembly time expired)
Useful ICMP + Ping	8 (Echo request)	0

3. Save the VPN Client configuration parameters by applying Save button.
   Result: All VPN Client configuration files are saved in the directory "/etc/openvpn/".

Notes: A static network route must be configured in each unique destination device referenced in all of the configured whitelists.

The route must be specified as follows:

Route Destination: The Network IP Address of the MCP's VPN Server Configuration.

Route Network Mask: The network mask of the Network IP Address of the MCP's VPN Server Configuration.

Route Gateway: The IP address of the MCP interface that is reachable by the destination device. In the case of Redundant system (not supported in MCP), it would be Active IP address of the device interface that is reachable by the destination device.

5.3 VPN Server Log

MCP HMI provides support for VPN Server Log available to Administrator Users. This Log is available under System Logs button and can be used for diagnostic purposes.

This log is also available from the MCP command prompt for Administrator or Root Users and can be accessible using command:

sudo tail –f /var/log/D400/openvpn.log

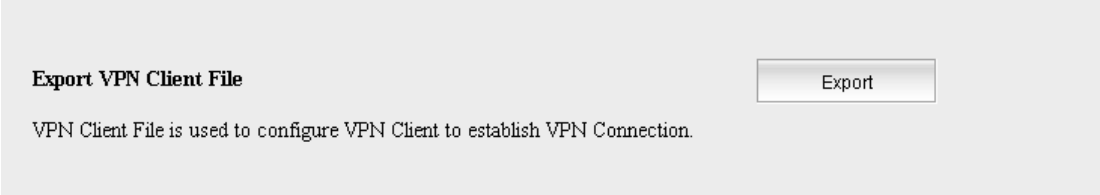
Refer to Appendix B for troubleshooting guide based on messages in this log.

6. Exporting VPN Client Configuration

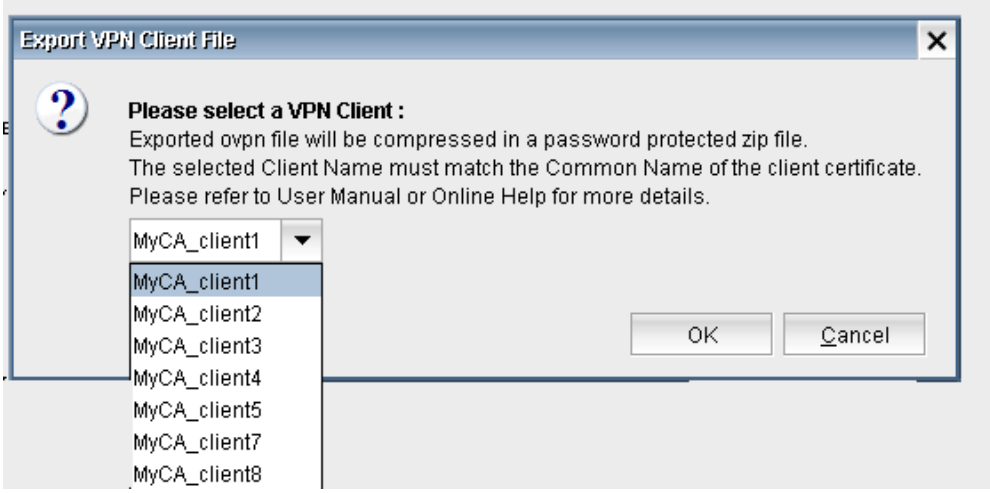
The VPN client configuration file is generated by MCP. This client configuration is archived with password protection into a file and exported into a PC or a shared location using option Export VPN Client File from the Utilities tab under Settings options as described below.

To export a VPN Client file:

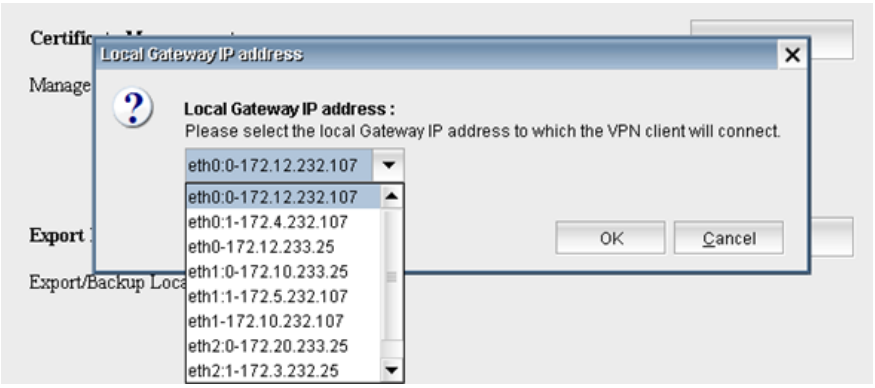
1. Go to Export VPN Client File option and click the **Export** button.



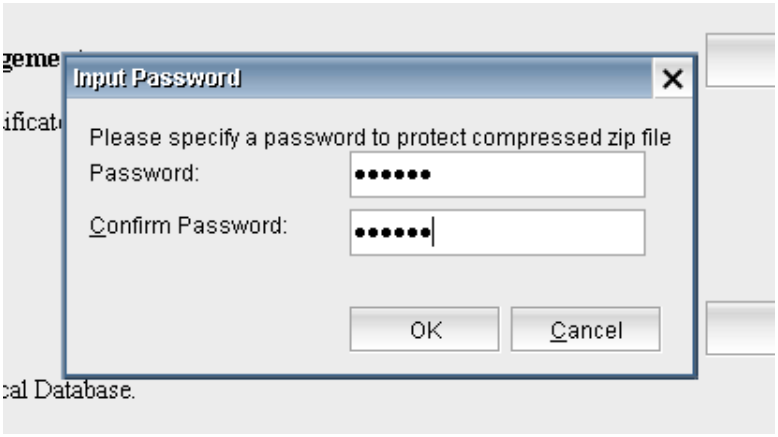
2. Select the Client from configured drop-down list of configured Clients.



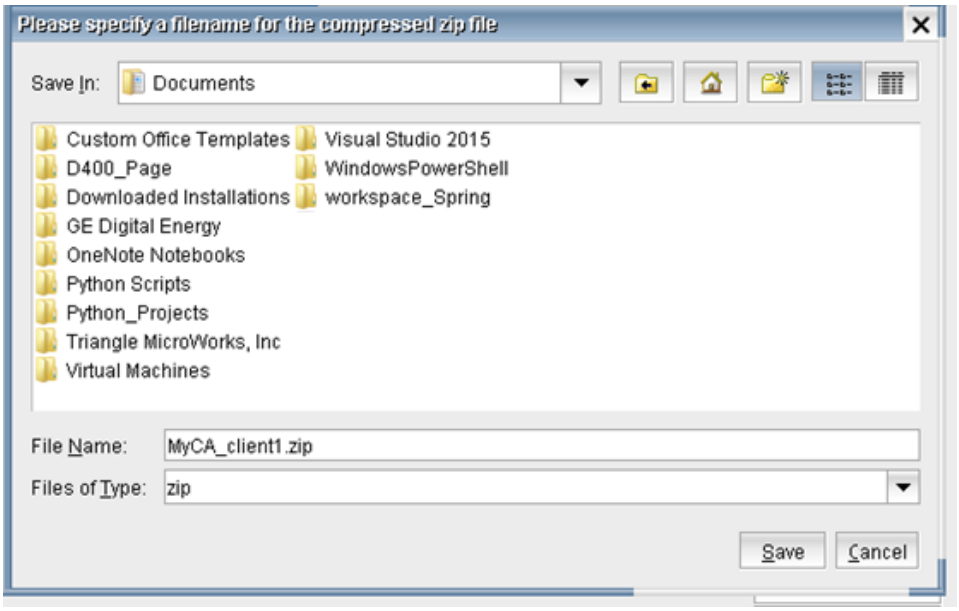
3. Select the Local Gateway IP address to which VPN Client will need to connect from the list of Configured IP address of MCP.



4. Enter the Password to save the Client Configuration file in protected &compressed format. You need to use the same password to uncompress the Client configuration file using 7Zip or WinRAR software.



5. Securely save the file into a PC/Shared Location/USB.

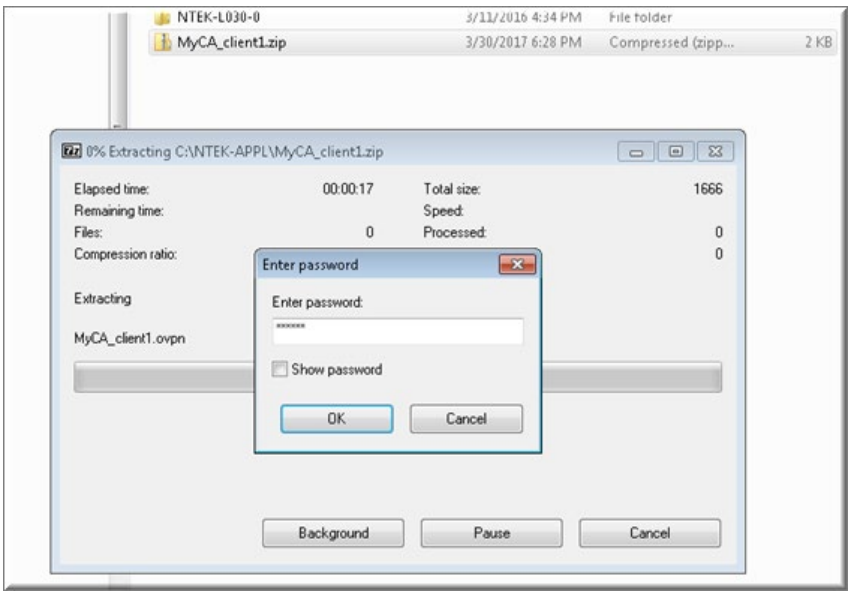


Note: Exporting VPN Client Configuration options is also available through File Explorer functionality in Local HMI. The compressed Client Configuration file is available in the USB.

NOTICE If exporting of a VPN client configuration file fails due to certificate errors, refer to **Appendix A: Certificate Error Messages Logged by OpenVPN Configuration** for details about these error messages.

7. Configuring OpenVPN Client

1. Download OpenVPN Client software from the below link
   https://openvpn.net/index.php/open-source/downloads.html
2. Install OpenVPN client software on Windows 7 PC or Windows 2012R2 Server.
3. After installation, the OpenVPN Client Configuration is present at the below folder.
   C:\Program Files\OpenVPN\config.
4. Download 7zip or WINRAR software from the below links and install on Windows 7 PC or Windows 2012R2 Server.
   www.7-zip.org/download.html
   www.win-rar.com/download.html
5. Use either 7zip or WINRAR software uncompressing the password protected zip file generated in step 5 of Chapter 6. and copy the contents of the uncompressed file into this configuration folder:
   C:\Program Files\OpenVPN\config\



NOTICE It is important to install ".pk12" (Client Certificate + Private Key) before importing VPN Client Configuration into a Windows® Server 2012 or a Windows 7 PC.

6. You can start OpenVPN client as a Service on system startup in Windows 2012 R2 Server or Windows 7 PC as follows:
   a. Run the Windows Service administrative tool:
   b. Press **Windows Key + R**
   c. Type **services.msc** and press **Enter**.
   d. Find the OpenVPN service and set its Startup Type to "automatic."
   e. Optionally, start the service now.

   OR

   If OpenVPN client could not start automatically on system startup in Windows 2012R2 Server or Windows 7 PC, then use NSSM (Non-Sucking Service Manager) Utility to start the OpenVPN client at system startup. Refer to Chapter 8.

7. OpenVPN client can run from GUI manually in Windows 2012R2 or Windows 7 PC. Refer to instructions in the below link to start OpenVPN Client from OpenVPN GUI.

   https://community.openvpn.net/openvpn/wiki/OpenVPN-GUI

The contents of the Client VPN Configuration file for Windows® Server 2012 or Windows 7 PC appears similar to the example shown below:

```
# Automatically generated OpenVPN client config file
# Note: this config file contains inline private keys
#       and therefore should be kept confidential!
client
proto udp
remote 172.12.232.72
port 1194
nobind
dev tun
persist-key
persist-tun
keepalive 10 60
comp-lzo no
auth SHA1
cipher AES-256-CBC



<ca>
-----BEGIN CERTIFICATE-----
MIIC1DCCAbygAwIBAgIBATANBgkqhkiG9w0BAQUFADANMQswCQYDVQQDEwJDQTAe
Fw0xNzA0MjAyMTU0MDBaFw0yNzA0MjAyMTU0MDBaMA0xCzAJBgNVBAMTAkNBMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAq1FoIWlAvmFHlsaZAAuOv65E
cpFLbQL3DhnE4/FOqSTPXSabBMu7IwtJPSPkBnmE8u4owttapLWoYE/D+zFvbPls
mfzbG6kbs2q/bnWKm5mX+oMa1gGBxjBktz64r/GR5uPe7UiF1CsfFBK/q+UzgpnR
WT+6y2OxIA8cOWZPtNpnTHd6/GbpM+J2OKrs3QhvV8y3YRj/BW/JAJQI/HEHIl8m
jNBszfGgTWYgotqfZcgZM9dPbi63B7ZYbhDOOgTUPKw2ojl+6zATvazy3cB6XasM
5APcWYqe6UOIc/mZH7iJ+OQuIzeroggdGYeNEoV4zF3IeyeJo9XHFm/+P3SZCQID
AQABoz8wPTAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBR4mvXf2gFYkkWFIxCj
vMItCRN7BTALBgNVHQ8EBAMCAQYwDQYJKoZIhvcNAQEFBQADggEBAJnlD+u9IYS2
bbW3Jl3gvbb/Fsp6QLoCT/xxxxXbctE4mQ2xSXfFmukUFL1GDbvKpgnbBRS22O/J
Pafjb1fAIuivunOgIeJMoKAADAT82OhUB48IdG9WDFwFI2U1O7XHZW2SsD7u/mPR
L+bynNhs6BqVRopjXgRIVyNdLcmFYIBNLV7xshLYpUeuCmZ1HD2xkODgBk5UcNNu
mKzeCM4h4CEVc79z+djnQAOsi1a3HpayHiKUfszpAprnpeDWcQ8VGsFQZWzV53m/
+mBcOkpQVLgN/DoCCWtYc1jFuTleY+Iz8kCzVSM6QlIarIcIE1p/mjCQKPsMfM7y
coe358PnPcU=
-----END CERTIFICATE-----
</ca>


remote-cert-tls server
key-direction 1
<tls-auth>
```

```
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
7e76e4562b001b50ab1c3fae9710f9c0
9405c3915dfea68121 0ca2f1290a7383
a9b2c153a7548374a4d6ad25325c3579
cefd0c9a20426ca96077811b7e40df49
1b37829b866dd027f0855bd0b9326206
68db25bfb3b11a70469fe8f100970993
23adca22708ed4e1afce43e3137f041b
fee8278e3710d0ae3b63720b0b81fc12
7937020679b9e56b55d8e4b240942ea7
1bf5969181e102e07b4f4b285e6cb0ed
0acc1998f8fb3a1c439cc2300eb77043
3d39bc5502a6d1a6b46f2ee193b68767
1cbf12cd7472e2d31f3f52e73fa487f0
1bd7a1a8d57e23cd57fb43532624df2a
7584f316a0d7268a60ec15e419293523
9060b8c2cb98459e594f006ec9b40159
-----END OpenVPN Static key V1-----
</tls-auth>
cryptoapicert "SUBJ:MyClient1"
```

Note: If <tls-auth> key is missing in the client configuration file then it is likely because the Netscape Cert Type is used in the MCP Server Certificate. Refer to step 11 section 3.1.1 Generating a MCP Server Certificate on page 16 for how to remove Netscape Cert Type from the MCP Server Certificate.Server & Client Certificate Generation You also would need to remove the Netscape Cert Type from the Client Certificate. Refer to step 11 in section 3.1.2 on page 21 for how to remove Netscape Cert Type from the Client Certificate.

8. Revoking a Client certificate

All certificates are issued for a restricted time period of validity. However, it can happen that a certificate should not be used or has become invalid before its expiry date. In this case, the issuing CA should revoke this certificate by putting it on the list of revoked certificates (CRL) and publishing it.

Together with a private key and a certificate, a client device can prove its identity to the MCP. If a malicious user ever discovered your private key, the malicious user would be able to access the MCP masquerading as you. The moment you are aware of a security breach that may involve the private key, you should revoke the associated certificate. If a certificate is revoked, the MCP does not accept any connections that use a revoked certificate.

Another reason for revoking a certificate may be that the owner of the certificate has left the company and no longer needs to connect to the MCP. Revoking the certificate prevents that person from accessing the MCP even if the person retained his or her private key.

To revoke a certificate:

1. Revoke the certificate on the CA 8.1.
2. Generate a new Certificate Revocation List (CRL) – See section 8.2.
3. Install the CRL on the MCP – See section 8.3.
4. OpenVPN server configuration, Save and Commit changes to reflect new CRL changes.

8.1 Revoking the Certificate in XCA

To revoke the certificate in XCA:

1. Launch XCA from the Windows Programs menu.
2. In the tree view under the **Certificates** tab, open the branch containing your Certificate Authority.
3. Select and right-click the Client certificate to be removed (e.g., MyName).
4. Click **Revoke** option from the right-click menu.
5. Provide the date of revocation under field **Invalid Since** and reason for revocation from the dropdown list **Revocation Reason**.
6. Click **OK**.

8.2 Exporting the CRL in XCA

To export the CRL in XCA:

1. In the tree view under the **Certificates** tab, right-click the branch containing your Certificate Authority (e.g., MyCA).
2. Select the **CA** option in the right-click menu, and then option **Generate CRL**.
3. Under the **Dates** section, leave the **last update** as today's date.
4. Choose a date for **next update** when you want to update CRL next time to the MCPs. If there is no planned date for next update, you can choose the expiry date of CA certificate as date for **next update.** Note: you can optionally use **Year/Month/Day** field and **Apply** to quickly change next update date.
5. Change the dropdown **Hashing Algorithm** to **SHA 256**.

6. Under the **Extensions**, leave the fields **CRL Number** and **Revocation reasons** checked. Leave the field **Authority key identifier** unchecked.
7. Click **OK**.
8. Under the **Revocation List** tab, select the CRL labelled as your Certificate Authority (e.g., MyCA). Verify that **Next update** field is set to what you have chosen in step 4.
9. Click **Export**.
10. In the dialog that appears, ensure the **Export Format** field is set to PEM. Browse to a protected location (e.g., My Documents->MyXCAFiles) and click **Save**. The file is named based upon the internal name of your CA with a ".pem" extension. Append "_CRL" to filename to indicate that this file is a CRL (e.g., MyCA_CRL.pem). Finally click **OK.**

8.3 Installing the CRL in the MCP

To install the CRL in the MCP:

1. Copy the CRL file generated in section 8.2 to one of two locations:
   - The folder /mnt/user/SecureScadaTransfer on the MCP. In this case, use an SFTP/SCP file transfer program such as WinSCP or Secure File Browser from DS Agile MCP Studio (Refer to Appendix B in SWM0101 for details).
   - The directory \SecureScadaTransfer on a USB drive.
2. If you are using the USB drive method of transferring the files, insert the drive into any USB slot on the MCP.
3. Connect to the MCP with a browser and click the Utilities tab under Settings options from the power bar.

   Note: This Option is available in Utilities Tab under Settings option from Local HMI or from the Connected Mode in DS Agile MCP Studio only.
4. Click the **Import** button. You should see a dialog indicating that 1 CRL was successfully imported. Click **OK** to dismiss the dialog.
5. Click the **Manage** button, and then click the **CRL** tab.
   Result: A dialog appears showing the CRL details in the Staged CRLs area.
6. Select the CRL and click **Install**.
   Result: The CRL moves into the Installed CRLs area.
7. Close the dialog and log out of the MCP.

9. Running OpenVPN Client as Windows Service using NSSM

Download the latest version of NSSM (Non-Sucking Service Manager) from link:

http://nssm.cc/download

NOTICE The following procedure is reproduced with permission from Peter Senft at http://www.rfc3092.net/. Peter's original blog can be found at http://www.rfc3092.net/2015/08/openvpn-windows-service-foo/.

9.1 How to install NSSM

NSSM does not come with a Windows Server 2012 R2 installer.

To install NSSM:

1. Create a folder; for instance, in your "Program Files" directory (or whatever directory name %PROGRAMFILES% represents).
2. Depending on your operating system, copy the win32 or win64 version of <nssm.exe> into the Program Files directory.
3. Open a console window with administrator rights.
4. Navigate to the newly created folder.
5. Execute NSSM install file. For example:

   C:\Program Files\NSSM>nssm.exe

   NSSM: The non-sucking service manager

   Version 2.24 64-bit, 2014-08-31

9.2 How to Use NSSM

Usage: nssm [<args> ...]

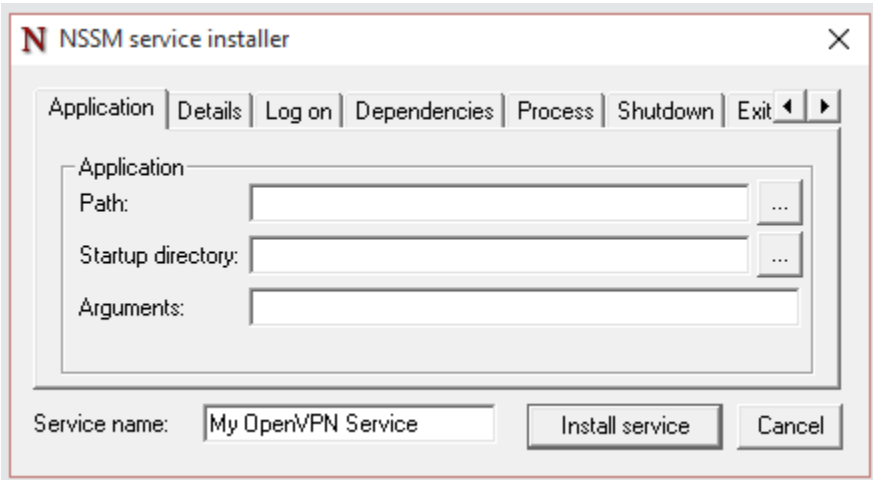
- To show service installation GUI:
  nssm install [<servicename>]
- To install a service without confirmation:
  nssm install <servicename> <app> [<args> ...]
- To show service editing GUI:
  nssm edit <servicename>
- To retrieve or edit service parameters directly:
  nssm get <servicename> <parameter> [<subparameter>]
  nssm set <servicename> <parameter> [<subparameter>]
  nssm reset <servicename> <parameter> [<subparameter>]
- To show service removal GUI:
  nssm remove [<servicename>]
- To remove a service without confirmation:
  nssm remove <servicename> confirm

- To manage a service:
  nssm start <servicename>
  nssm stop <servicename>
  nssm restart <servicename>
  nssm status <servicename>
  nssm rotate <servicename>

9.3 Running OpenVPN as Windows Service Using NSSM

To run OpenVPN as a Windows service using NSSM:

1. Go to the NSSM folder using the Windows Command Line with administrator access: **C:\Program Files\NSSM>**
2. Run the OpenVPN client as Service, execute the following command:
   nssm install "My OpenVPN Service"
   The NSSM service installer window Application tab appears.



9.4 Setting Up OpenVPN as a Service

To set up OpenVPN as a service:

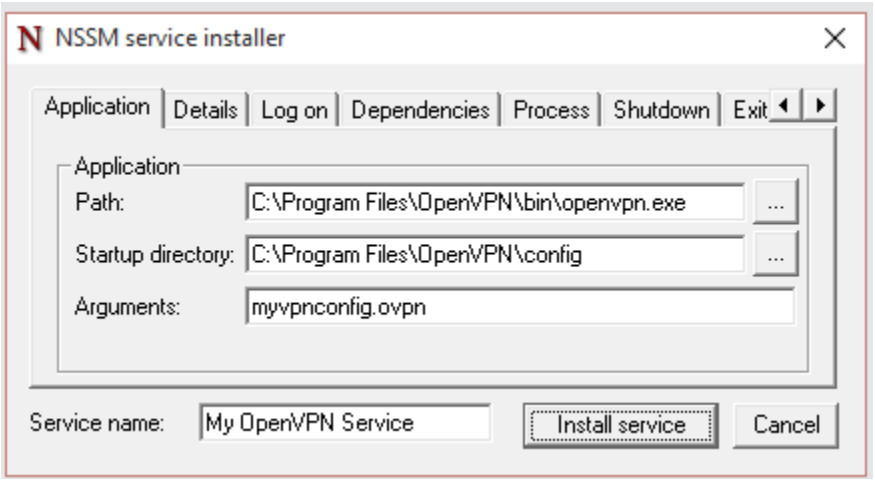
1. Complete the **Application** tab fields.

   Path: This is the path to the OpenVPN binary and should usually be C:\Program Files\OpenVPN\bin\openvpn.exe.

   Startup directory: This is the path to the directory where you store your OpenVPN configuration files. Usually that is C:\Program Files\OpenVPN\config. But if you want to run the OpenVPN UI with manual started tunnels in parallel, then create a separate folder, e.g., C:\Program Files\OpenVPN\config-nssm. Otherwise it is easy to confuse manual tunnels with service tunnels.

   In this example, since manual tunnels are being used, use the default values.

   Arguments: This is the configuration file for the tunnel, that should reside in the above defined startup directory.

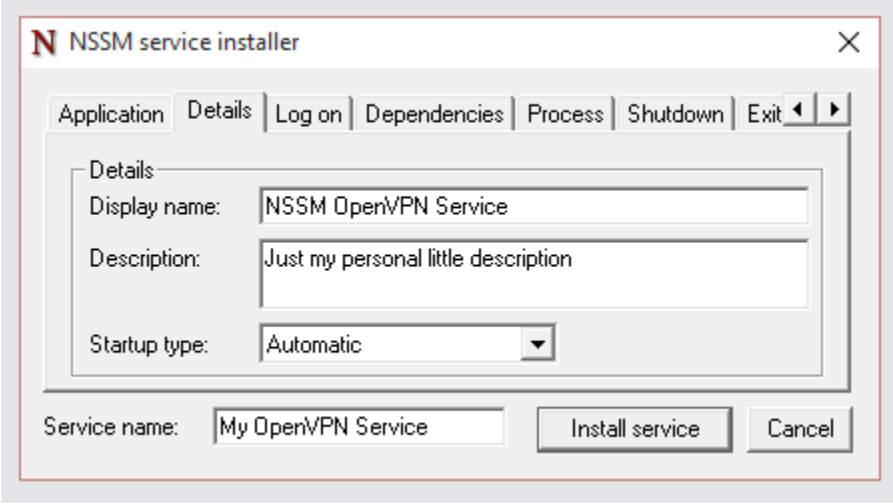


2. Complete the **Details** tab fields.

   Display name: This is the name that is basically visible everywhere. The name is editable, but most of the time this is the same as the service name.

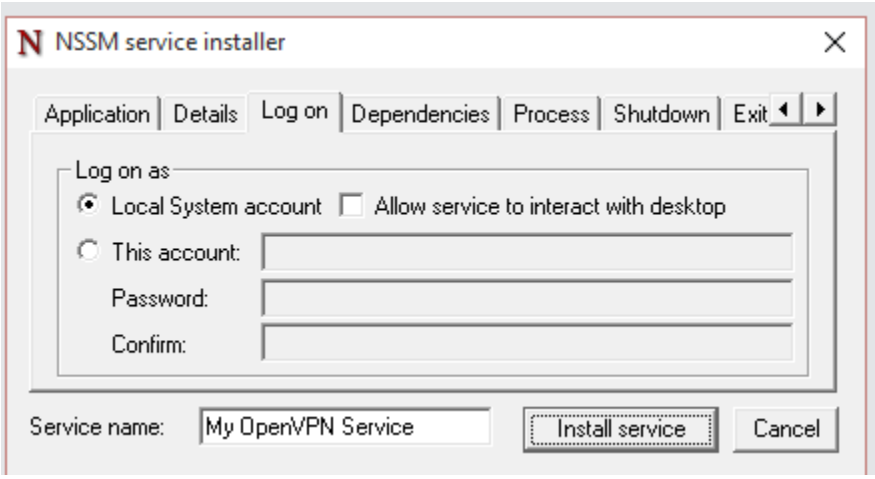
   Description: This is the description that can be viewed later in the services area.

   Start-up type: This is the standard service start up type setting for a window. Most likely choose Automatic here. But here user have the choice between Automatic, Automatic (Delayed Start), Manual and Disabled.



3. Complete the **Log On** tab fields.

   Define how this service needs to run. Unless you are doing something unusual here, you can leave the default settings unchanged (that is, **Local System account**).



4. Complete the **Update** tab fields.

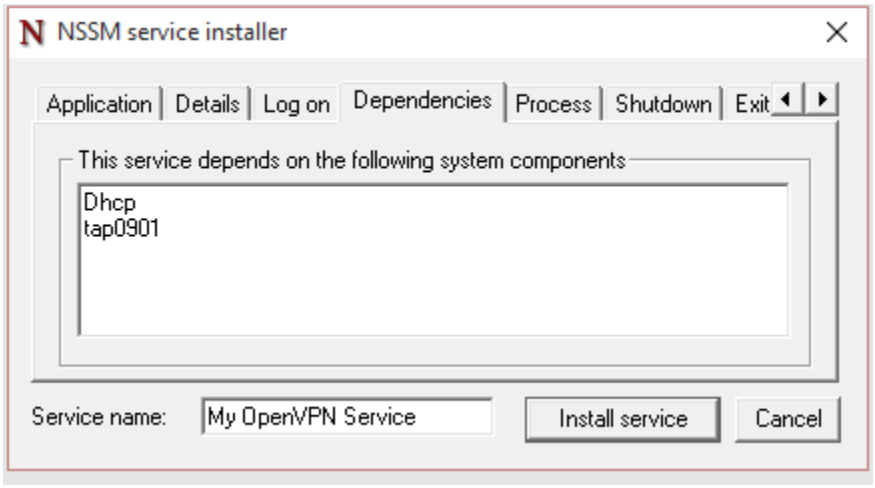
   If running Windows 10, this tab can be important. Using the system account, you are able to install the service, but when starting the service, you might see an error. In the event log, the following message appears:

   > *Program C:\Program Files\OpenVPN\bin\openvpn.exe for service OpenVPN siteopsvpn (NSSM) exited with return code 3221225794.*

   This means, that you used an account that has no rights to execute OpenVPN. This can be resolved by running the service as a user that has administrative rights on that computer.

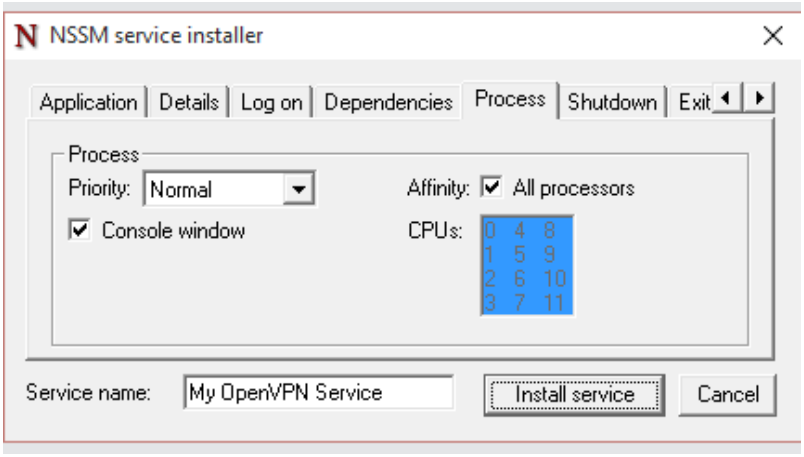
5. Complete the **Dependencies** tab fields.

   Add the services that OpenVPN is depending on (DHCP and Tap0901).



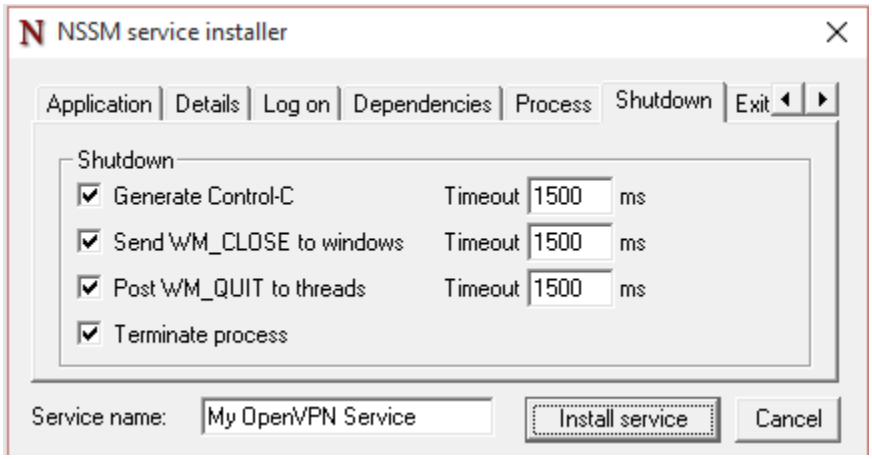
6. Complete the **Process** tab fields.

   In this tab, you can control how the service is handled by the processor. For instance, if it should only run on a specific processor or as a higher priority. For the normal use case this can be remain unchanged.

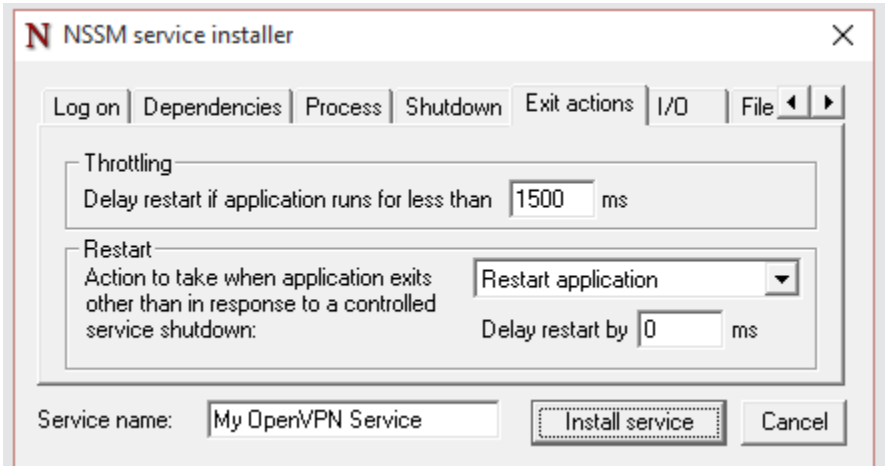


7. Complete the **Shutdown** tab fields.

   Under normal circumstances, no changes are required for this tab.



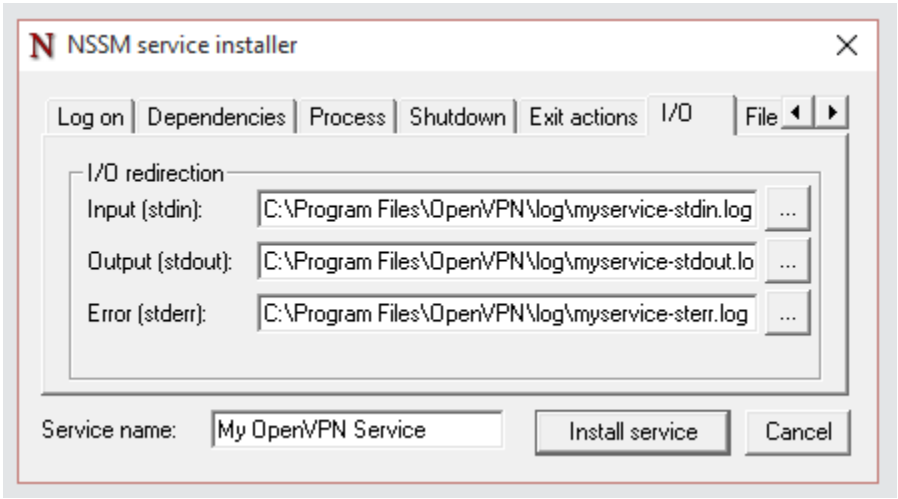
8. Complete the **Exit Actions** tab fields.
   Under normal circumstances, no changes are required for this tab.



9. Complete the **I/O** tab fields.

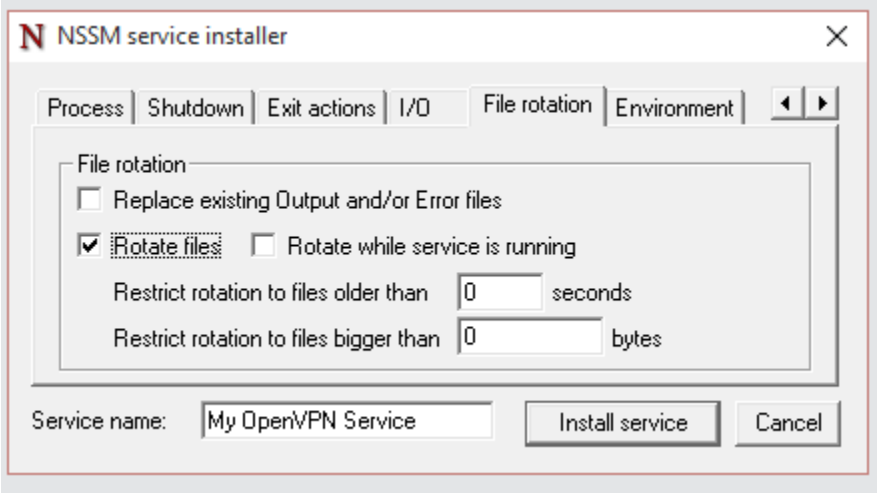
   With the OpenVPN UI you can view the log files. However, with services you cannot view the logs, unless you define them here. Log files are usually located in:

   C:\Program Files\OpenVPN\log.



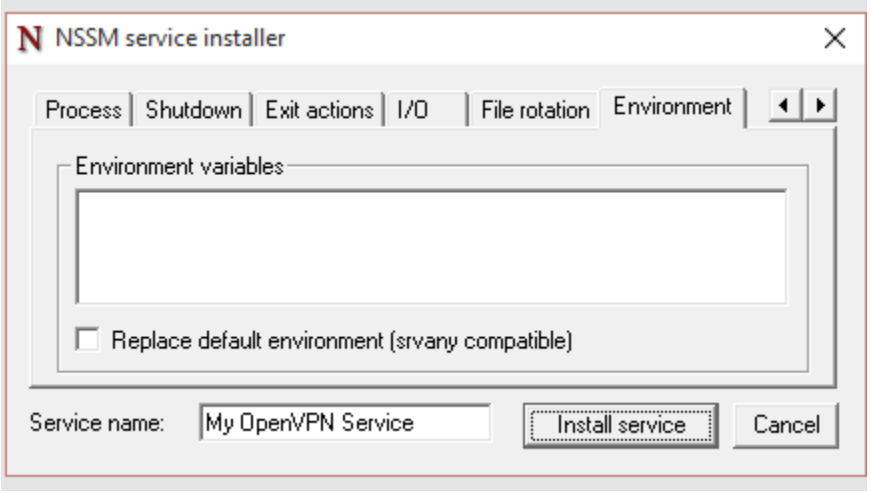
10. Complete the **File Rotation** tab fields.

    This tab is an extension of the I/O tab, as it configures the log rotation.



11. Complete the **Environment** tab fields.

    This last tab can usually be ignored. However, it can be useful if you want to add or even replace the environment.



12. Click **Install service**.
    Result: NSSM installs OpenVPN as a service that can survive standby and sluggish network connections.

13. Start the newly created service with the:
    - **net** command,
    - **nssm** command, or
    - Services in the control panel.

    If you want to change anything, this can be done by calling NSSM with the edit parameter.

    nssm edit "My OpenVPN Service"

    And, as previously stated, you can perform changes from the command line. The command sequence is:

    nssm install "My OpenVPN Service" C:\Program Files\OpenVPN\bin\openvpn.exe
    nssm set "My OpenVPN Service" AppDirectory "C:\Program Files\OpenVPN\config"
    nssm set "My OpenVPN Service" AppParameters myvpnconfig.ovpn

nssm set "My OpenVPN Service" AppStdin "C:\Program Files\OpenVPN\log\myservice-stdin.log"

nssm set "My OpenVPN Service" AppStdout "C:\Program Files\OpenVPN\log\myservice-stdout.log"

nssm set "My OpenVPN Service" AppStderr "C:\Program Files\OpenVPN\log\myservice-sterr.log"

nssm set "My OpenVPN Service" AppRotateFiles 1

nssm set "My OpenVPN Service" DependOnService Dhcp tap0901

A. Certificate Error Messages Logged by OpenVPN Configuration

This appendix describes possible error messages logged by the OpenVPN configuration HMI for errors in certificates.

Example Error Message:

List of Error Codes from OpenSSL.org:

Error Code	Description
0 X509_V_OK: ok	The operation was successful.
2 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT: unable to get issuer certificate	The issuer certificate of a looked-up certificate could not be found. This normally means the list of trusted certificates is not complete. Ensure that Issuer Certificate for the Installed Local Certificate exists. Also ensure that all certificates in the Issuer Certificate chain are installed in the MCP.
3 X509_V_ERR_UNABLE_TO_GET_CRL: unable to get certificate CRL	The CRL of a certificate could not be found.
4 X509_V_ERR_UNABLE_TO_DECRYPT_CERT_SIGNATURE: unable to decrypt certificate's signature	The certificate signature could not be decrypted. This means that the actual signature value could not be determined rather than it not matching the expected value, this is only meaningful for RSA keys.
5 X509_V_ERR_UNABLE_TO_DECRYPT_CRL_SIGNATURE: unable to decrypt CRL's signature	The CRL signature could not be decrypted: this means that the actual signature value could not be determined rather than it not matching the expected value. Unused.

Error Code	Description
6 X509_V_ERR_UNABLE_TO_DECODE_ISSUER_PUBLIC_KEY: unable to decode issuer public key	The public key in the certificate SubjectPublicKeyInfo could not be read.
7 X509_V_ERR_CERT_SIGNATURE_FAILURE: certificate signature failure	The signature of the certificate is invalid.
8 X509_V_ERR_CRL_SIGNATURE_FAILURE: CRL signature failure	The signature of the certificate is invalid.
9 X509_V_ERR_CERT_NOT_YET_VALID: certificate is not yet valid	The certificate is not yet valid: the not-Before date is after the current time. This issue could be caused by an incorrect time on the MCP. Ensure that the MCP time is correct. An incorrect time could occur if the MCP is configured for the UTC timezone but its time is set to a non-UTC local time. It is recommended that the MCP timezone be set to the correct local timezone and time corrected in this case.
10 X509_V_ERR_CERT_HAS_EXPIRED: certificate has expired	The certificate has expired: that is the notAfter date is before the current time.
11 X509_V_ERR_CRL_NOT_YET_VALID: CRL is not yet valid	The CRL is not yet valid.
12 X509_V_ERR_CRL_HAS_EXPIRED: CRL has expired	The CRL has expired.
13 X509_V_ERR_ERROR_IN_CERT_NOT_BEFORE_FIELD: format error in certificate's notBefore field	The certificate not Before field contains an invalid time.
14 X509_V_ERR_ERROR_IN_CERT_NOT_AFTER_FIELD: format error in certificate's notAfter field	The certificate notAfter field contains an invalid time.
15 X509_V_ERR_ERROR_IN_CRL_LAST_UPDATE_FIELD: format error in CRL's lastUpdate field	The CRL lastUpdate field contains an invalid time.
16 X509_V_ERR_ERROR_IN_CRL_NEXT_UPDATE_FIELD: format error in CRL's nextUpdate field	The CRL nextUpdate field contains an invalid time.
17 X509_V_ERR_OUT_OF_MEM: out of memory	An error occurred trying to allocate memory. This should never happen.
18 X509_V_ERR_DEPTH_ZERO_SELF_SIGNED_CERT: self-signed certificate	The passed certificate is self-signed, and the same certificate cannot be found in the list of trusted certificates.
19 X509_V_ERR_SELF_SIGNED_CERT_IN_CHAIN: self-signed certificate in certificate chain	The certificate chain could be built up using the untrusted certificates, but the root could not be found locally.

Error Code	Description
20 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY: unable to get local issuer certificate	The issuer certificate could not be found: this occurs if the issuer certificate of an untrusted certificate cannot be found. Ensure that Issuer Certificate for the Installed Local Certificate exists. Also ensure that all certificates in the Issuer Certificate chain are installed in the MCP.
21 X509_V_ERR_UNABLE_TO_VERIFY_LEAF_SIGNATURE: unable to verify the first certificate	No signatures could be verified because the chain contains only one certificate and it is not self-signed.
22 X509_V_ERR_CERT_CHAIN_TOO_LONG: certificate chain too long	The certificate chain length is greater than the supplied maximum depth. Unused.
23 X509_V_ERR_CERT_REVOKED: certificate revoked	The certificate has been revoked.
24 X509_V_ERR_INVALID_CA: invalid CA certificate	A CA certificate is invalid. Either it is not a CA, or its extensions are not consistent with the supplied purpose.
25 X509_V_ERR_PATH_LENGTH_EXCEEDED: path length constraint exceeded	The basic Constraints path length parameter has been exceeded.
26 X509_V_ERR_INVALID_PURPOSE: unsupported certificate purpose	The supplied certificate cannot be used for the specified purpose.
27 X509_V_ERR_CERT_UNTRUSTED: certificate not trusted	The root CA is not marked as trusted for the specified purpose.
28 X509_V_ERR_CERT_REJECTED: certificate rejected	The root CA is marked to reject the specified purpose.
29 X509_V_ERR_SUBJECT_ISSUER_MISMATCH: subject issuer mismatch	The current candidate issuer certificate was rejected because its subject name did not match the issuer name of the current certificate. Only displayed when the **-issuer_checks** option is set.
30 X509_V_ERR_AKID_SKID_MISMATCH: authority and subject key identifier mismatch	The current candidate issuer certificate was rejected because its subject key identifier was present and did not match the authority key identifier current certificate. Only displayed when the **-issuer_checks** option is set.
31 X509_V_ERR_AKID_ISSUER_SERIAL_MISMATCH: authority and issuer serial number mismatch	The current candidate issuer certificate was rejected because its issuer name and serial number was present and did not match the authority key identifier of the current certificate. Only displayed when the **-issuer_checks** option is set.

Error Code	Description
32 X509_V_ERR_KEYUSAGE_NO_CERTSIGN:key usage does not include certificate signing	The current candidate issuer certificate was rejected because its keyUsage extension does not permit certificate signing.
50 X509_V_ERR_APPLICATION_VERIFICATION: application verification failure	An application specific error. Unused.

B. OpenVPN Server Log Messages

This appendix describes common error or info messages logged by OpenVPN server log that can be used to troubleshoot the connectivity issues between VPN server and client.

VPN Server Log Message(s)	Cause of the issue and recommended actions
2017-05-07T08:33:36.597083+00:00,00000000,597,None,openvpn:N9219:ERR -: Cannot load CA certificate file [[INLINE]] (no entries were read),	Check INLINE CA entry(ies) are not properly embedded into either VPN Server (/etc/openvpn/ovpn-server.conf) or Client configuration files. Following is an example of a correctly embedded INLINE ca entry: <ca> -----BEGIN CERTIFICATE----- MIIDxTCCAq2gAwIBAgIBATANBgkqhkiG9w0BAQUFADB8MQswCQYDVQQGEwJDQTEL ... PG0MFqakCdoorEfVtsI73wSd5z+76fiOUcQF+JsXPBgYO2lY7TcCSNAf592tZC1w y22boL1ndWIC -----END CERTIFICATE----- </ca> Following is an example of an invalid (empty) entry: <ca> </ca> If an invalid or empty INLINE CA entry exists, contact GE Grid Solutions Technical Support for further assistance.
2017-05-07T08:41:25.710242+00:00,00000000,710,None,openvpn:N13694:ERR -: Insufficient key material or header text not found in file '[[INLINE]]' (0/128/256 bytes found/min/max),	Check INLINE <tls-auth> key is not properly embedded into either VPN Server (/etc/openvpn/ovpn-server.conf) or Client configuration files. Following is an example of correctly embedded INLINE <tls-auth> key entry. <tls-auth> # # 2048 bit OpenVPN static key # -----BEGIN OpenVPN Static key V1----- ddd5343a60c7313f2e0c1e0531533047 ..... f1578505715790cdb02e3548d4353fd0 -----END OpenVPN Static key V1----- </tls-auth> Following is an example of an invalid (empty) entry: <tls-auth> </tls-auth>If an invalid or empty <tls-auth> key exists, contact GE Grid Solutions Technical Support for further assistance.
2017-05-07T08:55:45.750417+00:00,00000000,750,None,openvpn:N20901:ERR -: Cannot load CA certificate file [[INLINE]] (no entries were read),	Check if INLINE CA entry(ies) embedded in the VPN Server (/etc/openvpn/ovpn-server.conf) and Client configuration files are the same. If not, try exporting the Client configuration again from the MCP Utilities tab under Settings option.
2017-05-07T09:01:11.621226+00:00,00000000,621,None,openvpn:N24633:ERR -: INLINE tls-auth file lacks the requisite 2 keys,	Check INLINE <tls-auth> key embedded in the VPN Server (/etc/openvpn/ovpn-server.conf) or Client configuration files are same. If different, try exporting the Client configuration again from the MCP Utilities tab under Settings option.

2017-05-07T01:21:23.203099+00:00,00000000,203,None,openvpn:N15234:NOTICE -: 172.12.233.68:63308 TLS: Initial packet from [AF_INET]172.12.233.68:63308, sid=2ee6fb0da06dc8a0,	Check if the client certificate is revoked. In this case you would need to create a new client certificate with the same common name. (Or) Check if the Client (.p12) certificate is not properly created (e.g., different CA than used by MCP Server certificate, mismatched common name etc..) or not properly installed in the client. Generate a new client certificate with the same common name and then install in the client.
2017-05-07T09:07:07.298309+00:00,00000000,298,None,openvpn:N28913:NOTICE -: 172.12.233.68:57360 SENT CONTROL [MyClient]: 'AUTH_FAILED' (status=1),	Check the Client is Disabled in configuration for openvpn server in MCP. If so, enable the Client. (Or) Check the common name of Client certificate is the same as the client name in the configuration for the OpenVPN server in the MCP. If not, correct the Client name in the OpenVPN server configuration.

C. VPN Client from Ubuntu PC

To integrate the OpenVPN client running in Ubuntu 16.04LTS with the MCP:

1. Setup your CA – see section 2.1.2 .
2. Generate Diffie Hellman (DH) parameters; see Chapter 2.
3. Generate private keys and certificates for your MCP; see section 3.1.1 .
4. Generate client certificate + private key in. pem format for OpenVPN client that runs in Ubuntu 16.04LTS PC.
5. Install the CA's Certificate on your MCP; see section 4.1.
6. Install the private keys, certificates and optional Diffie Hellman parameters on your MCP; see section 4.1
7. Copy the. pem client certificate + private key into "/etc/openvpn/" folder or any other location to which openvpn client can have a administrator privileges.
8. Using the "Export VPN Client File" option in Utilities tab under Settings option page, export the OpenVPN client configuration (*. ovpn) into a desired location; see section 5.3.
9. Securely copy the OpenVPN client configuration into "/etc/openvpn/" folder or any other location to which openvpn client can have a administrator privileges.
10. Open the VPN Client configuration file using "vi" or any other editor and do the below steps.
    - Comment the line starts with "cryptoapicert" with "#" as shown below.

      #cryptoapicert "SUBJ:MyCA_Client1"
    - And, add the below two lines to the bottom of the file as shown below.

      cert <Patch of MyCA_Client1.pem>/MyCA_Client1.pem

      key <Patch of MyCA_Client1.pem>/MyCA_Client1.pem

      e.g.:

      cert </etc/openvpn/MyCA_Client1.pem

      key </etc/openvpn/MyCA_Client1.pem
11. Save the Configuration file and Run the OpenVPN client software from Ubuntu 16.04LTS PC using the below command from the terminal.

    sudo openvpn –-config <path of the Client Config File>/ MyCA_Client1.ovpn file.

    For example:

    sudo openvpn –-config /etc/openvpn/ MyCA_Client1.ovpn file.
12. Verify in MCP VPN Server Log that VPN channel is established between OpenVPN Client running in Ubuntu 16.04 LTS and MCP.

D. List of Acronyms

Table 9 List of Acronyms

Abbreviation	Description
CA	Certification Authority
CN	Common Name
CRL	Certificate Revocation List
DCA	Data Collection Application
DHE	Diffie Hellman Ephemeral
DPA	Data Presentation Application
DTA	Data Translation Application
FQDN	Full Qualify Distinguished Name
HMAC	Hash-based Message Authentication Code
HMI	Human Machine Interface
IED	Intelligent Electronic Device
JVM	Java Virtual Machine
LAN	Local Area Network
NSSM	Non-Sucking Service Manager
OU	Organizational Unit
PEM	Privacy Enhanced Mail
PKCS	Public Key Cryptography
PKI	Public Key Infrastructure
PRF	Protective Relay Fault
RTDB	Real Time Data Base
RTU	Remote Terminal Unit
SDD	Software Design Document
SOE	Sequence of Event
SPT	Secure Pass-Through
SSDD	Software Subsystem Design Document
TLS	Transport Layer Security
VPN	Virtual Private Network
WAN	Wide Area Network
XCA	X Certificate and Key Management

MODIFICATION RECORD

Version	Revision	Date	Change Description
1.00	0	26th March, 2019	Document Created.
2.00	0	23rd April, 2021	Updated for MCP family.
2.00	1	26th April, 2021	Updated Technical Support Contacts.
2.00	2	29th July 2021	Updated VPN Client Configuration, clarified DN requirements and updated notes about certificate error messages

GE
Grid Solutions

Enterprise File Synchronization from MCP Sync Manager

Configuration Guide

SWM0104

Version 2.00 Revision 2

Associated Software Release: Version 1.00 and above

GE Information

COPYRIGHT NOTICE

© 2021, General Electric Company. All rights reserved.

The Software Product described in this documentation may only be used in accordance with the applicable License Agreement. The Software Product and Associated Material are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable, and are delivered with Restricted Rights. Such restricted rights are those identified in the License Agreement, and as set forth in the "Restricted Rights Notice" contained in paragraph (g) (3) (Alternate III) of FAR 52.227-14, Rights in Data-General, including Alternate III (June 1987).

If applicable, any use, modification, reproduction release, performance, display or disclosure of the Software Product and Associated Material by the U.S. Government shall be governed solely by the terms of the License Agreement and shall be prohibited except to the extent expressly permitted by the terms of the License Agreement.

The information contained in this online publication is the exclusive property of General Electric Company, except as otherwise indicated. You may view, copy and print documents and graphics incorporated in this online publication (the "Documents") subject to the following: (1) the Documents may be used solely for personal, informational, non-commercial purposes; (2) the Documents may not be modified or altered in any way; and (3) General Electric Company withholds permission for making the Documents or any portion thereof accessible via the internet. Except as expressly provided herein, you may not use, copy, print, display, reproduce, publish, license, post, transmit or distribute the Documents in whole or in part without the prior written permission of General Electric Company. If applicable, any use, modification, reproduction, release, performance, display, or disclosure of the Software Product and Associated Material by the U.S. Government shall be governed solely by the terms of the License Agreement and shall be prohibited except to the extent expressly permitted by the terms of the License Agreement.

The information contained in this online publication is subject to change without notice. The software described in this online publication is supplied under license and may be used or copied only in accordance with the terms of such license.

TRADEMARK NOTICES

GE and are trademarks and service marks of General Electric Company.

* Trademarks of General Electric Company.

Other company or product names mentioned in this document may be trademarks or registered trademarks of their respective companies.

Contents

About this Document 6

Purpose 6
Intended Audience 6
Additional Documentation 6

Product Support 8

GE Grid Solutions Web Site 8
GE Technical Support Library 8
Contact Technical Support 8

1. Overview 9

1.1 MCP Sync Manager 9
1.2 Copssh software 9
1.3 cwRsyncServer software 9
1.4 Installation Steps 9

2. Installation of copssh and cwRsyncServer 10

2.1 Software 10
2.2 Installation 10

3. Configuring MCP Sync Manager 23

3.1 Enable Sync Manager 23
3.2 Configure Sync Sets 23

4. Setting up Public Key Authentication 25

4.1 Update Permissions to SyncMgr Folder 25
4.2 Copy key from MCP to the Windows computer 25

A. Uninstalling cwRsyncServer and Copssh 27

B. Diagnostics 28

B.1 MCP Diagnostic Logs 28
B.2 Copssh Event Log on Enterprise Server 28

C. List of Acronyms 29

Figures

No table of figures entries found.

Tables

Table 1 Configure Sync Sets - Settings 23
Table 2 List of Acronyms 29

About this Document

Purpose

This document describes how to setup an enterprise server on a Windows-based computer to synchronize files from MCP device(s) that use the Sync Manager application (RSYNC/SSH protocol). This document outlines and details the procedures regarding:

- Installation and setup of CopSSH and cwRsyncServer tools on the computer. These are 3rd party software applications that have been tested with the MCP Sync Manager.
- Configuration of MCP Sync Manager Application to synchronize files to the enterprise server. The example is for ARRM files, but other user related files / folders may be synchronized too (e.g. Logs).

Once the data is present in the Windows Enterprise computer, the sharing of folders and files from this computer to Enterprise users is outside of scope of this document and can be achieved using any IT / Windows standard sharing methods.

NOTICE

This document applies to the MCP family (G100/G500) unless otherwise indicated.
Screen captures may show G500 in some areas, however the workflow applies to products in the MCP family (G100/G500).

Depending on the versions of the CopSSH and cwRsyncServer 3rd party tools – the exact presented workflow and dialogues may change according to changes made by the supplier. The 3rd party supplier may support newer versions of Windows Operating System. Workflow remains similar, screen captures may look different.

Intended Audience

This document serves as a reference for systems integrators who wish to setup enterprise server on Windows-based computer to synchronize files from MCP Sync Manager device(s).

Additional Documentation

For further information about the Enterprise File Synchronization from MCP Sync Manager, refer to the following documents:

- MCP Substation Gateway, Software Configuration Guide, SWM0101/15
- MCP Substation Gateway, HMI Online Help

Product Support

If you need help with any aspect of your GE Grid Solutions product, you can:

- Access the GE Grid Solutions Web site
- Search the GE Technical Support library
- Contact Technical Support

GE Grid Solutions Web Site

The GE Grid Solutions Web site provides fast access to technical information, such as manuals, release notes and knowledge base topics.

Visit us on the Web at: http://www.gegridsolutions.com

GE Technical Support Library

This site serves as a document repository for post-sales requests. To *get* access to the Technical Support Web site, go to: http://sc.ge.com/*SASTechSupport

Contact Technical Support

For help with any aspect of your GE Grid Solutions product, please contact our support team, 24/7, as follows:

Region	E-mail	Telephone
Global Contact Centre	ga.support@ge.com	+44 1785 250070
Central and East Asia andPacific	ga.supportCEAP@ge.com	+61 414 730 964
India	ga.supportIND@ge.com	+91 44 22648000
Middle East, North Africa andTurkey	ga.supportMENAT@ge.com	+971 42929467
Europe, Russia, CIS and Sub-Saharan Africa	ga.supportERCIS@ge.com	+34 94 4858854
North America	ga.supportNAM@ge.com	+1 877 605 6777
Latin America	ga.supportLAM@ge.com	+55 11 36187308

1. Overview

1.1 MCP Sync Manager

The Sync Manager is a MCP application that can be used to copy files securely and automatically from a location on your MCP device to a specified directory on a remote device. The application monitors the specified local directory for changed or added files. To reduce bandwidth demands on your network, only files found to have been changed or created since the last synchronization will be transferred. This utility employs the *rsync* protocol to perform this function, secured by an SSH layer.

Multiple file sets can be configured for synchronization in the MCP, to send data to one or multiple target remote devices, using one or multiple user authentications.

1.2 Copssh software

Copssh is a 3rd party Windows-based software that enables SSH server on Windows-based computer.

1.3 cwRsyncServer software

cwRsyncServer is a 3rd party Windows-based software that enables rsync utility on Windows-based computer.

1.4 Installation Steps

1. Install cwRsyncServer and Copssh softwares on Windows-based computer acting as Enterprise Server (Refer chapter 2. Installation of copssh and cwRsyncServer)
2. Configure MCP Sync Manager Application (Refer to chapter 3. Configuring MCP Sync Manager)
3. Setup public key authentication between MCP (client) and enterprise server (Refer to chapter 4. Setting up Public Key Authentication).

2. Installation of copssh and cwRsyncServer

This chapter describes how to install Copssh and cwRsyncServer software on Windows-based Enterprise Server.

2.1 Software

- Obtain the commercial version of cwRsyncServer software from: https://www.itefix.net/cwrsync

  Note: obtain the server version of cwRsync, i.e., cwRsyncServer.

- Obtain the commercial version of Copssh software from: https://www.itefix.net/copssh

  Note: GE Grid Solutions Grid Automation has no commercial / reseller agreements in place with ITeF!x

2.2 Installation

cwRsyncServer software must be installed before Copssh.

Note: Before starting the installation, ensure that any previous installation of cwRsyncServer and Copssh is completely uninstalled.

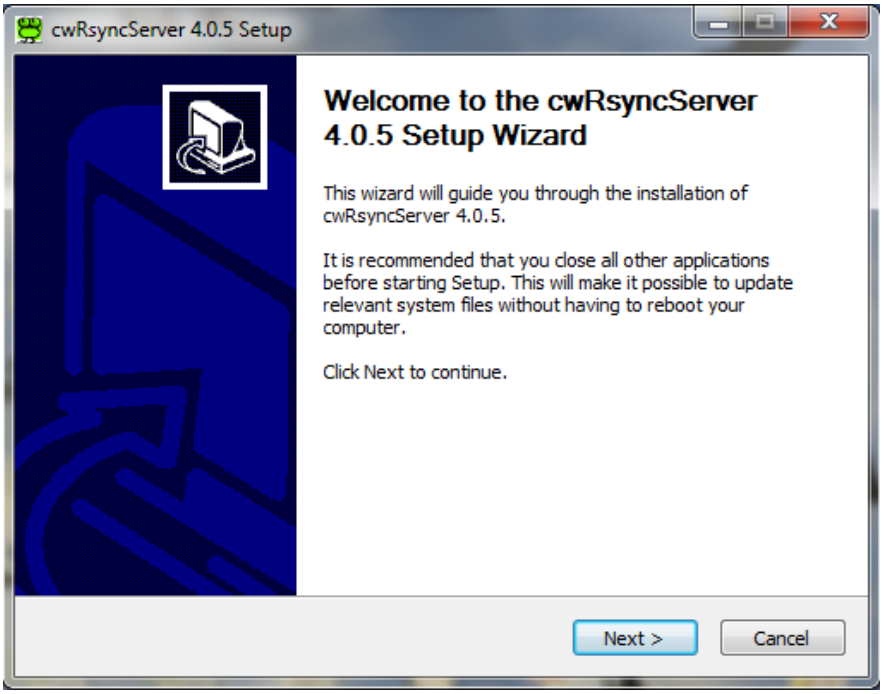
Follow Appendix A to completely uninstall cwRsyncServer and Copssh before proceeding with below steps.

2.2.1 cwRsyncServer

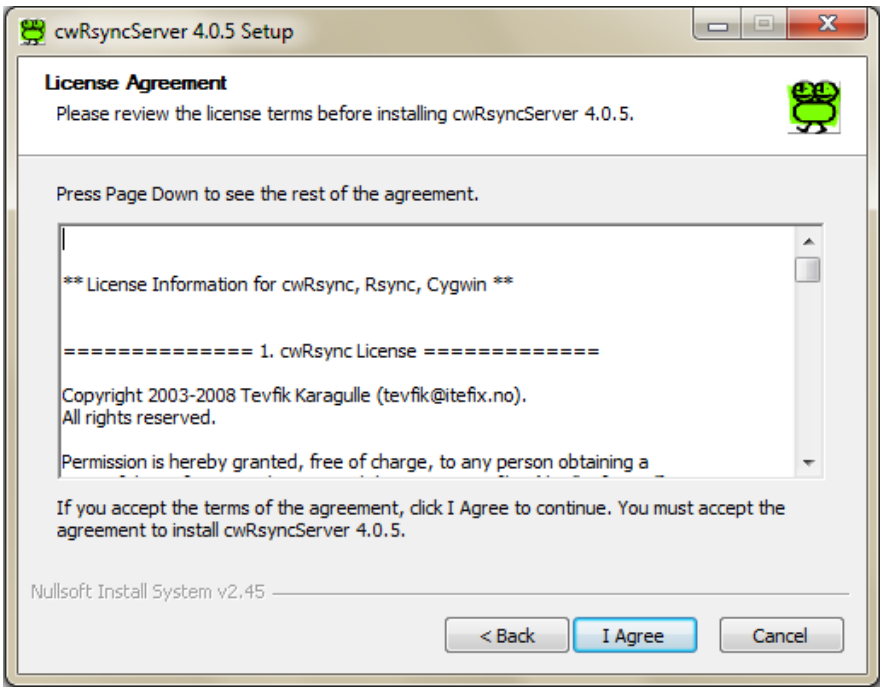
1. Start installation of cwRsyncServer by running its setup program. Follow the steps below to complete the installation.

   Note: The cwRsyncServer setup program must be run as administrator by Right click on the program and selecting “Run as administrator” (Windows 7).

2. cwRsyncServer Setup dialog appears. Click “Next”.

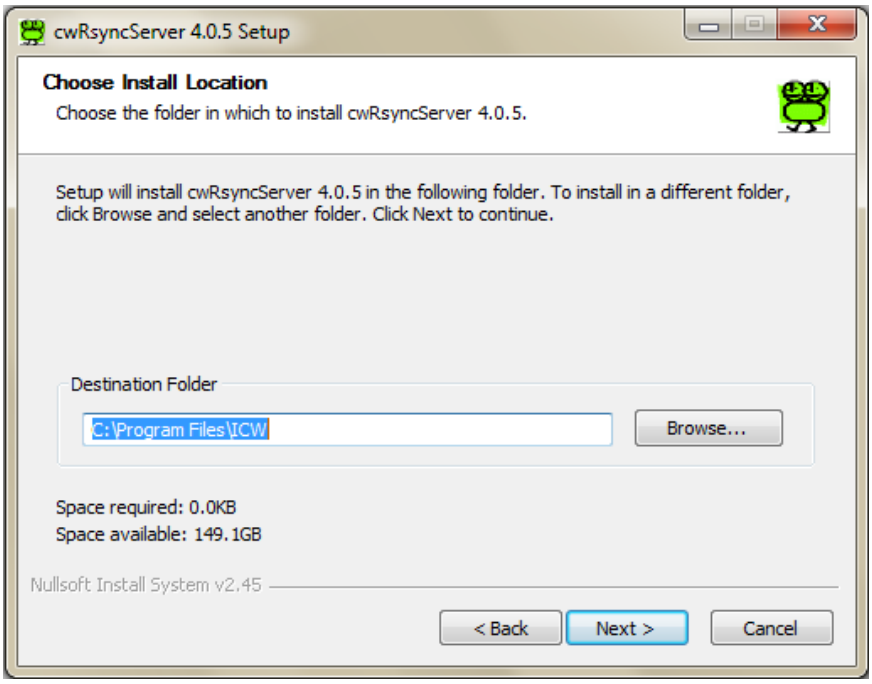


3. Click “I Agree” on the “License Agreement” window.

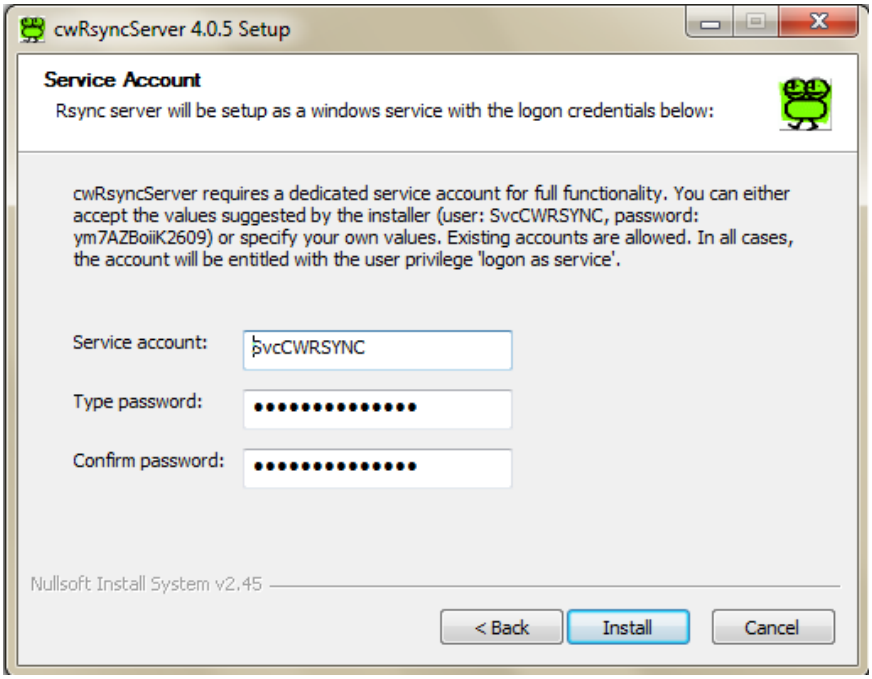


4. On the “Choose Install Location” window, click “Next” to select the default location.

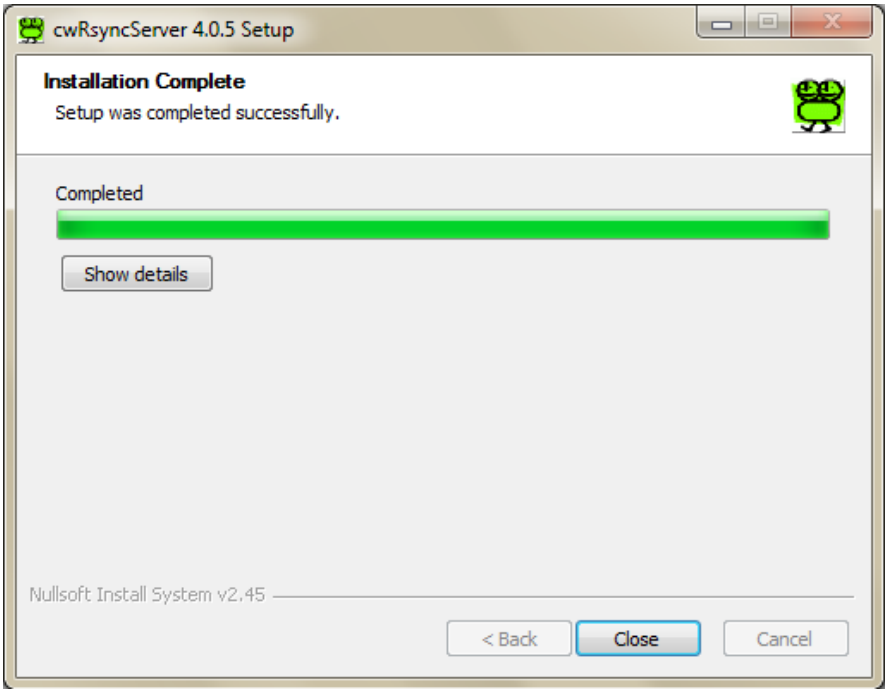
   Note: Ensure that destination folder is “**C:\Program Files\ICW**” on a 32-bit operating system or “**C:\Program Files (x86)\ICW**” on a 64-bit operating system. If not, manually update the installation location.



5. On the "Service Account" window, click "Install" to select default service account name and password.



6. On the “Installation Complete” window, click “Close” to complete the installation.



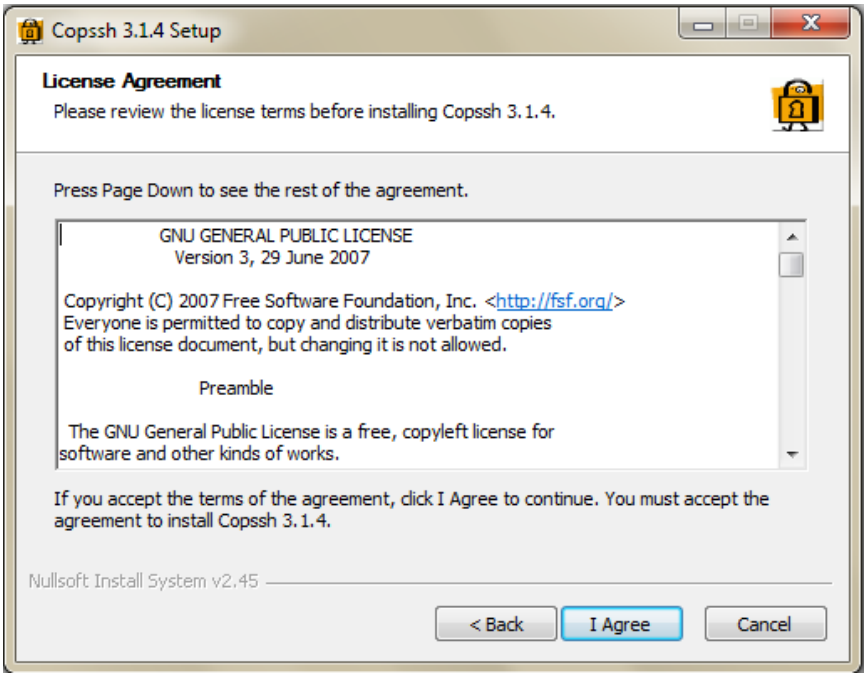
2.2.2 Copssh

1. Start installation of Copssh by running its setup program. Follow the steps below to complete the installation.

   Note: The Copssh setup program must be run as administrator by Right click on the program, and selecting “Run as administrator”.

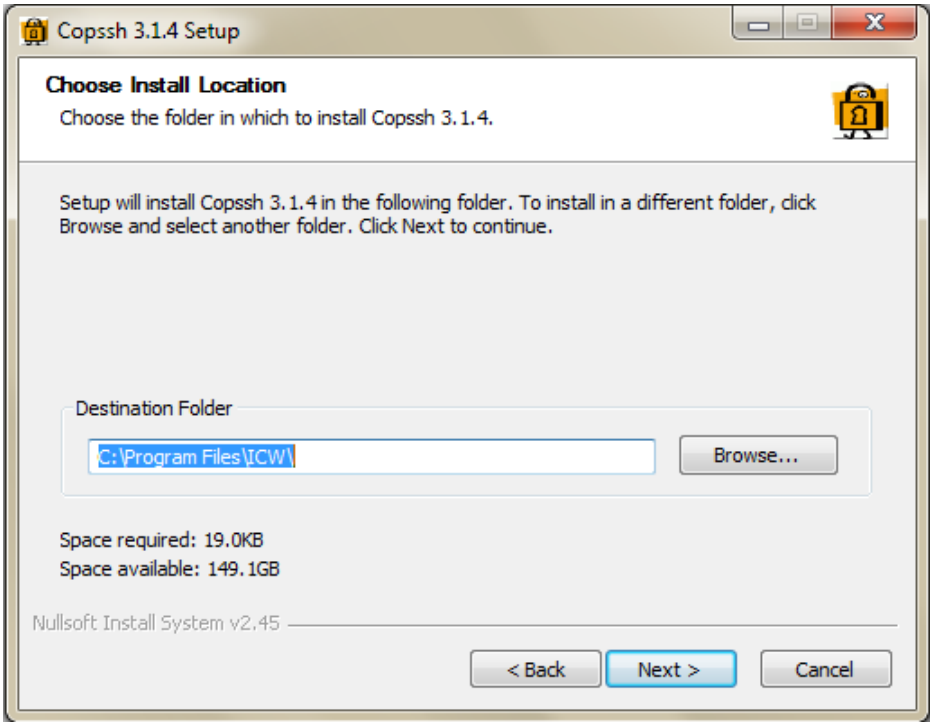
2. On the “Copssh Setup” window, select “Next”.

3. Click "I Agree" on the "License Agreement" window.

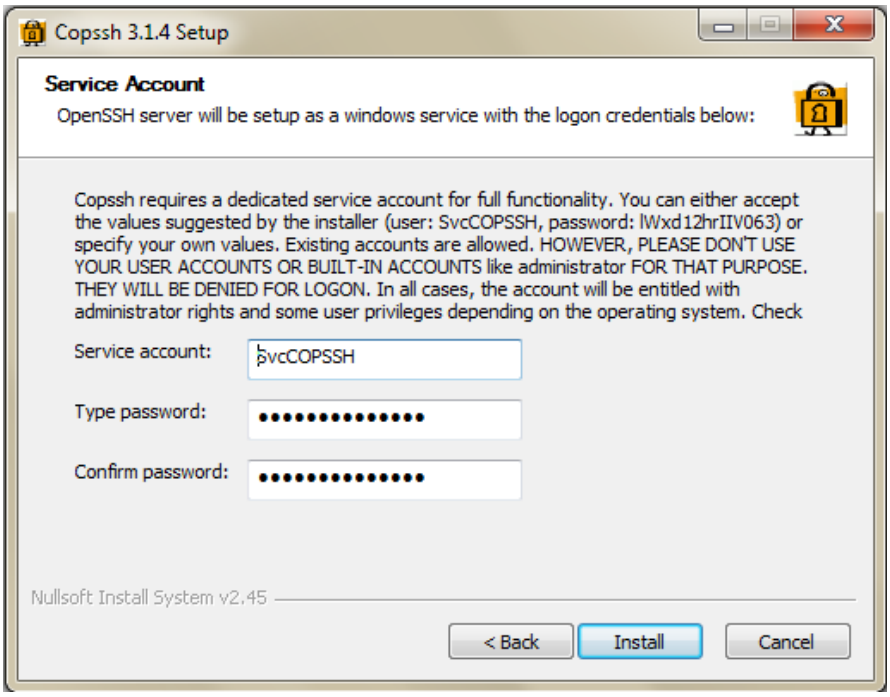


4. On the "Choose Install Location" window, click "Next" to select the default location.

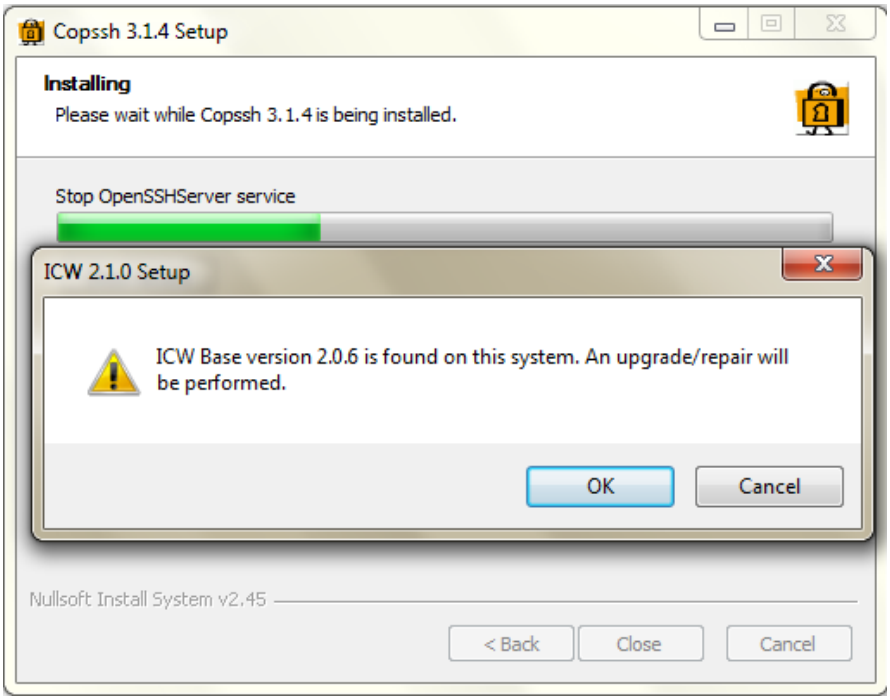
   Note: Ensure that destination folder is "**C:\Program Files\ICW**" on a 32-bit operating system or "**C:\Program Files (x86)\ICW**" on a 64-bit operating system. If not, manually update the installation location to match the installation location of the cwRsyncServer installation folder.



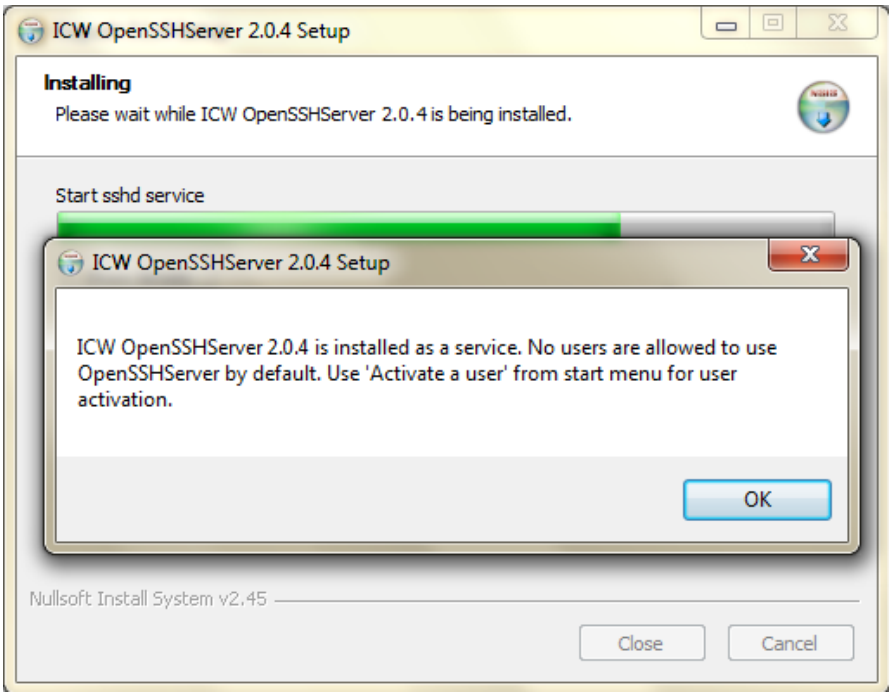
5. On the "Service Account" window, click "Install" to select default service account name and password.



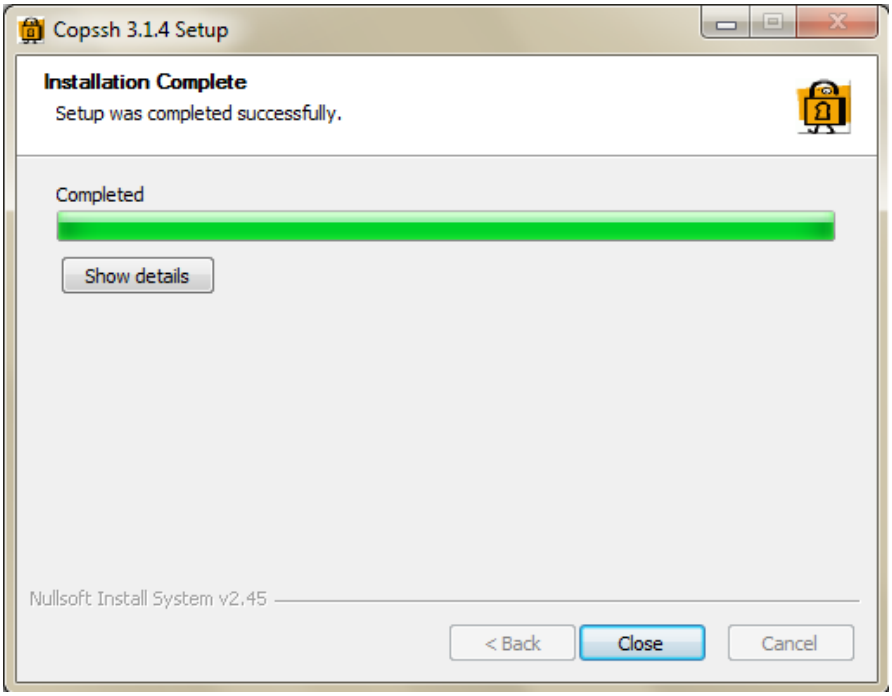
6. Since cwRsyncServer is already installed, installer will warn that ICW Base is already installed, and upgrade/repair will be performed. Click "OK".



7. At the end of installation, Setup program will notify to activate user(s) that are allowed to use OpenSSH server. Click "OK" to complete the installation.



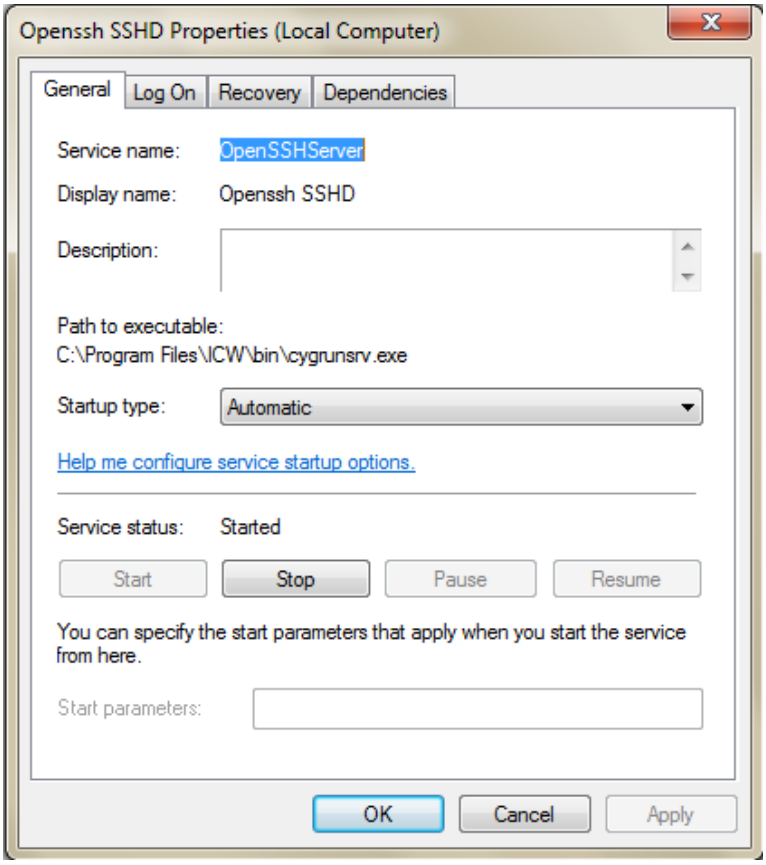
8. On the "Installation Complete" window, click "Close" to complete the installation.



9. Open Services Microsoft Management Console (MMC), from Control Panel → Administrative Tools → Services.

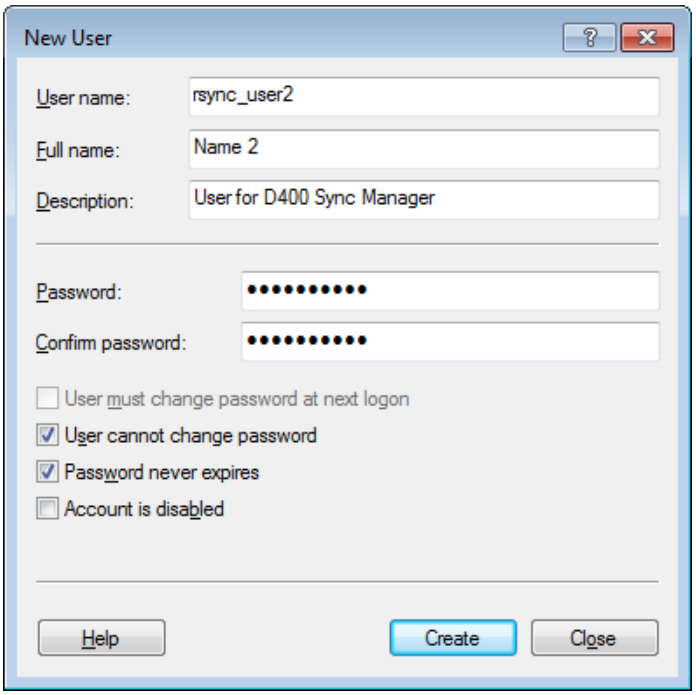
10. Double click on “Openssh SSHD” service to open its properties.

    Ensure that its Startup type is set to “Automatic”, and service is already in Started state.



2.2.3 Create Users in Windows computer

1. The users intended to be configured in MCP Sync Manager sync sets must exist in the Windows computer.
2. Use the Windows Control Panel / User management interface to add all users as needed. They should be “user” class, with password set to “user cannot change” and “no expire”. The password used here will not be used for MCP Sync Manager actions (Windows account only). These users have no need to login into the Windows computer account, and these credentials should be used only for establishing sessions between the MCP and the Enterprise server.



2.2.4 Activate Users

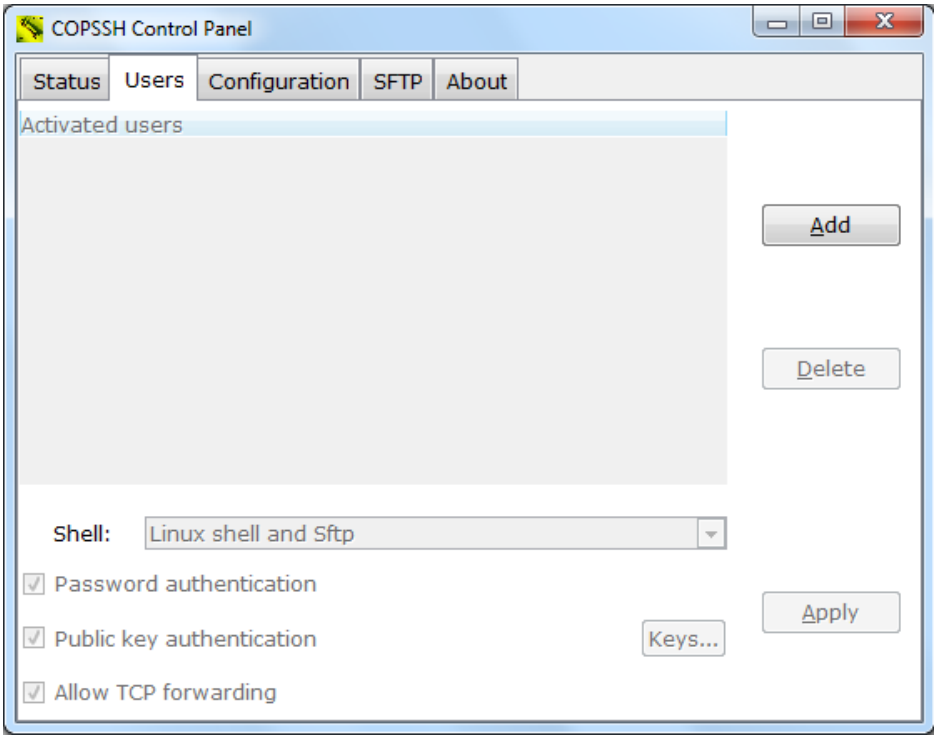
A Windows computer existing user must be activated before it can use OpenSSH service. This user will be used to sync files on this Windows-based computer from the MCP Rsync Manager. The user name must match the one configured in the MCP Sync Manager (each sync set has an option for a user name, they can be either common or distinct).

Depending on the software version, the dialog to activate users may be different.

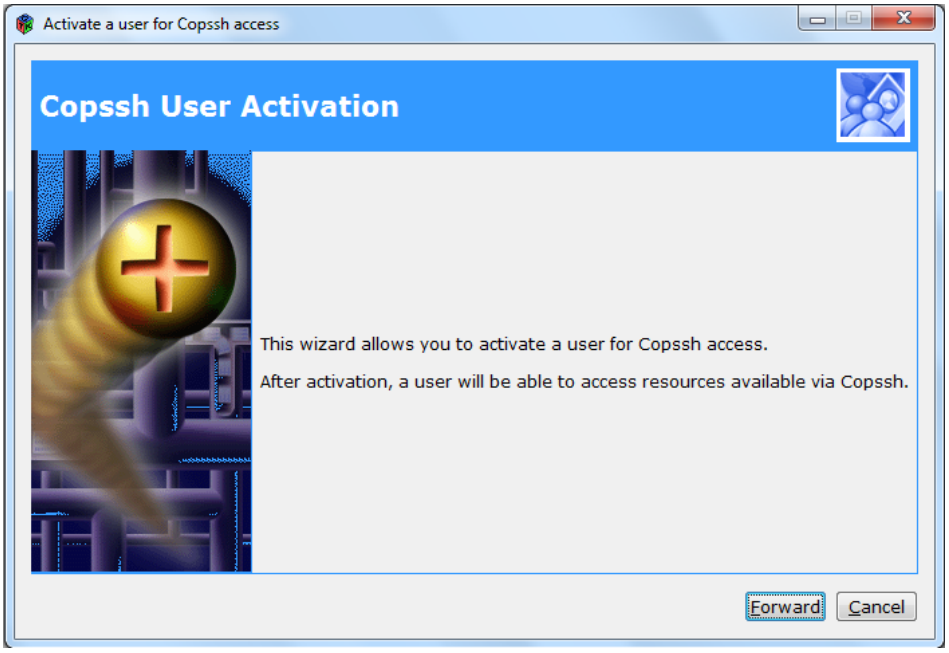
2.2.4.1 Method 1

1. Start "Copssh Control Panel" from Start Menu → All Programs → Copssh → Copssh Control Panel → Go to User tab.

   Note: The "Copssh Control Panel" program must be run as administrator.

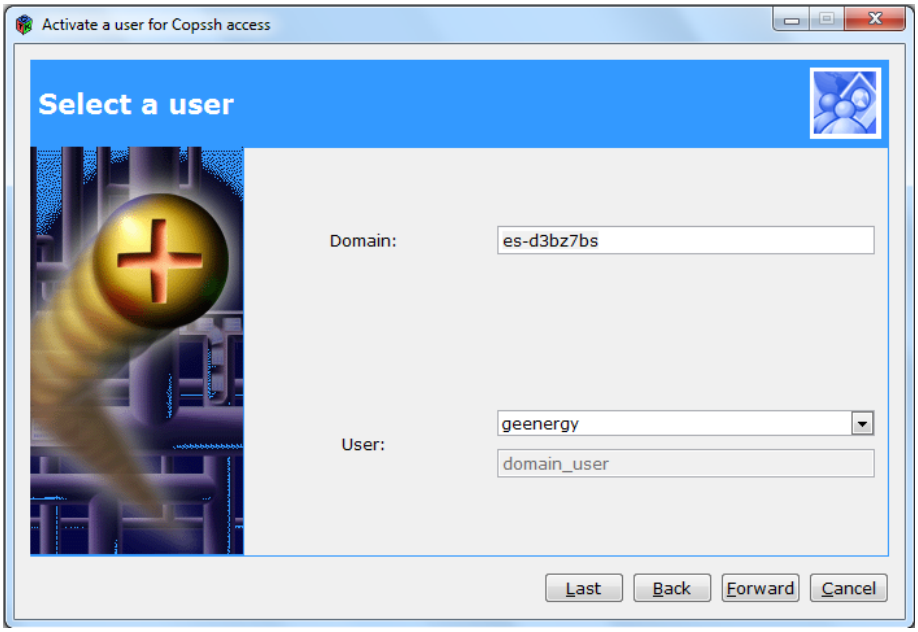


2. Click "Add" to activate a user: "Copssh User Activation" wizard opens.

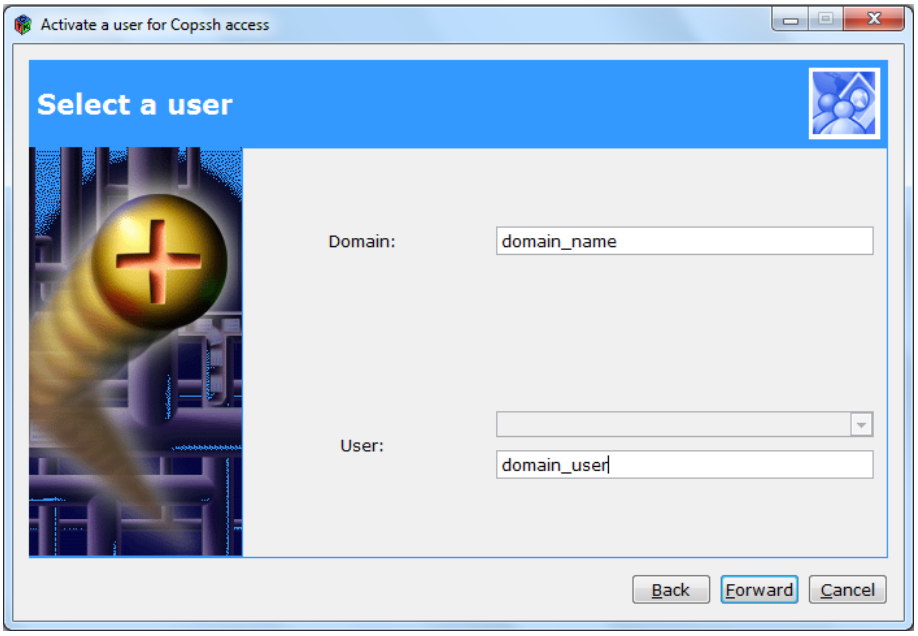


3. Click “Forward”: User selection interface opens. A local or domain user can be utilized on Windows-based computer for Copssh access.

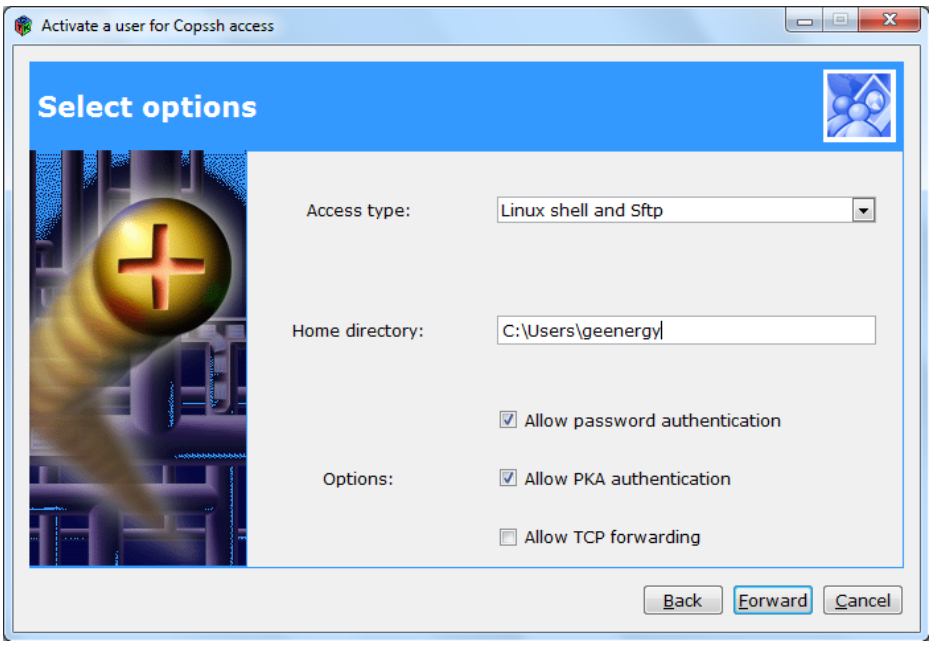
   Local User: Select a local user from the “User” drop down list.



   Domain User: Enter domain name and user name in respective fields.



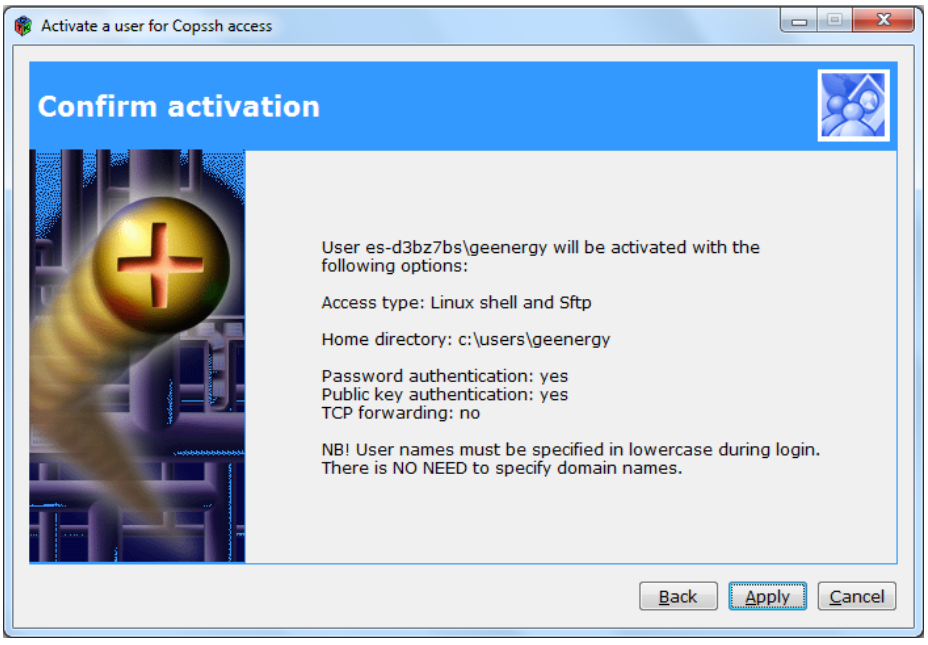
4. Click “Forward”: Select options interface opens.



5. Ensure that “Home directory” is set to “**C:\Users\<user_name>**”, where user_name is user selected in previous step. If not, manually update the “Home directory” field.

   Note: This is typical home directory on Windows 7 computer.

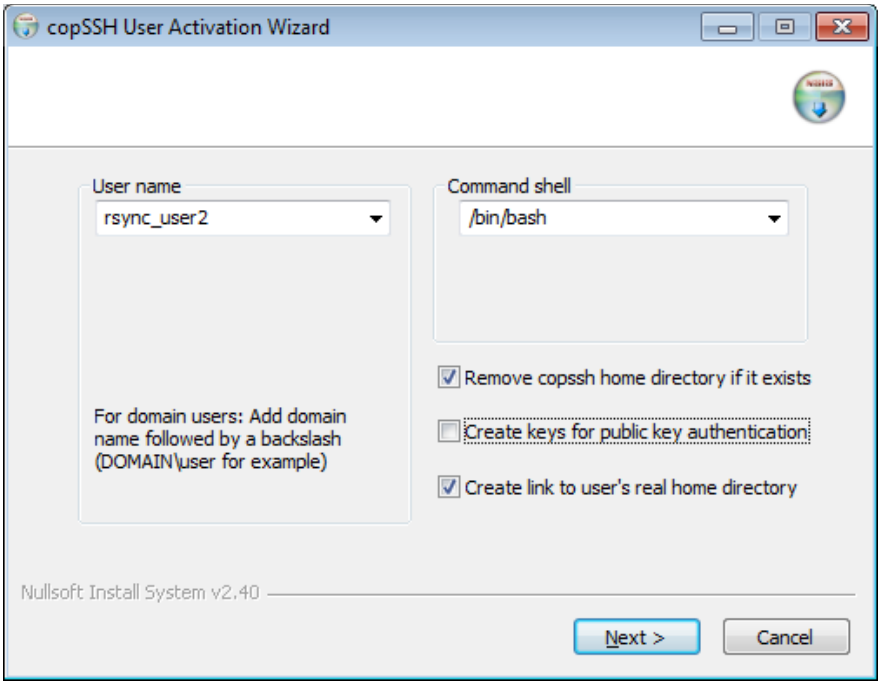
6. Deselect “Allow TCP forwarding” option.
7. Click “Forward”: Confirm activation interface appears.



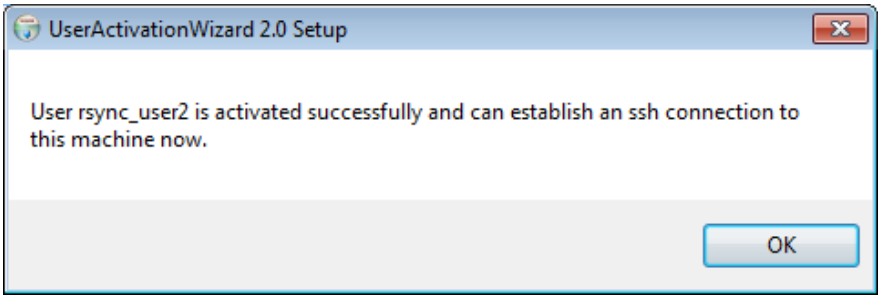
8. Verify details and click “Apply” to activate user.

2.2.4.2 Method 2

1. Use the direct entry under Start Menu → All Programs → Copssh → Activate User.
2. Select the user name from the drop down list, and the other options as in the following figure.
3. Ensure you don't select the option to create keys; these will be created by the MCP.
4. Click on Next.



A confirmation dialog will be presented, click on OK.



3. Configuring MCP Sync Manager

You can configure the settings of the MCP Sync Manager through the **Sync Manager** menu under MCP Config Tool (mcpcfg). MCP applications must be restarted after changes to the configuration of Sync Manager.

3.1 Enable Sync Manager

Enable Sync Manager Application using option "Enable Sync Manager" under "Configure Sync Manager" menu, in the MCP Config Tool (mcpcfg). When Sync Manager is enabled, a private/public key pair is generated.

Note: Files from the MCP are securely copied to the remote device over an SSH connection. To facilitate authentication on this link, a private/public key pair are used.

When a key set is generated, the files are stored in the MCP under **/mnt/datalog/SSHKeys/SyncMgr/**. You should copy the public key file (*id_rsa.pub*) from this location and store it in the appropriate location on the remote device. Refer to chapter 4. Setting up Public Key Authentication for details.

3.2 Configure Sync Sets

Up to 8 sync sets can be created at any time. The following settings can be configured for each set:

Table 1 Configure Sync Sets - Settings

Setting	Description	Range
Sync Set ID	A unique number used by the system to identify the sync set. Not editable; automatically assigned.	Auto-incremented from 1. Once a number has been assigned, it is never reused.
Destination IP Address	The IP address of the enterprise server where the files are to be copied.	Valid IPv4 address belonging to the Windows computer server
Destination User Name	The username used for SSH authentication on the enterprise server.	1 to 128 ASCII characters These are user names activated in section 2.2.3 Create Users in Windows computer
Source Path Name	The absolute directory pathname that will be synched to the remote device. **Note**: ARRM files are kept in **/mnt/datalog/arrm** folder in MCP. You can specify this folder or a device specific sub-folder.	2 to 120 ASCII characters pointing to a valid location on the MCP file system
Destination Path Name	The absolute directory pathname that the files will be copied to. **Note**: If destination folder is C:\ARRM\MCP_1\ on enterprise server, specify destination path name as **/cygdrive/c/ARRM/MCP_1**	2 to 120 ASCII characters pointing to a valid location on the remote device's file system

Setting	Description	Range
Check and rsync Interval	The amount of time, in seconds, that the Sync Manager waits before checking the source path for changes. If changed or created files are detected, an rsync operation is triggered. Typical value: 60 seconds	60 to 86400 seconds
Forced rsync Interval	The amount of time, in seconds, that the Sync Manager waits before a forced rsync operation is triggered, regardless of detected changes. This will recreate files that have been deleted from the remote device as well as forcing the transfer of files whose changes may not have been detected due to MD5 collision, an extremely rare occurrence. Typical value: 300 seconds	60 to 86400 seconds

Notes:

- The Sync Manager will only copy files to the remote Windows-based computer. Files are not deleted from the remote system if these are deleted from the MCP after synchronization. If files are deleted from the remote system, it will be recreated during the next sync operation.
- A forced rsync will be performed upon each startup of your MCP device.
- The path equivalence between the Windows computer file system and the MCP destination path name is as following:

  Windows file system:

  <drive_letter>:\<path1>\<path2>

  MCP Sync Manager destination path:

  /cygdrive/<drive_letter>/<path1>/<path2>

  (the drive letter must be lower case, and path strings same case as seen in Windows file system)

  For e.g.:

  Windows path:

  C:\ARRM\Sub_01

  Corresponds to the following in MCP Sync Manager:

  /cygdrive/c/ARRM/Sub_01

4. Setting up Public Key Authentication

MCP uses public key authentication to authenticate itself to Enterprise Server. When Sync Manager application is enabled in MCP, it creates a public key (**id_rsa.pub**). This public key is required to be transferred to Enterprise Server.

4.1 Update Permissions to SyncMgr Folder

When a key set is generated, the files are stored in `/mnt/datalog/SSHKeys/SyncMgr/`.

To copy the key from this folder to the computer, the permissions of this folder need to be updated after the Sync Manager is enabled (this must be performed every time a new set is generated or after MCP restarts or re-logins).

Upon exiting the MCP Config Tool (mcpcfg), execute the following command at the MCP prompt:

sudo chmod ug+x /mnt/datalog/SSHKeys/SyncMgr

(if prompted for a password, enter the password associated with the root account).

4.2 Copy key from MCP to the Windows computer

1. On the MCP the Sync Manager's public key **id_rsa.pub** is available in **/mnt/datalog/SSHKeys/SyncMger/** folder.

   This key must be transferred to the Windows computer. Depending on the copSSH software version and Windows OS version, the target location of the key file may be different.

2. `<C:\Users\<user name>\.ssh>` folder **is** present
   - If an `\.ssh\` folder exists in the `C:\Users\<user name>` , the public key shall be transferred to that **\.ssh** folder on the Enterprise Server.

3. `<C:\Users\<user name>\.ssh>` folder is **NOT** present
   - If an `\.ssh\` folder does not exist in the `C:\Users\<user name>` , the public key shall be transferred to the installation path of the software, typically:

     "**C:\Program Files\ICW\home\<user name>\.ssh**" on a 32-bit operating system or

     "**C:\Program Files (x86)\ICW\home\<user name>\.ssh**" on a 64-bit operating system.

4. The public key file in the Windows **\.ssh** folder must have the name **authorized_keys**

   There can be only one such file per user.

   First time a MCP is added to a user, rename the copied **id_rsa.pub** to **authorized_keys**

   If configuring multiple MCP units to sync files to an Enterprise Server, using the same user name, the public key content (one text line) from the **id_rsa.pub** of each MCP shall be appended to the already existent **authorized_keys** file on Enterprise Server using a text editor. Each public key is a single line entry in **authorized_keys** file; ensure that it is not broken in multiple lines while copying and pasting.

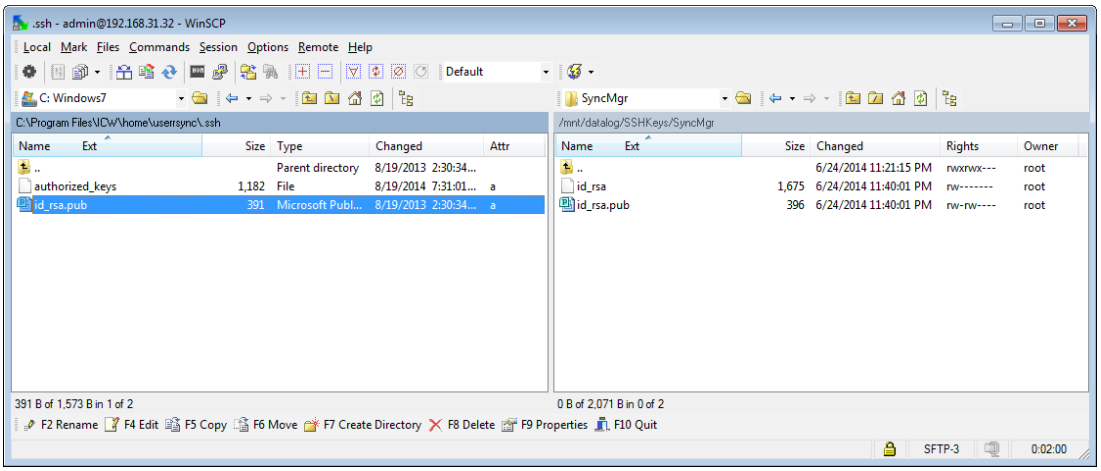
5. Ensure the user permissions are updated as shown in 4.1
6. Transfer Sync Manager's public key to Enterprise Server using WinSCP program or USB pen drive.

   Note: The WinSCP program must be run as administrator by Right click on the program and selecting "Run as administrator".

7. If this is the first MCP-user, rename **id_rsa.pub** to **authorized_keys**

   (In the left-side window of WinSCP, right click on file → Rename), or use a text editor to append the new key to an existing file "authorized_keys".

8. Repeat this for every user and MCP station.



9. Reboot the MCP and the Windows computer.

   The system is now ready to operate.

A. Uninstalling cwRsyncServer and Copssh

This chapter describes how to uninstall cwRsyncServer and Copssh softwares.

1. All active users must be deactivated first. To deactivate a user, use “copSSH User Activation Wizard”. Start “copSSH User Activation Wizard” from Start Menu → All Programs → Copssh → Deactivate Users.
2. Open Services Microsoft Management Console (MMC), from Control Panel → Administrative Tools → Services. Right click on service “Openssh SSHD” and select “Stop” to stop it.
3. Uninstall Copssh software from Start Menu → All Programs → Copssh → Uninstall COPSSH.
4. Uninstall cwRsyncServer software from Start Menu → All Programs → cwRsyncServer → Uninstall cwRsyncServer Server.
5. Delete Copssh service user from Control Panel → User Accounts → Manage User Accounts → Select SvcCOPSSH user → Click “Remove”.
6. Delete cwRsync service user from Control Panel → User Accounts → Manage User Accounts → Select SvcCWRSYNC user → Click “Remove”.

B. Diagnostics

B.1 MCP Diagnostic Logs

- Connect to MCP HMI
- Click on "System Logs" button on the power bar
- Select "Diagnostic Log" tab
- Filter Application field for "B048"
- Export logs to CSV file using "Export data" button
- If rsync command error is reported, check destination IP, user name, destination folder details mentioned in the message.
- If error message "Check destination server connectivity and SSH public key authentication with it" is reported, check:
    - IP connectivity to Enterprise Server
    - Correct installation of cwRwyncServer and Copssh softwares
    - Configuration of SSH keys in Enterprise Server

B.2 Copssh Event Log on Enterprise Server

Depending on the copSSH software application version, the following log may not be available.

- Start "Copssh Control Panel" from Start Menu → All Programs → Copssh → Copssh Control Panel → Go to Status tab.
- Check status of Copssh service
- Open "Copssh events" log; check whether access requests from MCP IP are reaching and successful to Enterprise Server.

C. List of Acronyms

Table 2 List of Acronyms

Abbreviation	Description
SSH	Secure Shell
ARRM	Automatic Record Retrieval Manager
DCA	Data Collection Application
DPA	Data Presentation Application
DTA	Data Translation Application
HMI	Human Machine Interface
IED	Intelligent Electronic Device
RTDB	Real Time Data Base
RTU	Remote Terminal Unit

MODIFICATION RECORD

VERSION	REV.	DATE	CHANGE DESCRIPTION
1.00	0	26th March, 2019	Document created.
2.00	0	22nd April, 2021	Updated for MCP family.
2.00	1	26th April, 2021	Updated Technical Support Contacts.
2.00	2	27th July, 2021	Added clarification about 3rd party tools.

GE
Grid Solutions

LogicLinx on a Multilin MCP Gateway Device

Quick Start Guide

LogicLinx* is an automation tool that enables you to create applications that have traditionally been too costly or difficult to implement – without the need for hardwiring. Using any or all the IEC® 61131-3 programming languages, you can create automation routines that run on your Multilin™ MCP gateway device.

NOTE: This document applies to the MCP family (G100/G500) unless otherwise indicated.

Prerequisites

Before you can configure LogicLinx on your Multilin™ MCP gateway device, the following components must be present:

- An MCP gateway device connected to the configuration computer through a serial or Ethernet connection.
- MCP Studio™ V2.3 or higher with LogicLinx Wizard add-in installed on the configuration computer.
- LogicLinx editor installed on the configuration computer.

Differences between the 16-bit and the 32-bit versions of the LogicLinx editor

- The 16-bit version only runs on 32-bit versions of the Windows operating system while the 32-bit version runs on both 32-bit and 64-bit versions of the Windows operating system.
- The 16-bit version requires users to run as administrators while the 32-bit version does not have this constraint.
- The 32-bit version allows users to compare LogicLinx programs in two different devices.
- Instruction language (IL) programs cannot be created or modified in the 32-bit version. Existing programs can be compiled and modified using a text editor.
- Function chart (FC) programs cannot be created or modified in 32-bit version. Existing programs can be compiled.
- Most programs created and modified in the 32-bit version can be opened in the 16-bit version provided they do not exceed the maximums for names, descriptions, and other artefacts of the 16-bit version.
- The user-interface in the 32-bit version is based on Visual Studio. Most of the functions previously available through the toolbar and menus in the 16-bit version are now available using a combination of the Solution Explorer and Properties windows of the 32-bit version.
- The Dictionary in the 16-bit version is now called Global Variables in the 32-bit version.
- Compile and Make operations in the 16-bit version are called Build in the 32-bit version.
- To set the target in the 32-bit version, you need to click on the drop-down in the Solution Explorer.
- To do simulation in the 32-bit version, you need to explicitly select the Simulate target for a program, build it and then switch to Online mode.
- You need to choose 'Online' mode to start real-time debugging in the 32-bit version.

To configure LogicLinx on your MCP gateway device:

Before LogicLinx can run on your MCP gateway device, you must configure the automation application.

1. Launch MCP Studio™ and open a project containing the MCP gateway device you want to configure LogicLinx on.

2. Select the MCP gateway device.
3. On the **Configure** tab, click **Wizard**.
4. On the welcome page of the wizard, click **Next**.
5. On the **Select Task** page of the wizard, select **Proceed to Configuration** and click **Next**.
6. On the **Connection** page of the wizard, select either Serial Port or Ethernet as the connection type to your MCP gateway device. If Ethernet is selected, Secure Debugger option is required between debugger and MCP gateway device. Based on the option you chose, configure the connection parameters and click **Next**.

   NOTICE The Secure Debugger connection is only made available for users of the following groups: Admin and Supervisor.

7. On the **Define Owned Points** page of the wizard, create your LogicLinx-owned points. For information on owned points, refer to *Owned and Mapped Points* below.

   » To create owned points:
   a) A tab is shown for each point type. Within each tab, click the **Add Point** button to insert a new row in the list.
   b) Click the cells in the new row to modify the default values.
   c) Once you have finished creating your LogicLinx owned points, click **Next**.

8. On the **Define Mapped Points** page of the wizard, select the MCP gateway device database points you want to give LogicLinx access to. For information on mapped points, refer to ***Owned and Mapped Points*** below.

   » To map points:
   a) All available points within the MCP gateway device are shown as a tree list. Click the **+** next to each entry to expand the list and view the points contained within.
   b) To select a point, select the checkbox in the **Map?** field. The point will be added to the **Mapped Points**.
   c) On the **Mapped Points** screen, you can review the selected points and modify the LogicLinx tag name from the default value.
      Tip: Internal transition counters can be added to digital input points. For more information, refer to *Internal Transition Counters* below.
   d) Mapped points shown with a red background have been invalidly mapped; these points do not exist within the Gateway device system point database. This can cause errors when running LogicLinx programs. To correct this, select the row and click **Delete invalid mapping**.
   e) Once you have finished mapping points from the Gateway device, click **Next**.

9. The LogicLinx editor is shown on the next page of the wizard. You can create and save your LogicLinx automation programs at this time. Once finished, click **Next**.

   To allow your LogicLinx programs to execute on the MCP gateway device, you must ensure that the **target** setting is correctly configured.

   » To ensure that the target setting is correctly configured:
   a) On the toolbar, select **Make** > **Compiler Options**.
   b) On the **Compiler Options** window, highlight *ISA86M: TIC code for Intel* and click **Select**. Once an arrow is added next to *ISA86M: TIC code for Intel*, click **OK**.
   c) On the program window, click **Make** > **Make Application**. The program is compiled.

10. On the completion page, click either:
    - **Exit & Save Changes** to save the configuration, or
    - **Exit & Discard Changes** to ignore the configuration.

11. Select the MCP gateway device. On the **Configure** tab, click **Sync To Device** to upload the configuration to your MCP gateway device. Once the synchronization is complete, the MCP gateway device restarts and loads LogicLinx.

Note: If the point mappings on your MCP gateway device are modified through the Online Configuration Tool after you have uploaded your configuration, you must synchronize the updated MCP gateway device configuration within MCP Studio to ensure that your LogicLinx mappings are still valid. To do this, select your MCP gateway device and click **Sync From Device** on the **Configure** tab. Once the synchronization is complete, click **Validate**. If any errors are reported, correct them by repeating the steps above.

Owned and Mapped Points

LogicLinx-owned points provide an interface between LogicLinx and other c device applications. From LogicLinx's perspective, the direction of these owned points is reversed compared to other mapped system points. Owned *input* points can be written to by LogicLinx to provide data to other applications. Owned *output* points can be used by external applications to send data into LogicLinx, allowing LogicLinx programs to read these values. LogicLinx documentation refers to these reverse-direction points as "conversion points".

Mapped points are those that are owned by applications external to LogicLinx. All system points in the MCP gateway device are available as mapped points, including LogicLinx-owned points. Each system point is assigned a unique tag name, with which the point is referenced as a LogicLinx variable in the Editor.

Internal Transition Counters

Since LogicLinx works on a cyclical basis, it may miss state changes on digital inputs that occur between input refresh cycles. To account for this, LogicLinx allows you to enable internal transition counters on digital inputs. The input point is monitored for changes between cycles and if a state change is detected, the associated internal transition counter is incremented. The internal transition counter variable reports the total number of state changes that occurred on the associated digital input during the previous cycle.

To add an internal transition counter to a digital input point, select the point and click **Add Internal Transition Counter**. A sub-row is added containing the default tag name for the counter.

Frequently Asked Questions

Q: Does LogicLinx on the MCP gateway device support files (that is, F_ROPEN, FX_READ, F_CLOSE, etc.)? If so, what paths do I have access to?

A: Yes, currently, all files and paths are available. Files can be stored in **`/tmp`** if they are small and do not need to be retained across a reboot. Otherwise, you may use **`/mnt/datalog`**, which is the largest partition on the user CompactFlash card.

Q: Does LogicLinx on the MCP gateway device support initial values for AO and DO, similar to the D20*/D200*?

A: Yes, initial values for AOs and DOs are supported in MCP family after firmware version 2.2.

Q: Does LogicLinx on the MCP gateway device support restore last value at startup for AO and DO similar to the D20*/D200*?

A: No, restoring of last values for AOs and DOs are not currently supported in MCP family.

Q: Does LogicLinx on the MCP gateway device support the OPERATE function (similar to the D20/D200)?

A: Yes, the OPERATE function is the same as on the D20/D200.

Q: Does LogicLinx on the MCP gateway device support multiple targets on a single MCP gateway device?

A: No, only one target is currently supported on the MCP gateway device.

Q: Does the MCP gateway device support a "Communications Watchdog" feature (similar to the D20/D200)?

A: The MCP gateway device supports watchdog-style monitoring via two methods:

- Every client application provides a digital input for every device that indicates when that device is online. There are also other points such as transaction counts and failure counts that can be used.
- The Calculator on the MCP gateway device allows you to create digital inputs that reflect a selected quality flag from a specific point, allowing you to monitor offline, loss of communications, scan inhibit, or any other quality flag that is reported. These points do not go offline when the point does, as other expressions would do.

By using these methods, you can monitor the health of an entire device (useful to reduce the number of pseudo points and the number of logic elements in a program) or to monitor selected points individually (separates the points from the device but requires more pseudo points). The first option is preferred when you have many points to monitor, while the second option allows for more granularity and is suggested for small numbers of points. You may also combine the two options by using Calculator to monitor the quality of a single representative point from a device.

Additional Documents

For further information about LogicLinx and the MCP gateway device, refer to the following documents:

- *LogicLinx IEC 61131-3 Soft Logic Getting Started* (SWM0018)
- *LogicLinx IEC 61131-3 Soft Logic User's Guide* (SWM0019)

Product Support

If you need help with any aspect of your GE Grid Solutions product, you can:

- Access the GE Grid Solutions Web site
- Search the GE Grid Solutions Technical Support library
- Contact GE Grid Solutions Technical Support

GE Grid Solutions Web Site

The GE Grid Solutions Web site provides fast access to technical information, such as manuals, release notes and knowledge base topics. Visit us on the Web at: http://www.gegridsolutions.com

GE Grid Solutions Technical Support Library

This site serves as a document repository for post-sales requests. To *get* access to the Technical Support Web site, go to: http://sc.ge.com/*SASTechSupport

Contact GE Grid Solutions Technical Support

For help with any aspect of your GE Grid Solutions product, please contact our support team, 24/7, as follows:

Region	E-mail	Telephone
Global Contact Centre	ga.support@ge.com	+44 1785 250070
Central and East Asia and Pacific	ga.supportCEAP@ge.com	+61 414 730 964
India	ga.supportIND@ge.com	+91 44 22648000
Middle East, North Africa and Turkey	ga.supportMENAT@ge.com	+971 42929467
Europe, Russia, CIS and Sub-Saharan Africa	ga.supportERCIS@ge.com	+34 94 4858854
North America	ga.supportNAM@ge.com	+1 877 605 6777
Latin America	ga.supportLAM@ge.com	+55 11 36187308

Copyright Notice

© 2021, General Electric Company. All rights reserved.

The Software Product described in this documentation may only be used in accordance with the applicable License Agreement. The Software Product and Associated Material are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable, and are delivered with Restricted Rights. Such restricted rights are those identified in the License Agreement, and as set forth in the "Restricted Rights Notice" contained in paragraph (g) (3) (Alternate III) of FAR 52.227-14, Rights in Data-General, including Alternate III (June 1987).

If applicable, any use, modification, reproduction release, performance, display or disclosure of the Software Product and Associated Material by the U.S. Government shall be governed solely by the terms of the License Agreement and shall be prohibited except to the extent expressly permitted by the terms of the License Agreement.

The information contained in this online publication is the exclusive property of General Electric Company, except as otherwise indicated. You may view, copy and print documents and graphics incorporated in this online publication (the "Documents") subject to the following: (1) the Documents may be used solely for personal, informational, non-commercial purposes; (2) the Documents may not be modified or altered in any way; and (3) General Electric Company withholds permission for making the Documents or any portion thereof accessible via the internet. Except as expressly provided herein, you may not use, copy, print, display, reproduce, publish, license, post, transmit or distribute the Documents in whole or in part without the prior written permission of General Electric Company. If applicable, any use, modification, reproduction, release, performance, display, or disclosure of the Software Product and Associated Material by the U.S. Government shall be governed solely by the terms of the License Agreement and shall be prohibited except to the extent expressly permitted by the terms of the License Agreement.

The information contained in this online publication is subject to change without notice. The software described in this online publication is supplied under license and may be used or copied only in accordance with the terms of such license.

Trademark Notice

GE and the GE monogram are trademarks and service marks of General Electric Company. * Trademarks of General Electric Company. IEC is a registered trademark of Commission Electrotechnique Internationale. Other company or product names mentioned in this document may be trademarks or registered trademarks of their respective companies.

Modification Record

Version	Revision	Date	Change Description
1.00	0	30th January, 2019	Created.
2.00	0	23rd April, 2021	Updated for MCP family.
	1	26th April, 2021	Updated Technical Support Contacts.

GE
Grid Solutions

Secure Integration of SCADA Third Party Equipment with the MCP

Configuration Guide

SWM0109

Version 2.00 Revision 2

Associated Software Release: Version 1.00 and above

imagination at work

General

COPYRIGHT NOTICE

© 2021, General Electric Company. All rights reserved.

The Software Product described in this documentation may only be used in accordance with the applicable License Agreement. The Software Product and Associated Material are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable, and are delivered with Restricted Rights. Such restricted rights are those identified in the License Agreement, and as set forth in the "Restricted Rights Notice" contained in paragraph (g) (3) (Alternate III) of FAR 52.227-14, Rights in Data-General, including Alternate III (June 1987).

If applicable, any use, modification, reproduction release, performance, display or disclosure of the Software Product and Associated Material by the U.S. Government shall be governed solely by the terms of the License Agreement and shall be prohibited except to the extent expressly permitted by the terms of the License Agreement.

The information contained in this online publication is the exclusive property of General Electric Company, except as otherwise indicated. You may view, copy and print documents and graphics incorporated in this online publication (the "Documents") subject to the following: (1) the Documents may be used solely for personal, informational, non-commercial purposes; (2) the Documents may not be modified or altered in any way; and (3) General Electric Company withholds permission for making the Documents or any portion thereof accessible via the internet. Except as expressly provided herein, you may not use, copy, print, display, reproduce, publish, license, post, transmit or distribute the Documents in whole or in part without the prior written permission of General Electric Company. If applicable, any use, modification, reproduction, release, performance, display, or disclosure of the Software Product and Associated Material by the U.S. Government shall be governed solely by the terms of the License Agreement and shall be prohibited except to the extent expressly permitted by the terms of the License Agreement.

The information contained in this online publication is subject to change without notice. The software described in this online publication is supplied under license and may be used or copied only in accordance with the terms of such license.

TRADEMARK NOTICES

GE and are trademarks and service marks of General Electric Company.

* Trademarks of General Electric Company.

Serial/IP is a registered trademark of Tactical Software, LLC.
Tactical Software is a registered trademark of Tactical Software, LLC.

Other company or product names mentioned in this document may be trademarks or registered trademarks of their respective companies.

Contents

About this Document 9

Purpose 9
Intended Audience 9
Additional Documentation 9
Safety words and definitions 9

Product Support 11

GE Grid Solutions Web Site 11
GE Technical Support Library 11
Contact Technical Support 11

1. Overview 12

1.1 Supported Client Devices 12
1.2 Setup Procedure 12
1.3 Certificate Revocation 13

2. Setting up a Certification Authority 14

2.1 Cipher Suites 14
2.2 Setting up the XCA Certification Authority 15

3. Certificate Generation 18

3.1 Generating Certificates Using XCA 18

4. Installing Certificates 23

4.1 Installing CA Certificate, Server Certificate and Diffie Hellman Parameters on the MCP 23
4.2 Installing CA Certificate and Client Certificate for use by a PC Client 25

5. Configuring Secure Connections on the MCP 26

5.1 Configuring a Secure Terminal Server Connection 26
5.2 Configuring a Secure Pass-through Connection 27
5.3 Configuring a Secure Connection Relay 29
5.4 Secure Application Parameters Dialog 29

6. Configuring a Secure Connection with Tactical Software Serial IP 31

6.1 Configuring Tactical Software Serial IP with Encryption 31

7. Configuring a Secure Connection with Stunnel 35

7.1 Configuring Stunnel 35
7.2 Configuring the Client Program 37

8. Revoking a client certificate 38

8.1 Revoking the Certificate in XCA 38
8.2 Exporting the CRL in XCA 38
8.3 Installing the CRL in the MCP 39

A. Error Messages 40

B. Connection Security 41

C. List of Acronyms 43

Figures

No table of figures entries found.

Tables

Table 1: Cipher Suites Supported by the MCP 14
Table 2 Example Distinguished Name Components 15
Table 3 Example Distinguished Name Components 19
Table 4 Example Distinguished Name Components 21
Table 5 Location of Files Exported by Certification Authorities 23
Table 6: Error Messages 40
Table 7 List of Acronyms 43

About this Document

Purpose

This document describes how to establish a secure channel between a client device and the MCP for accessing a protected service in the substation. This document outlines and details the procedures regarding:

- The implementation of a simple Certification Authority using XCA Certification Authority (Open Source tool).
- The installation of certificates on the MCP and Windows PC running Tactical Software Serial/IP or Stunnel.
- The configuration of Tactical Software Serial/IP and Stunnel to communicate to the MCP over TLS sessions.

NOTICE **This document applies to the MCP family (G100/G500) unless otherwise indicated.**
Screen captures may show G500 in some areas, however the workflow applies to products in the MCP family (G100/G500).

Intended Audience

This document serves as a reference for systems integrators who wish to setup a secure channel using Tactical Software Serial/IP or Stunnel with a MCP for the purposes of accessing a protected service in the substation.

Additional Documentation

For further information about the Secure Integration of SCADA Third Party Equipment with the MCP, refer to the following documents:

- MCP Substation Gateway, Software Configuration Guide
- MCP Substation Gateway, HMI Online Help

Safety words and definitions

Before attempting to install or use the device, review all safety indicators in this document to help prevent injury, equipment damage or downtime.

The following safety and equipment symbols are used in this document:

⚠DANGER **Indicates a hazardous situation which, if not avoided, will result in death or serious injury.**

⚠WARNING **Indicates a hazardous situation which, if not avoided, could result in death or serious injury.**

⚠CAUTION Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

NOTICE Indicates practices that are not related to personal injury.

Product Support

If you need help with any aspect of your GE Grid Solutions product, you can:

- Access the GE Grid Solutions Web site
- Search the GE Technical Support library
- Contact Technical Support

GE Grid Solutions Web Site

The GE Grid Solutions Web site provides fast access to technical information, such as manuals, release notes and knowledge base topics.

Visit us on the Web at: http://www.gegridsolutions.com

GE Technical Support Library

This site serves as a document repository for post-sales requests. To *get* access to the Technical Support Web site, go to: http://sc.ge.com/*SASTechSupport

Contact Technical Support

For help with any aspect of your GE Grid Solutions product, please contact our support team, 24/7, as follows:

Region	E-mail	Telephone
Global Contact Centre	ga.support@ge.com	+44 1785 250070
Central and East Asia andPacific	ga.supportCEAP@ge.com	+61 414 730 964
India	ga.supportIND@ge.com	+91 44 22648000
Middle East, North Africa andTurkey	ga.supportMENAT@ge.com	+971 42929467
Europe, Russia, CIS and Sub-Saharan Africa	ga.supportERCIS@ge.com	+34 94 4858854
North America	ga.supportNAM@ge.com	+1 877 605 6777
Latin America	ga.supportLAM@ge.com	+55 11 36187308

1. Overview

This document describes how to establish a secure channel between a client device and the MCP for accessing a protected service in the substation. The secure channel is implemented using a TLS (Transport Layer Security) connection and certificate-based mutual authentication. A client device could be a PC with Tactical Software Serial/IP or Stunnel, SCADA master that supports TLS and mutual authentication using certificates.

Certificates are issued by a Certification Authority (CA). The MCP does not come with a CA so you must make use of an existing CA or create your own. There are many third-party commercial and open source CAs available. This document describes one open source CA packages: X Certificate and Key Management (XCA).

1.1 Supported Client Devices

1.1.1 Tactical Software Serial/IP with Encryption

Tactical Software Serial/IP is a virtual serial port package that can be installed on a Windows-based PC. Virtual serial port software allows programs that would normally communicate to an IED using the serial port on the local PC to communicate with the IED using the serial port on a remote MCP. It does this by relaying the serial traffic over a TCP connection to the MCP, which then relays the data over the serial port. Tactical Software Serial/IP can use an TLS channel to securely relay the serial traffic to the MCP. This document describes how to configure Tactical Software Serial/IP and the MCP for this purpose.

1.1.2 Stunnel

Stunnel is an open source package that can be installed on a Windows-based PC to relay a local TCP connection over an TLS tunnel to a remote MCP, which then relays data over a TCP connection to an IED on the substation LAN. Stunnel can be configured to provide an TLS channel for programs that would access IEDs over a TCP connection. This document describes how to configure Stunnel and the MCP for this purpose.

1.1.3 SCADA Master

The SCADA Master is any SCADA master that supports TLS and mutual authentication using certificates.

1.2 Setup Procedure

To establish a secure channel between a client device and the MCP:

1. Setup your CA – see section 2.
2. If you plan to use ciphers that use the Diffie Hellman Key Exchange Algorithm (indicated by the dhe prefix in the cipher name), generate Diffie Hellman (DH) parameters – see section 2.

3. Install the CA's Certificate on your MCP and client device – see section 2.
4. Generate private keys and certificates for your MCP and client device.
5. Install the private keys, certificates and optional Diffie Hellman parameters on your MCP and client device.
6. Using the MCP online configuration, configure the parameters for the TLS channels.
7. Using the client software, configure the parameters for the TLS channel.
8. Connect your client software with the MCP and test access to the protected service.

1.3 Certificate Revocation

Together with a private key and a certificate, a client device can prove its identity to the MCP. If a malicious user ever discovered your private key, the malicious user would be able to access the MCP masquerading as you. The moment you are aware of a security breach that may involve the private key, you should revoke the associated certificate. If a certificate is revoked, the MCP does not accept any connections that use a revoked certificate.

Another reason for revoking a certificate may be that the owner of the certificate has left the company and no longer needs to connect to the MCP. Revoking the certificate prevents that person from accessing the MCP even if the person retained his or her private key.

To revoke a certificate:

1. Revoke the certificate on the CA – See section 8.1.
2. Generate a new Certificate Revocation List (CRL) – See section 8.2.
3. Install the CRL on the MCP – See section 8.3.

For information on Connection Security, see Appendix B: Connection Security.

2. Setting up a Certification Authority

Before you can configure a secure channel between a client device and the MCP you need a Certification Authority (CA). In case you don't already have a CA, this section describes how to set up the XCA certification authority.

Once your CA is up and running, export the CA certificate so that you can install it on the client devices and the MCP.

NOTICE A CA that is planned for field use should be protected with strong security measures. Such measures include dedicating a machine for the CA, physically securing the machine, ensuring the machine is accessible only by authorized users, and not connecting the machine to a network. Such measures are required because a security breach of a CA would impact all devices that used certificates generated by the CA.

2.1 Cipher Suites

Before you choose XCA or any other Certification Authority, there are a few differences you should be aware of:

- The MCP supports a fixed set of cipher suites as shown in the Table 1: Cipher Suites Supported by the MCP.
- Depending on which ciphers you use, the CA may or may not be suitable. Diffie Hellman (DH) parameters are required if the Key Exchange Algorithm is Diffie Hellman Ephemeral (DHE). XCA generates DH parameters.
- A DSA certificate for MCP is required for a DSS Signature. An RSA certificate for MCP is required for an RSA signature. XCA generates both DSA and RSA certificates.

Table 1: Cipher Suites Supported by the MCP

Key Exchange		Encryption	Hash	Works with XCA ?
Algorithm	Signature			
RSA		NULL	SHA	Yes
RSA		NULL	SHA256	Yes
RSA		WITH_3DES_EDE_CBC	SHA	Yes
RSA		WITH_AES128_CBC	SHA256	Yes
DHE		WITH_AES128_CBC	SHA256	Yes
DHE	DSS	WITH_3DES_EDE_CBC	SHA	Yes
DHE	RSA	WITH_3DES_EDE_CBC	SHA	Yes
DHE	RSA	WITH_AES_128_CBC	SHA	Yes
DHE	DSS	WITH_AES_128_CBC	SHA	Yes

DHE	DSS	WITH_AES_256_CBC	SHA	Yes
DHE	RSA	WITH_AES128_GCM	SHA256	Yes
DHE	RSA	WITH_AES256_GCM	SHA384	Yes
ECDHE	RSA	WITH_AES128_GCM	SHA256	Yes
ECDHE	RSA	WITH_AES256_GCM	SHA384	Yes
ECDHE	ECDSA	WITH_AES128_GCM	SHA256	Yes
ECDHE	ECDSA	WITH_AES256_GCM	SHA384	Yes

2.2 Setting up the XCA Certification Authority

XCA runs on Linux or Microsoft Windows. The following steps detail how to setup and initialize an XCA certification authority.

2.2.1 Install XCA

1. Download the latest version of XCA from here: http://sourceforge.net/projects/xca.
2. Run the installation wizard to install XCA.

2.2.2 Create a Database and Initialize the CA

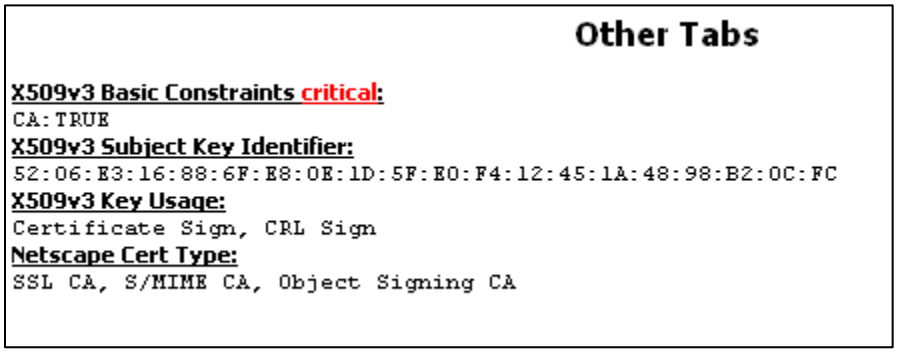
1. From XCA, select **File** > **New Database**.
2. Choose a protected location to save the database and then enter a strong password to encrypt the database.
3. Under the **Certificates** tab, choose **New Certificate**.
4. Under the **Source** tab, select the checkbox next to the label **Create a self signed certificate with the serial**. Leave the dropdown named **Signature Algorithm** as "SHA 256" and leave the dropdown named **Template for the new certificate** as "[default] CA".
5. Under the **Source** tab, click **Apply All**.
6. Under the **Subject** tab, click the button labeled **Generate a new key**.
7. In the dialog that appears, enter the name of the CA (e.g., "MyCA") in the **Name** field. Choose the **Keytype** as RSA or DSA to match the type of cipher suites you wish to use (see Table 1). Change the **Keysize** to 2048 and click **Create.**
8. Under the **Subject** tab, enter the distinguished name of the CA certificate. The following table provides example distinguished name components.

Table 2 Example Distinguished Name Components

Distinguished Name Component	Example
Internal name	MyCA
countryName	US

Distinguished Name Component	Example
stateOrProvinceName	MyState
localityName	MyCity
organizationName	MyCompany
organizationalUnitName	MyDivision
commonName	MyCA
emailAddress	mail@my.domain

9. Under the **Extensions** tab, if necessary, change the **Time Range** that the CA certificate is valid for and click **Apply**. The default is 10 years. Certificates generated with this CA certificate after this period are no longer valid.
10. Under the **Key usage** tab, do not change the defaults.
11. Under the **Netscape** tab, remove the value in the **Comment** field.
12. Under the **Advanced** tab, the following messages are expected except the value of the X509v3 Subject Key Identifier, which differs from key to key:



If above message is not displayed, click **Validate** to see the message.

13. Click **OK**. You now have a CA certificate to sign your MCP and Client certificates.
14. Under the **Certificates** tab of the main view of XCA, select the new Certification Authority and click on **Export**.
15. Ensure the **Export Format** is set to PEM.
16. Browse to a protected directory (e.g., My Documents->MyXCAFiles) and click **Save**. Finally click **OK**. The file is named based upon the internal name of your CA with a .crt extension.

2.2.3 Generate Diffie Hellman (DH) Parameters

1. From XCA, select **Extra** > **Generate DH parameter**.
2. Enter a key size of 2048 and click **OK**.
3. It may take a few minutes for the parameters to be generated and XCA may appear to be non-responsive. Be patient and allow XCA to complete.

4. When prompted, save the generated DH parameters file in a protected location (e.g., My Documents->MyXCAFiles) and leave the name as dh2048.pem.

3. Certificate Generation

This chapter describes how to generate private keys and certificates for both the Client computer and the MCP. These certificates allow the Client to authenticate itself to the MCP and the MCP to authenticate itself to the Client.

There are two types of certificates you can generate: a server certificate and a client certificate. The server certificate identifies a MCP. The client certificate identifies a user or a computer that is connected to the MCP.

If users are accessing the MCP directly from their own computers using programs such as Stunnel or Tactical Software Serial/IP to establish a secure channel, then you must generate separate certificates for each user.

If you are using a centralized access server such as ESNET, you have the option of creating only one computer certificate for the ESNET server. However, the centralized access computer must be locked down in such a way as to prevent users from getting direct access to the private key of this computer certificate. If a user could copy the private key, the user could access the MCP from any computer. This would allow the user to bypass any access controls that you put in place through the centralized access computer's security policy.

If you are accessing the MCP from SCADA master stations, then you must generate separate certificates for each master station.

NOTICE

It is important to keep the private keys associated with the Client and Server Certificates secure. For example, they should not be transmitted over the LAN unless you are using a strongly authenticated secure transport mechanism such as SSH with public/private key authentication or multi-factor authentication. Once the private keys reach their destination, they should be deleted from any devices used to transport them (e.g., a USB drive or laptop).

3.1 Generating Certificates Using XCA

3.1.1 Generating a MCP Server Certificate

A MCP Server certificate allows the MCP to authenticate itself to a Client. The MCP Server certificate contains a **commonName** field. This field should uniquely identify the MCP in your network. Follow these steps to generate a MCP Server Certificate.

1. Launch XCA from the Windows Programs menu.
2. In the tree view of the **Certificates** tab, select the branch containing your Certification Authority.
3. Under the **Certificates** tab, click the **New Certificate** button.
4. Under the **Source** tab:

a. Select the checkbox next to the label **Use this Certificate for signing**. On the dropdown to the right of this checkbox, select the CA you created in section 2.2.2 (e.g., MyCA).

b. Leave the dropdown **Signature Algorithm** as SHA 256.

c. Change the dropdown **Template for the new certificate** to "[default] HTTPS_server".

d. Click **Apply all**.

5. Under the **Subject** tab, click the **Generate a new key** button.

6. In the dialog that appears, enter a name that uniquely identifies the MCP in your network (for this example, that is "MyMCP"). Choose **Keytype** as RSA or DSA to match the type of cipher suites you wish to use (see Table 1). Change the **Keysize** to 2048. Click **OK**.

7. Back in the **Subject** tab, enter the Distinguished name of the MCP server certificate. The most important component is the ***commonName***. This is the name that your Clients is configured to accept. Any difference between the commonName of the certificate and the name configured in the Client results in a failed connection. Choose other name components that are appropriate for your company. The following table provides example distinguished name components.

Table 3 Example Distinguished Name Components

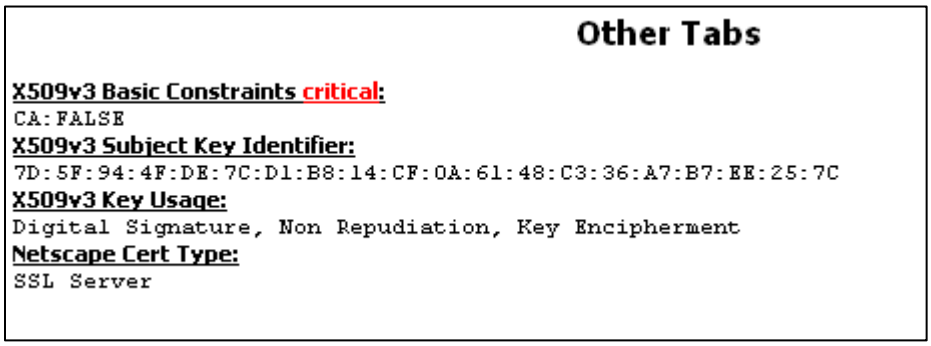
Distinguished Name Component	Example
Internal name	MyMCP
countryName	US
stateOrProvinceName	MyState
localityName	MyCity
organizationName	MyCompany
organizationalUnitName	MyDivision
commonName	**MyMCP**
emailAddress	mail@my.domain

8. Under the **Extensions** tab, if necessary, change the **Time Range** that the CA certificate is valid for and click **Apply**. The default is one year. The shorter the Time Range the more secure the certificate. The longer the Time Range, the more often you need to regenerate MCP Server certificates and deploy them into your MCPs.

9. Under the **Key usage** tab, leave the defaults.

10. Under the **Netscape** tab, remove the comment.

11. Under the **Advanced** tab, click **Validate**. The following messages are expected except the value of the X509v3 Subject Key Identifier, which differs from key to key:



If above message is not displayed, click **Validate** to see the message.

12. Click **OK**. You now have a MCP Server certificate.
13. In the tree view under the **Certificates** tab, open the branch labeled after your Certificate Authority, and select the new Server certificate.
14. Click **Export.**
15. In the dialog that appears, ensure the **Export Format** field is set to "PEM + key (*.pem)". Browse to a protected location (e.g., My Documents->MyXCAFiles) and click **Save**. Finally click **OK.** The certificate and private key will be in a file named with your MCP's Internal Name with the extension .pem (e.g., MyMCP.pem).

NOTICE This file is sensitive so keep it protected always. Remove the file after it has been installed on the MCP.

3.1.2 Generating a Client Certificate

A Client certificate allows the Client to authenticate itself to a MCP. The Client certificate contains a **commonName** field. If you are configuring a SCADA master to access the MCP, this name should identify a unique name for SCADA master. If users connect directly to the MCP from their own computers, this name should identify the user.

To generate a Client certificate:

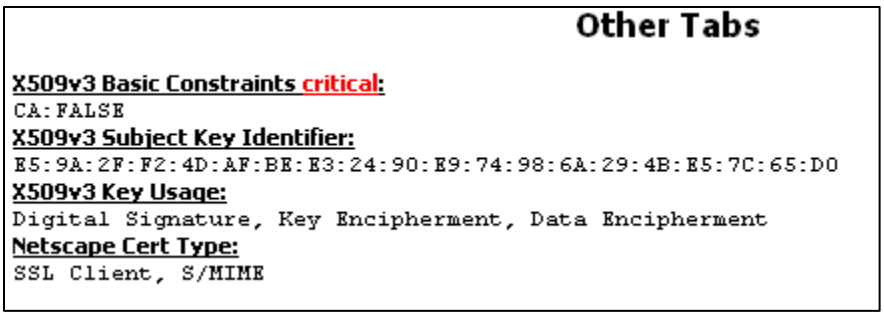
1. Launch XCA from the Windows Programs menu.
2. In the tree view of the **Certificates** tab, select the branch containing your Certification Authority.
3. Under the **Certificates** tab, click the **New Certificate** button.
4. Under the **Source** tab,
    a. Select **Use this Certificate for signing** checkbox. On the dropdown to the right of this checkbox, select the CA you created in section 2.2.2 (e.g., MyCA).
    b. Leave the dropdown **Signature Algorithm** as "SHA 256".
    c. Change the dropdown **Template for the new certificate** to "[default] HTTPS_client".
    d. Click **Apply all**.
5. Under the **Subject** tab, click the **Generate a new key** button**.**

6. In the dialog that appears, enter a name that uniquely identifies the Client (for this example, that is "MyName"). Choose **Keytype** as RSA or DSA to match the type of cipher suites you wish to use (see Table 1). Change the **Keysize** to 2048. Click **OK**.
7. Back in the **Subject** tab, enter the Distinguished name of the Client certificate. The most important component is the ***commonName***. This is the name that the MCP is configured to accept. Any difference between the commonName of the Client certificate and the name configured in the MCP results in a failed connection. Choose other name components that are appropriate for your company. The following table provides example distinguished name components.

Table 4 Example Distinguished Name Components

Distinguished Name Component	Example
Internal name	MyName
countryName	US
stateOrProvinceName	MyState
localityName	MyCity
organizationName	MyCompany
organizationalUnitName	MyDivision
commonName	MyName
emailAddress	mail@my.domain

8. Under the **Extensions** tab, if necessary, change the **Time Range** that the CA certificate is valid for and click **Apply**. The default is one year. The shorter the Time Range the more secure the certificate. The longer the Time Range, the more often you need to regenerate Client certificates and deploy them into Clients.
9. Under the **Key usage** tab, leave the defaults.
10. Under the **Netscape** tab, remove the comment.
11. Under the **Advanced** tab, click **Validate**. The following messages are expected except the value of the X509v3 Subject Key Identifier, which differs from key to key:



If above message is not displayed, click **Validate** to see the message.

12. Click **OK**. You now have a Client certificate.
13. In the tree view of the **Certificates** tab, open the branch labeled with your Certification Authority and select the new Client certificate.

14. Click **Export.**
15. In the dialog that appears, ensure the **Export Format** field is set to "PEM Cert + key". Browse to a protected location (e.g., My Documents->MyXCAFiles) and click **Save**. Finally click **OK.** The client certificate and its private key are stored in a file named with the Internal Name of your client certificate and the .pem extension (e.g., MyName.pem).

NOTICE This file is sensitive so keep it protected always. Remove the file after it has been installed on the client.

4. Installing Certificates

This chapter describes how the CA Certificate, Server Certificate, Client Certificates and DH Parameters are installed. The following table summarizes where to get the files containing the CA certificate, Server certificates, Client Certificates and DH parameters.

Table 5 Location of Files Exported by Certification Authorities

Files	Location
CA Certificate	The CA certificate is in a file downloaded to a location of your choice as described in Section 2.2.2 . The file is named with a .crt extension (e.g., MyCA.crt).
Server Certificate and Key	Server certificate and key are in the same file under the location of your choice as described in Section 3.1.1 . The file is named with a .pem extension (e.g., MyMCP.pem).
Client Certificate and Key	Client certificate and key are in the same file under the location of your choice as described in Section 0. The certificate is in a file named with a .pem extension (e.g., MyName.pem).
DH Parameters	DH parameters are in the file named dh2048.pem under the location of your choice as described in Section 2.2.3 .

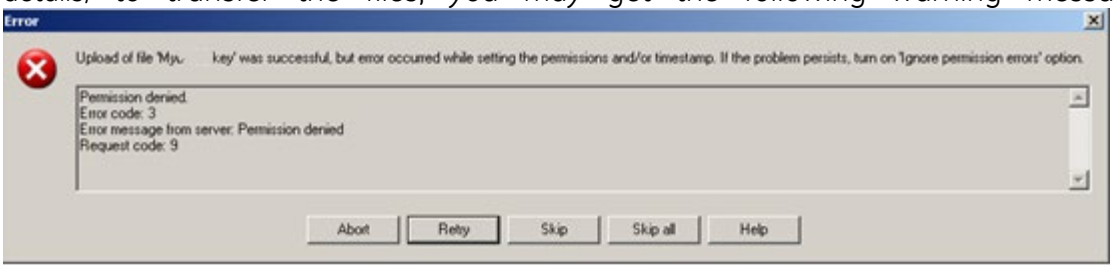
4.1 Installing CA Certificate, Server Certificate and Diffie Hellman Parameters on the MCP

1. Referring to Table 5 for file names and locations, copy the files containing the CA certificate, Server certificate, and DH parameters to one of two locations:
   - The folder /mnt/usr/SecureScadaTransfer on the MCP. In this case, use an SFTP/SCP file transfer program such as WinSCP or Secure File Browser (Refer to Appendix B in SWM0101/15 for details).
   - The directory \SecureScadaTransfer on a USB drive.

   Note: Do not install client certificates on the MCP.

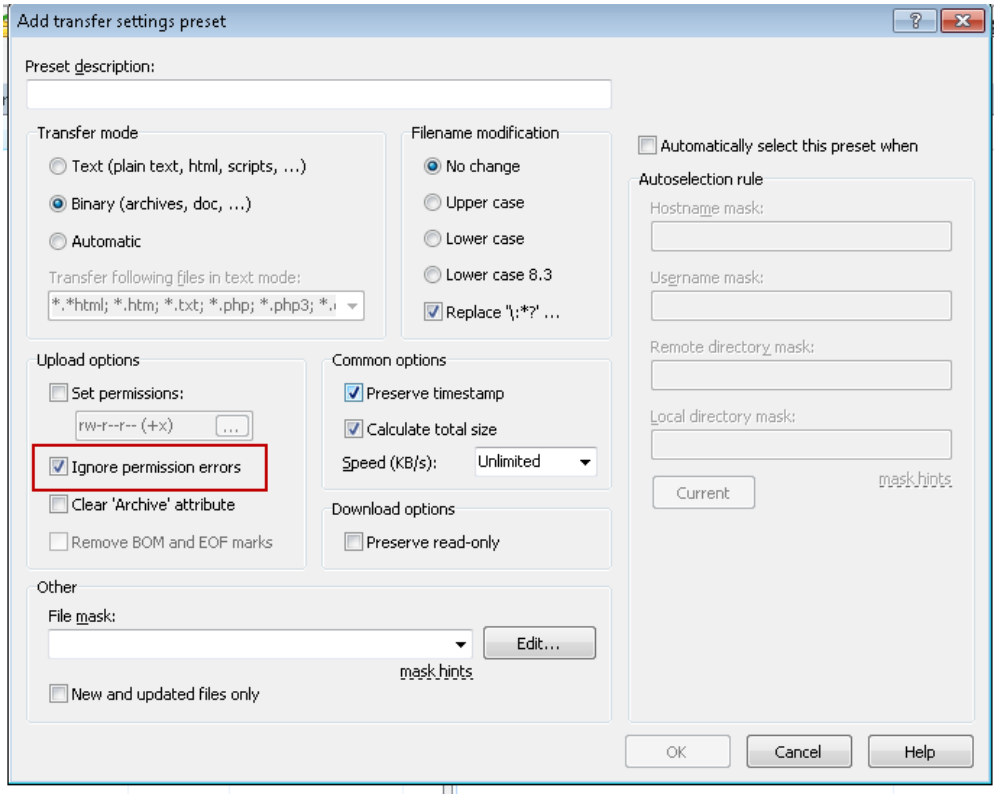
   NOTICE These files are sensitive so keep them protected always. Remove these files from USB drive after it has been installed on the MCP.

2. If you are using WinSCP or Secure File Browser (Refer to Appendix B in SWM0101/15 for details) to transfer the files, you may get the following warning message:



The reason for this warning is that the MCP file system does not support per-file permissions, so when WinSCP or Secure File Browser from DS Agile MCP Studio (Refer to Appendix B in SWM0101/15 for details) tries to set the permissions on a file, it is unable to do so. However, there is no security risk because the file takes on the default permissions of the files system which are correct. Therefore, this warning can be safely ignored by clicking **Skip**.

3. To prevent this warning from appearing in the future, in WinSCP or Secure File Browser from DS Agile MCP Studio (Refer to Appendix B in SWM0101 for details) go to **Options** > **Preferences**. Then select **Transfer** and click **Ignore permission errors**.



4. If you are using the USB drive method of transferring the files, insert the drive into any USB slot on the MCP.

5. Connect to the MCP with a browser and click the and click the Utilities tab under Settings option from the power bar.

   Note: This Option is available in Utilities Tab under Settings option from Local HMI or from the Connected Mode in DS Agile MCP Studio only.

6. Click the **Import** button. You should see a dialog indicating that 1 Local Certificate and 1 Issuer Certificate was successfully imported. Click **OK** to dismiss the dialog.
7. Click the **Manage** button, and then click the **Local** tab. You should see a dialog showing the Local certificate details in the Staged Local Certificates area. Select the certificate and click **Install**. This causes the certificate to move into the Installed Local Certificate area. This also installs the DH parameters file.
8. Click the **Issuer** tab. You should see the CA certificate in the Staged Issuer Certificates area. Select the row containing the CA certificate and click **Install**. This causes the certificate to move into the Installed Issuer Certificates area.
9. Close the dialog and log out of the MCP.
10. If you are using redundancy(not supported in MCP), you need to install same CA certificate, Server certificate and DH parameters on both MCPs. Follow steps 1 to 9 above on both MCPs.

4.2 Installing CA Certificate and Client Certificate for use by a PC Client

1. Copy the CA certificate to client PC or SCADA master system in a directory of your choice (e.g., CA.crt).
2. Copy the PEM file containing client certificate and key to client PC or SCADA master system in a directory of your choice (e.g., MyName.pem).

NOTICE This file is sensitive so keep it protected always. Remove this file from USB drive or any other temporary storage after it has been copied to the client.

5. Configuring Secure Connections on the MCP

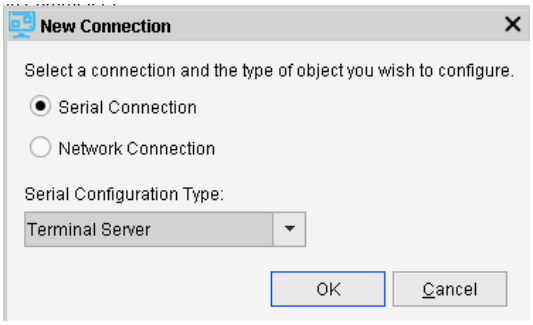
There are three types of secure connections that you can configure on the MCP:

- Secure terminal server
- Secure pass-through
- Secure connection relay

The following sections describe how to create one of each type.

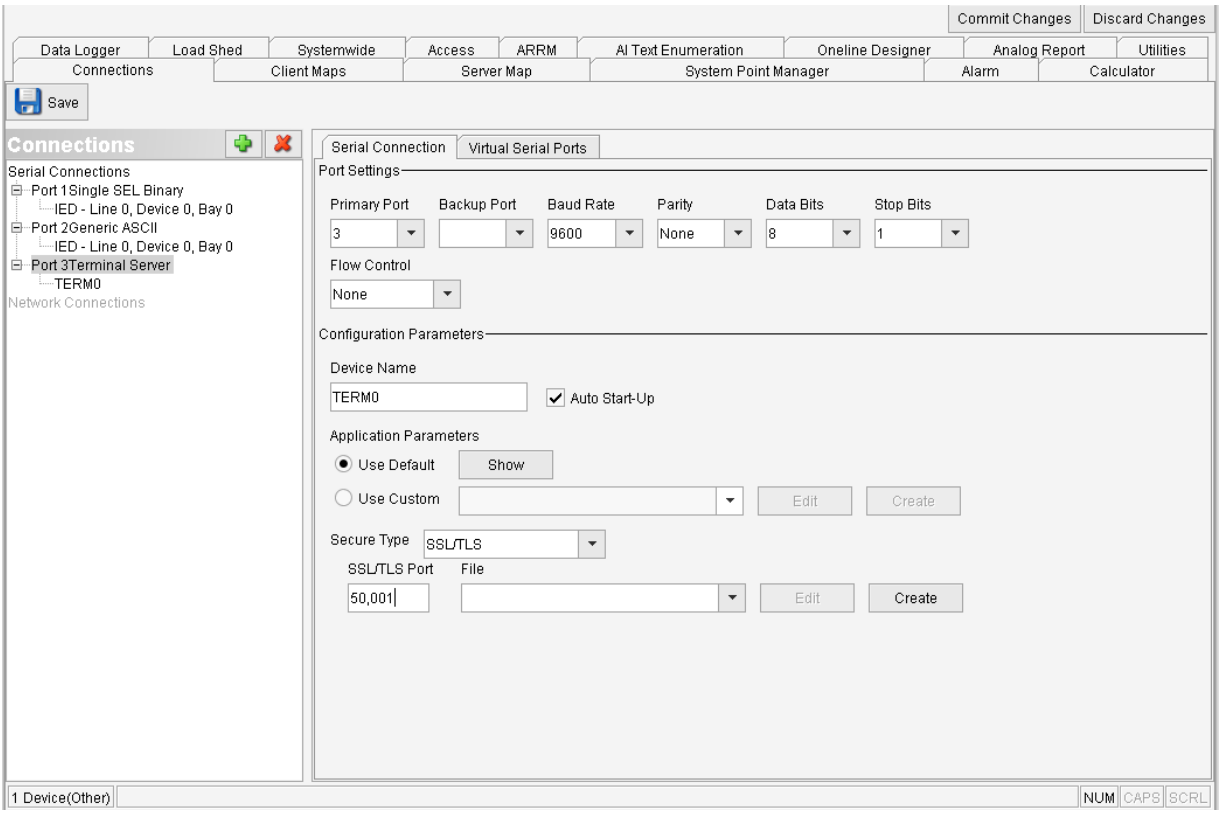
5.1 Configuring a Secure Terminal Server Connection

1. Login to the MCP.
2. Open the configuration screen.
3. Add a serial connection and select **Terminal Server**.
4. Click **OK**.



5. Click **Auto Start-Up** so that the terminal server connection is active.

6. Check the **Enable Security** button and in the **SSL/TLS Port** field, choose a TCP port that is not in use on the MCP.

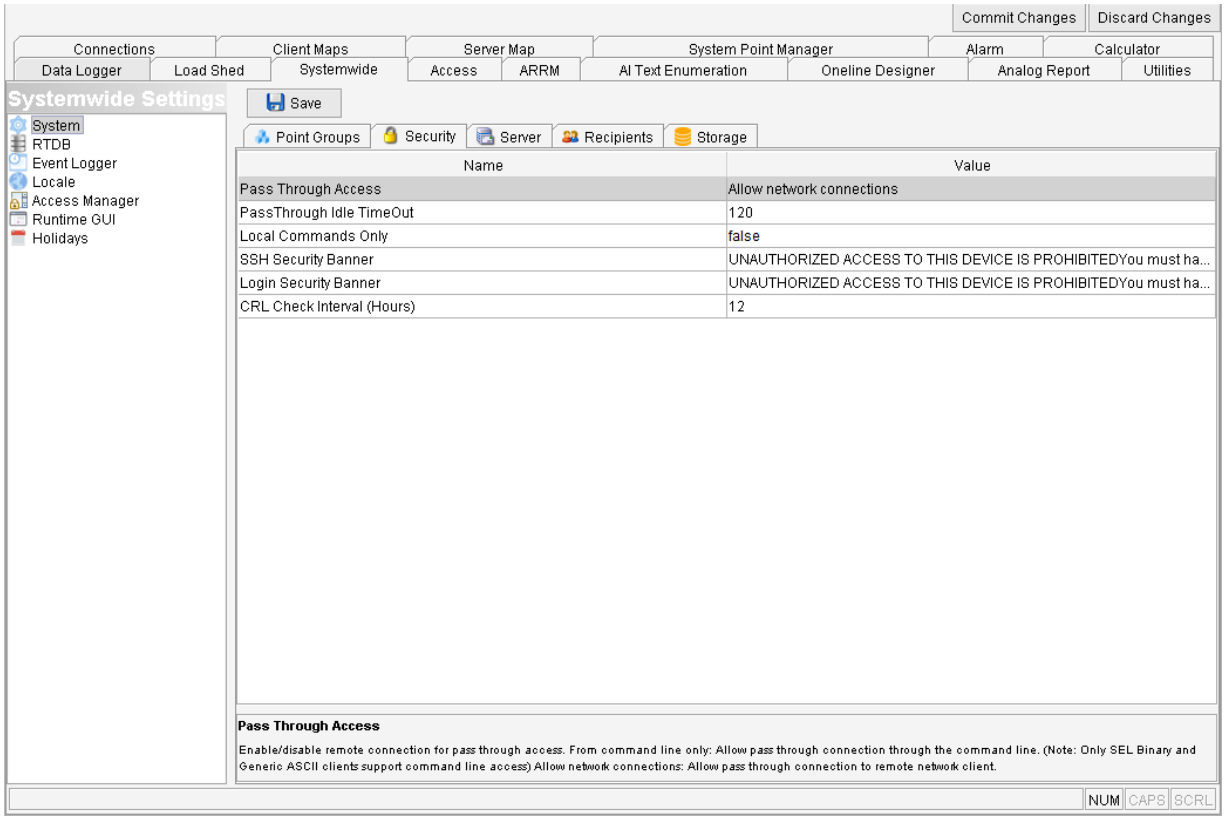


7. Click the **Create** button; the Secure Application Parameters dialog appears. Refer to Section 5.4 Secure Application Parameters Dialog for further steps.
8. Optionally, you may click **Use Custom** to open the Terminal Server Application Parameters dialog and specify **No** for **Password Authentication** and click **Save**. Because the TLS connection provides certificate-based authentication, password authentication may not be required. However, if the certificate is shared among many users you may still want to enable password authentication.
9. Click **Save**.
10. Click **Commit Changes**.

5.2 Configuring a Secure Pass-through Connection

1. Login to the MCP.
2. Open the configuration screen.

3. Click the **Systemwide** tab, select **Security**, and change **Pass Through Access** to **Allow network connections** if it is not already selected. The following figure shows the parameter and the correct setting.



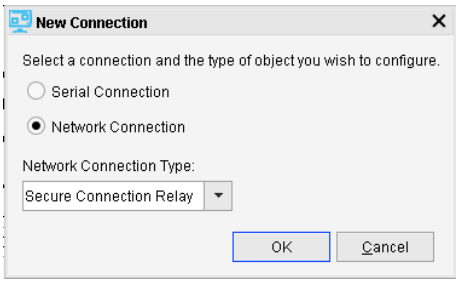
4. Click the **Connections** tab and select an existing connection that supports Pass-through (i.e., Hydran Multidrop, IEC 60870-5-103 Multidrop, Modbus RTU Multidrop, Single Generic ASCII, and Single SEL Binary). Alternatively, create a new connection that supports Pass-through.
5. Check the **Enable Security** button and in the **TLS Port** field, choose a TCP port that is not in use on the MCP.
6. Click the **Create** button; the Secure Application Parameters dialog appears. Refer to Section 5.4 for further steps.
7. Click **Save**.
8. Finally, click **Commit Changes**.
9. Optionally, you may want to disable the global setting for Pass-Through Password authentication. To do so, launch mcpcfg from the MCP console or SSH terminal window. Select **Configure Authentication** > **Pass-through Authentication**. If the screen indicates Pass-through Authentication is *Enabled*, then type **Y** at the prompt for disabling Pass-through Authentication. If the screen indicates Pass-through Authentication is *Disabled*, then type **N** at the prompt for enabling Pass-through Authentication. Finally, select **Back** > **Quit**.

Because the TLS connection provides certificate-based authentication, password authentication may not be required. However, if the certificate is shared among many users you may still want to enable password authentication.

Note: Because the Pass-through Password Authentication setting is global, be careful that you consider any Pass-through connections that are not protected by an TLS connection before disabling Pass-through Password Authentication.

5.3 Configuring a Secure Connection Relay

1. Login to the MCP.
2. Open the configuration screen.
3. Add a network connection and select **Secure Connection Relay**.



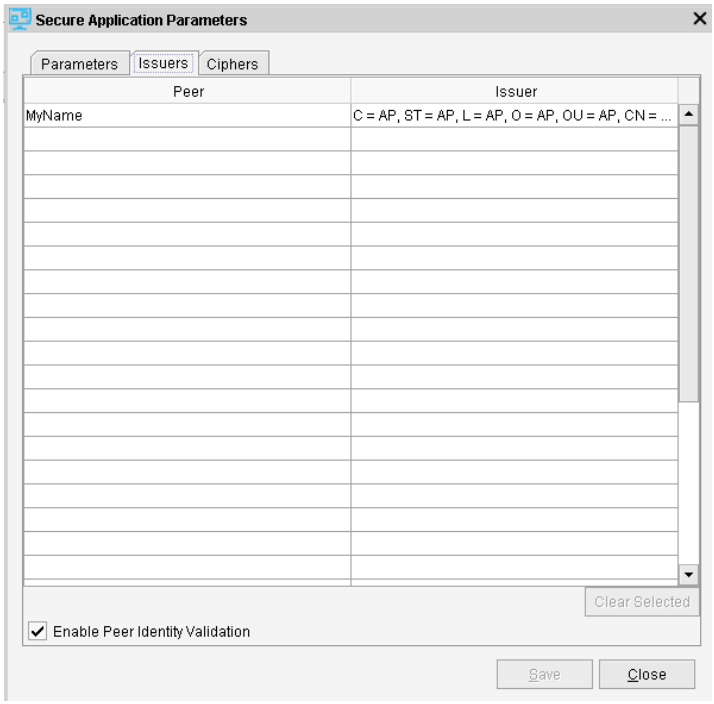
4. Click **OK**.
5. Ensure **Auto Start-Up** is selected so that the secure connection relay is active.
6. In the **Remote IP Address** field, enter the IP address of a device on the internal network or optionally the localhost IP address (127.0.0.1) if connecting to a service on the MCP itself.
7. In the **LAN Port** field, enter the TCP port number of the service you wish to connect to.
8. In the **TLS Port** field, enter a TCP port that is not in use on the MCP.
9. Click the **Create** button; the Secure Application Parameters dialog appears. Refer to Section 5.4 for further steps.
10. Click **Save**.
11. Click **Commit Changes**.

5.4 Secure Application Parameters Dialog

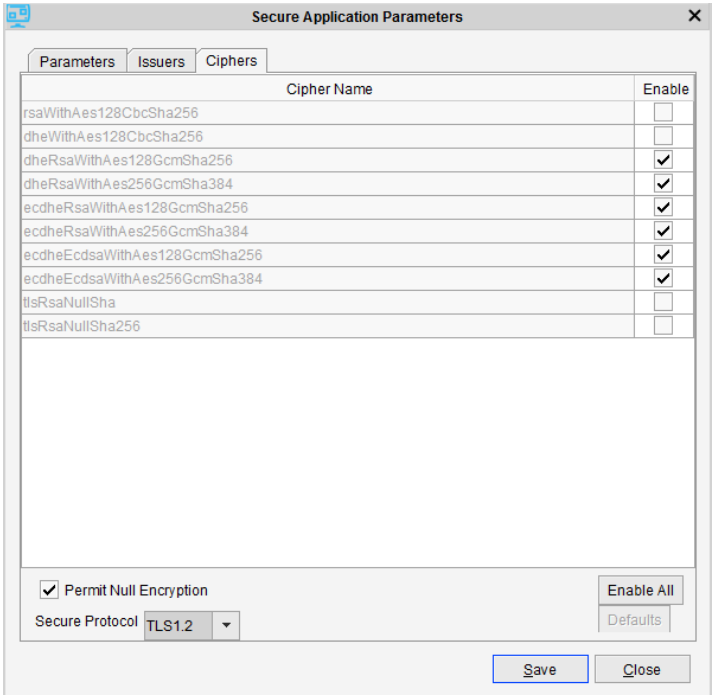
All secure connection types require a Secure Application Parameters File. This file can be reused with any secure connection, regardless of type. This section describes how to configure the file using the Secure Application Parameters Dialog.

1. Click the **Issuers** tab.

2. In the **Peer** column, type the *Common Name* of the client certificate that is to be used to authenticate and authorize the client for this connection. In the **Issuer** column, select the Issuer that signed the client certificate.
3. Repeat the previous step for other client certificates that may be used to authorize access for this connection.



4. Under the Ciphers tab, ensure **Secure Protocol** is set to **TLS1.2**.



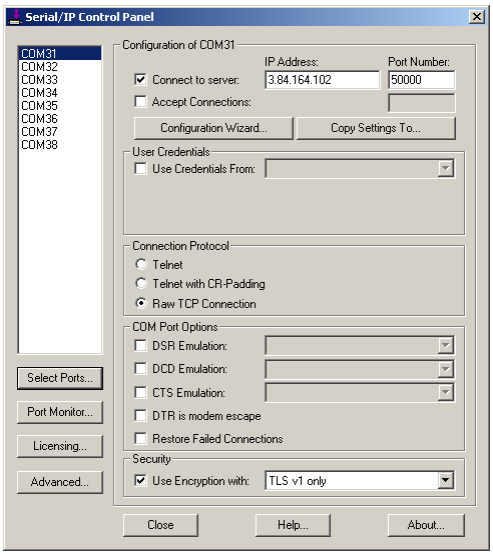
5. Click **Close** and enter a suitable file name when prompted.

6. Configuring a Secure Connection with Tactical Software Serial IP

6.1 Configuring Tactical Software Serial IP with Encryption

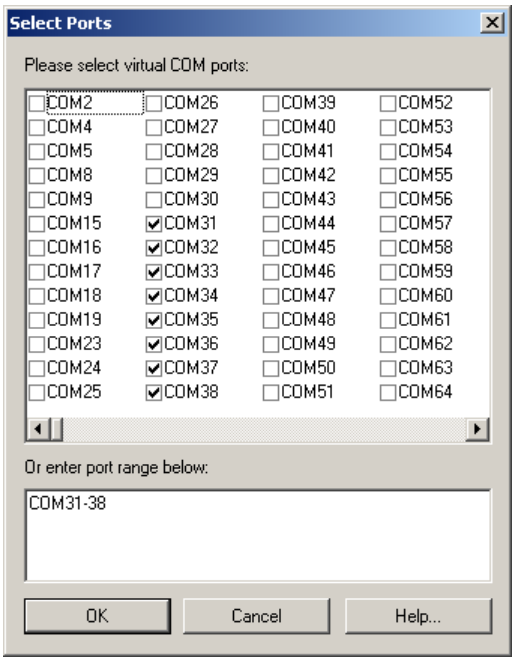
Tactical Software Serial/IP with Encryption creates a virtual serial port that connects to a Secure Terminal Server Connection (Section 5.1) or Secure Pass-through Connection (Section 5.2) on the MCP. The following steps demonstrate how to generate a configuration with secured access.

1. Launch the Serial/IP Control Panel.

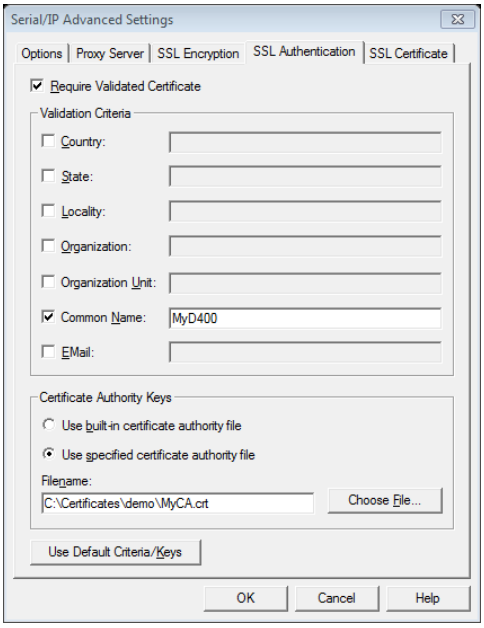


2. Under **Connection Protocol**, ensure **Raw TCP Connection** is selected.

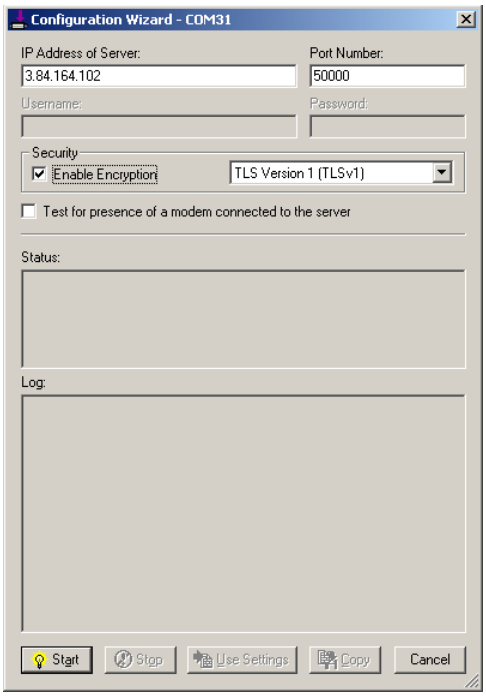
3. Click **Select Ports** to select the number of virtual COM ports to configure. In this example, COM 31 – 38 have been selected.



4. For a secured connection, certificates must first be configured.
5. If the connection configured on the MCP requires password authentication, click **Use Credentials From**, and select the appropriate setting.
6. In the Serial/IP Control Panel, click **Advanced** -> **SSL Authentication...**. This tab specifies the information from the MCP server certificate.
7. Select **Require Validated Certificate**. Under Validation Criteria, enter the Common Name of the MCP server certificate installed on the MCP.

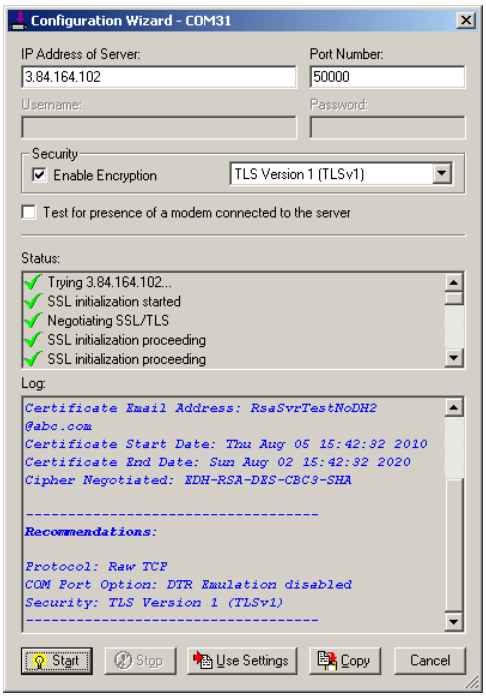


8. Under Certificate Authority Keys, click **Use Specified certificate authority file**, and click **Choose File...** Choose the CA certificate file you copied as described in Section 4.2 (e.g., CA.crt).
9. Select the **SSL Certificate** tab. This tab configures location of the client certificate and key.
10. Click **Supply Certificate** and click **Choose File...** Choose the client PEM file you installed as described in Section 4.2. Note this file contains the Client Certificate and key.
11. With all the certificates in place, select a virtual com port and click **Configuration Wizard...**.
12. Enter the IP address and port number for the MCP and ensure **Enable Encryption** is checked.



13. Enter the protocol as **TLS Version 1 (TLSv1)**. Also ensure the Secure Application Parameters settings on the MCP (see Section 5.4) are set as follows:
    - Secure Protocol is set to TLSv1,
    - Permit Null Encryption is checked or unchecked, and the Enable All button has been pressed.

14. Click **Start** and ensure the log does not show any error messages.



15. Click **Use Settings** to accept the configuration.

7. Configuring a Secure Connection with Stunnel

7.1 Configuring Stunnel

Stunnel is an open source program that can be used to secure TCP connections inside an TLS channel. Use Stunnel to connect to a Secure Connection Relay on the MCP. Configure the Secure Connection Relay on the MCP as described in Section 5.3. Generate the Stunnel configuration as follows:

1. Download and install the latest windows binary from http://www.stunnel.org/download/binaries.html
2. Click **Start** > **Programs** > **stunnel** > **Edit stunnel.conf**; the Stunnel configuration file appears in a text editor.
3. Change the value of the **cert** variable to the full path of the client PEM file installed in Section 4.2. Note this file contains the Client Certificate and key. For example:

```
; Certificate/key is needed in server mode and optional in client mode
; The default certificate is provided only for testing and should not
; be used in a production environment
cert = C:\certs\MyName.pem
```

4. Delete the semicolon before the **CAfile** variable and change the value to refer to the full path of the PEM file containing the CA certificate installed in Section 4.2. For example:

```
; It's often easier to use CAfile
CAfile=c:\certs\MyCA.crt
```

5. Delete the semicolon before the **client** variable to enable client mode:

```
; Use it for client mode
client = yes
```

6. Now add the TCP service that you wish to tunnel in the **Service-level configuration** section of the file. For example:

```
; Service-level configuration
; Create secure connection for Enervista UR Setup to connect to UR in
substation
[MYMCP-UR]
accept=502
connect=172.12.235.217:50000 (MCP IP and SSL/TLS Port Number)
sslversion=TLSv1.2
```

7. Comment out or delete the lines describing other services that you don't need. For example:

```
;[pop3s]
;accept  = 995
```

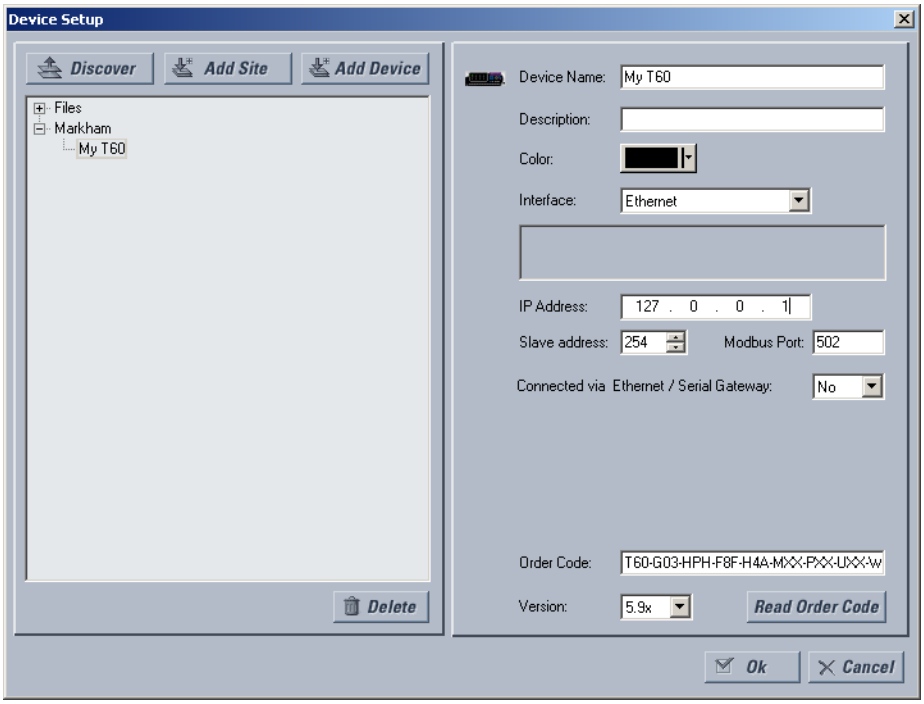
```
;connect = 110

;[imaps]
;accept  = 993
;connect = 143

;[ssmtp]
;accept  = 465
;connect = 25

;[https]
;accept  = 443
;connect = 80
;TIMEOUTclose = 0
```

8. Save the file.
9. Click **Start** > **Programs** > **stunnel** > **Run stunnel**
10. Right-click the tray icon for stunnel and select **log**. You should see a log with something similar like stunnel started successfully:

```
2019.03.29 16:53:43 LOG5[main]: stunnel 5.50 on x64-pc-mingw32-gnu platform

2019.03.29 16:53:43 LOG5[main]: Compiled/running with OpenSSL 1.1.1a  20 Nov 2018

2019.03.29 16:53:43 LOG5[main]: Threading:WIN32 Sockets:SELECT,IPv6 TLS:ENGINE,OCSP,PSK,SNI

2019.03.29 16:53:43 LOG5[main]: Reading configuration from file stunnel.conf

2019.03.29 16:53:43 LOG5[main]: UTF-8 byte order mark detected

2019.03.29 16:53:43 LOG4[main]: Service [MYMCP-UR] needs authentication to prevent MITM
attacks

2019.03.29 16:53:43 LOG5[main]: Configuration successful

2019.03.29 16:53:56 LOG5[0]: Service [MYMCP-UR] accepted connection from 127.0.0.1:64354

2019.03.29 16:53:56 LOG5[0]: s_connect: connected 172.12.235.217:50000

2019.03.29 16:53:56 LOG5[0]: Service [MYMCP-UR] connected remote server from
172.12.232.232:64355
```

7.2 Configuring the Client Program

1. Configure the TCP-based client program to connect to localhost (i.e. ,127.0.0.1) with the port number you specified in the stunnel configuration. If the TCP based client is Enervista UR Setup, configure the Device Setup dialog as follows:



2. Launch the TCP based client and make a connection to the device.
3. Right-click the tray icon for stunnel and select **log**. You should see a log with something similar like stunnel was able to successfully connect to the device via the MCP:

8. Revoking a client certificate

All certificates are issued for a restricted time of validity. However, it can happen that a certificate should not be used or becomes invalid before its expiry date. In this case, the issuing CA should revoke this certificate by putting it on the list of revoked certificates (CRL) and publishing it.

8.1 Revoking the Certificate in XCA

1. Launch XCA from the Windows Programs menu.
2. In the tree view under the **Certificates** tab, open the branch containing your Certificate Authority.
3. Select and right-click the Client certificate to be removed (e.g., MyName).
4. Click **Revoke** option from the right-click menu.
5. Provide the date of revocation under field **Invalid Since** and reason for revocation from the dropdown list **Revocation Reason**.
6. Click **OK**.

8.2 Exporting the CRL in XCA

1. In the tree view under the **Certificates** tab, right-click the branch containing your Certificate Authority (e.g., MyCA).
2. Select the **CA** option in the right-click menu, and then option **Generate CRL**.
3. Under **Dates** section, leave the **last update** as today's date.
4. Choose a date for **next update** when you want to update CRL next time to the MCPs. If there is no planned date for next update, you can choose the expiry date of CA certificate as date for **next update.** Note: you can optionally use **Year/Month/Day** field and **Apply** to quickly change next update date.
5. Leave the dropdown **Hashing Algorithm** as SHA 256.
6. Under the **Extensions**, leave the fields **CRL Number** and **Revocation reasons** checked. Leave the field **Authority key identifier** unchecked.
7. Click **OK**.
8. Under the **Revocation List** tab, select the CRL labelled as your Certificate Authority (e.g., MyCA). Verify that **Next update** field is set to what you have chosen in step 4.
9. Click **Export**.
10. In the dialog that appears, ensure the **Export Format** field is set to PEM. Browse to a protected location (e.g., My Documents->MyXCAFiles) and click **Save**. The file is named

based upon the internal name of your CA with a .pem extension. Append "_CRL" to filename to indicate that this file is a CRL (e.g., MyCA_CRL.pem). Finally click **OK.**

8.3 Installing the CRL in the MCP

1. Copy the CRL file generated in the previous section to one of two locations:
    a. The folder /mnt/usr/SecureScadaTransfer on the MCP. In this case, use an SFTP/SCP file transfer program such as WinSCP or Secure File Browser from DS Agile MCP Studio (Refer to Appendix B in SWM0101/15 for details).
    b. The directory \SecureScadaTransfer on a USB drive.
2. If you are using the USB drive method of transferring the files, insert the drive into any USB slot on the MCP.
3. Connect to the MCP with a browser and click the and click the Utilities tab under Settings option from the power bar.

    Note: This Option is available in Utilities Tab under Settings option from Local HMI or from the Connected Mode in DS Agile MCP Studio only.
4. Click the **Import** button. You should see a dialog indicating that 1 CRL was successfully imported. Click **OK** to dismiss the dialog.
5. Click the **Manage** button, and then click the **CRL** tab. You should see a dialog showing the CRL details in the Staged CRLs area. Select the CRL and click **Install**. This causes the CRL to move into the Installed CRLs area.
6. Close the dialog and log out of the MCP.

A. Error Messages

This appendix describes common error message logged by Secure SCADA Utility in the diagnostic log. These diagnostic messages are logged under application "stunnel" and application interface "P005".

Table 6: Error Messages

Error Message	Cause
SSL routines:SSL3_GET_CLIENT_HELLO:**no shared cipher**	All configured ciphers use DHE key exchange, but no DH parameters are installed
SSL_accept: 140890B2: error:140890B2:SSL routines:SSL3_GET_CLIENT_CERTIFICATE:**no certificate returned**	Client did not provide a certificate (It typically indicates certificate configuration error in the Client)
VERIFY ERROR: depth=0, error=**certificate has expired**	Peer Certificate expired
VERIFY ERROR: depth=2, error=**certificate has expired**	Issuer certificate expired
SSU exited because the issuer of the peer cert was not valid	Peer certificate is signed by an unsupported issuer
SSU exited because the issuer or subject of the peer cert was not valid	The common name does not match the connection
Certificate with serial 2 (0x2) revoked per CRL from issuer	Peer certificate is in the CRL
VERIFY ERROR: depth=1, error=certificate is not yet valid	Certificate validity period has not started yet. This error can also come if MCP time is set to a past date, which is earlier than certificate validity period start date.

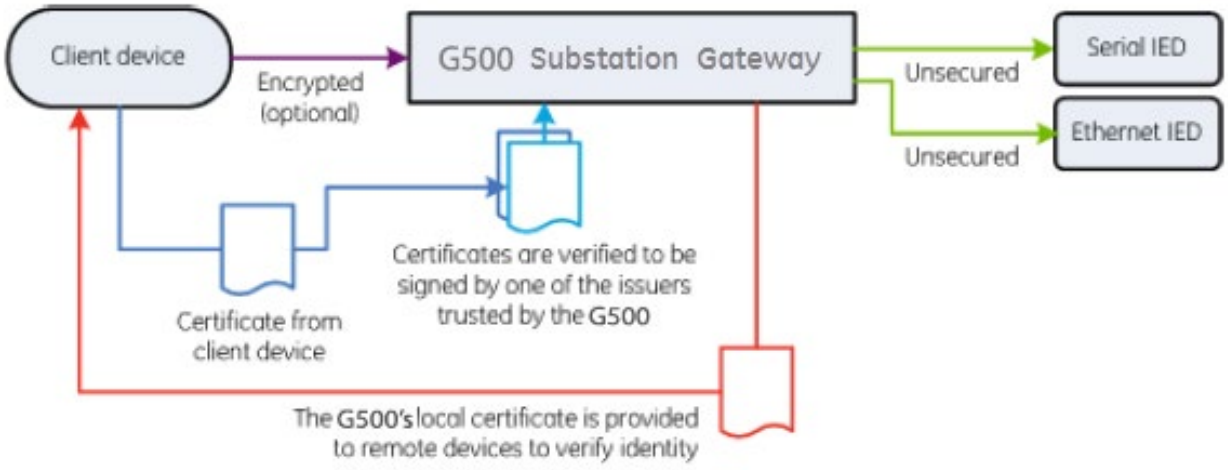
B. Connection Security

The MCP supports **Transport Layer Security (TLS)** which are cryptographic protocol that provide security for communications over networks such as the Internet. TLS encrypt the segments of network connections at the Application Layer to ensure secure end-to-end transit at the Transport Layer.

This security feature is available on the following types of connections:

- Hydran Multidrop (serial, on pass-through)
- IEC 60870-5-103 Multidrop (serial, on pass-through)
- Modbus RTU Multidrop (serial, on pass-through)
- Single Generic ASCII (serial, on pass-through)
- Single SEL Binary (serial, on pass-through)
- Terminal Server (serial, on pass-through)
- Secure connection relay (Ethernet)

The TLS protocol allows client/server applications to communicate across a network in a way designed to prevent eavesdropping and tampering. TLS provides endpoint authentication and communications confidentiality over Ethernet connections using cryptography.



The process of securing an Ethernet connection is shown above:

1. A communications link is established between the MCP and a client device. This is shown in the diagram by the **purple** arrow between the devices. The two devices exchange a list of ciphers, or algorithms that are used to perform message encryption. If both devices are configured to use one or more of the same ciphers, the most secure one is selected and the communications link between the devices from that point on is encrypted using it. Ciphers are selected on the **Secure Application Parameters** window when configuring a serial or network connection. If null encryption is enabled, the communications link between the devices is not encrypted and only identity

verification is performed with security certificates (see the following steps). Not enabling encryption will leave data vulnerable to interception by third parties who have access to the network traffic. If a cipher that uses Diffie Hellman is selected (indicated by the dhe prefix on the cipher name), the MCP sends the Diffie Hellman parameters to the remote device. If these parameters are not contained within the local certificate of the MCP, the parameters file can be uploaded using the **Utilities** > **Certificate** Import window.

2. The local certificate of the MCP is provided to remote devices to allow them to verify the identity of the MCP device. This is shown in the diagram by the **red** arrows and certificate between the MCP and the client device. Remote devices must have access to the certificate from the certificate authority who issued the MCP local certificate to verify its integrity. The local certificate of the MCP is managed on the Local tab of the **Utilities** > **Certificate Management** window.
3. The remote device provides the MCP with its certificate. This is shown in the diagram by the **blue** arrow and certificate between the MCP and the client device. These certificates must then be compared against the issuer certificate provided by the certificate authority to verify its validity, which is shown by the **cyan** arrow and certificate. Issuer certificates are managed on the Issuer tab of the **Utilities** > **Certificate Management** window.

If any of these steps fail, the connection is rejected, and an error is logged to the MCP system log. Once a secure connection has been established, the devices will periodically ensure that the connection remains secure by regenerating the session key (a short sequence of data used to encrypt the contents of the messages).

Note that the serial and Ethernet links between the MCP and IEDs (shown by the **green** arrows) are not identity-verified or encrypted. Security features are provided to remote client devices through secure pass-through or secure connection relay links to these devices.

C. List of Acronyms

Table 7 List of Acronyms

Abbreviation	Description
CA	Certification Authority
CN	Common Name
CRL	Certificate Revocation List
DCA	Data Collection Application
DPA	Data Presentation Application
DTA	Data Translation Application
ESNET	EnterpriseServer.NET
FQDN	Full Qualify Distinguished Name
HMAC	Hash-based Message Authentication Code
HMI	Human Machine Interface
IED	Intelligent Electronic Device
JVM	Java Virtual Machine
LAN	Local Area Network
OU	Organizational Unit
PEM	Privacy Enhanced Mail
PKCS	Public Key Cryptography
PKI	Public Key Infrastructure
PRF	Protective Relay Fault
RTDB	Real Time Data Base
RTU	Remote Terminal Unit
SCR	Secure Connection Relay
SDD	Software Design Document
SOE	Sequence of Event
SPT	Secure Pass-Through
SSDD	Software Subsystem Design Document
SSL	Secure Sockets Layer
ST	Secure Terminal Server
TLS	Transport Layer Security
WAN	Wide Area Network

MODIFICATION RECORD

VERSION	REV.	DATE	CHANGE DESCRIPTION
1.00	0	28th March, 2019	Created.
	1	12th August, 2019	Updated.
1.10	0	9th Sept, 2019	Added ciphers for TLS 1.2.
2.00	0	22nd April, 2021	Updated for MCP family.
2.00	1	26th April, 2021	Updated Technical Support Contacts.
2.00	2	26th July, 2021	Updated DN components requirements, SHA 256 and TLSv1 references.

GE

Grid Solutions

Configuring the Multilin™ MCP devices for Centralized LDAP Authentication using Windows Active Directory

Installation and Configuration Guide

SWM0111

Version 2.00 Revision 0

Copyright Notice

© 2021, General Electric Company. All rights reserved.

The information contained in this online publication is the exclusive property of General Electric Company, except as otherwise indicated. You may view, copy and print documents and graphics incorporated in this online publication (the "Documents") subject to the following: (1) the Documents may be used solely for personal, informational, non-commercial purposes; (2) the Documents may not be modified or altered in any way; and (3) General Electric Company withholds permission for making the Documents or any portion thereof accessible via the internet. Except as expressly provided herein, you may not use, copy, print, display, reproduce, publish, license, post, transmit or distribute the Documents in whole or in part without the prior written permission of General Electric Company.

The information contained in this online publication is proprietary and subject to change without notice. The software described in this online publication is supplied under license and may be used or copied only in accordance with the terms of such license.

Trademark Notices

GE and are trademarks and service marks of General Electric Company.

* Trademarks of General Electric Company.

Tera Term is a registered trademark of T. Teranishi, Incorporated. IEC is a registered trademark of Commission Electrotechnique Internationale. IEEE is a registered trademark of the Institute of Electrical and Electronics Engineers, Inc. Internet Explorer, Microsoft, and Windows are registered trademarks of Microsoft Corporation.

Other company or product names mentioned in this document may be trademarks or registered trademarks of their respective companies.

This printed manual is recyclable.
Please return for recycling where facilities exist.

Configuring the MCP devices for Centralized LDAP Authentication

Table of contents

PRODUCT SUPPORT
- Access the GE Grid Solutions web site. 5
- Search GE Grid Solutions technical support library 5
- Product support 6

ABOUT THIS DOCUMENT
- Purpose 7
- Intended audience 7
- Additional documentation 7

WINDOWS 2012 ACTIVE DIRECTORY
- Basic setup 9
- Configuration tasks 10
- Installing AD DS 10
  - Equipment setup to install AD DS 10
  - Prerequisites 10
  - Procedure to install AD DS 11
  - Procedure to test the AD DS domain controller installation 15
- Procedure to create MCP AD Groups on Active Directory 19
  - Procedure for Static Group Mapping 20
  - Procedure for Dynamic Group Mapping 23
  - Procedure to create MCP device Users on Active Directory 24
- Procedure for Adding MCP AD users to MCP AD Groups 25
- Installing AD CS 27
  - Install Active Directory Certificate Services on Windows Server 2012 procedure 28
- Installing CA Certificates on the MCP device 38
  - CA Certificate transfer procedure from PC to MCP 38
  - CA Certificate Installation procedure 42
- Configuring LDAP on the MCP device 46
  - Prerequisites to configuring LDAP on MCP device 47
  - Procedure to configure LDAP on the MCP device 62

CHECKING DN FORMAT

THIRD-PARTY CA CERTIFICATE

Creating and installing a third-party CA certificate 75
Creating a third-party X.509 certificate 75
Creating the Server X.509 Certificate 82
Installing the third-party CA X.509 Certificate and Server Certificate into the AD DS Windows Server 84
Installing the third-party X.509 CA Certificates on to the MCP device 87

TROUBLESHOOTING

LDAP error messages 89
LDAP Certificate error messages 90

LIST OF ACRONYMS

Acronym Definitions 93

REVISION HISTORY

Revision history 95

Configuring the MCP devices for Centralized LDAP Authentication

Product Support

If you need help with any aspect of your MCP product, you can:

- Access the GE Grid Solutions Web site
- Search the GE Technical Support library
- Contact Technical Support

Access the GE Grid Solutions web site

The GE Grid Solutions Web site provides fast access to technical information, such as manuals, release notes and knowledge base topics.

Visit us on the Web at: http://www.gegridsolutions.com

Search GE Grid Solutions technical support library

This site serves as a document repository for post-sales requests. To get access to the Technical Support Web site, go to: http://sc.ge.com/*SASTechSupport

Product support

For help with any aspect of your GE Grid Solutions product, please contact our support team, 24/7, as follows:

Region	E-mail	Telephone
Global Contact Centre	ga.support@ge.com	+44 1785 250070
Central and East Asia and Pacific	ga.supportCEAP@ge.com	+61 414 730 964
India	ga.supportIND@ge.com	+91 44 22648000
Middle East, North Africa and Turkey	ga.supportMENAT@ge.com	+971 42929467
Europe, Russia, CIS and Sub-Saharan Africa	ga.supportERCIS@ge.com	+34 94 4858854
North America	ga.supportNAM@ge.com	+1 877 605 6777
Latin America	ga.supportLAM@ge.com	+55 11 36187308

Configuring the MCP devices for Centralized LDAP Authentication

About this Document

Purpose

This manual describes how to install and configure the Windows® Server 2012 and Multilin™ MCP device for Centralized LDAP Authentication.

This document applies to the MCP family (G100/G500) unless otherwise indicated.

Screen captures may show G500 in some areas, however the workflow applies to products in the MCP family (G100/G500).

Intended audience

This manual is a helpful resource for utility personnel and system engineers who are implementing LDAP on Multilin™ MCP devices in an overall substation automation system.

Additional documentation

For the most current version of the Configuring Windows® Server 2012 and Multilin™ MCP for Centralized LDAP Authentication - Manual, please download a copy from GE Grid Solutions web site.

For information on fully installing, configuring, monitoring and testing a MCP device, refer to the:

- G500 Substation Gateway Instruction Manual, 994-0152
- G100 Substation Gateway Instruction Manual, 994-0155
- MCP Substation Gateway Software Configuration Guide, SWM0101

Configuring the MCP devices for Centralized LDAP Authentication

Chapter 1: Windows 2012 Active Directory

The Lightweight Directory Access Protocol (LDAP) is an application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network. This Directory services may provide any organized set of records, often with a hierarchical structure.

This chapter describes how to configure a Windows® Server 2012 and the MCP device for Centralized LDAP Authentication.

See section:

- Basic setup
- Configuration tasks
- Installing AD DS
- Procedure to create MCP AD Groups on Active Directory
- Procedure for Adding MCP AD users to MCP AD Groups
- Installing AD CS
- Installing CA Certificates on the MCP device
- Configuring LDAP on the MCP device

Basic setup

The following is required to configure the MCP device and the LDAP Servers:

- Windows Server 2012
- MCP device

The following is required only if Windows Server Active Directory Certificate Services (AD CS) are not installed:

- Open Source CA Package: X Certificate and Key Management (XCA):
  Certificates are issued by a Certification Authority (CA). The MCP device is not delivered with a CA; consequently, you must make use of an existing CA or create your own. There are many third-party commercial and open source CAs available. This document describes one such open source CA package.

Configuration tasks

To configure Active Directory on Windows Server 2012, the following tasks are performed:

- Installation of AD DS on Windows Server 2012. See section: Installing AD DS.
- Create AD Groups on Active Directory. See section: Procedure to create MCP AD Groups on Active Directory.
- Add MCP AD Users to MCP AD Groups. See section: Procedure for Adding MCP AD users to MCP AD Groups.
- Setup of Active Directory Certificate Services and generation of Root CA Certificate. See section: Installing AD CS.
- Importing and Installing of Root CA, generated using AD CS to MCP device. See section: Installing AD CS.
- Installation of the Certificate on the MCP device. See section: Installing CA Certificates on the MCP device.
- Configure LDAP on the MCP device. See section: Configuring LDAP on the MCP device.

Installing AD DS

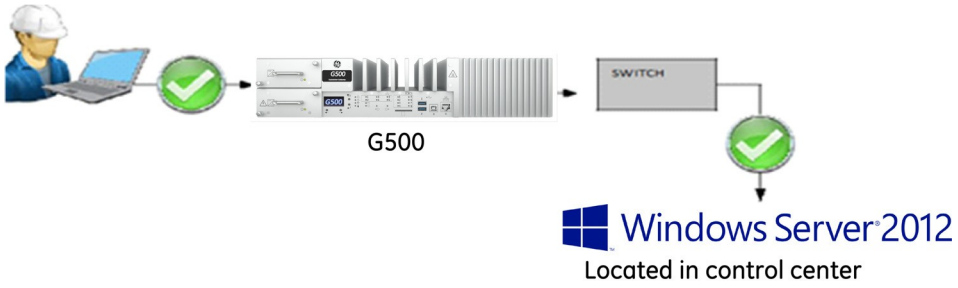
Windows Server Active Directory Domain Services (AD DS) enables the creation of an LDAP-enabled central storage for users, groups, and other objects.

This section describes the equipment setup, prerequisites, and the procedure to install Active Directory - Domain Services.

Equipment setup to install AD DS

Figure 1 shows a simple hardware configuration for installing central authentication services. G500 is shown, however the functionality and workflow applies to products in the MCP family (G100/G500).

Figure 1: Central authentication - equipment setup



Prerequisites

Before configuring LDAP authentication:

- The server must:
  - Be running Windows Server 2012.
  - Have AD DS installed.
  - Have an Internet Protocol (IP) address.
  - Be logged in with administrator privileges.

Computer and domain names

While performing the procedures provided in this guide, it is optional to enter your own computer name and domain names. If you choose to use your own computer and domain names, ensure that you substitute those names in the procedures provided in this guide.

To change the server name:

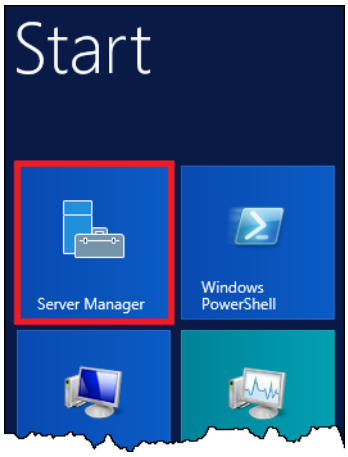
1. Click **Start**.
2. Right-click **computer**.
3. Select **Properties** > **Advanced system settings** > **Computer Name**.

Procedure to install AD DS

To install Active Directory Domain Services (AD DS) on the Windows server:

1. From the Windows 2012 desktop, open the Server Manager by selecting **Start** menu > **Server Manager**:

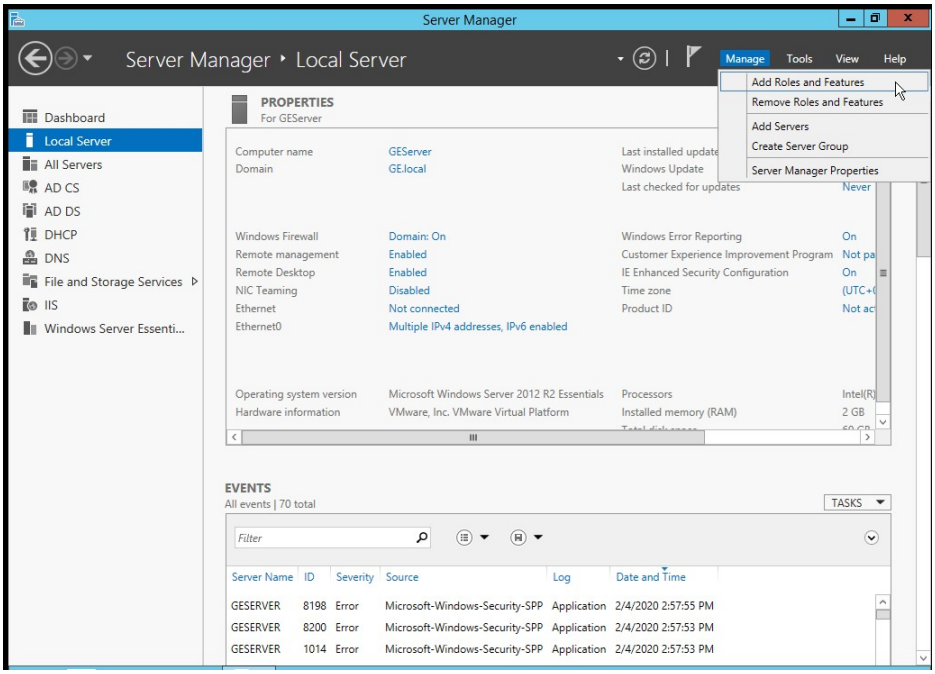
   Result: The Server Manager window appears.



Or open the Server manager through shortcut icon on Windows 2012 desktop:

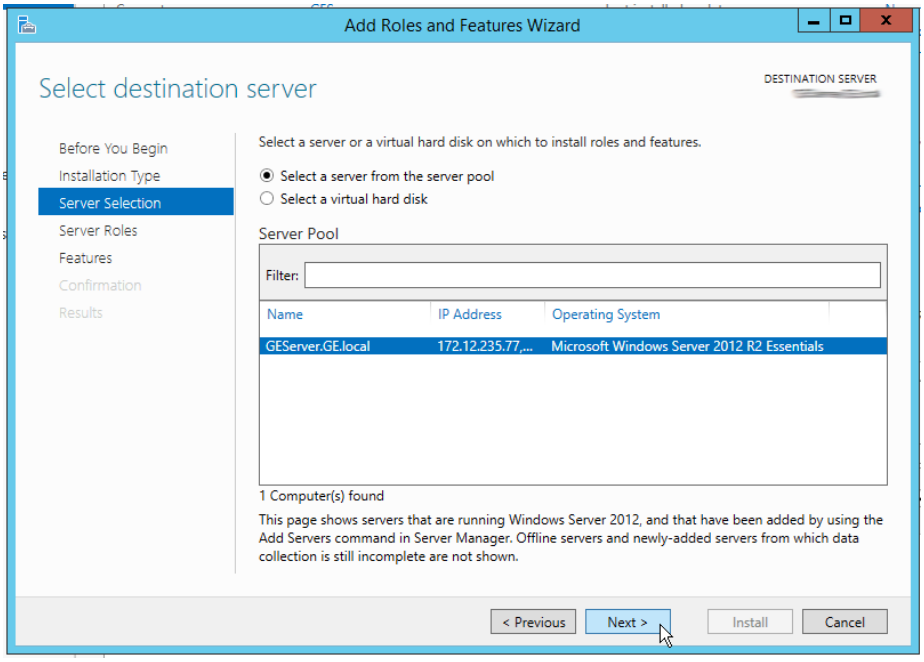
2. Add a new role:
   2.1. Select **Local Server**.

2.2. Click **Manage** > **Add Roles and Features**.

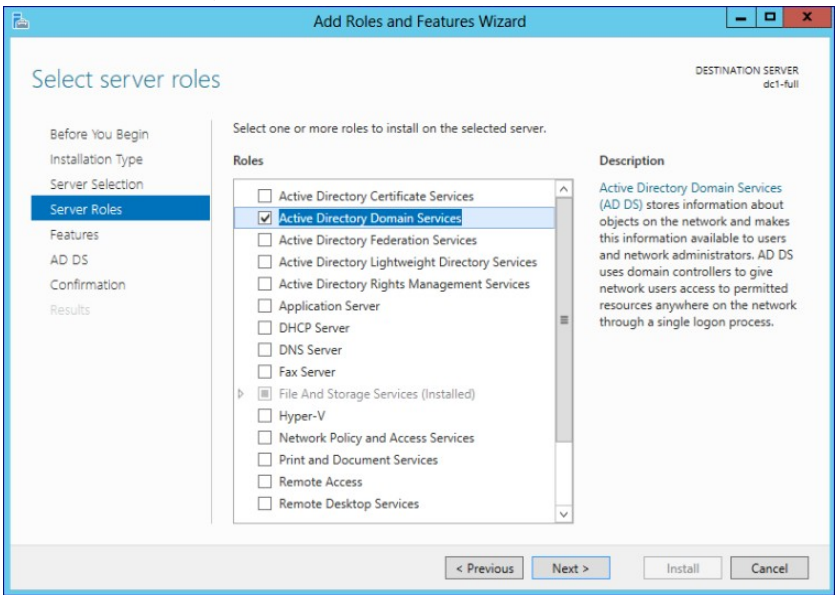


Result: The "Add Roles and features" wizard opens, showing the "Before you Begin" screen.

3. From the Before You Begin screen, click **Next**.
4. Select **Installation Type as Role-based or feature based installation**, and click **Next**.
5. Select a server from the server pool, click **Next.**



5.1. Under Server Roles menu, select the Roles option: **Active Directory Domain Services**, and click **Next.**



A notice displays that explains that you must also install additional roles, services, or features in order to install Domain Services. These additional capabilities include certificate services, federation services, lightweight directory services, and rights management.

5.2. When prompted to select the additional capabilities, click **Add Required Features**.
On the Select features screen, select the check boxes next to the features that you want to install during the AD DS installation process (if any or leave default selection) and click Next.

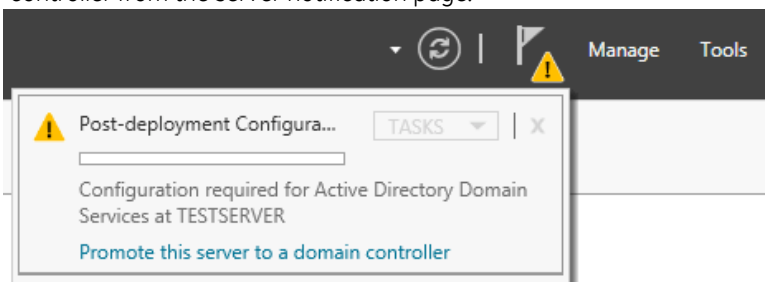
5.3. Review the information on the **AD DS** tab, then click **Next**.

5.4. Review the information on the **Confirm installation selections** screen, then click **Install**.

5.5. When the installation is complete, click **Close**.

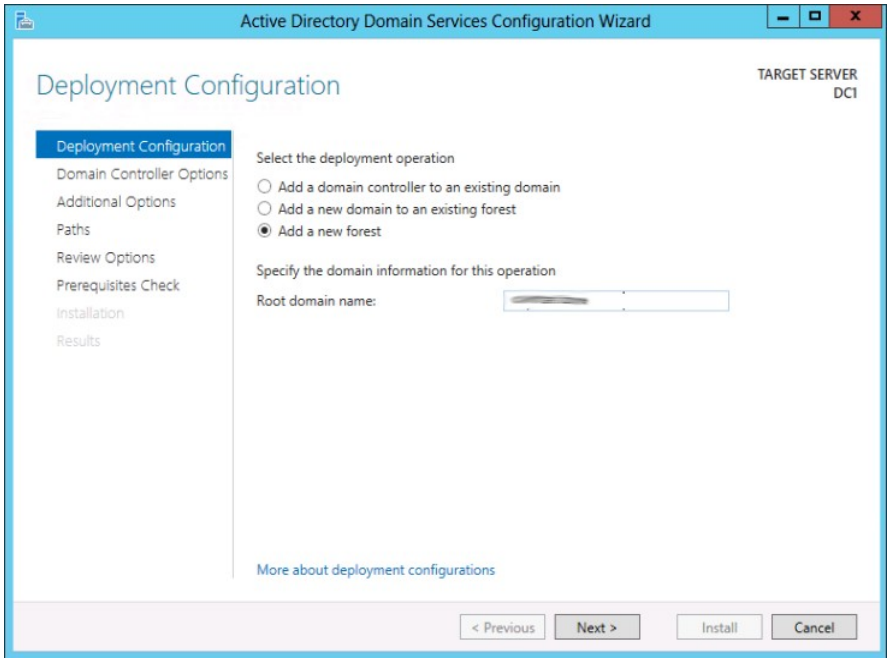
6. Promote Server as Domain Controller.

6.1. After installing Active directory services, select Promote server to a domain controller from the server notification page.



6.2. Once you select this option, a separate **Active Directory Domain Services Configuration Wizard** appears.

7. Deployment Configuration.
   Select Deployment option as per your requirement. If you are installing first Active Directory in the network, select Add a new forest.



   7.1. Type in the **Root domain name**. The Root domain is the Full Qualified Domain Name; for example, GEServer.GE.local

   Result: A prompt appears to install a domain name system (DNS) server.

   7.2. Ensure that the **DNS server** option is selected, and click **Next**.

   Result: If you have any unconfigured network interfaces, you are prompted to acknowledge the use of dynamically assigned IP addresses.

   7.3. Since this is acceptable in this example, select **Yes, the computer will use a dynamically assigned IP address**.

   If you receive a popup warning regarding a delegation for a DNS server, this is normal; click **Yes** to continue.

   Result: The computer will use a dynamically assigned IP address.

   Result: You are prompted for a Password; you can use the same password as the current administrator account.

8. Click **Finish**.

   Result: The system finalizes the installation and prompts you to restart the computer when the installation is complete.

9. Restart the Windows server.
10. Test the AD DS installation; see section: Procedure to test the AD DS domain controller installation.

NOTE

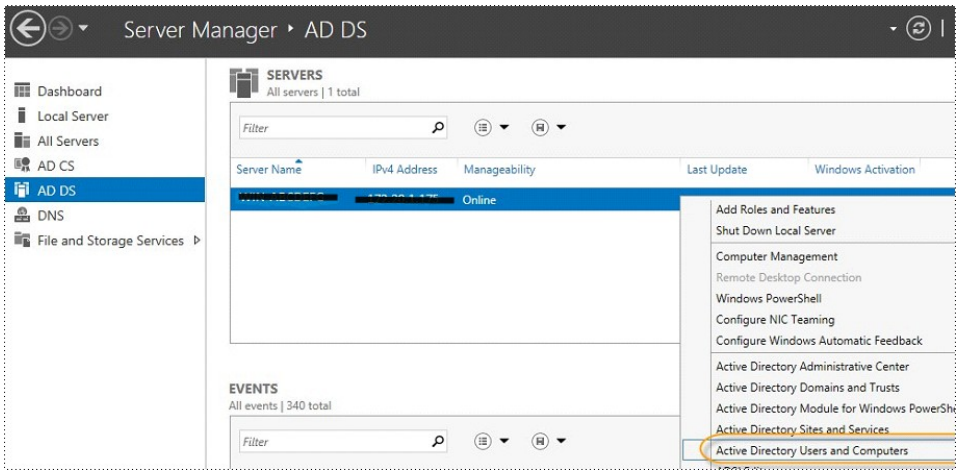
The local Windows Server 2012 account login will change from the local account to the domain account. For example, if the local computer name or account was Administrator or ADDS\Administrator, you must now log in to the device with CENTRAL\Administrator.

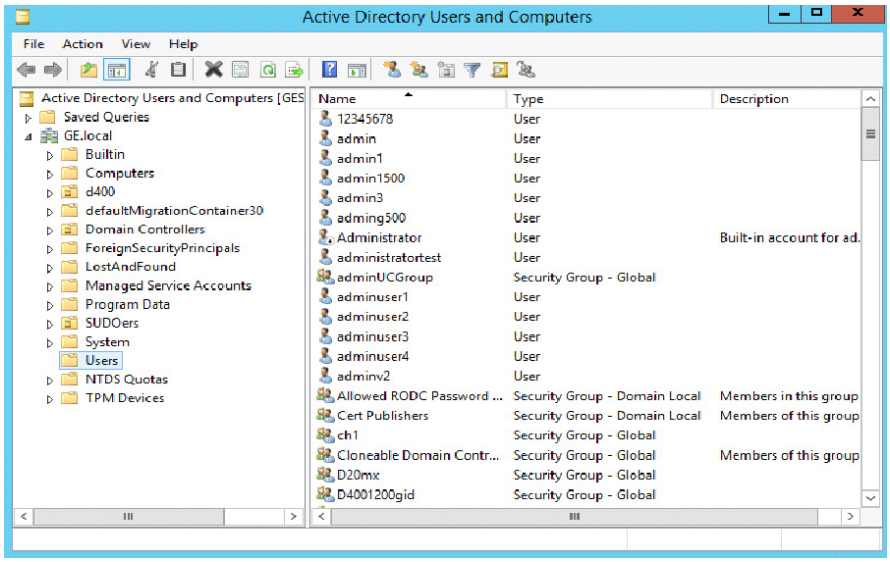
Procedure to test the AD DS domain controller installation

To test connectivity to an Active Directory Domain Controller (DC) from a Windows PC you can use several methods, one of which is **ldp.exe**.

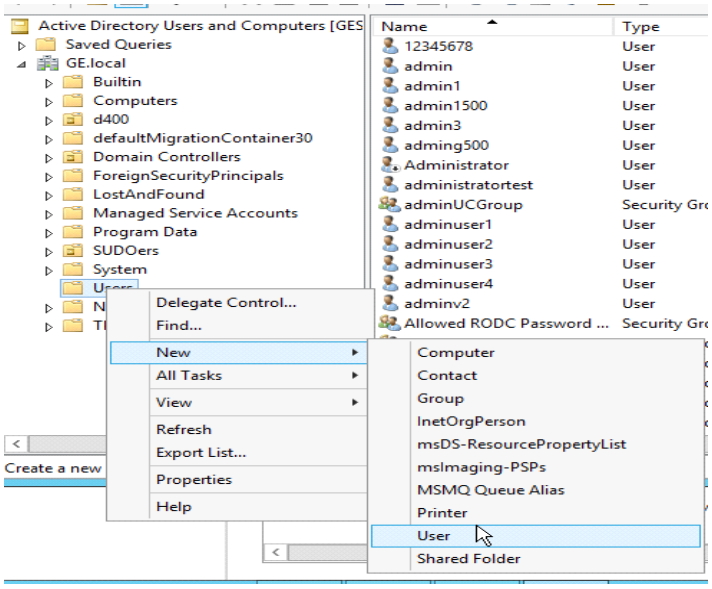
LDP.EXE is a GUI tool that acts as a Lightweight Directory Access Protocol (LDAP) client, which lets you perform connect, bind, search, modify, add or delete operations against AD. To test the AD DS domain controller installation, the Administrator of the domain is to:

1. Open the **Server Manager** from the Windows Server 2012 Start Menu and select **AD DS**.
2. Select the server and right click and select **Active Directory Users and Computes**.





3. Right-click the Users folder and select **New User**.



In this step a Bind User is being created.

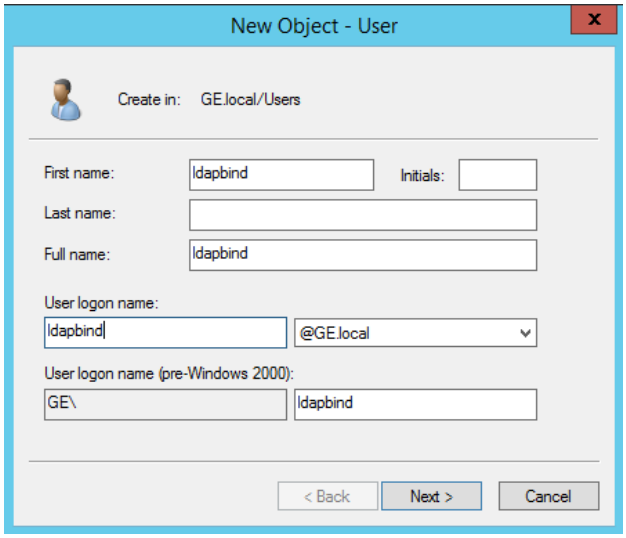
LDAP Bind Operation: Bind operations are used to authenticate clients (and the users or applications behind them) to the directory server, to establish an authorization identity that will be used for subsequent operations processed on that connection.

Once the bind user is created, binding is the step where LDAP server authenticates the MCP client and, if the client is successfully authenticated, allows the client access to the LDAP server based on that client's privileges. Rebinding is simply doing the process over to authenticate the client.

This bind user can have any username is usually different from the real users.

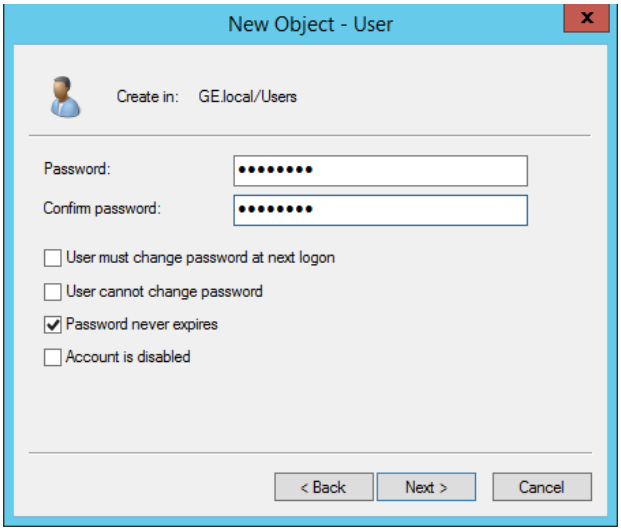
4. Create a new user name: **ldapbind**.

   The user name is comprised of only lower-case letters, numbers, "-" (dash), and "_" (underscore) characters.



5. Click **Next**.
6. Create a password for the **ldapbind** user.

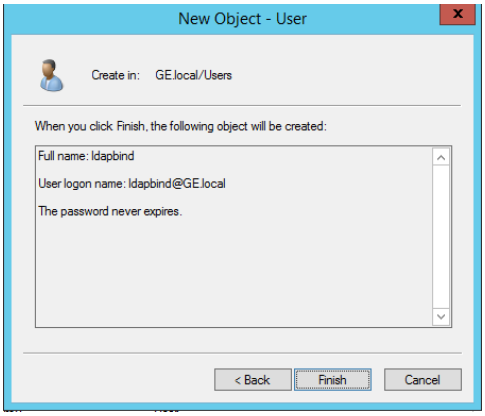
7. Select the option, **Password never expires**.



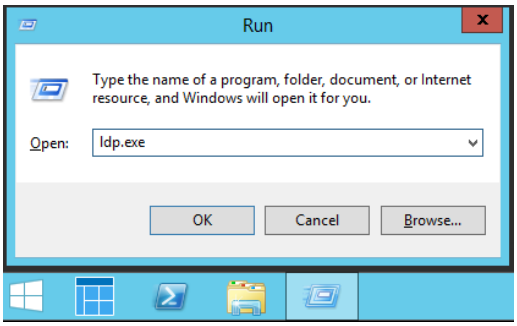
NOTE

The MCP device does not support the **User must change password at next logon** option.

8. Click **Next** and **Finish**.

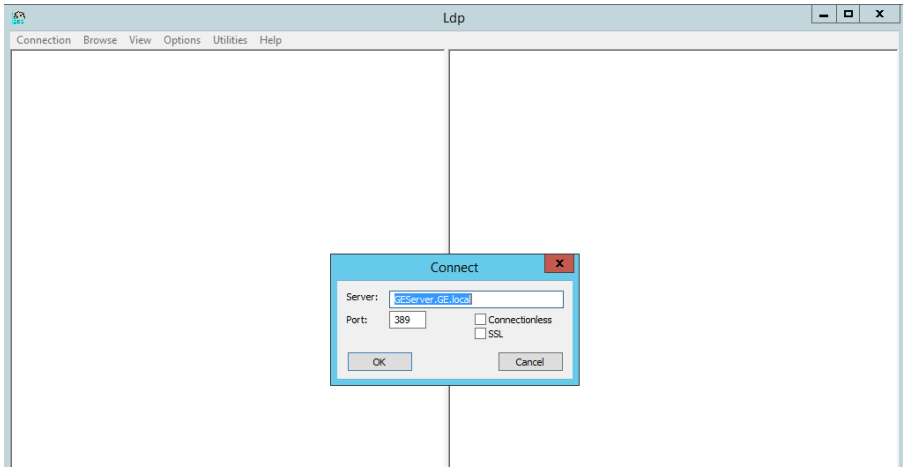


9. Go to **Start** menu > **Run**.
10. Type in **ldp.exe** and press the **Enter** key.

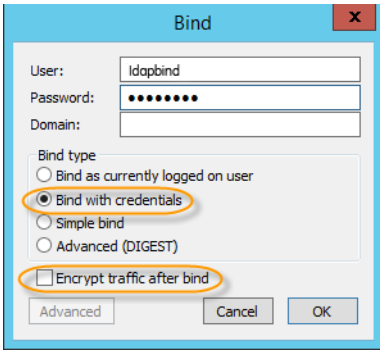


Result: The Ldp application window appears.

11. Click **Connection** > **Connect**. Enter the server name, e.g. "GEServer.GE.local" as per configured computer name with domain name.



12. Click **OK**.
13. Ensure that the connection has been successfully established to AD DS.
    Result: Information about supported LDAP versions and policies may appear.
    13.1. Click **Connection** > **Bind**, and select **Bind with credentials**.
    13.2. Type in **ldapbind** (lower-case characters only) as the User name, with the appropriate Password.
    13.3. De-select the option: **Encrypt traffic after bind**.
    13.4. Click **OK**.



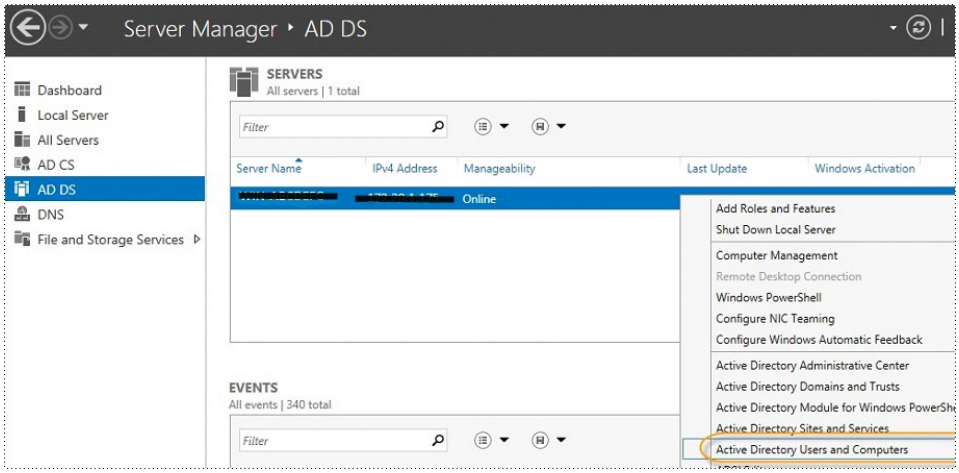
14. Ensure that you receive a successful authentication message; for example:

```
-----------
0 = ldap_set_option(ld, LDAP_OPT_ENCRYPT, 0)
res = ldap_bind_s(ld, NULL, &NtAuthIdentity, NEGOTIATE (1158)); // v.3
        {NtAuthIdentity: User='ldapadmin'; Pwd=<unavailable>; domain = ''}
Authenticated as: 'GEGRID\ldapbind'
-----------
```

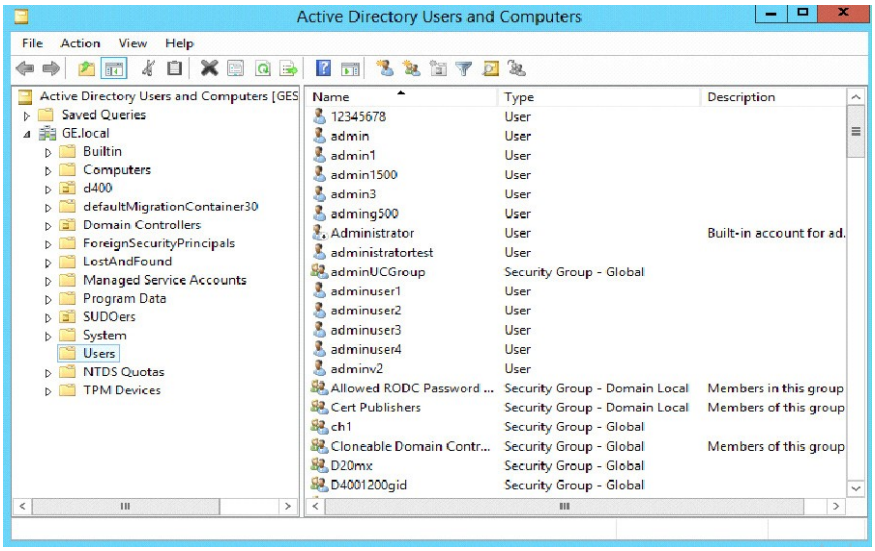
Procedure to create MCP AD Groups on Active Directory

MCP allows 5-different user roles on MCP. These are Administrator, Observer, Operator, Supervisor and Passthrough. To assign these roles we need to create 5-different groups in Active Directory. Follow the below steps to create MCP device AD group on an Active Directory:

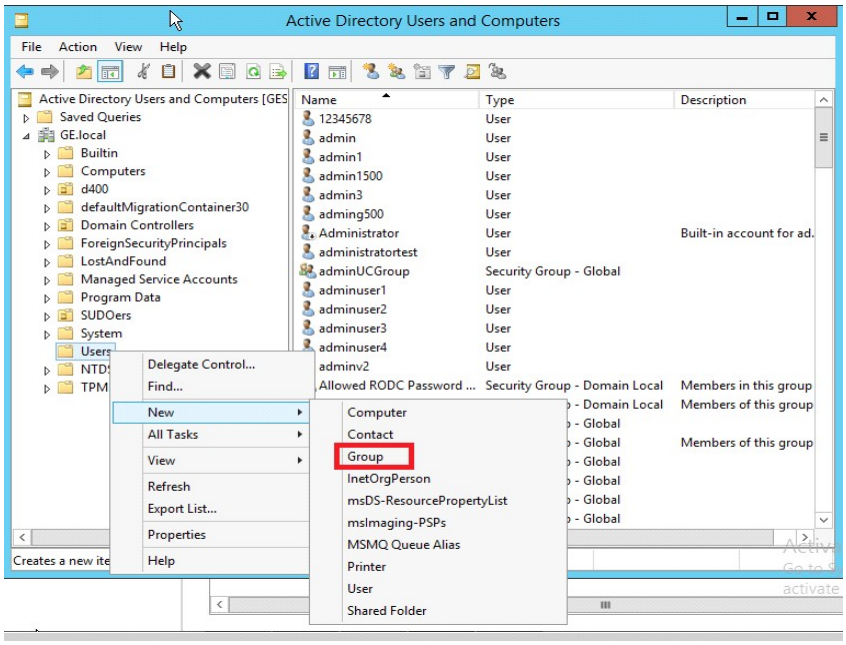
1. Open the **Server Manager** from the Windows Server 2012 **Start** menu and select **AD DS.**
2. Right-click on the server and select **Active Directory Users and Computers**.



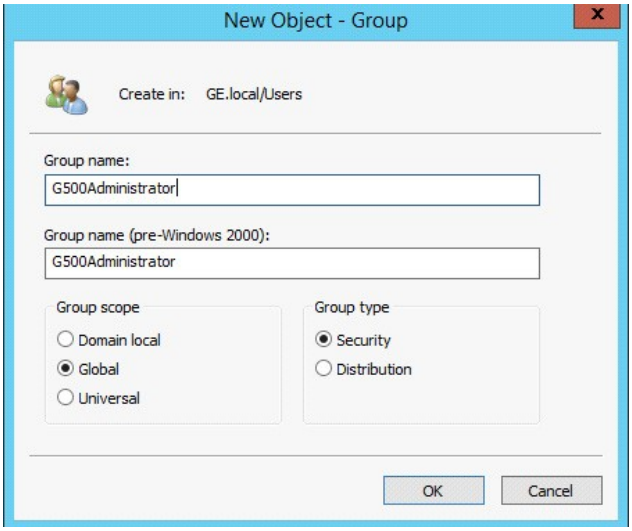
3. **Active Directory Users and Computers** window opens:



4. Right-click on Users and select **New -> Group.**



5. New index will open to create new object group. Type in the group name as below and click OK. This group name can be any name as per group representation (User defined name):



6. On completion of above step User group has been created successfully. Now this User Group is required to be mapped to MCP User Group. It can be done in two approaches:
   - Static Group Mapping
   - Dynamic Group Mapping

Procedure for Static Group Mapping

In this approach, the Windows Server **AD group gid** shall be configured as per Table 1.

Table 1: Group IDs mapping on the AD User Groups

AD Group Name	GID Number	Description
G500Administrator	0	To map AD Group G500Administrator to G500 group Administrator
G500Observer	501	To map AD Group G500Observer to G500 group Observer
G500Operator	502	To map AD Group G500Operator to G500 group Operator
G500Supervisor	503	To map AD Group G500Supervisor to G500 group Supervisor
G500SSHPassThrough	504	To map AD Group G500Passthrough to G500 group Passthrough

NOTE

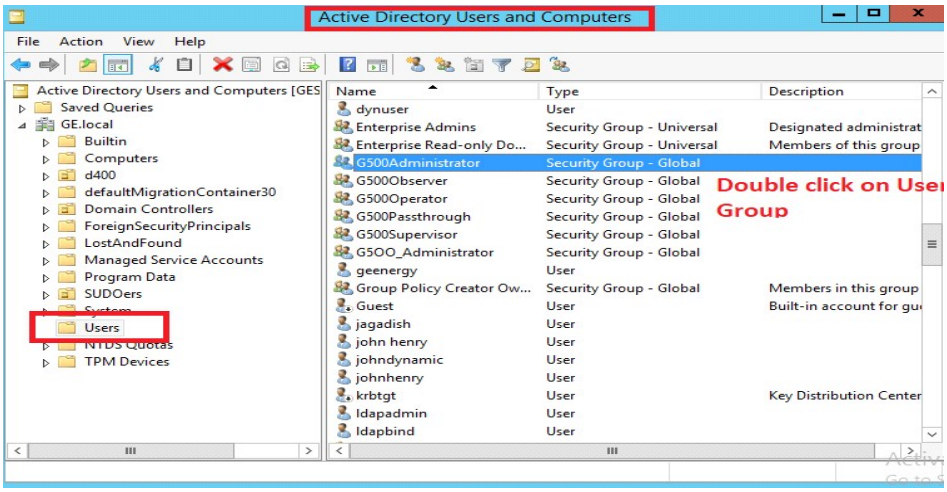
The AD Group Name in the table is an example. AD Group Name can be any name as configured by the user, Eg.: Test Group etc. In this example is listed as "G500…", could be "G100…".

Because the functionality is the same across MCP family, this could be "MCP…".

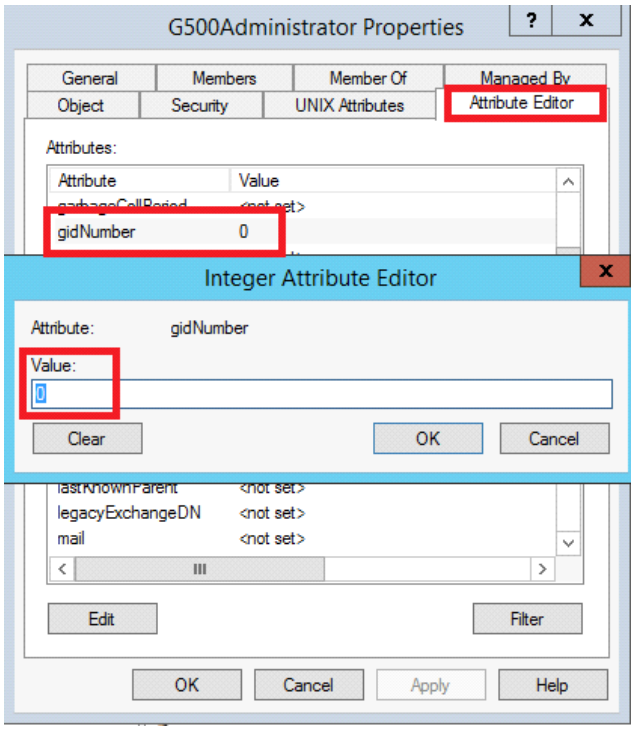
However, GID Number is fixed as specified in Table 1 for MCP (G500, G100) to recognize the same.

Example: In Active Directory, to map G500 device AD group with name "**G500Administrator**" to G500 group "**Administrator**" using static group mapping, the AD group **GID** must configured as in the Table 1.

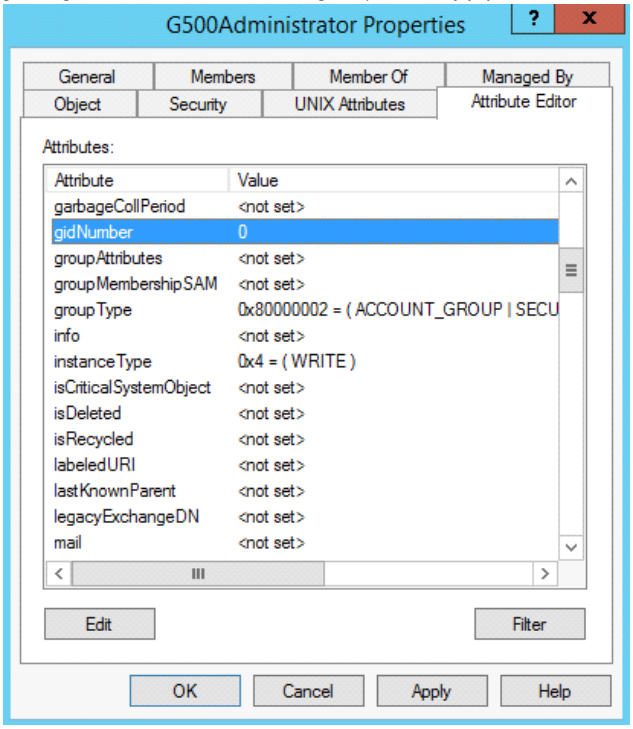
1. To input this GID Number double click on the group created in the above step and go to Attribute Editor tab:



2. Corresponding User Group properties index will be opened, click on **Attribute Editor** tab and enter the specific **gid number** as defined in Table 1 for different user role, like for administrator user group input the GID Number as 0.



3. After setting the gid number for AD User group click **Apply** and **OK**.

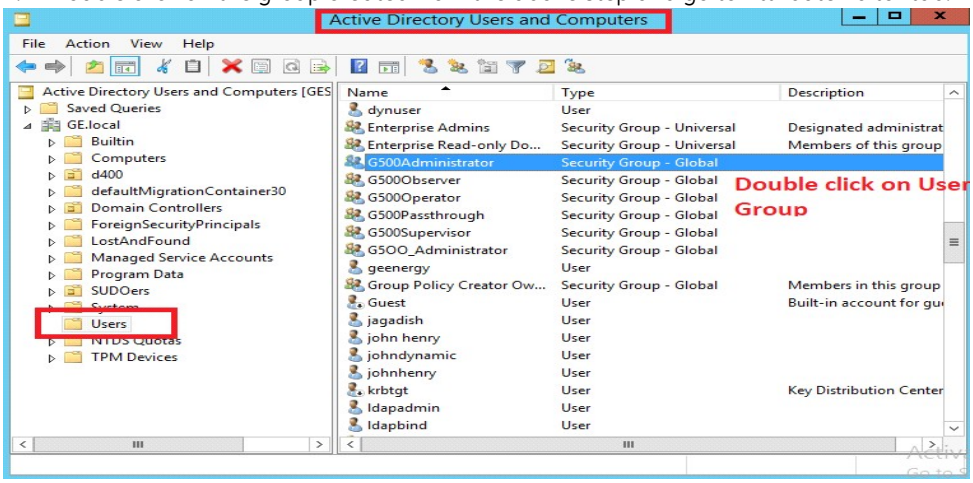


RESULT: G500Administrator group has been mapped successfully for **Administrator** role in G500. Now the user added to this group will have administrator role in G500 (MCP in general). "Procedure forAdding MCP AD users to MCP AD Groups" will be described in further sections in this document.

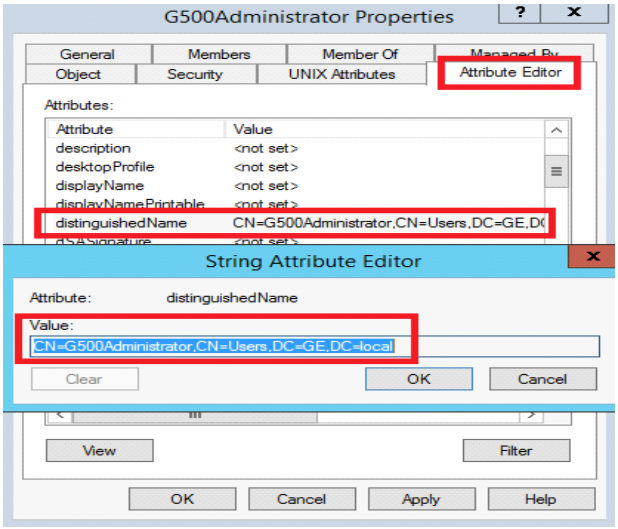
Procedure for Dynamic Group Mapping

In this approach, the MCP device AD Group distinguished name "DN" must be configured in MCP group mapping. If user want to go for this approach, then GID Number entry in AD Group is not required. To continue with Dynamic group Mapping follow the below steps (G500 is listed as example, applies to G100 and MCP family):

1. Double click on the group created from the above step and go to Attribute Editor tab:



2. Note down the distinguished name which is also called "**DN**" (double click AD User Group=>>Attribute Editor=>>distinguishedName):



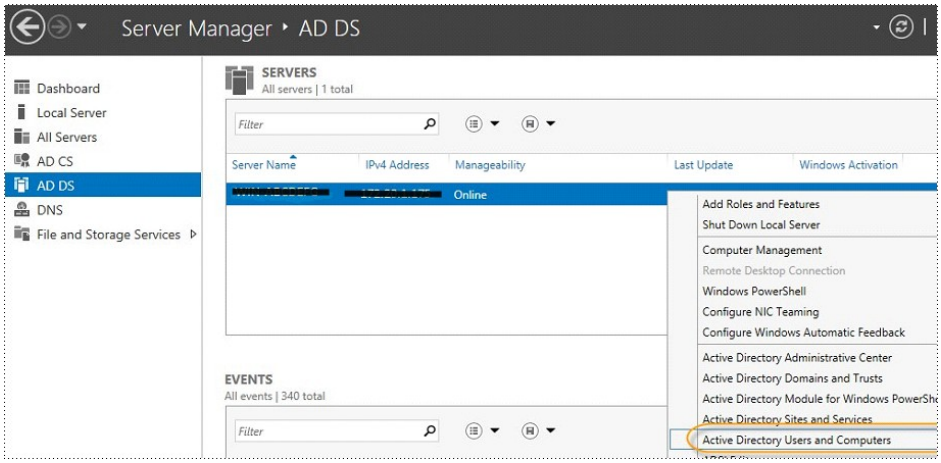
In the above example, the distinguished name (DN) of MCP device AD group G500Administrator is "**cn=G500Administrator,cn=users,dc=GE,dc=local**"

3. Login to MCP as administrator user and configure LDAP on the MCP device as mentioned in Procedure to configure LDAP on the MCP device.
4. Configure LDAP Group mapping as mentioned in "Procedure to configure Group Mapping on the MCP device".

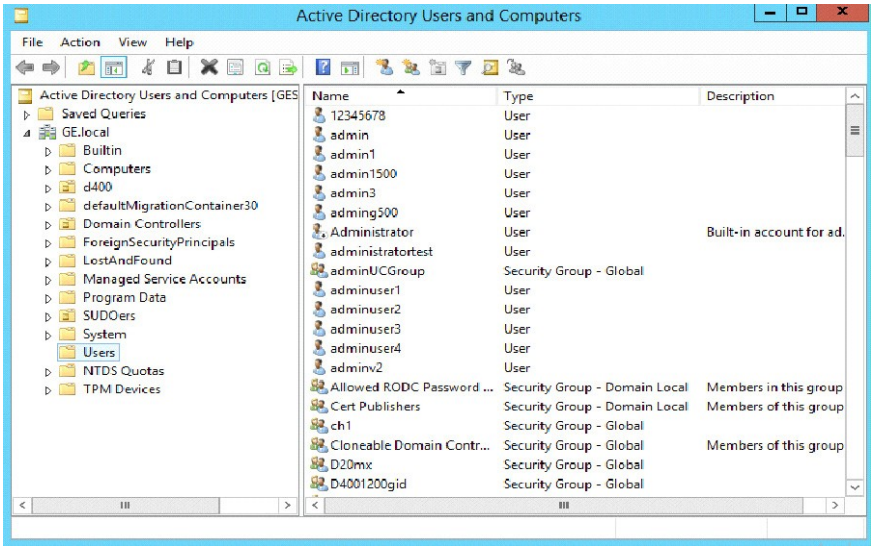
Procedure to create MCP device Users on Active Directory

Follow the below steps to create MCP device users on an Active Directory (AD):

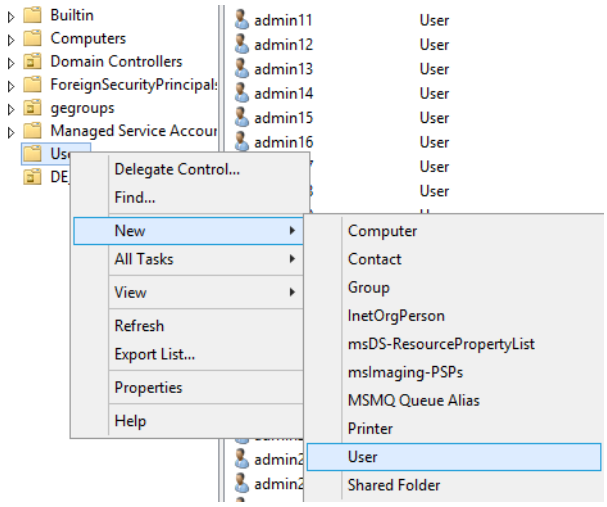
1. Open the Server Manager from the Windows Server 2012 **Start** menu and select **AD DS**.
2. Right-click on the server and select **Active Directory Users and Computers**.



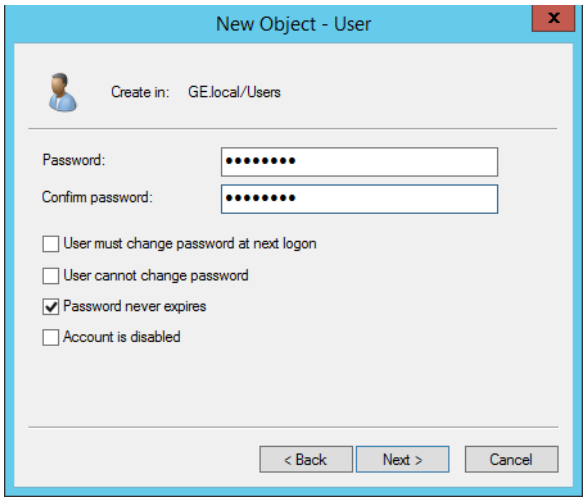
3. **Active Directory Users and Computers** window opens:



4. Right-click the Users folder and select **New User.**



5. Create a new User with Username: **ldapadmin.** The username must contain only the lower-case letters, numbers, "-" (dash), and "_" (underscore) characters. Click **Next**.
6. Type the password for the user, select **Password never expires** option and click **Next**.



NOTE The MCP device does not support the option **User must change password at next logon**.

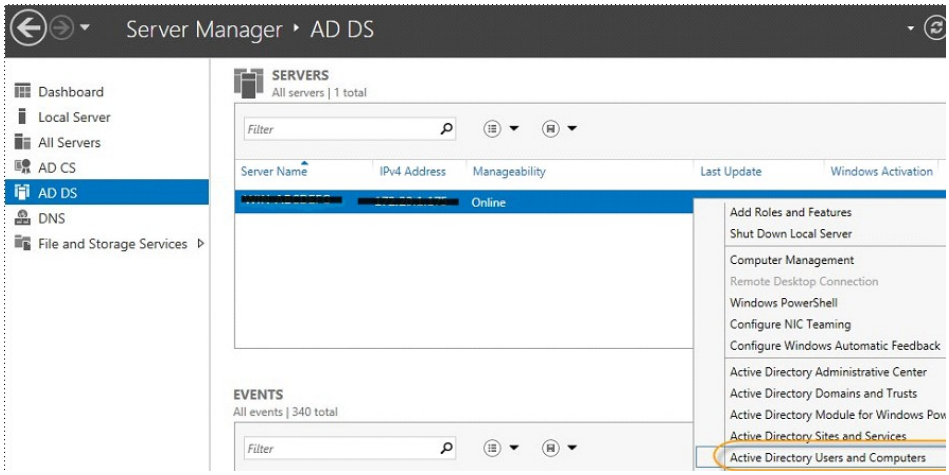
7. Click **Finish**.

   Result: The user is created in AD DS.

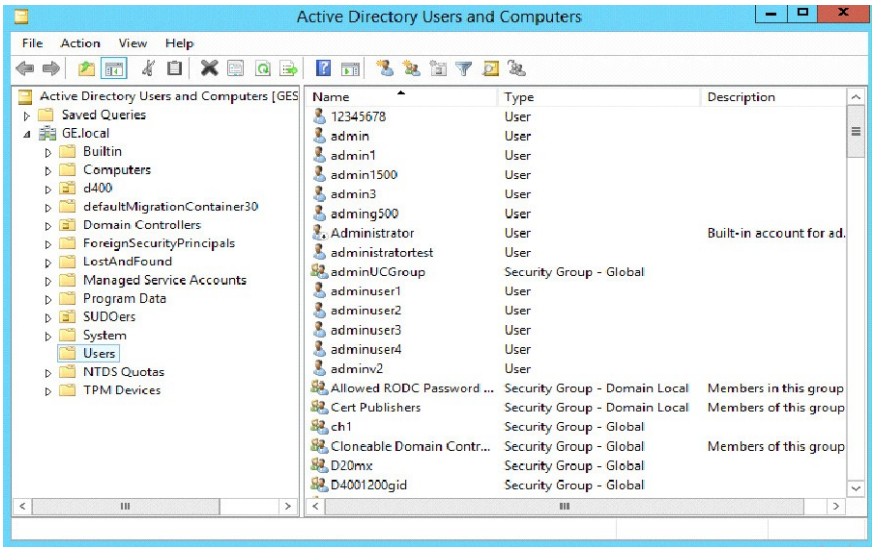
Procedure for Adding MCP AD users to MCP AD Groups

In the above sections MCP AD Groups and MCP AD Users have been created. Now it is required to add these users to corresponding groups. For example, add all the administrator users to administrator group, operator users to operator groups, observer users to observer group, supervisor user to supervisor group and passthrough users to passthrough group.

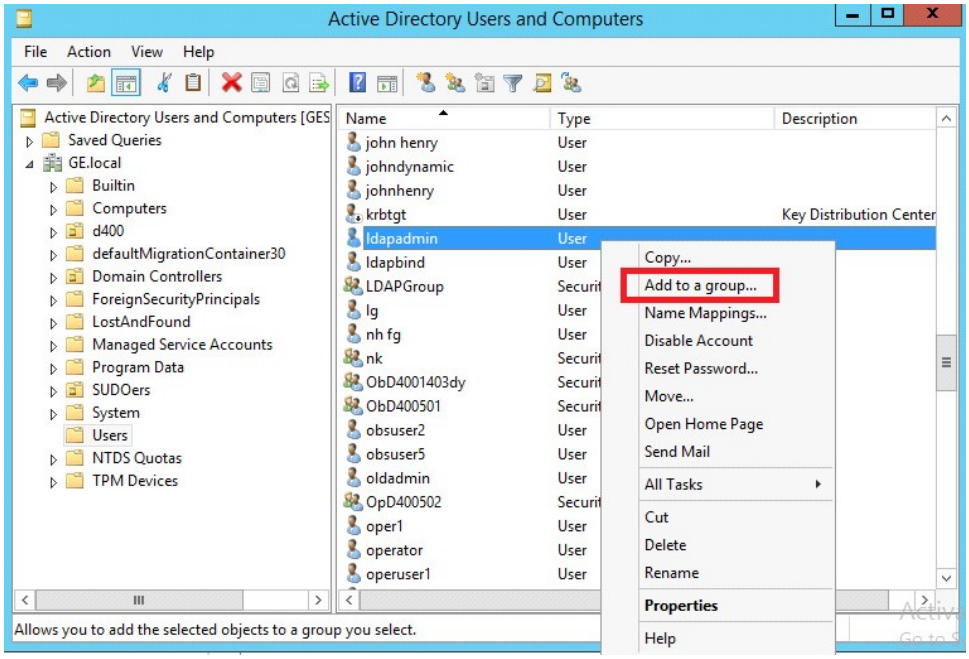
1. Open the Server Manager from the Windows Server 2012 **Start** menu and select **AD DS**.
2. Right-click on the server and select **Active Directory Users and Computers**.



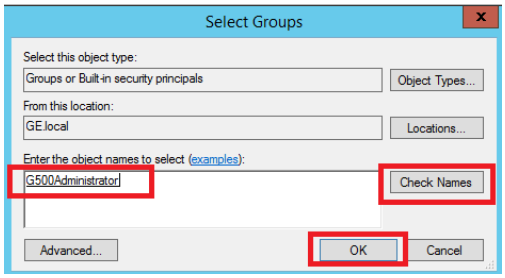
3. **Active Directory Users and Computers** window opens:



4. Right click on the **User** to be added and select **Add to a group** option (For example in above step we had created a user named "**ldapadmin**", so right click on it).



5. A new window will be opened to select User Group. Type the **MCP AD group name** (For example in above section we had created user group name **G500 Administrator**, type this name click on **Check Names** then click on **OK**).



RESULT: User is successfully added to MCP AD Group (G500Administrator in this example).

Installing AD CS

This section describes how to install Active Directory Certificate Service and import ROOT CA certificate onto the MCP device.

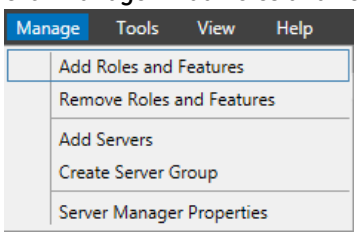
NOTE

If user would prefer to use a third-party certification authority instead of AD CS, the procedure to generate and import the certificate in Windows Server 2012 is described in the section Creating and installing a third-party CA certificate.

Install Active Directory Certificate Services on Windows Server 2012 procedure

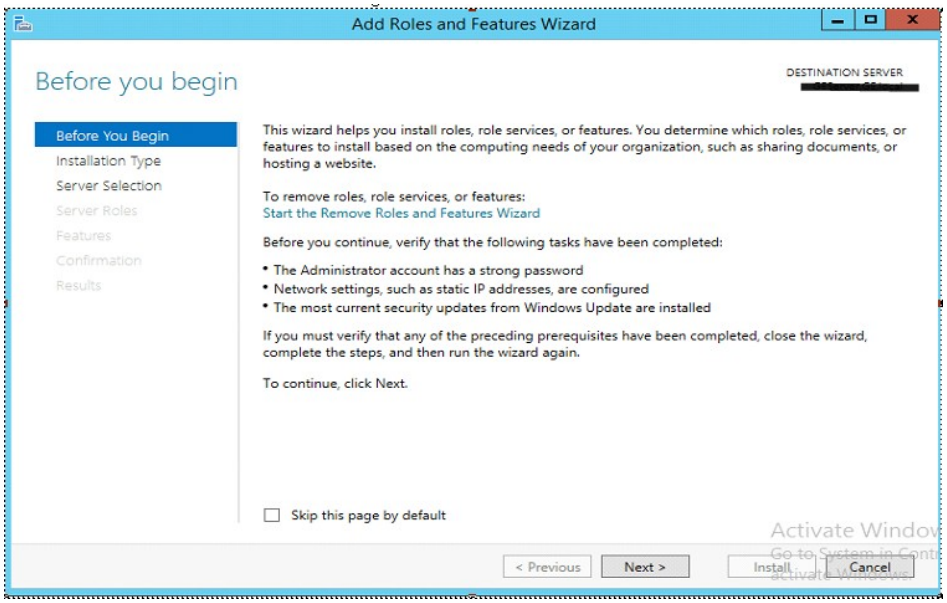
To install Active Directory Certificate Services on Windows Server 2012:

1. Add a new role:
   1.1. Select **Local Server** from the server manager.
   1.2. Click **Manage** > **Add Roles and Features**.

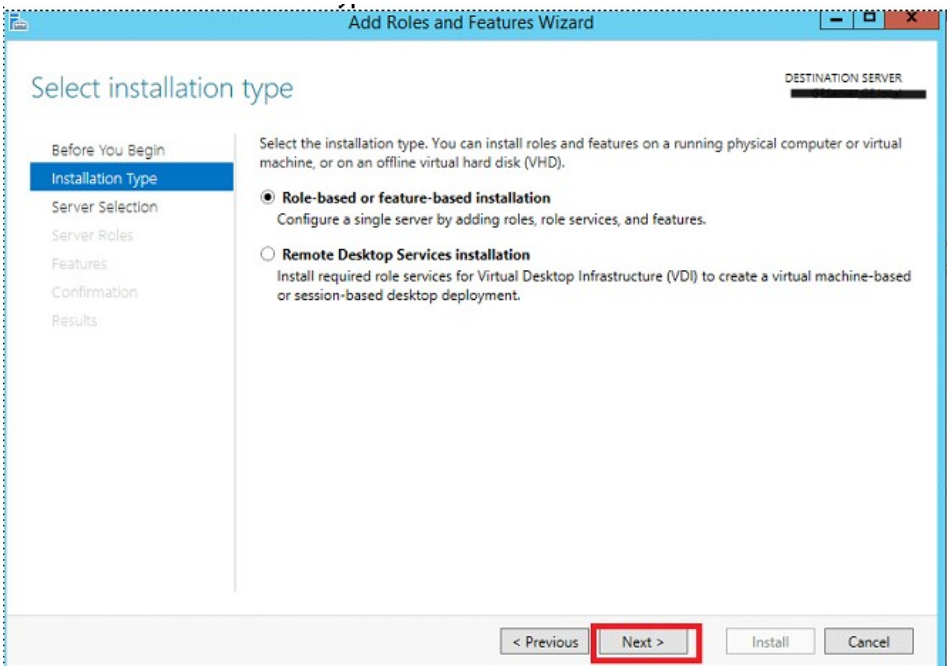


Result: The Add Roles wizard opens, showing the "Before You Begin" screen.

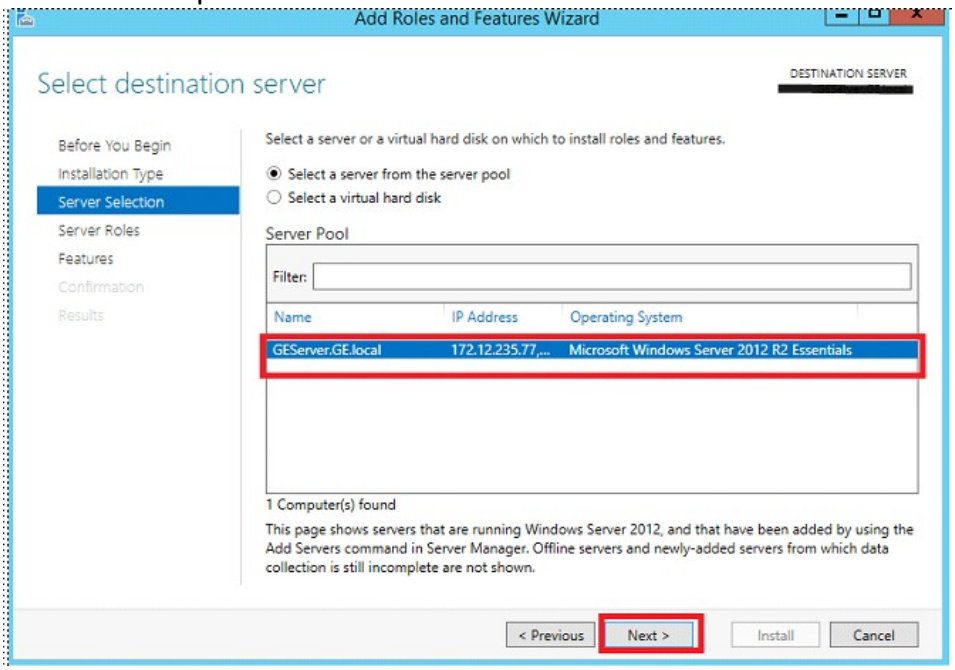
2. Steps for installing the Active Directory Certificate Authority:
   2.1. From the Before You Begin screen, click **Next**.



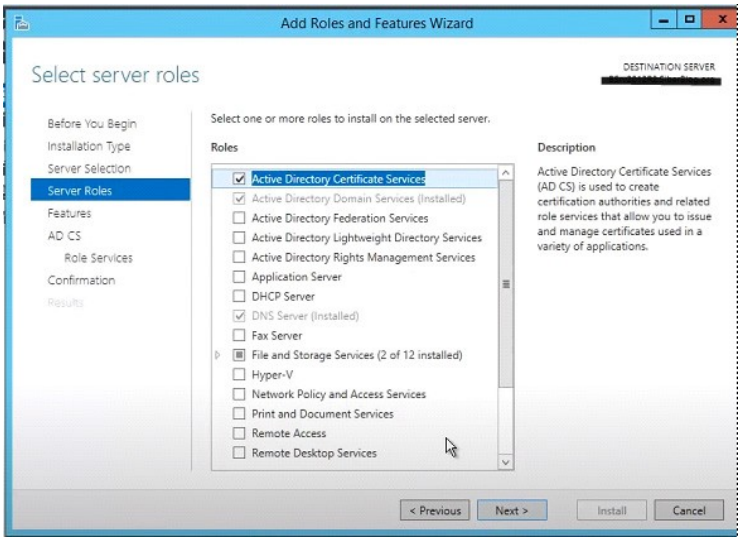
2.2. Select **Installation Type**: **Role-based or feature based installation**, click **Next**.



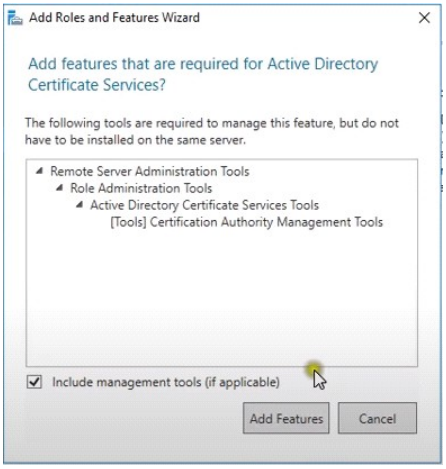
2.3. Under **Server Selection** menu, check the option **Select a server from the server pool** and click **Next**.



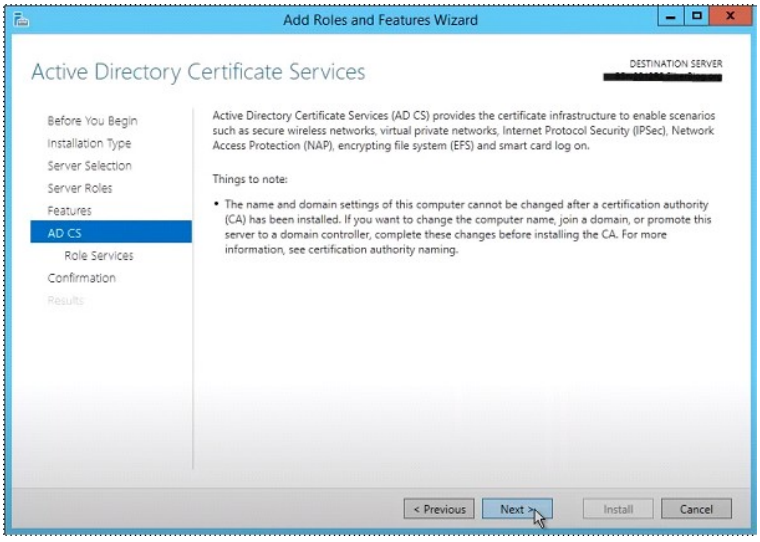
2.4. When the wizard displays list of **Server Roles**, select **Active Directory Certificate Services** check box and click **Next**.



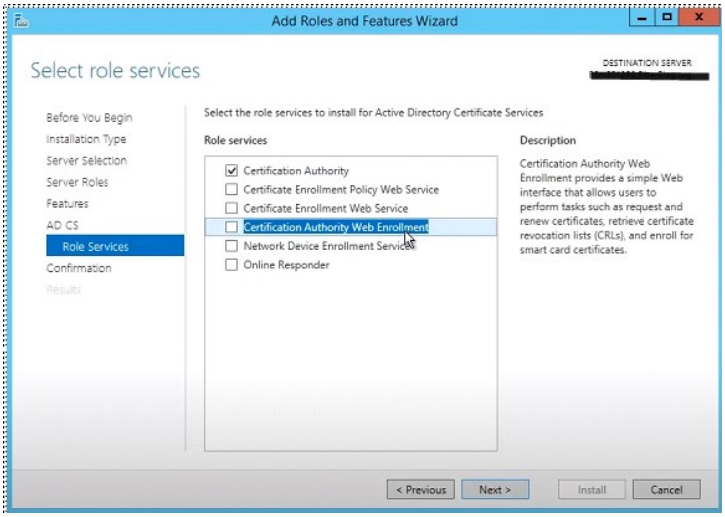
2.5. This opens up **Add Roles and Features** wizard. Click **Add Features**.



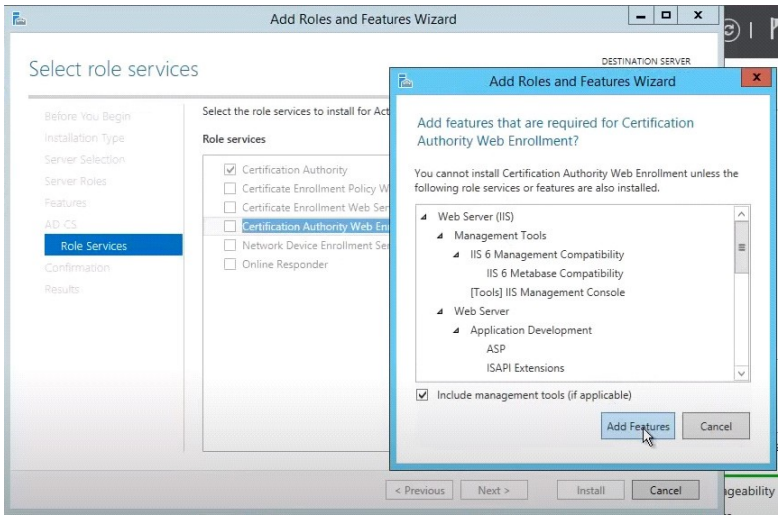
2.6. It opens the below screen. Click **Next**.



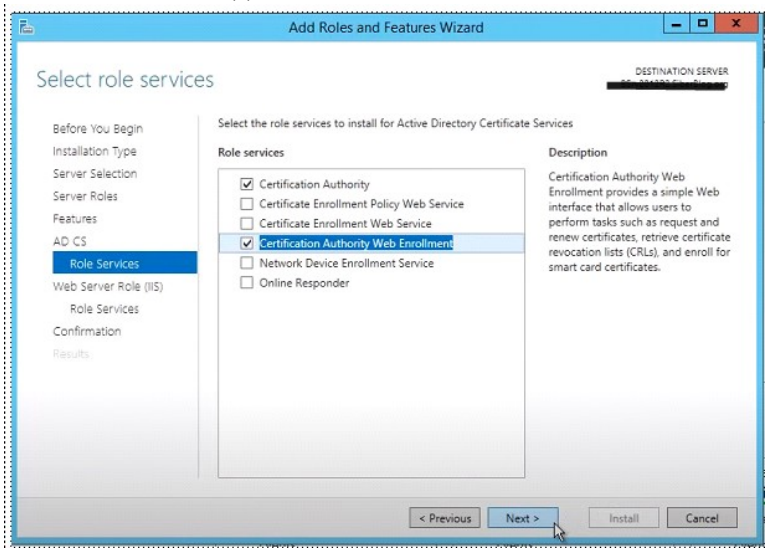
2.7. Select Certification Authority, Certification Authority Web Enrollment and click **Next**.



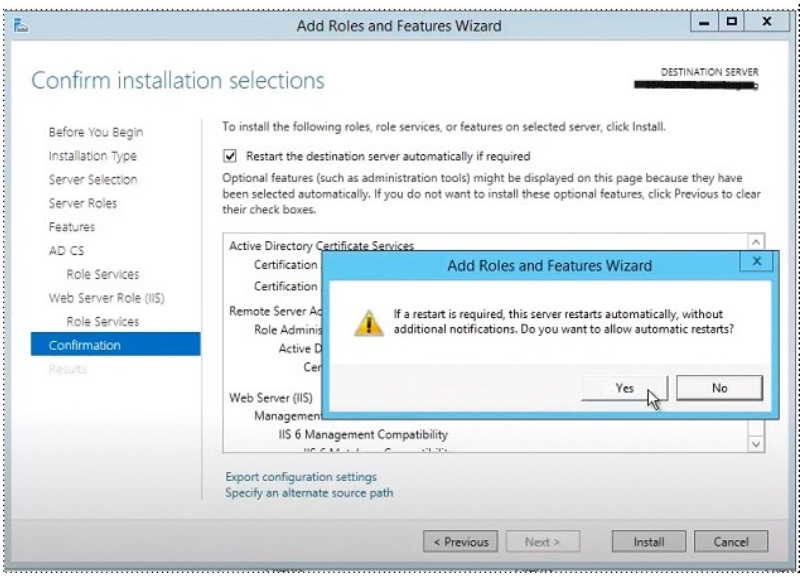
2.8. Click on **Add Features.**



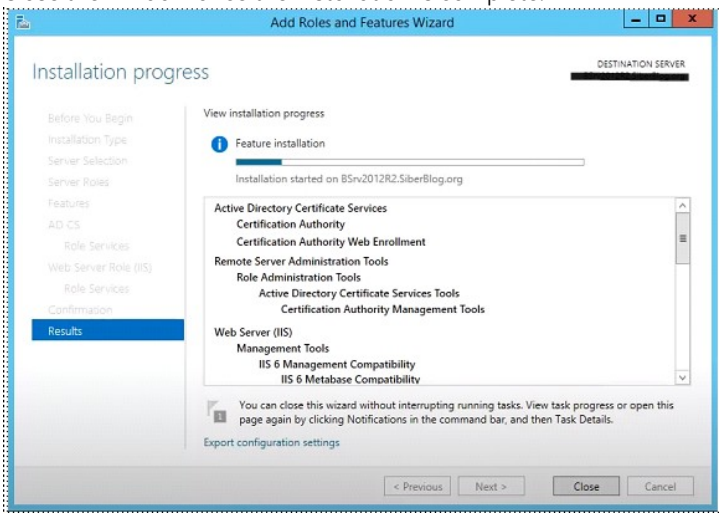
2.9. The below screen appears, click **Next.**



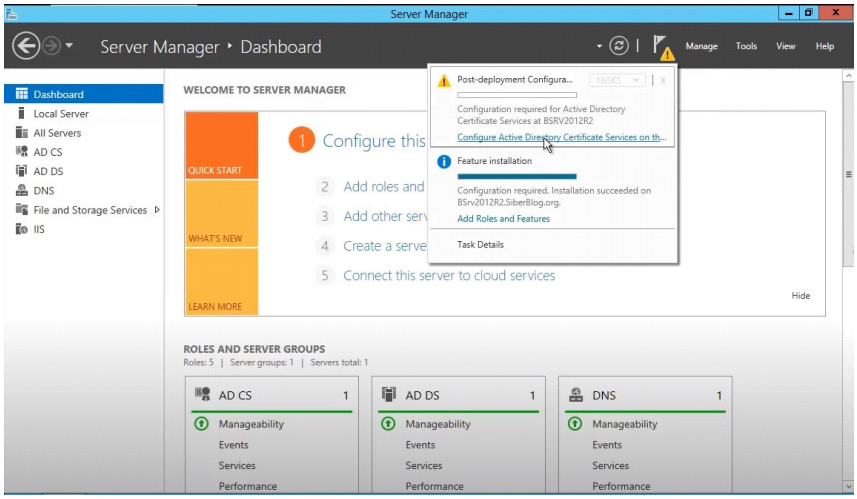
2.10. This goes to the confirmation Page. Check the check-box to Restart the destination server automatically if required and **Install**.



2.11. Close the window once the installation is complete.

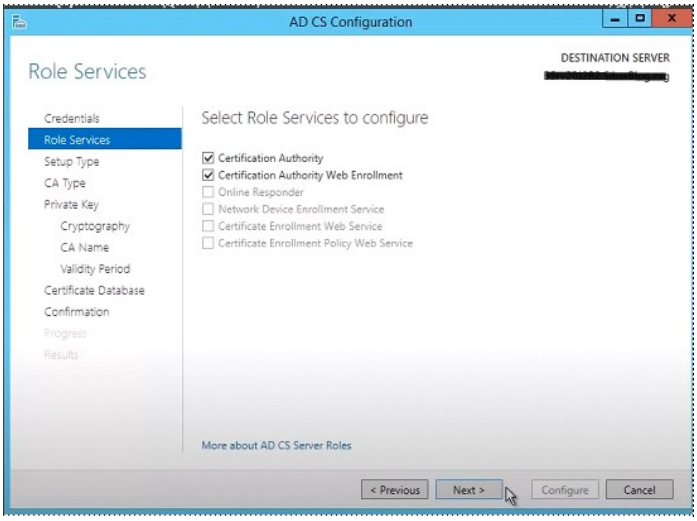


3. From the Server Manager Dashboard, click on the flag and click Active Directory Certificate Services.

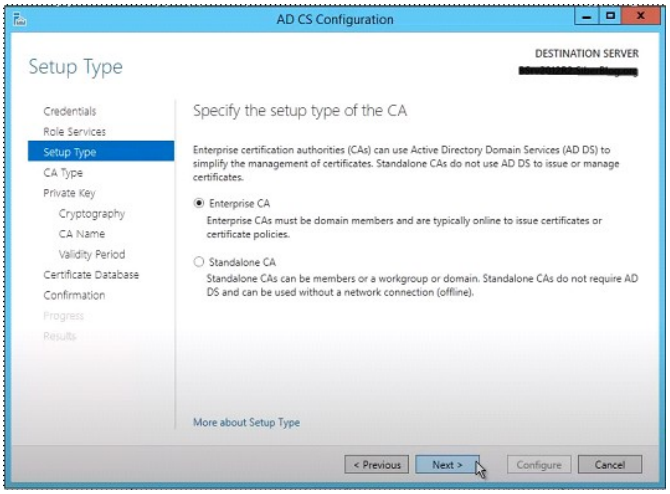


3.1. It opens the AD CS Configuration window, in which enter the server credentials and click **Next**.

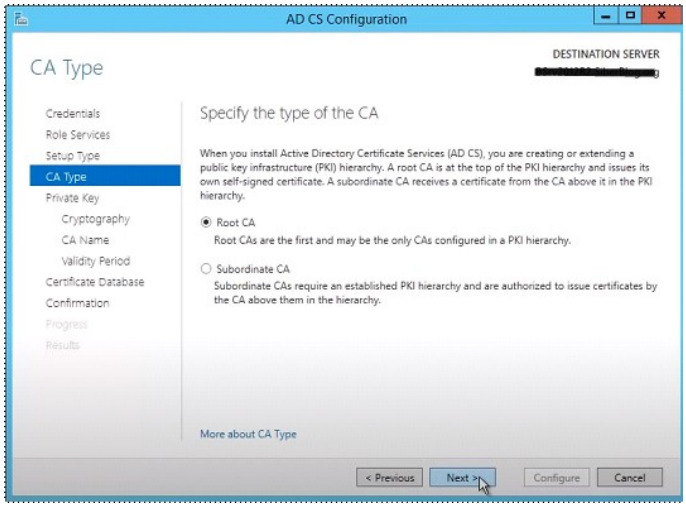
3.2. Select the below Role Services and click **Next**.



3.3. Select the Setup Type as Enterprise CA and click **Next**.



3.4. When prompted, select the **Root CA** option and click **Next**.

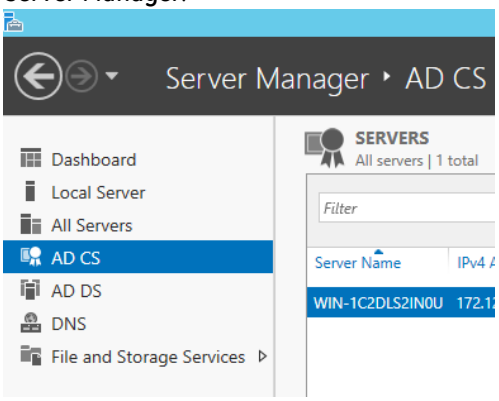


3.5. When prompted, select the **Create a new private key** option and click **Next**.

3.6. Select the hash algorithm, Common Name and Distinguished name of CA as per the Active Directory domain.

3.7. Set the CA certificate Validity period (default is 10 years but configurable) and complete the installation.

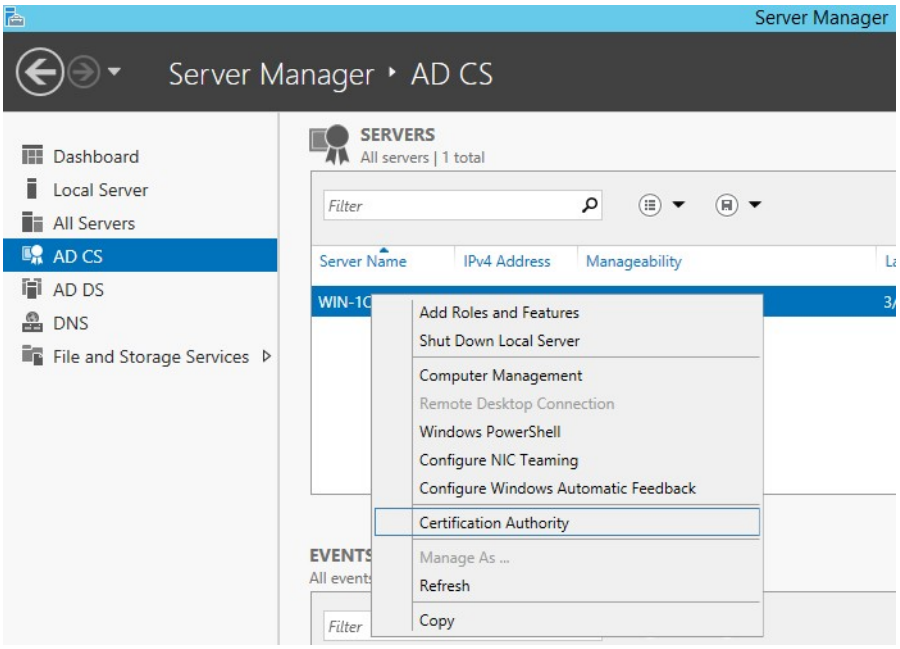
Result: Once installation is successfully completed, **AD CS** option is available in the **Server Manager**.



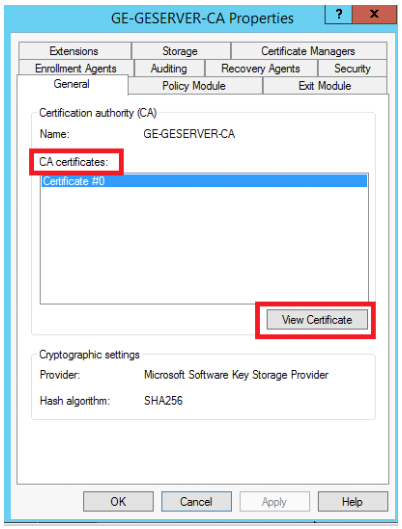
Exporting Root CA certificate to install on the MCP device

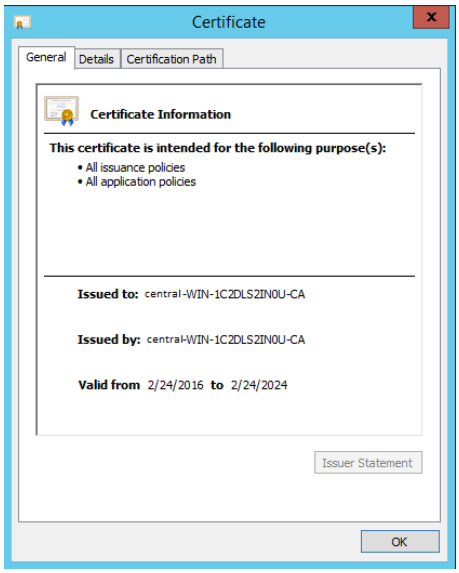
To export a Root CA certificate for installation on the MCP device:

1. From Server Manager select the **AD CS** option. Right click on the **Server** and select **Certification Authority**.

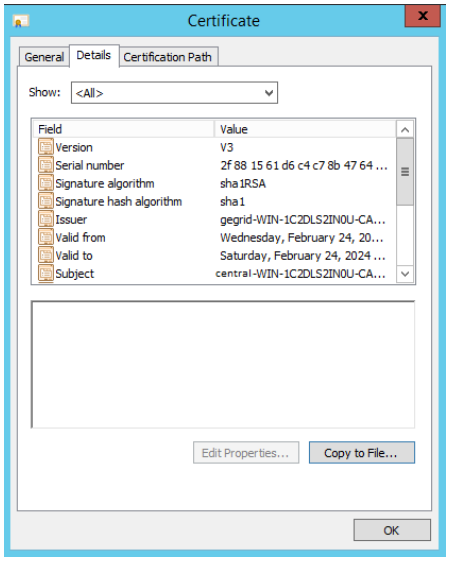


2. A new window opens, certsrv - Certification Authority.
3. In the Certification Authority window select the CA Certificate (i.e. root CA Certificate) and click **Properties**.
4. You can view the Root CA Certificate details like Issue to, Issue by, validity by clicking on **View Certificate**.

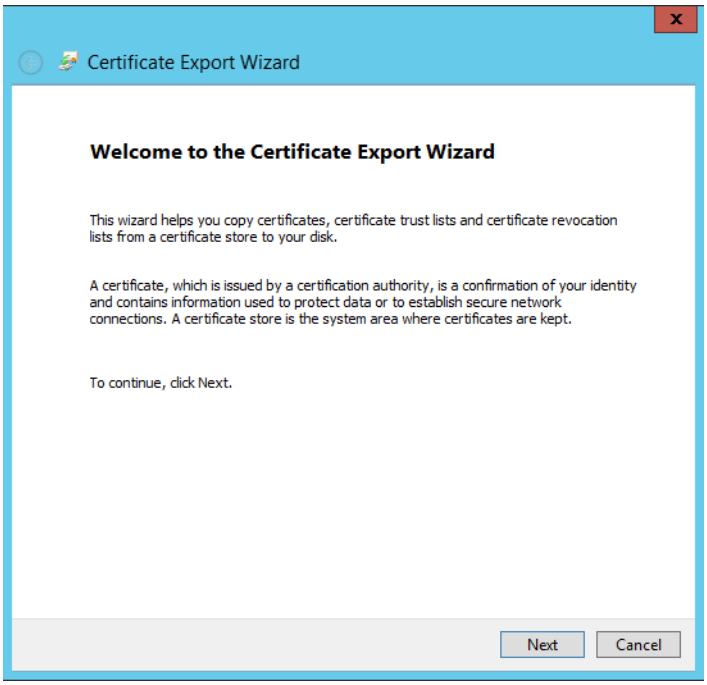




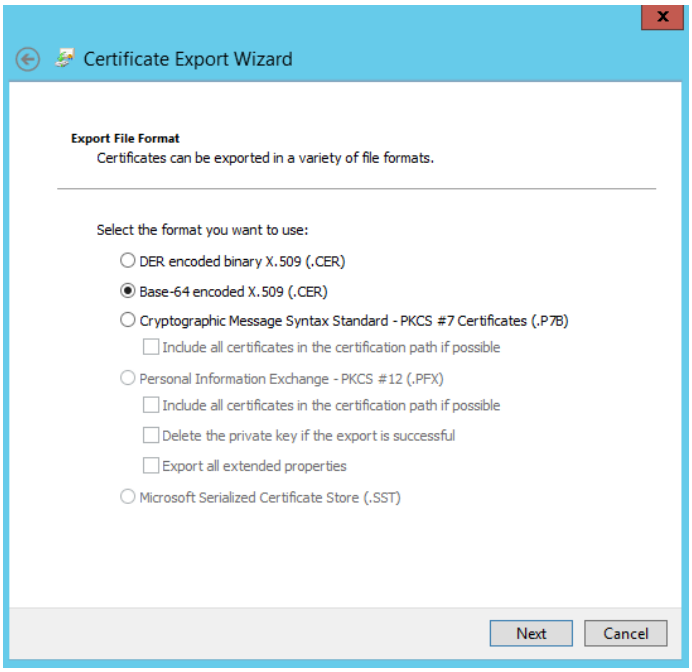
5. Export the root CA certificate to a file by clicking on the **Details** tab and then **Copy to File** button.



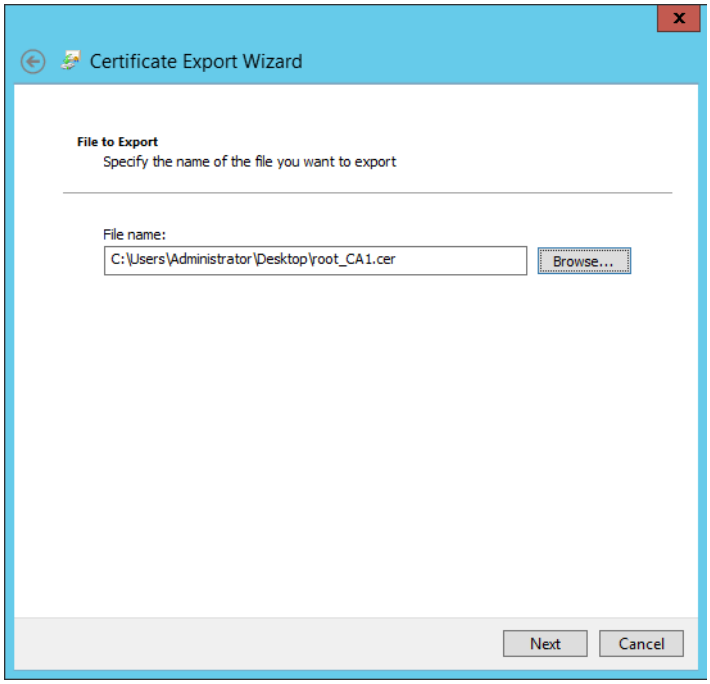
Result: The Certificate Export wizard opens.



6. Click **Next** to continue.
7. Select the export format by selecting the **Base-64 encoded x.509 (.CER)** option and click **Next**.



8. Give the certificate a name with **.cer** extension and then click **Next** to finish the certificate import from AD CS.



Result: A message appears: Export is successful. The certificate is saved in the destination path selected.

Installing CA Certificates on the MCP device

This section describes how to install the CA Certificate to the MCP device. There are two type of certificates you can create:

- Server certificate
- Client certificate

Files to be Created	• CA certificate to be installed in both the Client and Server. • Server Certificate to be installed in the Server for Server Authentication (This can be skipped if AD CS us used to create the CA Certificate).	
Files to be Transferred	**MCP**	MyCA.crt or MyCA.cer (LDAP Client)
	Windows Server 2012	MyCA.crt or MyCA.cer servercert.p12 (LDAP Server) (This can be skipped if AD CS is used as Certification Authority).

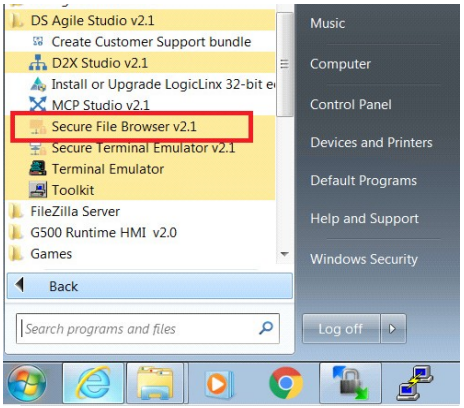
CA Certificate transfer procedure from PC to MCP

You can import and install the CA certificate to MCP. This certificate can be transferred to MCP for installation, using either of the below two options:

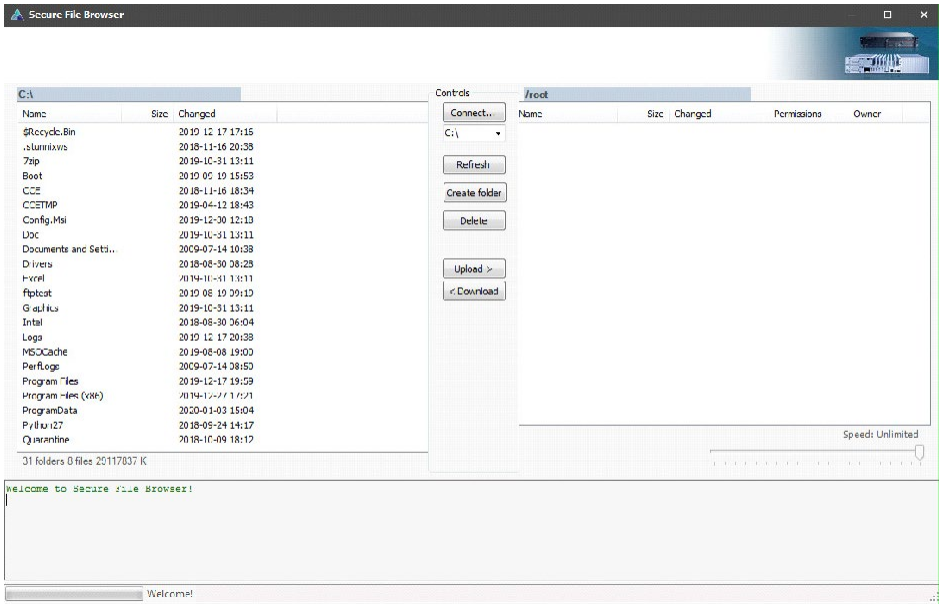
1. CA Certificate Transfer to MCP by using DSAS Secure File Browser
2. CA Certificate transfer to MCP by using external Secured USB

CA Certificate Transfer to MCP by using DSAS Secure File Browser

1. Copy the files containing the CA certificate to the following MCP location: **/mnt/usr/SecureScadaTransfer**
   - This can be done using the DSAS Secure File Browser (SFTP file transfer program).
   - To launch DSAS Secure File Browser, click on: **Start>All programs>DS Agile Studio vX.0> Secure File Browser vX.0**.

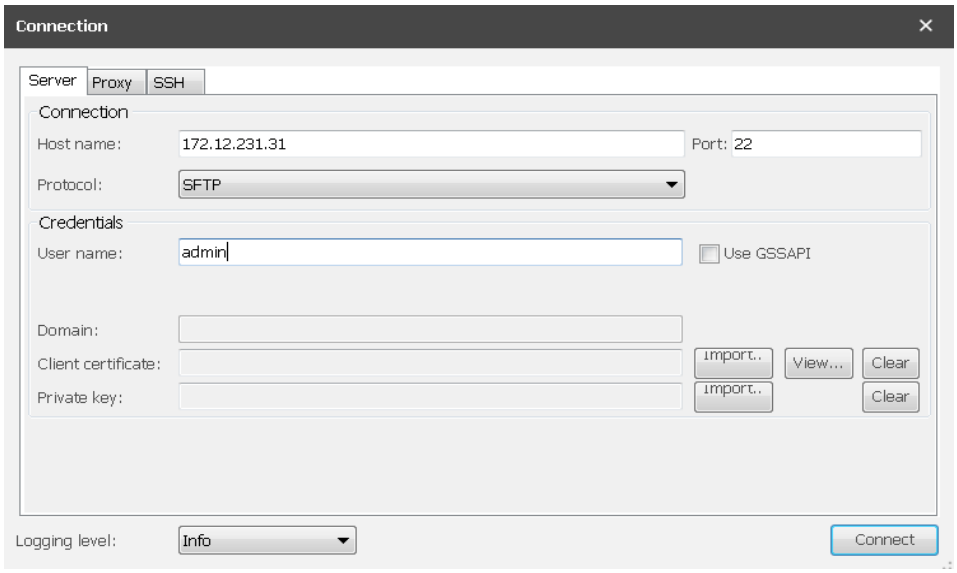


   - Secure File Browser screen will be launched as below:

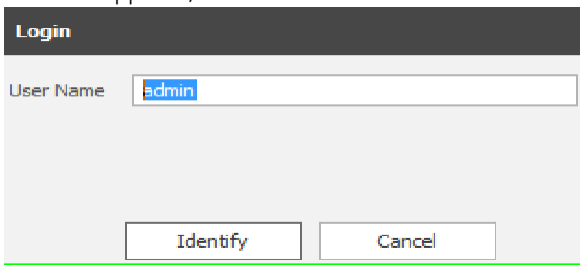


   - Click **Connect**.
   - The Connection Details window will appear.

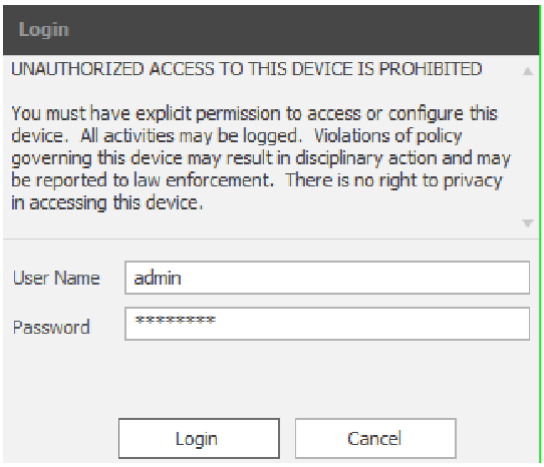
- Enter Host name: MCP IP, Protocol: SFTP, User name details and then click **Connect**.



- A Login window appears, enter the MCP User Name and click **Identify** tab.

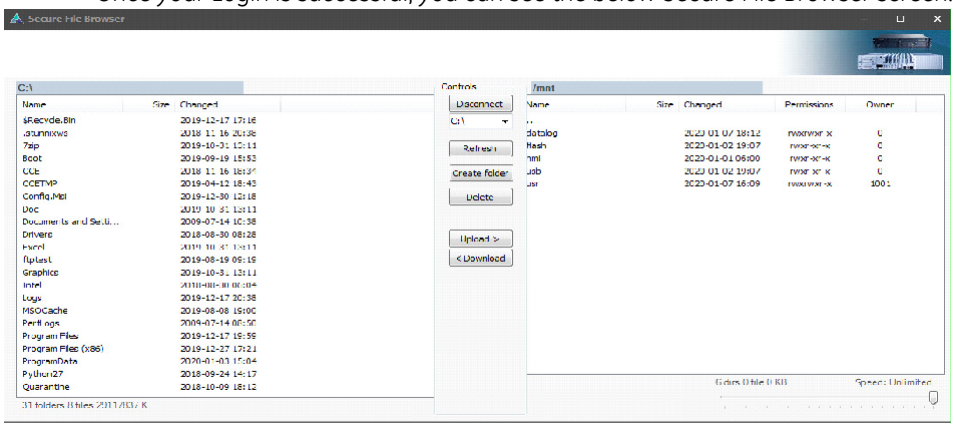


- Once the User Name is identified with the MCP, a Login window appears and prompt for the Password.

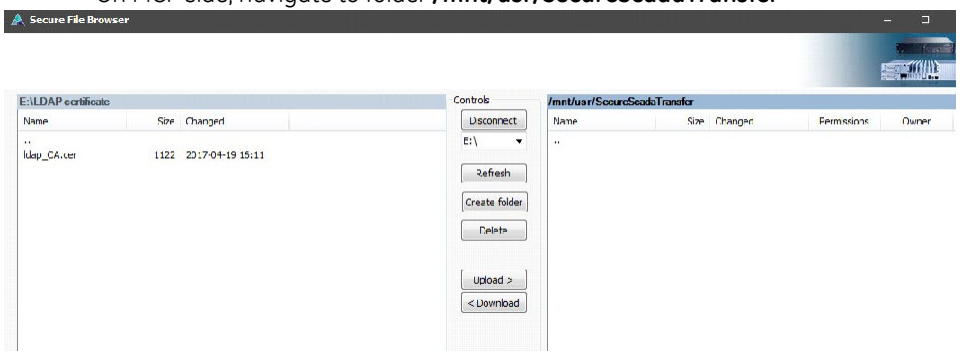


- Enter the Password and click **Login** to access the MCP folders.

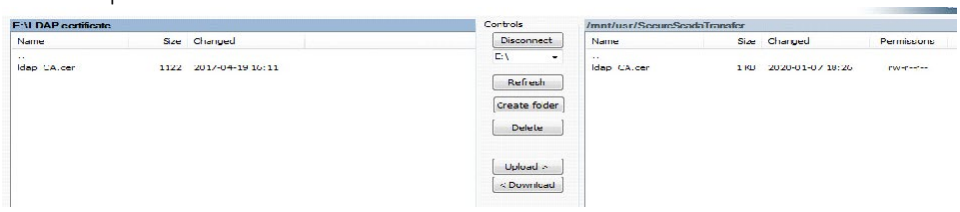
- Once your Login is successful, you can see the below Secure File Browser screen:



- In the Secure File Browser window, PC folders are displayed on the left side and the MCP folders are displayed on the right.
- On MCP side, navigate to folder **/mnt/usr/SecureScadaTransfer**



- Select the required certificate from the PC folder and click **Upload**. This will upload the files from PC to MCP.



NOTE

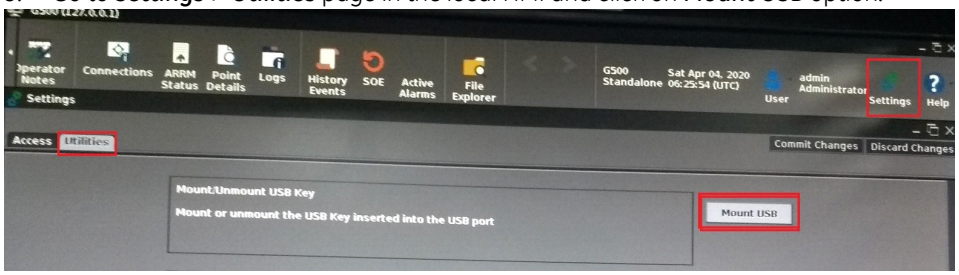
After completion of these steps, LDAP client certificate is transferred successfully to MCP and is ready for installation.

CA Certificate transfer to MCP by using external Secured USB

Once the LDAP client certificate (CA certificate) is created and available on the PC and you can transfer this CA certificate to MCP using USB as follows:

1. Create a directory in USB drive "**SecureScadaTransfer**".
2. Copy the CA certificate from PC to USB on a USB drive (LDAP Client certificate need to be available in USB at **\SecureScadaTransfer**).
3. Insert the USB drive into any USB slot on the MCP device. E.g.: USB Port-1
4. Open Local HMI and login as administrator user.

5. Go to **Settings > Utilities** page in the local HMI and click on **Mount USB** option.



6. Now USB is mounted successfully to MCP and CA certificate is available at **/mnt/usb/usb1/SecureScadaTransfer**.

CA Certificate Installation procedure

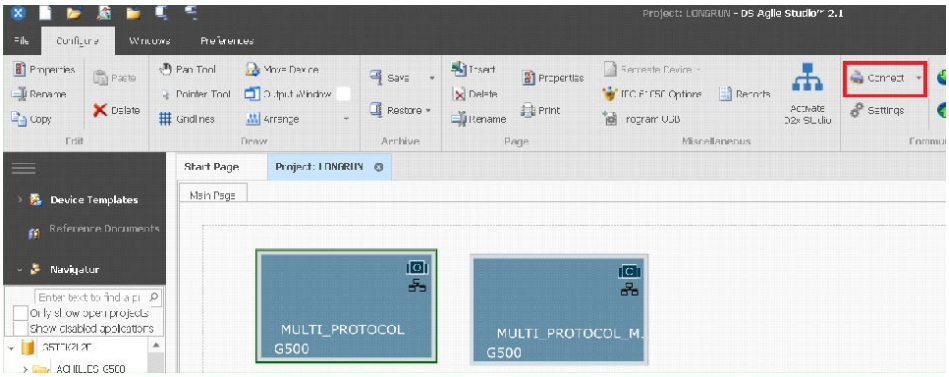
Once the certificate is available in MCP by any of the transfer procedure mentioned in page 39 (Secure DSAS Browser or USB), it can be installed by using either of the below two interfaces:

- Import and Install CA certificate through Runtime DSAS
- Import and Install CA certificate through Local HMI

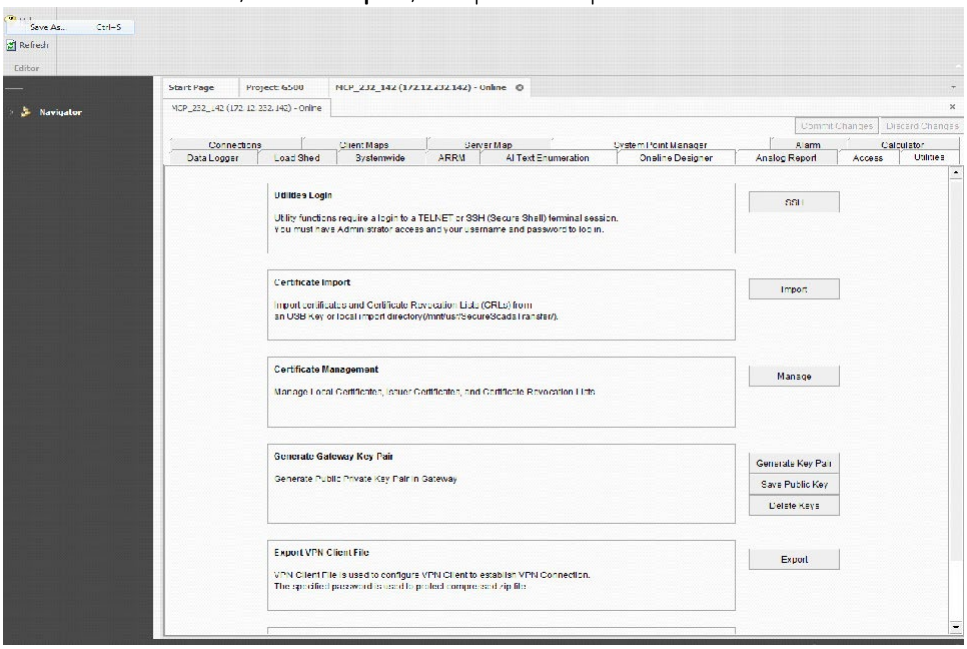
Import and Install CA certificate through Runtime DSAS

After certificate transfer to MCP at **/mnt/usr/SecureScadaTransfer/** or certificates can be installed to MCP using **DSAS > Utilities**. To proceed follow the below steps:

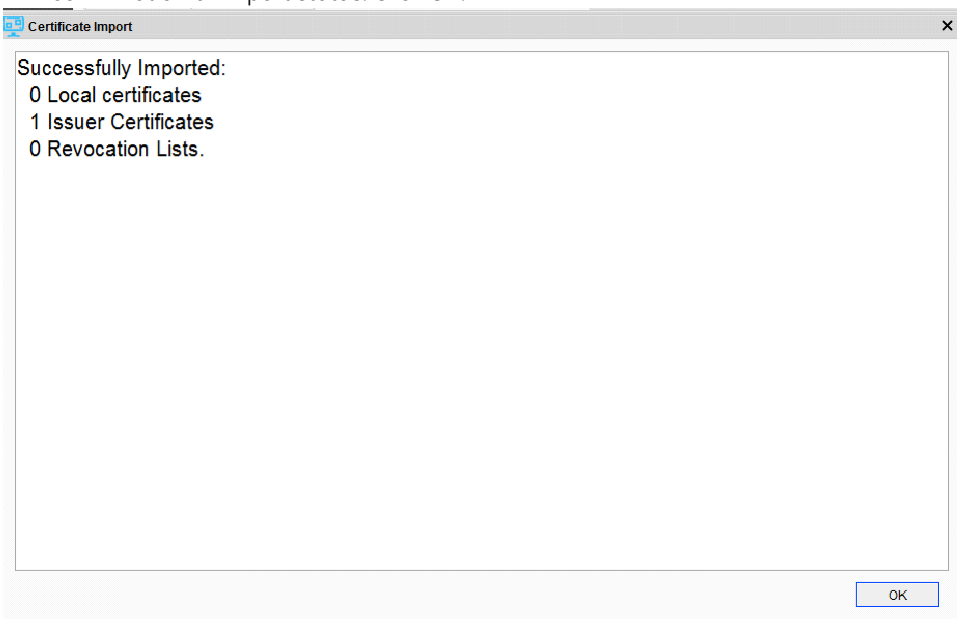
1. Open MCP Studio and click **Connect** to MCP.



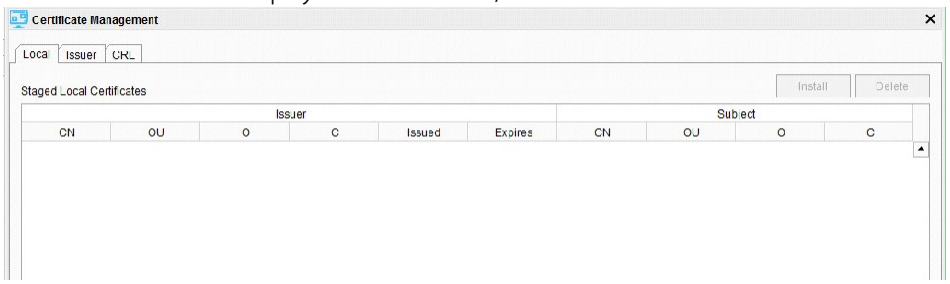
2. Select Utilities tab, click on **Import**, to import the copied certificates.



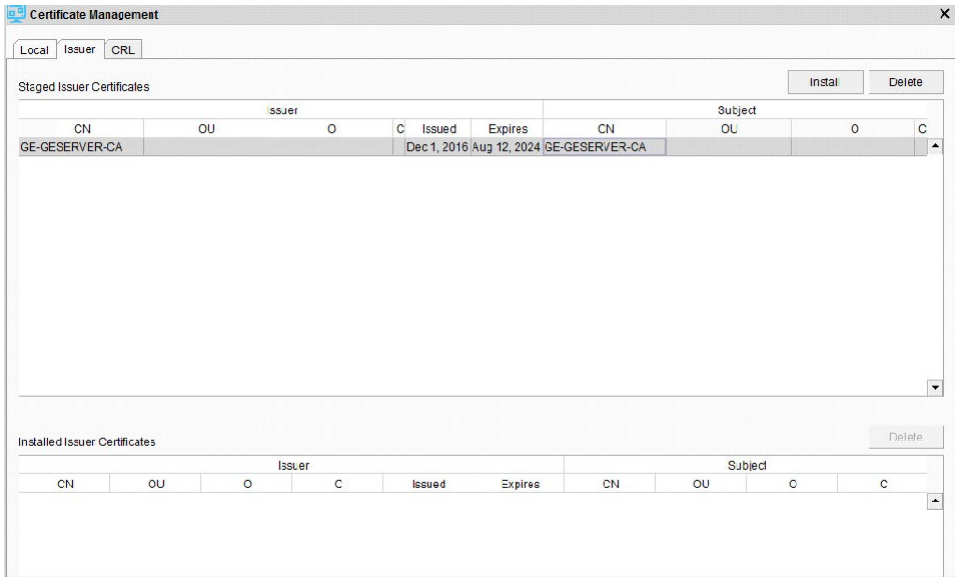
3. Once the certificates are imported, a Certificate Import window appears which shows confirmation of import status. Click **OK**.



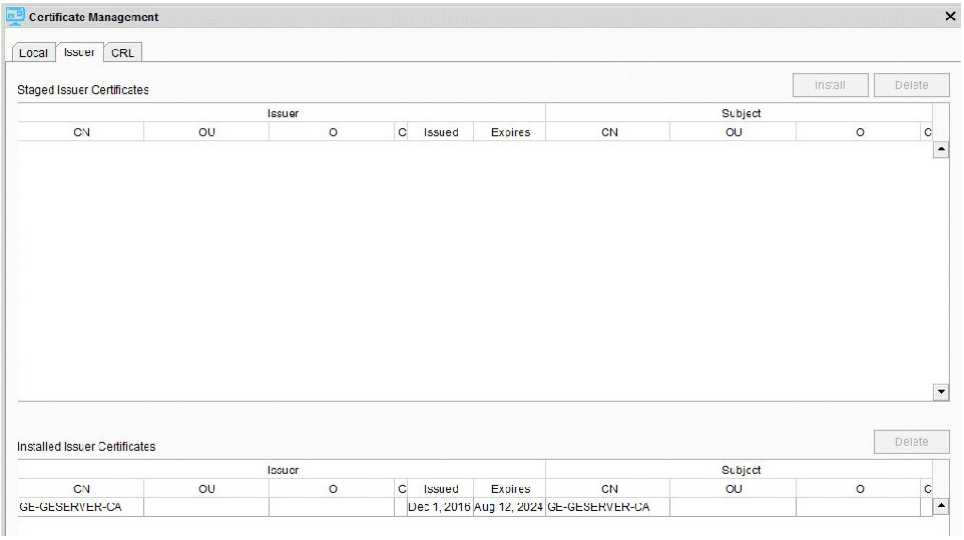
4. Once the certificates are imported successfully, click "**Manage**" to manage local certificates which display three tabs **Local**, **Issuer** and **CRL** as below:



5. Click on **Issuer** tab, select the Certificate and click **Install**.



6. Once the certificate is installed successfully, it is moved to the Installed Issuer Certificates section:



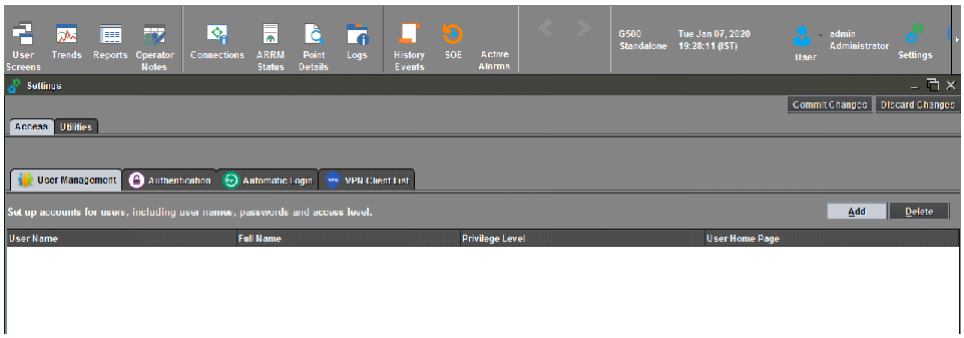
RESULT: This completes the Certification Installation process through DSAS Online HMI. You can use this certificate in LDAP Authentication.

Import and Install CA certificate through Local HMI

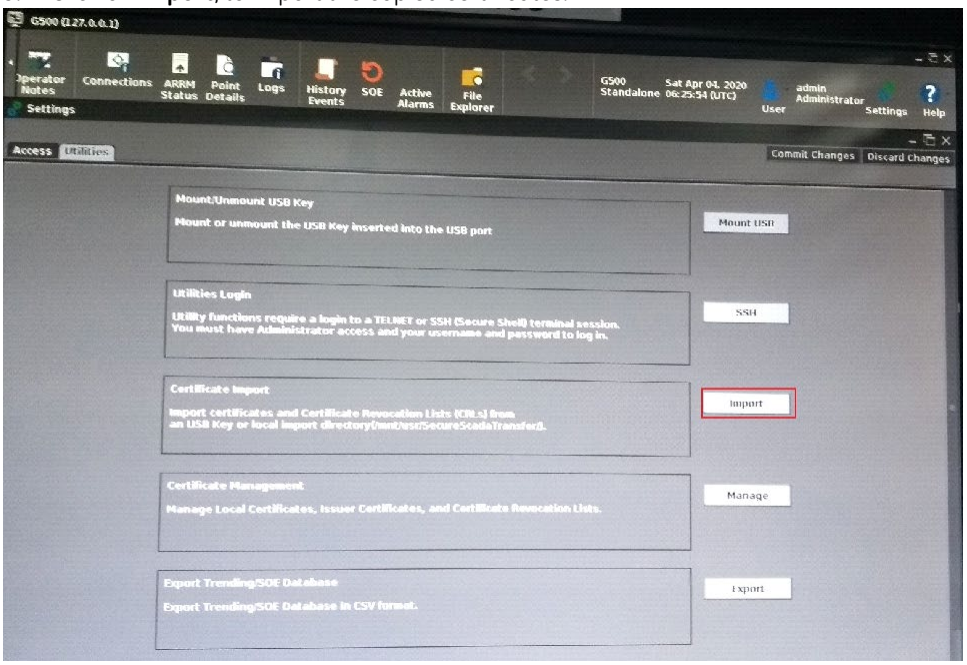
After the certificate is transferred to the MCP at **/mnt/usr/SecureScadaTransfer/** or **/mnt/ usb/usb1/SecureScadaTransfer/** certificates can be installed to MCP using **Local HMI > Settings > Utilities**. To proceed follow the prescribed steps as below:

1. Open Local HMI and click **Settings** tab.

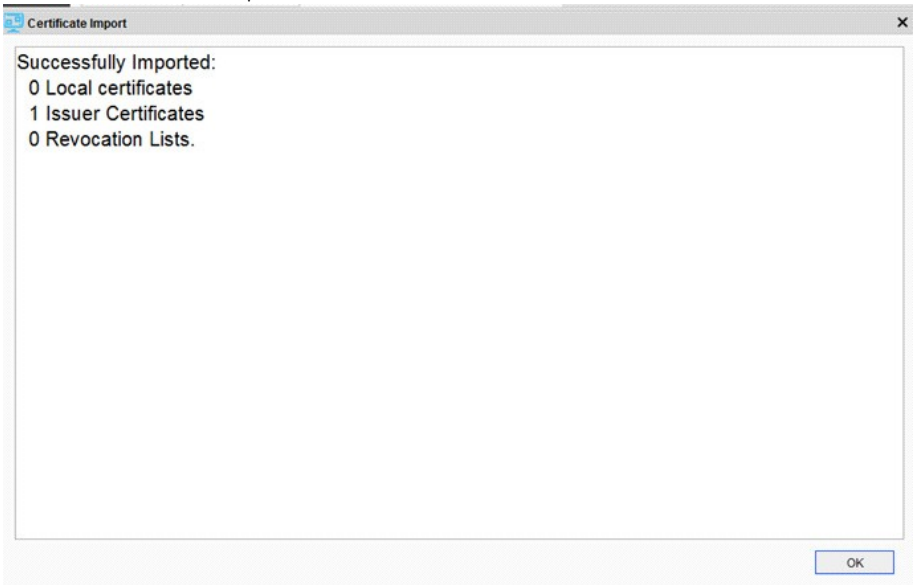
2. Click **Utilities** tab.



3. Click on **Import**, to import the copied certificates.

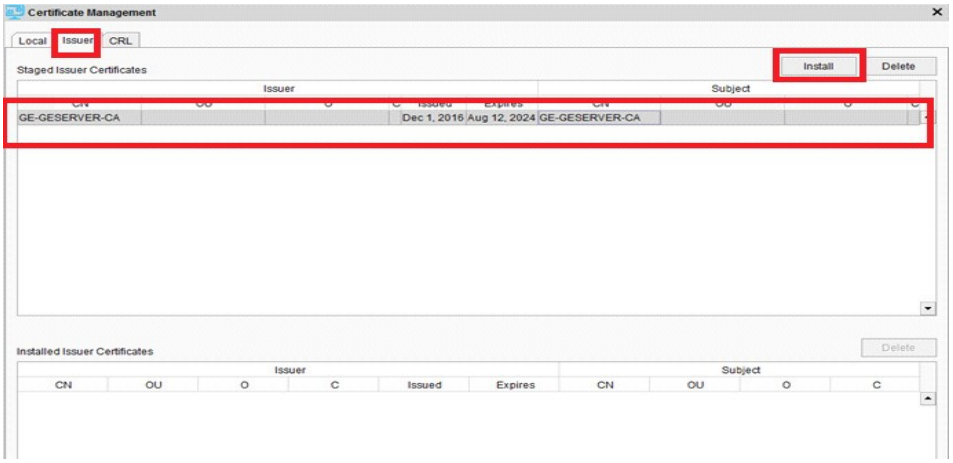


4. Once the certificates are imported, a Certificate Import window appears which shows confirmation of import status. Click **OK**.

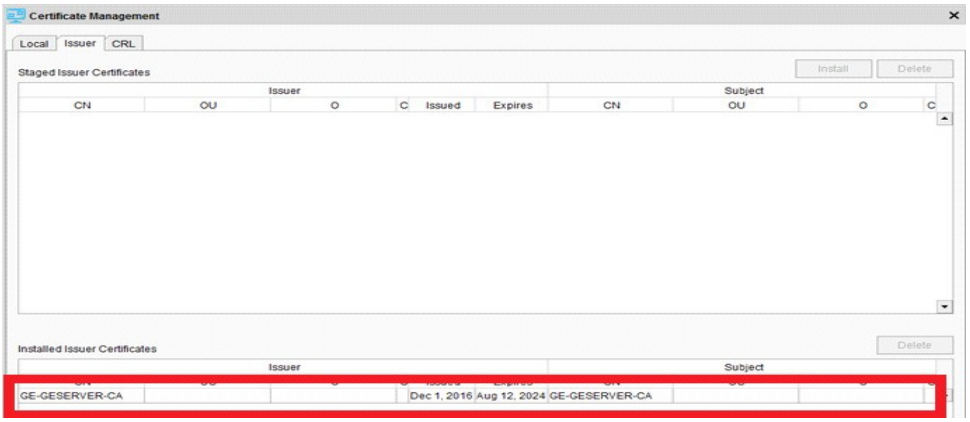


5. Once the certificates are imported successfully, click "**Manage**" to manage local certificates which display three tabs Local, Issuer and CRL as below:

6. Click on **Issuer** tab, select the Certificate and click **Install**.



7. Once the certificate is installed successfully, it's moved to the Installed IssuerCertificates section:



RESULT: This completes the Certification Installation process through DSAS Online HMI. You can use this certificate in LDAP Authentication.

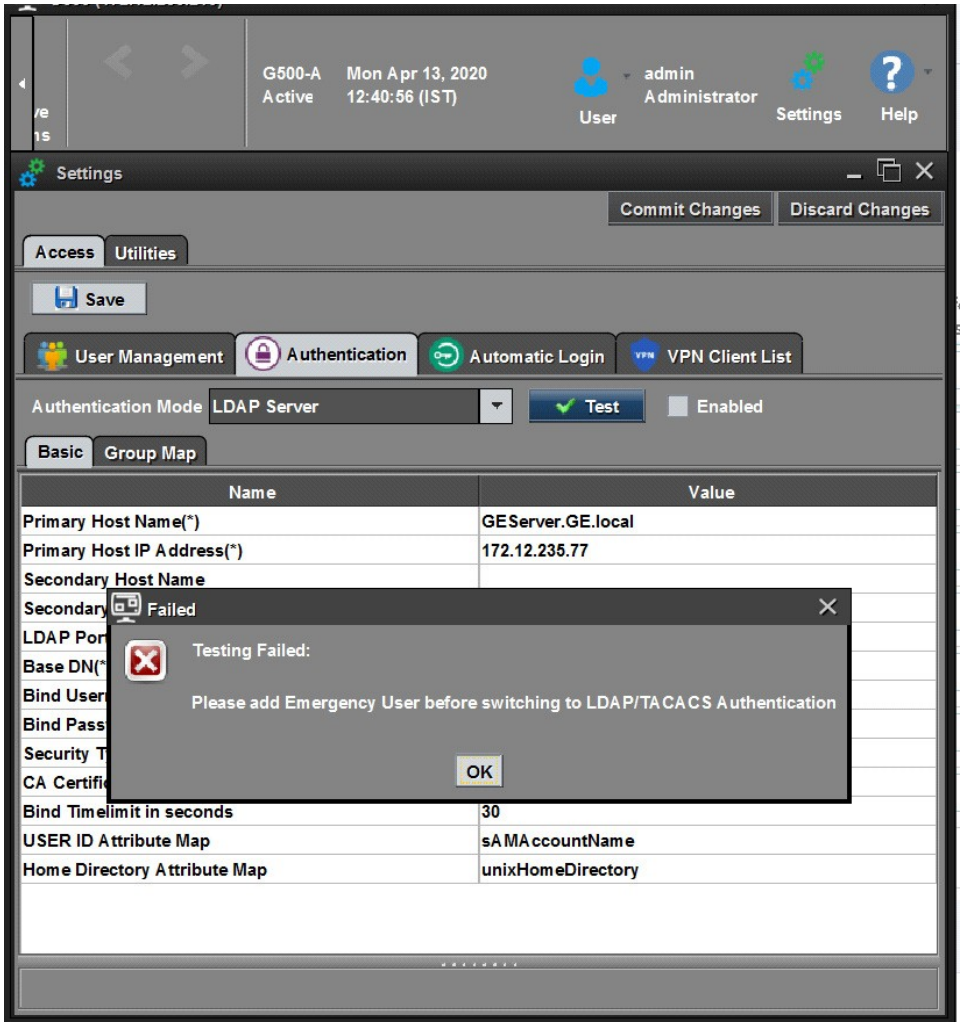
Configuring LDAP on the MCP device

This section describes the:

- Tasks performed prior to configuring the LDAP on the MCP device and
- The procedure to configure the LDAP on the MCP device.

Prerequisites to configuring LDAP on MCP device

Prior to configuring the LDAP on the MCP device it is mandatory to create emergency user in MCP. If user directly start LDAP configuration by using section Procedure to configure LDAP on the MCP device then user will get popup message that "Please add Emergency User before switching to LDAP/TACACS Authentication" and user will not be able to configure LDAP authentication without adding emergency users.



Create an Emergency Administrator User

This emergency user can be used when remote authentication server is not available and user in unable to access MCP using Remote Authentication. This emergency admin user is required to get access to the system in case of emergency, i.e. when LDAP server is not responsive / user forgets all credentials etc.

Emergency Users can be created by using any of the below two option:

- Using Web MCP Settings GUI
- Using the mcpcfg utility on MCP device through Secure Terminal Emulator

An emergency administrator user can login to MCP using any of the below three interfaces:

1. SSH session to MCP (Port-922)
2. Front serial port connection to MCP (Baud Rate- 115200)
3. MCP Emergency option in local console

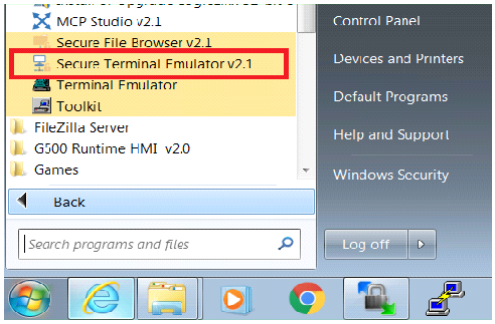
Once user logs into MCP as Emergency Administrator user, executing "emercfg" command shall provide options for user to perform the below two key functions:

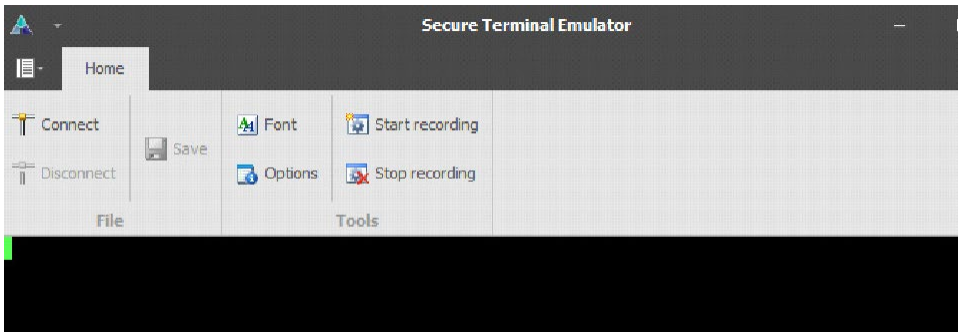
- Change the mode authentication from remote to local mode.
- Generate emergency code to login to HMI without changing authentication from remote to local mode.

Below sections describes how to add emergency user in MCP by using any of these option step by step:

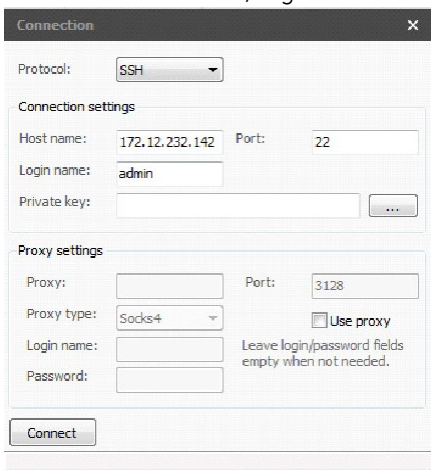
Using the mcpcfg utility on MCP device through Secure Terminal Emulator

1. To open Secure Terminal Emulator, select **Start > All Programs > DS Agile Studio vX.0 > Secure Terminal Emulator vX.0**

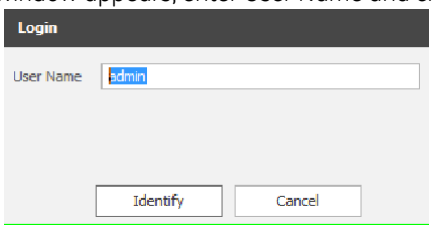




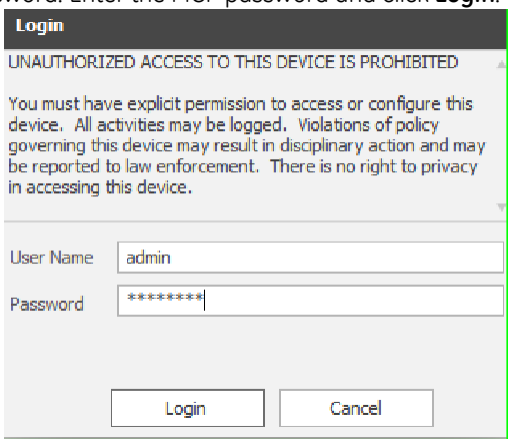
2. Click **Connect**. A pop-up window appears which shows Connections credentials.
3. Enter your MCP IP in Host name, Login name and Port 22 and click **Connect**.



4. A Login window appears, enter User Name and click **Identify**.



5. Once the User Name is identified with the MCP, a Login window appears to prompt for the Password. Enter the MCP password and click **Login**.



6. Once you login successfully, MCP Shell window appears:

```
GE Multilin MCP Firmware Release 110 Production Build 391 2020-01-01:04:41:24

admin@G500:~$
```

7. Type **sudo mcpcfg** and enter your Administrator User Name and Password if prompts.
8. The Gateway Settings Menu appears:

```
================================================================
        Gateway Settings Menu
================================================================

        0.   Back
        1.   Configure Authentication
        2.   Configure Network Settings
        3.   Configure Network Interfaces
        4.   Configure Secure Access
        5.   Configure Firewall
        6.   Configure Host Names
        7.   Configure Time & Time Sync
        8.   Reset System Logs
        9.   Reset Database Tables
        10.  Reset File Persistence Data
        11.  Local HMI
        12.  Configure Sync Manager
        13.  Redundancy
        14.  ARRM
        15.  Suppress Forced Qualities To Masters
        16.  Emulate D20 RTU IEC101 DPA Unbalanced Mode Functionality
        17.  Configure IEC101+104 DPA Startup Quality Event Suppress Interva
        18.  Configure Serial Ports
        19.  Configure D.20 Port Settings
        20.  EdgeOS Host
        21.  Clear Chassis Intrusion State
```

9. Enter **1** to select **Configure Authentication** option and the below menu appears:

```
         Gateway Settings Menu   Authentication
=================================================

         Current AuthMode Status : Local

         0.   Back
         1.   Root Administrator Settings
         2.   Pass-Through Password Authentication
         3.   Administrator Group Users
         4.   Emergency Group Users

Enter Your Choice : ( Between 0 and 4 ):
```

10. Enter **4** to select **Emergency Group Users** to Add an Emergency Admin User.

```
=====================================================
        Gateway Settings Menu
        Authentication - Emergency Admin Group Users
=====================================================

        0.   Back
        1.   List Users
        2.   Add User
        3.   Change Password
        4.   Remove User

Enter Your Choice : ( Between 0 and 4 ):
```

11. Enter **2** to Add User.
12. Enter the new emergency user name, full name, password and re-enter password.

```
=============================================================
        Gateway Settings Menu
        Emergency Group Users - Add user in Emergency group
=============================================================


Enter user name : emadmin

Enter user's full name : Emergency Administrator

Enter the password for emadmin:
Re-enter the password :
```

13. Type "**Y**" to confirm to the user.

```
=============================================================
        Gateway Settings Menu
        Emergency Group Users - Add user in Emergency group
=============================================================


Enter user name : emadmin

Enter user's full name : Emergency Administrator

Enter the password for emadmin:
Re-enter the password :

You entered:
User Name      : emadmin
User Full Name : Emergency Administrator

Confirm that you want to add this user ? <Y/N> :
```

14. Once user is added successfully, press **Enter**.

```
================================================================
        Gateway Settings Menu
        Emergency Group Users - Add user in Emergency group
================================================================


Enter user name : emadmin

Enter user's full name : Emergency Administrator

Enter the password for emadmin:
Re-enter the password :

You entered:
User Name      : emadmin
User Full Name : Emergency Administrator

Confirm that you want to add this user ? <Y/N> :        y


Successfully added user : emadmin

Press ENTER Key to continue....
```

15. Navigate back to Emergency Group Users and enter **1** to view the List of Emergency Admin Group Users.

```
=======================================================
        Gateway Settings Menu
        Authentication - Emergency Admin Group Users
=======================================================

        0.   Back
        1.   List Users
        2.   Add User
        3.   Change Password
        4.   Remove User

Enter Your Choice : ( Between 0 and 4 ):
```

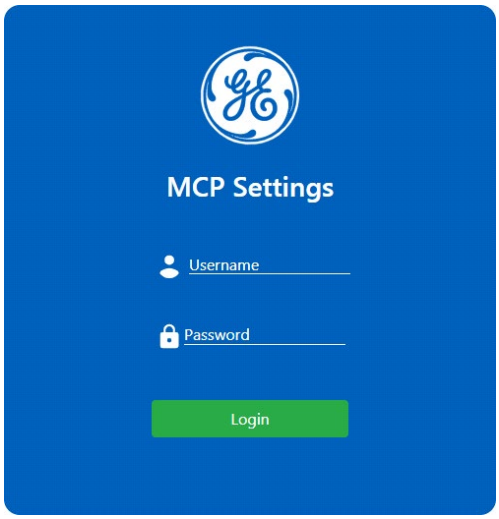
16. The menu displays the list of Added Emergency Admin Users.

```
================================================================
        Gateway Settings Menu
        Emergency Group Users - List of users in Emergency group
================================================================

   User Name                          UID    Full Name
=====================================================================

 1. emadmin                           1005   Emergency Administrator

           Press ENTER Key to continue....
```

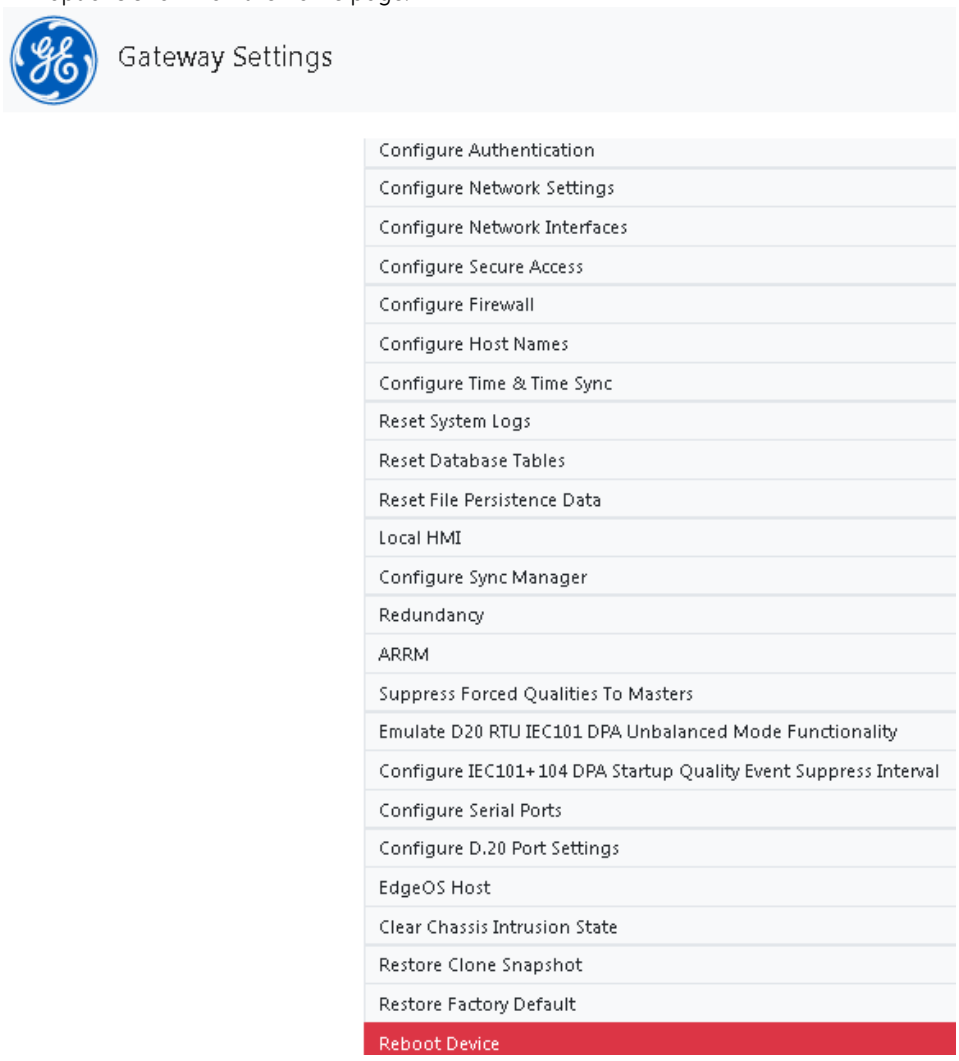
Using Web MCP Settings GUI

1. Login to MCP using local admin user authentication:
   - Entering their User Name.
   - Entering their Password.

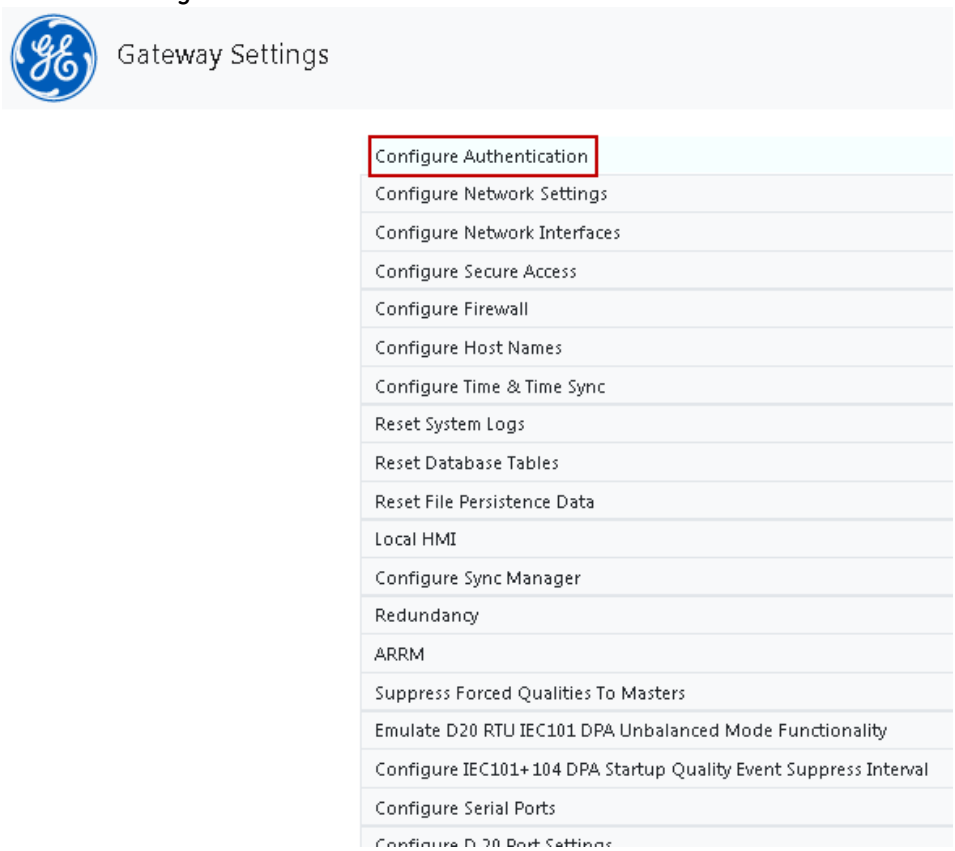
– Selecting Login to advance to the next screen and begin using the application.



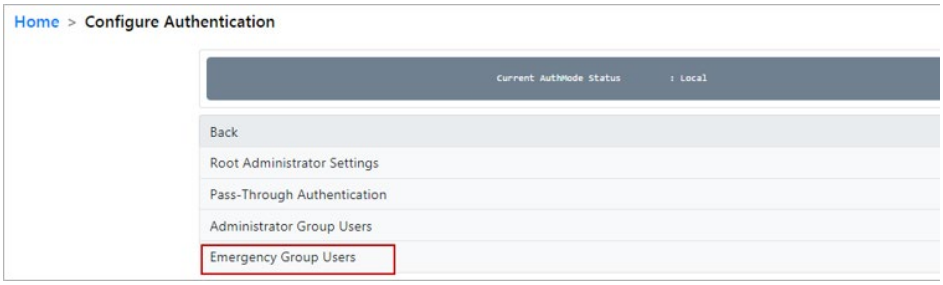
2. Once you have logged in to the MCP Settings, you can see a menu on the center and Logout option on the top right of the screen. To explore the MCP settings use the menu options shown on the home page:



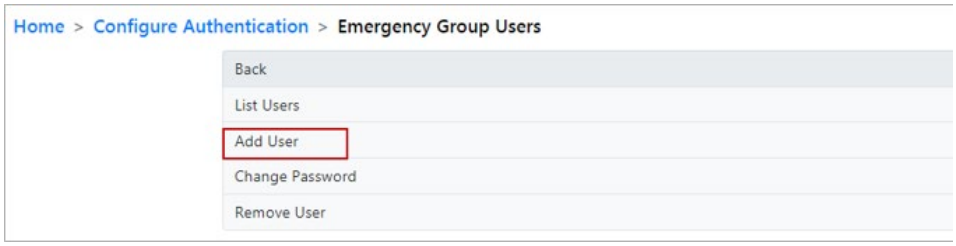
3. Select **Configure Authentication** from the main menu.



4. Click on **Emergency Group User** to add emergency User.

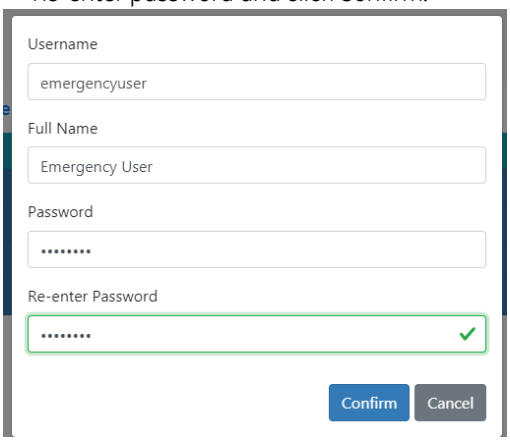


5. To add new emergency user click **Add User** tab.

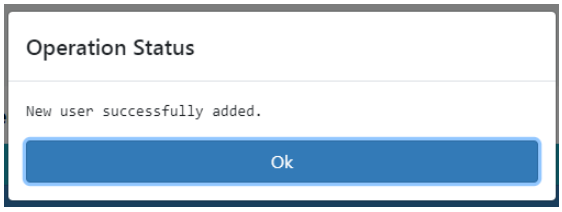


6. Enter the desired Emergency Group Username, conforming to the emergency group username rules as listed below:
   - Emergency Group Username must be between 2 and 31 characters.
   - Emergency Group Username must start with a lowercase alphabetical character.
   - Emergency Group Username must only contain [a-z][0-9][-,_] characters.

7. Enter the Full Name of the emergency group user.
8. Enter the Password, conforming to the password security rules as listed below:
   - Password must be between 8 and 199 characters in length
   - Password must contain:
     - 1 character from [a-z]
     - 1 character from [A-Z]
     - 1 digit from [0-9]
     - 1 special character from the set [$%@!&]
     - Re-enter password and click Confirm.



RESULT: Pop-up window appears showing the Operation Status: **New user successfully added**, click **OK**.



Retrieve LDAP Authentication Server information

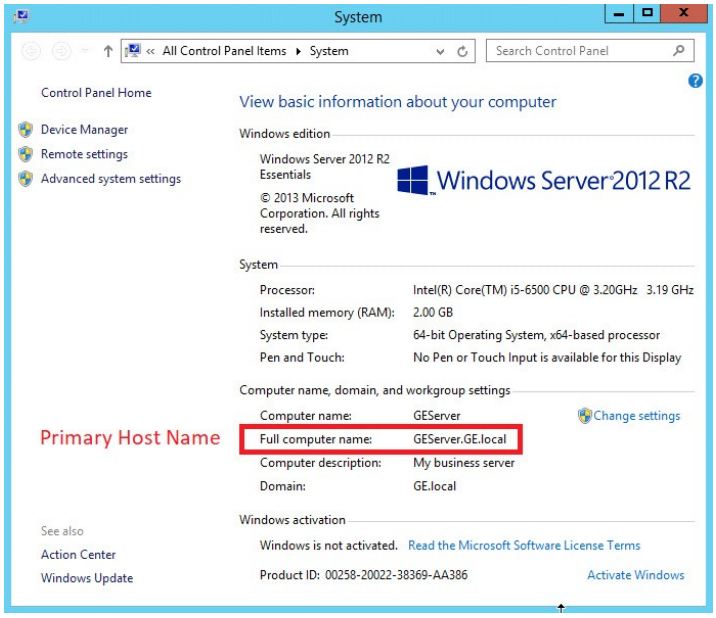
1. Retrieve the following LDAP authentication server information from the IT / Network team of your organization or company:

Name	Locate on LDAP Server
Primary Host Name	1. It is full name of your computer (LDAP Server). 2. Open properties of computer or server and view the **Full Name of Computer**
Primary Host IP Address	Open Server Manager in LDAP server and click on AD DS and note down the IP address of server.
Secondary Host Name	This is an optional field. It is full name of your secondary computer (LDAP Server). Open properties of computer or server and view the Full Name of Computer. If the Secondary LDAP Server is configured, MCP shall automatically switch to the secondary server when the primary server is not available.
Secondary Host IP Address	This is an optional field. Open Server Manager in secondary LDAP server and click on AD DS and note down the IP address of server.
LDAP Port	LDAP communication mechanism is TLS/SSL. Port-number = 389 for TLS communication Port-number = 636 for SSL communication

Name	Locate on LDAP Server
Base DN	1. It is Domain Name 2. Open properties of computer or server and view the Domain 3. If Domain is **GE.local** then Base DN will be "**dc=GE,DC=LOCAL**"
Bind User Name	Username of the bind user created in the LDAP server. Assume the user name to login LDAP machine or server is "**ldapbind**" and dc name is "**GE**" and dc type is "**local**" then the bind user name will be (in DN format) "**cn=ldapbind,cn=Users,dc=GE,dc=local**"
Bind Password	Password for the Bind User
Security Type	LDAP communication mechanism is TLS/SSL. Port-number = 389 for TLS communication Port-number = 636 for SSL communication
CA Certificate	Selected the imported CA certificate from the drop-down list.
Bind Time limit in Seconds	Use **30** as default value
User ID Attribute Map	User can use the default value "**sAMAccountName**"
Home Directory Attribute Map	User can use the default value "**unixHomeDirectory**"

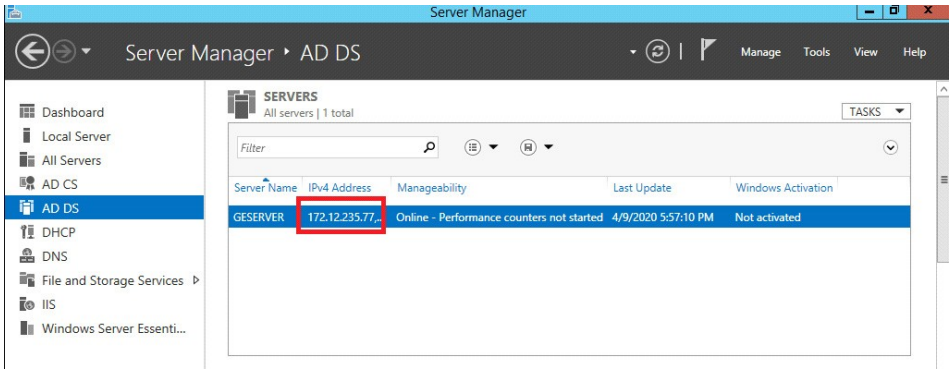
Procedure to find the above-mentioned parameter in LDAP machine or server:

1. **Primary Host Name/Secondary Host Name**
   - It is full name of computer (LDAP Server).
   - Open properties of computer or server and view the Full Computer Name as below screen shot:



2. **Primary Host IP Address/Secondary Host IP Address**

– Open Server Manager from in LDAP server and click on **AD DS** and note down the IP address of server (Start=>>Server Manager=>>AD DS).



3. LDAP Port

3.1. LDAP authentication mechanism (that is, SSL or TLS) and the configured port number.

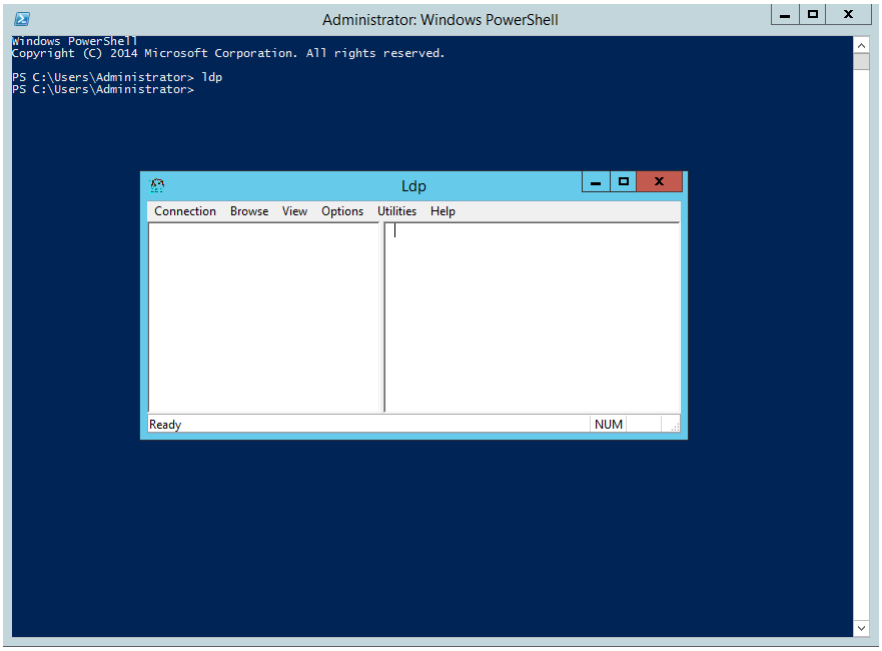
3.2. Example: For the Windows Active Directory the standard port numbers for TLS/ SSL communication:

– Portnumber = 389 for TLS communication

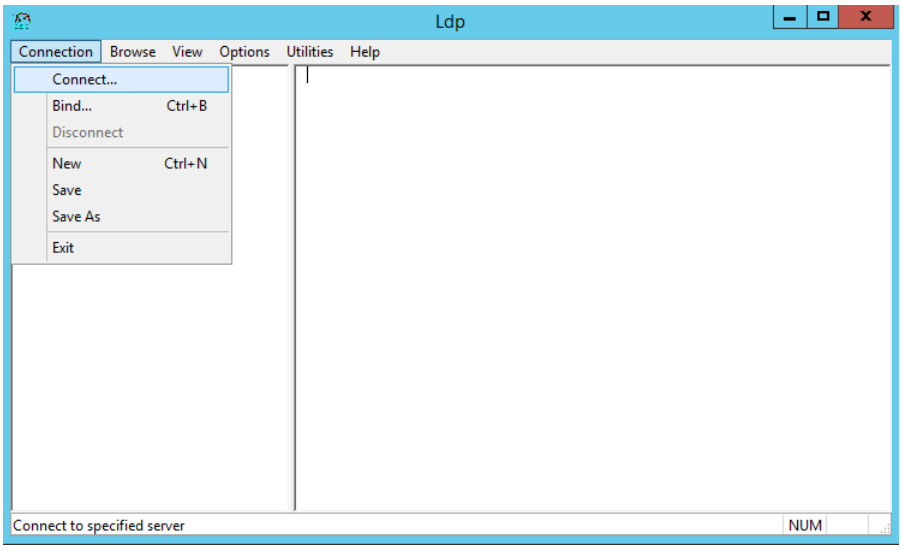
– Portnumber = 636 for SSL communication

3.3. LDAP port number can be checked by below steps in Windows Server:

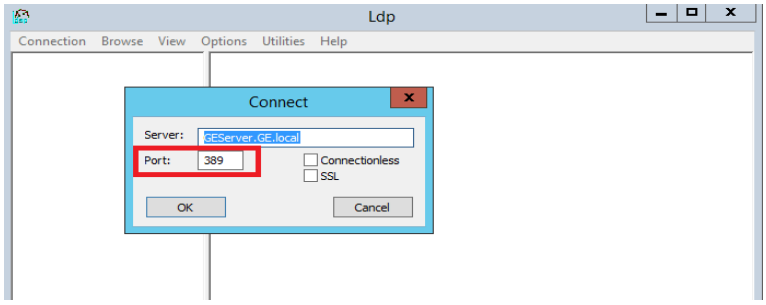
i. From Start menu-> run -> type **ldp** and press **Enter**.



ii. Select **Connection** menu > **Connect**.



iii. A new login index will be opened for login, the LDAP port will be automatically filled in the login prompt. Note down this port number: 389 as below:

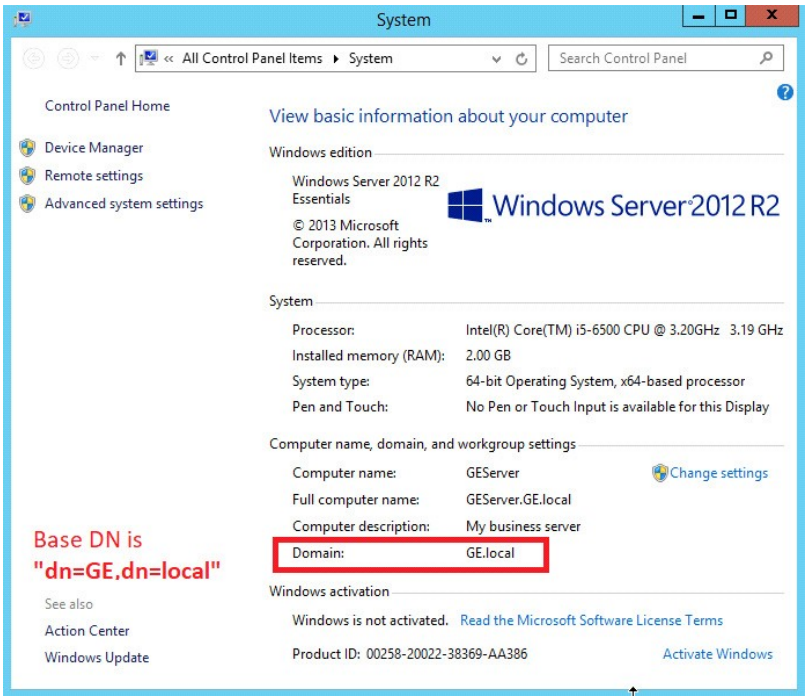


4. Base DN

4.1. It is a Domain Name.

4.2. Open **Properties** of computer or server and note the Domain name.

4.3. If Domain is **GE.local** then Base DN will be "**dc=GE,dc=LOCAL**"



5. Bind user name (in DN format)/Bind Password

5.1. If the user name of LDAP machine or server is "**ldapbind**" and dc name is "**GE**"and dc type is "**local**" as shown in above screen shot then the bind user namewill be (in DN format) "**cn=ldapbind,cn=Users,dc=GE,dc=local**"
Creation of Bind user is described in the section Procedure to test the AD DS domain controller installation.

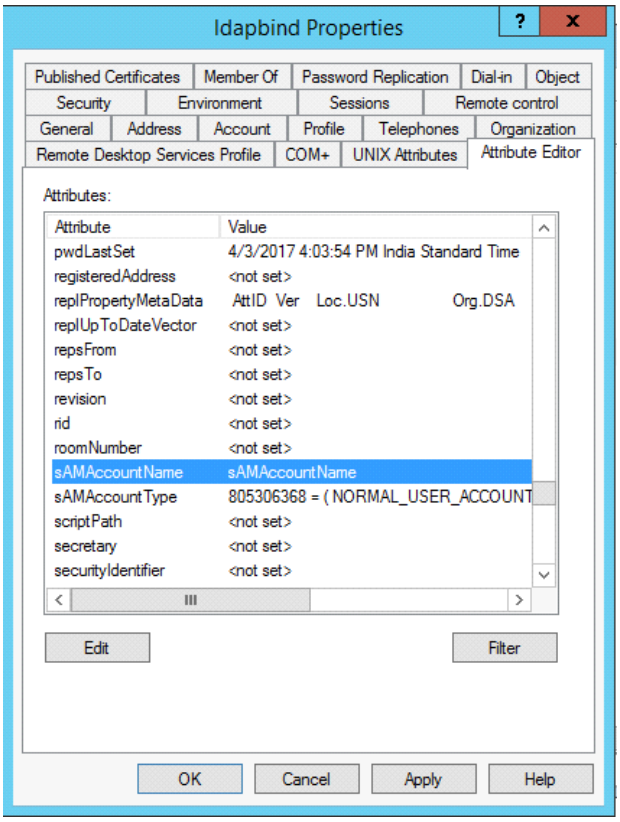
See Checking DN Format section for details on how to capture these details from the LDAP Server.

- The user name is comprised of only lower-case letters, numbers, "-" (dash), and "_" (underscore) characters.
- LDAP search is based on directory in DN format. For example: dc=GE,dc=local
  Checking DN Format for details.
- Bind password is the password created for the above bind user.
- For the LDAP Application to switch automatically to the Secondary LDAP server, when Primary LDAP server is not available, the exact same bind user should be created in both servers.

6. User ID Attribute Map

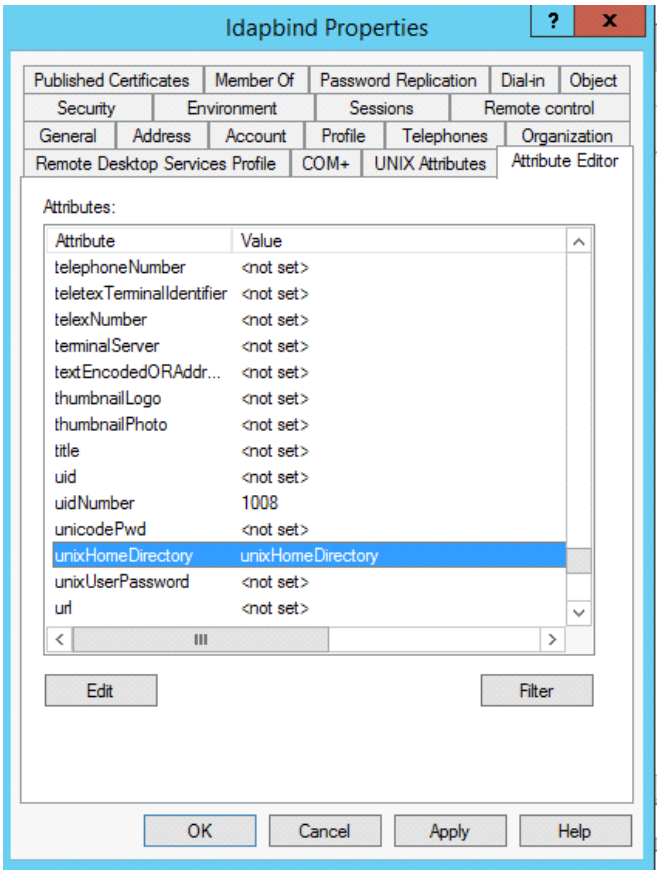
- Default/standard user ID attribute is sAMAccountName.

- To view the configured value open uid field for the Windows Active Directory. This can be viewed in the properties section of the user.



7. **Home Directory Attribute Map**
   - Default or standard value is unixHomeDirectory for the Windows Active Directory.

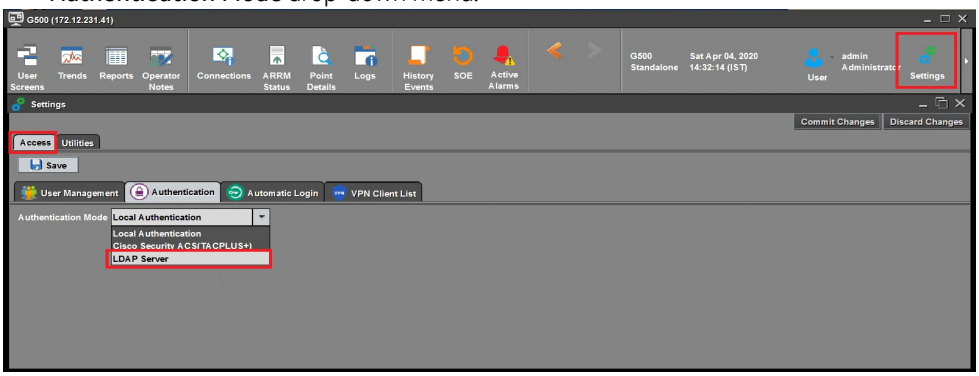
– This can be viewed in user attribute tab in the properties section of the user.



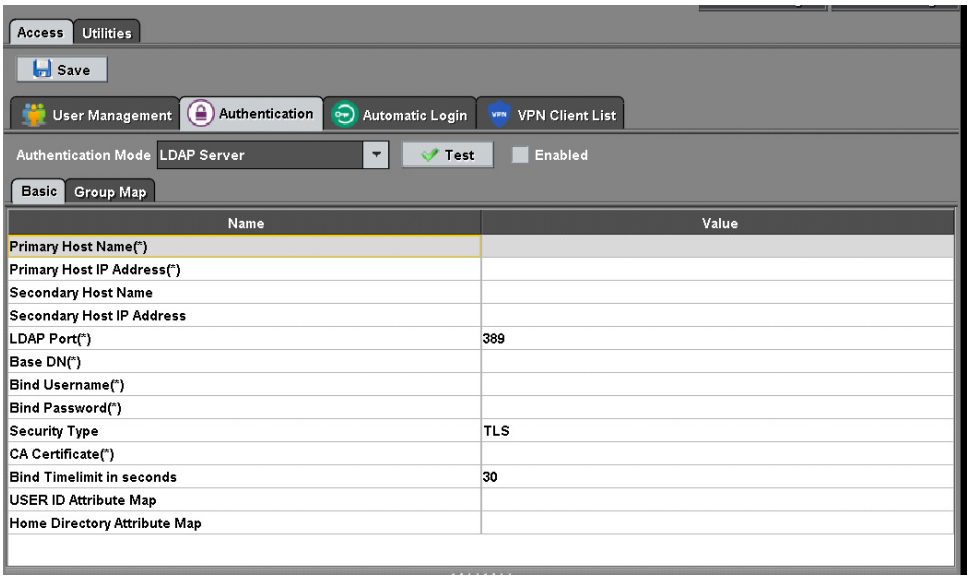
Procedure to configure LDAP on the MCP device

You can configure or change the authentication to LDAP Authentication mode by using HMI. In above section (Retrieve LDAP Authentication Server Information), we already had collected all the parameters that will be used here for configuration: To configure the LDAP in the MCP device:

1. Login in to MCP HMI with an administrator user name and password.
2. Go to **Settings > Access > Authentication** and select **LDAP server** from the **Authentication Mode** drop-down menu.



3. On selecting the LDAP Server authentication, LDAP configuration page will be opened as below:

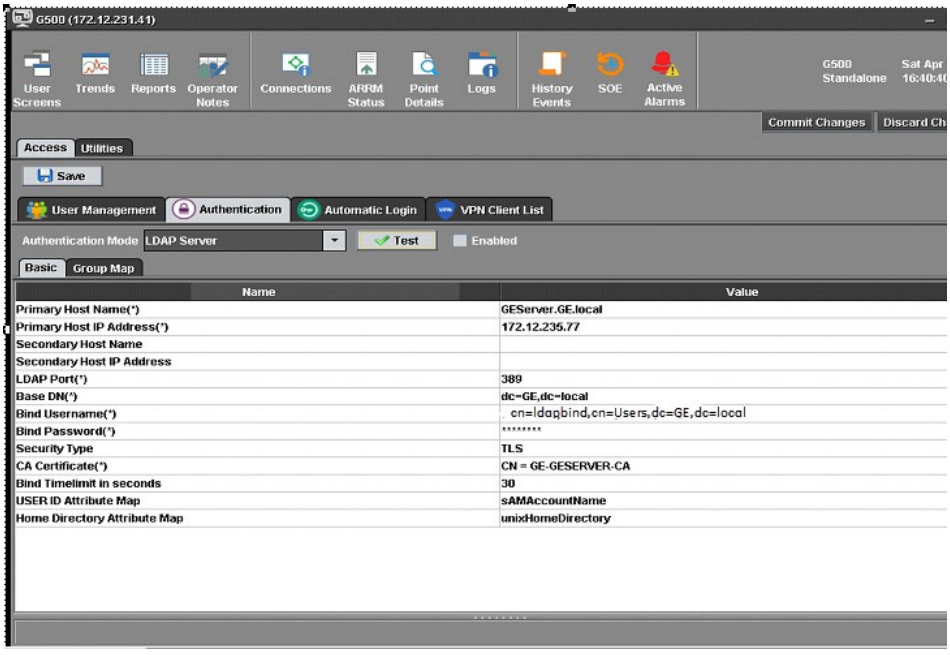


4. Input all the LDAP parameters we already had noted in the above section of this document. Follow the below table as an example to find all the parameter from LDAP server:

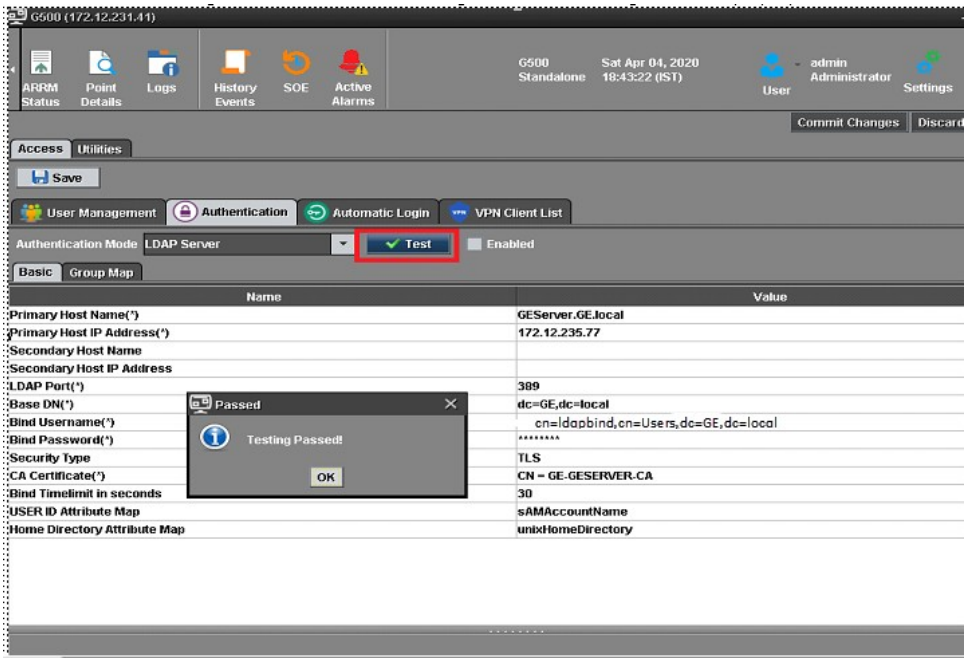
Name	Value	Locate on LDAP Server
Primary Host Name	GEServer.GE.local	1. It is full name of your computer (LDAP Server). 2. Open properties of computer or server and view the Full Name of Computer
Primary Host IP Address	172.12.235.77	Open Server Manager in LDAP server and click on AD DS and note down the IP address of server.
LDAP Port	389	LDAP communication mechanism is TLS/SSL. – Port-number = 389 for TLS communication – Port-number = 636 for SSL communication

Name	Value	Locate on LDAP Server
Base DN	dc=GE,dc=local	1. It is Domain Name 2. Open properties of computer or server and view the Domain 3. If Domain is GE.local then Base DN will be "dc=GE,DC=LOCAL"
Bind User Name	cn=ldapbind,cn=Users,dc=GE,dc=local	Assume the user name to login LDAP machine or server is "ldapbind" and dc name is "GE" and dc type is "local" then the bind user name will be (in DN format) "cn=ldapbind,cn=Users,dc=GE,dc=local"
Bind Password	Password	Enter the bind user password. (This is the password created for the Bind user in the LDAP Server in the earlier steps).
Security Type	TLS	LDAP communication mechanism is TLS/SSL. – Port-number = 389 for TLS communication – Port-number = 636 for SSL communication
CA Certificate	Certificate installed earlier	Select the INSTALLED CERTIFICATE appear on drop down list.
Bind Time limit in Seconds	30	Default Value
User ID Attribute Map	sAMAccountName	sAMAccountName is default value User can find it in user attribute tab in user properties of user in LDAP server
Home Directory Attribute Map	unixHomeDirectory	1. unixHomeDirectory is default value 2. User can find it in user attribute tab in user properties of user

3. Configure these LDAP parameters as shown below. Also, go to the drop-down menu of CA certificate and select the CA certificate for LDAP.

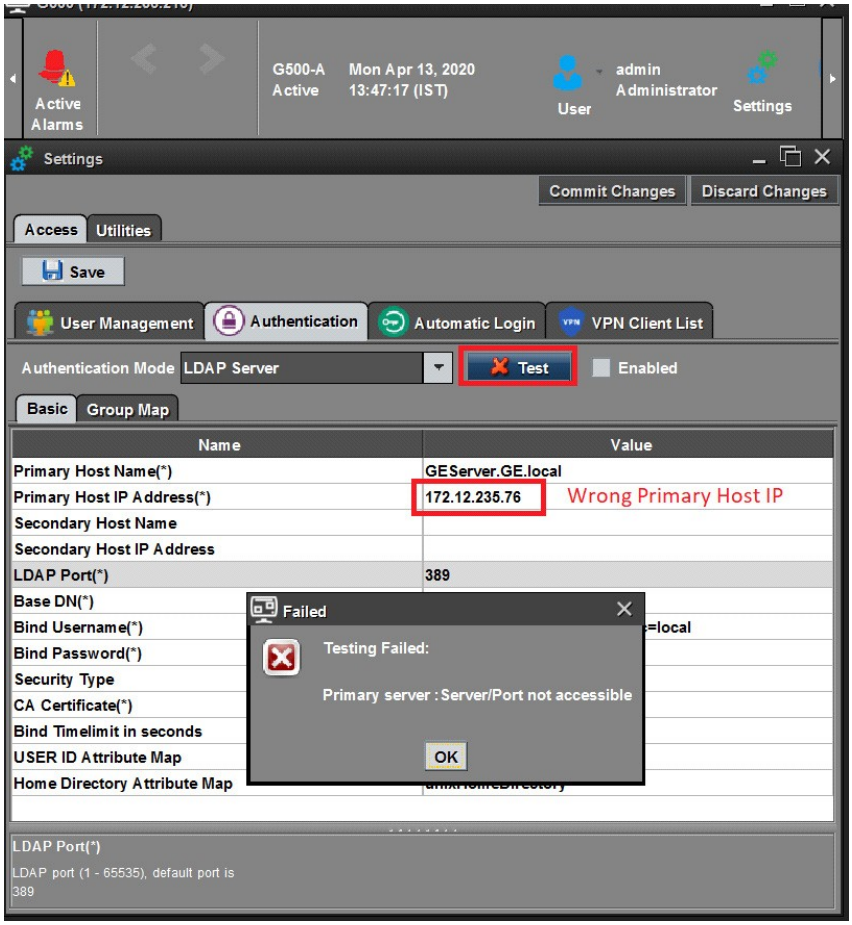


4. Click the **Test** button. It will validate the configuration and availability of LDAP server once the configuration verified, Testing Passed message will be popup. Click **OK**.



Result : The server connectivity is verified.

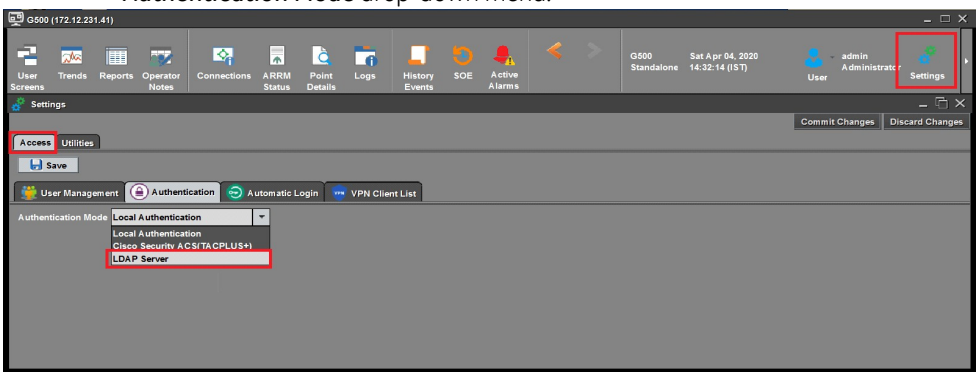
5. If user had input wrong parameter for any of the field and click on test button then it will popup message as "Testing Failed" as below:



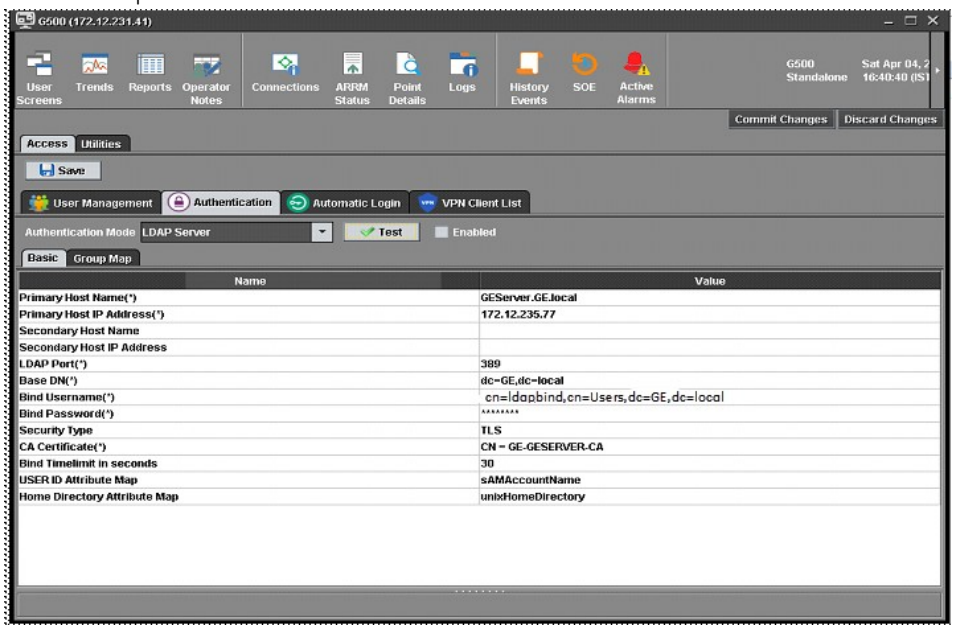
NOTE: Do not select the Enabled field.

6. Click on Save, it will save the configuration parameters, but still the authentication mode is local.
7. Till the above step LDAP configuration has been saved and tested successfully but still the authentication mode is Local. If user want to work with:
   7.1. If user want to work with Static mode of group mapping, then group mapping is not required in MCP. In this case user can directly enable and save the configuration as described in next steps. Static mode of group mapping is described in section Procedure for Static Group Mapping.
   7.2. If user want to work with Dynamic mode of group mapping, then group mapping needs to be done in MCP. Map the group in MCP by following the Procedure for Dynamic Group Mapping. After mapping all the groups in MCP proceed with next step.
8. Procedure to Configure Group Mapping on the MCP Device, if user want to work with dynamic user mapping approach then Group Mapping need to be done in MCP. Follow the below steps for Group Mapping in MCP. If you want to continue with static group mapping, skip the below steps from 8.1 to 8.8 and move to step 9:
   8.1. Procedure for Dynamic Group Mapping. It has been noted in an earlier example that the Distinguished Name (DN) of group "**G500Administrator**" is as "**cn=G500Administrator,cn=users,dc=GE,dc=local**".
   8.2. Login in to MCP HMI with an administrator user name and password.

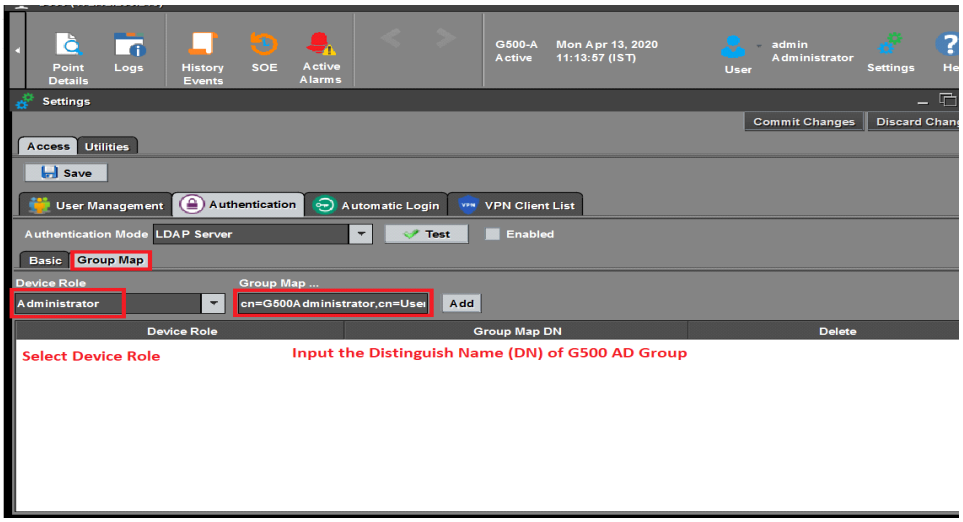
8.3. Go to **Settings > Access > Authentication** and select **LDAP server** from the **Authentication Mode** drop-down menu.



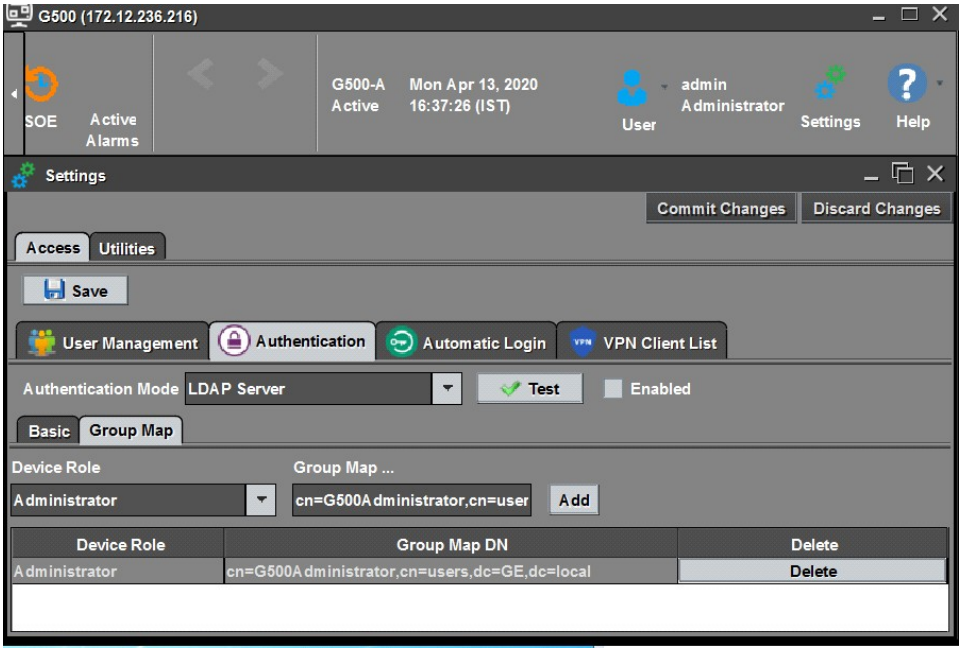
8.4. On selecting the LDAP Server authentication, LDAP configuration page will be opened as below:



8.5. Click on "**Group Map**" tab. Select the **Device Role** of Group from drop down and input the **DN** in Group Map field as shown in below (DN has been noted in step 8.3):



8.6. Click on "**Add**" button, it will add the group in MCP and that group members or users will be privileged with the selected Device Role. For example if User role is selected as Administrator for "**G500Administrator**" user group then users under G500Administrator group will have administrator privilege.

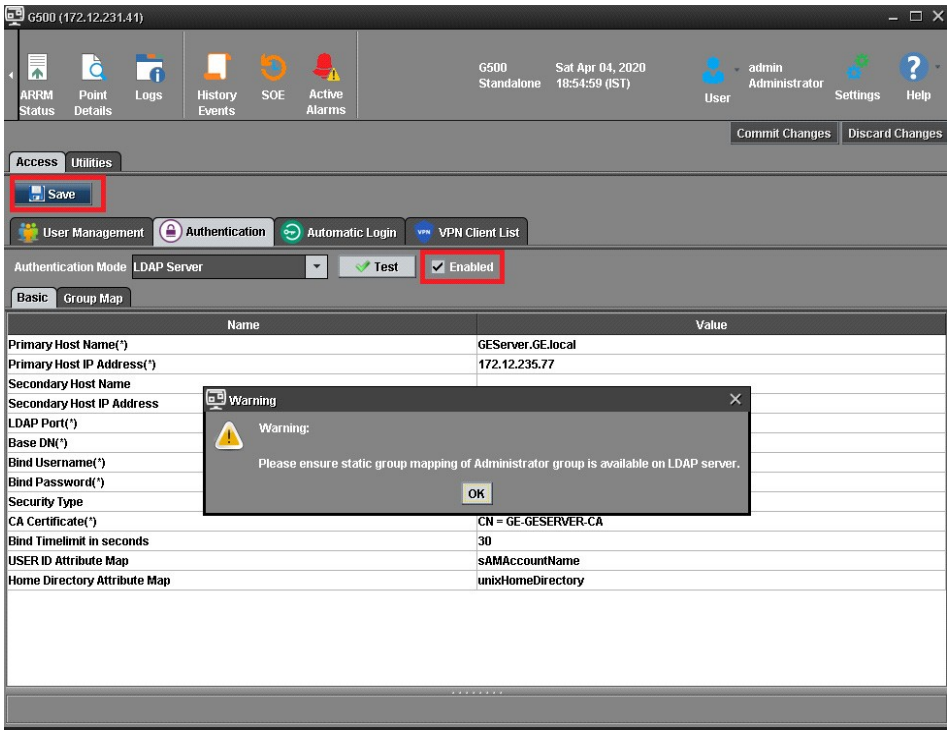


8.7. Similarly add different User groups like G500Operator for Operator privilege, G500Observer for Observer privilege, G500Supervisor for Supervisor privilege, G500Passthrough for Passthrough privilege.

8.8. After adding the user group click on Save to save the configuration.
RESULT: Group Mapping has been done successfully.

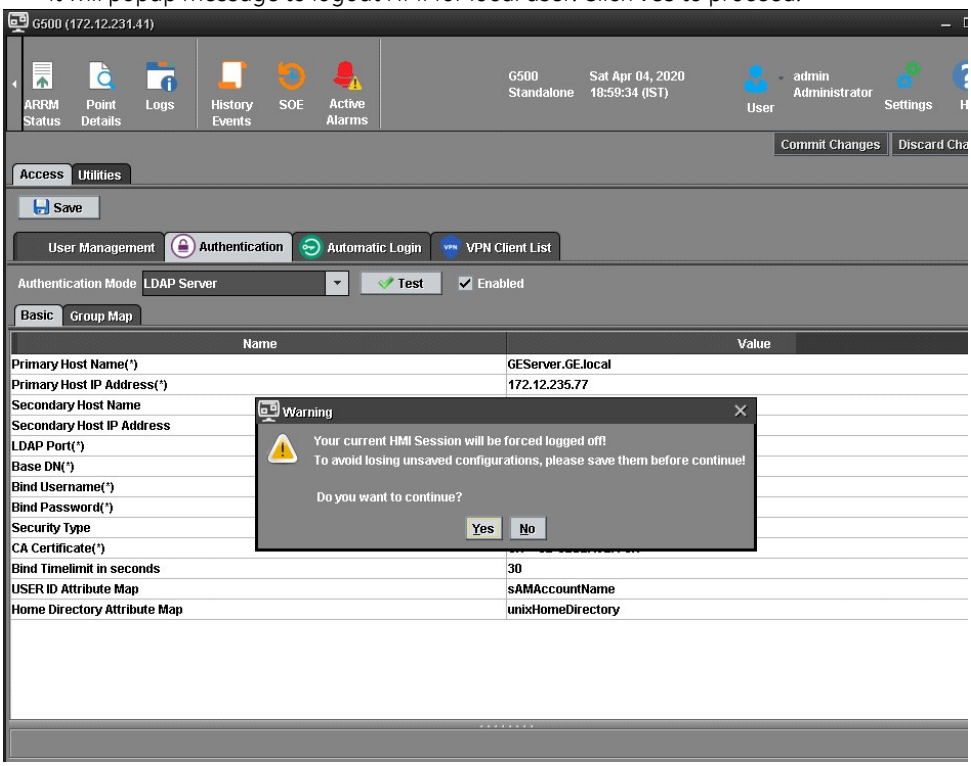
9. **Select the Enabled field and Save**, This step should be done only after completion of Static/ Dynamic Group Mapping it will save this configuration parameters and forcefully logout the HMI for local user and LDAP authentication will be enabled for MCP. Now user can login to MCP by using only LDAP authentication.
NOTE: Select the Enabled field and Save, this will switch to Remote Authentication

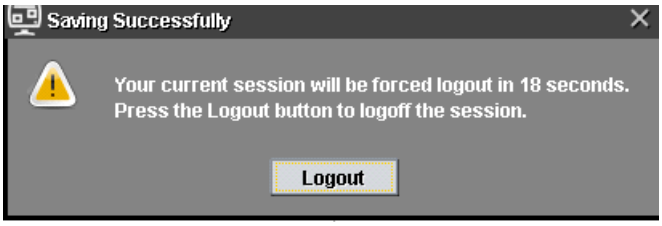
mode.



WARNING: Save with Enabled checked will switch to Remote Authentication immediately!

10. This warning is for the static user should be available to login MCP, click **OK** then again it will popup message to logout HMI for local user. Click **Yes** to proceed:





Result: Now LDAP Authentication mode is successfully enabled, user is required to use LDAP credentials, for login to HMI, DSAS and SSH sessions to MCP.

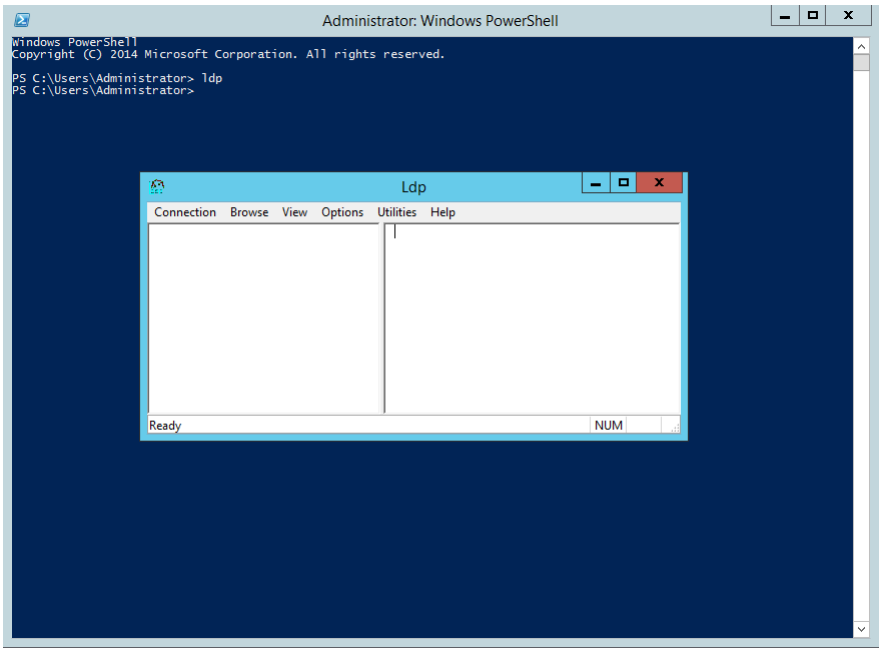
Configuring the MCP devices for Centralized LDAP Authentication

Appendix A: Checking DN Format

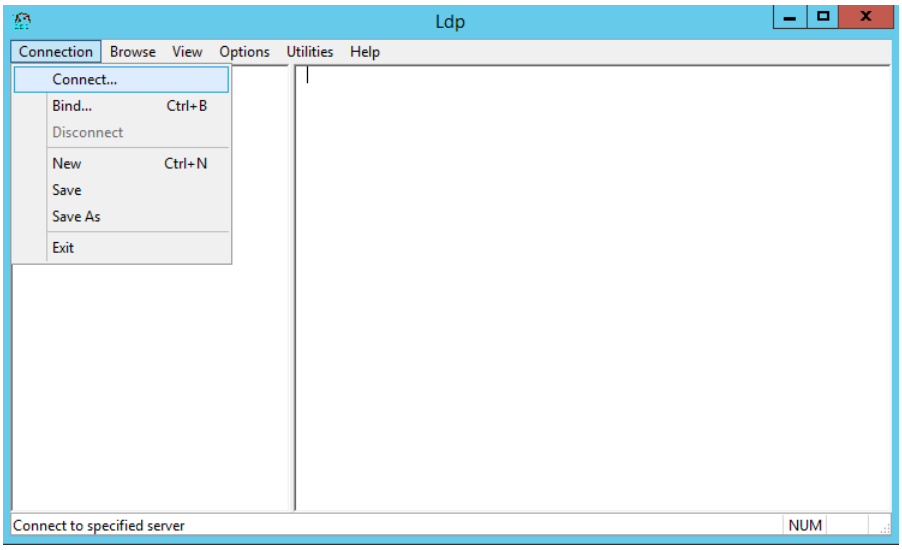
This appendix describes how to check DN format of Users and Domains in the Windows Active Directory.

To check DN format of Users and Domains in the Windows Active Directory:

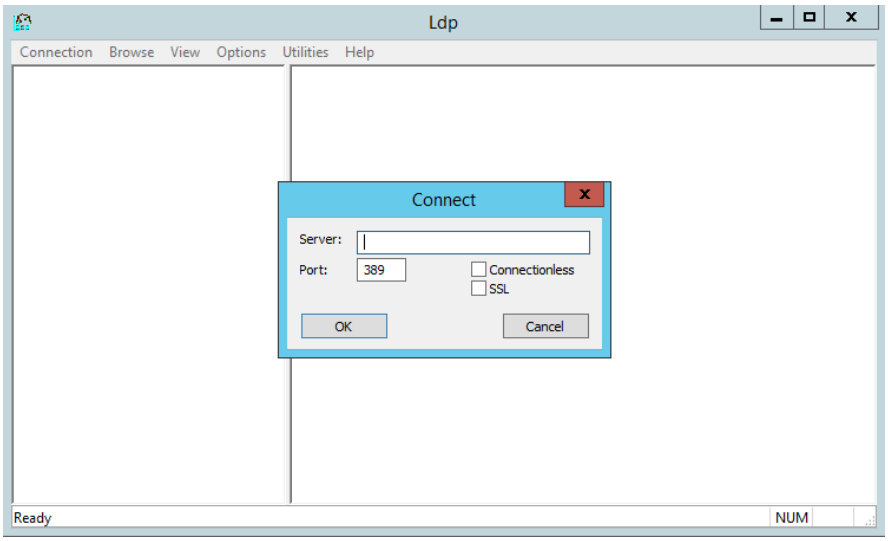
1. From **Start** menu, run, type **ldp** and press **Enter**.



2. Select **Connection** menu > **Connect.**

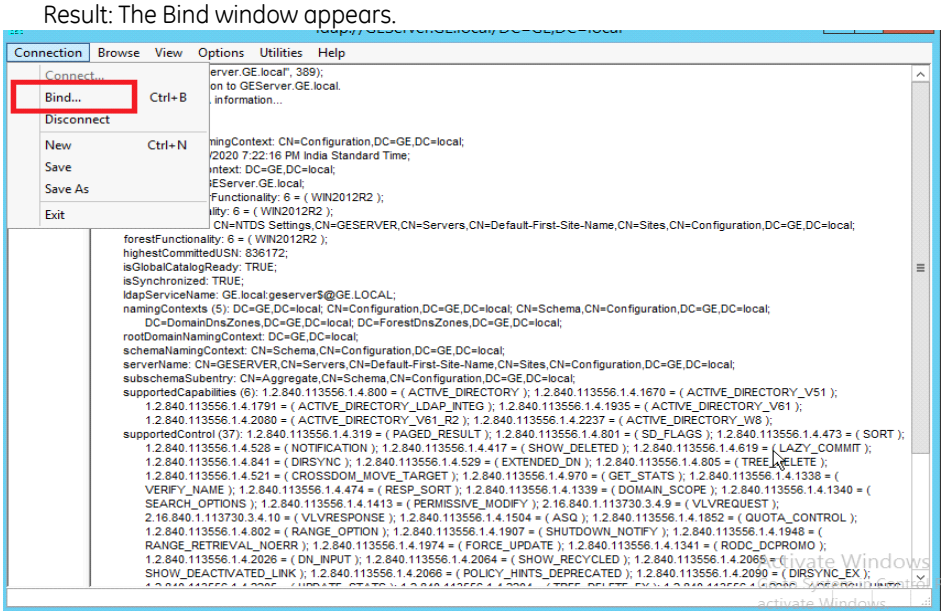


3. Click **OK** to continue.

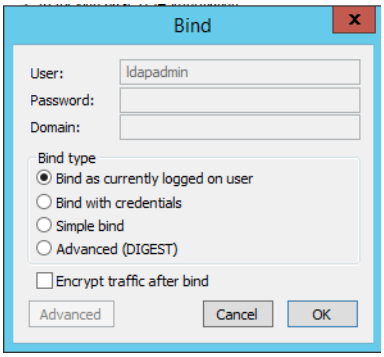


4. Select **Connection** menu >**Bind**.

   Result: The Bind window appears.

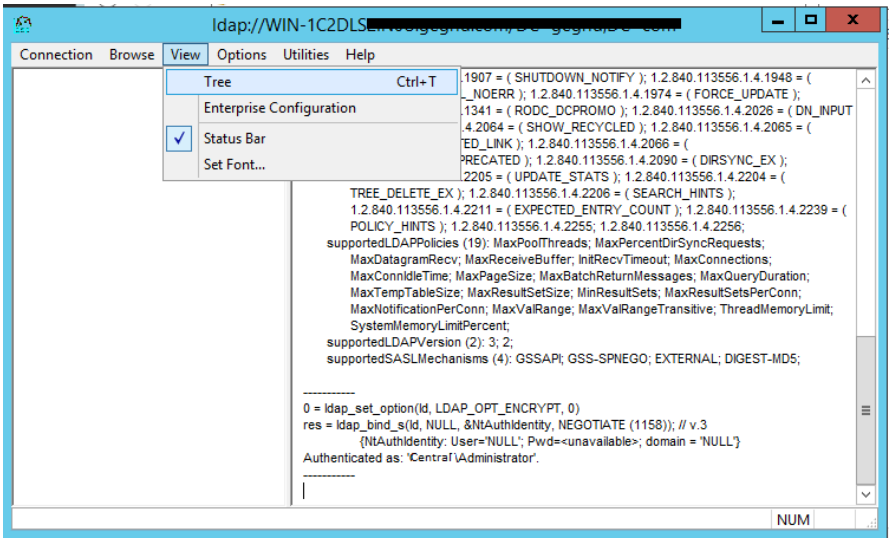


5. Select **Bind as Currently logged in user** and click **OK**.

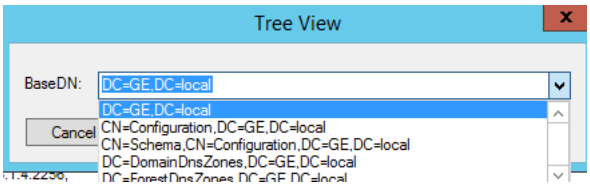


6. Select **View** menu >**Tree**.

   Result: The Tree View window appears.



7. Select the **BaseDN** and click **OK**.



8. Expand the Base DN (where DC = central, DC = home) which appears on the left half-window. The hierarchy is the same as that when created from AD DS in the server Manager.
9. Select the appropriate DN format for groups as well as users.

Configuring the MCP devices for Centralized LDAP Authentication

Appendix B: Third-party CA Certificate

This appendix describes how to create and install a third-party CA certificate on the MCP device.

Creating and installing a third-party CA certificate

This section describes how to create a third-party CA certificate from an XCA third party software for Windows Active Directory server.

Creating a third-party certificate involves:

- Creating a third-party X.509 certificate
- Creating the Server X.509 Certificate
- Installing the third-party CA X.509 Certificate and Server Certificate into the AD DS Windows Server
- Installing the third-party X.509 CA Certificates on to the MCP device

Creating a third-party X.509 certificate

Creation of third-party Certificates for Active Directory involves creation of two certificates: namely:

- CA certificate to be installed in both the Client and Server
- Server Certificate to be installed in the Server for Server Authentication

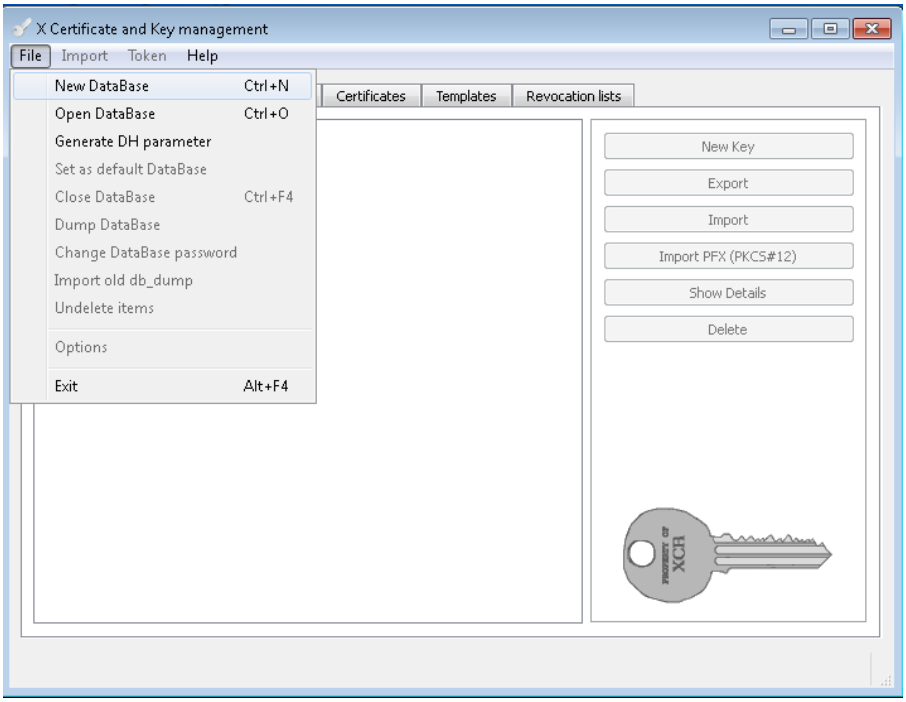
Before you start, ensure that you have downloaded and installed the latest Windows version of the XCA software (available at http://sourceforge.net/projects/xca/).

To create third party X.509 Certificates for the Active Directory:

1. Create a new XCA database.
   1.1. Click **File** > **New DataBase**.
   1.2. Assign the database a name, and place it in a folder you can access later.
   1.3. When prompted, give the database a new password.

You need to select this database manually whenever you open XCA.

NOTE

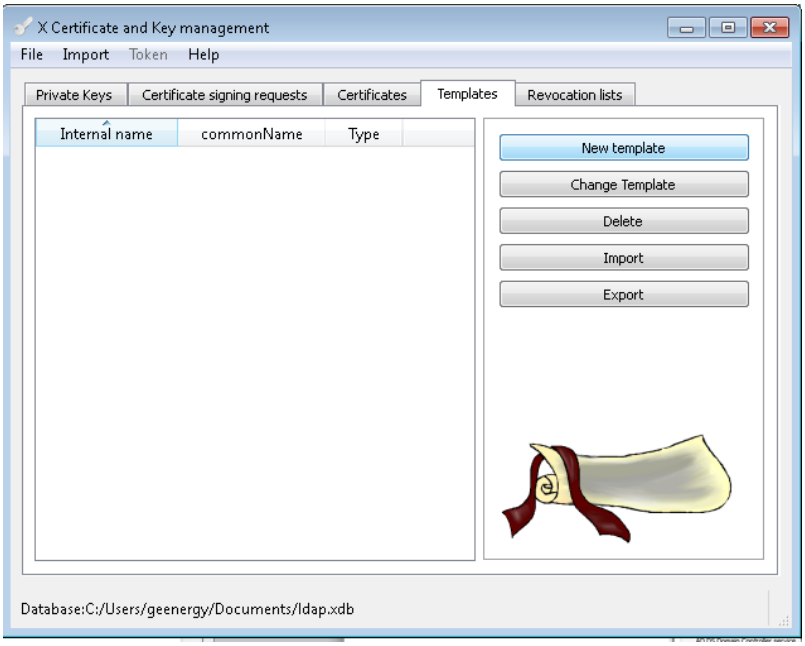


Using a strong password when encrypting your XCA database helps prevent an adversary from gaining access to your critical X.509 certificate private keys.

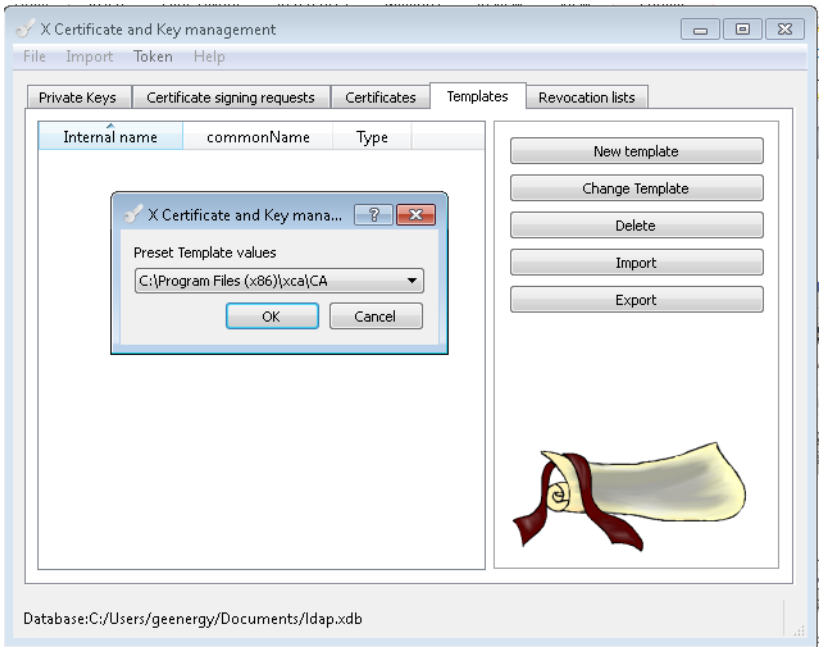
2. Create a root CA certificate.

   This root X.509 certificate will be used to sign the X.509 certificate used for AD DS on the Windows Server 2012 and will also be used on the MCP device.

3. From the **Templates** tab, click **New Template**.



4. Select **CA** as Preset Template Value and click **OK** to proceed with the creation of a new template.



5. On the **Subject** tab, enter your unique organizational information in the **Distinguished name** section.

   The most important component is the **commonName**. This is the name that your Clients is configured to accept. Any difference between the commonName of the certificate and the name configured in the Client results in a failed connection. Choose other name components that are appropriate for your company. Table 2 provides example distinguished name components.

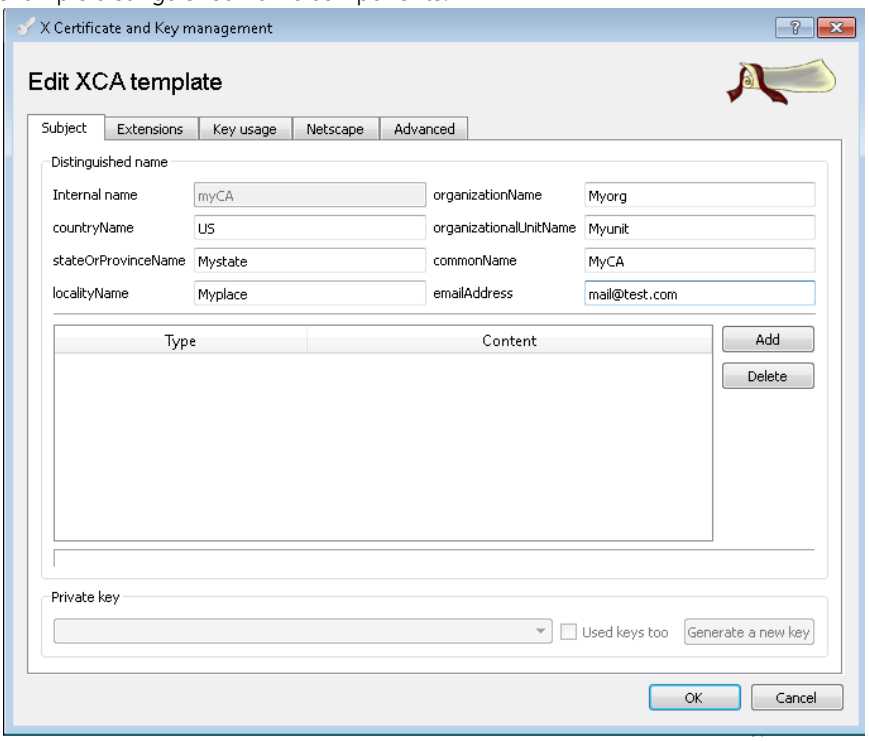
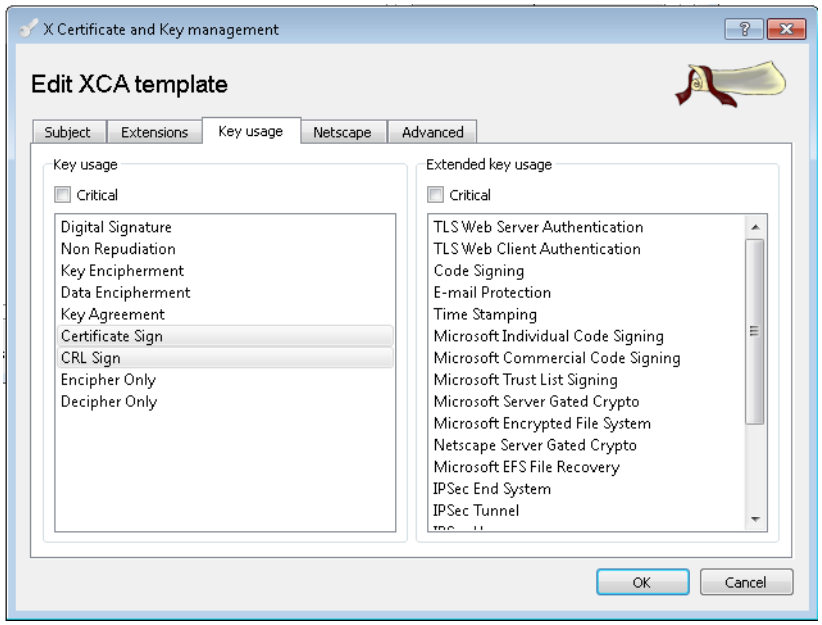


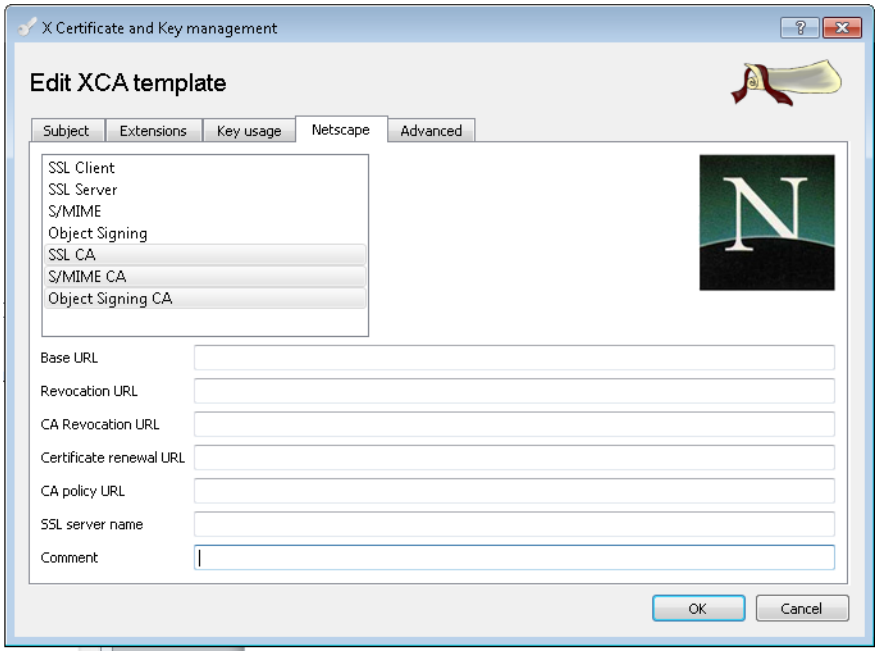
Table 2: Example Distinguished Name components

Distinguished Name Component	Example
Internal name	MyMCP
countryName	US
stateOrProvinceName	MyState
localityName	MyCity
organizationName	MyCompany
organizationalUnitName	MyDivision
commonName	MyMCP
emailAddress	mail@my.domain

6. Under the **Extensions** tab, if necessary change the **Time Range** that the CA certificate is valid for and click **Apply**. The default is 10 years. Certificates generated with this CA certificate after this period are no longer valid.
7. Under the **Key usage** tab, do not change the defaults.

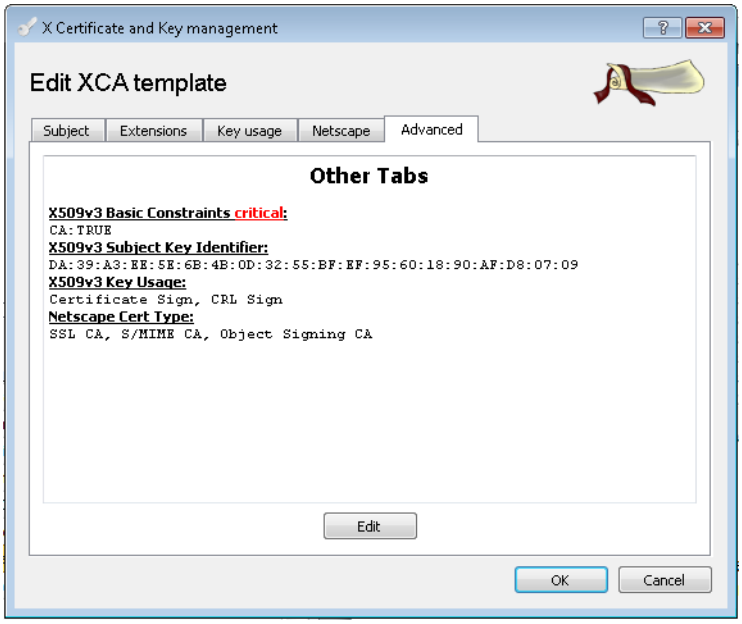


8. Under the **Netscape** tab, remove the value in the **Comment** field.



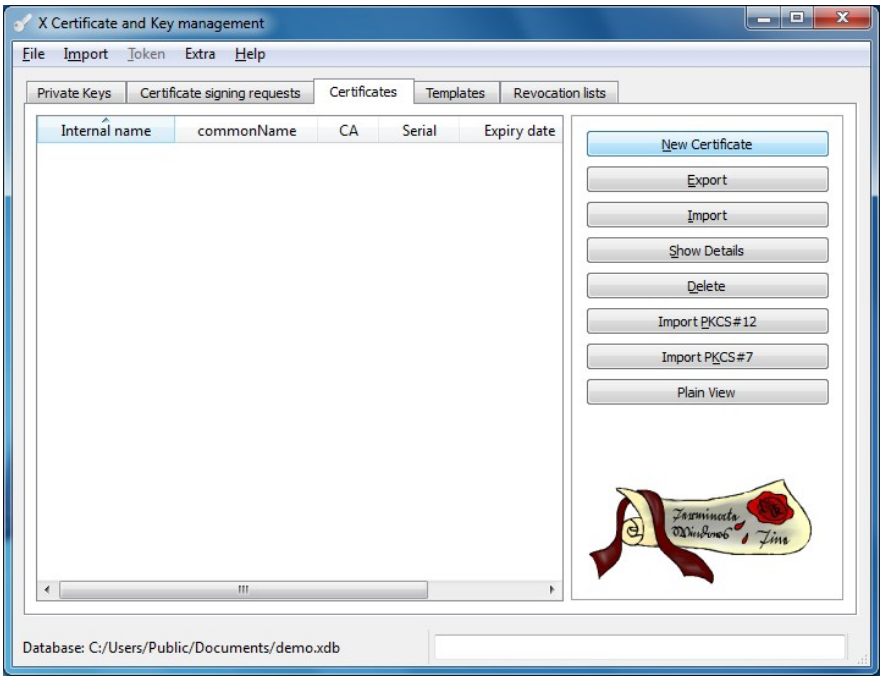
9. Under the **Advanced** tab, the following messages are expected, except the value of the X509v3 Subject Key Identifier, which differs from key to key:

   If following messages do not appear, click **Validate** to view the message.

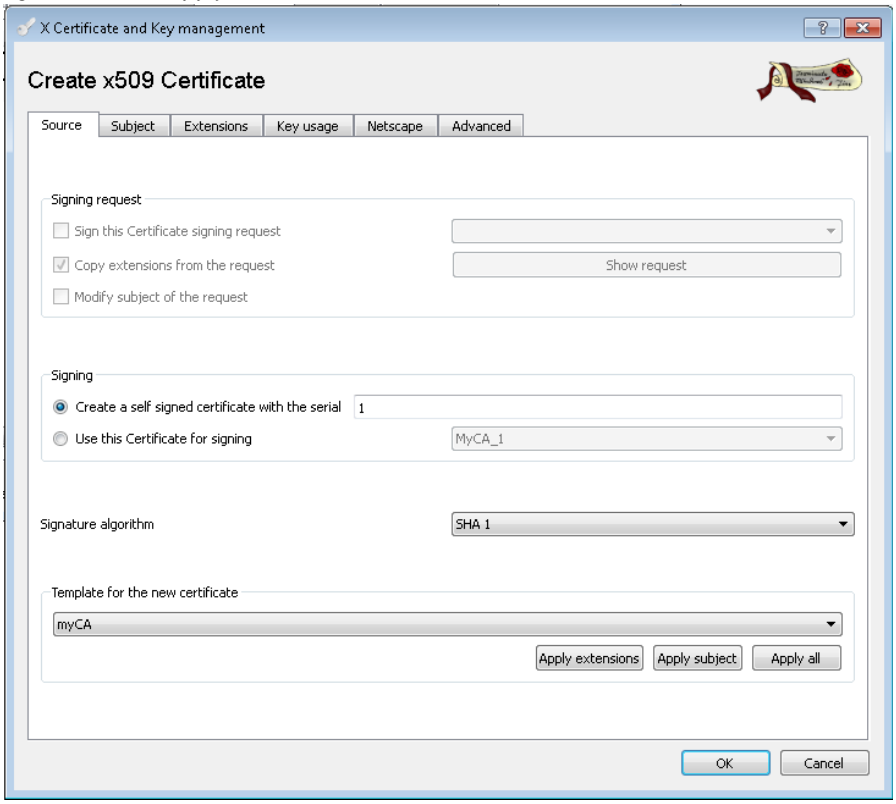


   Result: The CA certificate Template is added.

10. From the **Certificates** tab, click **New Certificate**.



11. Click the **Source** tab. Ensure the CA template created in the previous step is selected under **Template for New Certificate Option**, and choose **SHA 1** for the Signature algorithm. Click **Apply all**.



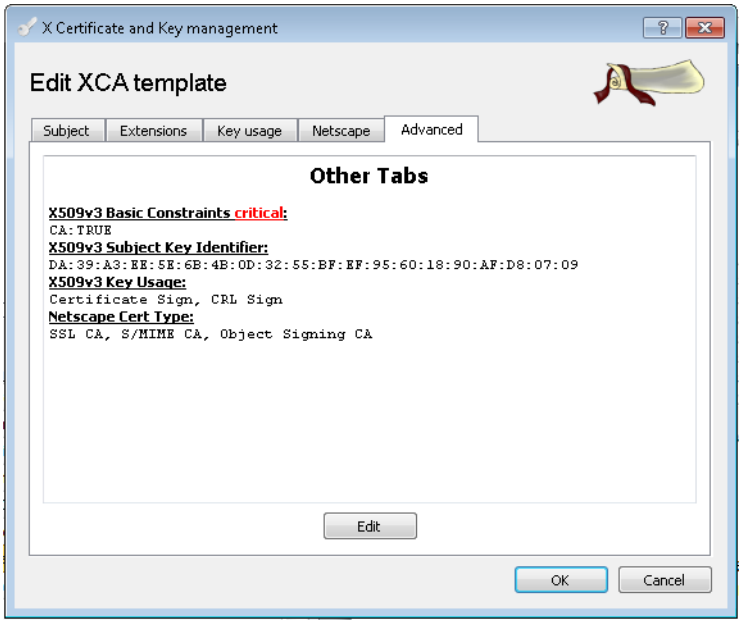
12. On the **Subject** tab, enter your unique organizational information in the **Distinguished name** section. See Table 3.

Table 3: Example Distinguished Name components

Distinguished Name Component	Example
Internal name	MyCA
countryName	US
stateOrProvinceName	MyState
localityName	MyCity
organizationName	MyCompany
organizationalUnitName	MyDivision
commonName	MyCA
emailAddress	mail@my.domain

13. Under the **Subject** tab, click the **Generate a new key** button.
14. In the dialog that appears, enter the name of the CA (e.g., **MyCA**) in the **Name** field. Choose the **Keytype** as **RSA** or **DSA** to match the type of cipher suites you wish to use. Change the **Keysize** to **2048**.
15. Under the **Key usage** tab, do not change the defaults.
16. Under the **Netscape** tab, remove the value in the **Comment** field.
17. Under the **Advanced** tab, the following messages are expected except the value of the X509v3 Subject Key Identifier, which differs from key to key.

    If the following messages do not appear, click **Validate** to view the messages.



18. Click **OK**.

    Result: The CA certificate is created.
19. Under the **Certificates** tab of the main view of XCA, select the new **Certification Authority** and click **Export**.
20. Ensure the Export Format is set to **PEM**.
21. Browse to a protected directory (e.g., **My Documents** > **MyXCAFiles**) and click **Save**.
22. Click **OK**.

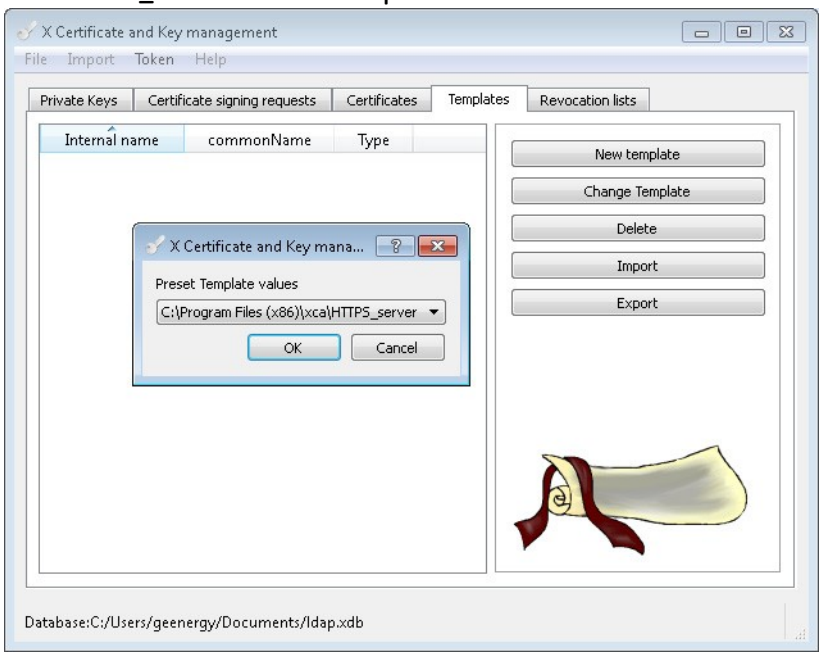
    Result: The file is named based upon the internal name of your CA with a .crt file extension.

Creating the Server X.509 Certificate

A Server certificate allows the Server to authenticate itself to a MCP device Client. The Server certificate contains a commonName field. This field should uniquely identify the server in your network; that is, the Full Qualified Domain Name (Hostname) of the server should be the common name in the server certificate.

To generate Server X.509 Certificate:

1. Launch **XCA** from the Windows Programs menu.
2. In the tree view of the **Templates** tab, select the **New Template** option.
3. Select **HTTPS_server** as **Preset Template values** and click **OK**.



4. On the **Subject** tab, enter your unique organizational information in the **Distinguished name** section.

   The most important component is the **commonName**. This should be the Full Qualified Domain Name of the server without which, it may result in a failed connection. Choose other name components that are appropriate for your company.

5. Under the **Extensions** tab, if necessary change the **Time Range** that the Server certificate is valid for and click **Apply**. The default is 1 year.
6. Under the **Key usage** tab, do not change the defaults.
7. Under the **Netscape** tab, remove the value in the **Comment** field.
8. Under the **Advanced** tab, click **Validate** to view the messages and verify that the **CA:false** message is observed

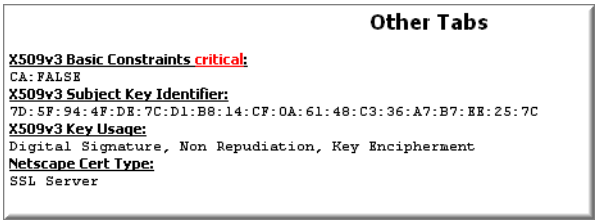
   Result: The Server certificate Template is added.

9. In the tree view of the **Certificates** tab, select the branch containing your Certification Authority and click the **New Certificate** button.

10. Under the **Source** tab:
    10.1. Select the **Use this Certificate for signing** option. From the drop-down menu to the right of this check-box, select the CA you created in section: "Creating a third-party X.509 certificate" on page 75 (e.g., MyCA).
    10.2. Do not change the drop-down selection **Signature Algorithm set** from **SHA 1**.
    10.3. Change the drop-down **Template** for the new certificate to the Server Certificate Template Created in previous steps.
    10.4. Click **Apply all**.
11. Under the **Subject** tab, click the **Generate a new key** button.
    11.1. In the dialog that appears, enter a name that uniquely identifies the MCP device in your network.
    11.2. Choose the **Keytype**, as **RSA** or **DSA** to match the type of cipher that suites your needs. Change the **Keysize** to **2048**. Click **OK**.
    11.3. In the **Subject** tab, verify that the common name is the Full Qualified Domain Name (FQDN) of the server.
12. Under the **Extensions** tab, if necessary change the **Time Range** that the Server certificate is valid for and click **Apply**. The default is one year.

    The shorter the Time Range the more secure the certificate. The shorter the Time Range, the more often you need to regenerate Server certificates and deploy them into your servers.
13. Under the **Key usage** tab, do not change the default values.
14. Under the **Netscape** tab, remove the comment.
15. Under the **Advanced** tab, click **Validate**.

    Result: The following messages are expected except the value of the X509v3 Subject Key Identifier, which differs from key to key.



16. Click **OK**.

    Result: You now have a Server certificate.
17. In the tree view under the **Certificates** tab, open the branch labeled after your Certificate Authority, and select the new Server certificate.
18. Click **Export**.
19. In the dialog that appears, ensure the Export Format field is set to **PKCS12 with Certificate Chain**. Browse to a protected location (e.g., **My Documents** > **MyXCAFiles**) and click **Save**.
20. Click **OK**.

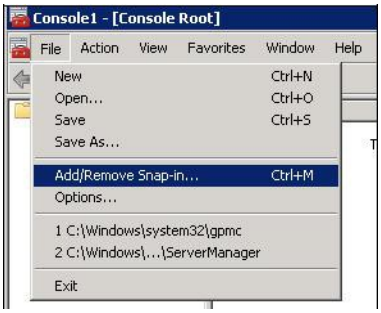
    Result: The certificate is in a file named with your Server Internal Name with the file extension **.p12** (e.g., servercert.p12).

    The certificate file is always security-sensitive so keep it protected at all times.
21. Remove the file after it has been installed on the server.

Installing the third-party CA X.509 Certificate and Server Certificate into the AD DS Windows Server

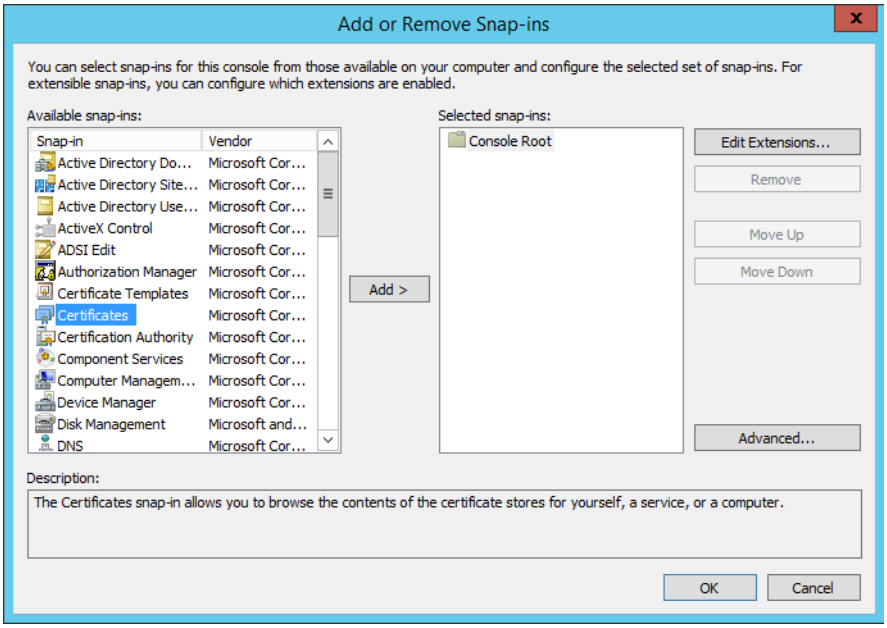
To install the newly created CA X.509 into the AD DS:

1. Copy the certificate on to Windows server 2012.
   1.1. Open the Microsoft Management Console by selecting the **Start** menu > **Run** > **mmc**, and clicking **OK**.
   1.2. Select **File** > **Add/Remove Snap-in**.



Result: The Add or Remove Snap-ins window appears.

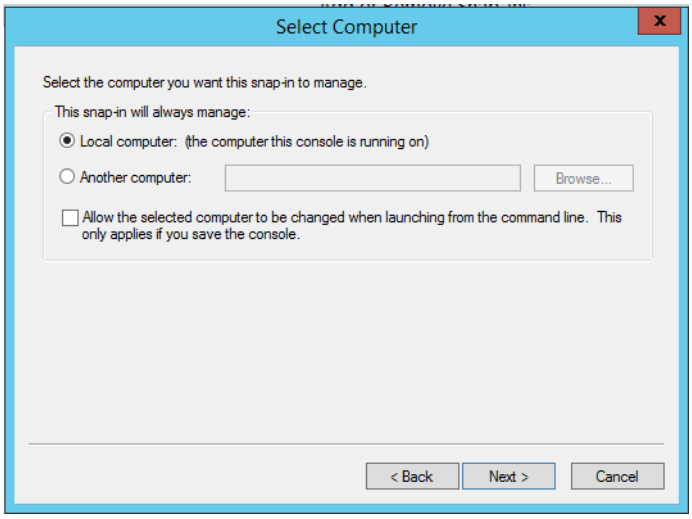
2. Select **Certificates** from the Available snap-ins window and click **Add**.



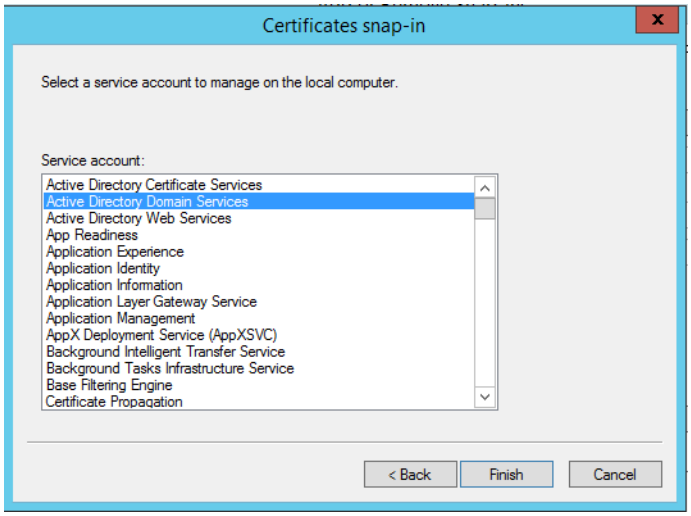
Result: The Certificates snap-in window appears.

3. Select **Service account** and click **Next**.

4. Select the **Local computer** option and click **Next**.

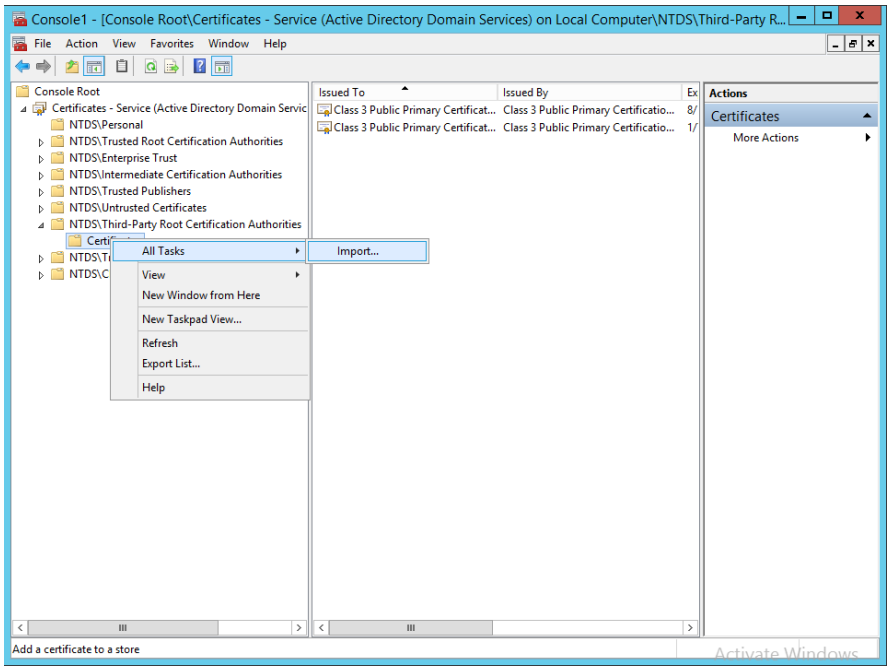


5. In the Service account menu, select the **Active Directory Domain Services** account and then click **Finish**.

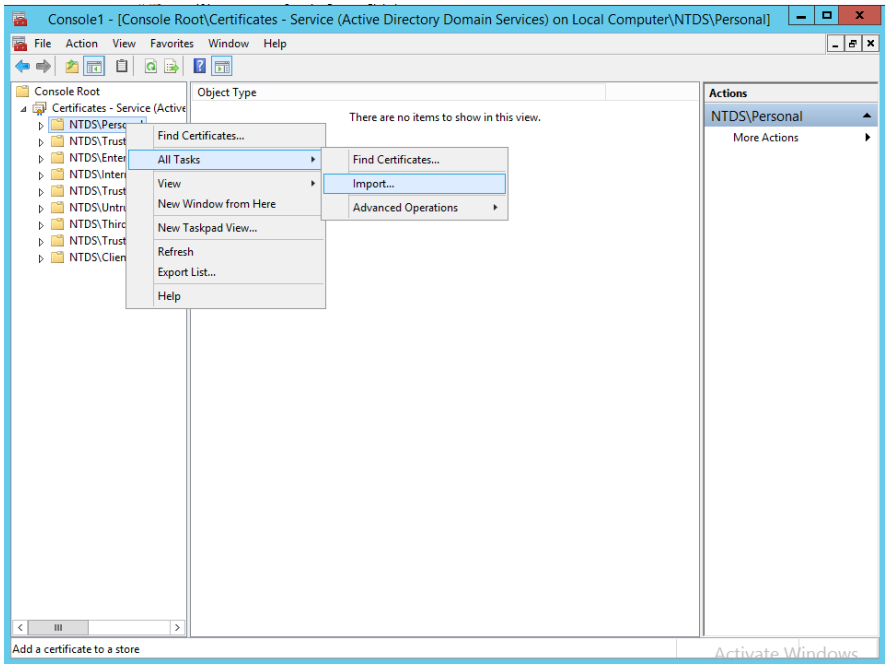


6. Click **OK** to finalize the snap-in selection.

7. Browse to **Third Party Root Certification Authorities** > **Certificates**. Right-click **All Tasks** and select **Import**.



8. Click **Next** on the first page of the Wizard.
9. Click **Browse** and select the Root CA certificated generated in the previous steps.
10. Click **Next** and follow the certificate Import Instructions
11. Click **Finish**.
12. Repeat this step, clicking on **Trusted Root Certification Authorities**.
13. From the Console window, expand the **Certificates - Service...** option, and right-click **NTDS\Personal**. select **All Tasks** > **Import**.



14. In the Certificate Import Wizard, select the certificate you exported from XCA.

15. On the next screen, click **Next** to place the certificate in the NTDS\Personal certificate store.
16. Click **Next** and then **Finish**.

    Result: A message appears notifying you that the import was successful.

    Result: The certificate is now in the NTDS\Personal certificate store.

    Result: The server certificate is automatically added after importing the CA certificate. If not, the manually follow the above procedure in step 13 to import the server certificate.
17. Click on **File** and follow steps 1 and step 2 in this procedure.

    From the Certificates snap-in window, select **Computer account** and click **Next**.
18. Follow steps 4 to 16
19. Reboot the Windows server.

Installing the third-party X.509 CA Certificates on to the MCP device

To install the third-party X.509 CA Certificates on the MCP device:

1. Save the root CA Certificate generated in section: Creating a third-party X.509 certificate, in a location on your PC.
2. Import the Root CA Certificate to the MCP device.

   Follow the steps in section: Installing CA Certificates on the MCP device.

Configuring the MCP devices for Centralized LDAP Authentication

Appendix C: Troubleshooting

If you encounter issues while testing the operation of the LDAP server configuration, refer to the following listed errors and the recommended responses. When you click the Test Button, if a particular field is configured improperly, the corresponding message appears on the HMI.
The exact error messages may refer to MCP, G500 or G100 – the meaning is identical.

See sections:

- LDAP error messages
- LDAP Certificate error messages

LDAP error messages

Error Message	Response
Host not reachable	Ensure LDAP server was accessible in the network.
	Ensure LDAP server was not shutdown.
unable to access ldap port	Ensure LDAP server was using the specified port for LDAP protocol communication.
Invalid binddn	Ensure mentioned bind user dn (distinguished name) was available in the mentioned domain on the LDAP server.
Invalid bind user credentials	Ensure bind user dn (distinguished name) mentioned in the MCP device LDAP server configuration was correct.
	Ensure bind user password entered was correct in the MCP device LDAP server configuration.
Hostname mismatch with server certificate	Ensure LDAP server host name entered in the MCP device LDAP server configuration was matching with the LDAP server certificate subject name.
Server/Port not accessible	Ensure LDAP server was accessible in the network.
	Ensure LDAP server was not shutdown.
	Ensure LDAP server was using the specified port for LDAP protocol communication.
Invalid Host Name. Full Qualified Domain Name (FQDN) has invalid characters	Ensure Primary Host Name is configured in MCP device LDAP server configuration.

Error Message	Response
Invalid Host IP Address	Ensure Primary Host IP Address configured in MCP device LDAP server configuration is correct.
Failed to connect to Primary Host	Ensure LDAP Server is accessible in the network.
	Ensure Primary Host Name configured in MCP device LDAP server configuration is correct.
	Ensure Base DN configured in MCP device LDAP server configuration is correct.
	Ensure Bind User credentials (Bind Username and Bind Password) configured in MCP device LDAP server configuration are correct.
Primary Server :Server/ Port not accessible	Ensure LDAP Server is not shutdown.
	Ensure Primary Host IP Address configured in MCP device LDAP server configuration is correct.
Configuration Timeout, please try again later	Ensure LDAP server was using the specified port for LDAP protocol communication.
Invalid User ID Attribute Map	Ensure User ID Attribute Map defined in LDAP Server is configured in MCP device LDAP server configuration.
Invalid HomeDirectory Attribute Map	Ensure HomeDirectory Attribute Map defined in LDAP server is configured in MCP device LDAP server configuration.
Connected to secondary Host, but failed to connect to primary Host	Ensure Primary Host Name and Primary Host IP Address configured in MCP device LDAP server configuration are correct.
Failed to connect to both primary and secondary Hosts	Ensure Primary Host Name and Secondary Host Name configured in MCP device LDAP server configuration are correct.
	Ensure Primary Host IP Address and Secondary Host IP Address configured in MCP device LDAP server configuration are correct.
	Ensure Base DN configured in MCP device LDAP server configuration is correct.
	Ensure Bind User credentials (Bind Username and Bind Password) configured in MCP device LDAP server configuration are correct.
Please add Emergency User before switching to LDAP/TACACS Authentication	Ensure at least one emergency admin group user is configured before switching to LDAP/TACACS Authentication.
The current Authentication Mode has been enabled. You cannot disable it unless switching to a different Authentication Mode	Current Authentication Mode is LDAP. Ensure to disable (Enabled checkbox unchecked) only when switching to a Authentication Mode other than LDAP.

LDAP Certificate error messages

Error Message	Response
List of trusted certificates is not complete	The issuer certificate of a looked up certificate could not be found. This normally means the list of trusted certificates installed on the MCP device or certificate list from LDAP server was not complete.
Unable to decrypt certificate's signature	The certificate signature could not be decrypted. This means that the actual signature value could not be determined rather than it not matching the expected value, this is only meaningful for RSA keys.
unable to decode issuer public key	The public key in the certificate SubjectPublicKeyInfo of MCP device server could not be read.
certificate signature failure	The signature of the installed certificate on MCP device server certificate was invalid.

Error Message	Response
certificate is not yet valid	MCP device time might be backward w.r.to certificate valid time.
	The certificate is not yet valid: the not Before date is after the current time.
certificate has expired	CA certificate installed on MCP device got expired w.r.to LDAP server.
	MCP device time might be forward w.r.to certificate valid time.
	The certificate has expired: that is the notAfter date is before the current time.
format error in certificate's notBefore field	The certificate notBefore field contains an invalid time.
format error in certificate's notAfter field	The certificate notAfter field contains an invalid time.
Self-signed certificate cannot be found in the list of trusted certificates.	The passed certificate is self-signed and the same certificate cannot be found in the list of trusted certificates.
self-signed certificate in certificate chain	Ensure Installed a trusted CA signed primary SSL certificate and an intermediate certificate.
	Verify that the Root CA is not included in the certificate chain (as this is almost always self-signed).
unable to get local issuer certificate	This error code is thrown when a local certificate path is not found during the certificate check.
	LDAP server certificate's issuer certificate was not found, after looking in both the chain provided by the LDAP server and in the local trusted storage. This usually means the peer chain was missing or incomplete.
unable to verify the first certificate	The primary certificate (the one you purchase from a vendor) cannot establish the chain of trust between itself and the Root certificate stored locally. Usually installing the intermediate certificates fixes this.
certificate chain too long	The certificate chain length is greater than the supplied maximum depth.
	The LDAP server certificate's chain length exceeded the limit set locally by sslverifydepth or SSL Verify Depth. The chain length (depth) is the number of certificates beyond the leaf (client or server) certificate itself.
	a chain of length 1 is a leaf certificate plus its issuer certificate.
invalid CA certificate	A CA certificate is invalid. Either it is not a CA or its extensions are not consistent with the supplied purpose.
path length constraint exceeded	The basicConstraints path length parameter has been exceeded for certificate.
invalid or inconsistent certificate extension	invalid or inconsistent certificate extension
Hostname mismatch	Ensure LDAP server host name entered in the MCP device LDAP server configuration was matching with the LDAP server certificate subject name.
Certificate directory empty	No certificates installed over to the MCP device.

Configuring the MCP devices for Centralized LDAP Authentication

Appendix D: List of Acronyms

Acronym Definitions

This Appendix lists and defines the acronyms used in this manual.

Table 4: Acronym list

Acronym	Definition
AD	Windows* Active Directory
AD CS	Active Directory Certificate Services
AD DS	Active Directory Domain Services
CA	Certificate Authority
MCP	MCP Substation Gateway
mcpcfg	Local configuration utility
DN	Domain Name
DNS	Domain Name System
FQDN	Full Qualified Domain Name
GE	General Electric
HMI	Human Machine Interface (also called Graphical User Interface – GUI)
IP	Internet Protocol
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
NIS	Network Information Service
NTDS	TechNet Directory Services
PC	Personal Computer
PEM	Privacy Enhanced Mail
PKCS	Public-Key Cryptography Standards, published by RSA Laboratories
SCADA	Supervisory Control and Data Acquisition
SCP	Session Control Protocol
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm

Acronym	Definition
SSL	Secure Sockets Layer
TLS	Transport Layer Security
USB	Universal Serial Bus
XCA	X Certificate and Key management

Appendix E: Revision History

This appendix provides the document revision history.

Revision history

Version	Revision	Date	Change Description
1.00	0	April 23, 2020	Initial release.
2.00	0	April 26, 2021	Updated for MCP family.

GE

Grid Solutions

Configuring the Multilin™ MCP for Centralized LDAP Authentication using Open LDAP Server

Installation and Configuration Guide

SWM0112

Version 2.00 Revision 0

Copyright Notice

© 2021, General Electric Company. All rights reserved.

The information contained in this online publication is the exclusive property of General Electric Company, except as otherwise indicated. You may view, copy and print documents and graphics incorporated in this online publication (the "Documents") subject to the following: (1) the Documents may be used solely for personal, informational, non-commercial purposes; (2) the Documents may not be modified or altered in any way; and (3) General Electric Company withholds permission for making the Documents or any portion thereof accessible via the internet. Except as expressly provided herein, you may not use, copy, print, display, reproduce, publish, license, post, transmit or distribute the Documents in whole or in part without the prior written permission of General Electric Company.

The information contained in this online publication is proprietary and subject to change without notice. The software described in this online publication is supplied under license and may be used or copied only in accordance with the terms of such license.

Trademark Notices

GE and are trademarks and service marks of General Electric Company.

* Trademarks of General Electric Company.

Tera Term is a registered trademark of T. Teranishi, Incorporated. IEC is a registered trademark of Commission Electrotechnique Internationale. IEEE is a registered trademark of the Institute of Electrical and Electronics Engineers, Inc. Internet Explorer, Microsoft, and Windows are registered trademarks of Microsoft Corporation.

Other company or product names mentioned in this document may be trademarks or registered trademarks of their respective companies.

This printed manual is recyclable.
Please return for recycling where facilities exist.

Configuring the MCP device for Centralized LDAP Authentication

Table of contents

PRODUCT SUPPORT
- Access the GE Grid Solutions web site. 5
- Search GE Grid Solutions technical support library 5
- Product support 6

ABOUT THIS DOCUMENT
- Purpose 7
- Intended audience 7
- Additional documentation 7

OPEN LDAP SERVER
- Creating OpenLDAP Server 10
- Changing default port numbers on OpenLDAP server 12
- Configuring OpenLDAP server 13
  - Creating role groups 13
  - Creating users 16
  - Group Mapping 18
- Generating certificates 19
  - Generating certificates from the server 19
  - Generating certificates using XCA 19
- Installing certificates on OpenLDAP server 34

CONFIGURE THE LDAP ON MCP DEVICES
- Installing CA Certificates on the MCP device 37
  - CA Certificate transfer procedure from PC to MCP 38
  - CA Certificate Installation procedure 41
- Configuring LDAP on the MCP device 46
  - Prerequisites to configuring LDAP on MCP device 47
  - Procedure to configure LDAP on the MCP device 57

TROUBLESHOOTING
- LDAP error messages 65
- LDAP Certificate error messages 66

LIST OF ACRONYMS Acronym Definitions 69

REVISION HISTORY Revision history 71

Configuring the MCP devices for Centralized LDAP Authentication using Open LDAP Server

Product Support

If you need help with any aspect of your MCP product, you can:

- Access the Multilin™ MCP devices Web site
- Search the GE Technical Support library
- Contact Product Support

Access the GE Grid Solutions web site

The MCP Web site provides fast access to technical information, such as manuals and knowledge base topics.
Visit us on the Web at: http://www.gegridsolutions.com

Search GE Grid Solutions technical support library

This site serves as a document repository for post-sales requests. To get access to the Technical Support Web site, go to: http://sc.ge.com/*SASTechSupport

Product support

For help with any aspect of your GE Grid Solutions product, please contact our support team, 24/7, as follows:

Region	E-mail	Telephone
Global Contact Centre	ga.support@ge.com	+44 1785 250070
Central and East Asia and Pacific	ga.supportCEAP@ge.com	+61 414 730 964
India	ga.supportIND@ge.com	+91 44 22648000
Middle East, North Africa and Turkey	ga.supportMENAT@ge.com	+971 42929467
Europe, Russia, CIS and Sub-Saharan Africa	ga.supportERCIS@ge.com	+34 94 4858854
North America	ga.supportNAM@ge.com	+1 877 605 6777
Latin America	ga.supportLAM@ge.com	+55 11 36187308

Configuring the MCP devices for Centralized LDAP Authentication using Open LDAP Server

About this Document

Purpose

This manual describes how to install and configure the Open LDAP Server and Multilin™ MCP device for Centralized LDAP Authentication.

This document applies to the MCP family (G100/G500) unless otherwise indicated.

Screen captures may show G500 in some areas, however the workflow applies to products in the MCP family (G100/G500).

Intended audience

This manual is a helpful resource for utility personnel and system engineers who are implementing LDAP on Multilin™ MCP device in an overall substation automation system.

Additional documentation

For the most current version of the Configuring Open LDAP Server and Multilin™ MCP for Centralized LDAP Authentication - Manual, please download a copy from GE Grid Solutions web site.

For information on fully installing, configuring, monitoring and testing a MCP device, refer to the:

- G500 Substation Gateway Instruction Manual, 994-0152
- G100 Substation Gateway Instruction Manual, 994-0155
- MCP Substation Gateway Software Configuration Guide, SWM0101

Configuring the MCP devices for Centralized LDAP Authentication using Open LDAP Server

Chapter 1: Open LDAP Server

This chapter describes how to install and configure OpenLDAP server on the Ubuntu operating system.

See sections:

- Creating OpenLDAP Server
- Changing default port numbers on OpenLDAP server
- Configuring OpenLDAP server
- Generating certificates
- Installing certificates on OpenLDAP server

The software versions used are:

- Ubuntu: 14.04
- Open LDAP is v3

Creating OpenLDAP Server

This section will guide you to install and configure OpenLDAP server on Ubuntu system.

1. Enter the **sudo su** command into the terminal emulator to switch to the root user.
2. Run the following command to install OpenLDAP. During the installation:

   apt-get install slapd ldap-utils

   Result: You are prompted to set a password for the LDAP admin account.
3. Reconfigure the slapd with the updated values using the following command:

   dpkg-reconfigure slapd

   For example, see the following example selections for the re-configuration options:
   - Omit OpenLDAP server configuration: **No**
   - DNS domain name: **gegrid.com**
   - Organization name: **gegrid**
   - Administrator Password: **Admin@123**
   - Database backend: **MDB**
   - Remove the database when slapd is purged: **No**
   - Move Old database: **Yes**
   - Allow LDAPv2 protocol: **No**
4. Test the LDAP server using the **ldapsearch -x** command.

   Result: The output towards the end should show `result: 0 Success`.
5. Install LDAP Web Interface administration package using the command:

   apt-get install phpldapadmin
6. Configure phpLDAPadmin using command:

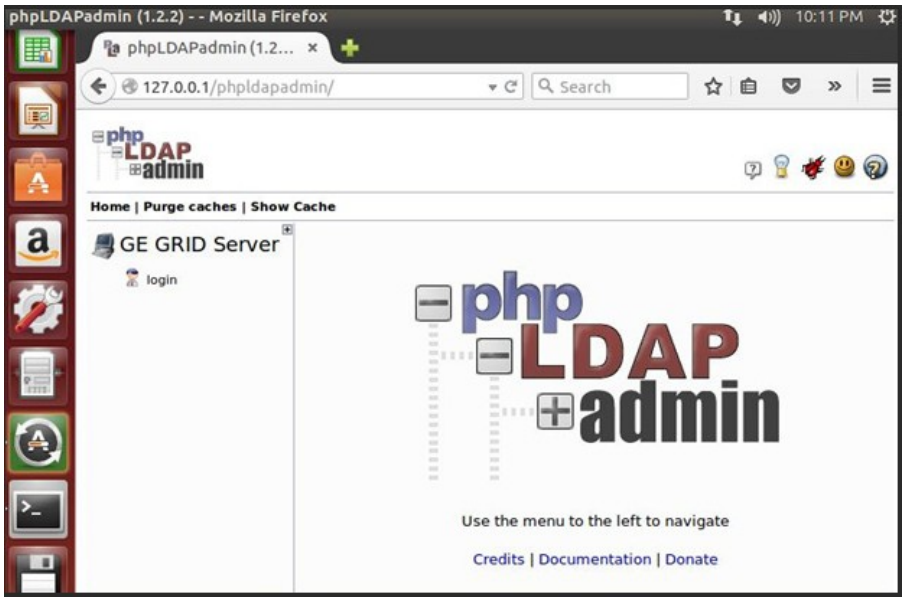
   vi /etc/phpldapadmin/config.php
7. Scroll down further and replace the domain names with your own values:

   7.1. Find the `Define LDAP Servers` section in the configuration file and edit the following lines as shown below. For example:

```
[...]
// Set your LDAP server name //
$servers->setValue('server','name','GE GRID Server');
[...]
// Set your LDAP server IP address //
$servers->setValue('server','host','127.0.0.1');
[...]
// Set Server domain name //
$servers-
>setValue('server','base',array('dc=gegrid,dc=com'));
[...]
// Set Server domain name again//
$servers-
>setValue('login','bind_id','cn=admin,dc=gegrid,dc=com');
[...]
```

8. Restart the apache service using command **systemctl restart apache2**. For Ubuntu 14.10 and older versions use command **service apache2 restart**.

9. Open http://127.0.0.1/phpldapadmin/ in a web browser.
   Result: The php > LDAP > Admin screen appears.



Changing default port numbers on OpenLDAP server

By default the port numbers are:

- 389 for TLS and
- 636 for SSL.

The default configuration **slapd** file is located at:

/etc/default/

The folder contains the following:

```
LAPD_SERVICES="ldap:/// ldapi:/// ldaps:///"
```

To change the default port numbers:

1. Enter the command:

   sudo vi /etc/default/slapd:

2. Modify the **slapd** file content as below where the port 1389 is assigned for TLS and 1636 for SSL.

   ```
   SLAPD_SERVICES="ldap://0.0.0.0:1389/ ldapi:/// ldaps://0.0.0.0:1636/"
   ```

3. Save any changes.

4. Restart the LDAP server service using command:

   sudo /etc/init.d/slapd restart

   Result: A message appears.

   ```
   hudson@ldap:/etc/ldap/slapd.d$ sudo /etc/init.d/slapd restart
    * Stopping OpenLDAP slapd                                            [ OK ]
    * Starting OpenLDAP slapd                                            [ OK ]
   hudson@ldap:/etc/ldap/slapd.d$
   ```

Configuring OpenLDAP server

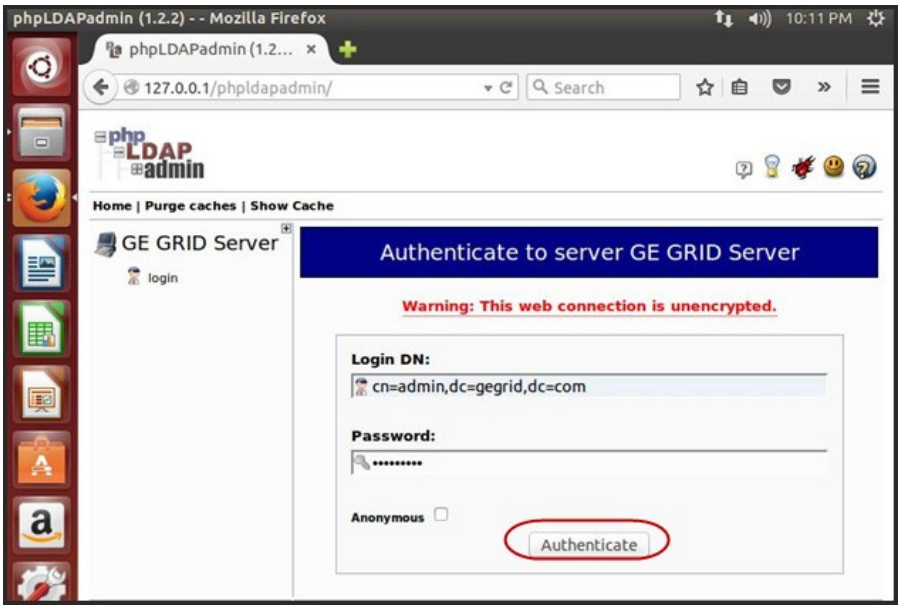
This section describes how to create groups and users which are used for authentication purposes.

Creating role groups

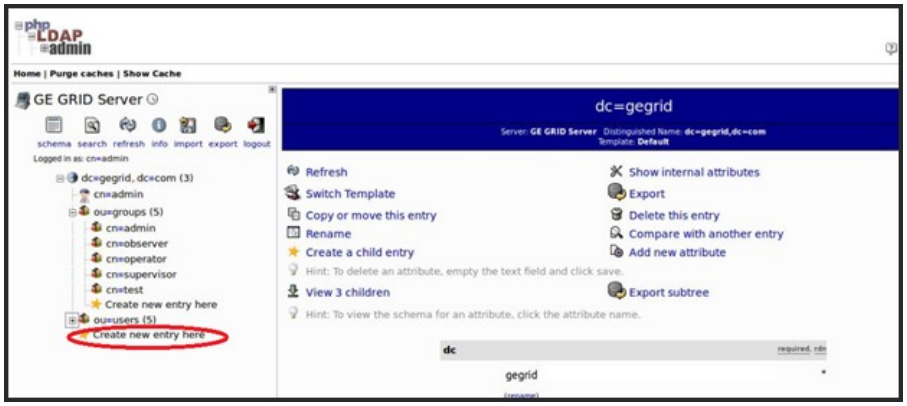
To create user groups:

1. Open a browser window on Ubuntu at:
   http://127.0.0.1/phpldapadmin/
2. Click on **login**.

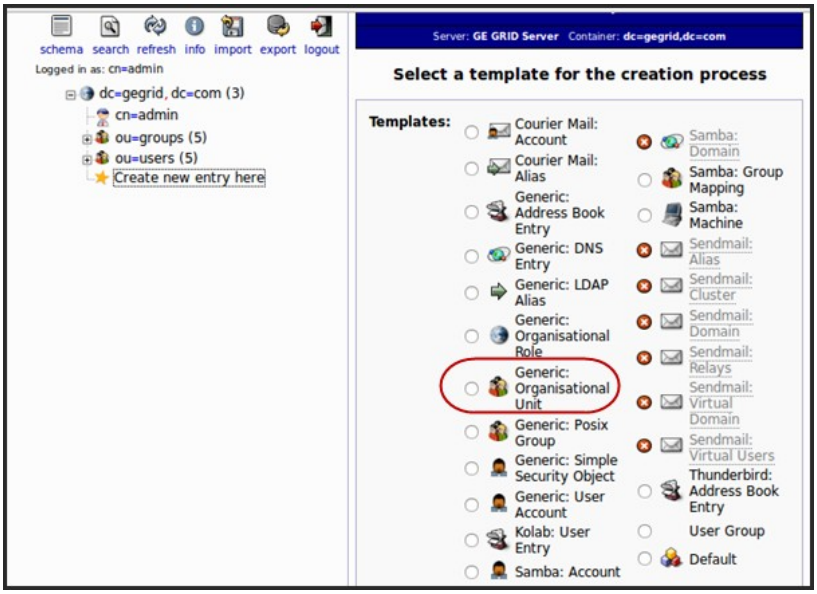
3. Click the **Authenticate** button



4. Expand the tree on the left-hand side and click **Create a new entry here**.



5. Select **Generic Organizational Unit**.

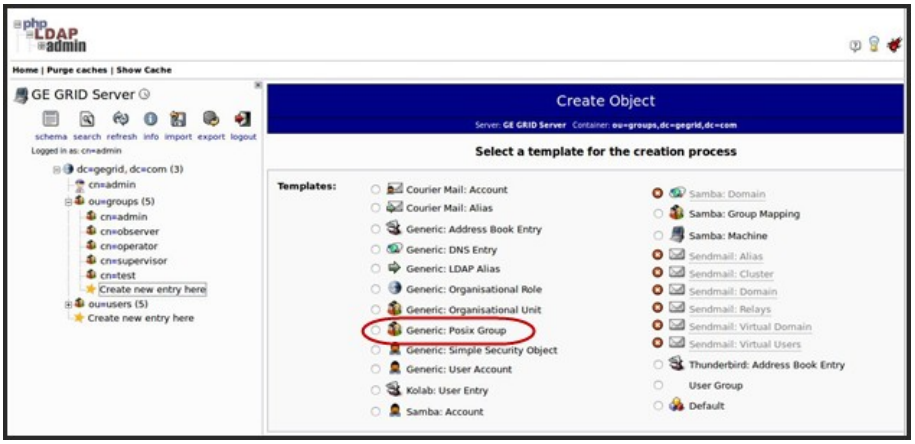


6. Type the name of the group; e.g., **groups** and click **Create Object**.

Result: The Organizational Unit **ou=groups** appears under the host tree.

7. Below the newly created **groups** entry, click **Create a new entry here**.

8. Select the **Generic Posix Group** option.



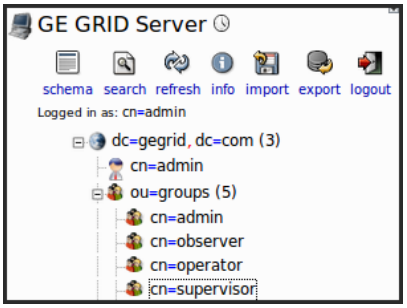
9. Provide the group name and GID number according to the role privilege required; see Table 1, and create the object.

Table 1: Roles and GID numbers

Role	GID number
admin	0
observer	501
operator	502
supervisor	503
passthrough	504

If GID number is not editable during creation, create the object with any GID number and then immediately afterward update it with the desired GID number according to the role required.

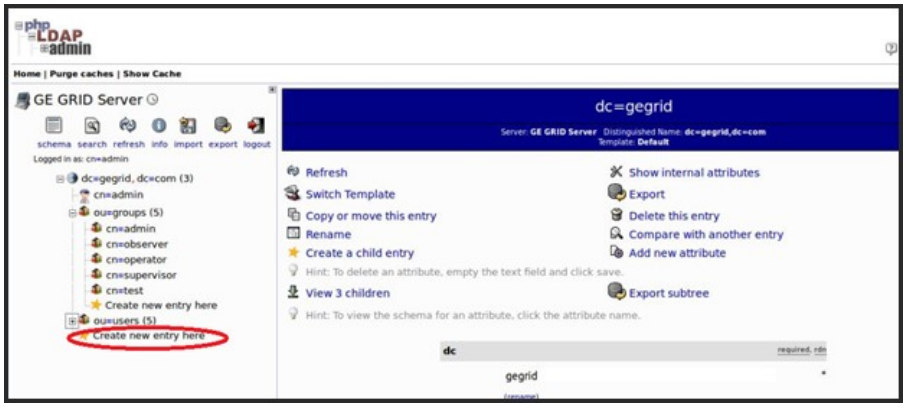
10. You can create different groups as required. See the example groups shown below:



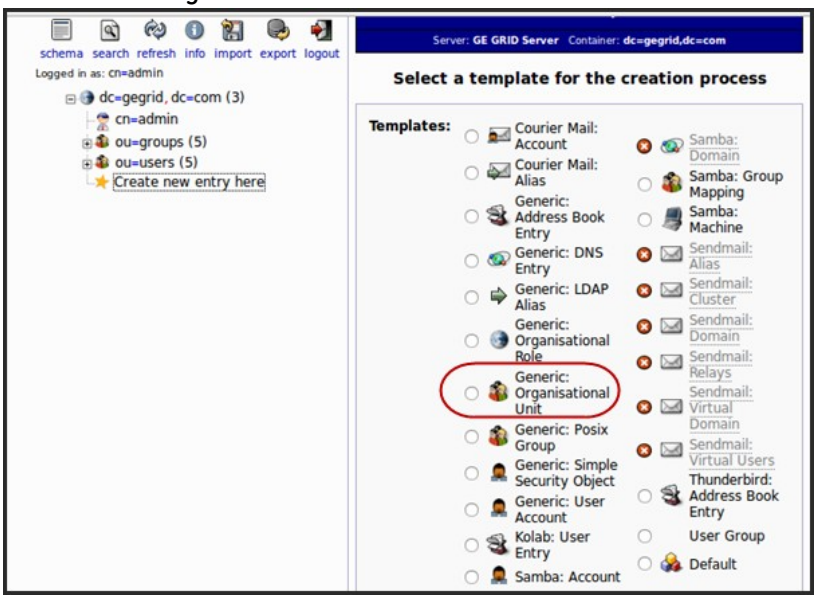
Creating users

To create users and link them to desired roles:

1. Expand the tree on the left-hand side and click **Create a new entry here**.



2. Select **Generic Organizational Unit**.

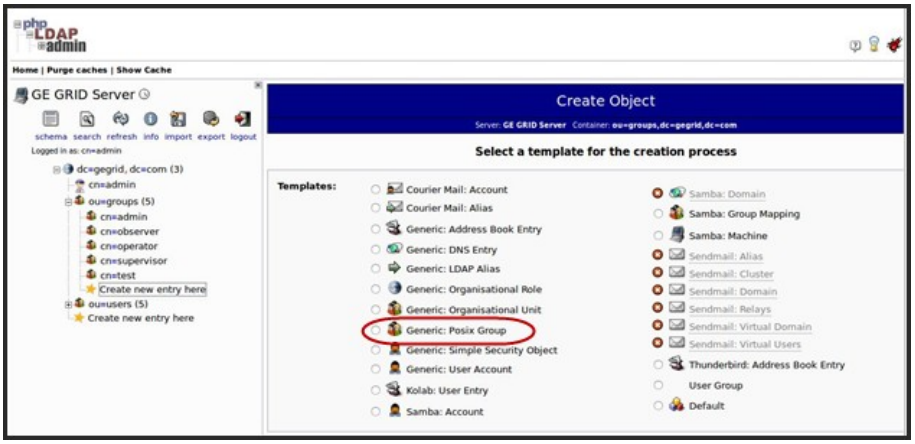


3. Type the name of the group; e.g., **groups** and click **Create Object**.

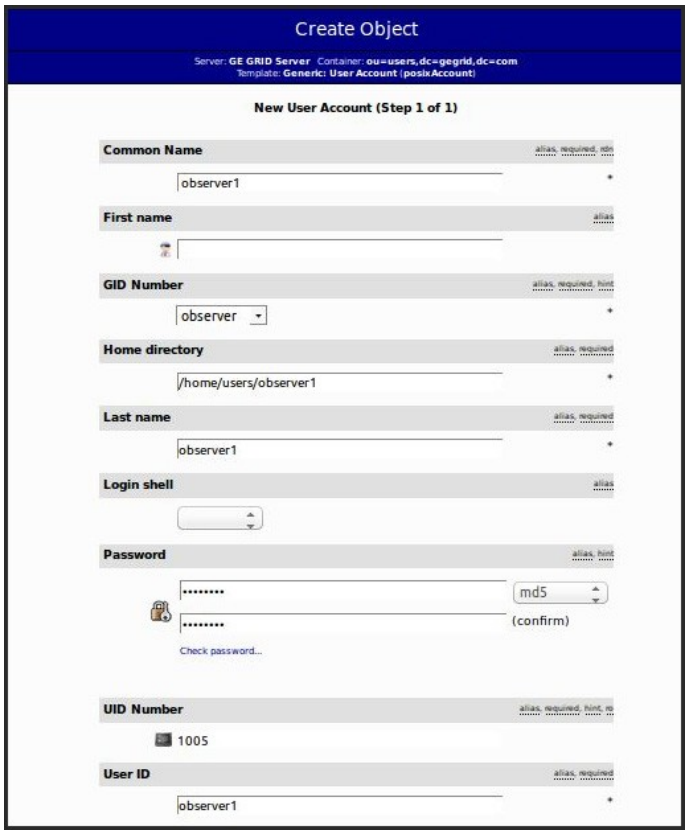
Result: The Organizational Unit `ou=groups` appears under the host tree.

4. Below the newly created `groups` entry, click **Create a new entry here**.

5. Select the **Generic Posix Group** option.

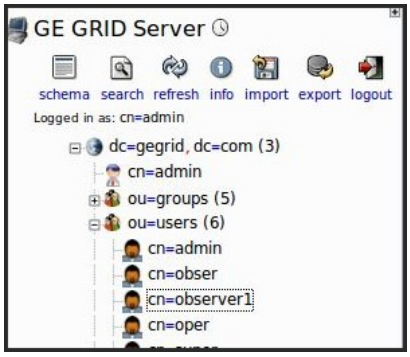


6. Complete the fields for the New User Account.
   6.1. Type in the **Common Name**.
   6.2. Select the required **GID number.**
   6.3. Type in the **Last Name**, **Password** and **User ID**.



7. Click **Create Object** and **Commit**.

8. You can create different users as required. Example users are shown below.



9. Result: The created users are available for authentication from the MCP device.

Group Mapping

Once the User group has been created successfully, these need to be mapped to MCP User Group. It can be done in two approaches:

Procedure for Static Group Mapping

In this approach, the MCP device **LDAP Server group gid** shall be configured as per Table 2.

Table 2: Group IDs mapping on the LDAP Server User Groups

LDAP Server Group Name	GID Number	Description
G500Administrator	0	To map LDAP Server Group G500Administrator to G500 groupAdministrator
G500Observer	501	To map LDAP Server Group G500Observer to G500 group Observer
G500Operator	502	To map LDAP Server Group G500Operator to G500 group Operator
G500Supervisor	503	To map LDAP Server Group G500Supervisor to G500 groupSupervisor
G500SSHPassThrough	504	To map LDAP Server Group G500Passthrough to G500 groupPassthrough

The LDAP Server Group Name in the table is an example. LDAP Server Group Name can be any name as configured by the user, Eg.: Test Group etc. In this example is listed as "G500…", could be "G100…".

Because the functionality is the same across MCP family, this could be "MCP…".
However, GID Number is fixed asspecified in the table for MCP to recognize the same.

Example: In LDAP Server, to map MCP device LDAP Server group with name "**G500Administrator**" to G500 group "**Administrator**" using static group mapping, the LDAP Server group **GID** must configured as in the Table 2.

- The procedure to set the GID number in the LDAP Server is described in the section Creating role groups.

RESULT: Once the G500Administrator group has been mapped successfully for **Administrator** role in MCP, the user added to this group will have administrator role in MCP.

Procedure for Dynamic Group Mapping

In this approach, the MCP device LDAP Server Group distinguished name "DN" must be configured in MCP group mapping. If user want to go for this approach, then GID Number entry in LDAP Server Group is not required.

- Login to MCP as administrator user and configure LDAP on the MCP device as mentioned in Procedure to configure LDAP on the MCP device.

Generating certificates

Before you can configure a secure channel between a MCP device and an LDAP server you need certificates for authorization. Certificates can be generated by either:

- The server itself, or
- A Certification Authority (CA).

Generating certificates from the server

This section describes how to generate certificates from the LDAP server which is installed in the MCP device and used for authorization. You can use the below links to generate CA certificate on Openldap Server in Ubuntu:

http://www.openldap.org/faq/data/cache/185.html

https://help.ubuntu.com/lts/serverguide/openldap-server.html

Generating certificates using XCA

This section describes how to set up the XCA certification authority and generate third party signed certificates.

Once your CA is ready, export the CA certificate so that you can install it on the server and the MCP device.

NOTICE

A CA that is planned for field use should be protected with strong security measures. Such measures include dedicating a computer for the CA, physically securing the computer, ensuring the computer is accessible only by authorized users, and not connecting the computer to a network. Such measures are required because a security breach of a CA impacts all devices that used certificates generated by the CA.

XCA runs on Linux or Microsoft Windows. The following procedures describe how to set up and initialize an XCA certification authority.

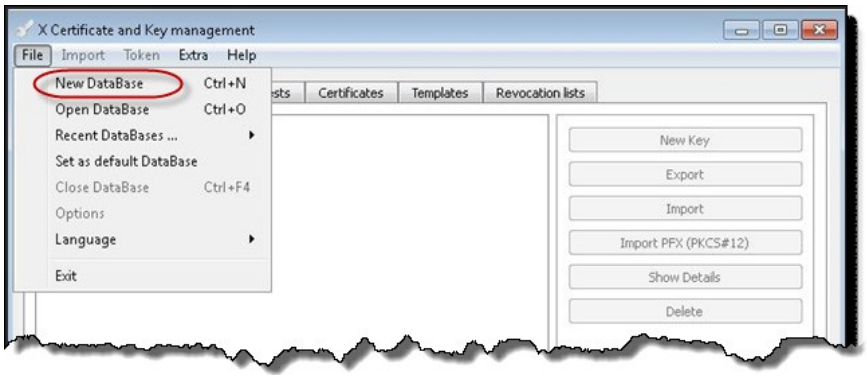
Install XCA

1. Download the latest version of XCA at: http://sourceforge.net/projects/xca.

2. Run the installation wizard to install XCA.

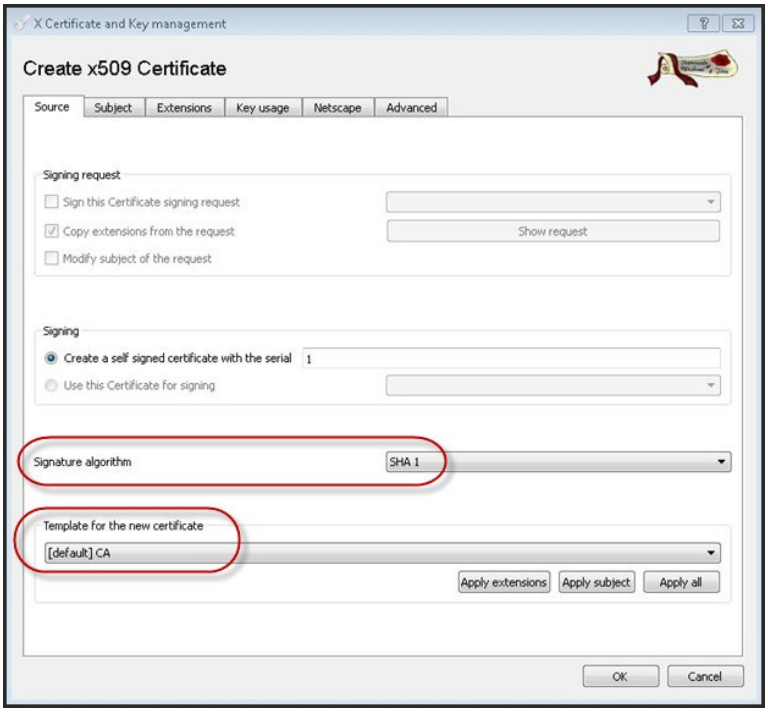
Generating root CA certificate

1. From XCA, select **File** > **New Database**.

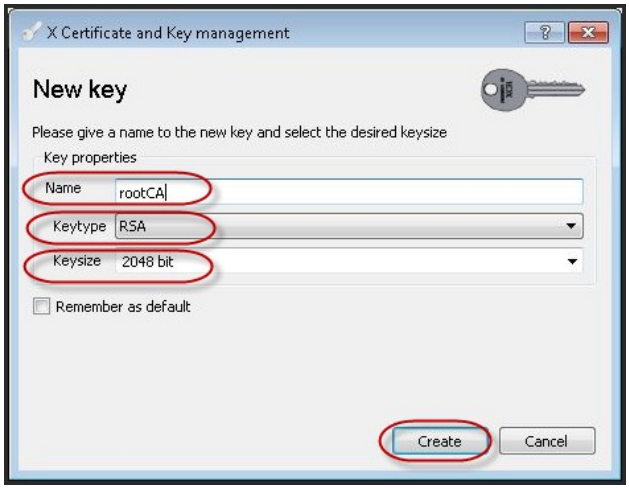


2. Choose a protected location to save the database and then enter a strong password to encrypt the database.
3. Under the **Certificates** tab, click **New Certificate**.

4. Under the **Source** tab:
   4.1. Select the checkbox next to the label: **Create a self signed certificate with the serial**.
   4.2. Do not change the **Signature Algorithm** selection from **SHA 1**.
   4.3. Do not change the **Template for the new certificate** selection from **[default] CA**.

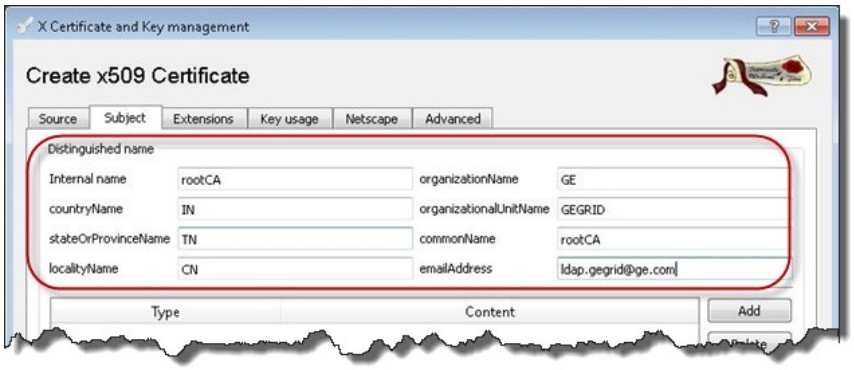


5. Under the **Source** tab, click **Apply All**.
6. Under the **Subject** tab, click the **Generate a new key** button.
7. Complete the fields in the New Key dialog:
   7.1. Type the name of the CA (e.g., **rootCA**) in the **Name** field.
   7.2. Choose the **Keytype** as **RSA** or **DSA** to match your needs.
   7.3. Change the **Keysize** to **2048**.
   7.4. Click **Create**.



8. Under the **Subject** tab, enter the distinguished name of the CA certificate.

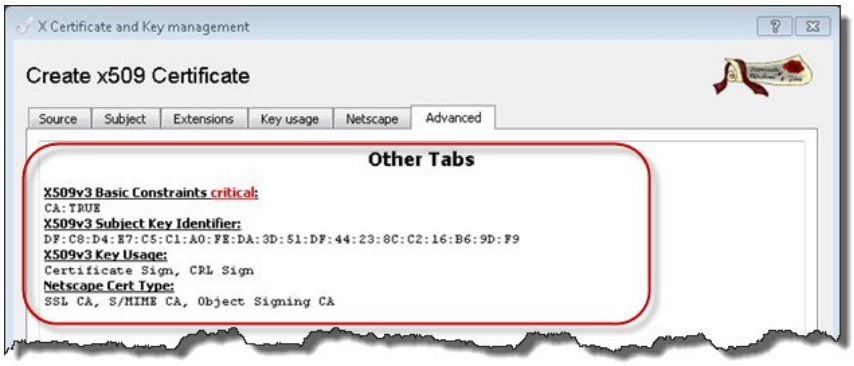
   Result: The following image provides examples for the **Distinguished name** fields.



9. Under the **Extensions** tab, if necessary change the **Time Range** that the CA certificate is valid for and click **Apply**.

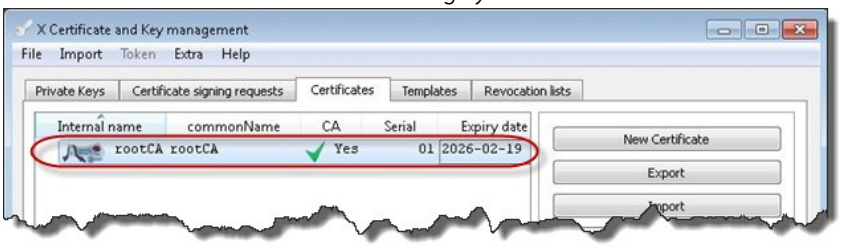
   The default is 10 years. Certificates generated with this CA certificate after this period are no longer valid.

10. Under the **Key usage** tab, do not change the defaults.
11. Under the **Netscape** tab, remove the value in the **Comment** field.
12. Under the **Advanced** tab, the following messages appear, except for the value of the X509v3 Subject Key Identifier, which differs from key to key:



13. Click **OK**.

    Result: You now have a CA certificate to sign your server and MCP device certificates.



14. Under the **Certificates** tab of the main view of XCA, select the new Certification Authority and click **Export**.
15. Ensure the Export Format is set to **PEM**.
16. Browse to a protected directory (e.g., My Documents->MyXCAFiles) and click **Save**.
17. Click **OK**.

    Result: The file is named based upon the internal name of your CA with a .crt extension.

Generating certificates using root CA certificate

This subsection describes how to generate private keys and certificates for LDAP server. These certificates allow the LDAP server to authenticate itself to the MCP device.

There are two types of server certificates:

- Type 1: The server certificate is issued by the root CA certificate.
  For the procedure, see Generating a LDAP server Certificate issued by root CA certificate.
- Type 2: A server certificate issued by an Intermediate CA certificate which is issued by a root CA certificate.
  Type 2 is the most secure since two CA certificates are used in authorization process.
  For the procedure, see Generating an Intermediate CA certificate issued by root CA certificate.

NOTICE

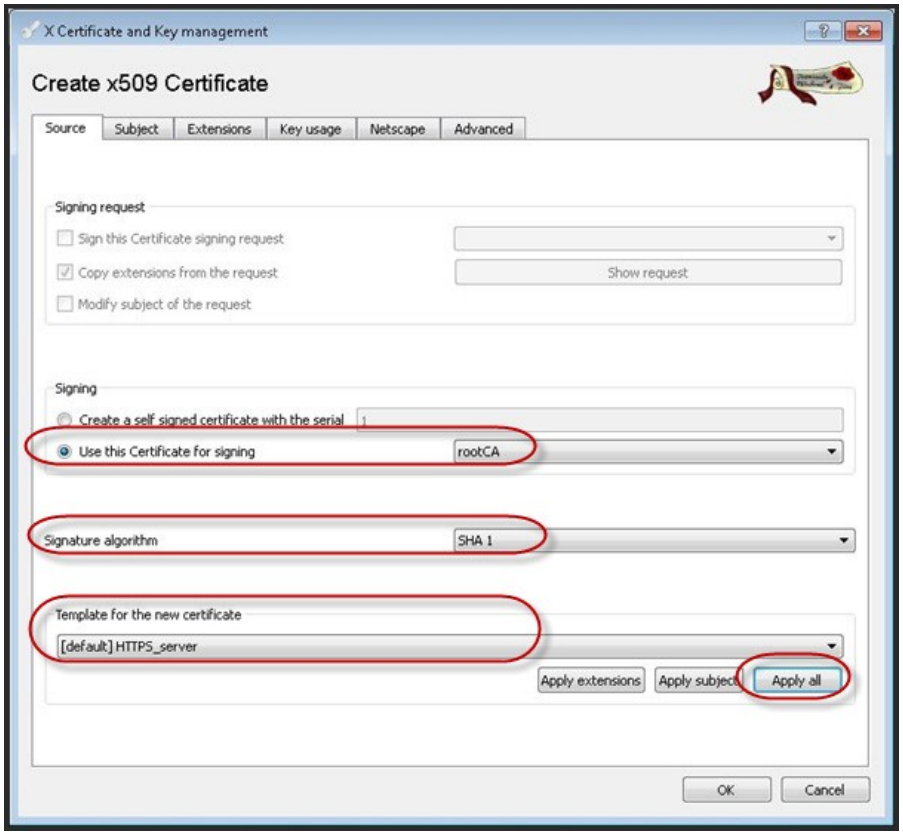
It is important to keep the private key associated with the Server Certificate secure. For example, they should not be transmitted over the LAN unless you are using a strongly authenticated secure transport mechanism such as SSH with public/private key authentication or multi-factor authentication. Once the private keys reach their destination, they should be deleted from any devices used to transport them (e.g., a USB drive or laptop).

Generating a LDAP server Certificate issued by root CA certificate

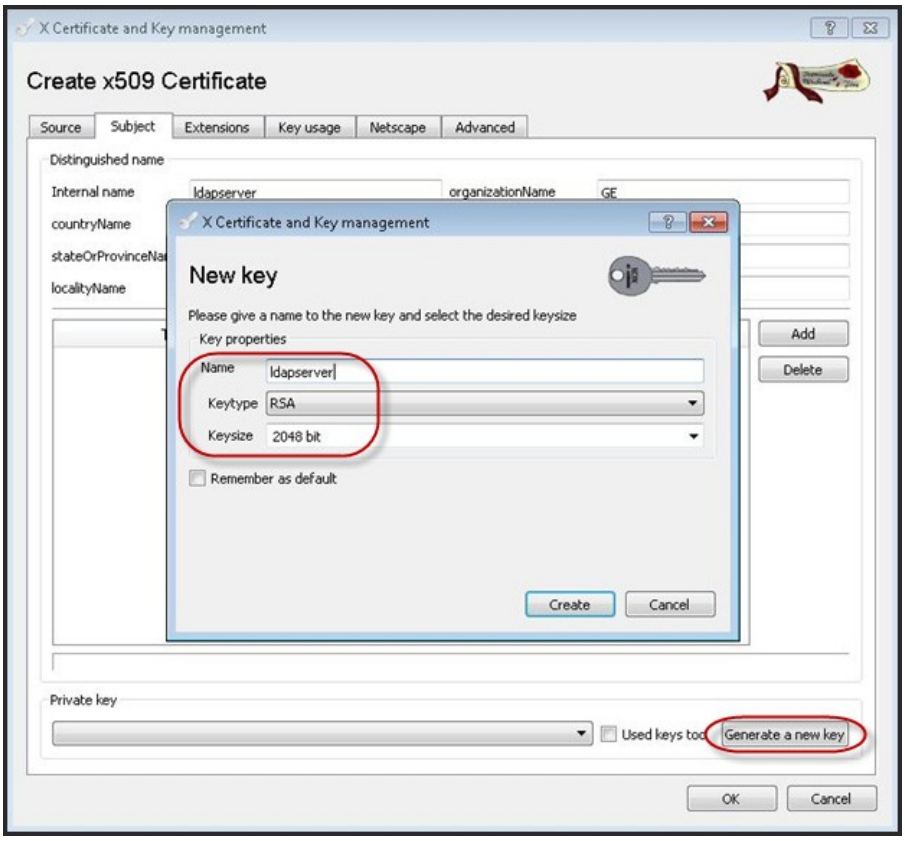
An LDAP Server certificate allows the LDAP server to authenticate itself to the MCP device. The LDAP Server certificate contains a commonName field. This field should match with the host name of LDAP server.

1. Launch XCA from the Windows Programs menu.
2. In the tree view of the **Certificates** tab, select the branch containing your Certification Authority.
3. Under the **Certificates** tab, click the **New Certificate** button.
4. Under the **Source** tab:
   4.1. Select the **Use this Certificate for signing** checkbox. From the drop-down menu to the right of this checkbox, select the CA you created in section:Generating certificates using XCA. (e.g., **rootCA**).
   4.2. Do not change the drop-down **Signature Algorithm** from **SHA 1**.
   4.3. Change the drop-down selection from **Template for the new certificate** to **[default] HTTPS_server**.

4.4. Click **Apply all**.



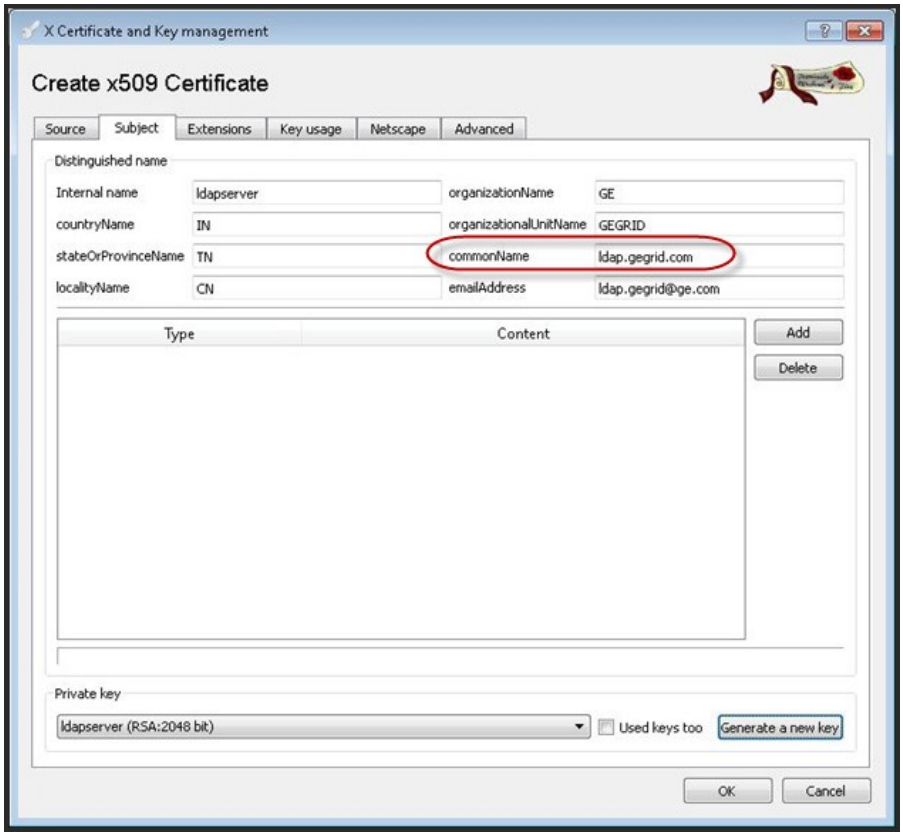
5. Under the **Subject** tab, click the **Generate a new key** button.



6. In the dialog that appears:
   6.1. Type in a name of the server key.
   6.2. Choose **Keytype** as **RSA** or **DSA** to match your needs.
   6.3. Change the Keysize to **2048**.
   6.4. Click **OK**.
7. Back in the **Subject** tab, type in the Distinguished name of the LDAP server certificate.

   The most important component is the **commonName** which should match with LDAP server host name. Any difference between the commonName of the certificate and the host name configured in the server results in a failed connection.

Choose other name components that are appropriate for your company. The following image provides example distinguished name components.



8. Under the **Extensions** tab, if necessary change the **Time Range** that the CA certificate is valid for and click **Apply**.

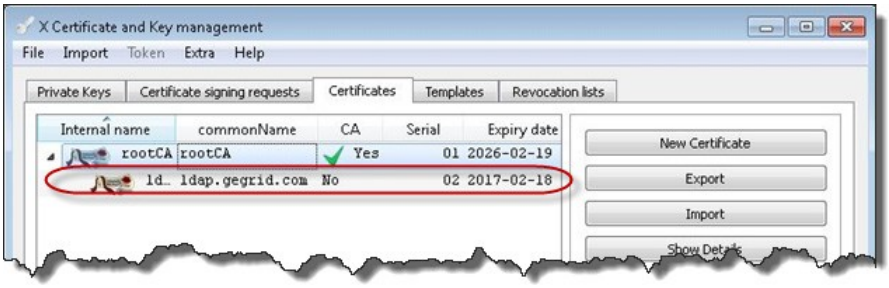
   The default is one year. The shorter the Time Range the more secure the certificate. The longer the Time Range, the more often you need to regenerate LDAP Server certificates and deploy them to your LDAP server.

9. Under the **Key usage** tab, leave the defaults.
10. Under the **Netscape** tab, remove the comment.
11. Under the **Advanced** tab, click **Validate**.

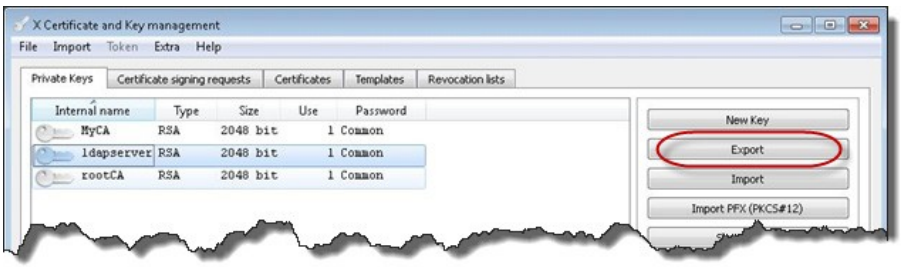
    The following messages are expected except the value of the X509v3 Subject Key Identifier, which differs from key to key:

12. Click **OK**.

    Result: You now have a LDAP Server certificate.



13. In the tree view under the **Certificates** tab, open the branch labeled after your Certificate Authority, and then selects the new Server certificate.
14. Click **Export**.



15. In the dialog that appears, ensure the **Export Format** field is set to **PEM**:
    15.1. Browse to a protected location (e.g., My Documents->MyXCAFiles)
    15.2. Click **Save**.
    15.3. Click **OK**.

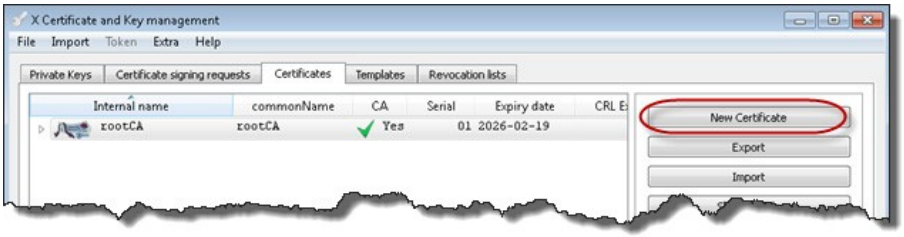
    The file is named based upon the internal name of your LDAP server certificate with a .crt extension.
16. Click on the **Private Keys** tab and then select the LDAP server key which you created earlier. Click **Export**.
17. In the dialog that appears, ensure the **Export Format** field is set to **PEM Private**.
    17.1. Browse to a protected location (e.g., My Documents->MyXCAFiles).
    17.2. Click **Save**.
    17.3. Click **OK**.

    The file is named based upon the key name of your LDAP server certificate with a .pem extension.

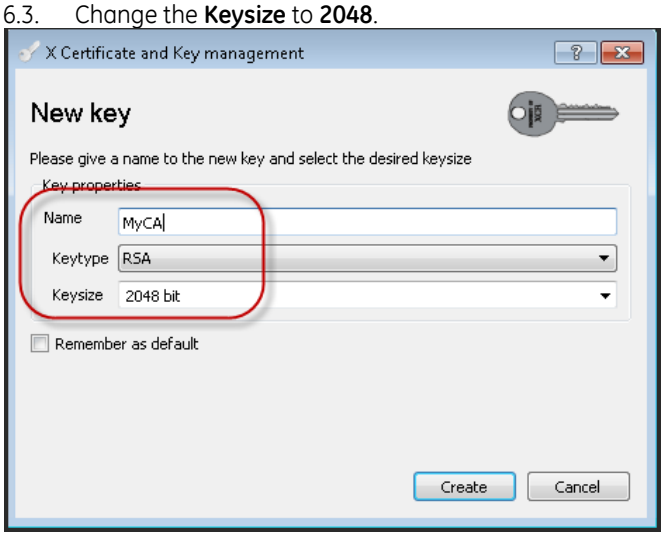
    These files are security-sensitive, so keep them protected at all times. Remove the files after they have been installed on the LDAP server.
18. Go to section: Installing certificates on OpenLDAP server.

Generating an Intermediate CA certificate issued by root CA certificate

1. In the tree view of the **Certificates** tab, select the branch containing your Certification Authority.
2. Under the **Certificates** tab, select **New Certificate**.

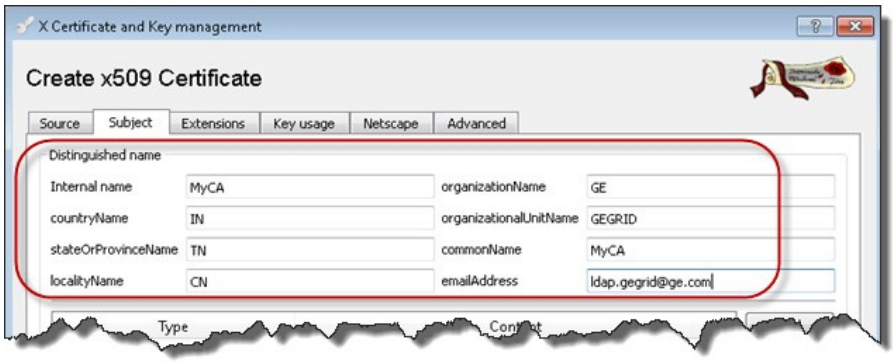


3. Under the **Source** tab:
   - 3.1. Select the **Use this Certificate for signing** checkbox.
   - 3.2. From the drop-down menu to the right of this checkbox, select the self-signed CA you created in section: Generating certificates using XCA.(e.g., **rootCA**).
   - 3.3. Do not change the drop-down selection **Signature Algorithm** from **SHA 1**.
   - 3.4. Change the drop-down **Template** for the new certificate to **[default] CA**.
   - 3.5. Click **Apply all**.
4. Under the **Source** tab, click **Apply All**.
5. Under the **Subject** tab, click the **Generate a new key** button.
6. In the dialog that appears:
   - 6.1. Type in the name of the CA (e.g., **MyCA**) in the **Name** field.
   - 6.2. Choose the **Keytype** as **RSA** or **DSA** to match your needs.
   - 6.3. Change the **Keysize** to **2048**.



7. Under the **Subject** tab, type in the distinguished name of the CA certificate.

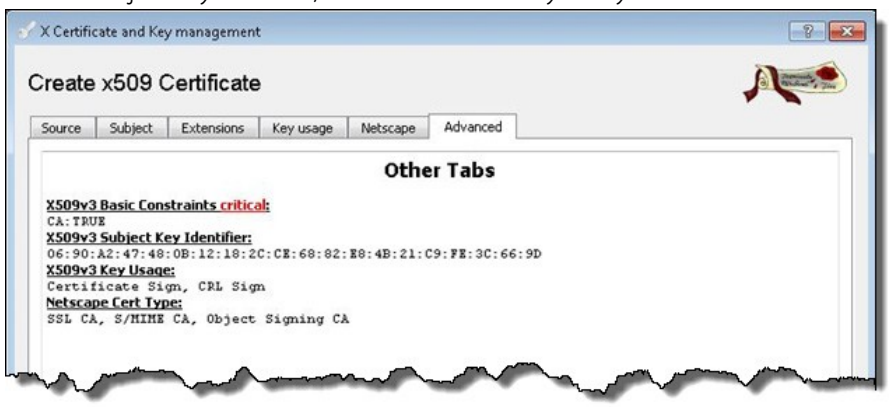
   Result: The following image provides example distinguished name components.



8. Under the **Extensions** tab, change the **Time Range** to a time period before the expiry of CA (e.g rootCA) which you created earlier and click Apply.

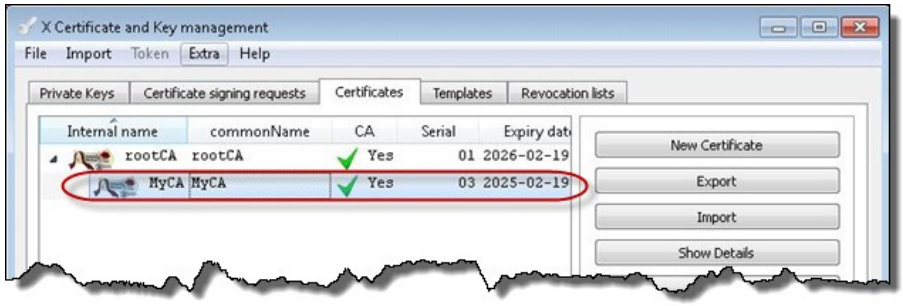
   The default is 10 years. Certificates generated with this CA certificate after this period are no longer valid.

9. Under the **Key usage** tab, do not change the defaults.
10. Under the **Netscape** tab, remove the value in the **Comment** field.
11. Under the **Advanced** tab, the following messages are expected except the value of the X509v3 Subject Key Identifier, which differs from key to key:



12. Click **OK**.

    Result: You now have an intermediate CA certificate.



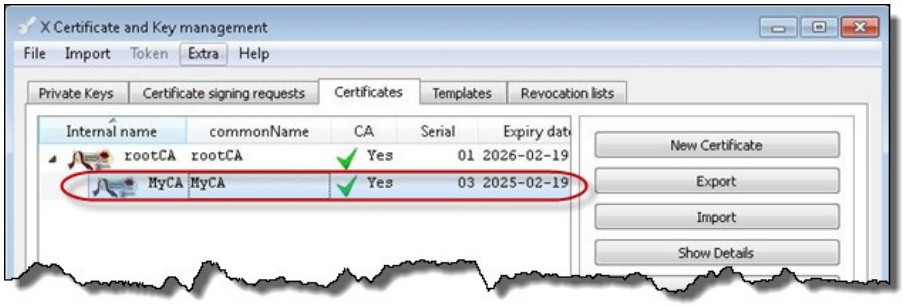
13. Under the **Certificates** tab of the main view of XCA, select the new Certification Authority and click **Export**.
14. Ensure the **Export Format** is set to **PEM**.

15. Browse to a protected directory (e.g., My Documents->MyXCAFiles) and click **Save**. Click **OK**. The file is named based upon the internal name of your CA with a .crt extension.

Generating a LDAP server Certificate issued by an Intermediate CA certificate

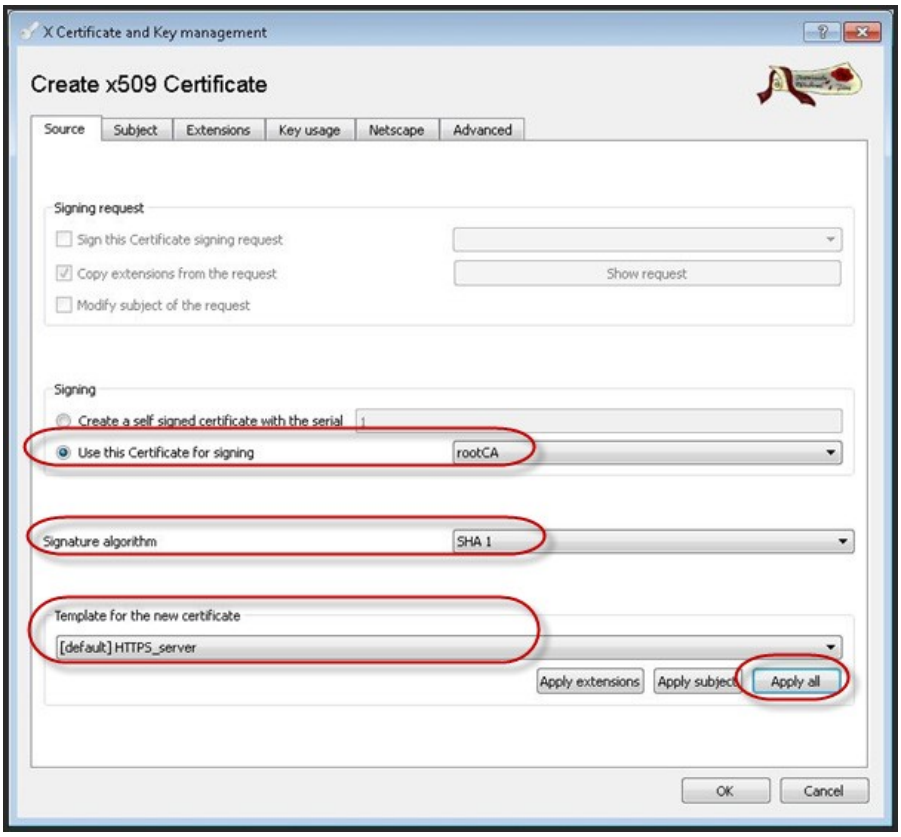
An LDAP Server certificate allows the LDAP server to authenticate itself to the MCP device. The LDAP Server certificate contains a commonName field. This field should match with the host name of LDAP server.

1. In the tree view of the **Certificates** tab, select the branch containing your Certification Authority.

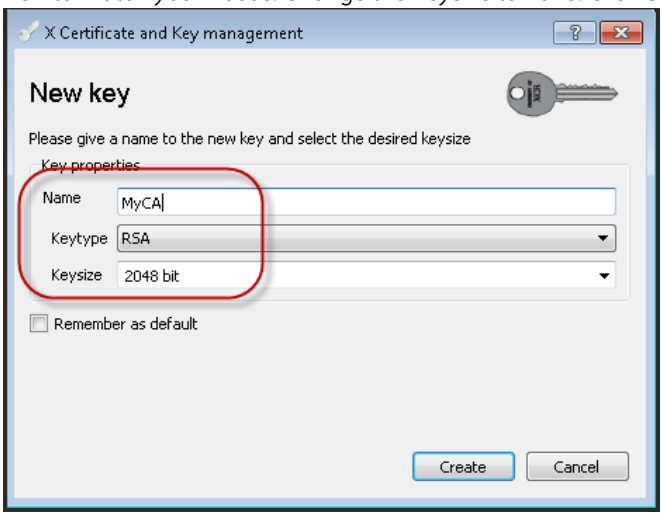


2. Under the **Certificates** tab, click the **New Certificate** button.
3. Under the **Source** tab:
   3.1. Select the **Use this Certificate for signing** checkbox. On the drop-down menu to the right of this checkbox, select the CA signed CA file you created in section: Generating an Intermediate CA certificate issued by root CA certificate (e.g., **MyCA**).
   3.2. Do not change the drop-down selection **Signature Algorithm** from **SHA 1**.
   3.3. Change the drop-down selection from **Template** for the new certificate to **[default] HTTPS_server**.

3.4. Click **Apply all**.



4. Under the **Subject** tab, click the **Generate a new key** button.
5. In the dialog that appears, enter a name of the server key. Choose **Keytype** as **RSA** or **DSA** to match your needs. Change the Keysize to **2048**. Click **OK**.



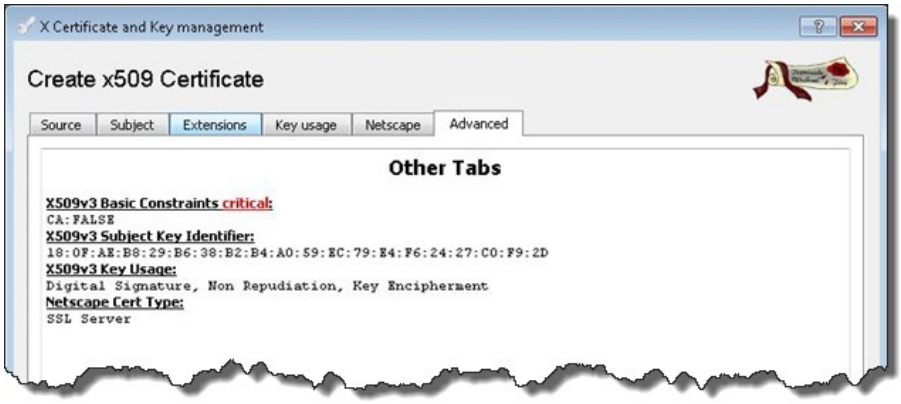
6. Back in the **Subject** tab:
   6.1. Type in the **Distinguished name** of the LDAP server certificate. The most important component is the commonName which should match with LDAP server host name. Any difference between the commonName of the certificate and the host name configured in the server results in a failed connection.
   6.2. Choose other name components that are appropriate for your company.

   The following image provides example distinguished name components.

7. Under the **Extensions** tab, if necessary change the **Time Range** that the CA certificate is valid for and click **Apply**.

   The default is one year. The shorter the Time Range the more secure the certificate. The longer the Time Range, the more often you need to regenerate LDAP Server certificates and deploy them into your LDAP server.
8. Under the **Key usage** tab, do not change the defaults.
9. Under the **Netscape** tab, remove the comment.
10. Under the **Advanced** tab, click **Validate**.

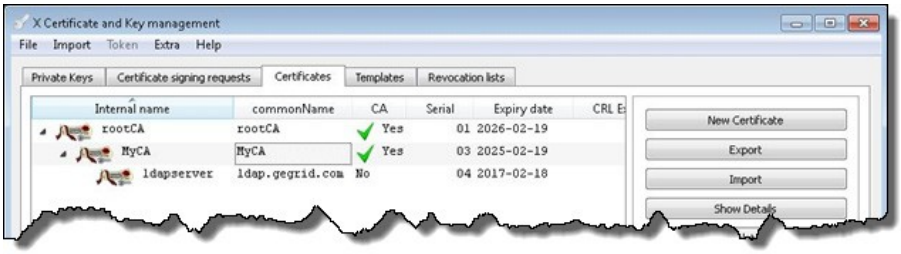
    Result: The following messages are expected except the value of the X509v3 Subject Key Identifier, which differs from key to key:



11. Click **OK**.

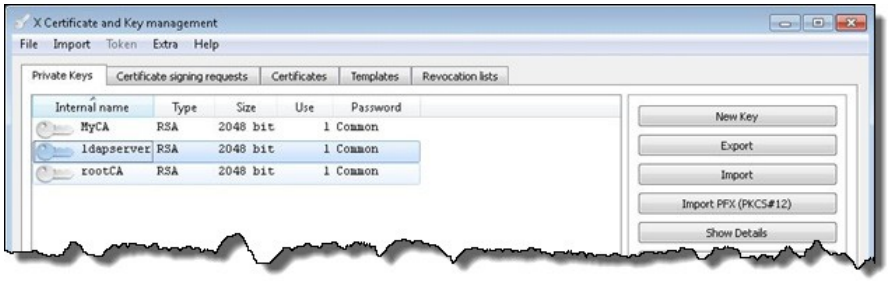
    Result: You now have a LDAP Server certificate.

12. In the tree view under the **Certificates** tab, open the branch labeled after your Certificate Authority, and then selects the new Server certificate.



13. Click **Export**.
14. In the dialog that appears:
    14.1. Ensure the **Export Format** field is set to **PEM**.
    14.2. Browse to a protected location (e.g., My Documents->MyXCAFiles)
    14.3. Click **Save**.
    14.4. Click **OK**.

    The file is named based upon the internal name of your LDAP server certificate with a .crt extension.
15. Under the **Private Keys** tab select the LDAP server key which you created earlier.



16. Click **Export**
17. In the dialog that appears,
    17.1. Ensure the **Export Format** field is set to **PEM Private**. Browse to a protected location (e.g., My Documents->MyXCAFiles).
    17.2. Click **Save**.
    17.3. Click **OK**.

    The file is named based upon the key name of your LDAP server certificate with a .pem extension.

    These files are security-sensitive so keep it protected at all times. Remove the files after they have been installed on the LDAP server.

Installing certificates on OpenLDAP server

Server certificate private key and Server Certificate along with its issuer CA certificate need to be installed on OpenLDAP server.

1. Open the terminal of the Ubuntu system.
2. Copy the server certificate (.crt) and its issuer certificate (rootCA.crt in case of single CA file and MyCA.crt in case of 2 CA files) to /etc/ssl/certs folder.
3. Copy the server private key (.pem) to /etc/ssl/private folder.
4. Go to the **/etc/ldap/slapd.d** folder
5. Create a file with ldf extension. For example create certinfo.ldf and contents of the file should be similar to image and match the filenames to actual filenames. Make sure the files are copied to respective locations as mentioned. If you are adding filenames for the very first time, then remove the line “changetype: modify” in below example and replace keyword “replace” with “add”. If you are modifying files names just follow the below example.

```
dn: cn=config
changetype: modify
replace: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ssl/certs/MyCA.crt
-
replace: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ssl/certs/ldapserver.crt
-
replace: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ssl/private/ldapserver.pem
~
~
~
~
~
```

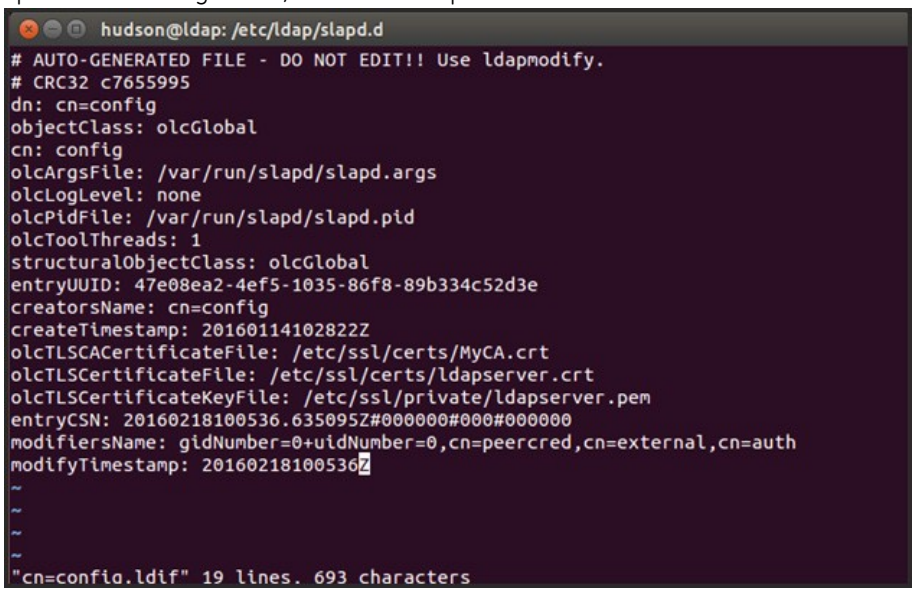
6. Execute the following command:

   sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f /etc/ldap/slapd.d/certinfo.ldf

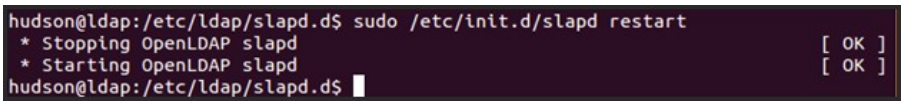
   Result: See the below image.

```
hudson@ldap:/etc/ldap/slapd.d$ sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f /etc/
ldap/slapd.d/certinfo.ldf
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "cn=config"
```

7. Open the cn=config.ldif file, Observer the updated file names in this file.



8. Restart the LDAP server service using command **sudo /etc/init.d/slapd restart**.
   Result: Messages appear as shown below:



Configuring the MCP devices for Centralized LDAP Authenticationusing Open LDAP Server

Chapter 2: Configure the LDAP on MCP

The Lightweight Directory Access Protocol (LDAP) is an application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network. This Directory services may provide any organized set of records, often with a hierarchical structure.

This chapter describes how to install CA Certificates on the MCP device and configure LDAP on the MCP device.

See section:

- Installing CA Certificates on the MCP device
  - CA Certificate transfer procedure from PC to MCP
    - CA Certificate Transfer to MCP by using DSAS Secure File Browser
    - CA Certificate transfer to MCP by using external Secured USB
  - CA Certificate Installation procedure
    - Import and Install CA certificate through Runtime DSAS
    - Import and Install CA certificate through Local HMI
- Configuring LDAP on the MCP device
  - Prerequisites to configuring LDAP on MCP device
    - Create an Emergency Administrator User
    - Retrieve LDAP Authentication Server information
  - Procedure to configure LDAP on the MCP device

Installing CA Certificates on the MCP device

This section describes how to install the CA Certificate to the MCP device. There are two type of certificates you can create:

- Server certificate
- Client certificate

Files to be Created	• CA certificate to be installed in both the Client and Server. • Server Certificate to be installed in the Server for Server Authentication (This can be skipped if LDAP Server CS us used to create the CA Certificate).	
Files to be Transferred	**MCP**	MyCA.crt or MyCA.cer (LDAP Client)
	Open LDAP Server	MyCA.crt or MyCA.cer servercert.p12 (LDAP Server)

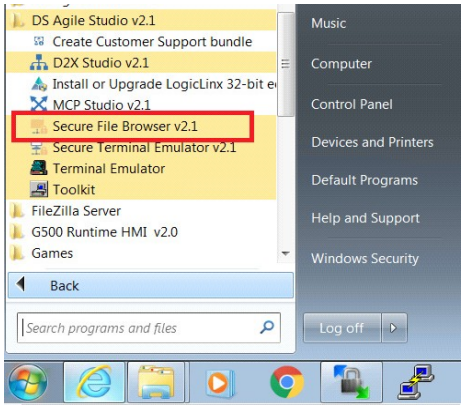
CA Certificate transfer procedure from PC to MCP

You can import and install the CA certificate to MCP. This certificate can be transferred to MCP for installation, using either of the below two options:

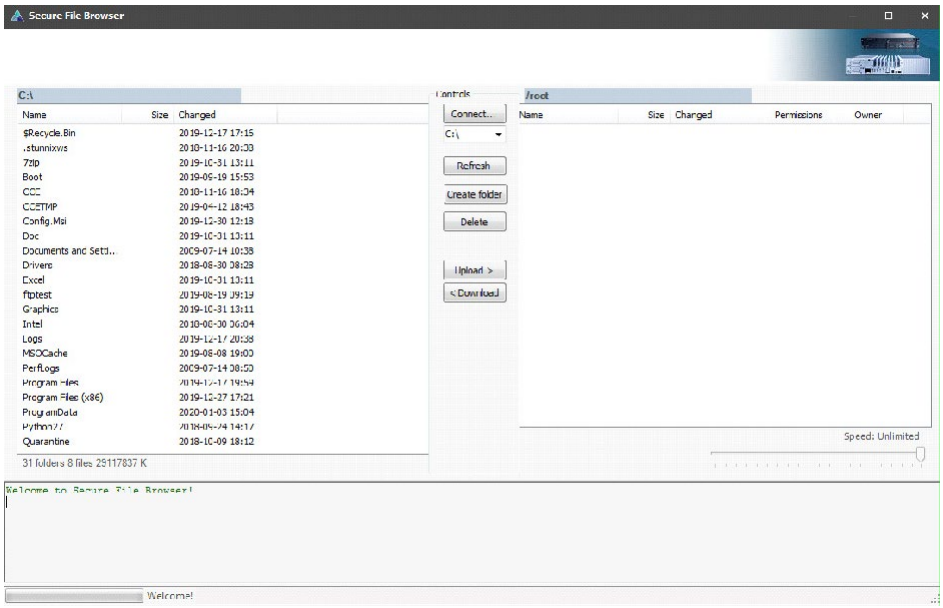
1. CA Certificate Transfer to MCP by using DSAS Secure File Browser
2. CA Certificate transfer to MCP by using external Secured USB

CA Certificate Transfer to MCP by using DSAS Secure File Browser

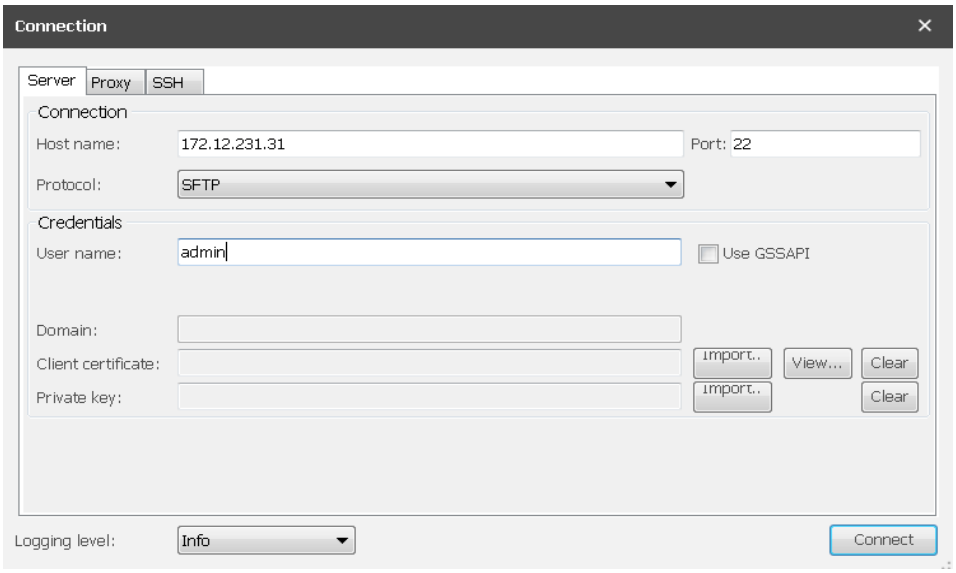
1. Copy the files containing the CA certificate to the following MCP location: **/mnt/user/SecureScadaTransfer**
   - This can be done using the DSAS Secure File Browser (SFTP file transfer program).
   - To launch DSAS Secure File Browser, click on: **Start>All programs>DS Agile Studio vX.0> Secure File Browser vX.0**.



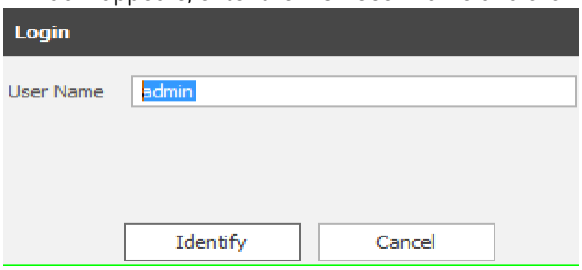
- Secure File Browser screen will be launched as below:



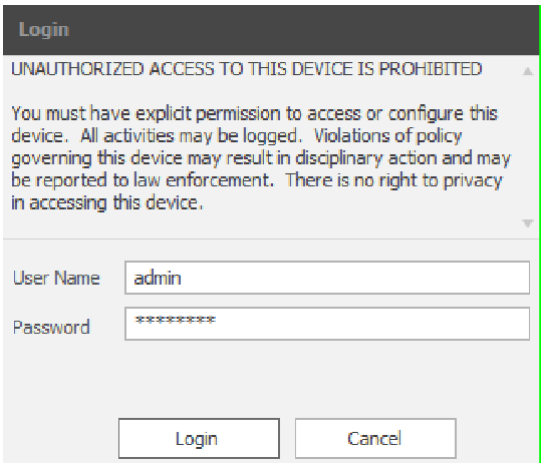
- Click **Connect**.
- The Connection Details window will appear.
- Enter Host name: MCP IP, Protocol: SFTP, User name details and then click **Connect**.



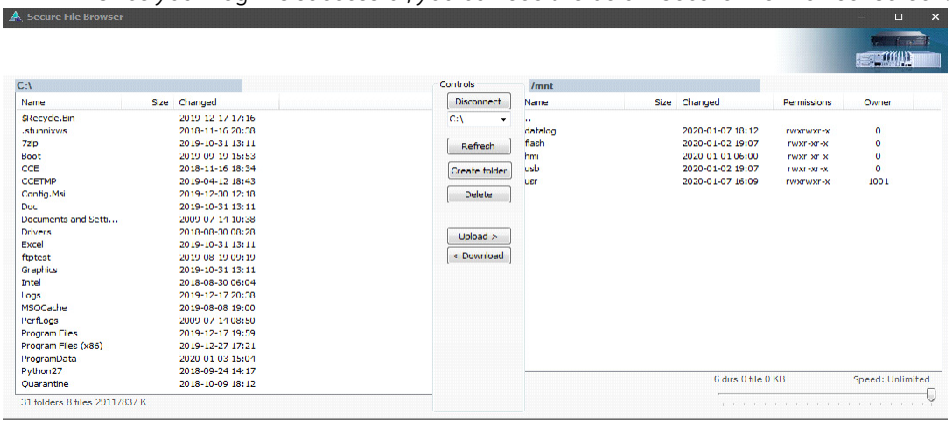
- A Login window appears, enter the MCP User Name and click **Identify** tab.



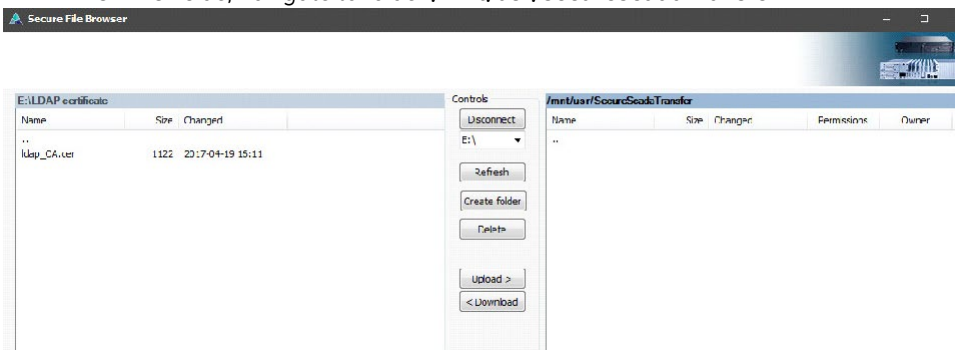
- Once the User Name is identified with the MCP, a Login window appears and prompt for the Password.



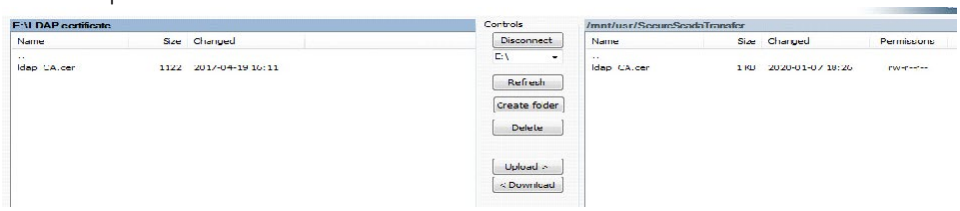
- Enter the Password and click **Login** to access the MCP folders.
- Once your Login is successful, you can see the below Secure File Browser screen:



- In the Secure File Browser window, PC folders are displayed on the left side and the MCP folders are displayed on the right.
- On MCP side, navigate to folder **/mnt/usr/SecureScadaTransfer**



– Select the required certificate from the PC folder and click **Upload**. This will upload the files from PC to MCP.



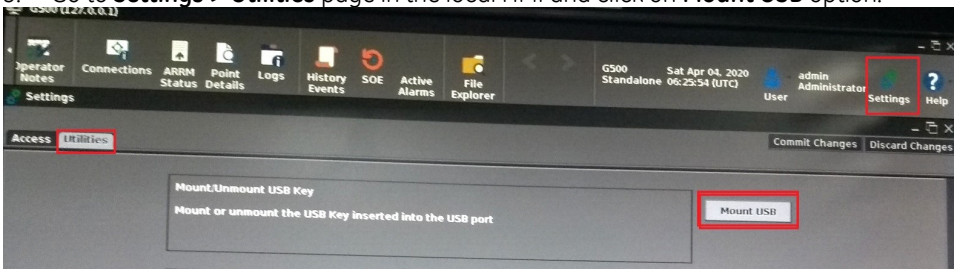
NOTE

After completion of these steps, LDAP client certificate is transferred successfully to MCP and is ready for installation.

CA Certificate transfer to MCP by using external Secured USB

Once the LDAP client certificate (CA certificate) is created and available on the PC and you can transfer this CA certificate to MCP using USB as follows:

1. Create a directory in USB drive "**SecureScadaTransfer**".
2. Copy the CA certificate from PC to USB on a USB drive (LDAP Client certificate need to be available in USB at **\SecureScadaTransfer**).
3. Insert the USB drive into any USB slot on the MCP device. E.g.: USB Port-1
4. Open Local HMI and login as administrator user.
5. Go to **Settings > Utilities** page in the local HMI and click on **Mount USB** option.



6. Now USB is mounted successfully to MCP and CA certificate is available at **/mnt/usb/usb1/SecureScadaTransfer**.

CA Certificate Installation procedure

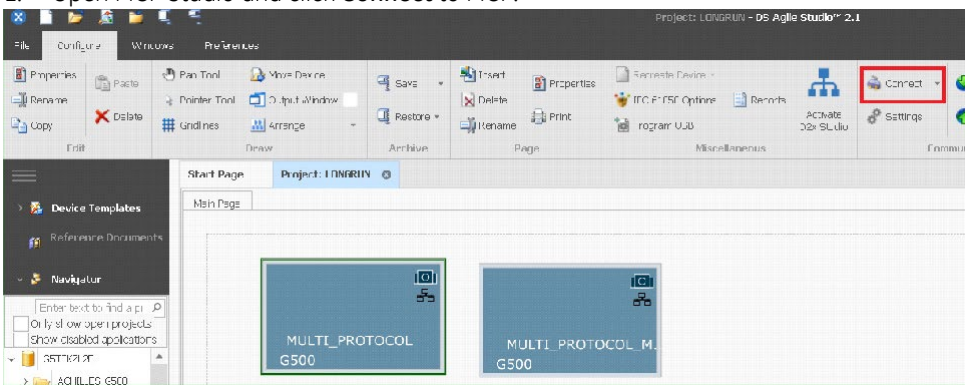
Once the certificate is available in MCP by any of the transfer procedure mentioned in page 38 (Secure DSAS Browser or USB), it can be installed by using either of the below two interfaces:

– Import and Install CA certificate through Runtime DSAS
– Import and Install CA certificate through Local HMI

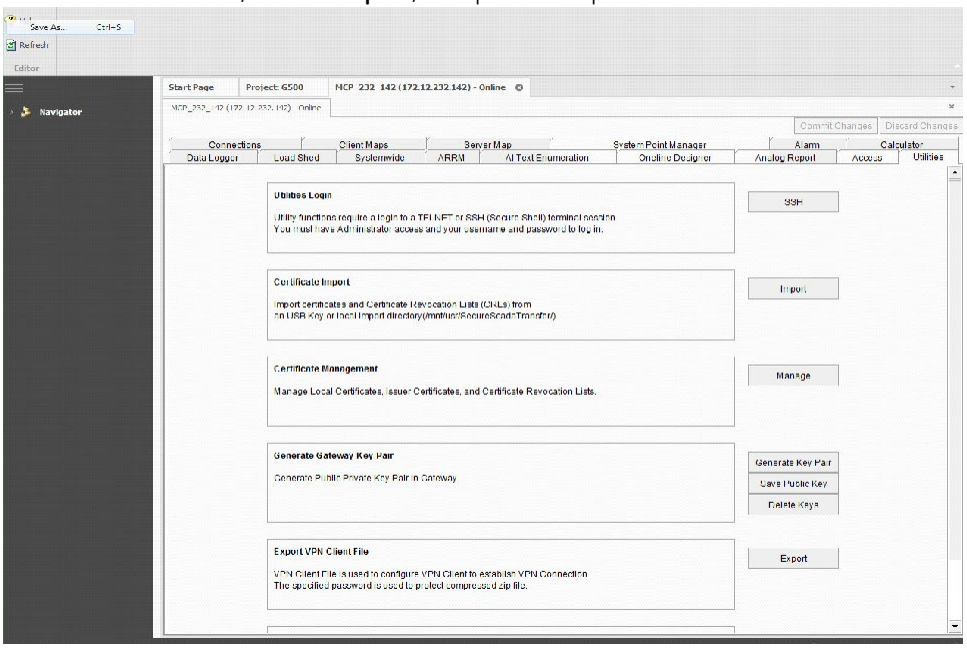
Import and Install CA certificate through Runtime DSAS

After certificate transfer to MCP at **/mnt/usr/SecureScadaTransfer/** or certificates can be installed to MCP using **DSAS > Utilities**. To proceed follow the below steps:

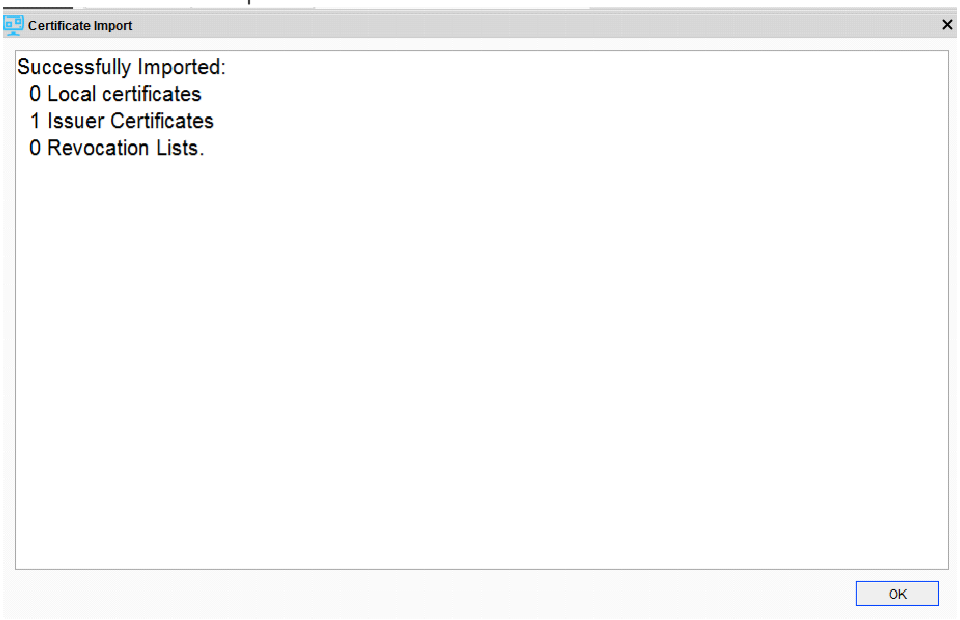
1. Open MCP Studio and click **Connect** to MCP.



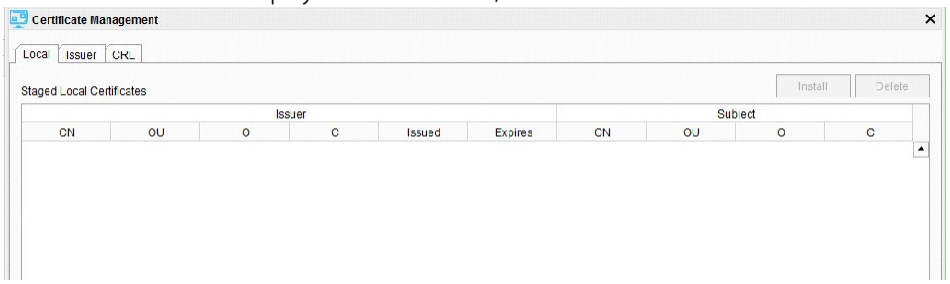
2. Select Utilities tab, click on **Import**, to import the copied certificates.



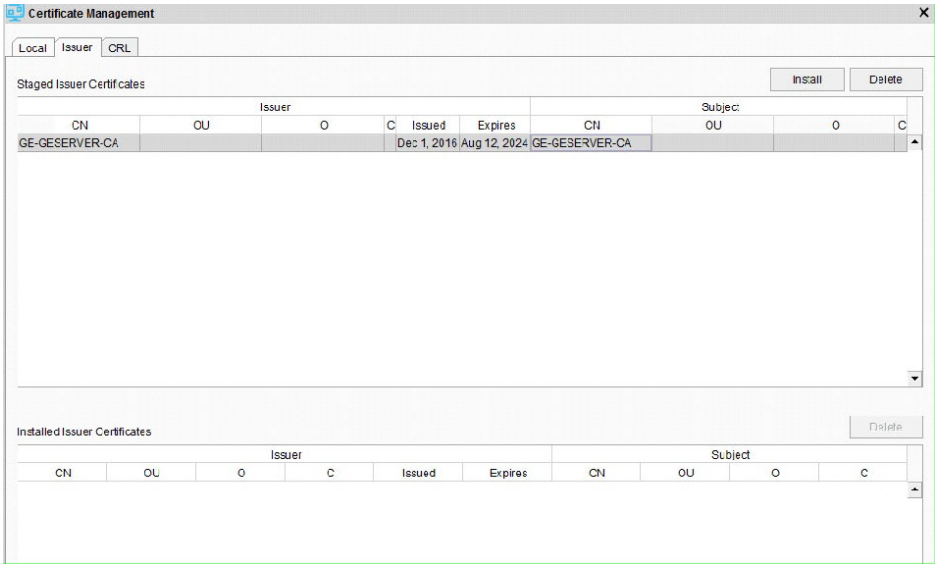
3. Once the certificates are imported, a Certificate Import window appears which shows confirmation of import status. Click **OK**.



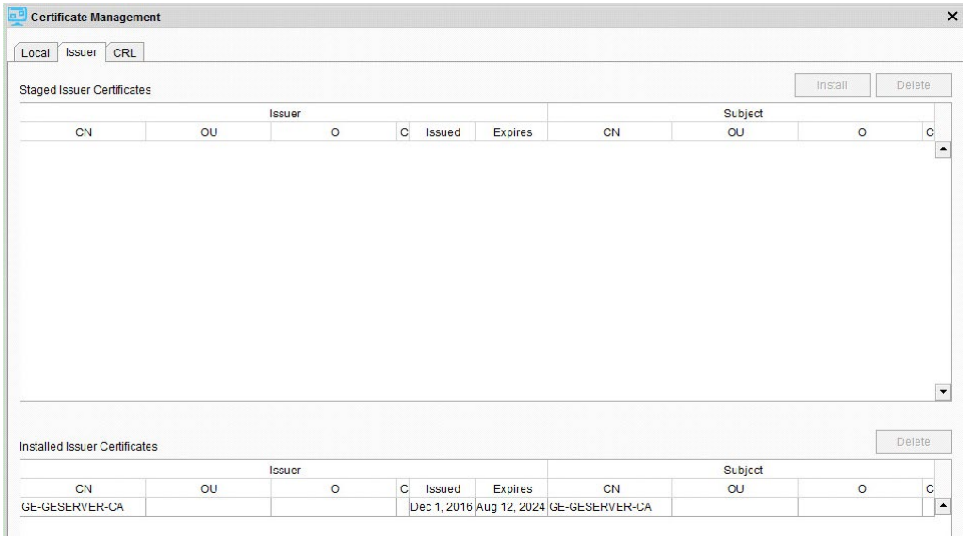
4. Once the certificates are imported successfully, click "**Manage**" to manage local certificates which display three tabs **Local**, **Issuer** and **CRL** as below:



5. Click on **Issuer** tab, select the Certificate and click **Install**.



6. Once the certificate is installed successfully, it is moved to the Installed Issuer Certificates section:

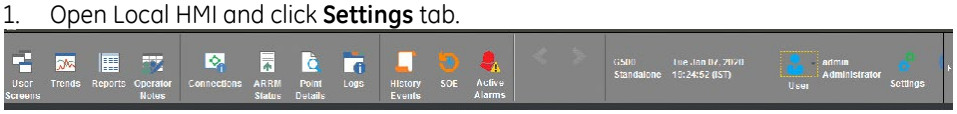


RESULT: This completes the Certification Installation process through DSAS Online HMI. You can use this certificate in LDAP Authentication.

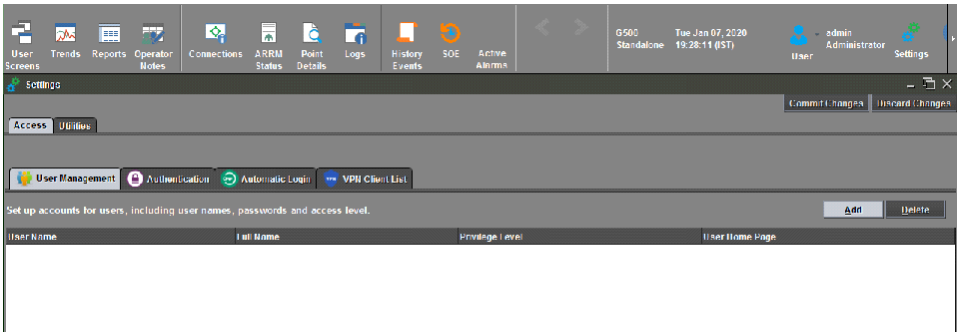
Import and Install CA certificate through Local HMI

After the certificate is transferred to the MCP at **/mnt/usr/SecureScadaTransfer/** or **/mnt/usb/usb1/SecureScadaTransfer/** certificates can be installed to MCP using **Local HMI > Settings > Utilities**. To proceed follow the prescribed steps as below:

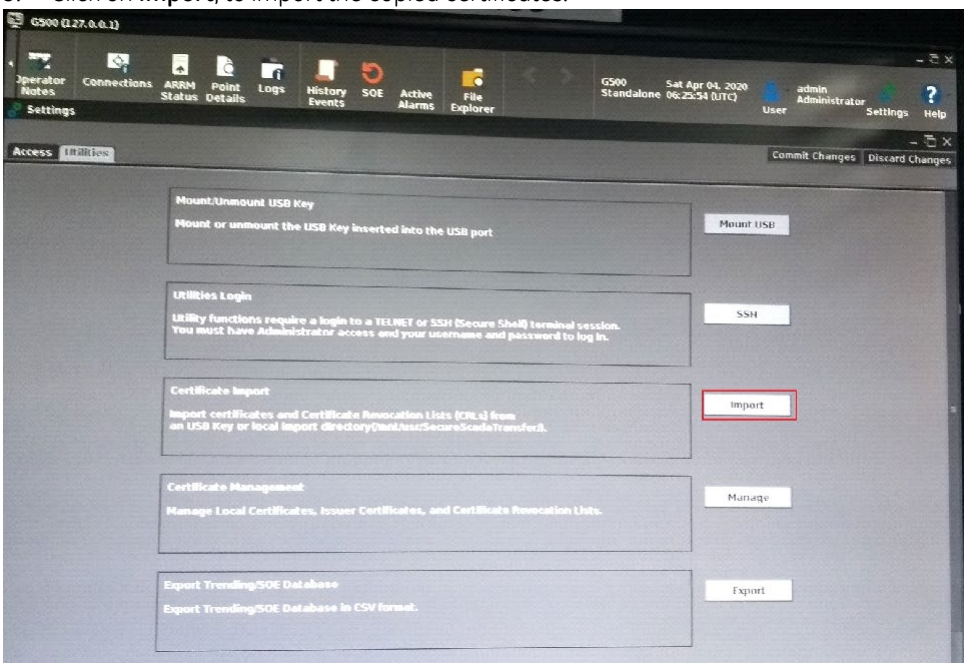
1. Open Local HMI and click **Settings** tab.



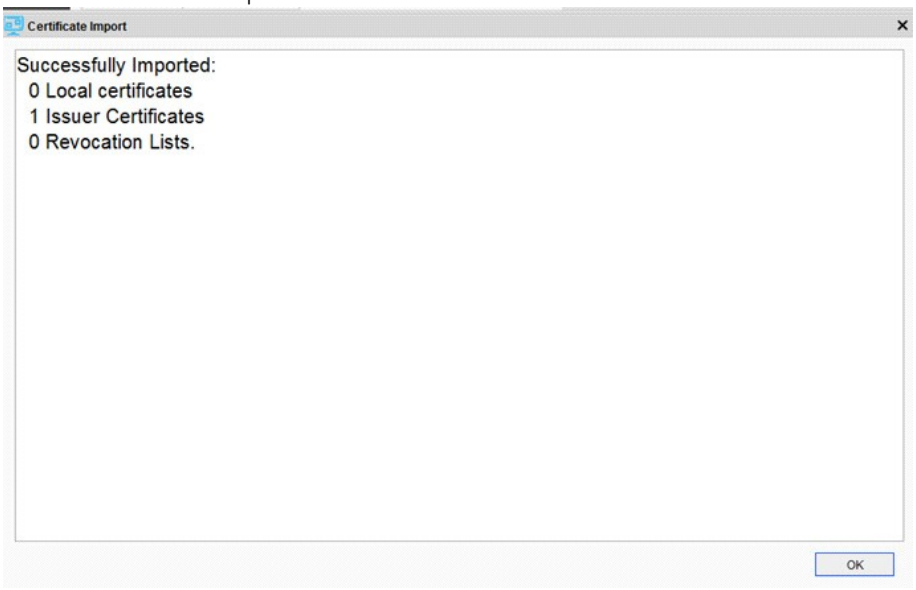
2. Click **Utilities** tab.



3. Click on **Import**, to import the copied certificates.

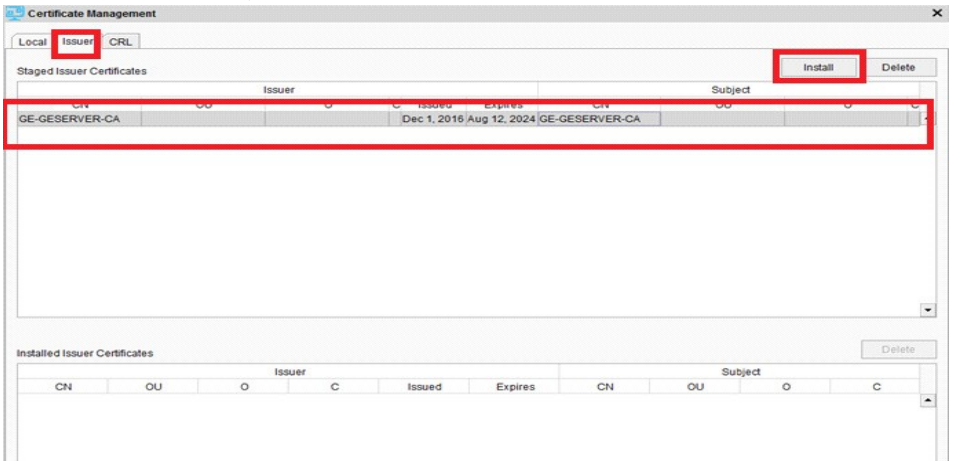


4. Once the certificates are imported, a Certificate Import window appears which shows confirmation of import status. Click **OK**.

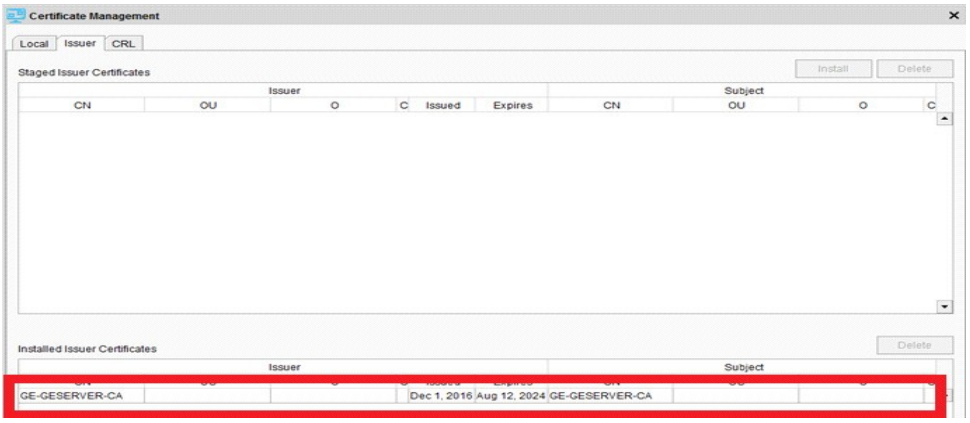


5. Once the certificates are imported successfully, click "**Manage**" to manage local certificates which display three tabs Local, Issuer and CRL as below:

6. Click on **Issuer** tab, select the Certificate and click **Install**.



7. Once the certificate is installed successfully, it's moved to the Installed IssuerCertificates section:



RESULT: This completes the Certification Installation process through DSAS Online HMI. You can use this certificate in LDAP Authentication.

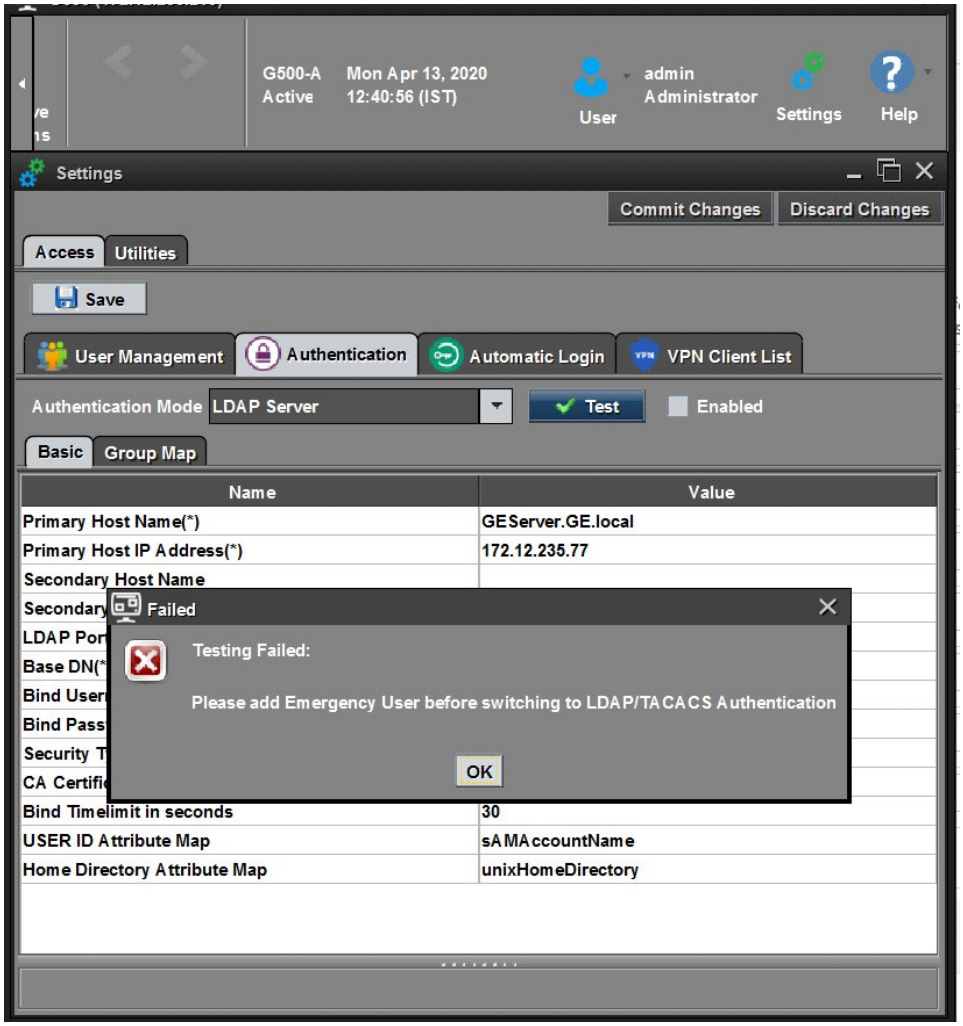
Configuring LDAP on the MCP device

This section describes the:

- Tasks performed prior to configuring the LDAP on the MCP device and
- The procedure to configure the LDAP on the MCP device.

Prerequisites to configuring LDAP on MCP device

Prior to configuring the LDAP on the MCP device it is mandatory to create emergency user in MCP. If user directly start LDAP configuration by using section Procedure to configure LDAP on the MCP device then user will get popup message that “Please add Emergency User before switching to LDAP/TACACS Authentication” and user will not be able to configure LDAP authentication without adding emergency users.



Create an Emergency Administrator User

This emergency user can be used when remote authentication server is not available and user in unable to access MCP using Remote Authentication. This emergency admin user is required to get access to the system in case of emergency, i.e. when LDAP server is not responsive / user forgets all credentials etc.

Emergency Users can be created by using any of the below two option:

- Using Web MCP Settings GUI
- Using the mcpcfg utility on MCP device through Secure Terminal Emulator

An emergency administrator user can login to MCP using any of the below three interfaces:

1. SSH session to MCP (Port-922)
2. Front serial port connection to MCP (Baud Rate- 115200)
3. MCP Emergency option in local console

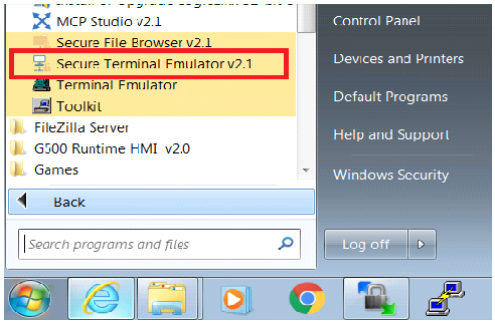
Once user logs into MCP as Emergency Administrator user, executing “emercfg” command shall provide options for user to perform the below two key functions:

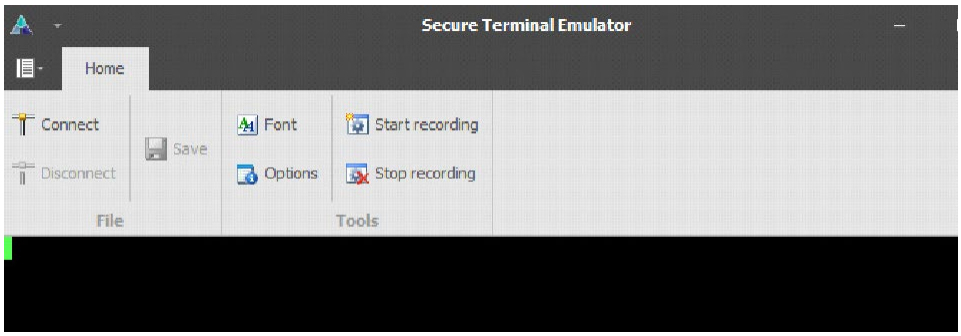
- Change the mode authentication from remote to local mode.
- Generate emergency code to login to HMI without changing authentication from remote to local mode.

Below sections describes how to add emergency user in MCP by using any of these option step by step:

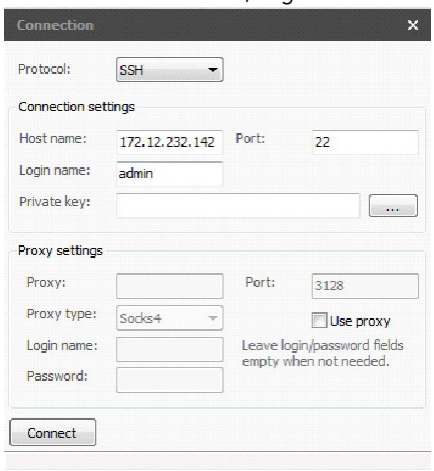
Using the mcpcfg utility on MCP device through Secure Terminal Emulator

1. To open Secure Terminal Emulator, select **Start > All Programs > DS Agile Studio vX.0 > Secure Terminal Emulator vX.0**

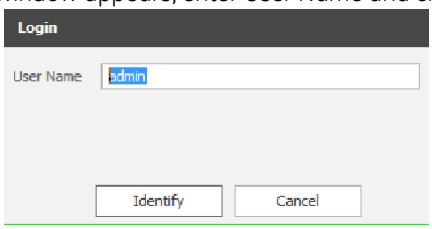




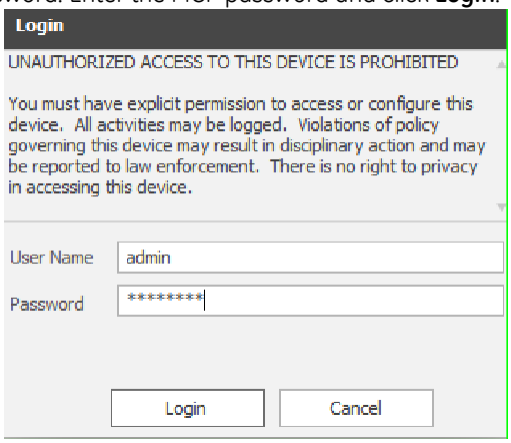
2. Click **Connect**. A pop-up window appears which shows Connections credentials.
3. Enter your MCP IP in Host name, Login name and Port 22 and click **Connect**.



4. A Login window appears, enter User Name and click **Identify**.



5. Once the User Name is identified with the MCP, a Login window appears to prompt for the Password. Enter the MCP password and click **Login**.



6. Once you login successfully, MCP Shell window appears:

```
GE Multilin MCP Firmware Release 110 Production Build 391 2020-01-01:04:41:24

admin@G500:~$
```

7. Type **sudo mcpcfg** and enter your Administrator User Name and Password if prompts.
8. The Gateway Settings Menu appears:

```
================================================================
        Gateway Settings Menu
================================================================

        0.   Back
        1.   Configure Authentication
        2.   Configure Network Settings
        3.   Configure Network Interfaces
        4.   Configure Secure Access
        5.   Configure Firewall
        6.   Configure Host Names
        7.   Configure Time & Time Sync
        8.   Reset System Logs
        9.   Reset Database Tables
        10.  Reset File Persistence Data
        11.  Local HMI
        12.  Configure Sync Manager
        13.  Redundancy
        14.  ARRM
        15.  Suppress Forced Qualities To Masters
        16.  Emulate D20 RTU IEC101 DPA Unbalanced Mode Functionality
        17.  Configure IEC101+104 DPA Startup Quality Event Suppress Interva
        18.  Configure Serial Ports
        19.  Configure D.20 Port Settings
        20.  EdgeOS Host
        21.  Clear Chassis Intrusion State
```

9. Enter **1** to select **Configure Authentication** option and the below menu appears:

```
         Gateway Settings Menu   Authentication
=================================================

         Current AuthMode Status : Local

         0.   Back
         1.   Root Administrator Settings
         2.   Pass-Through Password Authentication
         3.   Administrator Group Users
         4.   Emergency Group Users

Enter Your Choice : ( Between 0 and 4 ):
```

10. Enter **4** to select **Emergency Group Users** to Add an Emergency Admin User.

```
=========================================================
        Gateway Settings Menu
        Authentication - Emergency Admin Group Users
=========================================================

        0.   Back
        1.   List Users
        2.   Add User
        3.   Change Password
        4.   Remove User

Enter Your Choice : ( Between 0 and 4 ):
```

11. Enter **2** to Add User.
12. Enter the new emergency user name, full name, password and re-enter password.

```
=============================================================
        Gateway Settings Menu
        Emergency Group Users - Add user in Emergency group
=============================================================


Enter user name : emadmin

Enter user's full name : Emergency Administrator

Enter the password for emadmin:
Re-enter the password :
```

13. Type "**Y**" to confirm to the user.

```
=============================================================
        Gateway Settings Menu
        Emergency Group Users - Add user in Emergency group
=============================================================


Enter user name : emadmin

Enter user's full name : Emergency Administrator

Enter the password for emadmin:
Re-enter the password :

You entered:
User Name      : emadmin
User Full Name : Emergency Administrator

Confirm that you want to add this user ? <Y/N> :
```

14. Once user is added successfully, press **Enter**.

```
================================================================
        Gateway Settings Menu
        Emergency Group Users - Add user in Emergency group
================================================================


Enter user name : emadmin

Enter user's full name : Emergency Administrator

Enter the password for emadmin:
Re-enter the password :

You entered:
User Name      : emadmin
User Full Name : Emergency Administrator

Confirm that you want to add this user ? <Y/N> :        y


Successfully added user : emadmin

Press ENTER Key to continue....
```

15. Navigate back to Emergency Group Users and enter **1** to view the List of Emergency Admin Group Users.

```
=========================================================
        Gateway Settings Menu
        Authentication - Emergency Admin Group Users
=========================================================

        0.   Back
        1.   List Users
        2.   Add User
        3.   Change Password
        4.   Remove User

Enter Your Choice : ( Between 0 and 4 ):
```

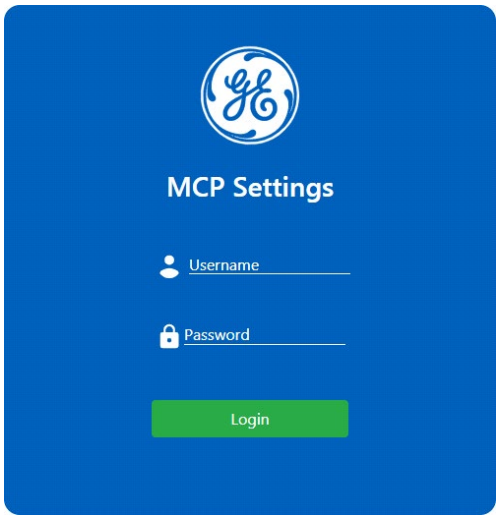
16. The menu displays the list of Added Emergency Admin Users.

```
================================================================
        Gateway Settings Menu
        Emergency Group Users - List of users in Emergency group
================================================================

   User Name                          UID    Full Name
=====================================================================

 1. emadmin                           1005   Emergency Administrator

           Press ENTER Key to continue....
```

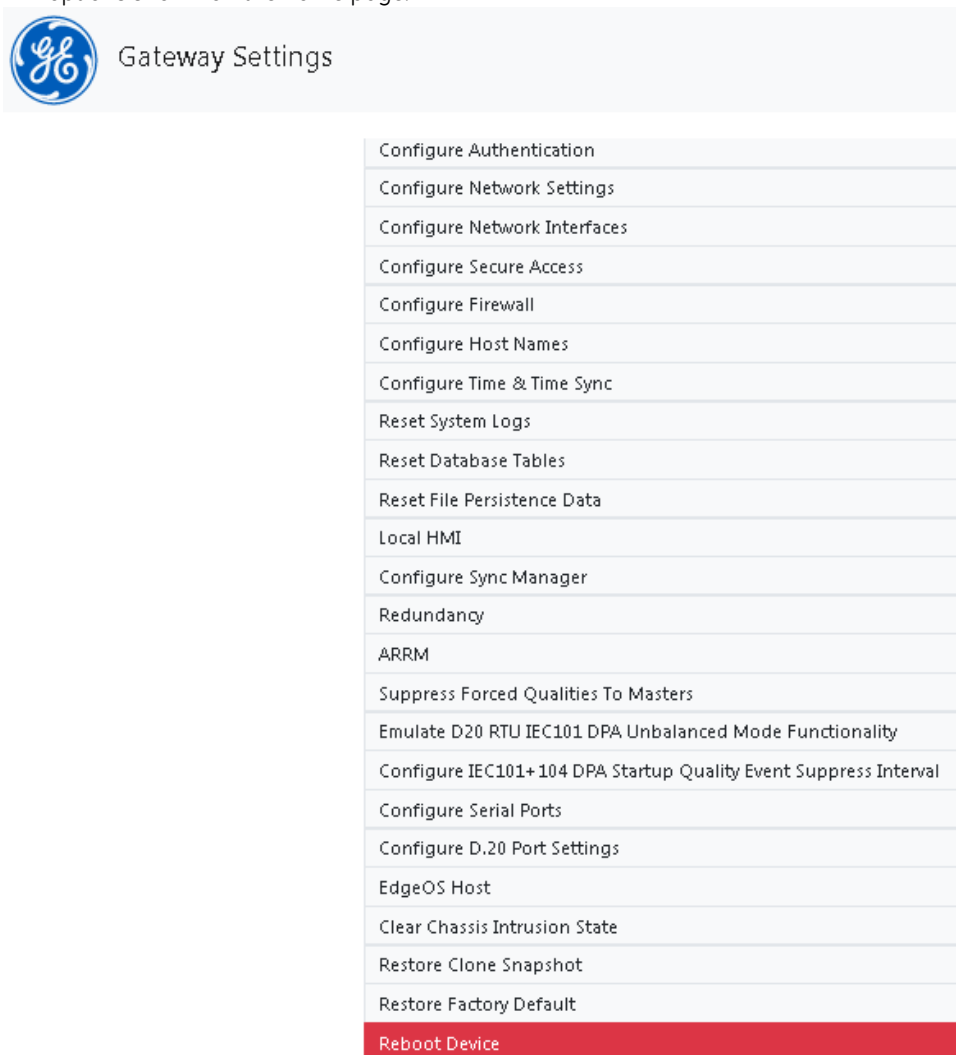
Using Web MCP Settings GUI

1. Login to MCP using local admin user authentication:
   - Entering their User Name.
   - Entering their Password.

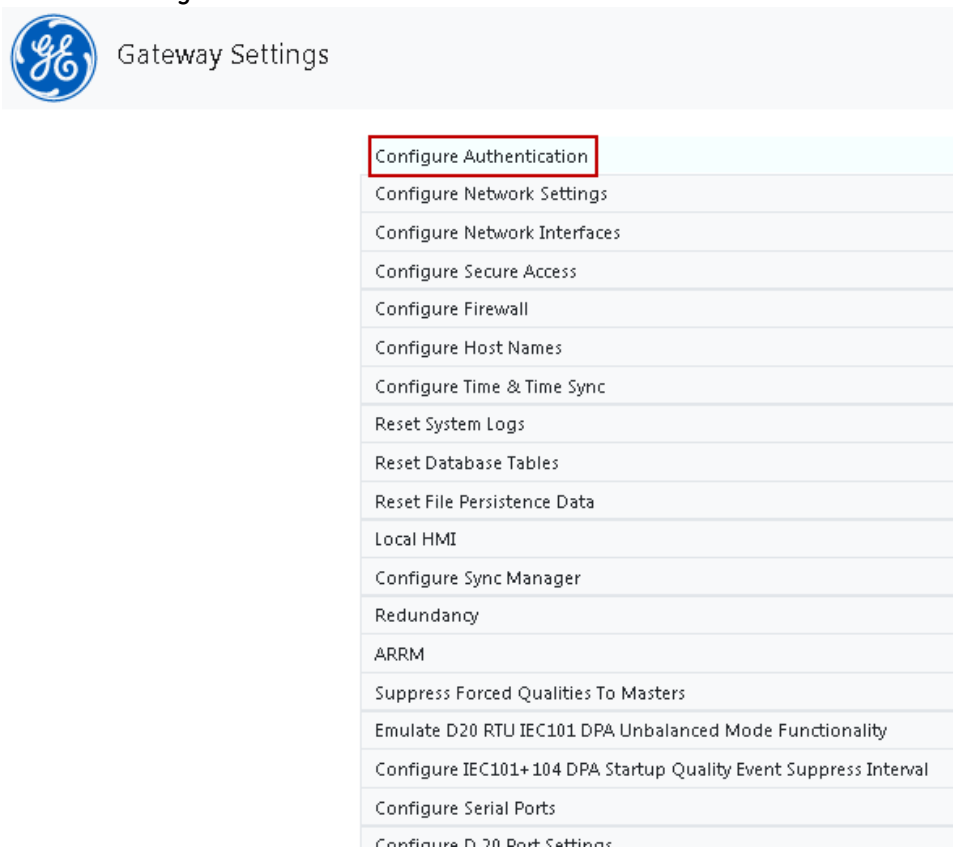
– Selecting Login to advance to the next screen and begin using the application.



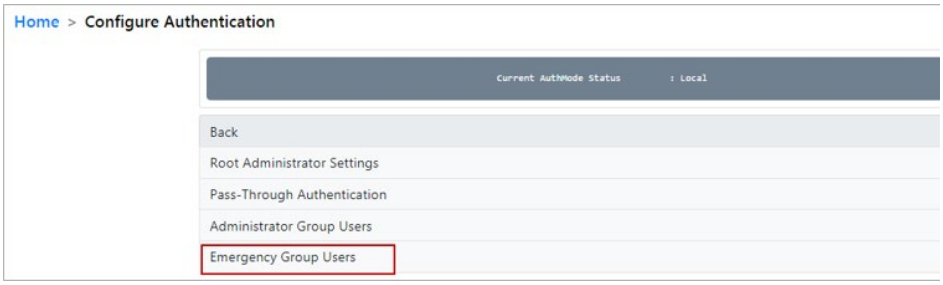
2. Once you have logged in to the MCP Settings, you can see a menu on the center and Logout option on the top right of the screen. To explore the MCP settings use the menu options shown on the home page:



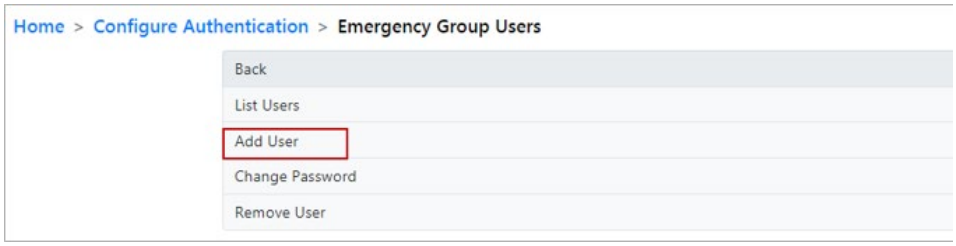
3. Select **Configure Authentication** from the main menu.



4. Click on **Emergency Group User** to add emergency User.

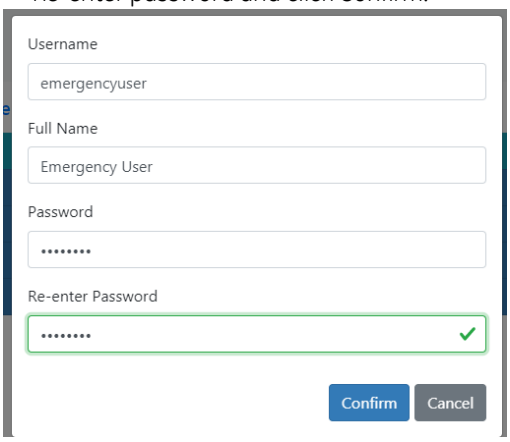


5. To add new emergency user click **Add User** tab.

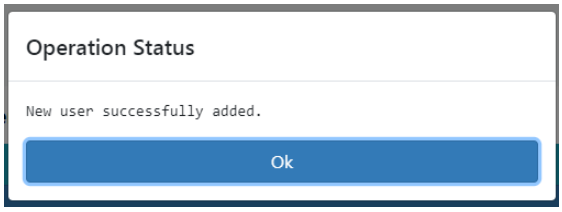


6. Enter the desired Emergency Group Username, conforming to the emergency group username rules as listed below:
   - Emergency Group Username must be between 2 and 31 characters.
   - Emergency Group Username must start with a lowercase alphabetical character.
   - Emergency Group Username must only contain [a-z][0-9][-,_] characters.

7. Enter the Full Name of the emergency group user.
8. Enter the Password, conforming to the password security rules as listed below:
   - Password must be between 8 and 199 characters in length
   - Password must contain:
     - 1 character from [a-z]
     - 1 character from [A-Z]
     - 1 digit from [0-9]
     - 1 special character from the set [$%@!&]
     - Re-enter password and click Confirm.



RESULT: Pop-up window appears showing the Operation Status: **New user successfully added**, click **OK**.



Retrieve LDAP Authentication Server information

Retrieve the following LDAP authentication server information from the IT / Network team of your organization or company:

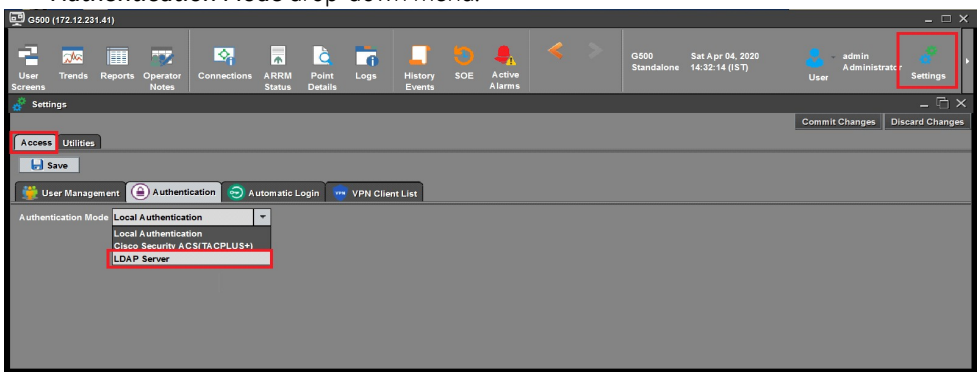
Name	Locate on LDAP Server
Primary Host Name	1. It is full name of your computer (LDAP Server). 2. Open properties of computer or server and view the **Full Name of Computer**
Primary Host IP Address	Open Server Manager in LDAP server and click on AD DS and note down the IP address of server.
Secondary Host Name	This is an optional field. It is full name of your secondary computer (LDAP Server). Open properties of computer or server and view the Full Name of Computer. If the Secondary LDAP Server is configured, MCP shall automatically switch to the secondary server when the primary server is not available.
Secondary Host IP Address	This is an optional field. Open Server Manager in secondary LDAP server and click on AD DS and note down the IP address of server.
LDAP Port	LDAP communication mechanism is TLS/SSL. Port-number = 389 for TLS communication Port-number = 636 for SSL communication

Name	Locate on LDAP Server
Base DN	1. It is Domain Name 2. Open properties of computer or server and view the Domain 3. If Domain is **GE.local** then Base DN will be "**dc=GE,DC=LOCAL**"
Bind User Name	Username of the bind user created in the LDAP server. Assume the user name to login LDAP machine or server is "**ldapbind**" and dc name is "**GE**" and dc type is "**local**" then the bind user name will be (in DN format) "**cn=ldapbind,cn=Users,dc=GE,dc=local**"
Bind Password	Password for the Bind User
Security Type	LDAP communication mechanism is TLS/SSL. Port-number = 389 for TLS communication Port-number = 636 for SSL communication
CA Certificate	Selected the imported CA certificate from the drop-down list.
Bind Time limit in Seconds	Use **30** as default value
User ID Attribute Map	User can use the default value "**sAMAccountName**"
Home Directory Attribute Map	User can use the default value "**unixHomeDirectory**"

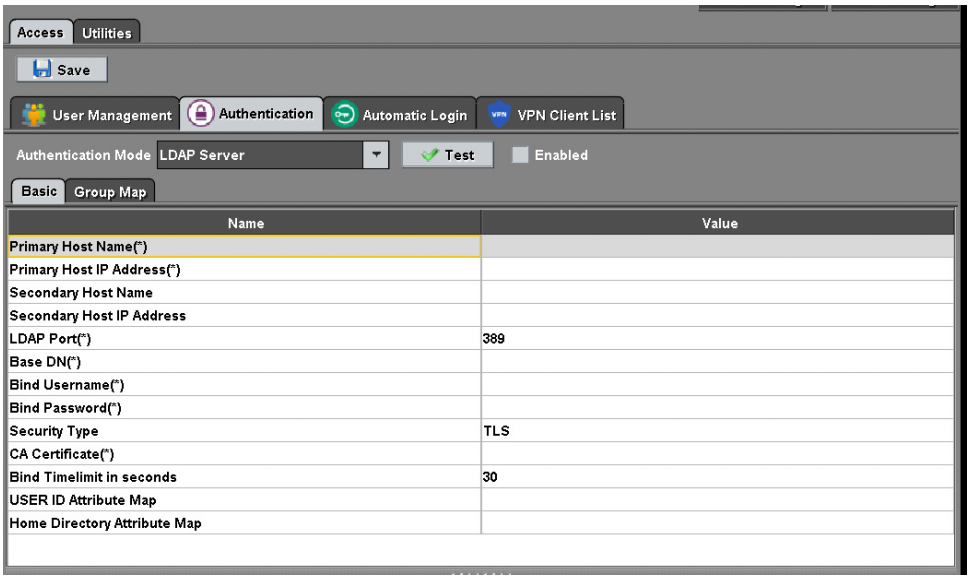
Procedure to configure LDAP on the MCP device

You can configure or change the authentication to LDAP Authentication mode by using HMI. In above section Retrieve LDAP Authentication Server information, we already had collected all the parameters that will be used here for configuration: To configure the LDAP in the MCP device:

1. Login in to MCP HMI with an administrator user name and password.
2. Go to **Settings > Access > Authentication** and select **LDAP server** from the **Authentication Mode** drop-down menu.



3. On selecting the LDAP Server authentication, LDAP configuration page will be opened as below:

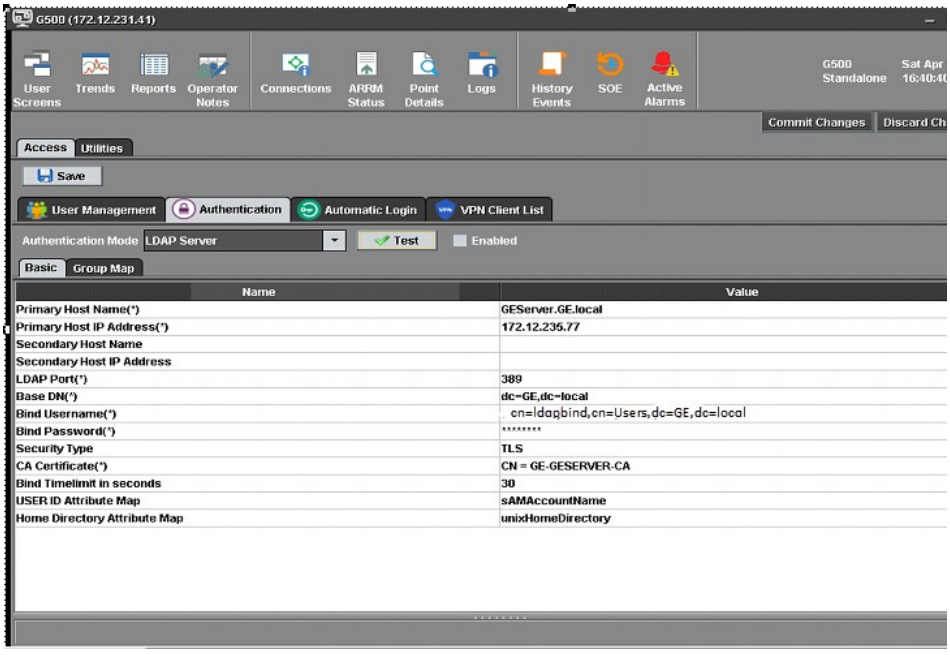


4. Input all the LDAP parameters we already had noted in the above section of this document. Follow the below table as an example to find all the parameter from LDAP server:

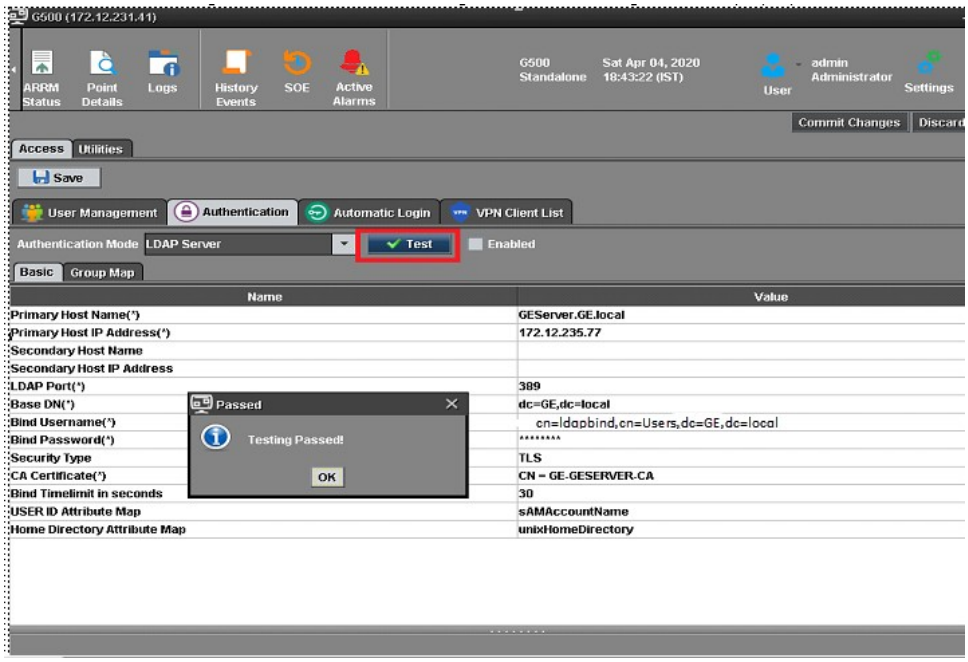
Name	Value	Locate on LDAP Server
Primary Host Name	GEServer.GE.local	1. It is full name of your computer (LDAP Server). 2. Open properties of computer or server and view the Full Name of Computer
Primary Host IP Address	172.12.235.77	Open Server Manager in LDAP server and click on AD DS and note down the IP address of server.
LDAP Port	389	LDAP communication mechanism is TLS/SSL. – Port-number = 389 for TLS communication – Port-number = 636 for SSL communication

Name	Value	Locate on LDAP Server
Base DN	dc=GE,dc=local	1. It is Domain Name 2. Open properties of computer or server and view the Domain 3. If Domain is GE.local then Base DN will be "dc=GE,DC=LOCAL"
Bind User Name	cn=ldapbind,cn=Users,dc=GE,dc=local	Assume the user name to login LDAP machine or server is "ldapbind" and dc name is "GE" and dc type is "local" then the bind user name will be (in DN format) "cn=ldapbind,cn=Users,dc=GE,dc=local"
Bind Password	Password	Enter the bind user password. (This is the password created for the Bind user in the LDAP Server in the earlier steps).
Security Type	TLS	LDAP communication mechanism is TLS/SSL. – Port-number = 389 for TLS communication – Port-number = 636 for SSL communication
CA Certificate	Certificate installed earlier	Select the INSTALLED CERTIFICATE appear on drop down list.
Bind Time limit in Seconds	30	Default Value
User ID Attribute Map	sAMAccountName	sAMAccountName is default value User can find it in user attribute tab in user properties of user in LDAP server
Home Directory Attribute Map	unixHomeDirectory	1. unixHomeDirectory is default value 2. User can find it in user attribute tab in user properties of user

3. Configure these LDAP parameters as shown below. Also, go to the drop-down menu of CA certificate and select the CA certificate for LDAP.

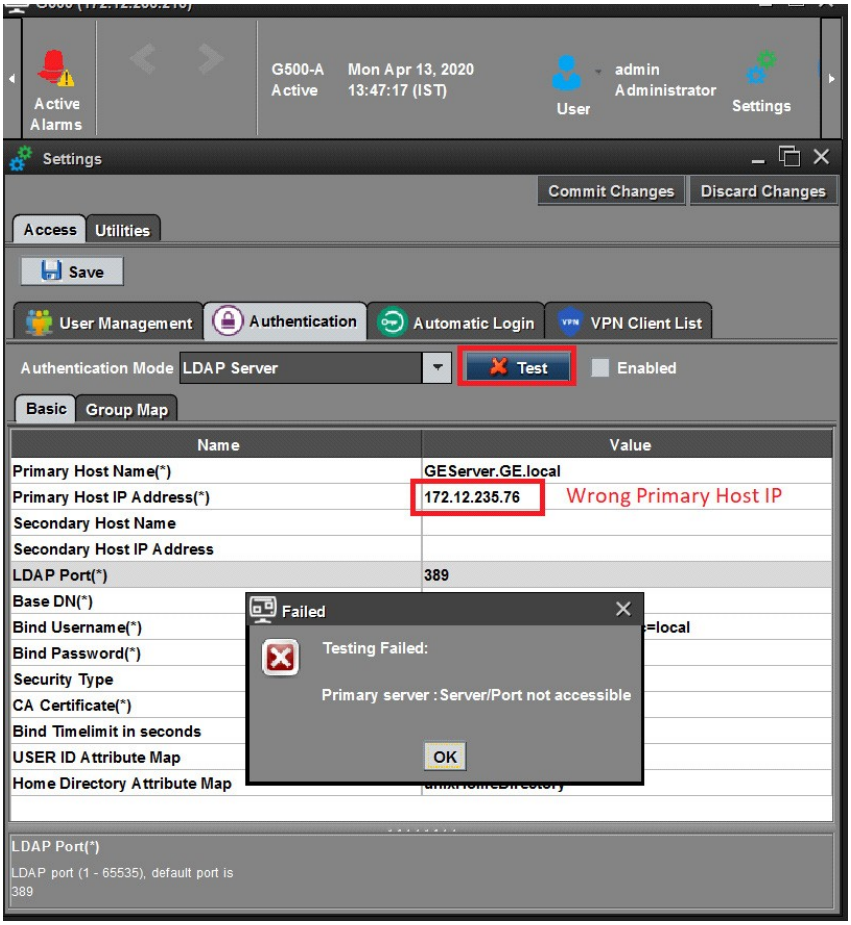


4. Click the **Test** button. It will validate the configuration and availability of LDAP server once the configuration verified, Testing Passed message will be popup. Click **OK**.



Result : The server connectivity is verified.

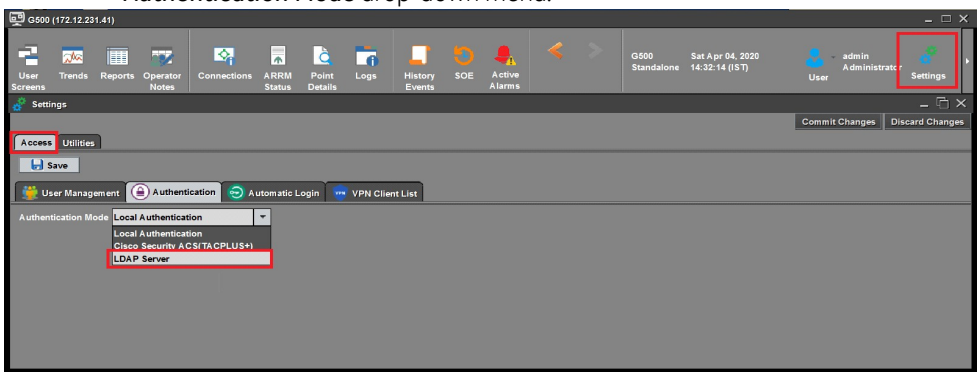
5. If user had input wrong parameter for any of the field and click on test button then it will popup message as "Testing Failed" as below:



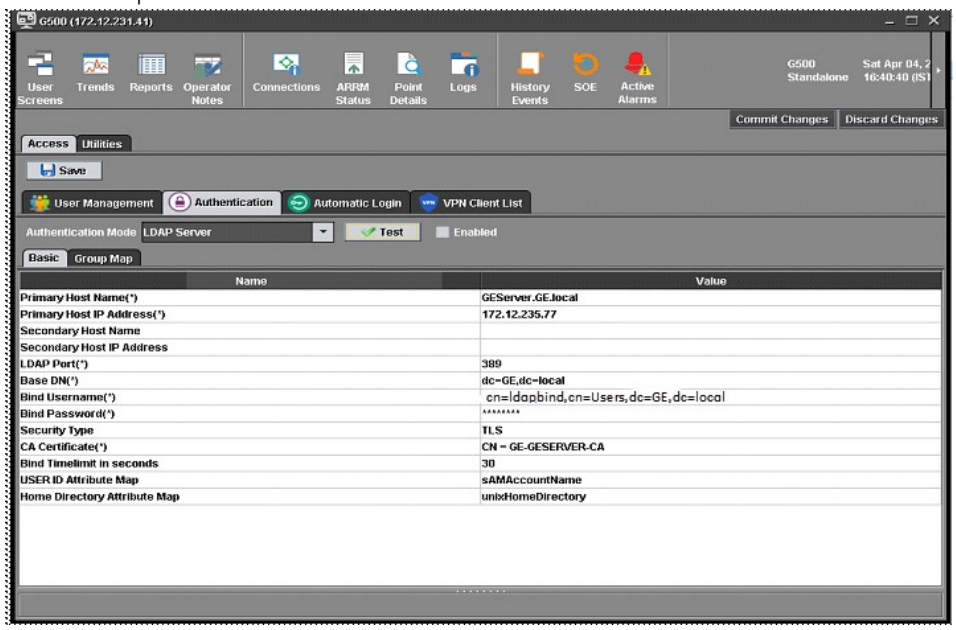
NOTE: Do not select the Enabled field.

6. Click on Save, it will save the configuration parameters, but still the authentication mode is local.
7. Till the above step LDAP configuration has been saved and tested successfully but still the authentication mode is Local. If user want to work with:
   7.1. If user want to work with Static mode of group mapping, then group mapping is not required in MCP. In this case user can directly enable and save the configuration as described in next steps. Static mode of group mapping is described in section Procedure for Static Group Mapping.
   7.2. If user want to work with Dynamic mode of group mapping, then group mapping needs to be done in MCP. Map the group in MCP by following the Procedure for Dynamic Group Mapping. After mapping all the groups in MCP proceed with next step.
8. Procedure to Configure Group Mapping on the MCP Device, if user want to work with dynamic user mapping approach then Group Mapping need to be done in MCP. Follow the below steps for Group Mapping in MCP. If you want to continue with static group mapping, skip the below steps from 8.1 to 8.8 and move to step 9:
   8.1. Procedure for Dynamic Group Mapping. It has been noted in an earlier example that the Distinguished Name (DN) of group "**G500Administrator**" is as "**cn=G500Administrator,cn=users,dc=GE,dc=local**".
   8.2. Login in to MCP HMI with an administrator user name and password.

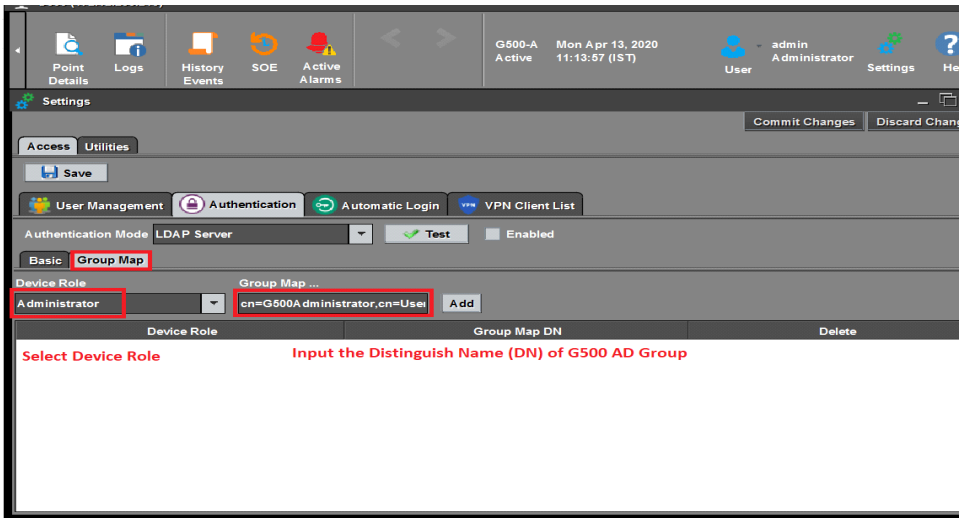
8.3. Go to **Settings > Access > Authentication** and select **LDAP server** from the **Authentication Mode** drop-down menu.



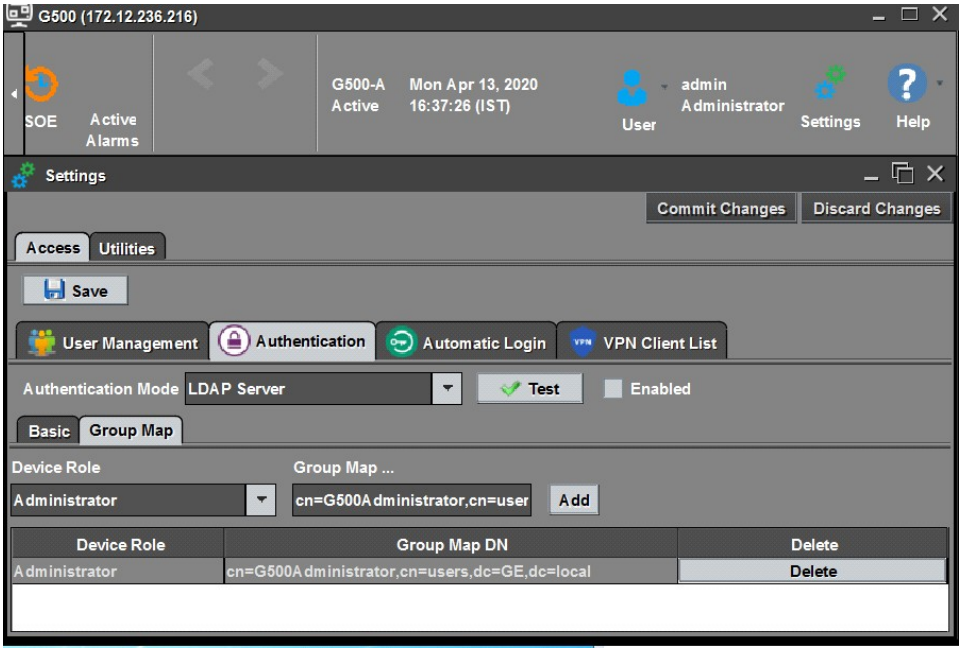
8.4. On selecting the LDAP Server authentication, LDAP configuration page will be opened as below:



8.5. Click on "**Group Map**" tab. Select the **Device Role** of Group from drop down and input the **DN** in Group Map field as shown in below (DN has been noted in step 8.3):



8.6. Click on "**Add**" button, it will add the group in MCP and that group members or users will be privileged with the selected Device Role. For example if User role is selected as Administrator for "**G500Administrator**" user group then users under G500Administrator group will have administrator privilege.

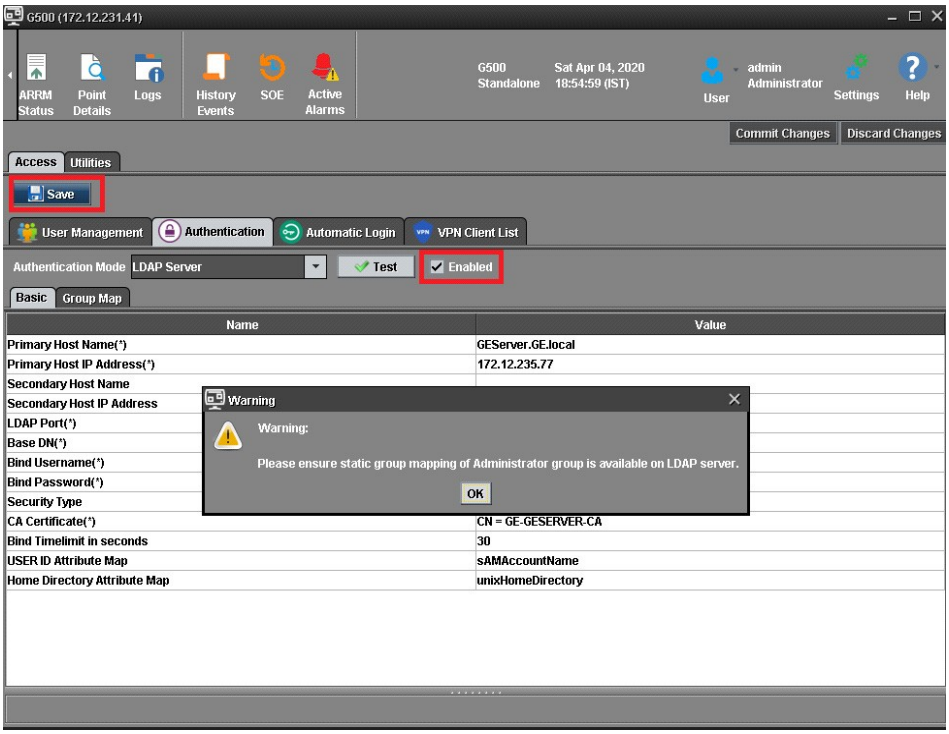


8.7. Similarly add different User groups like G500Operator for Operator privilege, G500Observer for Observer privilege, G500Supervisor for Supervisor privilege, G500Passthrough for Passthrough privilege.

8.8. After adding the user group click on Save to save the configuration.
RESULT: Group Mapping has been done successfully.

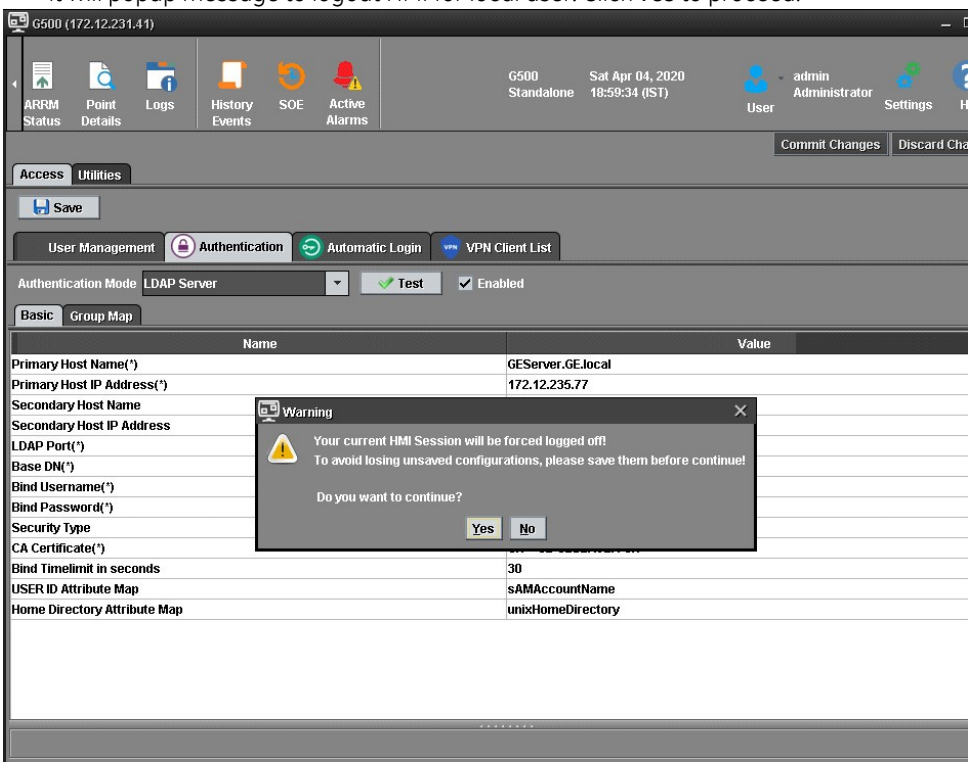
9. **Select the Enabled field and Save**, This step should be done only after completion of Static/ Dynamic Group Mapping it will save this configuration parameters and forcefully logout the HMI for local user and LDAP authentication will be enabled for MCP. Now user can login to MCP by using only LDAP authentication.
NOTE: Select the Enabled field and Save, this will switch to Remote Authentication

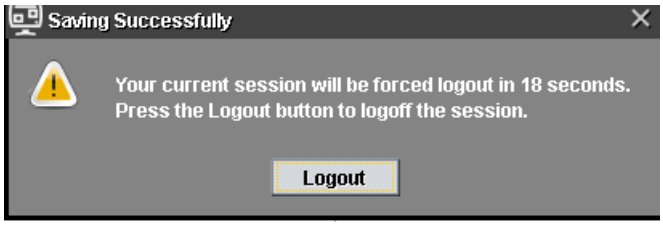
mode.



WARNING: Save with Enabled checked will switch to Remote Authentication immediately!

10. This warning is for the static user should be available to login MCP, click **OK** then again it will popup message to logout HMI for local user. Click **Yes** to proceed:





Result: Now LDAP Authentication mode is successfully enabled, user is required to use LDAP credentials, for login to HMI, DSAS and SSH sessions to MCP.

Configuring the MCP devices for Centralized LDAP Authentication using Open LDAP Server

Appendix A: Troubleshooting

If you encounter issues while testing the operation of the LDAP server configuration, refer to the following listed errors and the recommended responses. When you click the Test Button, if a particular field is configured improperly, the corresponding message appears on the HMI.
The exact error messages may refer to MCP, G500 or G100 – the meaning is identical.

See sections:

- LDAP error messages
- LDAP Certificate error messages

LDAP error messages

Error Message	Response
Host not reachable	Ensure LDAP server was accessible in the network.
	Ensure LDAP server was not shutdown.
unable to access ldap port	Ensure LDAP server was using the specified port for LDAP protocol communication.
Invalid binddn	Ensure mentioned bind user dn (distinguished name) was available in the mentioned domain on the LDAP server.
Invalid bind user credentials	Ensure bind user dn (distinguished name) mentioned in the MCP device LDAP server configuration was correct.
	Ensure bind user password entered was correct in the MCP device LDAP server configuration.
Hostname mismatch with server certificate	Ensure LDAP server host name entered in the MCP device LDAP server configuration was matching with the LDAP server certificate subject name.
Server/Port not accessible	Ensure LDAP server was accessible in the network.
	Ensure LDAP server was not shutdown.
	Ensure LDAP server was using the specified port for LDAP protocol communication.
Invalid Host Name. Full Qualified Domain Name (FQDN) has invalid characters	Ensure Primary Host Name is configured in MCP device LDAP server configuration.

Error Message	Response
Invalid Host IP Address	Ensure Primary Host IP Address configured in MCP device LDAP server configuration is correct.
Failed to connect to Primary Host	Ensure LDAP Server is accessible in the network.
	Ensure Primary Host Name configured in MCP device LDAP server configuration is correct.
	Ensure Base DN configured in MCP device LDAP server configuration is correct.
	Ensure Bind User credentials (Bind Username and Bind Password) configured in MCP device LDAP server configuration are correct.
Primary Server :Server/ Port not accessible	Ensure LDAP Server is not shutdown.
	Ensure Primary Host IP Address configured in MCP device LDAP server configuration is correct.
Configuration Timeout, please try again later	Ensure LDAP server was using the specified port for LDAP protocol communication.
Invalid User ID Attribute Map	Ensure User ID Attribute Map defined in LDAP Server is configured in MCP device LDAP server configuration.
Invalid HomeDirectory Attribute Map	Ensure HomeDirectory Attribute Map defined in LDAP server is configured in MCP device LDAP server configuration.
Connected to secondary Host, but failed to connect to primary Host	Ensure Primary Host Name and Primary Host IP Address configured in MCP device LDAP server configuration are correct.
Failed to connect to both primary and secondary Hosts	Ensure Primary Host Name and Secondary Host Name configured in MCP device LDAP server configuration are correct.
	Ensure Primary Host IP Address and Secondary Host IP Address configured in MCP device LDAP server configuration are correct.
	Ensure Base DN configured in MCP device LDAP server configuration is correct.
	Ensure Bind User credentials (Bind Username and Bind Password) configured in MCP device LDAP server configuration are correct.
Please add Emergency User before switching to LDAP/TACACS Authentication	Ensure at least one emergency admin group user is configured before switching to LDAP/TACACS Authentication.
The current Authentication Mode has been enabled. You cannot disable it unless switching to a different Authentication Mode	Current Authentication Mode is LDAP. Ensure to disable (Enabled checkbox unchecked) only when switching to a Authentication Mode other than LDAP.

LDAP Certificate error messages

Error Message	Response
List of trusted certificates is not complete	The issuer certificate of a looked up certificate could not be found. This normally means the list of trusted certificates installed on the MCP device or certificate list from LDAP server was not complete.
Unable to decrypt certificate's signature	The certificate signature could not be decrypted. This means that the actual signature value could not be determined rather than it not matching the expected value, this is only meaningful for RSA keys.
unable to decode issuer public key	The public key in the certificate SubjectPublicKeyInfo of MCP device server could not be read.
certificate signature failure	The signature of the installed certificate on MCP device server certificate was invalid.

Error Message	Response
certificate is not yet valid	MCP device time might be backward w.r.to certificate valid time.
	The certificate is not yet valid: the not Before date is after the current time.
certificate has expired	CA certificate installed on MCP device got expired w.r.to LDAP server.
	MCP device time might be forward w.r.to certificate valid time.
	The certificate has expired: that is the notAfter date is before the current time.
format error in certificate's notBefore field	The certificate notBefore field contains an invalid time.
format error in certificate's notAfter field	The certificate notAfter field contains an invalid time.
Self-signed certificate cannot be found in the list of trusted certificates.	The passed certificate is self-signed and the same certificate cannot be found in the list of trusted certificates.
self-signed certificate in certificate chain	Ensure Installed a trusted CA signed primary SSL certificate and an intermediate certificate.
	Verify that the Root CA is not included in the certificate chain (as this is almost always self-signed).
unable to get local issuer certificate	This error code is thrown when a local certificate path is not found during the certificate check.
	LDAP server certificate's issuer certificate was not found, after looking in both the chain provided by the LDAP server and in the local trusted storage. This usually means the peer chain was missing or incomplete.
unable to verify the first certificate	The primary certificate (the one you purchase from a vendor) cannot establish the chain of trust between itself and the Root certificate stored locally. Usually installing the intermediate certificates fixes this.
certificate chain too long	The certificate chain length is greater than the supplied maximum depth.
	The LDAP server certificate's chain length exceeded the limit set locally by sslverifydepth or SSL Verify Depth. The chain length (depth) is the number of certificates beyond the leaf (client or server) certificate itself.
	a chain of length 1 is a leaf certificate plus its issuer certificate.
invalid CA certificate	A CA certificate is invalid. Either it is not a CA or its extensions are not consistent with the supplied purpose.
path length constraint exceeded	The basicConstraints path length parameter has been exceeded for certificate.
invalid or inconsistent certificate extension	invalid or inconsistent certificate extension
Hostname mismatch	Ensure LDAP server host name entered in the MCP device LDAP server configuration was matching with the LDAP server certificate subject name.
Certificate directory empty	No certificates installed over to the MCP device.

Configuring the MCP devices for Centralized LDAP Authentication using Open LDAP Server

Appendix B: List of Acronyms

Acronym Definitions

This Appendix lists and defines the acronyms used in this manual.

Table 1: Acronym list

Acronym	Definition
CS	Certificate Services
DS	Domain Services
CA	Certificate Authority
MCP	MCP Substation Gateway
mcpcfg	Local configuration utility
DN	Domain Name
DNS	Domain Name System
FQDN	Full Qualified Domain Name
GE	General Electric
HMI	Human Machine Interface (also called Graphical User Interface – GUI)
IP	Internet Protocol
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
NIS	Network Information Service
NTDS	TechNet Directory Services
PC	Personal Computer
PEM	Privacy Enhanced Mail
PKCS	Public-Key Cryptography Standards, published by RSA Laboratories
SCADA	Supervisory Control and Data Acquisition
SCP	Session Control Protocol
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm

Acronym	Definition
SSL	Secure Sockets Layer
TLS	Transport Layer Security
USB	Universal Serial Bus
XCA	X Certificate and Key management

Configuring the MCP devices for Centralized LDAP Authentication using Open LDAP Server

Appendix C: Revision History

This appendix provides the document revision history.

Revision history

Version	Revision	Date	Change Description
1.00	0	April 27, 2020	Initial release.
2.00	0	April 26, 2021	Updated for MCP family.

GE

Grid Solutions

Configuring the Multilin™ MCP for Centralized LDAP Authentication using 389 Directory Server

Installation and Configuration Guide

SWM0113
Version 2.00 Revision 0

imagination at work

GE Information

Copyright Notice

© 2021, General Electric Company. All rights reserved.

The information contained in this online publication is the exclusive property of General Electric Company, except as otherwise indicated. You may view, copy and print documents and graphics incorporated in this online publication (the "Documents") subject to the following: (1) the Documents may be used solely for personal, informational, non-commercial purposes; (2) the Documents may not be modified or altered in any way; and (3) General Electric Company withholds permission for making the Documents or any portion thereof accessible via the internet. Except as expressly provided herein, you may not use, copy, print, display, reproduce, publish, license, post, transmit or distribute the Documents in whole or in part without the prior written permission of General Electric Company.

The information contained in this online publication is proprietary and subject to change without notice. The software described in this online publication is supplied under license and may be used or copied only in accordance with the terms of such license.

Trademark Notices

GE and are trademarks and service marks of General Electric Company.

* Trademarks of General Electric Company.

Tera Term is a registered trademark of T. Teranishi, Incorporated. IEC is a registered trademark of Commission Electrotechnique Internationale. IEEE is a registered trademark of the Institute of Electrical and Electronics Engineers, Inc. Internet Explorer, Microsoft, and Windows are registered trademarks of Microsoft Corporation.

Other company or product names mentioned in this document may be trademarks or registered trademarks of their respective companies.

This printed manual is recyclable.
Please return for recycling where facilities exist.

Configuring the MCP devices for Centralized LDAP Authentication using 389 Directory Server

Table of contents

PRODUCT SUPPORT
- Access the GE Grid Solutions web site. 5
- Search GE Grid Solutions technical support library 5
- Product support 6
- GE Grid Solutions address 6

ABOUT THIS DOCUMENT
- Purpose 7
- Intended audience 7
- Additional documentation 7

389 DIRECTORY SERVER
- Creating and installing the 389 directory server 9
  - 389 directory server installation 9
  - Update IP address and host name 11
  - Configuring the 389 DS 11
  - 389 Directory Server groups and users Configuration 16
  - Group Mapping 19
- Generating certificates 21
  - Generating certificates from server 21
  - Generate the CA 22
  - Generate and sign the server certificate 23
  - Install the certificates and enable SSL 25
- Retrieving certificates for 389 DS server 30

CONFIGURE THE LDAP ON MCP DEVICES
- Installing CA Certificates on the MCP device 31
  - CA Certificate transfer procedure from PC to MCP 32
  - CA Certificate Installation procedure 35
- Configuring LDAP on the MCP device 40
  - Prerequisites to configuring LDAP on MCP device 41
  - Procedure to configure LDAP on the MCP device 51

TROUBLESHOOTING
- LDAP error messages 59

LDAP Certificate error messages 60

LIST OF ACRONYMS Acronym Definitions 63

REVISION HISTORY Revision history 65

Configuring the MCP devices for Centralized LDAP Authentication using 389 Directory Server

Product Support

If you need help with any aspect of your MCP product, you can:

- Access the Multilin^{TM} MCP devices Web site
- Search the GE Technical Support library
- Contact Product Support

Access the GE Grid Solutions web site

The MCP Web site provides fast access to technical information, such as manuals and knowledge base topics.
Visit us on the Web at: http://www.gegridsolutions.com

Search GE Grid Solutions technical support library

This site serves as a document repository for post-sales requests. To get access to the Technical Support Web site, go to: http://sc.ge.com/*SASTechSupport

Product support

For help with any aspect of your GE Grid Solutions product, please contact our supportteam, 24/7, as follows:

Region	E-mail	Telephone
Global Contact Centre	ga.support@ge.com	+44 1785 250070
Central and East Asia and Pacific	ga.supportCEAP@ge.com	+61 414 730 964
India	ga.supportIND@ge.com	+91 44 22648000
Middle East, North Africa and Turkey	ga.supportMENAT@ge.com	+971 42929467
Europe, Russia, CIS and Sub-Saharan Africa	ga.supportERCIS@ge.com	+34 94 4858854
North America	ga.supportNAM@ge.com	+1 877 605 6777
Latin America	ga.supportLAM@ge.com	+55 11 36187308

Configuring the MCP devices for Centralized LDAP Authentication using 389 Directory Server

About this Document

Purpose

This manual describes how to install and configure the 389 Directory Server and Multilin™ MCP device for Centralized LDAP Authentication.

This document applies to the MCP family (G100/G500) unless otherwise indicated.

Screen captures may show G500 in some areas, however the workflow applies to products in the MCP family (G100/G500).

Intended audience

This manual is a helpful resource for utility personnel and system engineers who are implementing LDAP on Multilin™ MCP device in an overall substation automation system.

Additional documentation

For the most current version of the Configuring 389 Directory Server and Multilin™ MCP for Centralized LDAP Authentication - Manual, please download a copy from GE Grid Solutions web site.

For information on fully installing, configuring, monitoring and testing a MCP device, refer to the:

- G500 Substation Gateway Instruction Manual, 994-0152
- G100 Substation Gateway Instruction Manual, 994-0155
- MCP Substation Gateway Software Configuration Guide, SWM0101

Configuring the MCP devices for Centralized LDAP Authentication using 389 Directory Server

Chapter 1: 389 Directory Server

The 389 directory server is an LDAP (Lightweight directory access protocol) server developed by Red Hat.

See sections:

- Creating and installing the 389 directory server
- Generating certificates
- Retrieving certificates for 389 DS server

Creating and installing the 389 directory server

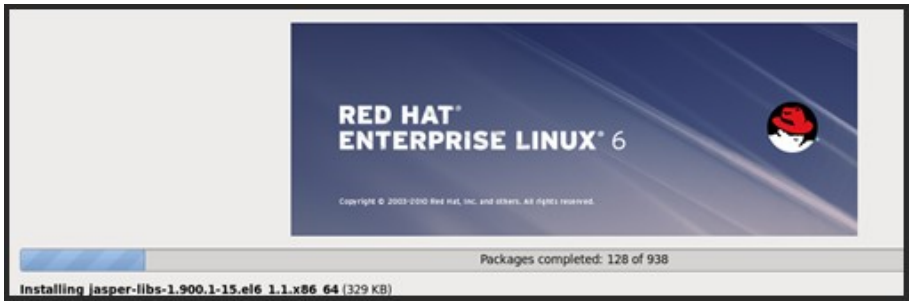
This section describes how to install and configure the 389 Directory Server on a RHEL operating system.

389 directory server installation

To install and configure a 389 Directory Server on a RHEL system:

1. Install RHEL 6.5 VM.
2. Type in the **username** and **password**.

   Result: The installation procedure begins.



3. After successful installation, login with root and execute the below command

   Install package:

   [root@dshost ~]# yum install 389-ds-base

Result: The below messages appear.

```
Transaction Summary
================================================================================
===
Install      10 Package(s)

Total download size: 3.3 M
Installed size: 11 M
Is this ok [y/N]: y
Downloading Packages:
--------------------------------------------------------------------------------
---
Total                                              33 MB/s | 3.3 MB     00:00
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing : svrcore-4.0.4-5.1.el6.x86_64                                1/10
  Installing : 389-ds-base-libs-1.2.11.15-29.el6.x86_64                    2/
10
  Installing : openldap-clients-2.4.23-32.el6_4.1.x86_64                   3/
10
  Installing : setools-libs-3.3.7-4.el6.x86_64                            4/10
  Installing : setools-libs-python-3.3.7-4.el6.x86_64                      5/
10
  Installing : perl-Mozilla-LDAP-1.5.3-4.el6.x86_64                        6/
10
  Installing : libsemanage-python-2.0.43-4.2.el6.x86_64                    7/
10
  Installing : audit-libs-python-2.2-2.el6.x86_64                          8/
10
  Installing : policycoreutils-python-2.0.83-19.39.el6.x86_64              9/
10
  Installing : 389-ds-base-1.2.11.15-29.el6.x86_64                        10/
10

Verifying : audit-libs-python-2.2-2.el6.x86_64   1/10
Verifying  : svrcore-4.0.4-5.1.el6.x86_64                                2/10
Verifying  : setools-libs-python-3.3.7-4.el6.x86_64                      3/10
Verifying  : 389-ds-base-libs-1.2.11.15-29.el6.x86_64                    4/10
Verifying  : 389-ds-base-1.2.11.15-29.el6.x86_64                         5/10
Verifying  : libsemanage-python-2.0.43-4.2.el6.x86_64                    6/10
Verifying  : policycoreutils-python-2.0.83-19.39.el6.x86_64              7/10
Verifying  : perl-Mozilla-LDAP-1.5.3-4.el6.x86_64                        8/10
Verifying  : setools-libs-3.3.7-4.el6.x86_64                             9/10
Verifying  : openldap-clients-2.4.23-32.el6_4.1.x86_64                  10/10

Installed:
  389-ds-base.x86_64 0:1.2.11.15-29.el6
Dependency Installed:
389-ds-base-libs.x86_64 0:1.2.11.15-29.el6
audit-libs-python.x86_64 0:2.2-2.el6
libsemanage-python.x86_64 0:2.0.43-4.2.el6
openldap-clients.x86_64 0:2.4.23-32.el6_4.1
  perl-Mozilla-LDAP.x86_64 0:1.5.3-4.el6          policycoreutils-
python.x86_64 0:2.0.83-19.39.el6    setools-libs.x86_64 0:3.3.7-4.el6
setools-libs-python.x86_64 0:3.3.7-4.el6
  svrcore.x86_64 0:4.0.4-5.1.el6

Complete!
[root@dshost ~]#
```

4. Download following pre-requisite packages:
   - idm-console-framework-1.1.7-2.el6.noarch.rpm
   - 389-adminutil-1.1.19-1.fc19.x86_64.rpm
   - 389-admin-1.1.35-1.fc19.x86_64.rpm

- 389-admin-console-1.1.8-1.el6.noarch.rpm
- 389-console-1.1.7-1.el6.noarch.rpm
- 389-ds-console-1.2.6-1.el6.noarch.rpm

from:

https://dl.fedoraproject.org/pub/epel/6/x86_64/
and
http://rpmfind.net/linux

5. Install the packages in the following manner;

[root@dshost ldap]# yum install /tmp/ldap/idm-console-framework-1.1.7-2.el6.noarch.rpm
[root@dshost ldap]# yum install /tmp/389-adminutil-1.1.19-1.el6.x86_64.rpm
[root@dshost ldap]# yum install /tmp/389-admin-1.1.35-1.el6.x86_64.rpm
[root@dshost ldap]# yum install /tmp/ldap/389-console-1.1.7-1.el6.noarch.rpm
[root@dshost ldap]# yuminstall /tmp/ldap/389-ds-console-1.2.6-1.el6.noarch.rpm
[root@dshost ldap]# yum install /tmp/ldap/389-console-1.1.7-1.el6.noarch.rpm

Update IP address and host name

To update the IP address and host name:

1. Type in command: **# vi /etc/hosts**
2. Enter the IP address and host name.

Configuring the 389 DS

To configure the 389 Directory Server

1. Execute command: **[root@dshost ldap]# setup-ds-admin.pl**

   Result: The below messages appear.

```
==============================================================================
This program will set up the 389 Directory and Administration Servers.

It is recommended that you have "root" privilege to set up the software.
Tips for using this program:
  - Press "Enter" to choose the default and go to the next screen
  - Type "Control-B" then "Enter" to go back to the previous screen
  - Type "Control-C" to cancel the setup program

Would you like to continue with set up? [yes]:
```

2. Enter **Yes** to specify that you want to continue the set up.

   Result: The below messages appear.

```
==============================================================================
Your system has been scanned for potential problems, missing patches,etc. The
following output is a report of the items found that need to be addressedbefore
running this software in a production environment.

389 Directory Server system tuning analysis version 23-FEBRUARY-2012.

NOTICE : System is x86_64-unknown-linux2.6.32-431.el6.x86_64 (1 processor).
NOTICE : The net.ipv4.tcp_keepalive_time is set to 7200000 milliseconds
(120 minutes). This may cause temporary server congestion from lost client
connections.
WARNING: There are only 1024 file descriptors (soft limit) available, which
limit the number of simultaneous connections.

WARNING  : The warning messages above should be reviewed before proceeding.
```

```
Would you like to continue? [no]:
```

3. Enter **Yes** to specify that you want to continue the set up.

   Result: The below messages appear.

```
==========================================================================
Choose a setup type:
    1. Express - Allows you to quickly set up the servers using the most
common options and pre-defined defaults. Useful for quick evaluation of the
products.
   2. Typical - Allows you to specify common defaults and options.
     3. Custom - Allows you to specify more advanced options. This is
recommended for experienced server administrators only.
To accept the default shown in brackets, press the Enter key.

Choose a setup type [2]: 2
```

4. Enter **2** to select the Typical setup.

   Result: The below messages appear.

```
==========================================================================
Enter the fully qualified domain name of the computer on which you're
setting up server software. Using the form <hostname>.<domainname>
Example: eros.example.com.

To accept the default shown in brackets, press the Enter key.

Warning: This step may take a few minutes if your DNS servers can not be
reached or if DNS is not configured correctly.  If you would rather not wait,
hit Ctrl-C and run this program again with the following command line option
to specify the hostname:
General.FullMachineName=your.hostname.domain.name
Computer name [dshost.project.com]:

WARNING: There are problems with the hostname. Hostname 'dshost.project.com'
is valid, but none of the IP addresses resolve back to dshost.project.com
- address 3.185.121.199 resolves to host dshost

Please check the spelling of the hostname and/or your network configuration.
If you proceed with this hostname, you may encounter problems.

Do you want to proceed with hostname 'dshost.project.com'? [no]:
```

5. Enter **Yes** to proceed with hostname 'dshost.project.com'.
6. Execute command:

   [root@dshost ldap]# setup-ds-admin.pl
   General.FullMachineName=dshost.project.com

   Result: The below messages appear.

```
==========================================================================
This program will set up the 389 Directory and Administration Servers.

It is recommended that you have "root" privilege to set up the software.
Tips for using this program:
  - Press "Enter" to choose the default and go to the next screen
  - Type "Control-B" then "Enter" to go back to the previous screen
  - Type "Control-C" to cancel the setup program

Would you like to continue with set up? [yes]:
```

7. Enter **Yes** to continue.

   Result: The below messages appear.

```
==========================================================================
Your system has been scanned for potential problems, missing patches, etc.
The following output is a report of the items found that need to be addressed
before running this software in a production environment.
```

```
389 Directory Server system tuning analysis version 23-FEBRUARY-2012.

NOTICE : System is x86_64-unknown-linux2.6.32-431.el6.x86_64 (1 processor).

NOTICE : The net.ipv4.tcp_keepalive_time is set to 7200000 milliseconds (120
minutes). This may cause temporary server congestion from lost client
connections.

WARNING: There are only 1024 file descriptors (soft limit) available, which
limit the number of simultaneous connections.

WARNING : The warning messages above should be reviewed before proceeding.

Would you like to continue? [no]:
```

8. Enter **Yes** to continue.

   Result: The below messages appear.

```
==========================================================================
Choose a setup type:
   1. Express
      Allows you to quickly set up the servers using the most common options
and pre-defined defaults. Useful for quick evaluation of the products.
   2. Typical - Allows you to specify common defaults and options.
     3. Custom - Allows you to specify more advanced options. This is
recommended for experienced server administrators only.
To accept the default shown in brackets, press the Enter key.
Choose a setup type [2]:
```

9. Enter **2** to choose the Typical setup type.

   Result: The below messages appear.

```
==========================================================================
Enter the fully qualified domain name of the computer on which you're
setting up server software. Using the form <hostname>.<domainname>
Example: eros.example.com.

To accept the default shown in brackets, press the Enter key.

Warning: This step may take a few minutes if your DNS servers can not be
reached or if DNS is not configured correctly.  If you would rather not wait,
hit Ctrl-C and run this program again with the following command line option
to specify the hostname:
General.FullMachineName=your.hostname.domain.name

Computer name [dshost.project.com]:

WARNING: There are problems with the hostname. Hostname 'dshost.project.com'
is valid, but none of the IP addresses resolve back to dshost.project.com
- address 3.185.121.199 resolves to host dshost

Please check the spelling of the hostname and/or your network configuration.
If you proceed with this hostname, you may encounter problems.

Do you want to proceed with hostname 'dshost.project.com'? [no]:
Computer name [dshost.project.com]:

WARNING: There are problems with the hostname. Hostname 'dshost.project.com'
is valid, but none of the IP addresses resolve back to dshost.project.com
- address 3.185.121.199 resolves to host dshost

Please check the spelling of the hostname and/or your network configuration.
If you proceed with this hostname, you may encounter problems.

Do you want to proceed with hostname 'dshost.project.com'? [no]:
```

10. Enter **Yes** to proceed with hostname 'dshost.project.com'.

    Result: The below messages appear.

```
==========================================================================
The servers must run as a specific user in a specific group. It is strongly
recommended that this user should have no privileges on the computer (i.e. a
non-root user). The setup procedure will give this user/group somepermissions
in specific paths/files to perform server-specific operations.

If you have not yet created a user and group for the servers, create this
user and group using your native operating system utilities.

System User [nobody]: ldapadmin
System Group [nobody]: ldapadmin
```

ldapadmin is a user created in this OS.

```
==========================================================================
Server information is stored in the configuration directory server. This
information is used by the console and administration server to configure and
manage your servers. If you have already set up a configuration directory
server, you should register any servers you set up or create withthe
configuration server. To do so, the following information about the
configuration server is required: the fully qualified host name of the form
<hostname>.<domainname>(e.g. hostname.example.com), the port number (default
389), the suffix, the DN and password of a user having permission to write
the configuration information, usually the configuration directory
administrator, and if you are using security (TLS/SSL). If you are using
TLS/SSL, specify the TLS/SSL (LDAPS) port number (default 636) instead of the
regular LDAP port number, and provide the CA certificate (in PEM/ASCII
format).

If you do not yet have a configuration directory server, enter 'No' to be
prompted to set up one.

Do you want to register this software with an existing configuration directory
server? [no]:
```

11. Enter **No** to specify that this software is not to be registered with an existing configuration directory server.

    Result: The below messages appear.

```
==========================================================================
Please enter the administrator ID for the configuration directory server.
This is the ID typically used to log in to the console. You will also be
prompted for the password.

Configuration directory server
administrator ID [admin]:
Password:
Password (confirm):
```

12. Enter the administrator ID and password created initially.

    Result: The below messages appear.

```
==========================================================================
The information stored in the configuration directory server can be separated
into different Administration Domains. If you are managing multiple software
releases at the same time, or managing information about multiple domains,
you may use the Administration Domain to keep them separate.

If you are not using administrative domains, press Enter to select the
default. Otherwise, enter some descriptive, unique name for the
administration domain, such as the name of the organization responsible for
managing the domain.
```

```
Administration Domain [project.com]:
```

13. Enter the domain name.

    Result: The below messages appear.

```
==========================================================================
The standard directory server network port number is 389. However, if you are
not logged as the superuser, or port 389 is in use, the default value will
be a random unused port number greater than 1024. If you want to use port
389, make sure that you are logged in as the superuser, that port 389 isnot in
use.

Directory server network port [389]:
```

14. Enter **389**.

    Result: The below messages appear.

```
==========================================================================
Each instance of a directory server requires a unique identifier. This
identifier is used to name the various instance specific files and directories
in the file system, as well as for other uses as a server instance identifier.

Directory server identifier [dshost]:
```

15. Enter any name. For example: **dshost**.

    Result: The below messages appear.

```
==========================================================================
The suffix is the root of your directory tree. The suffix must be a valid
DN.
It is recommended that you use the dc=domaincomponent suffix convention.
For example, if your domain is example.com, you should use dc=example,dc=com
for your suffix.
Setup will create this initial suffix for you, but you may have more than one
suffix.
Use the directory server utilities to create additional suffixes.
Suffix [dc=project, dc=com]:
```

16. Enter any name. For example: **dc=project**, **dc=com**.

    Result: The below messages appear.

```
==========================================================================
Certain directory server operations require an administrative user. This user
is referred to as the Directory Manager and typically has a bind Distinguished
Name (DN) of cn=Directory Manager. You will also be prompted for the password
for this user. The password must be at least 8 characterslong, and contain
no spaces.
Press Control-B or type the word "back", then Enter to back up and start
over.

Directory Manager DN [cn=Directory Manager]:
Password:*******
Password (confirm):*******
```

17. Enter the password.

    Result: The below messages appear.

```
==========================================================================
The Administration Server is separate from any of your web or application
servers since it listens to a different port and access to it is restricted.
```

```
Pick a port number between 1024 and 65535 to run your Administration Server
on. You should NOT use a port number which you plan to run a web or application
server on, rather, select a number which you will remember and which will not
be used for anything else.

Administration port [9830]:
```

18. Enter **9830**.

    Result: The below messages appear.

```
==========================================================================
The interactive phase is complete.  The script will now set up your servers.
Enter No or go Back if you want to change something.

Are you ready to set up your servers? [yes]:
Creating directory server . . .....
Warning: Hostname dshost.project.com is valid, but none of the IP addresses
resolve back to dshost.project.com
 address 3.185.121.199 resolves to host dshost
Your new DS instance 'dshost' was successfully created.
Creating the configuration directory server . . .
Beginning Admin Server creation . . .
Creating Admin Server files and directories . . .
Updating adm.conf . . .
Updating admpw . . .
Registering admin server with the configuration directory server . . .
Updating adm.conf with information from configuration directory server . . .
Updating the configuration for the httpd engine . . .
Starting admin server . . .
output: Starting dirsrv-admin:
output:                                                    [ OK  ]
The admin server was successfully started.
Admin server was successfully created, configured, and started.
Exiting . . .
Log file is '/tmp/setup7mVDia.log'
```

389 Directory Server groups and users Configuration

This section describes how to create groups and users which are used for authentication purposes.

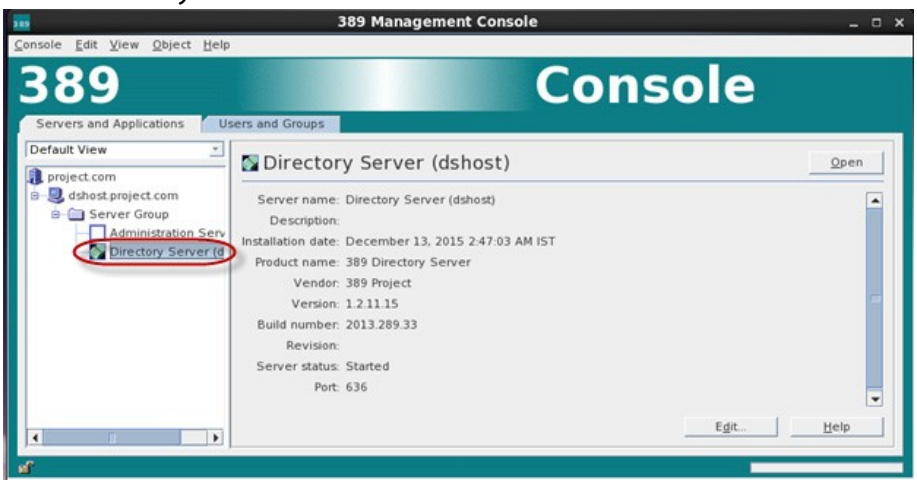
Creation of role groups

To create role groups:

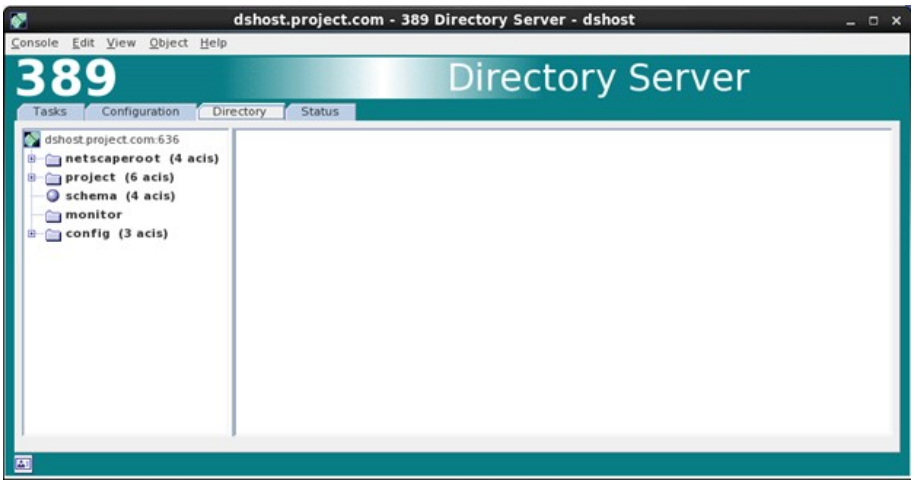
1. Open a browser window on the Ubuntu site.
2. Run the 389-console.

3. Enter the **user ID** and **Password**. Expand the created project.

4. Click on **Directory Server**.

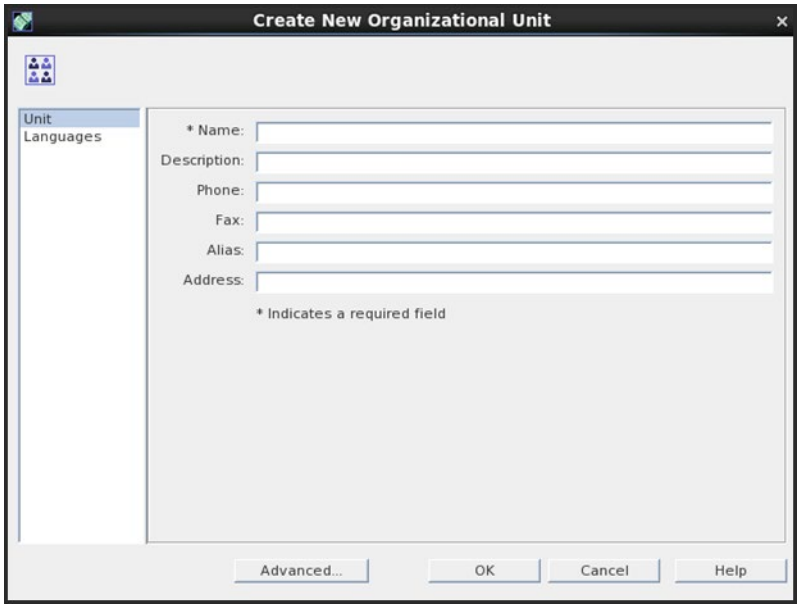


5. Double-click on **Directory server**.

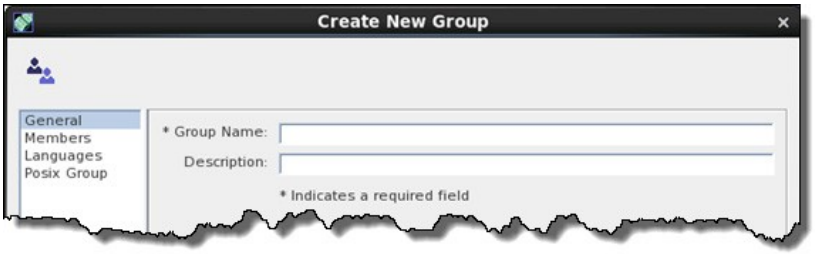


6. Select the **Directory** tab and expand the project tree on the left-hand side.
7. Right-click on Project and select **New** > **Organizational Unit**.

8. Enter the below parameters and click **OK**.



9. Right-click on Project and select **New** > **Group**.
10. Enter the below parameters and click **OK**.



11. Provide the group name and GID number excluding the GID numbers in Table 1 if you require dynamic mapping.

Table 1: Group name and GID number

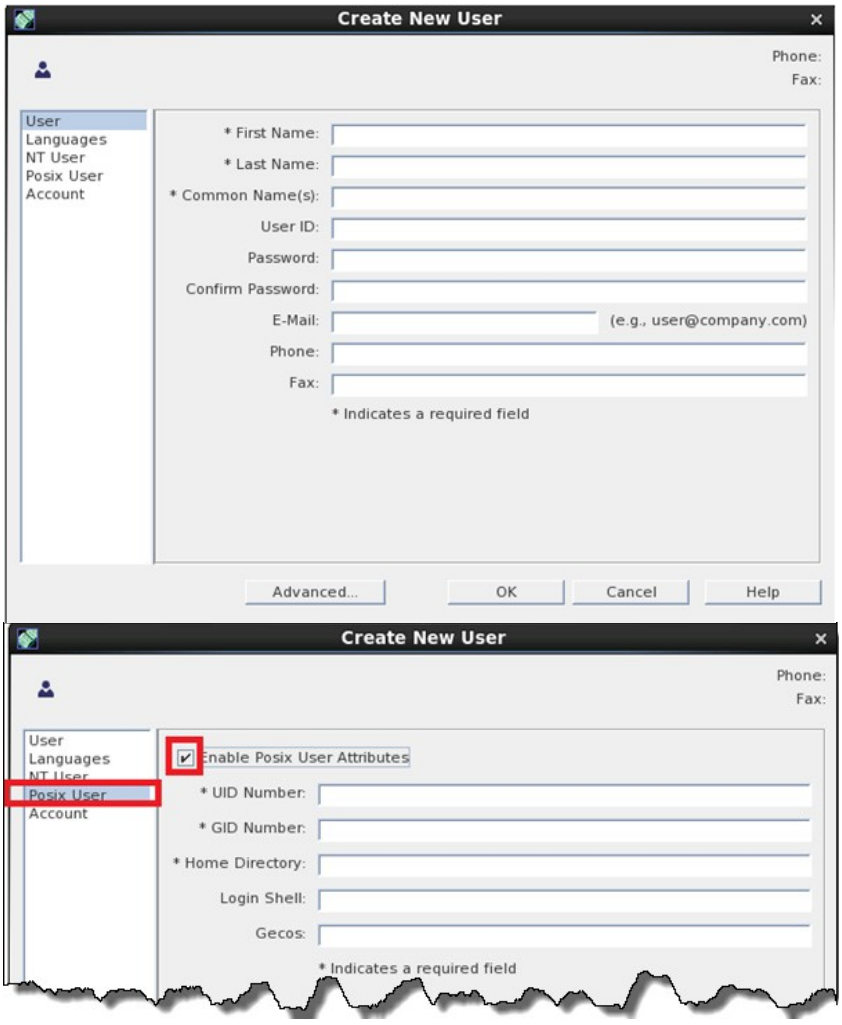
Role	GID number
admin	0
observer	501
operator	502
supervisor	503
Passthrough	504

You can create different groups as required.

Creation of Users

To create users and link them to desired roles:

1. Right-click on Project and select **New** > **User**.
2. Update the below parameters.



3. Click **OK**.

   You can create different users as required.

   Result: The users created in this procedure are used for authentication from the MCP device.

Group Mapping

Once the User group has been created successfully, these need to be mapped to MCP User Group. It can be done in two approaches:

Procedure for Static Group Mapping

In this approach, the MCP device **LDAP Server group gid** shall be configured as per Table 2.

Table 2: Group IDs mapping on the LDAP Server User Groups

LDAP Server Group Name	GID Number	Description
G500Administrator	0	To map LDAP Server Group G500Administrator to G500 groupAdministrator
G500Observer	501	To map LDAP Server Group G500Observer to G500 group Observer
G500Operator	502	To map LDAP Server Group G500Operator to G500 group Operator
G500Supervisor	503	To map LDAP Server Group G500Supervisor to G500 groupSupervisor
G500SSHPassThrough	504	To map LDAP Server Group G500Passthrough to G500 groupPassthrough

NOTE

The LDAP Server Group Name in the table is an example. LDAP Server Group Name can be any name as configured by the user, Eg.: Test Group etc. In this example is listed as "G500…", could be "G100…"

Because the functionality is the same across MCP family, this could be "MCP…".

However, GID Number is fixed asspecified in the table for MCP to recognize the same.

Example: In LDAP Server, to map MCP device LDAP Server group with name "**G500Administrator**" to MCP group "**Administrator**" using static group mapping, the LDAP Server group **GID** must configured as in the Table 2.

- The procedure to set the GID number in the LDAP Server is described in the section Creation of role groups.

RESULT: Once the G500Administrator group has been mapped successfully for **Administrator** role in MCP, the user added to this group will have administrator role in MCP.

Procedure for Dynamic Group Mapping

In this approach, the MCP device LDAP Server Group distinguished name "DN" must be configured in MCP group mapping. If user want to go for this approach, then GID Number entry in LDAP Server Group is not required.

- Login to MCP as administrator user and configure LDAP on the MCP device as mentioned in Procedure to configure LDAP on the MCP device.

Generating certificates

Before you can configure a secure channel between a MCP device and the LDAP server you need certificates for authorization. Certificates can be generated by the server itself orit can be generated by a Certification Authority (CA).

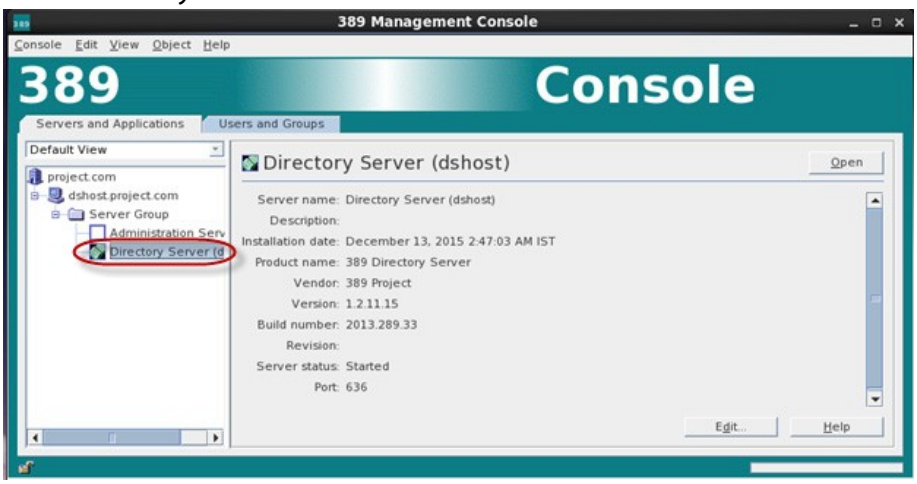
Generating certificates from server

This subsection describes how to generate certificates from LDAP server itself which is to be installed in the MCP device and used for authorization.

To generate certificates from the server:

1. Run the 389-console.

2. Enter the **user ID** and **Password**. Expand the created project.
3. Click on **Directory Server**.



4. Select the **Tasks** tab.

5. Click on **Manage Certificates**.

6. Generate the below passwords:
   - Generate Security Password *******
   - private/ca-cert.key: Passphrase: ******
   - KDC database master key: *****
   - password for principal "root/admin@PROJECT.COM": *****

Generate the CA

To generate the CA:

1. Navigate to the below path

   # cd /etc/pki/CA/

   # touch index.txt

   # echo '01' > serial

   # echo '01' > crlnumber

2. Execute the command:

   [root@dshost CA]# openssl req -new -x509 -extensions v3_ca -keyout private/ca-cert.key -out certs/ca-cert.crt -days 365

3. Enter values for the following parameters:
   - Country name
   - State or Province name
   - Locality name
   - Organization (e.g., company) name
   - Organization Unit name (e.g., section)
   - Common name (e.g., your name or server name)
   - Email address

```
Generating a 2048 bit RSA private key
.............+++
.....................................................+++
writing new private key to 'private/ca-cert.key'
Enter PEM pass phrase:ca@123
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
```

```
If you enter '.', the field will be left blank.
------
Country Name (2 letter code) [XX]:IN
State or Province Name (full name) []:Location xyz
Locality Name (eg, city) [Default City]: Location xyz
Organization Name (eg, company) [Default Company Ltd]:company
Organizational Unit Name (eg, section) []:Team
Common Name (eg, your name or your server's hostname) []:dshost.project.com
Email Address []:root@localhost
[root@dshost CA]#
```

4. Execute the below command

   # chmod 400 private/ca-cert.key

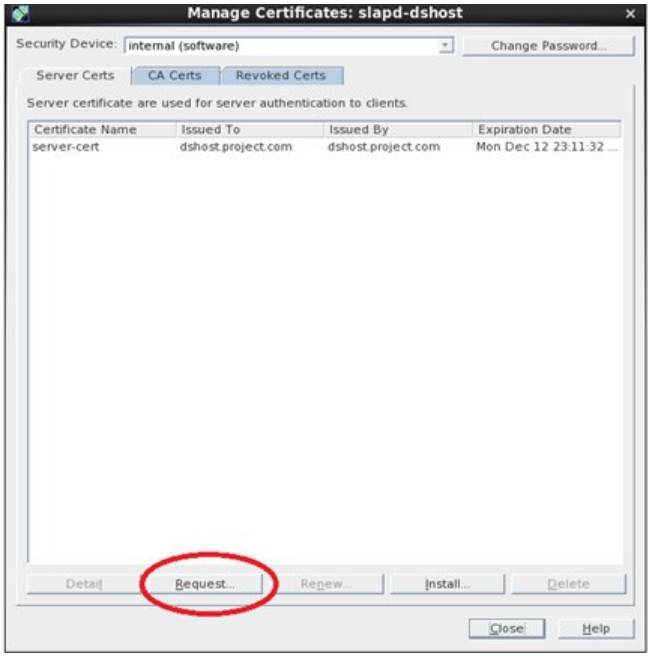
5. Ensure that the ca file does not need to match the certificates that it is signing.
6. Edit the openssl.cnf file and replace match with **optional**.

```
# vi /etc/pki/tls/openssl.cnf

[ policy_match ]
countryName             = optional
stateOrProvinceName     =   optional
organizationName  = optional
```

Generate and sign the server certificate

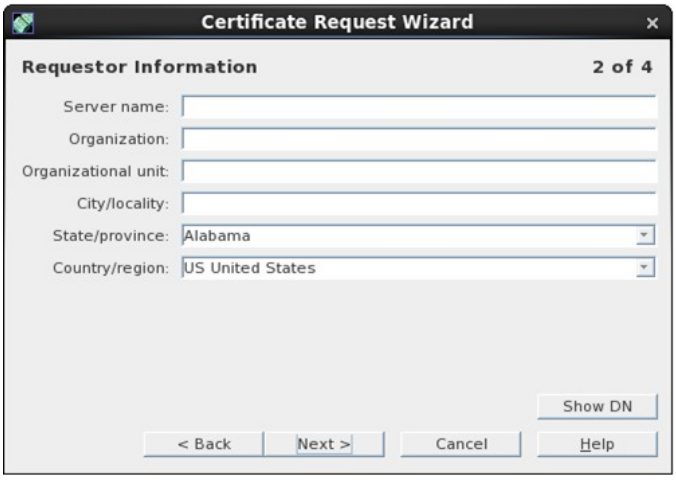
To generate and sign the server certificate:

1. Launch 389-console
2. Navigate to the **Manage certificates**
3. Under the **Server Certs** tab, click the **Request** button.



4. Select **Request certificate manually** and click **Next**.

5. Enter the **Server Name**, and other details, and click **Next**.



6. Enter the **Server Name**, and other details, and click **Next**.
7. Enter **Yes** and **Enter a Password**.
8. Save to file: **/tmp/dshost.project.com.csr** (or to respective path), and click **Save**.
9. Execute command:

   # mv /tmp/dshost.project.com.csr /etc/pki/CA/crl/

```
[root@dshost CA]# openssl ca -in /etc/pki/CA/crl/dshost.project.com.csr -out
/etc/pki/CA/newcerts/dshost.project.com.crt -keyfile /etc/pki/CA/private/
ca-cert.key -cert /etc/pki/CA/certs/ca-cert.crt
Using configuration from /etc/pki/tls/openssl.cnf
Enter pass phrase for /etc/pki/CA/private/ca-cert.key:******
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 1 (0x1)
        Validity
            Not Before: Dec 13 17:41:32 2015 GMT
            Not After : Dec 12 17:41:32 2016 GMT
        Subject:
            countryName                     = IN
              organizationName              = xyz
              organizationalUnitName    = xyzabc
              commonName                = dshost.project.com
        X509v3 extensions:
```

```
                X509v3 Basic Constraints:
                    CA:FALSE
                Netscape Comment:
                    OpenSSL Generated Certificate
                X509v3 Subject Key Identifier:
                    ..........................................................................................
                 X509v3 Authority Key Identifier:
                    ..........................................................................................
Certificate is to be certified until Dec 12 17:41:32 2016 GMT (365 days)
Sign the certificate? [y/n]:
```

10. Enter **Y** to sign the certificate.

    Result: The below messages appear.

    ```
    1 out of 1 certificate requests certified, commit? [y/n]
    ```

11. Enter **Y** to commit.

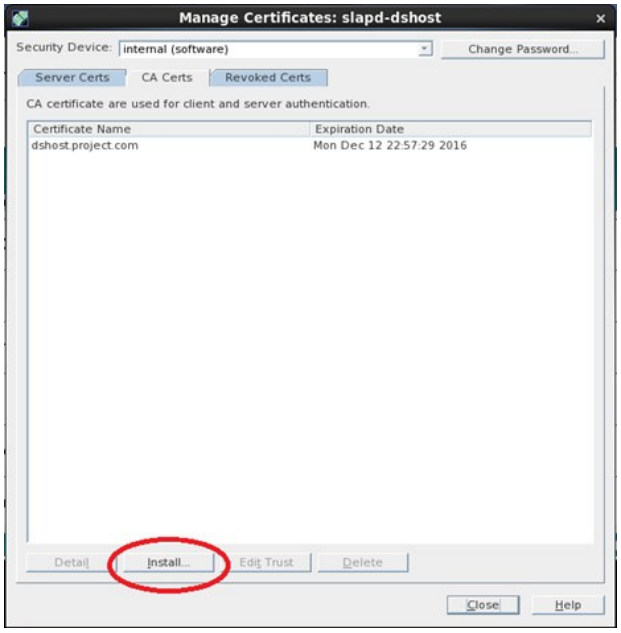
    Result: The below messages appear.

    ```
    Write out database with 1 new entries
    Data Base Updated
    [root@dshost CA]#
    ```

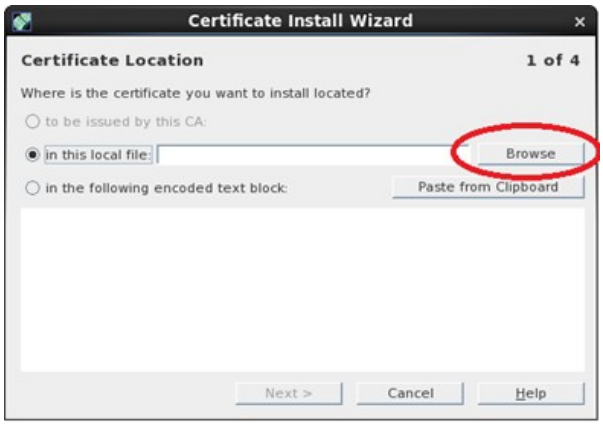
Install the certificates and enable SSL

To install the certificates and enable SSL:

1. Run 389-console.
2. Navigate to **Manage Certificates**.
3. Click **Install** to install the CA Public Cert.

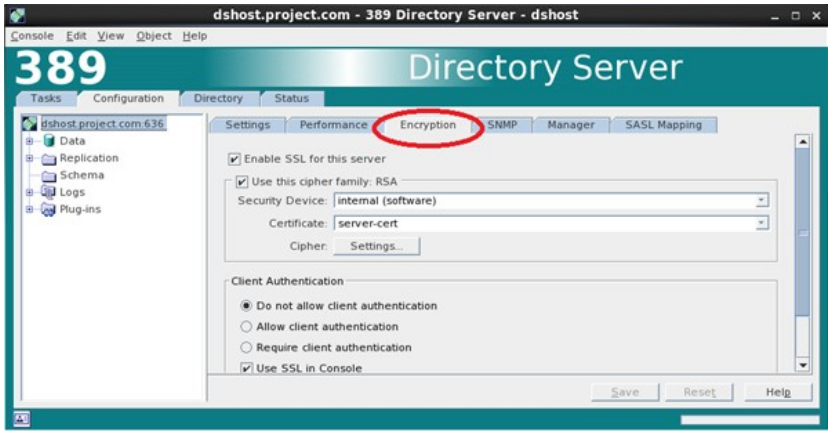


4. Select **in this local file** radio button and click **Browse**.



5. Select: file: **/etc/pki/CA/certs/ca-cert.crt**.
6. Click **Next** > **Next** > **Next** > **Done**.
7. In the Server Console, enable SSL:
   7.1. Select the **Configuration** tab.

   7.2. Configure the below options, and click **Save** and **OK**.
   7.3. Set up the pin file for directory server restarts.



8. Restart **dirsrv service**.

   Result: You are prompted for the certificate password which the pin.txt will fix)

   Result: The below messages appear.

```
admin[root@dshost ~]# /etc/init.d/dirsrv start
Starting dirsrv:
   dshost...Enter PIN for Internal (Software) Token: password@123
[  OK  ]
```

9. Execute command:

   # vi /etc/dirsrv/slapd-ldap01/pin.txt

```
Internal (Software) Token:<plain text password>
[root@dshost ~]# cat /etc/dirsrv/slapd-dshost/pin.txt
Internal (Software) Token:password@123
[root@dshost ~]#

# chmod 400 /etc/dirsrv/slapd-ldap01/pin.txt

# service dirsrv restart   (it should not ask for the cert password now)

[root@dshost ~]# /etc/init.d/dirsrv restart
Shutting down dirsrv:
    dshost...                                                  [ OK  ]
Starting dirsrv:
    dshost...                                                  [ OK  ]
[root@dshost ~]#

Set up Kerberos
Set up DNS

Kerberos requires a proper entry in the /etc/hosts file.

# vi /etc/hosts

  # Make sure the fqdn is set up before any aliases
  # Make sure only one entry exists for the public ip your using.
   3.185.121.199   dshost  dshost.project.com
```

10. Set up **ntpd**.

```
Servers require synced time for kerberos to work properly.
[root@dshost ~]# chkconfig --list ntpd
ntpd            0:off   1:off   2:off   3:off   4:off   5:off   6:off
[root@dshost ~]# crontab -l
# Sync Time with NTP Server using hostname.
1,16,31,46   * * * * /usr/sbin/ntpdate -u 3.185.120.21  >/dev/null
```

11. Edit the krb5.conf file and modify a few parameters to match your domain.

```
# vi /etc/krb5.conf

  [logging]
 default  =  FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 default_realm = PROJECT.COM
 dns_lookup_realm = false
 dns_lookup_kdc = false
 ticket_lifetime = 24h
 renew_lifetime = 7d
 forwardable = true

[realms]
 PROJECT.COM = {
  kdc = kerberos.example.com
```

```
  kdc = dshost.project.com
  admin_server = dshost.project.com
 }

[domain_realm]
 .project.com = PROJECT.COM
 project.com = PROJECT.COM
```

12. Install the server and set up the database and configure the basics.

```
# yum install krb5-server
You should have this package on our local dvd repository/ISO image.
[root@dshost ~]# rpm -qa | grep krb5-server
krb5-server-1.10.3-10.el6_4.6.x86_64
[root@dshost ~]#



[root@dshost ~]# kdb5_util create -r PROJECT.COM -s
Loading random data
Initializing database '/var/kerberos/krb5kdc/principal' for realm
'PROJECT.COM',
master key name 'K/M@PROJECT.COM'
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.
Enter KDC database master key: krb@123
Re-enter KDC database master key to verify: krb@123
[root@dshost ~]#


# vi /var/kerberos/krb5kdc/kdc.conf

  [kdcdefaults]
   kdc_ports = 88
   kdc_tcp_ports = 88

  [realms]
   LINUXRACKERS.COM = {
    #master_key_type = aes256-cts
    acl_file = /var/kerberos/krb5kdc/kadm5.acl
    dict_file = /usr/share/dict/words
    admin_keytab = /var/kerberos/krb5kdc/kadm5.keytab
    supported_enctypes = aes256-cts:normal aes128-cts:normal des3-hmac-
sha1:normal arcfour-hmac:normal des-hmac-sha1:normal des-cbc-md5:normal des-
cbc-crc:normal

    # May want to comment this out in production
    # default_principal_flags =+ preauth
   }


# vi /var/kerberos/krb5kdc/kadm5.acl

*/admin@PROJECT.COM     *
Set up a 'root' principle for administration and a 'host' principle for the
ldap server. Create a keytab from the 'host' principle.

[root@dshost ~]# kadmin.local
Authenticating as principal root/admin@PROJECT.COM with password.
kadmin.local:  addprinc root/admin
WARNING: no policy specified for root/admin@PROJECT.COM; defaulting to no
policy
Enter password for principal "root/admin@PROJECT.COM": krb@123
Re-enter password for principal "root/admin@PROJECT.COM": krb@123
Principal "root/admin@PROJECT.COM" created.
kadmin.local:  addprinc -randkey host/dshost.project.com
WARNING: no policy specified for host/dshost.project.com@PROJECT.COM;
defaulting to no policy
```

```
Principal "host/dshost.project.com@PROJECT.COM" created.
kadmin.local:  ktadd -k /etc/krb5.keytab host/dshost.project.com
Entry for principal host/dshost.project.com with kvno 2, encryption type
aes256-cts-hmac-sha1-96 added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal host/dshost.project.com with kvno 2, encryption type
aes128-cts-hmac-sha1-96 added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal host/dshost.project.com with kvno 2, encryption type
des3-cbc-sha1 added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal host/dshost.project.com with kvno 2, encryption type
arcfour-hmac added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal host/dshost.project.com with kvno 2, encryption type
des-hmac-sha1 added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal host/dshost.project.com with kvno 2, encryption type
des-cbc-md5 added to keytab WRFILE:/etc/krb5.keytab.
kadmin.local: q
[root@dshost ~]#

Enable/Start The Service

#
[root@dshost ~]# chkconfig krb5kdc on
[root@dshost ~]# chkconfig kadmin on
[root@dshost ~]# service kadmin start
Starting Kerberos 5 Admin Server:                          [ OK ]
[root@dshost ~]# service krb5kdc start
Starting Kerberos 5 KDC:                                   [ OK  ]
[root@dshost ~]#
```

13. Set up 389-ds to use Kerberos.

```
This will require setting up an ldap principle, exporting the keytab and
setting an environment variable for the 389-ds instance.

[root@dshost ~]# grep ldap /etc/passwd
ldapadmin:x:501:501::/home/ldapadmin:/bin/bash
[root@dshost ~]#


# kadmin.local
[root@dshost ~]# kadmin.local
Authenticating as principal root/admin@PROJECT.COM with password.
kadmin.local: add_principal -randkey ldapadmin/
dshost.project.com@PROJECT.COM
WARNING: no policy specified for ldapadmin/dshost.project.com@PROJECT.COM;
defaulting to no policy
Principal "ldapadmin/dshost.project.com@PROJECT.COM" created.
kadmin.local:  ktadd -k /etc/dirsrv/ds.keytab ldapadmin/dshost.project.com
Entry for principal ldapadmin/dshost.project.com with kvno 2, encryption
type aes256-cts-hmac-sha1-96 added to keytab WRFILE:/etc/dirsrv/ds.keytab.
Entry for principal ldapadmin/dshost.project.com with kvno 2, encryption
type aes128-cts-hmac-sha1-96 added to keytab WRFILE:/etc/dirsrv/ds.keytab.
Entry for principal ldapadmin/dshost.project.com with kvno 2, encryption
type des3-cbc-sha1 added to keytab WRFILE:/etc/dirsrv/ds.keytab.
Entry for principal ldapadmin/dshost.project.com with kvno 2, encryption
type arcfour-hmac added to keytab WRFILE:/etc/dirsrv/ds.keytab.
Entry for principal ldapadmin/dshost.project.com with kvno 2, encryption
type des-hmac-sha1 added to keytab WRFILE:/etc/dirsrv/ds.keytab.
Entry for principal ldapadmin/dshost.project.com with kvno 2, encryption
type des-cbc-md5 added to keytab WRFILE:/etc/dirsrv/ds.keytab.
kadmin.local:  quit
[root@dshost ~]#


[root@dshost ~]# ls -l /etc/dirsrv/ds.keytab
-rw-------. 1 root root 484 Dec 14 15:20 /etc/dirsrv/ds.keytab
[root@dshost ~]# chown ldapadmin: /etc/dirsrv/ds.keytab
[root@dshost ~]# ls -l /etc/dirsrv/ds.keytab
```

```
-rw-------. 1 ldapadmin ldapadmin 484 Dec 14 15:20 /etc/dirsrv/ds.keytab
[root@dshost ~]# chmod 600 /etc/dirsrv/ds.keytab
[root@dshost ~]# ls -l /etc/dirsrv/ds.keytab
-rw-------. 1 ldapadmin ldapadmin 484 Dec 14 15:20 /etc/dirsrv/ds.keytab
[root@dshost ~]#


# vi /etc/sysconfig/dirsrv
  KRB5_KTNAME=/etc/dirsrv/ds.keytab ; export KRB5_KTNAME


[root@dshost ~]# service dirsrv restart
Shutting down dirsrv:
    dshost...                                               [ OK  ]
Starting dirsrv:
    dshost...                                               [ OK  ]
[root@dshost ~]#
```

14. The 389-ds server needs a gssapi mapping from the kerberos user and realm to the ldap dn under the ou=People,dc=linuxrackers,dc=com container.

```
# 389-console -a http://localhost:9830

Drill down to:
  -> project.com
    -> dshost.project.com
      -> Directory Server
        -> Open

In the Server Console do the following to install the CA Public Cert:

  -> Configuration(tab) -> SASL Mappings(subtab)
    -> Add
      -> Name:                gssapi-map
      -> Regular Expression:  uid=(.*),cn=PROJECT.COM,cn=gssapi,cn=auth
      -> Search Base DN:      uid=\1,ou=People,dc=project,dc=com
      -> Search Filter:       (objectClass=*)
        -> Ok -> Save


[root@dshost ~]# service dirsrv restart
Shutting down dirsrv:
    dshost...                                               [ OK  ]
Starting dirsrv:
    dshost...                                               [ OK  ]
[root@dshost ~]# service dirsrv-admin restart
Shutting down dirsrv-admin:
                                                            [ OK  ]
Starting dirsrv-admin:
httpd.worker: Could not reliably determine the server's fully qualified
domain name, using dshost.project.com for ServerName
                                                            [ OK  ]
```

Retrieving certificates for 389 DS server

Server certificate installed on 389 DS can be retrieved through winscp or any other tool.

1. Launch winscp software.
2. Open the terminal of Red hat linux operating system.
3. Copy the server certificate (.crt) from **/etc/pki/CA/certs** to computer hard disk.
4. Follow procedure in next chapter to upload this certificate in the MCP device.

Configuring the MCP devices for Centralized LDAP Authentication using 389 Directory Server

Chapter 2: Configure the LDAP on MCP

The Lightweight Directory Access Protocol (LDAP) is an application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network. This Directory services may provide any organized set of records, often with a hierarchical structure.

This chapter describes how to install CA Certificates on the MCP device and configure LDAP on the MCP device.

See section:

- Installing CA Certificates on the MCP device
  - CA Certificate transfer procedure from PC to MCP
    - CA Certificate Transfer to MCP by using DSAS Secure File Browser
    - CA Certificate transfer to MCP by using external Secured USB
  - CA Certificate Installation procedure
    - Import and Install CA certificate through Runtime DSAS
    - Import and Install CA certificate through Local HMI
- Configuring LDAP on the MCP device
  - Prerequisites to configuring LDAP on MCP device
    - Create an Emergency Administrator User
    - Retrieve LDAP Authentication Server information
  - Procedure to configure LDAP on the MCP device

Installing CA Certificates on the MCP device

This section describes how to install the CA Certificate to the MCP device. There are two type of certificates you can create:

- Server certificate
- Client certificate

Files to be Created	• CA certificate to be installed in both the Client and Server. • Server Certificate to be installed in the Server for Server Authentication (This can be skipped if LDAP Server CS us used to create the CA Certificate).	
Files to be Transferred	**MCP**	MyCA.crt or MyCA.cer (LDAP Client)
	389 Directory Server	MyCA.crt or MyCA.cer servercert.p12 (LDAP Server)

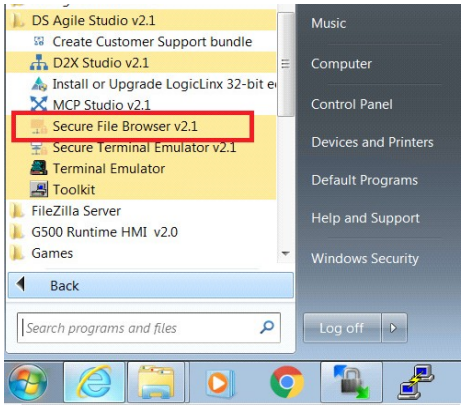
CA Certificate transfer procedure from PC to MCP

You can import and install the CA certificate to MCP. This certificate can be transferred to MCP for installation, using either of the below two options:

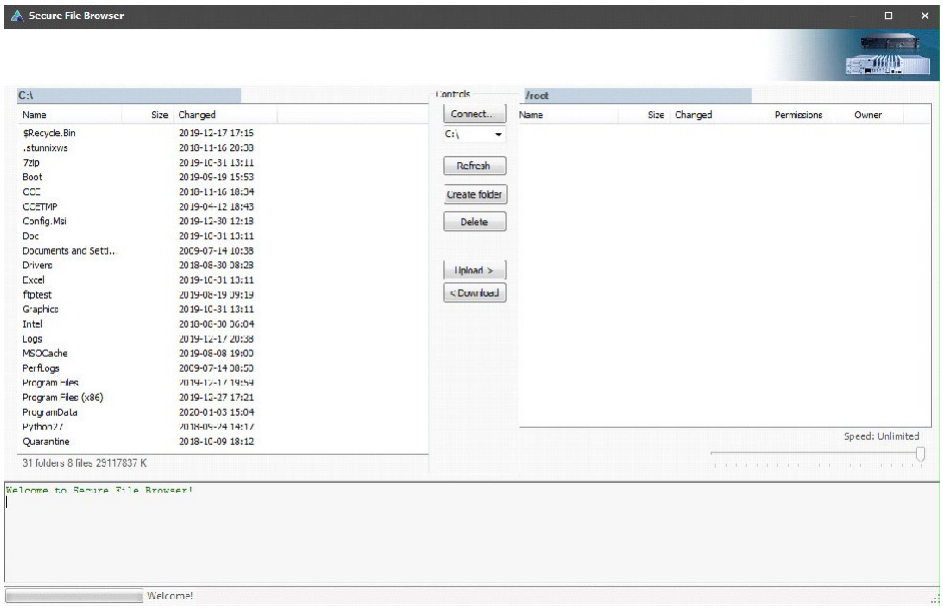
1. CA Certificate Transfer to MCP by using DSAS Secure File Browser
2. CA Certificate transfer to MCP by using external Secured USB

CA Certificate Transfer to MCP by using DSAS Secure File Browser

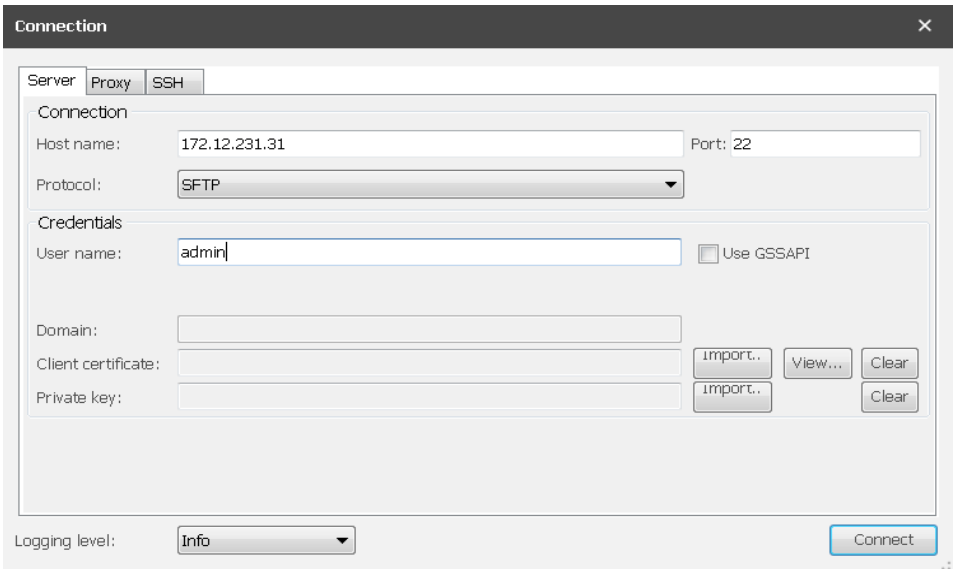
1. Copy the files containing the CA certificate to the following MCP location: **/mnt/usr/SecureScadaTransfer**
   - This can be done using the DSAS Secure File Browser (SFTP file transfer program).
   - To launch DSAS Secure File Browser, click on: **Start>All programs>DS Agile Studio vX.0> Secure File Browser vX.0**.



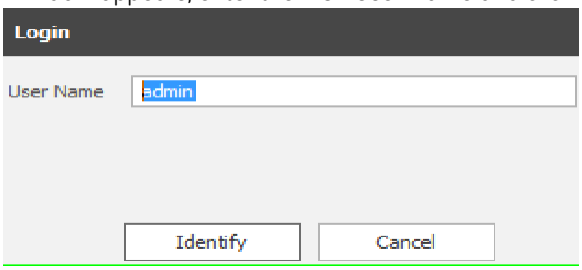
- Secure File Browser screen will be launched as below:



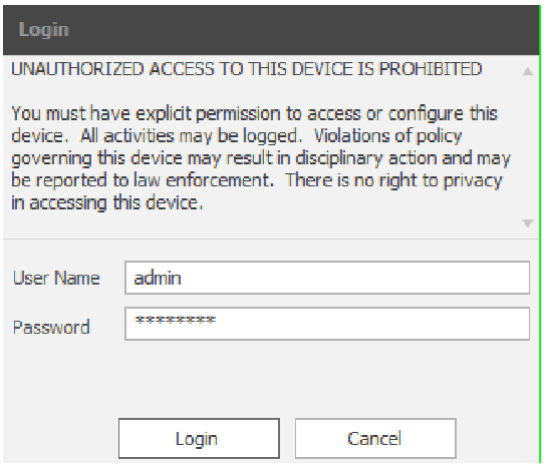
- Click **Connect**.
- The Connection Details window will appear.
- Enter Host name: MCP IP, Protocol: SFTP, User name details and then click **Connect**.



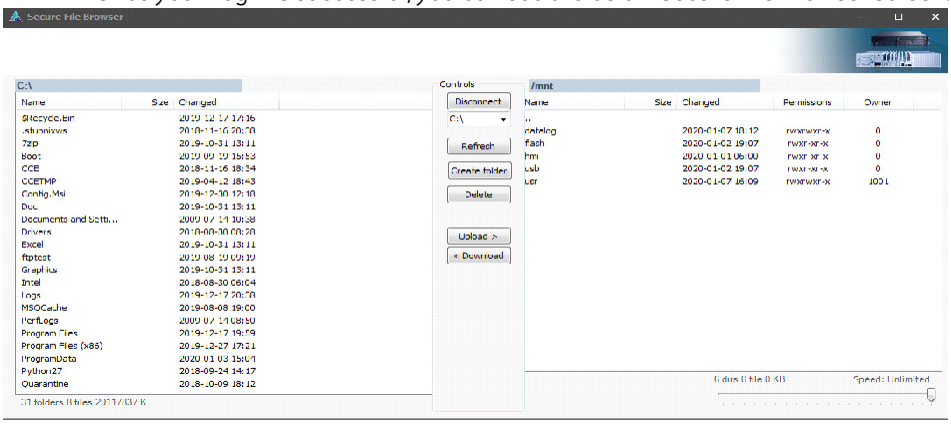
- A Login window appears, enter the MCP User Name and click **Identify** tab.



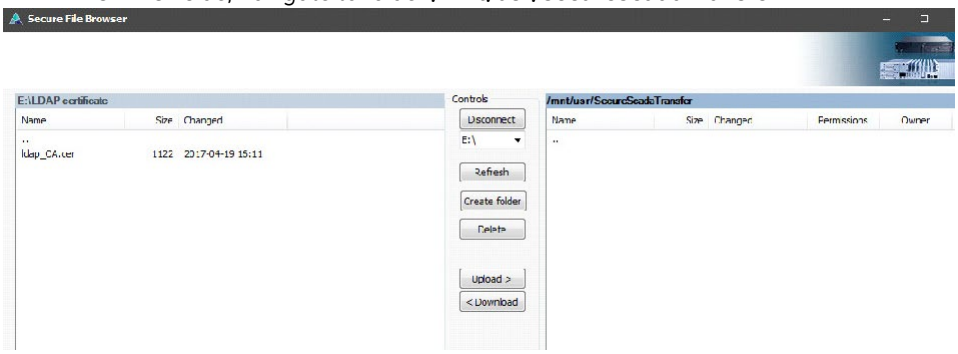
- Once the User Name is identified with the MCP, a Login window appears and prompt for the Password.



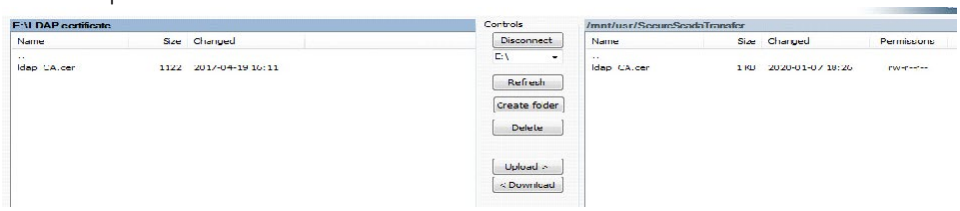
- Enter the Password and click **Login** to access the MCP folders.
- Once your Login is successful, you can see the below Secure File Browser screen:



- In the Secure File Browser window, PC folders are displayed on the left side and the MCP folders are displayed on the right.
- On MCP side, navigate to folder **/mnt/usr/SecureScadaTransfer**



- Select the required certificate from the PC folder and click **Upload**. This will upload the files from PC to MCP.



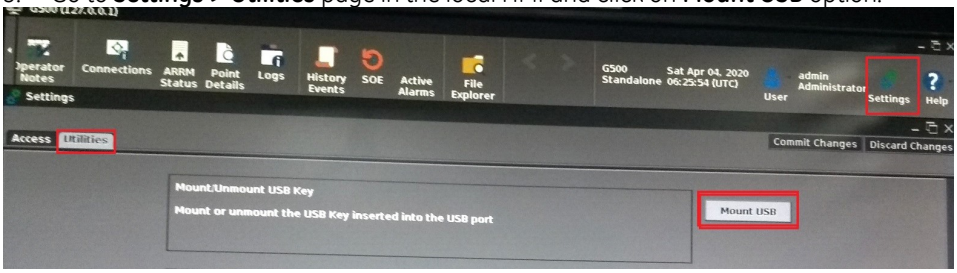
NOTE

After completion of these steps, LDAP client certificate is transferred successfully to MCP and is ready for installation.

CA Certificate transfer to MCP by using external Secured USB

Once the LDAP client certificate (CA certificate) is created and available on the PC and you can transfer this CA certificate to MCP using USB as follows:

1. Create a directory in USB drive "**SecureScadaTransfer**".
2. Copy the CA certificate from PC to USB on a USB drive (LDAP Client certificate need to be available in USB at **\SecureScadaTransfer**).
3. Insert the USB drive into any USB slot on the MCP device. E.g.: USB Port-1
4. Open Local HMI and login as administrator user.
5. Go to **Settings > Utilities** page in the local HMI and click on **Mount USB** option.



6. Now USB is mounted successfully to MCP and CA certificate is available at **/mnt/usb/usb1/SecureScadaTransfer**.

CA Certificate Installation procedure

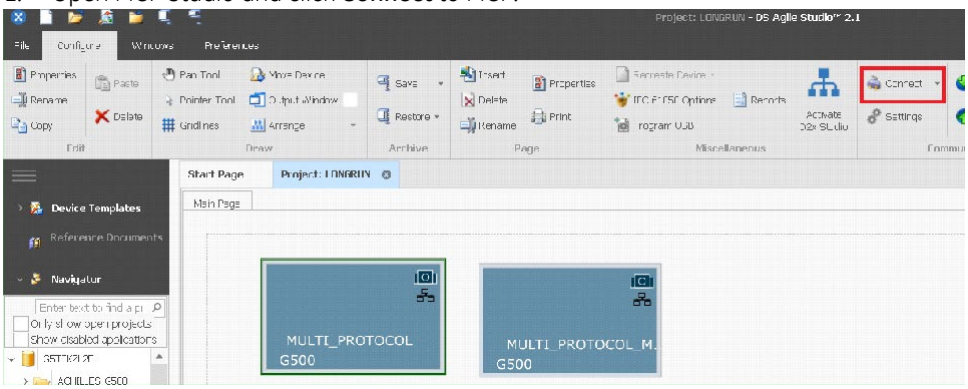
Once the certificate is available in MCP by any of the transfer procedure mentioned in page 32 (Secure DSAS Browser or USB), it can be installed by using either of the below two interfaces:

- Import and Install CA certificate through Runtime DSAS
- Import and Install CA certificate through Local HMI

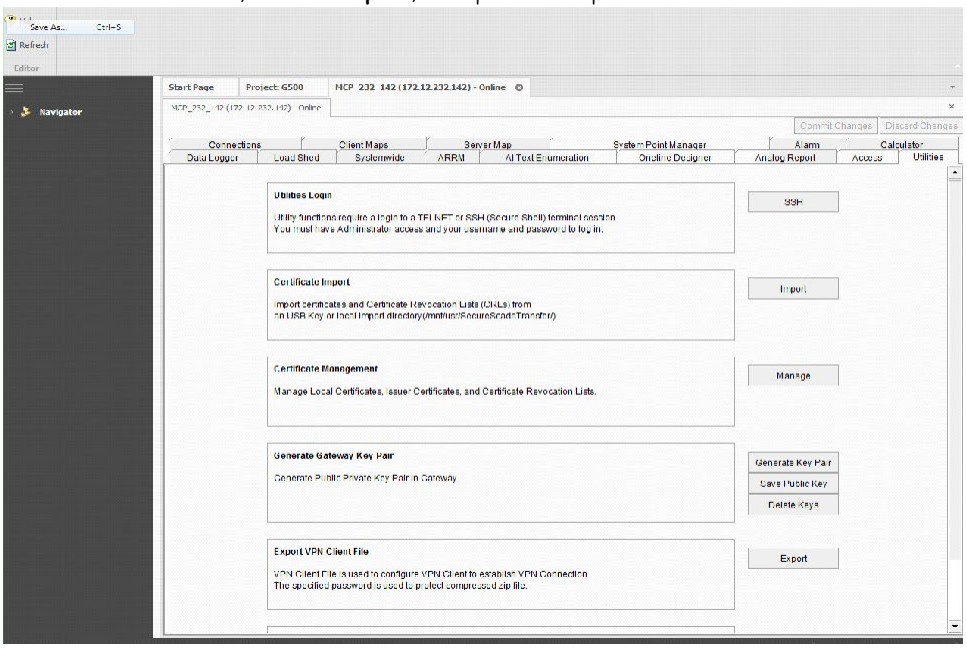
Import and Install CA certificate through Runtime DSAS

After certificate transfer to MCP at **/mnt/usr/SecureScadaTransfer/** or certificates can be installed to MCP using **DSAS > Utilities**. To proceed follow the below steps:

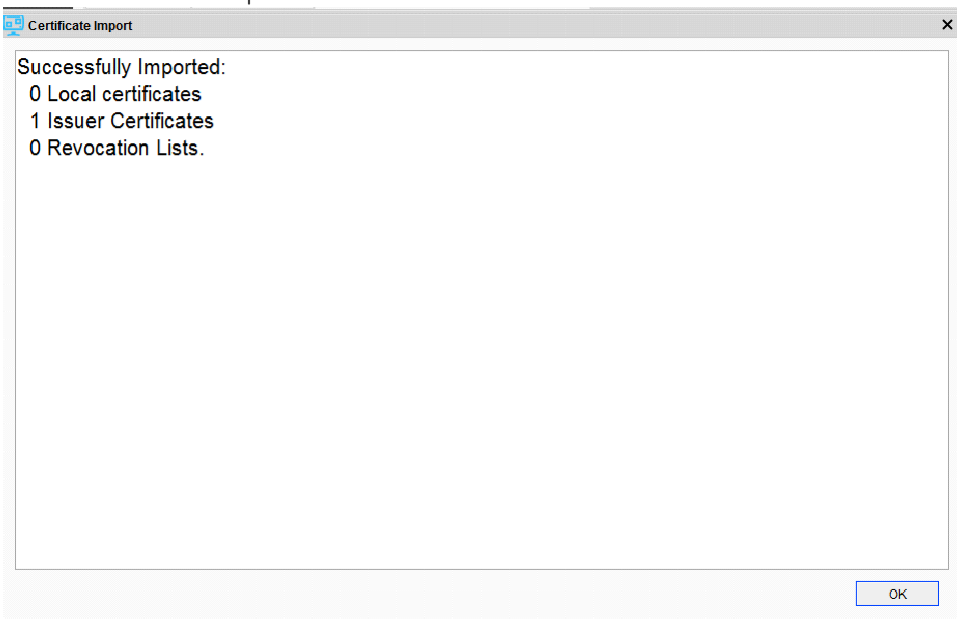
1. Open MCP Studio and click **Connect** to MCP.



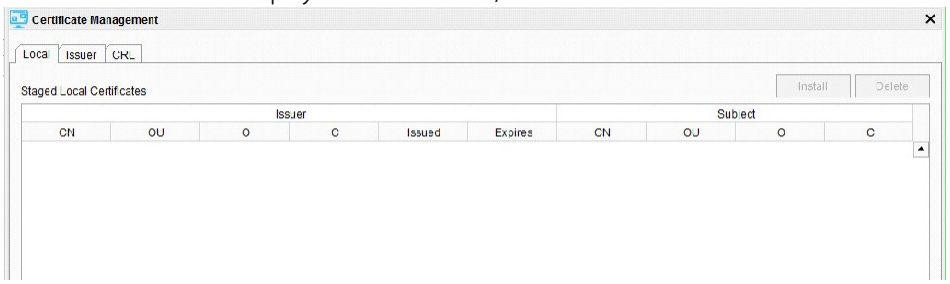
2. Select Utilities tab, click on **Import**, to import the copied certificates.



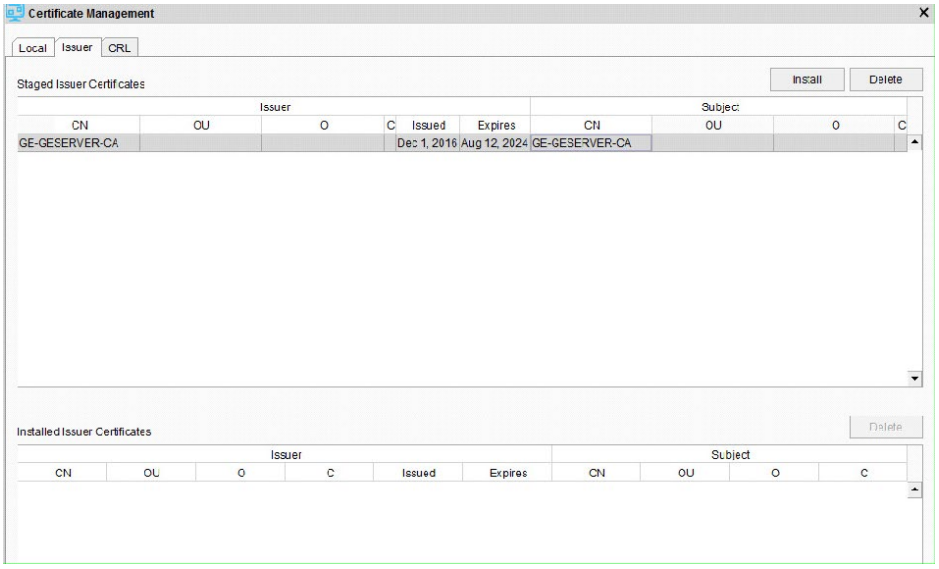
3. Once the certificates are imported, a Certificate Import window appears which shows confirmation of import status. Click **OK**.



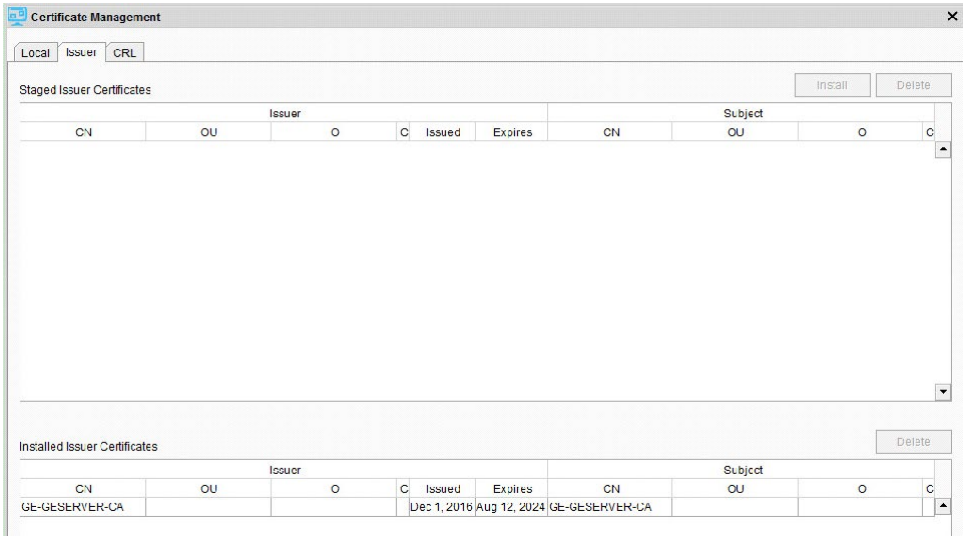
4. Once the certificates are imported successfully, click "**Manage**" to manage local certificates which display three tabs **Local**, **Issuer** and **CRL** as below:



5. Click on **Issuer** tab, select the Certificate and click **Install**.



6. Once the certificate is installed successfully, it is moved to the Installed Issuer Certificates section:

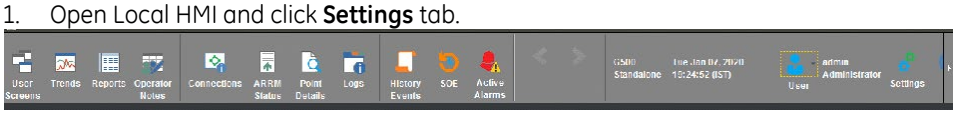


RESULT: This completes the Certification Installation process through DSAS Online HMI. You can use this certificate in LDAP Authentication.

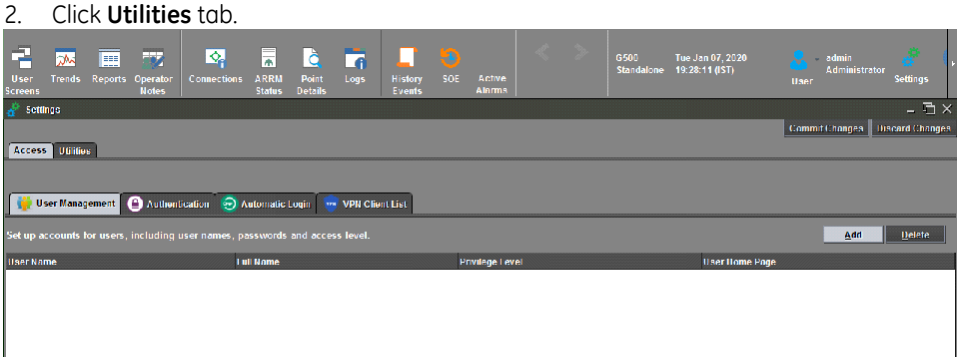
Import and Install CA certificate through Local HMI

After the certificate is transferred to the MCP at **/mnt/usr/SecureScadaTransfer/** or **/mnt/usb/usb1/SecureScadaTransfer/** certificates can be installed to MCP using **Local HMI > Settings > Utilities**. To proceed follow the prescribed steps as below:

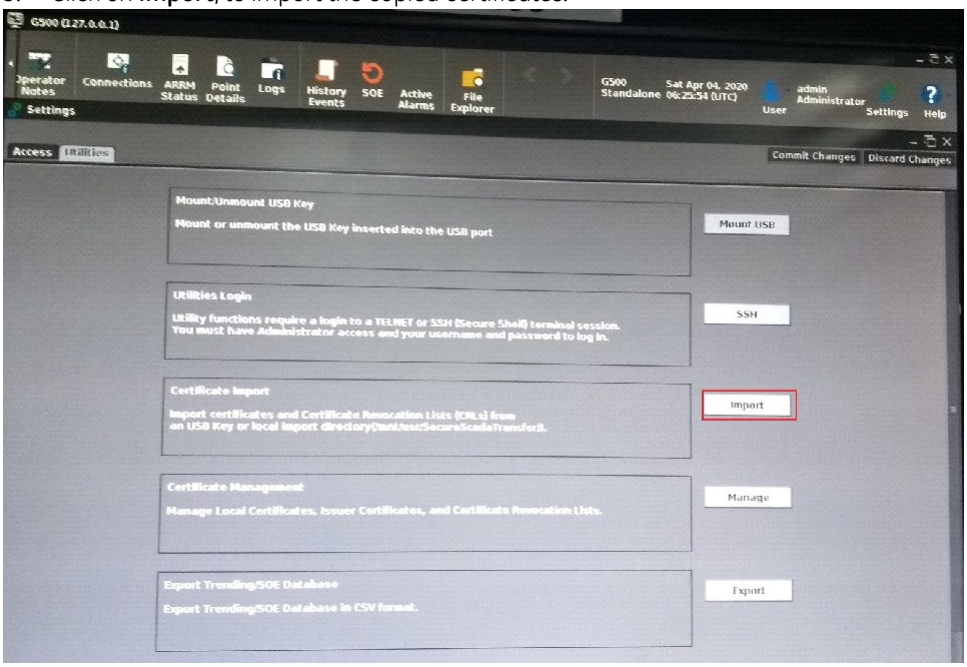
1. Open Local HMI and click **Settings** tab.



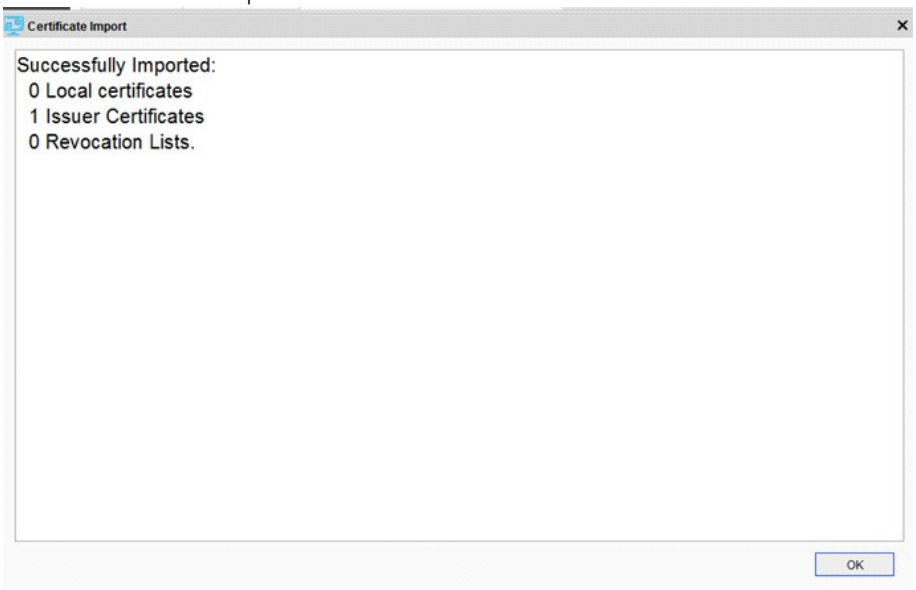
2. Click **Utilities** tab.



3. Click on **Import**, to import the copied certificates.

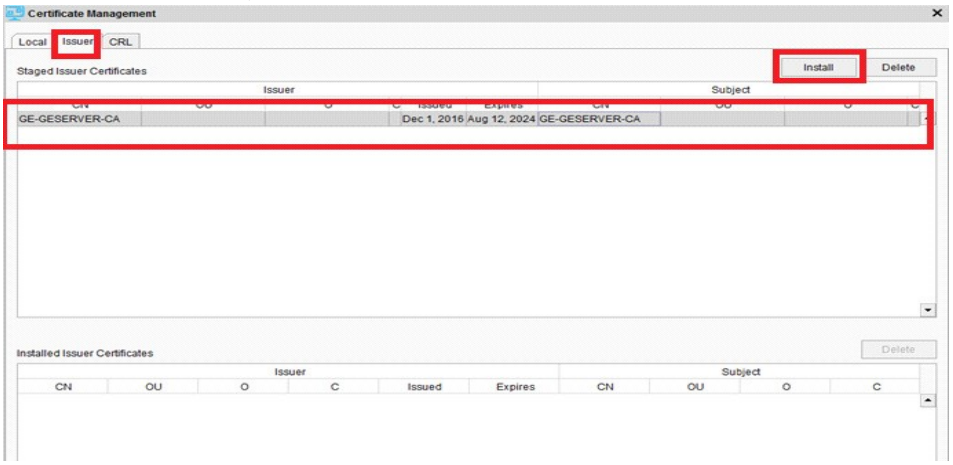


4. Once the certificates are imported, a Certificate Import window appears which shows confirmation of import status. Click **OK**.

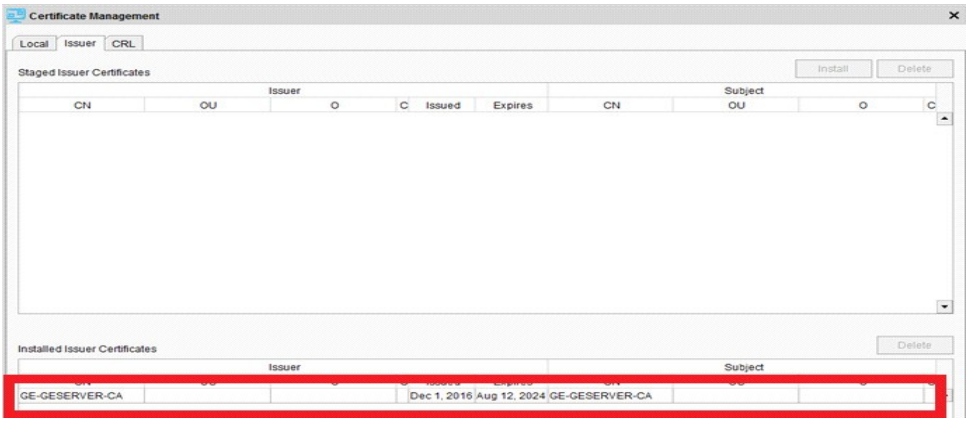


5. Once the certificates are imported successfully, click "**Manage**" to manage local certificates which display three tabs Local, Issuer and CRL as below:

6. Click on **Issuer** tab, select the Certificate and click **Install**.



7. Once the certificate is installed successfully, it's moved to the Installed IssuerCertificates section:



RESULT: This completes the Certification Installation process through DSAS Online HMI. You can use this certificate in LDAP Authentication.

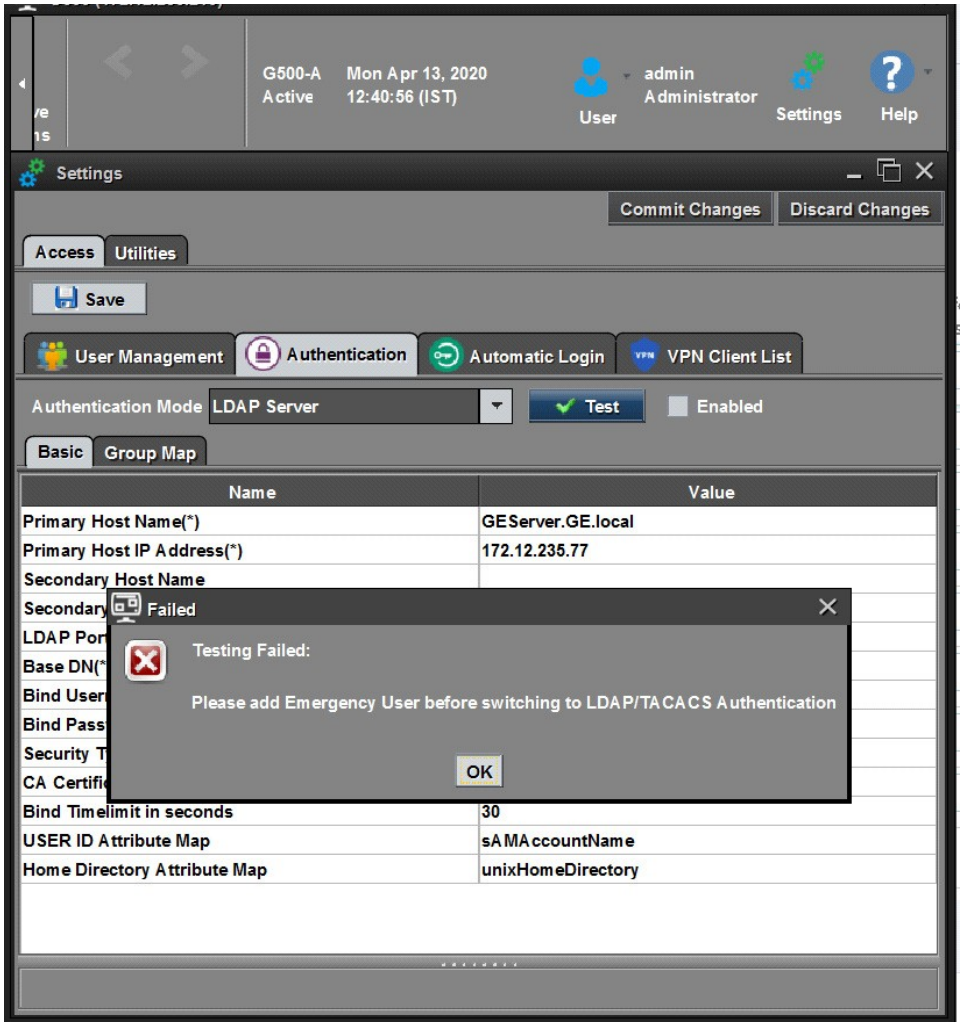
Configuring LDAP on the MCP device

This section describes the:

- Tasks performed prior to configuring the LDAP on the MCP device and
- The procedure to configure the LDAP on the MCP device.

Prerequisites to configuring LDAP on MCP device

Prior to configuring the LDAP on the MCP device it is mandatory to create emergency user in MCP. If user directly start LDAP configuration by using section Procedure to configure LDAP on the MCP device then user will get popup message that “Please add Emergency User before switching to LDAP/TACACS Authentication” and user will not be able to configure LDAP authentication without adding emergency users.



Create an Emergency Administrator User

This emergency user can be used when remote authentication server is not available and user in unable to access MCP using Remote Authentication. This emergency admin user is required to get access to the system in case of emergency, i.e. when LDAP server is not responsive / user forgets all credentials etc.

Emergency Users can be created by using any of the below two option:

- Using Web MCP Settings GUI
- Using the mcpcfg utility on MCP device through Secure Terminal Emulator

An emergency administrator user can login to MCP using any of the below three interfaces:

1. SSH session to MCP (Port-922)
2. Front serial port connection to MCP (Baud Rate- 115200)
3. MCP Emergency option in local console

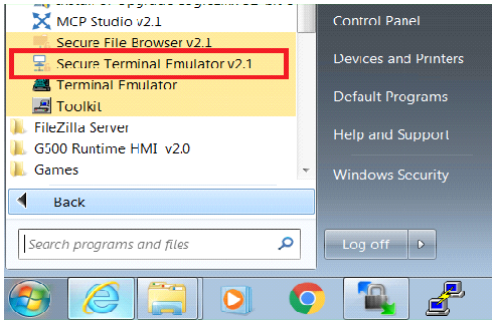
Once user logs into MCP as Emergency Administrator user, executing “emercfg” command shall provide options for user to perform the below two key functions:

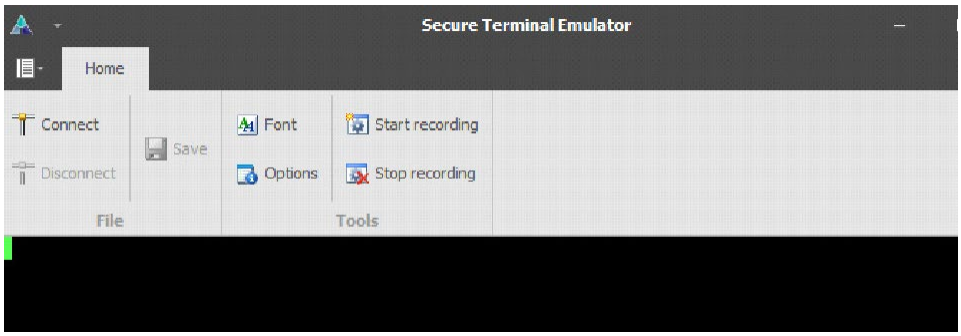
- Change the mode authentication from remote to local mode.
- Generate emergency code to login to HMI without changing authentication from remote to local mode.

Below sections describes how to add emergency user in MCP by using any of these option step by step:

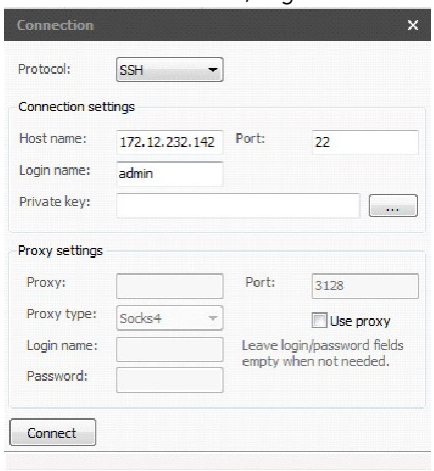
Using the mcpcfg utility on MCP device through Secure Terminal Emulator

1. To open Secure Terminal Emulator, select **Start > All Programs > DS Agile Studio vX.0 > Secure Terminal Emulator vX.0**

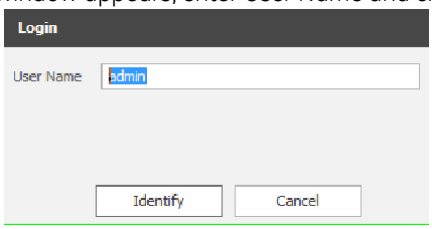




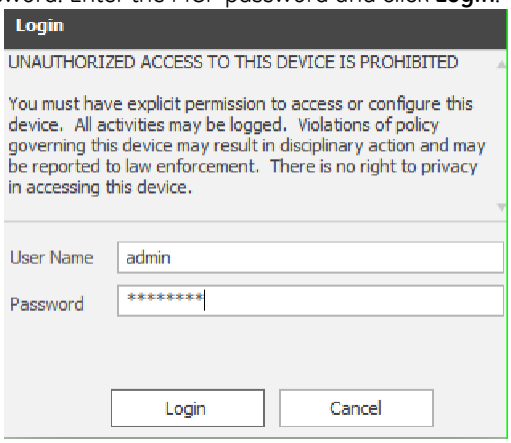
2. Click **Connect**. A pop-up window appears which shows Connections credentials.
3. Enter your MCP IP in Host name, Login name and Port 22 and click **Connect**.



4. A Login window appears, enter User Name and click **Identify**.



5. Once the User Name is identified with the MCP, a Login window appears to prompt for the Password. Enter the MCP password and click **Login**.



6. Once you login successfully, MCP Shell window appears:

```
GE Multilin MCP Firmware Release 110 Production Build 391 2020-01-01:04:41:24

admin@G500:~$
```

7. Type **sudo mcpcfg** and enter your Administrator User Name and Password if prompts.
8. The Gateway Settings Menu appears:

```
================================================================
        Gateway Settings Menu
================================================================

        0.   Back
        1.   Configure Authentication
        2.   Configure Network Settings
        3.   Configure Network Interfaces
        4.   Configure Secure Access
        5.   Configure Firewall
        6.   Configure Host Names
        7.   Configure Time & Time Sync
        8.   Reset System Logs
        9.   Reset Database Tables
        10.  Reset File Persistence Data
        11.  Local HMI
        12.  Configure Sync Manager
        13.  Redundancy
        14.  ARRM
        15.  Suppress Forced Qualities To Masters
        16.  Emulate D20 RTU IEC101 DPA Unbalanced Mode Functionality
        17.  Configure IEC101+104 DPA Startup Quality Event Suppress Interva
        18.  Configure Serial Ports
        19.  Configure D.20 Port Settings
        20.  EdgeOS Host
        21.  Clear Chassis Intrusion State
```

9. Enter **1** to select **Configure Authentication** option and the below menu appears:

```
         Gateway Settings Menu   Authentication
=================================================

         Current AuthMode Status : Local

         0.   Back
         1.   Root Administrator Settings
         2.   Pass-Through Password Authentication
         3.   Administrator Group Users
         4.   Emergency Group Users

Enter Your Choice : ( Between 0 and 4 ):
```

10. Enter **4** to select **Emergency Group Users** to Add an Emergency Admin User.

```
=========================================================
        Gateway Settings Menu
        Authentication - Emergency Admin Group Users
=========================================================

        0.   Back
        1.   List Users
        2.   Add User
        3.   Change Password
        4.   Remove User

Enter Your Choice : ( Between 0 and 4 ):
```

11. Enter **2** to Add User.
12. Enter the new emergency user name, full name, password and re-enter password.

```
=============================================================
        Gateway Settings Menu
        Emergency Group Users - Add user in Emergency group
=============================================================


Enter user name : emadmin

Enter user's full name : Emergency Administrator

Enter the password for emadmin:
Re-enter the password :
```

13. Type "**Y**" to confirm to the user.

```
=============================================================
        Gateway Settings Menu
        Emergency Group Users - Add user in Emergency group
=============================================================


Enter user name : emadmin

Enter user's full name : Emergency Administrator

Enter the password for emadmin:
Re-enter the password :

You entered:
User Name      : emadmin
User Full Name : Emergency Administrator

Confirm that you want to add this user ? <Y/N> :
```

14. Once user is added successfully, press **Enter**.

```
================================================================
        Gateway Settings Menu
        Emergency Group Users - Add user in Emergency group
================================================================


Enter user name : emadmin

Enter user's full name : Emergency Administrator

Enter the password for emadmin:
Re-enter the password :

You entered:
User Name      : emadmin
User Full Name : Emergency Administrator

Confirm that you want to add this user ? <Y/N> :        y


Successfully added user : emadmin

Press ENTER Key to continue....
```

15. Navigate back to Emergency Group Users and enter **1** to view the List of Emergency Admin Group Users.

```
=======================================================
        Gateway Settings Menu
        Authentication - Emergency Admin Group Users
=======================================================

        0.   Back
        1.   List Users
        2.   Add User
        3.   Change Password
        4.   Remove User

Enter Your Choice : ( Between 0 and 4 ):
```

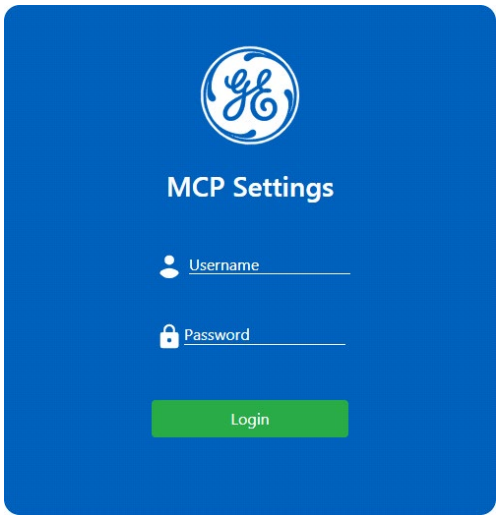
16. The menu displays the list of Added Emergency Admin Users.

```
            ================================================================
                    Gateway Settings Menu
                    Emergency Group Users - List of users in Emergency group
            ================================================================


    User Name                          UID    Full Name
=====================================================================

 1. emadmin                            1005   Emergency Administrator


            Press ENTER Key to continue....
```

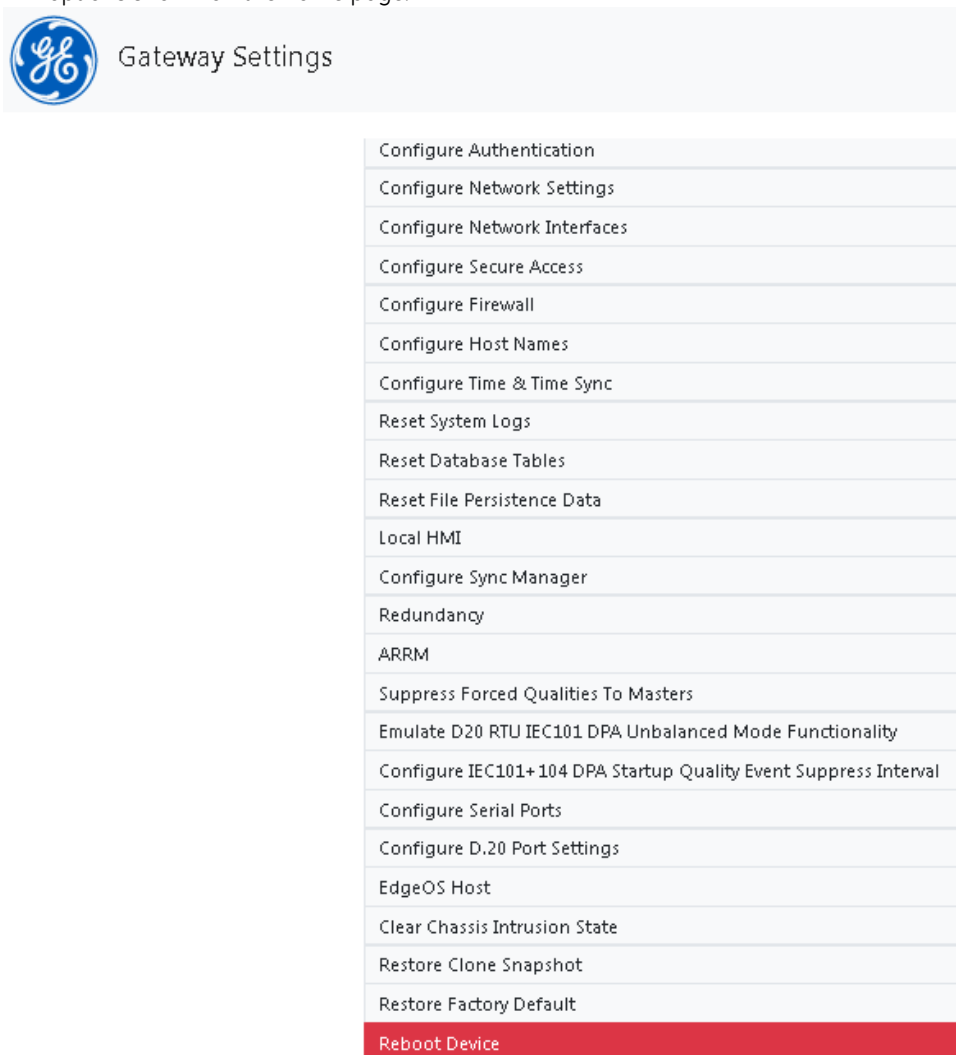
Using Web MCP Settings GUI

1. Login to MCP using local admin user authentication:
   - Entering their User Name.
   - Entering their Password.

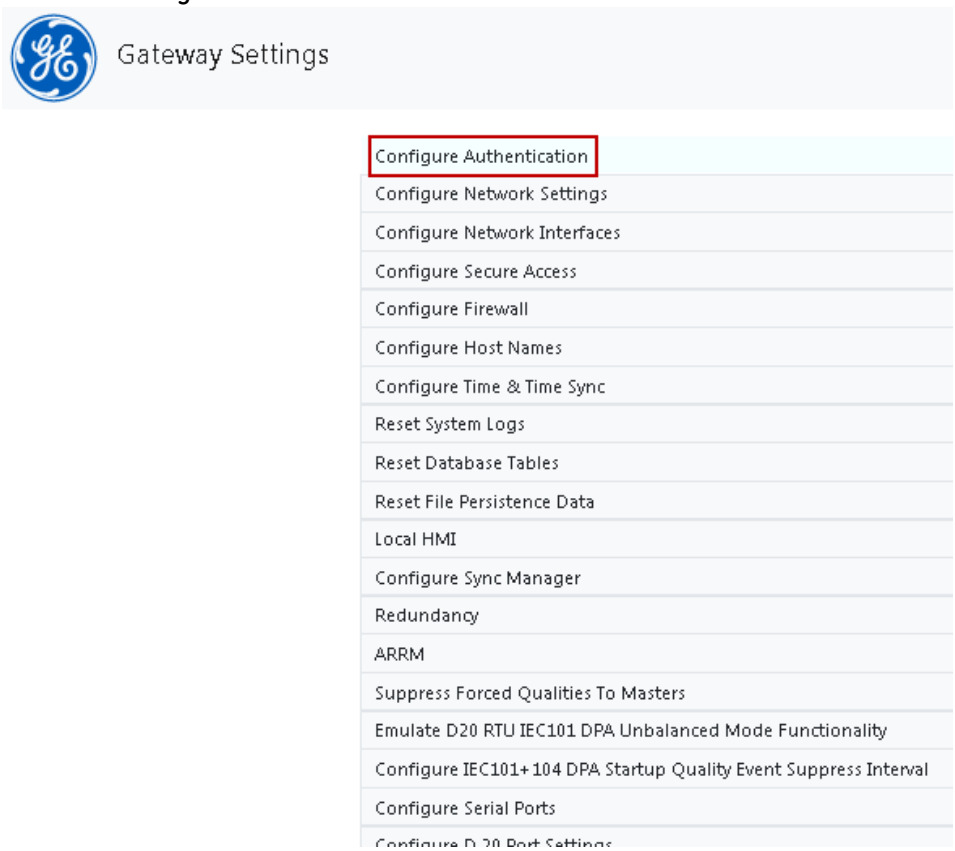
– Selecting Login to advance to the next screen and begin using the application.



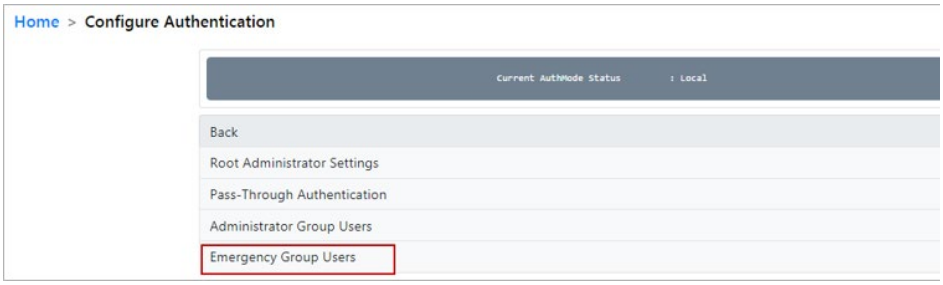
2. Once you have logged in to the MCP Settings, you can see a menu on the center and Logout option on the top right of the screen. To explore the MCP settings use the menu options shown on the home page:



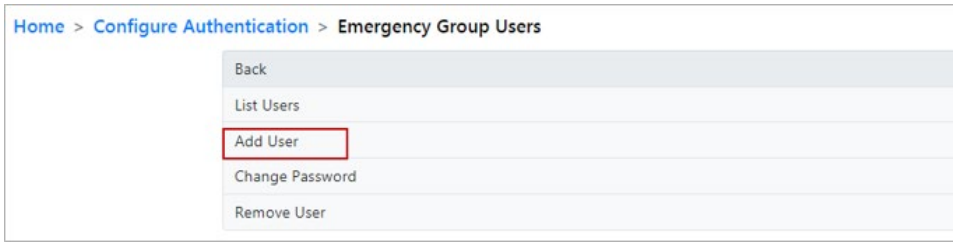
3. Select **Configure Authentication** from the main menu.



4. Click on **Emergency Group User** to add emergency User.

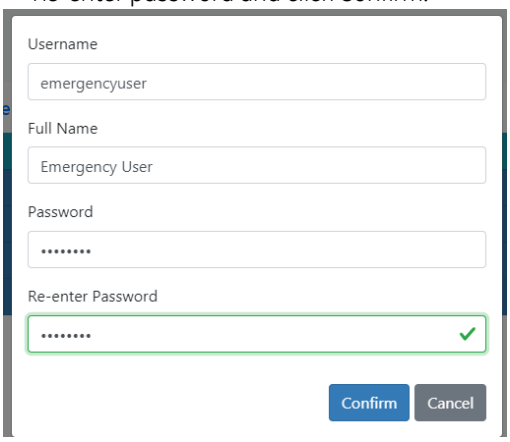


5. To add new emergency user click **Add User** tab.

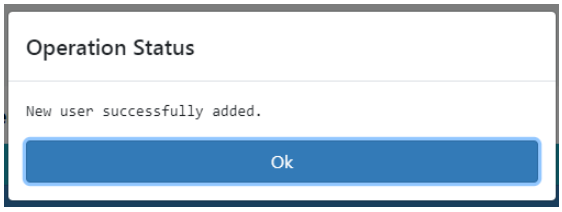


6. Enter the desired Emergency Group Username, conforming to the emergency group username rules as listed below:
   - Emergency Group Username must be between 2 and 31 characters.
   - Emergency Group Username must start with a lowercase alphabetical character.
   - Emergency Group Username must only contain [a-z][0-9][-,_] characters.

7. Enter the Full Name of the emergency group user.
8. Enter the Password, conforming to the password security rules as listed below:
   - Password must be between 8 and 199 characters in length
   - Password must contain:
     - 1 character from [a-z]
     - 1 character from [A-Z]
     - 1 digit from [0-9]
     - 1 special character from the set [$%@!&]
     - Re-enter password and click Confirm.



RESULT: Pop-up window appears showing the Operation Status: **New user successfully added**, click **OK**.



Retrieve LDAP Authentication Server information

Retrieve the following LDAP authentication server information from the IT / Network team of your organization or company:

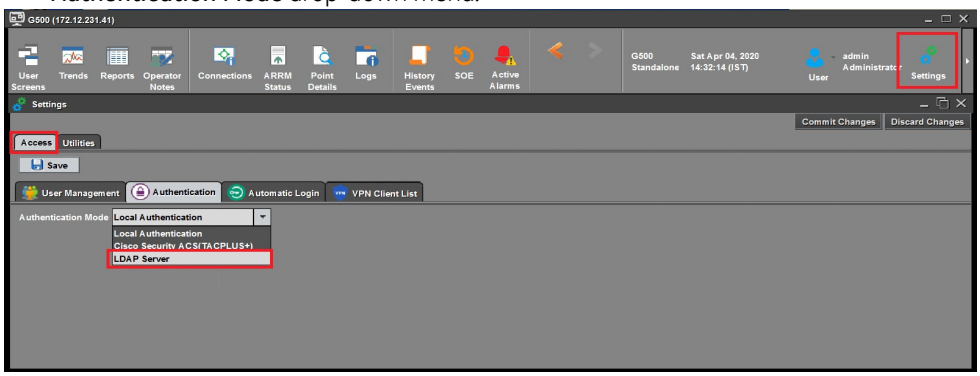
Name	Locate on LDAP Server
Primary Host Name	1. It is full name of your computer (LDAP Server). 2. Open properties of computer or server and view the **Full Name of Computer**
Primary Host IP Address	Open Server Manager in LDAP server and click on AD DS and note down the IP address of server.
Secondary Host Name	This is an optional field. It is full name of your secondary computer (LDAP Server). Open properties of computer or server and view the Full Name of Computer. If the Secondary LDAP Server is configured, MCP shall automatically switch to the secondary server when the primary server is not available.
Secondary Host IP Address	This is an optional field. Open Server Manager in secondary LDAP server and click on AD DS and note down the IP address of server.
LDAP Port	LDAP communication mechanism is TLS/SSL. Port-number = 389 for TLS communication Port-number = 636 for SSL communication

Name	Locate on LDAP Server
Base DN	1. It is Domain Name 2. Open properties of computer or server and view the Domain 3. If Domain is **GE.local** then Base DN will be "**dc=GE,DC=LOCAL**"
Bind User Name	Username of the bind user created in the LDAP server. Assume the user name to login LDAP machine or server is "**ldapbind**" and dc name is "**GE**" and dc type is "**local**" then the bind user name will be (in DN format) "**cn=ldapbind,cn=Users,dc=GE,dc=local**"
Bind Password	Password for the Bind User
Security Type	LDAP communication mechanism is TLS/SSL. Port-number = 389 for TLS communication Port-number = 636 for SSL communication
CA Certificate	Selected the imported CA certificate from the drop-down list.
Bind Time limit in Seconds	Use **30** as default value
User ID Attribute Map	User can use the default value "**sAMAccountName**"
Home Directory Attribute Map	User can use the default value "**unixHomeDirectory**"

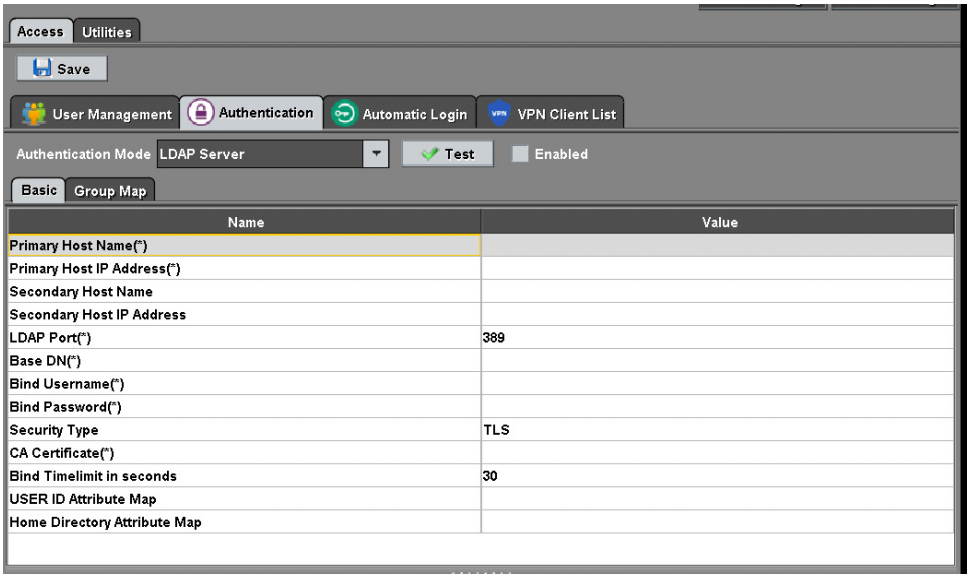
Procedure to configure LDAP on the MCP device

You can configure or change the authentication to LDAP Authentication mode by using HMI. In above section Retrieve LDAP Authentication Server information, we already had collected all the parameters that will be used here for configuration: To configure the LDAP in the MCP device:

1. Login in to MCP HMI with an administrator user name and password.
2. Go to **Settings > Access > Authentication** and select **LDAP server** from the **Authentication Mode** drop-down menu.



3. On selecting the LDAP Server authentication, LDAP configuration page will be opened as below:

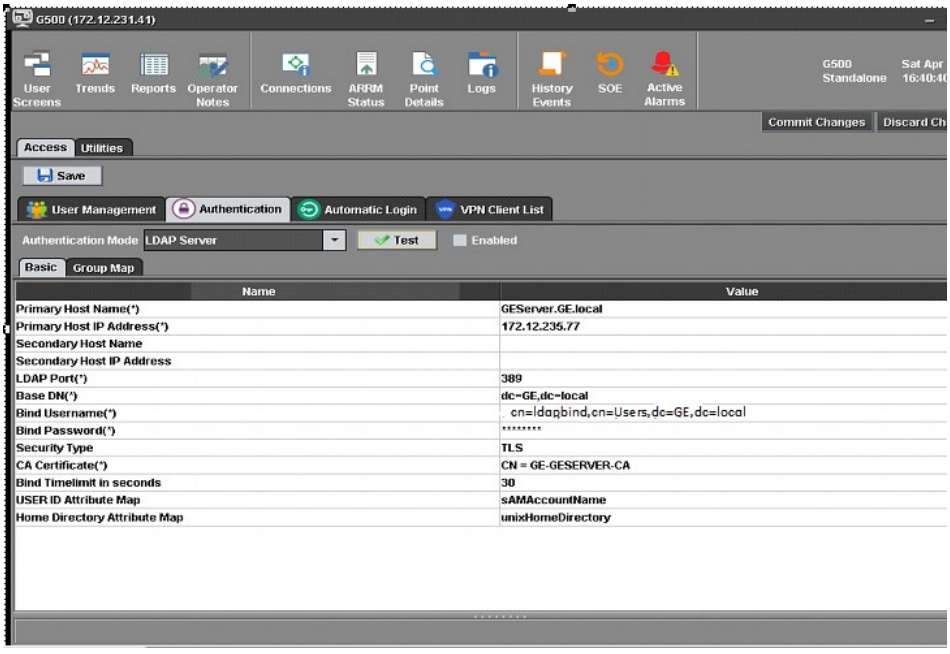


4. Input all the LDAP parameters we already had noted in the above section of this document. Follow the below table as an example to find all the parameter from LDAP server:

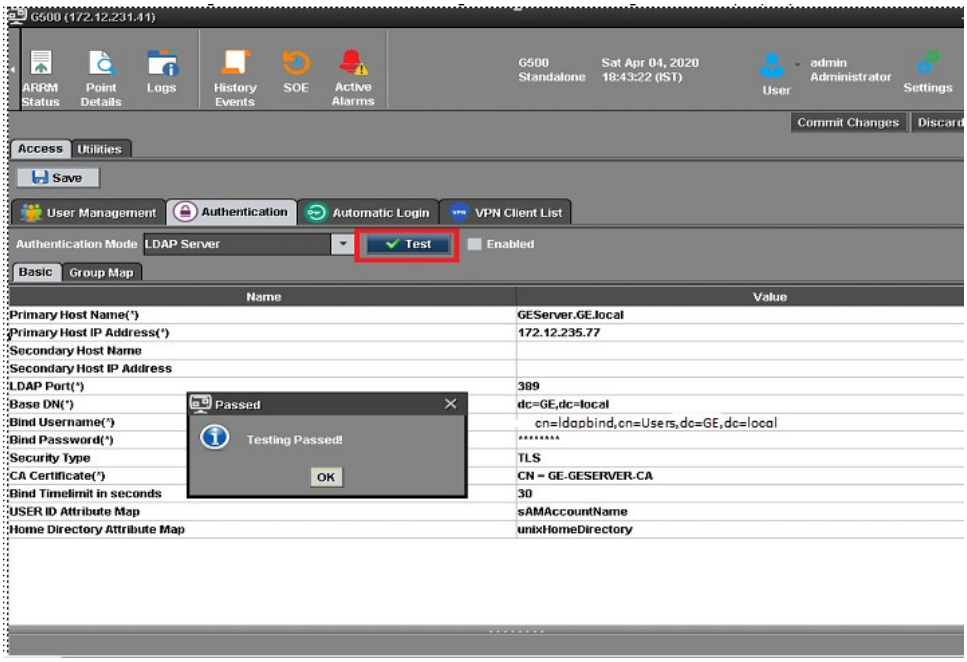
Name	Value	Locate on LDAP Server
Primary Host Name	GEServer.GE.local	1. It is full name of your computer (LDAP Server). 2. Open properties of computer or server and view the Full Name of Computer
Primary Host IP Address	172.12.235.77	Open Server Manager in LDAP server and click on AD DS and note down the IP address of server.
LDAP Port	389	LDAP communication mechanism is TLS/SSL. – Port-number = 389 for TLS communication – Port-number = 636 for SSL communication

Name	Value	Locate on LDAP Server
Base DN	dc=GE,dc=local	1. It is Domain Name 2. Open properties of computer or server and view the Domain 3. If Domain is GE.local then Base DN will be "dc=GE,DC=LOCAL"
Bind User Name	cn=ldapbind,cn=Users,dc=GE,dc=local	Assume the user name to login LDAP machine or server is "ldapbind" and dc name is "GE" and dc type is "local" then the bind user name will be (in DN format) "cn=ldapbind,cn=Users,dc=GE,dc=local"
Bind Password	Password	Enter the bind user password. (This is the password created for the Bind user in the LDAP Server in the earlier steps).
Security Type	TLS	LDAP communication mechanism is TLS/SSL. – Port-number = 389 for TLS communication – Port-number = 636 for SSL communication
CA Certificate	Certificate installed earlier	Select the INSTALLED CERTIFICATE appear on drop down list.
Bind Time limit in Seconds	30	Default Value
User ID Attribute Map	sAMAccountName	sAMAccountName is default value User can find it in user attribute tab in user properties of user in LDAP server
Home Directory Attribute Map	unixHomeDirectory	1. unixHomeDirectory is default value 2. User can find it in user attribute tab in user properties of user

3. Configure these LDAP parameters as shown below. Also, go to the drop-down menu of CA certificate and select the CA certificate for LDAP.

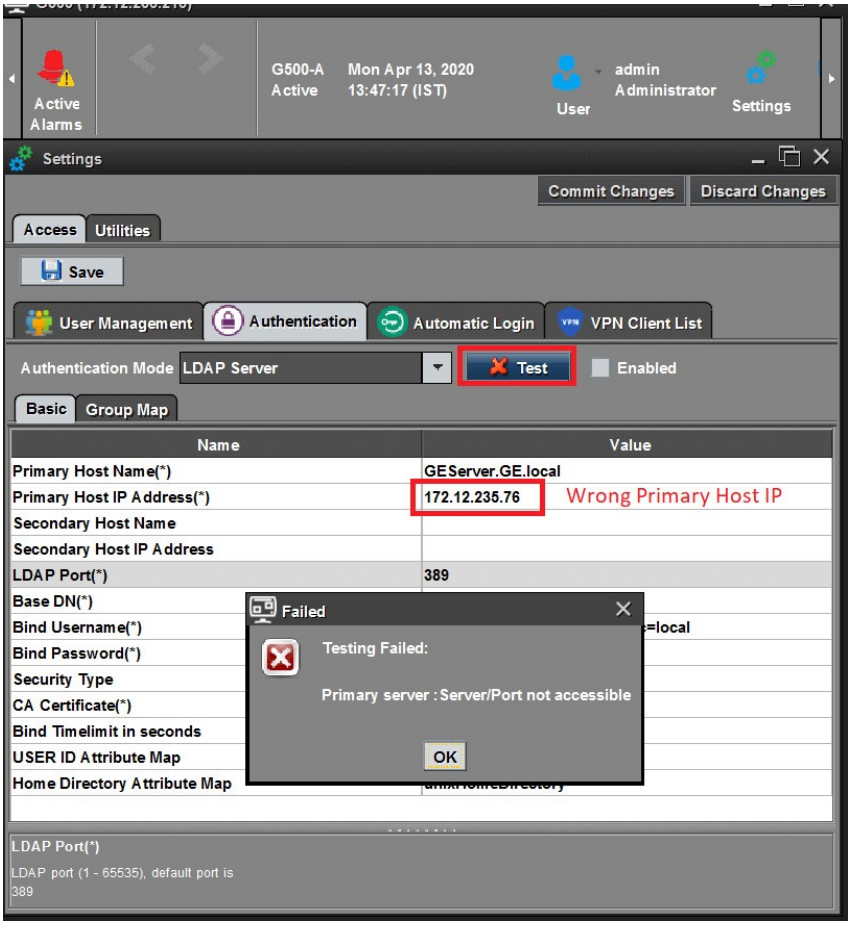


4. Click the **Test** button. It will validate the configuration and availability of LDAP server once the configuration verified, Testing Passed message will be popup. Click **OK**.



Result : The server connectivity is verified.

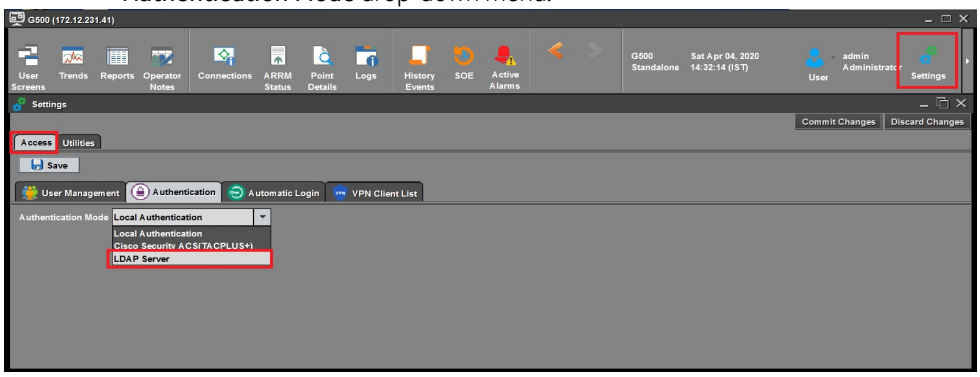
5. If user had input wrong parameter for any of the field and click on test button then it will popup message as "Testing Failed" as below:



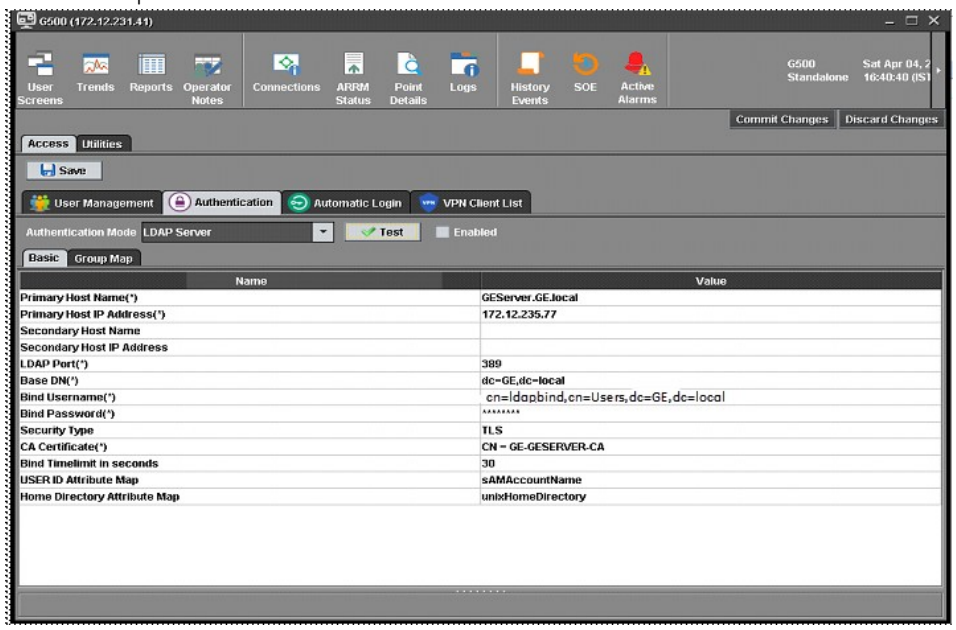
NOTE: Do not select the Enabled field.

6. Click on Save, it will save the configuration parameters, but still the authentication mode is local.
7. Till the above step LDAP configuration has been saved and tested successfully but still the authentication mode is Local. If user want to work with:
   7.1. If user want to work with Static mode of group mapping, then group mapping is not required in MCP. In this case user can directly enable and save the configuration as described in next steps. Static mode of group mapping is described in section Procedure for Static Group Mapping.
   7.2. If user want to work with Dynamic mode of group mapping, then group mapping needs to be done in MCP. Map the group in MCP by following the Procedure for Dynamic Group Mapping. After mapping all the groups in MCP proceed with next step.
8. Procedure to Configure Group Mapping on the MCP Device, if user want to work with dynamic user mapping approach then Group Mapping need to be done in MCP. Follow the below steps for Group Mapping in MCP. If you want to continue with static group mapping, skip the below steps from 8.1 to 8.8 and move to step 9:
   8.1. Procedure for Dynamic Group Mapping. It has been noted in an earlier example that the Distinguished Name (DN) of group "**G500Administrator**" is as "**cn=G500Administrator,cn=users,dc=GE,dc=local**".
   8.2. Login in to MCP HMI with an administrator user name and password.

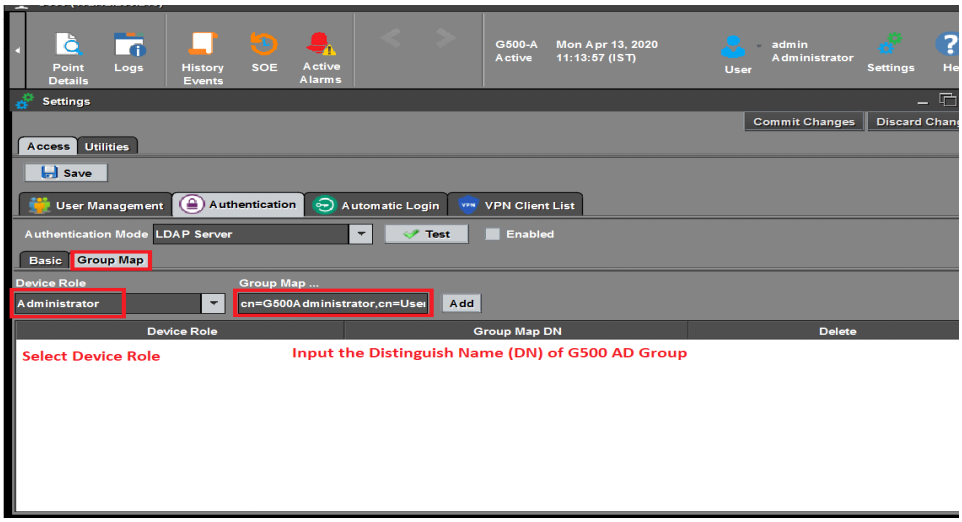
8.3. Go to **Settings > Access > Authentication** and select **LDAP server** from the **Authentication Mode** drop-down menu.



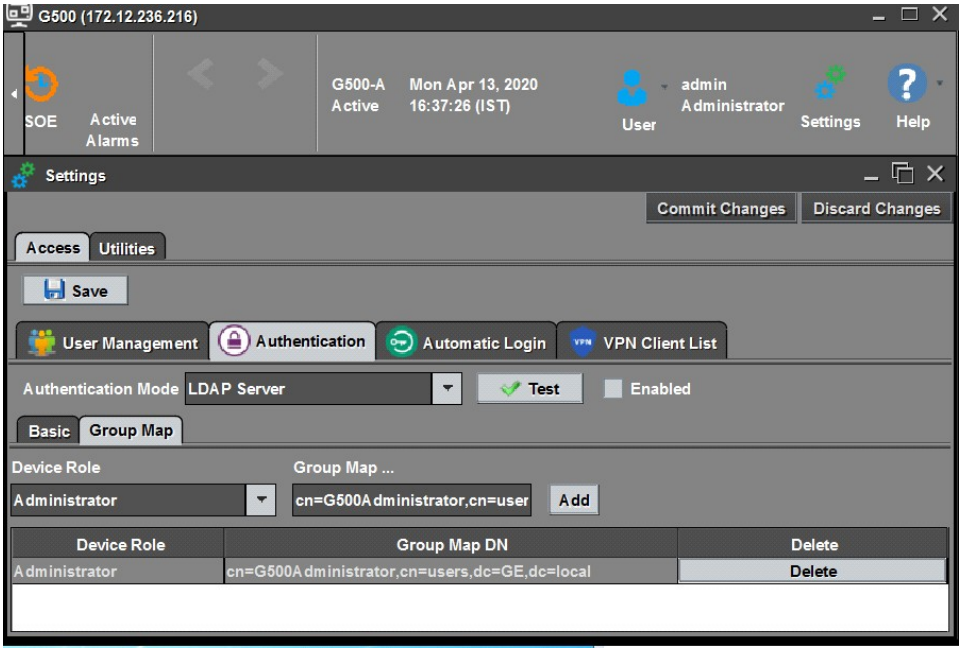
8.4. On selecting the LDAP Server authentication, LDAP configuration page will be opened as below:



8.5. Click on "**Group Map**" tab. Select the **Device Role** of Group from drop down and input the **DN** in Group Map field as shown in below (DN has been noted in step 8.3):



8.6. Click on "**Add**" button, it will add the group in MCP and that group members or users will be privileged with the selected Device Role. For example if User role is selected as Administrator for "**G500Administrator**" user group then users under G500Administrator group will have administrator privilege.

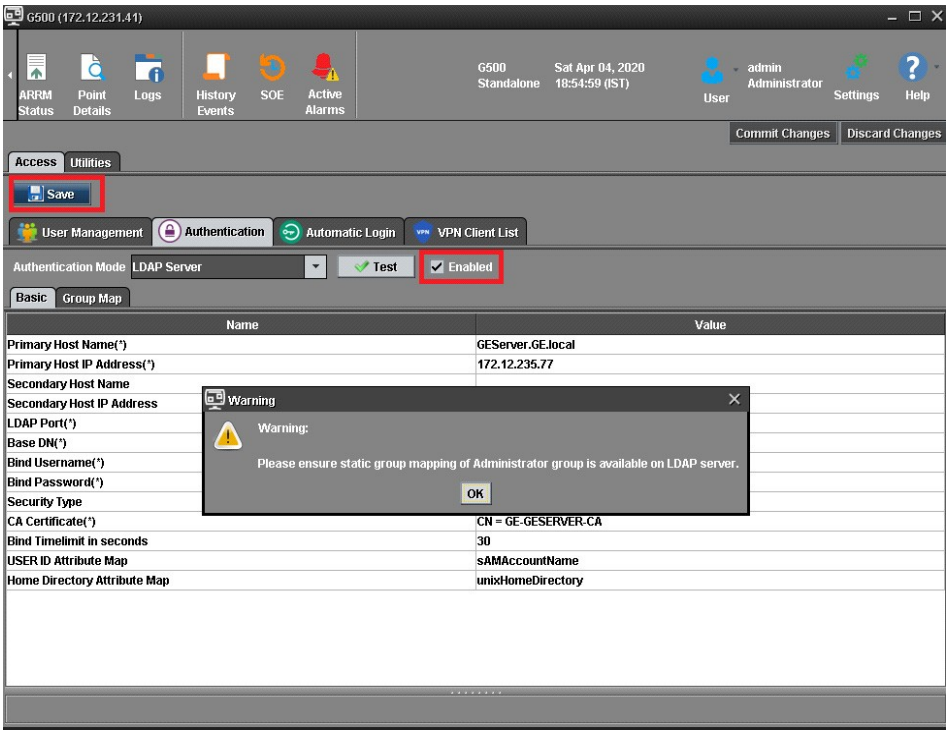


8.7. Similarly add different User groups like G500Operator for Operator privilege, G500Observer for Observer privilege, G500Supervisor for Supervisor privilege, G500Passthrough for Passthrough privilege.

8.8. After adding the user group click on Save to save the configuration.
RESULT: Group Mapping has been done successfully.

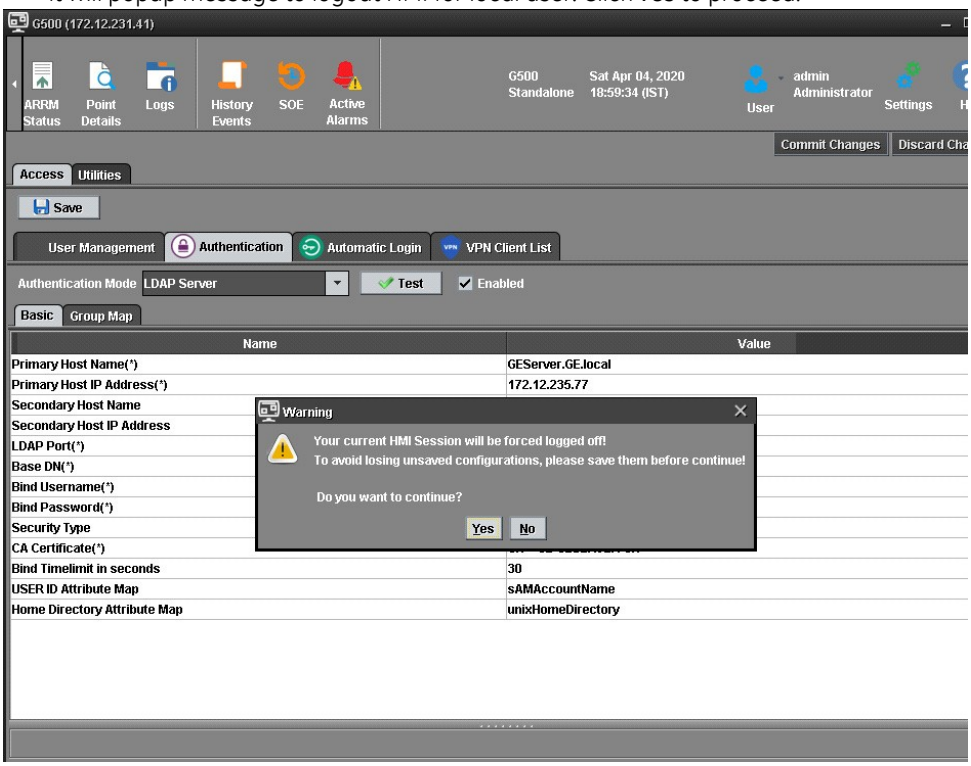
9. **Select the Enabled field and Save**, This step should be done only after completion of Static/ Dynamic Group Mapping it will save this configuration parameters and forcefully logout the HMI for local user and LDAP authentication will be enabled for MCP. Now user can login to MCP by using only LDAP authentication.
NOTE: Select the Enabled field and Save, this will switch to Remote Authentication

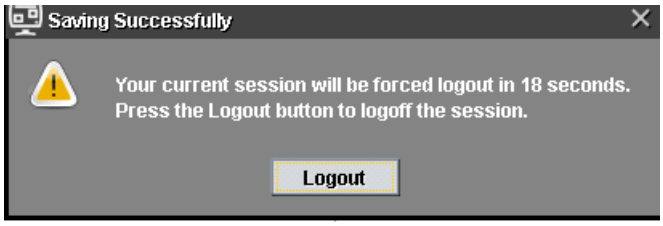
mode.



WARNING: Save with Enabled checked will switch to Remote Authentication immediately!

10. This warning is for the static user should be available to login MCP, click **OK** then again it will popup message to logout HMI for local user. Click **Yes** to proceed:





Result: Now LDAP Authentication mode is successfully enabled, user is required to use LDAP credentials, for login to HMI, DSAS and SSH sessions to MCP.

Configuring the MCP devices for Centralized LDAP Authentication using 389 Directory Server

Appendix A: Troubleshooting

If you encounter issues while testing the operation of the LDAP server configuration, refer to the following listed errors and the recommended responses. When you click the Test Button, if a particular field is configured improperly, the corresponding message appears on the HMI.
The exact error messages may refer to MCP, G500 or G100 – the meaning is identical.

See sections:

- LDAP error messages
- LDAP Certificate error messages

LDAP error messages

Error Message	Response
Host not reachable	Ensure LDAP server was accessible in the network.
	Ensure LDAP server was not shutdown.
unable to access ldap port	Ensure LDAP server was using the specified port for LDAP protocol communication.
Invalid binddn	Ensure mentioned bind user dn (distinguished name) was available in the mentioned domain on the LDAP server.
Invalid bind user credentials	Ensure bind user dn (distinguished name) mentioned in the MCP device LDAP server configuration was correct.
	Ensure bind user password entered was correct in the MCP device LDAP server configuration.
Hostname mismatch with server certificate	Ensure LDAP server host name entered in the MCP device LDAP server configuration was matching with the LDAP server certificate subject name.
Server/Port not accessible	Ensure LDAP server was accessible in the network.
	Ensure LDAP server was not shutdown.
	Ensure LDAP server was using the specified port for LDAP protocol communication.
Invalid Host Name. Full Qualified Domain Name (FQDN) has invalid characters	Ensure Primary Host Name is configured in MCP device LDAP server configuration.

Error Message	Response
Invalid Host IP Address	Ensure Primary Host IP Address configured in MCP device LDAP server configuration is correct.
Failed to connect to Primary Host	Ensure LDAP Server is accessible in the network.
	Ensure Primary Host Name configured in MCP device LDAP server configuration is correct.
	Ensure Base DN configured in MCP device LDAP server configuration is correct.
	Ensure Bind User credentials (Bind Username and Bind Password) configured in MCP device LDAP server configuration are correct.
Primary Server :Server/ Port not accessible	Ensure LDAP Server is not shutdown.
	Ensure Primary Host IP Address configured in MCP device LDAP server configuration is correct.
Configuration Timeout, please try again later	Ensure LDAP server was using the specified port for LDAP protocol communication.
Invalid User ID Attribute Map	Ensure User ID Attribute Map defined in LDAP Server is configured in MCP device LDAP server configuration.
Invalid HomeDirectory Attribute Map	Ensure HomeDirectory Attribute Map defined in LDAP server is configured in MCP device LDAP server configuration.
Connected to secondary Host, but failed to connect to primary Host	Ensure Primary Host Name and Primary Host IP Address configured in MCP device LDAP server configuration are correct.
Failed to connect to both primary and secondary Hosts	Ensure Primary Host Name and Secondary Host Name configured in MCP device LDAP server configuration are correct.
	Ensure Primary Host IP Address and Secondary Host IP Address configured in MCP device LDAP server configuration are correct.
	Ensure Base DN configured in MCP device LDAP server configuration is correct.
	Ensure Bind User credentials (Bind Username and Bind Password) configured in MCP device LDAP server configuration are correct.
Please add Emergency User before switching to LDAP/TACACS Authentication	Ensure at least one emergency admin group user is configured before switching to LDAP/TACACS Authentication.
The current Authentication Mode has been enabled. You cannot disable it unless switching to a different Authentication Mode	Current Authentication Mode is LDAP. Ensure to disable (Enabled checkbox unchecked) only when switching to a Authentication Mode other than LDAP.

LDAP Certificate error messages

Error Message	Response
List of trusted certificates is not complete	The issuer certificate of a looked up certificate could not be found. This normally means the list of trusted certificates installed on the MCP device or certificate list from LDAP server was not complete.
Unable to decrypt certificate's signature	The certificate signature could not be decrypted. This means that the actual signature value could not be determined rather than it not matching the expected value, this is only meaningful for RSA keys.
unable to decode issuer public key	The public key in the certificate SubjectPublicKeyInfo of MCP device server could not be read.
certificate signature failure	The signature of the installed certificate on MCP device server certificate was invalid.

Error Message	Response
certificate is not yet valid	MCP device time might be backward w.r.to certificate valid time.
	The certificate is not yet valid: the not Before date is after the current time.
certificate has expired	CA certificate installed on MCP device got expired w.r.to LDAP server.
	MCP device time might be forward w.r.to certificate valid time.
	The certificate has expired: that is the notAfter date is before the current time.
format error in certificate's notBefore field	The certificate notBefore field contains an invalid time.
format error in certificate's notAfter field	The certificate notAfter field contains an invalid time.
Self-signed certificate cannot be found in the list of trusted certificates.	The passed certificate is self-signed and the same certificate cannot be found in the list of trusted certificates.
self-signed certificate in certificate chain	Ensure Installed a trusted CA signed primary SSL certificate and an intermediate certificate.
	Verify that the Root CA is not included in the certificate chain (as this is almost always self-signed).
unable to get local issuer certificate	This error code is thrown when a local certificate path is not found during the certificate check.
	LDAP server certificate's issuer certificate was not found, after looking in both the chain provided by the LDAP server and in the local trusted storage. This usually means the peer chain was missing or incomplete.
unable to verify the first certificate	The primary certificate (the one you purchase from a vendor) cannot establish the chain of trust between itself and the Root certificate stored locally. Usually installing the intermediate certificates fixes this.
certificate chain too long	The certificate chain length is greater than the supplied maximum depth.
	The LDAP server certificate's chain length exceeded the limit set locally by sslverifydepth or SSL Verify Depth. The chain length (depth) is the number of certificates beyond the leaf (client or server) certificate itself.
	a chain of length 1 is a leaf certificate plus its issuer certificate.
invalid CA certificate	A CA certificate is invalid. Either it is not a CA or its extensions are not consistent with the supplied purpose.
path length constraint exceeded	The basicConstraints path length parameter has been exceeded for certificate.
invalid or inconsistent certificate extension	invalid or inconsistent certificate extension
Hostname mismatch	Ensure LDAP server host name entered in the MCP device LDAP server configuration was matching with the LDAP server certificate subject name.
Certificate directory empty	No certificates installed over to the MCP device.

Configuring the MCP devices for Centralized LDAP Authentication using 389 Directory Server

Appendix B: List of Acronyms

Acronym Definitions

This Appendix lists and defines the acronyms used in this manual.

Table 1: Acronym list

Acronym	Definition
CS	Certificate Services
DS	Domain Services
CA	Certificate Authority
MCP	MCP Substation Gateway
mcpcfg	Local configuration utility
DN	Domain Name
DNS	Domain Name System
FQDN	Full Qualified Domain Name
GE	General Electric
HMI	Human Machine Interface (also called Graphical User Interface – GUI)
IP	Internet Protocol
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
NIS	Network Information Service
NTDS	TechNet Directory Services
PC	Personal Computer
PEM	Privacy Enhanced Mail
PKCS	Public-Key Cryptography Standards, published by RSA Laboratories
SCADA	Supervisory Control and Data Acquisition
SCP	Session Control Protocol
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm

Acronym	Definition
SSL	Secure Sockets Layer
TLS	Transport Layer Security
USB	Universal Serial Bus
XCA	X Certificate and Key management

Configuring the MCP devices for Centralized LDAP Authentication using 389 Directory Server

Appendix C: Revision History

This appendix provides the document revision history.

Revision history

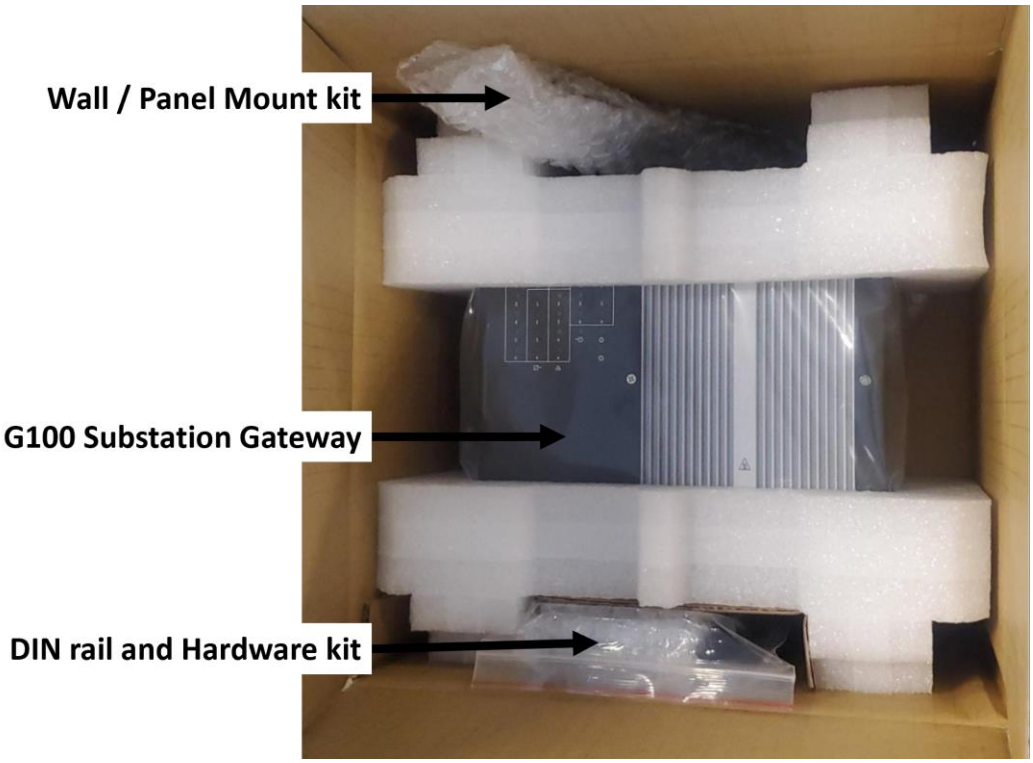
Version	Revision	Date	Change Description
1.00	0	April 27, 2020	Initial release.
2.00	0	April 26, 2021	Updated for MCP family.

GE Grid Solutions

G100 Substation Gateway

Quick Start Guide

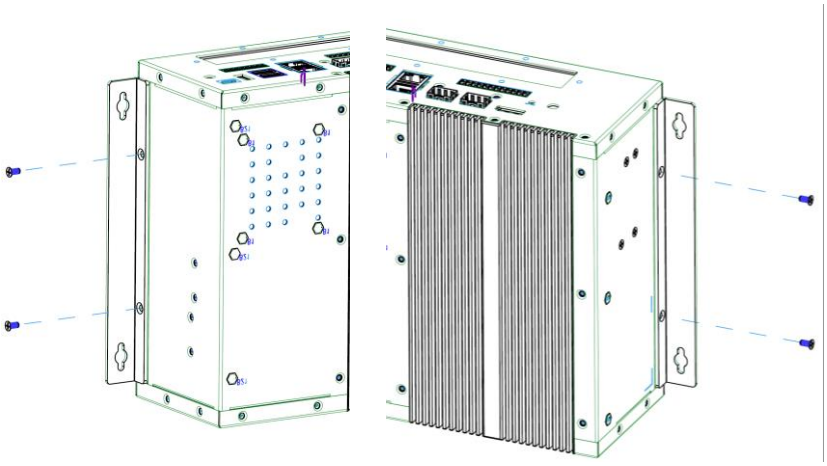
What's in the Box?



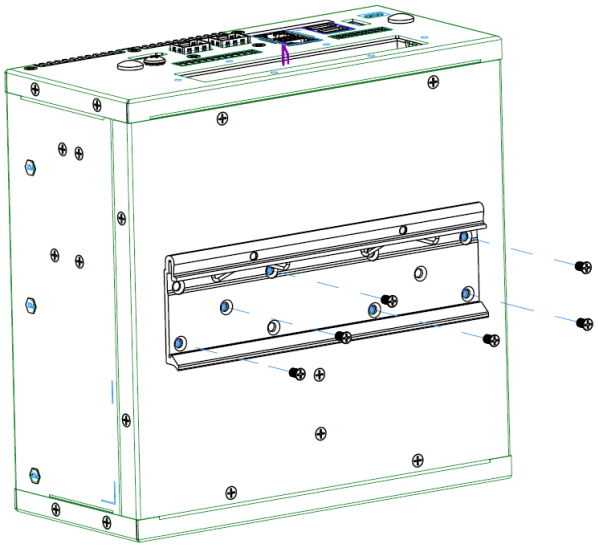
Your kit includes:

- G100 Substation Gateway
- Wall / Panel mount kit
  - Wall / panel mounting bracket (quantity 2)
- DIN rail and hardware kit
  - DIN Rail (quantity 1)
  - Screws (quantity 6)
  - Analog DC Input (AI) connector (quantity 1)
  - Binary Input (DI) connector (quantity 1)
  - Binary Output (DO) connector (quantity 1)
  - Power input connector (quantity 1)
  - IRIG-B input connector (quantity 1)

The Wall / Panel mount kit included in the G100 carton includes 2 wall/panel mount bracket. The 2 wall/panel mount brackets can be optionally attached to the G100 chassis for mounting the G100 to a wall or panel. The brackets are attached to the G100 chassis using the 2 lower M3 screws on the left and right side of the chassis. Refer to the Instruction Manual for full installation procedure.



The DIN rail and hardware kit included in the G100 carton includes a DIN rail bracket along with 6 mounting screws. The DIN rail bracket can be optionally attached to the back of the G100 chassis for DIN rail mounting applications. Refer to the Instruction Manual for full installation procedure.



Missing Something?

Contact GE Customer Service right away and we'll figure it out. Be sure to include your order number and mail address associated with your order.

Prerequisites

- DS-Agile Studio's MCP Studio.
- Minimum Windows 7 x64, 10 x64 and 8GB Memory required for DS Agile MCP Studio.

G100 Interface Options

The following connection/interface options are available after G100 first powers up.

- Local KVM (Keyboard, Video, Mouse)
- Ethernet port # 1 – Default IP address 192.168.168.81
- Serial port # 4 in RS232 mode, with a baud rate 115200

Setup & Configuration Tools

The following setup & configuration tools are available for the G100.

1. **DS Agile MCP Studio** Offline & Online Editor : To configure the Gateway & SCADA Configuration.
2. **G100 Runtime HMI** (Remote/Local) : To view and control the runtime stats including One-line diagrams and to configure the G100 Settings (e.g. User Management, Automatic Login etc.).
3. **G100 Gateway Settings GUI (or Shell based application)** : To configure G100 system settings and perform the initial G100 setup (e.g. Users, network, serial, time sync etc.).

NOTES:

- The G100 and G500 are part of the same ***MCP*** (Multifunction Controller Platform) family and share the same applications and workflows.
- Due to this, some options are available in G500 and not available in G100 and are marked as such where applicable (e.g. G500 has 6 Ethernet ports, G100 only 4, etc.). Attempting to configure settings marked as not available in G100 will not result in any changes.
- Sections and figures in this document, various prompts, and menus – refer to MCP, and are applicable to either G100 or G500, unless marked specifically otherwise.

Shell access-based Settings workflow

This document presents Settings workflows based on the Web based Settings GUI interface.

The same settings operations can be performed using a terminal emulator connected to the G100 Shell, either via the serial maintenance port #4 or using an SSH (port 22) connection.

1. Start a terminal session and log into the G100 with an Administrator-level or root user account.
2. At the G100 #>> prompt, enter the following commands:
    - **sudo mcpcfg**

Result: The shell-based settings application starts:

```
================================================================
        Gateway Settings Menu
================================================================

        0.   Back
        1.   Configure Authentication
        2.   Configure Network Settings
        3.   Configure Network Interfaces
        4.   Configure Secure Access
        5.   Configure Firewall
        6.   Configure Host Names
        7.   Configure Time & Time Sync
        8.   Reset System Logs
        9.   Reset Database Tables
        10.  Reset File Persistence Data
        11.  Local HMI
        12.  Configure Sync Manager
        13.  Redundancy (Not available in G100)
        14.  ARRM
        15.  Suppress Forced Qualities To Masters
        16.  Emulate D20 RTU IEC101 DPA Unbalanced Mode Functionality
        17.  Configure IEC101+104 DPA Startup Quality Event Suppress Interval
        18.  Configure Serial Ports
        19.  Configure D.20 Port Settings
        20.  EdgeOS Host
        21.  Clear Chassis Intrusion State (Not available in G100)
        22.  Restore Clone Snapshot
        23.  Restore Factory Default
        24.  Reboot Device

Enter Your Choice : ( Between 0 and 24 ):
```

G100 Gateway Settings GUI

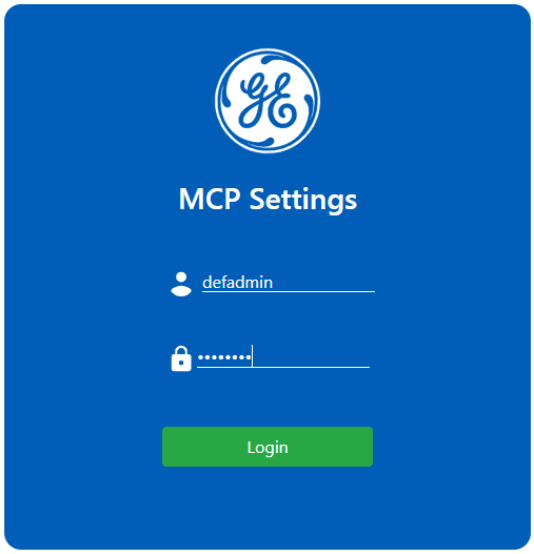
The local G100 settings, including Serial ports, Network configuration, Time settings, Administrators user management etc. are managed using the Gateway Settings GUI.

You can access MCP Settings Web Interface through Local (KVM) or Remote G100 connection. Remote access must be completed using a supported web browser (Internet Explorer, Microsoft Edge, Mozilla Firefox, Google Chrome).

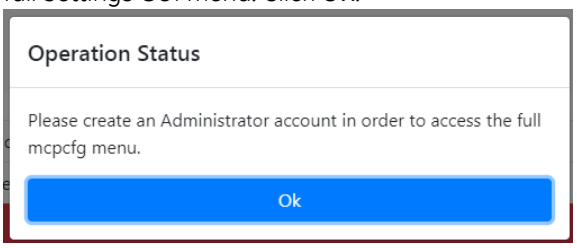
Initial Setup

NOTE: Initial Setup section is identical between Local KVM/Remote access.

1. Enter the default **Username** (defadmin), default **Password** (defadmin) and click **Login**.

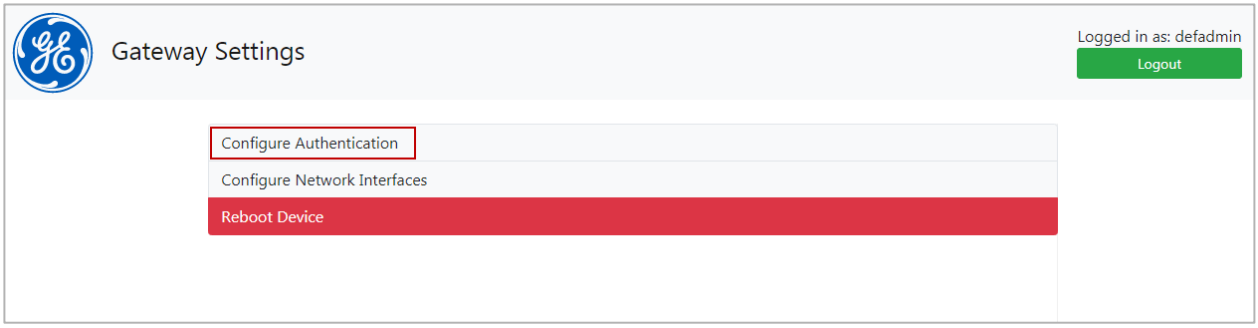


2. If the defadmin account is used to login, you will be prompted to create an Administrator account in order to access the full Settings GUI menu. Click **OK**.

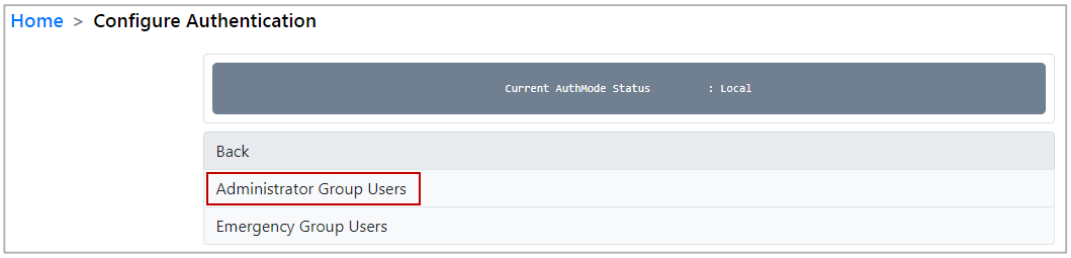


3. The Gateway Settings main menu appears:

4. Select **Configure Authentication** tab from main menu.

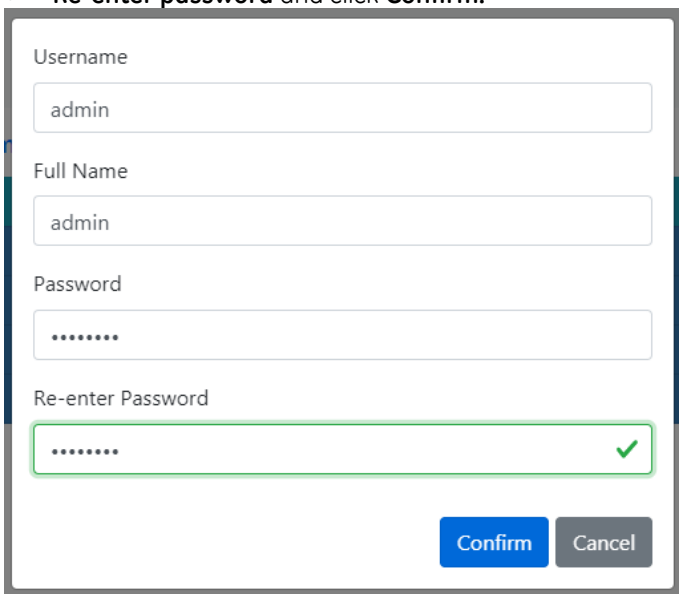


5. Select **Administrator Group Users** tab from Configure Authentication menu.

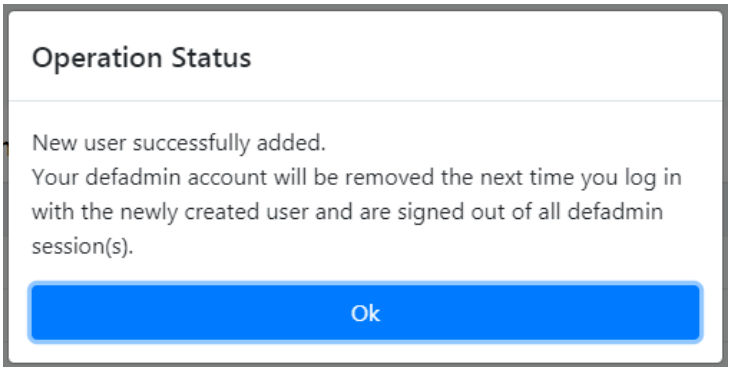


6. This function is used to perform the following actions:
   - List Users
   - Add User
   - Change Password
   - Remove User
7. Select **Add User** tab to create administrator-level users.
   - Enter the desired **Username**, conforming to the Username rules as listed below:
     - Username must be between 2 and 31 characters.
     - Username must start with a lowercase alphabetical character.
     - Username must only contain [a-z][0-9][-,_] characters.
   - Enter the **Full Name** of the User.
   - Enter the **Password**, conforming to the password security rules as listed below:
     - Password must be between 8 and 199 characters in length.
     - Password must contain:
       - 1 character from [a-z]
       - 1 character from [A-Z]
       - 1 digit from [0-9]
       - 1 special character from the set [$%@!&]

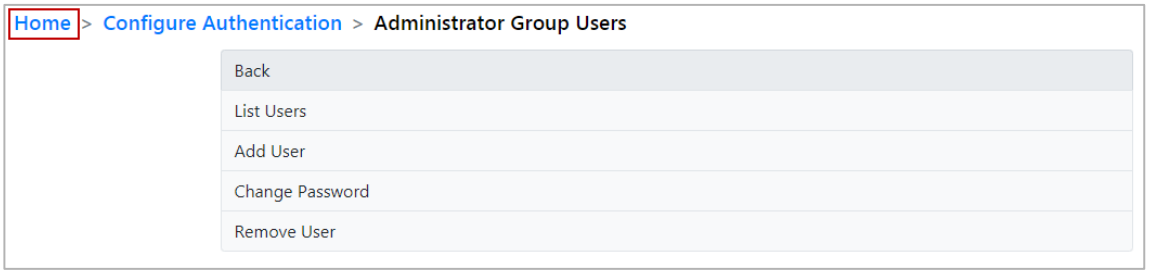
- **Re-enter password** and click **Confirm.**



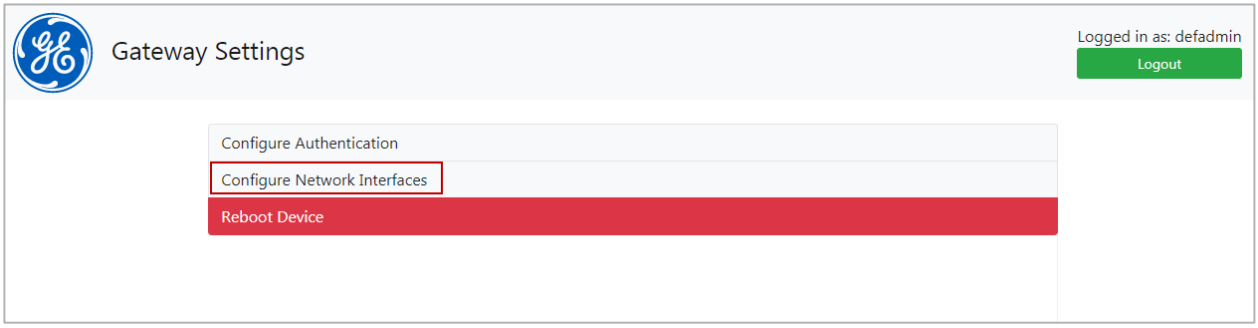
8. **RESULT:** Pop-up window appears showing the Operation Status, click **OK.**
NOTE: defadmin account will be removed the next time you log in with the newly-created user and are signed out of all defadmin sessions.



9. Navigate back to the main menu by clicking on the **HOME** link located at the upper left corner of the page.



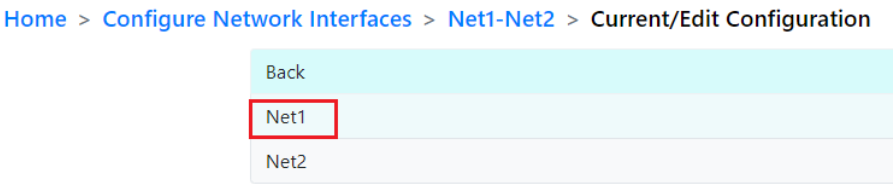
10. Select **Configure Network Interfaces** tab from main menu.



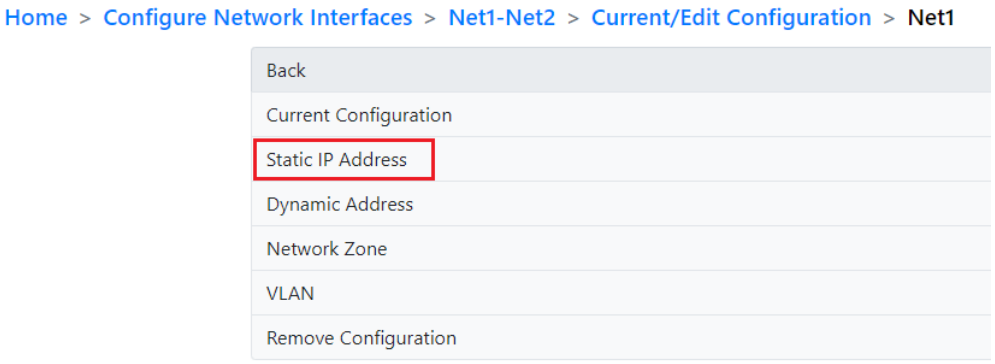
11. Select the desired Network port (default **Net1-Net2**/192.168.168.81) which is connected to G100 device from the list.

12. Select **Current/Edit Configuration** tab.

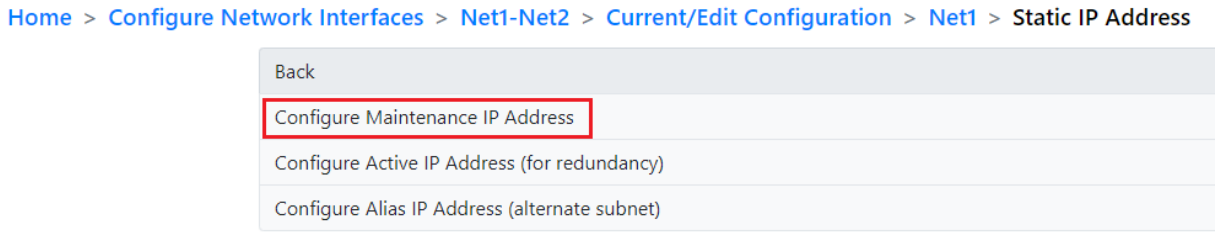
13. Select **Net1** tab.



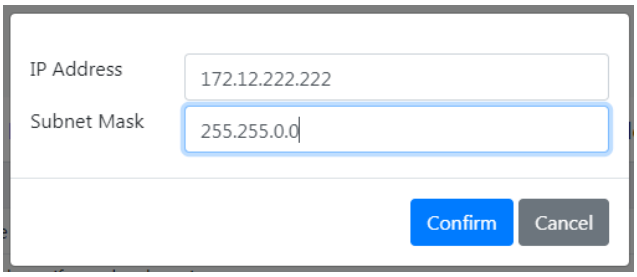
14. Select **Static IP Address** tab.



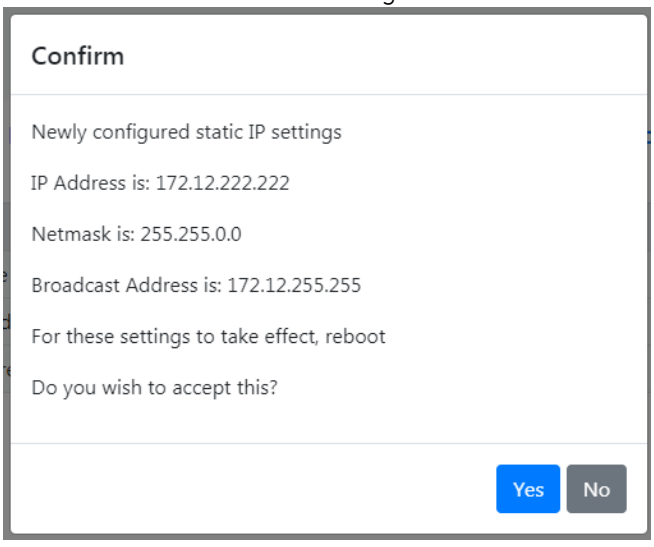
15. Select **Configure Maintenance IP Address** tab.



16. Enter **IP Address** and **Subnet Mask**. Click **Confirm**.

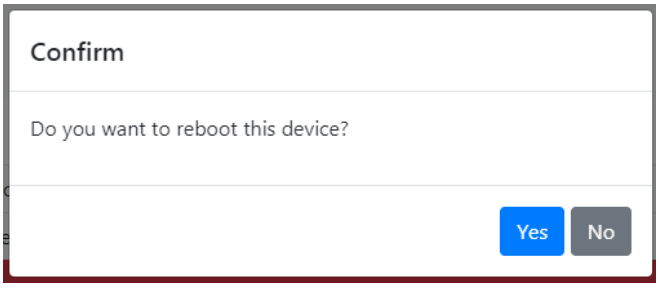


17. Click **Yes** to confirm the newly-configured static IP settings.
NOTE: Reboot the device for changes to take effect.

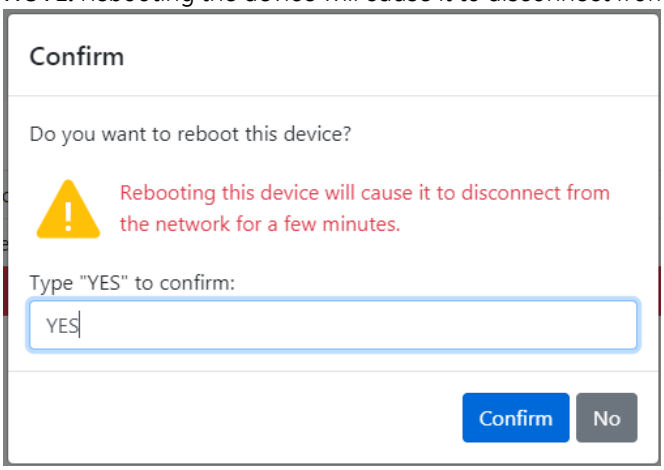


18. Navigate back to main menu and select **Reboot Device** tab.

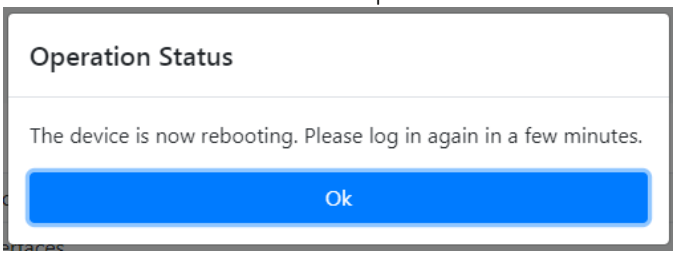
19. Click **Yes** to confirm Reboot the device.



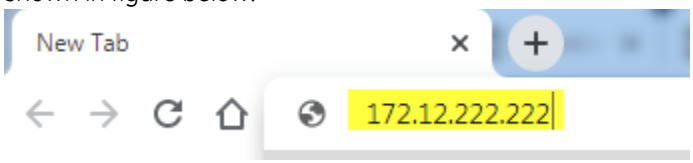
20. Type "**YES**" and click **Confirm**.
NOTE: Rebooting the device will cause it to disconnect from the network for a few minutes.



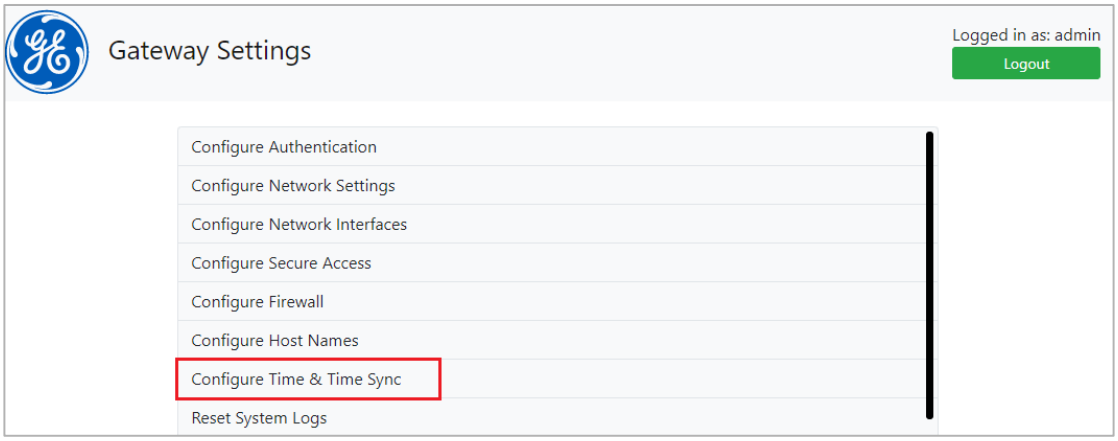
RESULT: The device reboot takes place. Click **OK**.



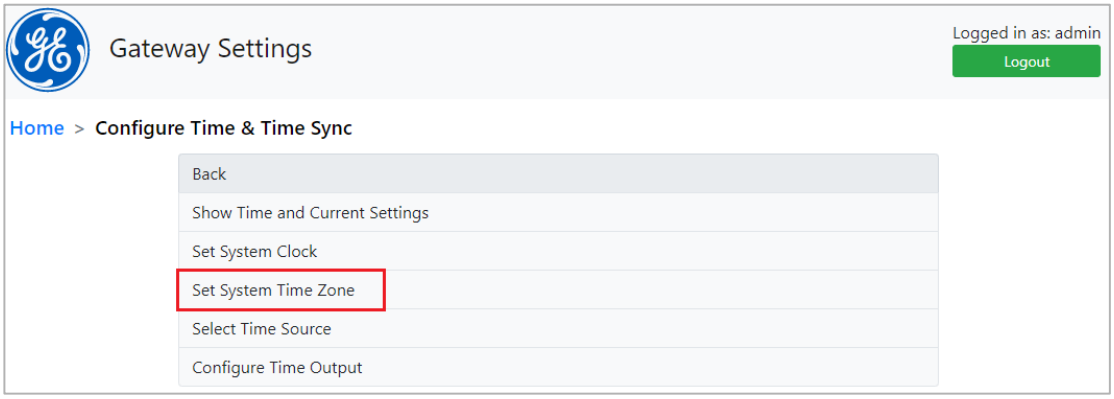
21. Upon G100 reconnect, you can access MCP Web Interface remotely via the newly configured IP Address and a supported web browser. In the supported browser address bar, type in the new G100 device IP (ex.: **172.12.222.222**) as shown in figure below:



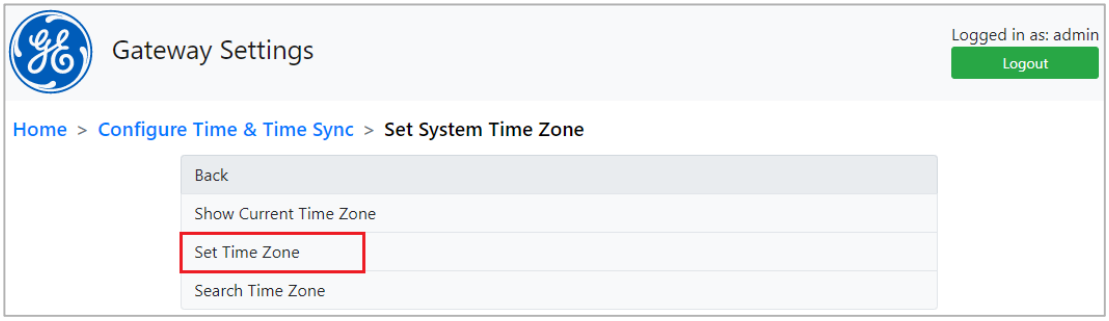
22. Press the 'Enter key' and the MCP Settings Login page appears.
23. Login using the newly created admin username/password and click on the "Login" button.
24. Select **Configure Time & Time Sync** tab.



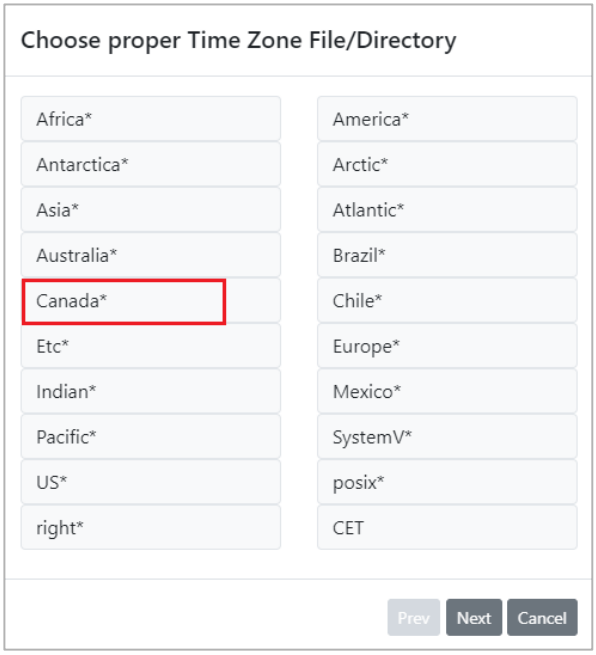
25. Select **Set System Time Zone** tab.



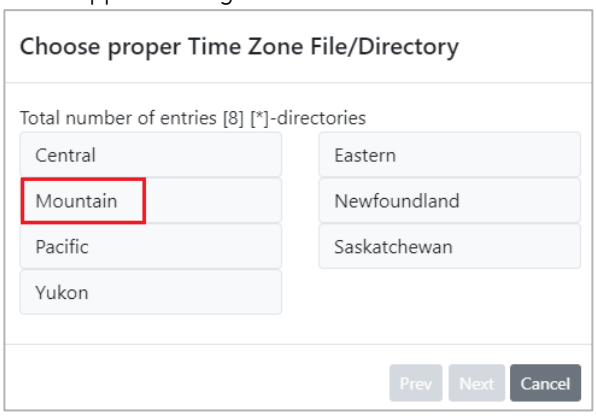
26. Select **Set Time Zone** tab. Configure the G100 to the same time zone as remote PC.



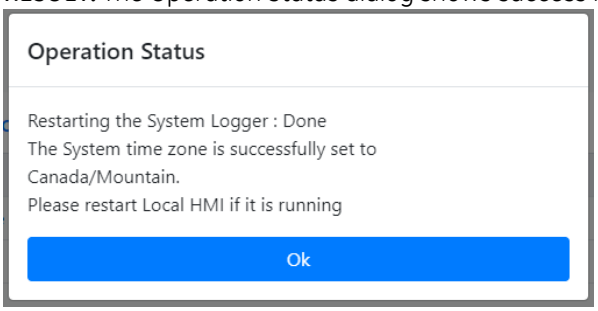
27. Select applicable time zone. User can navigate the menu using Prev/Next buttons.



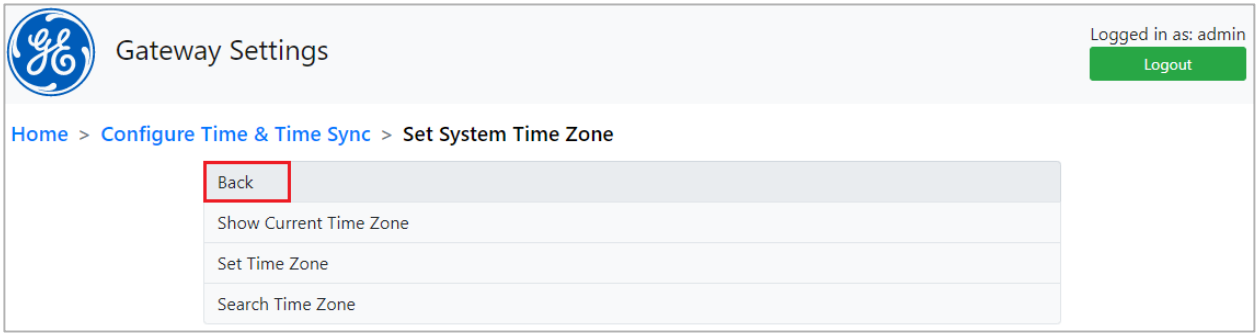
28. Select applicable region within the selected time zone.



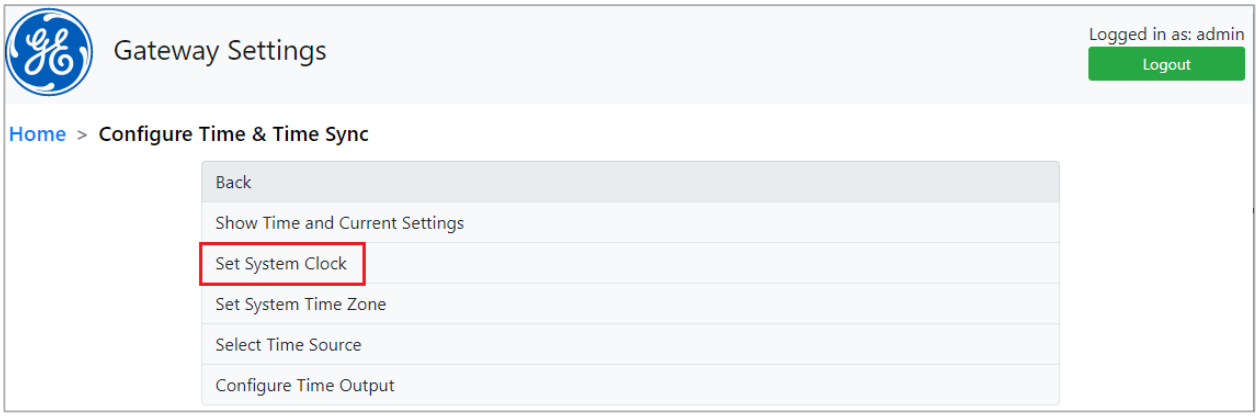
RESULT: The Operation Status dialog shows success message. Click **OK**.



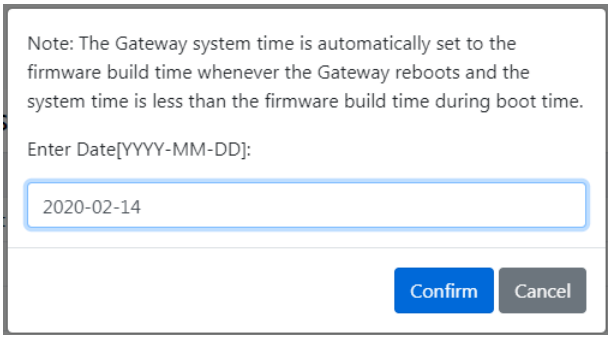
29. Select the **Back** tab.



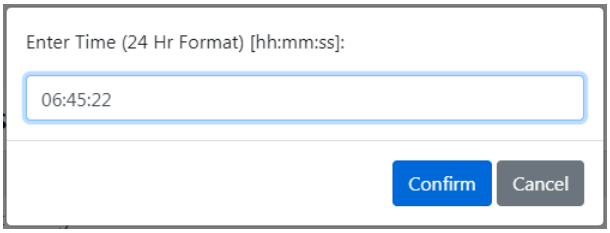
30. Select the **Set System Clock** tab.



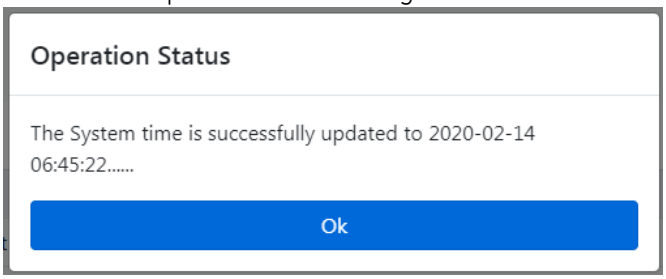
31. A dialog is displayed informing the user to enter a date using the format **YYYY-MM-DD**. Enter **today's date** and select the **Confirm** button.



32. A dialog is displayed informing the user to enter time, using the **24 Hr Format hh:mm:ss**. Enter **remote PC time** and select the **Confirm** button.

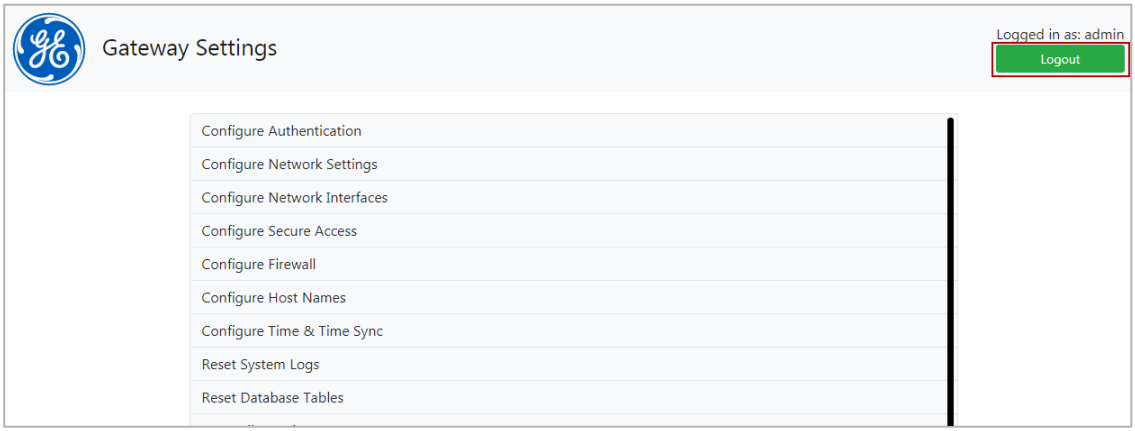


RESULT: The Operation Status dialog shows success message. Click **OK**.

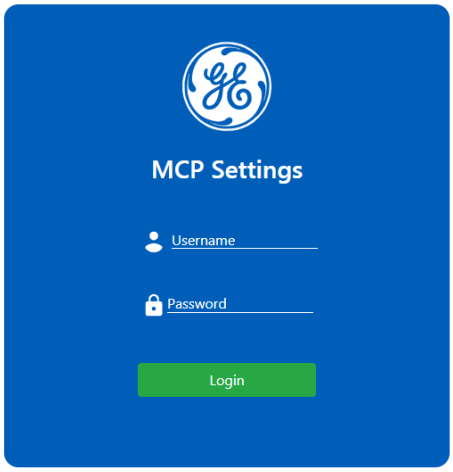


Logout

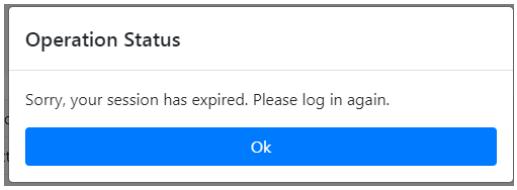
To logout, click on the link to "Logout" located at the upper right corner of the page as shown in figure below.



When you have successfully logged-out of the system, the screen below will be displayed.



NOTE: After 20 minutes of inactivity, the session is automatically timed out and a message will be displayed as shown in below figure. In such cases, either click on "OK" and login again or click on any of the links to be redirected to the log in page.



G100 Snapshot Compatibility

The below table shows the G100 Snapshot Compatibilities, as well as available conversion paths from D400 or G500 to G100:

FULL "Clone" Snapshot compatibility Configuration+Settings (using DSAS 2.1 or later)		Restore snapshot (Configuration and Settings) **to target device:**				Restore snapshot (Only Configuration part) **to offline device:**			
Save snapshot **from device:**		**D400**	**MCP (G500/G100 within same type)**			**D400**	**MCP (G500/G100 within same type)**		
		Any version	**1.00**	**1.10**	**2.00 or later**	**Any version**	**1.00**	**1.10**	**2.00 or later**
D400	<= 5.20	YES ONLY same D400 and same version	N/A	N/A	N/A	YES Direct same version	N/A	N/A	N/A
	5.30 or later	YES ONLY same D400 and same version	N/A	N/A	N/A	YES Direct same version	Indirect Via Create MCP	Indirect Via Create MCP	Indirect Via Create MCP
MCP	1.00	N/A	YES ONLY same MCP	N/A	YES ANY MCP	N/A	YES Direct	Indirect Via Offline Upgrade	Indirect Via Offline Upgrade
	1.10	N/A	N/A	YES ANY MCP	YES ANY MCP	N/A	N/A	YES Direct	Indirect Via Offline Upgrade
	2.00 or later	N/A	N/A	N/A	YES ANY MCP	N/A	N/A	N/A	YES Direct same version

G100 Snapshot Management

"Snapshots" are an archived image of the G100 configuration created using DS Agile MCP Studio, which include all settings required to completely recover a G100 device. This workflow greatly reduces time when replacing hardware, eliminating the need for additional manual configuration.

Using DS Agile MCP Studio, Snapshots can be restored to the G100 using the "**defadmin**" default credentials.

Restoring a Snapshot updates the new G100 with the following hardware and software settings as were defined in the original G100, at the time when the snapshot was taken:

1. User Authentication
2. Network Settings
3. Network Interfaces
4. Secure Access
5. Firewall settings
6. Host Names
7. Time settings and time synchronization
8. Local HMI settings – except number of displays and displays resolution which are specific to the G100 being restored
9. Synch Manager
10. Emulation of D20 IEC101 DPA Unbalanced Mode and quality event suppression at startup
11. Serial port modes (RS232/485, 2/4 wires)
12. Configuration implemented in MCP Studio:
    - Connections
    - Client and Server Map files
    - System Point Manager
    - Alarms
    - Calculator
    - Data Logger (storage may need to be re-adjusted if the target G100 has different storage sizes)
    - Load Shed
    - Systemwide (storage may need to be re-adjusted if the target G100 has different storage sizes)
    - Access (Local users, Automatic HMI login settings, VPN Client List)
    - ARRM
    - AI Text Enumeration
    - Oneline Screens
    - Analog Reports
    - IEC61850 Client
    - LogicLinx

Cyber security related Certificates are not included in snapshots, and therefore cannot be restored. All certificates must be imported again after the snapshot restore. All secure connections using certificates must be re-associated with the new imported certificates (e.g. Secure Connection Relay, VPN Server, etc.)

License file (key) is not restored with the snapshot.

G100 enrollment in Predix Edge Manager Cloud and associated settings are not restored with the snapshot.

Default Users

The G100 from the factory has two default users.

1. **Default Root User** – **root** (root has all permissions to the G100 but only available via the serial maintenance port).
2. **Default Administrator user** – **defadmin** (restricted permissions - used for initial setup).

NOTE: There are no other default users on a from factory G100.

Default Root User - root

The G100 unit that comes from factory has below default **root** user credentials.

User Name: **root**

Password: **geroot**

The default root user is a super user in G100 which can access all the settings and files. The **root** user access is restricted via:

- serial maintenance port.

NOTE: For Cyber Security reasons users are required to change this default root password using G100 Local Configuration Utility (**MCP Settings GUI**).

Warning: The User is responsible for the new root password. There is no back door, if lost a factory reset is required to recover a unit. Contact customer support for a Return Materials Authorization (RMA) estimate.

Default Administrator User – defadmin

The G100 unit that comes from factory has below default administrator **(defadmin)** user credentials.

User Name: **defadmin**

Password: **defadmin**

The G100 supplies a temporary default administrator user with limited access for initial hardware configuration. This **defadmin** user can perform only limited set of operations.

The default administrator (defadmin) user cannot perform other settings or gateway configuration changes, any operational workflows and login to runtime HMI. The default administrator (defadmin) user is intended to perform only below operations.

- To change or configure IP address to ethernet ports
- To add a nominated administrator-level user(s)
- To restore G100 Snapshots

Warning: The default administrator (defadmin) user will be deleted automatically once a nominated administrator user is created successfully. The local root user is required to recover the new administrator user if the credentials are lost.

Getting Started

Please refer to G100 *Substation Gateway Instruction Manual* (994-0155) for details about powering up the G100. Once the G100 is powered up use the below workflow(s) to prepare the G100 for operation.

1. Minimum setup for a new G100 without a pre-existing "Snapshot":
    - Setup G100 - First time setup
    - Task 1: Connect to the G100
    - Task 2: Create a New Administrator User
    - Task 3: Set the Network Ports parameters (IP Address, SFP Type if applicable)

- Task 4: Change the Root Password
- Task 5: Download existing G100 Configuration

Follow the below steps to download the G100 project in DS Agile Studio:

1. Launch the DS Agile MCP Studio.
2. Connect to the G100 from the ethernet port used for maintenance (default is **#1** using 192.168.168.81/24)
   See Task 3.
3. **Login with** the new nominated administrator user and password.
   See **Task 2.**
4. Select the desired G100 configuration and select the "Synch to" **button.**
5. Follow the steps as prompted on the screen.
6. Converting D400 configuration to G100
   DS Agile MCP Studio can restore D400 archives created in SGConfig.

D400 offline devices with v530 configuration or newer can be directly converted to G100. Previous D400 versions need to be first upgraded to v530 using the D400 Upgrade Manager.

Launch DS Agile MCP Studio.

If you need to obtain the D400 configuration from an existing operational unit - connect to D400 device and use Sync From to upload the configuration.
Alternatively, select the existing D400 offline configuration to be converted.

With the D400 device selected, select the Create G100 button in the menu. Follow the prompts.

- When the conversion is complete, the new configuration can be saved and downloaded to the G100 using the Sync To option.

2. To restore an existing G100 "Snapshot":
   - Task 1: Connect to the G100
   - Setup G100 - First time setup
   - Task 1: Connect to the G100 Snapshot

NOTE: In the following procedures/workflows, "**Enter**" indicates that the menu item number is typed in and then the Enter key is pressed.

Setup G100 - First time setup

Task 1: Connect to the G100

Three methods are available to connect to a new G100:

- Local monitor and keyboard via Local KVM interface (Keyboard Video Mouse).
- Using a supported Web Browser, connect to the front maintenance LAN port - default IP address 192.168.168.81
- USB Serial connection via the front USB type B maintenance port.

Connect to G100 via Local KVM GUI

1. Connect the Display Port on the rear panel of the G100 to a monitor with a Display cable.
2. Connect a keyboard and mouse to any of the USB ports.
3. Once the G100 device is powered up and has a valid license installed, click on the **G100** name via the taskbar.
4. Click **System Settings**.
5. A default web browser will be opened showing **MCP Settings** Login screen.
6. Enter the default **Username** (defadmin) and default **Password** (defadmin) and click **Login**.

Connect to G100 via LAN port

1. Connect a LAN cable between your computer and the G100 LAN port configured for maintenance (default is Net 1, but any configured LAN port allowed in the firewall can be used).
1. Using a supported web browser, type the Net0 default IP 192.168.168.81 into the address bar and press the 'Enter key'.
    - The PC's network settings will have to be configured to the same subnet as the G100 to establish communications.
2. User is required to **confirm security certificate** exception.
3. The **MCP Settings** Login screen is displayed.
4. Enter the default **Username** (defadmin) and default **Password** (defadmin) and click **Login**.

Connect to G100 via Serial Maintenance Port

NOTES:

The default maintenance serial port is enabled, set as # 4, and configured as RS232 at 115,200 bps. Please refer to the *G100 Substation Gateway Instruction Manual (994-0155)* for RJ45 serial port pinout.

The serial maintenance port can be disabled as following:

- In UEFI for the POST access only. Make sure that UEFI is set to RS232.
- In Settings for Shell access and use by other runtime applications.

If the serial maintenance port is disabled, users can still access the device using either Local KVM or Ethernet ports.

If the serial maintenance port was disabled, and the IP addresses are not known – then access can be done using Local KVM.

Steps:

1. Connect an RS232 cable between your PC and the maintenance serial port of the G100.
2. Launch the Secure Terminal Emulator from the DS Agile Studio folder in the start menu.
3. Select File > Connect and ensure the Protocol is set to Serial Port
4. confirm the settings before selecting Connect:
    - Serial Port: Select the PC serial port for the connection to G100
    - Baud rate: **115200**
5. At the G100 command shell login prompt, enter the default admin credentials:
    - Username: **defadmin**
    - Password: **defadmin**

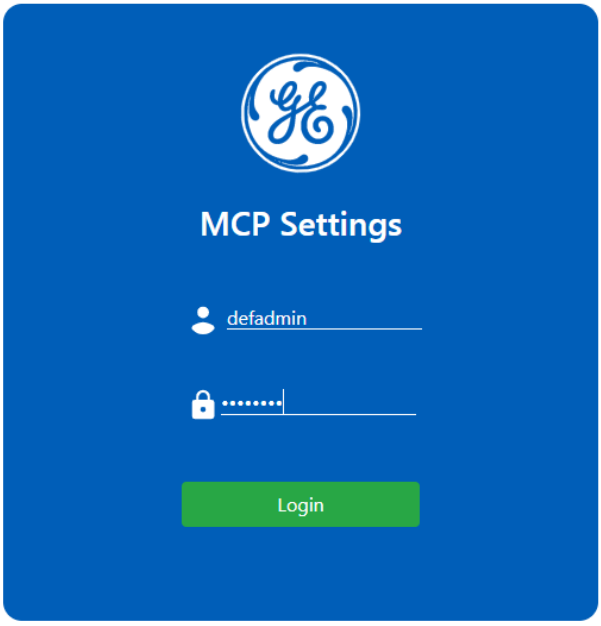
Task 2: Create a New Administrator User

The default administrator (defadmin) is restricted to prevent setting or gateway configuration changes. This is to force the creation of a new nominated administrator-level user account to continue the G100 Setup. New administrator-level user account(s) are created using G100 Local Configuration Utility (MCP Settings GUI). After completing this task, the defadmin user is removed automatically.

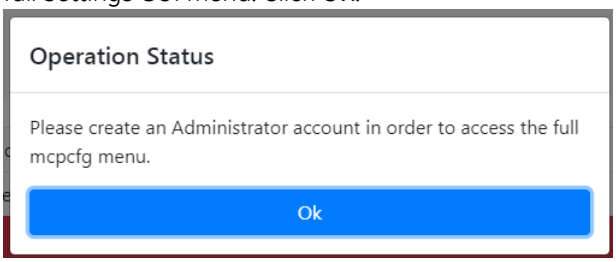
To create a new administrator-level user account follow the below steps using Settings GUI.

NOTE: This section is identical between Local and Remote Settings GUI access.

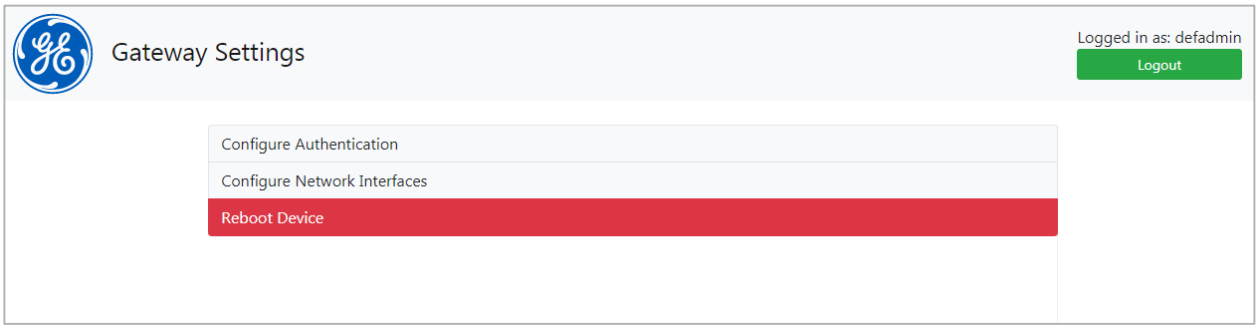
1. Enter the default **Username** (defadmin), default **Password** (defadmin) and click **Login**.



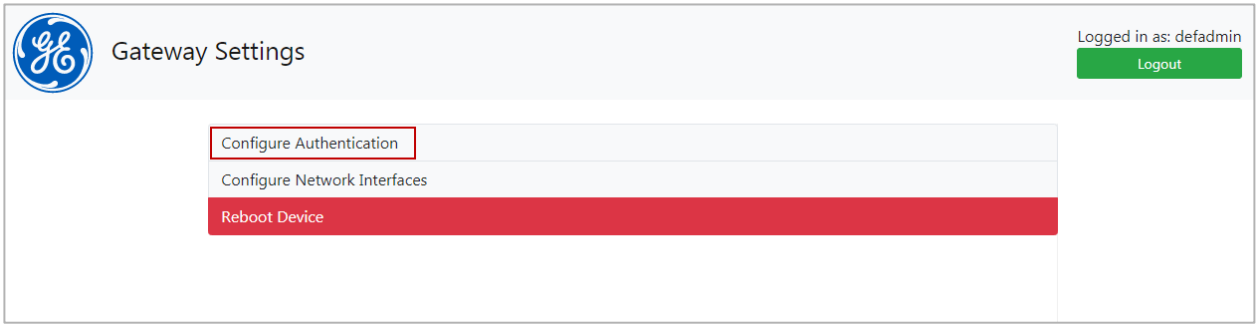
2. If the defadmin account is used to login, you will be prompted to create an Administrator account in order to access the full Settings GUI menu. Click **OK**.



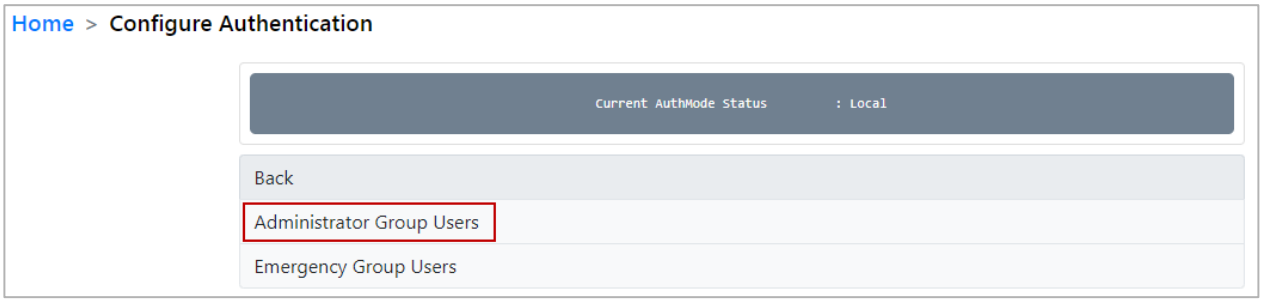
3. The Gateway Settings main menu appears:



4. Select **Configure Authentication** tab from main menu.

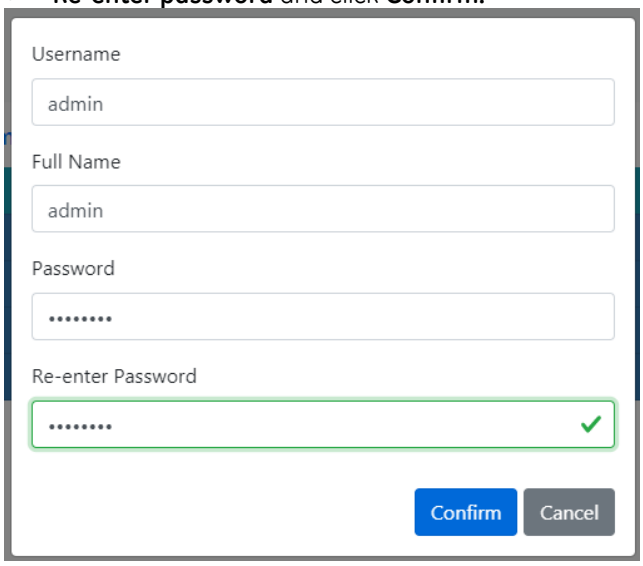


5. Select **Administrator Group Users** tab from Configure Authentication menu.

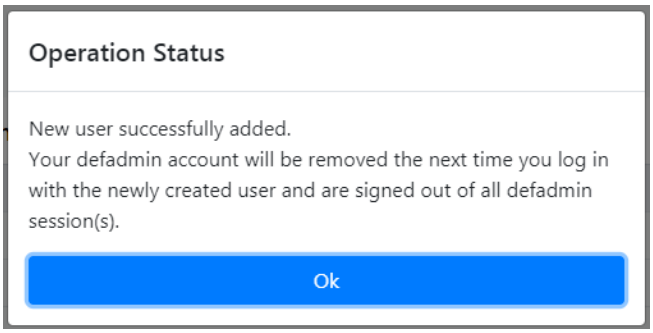


6. This function is used to perform the following actions:
   - List Users
   - Add User
   - Change Password
   - Remove User
7. Select **Add User** tab to create administrator-level users.
   - Enter the desired **Username**, conforming to the Username rules as listed below:
     - Username must be between 2 and 31 characters.
     - Username must start with a lowercase alphabetical character.
     - Username must only contain [a-z][0-9][-,_] characters.
   - Enter the **Full Name** of the User.
   - Enter the **Password**, conforming to the password security rules as listed below:
     - Password must be between 8 and 199 characters in length.
     - Password must contain:
       - 1 character from [a-z]
       - 1 character from [A-Z]
       - 1 digit from [0-9]
       - 1 special character from the set [$%@!&]

- **Re-enter password** and click **Confirm.**



8. **RESULT:** Pop-up window appears showing the Operation Status, click **OK.**
NOTE: defadmin account will be removed the next time you log in with the newly created user and are signed out of all defadmin sessions.



Navigate back to the main menu by clicking on the **HOME** link located at the upper left corner of the page.

NOTE:

- The defadmin user will be deleted automatically once nominated administrator-level user is logged in and all the defadmin opened sessions are logged/signed out.
- The root user is available to recover the new administrator password.

Task 3: Set the Network Ports parameters (IP Address, SFP)

Network Ports #1 and #2 are always available, #3 and #4 are pluggable SFP.

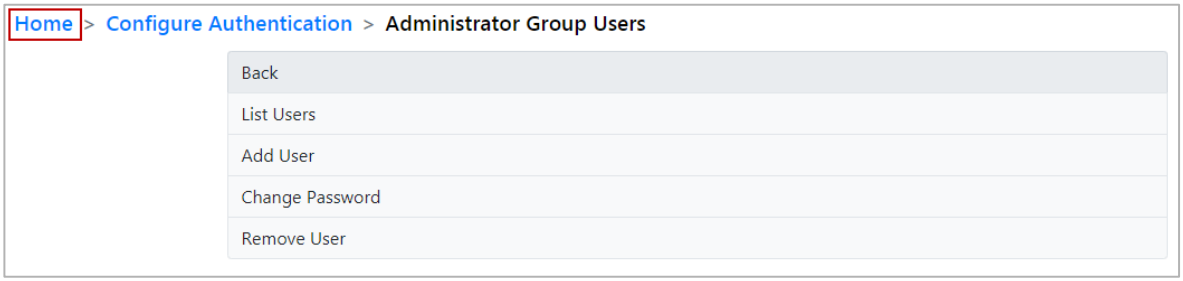
Each SFP adapter must be configured to match the inserted type.

The default enabled and configured Network port is #1, with 192.168.168.81/24 and can be used as such.

If is required to change the default IP Address, and/or to configure additional network ports, please follow the steps below using Settings GUI.

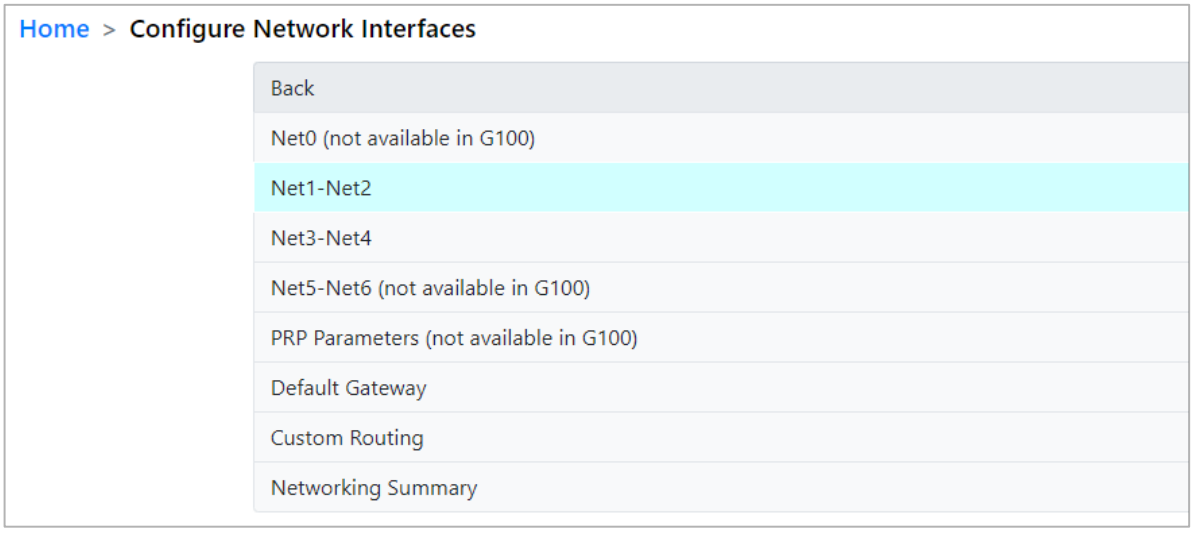
Setting Network Ports #1 and #2 (embedded ports)

1. If not already in **Home** screen, go the Settings GUI main menu by clicking on the **HOME** link located at the upper left corner of the page, for e.g.:



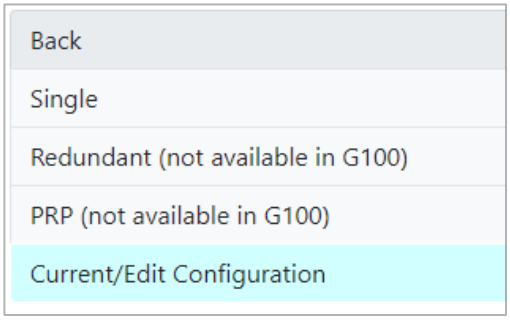
2. Select **Configure Network Interfaces** tab from main menu
   - **Note:** this screen will have additional options after a nominated administrator user was created and logged on.

3. Select the network interfaces **Net1-Net2**.

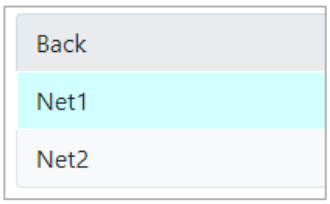


4. Only **Single** mode is supported in G100.

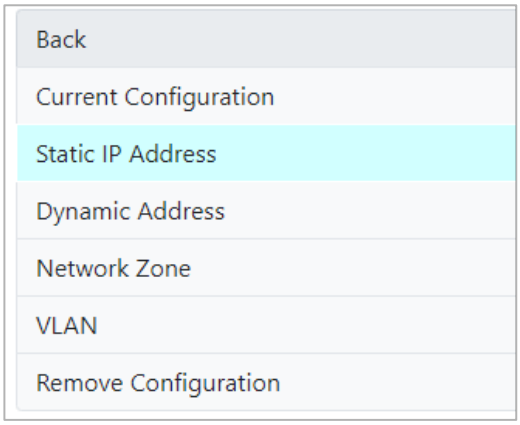
5. Select **Current/Edit Configuration** tab.



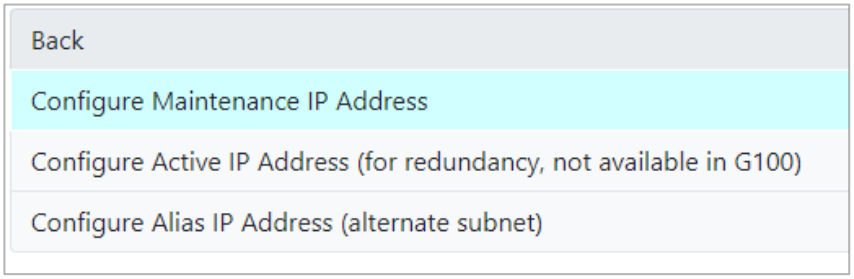
6. Select **Net1** tab (or **Net2** as desired).



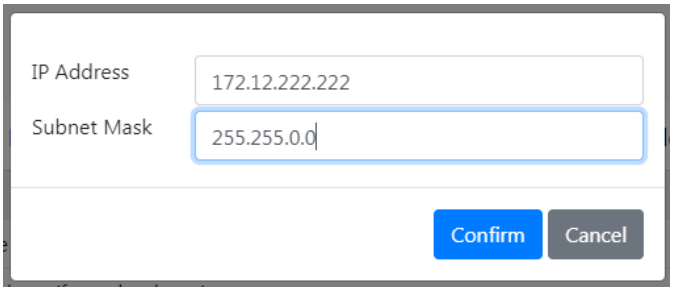
7. Select **Static IP Address** tab.



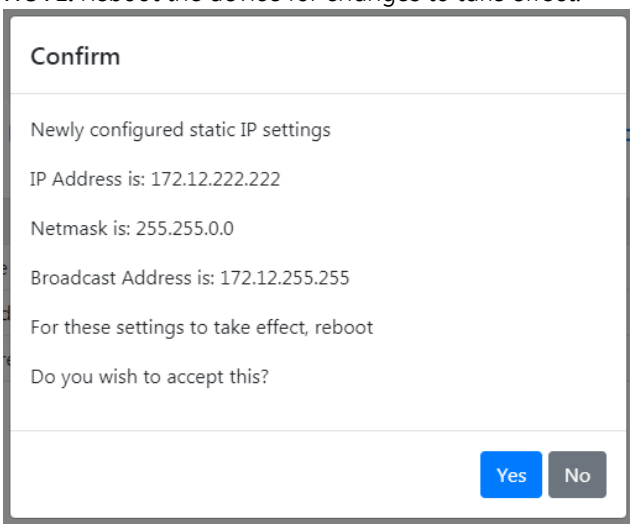
8. Select **Configure Maintenance IP Address** tab.



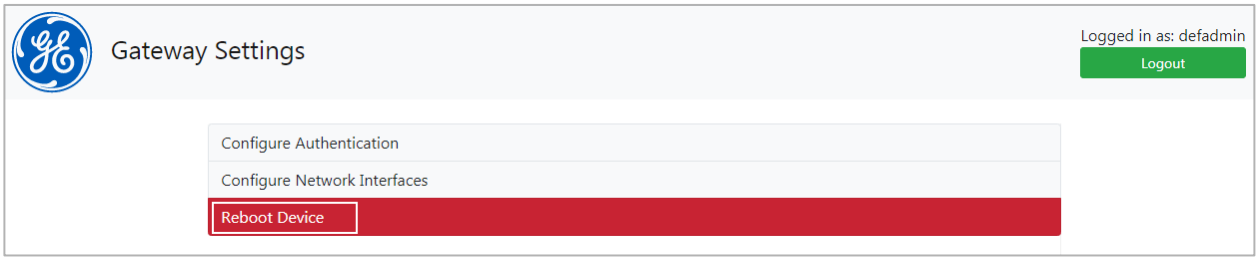
9. Enter **IP Address** and **Subnet Mask**. Click **Confirm**.



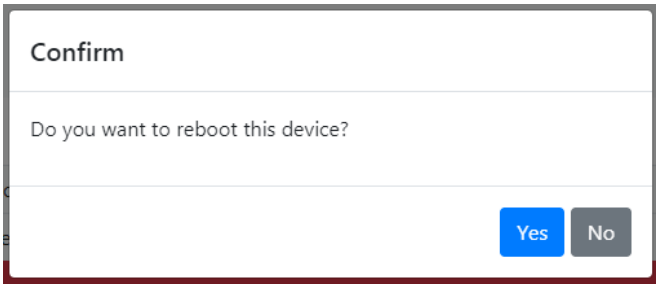
Click **Yes** to confirm the newly configured static IP settings.
NOTE: Reboot the device for changes to take effect.



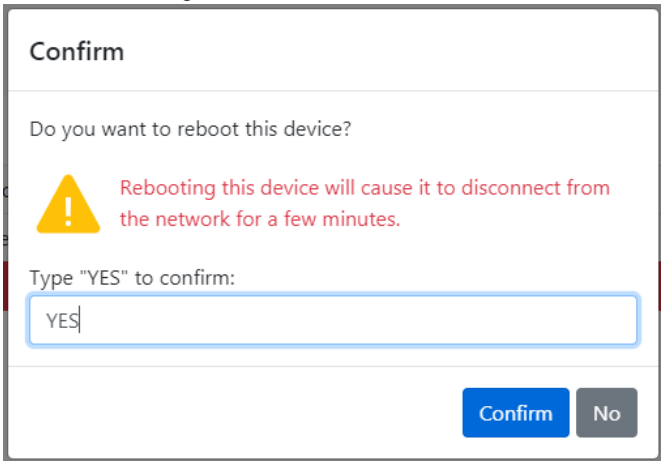
10. Navigate back to main menu and select **Reboot Device** tab.



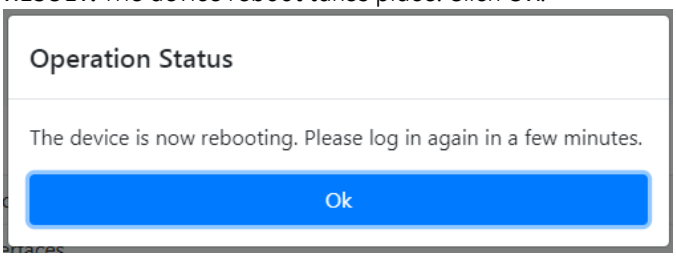
11. Click **Yes** to confirm Reboot the device.



12. Type "**YES**" and click **Confirm**.
NOTE: Rebooting the device will cause it to disconnect from the network for a few minutes.



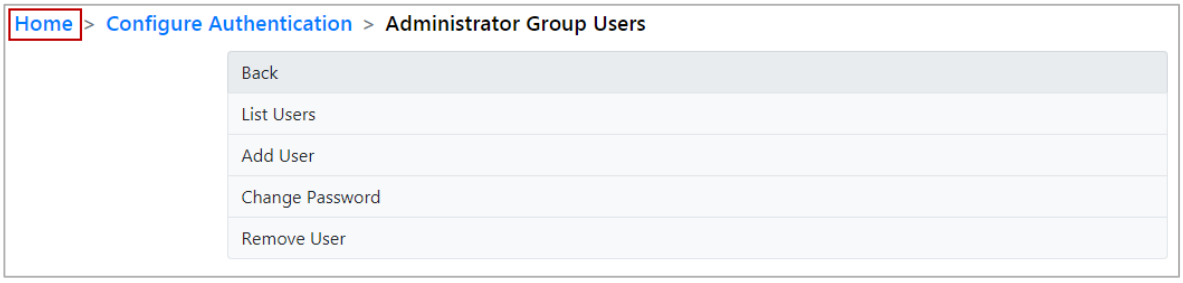
RESULT: The device reboot takes place. Click **OK**.



Setting Network Ports #3 and #4 (SFP)

The process to configure the IP Address is identical as for Network Ports #1 and #2, with the addition of the SFP selection for #3 and #4.
The G100 must be restarted after changing the SFP type(s).

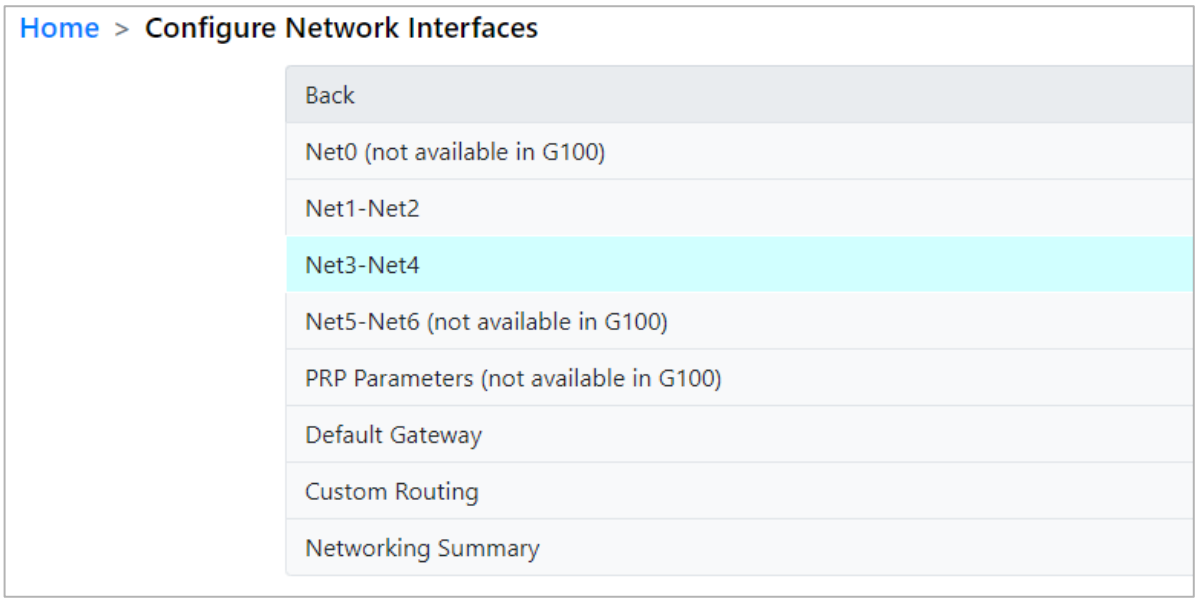
1. If not already in **Home** screen, go the Settings GUI main menu by clicking on the **HOME** link located at the upper left corner of the page, for e.g.:



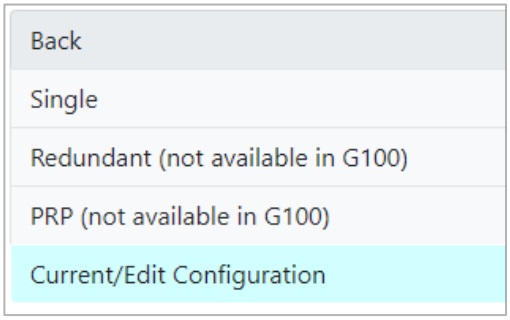
2. Select **Configure Network Interfaces** tab from main menu

a. **Note:** this screen will have additional options after a nominated administrator user was created and logged on.

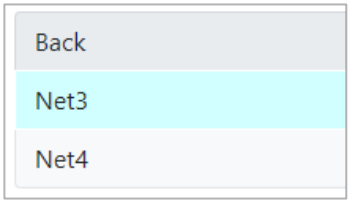
3. Select the network interfaces **Net3-Net4**.



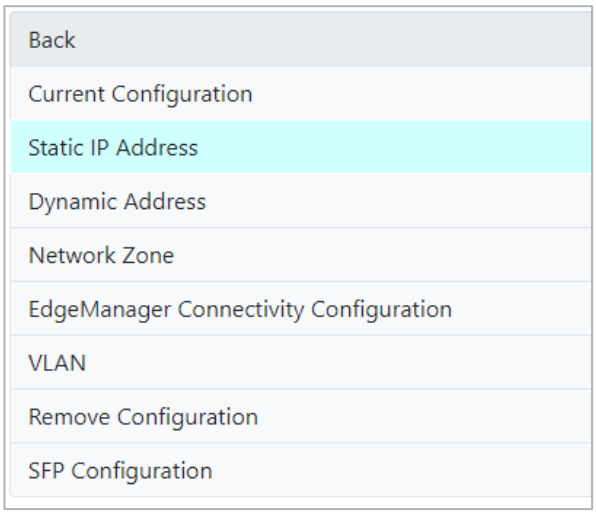
4. Only **Single** mode is supported in G100.
5. Select **Current/Edit Configuration** tab.



6. Select **Net3** tab (or **Net4** as desired).

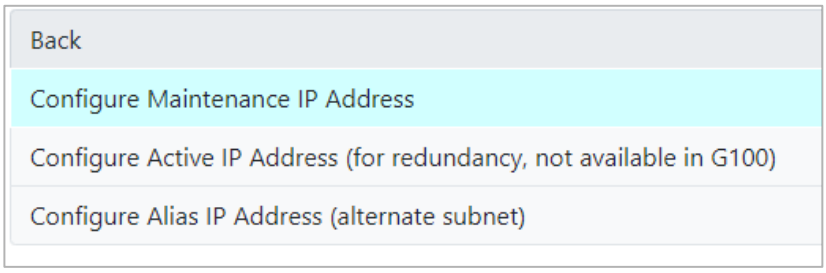


7. Select **Static IP Address** tab.

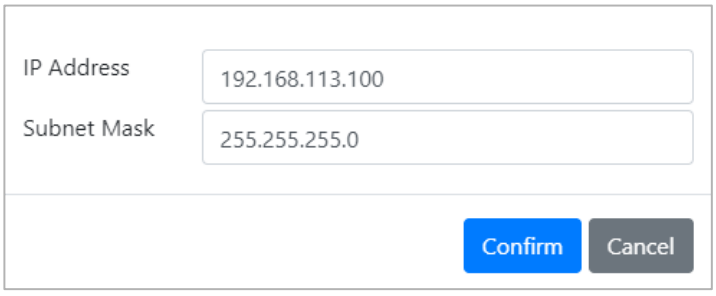


INFORMATION NOTE: The option "EdgeManager Connectivity Configuration" is available for all network ports except #1 which is reserved for the Predix Edge Technician Console (PETC).

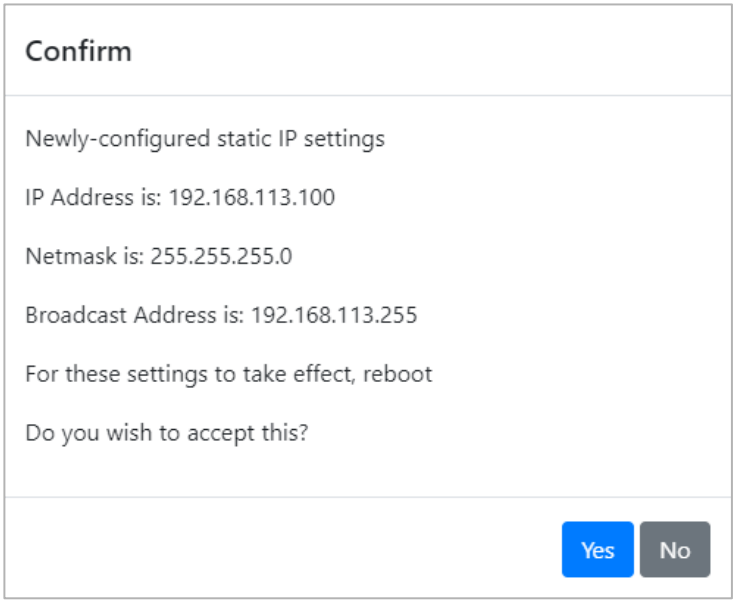
8. Select **Configure Maintenance IP Address** tab.



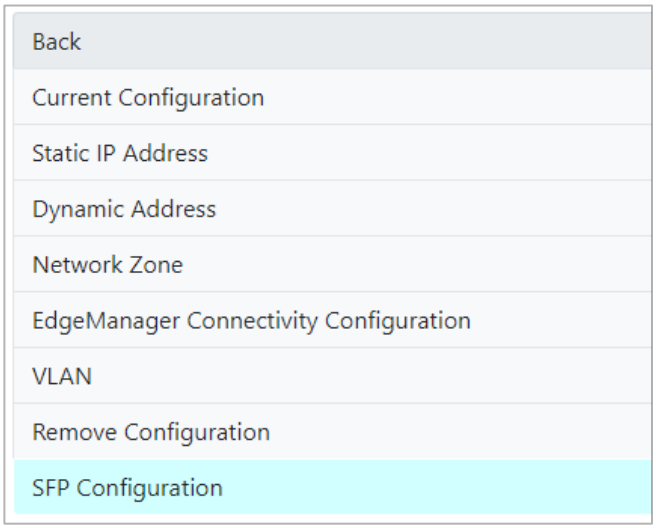
9. Enter **IP Address** and **Subnet Mask**. Click **Confirm**.



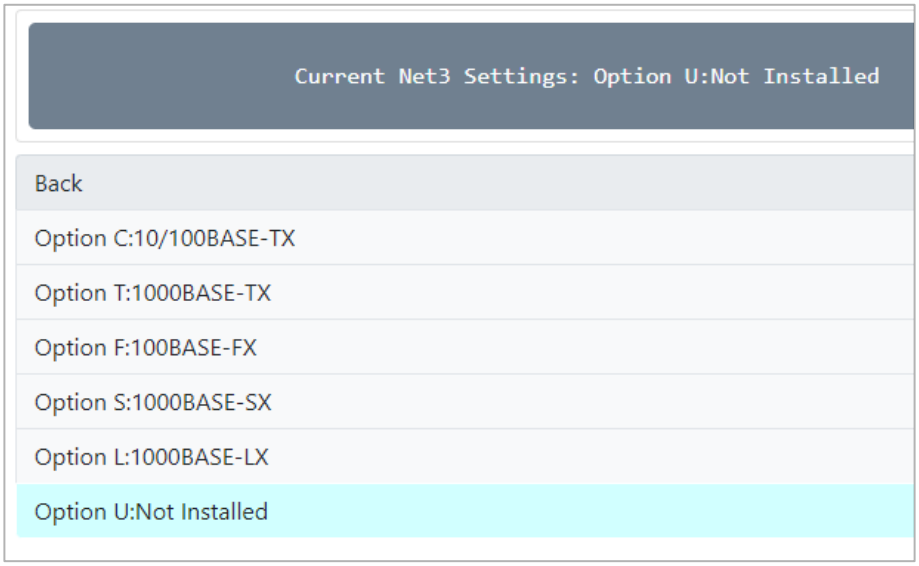
Click **Yes** to confirm the newly configured static IP settings.



10. Navigate back to the network edit configuration and select **SFP Configuration**:

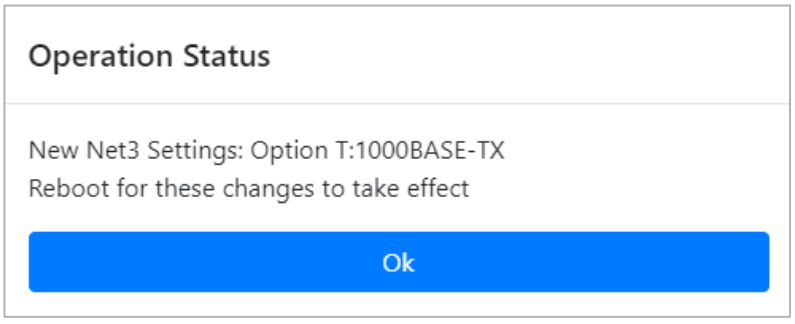


11. Select the option corresponding to the SFP adapter type inserted in the SFP slot for this port:

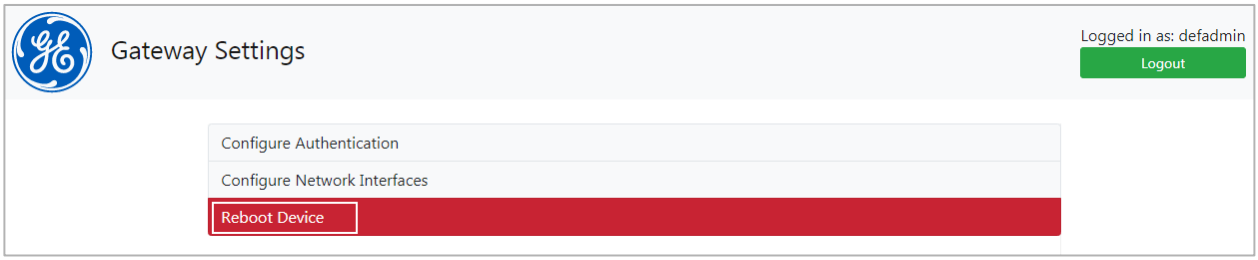


Default option is U (not installed).

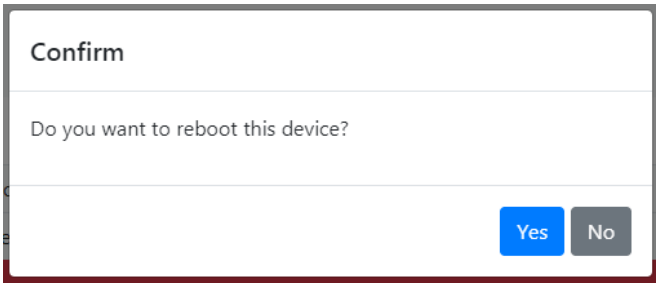
Select OK to acknowledge the selection:



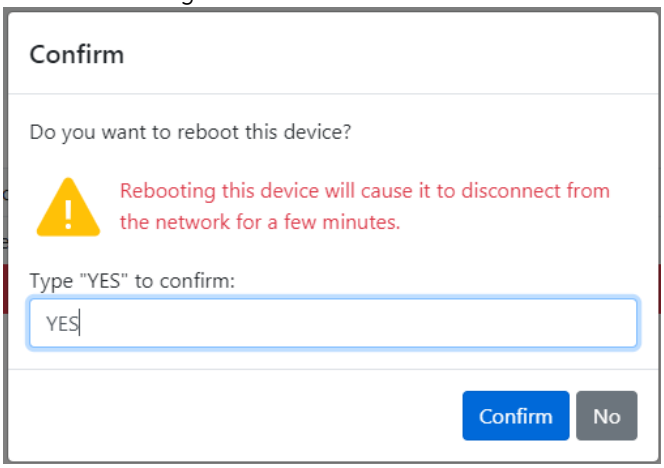
12. Navigate back to main menu and select **Reboot Device** tab.



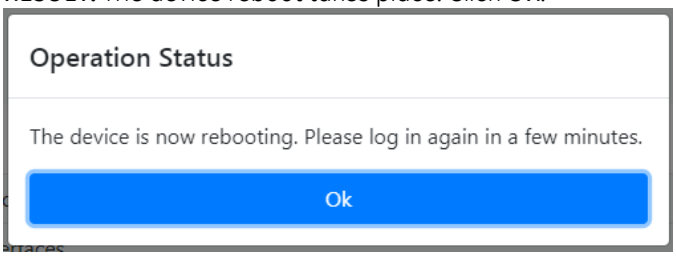
13. Click **Yes** to confirm Reboot the device.



14. Type "**YES**" and click **Confirm**.
NOTE: Rebooting the device will cause it to disconnect from the network for a few minutes.



RESULT: The device reboot takes place. Click **OK**.

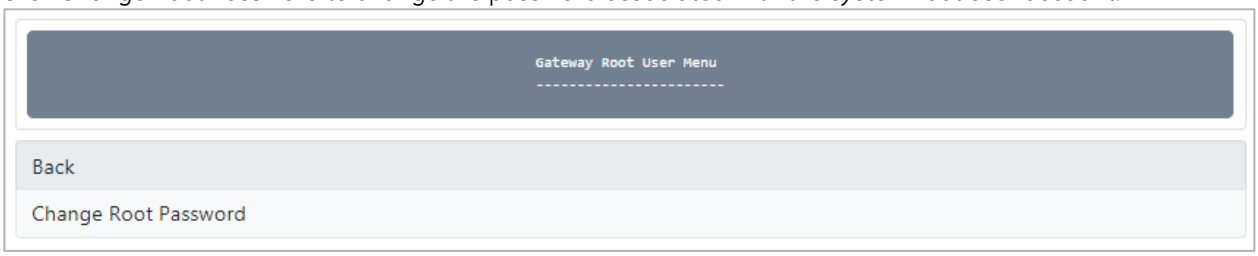


Task 4: Change the Root Password

1. Go the Settings GUI main menu by clicking on the **HOME** link located at the upper left corner of the page.

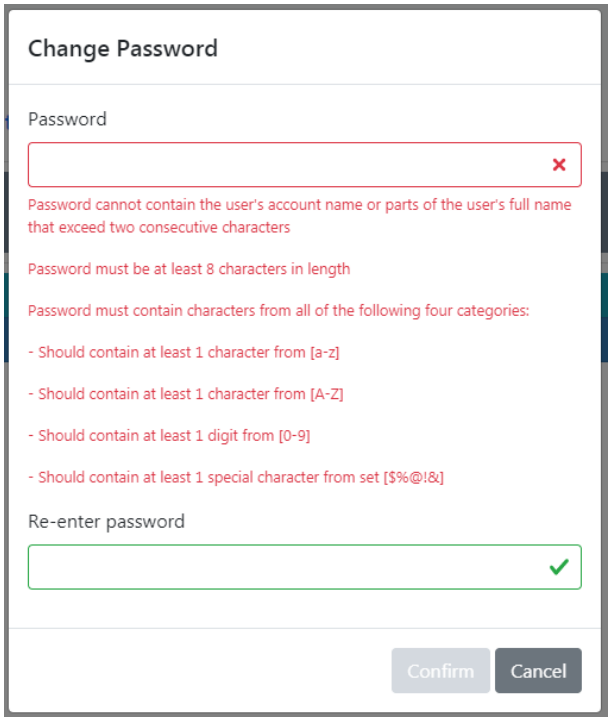
2. Click **Root Administrator Settings** tab.

3. Click Change Root Password to change the password associated with the system root user account.

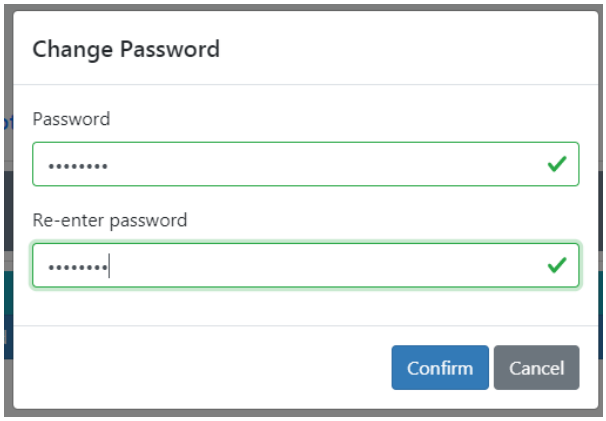


4. Change Password:
   - Password cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters.
   - Password must be at least 8 characters in length.
   - Password must contain characters from all the following four categories:
     - Should contain at least 1 character from [a-z]
     - Should contain at least 1 character from [A-Z]
     - Should contain at least 1 digit from [0-9]
     - Should contain at least 1 special character from set [$%@!&]

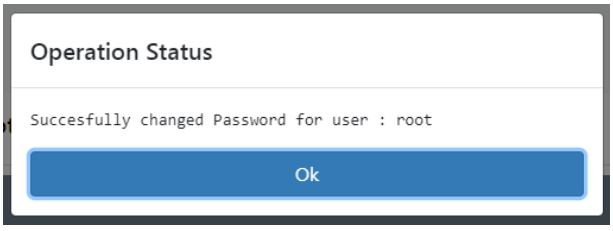
- Re-enter password.



5. Click **Confirm.**



RESULT: Pop-up window appears showing the Operation Status, click **OK.**



NOTICE

The root user's password should be defined and securely stored by the system administrator; This is crucial information. **No method is available for recovery** outside the factory.

Task 5: Download existing G100 Configuration

Follow the below steps to download the G100 project in DS Agile Studio:

7. Launch the DS Agile MCP Studio.
8. Connect to the G100 from the ethernet port used for maintenance (default is #1 using 192.168.168.81/24)
   See **Task 3**.
9. Login with the new nominated administrator user and password.
   See **Task 2.**
10. Select the desired G100 configuration and select the "Synch to" button.
    Follow the steps as prompted on the screen.

Converting D400 configuration to G100

DS Agile MCP Studio can restore D400 archives created in SGConfig.

D400 offline devices with v530 configuration or newer can be directly converted to G100. Previous D400 versions need to be first upgraded to v530 using the D400 Upgrade Manager.

Launch DS Agile MCP Studio.

1. If you need to obtain the D400 configuration from an existing operational unit - connect to D400 device and use Sync From to upload the configuration.
   Alternatively, select the existing D400 offline configuration to be converted.
2. With the D400 device selected, select the **Create G100** button in the menu. Follow the prompts.
3. When the conversion is complete, the new configuration can be saved and downloaded to the G100 using the Sync To option.

Setup G100 - With a Snapshot

Task 1: Connect to the G100

1. Connect a LAN cable between your computer and the G100 maintenance LAN port.
   - The PC's network settings will have to be configured to the same subnet as the G100 to establish communications.

Setup G100 - First time setup

Task 1: Connect to the G100 Snapshot

1. Launch the DS Agile MCP Studio on the local configuration PC.
2. Restore your G100 snapshot to a device in a project in DS Agile MCP Studio (**Archive > Restore Snapshot to Device**).
3. Edit the IP address in the device properties to match the default G100: 192.168.168.81
4. Select this device, initiate Synch To Device > Restore Snapshot to Device
5. Select all Restore options
   - Restore Configuration Data
   - Restore Network Settings
   - Restore information required to clone a device
6. If used, enter the Optional Password – This is the password selected when saving the snapshot, not the password on the G100. This feature will verify the Snapshots authenticity and allow restoration of confidential data from the snapshot image (if was saved when the snapshot was created).
7. Login with the default admin user:
   - User: *defadmin*
   - Password: *defadmin*

Refer to DS Agile Studio User Manual for more details.

8. Follow the steps as prompted on the screen.

Result: After successfully restoring the snapshot, the G100 will restart and finish applying the changes. The G100 runs with the same settings and configuration as when the snapshot was previously created, including all local users from the device where the snapshot was created from.

You can now change the Projects device properties IP address set in *step 3* as desired, to match the restored configuration running in G100.

Checking Licenses

The G100 unit should come from factory already licensed.

To check the provided licenses, two workflows are provided:

1. Shell access-based workflow (read only)
2. DSAS based workflow

Shell access-based workflow (read only)

3. Start a terminal session and log into the G100 with an Administrator-level or root user account.
4. At the G100 #>> prompt, enter the following commands:
   - **cd /home/MCP_APPS/**
   - **sudo ./swlic-report**

Result: The application output shows the G100 ownership information and a list of available features. Each item under Application License represents an application or feature that can be licensed. They are shown in the format:

3-digit application ID number: Description of feature License status

If the G100 unit does not contain a license file, please perform the following steps:

1. Start a terminal session and log into the G100 with an Administrator-level or root user account.
2. At the G100 #>> prompt, enter the following commands:
   - **cd /home/MCP_APPS/**
   - **sudo ./swlic-info**
3. Provide the information shown to GE Technical Support.

Please refer to the MCP Substation Gateway Software Configuration Guide (GE Part Number SWM0101) for additional details.

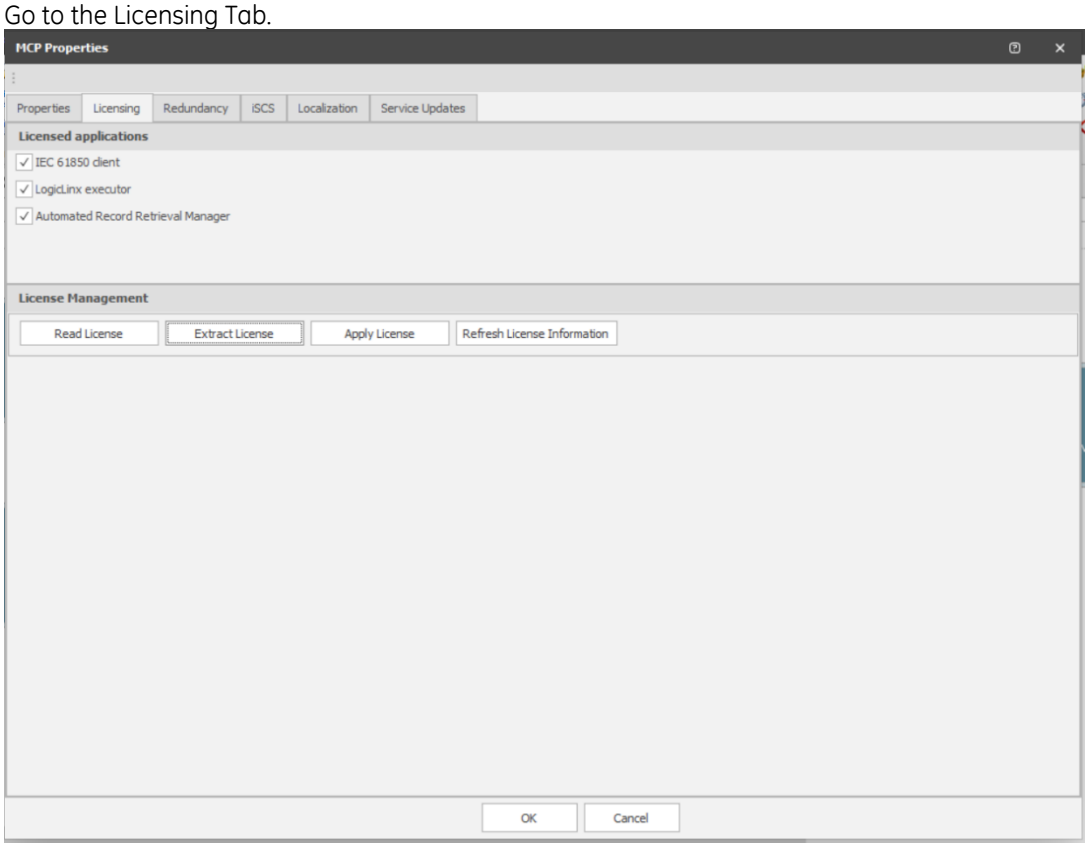
DSAS based workflow

Users have the possibility to read/extract/apply licenses to G100 using the Licensing option available in the DSAS Configuration Tool.

To access these options:

1. Open Device Properties for your DSAS offline Device in your Project. If one was not created, please follow the normal workflow to create one.

2. Go to the Licensing Tab.

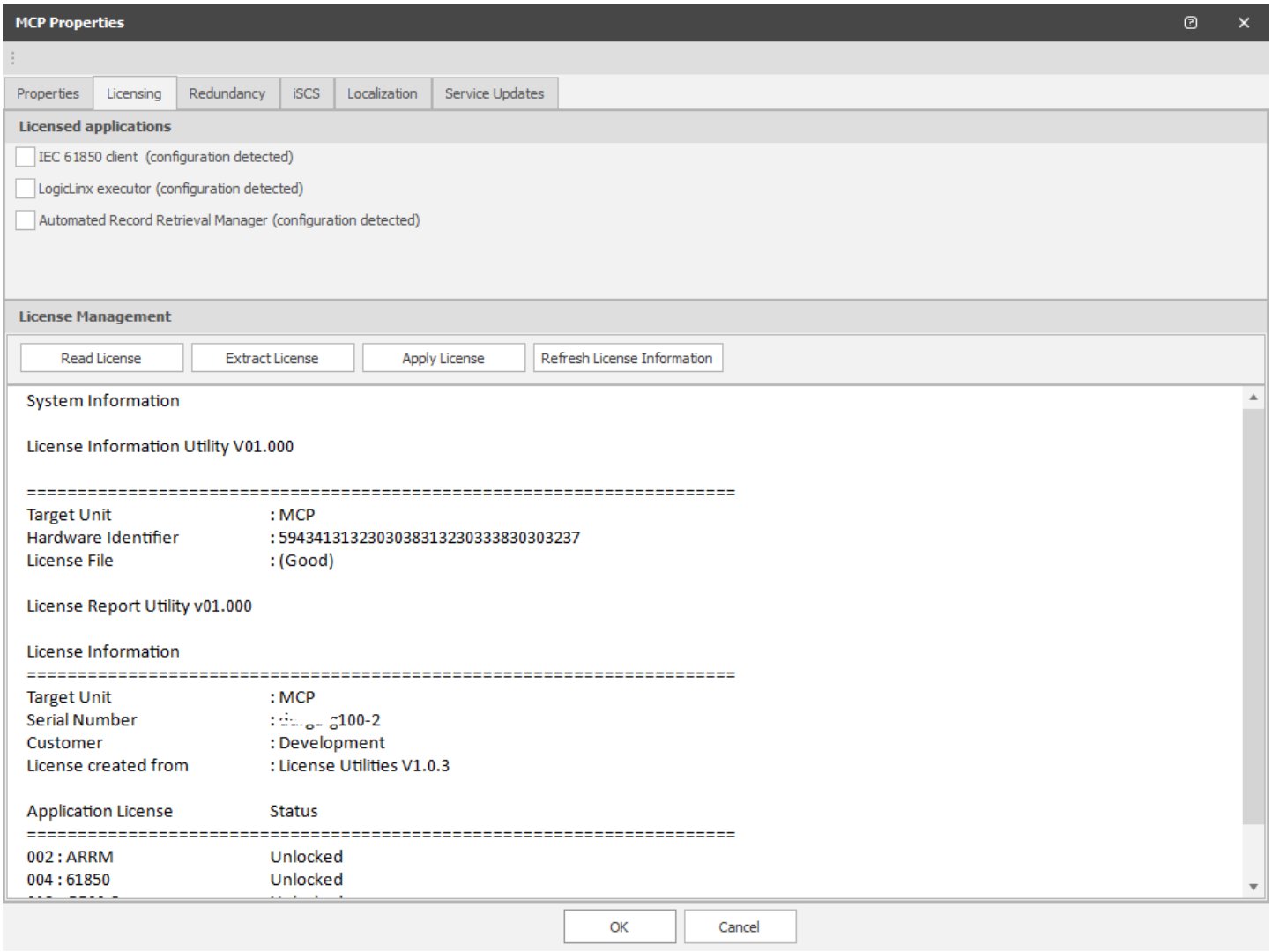


3. Under License Management there are three buttons:
    a. Read License
    b. Extract License
    c. Apply License
4. When user clicks on any of the three buttons, a login dialog is prompted to connect to G100 with Administrator privileges (this role is required to access any of the licensing information).
5. After successful authentication, user is authorized to access the license information. If the user stays within this tab, subsequent button actions will not prompt again to login.

Read License

This option displays the license information of the live target unit (connected G100 device).

Displayed information may be copied to the Windows Clipboard with regular actions (mouse click and drag or CTRL+A to select, right click or CTRL+C to copy).



Extract License

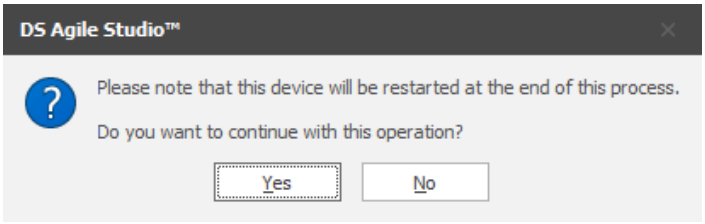
This option allows user to extract the current license file from the live target unit to a specified PC location, for example to archive a copy.

The extracted license file is saved as a *.key file (default name is license but can be changed as desired).

Apply License

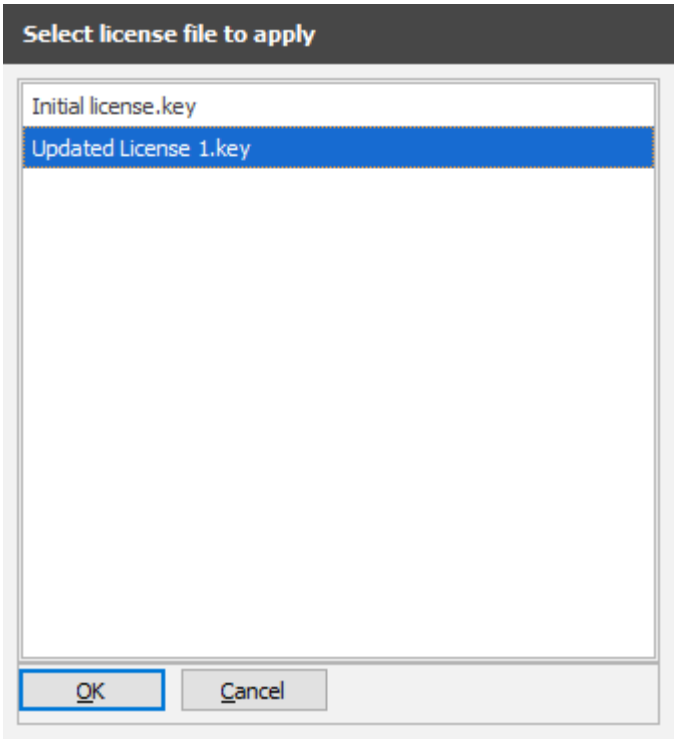
This option allows user to apply a compatible license key, from a location in the PC, to the live target unit.

NOTE: The live target unit is restarted at the end of this process, not immediately, and only if a hardware compatible license file was selected.

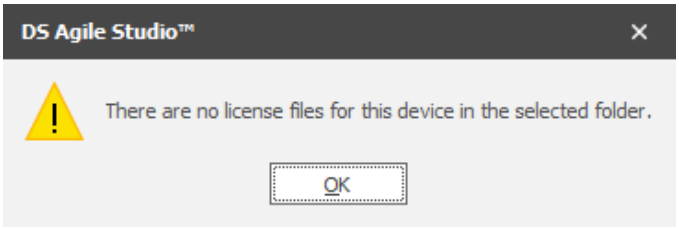


When browsing for license files, user must select the folder containing one or more license files. The action does not include sub-folders of the selection.

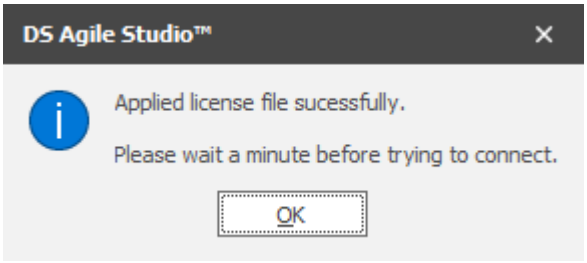
In the resulting dialog only license files (any filename) that match the Hardware Identifier of the live target unit are displayed for selection. This is the reason why users must first login to the live device as Administrators.



If the selected folder has no license compatible with the connected live unit, an information dialog is presented to this effect:



If a valid license file has been selected it will be applied and the device restarts:



The workflow to apply a license can be cancelled at any time before selecting a valid license and click on OK.

Read the G100 Order Code

To know the Order Code of your G100, run ***mcpsi*** command through the Shell access.

"As-Built" is the order code at factory build time.

"As-Is" is the order code at the time when the user runs the command.

In the example below, after the unit was built in the factory, there were added and configured two Fiber Optic SFP (F) and a D.20 PCIe card (D).

```
admin@G100:~$ mcpsi
Retrieving the GE Multilin MCP system information, please wait ...
================================================================================
                      GE Multilin MCP System Information
================================================================================
Model Number:
    As-Built:       G100-AAL-DA-4TTUU-UUU-B2022-UU
    As-Is   :       G100-AAL-DA-4TTFF-DUU-B2022-UU
```

Please visit the online store for application licenses ordering codes. For latest configuration and options, please visit the online store and search for G100:

https://store.gegridsolutions.com/Home.aspx

UEFI Settings checks

Please refer to the document *Configuring UEFI Settings on G100 User Guide (SWM0122)* for details.

G100 device has the following UEFI settings that will revert to default values after the internal super capacitor has been discharged due to the device being powered off for extended time (typically more than 5 days).

These UEFI settings are applicable only while the G100 is starting.

After the applications started, these settings are over-written by the values configured in *MCP Local Configuration Utility (mcpcfg)* or *MCP Settings GUI* (which are persistent).

- Default Serial Maintenance Port used as UEFI (boot) console when KVM is not available

(Advanced->Serial Port Console Redirection)
  - Console Redirection is set to Disabled for COM1-COM3, please do not change these settings.
  - Console Redirection for COM4 should be enabled/disabled and have the "Bits per second", to be same as in *the Serial Maintenance Port in MCP Studio (*See *MCP Software Configuration Guide SWM0101 > Serial Maintenance Port)*.
- Default Serial Ports Modes (Advanced->Super IO Configuration)
  - Please ensure are enabled/disabled as required for secure hardening purposes and set to RS-232.

Users should check again these UEFI settings when the G100 is powered on again, and adjust as necessary.

G100 Runtime HMI

The G100 Runtime Human Machine Interface (HMI) is available to view real time information on G100. With the HMI a user has the option to monitor the status of a substation network, view data, execute control commands and change the system set-up.

The G100 Runtime HMI is available on a local monitor (via the display ports on the rear panel of the G100) and on remote PC's as a standalone application.

The Local Runtime HMI (KVM) is already installed in the G100.

The remote G100 Runtime HMI runs as a standalone application.

Install G100 Runtime HMI

The remote G100 Runtime HMI requires Windows x64 bit OS. This is available via GE support channels and consists of a single installation file named "G100HMI_x64_v.*abc*.exe" – where "*abc*" represents the version (this must match the G100 firmware version).

Installation of Java/JRE on the Windows PC is not required.

To install the G100 Runtime HMI:

1. DoubleClick the "SetupG100HMI_x64_*vabc*.exe" install file
2. Select OK at the Windows security prompt
3. Select Next in the installation wizard
4. Select Finish to complete the install
5. Launch the G100 HMI from the Start Menu or install folder

Install Location: C:\Program Files\G100 Runtime HMI*abc*\G100HMI_x64_v*abc*.exe

Refer to MCP Substation Gateway Software Configuration Guide (GE Part Number SWM0101) for more details.

Accessing Remote HMI

1. Double click on "G100HMI_x64_v1.0.exe" file <shortcut> or launch from the start menu.
2. Enter the IP address (assigned in Task 3) of the G100.
   - The TCP port of the G100 HMI is always 443. If you need to use a different TCP port, due to routing rules existing between the PC and G100, you may enter it in the form of IP: TCP, for e.g. 10.10.11.50:30500
3. Login with the user credentials created in Task 2: Create a New Administrator User.
4. Click **Log In.**

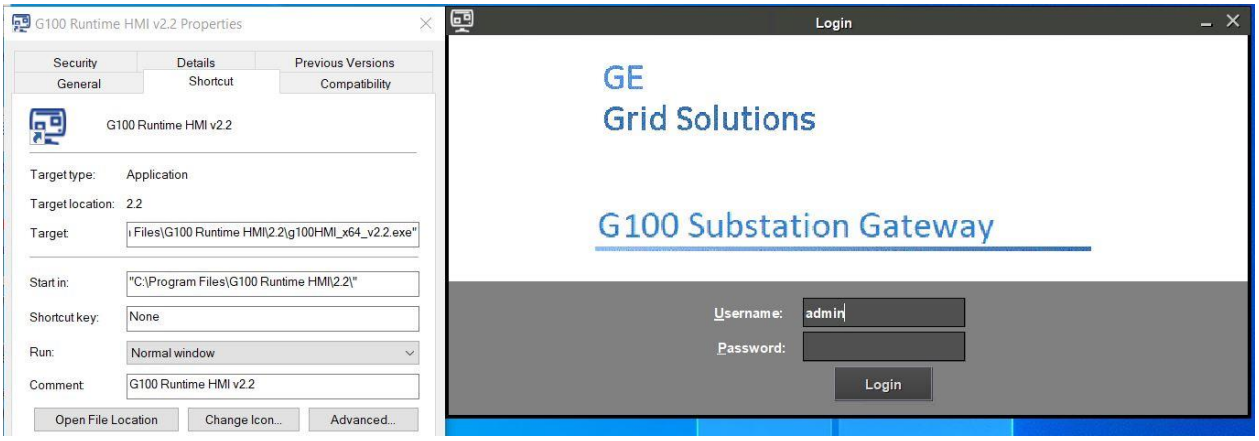
NOTE: Users can be assigned with different HMI access levels. Refer to *MCP Software Configuration Guide* (GE Part Number SWM0101) for additional details.

Remote HMI Auto Login

By customizing a G100 Runtime HMI shortcut the user can predefine the login User, IP Address, or Remote Port.

1. Locate the G100 Runtime HMI shortcut.
2. Copy the shortcut to the desktop, or a desired location, or pin it to Taskbar or Start Menu.
3. Right click on the shortcut and select "Properties".
4. Add the below parameters to the shortcut at the location "Target" as shown in the below table:

Target Parameters	Shortcut Target content
IP Address	C:\Program Files\G100 Runtime HMI\1.0\G100HMI_x64_v*1.0*.exe -host 192.168.168.81
IP address & Port (e.g. for local port re-direct)	C:\Program Files\G100 Runtime HMI\1.0\G100HMI_x64_v*1.0*.exe -host 127.0.0.1 -port 30500
Only User Name	C:\Program Files\G100 Runtime HMI\1.0\G100HMI_x64_v*1.0*.exe -username admin1
Shortcut with All Parameters	C:\Program Files\G100 Runtime HMI\1.0\G100HMI_x64_v*1.0*.exe -host 192.168.168.81 -port 30500 -username admin1



Shortcut properties display updated "Target" data launches the HMI with the IP and pre-defiled Username.

5. Double clicking the newly created shortcut will launch the G100 Runtime HMI using the parameters configured in the Target.

Accessing Local HMI

1. Local HMI starts automatically when a monitor is connected to the G100 display port on startup. If the G100 is configured for Auto Logon, then the G100 Home Page is launched with the configured user privileges on startup.
2. When prompted, login with the user credentials created in Task 2: Create a New Administrator User.
3. Click **Log In**.

NOTICE

When finished your work it is suggested to logout from the G100 Local HMI to secure the system. Logging out terminates the respective user session with the G100 and closes all G100 Local HMI displays and windows.

The internal G100 alarm buzzer is active only when the Local HMI runs. Create a default auto logged on Observer user if the internal alarm buzzer is required to operate in un-attended mode, and ensure the Local HMI is not shut down.

Configure Screen Layout:

1. Screen Layout and resolutions may be configured using Screen Layout utility in the Local HMI.
2. The utility can be launched from Local HMI start menu using G100 -> **System** -> **Screen Layout** as shown below.
3. The minimum resolution supported in Local HMI is 1280x1024 and the recommended resolution is FHD (1920x1080).

Configuring Monitor Layout:

G100 Local HMI supports up to 1 monitor using its display port Display Port.

Refer to *MCP Software Configuration Guide* (GE Part Number SWM0101) for more details.

Runtime HMI User Preferences

HMI Runtime (Remote/Local) supports the following features. These features are available from the **User** tab of G100 the Power Bar.

Mode of Operation:

- Docked = all windows open within the parent frame.
- Single = A single window is opened at a time in the parent frame, new windows replace the previous page.
- Floating = all windows open as independent windows in the desktop area (no parent frame).

Persistency

Windows Persistency is a default feature in Runtime HMI (Remote/Local) which maintains the following independently for each user:

- Persistence of sorting order of the columns, column filters, column width in all the tabular screens or windows.
- Vertical and horizontal re-sizing of all layout boundaries between screen areas of same screen.
- Size and position of all windows in floating mode, except location of child pop up dialogs.

NOTE: Use Reset Persistency option in the Runtime HMI Preferences to clear the persistency state of the windows for the current or all users, or when changing to a lower screen resolution and your persisted windows exceed the screen space. Refer to *MCP Software Configuration Guide* (GE Part Number SWM0101) for more details.

Secret Signature

The Secret Signature is a Cyber Security feature facilitating a user managed layer of protection on the Session Cookie for the HMI Interface. The G100 creates its own session cookie based on hashing a configurable sentence, called “Secret Signature”.

To ensure session cookie uniqueness users should change the Secret Signature.

To change the Secret Signature:

1. Launch DS Agile MCP Studio and connect to G100 using a nominated administrator user.
2. With the Offline or Online Editor, navigate to **Systemwide > Access Manager** tab.
3. Change the Secret Signature from the default to user defined and select “Save” button.
4. Apply “Sync To” in the case of Offline Editor to apply these changes to G100. In the case of Online Editor, these changes will be reflected automatically when User applies “Save” button.
5. Re-Login from the G100 Runtime HMI or G100 Command Line to check the updated Secret Signature.

NOTE: The default secret signature should be replaced with a secure signature chosen by your security administrator. This needs to be done after successful creation of nominated administrator level user.

List of factory default open ports – TCP and UDP

Refer to the following table for complete list of ports. Factory default open ports are indicated by "**Yes**" from the "Enabled by default?" column.

Port Numbers	TCP/UDP	Enabled by default ?	Used for…
443	TCP	Yes	Sync to/from, Online Editor, PETC, Remote runtime HMI.
22	TCP	Yes	Snapshot save/restore, shell access to gateway, file transfer with Gateway.
922	TCP	No	Emergency administrator access, open only when remote authentication configured.
80, 8081	TCP	Yes	Settings GUI.
123	TCP	No	NTP, if configured.
Configurable, default 502	TCP	No	MODBUS, if configured.
Configurable, default 2404	TCP	No	IEC60870-5-104, if configured.
514	UDP	No	Rsyslog, if configured.
10514	TCP	No	Rsyslog, if configured.
Configurable, default 20000	TCP/ UDP	No	DNP, if configured.
Configurable, default 8001 – 8020	TCP	No	Pass-through or terminal server, if configured.
Configurable	TCP	No	TLS tunnel for pass through, terminal server or secure connection relay, if configured.
54000	TCP	No	LogicLinx, if configured.
162	UDP	No	SNMP, if configured.
Configurable, default 1194	UDP	No	OpenVPN, if configured.
51000	TCP	No	Hot Standby Sync Service, if Hot Standby configured. (not supported by G100)
51001	TCP	No	Hot/Warm Standby Heart Beat, if Hot/Warm-Standby Configured. (Not supported by G100)
51003	TCP	No	Standby pointing to active tunnel, if configured. (Not supported by G100)

Port Numbers	TCP/UDP	Enabled by default ?	Used for...
51194, 51195	TCP	No	Hot/Warm Standby Tunnel, if Hot/Warm-Standby Configured. (Not supported by G100)

Additional Documentation

For further information about the G100, refer to the following documents:

- *G100 Substation Gateway Instruction Manual (994-0155)*
- *MCP Substation Gateway Software Configuration Guide (SWM0101)*
- *Configuring UEFI Settings on G100 User Guide (SWM0122)*

Product Support

If you need help with any aspect of your GE Grid Solutions product, you can:

- Access the GE Grid Solutions Web site
- Search the GE Technical Support library
- Contact Technical Support

GE Grid Solutions Web Site

The G100 Web site provides fast access to technical information, such as manuals, release notes and knowledge base topics.

Visit us on the Web at: http://www.gegridsolutions.com

GE Grid Solutions Technical Support Library

This site serves as a document repository for post-sales requests. To get access to the Technical Support Web site, go to:

Visit us on the Web at: http://sc.ge.com/*SASTechSupport

Contact GE Grid Solutions Technical Support

GE Grid Solutions Technical Support is open 24 hours a day, seven days a week for you to talk directly to a GE representative.

In the U.S. and Canada, call toll-free: 1 800-547-8629

International customers, please call: + 1 905-927-7070

Or e-mail to G100 Local region contact support:

- ga.supportNAM@ge.com - North America
- ga.supportLAM@ge.com - Latin America
- ga.supportCEAP@ge.com - China, East Asia, Pacific
- ga.supportERCIS@ge.com - Europe, Russia, Commonwealth of Independent States
- ga.supportIND@ge.com - India
- ga.supportMENAT@ge.com - Middle East, North Africa, Turkey

Have the following information ready to give to Technical Support:

- Ship to address (the address that the product is to be returned to)
- Bill to address (the address that the invoice is to be sent to)
- Contact name
- Contact phone number
- Contact fax number
- Contact e-mail address
- Product number / serial number
- Description of problem

Technical Support will provide you with a case number for your reference.

GE Grid Solutions Address

The GE Grid Solutions company address is:

GE Grid Solutions

650 Markland Street

Markham, Ontario

Canada L6C 0M1

Copyright Notice

© 2021, General Electric Company. All rights reserved.

The information contained in this online publication is the exclusive property of General Electric Company, except as otherwise indicated. You may view, copy and print documents and graphics incorporated in this online publication (the "Documents") subject to the following: (1) the Documents may be used solely for personal, informational, non-commercial purposes; (2) the Documents may not be modified or altered in any way; and (3) General Electric Company withholds permission for making the Documents or any portion thereof accessible via the internet. Except as expressly provided herein, you may not use, copy, print, display, reproduce, publish, license, post, transmit or distribute the Documents in whole or in part without the prior written permission of General Electric Company.

The information contained in this online publication is proprietary and subject to change without notice. The software described in this online publication is supplied under license and may be used or copied only in accordance with the terms of such license.

Trademark Notice

GE, Multilin™ and the GE monogram are trademarks and service marks of General Electric Company.

* Trademarks of General Electric Company.

IEC is a registered trademark of Commission Electrotechnique Internationale. IEEE is a registered trademark of the Institute of Electrical and Electronics Engineers, Inc. Internet Explorer, Microsoft, and Windows are registered trademarks of Microsoft Corporation.

Other company or product names mentioned in this document may be trademarks or registered trademarks of their respective companies.

This printed manual is recyclable. Please return for recycling where facilities exist.

Modification Record

Version	Revision	Date	Change Description
1.00	0	11th May, 2021	Created.
	1	18th May, 2021	Added UEFI Settings checks.

GE
Grid Solutions

Multilin™ G100
Substation Gateway

Configuring UEFI settings on G100 Substation Gateway User Guide

Product version: 1.00 and higher

GE publication code: SWM0122 (V1.00 R0)

imagination at work

Copyright Notice

© 2021, General Electric Company. All rights reserved.

The information contained in this online publication is the exclusive property of General Electric Company, except as otherwise indicated. You may view, copy and print documents and graphics incorporated in this online publication (the "Documents") subject to the following: (1) the Documents may be used solely for personal, informational, non-commercial purposes; (2) the Documents may not be modified or altered in any way; and (3) General Electric Company withholds permission for making the Documents or any portion thereof accessible via the Internet. Except as expressly provided herein, you may not use, copy, print, display, reproduce, publish, license, post, transmit or distribute the Documents in whole or in part without the prior written permission of General Electric Company.

The information contained in this online publication is proprietary and subject to change without notice. The software described in this online publication is supplied under license and may be used or copied only in accordance with the terms of such license.

Trademark Notices

GE, Multilin™ and are trademarks and service marks of General Electric Company.

* Trademarks of General Electric Company.

IEC is a registered trademark of Commission Electrotechnique Internationale. IEEE is a registered trademark of the Institute of Electrical and Electronics Engineers, Inc. Internet Explorer, Microsoft, and Windows are registered trademarks of Microsoft Corporation. DisplayPort™ are trademarks owned by the Video Electronics Standards Association (VESA®) in the United States and other countries.

Other company or product names mentioned in this document may be trademarks or registered trademarks of their respective companies.

This printed manual is recyclable.

Please return for recycling where facilities exist.

Multilin™ G100 Substation Gateway

Table of contents

1 INTRODUCTION
- 1.1 About the document 1-1
  - 1.1.1 Purpose 1-1
  - 1.1.2 Intended Audience 1-1
  - 1.1.3 Additional Documentation 1-1
- 1.2 Safety symbols and definitions 1-1
- 1.3 Product Support 1-2
  - 1.3.1 Access the GE Grid Solutions web site 1-2
  - 1.3.2 Search GE Grid Solutions Technical Support library 1-2
  - 1.3.3 Contact Technical Support 1-2

2 UEFI OVERVIEW
- 2.1 Introduction 2-1
- 2.2 UEFI Boot Flow 2-1

3 UEFI SETUP INFORMATION
- 3.1 Entering Setup 3-1
- 3.2 Main 3-2
- 3.3 Advanced 3-3
  - 3.3.1 Super IO Configuration 3-4
  - 3.3.2 Hardware Monitor 3-9
  - 3.3.3 Watch Dog Timer Configuration 3-10
  - 3.3.4 Serial Port Console Redirection 3-11
  - 3.3.5 CPU Configuration 3-13
  - 3.3.6 PCI Subsystem Setting 3-16
  - 3.3.7 USB configuration 3-17
- 3.4 Chipset 3-18
  - 3.4.1 South Cluster Configuration 3-19
- 3.5 Security 3-21
  - 3.5.1 Secure Boot 3-22
- 3.6 Boot Menu 3-24
- 3.7 Save and Exit Menu 3-25

A MISCELLANEOUS
- A.1 Revision History A-1

Multilin™ G100 Substation Gateway

Chapter 1: Introduction

This chapter outlines safety and technical support information.

1.1 About the document

1.1.1 Purpose

This document describes how to ACCESS AND USE the Unified Extensible Firmware Interface (UEFI) that is embedded in the system ROM of G100 device. All options and available responses are defined.

1.1.2 Intended Audience

This document provides a reference for the person who installs, administers, and troubleshoots G100 device.

1.1.3 Additional Documentation

For further information about UEFI, refer to the following documents:

- MCP Substation Gateway, Software Configuration Guide SWM0101
- G100 Substation Gateway, Instruction Manual (994-0155)

1.2 Safety symbols and definitions

Before attempting to install or use the device, review all safety indicators in this document to help prevent injury, equipment damage, or downtime.

The following safety and equipment symbols are used in this document.

DANGER **Indicates a hazardous situation which, if not avoided, will result in death or serious injury.**

WARNING **Indicates a hazardous situation which, if not avoided, could result in death or serious injury.**

1

⚠CAUTION **Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.**

NOTICE Indicates practices not related to personal injury.

1.3 Product Support

If you need help with any aspect of your GE Grid Solutions product, you can:

- Access the GE Grid Solutions Web site
- Search the GE Grid Solutions Technical Support library
- Contact Technical Support

1.3.1 Access the GE Grid Solutions web site

The G100 Web site provides fast access to technical information, such as manuals and knowledge base topics.

Visit us on the Web at: http://www.gegridsolutions.com.

1.3.2 Search GE Grid Solutions Technical Support library

This site serves as a document repository for post-sales requests. To get access to the Technical Support Web site, go to:

Visit us on the Web at: http://sc.ge.com/*SASTechSupport

1.3.3 Contact Technical Support

For help with any aspect of your GE Grid Solutions product, please contact our support team, 24/7, as follows:

Region	E-mail	Telephone
Global Contact Centre	ga.support@ge.com	+44 1785 250070
Central and East Asia and Pacific	ga.supportCEAP@ge.com	+61 414 730 964
India	ga.supportIND@ge.com	+91 44 22648000
Middle East, North Africa and Turkey	ga.supportMENAT@ge.com	+971 42929467
Europe, Russia, CIS and Sub-Saharan Africa	ga.supportERCIS@ge.com	+34 94 4858854
North America	ga.supportNAM@ge.com	+1 877 605 6777
Latin America	ga.supportLAM@ge.com	+55 11 36187308

Multilin™ G100 Substation Gateway

Chapter 2: UEFI Overview

2.1 Introduction

Unified Extensible Firmware Interface (UEFI) is the program that controls the computer boot process. The purpose of the UEFI is to identify and initialize processor, memory, hard drives, optical drives, and other hardware.

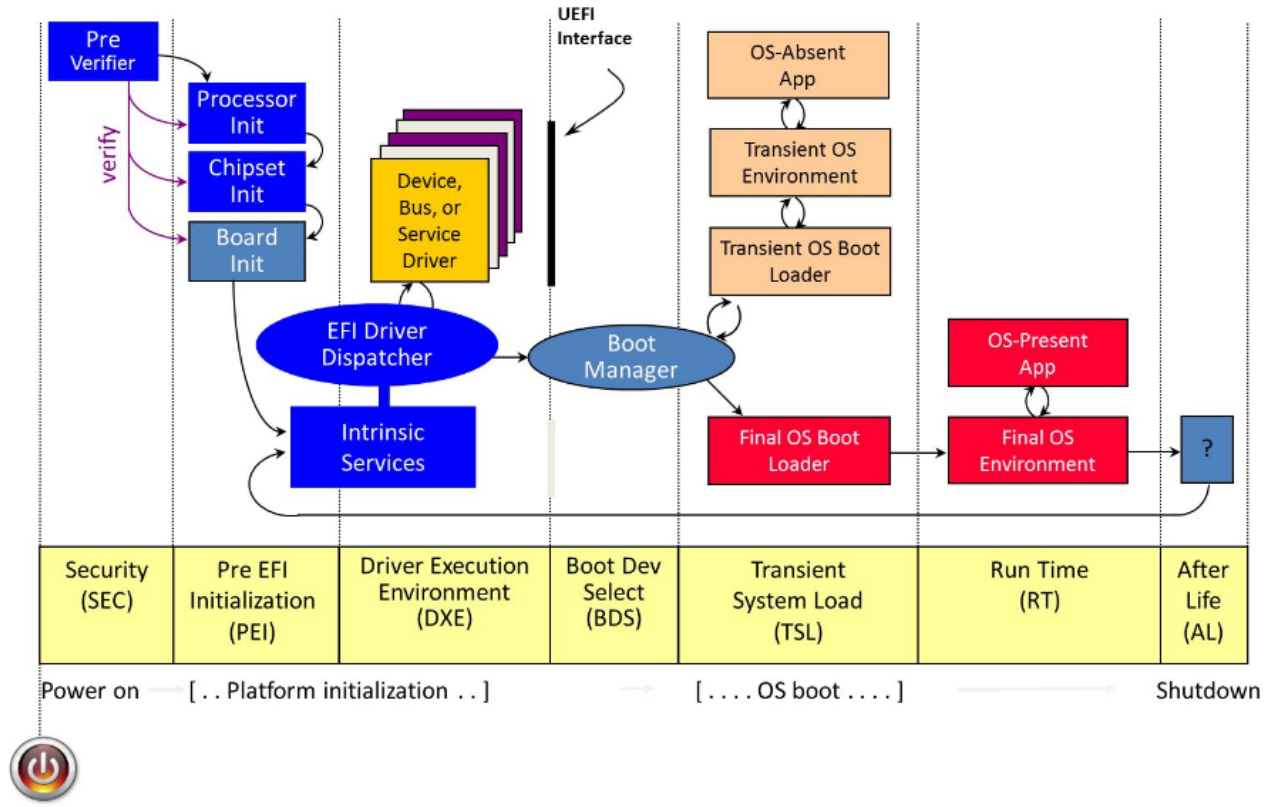
2.2 UEFI Boot Flow

UEFI core follows the firmware model described in the UEFI Platform Initialization Specification (PI). The PI Specification defines the following "boot phases", which can be applied to various checkpoints and beep code descriptions:

- **Security (SEC)** – low-level initialization
- **Pre-EFI Initialization (PEI)** – memory initialization
- **Driver Execution Environment (DXE)** – main hardware initialization
- **Boot Device Selection (BDS)** – system setup, pre-OS user interface & selecting a bootable device (CD/DVD, HDD, USB, Network, Shell, etc).

2

Figure 2-1: Platform Initialization (PI) Boot Phases



Multilin™ G100 Substation Gateway

Chapter 3: UEFI Setup Information

3.1 Entering Setup

To enter the UEFI setup utility, simply follow the steps below:

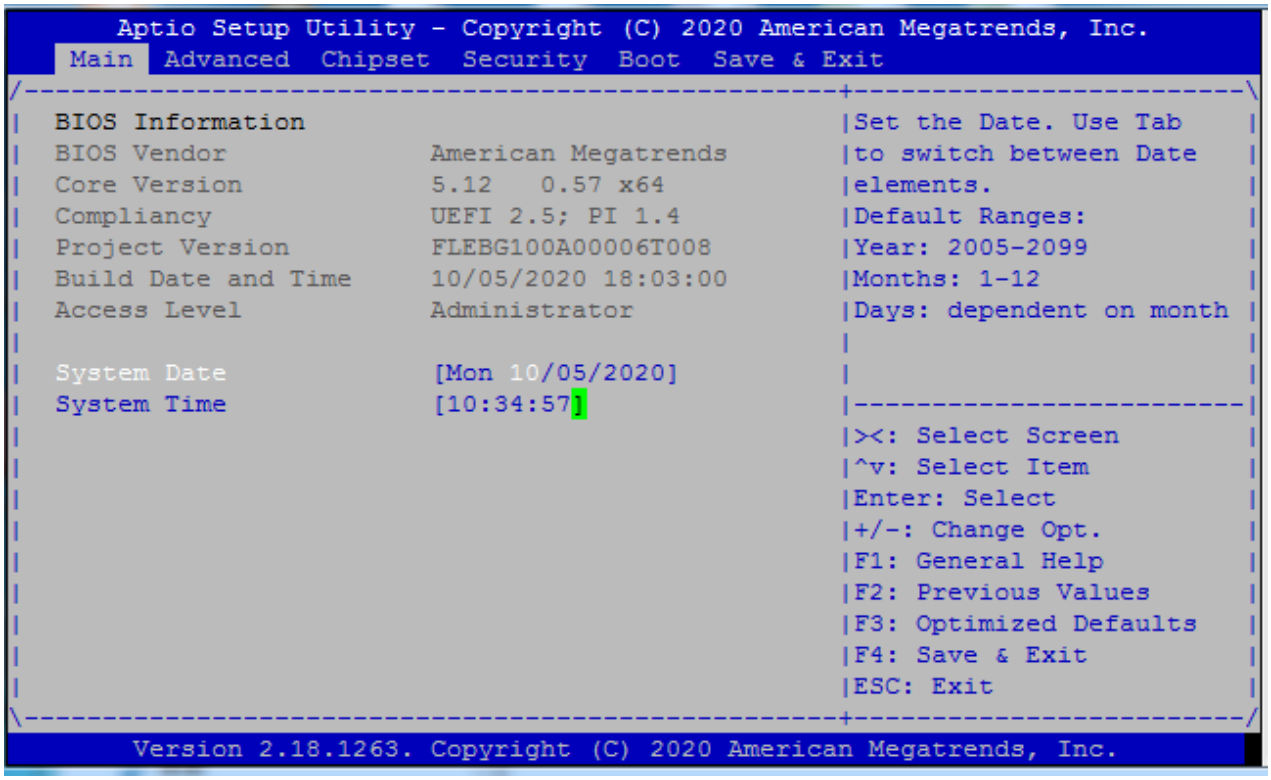
Boot up the system.

Pressing the **<Tab>** or **<Del>** key immediately allows you to enter the Setup utility, then you will be directed to the UEFI main screen. The instructions for UEFI navigations are as below:

Control Keys	Description
→←	Select a setup screen
↑↓	Select an item/option on a setup screen
<Enter>	Select an item/option or enter a sub-menu
+/-	Adjust values for the selected setup item/option
F1	Display General Help screen
F2	Retrieve previous values
F3	Load optimized default values
F4	Save configurations and exit UEFI
<Esc>	Exit current screen

3.2 Main

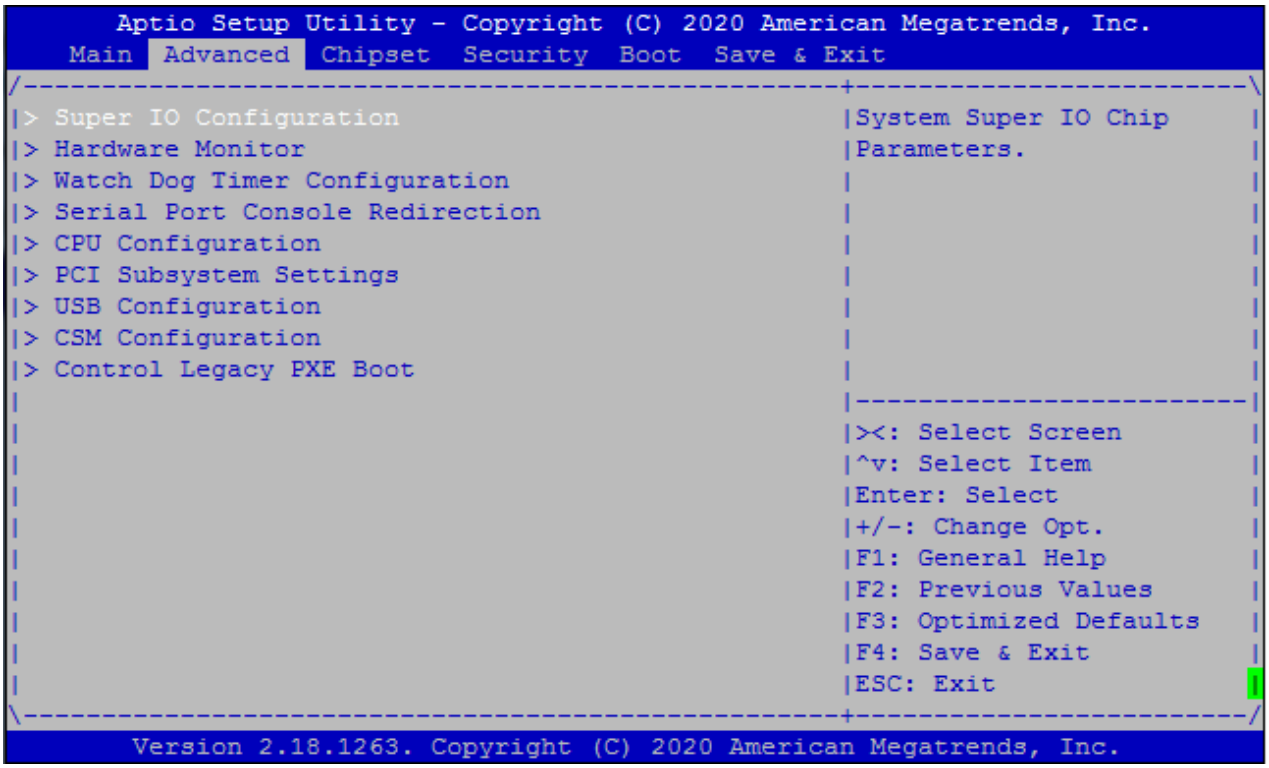
Setup main page contains UEFI information and project version information.



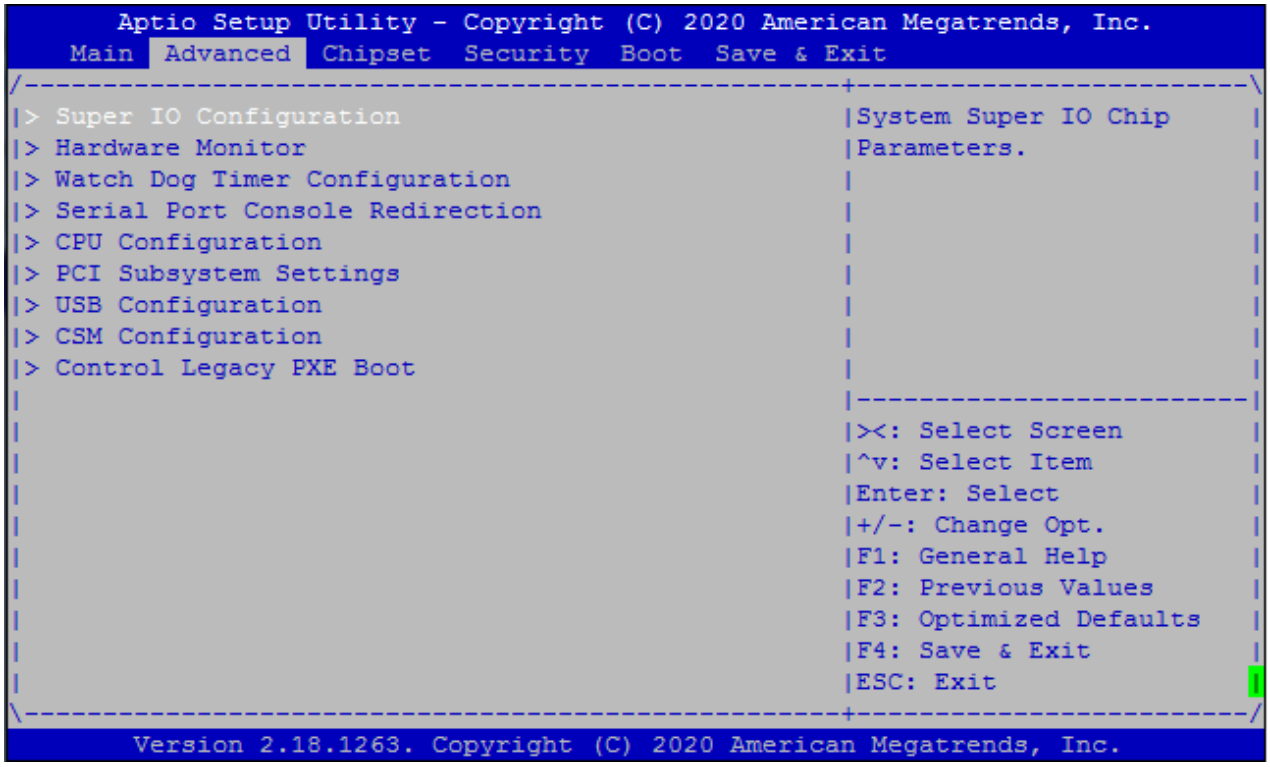
Feature	Description
BIOS Information	BIOS Vendor: American Megatrends
	Core Version: AMI Kernel version, CRB code base, X64
	Compliance: UEFI version, PI version
	Project Version: BIOS release version
	Build Date and Time: MM/DD/YYYY
	Access Level: Administrator / User
System Date	To set the Date, use <Tab> to switch between Date elements. Default Range of Year: 2005-2099
	Default Range of Month: 1-12
	Days: dependent on Month.
System Time	To set the Date, use <Tab> to switch between Date elements.

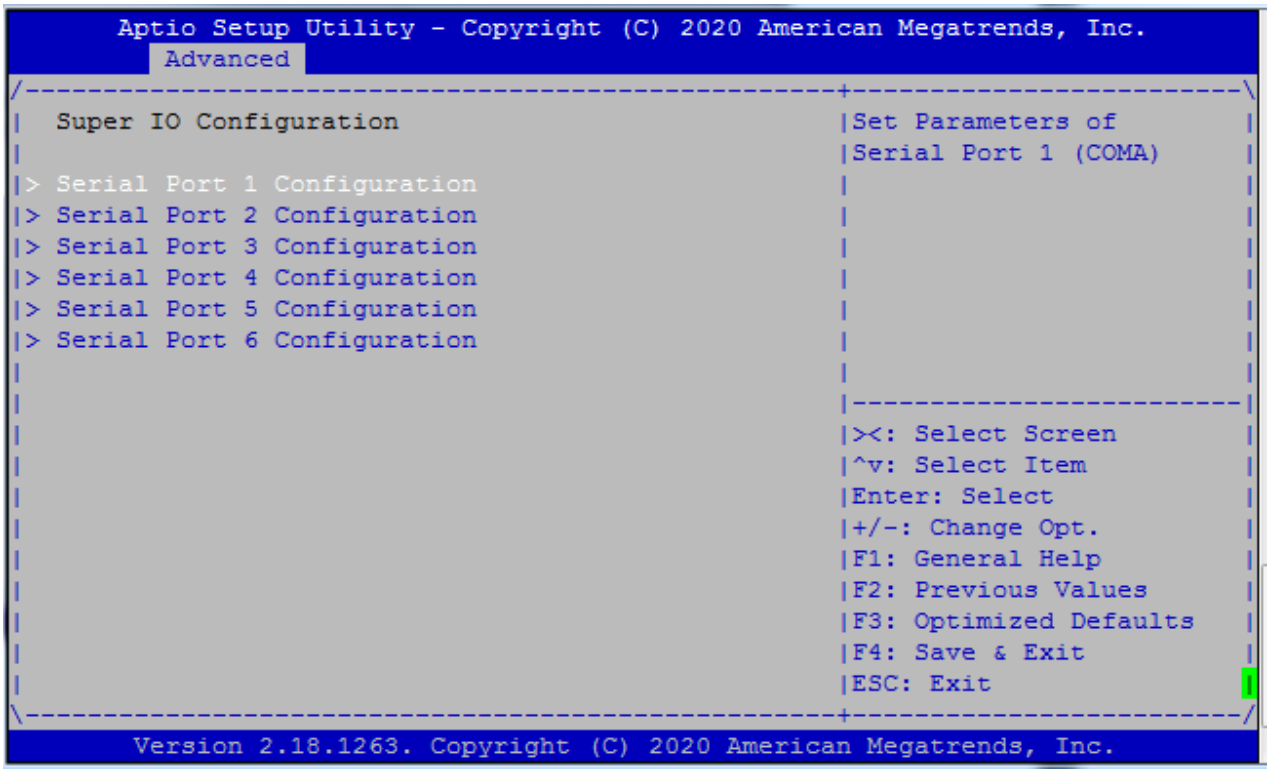
3.3 Advanced

Select the Advanced menu item from the UEFI setup screen to enter the “Advanced” setup screen. Users can select any of the items in the left frame of the screen.

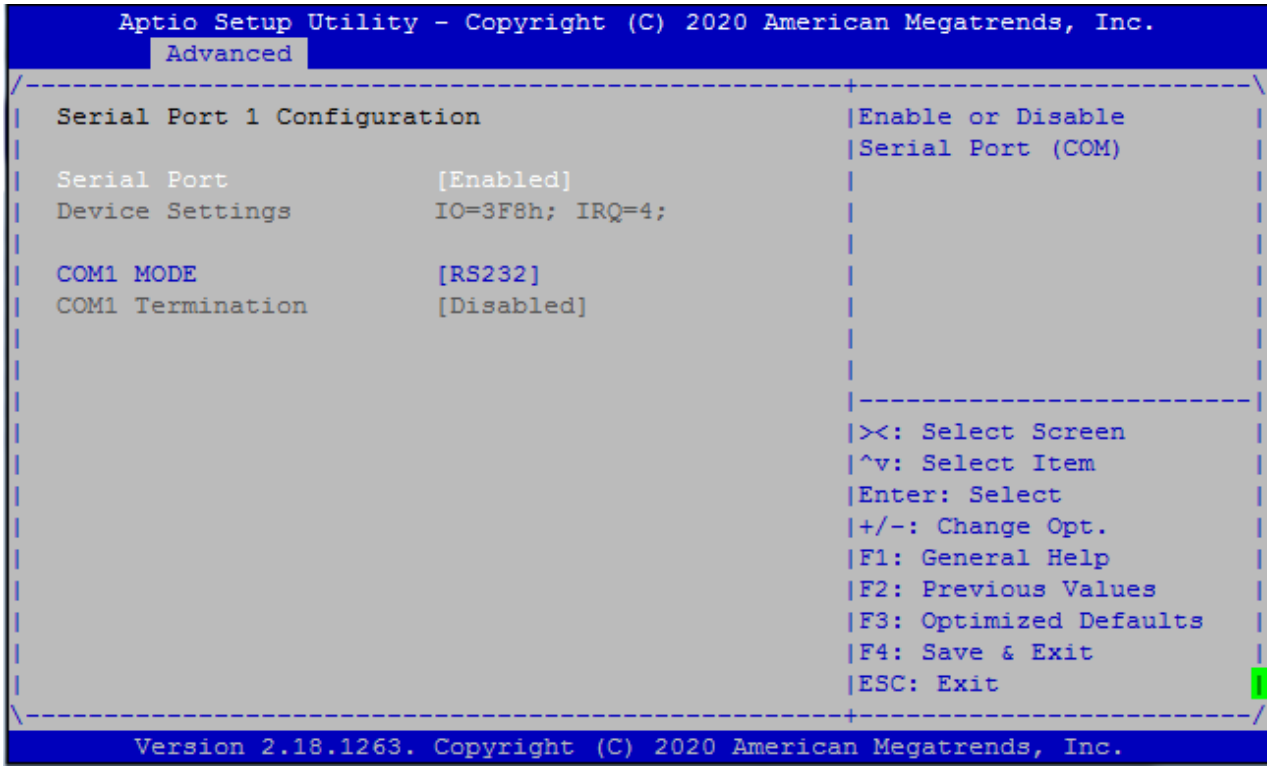


3.3.1 Super IO Configuration



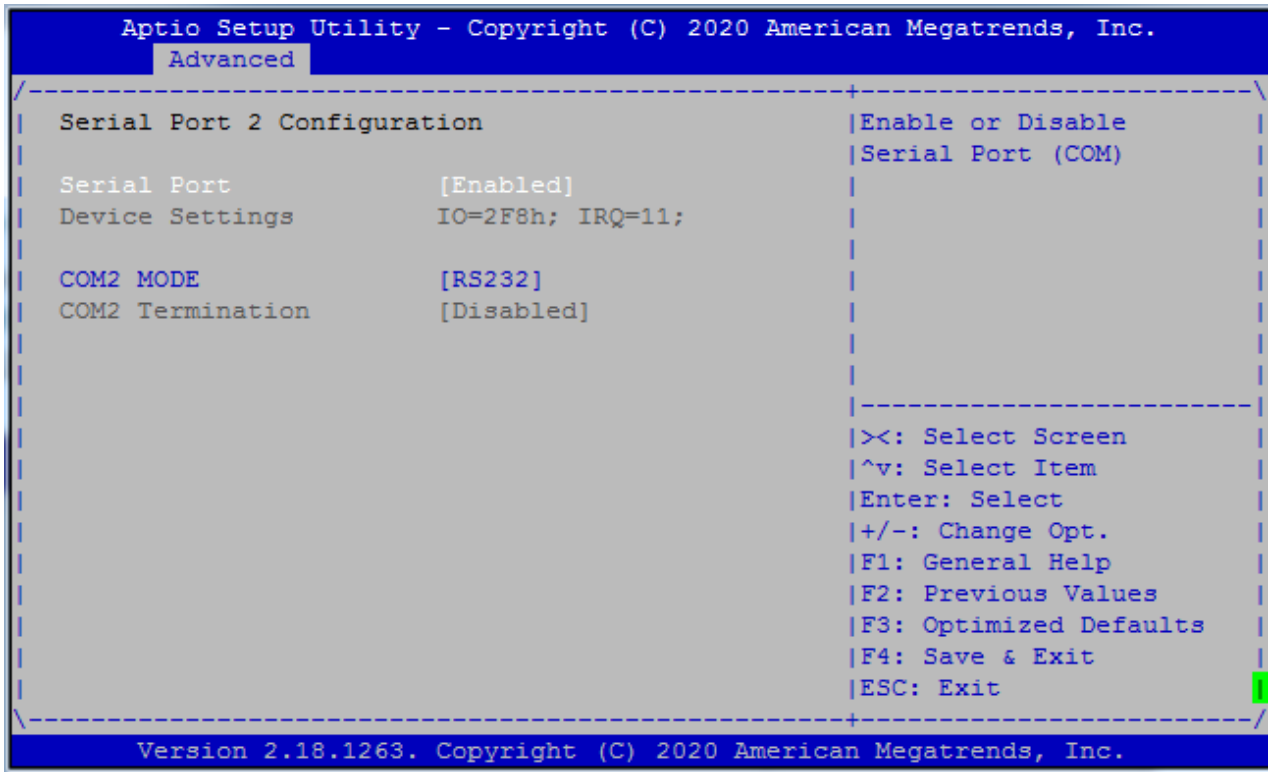


3.3.1.1 Serial Port 1 Configuration



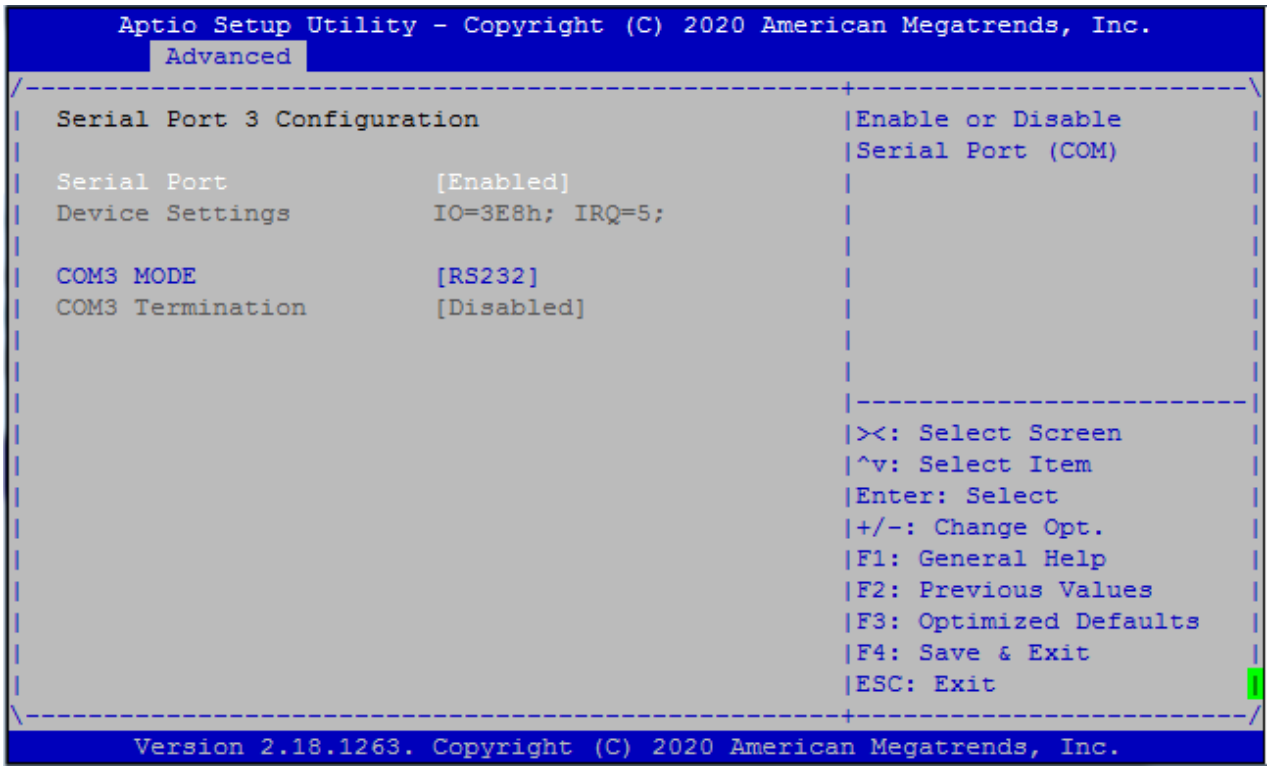
Feature	Options	Description
Serial Port Redirection	Enabled (Default) Disabled	Enable or Disable Serial Port (COM)
Device Settings	IO=3F8h; IRQ=4;	
COM1 MODE	RS232 (Default) RS485	Select Com Mode as RS232/RS485
COM1 Termination	Enabled Disabled (Default)	COM RS-422/485 Receiver Termination

3.3.1.2 Serial Port 2 Configuration



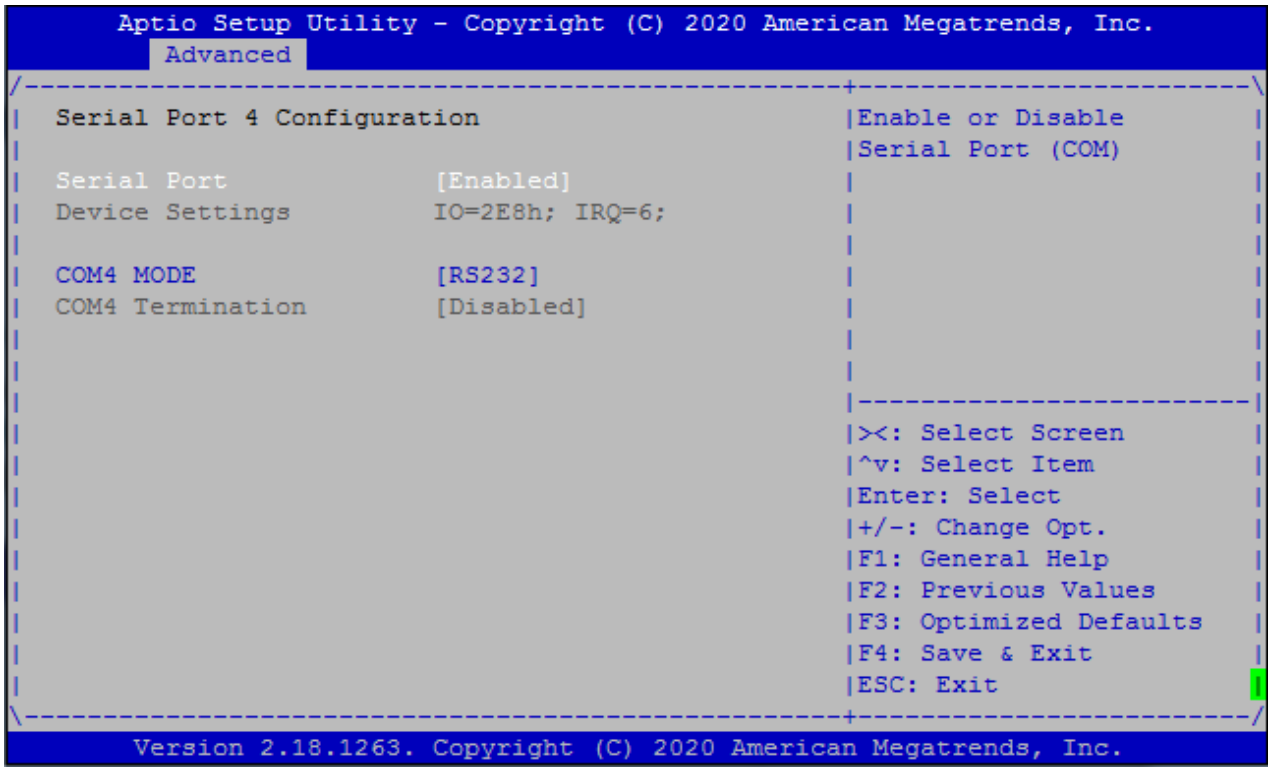
Feature	Options	Description
Serial Port Redirection	Enabled (Default) Disabled	Enable or Disable Serial Port (COM)
Device Settings	IO=2F8h; IRQ=11;	
COM1 MODE	RS232 (Default) RS485	Select Com Mode as RS232/RS485
COM2 Termination	Enabled Disabled (Default)	COM RS-422/485 Receiver Termination

3.3.1.3 Serial Port 3 Configuration



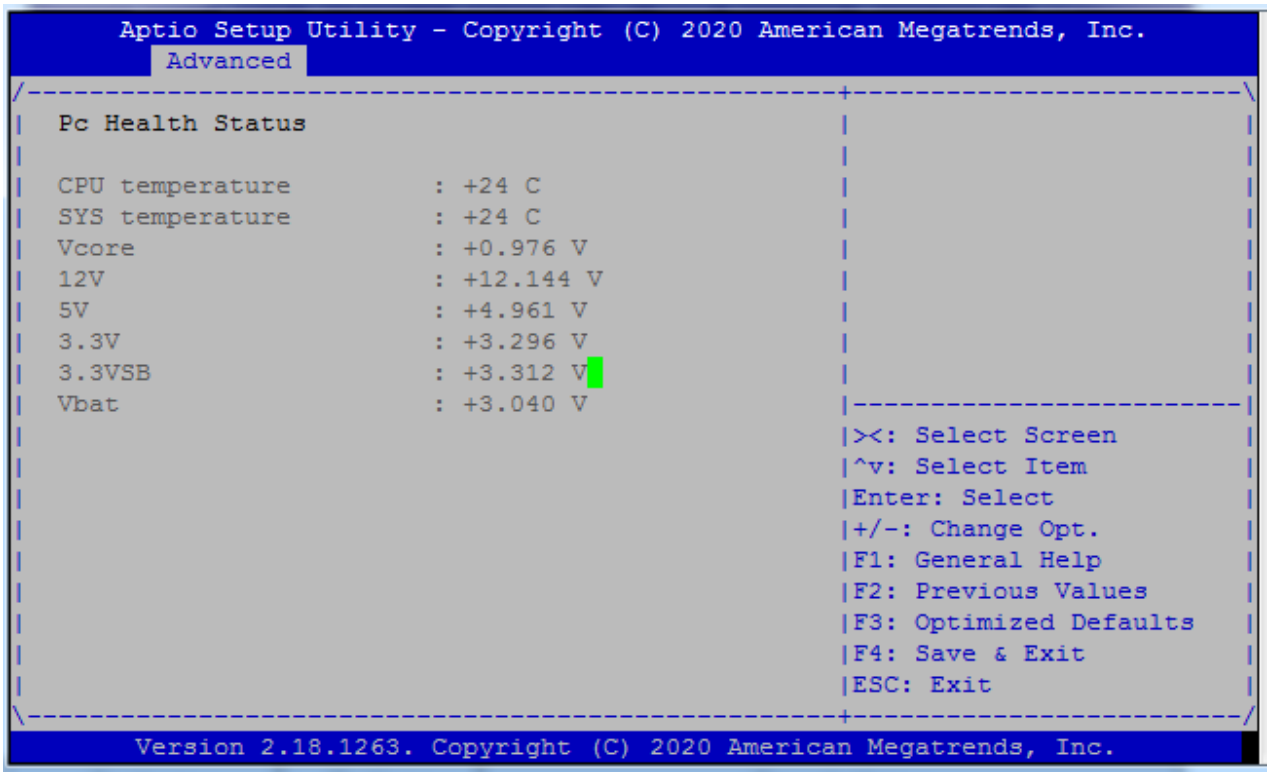
Feature	Options	Description
Serial Port Redirection	Enabled (Default) Disabled	Enable or Disable Serial Port (COM)
Device Settings	IO=3E8h; IRQ=5;	
COM1 MODE	RS232 (Default) RS485	Select Com Mode as RS232/RS485
COM3 Termination	Enabled Disabled (Default)	COM RS-422/485 Receiver Termination

3.3.1.4 Serial Port 4 Configuration



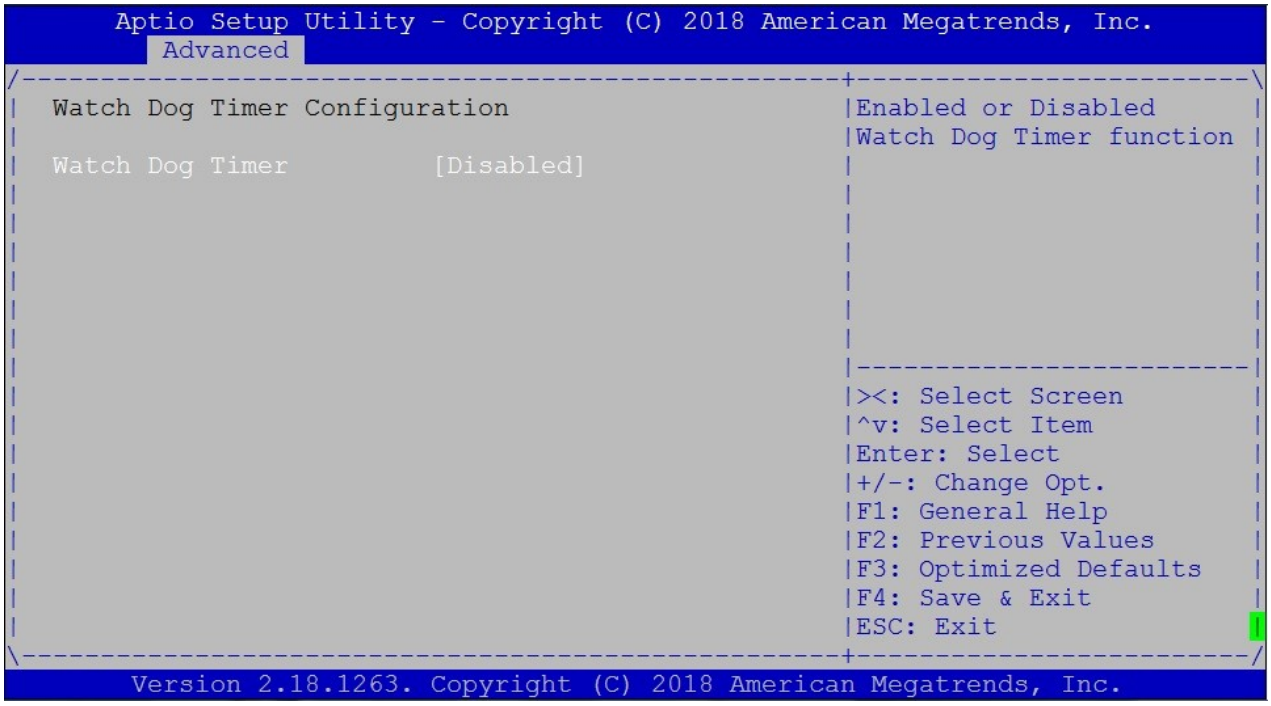
Feature	Options	Description
Serial Port Redirection	Enabled (Default) Disabled	Enable or Disable Serial Port (COM)
Device Settings	IO=2E8h; IRQ=6;	
COM1 MODE	RS232 (Default) RS485	Select Com Mode as RS232/RS485
COM4 Termination	Enabled Disabled (Default)	COM RS-422/485 Receiver Termination

3.3.2 Hardware Monitor



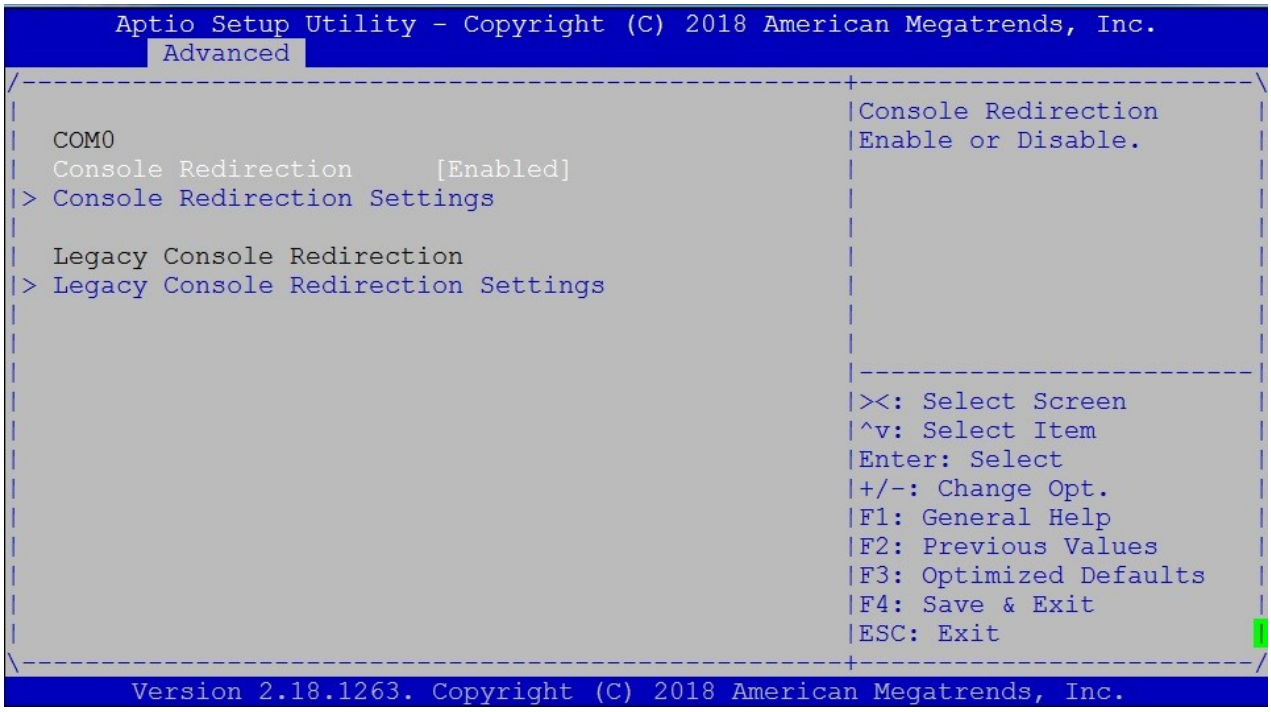
Feature	Description
CPU temperature	This value reports the CPU temperature.
System temperature	This value reports the System temperature.
Vcore	This value reports the CPU VCORE.
12V	This value reports the 12V Input voltage.
5V	This value reports the 5V Input voltage.
3.3V	This value reports the 3.3V Input voltage.
3.3VSB	This value reports the VSB3V Input voltage.
VBAT	This value reports the VBAT Input voltage.

3.3.3 Watch Dog Timer Configuration



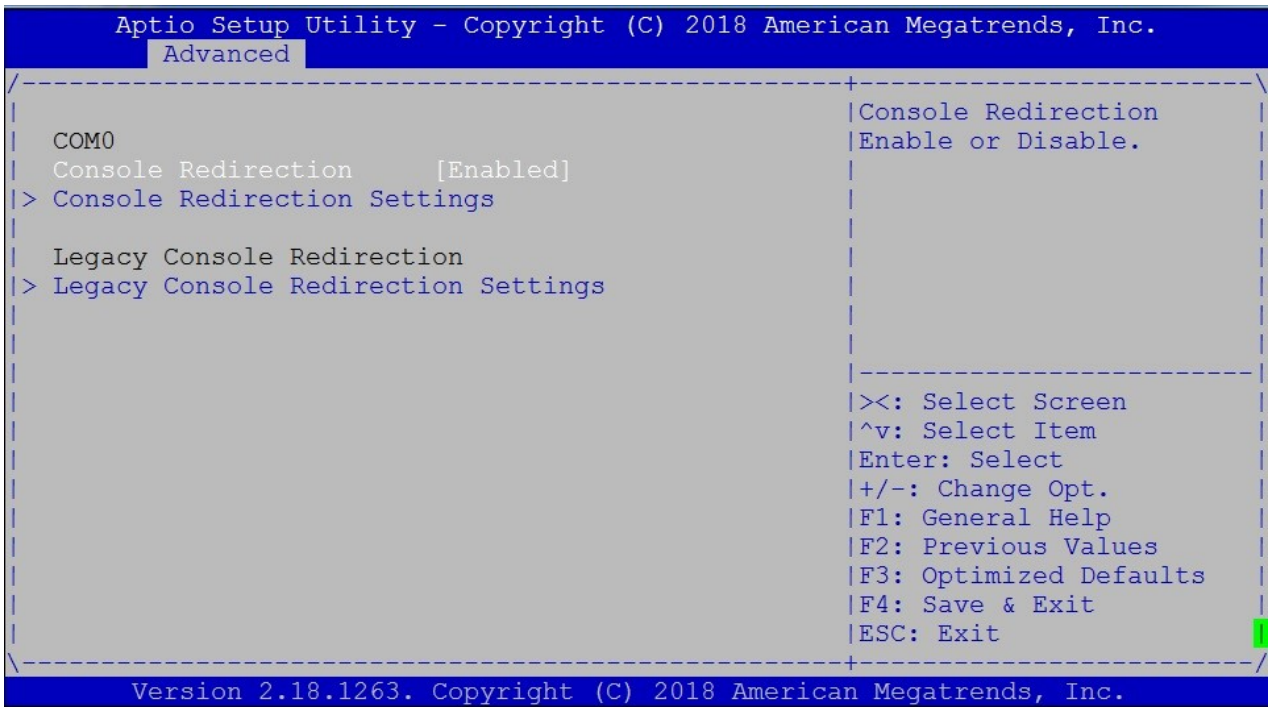
Feature	Options	Description
Watch Dog Timer	Enabled Disabled (Default)	Enable or Disable Watch Dog function

3.3.4 Serial Port Console Redirection



Feature	Options	Description
COM0 Console Redirection	Enabled (Default) Disabled	Console Redirection Enable or Disable.

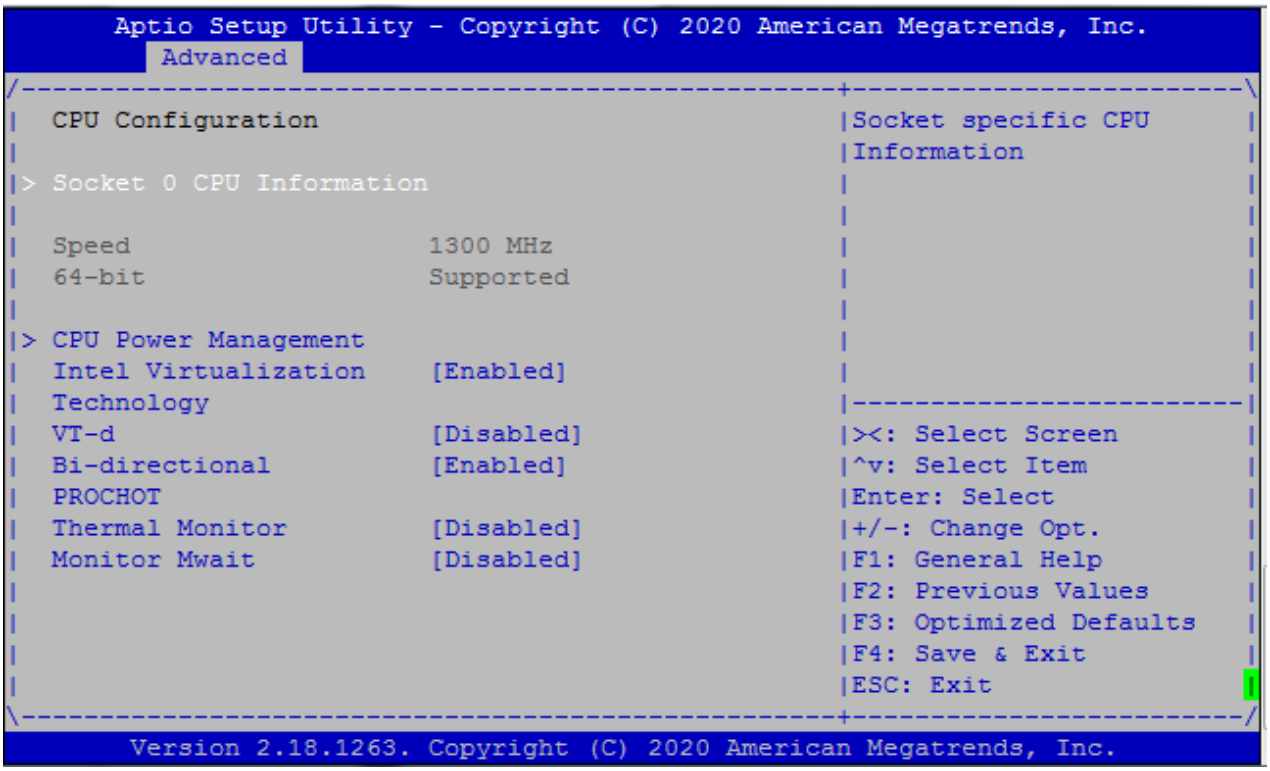
3.3.4.1 Console Redirection Setting



Feature	Options	Description
Terminal Type	VT100 VT100+ (Default) VT-UTF8 ANSI	ANSI: Extended ASCII char set. VT100: ASCII char set. VT100+: Extends VT100 to support color, function keys, etc. VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.
Bits per second	9600 19200 38400 57600 115200 (Default)	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Data Bits	7 8 (Default)	Data Bits
Parity	None (Default) Even Odd Mark Space	A parity bit can be sent with the data bits to detect some transmission errors.
Stop Bits	1 (Default) 2	Stop bits indicate the end of a serial data packet.
Flow Control	None (Default) Hardware RTS/CTS	Flow control can prevent data loss from buffer overflow.
VT-UTF8 Combo Key Support	Disabled Enabled (Default)	Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals
Recorder Mode	Disabled (Default) Enabled	With this mode enabled only text will be sent. This is to capture Terminal data.
Resolution 100x31	Disabled (Default) Enabled	Enables or disables extended terminal resolution.

Feature	Options	Description
Putty KeyPad	VT100 (Default) Intel LINUX XTERMR6 SCO ESCN VT400	Select FunctionKey and KeyPad on Putty.
Redirection COM Port	COM0	Select a COM port to display redirection of Legacy OS and Legacy OPROM Messages.
Resolution	80x24 (Default) 80x25	On Legacy OS, the Number of Rows and Columns supported redirection.
Redirection After POST	Always Enable (Default) BootLoader	When Bootloader is selected, then Legacy Console Redirection is disabled before booting to legacy OS. When Always Enable is selected, then Legacy Console Redirection is enabled for legacy OS. Default setting for this option is set to Always Enable.

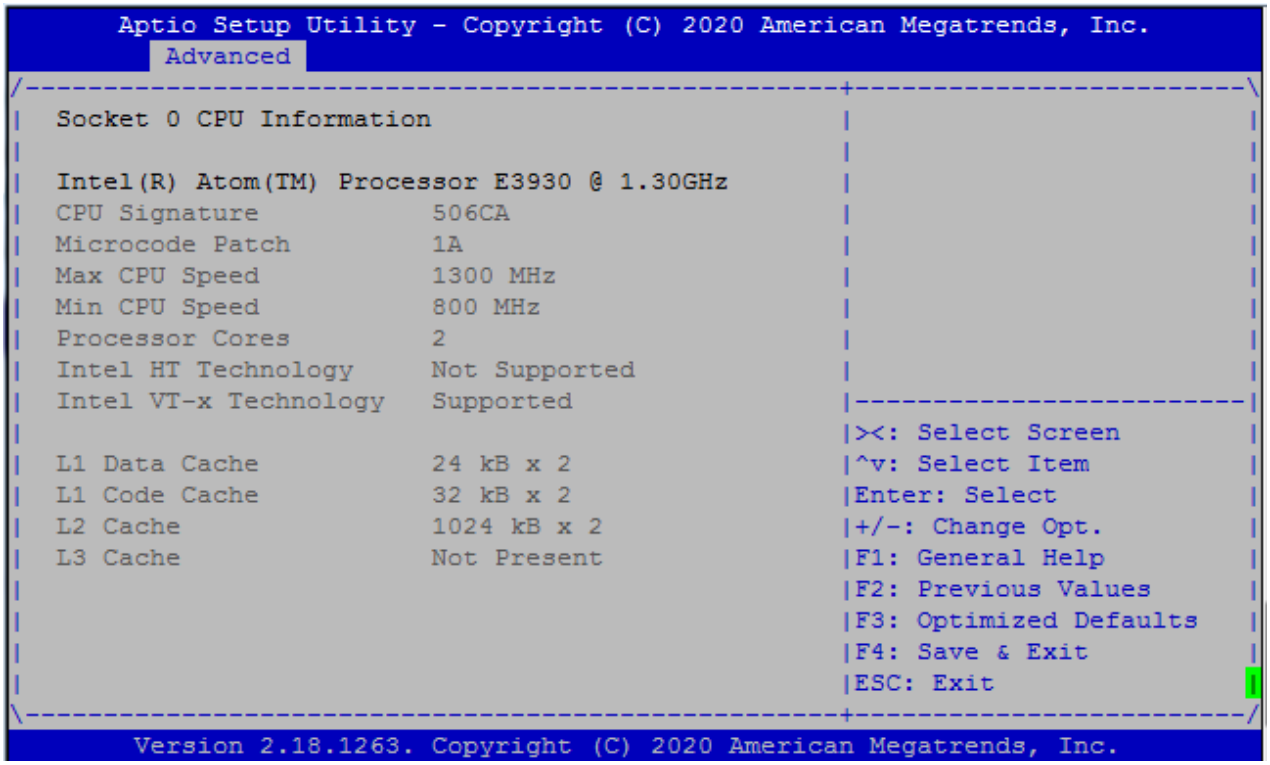
3.3.5 CPU Configuration



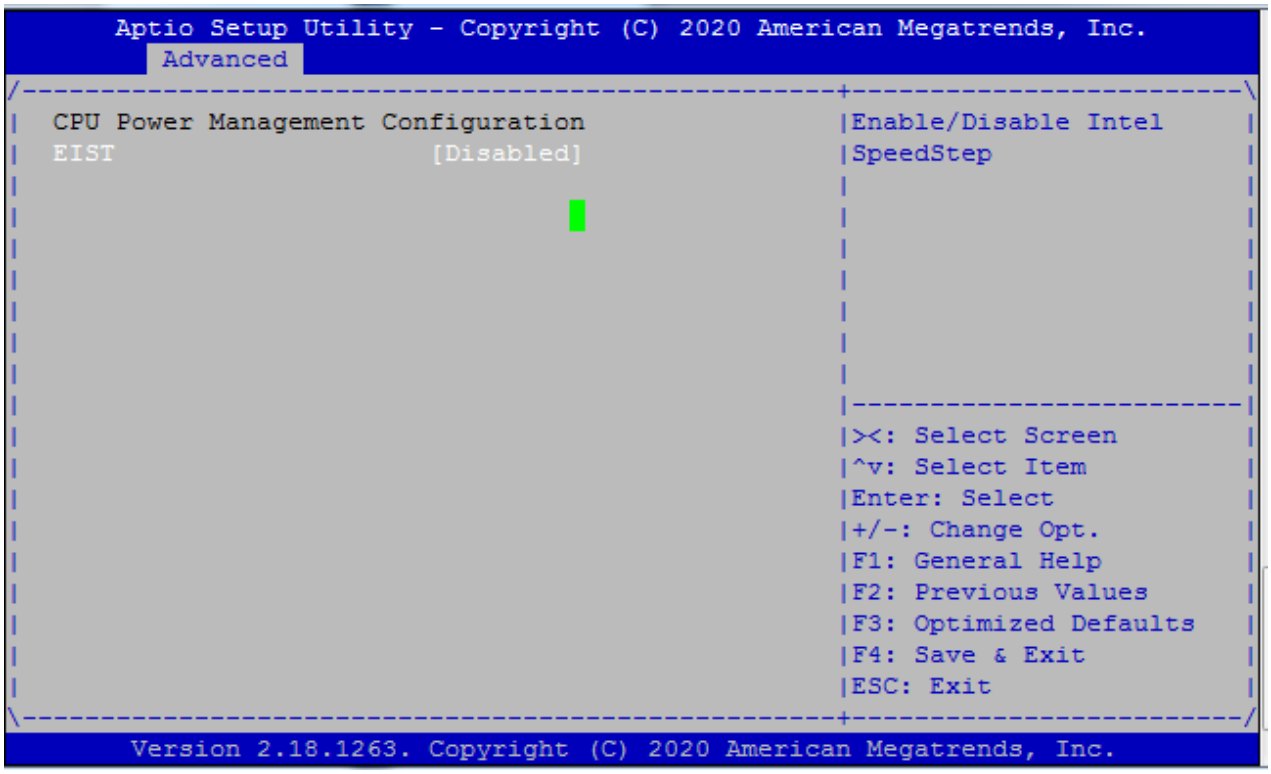
Feature	Options	Description
Intel Virtualization Technology	Disabled Enabled (Default)	When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology
VT-d	Disabled Enabled (Default)	Enable/Disable CPU VT-d
Bi-directional PROCHOT	Disabled Enabled (Default)	When a processor thermal sensor trips (either core), the PROCHOT# will be driven. If bi-direction is enabled, externl agents can drive PROCHOT# to throttle.

Feature	Options	Description
Thermal Monitor	Disabled (Default) Enabled	Enable/Disable Thermal Monitor.
Monitor Mwait	Disabled (Default) Enabled	Enable/Disable Monitor Mwait.

3.3.5.1 Socket 0 CPU Information

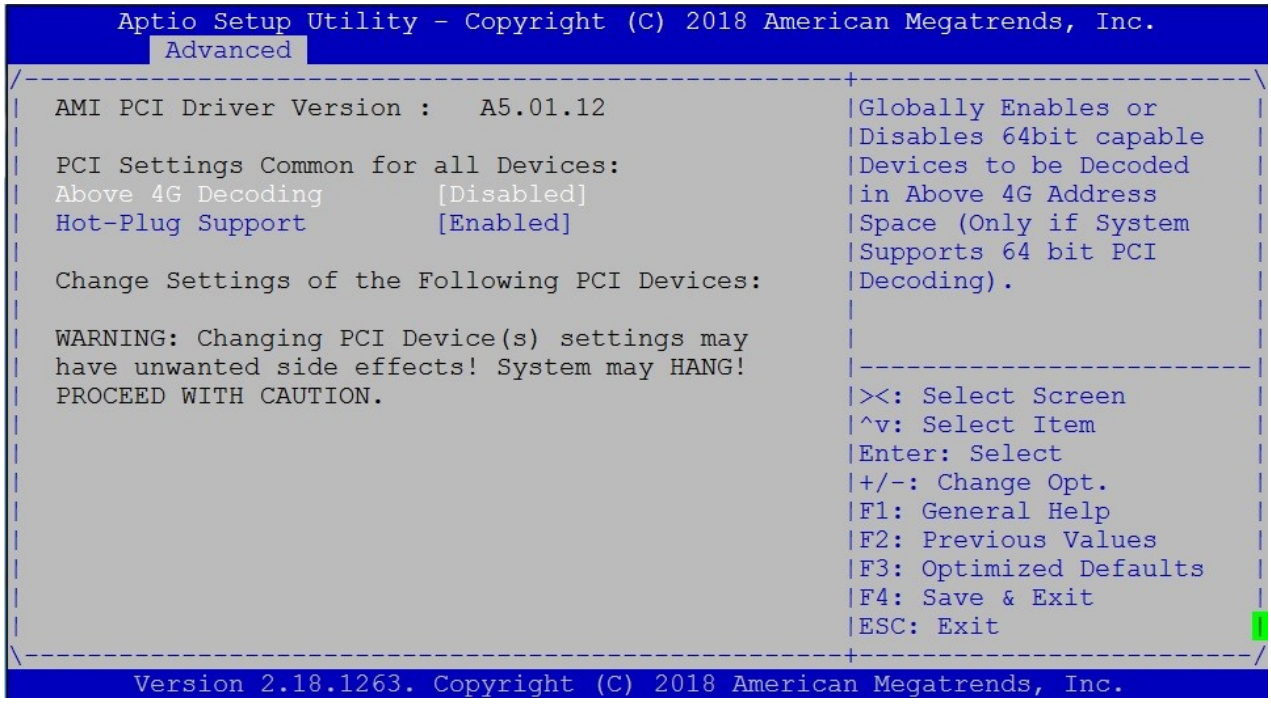


3.3.5.2 CPU Power Management



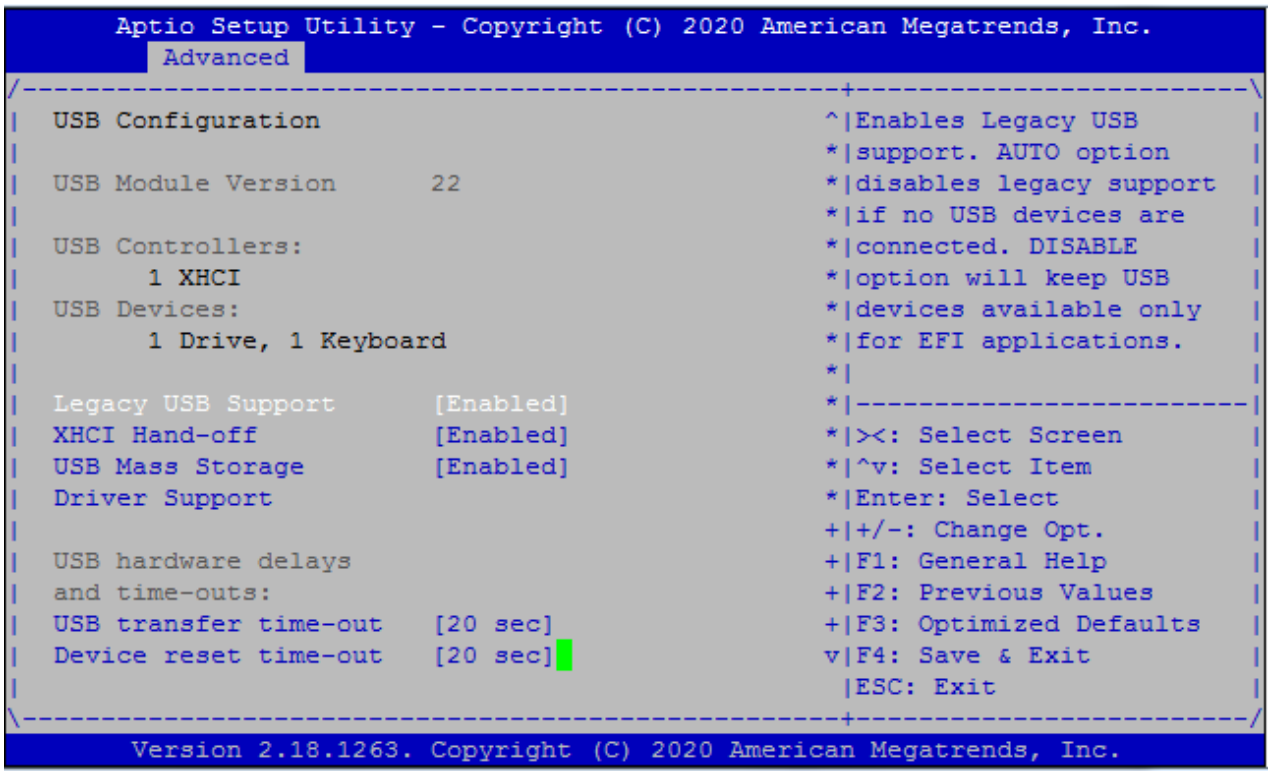
Feature	Options	Description
EIST	Disabled (Default) Enabled	Enable/Disable Intel SpeedStep

3.3.6 PCI Subsystem Setting



Feature	Options	Description
Above 4G Decoding	Disabled (Default) Enabled	Globally Enable or Disables 64bit capable Devices to be Decoded in Above 4G Address Space (Only if System Supports 64 bit PCI Decoding).
Hot-Plug Support	Disabled Enabled (Default)	Globally Enables or Disables Hot-Plug support for the entire System.

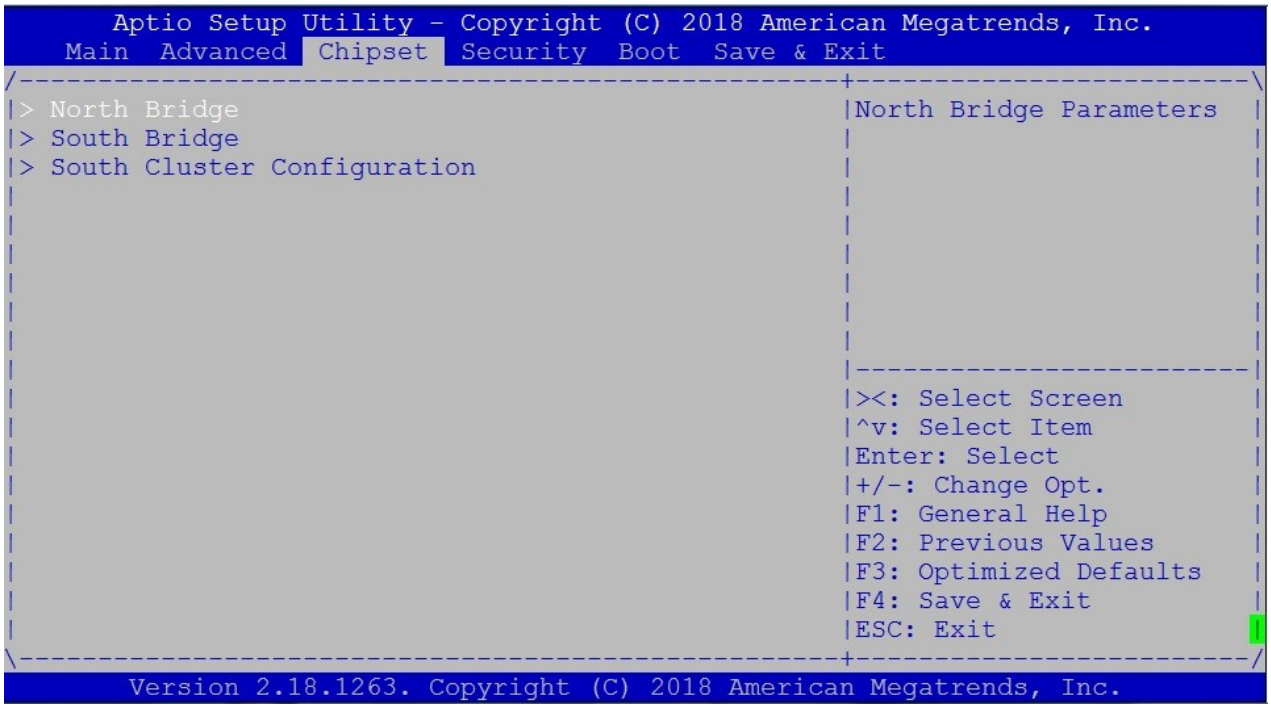
3.3.7 USB configuration



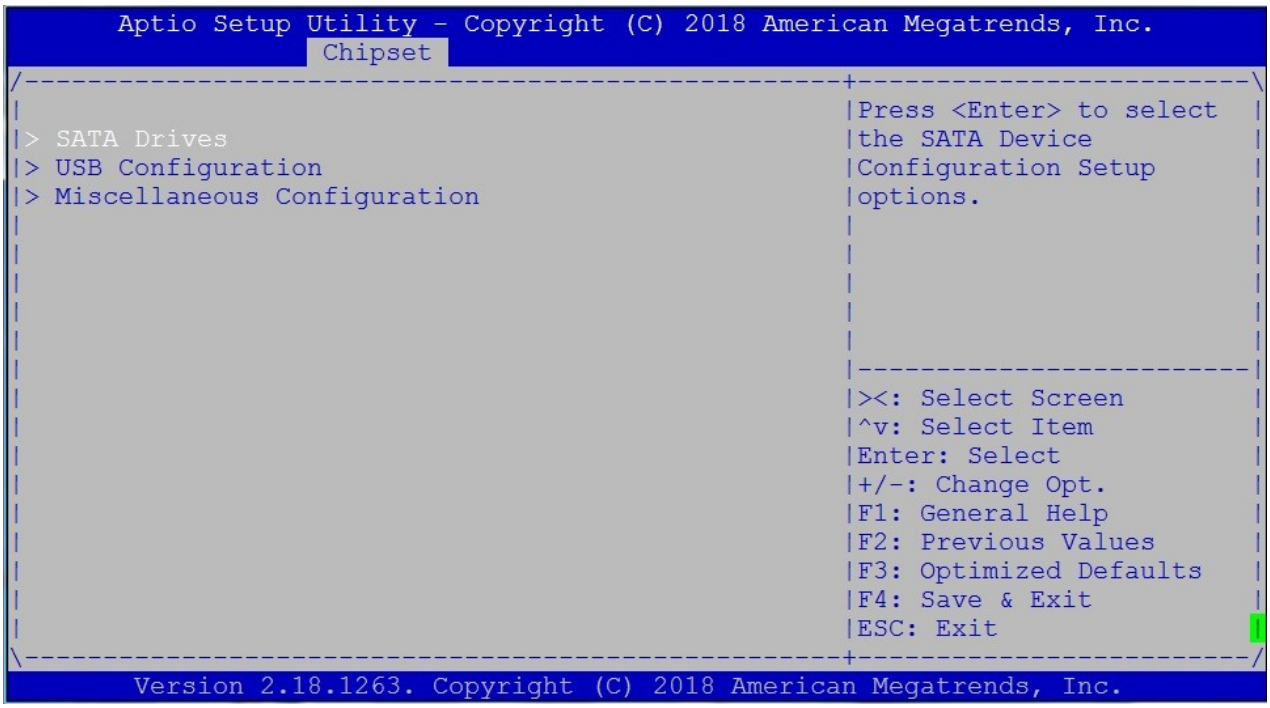
Feature	Options	Description
Legacy USB Support	Enabled (Default) Disabled Auto	Enables Legacy USB support. **Auto** option disables legacy support if no USB devices are connected; **Disabled** option will keep USB devices available only for EFI applications.
XHCI Hand-off	Enabled (Default) Disabled	This is a workaround for OSes without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.
USB Mass Storage Driver Support	Enabled (Default) Disabled	Enables or disables USB Mass Storage Driver Support.
USB transfer time-out	1 sec 5 sec 10 sec 20 sec (Default)	The time-out value for Control, Bulk, and Interrupt transfers.
Device reset time-out	1 sec 5 sec 10 sec 20 sec (Default)	USB mass storage device Start Unit command time-out
Device power-up delay	Auto (Default) Manual	Maximum time the device will take before it properly reports itself to the Host Controller. Auto uses default value: for a Root port, it is 100 ms, for a Hub port the delay is taken from Hub descriptor.

3.4 Chipset

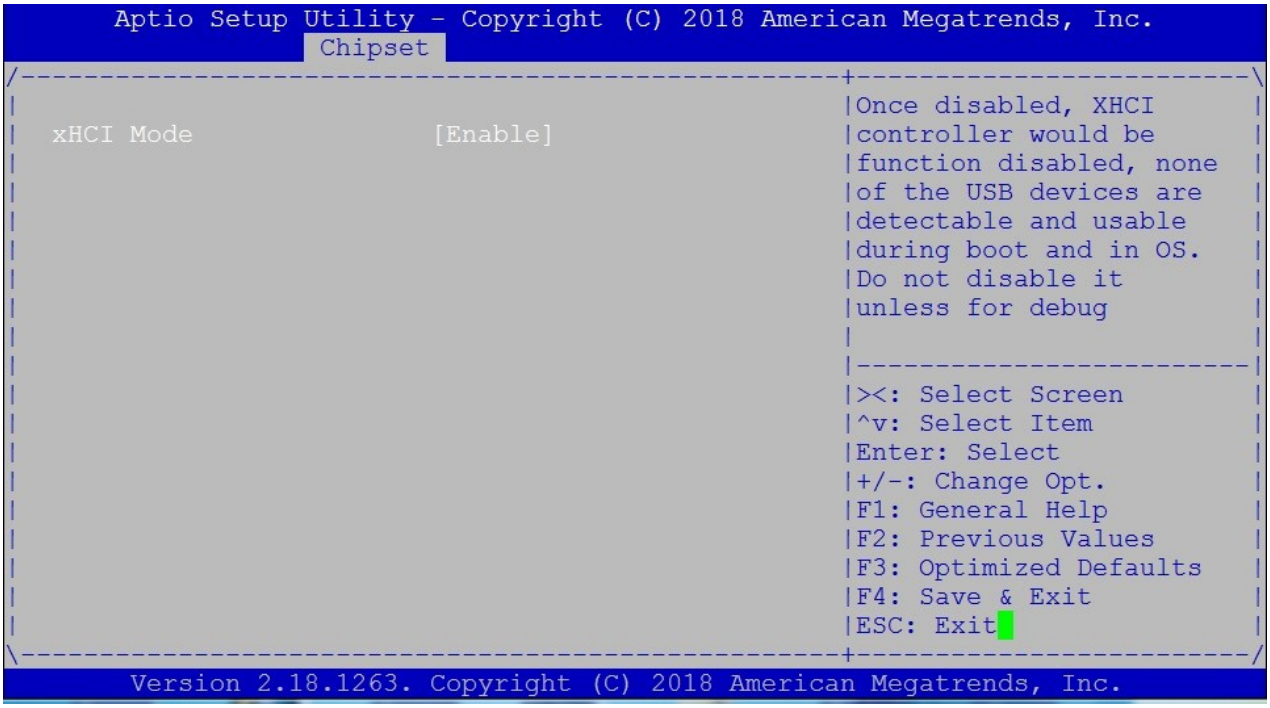
Select the **Chipset** menu item from the UEFI setup screen to enter the "Chipset" setup screen. Users can select any of the items in the left frame of the screen.



3.4.1 South Cluster Configuration

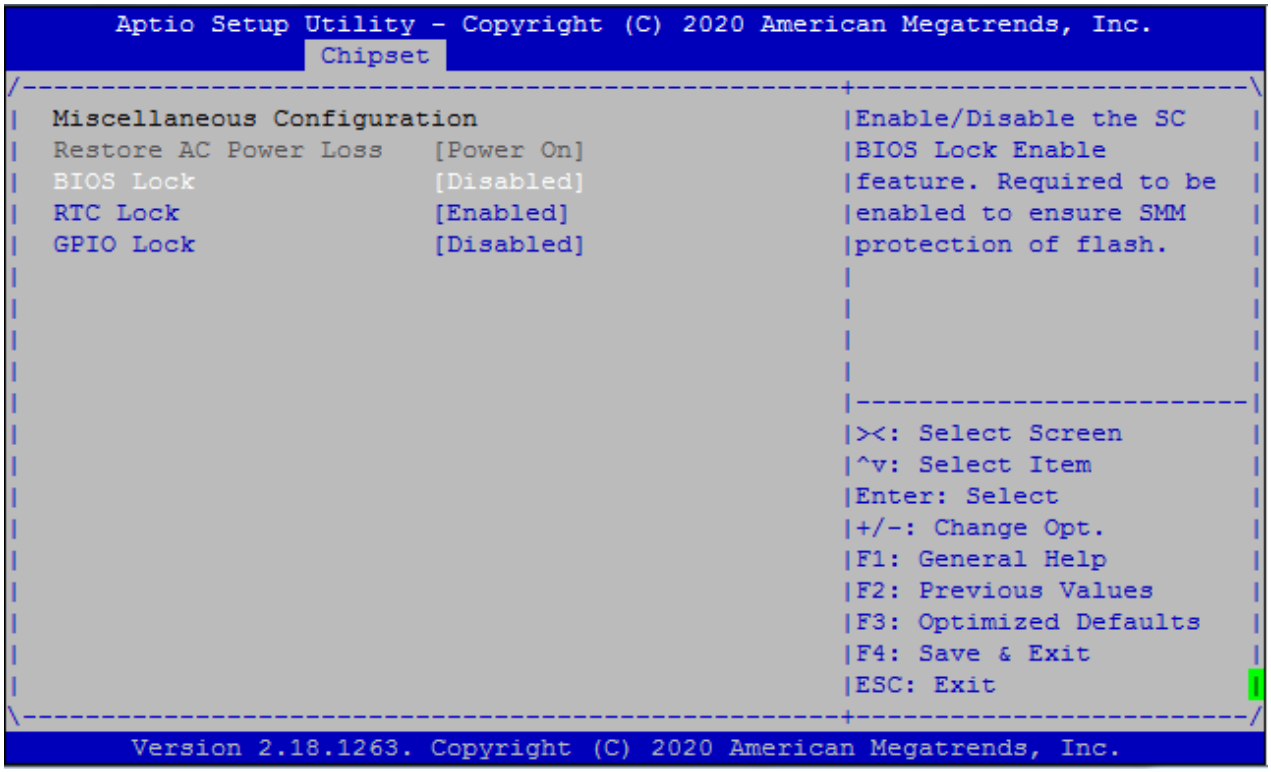


3.4.1.1 USB Configuration



Feature	Options	Description
xHCI Mode	Enable (Default) Disable	Once disabled . XHCI controller would be function disabled, none of the USB devices are detect and usable during boot and in OS. Do not disable it unless for debug

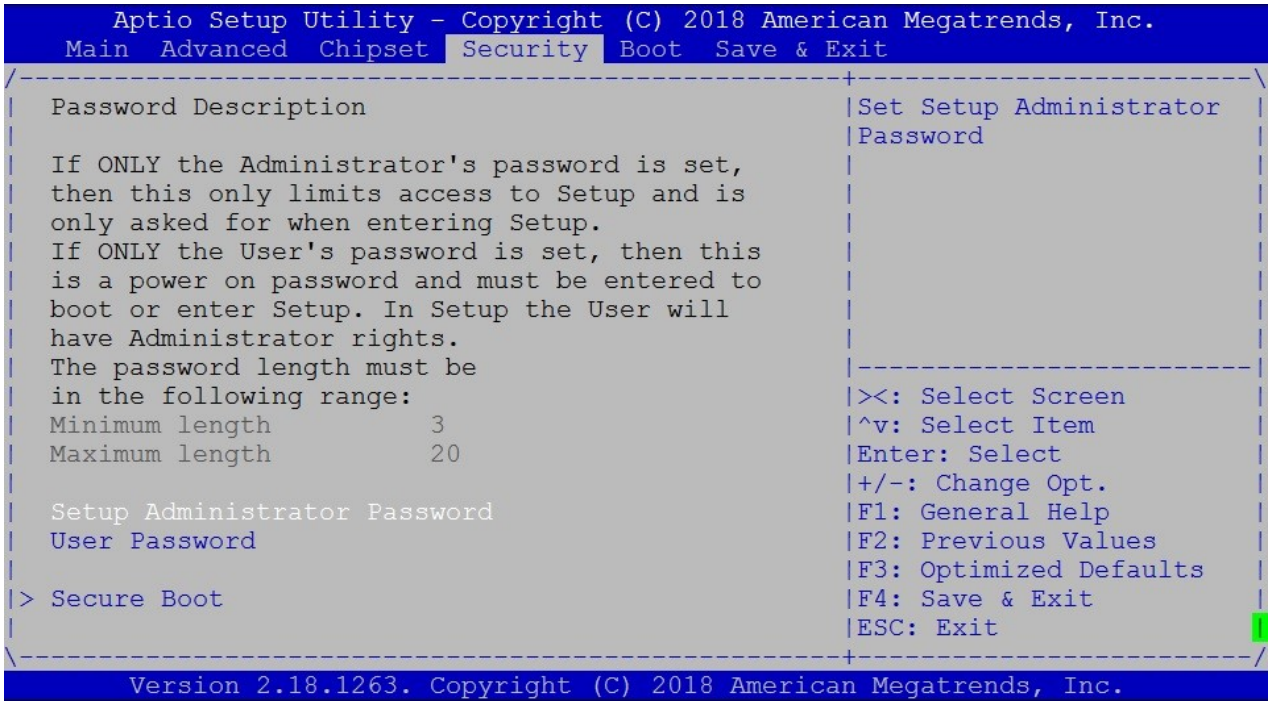
3.4.1.2 Miscellaneous Configuration



Feature	Options	Description
Restore AC Power Loss	Power On (Default) Power Off Last State	Specify what state to go to when power is re-applied after a power failure (G3 state). S0 State: System will boot directly as soon as power applied. S5 State: System keeps in power-off state until power button is pressed.
BIOS Lock	Disabled Enabled (Default)	Enable / Disable the SC BIOS Lock Enabled feature. Required to be enabled to ensure SMM protection of flash .
RTC Lock	Disabled Enabled (Default)	Enable will lock bytes 38h-3Fh in the lower/upper 128-byte bank of RAM.
GPIO Lock	Disabled Enabled (Default)	Enable to set GPIO Pad Configuration lock for security..

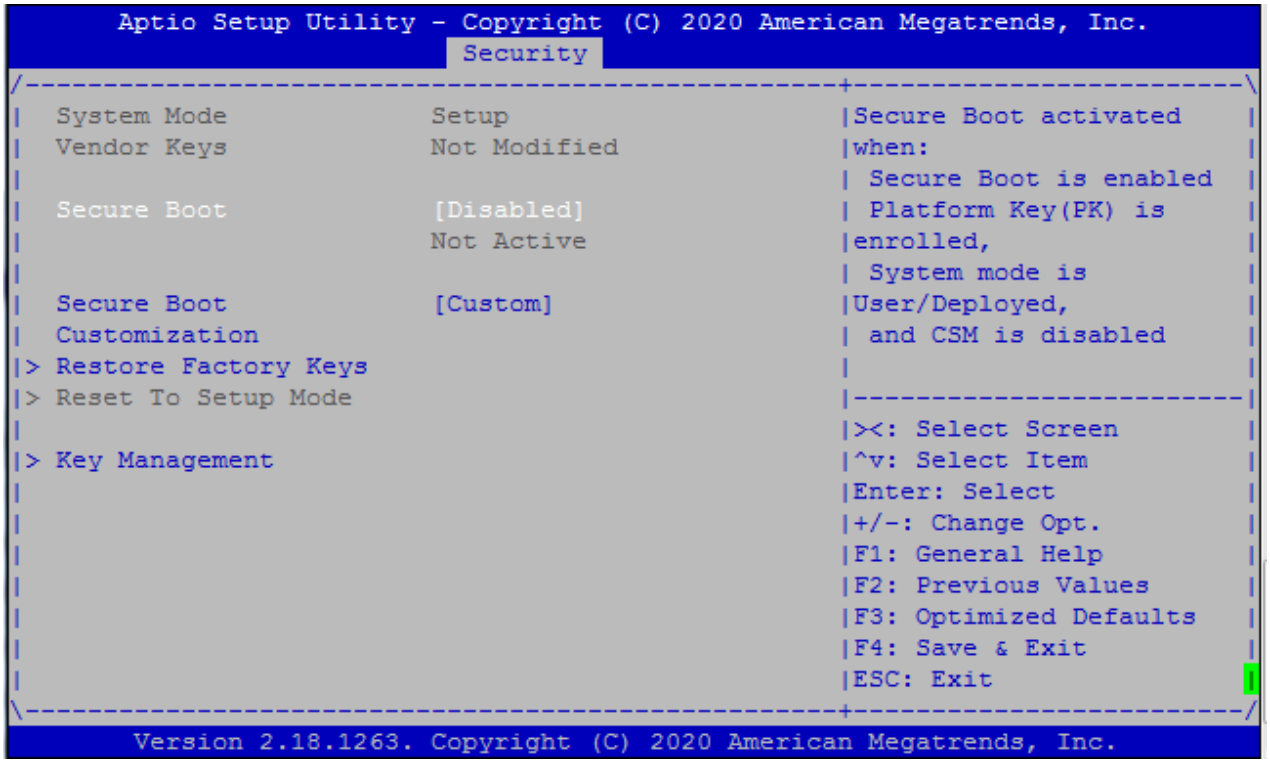
3.5 Security

Select the Security menu item from the UEFI setup screen to enter the Security Setup screen. Users can select any of the items in the left frame of the screen.



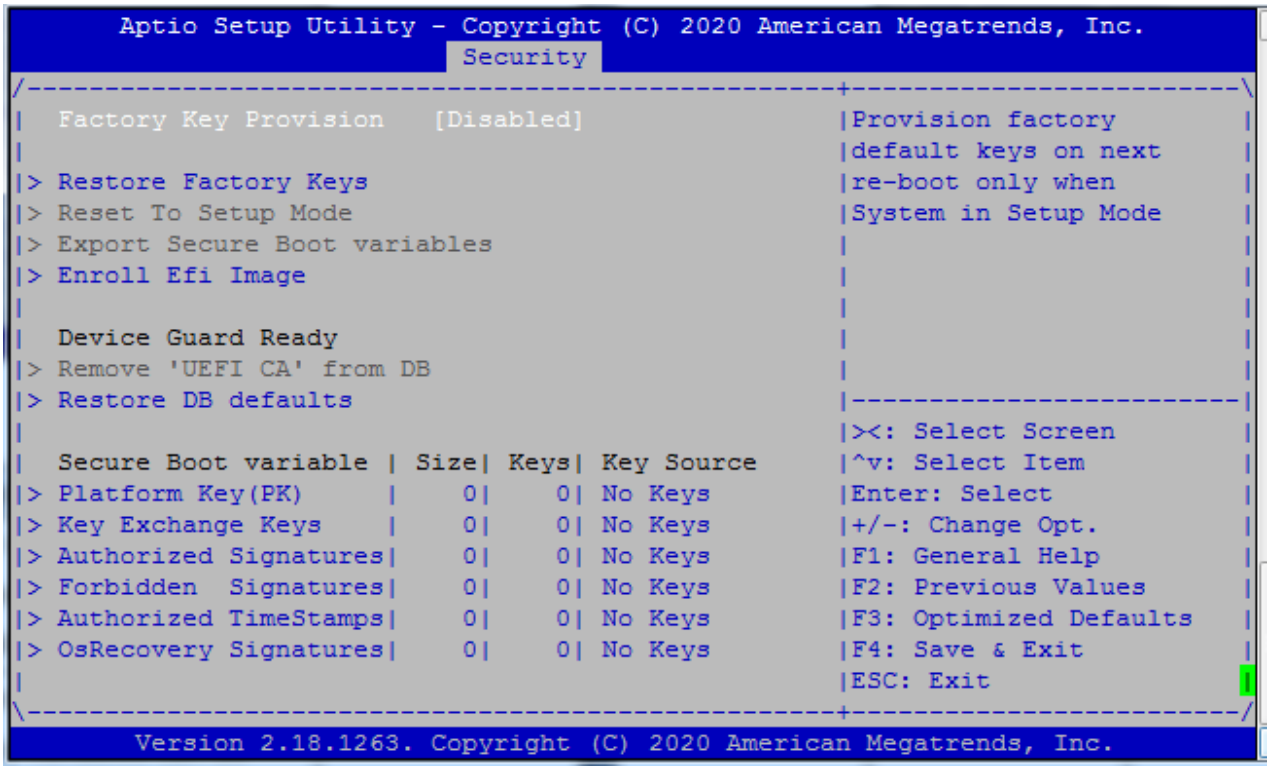
Feature	Description
Administrator Password	If ONLY the Administrator's password is set, it only limits access to Setup and is only asked for when entering Setup.
User Password	If ONLY the User's password is set, it serves as a power-on password and must be entered to boot or enter Setup. In Setup, the User will have Administrator rights.

3.5.1 Secure Boot



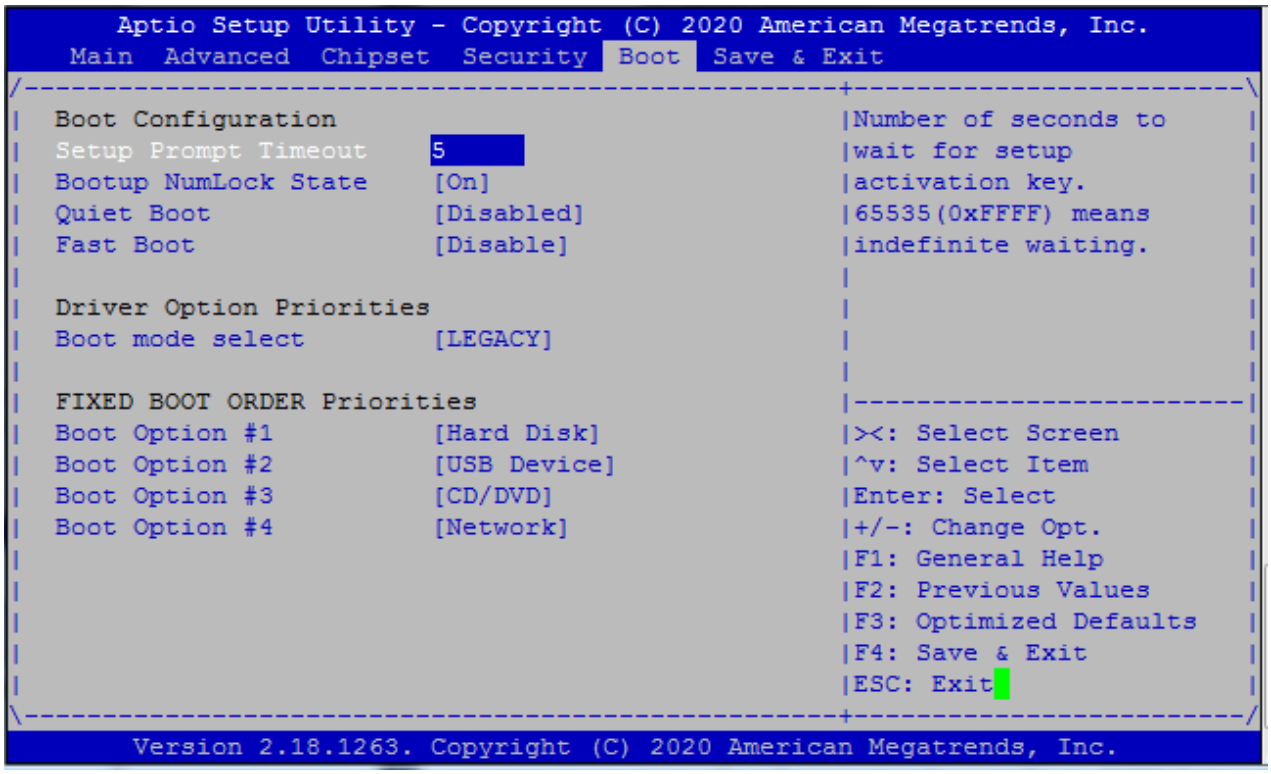
Feature	Options	Description
Secure Boot	Disabled (Default) Enabled	Secure Boot is activated when Platform Key(PK) is enrolled, System mode is User/Deployed, and CSM function is disabled.
Secure Boot Customization	Standard Custom (Default)	Customizable Secure Boot mode: In Custom mode, Secure Boot Policy variables can be configured by a physically present user without full authentication.

3.5.1.1 Key Management



3.6 Boot Menu

Select the Boot menu item from the UEFI setup screen to enter the Boot Setup screen. Users can select any of the items in the left frame of the screen.

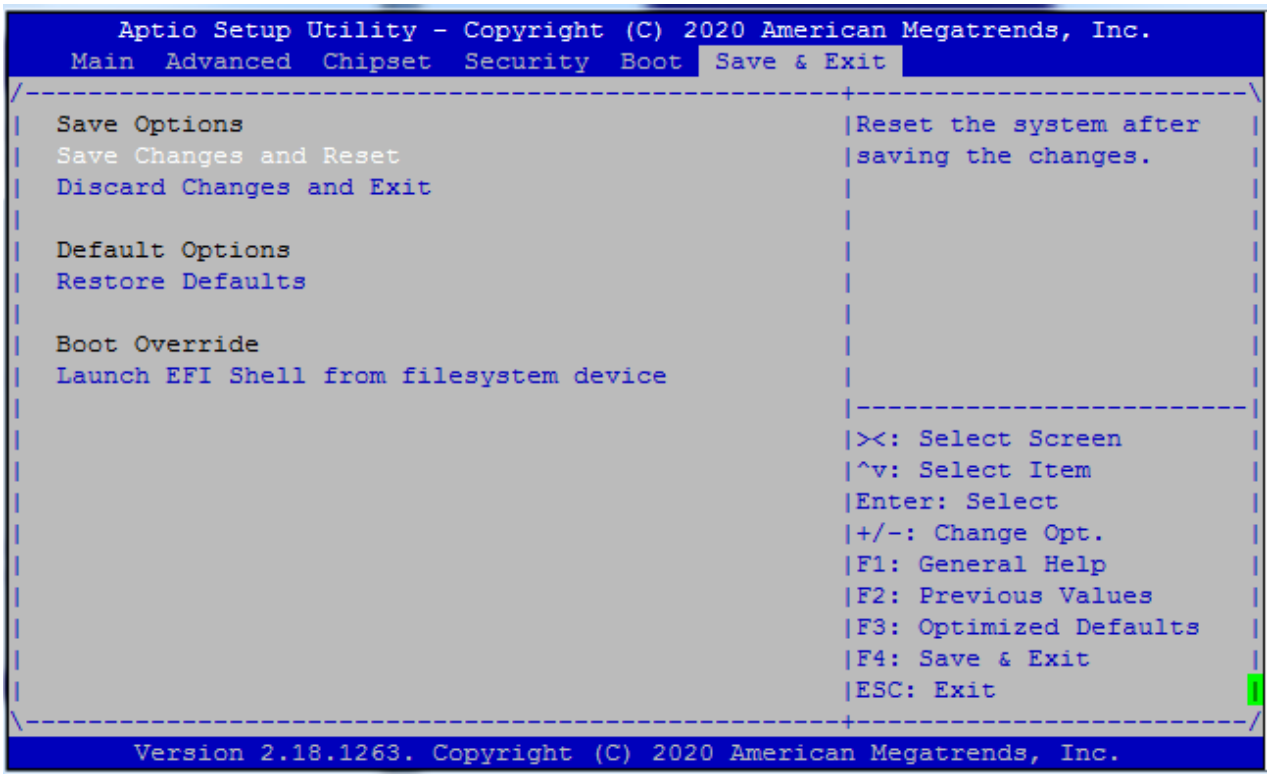


Feature	Options	Description
Setup Prompt Timeout	5 (Default)	The number of seconds to wait for setup activation key. 65535 means indefinite waiting.
Bootup NumLock State	On (Default) Off	Select the keyboard NumLock state
Quiet Boot	Disabled Enabled (Default)	Enable or disables Quiet Boot option.
Fast Boot	Disabled (Default) Enabled	Enable or Disable FastBoot features. Most probes are skipped to reduce time cost during boot.
Boot mode select	Boot mode selectLEGACY UEFI (Default) DUAL	Select boot mode for LEGACY or UEFI.

- Choose boot priority from boot option group.
- Choose specifies boot device priority sequence from available Group device.

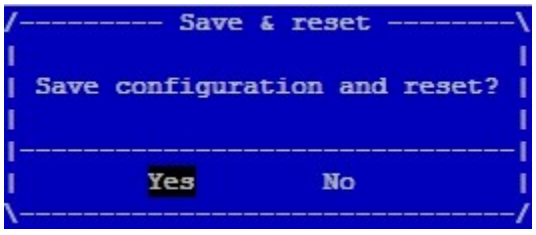
3.7 Save and Exit Menu

Select the Save and Exit menu item from the UEFI setup screen to enter the Save and Exit Setup screen. Users can select any of the items in the left frame of the screen.



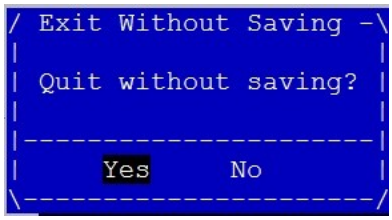
Save Changes and Reset

When Users have completed the system configuration changes, select this option to save the changes and reset from UEFI Setup in order for the new system configuration parameters to take effect. The following window will appear after selecting the "Save Changes and Reset" option is selected. Select "Yes" to Save Changes and reset.



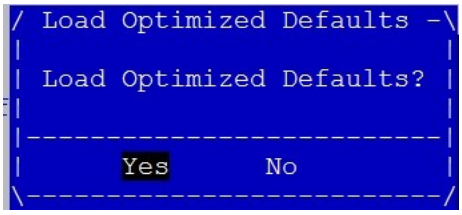
Discard Changes and Exit

Select this option to quit Setup without saving any modifications to the system configuration. The following window will appear after the “Discard Changes and Exit” option is selected. Select “Yes” to Discard changes and Exit Setup.



Restore Defaults

Restore default values for all setup options. Select “Yes” to load Optimized defaults.



PS: The items under Boot Override were not same with image. It should depend on devices connect on system.

Multilin™ G100 Substation Gateway

Appendix A: Miscellaneous

A.1 Revision History

Version	Revision	Date	Change Description
1.00	0	21st May, 2021	Document created.

GE
Grid Solutions

Multilin™ G100

Substation Gateway

G100 Secure Deployment User Guide

Product version: 1.00 and higher

GE publication code: SWM0123 (V1.00 R0)

IEC 61850

REGISTERED ISO 9001 GE MULTILIN

WORLDWIDE 10 YEAR WARRANTY

imagination at work

Copyright Notice

© 2021, General Electric Company. All rights reserved.

Multilin™G100 Substation Gateway - Secure Deployment User Guide.

The information contained in this online publication is the exclusive property of General Electric Company, except as otherwise indicated. You may view, copy and print documents and graphics incorporated in this online publication (the "Documents") subject to the following: (1) the Documents may be used solely for personal, informational, non-commercial purposes; (2) the Documents may not be modified or altered in any way; and (3) General Electric Company withholds permission for making the Documents or any portion thereof accessible via the Internet. Except as expressly provided herein, you may not use, copy, print, display, reproduce, publish, license, post, transmit or distribute the Documents in whole or in part without the prior written permission of General Electric Company.

The information contained in this online publication is proprietary and subject to change without notice. The software described in this online publication is supplied under license and may be used or copied only in accordance with the terms of such license.

Trademark Notices

GE, Multilin™ and are trademarks and service marks of General Electric Company.

* Trademarks of General Electric Company.

IEC is a registered trademark of Commission Electrotechnique Internationale. IEEE is a registered trademark of the Institute of Electrical and Electronics Engineers, Inc. Internet Explorer, Microsoft, and Windows are registered trademarks of Microsoft Corporation. DisplayPort™ are trademarks owned by the Video Electronics Standards Association (VESA®) in the United States and other countries.

Other company or product names mentioned in this document may be trademarks or registered trademarks of their respective companies.

This printed manual is recyclable.

Please return for recycling where facilities exist.

Multilin™ G100 Substation Gateway

Table of contents

1 INTRODUCTION
- 1.1 About the document 1-1
  - 1.1.1 Purpose 1-1
  - 1.1.2 Intended Audience 1-1
  - 1.1.3 Additional Documentation 1-1
- 1.2 Safety symbols and definitions 1-1
- 1.3 Product Support 1-2
  - 1.3.1 Access the GE Grid Solutions web site 1-2
  - 1.3.2 Search GE Grid Solutions Technical Support library 1-2
  - 1.3.3 Contact Technical Support 1-2

2 INITIAL HARDENING SETUP
- 2.1 Default Usernames and Passwords 2-1
- 2.2 Role Based Access Control 2-1
  - 2.2.1 HMI User Roles 2-1
  - 2.2.2 Non-HMI User Roles 2-3
- 2.3 Web HMI Secret Signature 2-3
- 2.4 Firewall 2-3
- 2.5 Disable Unused Serial Ports and USB Ports 2-5
- 2.6 Physical Tamper Detection 2-5

3 SECURE CONFIGURATION OF THE G100
- 3.1 Pass-through Secure Connectivity 3-1
- 3.2 Secure Substation LAN Access 3-3
  - 3.2.1 Secure Connection Relay 3-4
- 3.3 MODBUS TCP/SSH 3-4
- 3.4 Remote Authentication 3-4
  - 3.4.1 TACACS+ 3-5
  - 3.4.2 LDAP 3-5
- 3.5 Remote Logging – Rsyslog Client 3-5
- 3.6 Logs 3-5
  - 3.6.1 Predix Edge Technician Console logs 3-5
  - 3.6.2 G100 System Logs 3-6

4 REMOVING CONFIGURATION AND SENSITIVE DATA

5 CUSTOMER SUPPORT SSH ACCESS

A LIST OF ACRONYMS

B MISCELLANEOUS B.1 Revision History B-1

Multilin™ G100 Substation Gateway

Chapter 1: Introduction

This chapter outlines safety and technical support information.

1.1 About the document

1.1.1 Purpose

This document describes the Initial Hardening setup and Secure Configuration of G100 and provides guidelines on how to enable and configure the various cyber security features on the G100.

1.1.2 Intended Audience

This document is a helpful resource for utility personnel who are responsible for deploying the G100 in a secure manner.

1.1.3 Additional Documentation

For further information about G100 Substation Gateway, refer to the following documents:

MCP Substation Gateway Software Configuration Guide (SWM0101)

Integration of MCP with Open VPN Client (SWM0103)

Enterprise File Synchronization of MCP Sync Manager (SWM0104)

G100 Substation Gateway Quick Start Guide (SWM0116)

Secure Integration of SCADA Third Party Equipment with MCP (SWM0109)

G100 Substation Gateway Instruction Manual (994-0155).

G100 Substation Gateway, HMI Online Help.

1.2 Safety symbols and definitions

Before attempting to install or use the device, review all safety indicators in this document to help prevent injury, equipment damage, or downtime.

1

The following safety and equipment symbols are used in this document.

DANGER **Indicates a hazardous situation which, if not avoided, will result in death or serious injury.**

WARNING **Indicates a hazardous situation which, if not avoided, could result in death or serious injury.**

CAUTION **Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.**

NOTICE Indicates practices not related to personal injury.

1.3 Product Support

If you need help with any aspect of your GE Grid Solutions product, you can:

- Access the GE Grid Solutions Web site
- Search the GE Grid Solutions Technical Support library
- Contact Technical Support

1.3.1 Access the GE Grid Solutions web site

The G100 Web site provides fast access to technical information, such as manuals and knowledge base topics.

Visit us on the Web at: http://www.gegridsolutions.com.

1.3.2 Search GE Grid Solutions Technical Support library

This site serves as a document repository for post-sales requests. To get access to the Technical Support Web site, go to:

Visit us on the Web at: http://sc.ge.com/*SASTechSupport

1.3.3 Contact Technical Support

For help with any aspect of your GE Grid Solutions product, please contact our support team, 24/7, as follows:

Region	E-mail	Telephone
Global Contact Centre	ga.support@ge.com	+44 1785 250070
Central and East Asia and Pacific	ga.supportCEAP@ge.com	+61 414 730 964
India	ga.supportIND@ge.com	+91 44 22648000
Middle East, North Africa and Turkey	ga.supportMENAT@ge.com	+971 42929467
Europe, Russia, CIS and Sub-Saharan Africa	ga.supportERCIS@ge.com	+34 94 4858854
North America	ga.supportNAM@ge.com	+1 877 605 6777
Latin America	ga.supportLAM@ge.com	+55 11 36187308

Multilin™ G100 Substation Gateway

Chapter 2: Initial Hardening Setup

Upon receiving the G100 the following is recommended to be done:

- Change password and/or usernames for all default users.
- Create users with restricted access.
- Change the web HMI secret signature
- Setup firewall
- Physical Security Measures

2.1 Default Usernames and Passwords

Upon receiving the G100, all default usernames and password must be changed. It's crucial to change all the usernames and passwords for the default users as most of them have administrator privileges and allow the user to create new administrator users.

Here is a list of the default users that must be updated:

- Front serial port, command line interface of local HMI and remote SSH access to the device: defadmin/ defadmin
- Front serial port access: root/ geroot
- Predix Edge Technician Console PETC: admin/admin

See **SWM0101 MCP Software Configuration Guide, Chapter 4, MCP Local Configuration Utility (mcpcfg) -> Administrators User Management -> Default Users** and same document **Chapter 8, PETC**.

2.2 Role Based Access Control

2.2.1 HMI User Roles

To control access to the DSAS Online Configuration, G100 Runtime HMI and G100 Local HMI, the following types of access users can be created:

Observer : View only privileges for all runtime screens.

Operator : Substation operator privileges to operate controls, force points and perform maintenance tagging.

Supervisor : Full privileges to access and modify all non-security configuration settings and some security configuration settings, runtime, operation, and system administration screens. This user can add new HMI users.

Administrator : Supervisor-level access to all configuration, runtime, operation, and system screens in the G100 Online/Runtime HMI. In addition, administrator-level users have access to run commands at the G100 command line interface.

Table 1 indicates the system privileges for each access level.

Table 2-1: User Level Permissions

HMI Function	Administrator	Supervisor	Operator	Observer
Access built-in TELNET/SSH client	Yes	Yes	Yes	No
Acknowledge Alarms	Yes	Yes	Yes	No
Clear Logs	Yes	Yes	No	No
Enable/Disable Device	Yes	Yes	Yes	No
Add/Delete Operator Notes	Yes	Yes	Yes	No
Execute Digital/Analog Controls	Yes	Yes	Yes	No
Place/Remove Alarm Inhibit	Yes	Yes	Yes	No
Place/Remove Control Inhibit	Yes	Yes	Yes	No
Place/Remove Local force	Yes	Yes	Yes	No
Place/Remove Scan Inhibit	Yes	Yes	Yes	No
Place/Remove Tags	Yes	Yes	Yes	No
Enable/Disable Unsolicited Responses	Yes	Yes	Yes	No
View Alarms	Yes	Yes	Yes	Yes
View Events	Yes	Yes	Yes	Yes
View I/O Traffic	Yes	Yes	Yes	Yes
View Logs (Except OpenVPN Log)	Yes	Yes	Yes	Yes
View Operator Notes	Yes	Yes	Yes	Yes
View One-Line Diagrams	Yes	Yes	Yes	Yes
View Point Summary & Detail Pages	Yes	Yes	Yes	Yes
View Communication Statistics	Yes	Yes	Yes	Yes
View OpenVPN Log	Yes	No	No	No
Edit/View SCADA Configuration	Yes	Yes	No	No
Edit/View HMI User Configuration	Yes	Yes	No	No
Edit/View Admin User Configuration	Yes	No	No	No
Sync To/Sync From	Yes	Yes	No	No
Commit/Discard Changes in Online Config	Yes	Yes	No	No
Save Configuration	Yes	Yes	No	No
Mount USB Device	Yes	Yes	Yes	No
Edit/View Authentication Mode Configuration	Yes	No	No	No
Extract/View SOE/Alarms/PRF/Datalogger Records	Yes	Yes	Yes	Yes
ARRM: Trigger FileSet Retrieval	Yes	Yes	Yes	No
ARRM: Clear Recording on IED	Yes	Yes	No	No
ARRM: Enable Auto Retrieval	Yes	Yes	No	No
ARRM: Enable Connection Polling	Yes	Yes	No	No

HMI Function	Administrator	Supervisor	Operator	Observer
ARRM: View ARRM Log	Yes	Yes	Yes	Yes
View/Update/Import PKI Information	Yes	Yes	No	No
Generate SSH Key Pair for Rsync	Yes	Yes	No	No
Export VPN Client Configuration	Yes	Yes	No	No
Pair and Rotate Modbus/SSH Keys	Yes	Yes	No	No
Deploy HTTPS certificate and private key	Yes	Yes	No	No

To learn how to add new Supervisor, Operator and Observer users see **SWM0101 MCP Software Configuration Guide** in **Chapter 6** under **Configure System Security -> User Accounts and Authentication** and **Setting up a User Account.**

2.2.2 Non-HMI User Roles

SSHPassThrough : The privilege level SSHPassThrough is not available to access the G100 HMI. Users configured under this privilege level or role are only allowed access for Pass-through.

2.3 Web HMI Secret Signature

The Secret Signature is a Cyber Security feature facilitating a user managed layer of protection on the Session Cookie for the HMI Interface. The G100 creates its own session cookie based on hashing a configurable sentence, called "Secret Signature".

To ensure session cookie uniqueness users should change the Secret Signature.

More on how to configure this, see **SWM0116 G100 Quick Guide** under **Secret Signature** section.

2.4 Firewall

The G100 contains a firewall capable of stateful packet inspection to protect the device from unauthorized access. By default, network interfaces on the G100 drop packets that are determined to be invalidly routed or unsolicited.

The G100 firewall is intended only to protect itself and does not extend protection to other devices on the network. As such, it does not replace the need for a network firewall which offers deep packet inspection and detailed configuration capabilities.

Configure the settings of the firewall through the **Firewall** menu. The Secure Access settings are described in Network interfaces can operate in one of two modes:

Internal : The Internal mode permits traffic from known protocols and should only be enabled on interfaces connected to known devices only. The Internal mode is the default mode for Net 0 and Net 1 and would typically be used when the interface is connected to the substation LAN.

External : The External mode offers a stricter set of rules and is the default mode for all interfaces except Net 1 and Net 2. The External mode would typically be used when the interface is connected to a WAN.

By default, the firewall allows outbound traffic on internal interfaces and blocks all outbound traffic except outbound SSH on external interfaces. If you want the firewall to allow outbound traffic for a protocol on an external interface, you must create a "custom" rule.

By default, the firewall blocks inbound traffic on both internal and external interfaces. The G100 automatically generates rules allowing inbound traffic on internal interfaces for all configured services. If you want the firewall to allow inbound traffic on an external interface, you may modify the associated "generated" rule to allow the traffic on ALL interfaces rather than only the "Internal" interface.

The default firewall rules should be enough for most users. However, the user may create a set of custom rules if desired more granular permissions for the protocols you are accessing.

Additional notes on the G100 firewall:

- When the firewall is active, you cannot perform IP routing between an external and internal interface. The only way to pass through the firewall is by using a secure TLS connection or the proxy.

To change the interface zones (internal/external) go to each interface setup and you have the option to change it there.

The G100 firewall is configured by default to its most secure setting. The user assumes all responsibility for associated security risks if the firewall configuration is manually changed.

It is the user's responsibility to connect Internal zone interfaces to networks that are protected from unauthorized use.

Also, if the firewall is disabled then all the ports that are internal to the G100 will be visible/available to the external scanner tools.

Table 2-2: Service traffic through the firewall

Service Name	Notes	External Mode	Internal Mode
Modbus/TCP Server (Inbound)		Deny	Allow
DNP/UDP Server (Inbound)		Deny	Allow
DNP/TCP Server (Inbound)		Deny	Allow
DNP/TCP Client (Inbound)	Dual Endpoint Enabled	Deny	Allow
DNP/UDP Client (Inbound)			
IEC 60870-5-104 Server (Inbound)		Deny	Allow
Terminal Server (Inbound)	TLS Disabled	Deny	Allow
DCA Pass-Through (Inbound)	TLS Disabled	Deny	Allow
Secure Connection Relay (Inbound)		Allow	Allow
Secure DCA Pass-Through (Inbound)	TLS Enabled	Allow	Allow
Secure Terminal Server (Inbound)	TLS Enabled	Allow	Allow
SNMP Client (Inbound)		Deny	Allow
LogicLinx Executor (Inbound)		Deny	Allow
HTTPS (Inbound)	When enabled in mcpcfg, see note below	Deny	Allow
DHCP Client (Inbound)	When enabled in mcpcfg	Deny	Allow
NTP Client (Inbound)	When enabled in mcpcfg	Deny	Allow
NTP Server (Inbound)	When enabled in mcpcfg	Deny	Allow
SSH/SFTP/SCP (Outbound)	When enabled in mcpcfg for SCP/SFTP.	Allow	Allow
Secure Tunnel -Redundancy (Inbound)	When enabled in mcpcfg	Deny	Allow
Standby Local HMI Redirection to Active (Inbound)	When enabled in mcpcfg	Deny	Allow

Settings GUI(Inbound)		Deny	Allow
Emergency SSH Server (Inbound)		Deny	Allow
Emergency SSH Serve (Outbound)		Allow	Allow
LDAP Client (Outbound)		Allow	Deny
Modbus/TCP Server (Inbound)		Deny	Allow
DNP/UDP Server (Inbound)		Deny	Allow
DNP/TCP Server (Inbound)		Deny	Allow
Note: By default, HTTPS and SSH do not provide strong client authentication since only a password is required to access the system. Therefore, these protocols are not considered secure enough for use over external interfaces. They can be considered secure if you employ a remote authentication server that provides two-factor authentication. In that case, you may opt to modify the firewall rule and allow HTTPS and SSH on external interfaces.			

Additional notes on the G100 firewall:

- In a redundant setup, the same firewall rules above apply to both the active and standby device.
- When the firewall is active, you cannot perform IP routing between an external and internal interface. The only way to pass through the firewall is by using a secure TLS connection or the proxy.
- To configure the firewall and interface zones see **SWM0101 MCP Software Configuration Guide, Chapter 6, Configure System Security -> Firewall Settings.**

2.5 Disable Unused Serial Ports and USB Ports

To decrease attack surface on the G100, it is recommended to disable unused serial and USB ports in the UEFI settings. Unused serial ports can be disabled in the UEFI Settings under Advanced-> Super IO Configuration. All USB ports can be disabled in the UEFI Settings under **Chipset** -> **USB Configuration** -> **xHCI mode**. For detailed information on the UEFI Settings, refer to **G100 UEFI Settings Manual (SWM0122)**.

2.6 Physical Tamper Detection

As part of the physical security measures in the device environment, it is recommended to use tamper resistance/ detection mechanisms such as a seal or a tape.

Applying a security tape is a simple and most cost-effective way to provide evidence that the device was physically tampered with.

For more efficiency the tape should be placed on one screw on each removable panel of the G100. The following two figures show suggested locations to place the seal.

This good practice is part of the IEC-62443-4-2 SL2 requirements (EDR 3.11 – Physical tamper resistance and detection).

NOTE GE does not recommend a particular brand or type of security tape; the choice of tape, as well as other physical security measures should be decided based on the customer risk analysis.

2

Figure 2-1: Front View of G100 with suggested security seal locations

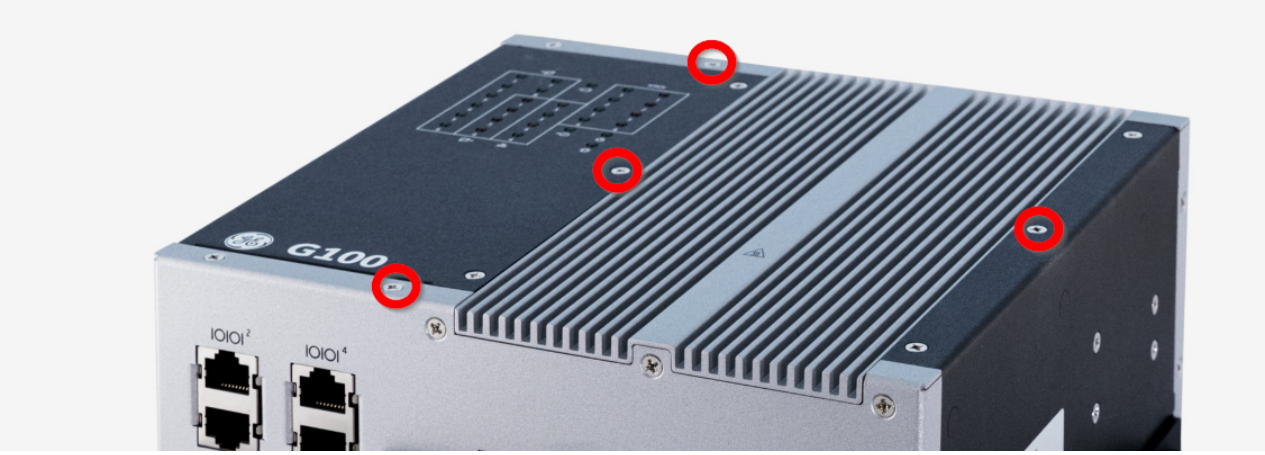


Figure 2-2: Back view of G100 with suggested security seal location

Multilin™ G100 Substation Gateway

Chapter 3: Secure Configuration of the G100

3.1 Pass-through Secure Connectivity

A secure LAN connection can be established through the G100 to connect to a serial server device in the substation. The G100 support different types of secure pass-through connectivity options, available for the following G100 applications:

- IEC 60870-5-103 Multidrop
- Modbus RTU Multidrop
- Generic ASCII
- SEL DCA
- Terminal Server

By default, a username and a password are required to establish the pass-through connection. However, the user can disable this pass-through user authentication in the Settings GUI or the mcpcfg under Configure Authentication/ Pass-Through Authentication or when setting up the terminal server connection. It is strongly recommended to keep the pass-through authentication enabled, unless the TLS connection type is used, see below.

The ssh-passthrough user is created in the HMI under Settings/ Access/ User Management. Admin and root users are created in the Settings GUI or mcpcfg under Configure Authentication. Depending on the pass-through connection type configured, different users have different rules. The table below shows the different type of users and their authentication rules.

Table 3-1: Pass-through User Authentication Rules

Service	User Type						Additional Security Notes
	Admin User Types		HMI User Types			SSHPass Through	
	root	Administrator	Supervisor	Operator	Observer		
Pass-through Connection (Telnet & TLS)	Not Allowed	Allowed	Allowed	Not Allowed	Not Allowed	Not Allowed	Pass-through for remote TCP clients is enabled using **Pass Through Access** in Security parameters under **Configuration** > **Systemwide** and select **Secure Type** under **Configuration** > **Connection to Telnet or TLS**. Pass-through is allowed without Login/Password if its Pass-through Authentication is disabled in G100 Config Tool (**mcpcfg**) > **Configure Authentication**.
Terminal Server Connection (Telnet & TLS)	Not Allowed	Allowed	Allowed	Allowed	Not Allowed	Not Allowed	Terminal Server is allowed without Login/Password, if its application parameter **Password Authentication** is set to No. Terminal Server for remote TCP clients is enabled by selecting "Secure Type" under **Configuration** > **Connection to Telnet or TLS**. Terminal Server application parameter **Minimum Privilege Level** specifies if Operator user is allowed or not.
Pass-through Connection (SSH Secure Tunnel)	Not Allowed	Allowed	Not Allowed	Not Allowed	Not Allowed	Allowed	Pass-through for remote SSH clients is enabled using **Pass Through Access** in Security parameters under **Configuration** > **Systemwide** and select **Secure Type** under **Configuration** > **Connection to SSH Secure Tunnel**. Pass-through for SSH Secure Tunnel is always allowed with Login/ Password,
Terminal Server Connection (SSH Secure Tunnel)	Not Allowed	Allowed	Not Allowed	Not Allowed	Not Allowed	Allowed	Terminal Server for remote TCP clients is enabled by selecting **Secure Type** under Configuration > Connection to SSH Secure Tunnel. Terminal Server for SSH Secure Tunnel is always allowed with Login/ Password. The parameter **Minimum Privilege Level** for SSH Secure Tunnel is always SSHPassThrough only.

More about how to configure the pass-through connections, see **SWM0101 MCP Software Configuration Guide** under **Chapter 6, DS Agile Studio Configuration -> Miscellaneous Utilities -> Pass-Through Connections.**

The user can use third party software to securely access terminal server or pass-through connection, more about how to configure a secure connection with **Tactical Software Serial IP** is found in **SWM0109 Secure Integration of SCADA Third Party Equipment with MCP**, under **Chapter 6. Configuring a Secure Connection with Tactical Software Serial IP.**

For each client application the secure pass-through is configured using the G100 configuration tool, under Connection tab/ Secure Type. The following options are available:

3.1.0.1 SSH Security Tunnel

The G100 supports SSH tunnel connection for pass-through and terminal server connectivity. Once configured, an SSH client configuration tool, e.g. Secure Terminal Emulator from DS Agile Studio, is used to connect to a device in the substation, The SSH port used connect is automatically assigned port number 8000 + the serial port number the G100 client is using to communicate to the device in the substation. For example, if the client is configured to use serial port 1, the pass-through connection port is 8001.

More about how to configure this type of pass-through connection, see **SWM0101 MCP Software Configuration Guide** under **Chapter 6, DS Agile Studio Configuration -> Miscellaneous Utilities -> SSH Secure Tunnel Pass-Through Connections.**

3.1.0.2 TLS

The G100 supports Transport Layer Security (TLS) cryptographic protocol versions 1.0, 1.1, and 1.2. It is recommended to choose version 1.2, which is set by default, as it has the latest and strongest ciphers. Using TLS option requires to setup certificate-based mutual authentication, refer to **SWM0109 Secure Integration of SCADA Third Party Equipment with MCP** on how to setup the certificates.

3.1.0.3 Telnet

The G100 supports pass-through and terminal server access to the devices from PC-based configuration tools and, if necessary, COM port redirection software. These connections are accessible through a TCP port on the G100.

It is not recommended to use telnet pass-through and terminal server as it's less secure than SSH Secure Channel and TLS options.

NOTE

The following services are considered unsecure:

- IEC 60870-5-103 Multi-drop (Passthrough-Telnet)
- Modbus Multi-drop (Passthrough-Telnet)
- Generic ASCII (Passthrough-Telnet)
- SEL Binary with G100 as Master (Passthrough-Telnet)
- Terminal Server

It is strongly recommended to employ TLS tunnels or SSH Secure Tunnels to protect these services.

3.1.0.4 Disabled

The default pass-through and terminal server secure type is Disabled.

3.2 Secure Substation LAN Access

The user can setup a secure channel between a client device and the G100 for accessing a protected service in the substation. The secure channel is implemented using a TLS (Transport Layer Security) connection and certificate-based mutual authentication. A client device could be a PC with Tactical Software Serial/IP or Stunnel, SCADA master that supports TLS and mutual authentication using certificates.

Certificates are issued by a Certification Authority (CA). The G100 does not come with a CA so you must make use of an existing CA or create your own.

3.2.1 Secure Connection Relay

A secure connection relay is used to apply security features to any existing ethernet connection. A secure TLS connection is established to connect an external client device to the G100 to access a protected service in the substation.

A client device could be a PC with Tactical Software Serial/IP or Stunnel, SCADA master that supports TLS and mutual authentication using certificates.

A master device could be a DNP3 master, IEC60870-5-104 master, or Modbus TCP master on the G100 or any other device connected to the G100 in the substation.

It is strongly recommended to setup a secure connection relay for every LAN connection on the G100.

NOTE

It is strongly recommended that the user employ TLS tunnels to protect the following services:

- DNP3 Master
- IEC 60870-5-104 Master Station
- Modbus TCP Master

The user assumes all responsibility for associated security risks when enabling unsecured services onto an unprotected network.

3.2.1.1 Secure Tunnel for redundancy setup (OpenVPN)

A VPN (Virtual Private Network) channel is available between the G100 and an OpenVPN client running on a remote computer running Windows® Server 2012 R2 or Windows 7; this VPN channel allows access to one or more protected services in the substation. The VPN channel is implemented using OpenVPN, which uses a custom protocol based on TLS (Transport Layer Security), and certificate-based mutual authentication.

For details on how to configure VPN server see **SWM0101 MCP Software Configuration Guide** under **Chapter 6, DS Agile Studio Configuration -> Communications -> Configure Network Communications -> VPN Server** and **SWM0103 Integration of MCP with OpenVPN Client** document.

3.3 MODBUS TCP/SSH

The G100 supports Modbus TCP/SSH protocol to establish a secure SSH connection with the UR7.6 IEDs that support SSHv2 protocol through Machine-to-Machine (M2M) access role. The G100 provides an option in the IED communication summary GUI.

The G100 provides an option for rotating the G100's public key into the UR7.6 on an on-demand basis.

Only administrator user can pair and rotate keys.

For further information on how to configure Modbus TCP/SSH client, go to **SWM0101 MCP Software Configuration Guide** under **Chapter 7, MCP Pseudo Points -> Modbus Serial with MCP as Slave application -> Modbus TCP/SSH Client – SSH Tunnel Interface.**

3.4 Remote Authentication

It is recommended to setup centralized remote authentication to manage users and their authentication remotely and securely.

At least one emergency user must be created when remote authentication is configured. Only emergency user can access the G100 in case the remote authentication server is down. The emergency user is added in the Settings GUI or sudo mcpcfg under Configure Authentication / Emergency Group Users / Add User.

The following remote authentication protocols are supported in the G100:

- TACACS+
- LDAP

3.4.1 TACACS+

Cisco TACACS+ (Terminal Access Controller Access-Control System +) remote authentication is supported by the G100. To configure TACACS+ see **SWM0115 G100 Software Configuration Guide** under **Chapter 6, DS Agile Studio Configuration -> User Accounts and Authentication -> Remote Authentication.**

3.4.2 LDAP

LDAP (Lightweight Directory Access Protocol) remote authentication is supported by the G100. To configure LDAP, see **SWM0111/12/13 Configuring the MCP for Centralized LDAP Authentication using Windows AD/Open LDAP Server / 389 Directory Server** documents and **SWM0101 MCP Software Configuration Guide** under **Chapter 6, DS Agile Studio Configuration -> Configure System Security -> User Accounts and Authentication -> Remote Authentication.**

3.5 Remote Logging – Rsyslog Client

The G100 has a Rsyslog client that accepts system logs from any IED or substation equipment that support the syslog remote logging feature. G100 supports both UDP- and TCP- based connections, both TCP and UDP ports can be simultaneously open to listen on internal interface zones. The received logs are saved in a default file under a set path in the G100.

By default, the G100 saves all incoming logs being pushed from any of the IEDs connected to the network and configured with the G100 IP address and syslog port).

The G100 also allows you to configure the:

- **Subnets-based binding filter**: By selecting a subnet from the displayed list or by specifying a subnet from the Custom Filters options, the G100 starts logging messages from IEDs whose IP addresses fall under the subnet's range)
- **Host-based binding filter**: By Specifying a Host's IP address, the G100 starts logging messages being pushed from the specified host.
- Configuring Subnet address and Host IP address is beneficial when:
- An IED or substation equipment's IP address is not under any of the subnets available in the G100.
- The G100 is in redundant mode and the Standby's Ethernet Interface (Alias IP/Gateways etc...) are configured to be in different subnets from that of the Active's Ethernet Interface.

To configure Rsyslog, see **SWM0101 MCP Software Configuration guide** under **Chapter 4, MCP Local Configuration Utility (mcpcfg) -> Other Services/Settings -> Configure Rsyslog service** or **Chapter 5, MCP Settings (GUI) -> MCP Settings Workflows -> Configure Secure Access -> Configure Rsyslog service.**

3.6 Logs

3.6.1 Predix Edge Technician Console logs

Predix Edge Technician Console (PETC) implements full journal logging to allow the user to query and view logs in the console.

Logging is received from a variety of sources, such as kernel log messages, simple and structured log messages, and audit records. The logs can be filtered to be viewed by date and time, as well as pre-set units of time, for example, the last six hours, or the last five minutes. You can also filter logs by component and process or view only kernel messages. Additional options for viewing logs include by message priority, for example, Error or Debug.

For more on viewing these logs see **SWM0101 MCP Software Configuration guide** under **Chapter 8, Edge Manager and PETC.**

3.6.2 G100 System Logs

The following logs are saved in the HMI view under Logs:

- Control Log
- Diagnostic Log
- System Event Log
- User Activity Log
- Analog report Log
- VPN Server Log (available only to administrator user)

Only administrator user can clear the logs in the Settings GUI or sudo mcpcfg.

For more on these logs see **SWM0101 MCP Software Configuration guide under Chapter 3, MCP HMI Runtime -> View Data -> Logs.**

Multilin™ G100 Substation Gateway

Chapter 4: Removing Configuration and Sensitive Data

For removal of configuration and sensitive data, follow the procedure in **994-0155 G100 Instruction Manual,** under **Chapter 6, Removing the G100 from service -> Remove configuration data and sensitive information from the G100**.

Multilin™ G100 Substation Gateway

Chapter 5: Customer Support SSH Access

You may be asked to access the Predix EdgeOS host shell of the G100 for purposes of collecting customer support data while troubleshooting an issue. The access is granted for this shell through the Signed Keys option of the left navigation pane in PETC. Further documentation on how to generate, upload and revoke a signed SSH key will be provided by the GE customer support specialist when required to troubleshoot an issue.

Multilin™ G100 Substation Gateway

Appendix A: List of Acronyms

Table A-1: List of Acronyms

Abbreviation	Description
CA	Certification Authority
CN	Common Name
CRL	Certificate Revocation List
DCA	Data Collection Application
DPA	Data Presentation Application
DTA	Data Translation Application
ESNET	EnterpriseServer.NET
FQDN	Full Qualify Distinguished Name
HMAC	Hash-based Message Authentication Code
HMI	Human Machine Interface
IED	Intelligent Electronic Device
JVM	Java Virtual Machine
LAN	Local Area Network
OU	Organizational Unit
PEM	Privacy Enhanced Mail
PKCS	Public Key Cryptography
PKI	Public Key Infrastructure
PRF	Protective Relay Fault
RTDB	Real Time Data Base
RTU	Remote Terminal Unit
SCR	Secure Connection Relay
SDD	Software Design Document
SOE	Sequence of Event
SPT	Secure Pass-Through
SSDD	Software Subsystem Design Document
ST	Secure Terminal Server
TLS	Transport Layer Security
WAN	Wide Area Network

Multilin™ G100 Substation Gateway

Appendix B: Miscellaneous

B.1 Revision History

Version	Revision	Date	Change Description
1.00	0	20th May, 2021	Document created.

MCP Firmware Upgrade and Restore to Defaults Workflows

Technical Note

Overview

The firmware of the MCP can be upgraded to provide the latest functionality and improvements. The same process can be used to recover a MCP unit for which all administrator credentials have been lost and it cannot be accessed anymore, resulting into a factory default device.

NOTICE **This document applies to the MCP family (G100/G500) unless otherwise indicated.**
Screen captures may show G500 in some areas, however the workflow applies to products in the MCP family (G100/G500).

Prerequisites

For this workflow you require:

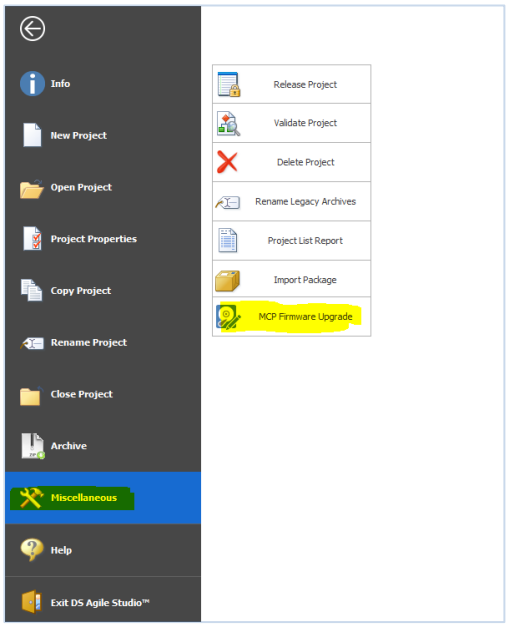
1. A G500 or G100 device with:
    - Keyboard, Mouse and Monitor (or)
        - For G500 only: Type A to B USB cable connecting G500 front Type B USB port to laptop/PC.
        - For G100 only: Serial null modem cable and a serial port on laptop/PC. Also, for the G100 only, console port redirection must be enabled for COM4. This is the default setting and can be changed from the G100 UEFI. Refer to "SWM0122 Configuring UEFI Settings on G100 User Guide" for details on how to view or edit the console port redirection for COM4.
2. A portable USB Flash Drive with storage size **between 8GB and 32GB** inclusively.
    - When MCP backups are taken on the USB drive, and to ensure strong protection of the backup data at rest, a hardware encrypted USB drive is recommended to be used.
      NOTE: GE tested the following hardware protected USB model: Apricorn Aegis 3NX.
    - Please note that hardware encrypted USB drives will have to be placed into a temporary "open" mode while they are connected to the MCP USB port, in order to preserve access across MCP reboot operations. The exact method to do this depends on each hardware encrypted USB, please refer to their associated manuals (e.g. Lock-Override Mode of Apricorn Aegis 3NX USB Drive).
    - When a hardware encrypted USB drive is connected in "open" state to the MCP, to initiate process, do not use a cold re-start of the MCP, because this will remove power from the USB which will likely result in a closed USB drive. Instead, use soft reboot commands for the MCP, from the console, after activating the human presence feature if applicable."
    - The MCP does not support software encrypted USB drives.

3. A Windows 7 or 10 PC loaded with the following:
   - **DS Agile Studio** v2.1 or higher for G500
   - **DS Agile Studio** v2.3 or higher for G100
4. If monitor is not available, for the G500, the G500 front serial USB driver (CDM21228_Setup.exe which can be found on the G500 Documentation CD (Part no. 588-0100) in the folder "G500 Front Serial USB Driver").

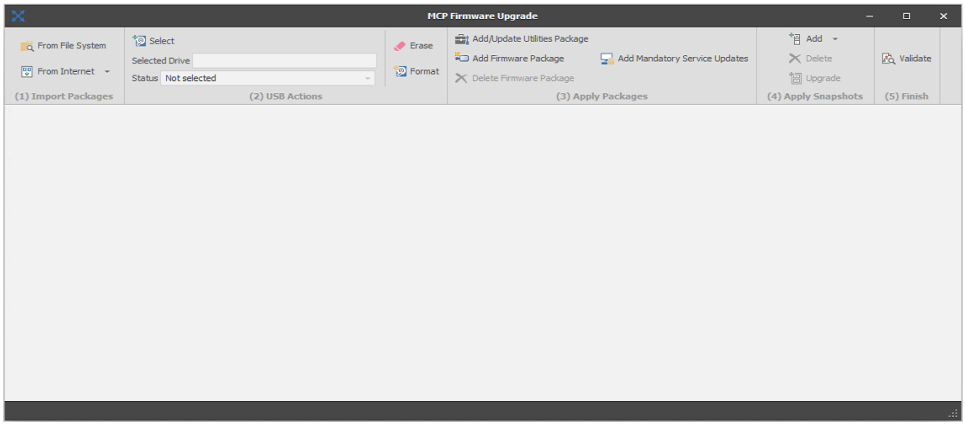
Section 1: Using DSAS "MCP Firmware Upgrade" tool to create the USB disk image

Use the DSAS "MCP Firmware Upgrade" tool to create the USB disk image

1. Insert the USB drive into your PC and Start DS Agile Studio.
2. Launch MCP Firmware Upgrade tool.
   - From the **File** menu, select **Miscellaneous → MCP Firmware Upgrade**



   - MCP Firmware Upgrade tool window appears.



3. The ribbon shows from left to right the steps in the order they should be performed in this workflow.
4. Import the desired MCP firmware, MCP utilities and MCP Service Update Packages.

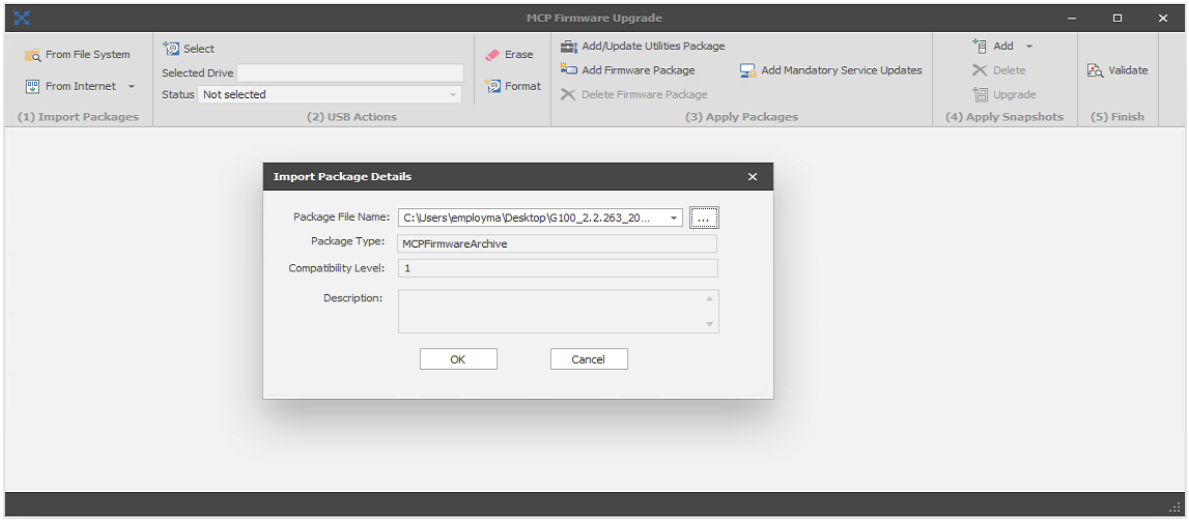
At least one MCP Firmware package and one MCP Utilities package is required to be imported. MCP Service Update packages can be optionally imported.

If the packages are already available in the computer, or on a shared drive, for example they have been downloaded and saved previously, you can choose to import them **From File System** otherwise you will need to download them **From Internet.**

If this PC has the packages already imported into this tool, you may skip this process.

To Import the packages from file system:

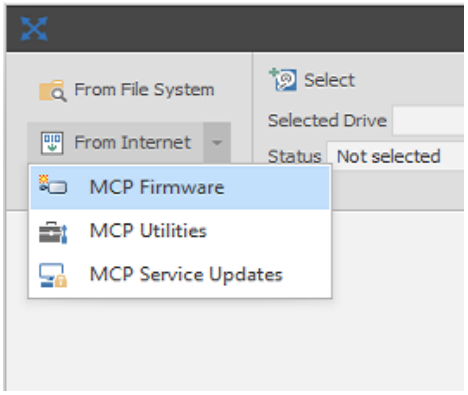
- Click **From File System** to open Import Package Details dialog.
- Click **...** to browse the file system to select the package file.



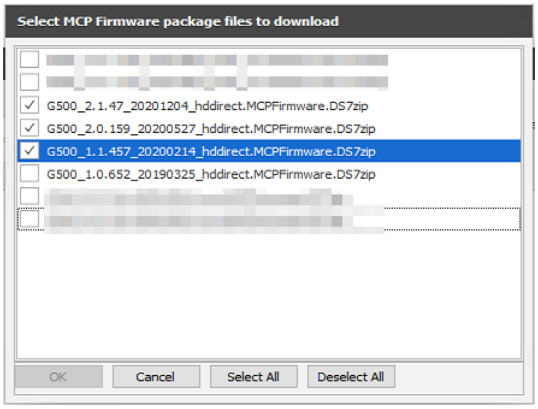
- Click **OK** to import the selected package.
- Repeat the same process to import more Packages.

To Import the packages from Internet: (Internet Access is required)

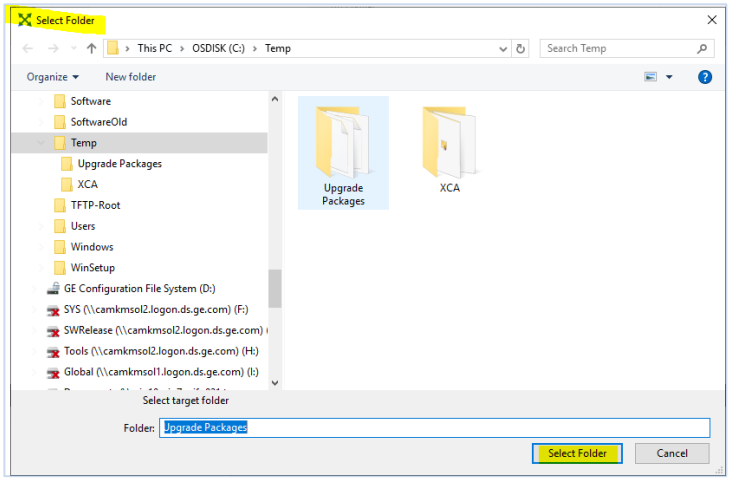
- Click the drop-down list of **From Internet.**
- Select **MCP Firmware.**



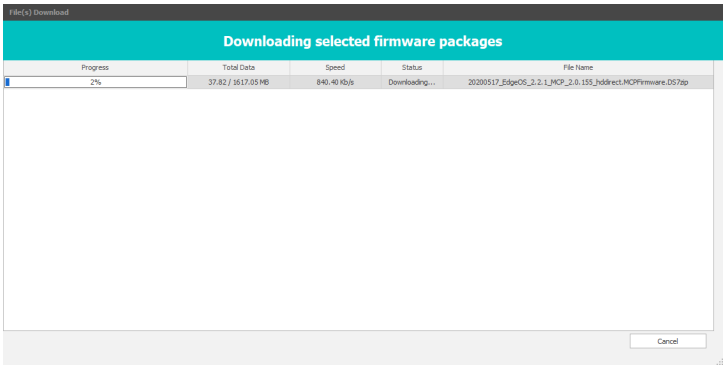
- The list of available MCP Firmware package files will appear.



- Select the desired Firmware Packages that you want to upgrade to and then click **OK.**
- Select a folder to store the packages that is about to download.



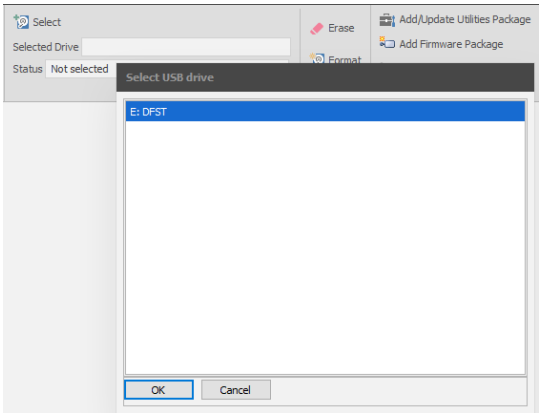
- Once a folder is selected, the downloading will begin.



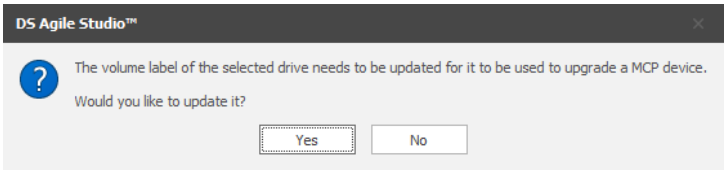
- The package file(s) will be imported after it is downloaded.
- Repeat the same procedure to download and import an MCP Utilities package.
- Repeat the same procedure to download and import one or more MCP Service Update packages.
- Multiple MCP Firmware, MCP Utilities and MCP Service Update packages can be imported.

5. Select the target USB Drive.

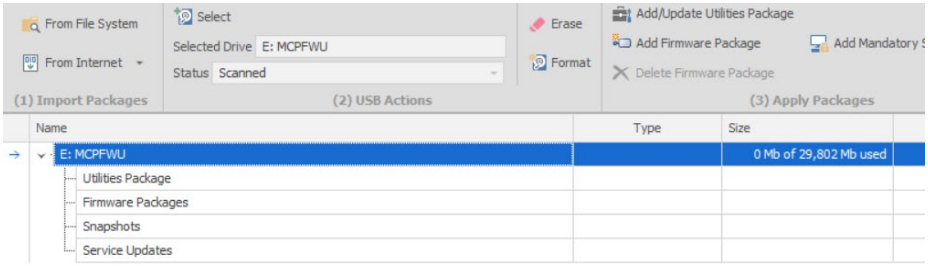
- Select the USB drive that you want to use to perform the firmware upgrade and click OK.



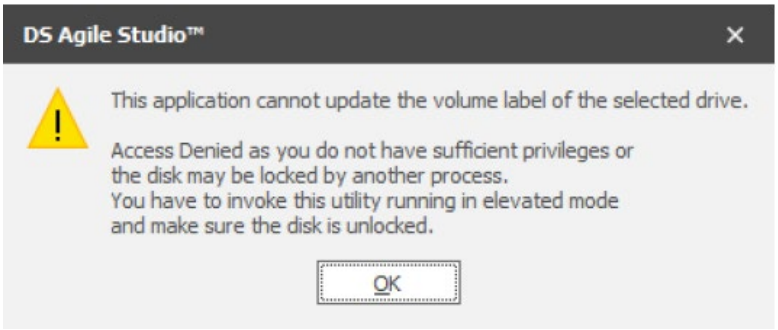
- If the volume label of the USB drive needs to be updated, click **Yes** to procced further or click **No** to cancel the process.



- Once completed, the volume label will be changed to **MCPFWU** or **G500FWU** (for DS Agile Studio v2.1 and v2.2) and the status is **Scanned**.



Note: If you are prompted with the following warning message, it basically means that you have enhanced security policy in place on your Windows system.



The suggested solutions are:

Option 1:

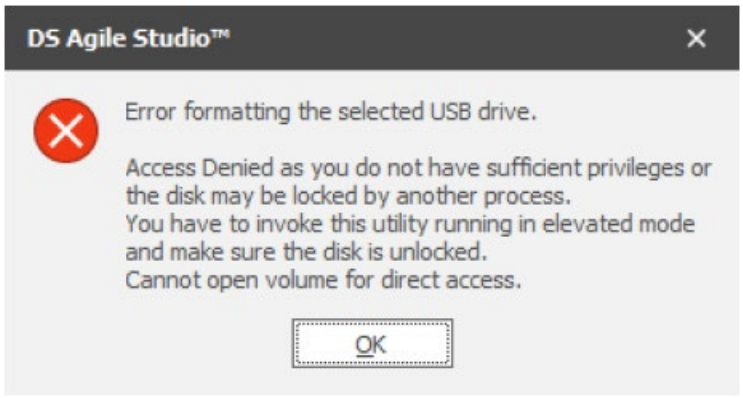
1) Close **MCP Firmware Upgrade** tool and **DS Agile Studio.**
2) Re-launch **DS Agile Studio** in elevated mode, that is, Right click the icon and choose **Run as Administrator**.
3) Re-do the above USB actions.

Option 2:

1) Close **MCP Firmware Upgrade** tool.
2) Open **File Explorer** from Windows.
3) Right click the USB drive to rename it to **MCPFWU** or **G500FWU** for DS Agile Studio v2.1 and v2.2 only**.** Click **Continue** when you are being prompted with security warning.

- Click **Erase** to erase the USB drive as needed.
- Click **Format** to format the USB drive as needed.

Note: If you are prompted with the following warning message, it basically means that you have enhanced security policy in place on your Windows system.



The suggested solutions are similar as those described above when updating the volume label.

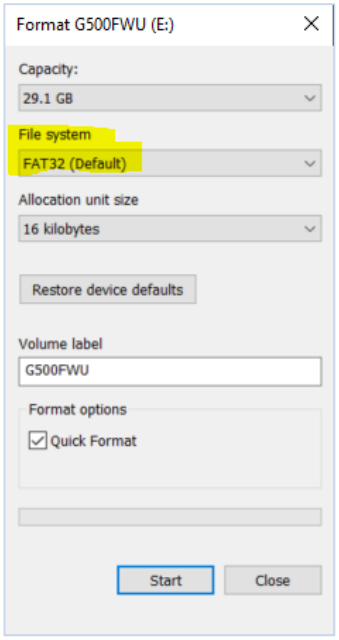
Option 1:

1) Close **MCP Firmware Upgrade** tool and **DS Agile Studio.**
2) Re-launch **DS Agile Studio** in elevated mode, that is, Right click the icon and choose **Run as Administrator.**
3) Select the USB drive and then click **Format**.

Option 2:

1) Close **MCP Firmware Upgrade** tool.
2) Open **File Explorer** from Windows.
3) Right click the USB drive to choose **Format.** Click **Continue** when You are being prompted with security warning.

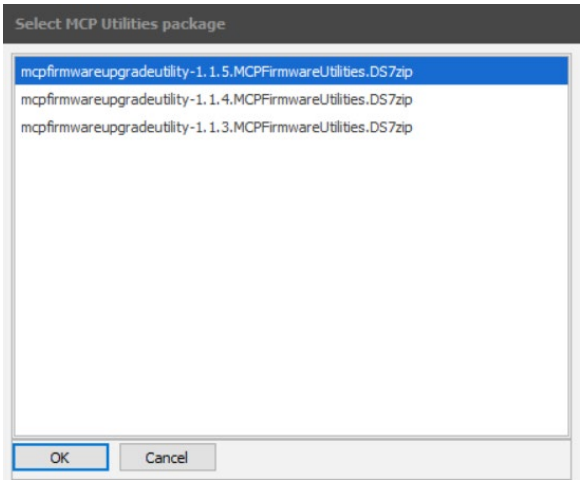
4) Ensure **FAT32** is selected for the File system.



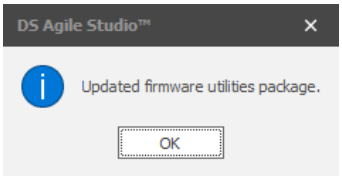
6. Add MCP firmware, MCP utilities and MCP Service Update packages.

Add Utilities Package

- Only one MCP Utilities package can be added to the USB drive at a time. The latest version of the MCP Utilities package is compatible with all MCP firmware versions.
- Click **Add/Update Utilities Package** to select the desired MCP Utilities package from the list and click **OK**.

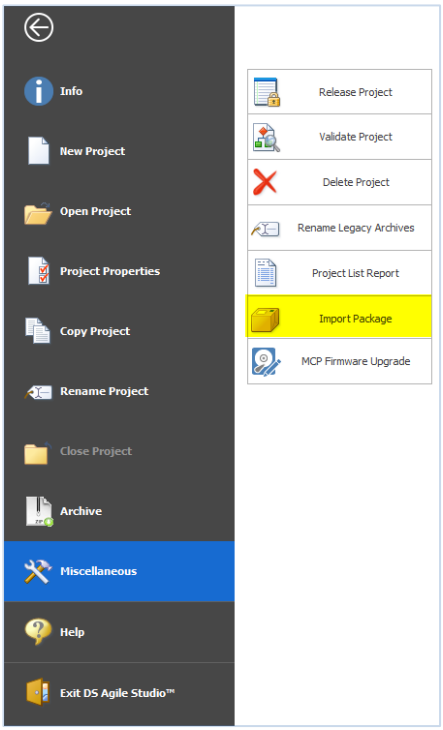


- It starts verifying and extracting the package and then apply to the USB drive with below message once completed.

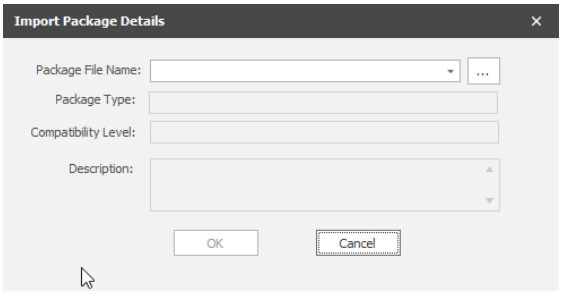


Update Platform Package

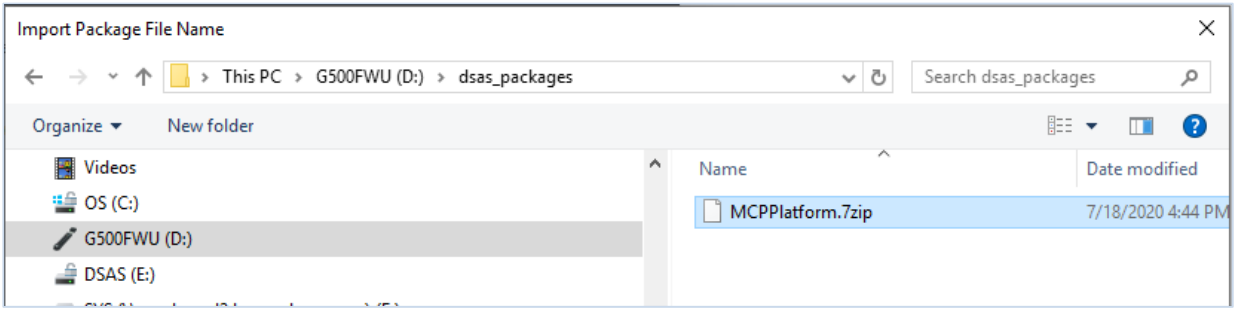
- From the **File** menu, select **Miscellaneous** -> **Import Package**



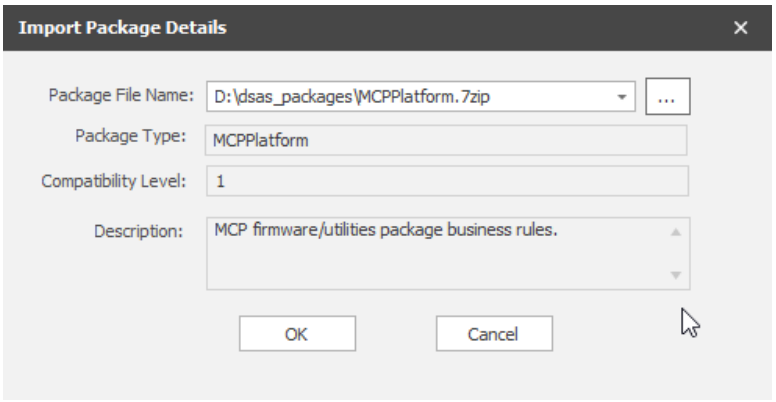
- The Import Package Details window appears:



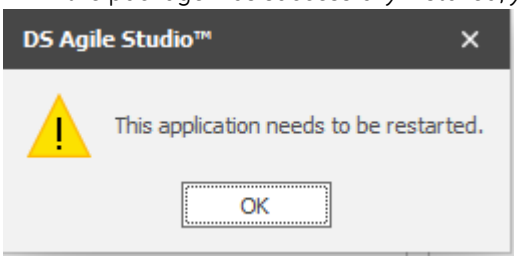
- Click the ellipsis after the Package File Name box and browse to the folder named **dsas_packages** on the USB drive. Then, select the **MCPPlatform.7zip** file:



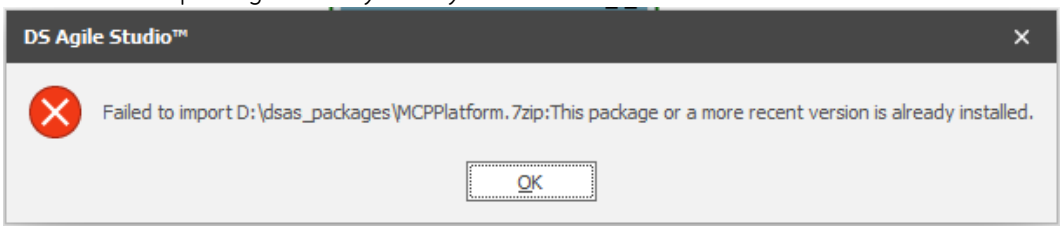
- The Import Package Details dialog shows the MCPPlatform Package selected:



- Click OK.
- If the package was successfully installed, you will get the following message:



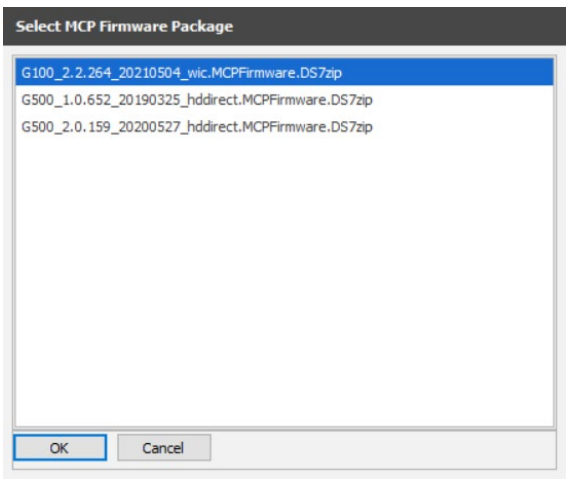
- If the package is already installed, you will get the following message. However, this means you already have the correct package and so you may continue.



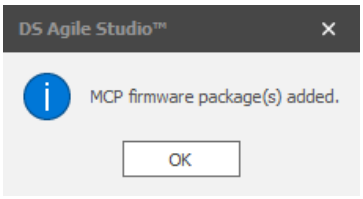
- In either case, Click OK.

Add Firmware Packages

- Multiple MCP Firmware package can be added to the USB drive.
- Click **Add Firmware Package** to select the desired firmware package from the list and click **OK**.

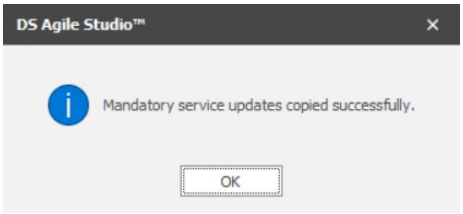


- It starts verifying and extracting the package and then apply to the USB drive with below message once completed. This may take a long time.



Add Service Update Packages

- Multiple MCP Firmware package can be added to the USB drive.
- Click **Add Mandatory Service Updates** to add mandatory service updates associated with the firmware packages on the USB drive and click **OK**.
- It starts verifying and extracting the package and then apply to the USB drive with below message once completed.



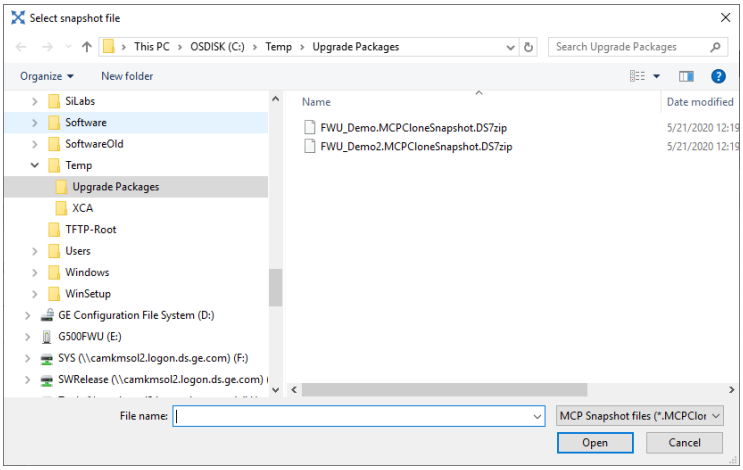
7. Add the MCP Clone Snapshots as needed.

   Multiple MCP Clone Snapshots can be added to the USB drive.

   If the MCP Clone Snapshots are already available in the computer, for example, they have been saved from the device previously, you can add them **From File System** otherwise you will need to add it **From Device** directly.

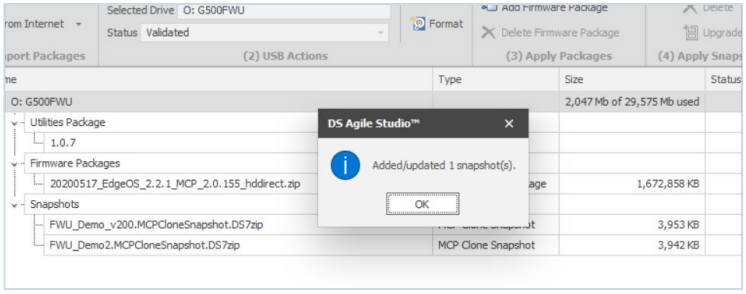
To Add the snapshot from file system:

- Click **Add → From File System** to open Select snapshot file dialog:



- Browse the file system to select the MCP Clone Snapshot file and click **Open**. Multiple file selection under the same folder is also supported.

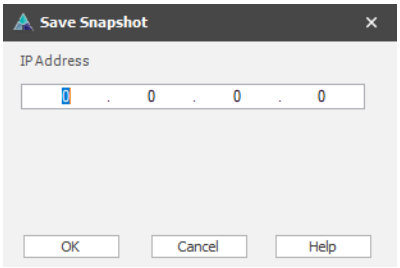
- The snapshot is then being added to the USB drive with below message once completed.



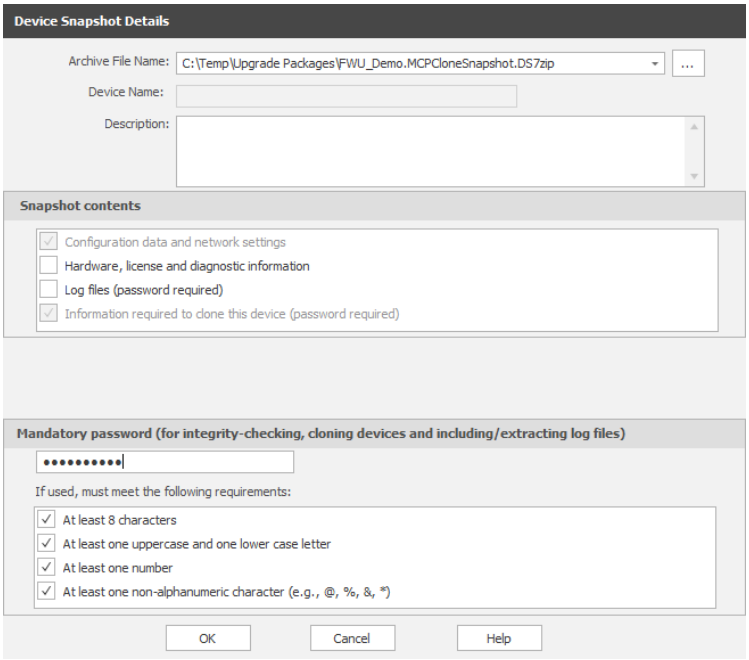
- Repeat the same procedure to add more snapshots to the USB drive as needed.

To Add the snapshot from Device:

- This is very useful if you are already connected to the device to be upgraded and you wish to take the clone snapshot at exact same moment.
- Click **Add → From Device** to open Save Snapshot dialog.

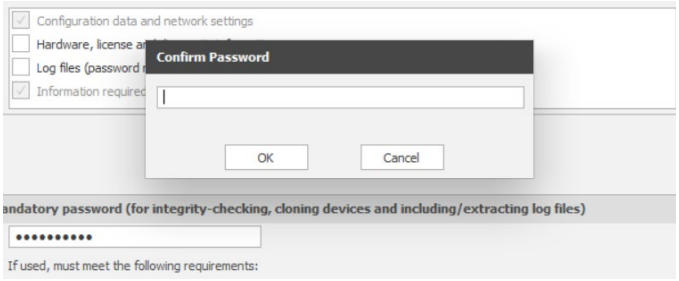


- Enter the IP Address of the MCP and click OK.
- The Device Snapshot Details window appears.

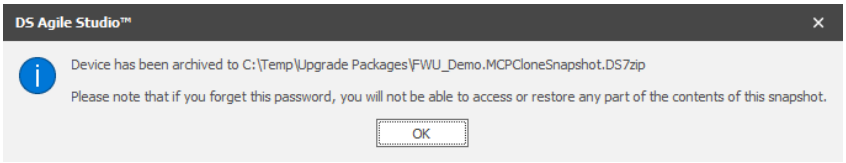


- Specify the user-defined Archive File Name and leave the default checkbox selections.

- Enter Mandatory password and ensure this password is available while performing the snapshot restoration after the firmware upgrade.
- Click OK and then the Confirm Password window appears.



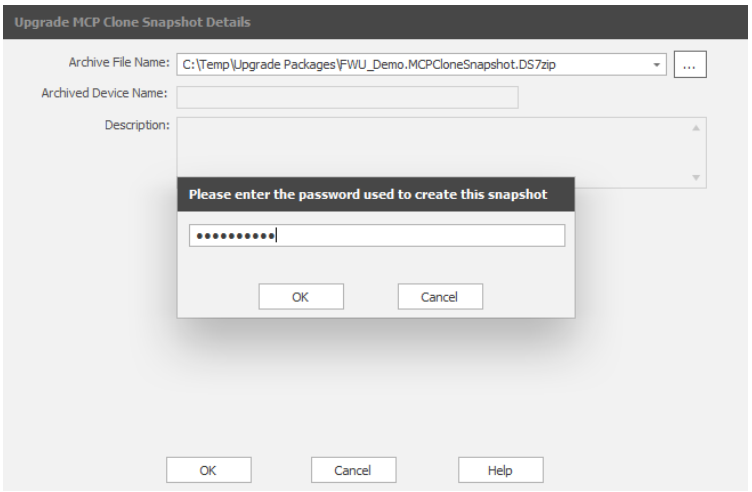
- Enter password again and click OK and then a Login popup appears.
- Enter User Name and Password for the physical MCP device and click Login as an administrator.
- The MCP Clone Snapshot file from the MCP device is then saved to the selected location and added the USB drive as well.



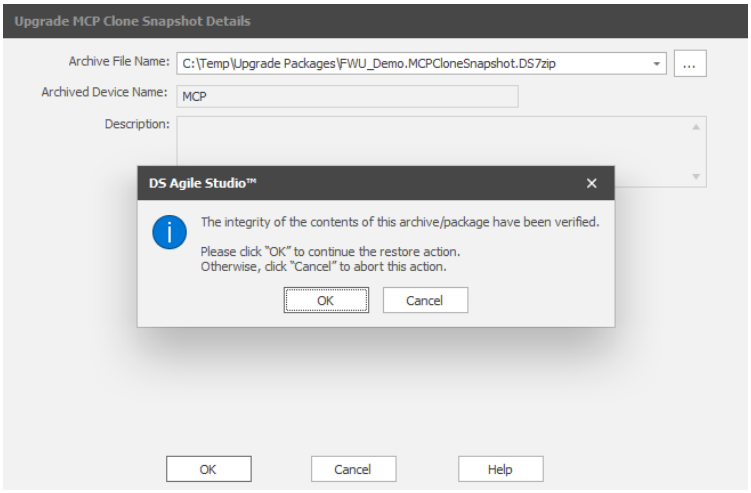
8. Upgrade the snapshots as needed.

   This step is intended to convert the configuration settings to the format required by the new MCP firmware version.

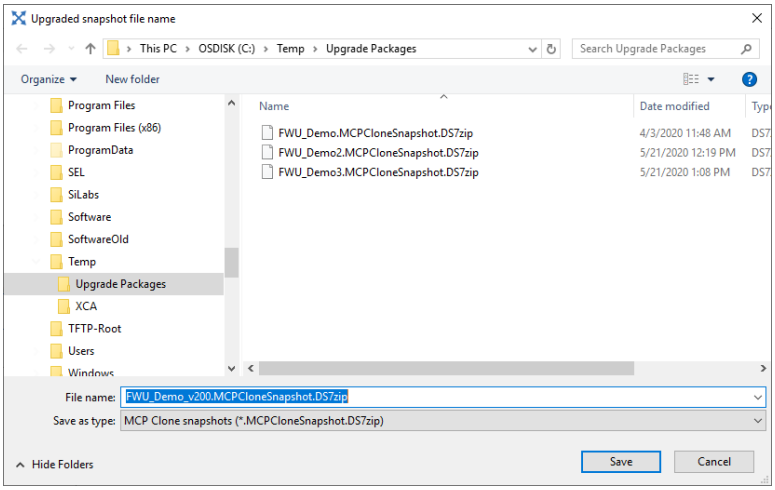
   - Select the archived MCP Clone snapshot in the main tool screen area and click **Upgrade.**
   - Enter the password when prompted for and click **OK**.



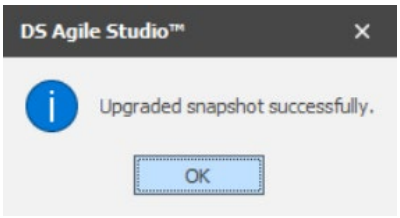
- After processing archive is done, click **OK** to go further. Then click **OK** again when prompted to continue.



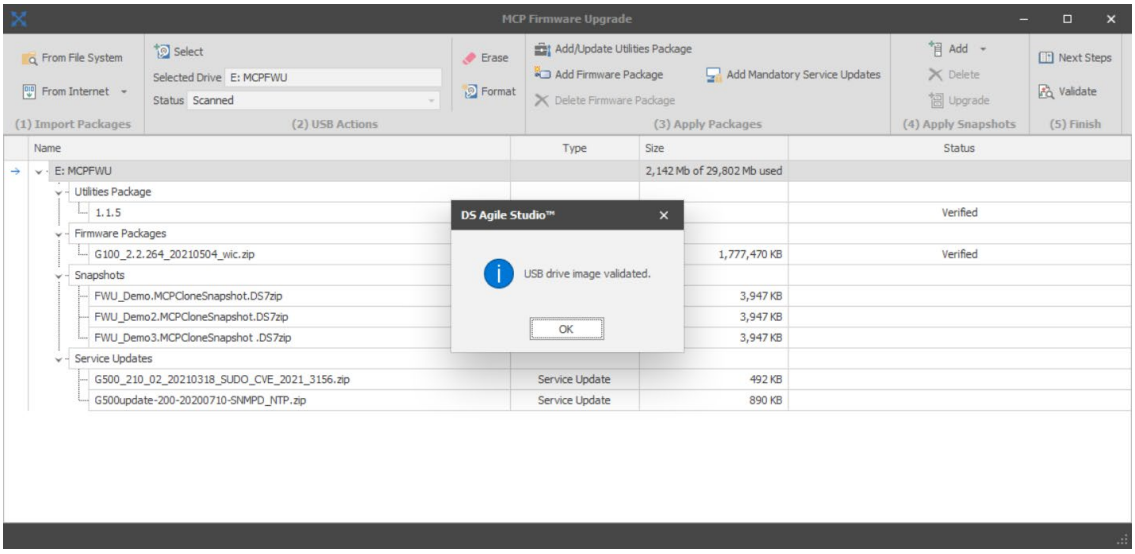
- Specify the file name if you want to, otherwise leave the name as what it suggests (it appends _Vxx). Then click **Save**.



- A success message will display once the upgrade is done.



9. To conclude, click **Validate** to validate the prepared USB drive to make sure it is ready to be used for firmware upgrade. Once this process is complete, the status of the integrity of the utility package as well as any firmware packages will be displayed.



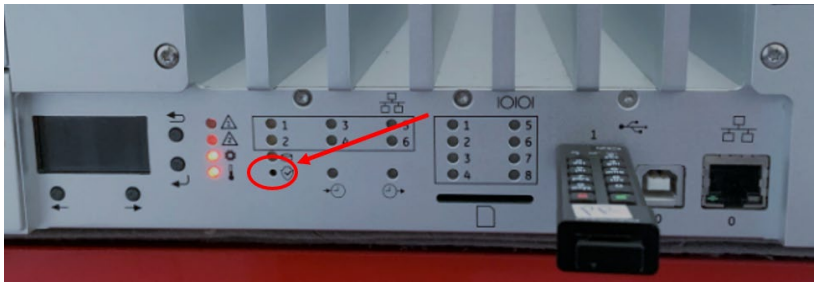
10. The USB can now be removed from the PC, to be used in one or more MCP devices.

Section 2: Use the external USB to upgrade the existing firmware and configuration

1. Insert the prepared USB Drive into one of the blue USB ports of the MCP to be updated.
2. Boot from the USB drive.
    - (Optional) If using the front serial port of the G500 or COM4 of the G100 to perform the upgrade, then start DS Agile Terminal Emulator and connect to the COM port connected to the G500 or G100. Set the baud rate to 115200, with no parity.

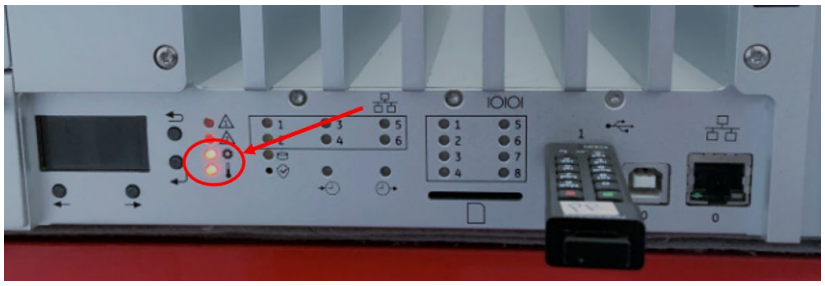
On the G500 perform the following steps:

i. Press the physical presence button with a paper clip. The physical presence button is shown in the following picture:



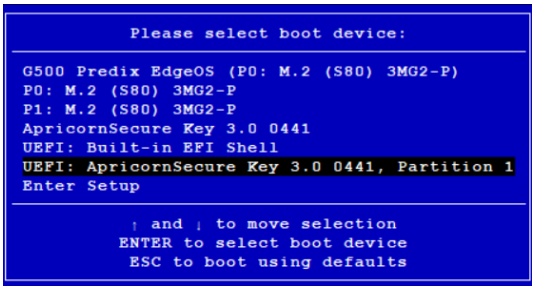
ii. Reboot without removing the paper clip.

iii. For the G500, wait until the CPU and Temp LEDs are flashing.



iv. Remove the paper clip from the physical presence button.

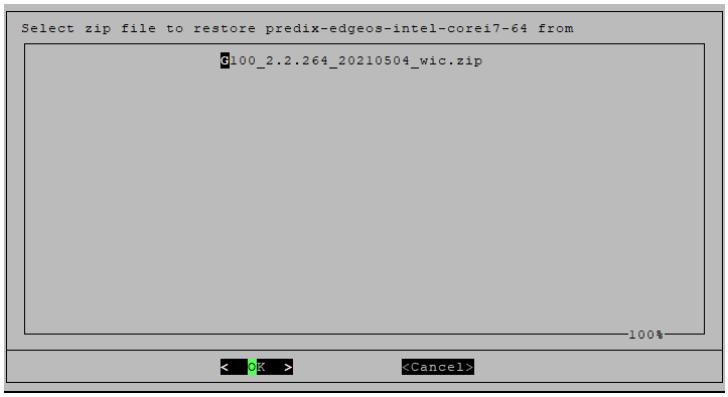
- On the G100, simply reboot the unit.
- Press **F7** repeatedly until the Boot Menu appears.
- Select the UEFI option for Partition 1 of your USB Drive (e.g. UEFI: ApricornSecure Key 3.0 0441, Partition 1).



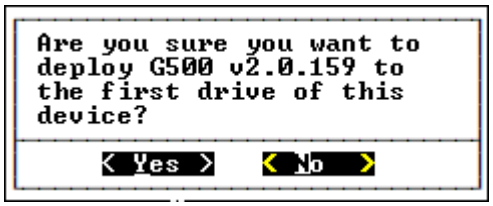
- A Boot screen will be displayed. Select the first option "**MCP Image Upgrade (64bit)**", if using a monitor. Select the second option "**MCP Image Upgrade (64bit, serial console)**", if using the front USB serial port.

3. Select the desired firmware image that you want the MCP to upgrade to.

- Select the firmware zip file to restore from the list.

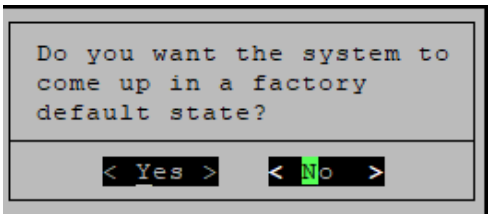


- A Linux OS will startup and first verify the zip file. Once the zip file is verified, it won't be verified again. This verification process takes about 2 minutes.
- The Linux OS will then prompt whether to install the image on the first disk of your MCP. Press **Yes** or **No**:
  - If you press **Yes**, the firmware upgrade will proceed.
  - If you press **No**, the firmware upgrade will be aborted: you will be prompted to remove the USB drive. Afterwards, the system will reboot and come up with the original firmware and configuration.



NOTE: All MCP units have only one drive, so it is of no concern that the image is always deployed on the first drive.

4. Choose whether you want the system to come up in a factory default state. If you press **Yes**, you will *not* be prompted to restore the clone snapshot in step 7; in other words, the system will be loaded with factory default configuration when the process is done. If you press **No**, you will be able to restore a clone snapshot in step 7.

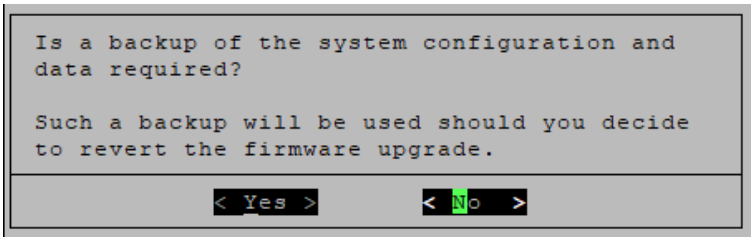


NOTE: If you select **No** to the above dialog, runtime information such as logs and database records from the current system will be archived in the folder /prev_version_backup on the upgraded system. Select **Yes** if you do not wish to retain such information (e.g. when wanting to release the system for reuse).

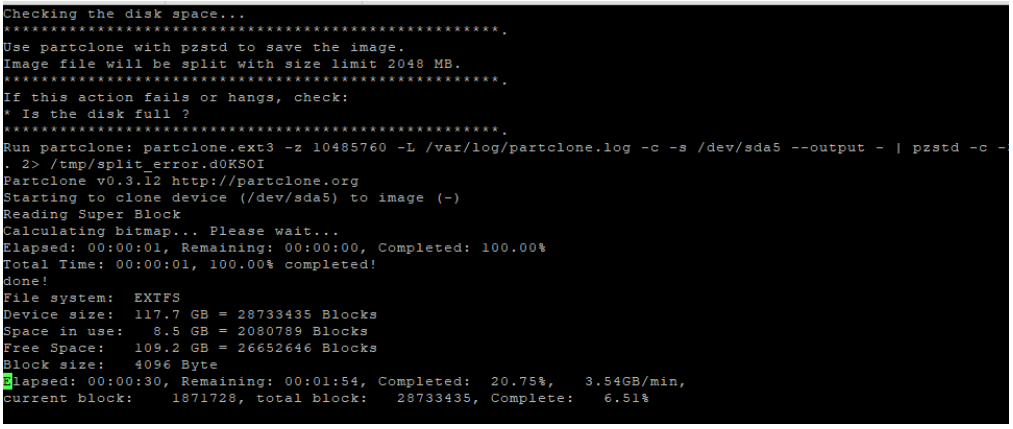
5. Backup and/or Restore current system configuration and data as needed.

   - This setup is intended to address the need of reverting the firmware upgrade so that the original configuration and data will be restored.
   - If you have previously made a system backup during firmware upgrade attempts in the past, you may be prompted whether to restore a system backup. Press **Yes** if you are reverting the firmware upgrade and restore back the saved backup of system configuration and data otherwise simply press **No** to skip it.

   - You will be prompted whether to make a backup of the system configuration and data on this MCP that is to be updated. Such a backup will be used should you decide to revert the firmware upgrade.

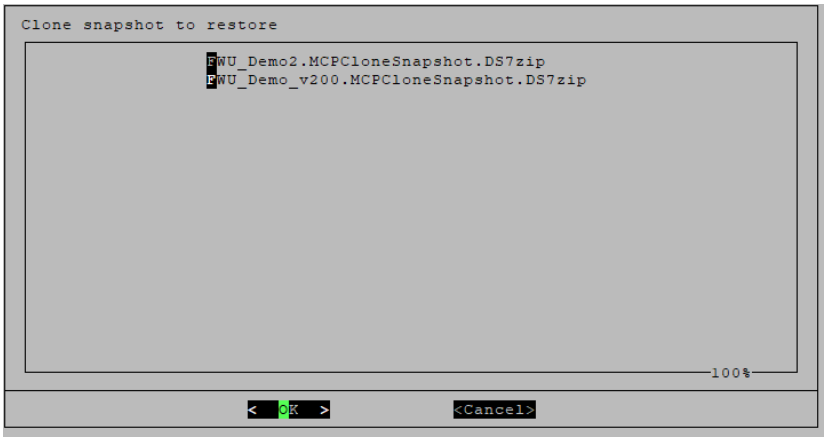


- If you press Yes, it will proceed to back up current system configuration and data.

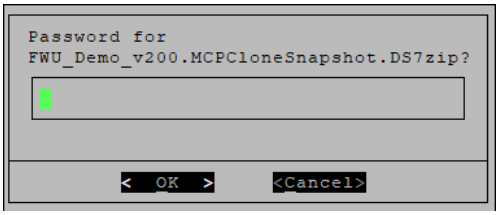


- If you press **No**, the backup process will be bypassed.

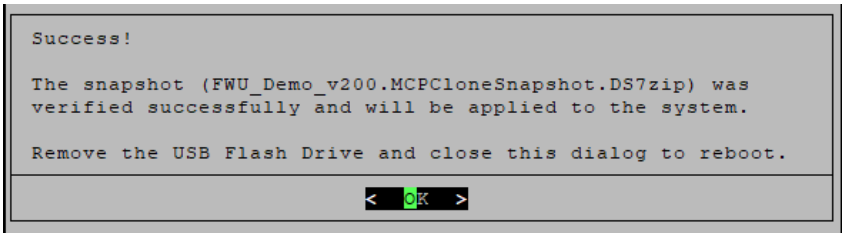
6. Restore the new firmware image to the MCP and verify the integrity.
   - The Linux OS will then restore the new firmware image to the first disk.
   - The image will be verified on the drive.
   - This process will take about 6 minutes to complete.
7. Restore the clone snapshot as needed. Only snapshots compatible with the same firmware version will be accepted. The option to restore a clone snapshot will not be available if a backup was selected previously. The option to restore a clone snapshot will not be available if you chose that you wanted the system to come up in a factory default state previously.
   - Select the MCP clone snapshot to restore from the USB and press **OK** to proceed further or press **Cancel** to bypass the restoring of snapshot.



   - Enter the password for the MCP Clone snapshot.

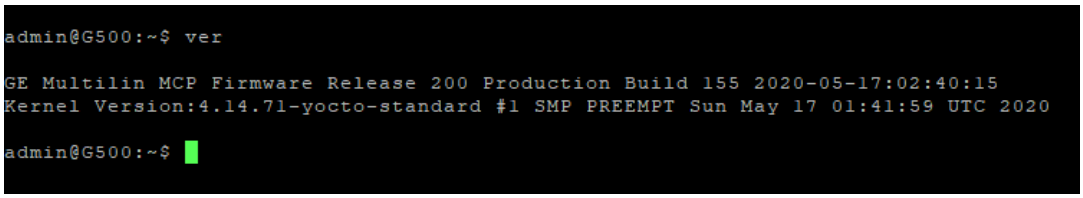


- When done, you will be prompted to remove the USB Drive and close the dialog to reboot the unit. Remove your USB Drive and press **OK**.



NOTE: Cyber security related Certificates are not included in the MCP clone snapshots, and therefore cannot be restored. All certificates must be imported again after the clone snapshot restore. All secure connections using certificates must be re-associated with the new imported certificates (e.g. Secure Connection Relay, VPN Server, etc.)

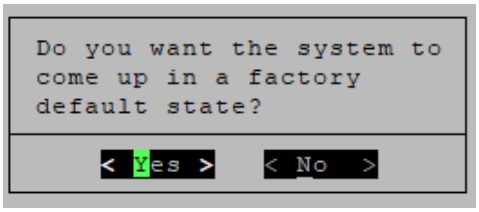
8. The MCP will reboot to finalize the upgrade.
   - The system will now boot Predix Edge OS and finalize the installation. This will take about 5-15 minutes. You will see the Predix Edge OS boot up messages. Once installation is finalized, the system will reboot automatically.
   - Wait for the system to come up again. On the G500, also wait for the G500 product name to appear on the front OLED.
9. The upgraded MCP device will now be loaded with MCP clone snapshot or backup, if one was selected above. If not – it will run the default configuration.
10. Login to verify the firmware and the restored configuration.
    - Login with a previous administrator user that was defined in the MCP Clone Snapshot or backup, if one was selected above. If not – use “defadmin”.
    - Verify the firmware version number by typing the command “ver”.



Section 3: Use the external USB to re-image the MCP

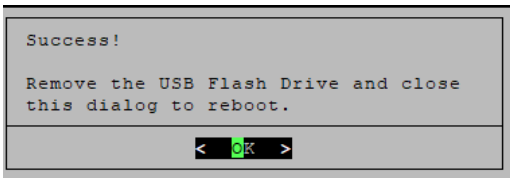
Use this procedure to erase data and restore to defaults in case where all administrators' credentials have been lost.

1. Insert the prepared USB Drive into one of the blue USB ports of the MCP to be defaulted.
2. Boot from the USB drive.
    - Follow the same procedure as step 2 in Use the DSAS "MCP Firmware Upgrade" tool to create the USB disk image.
3. Select the firmware image of which the version is identical with the MCP to be defaulted.
    - Follow the same procedure as step 3 in Use the DSAS "MCP Firmware Upgrade" tool to create the USB disk image.
4. Make sure to press **Yes** when this dialog pops up.



5. Bypass the step to backup and/or restore the system configuration and data.
    - You may be prompted whether to restore system backup If you have previously made a system backup during firmware upgrade attempts in the past. Make sure to press **Cancel** to bypass it.

6. Restore the firmware image to the MCP and verify the integrity.
    - The Linux OS will then restore the new firmware image to the first disk.
    - The image will be verified on the drive.
    - This process will take about 6 minutes to complete.
    - When done, you will be prompted to remove the USB Drive and close the dialog to reboot the unit. Remove your USB Drive and press **OK**.



7. The MCP will reboot to finalize the upgrade.
    - The system will now boot Predix Edge OS and finalize the installation. This will take about 5-15 minutes. You will see the Predix Edge OS boot up messages. On the G500, once installation is finalized, the system will reboot automatically.
    - Wait for the system to come up again. On the G500, wait for the G500 product name to appear on the front OLED.
8. The upgraded MCP device will be loaded with factory default configuration.
9. Login to verify the firmware and the restored configuration.
    - Login with the default administrator user credentials, that is, “defadmin” for the username and “ defadmin” for the password.
    - Verify the firmware version number by typing the command “ver”.

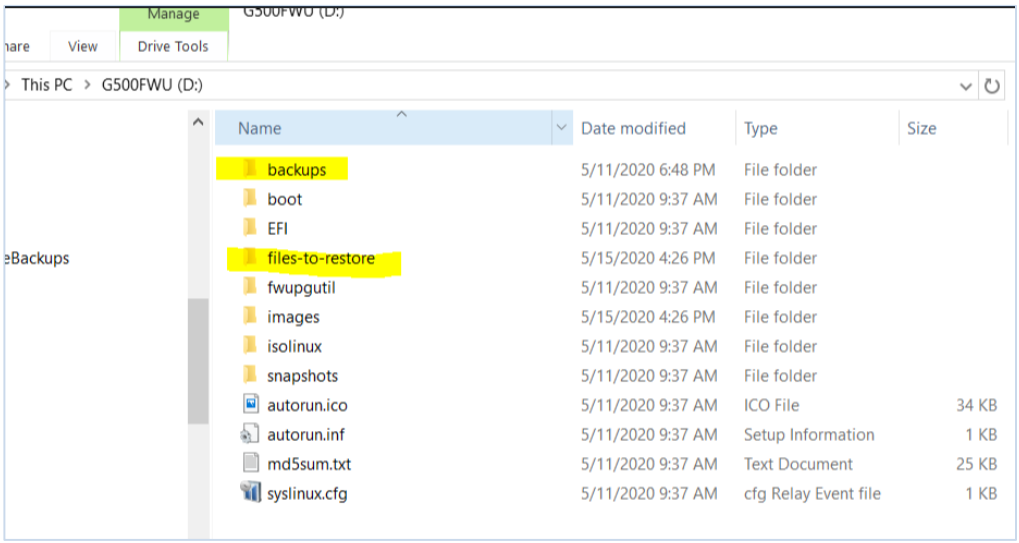
```
GE Multilin MCP Firmware Release 200 Production Build 159 2020-05-27:08:57:24 + Updates
Kernel Version:4.14.71-yocto-standard #1 SMP PREEMPT Wed May 27 08:28:24 UTC 2020
```

Section 4: Troubleshooting

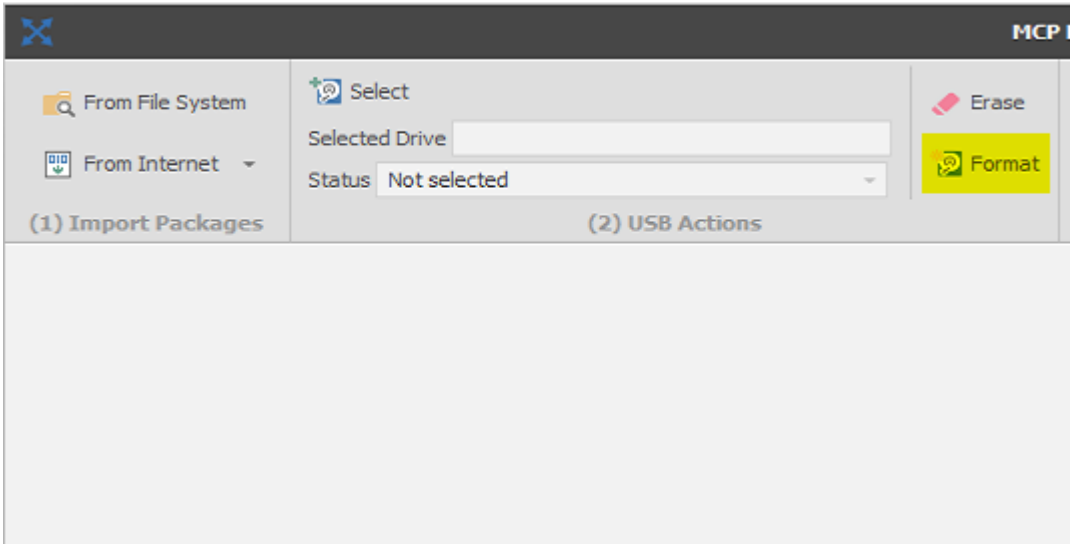
Power failure during the firmware upgrade

In the event of power failure during the firmware upgrade, the USB drive may be corrupted in some ways. It should be reformatted before using it to resume the upgrade.

1. Copy the files under files-to-restore and backups on the USB to a folder on your PC.



2. Format the USB by using MCP Firmware Upgrade tool.



3. Copy the files under files-to-restore and backups back from the folder on the PC.
4. Repeat the steps to prepare the USB drive and then perform the firmware upgrade once again.

Product Support

If you need help with any aspect of your GE Grid Solutions product, you can:

- Access the GE Grid Solutions Web site
- Search the GE Grid Solutions Technical Support library
- Contact GE Grid Solutions Technical Support

GE Grid Solutions Web Site

The GE Grid Solutions Web site provides fast access to technical information, such as manuals, release notes and knowledge base topics. Visit us on the Web at: http://www.gegridsolutions.com

GE Grid Solutions Technical Support Library

This site serves as a document repository for technical information, such as manuals, release notes, and software. To *get* access to the Technical Support Web site, go to: http://supportcentral.ge.com/*SASTechSupport

Contact GE Grid Solutions Technical Support

For help with any aspect of your GE Grid Solutions product, please contact our support team, 24/7, as follows:

Region	E-mail	Telephone
Global Contact Centre	ga.support@ge.com	+44 1785 250070
Central and East Asia and Pacific	ga.supportCEAP@ge.com	+61 414 730 964
India	ga.supportIND@ge.com	+91 44 22648000
Middle East, North Africa and Turkey	ga.supportMENAT@ge.com	+971 42929467
Europe, Russia, CIS and Sub-Saharan Africa	ga.supportERCIS@ge.com	+34 94 4858854
North America	ga.supportNAM@ge.com	+1 877 605 6777
Latin America	ga.supportLAM@ge.com	+55 11 36187308

Copyright Notice

© 2021, General Electric Company. All rights reserved.

The information contained in this online publication is the exclusive property of General Electric Company, except as otherwise indicated. You may view, copy and print documents and graphics incorporated in this online publication (the "Documents") subject to the following: (1) the Documents may be used solely for personal, informational, non-commercial purposes; (2) the Documents may not be modified or altered in any way; and (3) General Electric Company withholds permission for making the Documents or any portion thereof accessible via the internet. Except as expressly provided herein, you may not use, copy, print, display, reproduce, publish, license, post, transmit or distribute the Documents in whole or in part without the prior written permission of General Electric Company. If applicable, any use, modification, reproduction, release, performance, display, or disclosure of the Software Product and Associated Material by the U.S. Government shall be governed solely by the terms of the License Agreement and shall be prohibited except to the extent expressly permitted by the terms of the License Agreement.

The information contained in this online publication is subject to change without notice. The software described in this online publication is supplied under license and may be used or copied only in accordance with the terms of such license.

Trademark Notice

GE and the GE monogram are trademarks and service marks of General Electric Company.

* Trademarks of General Electric Company.

Other company or product names mentioned in this document may be trademarks or registered trademarks of their respective companies.

Modification Record

Version	Revision	Date	Change Description
1.0	0	14th Feb, 2020	Initial Release.
	1	23rd Feb, 2020	Added config update steps.
2.0	0	26th May, 2020	Updated for G500 v2.0 release.
	1	15th June, 2020	Updated factory default workflow.
	2	29th June, 2020	Updated certificates related information.
	3	13th July, 2020	Added MCP Platform Package prerequisite.
	4	23rd July, 2020	Updated to take MCP Platform Package prerequisite from USB.
	5	6th Nov, 2020	Updated to take MCP Platform Package prerequisite from USB for DSAS 2.2 and below.
3.0	0	6th May, 2021	Updated for MCP family and Service Update workflows.
	1	26th May, 2021	Updated "SWM0122 Configuring UEFI Settings on G100 User Guide" reference.
	2	27th July, 2021	Updated for backwards compatibility with DSAS 2.1 and 2.2, and to always attempt to install the MCP Platform package.

GE
Grid Solutions

TN0123 V1.00

Installing Service Updates on MCP

Technical Note

Overview

The MCP Substation Gateway can be updated to correct software defects or to provide new features between firmware releases. A service update should only be applied if you are experiencing a particular issue addressed by the update. Software modifications that are contained in service updates are all implemented on subsequent firmware releases.

All MCP Service Updates are signed by GE to ensure end to end integrity.

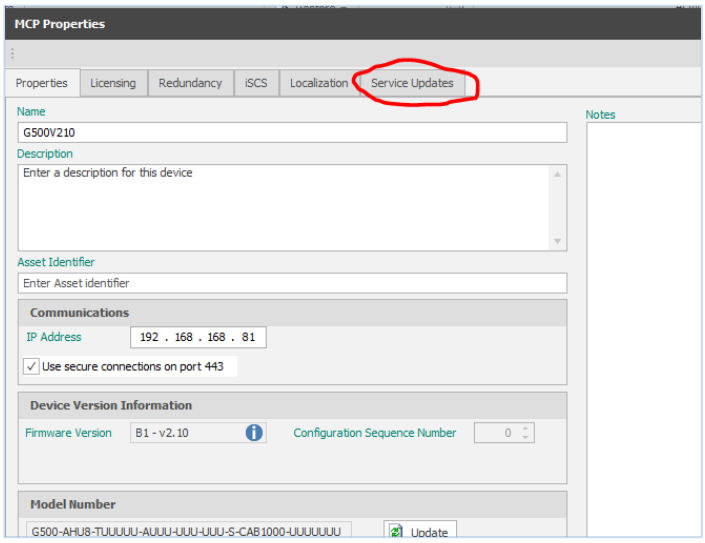
NOTICE **This document applies to the MCP family (G100/G500) unless otherwise indicated.**
Screen captures may show G500 in some areas, however the workflow applies to products in the MCP family (G100/G500).

Installing Service Updates

Please refer to the release notes provided with each service update file for information on any restrictions or warning.

This workflow applies to the DSAS MCP Studio v2.3 or later version working with full range of the firmware versions of MCP.

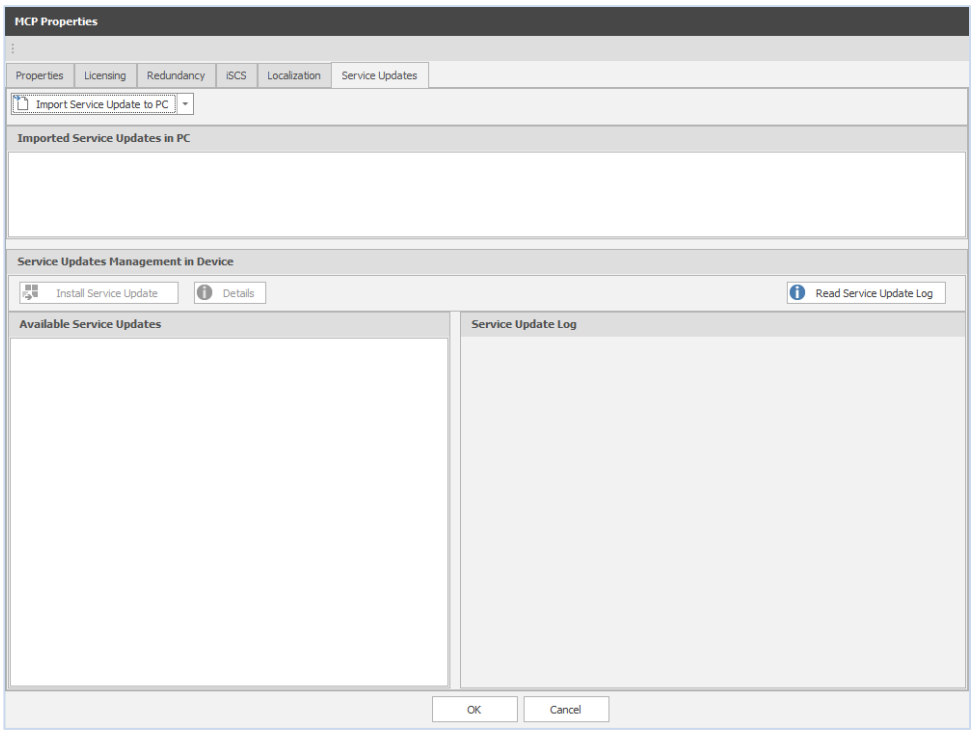
1. Create a device that matches your MCP device if you don't have such an existing device (firmware version, IP address to connect).
2. Perform "Sync From Device" operation if you haven't done so previously.
3. Select the device and click the Properties button to open the device Properties page.
4. Select Service Updates tab.



5. Import Service Updates to PC.

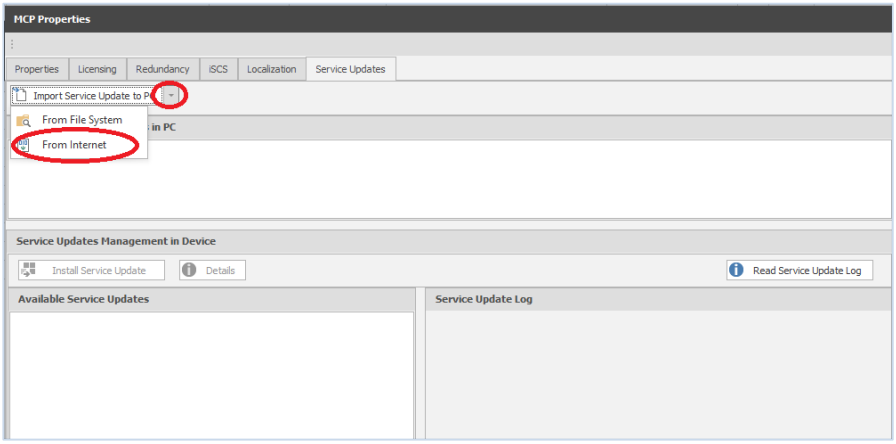
   If the service updates are already available in the computer, or on a shared drive, for example they have been downloaded and saved previously, you can choose to import them **From File System** otherwise you will need to download and import them **From Internet**.

   If this PC has the service update files already imported into this tool, you may skip this process.

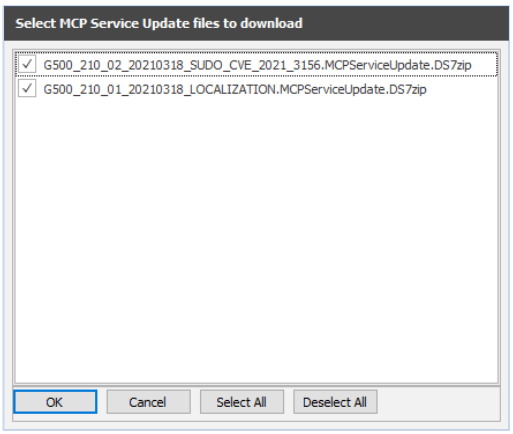


To Import Service Updates from Internet. (Internet Access is Required)

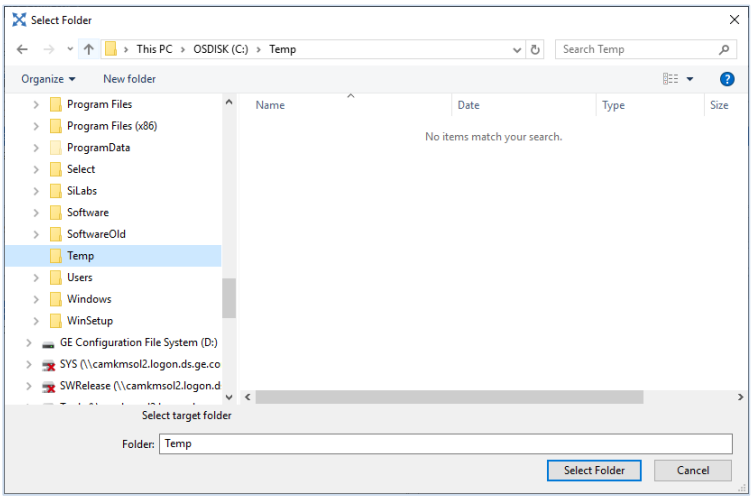
- Click the drop-down list of **Import Service Update to PC**
- Select **From Internet.**



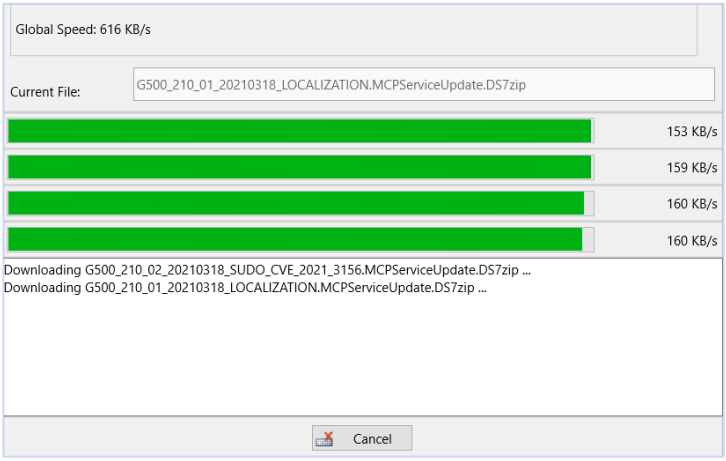
- The list of available MCP Service Update files will appear.



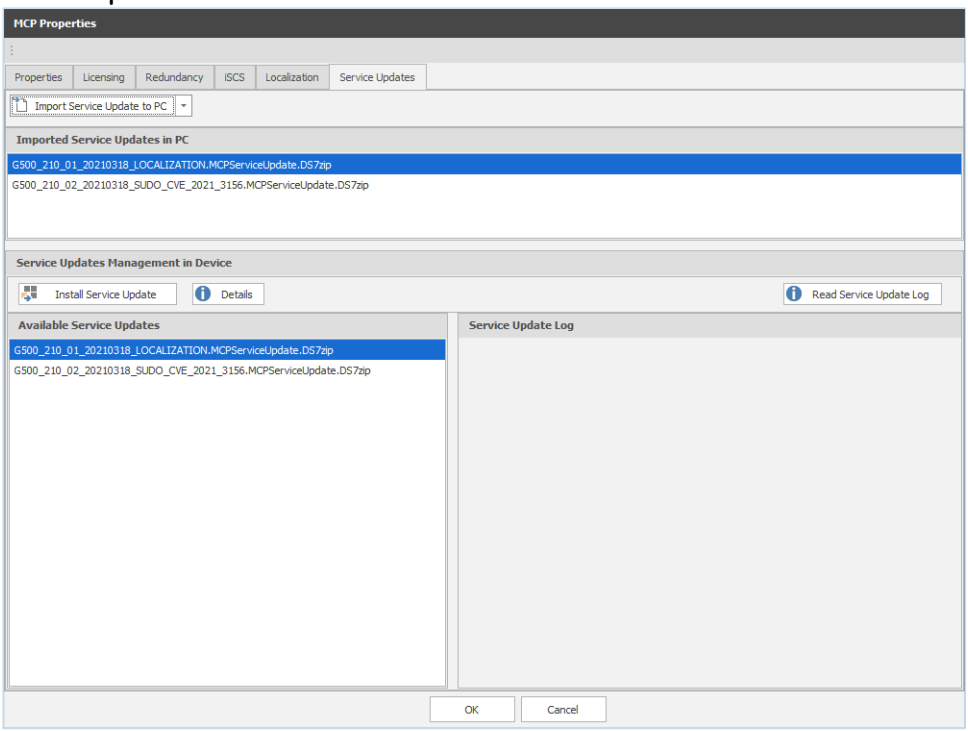
- Select the desired MCP Service Update(s) that you want to import to your PC and then click OK.
- Select a folder to store the service updates that are about to download. This folder is for your future re-distribution of the saved files. The import operation will also place the files automatically in their reserved DSAS environment in the PC.



- Once a folder is selected, the downloading will begin.

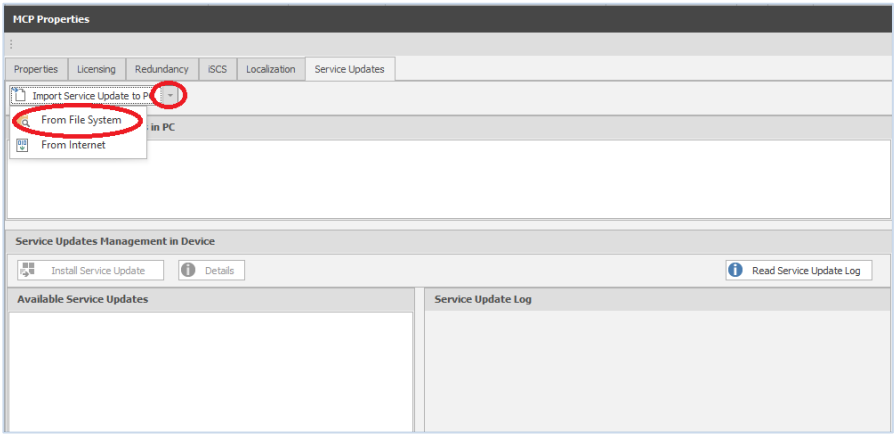


- The service update file will be imported after it is downloaded (i.e. placed in a reserved DSAS location). If you do not need the files in the folder above (e.g. Temp), you can later remove them, this action will not remove the imported files from the PC.
- You only need to import a given service update once into a given PC, and the list will be shown under **Imported Service Updates in PC**.

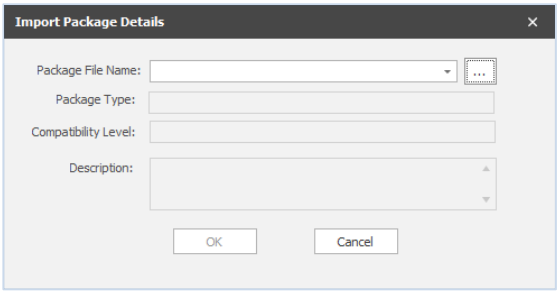


To Import Service Updates from file system

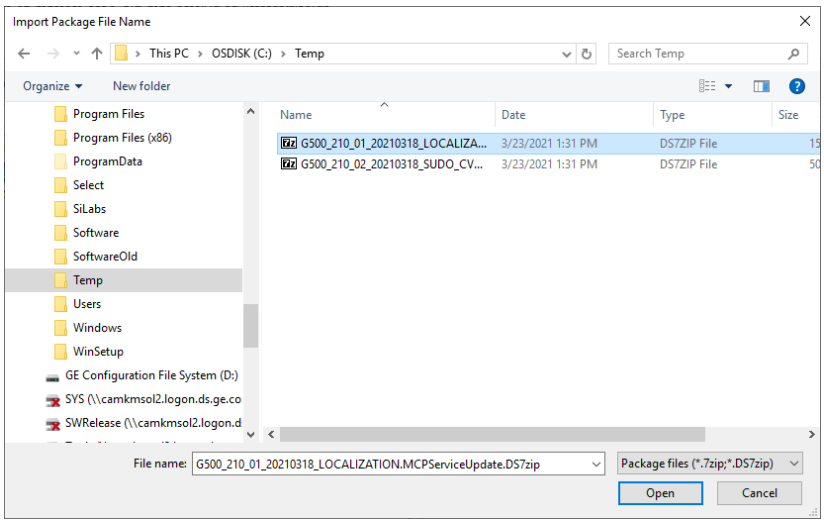
- Click the drop-down list of **Import Service Update to PC**
- Select **From File System** to open Import Package Details dialog.



- Click **...** to browse the file system to select the service update file.



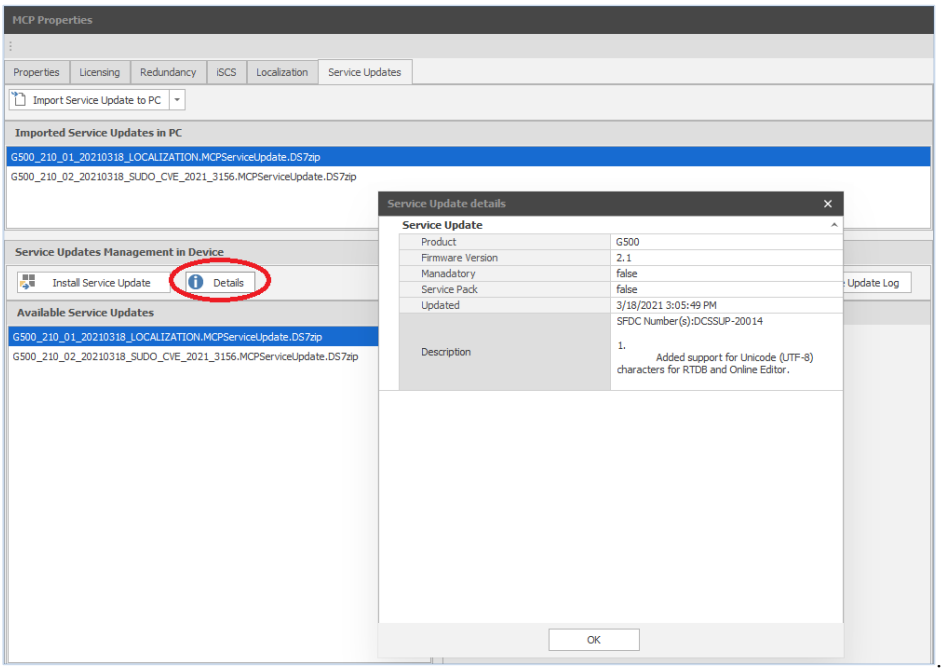
- Click **OK** to import the selected service update.



- The service update file will be imported after it is selected (i.e. placed in a reserved DSAS location). If you do not need the files in the folder above (e.g. Temp), you can later remove them, this action will not remove the imported files from the PC.
- You only need to import a given service update once into a given PC, and the list will be shown under **Imported Service Updates in PC**.

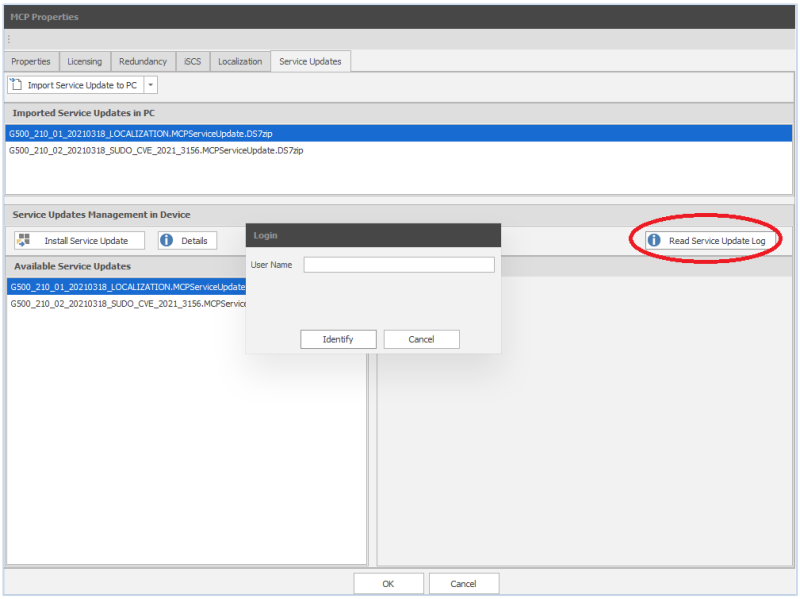
Available Service Updates

6. Under the area **Available Service Updates** you will see a list of only service updates compatible with this device firmware version. This may be a subset of the **Imported Service Updates in PC** list.
7. You may Verify service update **Details**

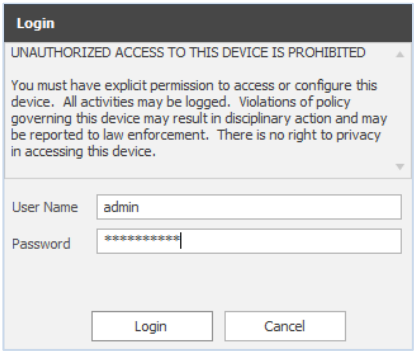


- The Details dialog can be re-sized as needed, including the vertical separation bar.
- If you need, with the Details dialog open, press **CTRL+C** to copy the *Description* content into the Windows Clipboard.

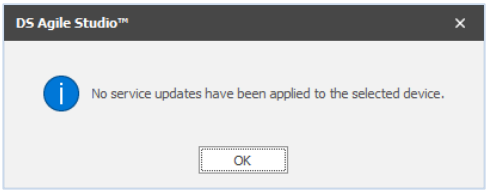
8. You can Read Service Update History (Access as Administrator role to MCP device is required)
   - Click **Read Service Update Log** button to bring forth Login process (this will use the IP address configured under the main Properties tab).
   - If you have connected to the device and it is still connected, the login process will be bypassed (as long as the Device Properties dialog is kept open).



- Type in an administrator role User Name and Login window will pop up after clicking **Identify**.



- Type in password and click **Login**.
- Service Update History will then be displayed.
- The following message will pop up in case there are no service updates that have been applied before.

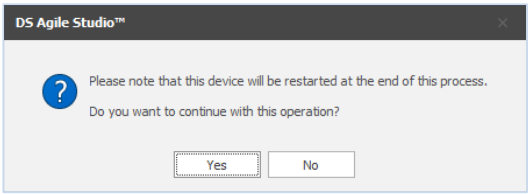


9. Install Service Update.
   - Select the desired service update that you want to apply to the MCP and click **Install Service Update**.

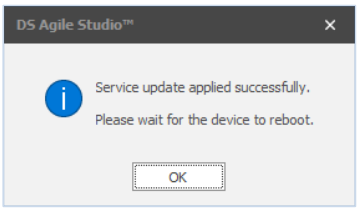
     Notes:

     If there are multiple service updates to be applied, apply one service update at a time.

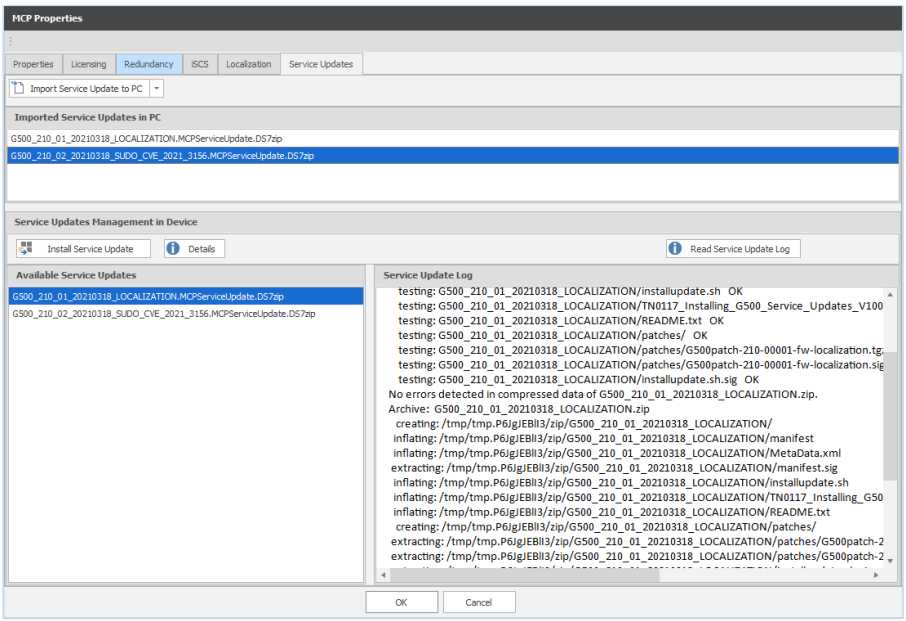
     Unless otherwise instructed in service updates release notes, you should deploy them as needed and in the ascending order of their date.
   - You will be prompted with a confirmation dialog to confirm this operation, and that the **MCP will be restarted if you choose to proceed.**
   - Click **No** to cancel the operation and **Yes** to continue.



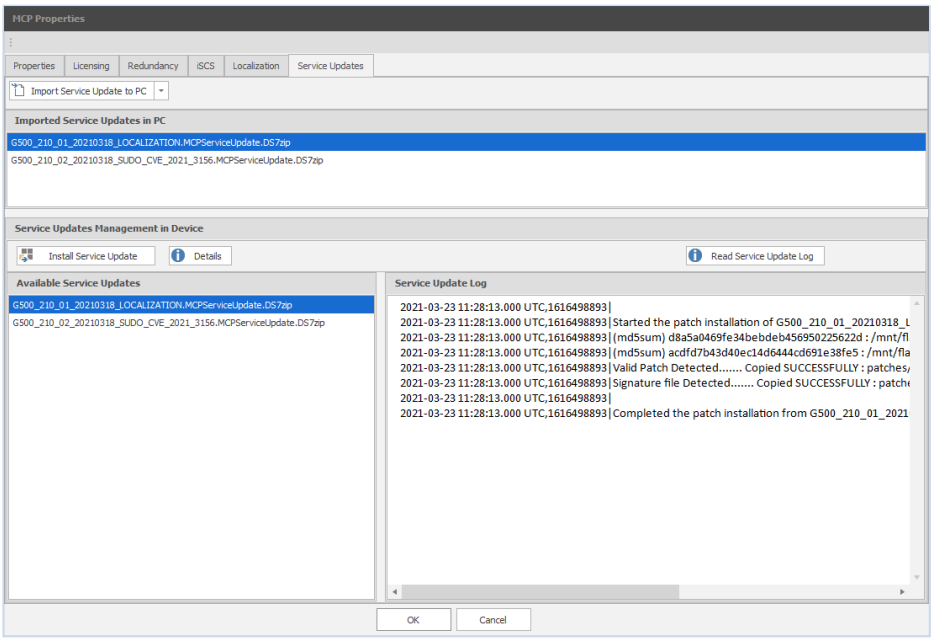
   - The process to login to the device is not required if you have already connected to the device in last step and never exited the Device Properties window.
   - The message “Applying service update…” will be displayed during the progress.
   - The signature of the Service Update is verified, and the service update is placed into to the MCP target device.
   - The MCP device will reboot when the update is finished, and a successful message will be displayed as follows.



- When clicking OK, the detailed update log during the process will be displayed as following:



- You may want to review the detailed service update log by scrolling up/down and right/left while waiting for the MCP device to complete the reboot.
- Once the device is ready, click **Read Service Update Log** button again to retrieve and review the summary of service update history and confirm the successful update(s).
- You may copy the log content to the Windows clipboard by click inside the Service Update Log window, then **CTRL+A** and **CTRL+C**



- Repeat the above steps to apply another service update if needed.

Product Support

If you need help with any aspect of your GE Grid Solutions product, you can:

- Access the GE Grid Solutions Web site
- Search the GE Grid Solutions Technical Support library
- Contact GE Grid Solutions Technical Support

GE Grid Solutions Web Site

The GE Grid Solutions Web site provides fast access to technical information, such as manuals, release notes and knowledge base topics. Visit us on the Web at: http://www.gegridsolutions.com

GE Grid Solutions Technical Support Library

This site serves as a document repository for technical information, such as manuals, release notes, and software. To *get* access to the Technical Support Web site, go to: http://supportcentral.ge.com/*SASTechSupport

Contact GE Grid Solutions Technical Support

For help with any aspect of your GE Grid Solutions product, please contact our support team, 24/7, as follows:

Region	E-mail	Telephone
Global Contact Centre	ga.support@ge.com	+44 1785 250070
Central and East Asia and Pacific	ga.supportCEAP@ge.com	+61 414 730 964
India	ga.supportIND@ge.com	+91 44 22648000
Middle East, North Africa and Turkey	ga.supportMENAT@ge.com	+971 42929467
Europe, Russia, CIS and Sub-Saharan Africa	ga.supportERCIS@ge.com	+34 94 4858854
North America	ga.supportNAM@ge.com	+1 877 605 6777
Latin America	ga.supportLAM@ge.com	+55 11 36187308

Copyright Notice

© 2021, General Electric Company. All rights reserved.

The information contained in this online publication is the exclusive property of General Electric Company, except as otherwise indicated. You may view, copy and print documents and graphics incorporated in this online publication (the "Documents") subject to the following: (1) the Documents may be used solely for personal, informational, non-commercial purposes; (2) the Documents may not be modified or altered in any way; and (3) General Electric Company withholds permission for making the Documents or any portion thereof accessible via the internet. Except as expressly provided herein, you may not use, copy, print, display, reproduce, publish, license, post, transmit or distribute the Documents in whole or in part without the prior written permission of General Electric Company. If applicable, any use, modification, reproduction, release, performance, display, or disclosure of the Software Product and Associated Material by the U.S. Government shall be governed solely by the terms of the License Agreement and shall be prohibited except to the extent expressly permitted by the terms of the License Agreement.

The information contained in this online publication is subject to change without notice. The software described in this online publication is supplied under license and may be used or copied only in accordance with the terms of such license.

Trademark Notice

GE and the GE monogram are trademarks and service marks of General Electric Company.

* Trademarks of General Electric Company.

Other company or product names mentioned in this document may be trademarks or registered trademarks of their respective companies.

Modification Record

Version	Revision	Date	Change Description
1.00	0	25th March, 2021	Initial Release.
	1	29th July, 2021	Updated for MCP family

GE

Grid Solutions

MCP Snapshot and Configuration Workflows

Application Note AN0015

How to Save and Restore Snapshot….

NOTICE

This Application Note supplements the information in the user documentation provided with your product. Read and thoroughly understand all provided user documentation before undertaking any actions shown in this document. Only qualified personnel should perform this procedure.

NOTICE

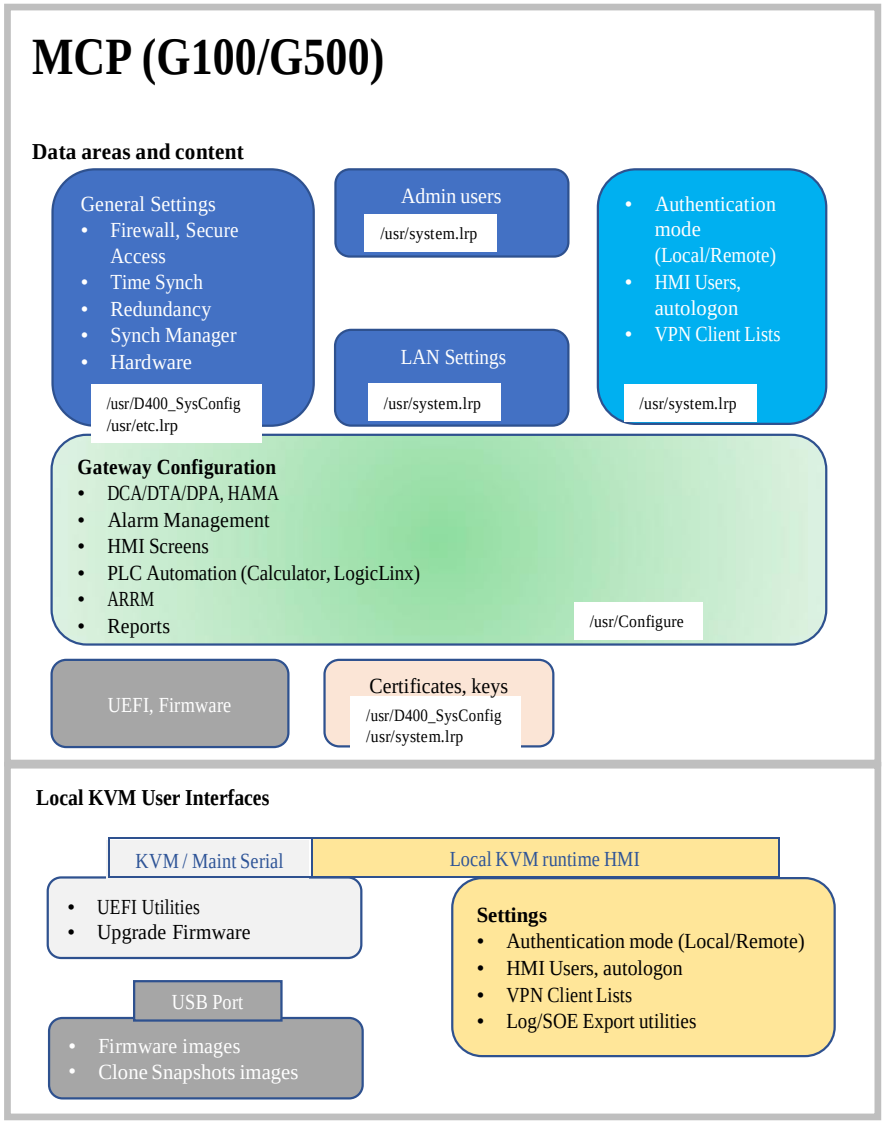
This document applies to the MCP family (G100/G500).

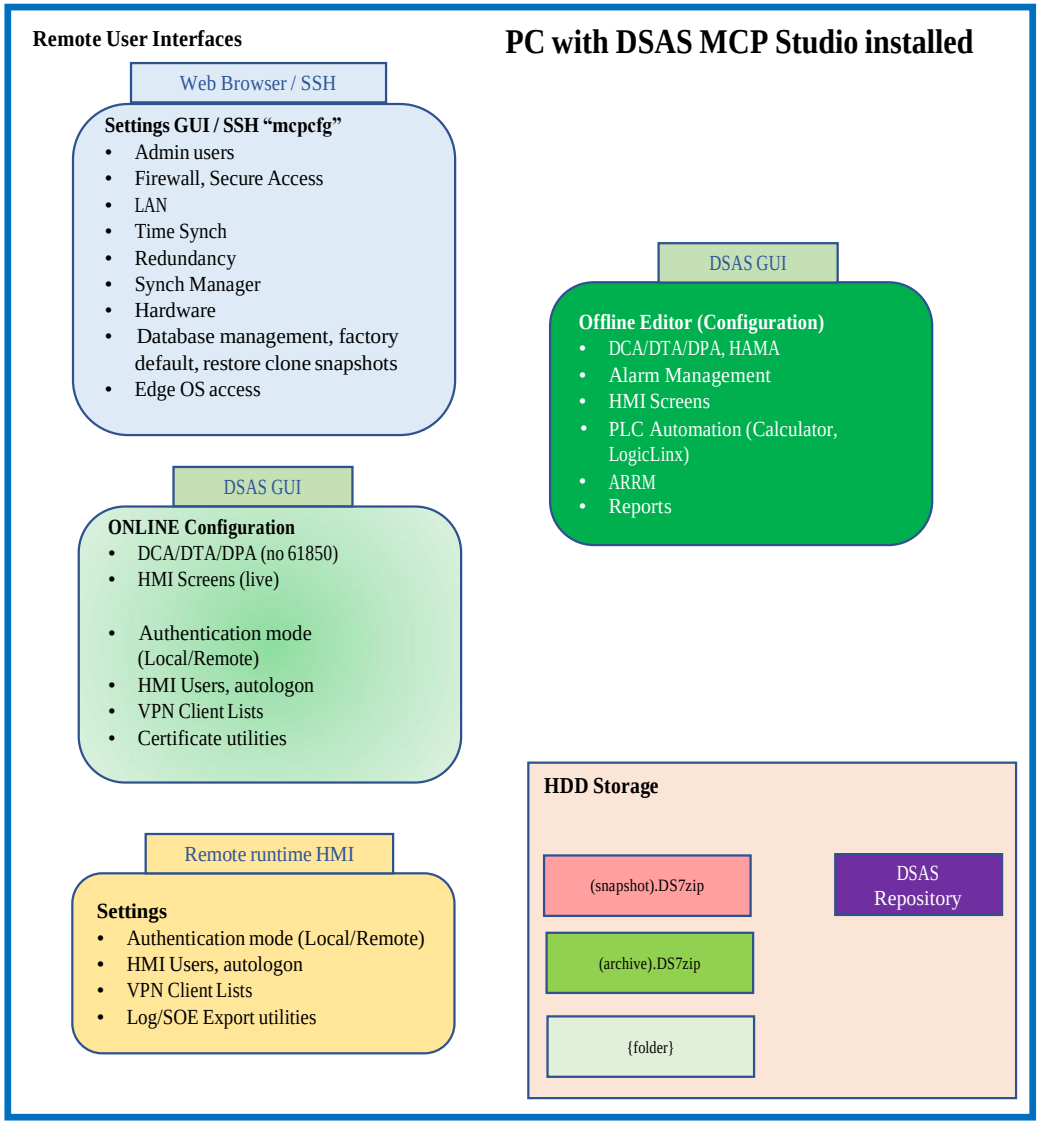
Screen captures may show G500 in some areas, however the described workflows apply to products in the MCP family (G100/G500).

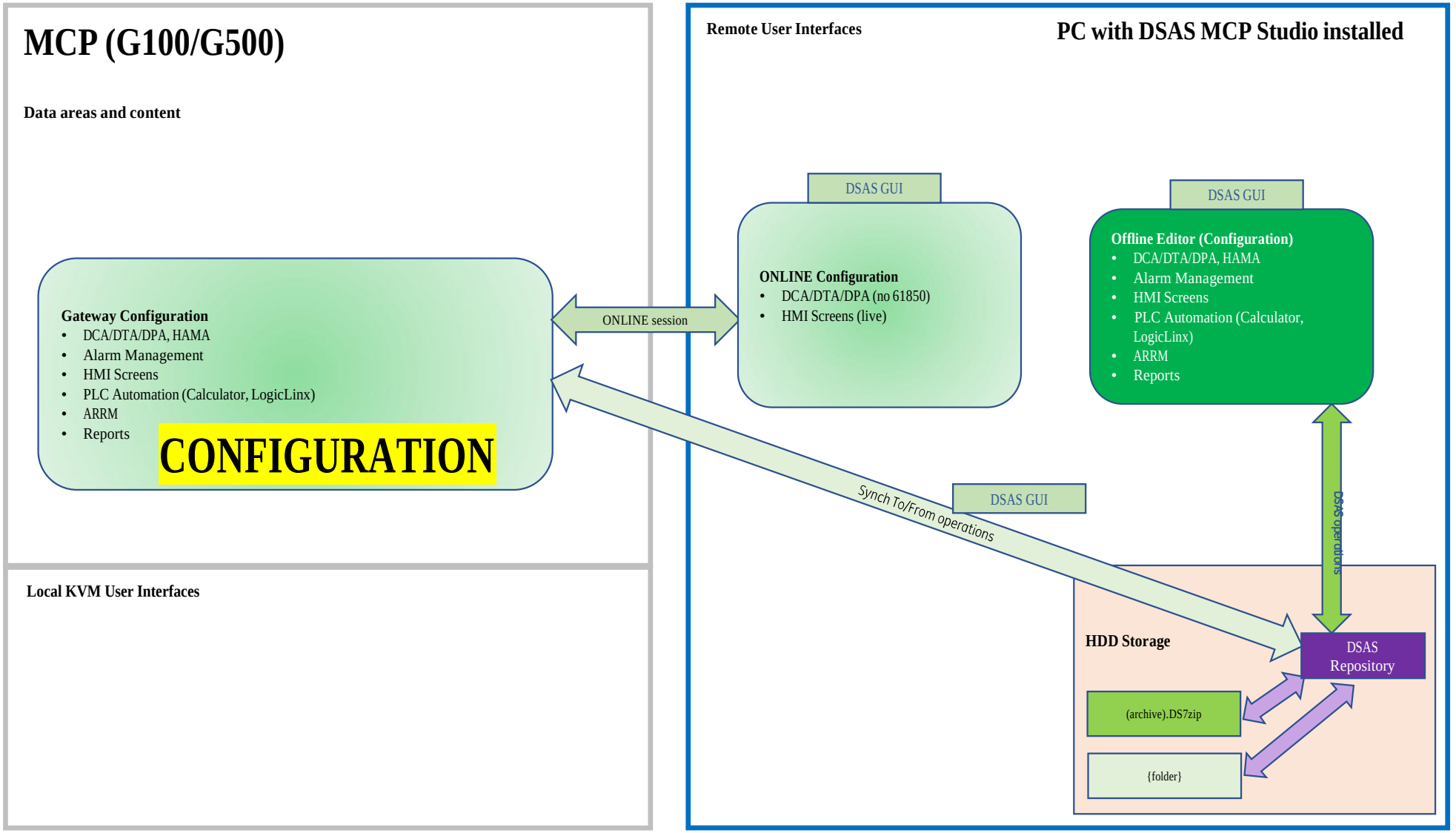
Snapshots are valid within same MCP product type, are not directly portable between G100-G500.

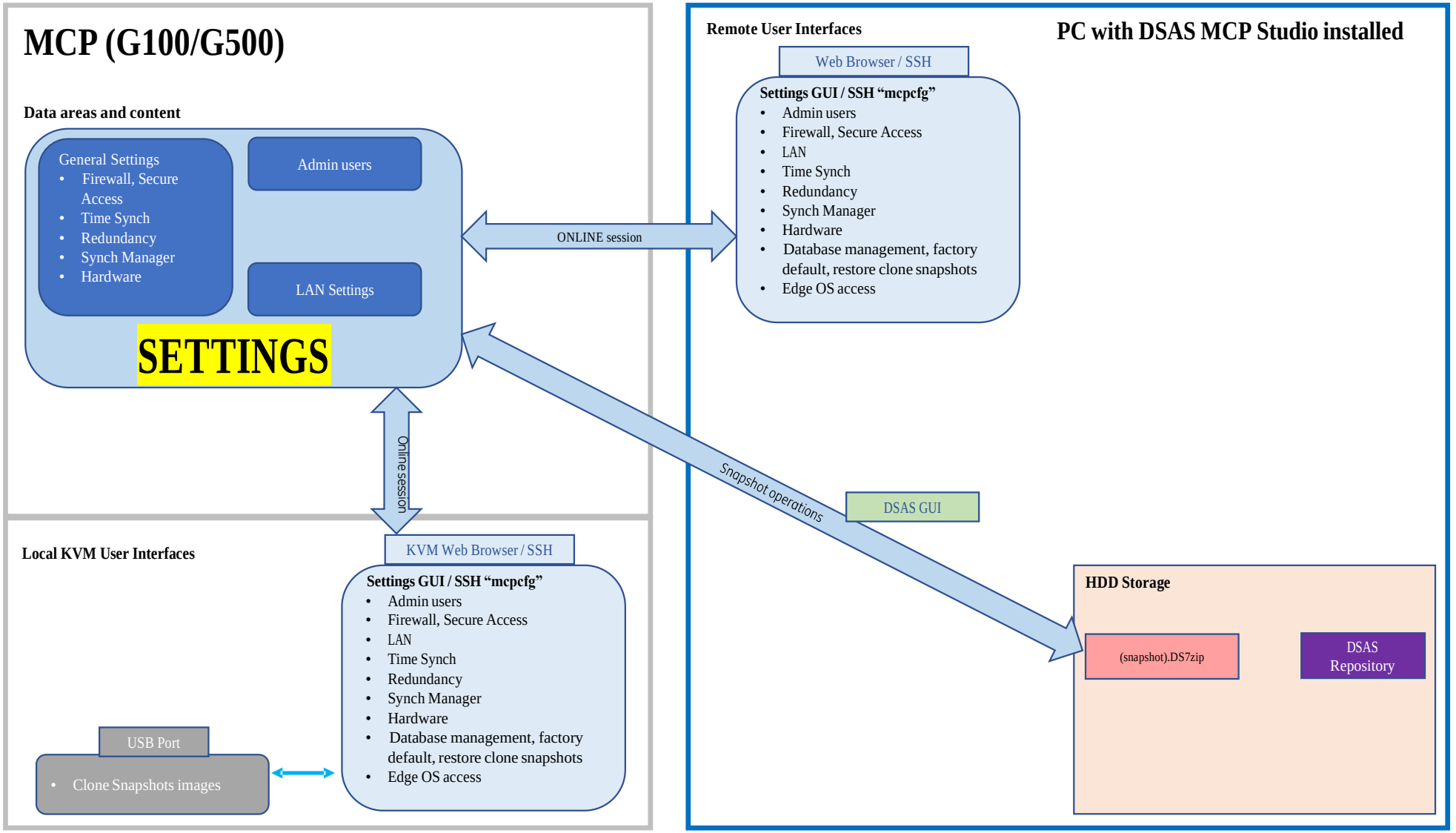
MCP (G100/G500)

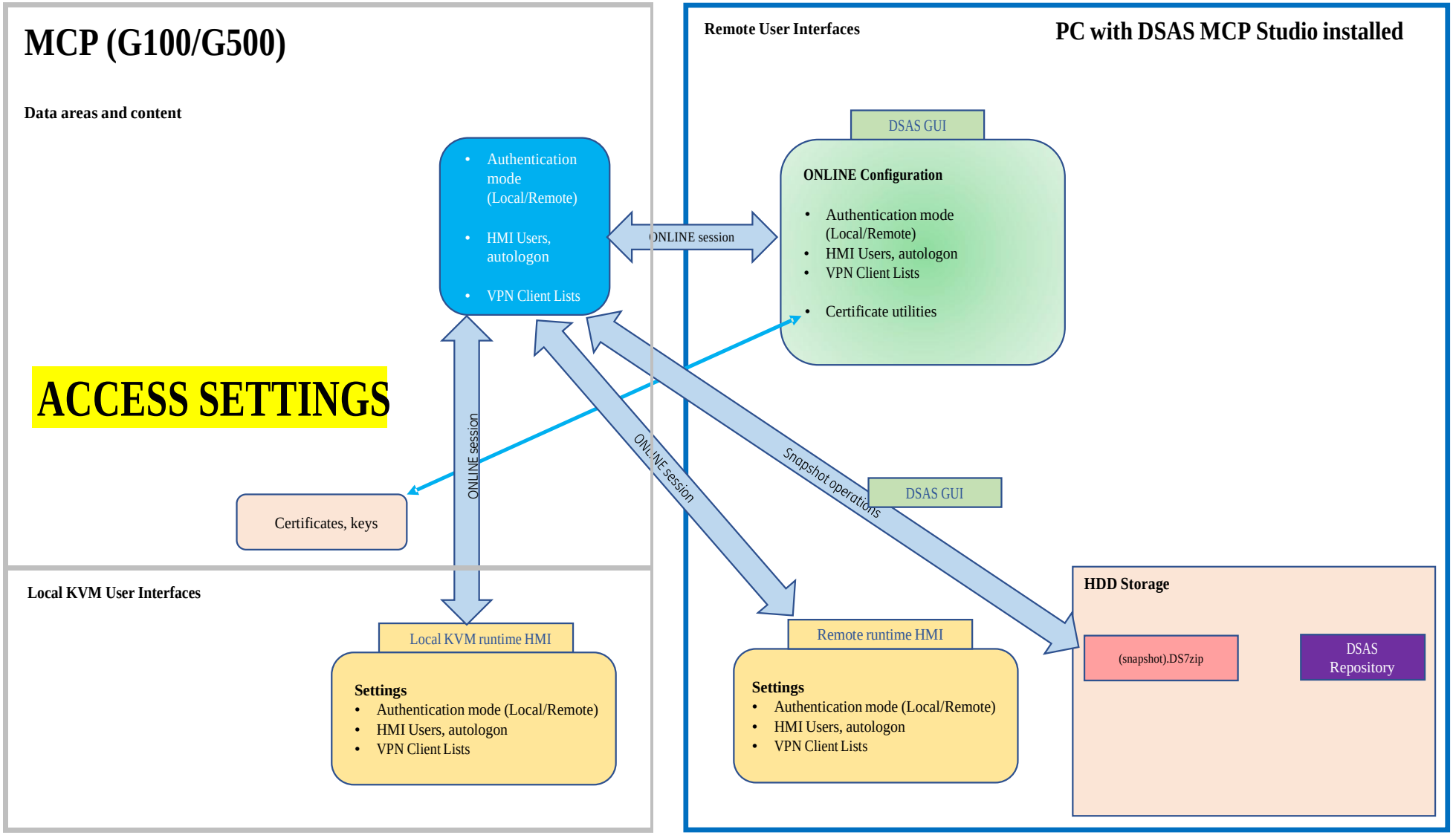
Data Areas, Content & User Interfaces

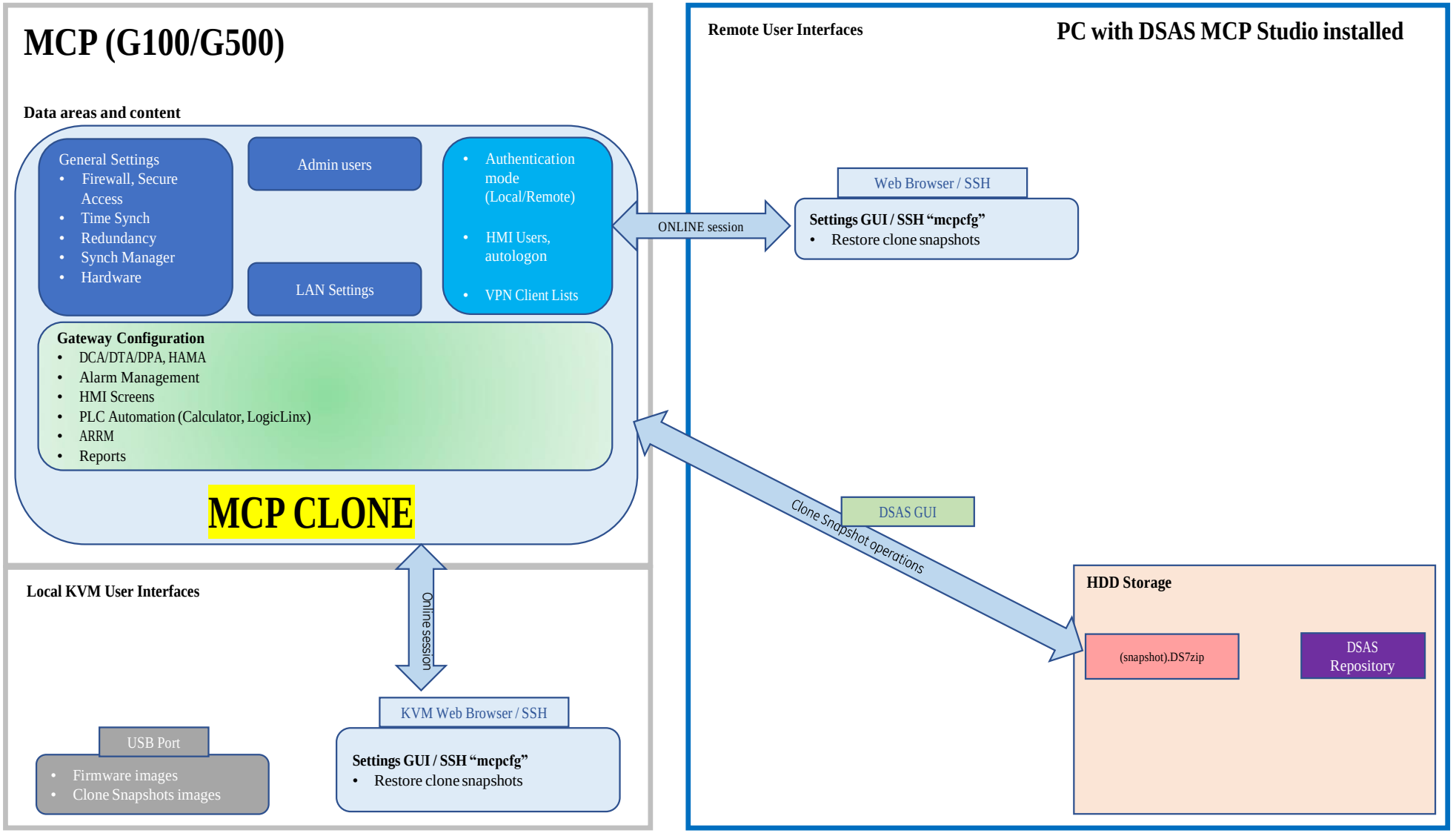

MCP (G100/G500)
Data areas and content
General Settings
• Firewall, Secure Access
• Time Synch
• Redundancy
• Synch Manager
• Hardware
/usr/D400_SysConfig
/usr/etc.lrp
Admin users
/usr/system.lrp
LAN Settings
/usr/system.lrp
• Authentication mode (Local/Remote)
• HMI Users, autologon
• VPN Client Lists
/usr/system.lrp
Gateway Configuration
• DCA/DTA/DPA, HAMA
• Alarm Management
• HMI Screens
• PLC Automation (Calculator, LogicLinx)
• ARRM
• Reports
/usr/Configure
UEFI, Firmware
Certificates, keys
/usr/D400_SysConfig
/usr/system.lrp
Local KVM User Interfaces
KVM / Maint Serial
Local KVM runtime HMI
• UEFI Utilities
• Upgrade Firmware
USB Port
• Firmware images
• Clone Snapshots images
Settings
• Authentication mode (Local/Remote)
• HMI Users, autologon
• VPN Client Lists
• Log/SOE Export utilities


Remote User Interfaces
PC with DSAS MCP Studio installed
Web Browser / SSH
Settings GUI / SSH "mcpcfg"
• Admin users
• Firewall, Secure Access
• LAN
• Time Synch
• Redundancy
• Synch Manager
• Hardware
• Database management, factory default, restore clone snapshots
• Edge OS access
DSAS GUI
Offline Editor (Configuration)
• DCA/DTA/DPA, HAMA
• Alarm Management
• HMI Screens
• PLC Automation (Calculator, LogicLinx)
• ARRM
• Reports
DSAS GUI
ONLINE Configuration
• DCA/DTA/DPA (no 61850)
• HMI Screens (live)
• Authentication mode (Local/Remote)
• HMI Users, autologon
• VPN Client Lists
• Certificate utilities
Remote runtime HMI
Settings
• Authentication mode (Local/Remote)
• HMI Users, autologon
• VPN Client Lists
• Log/SOE Export utilities
HDD Storage
(snapshot).DS7zip
(archive).DS7zip
{folder}
DSAS Repository


MCP (G100/G500)
Data areas and content
Gateway Configuration
• DCA/DTA/DPA, HAMA
• Alarm Management
• HMI Screens
• PLC Automation (Calculator, LogicLinx)
• ARRM
• Reports
CONFIGURATION
ONLINE session
Local KVM User Interfaces
Remote User Interfaces
PC with DSAS MCP Studio installed
DSAS GUI
ONLINE Configuration
• DCA/DTA/DPA (no 61850)
• HMI Screens (live)
DSAS GUI
Offline Editor (Configuration)
• DCA/DTA/DPA, HAMA
• Alarm Management
• HMI Screens
• PLC Automation (Calculator, LogicLinx)
• ARRM
• Reports
DSAS GUI
Synch To/From operations
DSAS operations
HDD Storage
DSAS Repository
(archive).DS7zip
{folder}


MCP (G100/G500)
Data areas and content
General Settings
• Firewall, Secure Access
• Time Synch
• Redundancy
• Synch Manager
• Hardware
Admin users
LAN Settings
SETTINGS
ONLINE session
Online session
Snapshot operations
Local KVM User Interfaces
KVM Web Browser / SSH
Settings GUI / SSH "mcpcfg"
• Admin users
• Firewall, Secure Access
• LAN
• Time Synch
• Redundancy
• Synch Manager
• Hardware
• Database management, factory default, restore clone snapshots
• Edge OS access
USB Port
• Clone Snapshots images
Remote User Interfaces
PC with DSAS MCP Studio installed
Web Browser / SSH
Settings GUI / SSH "mcpcfg"
• Admin users
• Firewall, Secure Access
• LAN
• Time Synch
• Redundancy
• Synch Manager
• Hardware
• Database management, factory default, restore clone snapshots
• Edge OS access
DSAS GUI
HDD Storage
(snapshot).DS7zip
DSAS Repository


MCP (G100/G500)
Data areas and content
ACCESS SETTINGS
Authentication mode (Local/Remote)
HMI Users, autologon
VPN Client Lists
Certificates, keys
ONLINE session
Local KVM User Interfaces
Local KVM runtime HMI
Settings
Authentication mode (Local/Remote)
HMI Users, autologon
VPN Client Lists
Remote User Interfaces
PC with DSAS MCP Studio installed
DSAS GUI
ONLINE Configuration
Authentication mode (Local/Remote)
HMI Users, autologon
VPN Client Lists
Certificate utilities
ONLINE session
Snapshot operations
ONLINE session
DSAS GUI
Remote runtime HMI
Settings
Authentication mode (Local/Remote)
HMI Users, autologon
VPN Client Lists
HDD Storage
(snapshot).DS7zip
DSAS Repository


MCP (G100/G500)
Data areas and content
General Settings
• Firewall, Secure Access
• Time Synch
• Redundancy
• Synch Manager
• Hardware
Admin users
LAN Settings
• Authentication mode (Local/Remote)
• HMI Users, autologon
• VPN Client Lists
Gateway Configuration
• DCA/DTA/DPA, HAMA
• Alarm Management
• HMI Screens
• PLC Automation (Calculator, LogicLinx)
• ARRM
• Reports
MCP CLONE
Local KVM User Interfaces
Online session
KVM Web Browser / SSH
Settings GUI / SSH "mcpcfg"
• Restore clone snapshots
USB Port
• Firmware images
• Clone Snapshots images
Remote User Interfaces
PC with DSAS MCP Studio installed
ONLINE session
Web Browser / SSH
Settings GUI / SSH "mcpcfg"
• Restore clone snapshots
Clone Snapshot operations
DSAS GUI
HDD Storage
(snapshot).DS7zip
DSAS Repository

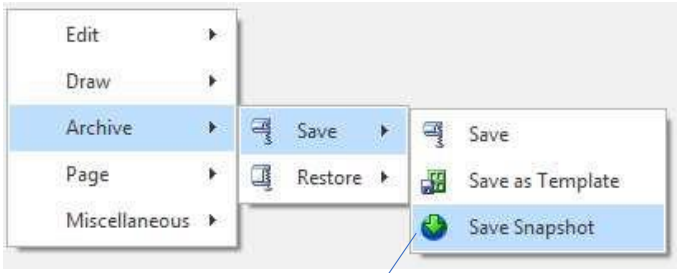
Save Standard Snapshot Workflow

This creates a file that contains selected settings and configuration of the live MCP

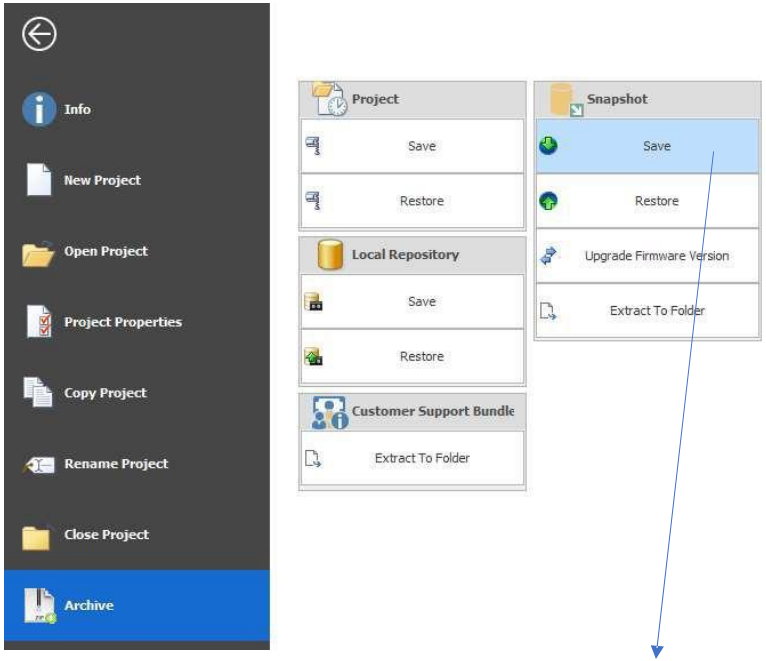
Start workflow:

From Ribbon, Archive:

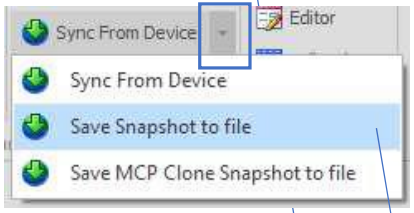
From Right click in a project space:



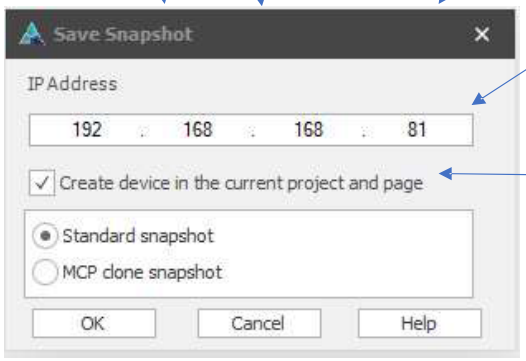
From File > Archive menu:



From Ribbon, Synch From:

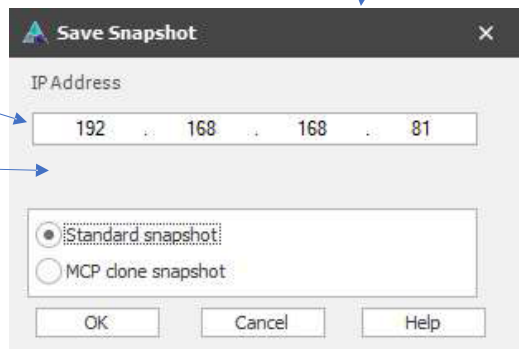


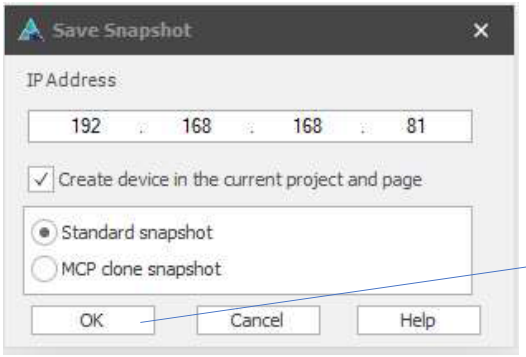
Enter IP address of live device



The option to create an offline device is not present because the workflow started outside of a Project context.

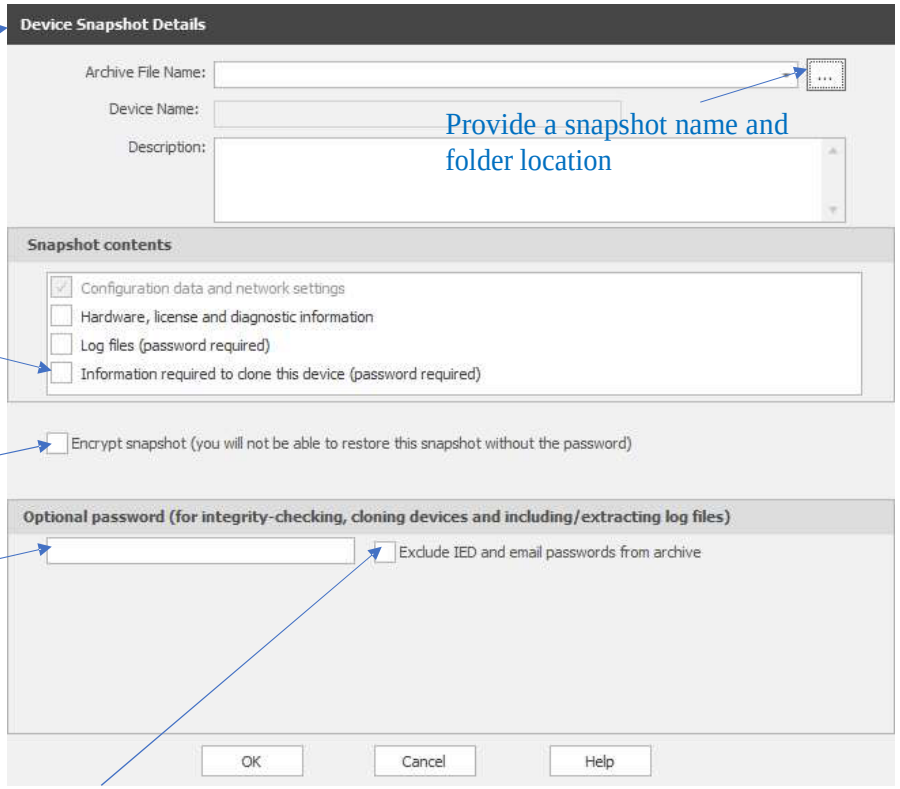
All else is identical to workflow started within a Project.





Creating a **Standard** Snapshot comes with various options to include/exclude information from the live device – see the tooltip explanations.

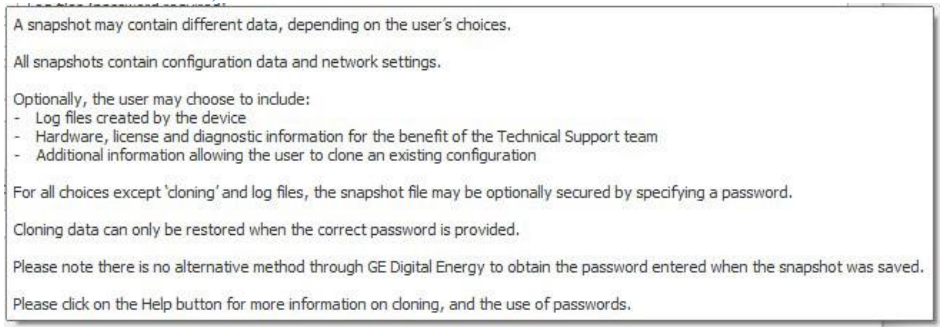
Internal "secrets" are for e.g. internally configured IED passwords, ARRM passwords, email server credentials, etc.



The live device's own user data and credentials are saved only if the clone checkbox is selected.

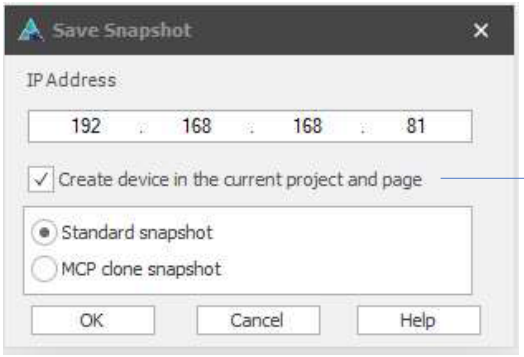
User has an option to encrypt the entire snapshot if this checkbox is selected.
If left clear – only existing "secrets" shall be encrypted, and if such "secrets" are present in the live device.
If the standard snapshot is **encrypted** and the snapshot password is lost, NOTHING from this snapshot can be restored!

This is the password associated with the created snapshot.
The password becomes mandatory if the snapshot contains confidential data (device's own users, internal "secrets")

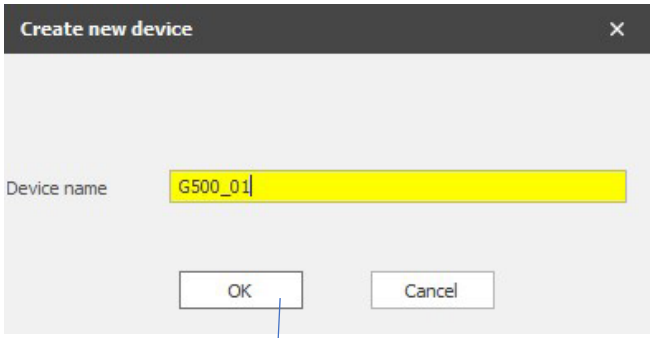


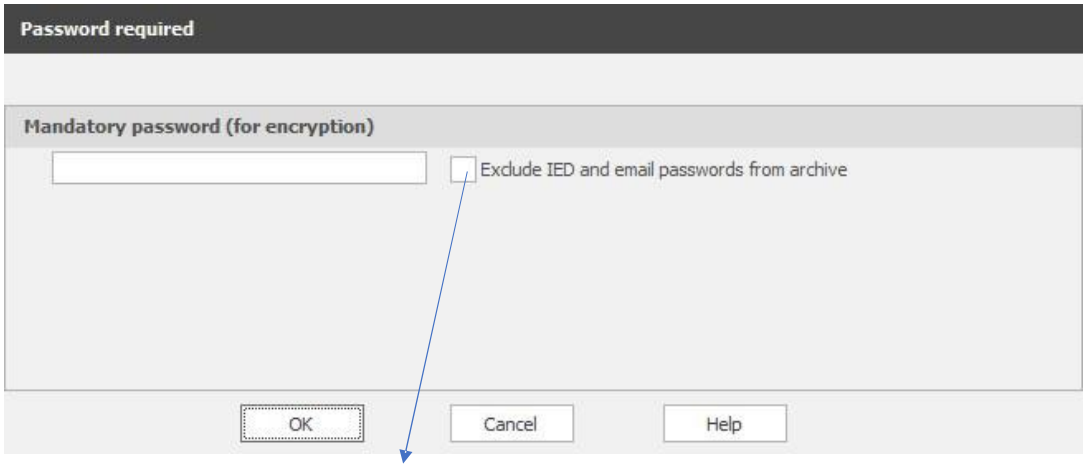
If the live device contains internal "secrets" – the user has an option to exclude these from the snapshot.

This is useful when the resulting snapshot is being handled by 3rd party entities / vendors who cannot be in possession of the IED passwords.



If this checkbox was selected, after the snapshot has been saved, user will be prompted to enter a Device Name for the device offline creation.

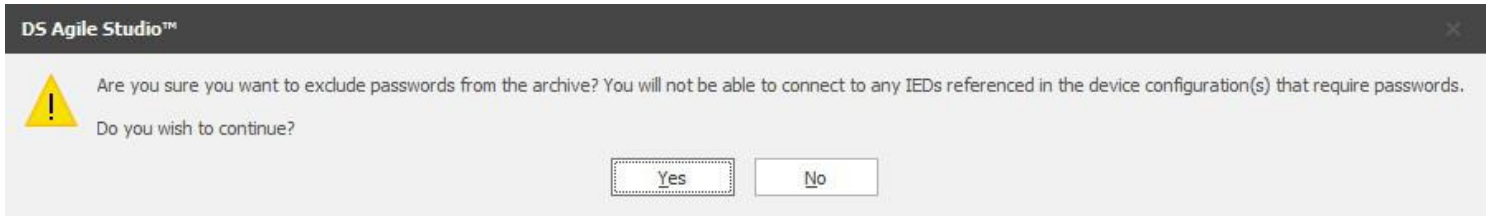




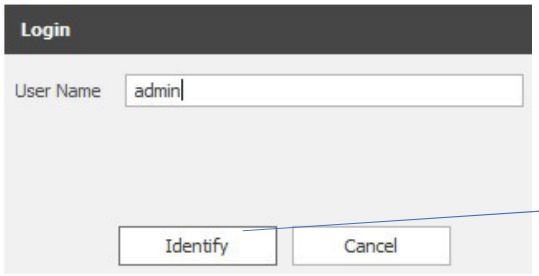
In this case, the live device contains internal "secrets" – and the user chose to **exclude** these from the snapshot.

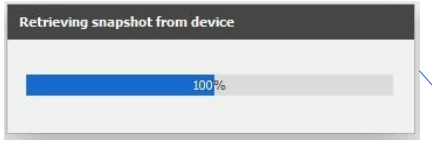
The resulting snapshot (and offline device if selected to be created) are void of any "secrets" that were configured in the live device.

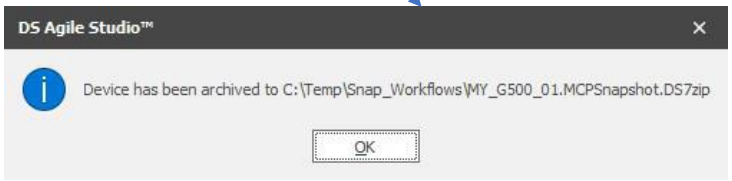
If an optional password was applied, and this password is lost - the non-clone Settings and Configuration data can still be restored, but the anti-tampering data at rest confidence cannot be verified.



Enter the live device's administrator credentials (must use administrator role)

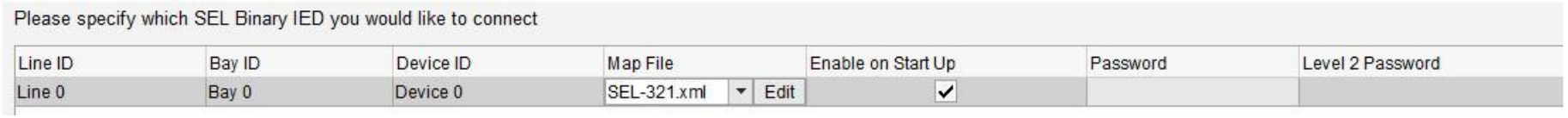


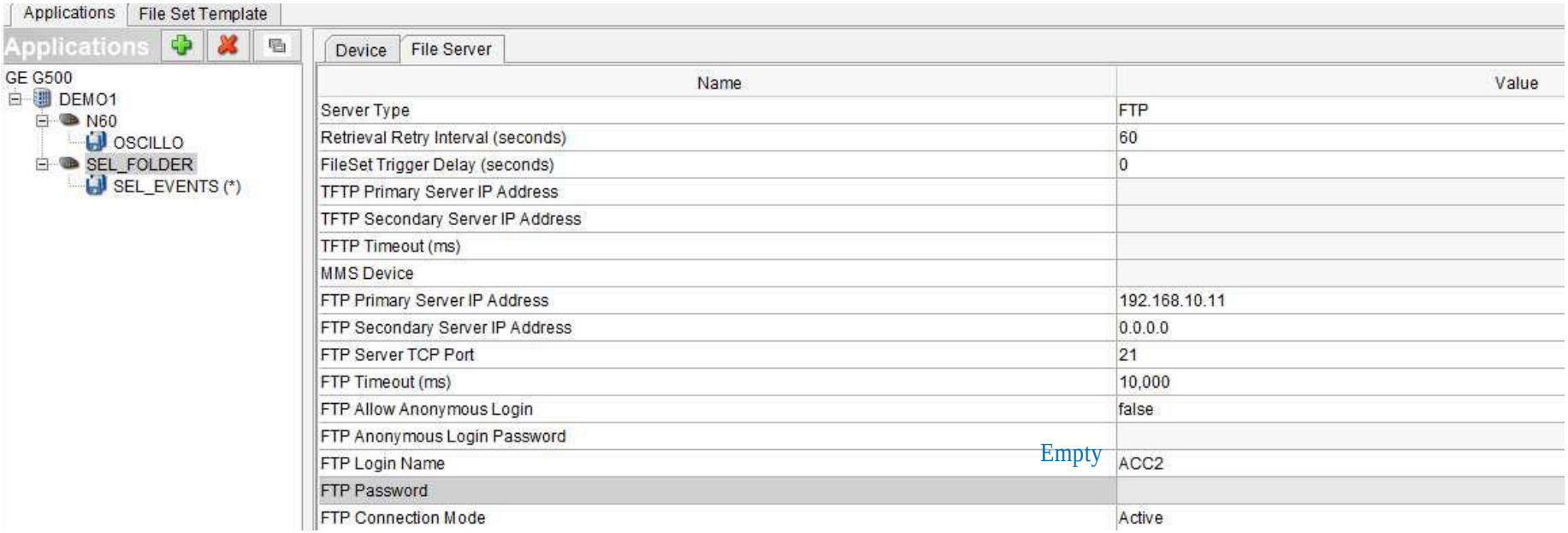


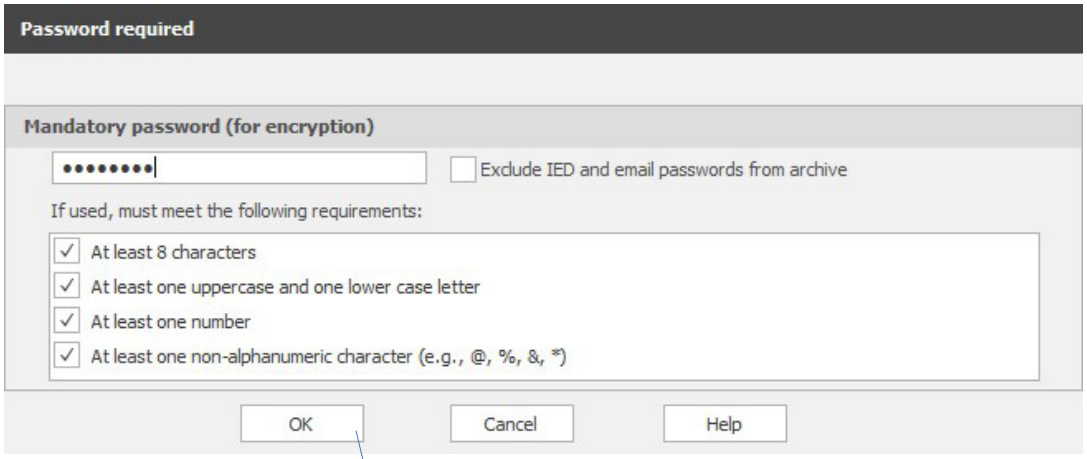


Offline devices do NOT contain credentials for the users in the live device (only snapshots do, and only if the "clone" option has been selected).

The resulting offline device (if selected to be created) has no "secrets":







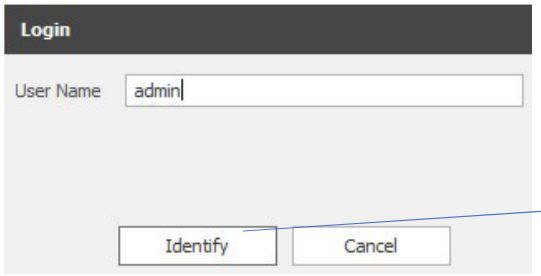
In this case, the live device contains internal "secrets" – and the user chose to include these in the snapshot.
The password is now mandatory, and is used to encrypt the secrets.

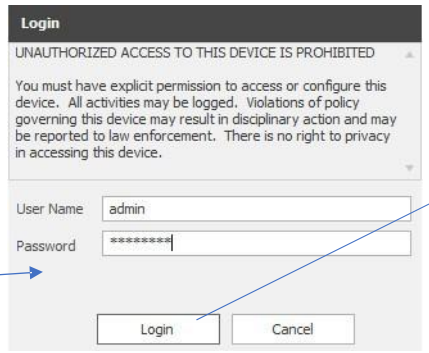
The resulting snapshot (and offline device if selected to be created) contains all secrets from the live device.

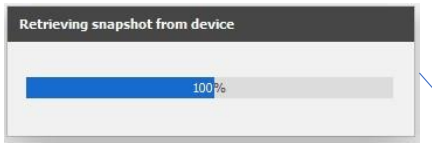
If the standard snapshot was **encrypted** and the snapshot password is lost, NOTHING from this snapshot can be restored!

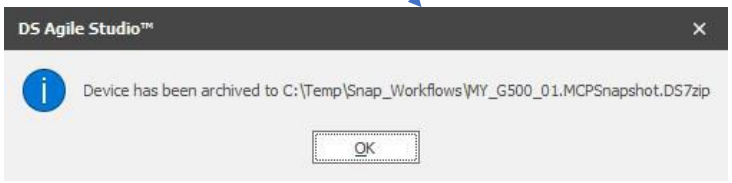
If the standard snapshot was not encrypted, but still protected with a password for the clone and secrets data – if snapshot password is lost only the clone data and secrets are lost.
The remaining Settings and Configuration data can still be restored.

Enter the live device's administrator credentials (must use administrator role)





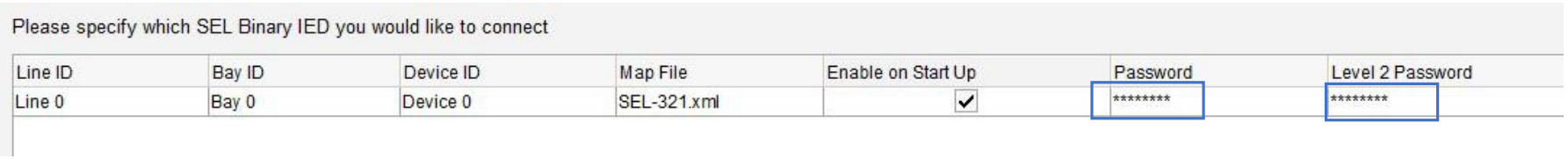


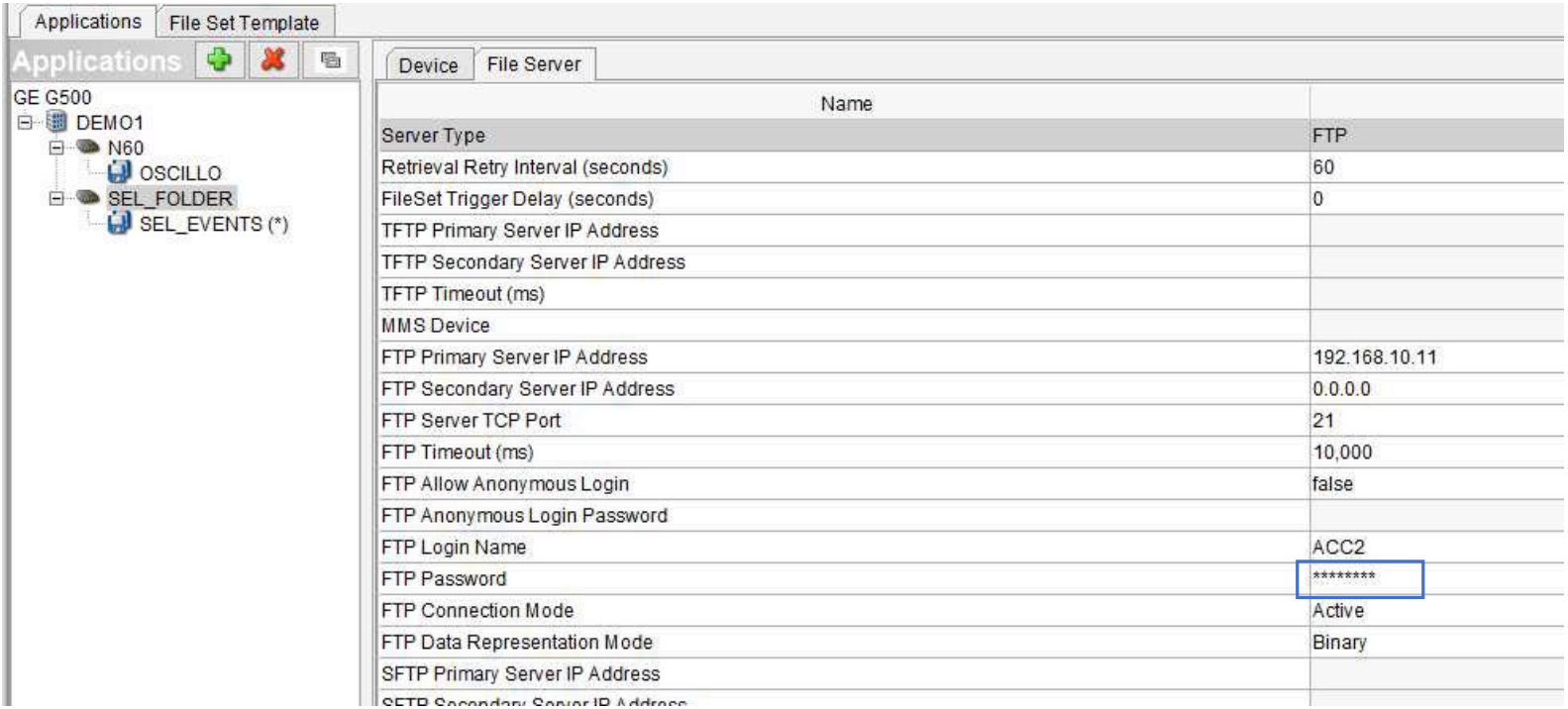


Offline devices do NOT contain credentials for the users in the live device (only snapshots do, and only if the "clone" option has been selected).

The resulting offline device (if selected to be created) retains all "secrets" from the live device, but these can only be used to connect to the specific IEDs.

User cannot read back any secrets (and these are securely stored inside DSAS repository).





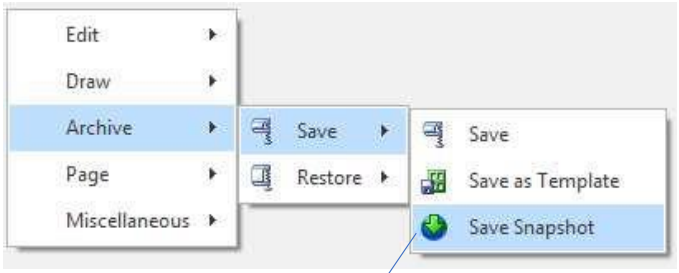
Save MCP Clone Snapshot Workflow (used also for Firmware Upgrade)

This creates a file that contains
all settings, users, and configuration of the live MCP

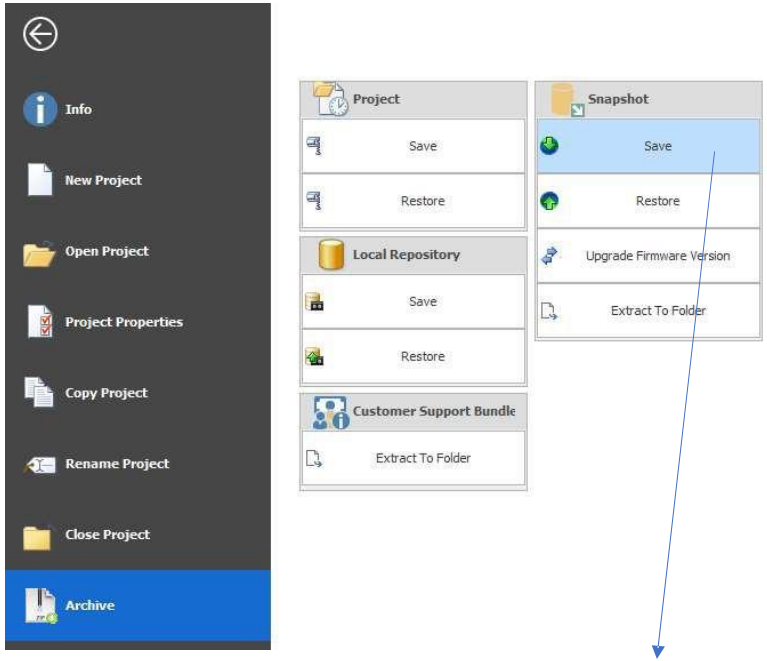
Start workflow:

From Ribbon, Archive:

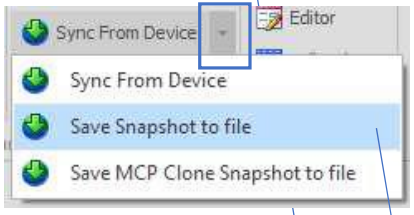
From Right click in a project space:



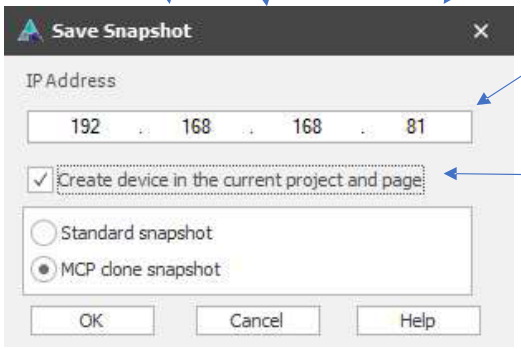
From File > Archive menu:



From Ribbon, Synch From:

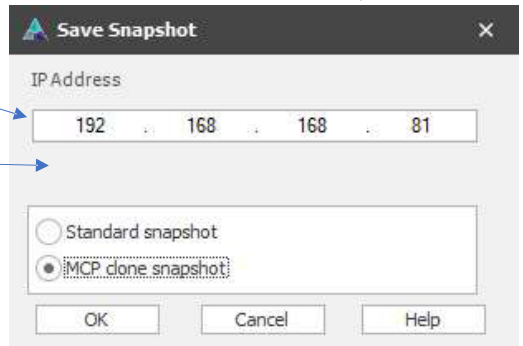


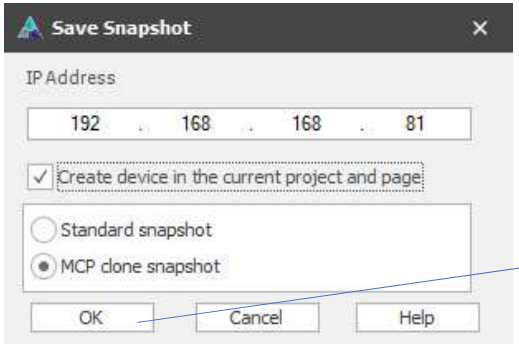
Enter IP address of live device



The option to create an offline device is not present because the workflow started outside of a Project context.

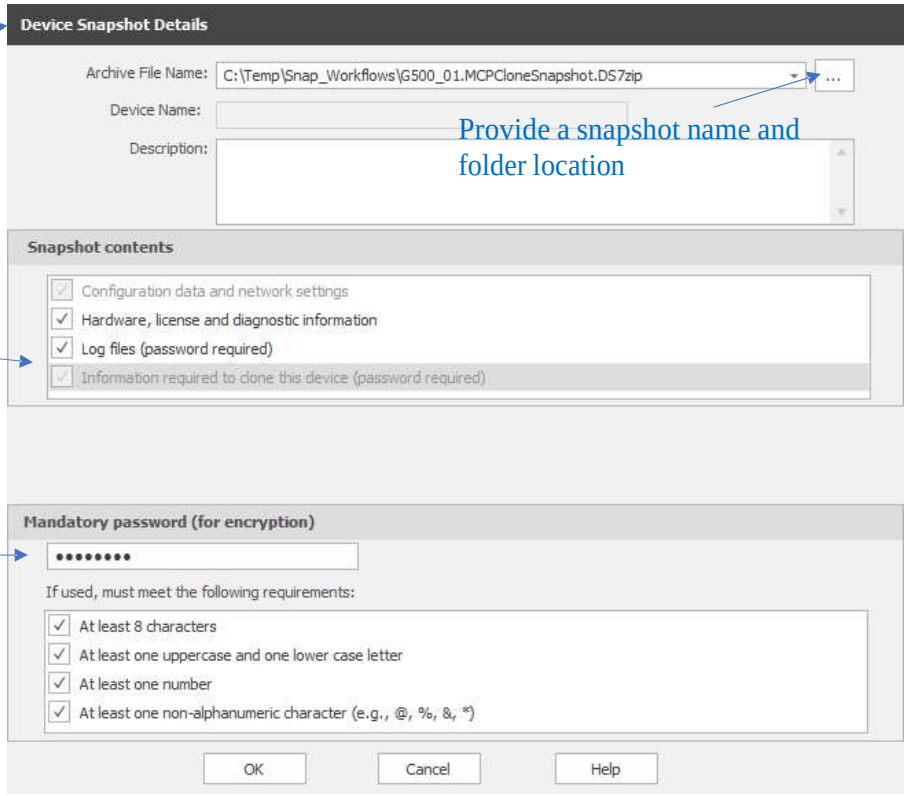
All else is identical to workflow started within a Project.





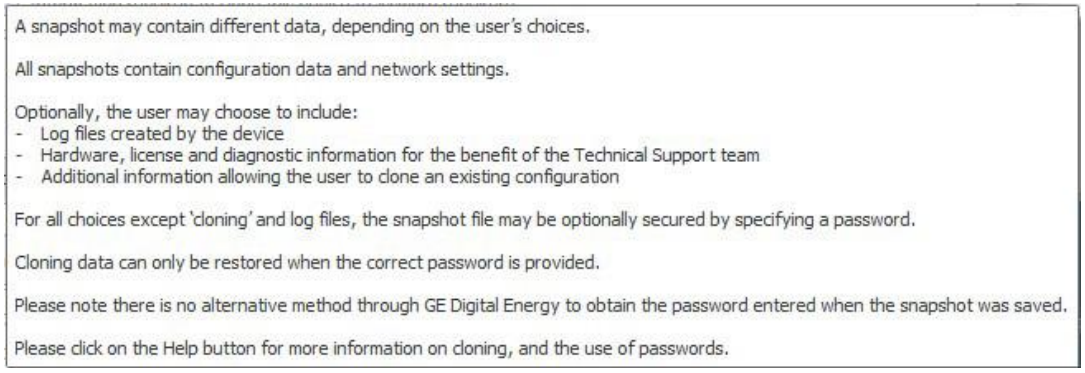
Creating a MCP Clone Snapshot comes with various options to include/exclude information from the live device (HW, License, Logs).

Internal "secrets" are for e.g. internally configured IED passwords, ARRM passwords, email server credentials, etc.

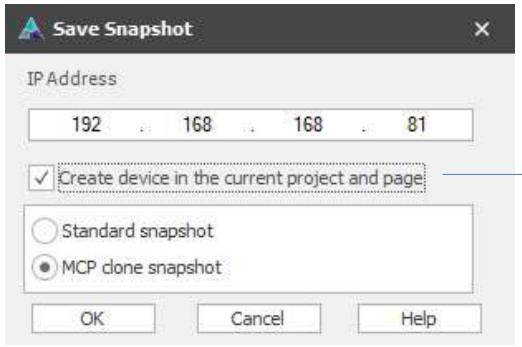


The live device's own user data and credentials, and all internal "secrets" are always part of an MCP Clone snapshot.

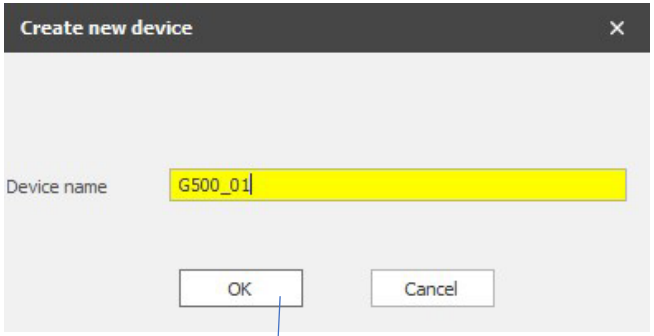
The MCP Clone snapshot is always encrypted using this password.
If the snapshot password is lost, NOTHING from this snapshot can be restored!

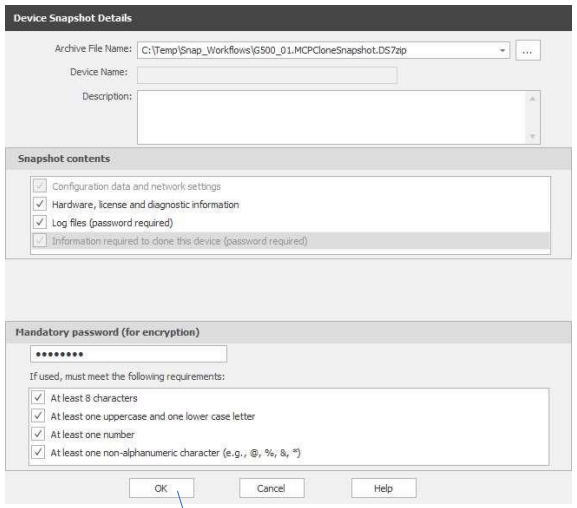


There is no option to exclude "secrets" from the MCP Clone snapshot.



If this checkbox was selected, after the snapshot has been saved, user will be prompted to enter a Device Name for the device offline creation.

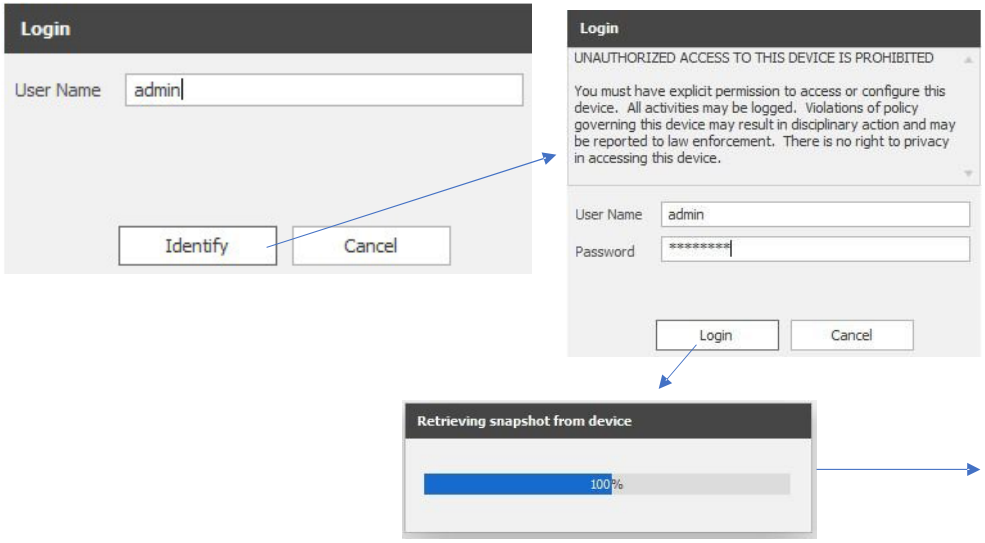




The MCP Clone snapshot (and offline device if selected to be created) contains all live device's user confidential data and secrets, and is protected with the user provided strong password.

If the MCP Clone snapshot password is lost, NOTHING from this snapshot can be restored!

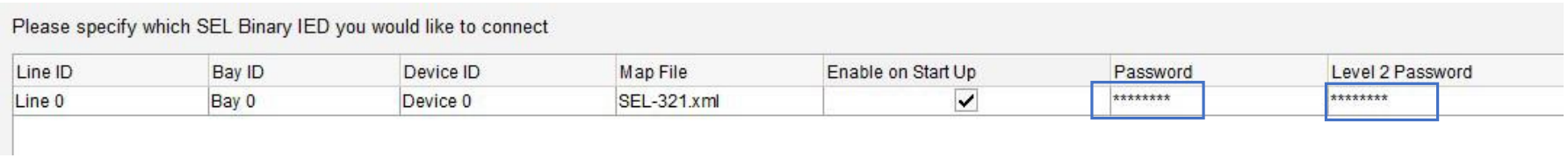
Enter the live device's administrator credentials (must use administrator role)

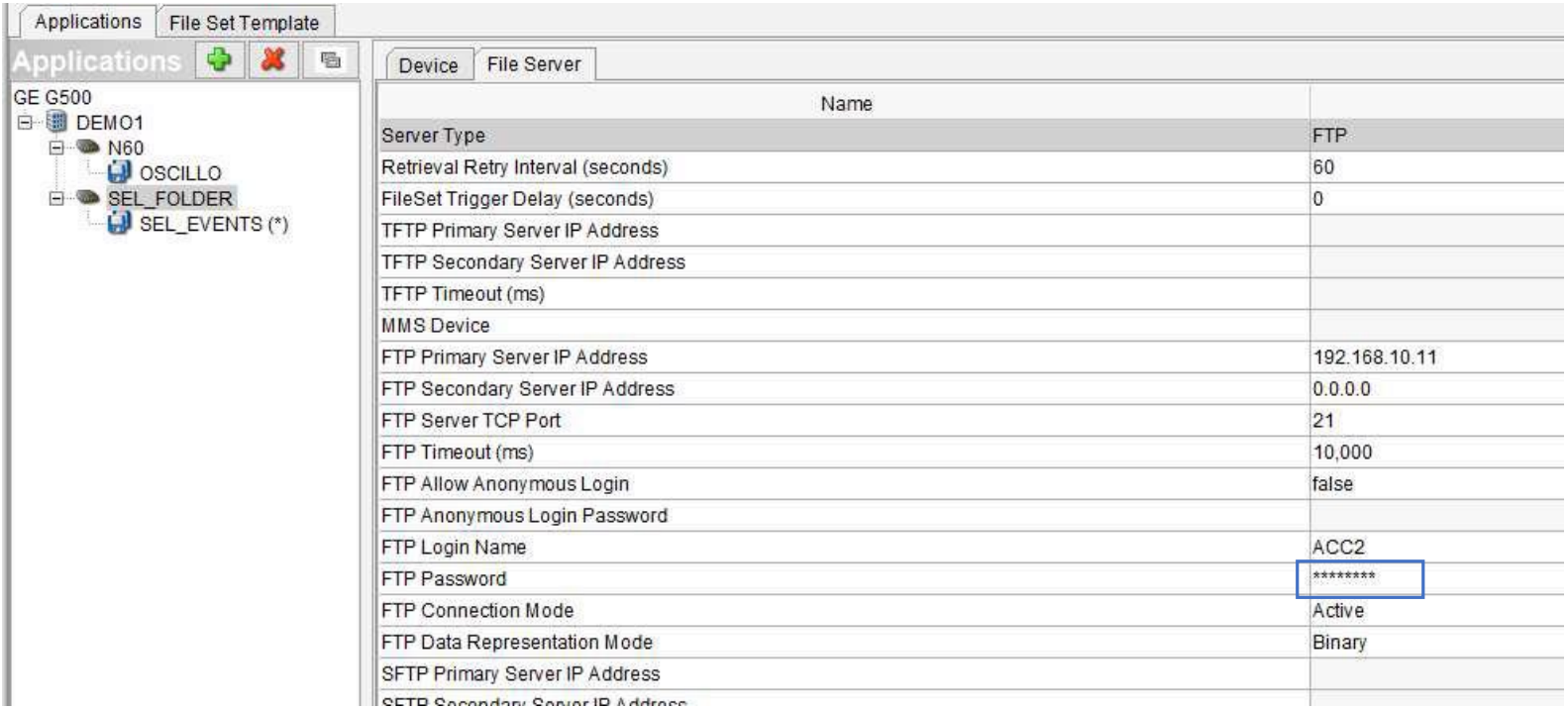


Offline devices do NOT contain credentials for the users in the live device (only snapshots do, and only if the "clone" option has been selected).

The resulting offline device (if selected to be created) retains all "secrets" from the live device, but these can only be used to connect to the specific IEDs.

User cannot read back any secrets (and these are securely stored inside DSAS repository).



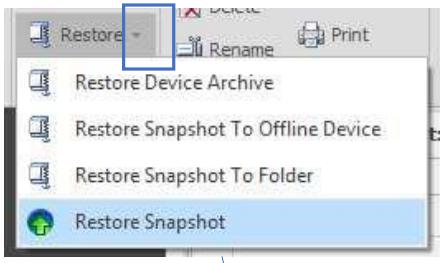


Restore Snapshot to a Live Device Workflow

This restores to a MCP all or selected settings, users, and configuration data from a snapshot file.

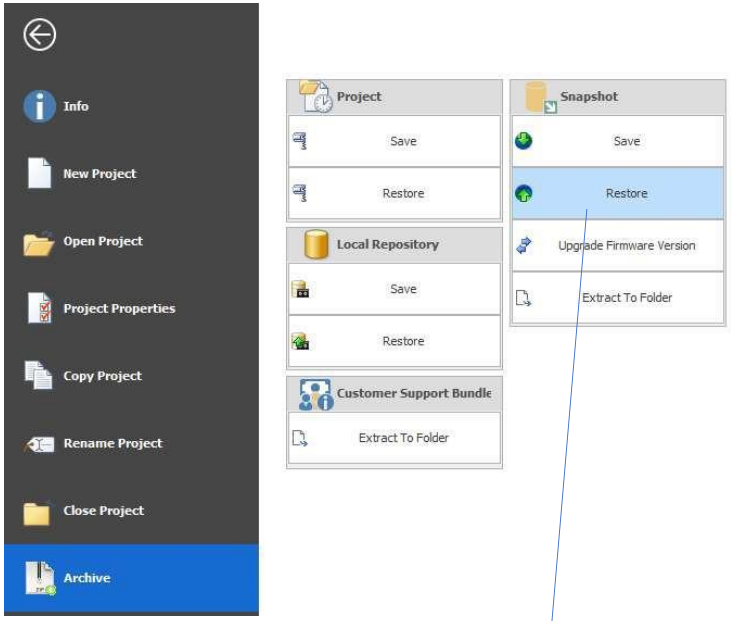
Start workflow:

From Ribbon, Archive:

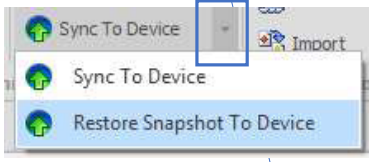


From Right click in a project space:

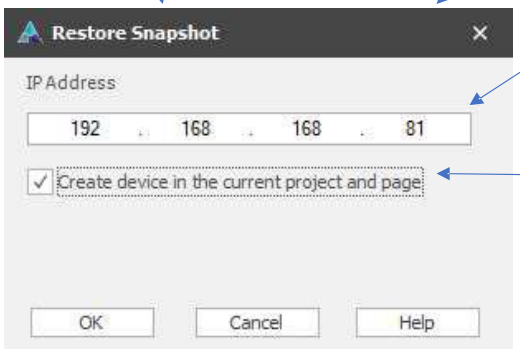
From File > Archive menu:



From Ribbon, Synch To:

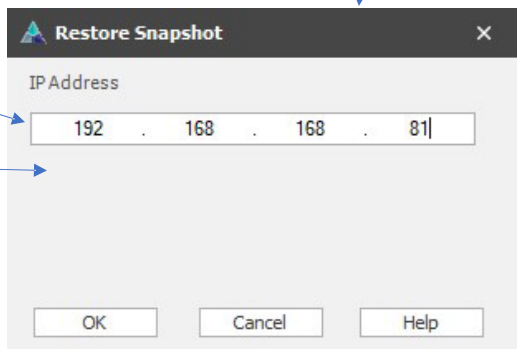


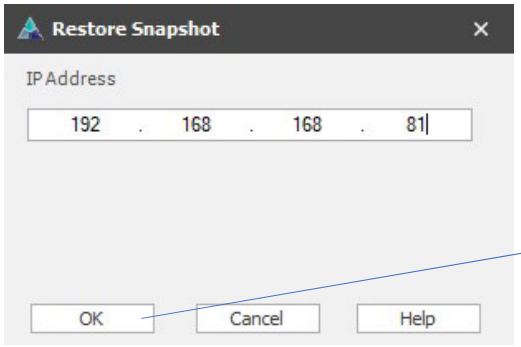
Enter IP address of live device



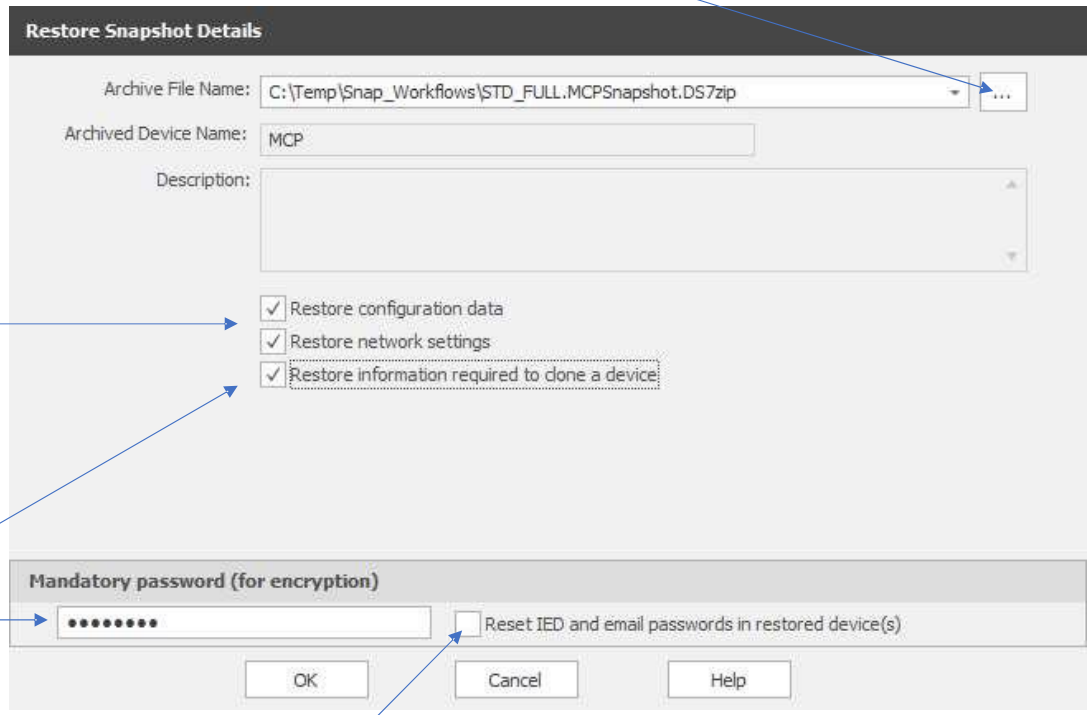
The option to create an offline device is not present because the workflow started outside of a Project context.

All else is identical to workflow started within a Project.





Select the snapshot file to be restored



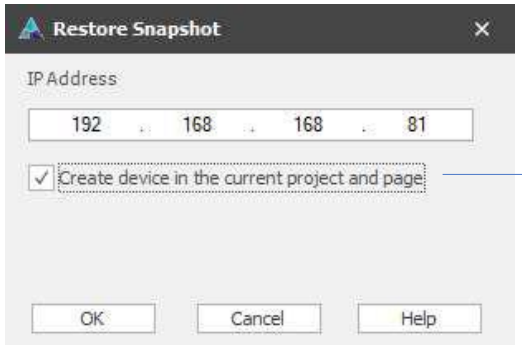
The data options to be restored depend on the type and content of the selected snapshot file.
If various data types were not included in the snapshot file, the associated options will not be visible here.

User has a choice to select what data types to restore.

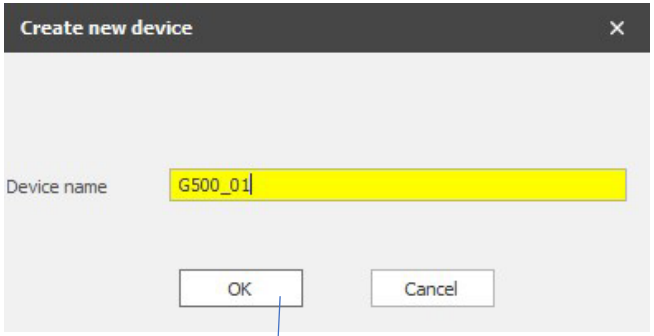
If the snapshot file contains confidential data (users, "secrets"), the snapshot password must be provided for this type of data to be restored.
Otherwise, this data will be excluded from the restore operations.

If the selected snapshot file is of type "MCP Clone", or "Standard and Encrypted", the password associated with the snapshot file must be provided, otherwise NOTHING can be restored!

If the snapshot file contains internal "secrets" – the user has an option to exclude these from the restore operation.



If this checkbox was selected, after the snapshot has been restored, user will be prompted to enter a Device Name for the device offline creation.



Firmware upgrade:

If the live device contains a firmware version higher than the one in the snapshot – the snapshot is first upgraded to the firmware version of the live device, after which is restored to the live device.

In addition in this case, if "create device in current project" checkbox was also selected – the offline device created will also the new firmware version, same as the live device. This is to allow user to have both a restored online device and an offline one that match each other.

Configuration compare:

Optionally, the user may wish to perform workflow "Restore Snapshot to an Offline Device", selecting the same initial snapshot (with the older firmware version) – resulting into a second offline device (with a different name), with the initial firmware version from the snapshot.

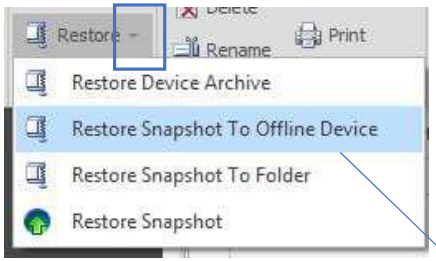
A configuration compare action can then be performed across the two offline devices if desired.

Restore Snapshot to an Offline Device Workflow

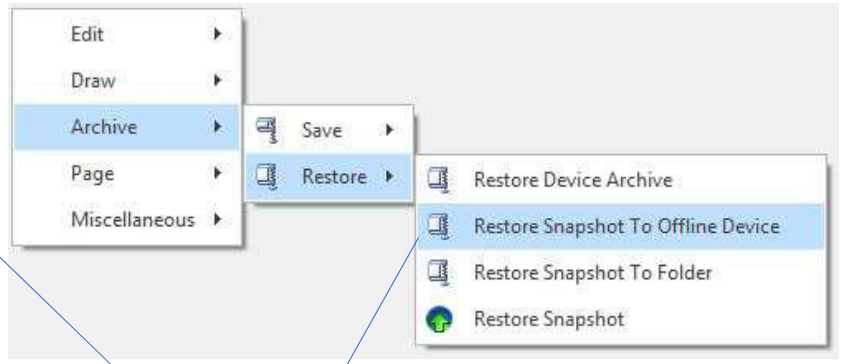
This creates an offline device from a snapshot file (only Configuration data)

Start workflow:

From Ribbon, Archive:



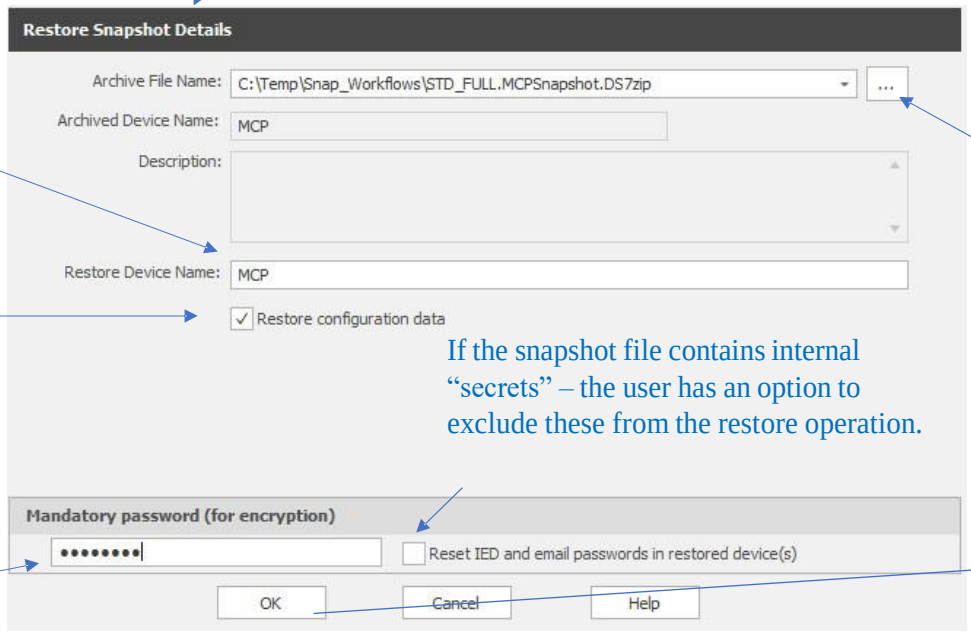
From Right click in a project space:



Enter the Name for the offline device

Only Configuration data can be restored to an offline device

If the snapshot file contains confidential data (“secrets”), the snapshot password must be provided for this type of data to be restored. Otherwise, this data will be excluded from the restore operations.



Select the snapshot file to be restored

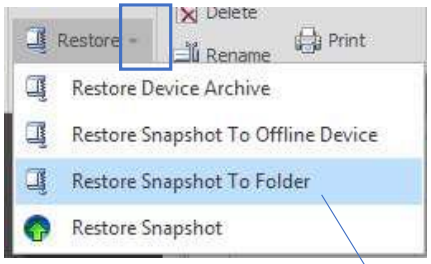
If the snapshot file contains internal “secrets” – the user has an option to exclude these from the restore operation.

Restore Snapshot to a Folder Workflow

This creates an offline Folder with Configuration data from a snapshot file.

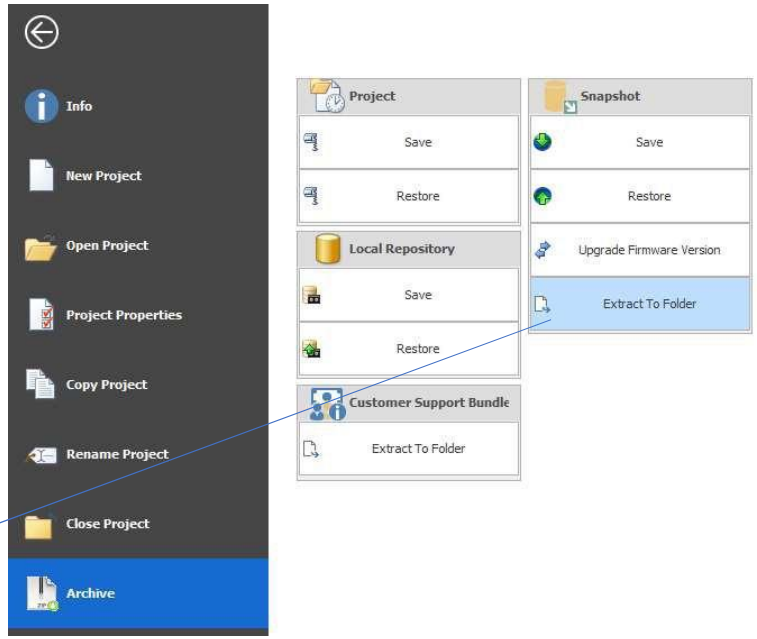
Start workflow:

From Ribbon, Archive:



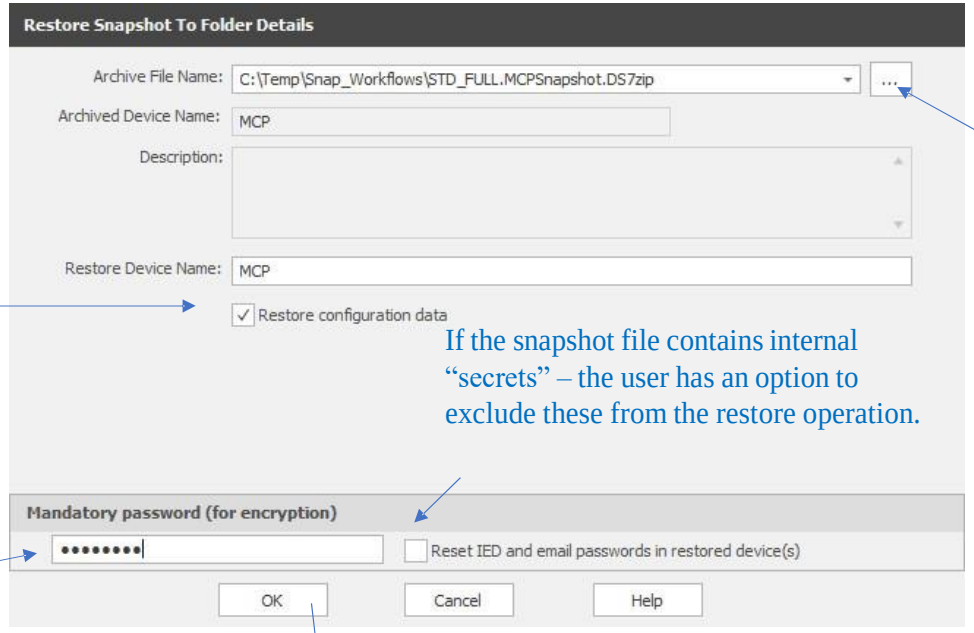
From Right click in a project space:

From File > Archive menu:



See next page

From previous page:



Select the snapshot file to be restored

Only Configuration data can be restored to a Folder

If the snapshot file contains internal "secrets" – the user has an option to exclude these from the restore operation.

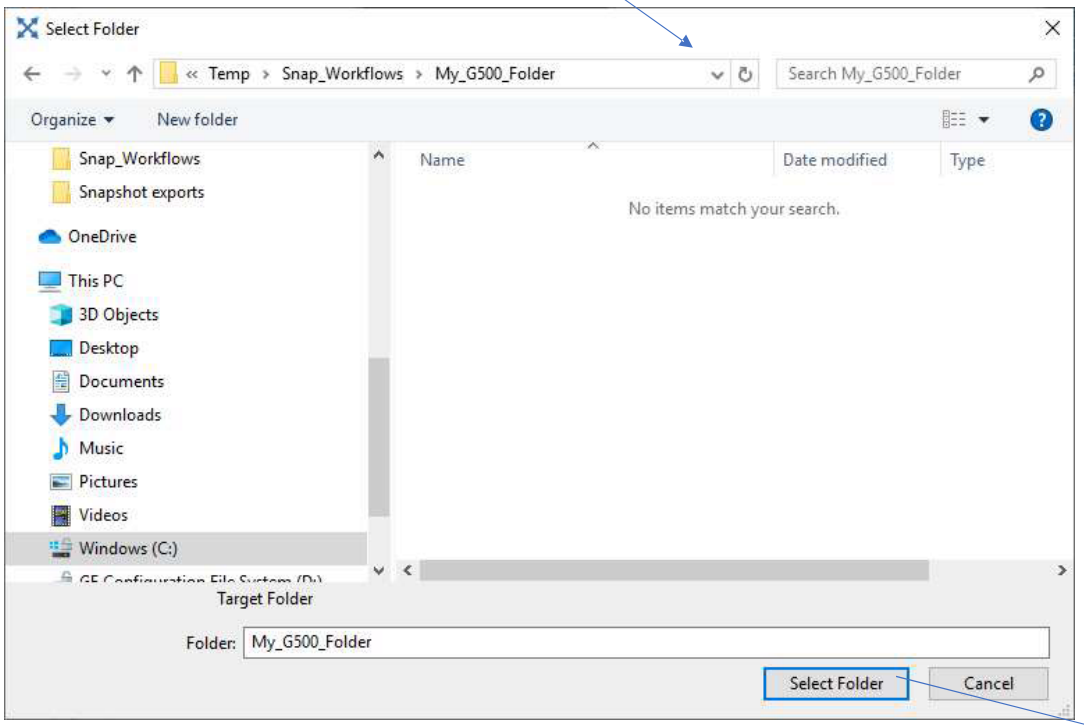
If the snapshot file contains confidential data ("secrets"), the snapshot password must be provided for this type of data to be restored, but will remain encrypted.

Otherwise, this data will be excluded from the restore operations.

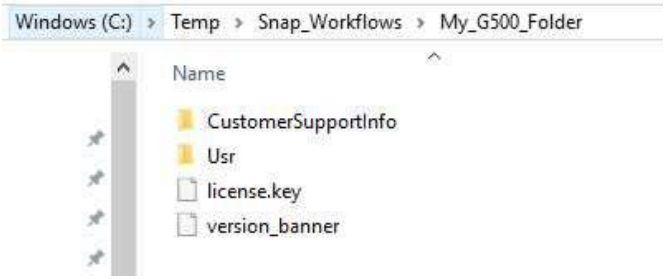
See next page

From previous page:

Select the target folder



Result:



Product Support

If you need help with any aspect of your GE Grid Solutions product, you can:

- Access the GE Grid Solutions Web site
- Search the GE Grid Solutions Technical Support library
- Contact GE Grid Solutions Technical Support

GE Grid Solutions Web Site

The GE Grid Solutions Web site provides fast access to technical information, such as manuals, release notes and knowledge base topics.
Visit us on the Web at: http://www.gegridsolutions.com

GE Grid Solutions Technical Support Library

This site serves as a document repository for post-sales requests. To *get* access to the Technical Support Web site, go to:
http://supportcentral.ge.com/*SASTechSupport
or
http://www.gegridsolutions.com/TDSASSupport

Contact Technical Support

For help with any aspect of your GE Grid Solutions product, please contact our support team, 24/7, as follows:

Region	E-mail	Telephone
Global Contact Centre	ga.support@ge.com	+44 1785 250070
Central and East Asia andPacific	ga.supportCEAP@ge.com	+61 414 730 964
India	ga.supportIND@ge.com	+91 44 22648000
Middle East, North Africa andTurkey	ga.supportMENAT@ge.com	+971 42929467
Europe, Russia, CIS and Sub-Saharan Africa	ga.supportERCIS@ge.com	+34 94 4858854
North America	ga.supportNAM@ge.com	+1 877 605 6777
Latin America	ga.supportLAM@ge.com	+55 11 36187308

Copyright Notice

© 2021, General Electric Company. All rights reserved.

The information contained in this online publication is the exclusive property of General Electric Company, except as otherwise indicated. You may view, copy and print documents and graphics incorporated in this online publication (the "Documents") subject to the following: (1) the Documents may be used solely for personal, informational, non-commercial purposes; (2) the Documents may not be modified or altered in any way; and (3) General Electric Company withholds permission for making the Documents or any portion thereof accessible via the internet. Except as expressly provided herein, you may not use, copy, print, display, reproduce, publish, license, post, transmit or distribute the Documents in whole or in part without the prior written permission of General Electric Company. If applicable, any use, modification, reproduction, release, performance, display, or disclosure of the Software Product and Associated Material by the U.S. Government shall be governed solely by the terms of the License Agreement and shall be prohibited except to the extent expressly permitted by the terms of the License Agreement.

The information contained in this online publication is subject to change without notice. The software described in this online publication is supplied under license and may be used or copied only in accordance with the terms of such license.

Trademark Notice

GE and the GE monogram are trademarks and service marks of General Electric Company.

* Trademarks of General Electric Company.

Other company or product names mentioned in this document may be trademarks or registered trademarks of their respective companies.

Modification Record

Version	Revision	Date	Change Description
1.00	0	April 22nd, 2020	Initial release.
2.00	0	April 14th, 2021	Updated for MCP family.
2.00	1	April 23rd , 2021	Updated Technical Support Contacts.

GE

Grid Solutions

Open Source Components

Licensing Information

The software included in this product contains copyrighted software that is licensed under the GPL and other open source licenses.

A copy of each of these licenses is included in this document. You may obtain the complete corresponding source code from us for a period of three years after our last shipment of this product, by contacting the GE Customer Service Center.

In the U.S. and Canada, call toll-free: 1 877 547 8629

International customers, please call: +1 905 927 7070

Or send an e-mail to: multilin.tech@ge.com

This offer is valid to anyone in receipt of this information.

NOTICE This document applies to the MCP family (G100/G500) unless otherwise indicated.

The document lists all open source software licenses used in the MCP Version 2.3.

The MCP also includes GE's Predix Edge OS (PEOS) and standard distributions of Debian and Ubuntu. The list of packages inherited from these distributed are captured in their respective folders from the MCP Product CD (PEOS, Debian and Ubuntu).

The MCP also uses a standard distribution of Arch Linux with the MCP Utilities Package. The list of packages inherited from the Arch Linux distribution is captured on a USB flash drive created by DS Agile Studio in the file “pkglist.x86_64.txt” under the folder “fwupgutil”. The licenses for the packages are captured in the folder “/usr/share/” in the squash file archive found on the same USB flash drive in the file “airootfs.sfs”, under the folder “fwupgutil/x86_64”.

GNU General Public License | Version 1, Febrauary 1989

- Perl modules version 1.00 are licensed *under GPL v1* License category.

GPL v1 License

GNU GENERAL PUBLIC LICENSE

Version 1, February 1989

Copyright (C) 1989 Free Software Foundation, Inc.

51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies

of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Library General Public License, applies to some specially designated Free Software Foundation software, and to any other libraries whose authors decide to use it. You can use it for your libraries, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library, or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link a program with the library, you must provide complete object files to the recipients so that they can relink them with the library, after making changes to the library and recompiling it. And you must show them these terms, so they know their rights.

Our method of protecting your rights has two steps:

(1) copyright the library, and

(2) offer you this license which gives you legal permission to copy, distribute and/or modify the library.

Also, for each distributor's protection, we want to make certain that everyone understands that there is no warranty for this free library. If the library is modified by someone else and passed on, we want its recipients to know that what they have is not the original version, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that companies distributing free software will individually obtain patent licenses, thus in effect transforming the program into proprietary software. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License, which was designed for utility programs. This license, the GNU Library General Public License, applies to certain designated libraries. This license is quite different from the ordinary one; be sure to read it in full, and don't assume that anything in it is the same as in the ordinary license.

The reason we have a separate public license for some libraries is that they blur the distinction we usually make between modifying or adding to a program and simply using it. Linking a program with a library, without changing the library, is in some sense simply using the library, and is analogous to running a utility program or application program. However, in a textual and

legal sense, the linked executable is a combined work, a derivative of the original library, and the ordinary General Public License treats it as such.

Because of this blurred distinction, using the ordinary General Public License for libraries did not effectively promote software sharing, because most developers did not use the libraries. We concluded that weaker conditions might promote sharing better.

However, unrestricted linking of non-free programs would deprive the users of those programs of all benefit from the free status of the libraries themselves. This Library General Public License is intended to permit developers of non-free programs to use free libraries, while preserving your freedom as a user of such programs to change the free libraries that are incorporated in them. (We have not seen how to achieve this as regards changes in header files, but we have achieved it as regards changes in the actual functions of the Library.) The hope is that this will lead to faster development of free libraries.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, while the latter only works together with the library.

Note that it is possible for a library to be covered by the ordinary General Public License rather than by this special one.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0) This License Agreement applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any work containing the Program or a portion of it, either verbatim or with modifications. Each licensee is addressed as "you".

1) You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this General Public License and to the absence of any warranty; and give any other recipients of the Program a copy of this General Public License along with the Program. You may charge a fee for the physical act of transferring a copy.

2) You may modify your copy or copies of the Program or any portion of it, and copy and distribute such modifications under the terms of Paragraph1 above, provided that you also do the following:

   a. cause the modified files to carry prominent notices stating that you changed the files and the date of any change; and

   b. cause the whole of any work that you distribute or publish, that in whole or in part contains the Program or any part thereof, either with or without modifications, to be licensed at no charge to all third parties under the terms of this General Public License (except that you may choose to grant warranty protection to some or all third parties, at your option).

   c. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the simplest and most usual way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this General Public License.

   d. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee. Mere aggregation of another independent work with the Program (or its derivative) on a volume of a storage or distribution medium does not bring the other work under the scope of these terms.

3) You may copy and distribute the Program (or a portion or derivative of it, under Paragraph 2) in object code or executable form under the terms of Paragraphs 1 and 2 above provided that you also do one of the following:

   a. accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Paragraphs 1 and 2 above; or,

b. accompany it with a written offer, valid for at least three years, to give any third party free (except for a nominal charge for the cost of distribution) a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Paragraphs 1 and 2 above; or,

c. accompany it with the information you received as to where the corresponding source code may be obtained. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form alone.)

Source code for a work means the preferred form of the work for making modifications to it. For an executable file, complete source code means all the source code for all modules it contains; but, as a special exception, it need not include source code for modules which are standard libraries that accompany the operating system on which the executable file runs, or for standard header files or definitions files that accompany that operating system.

4) You may not copy, modify, sublicense, distribute or transfer the Program except as expressly provided under this General Public License. Any attempt otherwise to copy, modify, sublicense, distribute or transfer the Program is void, and will automatically terminate your rights to use the Program under this License. However, parties who have received copies, or rights to use copies, from you under this General Public License will not have their licenses terminated so long as such parties remain in full compliance.

5) By copying, distributing or modifying the Program (or any work based on the Program) you indicate your acceptance of this license to do so, and all its terms and conditions.

6) Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein.

7) The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of the license which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the license, you may choose any version ever published by the Free Software Foundation.

8) If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

9) BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

10) IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs:

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990

Ty Coon, President of Vice

That's all there is to it!

GNU General Public License | Version 2, June 1991

- stunnel version 5.57, socat version 1.7.3.1,pam_tacplus and pam-ldap version 186 and postgres version 13.1 are licensed *under GPL v2* License category.

GPL v2 License

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0) This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents

constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1) You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2) You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

      These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

      Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

      In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3) You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4) You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5) You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6) Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7) If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

   If any portion of this section is held invalid or unenforceable under any circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

   It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

   This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8) 8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9) 9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version but may differ in detail to address new problems or concerns.

   Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that

version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10) 10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11) 11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12) 12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the program's name and an idea of what it does.

Copyright (C) yyyy name of author

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License

along with this program; if not, write to the Free Software

Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright

interest in the program `Gnomovision'

(which makes passes at compilers) written by James Hacker.

signature of Ty Coon, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

GNU General Public License | Version 3, 29 June 2007

- inetutils version 1.9.4 and rsync version 3.2.3 are licensed under *GPL v3 License category*

GPL v3 License

Copyright © 2007 Free Software Foundation, Inc. <https://fsf.org/>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0) Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1) Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2) Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3) Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4) Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5) Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to “keep intact all notices”.

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an “aggregate” if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6) Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge) and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A “User Product” is either (1) a “consumer product”, which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, “normally used” refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

“Installation Information” for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form) and must require no special password or key for unpacking, reading or copying.

7) Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8) Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9) Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10) Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An “entity transaction” is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11) Patents.

A “contributor” is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's “contributor version”.

A contributor's “essential patent claims” are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, “control” includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a “patent license” is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To “grant” such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. “Knowingly relying” means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12) No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13) Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14) Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15) Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE

OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16) Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTYL WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17) Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of

MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see https://www.gnu.org/licenses/.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>

This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, your program's commands might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school, if any, to sign a "copyright disclaimer" for the program, if necessary. For more information on this, and how to apply and follow the GNU GPL, see https://www.gnu.org/licenses/.

The GNU General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you

want to do, use the GNU Lesser General Public License instead of this License. But first, please read https://www.gnu.org/licenses/why-not-lgpl.html.

GNU Lesser General Public License | Version 2.1, Febrauary 1999

- libssh version 0.9.5, is licensed under *LGPL v2.1*.

GNU Lesser General Public License Version 2.1

Copyright © 2007 Free Software Foundation, Inc. https://fsf.org/

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General Public License, supplemented by the additional permissions listed below.

1) Additional Definitions.

   As used herein, "this License" refers to version 3 of the GNU Lesser General Public License, and the "GNU GPL" refers to version 3 of the GNU General Public License.

   "The Library" refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

   An "Application" is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library. Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.

   A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

   The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

   The "Corresponding Application Code" for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

2) Exception to Section 3 of the GNU GPL.

   You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

3) Conveying Modified Versions.

   If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

   a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

   b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

4) Object Code Incorporating Material from Library Header Files.

   The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

a. Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

b. Accompany the object code with a copy of the GNU GPL and this license document.

5) Combined Works.

You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:

1. Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.
2. Accompany the Combined Work with a copy of the GNU GPL and this license document.
3. For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.
4. Do one of the following:
    1. Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.
    2. Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.
5. Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

6) Combined Libraries.

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a. Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

b. Give prominent notice with the combined library that part of it is a work based on the Library and explaining where to find the accompanying uncombined form of the same work.

1. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License “or any later version” applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

GNU Library| Lesser General Public License

- qpthread version 1.1, libnss-ldap version 265 and argtable version 2.9 are licensed under *LGPL or GNU Library GPL License Category.*

GNU Library | Lesser General Public License

GNU LIBRARY GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1991 Free Software Foundation, Inc.

675 Mass Ave, Cambridge, MA 02139, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the library GPL. It is numbered 2 because it goes with version 2 of the ordinary GPL.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Library General Public License, applies to some specially designated Free Software Foundation software, and to any other libraries whose authors decide to use it. You can use it for your libraries, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library, or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link a program with the library, you must provide complete object files to the recipients so that they can relink them with the library, after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

Our method of protecting your rights has two steps:

(1) copyright the library, and

(2) offer you this license which gives you legal permission to copy, distribute and/or modify the library.

Also, for each distributor's protection, we want to make certain that everyone understands that there is no warranty for this free library. If the library is modified by someone else and passed on, we want its recipients to know that what they have is not the original version, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that companies distributing free software will individually obtain patent licenses, thus in effect transforming the program into proprietary software. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License, which was designed for utility programs. This license, the GNU Library General Public License, applies to certain designated libraries. This license is quite different from the ordinary one; be sure to read it in full, and don't assume that anything in it is the same as in the ordinary license.

The reason we have a separate public license for some libraries is that they blur the distinction we usually make between modifying or adding to a program and simply using it. Linking a program with a library, without changing the library, is in some sense simply using the library, and is analogous to running a utility program or application program. However, in a textual and legal sense, the linked executable is a combined work, a derivative of the original library, and the ordinary General Public License treats it as such.

Because of this blurred distinction, using the ordinary General Public License for libraries did not effectively promote software sharing, because most developers did not use the libraries. We concluded that weaker conditions might promote sharing better.

However, unrestricted linking of non-free programs would deprive the users of those programs of all benefit from the free status of the libraries themselves. This Library General Public License is intended to permit developers of non-free programs to use free libraries, while preserving your freedom as a user of such programs to change the free libraries that are incorporated in them. (We have not seen how to achieve this as regards changes in header files, but we have achieved it as regards changes in the actual functions of the Library.) The hope is that this will lead to faster development of free libraries.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, while the latter only works together with the library.

Note that it is possible for a library to be covered by the ordinary General Public License rather than by this special one.

GNU LIBRARY GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a. The modified work must itself be a software library.

   b. You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

   c. You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

   d. If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

   (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

   These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

   Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

   In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

   Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

   This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

   If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

   However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

   You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

   a. Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

   b. Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

   c. Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

   d. If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

   e. Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

      For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

      It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

   a. Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b. Give prominent notice with the combined library of the fact that part of it is a work based on the Library and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

    If any portion of this section is held invalid or unenforceable under any circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

    It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

    This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version but may differ in detail to address new problems or concerns.

    Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990

Ty Coon, President of Vice

That's all there is to it!

Apache License | Version 2.0, January 2004

- Xerces-c version 2.70 is licensed under *Apache2.0 License category.*

Apache License v2

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

   "License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

   "Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

   "Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

   "You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

   "Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

   "Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation and conversions to other media types.

   "Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

   "Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

   "Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

   "Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

   b) You must cause any modified files to carry prominent notices stating that You changed the files; and

   c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

   d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

   You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

OpenSSL License

- OpenSSL version 1.02g-lubuntu4.19 and version **openssl-1.1.1k** are licensed under *OpenSSL & Open SSLeay License category*.

OpenSSL License

LICENSE ISSUES

==========

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit.

See below for the actual license texts. Actually, both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org

==========

Copyright (c) 1998-2018 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR NSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER

IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

Net-SNMP License

- Net-SNMP version 5.9 is licensed under *Net-SNMP License category*.

Net-SNMP License

Various copyrights apply to this package, listed in various separate parts below. Please make sure that you read all the parts.

---- Part 1: CMU/UCD copyright notice: (BSD like) -----

Copyright 1989, 1991, 1992 by Carnegie Mellon University Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

Copyright (c) 2001-2003, Networks Associates Technology, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN

NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2009, Sparta, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

Copyright (c) 2004, Cisco, Inc and Information Network Center of Beijing University of Posts and Telecommunications.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS `AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) -----

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003 oss@fabasoft.com

Author: Bernhard Penz

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or product names may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER `AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 8: Apple Inc. copyright notice (BSD) -----

Copyright (c) 2007 Apple Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of Apple Inc. ("Apple") nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY APPLE AND ITS CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL APPLE OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 9: ScienceLogic, LLC copyright notice (BSD) -----

Copyright (c) 2009, ScienceLogic, LLC

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of ScienceLogic, LLC nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THEUSE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

BSD License

- openssh version 8.4-p1 and openssh 4.2-p1 are licensed under *BSD License category*.

BSD License

This file is part of the OpenSSH software.

The licences which components of this software fall under are as follows. First, we will summarize and say that all components are under a BSD licence, or a licence more free than that.

OpenSSH contains no GPL code.

1) Copyright (c) 1995 Tatu Ylonen ylo@cs.hut.fi , Espoo, Finland

All rights reserved

As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name other than "ssh" or "Secure Shell".

However, I am not implying to give any licenses to any patents or copyrights held by third parties, and the software includes parts that are not under my direct control. As far as I know, all included source code is used in accordance with the relevant license agreements and can be used freely for any purpose (the GNU license being the most restrictive); see below for details.

[However, none of that term is relevant at this point in time. All of these restrictively licenced software components which he talks about have been removed from OpenSSH, i.e.,

- RSA is no longer included, found in the OpenSSL library
- IDEA is no longer included, its use is deprecated
- DES is now external, in the OpenSSL library
- GMP is no longer used, and instead we call BN code from OpenSSL
- Zlib is now external, in a library
- The make-ssh-known-hosts script is no longer included
- TSS has been removed
- MD5 is now external, in the OpenSSL library
- RC4 support has been replaced with ARC4 support from OpenSSL
- Blowfish is now external, in the OpenSSL library

Note that any information and cryptographic algorithms used in this software are publicly available on the Internet and at any major bookstore, scientific library, and patent office worldwide. More information can be found e.g. at http://www.cs.hut.fi/crypto .

The legal status of this program is some combination of all these permissions and restrictions. Use only at your own responsibility.

You will be responsible for any legal consequences yourself; I am not making any claims whether possessing or using this is legal or not in your country, and I am not taking any responsibility on your behalf.

NO WARRANTY

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED

OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

2) The 32-bit CRC compensation attack detector in deattack.c was contributed by CORE SDI S.A. under a BSD-style license.

Cryptographic attack detector for ssh - source code

Copyright (c) 1998 CORE SDI S.A., Buenos Aires, Argentina.

All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that this copyright notice is retained.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES ARE DISCLAIMED. IN NO EVENT SHALL CORE SDI S.A. BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OR MISUSE OF THIS SOFTWARE.

Ariel Futoransky futo@core-sdi.com http://www.core-sdi.com

3) ssh-keyscan was contributed by David Mazieres under a BSD-style license.

Copyright 1995, 1996 by David Mazieres dm@lcs.mit.edu .

Modification and redistribution in source and binary forms is permitted provided that due credit is given to the author and the OpenBSD project by leaving this copyright notice intact.

4) The Rijndael implementation by Vincent Rijmen, Antoon Bosselaers and Paulo Barreto is in the public domain and distributed with the following license:

@version 3.0 (December 2000)

Optimised ANSI C code for the Rijndael cipher (now AES)

@author Vincent Rijmen vincent.rijmen@esat.kuleuven.ac.be

@author Antoon Bosselaers antoon.bosselaers@esat.kuleuven.ac.be

@author Paulo Barreto paulo.barreto@terra.com.br

This code is hereby placed in the public domain.

THIS SOFTWARE IS PROVIDED BY THE AUTHORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

5) One component of the ssh source code is under a 3-clause BSD license, held by the University of California, since we pulled these parts from original Berkeley code.

Copyright (c) 1983, 1990, 1992, 1993, 1995

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)

HOWEVER, CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

6) Remaining components of the software are provided under a standard

2-term BSD licence with the following names as copyright holders:

Markus Friedl

Theo de Raadt

Niels Provos
Dug Song
Aaron Campbell
Damien Miller
Kevin Steves
Daniel Kouril
Wesley Griffin
Per Allansson
Nils Nordman
Simon Wilkinson

7) Portable OpenSSH additionally includes code from the following copyright holders, also under the 2-term BSD license:

Ben Lindstrom
Tim Rice
Andre Lucas
Chris Adams
Corinna Vinschen
Cray Inc.
Denis Parker
Gert Doering
Jakob Schlyter
Jason Downs
Juha Yrjölä
Michael Stone
Networks Associates Technology, Inc.
Solar Designer
Todd C. Miller
Wayne Schroeder
William Jones
Darren Tucker
Sun Microsystems
The SCO Group

Redistribution and use in source and binary forms, with or without modification are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.

IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

8) Portable OpenSSH contains the following additional licenses:

a) md5crypt.c, md5crypt.h

"THE BEER-WARE LICENSE" (Revision 42): phk@login.dknet.dk wrote this file. As long as you retain this notice you can do whatever you want with this stuff. If we meet someday, and you think this stuff is worth it, you can buy me a beer in return. Poul-Henning Kamp

b) snprintf replacement

* Copyright Patrick Powell 1995

This code is based on code written by Patrick Powell (papowell@astart.com) It may be used for any purpose as long as this notice remains intact on all source code distributions

c) Compatibility code (openbsd-compat)

Apart from the previously mentioned licenses, various pieces of code in the openbsd-compat/ subdirectory is licensed as follows:

Some code is licensed under a 3-term BSD license, to the following copyright holders:

Todd C. Miller

Theo de Raadt

Damien Miller

Eric P. Allman

The Regents of the University of California

Constantin S. Svintsoff

Redistribution and use in source and binary forms, with or without modification are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)

HOWEVER, CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Some code is licensed under an ISC-style license, to the following copyright holders:

Internet Software Consortium.

Todd C. Miller

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND TODD C. MILLER DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL TODD C. MILLER BE LIABLE

FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Some code is licensed under a MIT-style license to the following copyright holders:

Free Software Foundation, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including* without limitation the rights to use, copy, modify, merge, publish, distribute, distribute with modifications, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name(s) of the above copyright holders shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization.

BSD License 2.0 | 3-Clause License | Revised BSD License

1. libssh2 version 1.9 under 3-Clause BSD 2.0 License category.

BSD License 2.0 | Revised BSD License

Copyright (c) 2004-2007 Sara Golemon sarag@libssh2.org

Copyright (c) 2005,2006 Mikhail Gusarov dottedmag@dottedmag.net

Copyright (c) 2006-2007 The Written Word, Inc.

Copyright (c) 2007 Eli Fant elifantu@mail.ru

Copyright (c) 2009-2014 Daniel Stenberg

Copyright (C) 2008, 2009 Simon Josefsson

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the <organization> nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL <COPYRIGHT HOLDER> BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Simplified BSD License | 2-Clause License | Free BSD License

- Nocache-master is licensed under 2-Clause Free BSD License category.

2-Clause License | Free BSD License

Copyright (c) 2011, Julius Plenz julius@plenz.com

All rights reserved.

Redistribution and use in source and binary forms, with or without modification are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the <project name> project.

Generic License – CGIC

- cgic version 205 is licensed CGIC *License category*.

CGIC License Terms

Basic License

CGIC, copyright 1996-2011 by Thomas Boutell and Boutell.Com, Inc. Permission is granted to use CGIC in any application, commercial or noncommercial, at no cost. HOWEVER, this copyright paragraph must appear on a "credits" page accessible in the public online and offline documentation of the program. Modified versions of the CGIC library should not be distributed without the

attachment of a clear statement regarding the author of the modifications, and this notice may in no case be removed. Modifications may also be submitted to the author for inclusion in the main CGIC distribution.

IF YOU WOULD PREFER NOT TO ATTACH THE ABOVE NOTICE to the public documentation of your application, consult the information which follows regarding the availability of a nonexclusive commercial license for CGIC.

Commercial License

The price of a nonexclusive commercial license is $200 U.S.

To purchase the license, visit our online store here:

https://www.boutell.com/

Signed originals are available on request after purchase.

Commercial licensees are entitled to ongoing email support and update notifications.

* * *

CGIC Nonexclusive Commercial License

The party purchasing this license is granted the right to utilize CGIC, major version 1 or 2, any minor version thereof, in CGI applications without the need for a credit notice of any kind. CGI applications developed by the holder of this license may be distributed freely in source code or binary form without additional fees or royalties. This license does not grant the right to use CGIC to create a development tool which passes on substantially all of the capabilities of the CGIC library to the user of the tool, unless that tool is to be used internally by the license holder only in order to develop CGI applications. This license may not be resold, but applications developed in accordance with the terms of the license may be distributed freely subject to the limitations described above.

Future minor (2.x) versions of CGIC will be covered by this license free of charge. If significant defects of workmanship are discovered in version 2.x, minor releases to correct them will be made available before or at the same time that those defects are addressed in any future major version.

Future "major" (3.x) versions will be available to licensees at an upgrade price of $50.

If, for any reason, any portion of this license is found to be invalid, that portion of the license only is invalidated, and the remainder of the agreement remains in effect.

Generic License – Zlib

- zlib version 1.2.3 is licensed Zlib *License category*.

Copyright notice:

(C) 1995-2004 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly ***Mark Adler***

jloup@gzip.org ***madler@alumni.caltech.edu***

If you use the zlib library in a product, we would appreciate not receiving lengthy legal documents to sign. The sources are provided for free but without warranty of any kind. The library has been entirely written by Jean-loup Gailly and Mark Adler; it does not include third-party code.

If you redistribute modified sources, we would appreciate that you include in the file ChangeLog history information documenting your changes. Please read the FAQ for more information on the distribution of modified source versions.

Generic License – Linux-PAM

- Linux-PAM version 1.1.8 is licensed *Linux-PAM License category*.

Unless otherwise explicitly stated the following text describes the licensed conditions under which the contents of this Linux-PAM release may be distributed:

Redistribution and use in source and binary forms of Linux-PAM, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain any existing copyright notice, and this entire permission notice in its entirety, including the disclaimer of warranties.
2. Redistributions in binary form must reproduce all prior and current copyright notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of any author may not be used to endorse or promote products derived from this software without their specific prior written permission.

ALTERNATIVELY, this product may be distributed under the terms of the GNU General Public License, in which case the provisions of the GNU GPL are required INSTEAD OF the above restrictions. (This clause is necessary due to a potential conflict between the GNU GPL and the restrictions contained in a BSD-style copyright.)

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.

IN NO EVENT SHALL THE AUTHOR(S) BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR

TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THEUSE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright Notice

© 2021, General Electric Company. All rights reserved.

The information contained in this online publication is the exclusive property of General Electric Company, except as otherwise indicated. You may view, copy and print documents and graphics incorporated in this online publication (the "Documents") subject to the following: (1) the Documents may be used solely for personal, informational, non-commercial purposes; (2) the Documents may not be modified or altered in any way; and (3) General Electric Company withholds permission for making the Documents or any portion thereof accessible via the internet. Except as expressly provided herein, you may not use, copy, print, display, reproduce, publish, license, post, transmit or distribute the Documents in whole or in part without the prior written permission of General Electric Company. If applicable, any use, modification, reproduction, release, performance, display, or disclosure of the Software Product and Associated Material by the U.S. Government shall be governed solely by the terms of the License Agreement and shall be prohibited except to the extent expressly permitted by the terms of the License Agreement.

The information contained in this online publication is subject to change without notice. The software described in this online publication is supplied under license and may be used or copied only in accordance with the terms of such license.

Trademark Notice

GE and the GE monogram are trademarks and service marks of General Electric Company.

* Trademarks of General Electric Company.

Other company or product names mentioned in this document may be trademarks or registered trademarks of their respective companies.

Modification Record

Version	Rev.	Date	Change Description
1.00	0	1st April, 2019	Created.
2.00	0	12th April, 2021	Updated for MCP family.
2.30	0	28th July, 2021	Updated for MCP v2.3

GE
Grid Solutions

DNP3 Server (DPA) for the Multifunction Controller Platform

Conformance Statement

Associated with NTEK-A022M-0CS

Version 1.00 Revision 0

Associated Software Release: Version 1.00

imagination at work

General

COPYRIGHT NOTICE

© 2019, General Electric Company. All rights reserved.

The Software Product described in this documentation may only be used in accordance with the applicable License Agreement. The Software Product and Associated Material are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable, and are delivered with Restricted Rights. Such restricted rights are those identified in the License Agreement, and as set forth in the "Restricted Rights Notice" contained in paragraph (g) (3) (Alternate III) of FAR 52.227-14, Rights in Data-General, including Alternate III (June 1987).

If applicable, any use, modification, reproduction release, performance, display or disclosure of the Software Product and Associated Material by the U.S. Government shall be governed solely by the terms of the License Agreement and shall be prohibited except to the extent expressly permitted by the terms of the License Agreement.

The information contained in this online publication is the exclusive property of General Electric Company, except as otherwise indicated. You may view, copy and print documents and graphics incorporated in this online publication (the "Documents") subject to the following: (1) the Documents may be used solely for personal, informational, non-commercial purposes; (2) the Documents may not be modified or altered in any way; and (3) General Electric Company withholds permission for making the Documents or any portion thereof accessible via the internet. Except as expressly provided herein, you may not use, copy, print, display, reproduce, publish, license, post, transmit or distribute the Documents in whole or in part without the prior written permission of General Electric Company. If applicable, any use, modification, reproduction, release, performance, display, or disclosure of the Software Product and Associated Material by the U.S. Government shall be governed solely by the terms of the License Agreement and shall be prohibited except to the extent expressly permitted by the terms of the License Agreement.

The information contained in this online publication is subject to change without notice. The software described in this online publication is supplied under license and may be used or copied only in accordance with the terms of such license.

TRADEMARK NOTICES

GE and are trademarks and service marks of General Electric Company.

* Trademarks of General Electric Company.

Other company or product names mentioned in this document may be trademarks or registered trademarks of their respective companies.

Contents

1. DNP3 Server Application on MCP - Device Profile Document.....5

Tables

Table 1 Objects/Variations/Qualifiers/Function Codes supported by the MCP DNP3 Server... 8

1. DNP3 Server Application on MCP - Device Profile Document

This document summarizes the MCP DNP3 Server implementation of the DNP3 protocol.

Several items in the Device Profile Document require additional explanation. All timeouts used by the DNP3 Server are configurable.

Each digital input point configured in the DNP3 Server is monitored for digital input change events. The user configures whether to report these as time-tagged or non-time-tagged digital events.

Counters rollover at whatever variation they are configured for. For example, if the counter is configured for a 32-bit variation, then it rolls over at 32 bits.

Unsolicited responses in the DNP3 Server are enabled and disabled for all classes (class 1, class 2 and class 3). However, if unsolicited responses are disabled in the configuration, unsolicited responses cannot be enabled or disabled during run-time via requests from the master station.

If unsolicited responses are enabled for one or more classes, the following IIN exceptions generate unsolicited responses: device restart, need time synchronization, and digital event buffer overflow.

The default variation of the static objects and change objects are configurable. When the Master requests data with all variations, the DNP3 Server responds with the configured variation. When the Master requests with a specific variation, the DNP3 Server responds with requested variation.

<table>
<tr><td colspan="2">DNP3
DEVICE PROFILE DOCUMENT
This document is accompanied by a table having the following headings:
Object Group | Request Function Codes | Response Function Codes
Object Variation | Request Qualifiers | Response Qualifiers
Object Name (optional)</td></tr>
<tr><td colspan="2">Vendor Name: GE Grid Solutions</td></tr>
<tr><td colspan="2">Device Name: MCP DNP3 Server (both Serial and LAN)</td></tr>
<tr><td>Highest DNP3 Level Supported:
For Requests Level 3
For Responses Level 3</td><td>Device Function:
□ Master ■ Outstation</td></tr>
<tr><td colspan="2">Notable objects, functions, and/or qualifiers supported in addition to the Highest DNP3 Levels Supported (the complete list is described in the attached table):
<u>Optionally assigning class 1, 2 or 3 for each point.</u></td></tr>
</table>

Optionally forcing digital input points.

Optionally send Unsolicited messages for Indication or Indications and Events.

Time tagged available analog inputs returned.

Maximum Data Link Frame Size (octets):	Maximum Application Fragment Size (octets):
Transmitted 292_____	Transmitted 100 - 64K (configurable)
Received (must be 292)	Received 100 - 64K (must be > 249)
Maximum Data Link Re-tries:	Maximum Application Layer Re-tries:
□ None	□ None
□ Fixed at _____	■ Configurable, range __0_ to __32767___ (Fixed is not permitted)
■ Configurable, range __0_ to _255__	

Requires Data Link Layer Confirmation:

□ Never

□ Always

□ Sometimes If 'Sometimes', when? _____

■ Configurable If 'Configurable', how? User enables or disables confirm service.

Requires Application Layer Confirmation:

□ Never

□ Always (not recommended)

□ When reporting Event Data (Slave devices only)

□ When sending multi-fragment responses (Slave devices only)

□ Sometimes If 'Sometimes', when?

■ Configurable If 'Configurable', how? User enables or disables confirm service.

Timeouts while waiting for:

Data Link Confirm	□ None	□ Fixed at _____	□ Variable	■ Configurable
Complete Appl. Fragment	□ None	□ Fixed at _____	□ Variable	□ Configurable
Application Confirm	□ None	□ Fixed at _____	□ Variable	■ Configurable
Complete Appl. Response	□ None	□ Fixed at _____	□ Variable	□ Configurable

Others _____

Attach explanation if 'Variable' or 'Configurable' was checked for any timeout

Sends/Executes Control Operations:

WRITE Binary Outputs	□ Never	■ Always	□ Sometimes	□ Configurable
SELECT/OPERATE	□ Never	■ Always	□ Sometimes	□ Configurable
DIRECT OPERATE	□ Never	■ Always	□ Sometimes	□ Configurable
DIRECT OPERATE - NO ACK	□ Never	■ Always	□ Sometimes	□ Configurable
Count > 1	□ Never	■ Always	□ Sometimes	□ Configurable
Pulse On	□ Never	■ Always	□ Sometimes	□ Configurable
Pulse Off	□ Never	■ Always	□ Sometimes	□ Configurable
Latch On	□ Never	■ Always	□ Sometimes	□ Configurable

Latch Off	□ Never	■ Always	□ Sometimes	□ Configurable
Queue	□ Never	■ Always	□ Sometimes	□ Configurable
Clear Queue	□ Never	■ Always	□ Sometimes	□ Configurable

Attach explanation if 'Sometimes' or 'Configurable' was checked for any operation.

FILL OUT THE FOLLOWING ITEM FOR MASTER DEVICES ONLY:

Expects Binary Input Change Events:

□ Either time-tagged or non-time-tagged for a single event

□ Both time-tagged and non-time-tagged for a single event

□ Configurable (attach explanation)

FILL OUT THE FOLLOWING ITEMS FOR SLAVE DEVICES ONLY:

Reports Binary Input Change Events when no specific variation requested: □ Never □ Only time-tagged □ Only non-time-tagged ■ Configurable to one or the other (attach explanation)	Reports time-tagged Binary Input Change Events when no specific variation requested: □ Never □ Binary Input Change with Time □ Binary Input Change with Relative Time ■ Configurable (attach explanation)
Sends Unsolicited Responses: □ Never ■ Configurable (attach explanation) □ Only certain objects □ Sometimes (attach explanation) ■ ENABLE/DISABLE UNSOLICITED Function codes supported	Sends Static Data in Unsolicited Responses: □ Never ■ When Device Restarts ■ When Status Flags Change No other options are permitted.
Default Counter Object/Variation: □ No Counters Reported ■ Configurable (attach explanation) □ Default Object _____ Default Variation _____ □ Point-by-point list attached	Counters Roll Over at: □ No Counters Reported ■ Configurable (attach explanation) □ 16 Bits □ 32 Bits □ Other Value _____ □ Point-by-point list attached

Sends Multi-Fragment Responses: ■ Yes □ No

Table 1 explains which objects/variations are used with which Function Codes and Qualifier Codes by the MCP DNP3 Server implementation.

To understand the table, consider the third row of Table 1. This row specifies how object 1, variation 2 (Binary Input with Status) is accessed. To access this type of object, the DNP3 Server shall process a request using Function Code 1 (READ) with a Qualifier Code in the range of 00, 01, or 06. The DNP3 Server shall respond with Function Code 129 (RESPONSE), Qualifier Code 01. The DNP3 Server shall also support a request using Function 2 (WRITE).

Table 1 Objects/Variations/Qualifiers/Function Codes supported by the MCP DNP3 Server

Obj.	Var.	Description	Request Function Code	Request Qualifier Codes (Hexadecimal)	Response Function Code	Response Qualifier Codes (Hexadecimal)
1	0	BINARY INPUT-ALL VARIATIONS	1, 22	00, 01, 06	Not Used	Not Used
1	1	SINGLE-BIT BINARY INPUT	1	00, 01, 06	129	01
1	2	BINARY INPUT WITH STATUS	1	00, 01, 06	129	01
			2	00, 01	129	01
2	0	BINARY INPUT CHANGE - ALL VARIATIONS	1	06, 07, 08	Not Used	Not Used
2	1	BINARY INPUT CHANGE WITHOUT TIME	1	06, 07, 08	129, 130	28
2	2	BINARY INPUT CHANGE WITH TIME	1	06, 07, 08	129, 130	28
2	3	BINARY INPUT CHANGE WITH RELATIVE TIME	1	06, 07, 08	129, 130	28
10	0	BINARY OUTPUT - ALL VARIATIONS	1	00, 01, 06	Not Used	Not Used
10	1	BINARY OUTPUT	Not Used	Not Used	Not Used	Not Used
10	2	BINARY OUTPUT STATUS	1	00, 01, 06	129	01
12	0	CONTROL RELAY OUTPUT BLOCK - ALL VARIATIONS	Not Used	Not Used	Not Used	Not Used
12	1	CONTROL RELAY OUTPUT BLOCK	3, 4, 5, 6	17, 28	129	Echo of request qualifier codes
12	2	PATTERN CONTROL BLOCK	5, 6	17,28	129	Echo of request qualifier codes
12	3	PATTERN MASK	5, 6	00, 01	129	Echo of request qualifier codes
20	0	BINARY COUNTER - ALL VARIATIONS	1, 7, 8, 9, 10, 22	00, 01, 06	Not Used	Not Used
20	1	32-BIT BINARY COUNTER	1, 7, 8, 9, 10	00, 01, 06	129	01
20	2	16-BIT BINARY COUNTER	1, 7, 8, 9, 10	00, 01, 06	129	01
20	3	32-BIT DELTA COUNTER	Not Used	Not Used	Not Used	Not Used
20	4	16-BIT DELTA COUNTER	Not Used	Not Used	Not Used	Not Used
20	5	32-BIT BINARY COUNTER WITHOUT FLAG	1, 7, 8, 9, 10	00, 01, 06	129	01
20	6	16-BIT BINARY COUNTER WITHOUT FLAG	1, 7, 8, 9, 10	00, 01, 06	129	01

Obj.	Var.	Description	Request Function Code	Request Qualifier Codes (Hexadecimal)	Response Function Code	Response Qualifier Codes (Hexadecimal)
20	7	32-BIT DELTA COUNTER WITHOUT FLAG	Not Used	Not Used	Not Used	Not Used
20	8	16-BIT DELTA COUNTER WITHOUT FLAG	Not Used	Not Used	Not Used	Not Used
21	0	FROZEN COUNTER - ALL VARIATIONS	1, 22	00, 01, 06	Not Used	Not Used
21	1	32-BIT FROZEN COUNTER	1	00, 01, 06	129	01
21	2	16-BIT FROZEN COUNTER	1	00, 01, 06	129	01
21	3	32-BIT FROZEN DELTA COUNTER	Not Used	Not Used	Not Used	Not Used
21	4	16-BIT FROZEN DELTA COUNTER	Not Used	Not Used	Not Used	Not Used
21	5	32-BIT FROZEN COUNTER WITH TIME OF FREEZE	1	00, 01, 06	129	01
21	6	16-BIT FROZEN COUNTER WITH TIME OF FREEZE	1	00, 01, 06	129	01
21	7	32-BIT FROZEN DELTA COUNTER WITH TIME OF FREEZE	Not Used	Not Used	Not Used	Not Used
21	8	16-BIT FROZEN DELTA COUNTER WITH TIME OF FREEZE	Not Used	Not Used	Not Used	Not Used
21	9	32-BIT FROZEN COUNTER WITHOUT FLAG	1	00, 01, 06	129	01
21	10	16-BIT FROZEN COUNTER WITHOUT FLAG	1	00, 01, 06	129	01
21	11	32-BIT FROZEN DELTA COUNTER WITHOUT FLAG	1	00, 01, 06	Not Used	Not Used
21	12	16-BIT FROZEN DELTA COUNTER WITHOUT FLAG	1	00, 01, 06	Not Used	Not Used
22	0	COUNTER CHANGE EVENT - ALL VARIATIONS	1	06, 07, 08	Not Used	Not Used
22	1	32-BIT COUNTER CHANGE EVENT WITHOUT TIME	1	06, 07, 08	129, 130	28
22	2	16-BIT COUNTER CHANGE EVENT WITHOUT TIME	1	06, 07, 08	129, 130	28
22	3	32-BIT DELTA COUNTER CHANGE EVENT WITHOUT TIME	Not Used	Not Used	Not Used	Not Used
22	4	16-BIT DELTA COUNTER CHANGE EVENT WITHOUT TIME	Not Used	Not Used	Not Used	Not Used
22	5	32-BIT COUNTER CHANGE EVENT WITH TIME	1	06, 07, 08	129, 130	28

Obj.	Var.	Description	Request Function Code	Request Qualifier Codes (Hexadecimal)	Response Function Code	Response Qualifier Codes (Hexadecimal)
22	6	16-BIT COUNTER CHANGE EVENT WITH TIME	1	06, 07, 08	129, 130	28
22	7	32-BIT DELTA COUNTER CHANGE EVENT WITH TIME	Not Used	Not Used	Not Used	Not Used
22	8	16-BIT DELTA COUNTER CHANGE EVENT WITH TIME	Not Used	Not Used	Not Used	Not Used
23	0	FROZEN COUNTER - ALL VARIATIONS	1	06, 07, 08	Not Used	Not Used
23	1	32-BIT FROZEN COUNTER EVENT WITHOUT TIME	1	06, 07, 08	129, 130	28
23	2	16-BIT FROZEN COUNTER EVENT WITHOUT TIME	1	06, 07, 08	129, 130	28
23	3	32-BIT FROZEN DELTA COUNTER EVENT WITHOUT TIME	Not Used	Not Used	Not Used	Not Used
23	4	16-BIT FROZEN DELTA COUNTER EVENT WITHOUT TIME	Not Used	Not Used	Not Used	Not Used
23	5	32-BIT FROZEN COUNTER EVENT WITH TIME	1	06, 07, 08	129, 130	28
23	6	16-BIT FROZEN COUNTER EVENT WITH TIME	1	06, 07, 08	129, 130	28
23	7	32-BIT FROZEN DELTA COUNTER EVENT WITH TIME	Not Used	Not Used	Not Used	Not Used
23	8	16-BIT FROZEN DELTA COUNTER EVENT WITH TIME	Not Used	Not Used	Not Used	Not Used
30	0	ANALOG INPUT – ALL VARIATIONS	1, 22	00, 01, 06	Not Used	Not Used
30	1	32-BIT ANALOG INPUT	1	00, 01, 06	129	01
30	2	16-BIT ANALOG INPUT	1	00, 01, 06	129	01
30	3	32-BIT ANALOG INPUT WITHOUT FLAG	1	00, 01, 06	129	01
30	4	16-BIT ANALOG INPUT WITHOUT FLAG	1	00, 01, 06	129	01
30	5	32-BIT FLOATING POINT ANALOG INPUT	1	00, 01, 06	129	01
31	0	FROZEN ANALOG INPUT - ALL VARIATIONS	Not Used	Not Used	Not Used	Not Used
31	1	32-BIT FROZEN ANALOG INPUT	Not Used	Not Used	Not Used	Not Used
31	2	16-BIT FROZEN ANALOG INPUT	Not Used	Not Used	Not Used	Not Used
31	3	32-BIT FROZEN ANALOG INPUT WITH TIME OF FREEZE	Not Used	Not Used	Not Used	Not Used

Obj.	Var.	Description	Request Function Code	Request Qualifier Codes (Hexadecimal)	Response Function Code	Response Qualifier Codes (Hexadecimal)
31	4	16-BIT FROZEN ANALOG INPUT WITH TIME OF FREEZE	Not Used	Not Used	Not Used	Not Used
31	5	32-BIT FROZEN ANALOG INPUT WITHOUT FLAG	Not Used	Not Used	Not Used	Not Used
31	6	16-BIT FROZEN ANALOG INPUT WITHOUT FLAG	Not Used	Not Used	Not Used	Not Used
32	0	ANALOG CHANGE EVENT - ALL VARIATIONS	1	06, 07, 08	Not Used	Not Used
32	1	32-BIT ANALOG CHANGE EVENT WITHOUT TIME	1	06, 07, 08	129, 130	28
32	2	16-BIT ANALOG CHANGE EVENT WITHOUT TIME	1	06, 07, 08	129, 130	28
32	3	32-BIT ANALOG CHANGE EVENT WITH TIME	1	06, 07, 08	129, 130	28
32	4	16-BIT ANALOG CHANGE EVENT WITH TIME	1	06, 07, 08	129, 130	28
32	5	32-BIT FLOATING POINT ANALOG CHANGE EVENT WITHOUT TIME	1	06, 07, 08	129, 130	28
32	7	32-BIT FLOATING POINT ANALOG CHANGE EVENT WITH TIME	1	06, 07, 08	129, 130	28
33	0	FROZEN ANALOG EVENT - ALL VARIATIONS	Not Used	Not Used	Not Used	Not Used
33	1	32-BIT FROZEN ANALOG EVENT WITHOUT TIME	Not Used	Not Used	Not Used	Not Used
33	2	16-BIT FROZEN ANALOG EVENT WITHOUT TIME	Not Used	Not Used	Not Used	Not Used
33	3	32-BIT FROZEN ANALOG EVENT WITH TIME	Not Used	Not Used	Not Used	Not Used
33	4	16-BIT FROZEN ANALOG EVENT WITH TIME	Not Used	Not Used	Not Used	Not Used
40	0	ANALOG OUTPUT STATUS - ALL VARIATIONS	1	00, 01, 06	Not Used	Not Used
40	1	32-BIT ANALOG OUTPUT STATUS	1	00, 01, 06	129	01
40	2	16-BIT ANALOG OUTPUT STATUS	1	00, 01, 06	129	01
41	0	ANALOG OUTPUT BLOCK - ALL VARIATIONS	Not Used	Not Used	Not Used	Not Used
41	1	32-BIT ANALOG OUTPUT BLOCK	3, 4, 5, 6	17, 28	129	Echo of request qualifier codes
41	2	16-BIT ANALOG OUTPUT BLOCK	3, 4, 5, 6	17, 28	129	Echo of request qualifier codes

Obj.	Var.	Description	Request Function Code	Request Qualifier Codes (Hexadecimal)	Response Function Code	Response Qualifier Codes (Hexadecimal)
50	0	TIME AND DATE - ALL VARIATIONS	Not Used	Not Used	Not Used	Not Used
50	1	TIME AND DATE	1, 2	07, where quantity = 1	129	07, Quantity = 1
50	2	TIME AND DATE WITH INTERVAL	Not Used	Not Used	Not Used	Not Used
51	0	TIME AND DATE CTO - ALL VARIATIONS	Not Used	Not Used	Not Used	Not Used
51	1	TIME AND DATE CTO	Not Used	Not Used	129, 130	07, Quantity = 1
51	2	UN-SYNCHRONIZED TIME AND DATE CTO	Not Used	Not Used	129, 130	07, Quantity = 1
52	0	TIME DELAY – ALL VARIATIONS	Not Used	Not Used	Not Used	Not Used
52	1	TIME DELAY COARSE	Not Used	Not Used	Not Used	Not Used
52	2	TIME DELAY FINE	Not Used	Not Used	129	07, Quantity = 1
60	0	CLASS DATA – ALL VARIATIONS	Not Used	Not Used	Not Used	Not Used
60	1	CLASS 0 DATA	1	06	Not Used	1
60	2	CLASS 1 DATA	1	06, 07, 08	Not Used	Not Used
			20, 21, 22	06		
60	3	CLASS 2 DATA	1	06, 07, 08	Not Used	Not Used
			20, 21, 22	06		
60	4	CLASS 3 DATA	1	06, 07, 08	Not Used	Not Used
			20, 21, 22	06		
70	1	FILE IDENTIFIER	Not Used	Not Used	Not Used	Not Used
80	1	INTERNAL INDICATIONS	1	00, 01	129, 130	00
			2	00		
81	0	STORAGE OBJECT - ALL VARIATIONS	Not Used	Not Used	Not Used	Not Used
81	1	STORAGE OBJECT	Not Used	Not Used	Not Used	Not Used
82	1	DEVICE PROFILE	Not Used	Not Used	Not Used	Not Used
83	1	PRIVATE REGISTRATION OBJECT	Not Used	Not Used	Not Used	Not Used
83	2	PRIVATE REGISTRATION OBJECT DESCRIPTOR	Not Used	Not Used	Not Used	Not Used
90	1	APPLICATION IDENTIFIER	Not Used	Not Used	Not Used	Not Used
100	1	SHORT FLOATING POINT	Not Used	Not Used	Not Used	Not Used
100	2	LONG FLOATING POINT	Not Used	Not Used	Not Used	Not Used
100	3	EXTENDED FLOATING POINT	Not Used	Not Used	Not Used	Not Used

Obj.	Var.	Description	Request Function Code	Request Qualifier Codes (Hexadecimal)	Response Function Code	Response Qualifier Codes (Hexadecimal)
101	1	SMALL-PACKED BINARY CODED DECIMAL	Not Used	Not Used	Not Used	Not Used
101	2	MEDIUM-PACKED BINARY CODED DECIMAL	Not Used	Not Used	Not Used	Not Used
101	3	LARGE-PACKED BINARY CODED DECIMAL	Not Used	Not Used	Not Used	Not Used

MODIFICATION RECORD

VERSION	REV.	DATE	AUTHOR	CHANGE DESCRIPTION
1.00	0	2nd May, 2019	G. LaMarre	Created.

GE
Grid Solutions

DNP3 Client (DCA) for the Multifunction Controller Platform

Conformance Statement

Associated with NTEK-A023M-0CS

Version 1.00 Revision 0

Associated Software Release: Version 1.00

imagination at work

General

COPYRIGHT NOTICE

© 2019, General Electric Company. All rights reserved.

The Software Product described in this documentation may only be used in accordance with the applicable License Agreement. The Software Product and Associated Material are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable, and are delivered with Restricted Rights. Such restricted rights are those identified in the License Agreement, and as set forth in the "Restricted Rights Notice" contained in paragraph (g) (3) (Alternate III) of FAR 52.227-14, Rights in Data-General, including Alternate III (June 1987).

If applicable, any use, modification, reproduction release, performance, display or disclosure of the Software Product and Associated Material by the U.S. Government shall be governed solely by the terms of the License Agreement and shall be prohibited except to the extent expressly permitted by the terms of the License Agreement.

The information contained in this online publication is the exclusive property of General Electric Company, except as otherwise indicated. You may view, copy and print documents and graphics incorporated in this online publication (the "Documents") subject to the following: (1) the Documents may be used solely for personal, informational, non-commercial purposes; (2) the Documents may not be modified or altered in any way; and (3) General Electric Company withholds permission for making the Documents or any portion thereof accessible via the internet. Except as expressly provided herein, you may not use, copy, print, display, reproduce, publish, license, post, transmit or distribute the Documents in whole or in part without the prior written permission of General Electric Company. If applicable, any use, modification, reproduction, release, performance, display, or disclosure of the Software Product and Associated Material by the U.S. Government shall be governed solely by the terms of the License Agreement and shall be prohibited except to the extent expressly permitted by the terms of the License Agreement.

The information contained in this online publication is subject to change without notice. The software described in this online publication is supplied under license and may be used or copied only in accordance with the terms of such license.

TRADEMARK NOTICES

GE and are trademarks and service marks of General Electric Company.

* Trademarks of General Electric Company.

Other company or product names mentioned in this document may be trademarks or registered trademarks of their respective companies.

Contents

1. DNP3 Client Application on MCP – Device Profile Document 5

1.1 Profile of Normal Operation 11

Tables

Table 1 DNP3 Subset Sent by the Client under normal operation 9
Table 2 - DNP3 Subset Implemented by the Client 12

1. DNP3 Client Application on MCP – Device Profile Document

This document contains the Device Profile for the DNP3 Client Application on the MCP. Note that this Profile applies to the Client Application, not to the entire MCP.

DNP3 **Device Profile Document**	
Vendor Name: GE Grid Solutions	
Device Name: MCP DNP3 Client (both Serial and LAN).	
Highest DNP Level Supported: For Requests 2 For Responses 3	Device Function: ☒ Master ☐ Slave
Notable objects, functions, and/or qualifiers supported in addition to the Highest DNP Levels Supported (the complete list is described in the attached table): = Accepts many more qualifiers than specified in Level 3. = Can issue Enable Unsolicited Response for Class 1, 2 and 3 upon receipt of Null Unsolicited Response.	
Maximum Data Link Frame Size (octets): Transmitted ____292____ Received ____292____	Maximum Application Fragment Size (octets): Transmitted ___100 to 65535___ Received ___100 to 65535___

DNP3 **Device Profile Document**	
Maximum Data Link Re-tries: ☐ None ☐ Fixed at _____ ☒ Configurable, range 0 to 255 (config file)	Maximum Application Layer Re-tries: ☐ None ☐ Fixed at _____ ☒ Configurable, range 0 to 255 (config file)
Requires Data Link Layer Confirmation: ☐ Never ☐ Always ☐ Sometimes If 'sometimes', when? _____ ☒ Configurable If 'configurable', how? Using a config file	
Requires Application Layer Confirmation: ☒ Never ☐ Always (not recommended) ☐ When reporting Event Data (Slave devices only) ☐ When sending multi-fragment responses (Slave devices only) ☐ Sometimes If 'sometimes', when? _____ ☐ Configurable If 'configurable', how?	
Timeouts while waiting for: Data Link Confirm ☐ None ☐ Fixed at _____ ☐ Variable ☒ Configurable Complete Appl. Fragment ☐ None ☐ Fixed at _____ ☐ Variable ☒ Configurable Application Confirm ☒ None ☐ Fixed at _____ ☐ Variable ☐ Configurable Complete Appl. Response ☒ None ☐ Fixed at _____ ☐ Variable ☐ Configurable Others_____	

DNP3 Device Profile Document		
Sends/Executes Control Operations:		
WRITE Binary Outputs	☒ Never	☐ Always
	☐ Sometimes	☐ Configurable
SELECT/OPERATE	☐ Never	☐ Always
	☒ Sometimes	☐ Configurable
DIRECT OPERATE	☐ Never	☐ Always
	☒ Sometimes	☐ Configurable
DIRECT OPERATE - NO ACK	☐ Never	☐ Always
	☒ Sometimes	☐ Configurable
Count > 1	☐ Never	☐ Always
	☒ Sometimes	☐ Configurable
Pulse On	☐ Never	☐ Always
	☒ Sometimes	☐ Configurable
Pulse Off	☐ Never	☐ Always
	☒ Sometimes	☐ Configurable
Latch On	☐ Never	☐ Always
	☒ Sometimes	☐ Configurable
Latch Off	☐ Never	☐ Always
	☒ Sometimes	☐ Configurable
Queue	☒ Never	☐ Always
	☐ Sometimes	☐ Configurable
Clear Queue	☒ Never	☐ Always
	☐ Sometimes	☐ Configurable
The type of control operation issued depends on the local softw are executing and the configuration of the DNP3 Client. The Client can be configured to send all controls as Direct Operate, SBO, or Direct Operate No Ack. The Client can only send one control per DNP message.		
Reports Binary Input Change Events when no specific variation requested (Slave Only): ☒ Never ☐ Only time-tagged ☐ Only non time-tagged ☐ Configurable to send both, one or the other (attach explanation)		Reports time-tagged Binary Input Change Events when no specific variation requested: ☒ Never ☐ Binary Input change with time ☐ Binary Input change with Relative time ☐ Configurable (attach explanation)

<table>
<tr><th colspan="2">DNP3
Device Profile Document</th></tr>
<tr><td colspan="2">Master Expects Binary Input Change Events:
☒ Either time-tagged or non-time-tagged for a single event
☐ Both time-tagged and non-time-tagged for a single event
☐ Configurable (attach explanation)</td></tr>
<tr><td>Sends Unsolicited Responses (Slave Only):
☒ Never
☐ Configurable (attach explanation)
☐ Only certain objects
☐ Sometimes (attach explanation)
☐ ENABLE/DISABLE UNSOLICITED Function codes Supported</td><td>Sends Static Data in Unsolicited Responses (Slave Only):
☒ Never
☐ When Device Restarts
☐ When Status Flags Change
No other options are permitted.</td></tr>
<tr><td colspan="2">Sends Multi-Fragment Responses (Slave Only): ☐ Yes ☒ No</td></tr>
</table>

The Client sends to remote devices the subset of DNP3 objects, variations, qualifiers and function codes listed in Table 1.

Table 1: DNP3 Subset Sent by the Client under normal operation

Object			Request		
Obj	**Var**	**Description**	**Function Codes**	**Qual Codes (Hex)**	**Sent...**
1	0	Binary Input [All variations]	READ (1)	06	On a periodic basis as configured by the user
2	0	Binary Input Change [All variations]	READ (1)	06	On a periodic basis as configured by the user
10	1	Binary Output Status	READ (1)	06	On a periodic basis as configured by the user Sent immediately following the issue of a CROB command. Also sent (according to user config) if LOCAL IIN detected.
12	1	Control Relay Output Block	SELECT (3) OPERATE (4) DIRECT OPERATE (5) DIRECT OPERATE - NO ACK (6)	28	Only on demand.
20	0	Binary Accumulators [All Variations]	READ(1)	06	On a periodic basis as configured by the user
21	0	Frozen Accumulators [All Variations]	READ(1)	06	On a periodic basis as configured by the user
22	0	Accumulator Change Events [All Variations]	READ(1)	06	On a periodic basis as configured by the user
23	0	Frozen Accumulator Change Events [All Variations]	READ(1)	06	On a periodic basis as configured by the user
30	0,1,2,5,6	Analog Inputs [All Variations, 16 Bit, 32 Bit, Float, Long Float]	READ(1)	06	On a periodic basis as configured by the user
31	0	Frozen Analog Inputs [All Variations]	READ(1)	06	On a periodic basis as configured by the user
32	0	Analog Input Change Events [All Variations]	READ(1)	06	On a periodic basis as configured by the user

Object			Request		
Obj	Var	Description	Function Codes	Qual Codes (Hex)	Sent...
33	0	Frozen Analog Input Change Events [All Variations]	READ(1)	06	On a periodic basis as configured by the user
40	0,1,2	Analog Outputs [All Variations, 16 Bit, 32 Bit]	READ(1)	06	On a periodic basis as configured by the user
50	1	Time and Date	WRITE (2)	07 quant = 1	Regularly scheduled and/or in response to TIME SYNC REQUIRED IIN.
60	1	Class 0 Data	READ (1) ENABLE UNSOLICITED (20) DISABLE UNSOLICITED (21)	06	READ sent periodically, in response to various IINs. ENABLE/DISABLE UNSOLICITED sent as configured upon startup, and on receipt of a NULL Unsolicited Response
60	2	Class 1 Data	READ (1)	06	On periodic basis, to retrieve a configured number of class 1 events.
				06	On periodic basis, in response to various IINs.
			ENABLE UNSOLICITED (20) DISABLE UNSOLICITED (21)	06	ENABLE/DISABLE UNSOLICITED sent as configured upon startup, and on receipt of a NULL Unsolicited Response
60	3	Class 2 Data	READ (1)	08	On periodic basis, to retrieve a configured number of class 2 events.
				06	On periodic basis, in response to various IINs.
			ENABLE UNSOLICITED (20) DISABLE UNSOLICITED (21)	06	ENABLE/DISABLE UNSOLICITED sent as configured upon startup, and on receipt of a NULL Unsolicited Response
60	4	Class 3 Data	READ (1)	08	On periodic basis, to retrieve a configured number of class 3 events.
				06	On periodic basis, in response to various IINs.
			ENABLE UNSOLICITED (20) DISABLE UNSOLICITED (21)	06	ENABLE/DISABLE UNSOLICITED sent as configured upon startup, and on receipt of a NULL Unsolicited Response

Object			Request		
Obj	Var	Description	Function Codes	Qual Codes (Hex)	Sent...
80	1	Internal Indication	WRITE (2)	00	On receipt of a response containing the DEVICE RESTART bit set.
No object			DELAY MEASUREMENT (23)	None	On demand. If Auto Time Synchronization Enable is True it will also be sent in response to the TIME SYNC NEEDED IIN.

1.1 Profile of Normal Operation

The following table describes all the DNP3 objects, function codes, and qualifiers sent or received by the DNP3 Client software during normal operation. Each line of the table lists an object variation.

If the *Request* columns are blank, the Client does not send that object variation to remote devices. If the *Request* columns are non-blank, they indicate that the Client sends that object variation, with the specified function codes, under certain conditions.

The *Sent When* column describes these conditions, as follows:

D : The Client sends the request when a local software application **Demands** it do so.

O : The Client sends the request following a previous **Output** request.

I : The Client sends the request as a result of an **Internal Indication** from the remote device.

A : The Client sends the request **Automatically** as a part of its own operation, e.g. at start-up time, or if the local time changes.

P : The Client sends the request **Periodically**.

(C) : Following any of the above indicates the Client can be **Configured** to perform or not perform the request in this manner.

If the *Response* columns are blank, the Client does not accept the object variation and will discard any message containing that object variation. If the *Response* columns are non-blank, the Client accepts the object variation in responses, provided the remote device uses a valid function code and qualifier.

A "✓" in the *Uses* column means that the Client stores or forwards the data; otherwise, it ignores the object when parsing.

Table 2: DNP3 Subset Implemented by the Client

Object			Request			Response	
Obj	Var	Description	Func Codes (Dec)	Qual Codes (Hex)	Sent When ...	Func Codes (Dec)	Uses
1	0	Binary Input - All Variations	1	06	P(c)		
1	1	Binary Input				129, 130	✓
1	2	Binary Input With Status				129, 130	✓
2	0	Binary Input Change - All Variations	1	06	P(c)		
2	1	Binary Input Change Without Time				129, 130	✓
2	2	Binary Input Change With Time				129, 130	✓
2	3	Binary Input Change With Relative Time				129, 130	✓
10	0	Binary Output - All	1	06	P(c), I(c), O	129	
10	1	Binary Output					
10	2	Binary Output Status				129, 130	✓
12	0	Control Block - All Variations					
12	1	Control Relay Output Block	3, 4, 5, 6	28	D (c)	129	✓
12	2	Pattern Control Block					
12	3	Pattern Mask					
20	0	Binary Counter - All Variations	1, 7	06	P (C), O		
20	1	32-Bit Binary Counter				129, 130	✓
20	2	16-Bit Binary Counter				129, 130	✓
20	3	32-Bit Delta Counter				129, 130	✓
20	4	16-Bit Binary Counter				129, 130	✓
20	5	32-Bit Binary Counter Without Flag				129, 130	✓
20	6	16-Bit Binary Counter Without Flag				129, 130	✓
20	7	32-Bit Delta Counter Without Flag				129, 130	✓
20	8	16-Bit Delta Counter Without Flag				129, 130	✓
21	0	Frozen Counter - All Variations	1	06	P (C), O		
21	1	32-Bit Frozen Counter				129, 130	✓
21	2	16-Bit Frozen Counter				129, 130	✓

Object			Request			Response	
Obj	Var	Description	Func Codes (Dec)	Qual Codes (Hex)	Sent When ...	Func Codes (Dec)	Uses
21	3	32-Bit Frozen Delta Counter				129, 130	✓
21	4	16-Bit Frozen Delta Counter				129, 130	✓
21	5	32-Bit Frozen Counter With Time of Freeze				129, 130	✓
21	6	16-Bit Frozen Counter With Time of Freeze				129, 130	✓
21	7	32-Bit Frozen Delta Counter With Time of Freeze				129, 130	✓
21	8	16-Bit Frozen Delta Counter With Time of Freeze				129, 130	✓
21	9	32-Bit Frozen Counter Without Flag				129, 130	✓
21	10	16-Bit Frozen Counter Without Flag				129, 130	✓
21	11	32-Bit Frozen Delta Counter Without Flag				129, 130	✓
21	12	16-Bit Frozen Delta Counter Without Flag				129, 130	✓
22	0	Counter Change Event - All Variations	1	06	P(c)		
22	1	32-Bit Counter Change Event Without Time				129, 130	✓
22	2	16-Bit Counter Change Event Without Time				129, 130	✓
22	3	32-Bit Delta Counter Change Event Without Time				129, 130	✓
22	4	16-Bit Delta Counter Change Event Without Time				129, 130	✓
22	5	32-Bit Counter Change Event With Time				129, 130	✓
22	6	16-Bit Counter Change Event With Time				129, 130	✓
22	7	32-Bit Delta Counter Change Event With Time				129, 130	✓
22	8	16-Bit Delta Counter Change Event With Time				129, 130	✓
23	0	Frozen Counter Event - All Variations	1	06	P(c)		
23	1	32-Bit Frozen Counter Event Without Time				129, 130	✓
23	2	16-Bit Frozen Counter Event Without Time				129, 130	✓

Object			Request			Response	
Obj	Var	Description	Func Codes (Dec)	Qual Codes (Hex)	Sent When ...	Func Codes (Dec)	Uses
23	3	32-Bit Frozen Delta Counter Event Without Time				129, 130	✓
23	4	16-Bit Frozen Delta Counter Event Without Time				129, 130	✓
23	5	32-Bit Frozen Counter Event With Time				129, 130	✓
23	6	16-Bit Frozen Counter Event With Time				129, 130	✓
23	7	32-Bit Frozen Delta Counter Event With Time				129, 130	✓
23	8	16-Bit Frozen Delta Counter Event With Time				129, 130	✓
30	0	Analog Input - All Variations	1	06	P(c) O(c)		
30	1	32-Bit Analog Input	1	06	P(c)	129, 130	✓
30	2	16-Bit Analog Input	1	06	P(c)	129, 130	✓
30	3	32-Bit Analog Input Without Flag				129, 130	✓
30	4	16-Bit Analog Input Without Flag				129, 130	✓
30	5	32-Bit Floating Point Analog Input	1	06	P(c)	129, 130	✓
30	6	64-Bit Floating Point Analog Input	1	06	P(c)	129, 130	✓
31	0	Frozen Analog Input - All Variations	1	06	P(c)		
31	1	32-Bit Frozen Analog Input				129, 130	✓
31	2	16-Bit Frozen Analog Input				129, 130	✓
31	3	32-Bit Frozen Analog Input With Time of Freeze				129, 130	✓
31	4	16-Bit Frozen Analog Input With Time of Freeze				129, 130	✓
31	5	32-Bit Frozen Analog Input Without Flag				129, 130	✓
31	6	16-Bit Frozen Analog Input Without Flag				129, 130	✓
32	0	Analog Change Event - All Variations	1	06	P(c)		
32	1	32-Bit Analog Change Event Without Time				129, 130	✓

Object			Request			Response	
Obj	Var	Description	Func Codes (Dec)	Qual Codes (Hex)	Sent When ...	Func Codes (Dec)	Uses
32	2	16-Bit Analog Change Event Without Time				129, 130	✓
32	3	32-Bit Analog Change Event With Time				129, 130	✓
32	4	16-Bit Analog Change Event With Time				129, 130	✓
32	5	32-Bit Floating Point Analog Change Event without Time				129, 130	✓
32	6	64-Bit Floating Point Analog Change Event without Time				129, 130	✓
32	7	32-Bit Floating Point Analog Change Event with Time				129, 130	✓
32	8	64-Bit Floating Point Analog Change Event with Time				129, 130	✓
33	0	Frozen Analog Event - All Variations	1	06	P(c)		
33	1	32-Bit Frozen Analog Event Without Time				129, 130	✓
33	2	16-Bit Frozen Analog Event Without Time				129, 130	✓
33	3	32-Bit Frozen Analog Event With Time				129, 130	✓
33	4	16-Bit Frozen Analog Event With Time				129, 130	✓
40	0	Analog Output Status - All Variations	1	06	P(c), O		
40	1	32-Bit Analog Output Status	1	06	P(c)	129, 130	✓
40	2	16-Bit Analog Output Status	1	06	P(c)	129, 130	✓
41	0	Analog Output Block - All Variations					
41	1	32-Bit Analog Output Block					
41	2	16-Bit Analog Output Block					
50	0	Time and Date - All Variations					
50	1	Time and Date	2	07 where qnty = 1	I (C), P (C)	129, 130	
50	2	Time and Date With Interval				129, 130	
51	0	Time and Date CTO - All Variations					
51	1	Time and Date CTO				129, 130	✓

Object			Request			Response	
Obj	Var	Description	Func Codes (Dec)	Qual Codes (Hex)	Sent When ...	Func Codes (Dec)	Uses
51	2	Unsynchronized Time and Date CTO				129, 130	✓
52	0	Time Delay - All Variations					
52	1	Time Delay Coarse				129	✓
52	2	Time Delay Fine				129	✓
60	0						
60	1	Class 0 Data	1	06	P (C), I		
60	2	Class 1 Data	1	06	P (C), I, O(C)		
60	3	Class 2 Data	1	06	P (C), I, O(C)		
60	4	Class 3 Data	1	06	P (C) I, O(C)		
70	1	File Identifier				129	
80	1	Internal Indications	2	00	I	129, 130	✓
81	1	Storage Object				129, 130	
82	1	Device Profile				129, 130	
83	1	Private Registration Object				129, 130	
83	2	Private Registration Object Descriptor				129, 130	
90	1	Application Identifier					
100	1	Short Floating Point					
100	2	Long Floating Point					
100	3	Extended Floating Point					
101	1	Small Packed Binary-Coded Decimal					
101	2	Medium Packed Binary Coded Decimal					
101	3	Large Packed Binary_Coded Decimal					
No Object			23		I (C)		

MODIFICATION RECORD

VERSION	REV.	DATE	AUTHOR	CHANGE DESCRIPTION
1.00	0	2nd May, 2019	G. LaMarre	Created.

GE
Grid Solutions

IEC 60870-5-101-104 Server (DPA) for the Multifunction Controller Platform

Conformance Statement

NTEK-A024M-0CS

Version 1.00 Revision 0

Associated Software Release: Version 1.00

imagination at work

General

COPYRIGHT NOTICE

© 2019, General Electric Company. All rights reserved.

The Software Product described in this documentation may only be used in accordance with the applicable License Agreement. The Software Product and Associated Material are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable, and are delivered with Restricted Rights. Such restricted rights are those identified in the License Agreement, and as set forth in the "Restricted Rights Notice" contained in paragraph (g) (3) (Alternate III) of FAR 52.227-14, Rights in Data-General, including Alternate III (June 1987).

If applicable, any use, modification, reproduction release, performance, display or disclosure of the Software Product and Associated Material by the U.S. Government shall be governed solely by the terms of the License Agreement and shall be prohibited except to the extent expressly permitted by the terms of the License Agreement.

The information contained in this online publication is the exclusive property of General Electric Company, except as otherwise indicated. You may view, copy and print documents and graphics incorporated in this online publication (the "Documents") subject to the following: (1) the Documents may be used solely for personal, informational, non-commercial purposes; (2) the Documents may not be modified or altered in any way; and (3) General Electric Company withholds permission for making the Documents or any portion thereof accessible via the internet. Except as expressly provided herein, you may not use, copy, print, display, reproduce, publish, license, post, transmit or distribute the Documents in whole or in part without the prior written permission of General Electric Company. If applicable, any use, modification, reproduction, release, performance, display, or disclosure of the Software Product and Associated Material by the U.S. Government shall be governed solely by the terms of the License Agreement and shall be prohibited except to the extent expressly permitted by the terms of the License Agreement.

The information contained in this online publication is subject to change without notice. The software described in this online publication is supplied under license and may be used or copied only in accordance with the terms of such license.

TRADEMARK NOTICES

GE and are trademarks and service marks of General Electric Company.

* Trademarks of General Electric Company.

IEC is a registered trademark of Commission Electrotechnique Internationale.

Other company or product names mentioned in this document may be trademarks or registered trademarks of their respective companies.

Contents

1. IEC 60870-5-101 DPA Interoperability Profile 4

1.1 System or Device (8.1) 5
1.2 Network Configuration (8.2) 5
1.3 Physical Layer (8.3) 5
1.4 Link Layer (8.4) 6
1.5 Application Layer (8.5) 7
1.6 Basic Application Functions (8.6) 12

2. IEC 60870-5-104 DPA Interoperability Profile 16

2.1 System or Device (9.1) 16
2.2 Network Configuration (9.2) 16
2.3 Physical layer (9.3) 16
2.4 Link Layer (9.4) 17
2.5 Application Layer (9.5) 17
2.6 Basic Application Functions (9.6) 23

1. IEC 60870-5-101 DPA Interoperability Profile

This interoperability profile presents the sets of parameters and alternatives, and identifies by selection, those items required for implementation in the GE Grid Solutions MCP. The following legend reflects the options used in this selection of requirements:

- ☒ Function or ASDU is used as standardized (default)
- ■ A black check box indicate that the option cannot be selected (and is thus not required)
- R Function or ASDU is used in reverse mode
- B Function or ASDU is used in standard and reverse mode
- ☐ Function or ASDU is not used

In cases where several options are available, for example, multiple lengths of address fields, the GE Grid Solutions MCP shall be configurable to use the required value.

In this document, the bracketed number trailing each subheading title refers to the corresponding section number within the IEC® 60870-5-101 standard.

1.1 System or Device (8.1)

- ☐ System definition
- ☐ Controlling station definition (Master)
- ☒ Controlled station definition (Slave)

1.2 Network Configuration (8.2)

(network-specific parameter)

- ☒ Point-to-point
- ☒ Multiple point-to-point
- ☒ Multipoint-party line
- ☒ Multipoint-star

1.3 Physical Layer (8.3)

(network-specific parameter)

1.3.1 Transmission Speed (Control Direction)

Unbalanced interchange circuit V.24/V.28 Standard	**Unbalanced interchange circuit V.24/V.28 Recommended if > 1,200 bit/s**	**Balanced Interchange Circuit X.24/X.27**	
☐ 100 bit/s	☒ 2,400 bit/s	☐ 2,400 bit/s	☐ 56,000 bit/s
☐ 200 bit/s	☒ 4,800 bit/s	☐ 4,800 bit/s	☐ 64,000 bit/s
☒ 300 bit/s	☒ 9,600 bit/s	☐ 9,600 bit/s	
☒ 600 bit/s	☒ 19,200 bit/s	☐ 19,200 bit/s	
☒ 1,200 bit/s		☐ 38,400 bit/s	

1.3.2 Transmission Speed (Monitor Direction)

Unbalanced Interchange Circuit V.24/V.28 Standard	**Unbalanced Interchange Circuit V.24/V.28 Recommended if > 1,200 bit/s**	**Balanced Interchange Circuit X.24/X.27**	
☐ 100 bit/s	☒ 2,400 bit/s	☐ 2,400 bit/s	☐ 56,000 bit/s
☐ 200 bit/s	☒ 4,800 bit/s	☐ 4,800 bit/s	☐ 64,000 bit/s
☒ 300 bit/s	☒ 9,600 bit/s	☐ 9,600 bit/s	
☒ 600 bit/s	☒ 19,200 bit/s	☐ 19,200 bit/s	
☒ 1,200 bit/s		☐ 38,400 bit/s	

NOTE: The DPA shall only support the Unbalanced Interchange (Circuit V2.4/V2.8). The combination of V.24 and V.28 is ITU-T's equivalent to the EIA's RS-232.

1.4 Link Layer (8.4)

(network-specific parameter)

Frame format FT 1.2 (IEC 60870-5-1 Section 6.2.4.2) fixed and variable length is used (length is configurable).
Single character 1 (IEC 60870-5-1 Section 6.2.4.3) is used as an acknowledge.
Fixed time out interval is used (value is configurable).

Link Transmission Procedure

- ☒ Balanced transmission
- ☒ Unbalanced transmission

Address Field of the Link

- ☐ Not present (balanced transmission only)
- ☒ One byte
- ☒ Two bytes
- ☒ Structured
- ☒ Unstructured

Frame Length

255 Maximum length L (number of bytes)

configurable Number of repetitions.

NOTE: For unbalanced mode, Maximum Frame Length (L) = Maximum ASDU frame length. For balanced mode, Max Frame Length (L) = Maximum ASDU frame length + 1 + Link Address Length.

When using an unbalanced link layer, the following ASDU types are returned in Class 2 messages (low priority) with the indicated clauses of transmission:

☒ The standard assignment of ASDUs to Class 2 messages is used as follows

Type identification	Cause of transmission
9,11,13,21	<1>

☒ A special assignment of ASDUs to Class 2 messages is used as follows

Type identification	Cause of transmission
1,2,3,4,5,6,7,8,9,10,11,12,13,14,20,21,30,31,32,33,34,35	<2>
1,2,3,4,5,6,7,8,9,10,11,12,13,14,20,21,30,31,32,33,34,35	<5>
1,2,3,4,5,6,7,8,9,10,11,12,13,14,20,21,30,31,32,33,34,35	<20-36>

NOTE: In response to a Class 2 poll, a controlled station can respond with Class 1 data when there is no Class 2 data available.

1.5 Application Layer (8.5)

1.5.1 Transmission Mode for Application Data

Mode 1 (Least significant byte first), as defined in clause 4.10 of IEC 60870-5-4, is used exclusively for all application data.

1.5.2 Common Address of ASDU

(system-specific parameter)

☒ One byte ☒ Two bytes

1.5.3 Information Object Address

(system-specific parameter)

☒ One byte
☒ Two bytes
☒ Three bytes

☒ Structured
☒ Unstructured

1.5.4 Cause of Transmission

(system- specific parameter)

☒ One byte

☒ Two bytes (with originator address).
Set to zero in case of no originator address

1.5.5 Selection of Standard ASDUs

1.5.5.1 Process Information in Monitor Direction

(station-specific parameter)

☒	<1>	:=	Single-point information	M_SP_NA_1
☒	<2>	:=	Single-point information with time tag	M_SP_TA_1
☒	<3>	:=	Double-point information	M_DP_NA_1
☒	<4>	:=	Double-point information with time tag	M_DP_TA_1
☒	<5>	:=	Step position information	M_ST_NA_1
☒	<6>	:=	Step position information with time tag	M_ST_TA_1
☒	<7>	:=	Bitstring of 32 bits	M_BO_NA_1
☒	<8>	:=	Bitstring of 32 bits with time tag	M_BO_TA_1
☒	<9>	:=	Measured value, normalized value	M_ME_NA_1
☒	<10>	:=	Measured value, normalized value with time tag	M_ME_TA_1
☒	<11>	:=	Measured value, scaled value	M_ME_NB_1
☒	<12>	:=	Measured value, scaled value with time tag	M_ME_TB_1

☒	<13>	:=	Measured value, short floating-point value	M_ME_NC_1
☒	<14>	:=	Measured value, short floating-point value with time tag	M_ME_TC_1
☒	<15>	:=	Integrated totals	M_IT_NA_1
☒	<16>	:=	Integrated totals with time tag	M_IT_TA_1
☐	<17>	:=	Event of protection equipment with time tag	M_EP_TA_1
☐	<18>	:=	Packed start events of protection equipment with time tag	M_EP_TB_1
☐	<19>	:=	Packed output circuit information of protection equipment with time tag	M_EP_TC_1
☒	<20>	:=	Packed single-point information with status change detection	M_PS_NA_1
☒	<21>	:=	Measured value, normalized value without quality descriptor	M_ME_ND_1
☒	<30>	:=	Single-point information with time tag CP56Time2a	M_SP_TB_1
☒	<31>	:=	Double-point information with time tag CP56Time2a	M_DP_TB_1
☒	<32>	:=	Step position information with time tag CP56Time2a	M_ST_TB_1
☒	<33>	:=	Bit string of 32 bits with time tag CP56Time2a	M_BO_TB_1
☒	<34>	:=	Measured value, normalized value with time tag CP56Time2a	M_ME_TD_1
☒	<35>	:=	Measured value, scaled value with time tag CP56Time2a	M_ME_TE_1
☒	<36>	:=	Measured value, short floating point with time tag CP56Time2a	M_ME_TF_1
☒	<37>	:=	Integrated totals with time tag CP56Time2a	M_IT_TB_1
☐	<38>	:=	Event of protection equipment with time tag CP56Time2a	M_EP_TD_1
☐	<39>	:=	Packed start events of protection equipment with time tag CP56Time2a	M_EP_TE_1
☐	<40>	:=	Packed output circuit information of protection equipment with time tag CP56Time2a	M_EP_TF_1

1.5.5.2 Process Information in Control Direction

(station-specific parameter)

☒	<45>	:=	Single command	C_SC_NA_1
☒	<46>	:=	Double command	C_DC_NA_1
☒	<47>	:=	Regulating step command	C_RC_NA_1
☒	<48>	:=	Set point command, normalized values	C_SE_NA_1
☒	<49>	:=	Set point command, scaled value	C_SE_NB_1
☒	<50>	:=	Set point command, short floating-point value	C_SE_NC_1
☐	<51>	:=	Bitstring of 32 bits	C_BO_NA_1

1.5.5.3 System Information in Monitor Direction

(station-specific parameter)

☒	<70>	:=	End of initialization	M_EI_NA_1

1.5.5.4 System Information in Control Direction

(station specific parameter)

☒	<100>	:=	Interrogation command	C_IC_NA_1
☒	<101>	:=	Counter interrogation command	C_CI_NA_1
☒	<102>	:=	Read command	C_RD_NA_1
☒	<103>	:=	Clock synchronization command	C_CS_NA_1
☒	<104>	:=	Test command	C_TS_NA_1
☒	<105>	:=	Reset process command	C_RP_NC_1
☒	<106>	:=	Delay acquisition command	C_CD_NA_1

1.5.5.5 Parameter in Control Direction

(station-specific parameter)

☒	<110>	:=	Parameter of measured value, normalized value	P_ME_NA_1
☒	<111>	:=	Parameter of measured value, scaled value	P_ME_NB_1
☒	<112>	:=	Parameter of measured value, short floating-point value	P_ME_NC_1
☒	<113>	:=	Parameter activation	P_AC_NA_1

1.5.5.6 File Transfer

(station-specific parameter)
File Download and Upload

☒	<120>	:=	File ready	F_FR_NA_1
☒	<121>	:=	Section ready	F_SR_NA_1
☒	<122>	:=	Call directory, select file, call file, call section	F_SC_NA_1
☒	<123>	:=	Last section, last segment	F_LS_NA_1
☒	<124>	:=	Ack file, ack section	F_AF_NA_1
☒	<125>	:=	Segment	F_SG_NA_1
☒	<126>	:=	Directory {blank or **x**, only available in monitor (standard) direction}	F_DR_TA_1

1.5.5.7 Type identifier and Cause of Transmission Assignments

(station-specific parameter)
Shaded box[es] are not required.
Blank = Function or ASDU is not used

Type identification		Cause of transmission																		
		1	2	3	4	5	6	7	8	9	10	11	12	13	20 to 36	37 to 41	44	45	46	47
<1>	M_SP_NA_1		x	x		x									x					
<2>	M_SP_TA_1			x		x														
<3>	M_DP_NA_1		x	x		x									x					
<4>	M_DP_TA_1			x		x														
<5>	M_ST_NA_1		x	x		x									x					
<6>	M_ST_TA_1			x		x														
<7>	M_BO_NA_1		x	x		x									x					
<8>	M_BO_TA_1			x		x														
<9>	M_ME_NA_1	x	x	x		x									x					
<10>	M_ME_TA_1			x		x														
<11>	M_ME_NB_1	x	x	x		x									x					
<12>	M_ME_TB_1			x		x														
<13>	M_ME_NC_1	x	x	x		x									x					
<14>	M_ME_TC_1			x		x														
<15>	M_IT_NA_1			x												x				
<16>	M_IT_TA_1			x												x				
<17>	M_EP_TA_1																			
<18>	M_EP_TB_1																			
<19>	M_EP_TC_1																			
<20>	M_PS_NA_1		x	x		x									x					
<21>	M_ME_ND_1		x	x		x									x					
<30>	M_SP_TB_1			x		x														
<31>	M_DP_TB_1			x		x														
<32>	M_ST_TB_1			x		x														
<33>	M_BO_TB_1			x		x														
<34>	M_ME_TD_1			x		x														
<35>	M_ME_TE_1			x		x														
<36>	M_ME_TF_1			x		x														
<37>	M_IT_TB_1			x												x				
<38>	M_EP_TD_1																			
<39>	M_EP_TE_1																			
<40>	M_EP_TF_1																			
<45>	C_SC_NA_1						x	x	x	x	x						x	x	x	x
<46>	C_DC_NA_1						x	x	x	x	x						x	x	x	x
<47>	C_RC_NA_1						x	x	x	x	x						x	x	x	x
<48>	C_SE_NA_1						x	x	x	x	x						x	x	x	x
<49>	C_SE_NB_1						x	x	x	x	x						x	x	x	x

Type identification		Cause of transmission																	
		1	2	3	4	5	6	7	8	9	10	11	12	13	20 to 36	37 to 41	44	45	46	47
<50>	C_SE_NC_1						x	x	x	x	x						x	x	x	x
<51>	C_BO_NA_1																			
<70>	M_EI_NA_1				x															
<100>	C_IC_NA_1						x	x	x	x	x						x	x	x	x
<101>	C_CI_NA_1						x	x			x						x	x	x	x
<102>	C_RD_NA_1					x											x	x	x	x
<103>	C_CS_NA_1			x			x	x									x	x	x	x
<104>	C_TS_NA_1						x	x									x	x	x	x
<105>	C_RP_NA_1						x	x									x	x	x	x
<106>	C_CD_NA_1			x			x	x									x	x	x	x
<110>	P_ME_NA_1						x	x												
<111>	P_ME_NB_1						x	x												
<112>	P_ME_NC_1						x	x												
<113>	P_AC_NA_1						x	x	x	x										
<120>	F_FR_NA_1													x						
<121>	F_SR_NA_1													x						
<122>	F_SC_NA_1					x								x						
<123>	F_LS_NA_1													x						
<124>	F_AF_NA_1													x						
<125>	F_SG_NA_1													x						
<126>	F_DR_TA_1					x														

1.6 Basic Application Functions (8.6)

1.6.1 Station Initialization

(station-specific parameter)

☒ Remote initialization

1.6.2 Cyclic Data Transmission

(station-specific parameter)

☒ Cyclic data transmission

1.6.3 Read Procedure

(station-specific parameter)

☒ Read Procedure

1.6.4 Spontaneous Transmission

(station-specific parameter)

☒ Spontaneous transmission

1.6.5 Double Transmission of Information Objects with Cause of Transmission Spontaneous

(Station-specific parameter)
The following type identification can be transmitted in succession caused by a single status change of an information object. The information object addresses for which double transmission is enabled are defined in a project-specific list.

☐ Single-point information M_SP_NA_1, M_SP_TA_1, M_SP_TB_1 and M_PS_NA_1
☐ Double-point information M_DP_NA_1, M_DP_TA_1 and M_DP_TB_1
☐ Step position information M_ST_NA_1, M_ST_TA_1 and M_ST_TB_1
☐ Bitstring of 32 bits M_BO_NA_1, M_BO_TA_1 and M_BO_TB_1
☐ Measured value, normalized value M_ME_NA_1, M_ME_TA_1, M_ME_ND_1 and M_ME_TD_1
☐ Measured value, scaled value M_ME_NB_1, M_ME_TB_1 and M_ME_TE_1
☐ Measured value, short floating-point number M_ME_NC_1, M_ME_TC_1 and M_ME_TF_1

1.6.6 Station Interrogation

(station-specific parameter)

☒ global
☒ group 1 ☒ group 7 ☒ group 13

☒ group 2	☒ group 8	☒ group 14
☒ group 3	☒ group 9	☒ group 15
☒ group 4	☒ group 10	☒ group 16
☒ group 5	☒ group 11	Information Object Address assigned to each group shall be shown in a separate table
☒ group 6	☒ group 12	

1.6.7 Clock Synchronization

(station-specific parameter)

- ☒ Clock synchronization
- ☐ Day of week used
- ☐ RES1, GEN (time tag substituted/not substituted used
- ☐ SU-bit (summertime) used

1.6.8 Command Transmission

(object-specific parameter)

- ☒ Direct command transmission
- ☒ Direct set point command transmission
- ☒ Selected and Execute Command
- ☒ Select and execute set point command
- ☒ C-SE ACTTERM Used

- ☒ No additional definition
- ☒ Short pulse duration (duration determined by a system parameter in the controlled station)
- ☒ Long pulse duration (duration determined by a system parameter in the controlled station)
- ☒ Persistent output

1.6.9 Transmission of Integrated Totals

(station or object-specific parameter)

- ☒ Mode A: Local freeze with spontaneous transmission
- ☐ Mode B: Local freeze with counter interrogation
- ☒ Mode C: Freeze and transmit by counter-interrogation command
- ☐ Mode D: Freeze by counter-interrogation command, frozen values reported spontaneously

- ☒ Counter read
- ☒ Counter freeze without reset
- ☒ Counter freeze with reset
- ☒ Counter reset

- ☒ General request counter
- ☒ Request counter group 1
- ☒ Request counter group 2
- ☒ Request counter group 3
- ☒ Request counter group 4

Addresses per group must be defined

1.6.10 Parameter Loading

(object-specific parameter)

- ☒ Threshold value
- ☐ Smoothing factor
- ☒ Low limit for transmission of measured value
- ☒ High limit for transmission of measured value

1.6.11 Parameter Activation

(object-specific parameter)

- ☒ Activ/deactiv. of persistent cyclic or periodic transmission of the addressed object

1.6.12 Test Procedure

(station-specific parameter)

☒ Test procedure

1.6.13 File Transfer

(station-specific parameter)

1.6.13.1 File Transfer in Monitor Direction

☐ Transparent file
☐ Transmission of disturbance data of protection equipment
☐ Transmission of sequences of events
☐ Transmission of sequences of recorded analogue values

1.6.13.2 File Transfer in Control Direction

☒ Transparent file

1.6.14 Background Scan

(station-specific parameter)

☒ Background scan

1.6.15 Acquisition of Transmission Delay

(station-specific parameter)

☒ Acquisition of transmission delay

2. IEC 60870-5-104 DPA Interoperability Profile

This interoperability profile presents the sets of parameters and alternatives, and identifies by selection, those items required for implementation in the GE Grid Solutions MCP. The following legend reflects the options used in this selection of requirements:

- ☒ Function or ASDU is used as standardized (default)
- ■ A black check box indicate that the option cannot be selected (and is thus not required)
- R Function or ASDU is used in reverse mode
- B Function or ASDU is used in standard and reverse mode
- ☐ Function or ASDU is not used

The text descriptions of parameters, which are not applicable to this standard, are strike-through (corresponding check box is marked black).

In this document, the bracketed number trailing each subheading title refers to the corresponding section number within the IEC 60870-5-104 standard.

NOTE: In addition, the full specification of a system shall possibly require individual selection of certain parameters for certain parts of the system, such as the individual selection of scaling factors for individually addressable measured values.

2.1 System or Device (9.1)

- ☐ System definition
- ☐ Controlling station definition (Master)
- ☒ Controlled station definition (Slave)

2.2 Network Configuration (9.2)

(network-specific parameter)

- ■ ~~Point-to-point~~
- ■ ~~Multiple point-to-point~~
- ■ ~~Multipoint party line~~
- ■ ~~Multipoint star~~

2.3 Physical layer (9.3)

(network-specific parameter)

2.3.1 Transmission Speed (Control Direction)

Unbalanced interchange circuit V.24/V.28 Standard

- ~~100 bit/s~~
- ~~200 bit/s~~
- ~~300 bit/s~~
- ~~600 bit/s~~
- ~~1,200 bit/s~~

Unbalanced interchange circuit V.24/V.28 Recommended if > 1200 bit/s

- ~~2,400 bit/s~~
- ~~4,800 bit/s~~
- ~~9,600 bit/s~~
- ~~19,200 bit/s~~

Balanced Interchange Circuit X.24/X.27

- ~~2,400 bit/s~~
- ~~4,800 bit/s~~
- ~~9,600 bit/s~~
- ~~19,200 bit/s~~
- ~~38,400 bit/s~~
- ~~56,000 bit/s~~
- ~~64,000 bit/s~~

2.3.2 Transmission Speed (Monitor Direction)

Unbalanced Interchange Circuit V.24/V.28 Standard

- ~~100 bit/s~~
- ~~200 bit/s~~
- ~~300 bit/s~~
- ~~600 bit/s~~
- ~~1,200 bit/s~~

Unbalanced Interchange Circuit V.24/V.28 Recommended if > 1200 bit/s

- ~~2,400 bit/s~~
- ~~4,800 bit/s~~
- ~~9,600 bit/s~~
- ~~19,200 bit/s~~

Balanced Interchange Circuit X.24/X.27

- ~~2,400 bit/s~~
- ~~4,800 bit/s~~
- ~~9,600 bit/s~~
- ~~19,200 bit/s~~
- ~~38,400 bit/s~~
- ~~56,000 bit/s~~
- ~~64,000 bit/s~~

2.4 Link Layer (9.4)

(network-specific parameter)

Frame format FT1.2, single character 1 and the fixed time out interval is used exclusively in this companion standard.

Link Transmission Procedure

- ~~Balanced transmission~~
- ~~Unbalanced transmission~~

Frame Length

- ~~Maximum length L (number of bytes)~~

Address Field of the Link

- ~~Not present (balanced transmission only)~~
- ~~One byte~~
- ~~Two bytes~~
- ~~Structured~~
- ~~Unstructured~~

2.5 Application Layer (9.5)

2.5.1 Transmission Mode for Application Data

Mode 1 (Least significant byte first), as defined in clause 4.10 of IEC 870-5-4, is used exclusively in this companion standard.

2.5.2 Common address of ASDU

(system-specific parameter)

- ■ ~~One byte~~
- ☒ Two bytes

2.5.3 Information Object Address

(system-specific parameter)

- ■ ~~One byte~~
- ■ ~~Two bytes~~
- ☒ Three bytes
- ☒ Structured
- ☒ Unstructured

2.5.4 Cause of Transmission

(system-specific parameter)

- ■ ~~One byte~~
- ☒ Two bytes (with originator address). Originator address is set to zero if not used

2.5.5 Length of APDU

(system specific parameter)

The maximum length of APDU is 253 (default). The maximum length can be reduced by the system.

☐ 2**53** Maximum length of APDU

2.5.6 Selection of Standard ASDUs

2.5.6.1 Process Information in Monitor Direction

(station-specific parameter)

☒	<1>	:=	Single-point information	M_SP_NA_1
■	~~<2>~~	~~:=~~	~~Single-point information with time tag~~	~~M_SP_TA_1~~
☒	<3>	:=	Double-point information	M_DP_NA_1
■	~~<4>~~	~~:=~~	~~Double-point information with time tag~~	~~M_DP_TA_1~~
☒	<5>	:=	Step position information	M_ST_NA_1
■	~~<6>~~	~~:=~~	~~Step position information with time tag~~	~~M_ST_TA_1~~
☒	<7>	:=	Bitstring of 32 bits	M_BO_NA_1
■	~~<8>~~	~~:=~~	~~Bitstring of 32 bits with time tag~~	~~M_BO_TA_1~~
☒	<9>	:=	Measured value, normalized value	M_ME_NA_1
■	~~<10>~~	~~:=~~	~~Measured value, normalized value with time tag~~	~~M_ME_TA_1~~
☒	<11>	:=	Measured value, scaled value	M_ME_NB_1
■	~~<12>~~	~~:=~~	~~Measured value, scaled value with time tag~~	~~M_ME_TB_1~~
☒	<13>	:=	Measured value, short floating-point value	M_ME_NC_1
■	~~<14>~~	~~:=~~	~~Measured value, short floating-point value with time tag~~	~~M_ME_TC_1~~
☒	<15>	:=	Integrated totals	M_IT_NA_1

■	~~<16>~~	~~:=~~	~~Integrated totals with time tag~~	~~M_IT_TA_1~~
■	~~<17>~~	~~:=~~	~~Event of protection equipment with time tag~~	~~M_EP_TA_1~~
■	~~<18>~~	~~:=~~	~~Packed start events of protection equipment with time tag~~	~~M_EP_TB_1~~
■	~~<19>~~	~~:=~~	~~Packed output circuit information of protection equipment with time tag~~	~~M_EP_TC_1~~
☒	<20>	:=	Packed single-point information with status change detection	M_PS_NA_1
☒	<21>	:=	Measured value, normalized value without quality descriptor	M_ME_ND_1
☒	<30>	:=	Single-point information with time tag CP56Time2a	M_SP_TB_1
☒	<31>	:=	Double-point information with time tag CP56Time2a	M_DP_TB_1
☒	<32>	:=	Step position information with time tag CP56Time2a	M_ST_TB_1
☒	<33>	:=	Bit string of 32 bits with time tag CP56Time2a	M_BO_TB_1
☒	<34>	:=	Measured value, normalized value with time tag CP56Time2a	M_ME_TD_1
☒	<35>	:=	Measured value, scaled value with time tag CP56Time2a	M_ME_TE_1
☒	<36>	:=	Measured value, short floating point with time tag CP56Time2a	M_ME_TF_1
☒	<37>	:=	Integrated totals with time tag CP56Time2a	M_IT_TB_1
☐	<38>	:=	Event of protection equipment with time tag CP56Time2a	M_EP_TD_1
☐	<39>	:=	Packed start events of protection equipment with time tag CP56Time2a	M_EP_TE_1
☐	<40>	:=	Packed output circuit information of protection equipment with time tag CP56Time2a	M_EP_TF_1

Either the ASDUs of the set <2>, <4>, <6>, <8>, <10>, <12>, <14>, <16>, <17>, <18>, <19> or of the set <30> – <40> are used.

2.5.6.2 Process Information in Control Direction

(station-specific parameter)

☒	<45>	:=	Single command	C_SC_NA_1
☒	<46>	:=	Double command	C_DC_NA_1
☒	<47>	:=	Regulating step command	C_RC_NA_1
☒	<48>	:=	Set point command, normalized values	C_SE_NA_1
☒	<49>	:=	Set point command, scaled value	C_SE_NB_1
☒	<50>	:=	Set point command, short floating-point value	C_SE_NC_1
☐	<51>	:=	Bitstring of 32 bits	C_BO_NA_1
☒	<58>	:=	Single command with time tag CP56Time2a	C_SC_TA_1
☒	<59>	:=	Double command with time tag CP56Time2a	C_DC_TA_1
☒	<60>	:=	Regulating step command with time tag CP56Time2a	C_RC_TA_1
☒	<61>	:=	Set point command, normalized values with time tag CP56Time2a	C_SE_TA_1
☒	<62>	:=	Set point command, scaled value with time tag CP56Time2a	C_SE_TB_1
☒	<63>	:=	Set point command, short floating-point value with time tag CP56Time2a	C_SE_TC_1
☐	<64>	:=	Bitstring of 32 bits with time tag CP56Time2a	C_BO_TA_1

Either the ASDUs of the set <45> – <51> or of the set <58> – <64> are used.

2.5.6.3 System Information in Monitor Direction

(station-specific parameter)

☒	<70>	:=	End of initialization	M_EI_NA_1

2.5.6.4 System Information in Control Direction

(station-specific parameter)

☒	<100>	:=	Interrogation command	C_IC_NA_1
☒	<101>	:=	Counter interrogation command	C_CI_NA_1
☒	<102>	:=	Read command	C_RD_NA_1
☒	<103>	:=	Clock synchronization command	C_CS_NA_1
■	~~<104>~~	~~:=~~	~~Test command~~	~~C_TS_NA_1~~
☒	<105>	:=	Reset process command	C_RP_NC_1
■	~~<106>~~	~~:=~~	~~Delay acquisition command~~	~~C_CD_NA_1~~
☒	<107>	:=	Test command with time tag CP56Time2a	C_TS_TA_1

2.5.6.5 Parameter in Control Direction

(station-specific parameter)

☒	<110>	:=	Parameter of measured value, normalized value	P_ME_NA_1
☒	<111>	:=	Parameter of measured value scaled value	P_ME_NB_1
☒	<112>	:=	Parameter of measured value, short floating-point value	P_ME_NC_1
☒	<113>	:=	Parameter activation	P_AC_NA_1

2.5.6.6 File Transfer

(station-specific parameter)

File Download and Upload

☒	<120>	:=	File ready	F_FR_NA_1
☒	<121>	:=	Section ready	F_SR_NA_1
☒	<122>	:=	Call directory, select file, call file, call section	F_SC_NA_1
☒	<123>	:=	Last section, last segment	F_LS_NA_1
☒	<124>	:=	Ack file, ack section	F_AF_NA_1
☒	<125>	:=	Segment	F_SG_NA_1
☒	<126>	:=	Directory	F_DR_TA_1

2.5.6.7 Type identifier and Cause of Transmission Assignments

(station-specific parameter)
Shaded box[es] are not required.
Blank = Function or ASDU is not used

Type identification		Cause of transmission																		
		1	2	3	4	5	6	7	8	9	10	11	12	13	20 to 36	37 to 41	44	45	46	47
<1>	M_SP_NA_1		x	x		x									x					
~~<2>~~	~~M_SP_TA_1~~			■		■						■	■							
<3>	M_DP_NA_1		x	x		x									x					
~~<4>~~	~~M_DP_TA_1~~			■		■						■	■							
<5>	M_ST_NA_1		x	x		x									x					
~~<6>~~	~~M_ST_TA_1~~			■		■						■	■							
<7>	M_BO_NA_1		x	x		x									x					
~~<8>~~	~~M_BO_TA_1~~			■		■														
<9>	M_ME_NA_1	x	x	x		x									x					
~~<10>~~	~~M_ME_TA_1~~			■		■														
<11>	M_ME_NB_1	x	x	x		x									x					
~~<12>~~	~~M_ME_TB_1~~			■		■														
<13>	M_ME_NC_1	x	x	x		x									x					
~~<14>~~	~~M_ME_TC_1~~			■		■														
<15>	M_IT_NA_1			x												x				
~~<16>~~	~~M_IT_TA_1~~			■												■				
~~<17>~~	~~M_EP_TA_1~~			■																
~~<18>~~	~~M_EP_TB_1~~			■																
~~<19>~~	~~M_EP_TC_1~~			■																
<20>	M_PS_NA_1		x	x		x									x					
<21>	M_ME_ND_1	x	x	x		x									x					
<30>	M_SP_TB_1			x		x														
<31>	M_DP_TB_1			x		x														
<32>	M_ST_TB_1			x		x														
<33>	M_BO_TB_1			x		x														
<34>	M_ME_TD_1			x		x														
<35>	M_ME_TE_1			x		x														
<36>	M_ME_TF_1			x		x														
<37>	M_IT_TB_1			x												x				
<38>	M_EP_TD_1																			
<39>	M_EP_TE_1																			
<40>	M_EP_TF_1																			
<45>	C_SC_NA_1						x	x	x	x	x						x	x	x	x
<46>	C_DC_NA_1						x	x	x	x	x						x	x	x	x
<47>	C_RC_NA_1						x	x	x	x	x						x	x	x	x
<48>	C_SE_NA_1						x	x	x	x	x						x	x	x	x
<49>	C_SE_NB_1						x	x	x	x	x						x	x	x	x

Type identification		Cause of transmission																	
		1	2	3	4	5	6	7	8	9	10	11	12	13	20 to 36	37 to 41	44	45	46	47
<50>	C_SE_NC_1						x	x	x	x	x						x	x	x	x
<51>	C_BO_NA_1																			
<58>	C_SC_TA_1						x	x	x	x	x						x	x	x	x
<59>	C_DC_TA_1						x	x	x	x	x						x	x	x	x
<60>	C_RC_TA_1						x	x	x	x	x						x	x	x	x
<61>	C_SE_TA_1						x	x	x	x	x						x	x	x	x
<62>	C_SE_TB_1						x	x	x	x	x						x	x	x	x
<63>	C_SE_TC_1						x	x	x	x	x						x	x	x	x
<64>	C_BO_TA_1																			
<70>	M_EI_NA_1				x															
<100>	C_IC_NA_1						x	x	x	x	x						x	x	x	x
<101>	C_CI_NA_1						x	x			x						x	x	x	x
<102>	C_RD_NA_1					x											x	x	x	x
<103>	C_CS_NA_1			x			x	x									x	x	x	x
~~<104>~~	~~C_TS_NA_1~~																			
<105>	C_RP_NA_1						x	x									x	x	x	x
~~<106>~~	~~C_CD_NA_1~~																			
<107>	C_TS_TA_1						x	x									x	x	x	x
<110>	P_ME_NA_1						x	x												
<111>	P_ME_NB_1						x	x												
<112>	P_ME_NC_1						x	x												
<113>	P_AC_NA_1						x	x	x	x										
<120>	F_FR_NA_1													x						
<121>	F_SR_NA_1													x						
<122>	F_SC_NA_1					x								x						
<123>	F_LS_NA_1													x						
<124>	F_AF_NA_1													x						
<125>	F_SG_NA_1													x						
<126>	F_DR_TA_1					x														

2.6 Basic Application Functions (9.6)

2.6.1 Station Initialization

(station-specific parameter)

☒ Remote initialization

2.6.2 Cyclic Data Transmission

(station-specific parameter)

☒ Cyclic data transmission

2.6.3 Read Procedure

(station-specific parameter)

☒ Read Procedure

2.6.4 Spontaneous Transmission

(station-specific parameter)

☒ Spontaneous transmission

2.6.5 Double Transmission of Information Objects with Cause of Transmission Spontaneous

(station-specific parameter)

The following type identification can be transmitted in succession caused by a single status change of an information object. The information object addresses for which double transmission is enabled are defined in a project-specific list.

☐ Single-point information M_SP_NA_1, M_SP_TA_1, M_SP_TB_1 and M_PS_NA_1
☐ Double-point information M_DP_NA_1, M_DP_TA_1 and M_DP_TB_1
☐ Step position information M_ST_NA_1, M_ST_TA_1 and M_ST_TB_1
☐ Bitstring of 32 bits M_BO_NA_1, M_BO_TA_1 and M_BO_TB_1
☐ Measured value, normalized value M_ME_NA_1, M_ME_TA_1, M_ME_ND_1 and M_ME_TD_1
☐ Measured value, scaled value M_ME_NB_1, M_ME_TB_1 and M_ME_TE_1
☐ Measured value, short floating-point number M_ME_NC_1, M_ME_TC_1 and M_ME_TF_1

2.6.6 Station Interrogation

(station-specific parameter)

☒ Global
☒ Group 1 ☒ Group 7 ☒ Group 13

- ☒ Group 2
- ☒ Group 3
- ☒ Group 4
- ☒ Group 5
- ☒ Group 6
- ☒ Group 8
- ☒ Group 9
- ☒ Group 10
- ☒ Group 11
- ☒ Group 12
- ☒ Group 14
- ☒ Group 15
- ☒ Group 16

Information Object Address assigned to each group shall be shown in a separate table

2.6.7 Clock Synchronization

(station-specific parameter)

- ☒ Clock synchronization

2.6.8 Command Transmission

(object-specific parameter)

- ☒ Direct Command Transmission (Step Position)
- ☒ Direct set point command transmission
- ☒ Selected and Execute Command (Single & Double CMDS)
- ☒ Select and execute set point command
- ☒ C-SE ACTTERM Used
- ☒ No additional definition
- ☒ Short pulse duration (duration determined by a system parameter in the outstation)
- ☒ Long pulse duration (duration determined by a system parameter in the outstation)
- ☒ Persistent output

- ☒ Supervision of maximum delay in command direction of Commands and Set Point Commands

Configurable Maximum allowable delay for Commands and Set Point Commands

2.6.9 Transmission of Integrated Totals

(station or object-specific parameter)

- ☒ Mode A: Local freeze with spontaneous transmission
- ☐ Mode B: Local freeze with counter interrogation
- ☒ Mode C: Freeze and transmit by counter-interrogation command
- ☐ Mode D: Freeze by counter-interrogation command, frozen values reported spontaneously

- ☒ Counter read
- ☒ Counter freeze without reset
- ☒ Counter freeze with reset
- ☒ Counter reset
- ☒ General request counter
- ☒ Request counter group 1
- ☒ Request counter group 2
- ☒ Request counter group 3
- ☒ Request counter group 4

Addresses per group must be defined

2.6.10 Parameter Loading

(object-specific parameter)

- ☒ Threshold value
- ☐ Smoothing factor
- ☒ Low limit for transmission of measured value
- ☒ High limit for transmission of measured value

2.6.11 Parameter Activation

(object-specific parameter)

- ☒ Act/de-act of persistent cyclic or periodic transmission of the addressed object

2.6.12 Test Procedure

(station-specific parameter)

- ☒ Test procedure

2.6.13 File Transfer

(station-specific parameter)

2.6.13.1 File Transfer in Monitor Direction

- ☐ Transparent file
- ☐ Transmission of disturbance data of protection equipment
- ☐ Transmission of sequences of events
- ☐ Transmission of sequences of recorded analogue values

2.6.13.2 File Transfer in Control Direction

- ☒ Transparent file

2.6.14 Background Scan

(station-specific parameter)

- ☒ Background scan

2.6.15 Acquisition of Transmission Delay

(station-specific parameter)

- ■ ~~Acquisition of transmission delay~~

2.6.16 Definition of Time Outs

Parameter	Default value	Remarks	Selected value
t_0	30 s	Time-out of connection establishment	**Configurable**
t_1	15 s	Time-out of send or test APDUs	**Configurable**
t_2	10 s	Time-out for acknowledges in case of no data messages $t_2 < t_1$	**Configurable**
t_3	20 s	Time-out of sending test frames in case of a long idle state	**Configurable**

Maximum range of values for all time-outs: 1 to 255 s, accuracy 1 s.

2.6.17 Maximum Number of Outstanding I Format APDUs *k* and Latest Acknowledge APDUs (*w*)

Parameter	Default value	Remarks	Selected value
K	12 APDUs	Maximum difference receives sequence number to send state variable	**Configurable**
W	8 APDUs	Latest acknowledge after receiving *w* I format APDUs	**Configurable**

Maximum range of values k: 1 to 32767 (2_{15}–1) APDUs, accuracy 1 APDU
Maximum range of values w: 1 to 32767 APDUs, accuracy 1 APDU (Recommendation: w should not exceed two-thirds of k).

2.6.18 Port Number

Parameter	Value	Remarks
Port number	2404	In all cases

2.6.19 RFC 2200 suite

RFC 2200 suite is an official Internet Standard that describes the state of standardization of protocols used in the Internet as determined by Internet Architecture Board (IAB). It offers a broad spectrum of actual standards used in the Internet. The suitable selection of documents from RFC 2200 defined in this standard for given projects must be chosen by the user of this standard.

- ☒ Ethernet 802.3
- ☐ Serial X.21 interface
- ☐ Other selection from RFC 2200:

List of valid documents from RFC 2200

1. .....
2. .....
3. .....
4. .....
5. .....

6. .....

MODIFICATION RECORD

VERSION	REV.	DATE	AUTHOR	CHANGE DESCRIPTION
1.00	0	2nd May, 2019	G. LaMarre	Created.

GE
Grid Solutions

IEC 60870-5-103 Client (DCA) for the Multifunction Controller Platform

Conformance Statement

NTEK-A025M-0CS

Version 1.00 Revision 0

Associated Software Release: Version 1.00

imagination at work

General

COPYRIGHT NOTICE

© 2019, General Electric Company. All rights reserved.

The Software Product described in this documentation may only be used in accordance with the applicable License Agreement. The Software Product and Associated Material are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable, and are delivered with Restricted Rights. Such restricted rights are those identified in the License Agreement, and as set forth in the "Restricted Rights Notice" contained in paragraph (g) (3) (Alternate III) of FAR 52.227-14, Rights in Data-General, including Alternate III (June 1987).

If applicable, any use, modification, reproduction release, performance, display or disclosure of the Software Product and Associated Material by the U.S. Government shall be governed solely by the terms of the License Agreement and shall be prohibited except to the extent expressly permitted by the terms of the License Agreement.

The information contained in this online publication is the exclusive property of General Electric Company, except as otherwise indicated. You may view, copy and print documents and graphics incorporated in this online publication (the "Documents") subject to the following: (1) the Documents may be used solely for personal, informational, non-commercial purposes; (2) the Documents may not be modified or altered in any way; and (3) General Electric Company withholds permission for making the Documents or any portion thereof accessible via the internet. Except as expressly provided herein, you may not use, copy, print, display, reproduce, publish, license, post, transmit or distribute the Documents in whole or in part without the prior written permission of General Electric Company. If applicable, any use, modification, reproduction, release, performance, display, or disclosure of the Software Product and Associated Material by the U.S. Government shall be governed solely by the terms of the License Agreement and shall be prohibited except to the extent expressly permitted by the terms of the License Agreement.

The information contained in this online publication is subject to change without notice. The software described in this online publication is supplied under license and may be used or copied only in accordance with the terms of such license.

TRADEMARK NOTICES

GE and are trademarks and service marks of General Electric Company.

* Trademarks of General Electric Company.

IEC is a registered trademark of Commission Electrotechnique Internationale.

Other company or product names mentioned in this document may be trademarks or registered trademarks of their respective companies.

Contents

1. Interoperability Tables 5

1.1 Network Configuration (IEC 870-5-101 Section 8.1) 5
1.2 Physical Layer (IEC 870-5-101 Section 8.2) 5
1.3 Link Layer (IEC 870-5-101 Section 8.3) 5
1.4 Link Transmission Procedures 6
1.5 Address Field of The Link 6
1.6 Application Layer (IEC 60870-5-103 Section 8.3) 6
1.7 DCA Handling of COT in Monitor Direction 7
1.8 Standard Information Numbers in Monitor Direction 8
1.9 Standard Information Numbers in Control Direction 10
1.10 Supported Application Functions 11
1.11 Miscellaneous 11
1.12 Selections of Standard Application Service Data Units 12

Tables

Table 1 Physical Layer 5
Table 2 DCA Handling of COT in Monitor Direction 7
Table 3 Standard Information Numbers in Monitor Direction 8
Table 4 Standard Information Numbers in Control Direction 10
Table 5 Supported Application Functions 11
Table 6 Miscellaneous Functions 11
Table 7 Process Information in Monitor Direction 12
Table 8 Process Information in Control Direction 12

1. Interoperability Tables

In cases where several options are available, for example multiple lengths of address fields, the GE Grid Solutions MCP shall be able to be configured to use the required value.

1.1 Network Configuration (IEC 870-5-101 Section 8.1)

Point to Point - Supported

Multi Point-Party Line - Supported

Multiple Point to Point - Supported

Multi Point Star - Supported

1.2 Physical Layer (IEC 870-5-101 Section 8.2)

Table 1 Physical Layer

Transmission Speed	Control Direction	Monitor Direction
100 bit/s	Not Supported	Not Supported
200 bit/s	Not Supported	Not Supported
300 bit/s	Supported	Supported
600 bit/s	Supported	Supported
1200 bit/s	Supported	Supported
2400 bit/s	Supported	Supported
4800 bit/s	Supported	Supported
9600 bit/s	Supported	Supported
19200 bit/s	Supported	Supported
38400 bit/s	Not Supported	Not Supported
56000 bit/s	Not Supported	Not Supported
64000 bit/s	Not Supported	Not Supported

1.3 Link Layer (IEC 870-5-101 Section 8.3)

- Frame format FT1.2 (*IEC® 870-5-1 Section 6.2.4.2*) of fixed and variable length.
- Single character I, 0xE5, (*IEC 870-5-1 Section 6.2.4.2.3*) - used as a positive acknowledge.
- Single character II, 0xA2, (*IEC 870-5-1 Section 6.2.4.2.3*) - used as a negative acknowledge.
- Fixed CONFIRM time out interval (value is configurable).
- Fixed RESPOND time out interval (value is configurable).

1.4 Link Transmission Procedures

Balanced transmission : Not Supported

Unbalanced transmission : Supported

1.5 Address Field of The Link

Not present (balanced transmission only)	:	Not Supported
One octet	:	Supported
Two octets	:	Not Supported
Structured	:	Supported
Unstructured	:	Supported
Maximum frame length	:	255

1.6 Application Layer (IEC 60870-5-103 Section 8.3)

Transmission Mode for Application Data

Mode 1 (Least significant octet first) for all application data.

Common Address of ASDU

One common address of ASDU (identical with station address) - Supported

More than one common address of ASDU - Supported

(Different from station address)

Information Object Address

No choice. Always ONE Octet.

Cause of Transmission

The size of Cause of Transmission is always ONE octet. The DCA supports the following Cause of Transmission (COT):

Monitor direction:

- Spontaneous (1).
- Cyclic (2).
- Reset frame count bit (3).
- Reset communication unit (4).
- Start / restart (5).
- Power on (6).
- Test mode (7).
- Time synchronization (8).

- General interrogation (9).
- Termination of general interrogation (10).
- Positive acknowledgement of command (20).
- Negative acknowledgement of command (21).

Control direction:

- Time synchronization (8).
- General interrogation (9).
- General command (20).

1.7 DCA Handling of COT in Monitor Direction

Table 2 DCA Handling of COT in Monitor Direction

COT in Monitor Direction	DCA Processing of COT
Spontaneous	The DCA updates the system database with the received values for the data points.
Cyclic	The DCA updates the system database with the received values for the data points.
Reset FCB	The remote device is ready to accept messages. The DCA queues a General Interrogation then followed by a Time Sync request (if required).
Reset CU	The remote device is ready to accept messages. The DCA queues a General Interrogation then followed by a Time Sync request (if required).
Start/Restart	The DCA toggles the devices' Start/Restart pseudo BI point ON then OFF.
Power ON	The DCA toggles the devices' Start/Restart pseudo BI point ON then OFF. The DCA also posts a message to the system log to indicate the device is powered ON.
Test Mode	The DCA updates the system database for the corresponding point flag to indicate Remote Force ON.
Time Synchronization	The DCA updates the device's Time Sync In-Progress pseudo BI point to OFF.
General Interrogation	The DCA updates the system database with the received values for the data points.
General Interrogation Termination	The DCA updates the device's General Interrogation In-Progress pseudo BI point to OFF.
ACK	The DCA returns an ACK to RtDB to indicate success of the general command.
NACK	The DCA returns a NACK to RtDB with the IO_OFF_LINE_ERR status to indicate failure of the general command.

1.8 Standard Information Numbers in Monitor Direction

Table 3 Standard Information Numbers in Monitor Direction

	Information Number	Semantics	Type ID Used	Supported
System Functions	0	End of general interrogation	8	✓
	0	Time synchronization	6	✓
	2	Reset Frame Count Bit (FCB)	5	✓
	3	Reset Communication Unit (CU)	5	✓
	4	Start/Restart	5	✓
	5	Power On	5	✓
Status Indications	16	Auto-recloser active	1	✓
	17	Tele-protection active	1	✓
	18	Protection active	1	✓
	19	LED reset	1	✓
	20	Monitor direction blocked	1	✓
	21	Test mode	1	✓
	22	Local parameter setting	1	✓
	23	Characteristic 1	1	✓
	24	Characteristic 2	1	✓
	25	Characteristic 3	1	✓
	26	Characteristic 4	1	✓
	27	Auxiliary input 1	1	✓
	28	Auxiliary input 2	1	✓
	29	Auxiliary input 3	1	✓
	30	Auxiliary input 4	1	✓
Supervision Indications	32	Measurand supervision I	1	✓
	33	Measurand supervision V	1	✓
	35	Phase sequence supervision	1	✓
	36	Trip circuit supervision	1	✓
	37	I>> backup operation	1	✓
	38	VT fuse failure	1	✓
	39	Tele-protection disturbed	1	✓
	46	Group warning	1	✓
	47	Group alarm	1	✓
Earth Fault	48	Earth fault L1	1	✓
	49	Earth fault L2	1	✓
	50	Earth fault L3	1	✓

	Information Number	Semantics	Type ID Used	Supported
Indications	51	Earth fault forward (i.e. line)	1	✓
	52	Earth fault reverse (i.e. busbar)	1	✓
Fault Indications	64	Start / pick-up L1	2	✓
	65	Start / pick-up L2	2	✓
	66	Start / pick-up L3	2	✓
	67	Start / pick-up N	2	✓
	68	General Trip	2	✓
	69	Trip L1	2	✓
	70	Trip L2	2	✓
	71	Trip L3	2	✓
	72	Trip I>> (back-up operation)	2	✓
	73	Fault location X in Ohm	4	✓
	74	Fault forward/line	2	✓
	75	Fault reverse/busbar	2	✓
	76	Tele-protection signal transmitted	2	✓
	77	Tele-protection signal received	2	✓
	78	Zone 1	2	✓
	79	Zone 2	2	✓
	80	Zone 3	2	✓
	81	Zone 4	2	✓
	82	Zone 5	2	✓
	83	Zone 6	2	✓
	84	General start / pick-up	2	✓
	85	Breaker failure	2	✓
	86	Trip measuring system L1	2	✓
	87	Trip measuring system L2	2	✓
	88	Trip measuring system L3	2	✓
	89	Trip measuring system E	2	✓
	90	Trip I>	2	✓
	91	Trip I>>	2	✓
	92	Trip IN>	2	✓
	93	Trip IN>>	2	✓
Auto Reclosure Indications	128	CB >on by AR	1	✓
	129	CB >on by long-time AR	1	✓
	130	AR blocked	1	✓
Measurands	144	Measurand I	3, 9, 140	✓
	145	Measurands I, V	3, 9, 140	✓

	Information Number	Semantics	Type ID Used	Supported
	146	Measurands I, V, P, Q	3, 9, 140	✓
	147	Measurands IN, VEN	3, 9, 140	✓
	148	Measurands IL1,2,3, VL1,2,3, P, Q, f	3, 9, 140	✓
Generic Functions	240	Read headings of all defined groups	10	×
	241	Read values or attributes of all entries of one group	10	×
	243	Read directory of a single entry	11	×
	244	Read value or attribute of a single entry	10	×
	245	End of General interrogation of generic data	10	×
	249	Write entry with confirmation	10	×
	250	Write entry with execution	10	×
	251	Write entry aborted	10	×

1.9 Standard Information Numbers in Control Direction

Table 4 Standard Information Numbers in Control Direction

	Information Number	Semantics	Type ID Used	Supported
System Functions	0	General interrogation	7	✓
	0	Time synchronization	6	✓
General Commands	16	Auto-recloser On/Off	20	✓
	17	Tele-protection On/Off	20	✓
	18	Protection On/Off	20	✓
	19	LED reset	20	✓
	23	Activate Characteristic 1	20	✓
	24	Activate Characteristic 2	20	✓
	25	Activate Characteristic 3	20	✓
	26	Activate Characteristic 4	20	✓
Generic Functions	240	Read headings of all defined groups	21	×
	241	Read values of attributes of all entries of one group	21	×
	243	Read directory of a single entry	21	×
	244	Read value or attribute of a single entry	21	×
	245	General interrogation of generic data	21	×
	248	Write entry	10	×
	249	Write entry with confirmation	10	×

	Information Number	Semantics	Type ID Used	Supported
	250	Write entry with execution	10	×
	251	Write entry abort	10	×

1.10 Supported Application Functions

Table 5 Supported Application Functions

Application Functions	Supported
Station initialization with Reset Communication Unit (CU)	✓
Station initialization with Reset Frame Count Bit (FCB)	✓
General Interrogation	✓
Time Synchronization of remote device	✓
Broadcast Time Synchronization	×
General Command Transmission	✓
Test Mode	✓
Blocking of Monitor Direction	✓
Transmission of Disturbance Data	×
Generic Services	×
Private Data (Only for known ASDU Type ID as configured)	×

1.11 Miscellaneous

Table 6 Miscellaneous Functions

Measurand	Support Max. MVAL= 1, 2 times of rated value	Support Max. MVAL= 2, 4 times of rated value
Current L_1	✓	✓
Current L_2	✓	✓
Current L_3	✓	✓
Voltage L_{1-E}	✓	✓
Voltage L_{2-E}	✓	✓
Voltage L_{3-E}	✓	✓
Active Power P	✓	✓
Reactive Power Q	✓	✓
Frequency f	✓	✓
Voltage L_1 - L_2	✓	✓

Note: The DCA does not perform scaling of ASDU Type 4 measurand values.

1.12 Selections of Standard Application Service Data Units

Table 7 Process Information in Monitor Direction

PROCESS INFORMATION IN MONITOR DIRECTION				
Type ID	**Description**	**Supported**	**SCADA Data Types**	**RtDB Type**
1	Time-tagged message.	✓	DI	Binary Input
2	Time-tagged message with relative time. Note: Fault Number is ignored.	✓	DI	Binary Input
3	Measurands Type I.	✓	AI	Analog Input
4	Time-tagged measurands with relative time.	✓	AI	Analog Input
5	Identification message.	✓	N/A	N/A
6	Time synchronization.	✓	N/A	N/A
8	General interrogation termination.	✓	N/A	N/A
9	Measurands Type II.	✓	AI	Analog Input
10	Generic data.	×		
11	Generic identification.	×		
23	List of recorded disturbances.	×		
26	Ready for transmission of disturbance data.	×		
27	Ready for transmission of a channel.	×		
28	Ready for transmission of tags.	×		
29	Transmission of tags.	×		
30	Transmission of disturbance values.	×		
31	End of transmission.	×		
140	Measurands Type II - Not Compatible.	✓	AI	Analog Input

Table 8 Process Information in Control Direction

PROCESS INFORMATION IN CONTROL DIRECTION				
Type ID	**Short Name**	**Description**	**Supported**	**SCADA Data Types**
6		Time Synchronization.	✓	N/A
7		General interrogation initiation.	✓	N/A
10		Generic data.	×	
20		General command.	✓	DO
21		Generic command.	×	
24		Order for disturbance data transmission.	×	
25		Acknowledgement for disturbance data transmission.	×	

Note: The DCA discards data in monitor direction that is listed as not supported.

MODIFICATION RECORD

VERSION	REV.	DATE	AUTHOR	CHANGE DESCRIPTION
1.00	0	2nd May, 2019	G. LaMarre	Created.

GE

Grid Solutions

IEC 61850 Client (DCA) for MCP

Conformance Statement

NTEK-A027M-0CS

Version 2.00 Revision 2

Associated Software Release: Version 2.00

imagination at work

COPYRIGHT NOTICE

© 2020, General Electric Canada. All rights reserved.

The Software Product described in this documentation may only be used in accordance with the applicable License Agreement. The Software Product and Associated Material are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable, and are delivered with Restricted Rights. Such restricted rights are those identified in the License Agreement, and as set forth in the "Restricted Rights Notice" contained in paragraph (g) (3) (Alternate III) of FAR 52.227-14, Rights in Data-General, including Alternate III (June 1987).

If applicable, any use, modification, reproduction release, performance, display or disclosure of the Software Product and Associated Material by the U.S. Government shall be governed solely by the terms of the License Agreement and shall be prohibited except to the extent expressly permitted by the terms of the License Agreement.

The information contained in this online publication is the exclusive property of General Electric Canada, except as otherwise indicated. You may view, copy and print documents and graphics incorporated in this online publication (the "Documents") subject to the following: (1) the Documents may be used solely for personal, informational, non-commercial purposes; (2) the Documents may not be modified or altered in any way; and (3) General Electric Canada withholds permission for making the Documents or any portion thereof accessible via the internet. Except as expressly provided herein, you may not use, copy, print, display, reproduce, publish, license, post, transmit or distribute the Documents in whole or in part without the prior written permission of General Electric Canada. If applicable, any use, modification, reproduction, release, performance, display, or disclosure of the Software Product and Associated Material by the U.S. Government shall be governed solely by the terms of the License Agreement and shall be prohibited except to the extent expressly permitted by the terms of the License Agreement.

The information contained in this online publication is subject to change without notice. The software described in this online publication is supplied under license and may be used or copied only in accordance with the terms of such license.

TRADEMARK NOTICES

GE and are trademarks and service marks of General Electric Canada.

* Trademarks of General Electric Canada.

Firefox is a registered trademark of Mozilla Foundation. Internet Explorer and Microsoft are registered trademarks of Microsoft Corporation. Java and Sun are registered trademarks of SUN Microsystems, Inc.

Other company or product names mentioned in this document may be trademarks or registered trademarks of their respective companies.

Contents

1. Protocol Implementation Conformance Statement (PICS) 5

1.1 GENERAL 5
1.2 ACSI Basic Conformance Statement 5
1.3 ACSI Models Conformance Statement 6
1.4 ACSI Service Conformance Statement 8

2. Model Implementation Conformance Statement (MICS) 12

2.1 Introduction 12
2.2 SUPPORTED COMMON DATA CLASSES 12
2.2.1 Common data class specifications for status information 12
2.2.2 Common data class specifications for measurement information 12
2.2.3 Common data class specifications for controls 13
2.2.4 Common data class specifications for status settings 13
2.2.5 Common data class specifications for analogue settings 13
2.2.6 Common data class specifications for description information 14
2.2.7 Common data class specifications for tracking 14

3. Protocol Implementation eXtra Information for Testing (PIXIT) 15

3.1 Introduction 15
3.2 PIXIT for Configuration 15
3.3 PIXIT for Association model 15
3.4 PIXIT for Server model 16
3.5 PIXIT for Data set model 18
3.6 PIXIT for Substitution model 19
3.7 PIXIT for Setting group control model 19
3.8 PIXIT for Reporting model 19
3.9 PIXIT for Logging model 22
3.10 PIXIT for GOOSE control block model 22
3.11 PIXIT for Control model 22
3.12 PIXIT for Time and time synchronization model 23
3.13 PIXIT for File transfer model 23
3.14 PIXIT for Service Tracking Model 24

4. TISSUES Implementation Conformance Statement (TICS) 25

4.1 Introduction 25
4.2 Mandatory Edition 2 Tissues 25

4.2.1 Part 6 Tissue List 25
4.2.2 Part 7-1 Tissue List 26
4.2.3 Part 7-2 Tissue List 26
4.2.4 Part 7-3 Tissue List 26
4.2.5 Part 7-4 Tissue List 27
4.2.6 Part 8-1 Tissue List 28

1. Protocol Implementation Conformance Statement (PICS)

1.1 GENERAL

The Multifunction Controller Platform (MCP) is a family of individual branded product names, with G500 being one of them.

The following ACSI conformance statements are used to provide an overview and details about G500 with firmware version 2.0:

- ACSI basic conformance statement
- ACSI models conformance statement
- ACSI service conformance statement

The tables in this document are identical to those given in IEC® 61850-7-2, except for the Value/comments column. This column shows the compliance of the MCP IEC 61850 Client to the ACSI.

1.2 ACSI Basic Conformance Statement

The basic conformance statement is defined as below:

Table 1.1: ACSI Basic Conformance Statement

		Client/ subscriber	Server/ publisher	Value/ comments
DCA-server roles				
B11	**Server** side (of TWO-PARTY-APPLICATION-ASSOCIATION)	–	c1	**No**
B12	**Client** side of (TWO-PARTY-APPLICATION-ASSOCIATION)	c1	–	**Yes**
SCSMs supported				
B21	**SCSM**: IEC 61850-8-1 used			**Yes**
B22	**SCSM**: IEC 61850-9-1 used			**No**
B23	**SCSM**: IEC 61850-9-2 used			**No**
B24	**SCSM**: other			**No**
Generic substation event model (GSE)				
B31	**Publisher** side	–	O	**No**

		Client/ subscriber	Server/ publisher	Value/ comments
B32	**Subscriber** side	O	–	**No**
Transmission of sampled value model (SVC)				
B41	**Publisher** side	–	O	**No**
B42	**Subscriber** side	O	–	**No**
c1 – shall be 'M' if support for **logical-device** model has been declared. O – Optional M – Mandatory				

1.3 ACSI Models Conformance Statement

The ACSI models conformance statement shall be as defined below:

Table 1.2: ACSI Models Conformance Statement

		Client/ subscriber	Server/ publisher	Value/ comments
If Server side (B11) or DCA side (B12) supported				
M1	**Logical device**	c2	c2	**Yes**
M2	**Logical node**	c3	c3	**Yes**
M3	**Data**	c4	c4	**Yes**
M4	**Data set**	c5	c5	**Yes**
M5	**Substitution**	O	O	**No**
M6	**Setting group control**	O	O	**No**
Reporting				
M7	**Buffered report control**	O	O	**Yes**
M7-1	sequence-number			**Yes**
M7-2	report-time-stamp			**Yes**
M7-3	reason-for-inclusion			**Yes**
M7-4	data-set-name			**Yes**
M7-5	data-reference			**Yes**
M7-6	buffer-overflow			**Yes**
M7-7	entryID			**Yes**
M7-8	BufTm			**Yes**
M7-9	IntgPd			**Yes**
M7-10	GI			**Yes**

		Client/ subscriber	Server/ publisher	Value/ comments
M7-11	conf-revision			**No**
M8	**Unbuffered report control**	O	O	**Yes**
M8-1	sequence-number			**Yes**
M8-2	report-time-stamp			**Yes**
M8-3	reason-for-inclusion			**Yes**
M8-4	data-set-name			**Yes**
M8-5	data-reference			**Yes**
M8-6	BufTm			**Yes**
M8-7	IntgPd			**Yes**
M8-8	GI			**Yes**
M8-9	conf-revision			**No**
	Logging	O	O	**No**
M9	**Log control**	O	O	**No**
M9-1	IntgPd			**No**
M10	**Log**	O	O	**No**
M11	**Control**	M	M	**Yes**
If GSE (B31/B32) is supported				
M12	**GOOSE**	O	O	**No**
M13	**GSSE**	O	O	**deprecated**
If SVC (B41/B42) is supported				
M14	Multicast SVC	O	O	**No**
M15	Unicast SVC	O	O	**No**
For all IEDs				
M16	**Time**	M	M	**N/A**
M17	**File Transfer**	O	O	**Yes**

c2 – shall be 'M' if support for **LOGICAL-NODE** model has been declared.
c3 – shall be 'M' if support for **DATA** model has been declared.
c4 – shall be 'M' if support for **DATA-SET**, Substitution, Report, Log Control, or Time model has been declared.
c5 – shall be 'M' if support for Report, GSE, or SV models has been declared.

M – Mandatory

O-Optional

1.4 ACSI Service Conformance Statement

The ACSI service conformance statement shall be as defined below:

Table 1.3: ACSI Services Conformance Statement

	Services	AA: TP/MC	Client/ subscriber	Server/ publisher	Comments Value	Ed
Server (Clause 7)						
S1	ServerDirectory	TP		M	**No**	**1,2**
Application association (Clause 8)						
S2	Associate		M	M	**Yes**	**1,2**
S3	Abort		M	M	**Yes**	**1,2**
S4	Release		M	M	**Yes**	**1,2**
Logical device (Clause 9)						
S5	LogicalDeviceDirectory	TP	M	M	**No**	**1,2**
Logical node (Clause 10)						
S6	LogicalNodeDirectory	TP	M	M	**No**	**1,2**
S7	GetAllDataValues	TP	O	M	**No**	**1,2**
Data (Clause 11)						
S8	GetDataValues	TP	M	M	**Yes**	**1,2**
S9	SetDataValues	TP	O	O	**Yes**	**1,2**
S10	GetDataDirectory	TP	O	M	**No**	**1,2**
S11	GetDataDefinition	TP	O	M	**Yes**	**1,2**
Data set (Clause 12)						
S12	GetDataSetValues	TP	O	M	**Yes**	**1,2**
S13	SetDataSetValues	TP	O	O	**No**	**1,2**
S14	CreateDataSet	TP	O	O	**Yes**	**1,2**
S15	DeleteDataSet	TP	O	O	**Yes**	**1,2**
S16	GetDataSetDirectory	TP	O	O	**No**	**1,2**
Substitution						
S17	SetDataValues	TP	M	M	**No**	**1**
Setting group control (Clause 16)						
S18	SelectActiveSG	TP	O	O	**No**	**1,2**
S19	SelectEditSG	TP	O	O	**No**	**1,2**
S20	SetSGValues	TP	O	O	**No**	**1,2**
S21	ConfirmEditSGValues	TP	O	O	**No**	**1,2**
S22	GetSGValues	TP	O	O	**No**	**1,2**
S23	GetSGCBValues	TP	O	O	**No**	**1,2**

	Services	AA: TP/MC	Client/ subscriber	Server/ publisher	Comments Value	Ed
Reporting (Clause 17)						
Buffered report control block (BRCB)						
S24	Report	TP	c6	c6	**Yes**	**1,2**
S24-1	data-change (dchg)				**Yes**	**1,2**
S24-2	qchg-change (qchg)				**Yes**	**1,2**
S24-3	data-update (dupd)				**Yes**	**1,2**
S25	GetBRCBValues	TP	c6	c6	**Yes**	**1,2**
S26	SetBRCBValues	TP	c6	c6	**Yes**	**1,2**
Unbuffered report control block (URCB)						
S27	Report	TP	c6	c6	**Yes**	**1,2**
S27-1	data-change (dchg)				**Yes**	**1,2**
S27-2	qchg-change (qchg)				**Yes**	**1,2**
S27-3	data-update (dupd)				**Yes**	**1,2**
S28	GetURCBValues	TP	c6	c6	**Yes**	**1,2**
S29	SetURCBValues	TP	c6	c6	**Yes**	**1,2**
c6 – shall declare support for at least one (BRCB or URCB).						
Logging (Clause 17)						
Log control block						
S30	GetLCBValues	TP	M	M	**No**	**1,2**
S31	SetLCBValues	TP	O	M	**No**	**1,2**
Log						
S32	QueryLogByTime	TP	c7	M	**No**	**1,2**
S33	QueryLogAfter	TP	c7	M	**No**	**1,2**
S34	GetLogStatusValues	TP	M	M	**No**	**1,2**
c7 – shall declare support for at least one (QueryLogByTime or QueryLogAfter).						
Generic substation event model (GSE) (14.3.5.3.4)						
GOOSE-CONTROL-BLOCK						
S35	SendGOOSEMessage	MC	c8	c8	**No**	**1,2**
S36	GetGoReference	TP	O	c9	**No**	**1,2**
S37	GetGOOSEElementNumber	TP	O	c9	**No**	**1,2**
S38	GetGoCBValues	TP	O	O	**No**	**1,2**
S39	SetGoCBValues	TP	O	O	**No**	**1,2**
GSSE-CONTROL-BLOCK						
S40	SendGSSEMessage	MC	c8	c8	**No**	**1**

	Services	AA: TP/MC	Client/ subscriber	Server/ publisher	Comments Value	Ed
						Deprecated in Ed2
S41	GetGsReference	TP	O	c9	**No**	**1 Deprecated in Ed2**
S42	GetGSSEElementNumber	TP	O	c9	**No**	**1 Deprecated in Ed2**
S43	GetGsCBValues	TP	O	O	**No**	**1 Deprecated in Ed2**
S44	SetGsCBValues	TP	O	O	**No**	**1 Deprecated in Ed2**
c8 – shall declare support for at least one (SendGOOSEMessage or SendGSSEMessage). c9 – shall declare support if TP association is available.						
Transmission of sampled value model (SVC) (Clause 19)						
Multicast SVC						
S45	SendMSVMessage	MC	c10	c10	**No**	**1,2**
S46	GetMSVCBValues	TP	O	O	**No**	**1,2**
S47	SetMSVCBValues	TP	O	O	**No**	**1,2**
Unicast SVC						
S48	SendUSVMessage	TP	c10	c10	**No**	**1,2**
S49	GetUSVCBValues	TP	O	O	**No**	**1,2**
S50	SetUSVCBValues	TP	O	O	**No**	**1,2**
c10 – shall declare support for at least one (SendMSVMessage or SendUSVMessage).						
Control (Clause 20)						
S51	Select		M	O	**Yes**	**1,2**
S52	SelectWithValue	TP	M	O	**Yes**	**1,2**
S53	Cancel	TP	O	O	**Yes**	**1,2**
S54	Operate	TP	M	M	**Yes**	**1,2**
S55	Command-Termination	TP	M	O	**Yes**	**1,2**
S56	TimeActivated-Operate	TP	O	O	**No**	**1,2**
File transfer (Clause 23)						
S57	GetFile	TP	O	M	**Yes**	**1,2**

	Services	AA: TP/MC	Client/ subscriber	Server/ publisher	Comments Value	Ed
S58	SetFile	TP	O	O	**No**	**1,2**
S59	DeleteFile	TP	O	O	**No**	**1,2**
S60	GetFileAttributeValues	TP	O	M	**Yes**	**1,2**
Time (5.5)						
T1	Time resolution of internal clock				Nearest negative power of 2 in seconds: **10**	**1,2**
T2	Time accuracy of internal clock				T0	**1,2**
					T1	**1,2**
					T2	**1,2**
					T3	**1,2**
					T4	**1,2**
					T5	**1,2**
T3	Supported TimeStamp resolution				Nearest value of 2**-n in seconds according to 5.5.3.7.3.3: **10**	**1,2**

2. Model Implementation Conformance Statement (MICS)

2.1 Introduction

This model implementation conformance statement is applicable for the IEC 61850 client interface in G500 Firmware Version 2.00. This MICS document specifies the supported Common Data Classes for IEC 61850 Edition 1 and Edition 2.

Note: MICS template taken from 1p0p1_rev1, which is current latest released document.

Note: When a CDC is supported it is assumed that all mandatory and optional attributes are supported. All exceptions should be mentioned in the comment column.

2.2 SUPPORTED COMMON DATA CLASSES

2.2.1 Common data class specifications for status information

CDC	Ed	Description	Supported	Comment
SPS	1,2	Single point status	Y	
DPS	1,2	Double point status	Y	
INS	1,2	Integer status	Y	
ENS	1,2	Enumerated status	Y	
ACT	1,2	Protection activation information	Y	
ACD	1,2	Directional protection activation information	Y	
SEC	1,2	Security violation counting	Y	
BCR	1	Binary counter reading	Y	
BCR	2	Binary counter reading	N	
HST	1,2	Histogram	N	
VSS	1,2	Visible string status	N	
Notes:				

2.2.2 Common data class specifications for measurement information

CDC	Ed	Description	Supported	Comment
MV	1,2	Measured value	Y	
CMV	1,2	Complex measured value	Y	
SAV	1,2	Sampled value	N	
WYE	1,2	Phase to ground/neutral related measured values of a three-phase system	Y	
DEL	1,2	Phase to phase related measured values of a three-phase system	Y	
SEQ	1,2	Sequence	Y	
HMV	1	Harmonic value	Y	

HMV	2	Harmonic value	Y	
HWYE	1	Harmonic value for WYE	Y	
HWYE	2	Harmonic value for WYE	Y	
HDEL	1	Harmonic value for DEL	Y	
HDEL	2	Harmonic value for DEL	Y	
Notes:				

NOTE: It is assumed that when a CDC is supported, all supported control models as specified in the PIXIT are supported. Please specify exceptions in the comment's column.

2.2.3 Common data class specifications for controls

CDC	Ed	Description	Supported	Comment
SPC	1,2	Controllable single point	Y	
DPC	1,2	Controllable double point	Y	
INC	1,2	Controllable integer status	Y	
ENC	1,2	Controllable enumerated status	Y	
BSC	1,2	Binary controlled step position information	Y	
ISC	1,2	Integer controlled step position information	Y	
APC	1	Controllable analogue process value	Y	
APC	2	Controllable analogue process value	Y	
BAC	1,2	Binary controlled analog process value	N	
Notes:				

2.2.4 Common data class specifications for status settings

CDC	Ed	Description	Supported	Comment
SPG	1,2	Single point setting	N	
ING	1,2	Integer status setting	N	
ENG	1,2	Enumerated status setting	N	
ORG	1,2	Object reference setting	N	
TSG	1,2	Time setting group	N	
CUG	2	Currency setting group	N	
VSG	2	Visible string setting	N	
Notes:				

2.2.5 Common data class specifications for analogue settings

CDC	Ed	Description	Supported	Comment
ASG	1,2	Analogue setting	N	
CURVE	1,2	Setting curve	N	
CSG	1,2	Curve shape setting	N	
Notes:				

2.2.6 Common data class specifications for description information

CDC	Ed	Description	Supported	Comment
DPL	1,2	Device name plate	N	
LPL	1,2	Logical node name plate	N	
CSD	1,2	Curve shape description	N	
Notes:				

2.2.7 Common data class specifications for tracking

CDC	Ed	Description	Supported	Comment
CST	2	Common service tracking	N	
BTS	2	Buffered report tracking service	N	
CTS	2	Control tracking service	N	
GTS	2	GOOSE Control block tracking service	N	
LTS	2	Log control block tracking service	N	
MTS	2	MSVCB tracking service	N	
NTS	2	USVCB control block tracking service	N	
OTS	2	Log tracking service	N	
STS	2	SGCB tracking service	N	
UTS	2	Unbuffered report tracking service	N	
Notes:				

Supported:

Y = Client can issue an ASCI service on this CDC and process the data from/to the CDC

N = Client can't issue an ASCI service on this CDC and doesn't process the data from/to the CDC

3. Protocol Implementation eXtra Information for Testing (PIXIT)

3.1 Introduction

This document specifies the protocol implementation extra information for testing (PIXIT) of the IEC 61850 interface in the client system: "<G500>" with version "<2.00>", further referred to as "client".

Together with the PICS and the MICS the PIXIT forms the basis for a conformance test according to IEC 61850-10.

The following chapters specify the PIXIT for each applicable ACSI service model as structured in IEC 61850-10 and the "Conformance Test Procedures for Client System with IEC 61850-8-1 interface".

3.2 PIXIT for Configuration

ID	Ed	Description	Value / Clarification
Cf1	1,2	Describe how the client handles nameplate configuration revision mismatches	Not Supported
Cf2	1,2	Describe how the client handles report control block configuration revision mismatches	Not Supported

3.3 PIXIT for Association model

ID	Ed	Description	Value / Clarification
As1	1,2	Guaranteed number of servers that can set-up an association simultaneously (one association per server)	500 (for Model G500-B - 4 core APU, 16 GB RAM) 250 (for Model G500-A - 2 core APU, 8 GB RAM)
As2	1,2	Lost connection detection time range (default range of TCP_KEEPALIVE is 1 – 20 seconds)	7200 seconds
As3	1,2	Describe the behavior when association fails	Retry after configured no of Seconds. Default time is 30 seconds. But user can configure using config tool.
As4	3	Is authentication supported	N

As5	1,2	What is the maximum and minimum MMS PDU size.	Max MMS PDU size: It is a configuration parameter. Default is 32 KB Range: 64 to 262144
As6	1,2	What is the typical startup time after a power supply interrupt.	Time from power on to initialization complete is 2-3 minutes. After device startup, the device database points will initially be Invalid and Offline; Analog and Accumulator points will have zero value, and Digital Inputs will be OFF. Once association is established with the IED, the points will reflect the quality and value reported by the IED and Digital Outputs and Analog Outputs will be Online. Note that the device doesn't persist the point database so after restart, the points will again revert as indicated above: "After device startup".
As7	1,2	How does the client disconnect from the server?	Restart of device or device enable/disable option in HMI

3.4 PIXIT for Server model

ID	Ed	Description	Value / Clarification
Sr1	1,2	Maximum object identification length.	96 octets (32/64).
Sr2	1,2	Does client support auto description.	Not supported
Sr3	1,2	Describe how to view data values.	Data values can be viewed using Device Local HMI or Remote HMI
Sr4	1,2	What analogue value (MX) quality bits are used in the client.	Y Good, Y Invalid, Y Reserved, Y Questionable Y Overflow Y OutofRange Y BadReference Y Oscillatory Y Failure Y OldData N Inconsistent N Inaccurate Y Process Y Substituted Y Test Y OperatorBlocked

Sr5	1,2	Which status value (ST) quality bits are used in the client	Y Good, Y Invalid, Y Reserved, Y Questionable Y BadReference Y Oscillatory Y Failure Y OldData N Inconsistent N Inaccurate Y Process Y Substituted Y Test Y OperatorBlocked
Sr6	1,2	Describe how to view/display quality values	Quality Values can be viewed using the HMI. Use shmsingle command line tool for viewing test flag.
Sr7	1,2	Describe how to force a SetDataValues request	Enable the CF parameter write option in the Loader (Config tool) and issue a control to IED from Local HMI and user shall see PulseConfig attributes in a SetDataValues request.
Sr8	1,2	Describe how to force a GetDataValues request	GetDataValues request can be issued from Device HMI using pseudo point command and can be polled with a configurable interval
Sr9	1,2	Describe how to force a GetAllDataValues request	Not Supported
Sr10	1,2	Does the client support writing blkEna values?	N
ID	Ed	Description	Value / Clarification
Sr11	1,2	Describe how the client behaves in case of: - GetDataDefinition response- - GetDataDefinition response+ with more or less attributes as expected - GetLogicalDeviceDirectory response- - GetAllDataValues response- - GetAllDataValues response+ with more or less attributes as expected - GetDataValues response- - GetDataValues response+ with more or less attributes as expected - SetDataValues response-	All are Not Supported
Sr12	1,2	Which time quality attributes from the server are used in the client	N Leap Second Known, N ClockFailure Y Clock not synchronized

			N Accuracy
Sr13	1,2	Describe how to view time quality attributes	Use shmsingle command line tool

3.5 PIXIT for Data set model

ID	Ed	Description	Value / Clarification
Ds1	1,2	Describe how to force a GetDataSetValues request	GetDataSetValues request can be issued from Device HMI using pseudo point command
Ds2	1,2	Describe how to force a SetDataSetValues request	Not Supported
Ds3	1,2	Describe how to force a DeleteDataSet request	If the IED has a mismatched dataset, then the devjce will try to delete the dataset and then create a dynamic dataset.
Ds4	1,2	Describe how the client handles following dataset mismatches between the SCL and the data sets exposed via MMS: (1) new dataset element (2) missing dataset element (3) Reordered dataset members in a dataset of a different data type (4) Reordered dataset members in a dataset of the same data type	Device logs a message in its diagnostic log, tries to delete the dataset and then create a dynamic dataset.
Ds5	1,2	Describe how the client behaves in case of: - GetLogicalNodeDirectory(DATA-SET) response- - GetDataSetDirectory response- - GetDataSetValues response- - SetDataSetValues response-	Not Supported except GetDataSetValues. In the case of GetDataSetValues response, device logs a message in its diagnostic log and then marks the database points as Questionable and OldData.
Ds6	1,2	Maximum name length for dataset Maximum name length for dataset member, including LD and FC	<32/11$32> <32/61+3>
Ds11	1,2	Describe how to force a CreateDataSet request - non-persistent - persistent	For both types: CreateDataSet request will be issued automatically by the Device if it detects any mismatch between configured dataset using SCL file and IED supported Dataset through MMS requests. The new dataset shall always be persistent
Ds12	1,2	Describe how to force a DeleteDataSet request - non-persistent - persistent	For both types: Delete DataSet request will be issued automatically by the Device if it detects any mismatch between configured dataset using SCL file and IED supported Dataset through MMS requests. The new dataset shall always be persistent
Ds13	1,2	Describe how the client behaves in case of: - CreateDataSet response- - DeleteDataSet response-	Device logs the message in its diagnostic log and will revert to polling using the GetDataValues service

3.6 PIXIT for Substitution model

ID	Ed	Description	Value / Clarification
Sub1	1,2	Describe how to substitute a value	Not Supported

3.7 PIXIT for Setting group control model

ID	Ed	Description	Value / Clarification
Sg1	1,2	How can the client be forced to send a GetLogicalNodeDirectory(SGCB) request	Not Supported
Sg2	1,2	Describe how to change the active setting group	Not Supported
Sg3	1,2	Describe how to get the actual setting group values	Not Supported
Sg4	1,2	Describe how to edit setting group values	Not Supported
Sg5	1,2	Describe how the client behaves in case of: - GetSGCBValues response- - SelectEditSG response- - SetEditSGValue response- - SelectActiveSG response- - ConfirmEditSGValues response- - The configured SG differs from the actual setting group	Not Supported
Sg6		Does the client read the optional ResvTms value?	Not supported

3.8 PIXIT for Reporting model

ID	Ed	Description	Value / Clarification
Rp1	1,2	Does the client search for RCB in all logical nodes? If not, specify the logical nodes	No Client does not search for RCB. It directly accesses the pre-configured RCB's
Rp2	1,2	Which dynamic RCB attributes are/can be configured by the client	RptID Y DataSet Y Optional fields Y Trigger conditions Y Buffer time Y Integrity period Y
Rp3	1,2	Does the client supports IED's with indexed and non-indexed report control blocks (RCB)	BRCB indexed Y BRCB not indexed Y URCB indexed Y UCB not indexed Y

Rp4	1,2	The supported trigger conditions are	integrity Y data change Y quality change Y data update Y general interrogation Y
Rp5	1,2	The minimum required optional fields are	sequence-number N report-time-stamp Y reason-for-inclusion Y data-set-name N data-reference N buffer-overflow Y entryID Y confRev N
Rp6	1,2	Does the client support segmented reports	Y
Rp7	1	Does the client support pre-assigned RCB	N
Rp8	1,2	Does the client support reported data set containing structured data objects or data attributes?	reporting of data objects Y reporting of data attributes Y
Rp9	1,2	Describe how the client does respond when an previously used URCB is reserved by another client for: • Indexed URCB with max>1 configured in SCL (static reporting) • Indexed URCB with max=1 configured in SCL (static reporting) • URCB not configured in SCL (dynamic reporting	First two bullets, client will continue to retry until URCB is available. Client does not support last bullet.
Rp10	1,2	Describe how the client does respond when an previously used BRCB is reserved by another client for: • Indexed BRCB with max>1 configured in SCL (static reporting) • Indexed BRCB with max=1 configured in SCL (static reporting) • BRCB not configured in SCL (dynamic reporting	First two bullets, client will continue to retry until BRCB is available. Client does not support last bullet
Rp11	1,2	Describe how the client does respond on a SetBRCBValues(EntryID) respond-	No special processing. The Client will always issue a write to the GI during RCB initialization.

Rp12	1,2	Describe how the client does respond when a report has an unknown: dataset, RptID, unexpected number of dataset entries, and/or unexpected data type format entries	The client will accept any report that has a matching RptID and will process all expected dataset entries. It will ignore unexpected dataset entries. However, it will accept a report with a different dataset name if the RptID and dataset entries match the expected values.
Rp13	1,2	Describe how the client detects reporting configuration changes (mismatches). Does it check the "configuration revision" attributes and/or does it check the dataset members? Is the dataset update done online or offline?	Check ConfRev N Check dataset members Y Dataset update online or offline: **Online** If device supports deleting and creating of a dataset, update of dataset elements are Online else Offline)
Rp14	1,2	Describe how to force the client to change the RCB buffer time	Client will automatically write the RCB buffer time on startup based on the configuration.
Rp15	1,2	Does client set server TrgOps.GI prior to first issuance of GI command?	Y
Rp16	1,2	Describe how to force the client to send the GI request	Operate the Retrieve All Datasets pseudo DO point for the IED from the device HMI.
Rp17	1,2	Describe how to force the client to enable a RCB	It is done automatically based on the configuration
Rp18	1,2	Describe how the client does respond when a report control block is renamed or deleted - Does it prevent reading the deleted RCB - If it reads the missing RCB, how does it handle the GetURCBValues or GetBRCBValues response-	Device will continue to retry reading the RCB. A message shall be logged in the diagnostic log on response-
Rp19	1,2	Describe how the client behaves in case of: - SetURCBValues response- - Unsupported optional fields - Unsupported trigger condition(s)	Device will continue to retry reading the RCB. Device will write the optional fields and trigger conditions as part of its initialization procedure, so the last two bullets are not applicable.
Rp20	1,2	Describe how the client behaves in case of: - Buffer overflow	Device sets the Reporting Buffer Overflow DI pseudo point, which can be viewed in the HMI. Device sets the GI data attribute n the Buffered RCB.
Rp21	1,2	Describe how to force the client to send SetBRCBValues request for - EntryID - PurgeBuf	After the device has received at least one report, restart the device and it will write the EntryID received from the last report as part of initialization of the remote server. The device will never send a PurgeBuf.
Rp22	1,2	Does the client support writing resvTms	Y
Rp23	1,2	Does the client support reading owner	N
Rp24	2	Does the device function only as test equipment?	N

3.9 PIXIT for Logging model

ID	Ed	Description	Value / Clarification
Lg1	1,2	Does the client search for LCB in all logical nodes? when not specify the logical nodes	Not Supported
Lg2	1,2	Describe how to change LCB attributes	Not Supported
Lg3	1,2	Describe how to force the client to enable a LCB	Not Supported
Lg4	1	Does the client support sending QueryLogByTime and/or QueryLogAfter	Not Supported
Lg5	2	Describe how to force the client to change GLOG settings	Not Supported
Lg6	1,2	Describe how the client behaves in case of: - Renamed LCB - Removed LCB - Renamed Logical Device - Renamed LOG	Not Supported
Lg7	1,2	Describe how the client behaves in case of: - GetLCBValues response- - GetLogStatusValues response- - SetLCBValues response-	Not Supported

3.10 PIXIT for GOOSE control block model

ID	Ed	Description	Value / Clarification
		<additional items>	Not supported

3.11 PIXIT for Control model

ID	Ed	Description	Value / Clarification
Ctl1	1,2	What control modes are supported	Y status-only Y direct-with-normal-security Y sbo-with-normal-security Y direct-with-enhanced-security Y sbo-with-enhanced-security
Ctl2	1,2	Is Time activated operate (operTm) supported	N
Ctl3	1,2	Is “operate-many” supported	Y
Ctl4	1,2	Can the client set the test flag?	Y
Ctl5	1,2	What check conditions can be set	Y synchrocheck Y interlock-check
Ctl6	1,2	Which originator categories are supported and what is the originator identification?	Orcat **Station control, Remote control,** and **Automatic Station Control** is supported OrIdent is **D400**
Ctl7	1,2	Describe if and how the client sets/increments the ctlNum	It is incremented each time a new sequence control is done

Ctl8	1,2	What does the client when it receives a LastApplicationError and describe how to view the additional cause?	It displays the AddCause on its HMI
Ctl9	1,2	What does the client when its receives a Select, SelectWithValue or Operate respond negative ?	It displays the AddCause on its HMI
Ctl10	1,2	Can the client change the control model via online services?	No
Ctl11	1	What does the client when the ctlModel is not initialized in the SCL?	It retrieves the ctlModel from the IED
Ctl12	1,2	What does the client when the ctlModel in SCD and in SERVER SIMULATOR is different?	It uses retrieved ctlModel from the IED
Ctl13	1,2	Describe how to view a - CommandTermination request+ - CommandTermination request- - TimeActivatedOperateTermination request+ and request-	Command Termination request positive and negative responses will be logged by the client in its log file. The AddCause of the CommandTermination will be displayed in the HMI.

3.12 PIXIT for Time and time synchronization model

ID	Ed	Description	Value / Clarification
Tm1	1,2	Describe how to view the internal time & quality or how to expose the timestamp and timestamp quality via the IEC 61850 interface	View: timestamp can be viewed on HMI Expose: for example, in Operate request
Tm2	1,2	What time quality bits are supported	N LeapSecondsKnown N ClockFailure N ClockNotSynchronized
Tm3	1,2	What is the behavior when the time synchronization signal/messages are lost	No change in behavior.
Tm4	1,2	When is the quality bit "Clock failure" set?	Not Supported
Tm5	1	When is the quality bit "Clock not synchronized" set?	Not Supported

3.13 PIXIT for File transfer model

ID	Ed	Description	Value / Clarification
Ft1	1,2	Describe when or how to force the client to request GetServerDirectory(FILE) and what it does with the responded filenames	The test configuration includes the ARRM application configured to retrieve files from a simulated IED defined in the test gateway IID file using the RDRE logical node and the RcdMade DI point. The ARRM application will automatically request the IEC 61850 client to retrieve new files whenever the RcdMade DI toggles.

			Toggle the RcdMade DI on the server simulator. The device will issue the request and then retrieve new files that were not retrieved since the last RcdMade DI change.
Ft2	1,2	Does the client uses a wildcard in the GetServerDirectory(FILE) request	Y, wildcard = "*"
Ft3	1,2	Does the client support IED's that include the path in the file name in the GetServerDirectory(FILE) respond?	N path included Y path not included
Ft4	1,2	Does the client support IED's that use the file separator	Y "/" N "\"
Ft5	1,2	What is the maximum file name size including path	160
Ft6	1,2	Can the client read a file with size 0	Y
Ft7	1,2	Are directory/file names case sensitive	Case sensitive
Ft8	1,2	Maximum file size	100M
Ft9	1,2	Describe how the client behaves in case of: - GetFile response- - GetFileAttributes response- - SetFile response-	Device will log a message in the device diagnostic log and abort the file transfer. SetFile is not supported.

3.14 PIXIT for Service Tracking Model

ID	Ed	Description	Value / Clarification
Tr1	2	Which tracking services are supported by the client: - BrcbTrk - UrcbTrk - LocbTrk - GocbTrk - MsvcbTrk - UsvcbTrk - SgcbTrk - SpcTrk - DpcTrk - IncTrk - EncTrk - ApcFTrk - ApcIntTrk - BscTrk - IscTrk - BacTrk - GenTrk	 N N N N N N N N N N N N N N N N N N N
Tr2	2	Describe how to view the tracking objects or their attributes	Not supported

4. TISSUES Implementation Conformance Statement (TICS)

4.1 Introduction

This tissue implementation conformance statement is applicable for the IEC 61850 client interface in G500 Firmware Version 2.00. According to the UCA IUG QAP the Tissue conformance statement is required to perform a conformance test and is referenced on the certificate.

4.2 Mandatory Edition 2 Tissues

Below tables give an overview of the applicable mandatory Tissues.

"Supported by client":

"**Y**": means that the client supports servers that have implemented the respective tissue.

"**ni**": No impact on testing

"**na**": not applicable if the client does not support the corresponding ACSI service(s)

4.2.1 Part 6 Tissue List

Part 6 Tissue	Description	Supported by client
658	Tracking related features	na
663	FCDA element cannot be a "functionally constrained logical node"	Y
668	Autotransformer modeling	na
719	ConfDataSet - maxAttributes definition is confusing	Y
721	Log element name	na
768	bType VisString65 is missing	Y
779	object references	Y
788	SICS S56 from optional to mandatory	na
789	ConfLdName as services applies to both server and client (supportsLdname)	na
804	valKind and IED versus System configuration (valimport)	Y
806	Max length of log name inconsistent between -6 and -7-2	ni
807	Need a way to indicate if "Owner" present in RCB	Y
822	Extension of IED capabilities	Y
823	ValKind for structured data attributes	Y
824	Short addresses on structured data attributes	Y
825	Floating point value	Y
845	SGCB ResvTms	na
853	SBO and ProtNs	Y

855	Recursive SubFunction	na
856	VoltageLevel frequency and phases	ni
857	Function/SubFunction for ConductingEquipment	na
886	Missing 8-1 P-types	na
901	tServices as AP or as IED element	Y
936	SupSubscription parameter usage is difficult	na
1175	IPv6 address lowercase only	na

4.2.2 Part 7-1 Tissue List

Part 7-1 Tissue	Description	Supported by client
828	Data model namespace revision IEC 61850-7-4:2007[A]	Y
1151	simulated GOOSE disappears after 1st appearance when LPHD.Sim = TRUE	na
1196	Extensions to standardized LN classes made by third parties Note: this tissue is not final yet	na

4.2.3 Part 7-2 Tissue List

Part 7-2 Tissue	Description	Supported by client
778	AddCause values – add value not-supported	Y
780	What are unsupported trigger option at a control block?	Y
783	TimOper Resp- ; add Authorization check	na
786	AddCause values 26 and 27 are switched	Y
820	Mandatory ACSI services (use for PICS template)	Y
858	typo in enumeration ServiceType	ni
861	dchg of ConfRev attribute	na
876	GenLogiclNodeClass and SGCB, GoCB, MsvCB, UsvCB	ni
1038	Loss of Info Detection After Resynch	Y
1062	Entrytime not used in CDC	ni
1071	Length of DO name	ni
1091	The sentence "The initial value of EditSG shall be 0", has to be stated in part 7.2 not in 8.1	na
1127	Missing owner attribute in BTS and UTS	na
1163	Old report in URCB	ni
1202	GI not optional	ni

4.2.4 Part 7-3 Tissue List

Part 7-3 Tissue	Description	Supported by client
697	persistent command / PulseConfig	Y
698	Wrong case is BAC.dB attribute	na
722	Units for 'h' and 'min' not in UnitKind enumeration.	ni
919	Presence Condition for sVC	ni
925	Presence of i or f attribute - Problem with writing	Y
926	Presence Conditions within RangeConfig	na

4.2.5 Part 7-4 Tissue List

Part 7-4 Tissue	Description	Supported by client
671	mistake in definition of Mod & Beh	Y
674	CDC of ZRRC.LocSta is wrong	na
675	SIML LN	ni
676	Same data object name used with different CDC	na
677	MotStr is used with different CDC in PMMS and SOPM LN classes	na
679	Remove CycTrMod Enum	na
680	SI unit for MHYD.Cndct	ni
681	Enum PIDAlg	ni
682	ANCR.ParColMod	ni
683	Enum QVVR.IntrDetMth	ni
685	Enum ParTraMod	ni
686	New annex H - enums types in XML	Y
694	Data object CmdBlk	ni
696	LSVS.St (Status of subscription)	ni
712	interpretation of quality operatorBlocked	Y
713	DO Naming of time constants in FFIL	na
724	ANCR.Auto	na
725	Loc in LN A-group	Y
734	LLN0.OpTmh vs. LPHD.OpTmh	na
735	ISAF.Alm and ISAF.AlmReset	na
736	PFSign	na
742	GAPC.Str, GAPC.Op and GAPC.StrVal	Y
743	CCGR.PmpCtl and CCGR.FanCtl	na
744	LN STMP, EEHealth and EEName	na
772	LPHD.PwrUp/PwrDn shall be transient	Y
773	Loc, LocKey and LocSta YPSH and YLTC	Y
774	ITCI.LocKey	na
775	KVLV.ClsLim and OpnLim	ni
776	LPHD.OutOv/InOv and LCCH.OutOv/InOv	ni
800	Misspelling in CSYN	na
802	CCGR and Harmonized control authority	na
808	Presence condition of ZMOT.DExt and new DOs	na
831	Setting of ConfRevNum in LGOS	na
838	Testing in Beh=Blocked	Y
844	MFLK.PhPiMax, MFLK.PhPiLoFil, MFLK.PhPiRoot DEL->WYE	na
849	Presence conditions re-assessing in case of derived statistical calculation	na
877	QVUB -settings should be optional	na
909	Remove ANCR.ColOpR and ColOpL	na
920	Resetable Counter is NOT resetable	Y
932	Rename AVCO.SptVol to AVCO.VolSpt	na
939	Change CDC for ANCR.FixCol	na
991	LGOS: GoCBRef (as well as LSVS.SvCBRef) should be mandatory	ni
1007	PTRC as fault indicator - Update of description required	ni
1044	TapChg in AVCO	na
1077	Rename DOnames within LTIM	na

Note: Tissues 675, 735, 772, 775, 776, 878 are not relevant for conformance testing.

4.2.6 Part 8-1 Tissue List

Part 8-1 Tissue	Description	Supported by client
784	Tracking of control (CTS)	na
817	Fixed-length GOOSE float encoding	ni
834	File dir name length 64	Y
951	Encoding of Owner attribute	Y
1040	More associate error codes	Y
1178	Select Response+ is non-null value	Y

Compare the TISSUE database for more details: www.tissues.iec61850.com

MODIFICATION RECORD

VERSION	REV.	DATE	Author	Change Description
1.00	0	2nd May, 2019	G. LaMarre	Created.
2.00	0	11th May, 2020	N. Kandula	Updated PICS for Ed2, appended MICS/PIXIT/TICS.
	1	13th May, 2020	G. LaMarre	Updated PIXIT for Association Model, PIXIT for File transfer model.
	2	3rd June, 2020	N. Kandula	Updated PIXIT for Dataset Model, PIXIT for Server Model, PIXIT for Reporting Model, ACSI Service Conformance Statement.
			B. Popescu	Added clarification about MCP family and G500.

GE
Grid Solutions

IEC 60870-5-101/104 Client (DCA) for the Multifunction Controller Platform

Conformance Statement

NTEK-A031M-0CS

Version 1.00 Revision 0

Associated Software Release: Version 1.00

imagination at work

General

COPYRIGHT NOTICE

© 2019, General Electric Company. All rights reserved.

The Software Product described in this documentation may only be used in accordance with the applicable License Agreement. The Software Product and Associated Material are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable, and are delivered with Restricted Rights. Such restricted rights are those identified in the License Agreement, and as set forth in the "Restricted Rights Notice" contained in paragraph (g) (3) (Alternate III) of FAR 52.227-14, Rights in Data-General, including Alternate III (June 1987).

If applicable, any use, modification, reproduction release, performance, display or disclosure of the Software Product and Associated Material by the U.S. Government shall be governed solely by the terms of the License Agreement and shall be prohibited except to the extent expressly permitted by the terms of the License Agreement.

The information contained in this online publication is the exclusive property of General Electric Company, except as otherwise indicated. You may view, copy and print documents and graphics incorporated in this online publication (the "Documents") subject to the following: (1) the Documents may be used solely for personal, informational, non-commercial purposes; (2) the Documents may not be modified or altered in any way; and (3) General Electric Company withholds permission for making the Documents or any portion thereof accessible via the internet. Except as expressly provided herein, you may not use, copy, print, display, reproduce, publish, license, post, transmit or distribute the Documents in whole or in part without the prior written permission of General Electric Company. If applicable, any use, modification, reproduction, release, performance, display, or disclosure of the Software Product and Associated Material by the U.S. Government shall be governed solely by the terms of the License Agreement and shall be prohibited except to the extent expressly permitted by the terms of the License Agreement.

The information contained in this online publication is subject to change without notice. The software described in this online publication is supplied under license and may be used or copied only in accordance with the terms of such license.

TRADEMARK NOTICES

GE and are trademarks and service marks of General Electric Company.

* Trademarks of General Electric Company.

Other company or product names mentioned in this document may be trademarks or registered trademarks of their respective companies.

Contents

1. IEC 60870-5-101 Client Interoperability Profile 4

1.1 System or Device (8.1) 4
1.2 Network Configuration (8.2) 4
1.3 Physical Layer (8.3) 4
1.4 Link Layer (8.4) 5
1.5 Application Layer (8.5) 6
1.6 Basic Application Functions (8.6) 10

2. IEC 60870-5-104 Client Interoperability Profile 14

2.1 System or Device (9.1) 14
2.2 Network Configuration (9.2) 14
2.3 Physical layer (9.3) 14
2.4 Link Layer (9.4) 15
2.5 Application Layer (9.5) 15
2.6 Basic Application Functions (9.6) 20

1. IEC 60870-5-101 Client Interoperability Profile

This interoperability profile presents the sets of parameters and alternatives, and identifies by selection, those items required for implementation in the GE Grid Solutions MCP. The following legend reflects the options used in this selection of requirements:

- ☒ Function or ASDU is used as standardized (default)
- ■ A black check box indicate that the option cannot be selected (and is thus not required)
- R Function or ASDU is used in reverse mode
- B Function or ASDU is used in standard and reverse mode
- ☐ Function or ASDU is not used

In cases where several options are available, for example, multiple lengths of address fields, the GE Grid Solutions MCP shall be configurable to use the required value.

In this document, the bracketed number trailing each subheading title refers to the corresponding section number within the IEC 60870-5-101 standard.

1.1 System or Device (8.1)

- ☐ System definition
- ☒ Controlling station definition (Master)
- ☐ Controlled station definition (Slave)

1.2 Network Configuration (8.2)

(network-specific parameter)

- ☒ Point-to-point
- ☒ Multiple point-to-point
- ☒ Multipoint-party line
- ☒ Multipoint-star

1.3 Physical Layer (8.3)

(network-specific parameter)

1.3.1 Transmission Speed (Control Direction)

Unbalanced interchange circuit V.24/V.28 Standard	Unbalanced interchange circuit V.24/V.28 Recommended if > 1,200 bit/s	Balanced Interchange Circuit X.24/X.27	
☐ 100 bit/s	☒ 2,400 bit/s	☐ 2,400 bit/s	☐ 56,000 bit/s
☐ 200 bit/s	☒ 4,800 bit/s	☐ 4,800 bit/s	☐ 64,000 bit/s
☒ 300 bit/s	☒ 9,600 bit/s	☐ 9,600 bit/s	
☒ 600 bit/s	☒ 19,200 bit/s	☐ 19,200 bit/s	
☒ 1,200 bit/s		☐ 38,400 bit/s	

1.3.2 Transmission Speed (Monitor Direction)

Unbalanced Interchange Circuit V.24/V.28 Standard	Unbalanced Interchange Circuit V.24/V.28 Recommended if > 1,200 bit/s	Balanced Interchange Circuit X.24/X.27	
☐ 100 bit/s	☒ 2,400 bit/s	☐ 2,400 bit/s	☐ 56,000 bit/s
☐ 200 bit/s	☒ 4,800 bit/s	☐ 4,800 bit/s	☐ 64,000 bit/s
☒ 300 bit/s	☒ 9,600 bit/s	☐ 9,600 bit/s	
☒ 600 bit/s	☒ 19,200 bit/s	☐ 19,200 bit/s	
☒ 1,200 bit/s		☐ 38,400 bit/s	

Note: The master station shall only support the Unbalanced Interchange (Circuit V2.4/V2.8). The combination of V.24 and V.28 is ITU-T's equivalent to the EIA's RS-232.

1.4 Link Layer (8.4)

(network-specific parameter)

Frame format FT 1.2 (IEC 60870-5-1 Section 6.2.4.2) fixed and variable length is used (length is configurable).
Single character 1 (IEC 60870-5-1 Section 6.2.4.3) is used as an acknowledge.
Fixed time out interval is used (value is configurable).

Link Transmission Procedure

- ☒ Balanced transmission
- ☒ Unbalanced transmission

Address Field of the Link

- ☐ Not present (balanced transmission only)
- ☒ One byte
- ☒ Two bytes
- ☒ Structured
- ☒ Unstructured

Frame Length

☐☐255 Maximum length L (number of bytes)

configurable ~~Time during which repetitions are permitted (Trp) or~~ number of repetitions.

Note: For unbalanced mode, Maximum Frame Length (L) = Maximum Length of ADSU Frame. For balanced mode, Max Frame Length (L) = Maximum Length of ADSU Frame + 1 + Link Address Length.

When using an unbalanced link layer, the following ASDU types are returned in Class 2 messages (low priority) with the indicated clauses of transmission:

☐ The standard assignment of ASDUs to Class 2 messages is used as follows

Type identification	Cause of transmission
9,11,13,21	<1>

☐ A special assignment of ASDUs to Class 2 messages is used as follows

Type identification	Cause of transmission

Note: In response to a Class 2 poll, a controlled station can respond with Class 1 data when there is no Class 2 data available.

1.5 Application Layer (8.5)

1.5.1 Transmission Mode for Application Data

Mode 1 (Least significant byte first), as defined in clause 4.10 of IEC 60870-5-4, is used exclusively for all application data.

1.5.2 Common Address of ASDU

(system-specific parameter)

☒ One byte ☒ Two bytes

1.5.3 Information Object Address

(system-specific parameter)

☒ One byte
☒ Two bytes
☒ Three bytes
☒ Structured
☒ Unstructured

1.5.4 Cause of Transmission

(system- specific parameter)

☒ One byte

☒ Two bytes (with originator address).
Set to zero in case of no originator address

1.5.5 Selection of Standard ASDUs

1.5.5.1 Process Information in Monitor Direction

(station-specific parameter)

☒	<1>	:=	Single-point information	M_SP_NA_1
☒	<2>	:=	Single-point information with time tag	M_SP_TA_1
☒	<3>	:=	Double-point information	M_DP_NA_1
☒	<4>	:=	Double-point information with time tag	M_DP_TA_1
☒	<5>	:=	Step position information	M_ST_NA_1
☒	<6>	:=	Step position information with time tag	M_ST_TA_1
☒	<7>	:=	Bitstring of 32 bits	M_BO_NA_1
☒	<8>	:=	Bitstring of 32 bits with time tag	M_BO_TA_1
☒	<9>	:=	Measured value, normalized value	M_ME_NA_1
☒	<10>	:=	Measured value, normalized value with time tag	M_ME_TA_1
☒	<11>	:=	Measured value, scaled value	M_ME_NB_1
☒	<12>	:=	Measured value, scaled value with time tag	M_ME_TB_1
☒	<13>	:=	Measured value, short floating-point value	M_ME_NC_1
☒	<14>	:=	Measured value, short floating-point value with time tag	M_ME_TC_1
☒	<15>	:=	Integrated totals	M_IT_NA_1
☒	<16>	:=	Integrated totals with time tag	M_IT_TA_1
☐	<17>	:=	Event of protection equipment with time tag	M_EP_TA_1
☐	<18>	:=	Packed start events of protection equipment with time tag	M_EP_TB_1
☐	<19>	:=	Packed output circuit information of protection equipment with time tag	M_EP_TC_1
☒	<20>	:=	Packed single-point information with status change detection	M_PS_NA_1
☒	<21>	:=	Measured value, normalized value without quality descriptor	M_ME_ND_1
☒	<30>	:=	Single-point information with time tag CP56Time2a	M_SP_TB_1
☒	<31>	:=	Double-point information with time tag CP56Time2a	M_DP_TB_1
☒	<32>	:=	Step position information with time tag CP56Time2a	M_ST_TB_1
☒	<33>	:=	Bit string of 32 bits with time tag CP56Time2a	M_BO_TB_1
☒	<34>	:=	Measured value, normalized value with time tag CP56Time2a	M_ME_TD_1
☒	<35>	:=	Measured value, scaled value with time tag CP56Time2a	M_ME_TE_1
☒	<36>	:=	Measured value, short floating point with time tag CP56Time2a	M_ME_TF_1
☒	<37>	:=	Integrated totals with time tag CP56Time2a	M_IT_TB_1
☐	<38>	:=	Event of protection equipment with time tag CP56Time2a	M_EP_TD_1
☐	<39>	:=	Packed start events of protection equipment with time tag CP56Time2a	M_EP_TE_1

☐	<40>	:=	Packed output circuit information of protection equipment with time tag CP56Time2a	M_EP_TF_1

1.5.5.2 Process Information in Control Direction

(station-specific parameter)

☒	<45>	:=	Single command	C_SC_NA_1
☒	<46>	:=	Double command	C_DC_NA_1
☒	<47>	:=	Regulating step command	C_RC_NA_1
☒	<48>	:=	Set point command, normalized values	C_SE_NA_1
☒	<49>	:=	Set point command, scaled value	C_SE_NB_1
☒	<50>	:=	Set point command, short floating-point value	C_SE_NC_1
☐	<51>	:=	Bitstring of 32 bits	C_BO_NA_1

1.5.5.3 System Information in Monitor Direction

(station-specific parameter)

☒	<70>	:=	End of initialization	M_EI_NA_1

1.5.5.4 System Information in Control Direction

(station specific parameter)

☒	<100>	:=	Interrogation command	C_IC_NA_1
☒	<101>	:=	Counter interrogation command	C_CI_NA_1
☐	<102>	:=	Read command	C_RD_NA_1
☒	<103>	:=	Clock synchronization command	C_CS_NA_1
☒	<104>	:=	Test command	C_TS_NA_1
☐	<105>	:=	Reset process command	C_RP_NA_1
☒	<106>	:=	Delay acquisition command	C_CD_NA_1

1.5.5.5 Parameter in Control Direction

(station-specific parameter)

☐	<110>	:=	Parameter of measured value, normalized value	P_ME_NA_1
☐	<111>	:=	Parameter of measured value scaled value	P_ME_NB_1
☐	<112>	:=	Parameter of measured value, short floating-point value	P_ME_NC_1
☐	<113>	:=	Parameter activation	P_AC_NA_1

1.5.5.6 File Transfer

(station-specific parameter)
File Download and Upload

☐	<120>	:=	File ready	F_FR_NA_1
☐	<121>	:=	Section ready	F_SR_NA_1
☐	<122>	:=	Call directory, select file, call file, call section	F_SC_NA_1
☐	<123>	:=	Last section, last segment	F_LS_NA_1
☐	<124>	:=	Ack file, ack section	F_AF_NA_1
☐	<125>	:=	Segment	F_SG_NA_1
☐	<126>	:=	Directory {blank or **x**, only available in monitor (standard) direction}	F_DR_TA_1

1.5.5.7 Type identifier and Cause of Transmission Assignments

(station-specific parameter)
Shaded box[es] are not required.
Blank = Function or ASDU is not used

Type identification		Cause of transmission																	
		1	2	3	4	5	6	7	8	9	10	11	12	13	20 to 36	37 to 41	44	45	46	47
<1>	M_SP_NA_1		x	x								x	x		x					
<2>	M_SP_TA_1			x								x	x							
<3>	M_DP_NA_1		x	x								x	x		x					
<4>	M_DP_TA_1			x								x	x							
<5>	M_ST_NA_1		x	x								x	x		x					
<6>	M_ST_TA_1			x								x	x							
<7>	M_BO_NA_1		x	x											x					
<8>	M_BO_TA_1			x																
<9>	M_ME_NA_1	x	x	x											x					
<10>	M_ME_TA_1			x																
<11>	M_ME_NB_1	x	x	x											x					
<12>	M_ME_TB_1			x																
<13>	M_ME_NC_1	x	x	x											x					
<14>	M_ME_TC_1			x																
<15>	M_IT_NA_1			x												x				
<16>	M_IT_TA_1			x												x				
<17>	M_EP_TA_1																			
<18>	M_EP_TB_1																			
<19>	M_EP_TC_1																			
<20>	M_PS_NA_1		x	x											x					
<21>	M_ME_ND_1	x	x	x											x					
<30>	M_SP_TB_1			x								x	x							
<31>	M_DP_TB_1			x								x	x							
<32>	M_ST_TB_1			x								x	x							
<33>	M_BO_TB_1			x																
<34>	M_ME_TD_1			x																
<35>	M_ME_TE_1			x																
<36>	M_ME_TF_1			x																
<37>	M_IT_TB_1			x												x				
<38>	M_EP_TD_1																			

<39>	M_EP_TE_1																		
<40>	M_EP_TF_1																		
<45>	C_SC_NA_1						x	x			x						x	x	x	x
<46>	C_DC_NA_1						x	x			x						x	x	x	x
<47>	C_RC_NA_1						x	x			x						x	x	x	x
<48>	C_SE_NA_1						x	x			x						x	x	x	x
<49>	C_SE_NB_1						x	x			x						x	x	x	x

Type identification		Cause of transmission																		
		1	2	3	4	5	6	7	8	9	10	11	12	13	20 to 36	37 to 41	44	45	46	47
<50>	C_SE_NC_1						x	x			x						x	x	x	x
<51>	C_BO_NA_1																			
<70>	M_EI_NA_1				x															
<100>	C_IC_NA_1						x	x			x						x	x	x	x
<101>	C_CI_NA_1						x	x			x						x	x	x	x
<102>	C_RD_NA_1																			
<103>	C_CS_NA_1			x			x	x									x	x	x	x
<104>	C_TS_NA_1						x	x									x	x	x	x
<105>	C_RP_NA_1																			
<106>	C_CD_NA_1						x	x									x	x	x	x
<110>	P_ME_NA_1																			
<111>	P_ME_NB_1																			
<112>	P_ME_NC_1																			
<113>	P_AC_NA_1																			
<120>	F_FR_NA_1																			
<121>	F_SR_NA_1																			
<122>	F_SC_NA_1																			
<123>	F_LS_NA_1																			
<124>	F_AF_NA_1																			
<125>	F_SG_NA_1																			
<126>	F_DR_TA_1																			

1.6 Basic Application Functions (8.6)

1.6.1 Station Initialization

(station-specific parameter)

☐ Remote initialization

1.6.2 Cyclic Data Transmission

(station-specific parameter)

☒ Cyclic data transmission

1.6.3 Read Procedure

(station-specific parameter)

☐ Read Procedure

1.6.4 Spontaneous Transmission

(station-specific parameter)

☒ Spontaneous transmission

1.6.5 Double Transmission of Information Objects with Cause of Transmission Spontaneous

(Station-specific parameter)
The following type identification can be transmitted in succession caused by a single status change of an information object. The information object addresses for which double transmission is enabled are defined in a project-specific list.

☐ Single-point information M_SP_NA_1, M_SP_TA_1, M_SP_TB_1 and M_PS_NA_1
☐ Double-point information M_DP_NA_1, M_DP_TA_1 and M_DP_TB_1
☐ Step position information M_ST_NA_1, M_ST_TA_1 and M_ST_TB_1
☐ Bitstring of 32 bits M_BO_NA_1, M_BO_TA_1 and M_BO_TB_1
☐ Measured value, normalized value M_ME_NA_1, M_ME_TA_1, M_ME_ND_1 and M_ME_TD_1
☐ Measured value, scaled value M_ME_NB_1, M_ME_TB_1 and M_ME_TE_1
☐ Measured value, short floating-point number M_ME_NC_1, M_ME_TC_1 and M_ME_TF_1

1.6.6 Station Interrogation

(station-specific parameter)

☒ global

☒ group 1	☒ group 7	☒ group 13
☒ group 2	☒ group 8	☒ group 14
☒ group 3	☒ group 9	☒ group 15
☒ group 4	☒ group 10	☒ group 16
☒ group 5	☒ group 11	
☒ group 6	☒ group 12	

Information Object Address assigned to each group shall be shown in a separate table

1.6.7 Clock Synchronization

(station-specific parameter)

☒ Clock synchronization
☒ Day of week used
☐ RES1, GEN (time tag substituted/not substituted used
☐ SU-bit (summertime) used

1.6.8 Command Transmission

(object-specific parameter)

- ☒ Direct command transmission
- ☒ Direct set point command transmission
- ☒ Selected and Execute Command
- ☐ Select and execute set point command
- ☒ C-SE ACTTERM Used

- ☒ No additional definition
- ☒ Short pulse duration (duration determined by a system parameter in the controlled station)
- ☒ Long pulse duration (duration determined by a system parameter in the controlled station)
- ☒ Persistent output

1.6.9 Transmission of Integrated Totals

(station or object-specific parameter)

- ☒ Mode A: Local freeze with spontaneous transmission
- ☒ Mode B: Local freeze with counter interrogation
- ☐ Mode C: Freeze and transmit by counter-interrogation command
- ☐ Mode D: Freeze by counter-interrogation command, frozen values reported spontaneously

- ☐ Counter read
- ☐ Counter freeze without reset
- ☐ Counter freeze with reset
- ☐ Counter reset

- ☒ General request counter
- ☒ Request counter group 1
- ☒ Request counter group 2
- ☒ Request counter group 3
- ☒ Request counter group 4

Addresses per group must be defined

1.6.10 Parameter Loading

(object-specific parameter)

- ☐ Threshold value
- ☐ Smoothing factor
- ☐ Low limit for transmission of measured value
- ☐ High limit for transmission of measured value

1.6.11 Parameter Activation

(object-specific parameter)

☐ Activ/deactiv. of persistent cyclic or periodic transmission of the addressed object

1.6.12 Test Procedure

(station-specific parameter)

☒ Test procedure

1.6.13 File Transfer

(station-specific parameter)

1.6.13.1 File Transfer in Monitor Direction

☐ Transparent file
☐ Transmission of disturbance data of protection equipment
☐ Transmission of sequences of events
☐ Transmission of sequences of recorded analogue values

1.6.13.2 File Transfer in Control Direction

☐ Transparent file

1.6.14 Background Scan

(station-specific parameter)

☒ Background scan

1.6.15 Acquisition of Transmission Delay

(station-specific parameter)

☒ Acquisition of transmission delay

2. IEC 60870-5-104 Client Interoperability Profile

This interoperability profile presents the sets of parameters and alternatives, and identifies by selection, those items required for implementation in the GE Grid Solutions MCP. The following legend reflects the options used in this selection of requirements:

- ☒ Function or ASDU is used as standardized (default)
- ■ A black check box indicate that the option cannot be selected (and is thus not required)
- R Function or ASDU is used in reverse mode
- B Function or ASDU is used in standard and reverse mode
- ☐ Function or ASDU is not used

The text descriptions of parameters, which are not applicable to this standard, are strike-through (corresponding check box is marked black).

In this document, the bracketed number trailing each subheading title refers to the corresponding section number within the IEC 60870-5-104 standard.

Note: In addition, the full specification of a system shall possibly require individual selection of certain parameters for certain parts of the system, such as the individual selection of scaling factors for individually addressable measured values.

2.1 System or Device (9.1)

- ☐ System definition
- ☒ Controlling station definition (Master)
- ☐ Controlled station definition (Slave)

2.2 Network Configuration (9.2)

(network-specific parameter)

- ■ ~~Point-to-point~~
- ■ ~~Multiple point-to-point~~
- ■ ~~Multipoint party line~~
- ■ ~~Multipoint star~~

2.3 Physical layer (9.3)

(network-specific parameter)

2.3.1 Transmission Speed (Control Direction)

Unbalanced interchange circuit V.24/V.28 Standard	Unbalanced interchange circuit V.24/V.28 Recommended if > 1200 bit/s	Balanced Interchange Circuit X.24/X.27	
~~100 bit/s~~	~~2,400 bit/s~~	~~2,400 bit/s~~	~~56,000 bit/s~~
~~200 bit/s~~	~~4,800 bit/s~~	~~4,800 bit/s~~	~~64,000 bit/s~~
~~300 bit/s~~	~~9,600 bit/s~~	~~9,600 bit/s~~	
~~600 bit/s~~	~~19,200 bit/s~~	~~19,200 bit/s~~	
~~1,200 bit/s~~		~~38,400 bit/s~~	

2.3.2 Transmission Speed (Monitor Direction)

Unbalanced Interchange Circuit V.24/V.28 Standard	Unbalanced Interchange Circuit V.24/V.28 Recommended if > 1200 bit/s	Balanced Interchange Circuit X.24/X.27	
~~100 bit/s~~	~~2,400 bit/s~~	~~2,400 bit/s~~	~~56,000 bit/s~~
~~200 bit/s~~	~~4,800 bit/s~~	~~4,800 bit/s~~	~~64,000 bit/s~~
~~300 bit/s~~	~~9,600 bit/s~~	~~9,600 bit/s~~	
~~600 bit/s~~	~~19,200 bit/s~~	~~19,200 bit/s~~	
~~1,200 bit/s~~		~~38,400 bit/s~~	

2.4 Link Layer (9.4)

(network-specific parameter)

Frame format FT1.2, single character 1 and the fixed time out interval is used exclusively in this companion standard.

Link Transmission Procedure

- ~~Balanced transmission~~
- ~~Unbalanced transmission~~

Frame Length

- ~~Maximum length L (number of bytes)~~

Address Field of the Link

- ~~Not present (balanced transmission only)~~
- ~~One byte~~
- ~~Two bytes~~
- ~~Structured~~
- ~~Unstructured~~

2.5 Application Layer (9.5)

2.5.1 Transmission Mode for Application Data

Mode 1 (Least significant byte first), as defined in clause 4.10 of IEC 870-5-4, is used exclusively in this companion standard.

2.5.2 Common address of ASDU

(system-specific parameter)

- ■ ~~One byte~~
- ☒ Two bytes

2.5.3 Information Object Address

(system-specific parameter)

- ■ ~~One byte~~
- ■ ~~Two bytes~~
- ☒ Three bytes
- ☒ Structured
- ☒ Unstructured

2.5.4 Cause of Transmission

(system-specific parameter)

- ■ ~~One byte~~
- ☒ Two bytes (with originator address). Originator address is set to zero if not used

2.5.5 Length of APDU

(system specific parameter)

The maximum length of APDU is 253 (default). The maximum length can be reduced by the system.

☐ 253 Maximum length of APDU

2.5.6 Selection of Standard ASDUs

2.5.6.1 Process Information in Monitor Direction

(station-specific parameter)

☒	<1>	:=	Single-point information	M_SP_NA_1
■	~~<2>~~	~~:=~~	~~Single-point information with time tag~~	~~M_SP_TA_1~~
☒	<3>	:=	Double-point information	M_DP_NA_1
■	~~<4>~~	~~:=~~	~~Double-point information with time tag~~	~~M_DP_TA_1~~
☒	<5>	:=	Step position information	M_ST_NA_1
■	~~<6>~~	~~:=~~	~~Step position information with time tag~~	~~M_ST_TA_1~~
☒	<7>	:=	Bitstring of 32 bits	M_BO_NA_1
■	~~<8>~~	~~:=~~	~~Bitstring of 32 bits with time tag~~	~~M_BO_TA_1~~
☒	<9>	:=	Measured value, normalized value	M_ME_NA_1
■	~~<10>~~	~~:=~~	~~Measured value, normalized value with time tag~~	~~M_ME_TA_1~~
☒	<11>	:=	Measured value, scaled value	M_ME_NB_1
■	~~<12>~~	~~:=~~	~~Measured value, scaled value with time tag~~	~~M_ME_TB_1~~
☒	<13>	:=	Measured value, short floating-point value	M_ME_NC_1
■	~~<14>~~	~~:=~~	~~Measured value, short floating-point value with time tag~~	~~M_ME_TC_1~~
☒	<15>	:=	Integrated totals	M_IT_NA_1

■	~~<16>~~	~~:=~~	~~Integrated totals with time tag~~	~~M_IT_TA_1~~
■	~~<17>~~	~~:=~~	~~Event of protection equipment with time tag~~	~~M_EP_TA_1~~
■	~~<18>~~	~~:=~~	~~Packed start events of protection equipment with time tag~~	~~M_EP_TB_1~~
■	~~<19>~~	~~:=~~	~~Packed output circuit information of protection equipment with time tag~~	~~M_EP_TC_1~~
☒	<20>	:=	Packed single-point information with status change detection	M_PS_NA_1
☒	<21>	:=	Measured value, normalized value without quality descriptor	M_ME_ND_1
☒	<30>	:=	Single-point information with time tag CP56Time2a	M_SP_TB_1
☒	<31>	:=	Double-point information with time tag CP56Time2a	M_DP_TB_1
☒	<32>	:=	Step position information with time tag CP56Time2a	M_ST_TB_1
☒	<33>	:=	Bit string of 32 bits with time tag CP56Time2a	M_BO_TB_1
☒	<34>	:=	Measured value, normalized value with time tag CP56Time2a	M_ME_TD_1
☒	<35>	:=	Measured value, scaled value with time tag CP56Time2a	M_ME_TE_1
☒	<36>	:=	Measured value, short floating point with time tag CP56Time2a	M_ME_TF_1
☒	<37>	:=	Integrated totals with time tag CP56Time2a	M_IT_TB_1
☐	<38>	:=	Event of protection equipment with time tag CP56Time2a	M_EP_TD_1
☐	<39>	:=	Packed start events of protection equipment with time tag CP56Time2a	M_EP_TE_1
☐	<40>	:=	Packed output circuit information of protection equipment with time tag CP56Time2a	M_EP_TF_1

Either the ASDUs of the set <2>, <4>, <6>, <8>, <10>, <12>, <14>, <16>, <17>, <18>, <19> or of the set <30> – <40> are used.

2.5.6.2 Process Information in Control Direction

(station-specific parameter)

☒	<45>	:=	Single command	C_SC_NA_1
☒	<46>	:=	Double command	C_DC_NA_1
☒	<47>	:=	Regulating step command	C_RC_NA_1
☒	<48>	:=	Set point command, normalized values	C_SE_NA_1
☒	<49>	:=	Set point command, scaled value	C_SE_NB_1
☒	<50>	:=	Set point command, short floating-point value	C_SE_NC_1
☐	<51>	:=	Bitstring of 32 bits	C_BO_NA_1
☒	<58>	:=	Single command with time tag CP56Time2a	C_SC_TA_1
☒	<59>	:=	Double command with time tag CP56Time2a	C_DC_TA_1
☒	<60>	:=	Regulating step command with time tag CP56Time2a	C_RC_TA_1
☒	<61>	:=	Set point command, normalized values with time tag CP56Time2a	C_SE_TA_1
☒	<62>	:=	Set point command, scaled value with time tag CP56Time2a	C_SE_TB_1
☒	<63>	:=	Set point command, short floating-point value with time tag CP56Time2a	C_SE_TC_1
☐	<64>	:=	Bitstring of 32 bits with time tag CP56Time2a	C_BO_TA_1

Either the ASDUs of the set <45> – <51> or of the set <58> – <64> are used.

2.5.6.3 System Information in Monitor Direction

(station-specific parameter)

☒	<70>	:=	End of initialization	M_EI_NA_1

2.5.6.4 System Information in Control Direction

(station-specific parameter)

☒	<100>	:=	Interrogation command	C_IC_NA_1
☒	<101>	:=	Counter interrogation command	C_CI_NA_1
☐	<102>	:=	Read command	C_RD_NA_1
☒	<103>	:=	Clock synchronization command	C_CS_NA_1
■	~~<104>~~	~~:=~~	~~Test command~~	~~C_TS_NA_1~~
☐	<105>	:=	Reset process command	C_RP_NA_1
■	~~<106>~~	~~:=~~	~~Delay acquisition command~~	~~C_CD_NA_1~~
☒	<107>	:=	Test command with time tag CP56Time2a	C_TS_TA_1

Note that the master station sends an ASDU <107> (Test command with time tag) after channel switchover.

2.5.6.5 Parameter in Control Direction

(station-specific parameter)

☐	<110>	:=	Parameter of measured value, normalized value	P_ME_NA_1
☐	<111>	:=	Parameter of measured value scaled value	P_ME_NB_1
☐	<112>	:=	Parameter of measured value, short floating-point value	P_ME_NC_1
☐	<113>	:=	Parameter activation	P_AC_NA_1

2.5.6.6 File Transfer

(station-specific parameter)

File Download and Upload

☐	<120>	:=	File ready	F_FR_NA_1
☐	<121>	:=	Section ready	F_SR_NA_1
☐	<122>	:=	Call directory, select file, call file, call section	F_SC_NA_1
☐	<123>	:=	Last section, last segment	F_LS_NA_1
☐	<124>	:=	Ack file, ack section	F_AF_NA_1
☐	<125>	:=	Segment	F_SG_NA_1
☐	<126>	:=	Directory	F_DR_TA_1

2.5.6.7 Type identifier and Cause of Transmission Assignments

(station-specific parameter)
Shaded box[es] are not required.
Blank = Function or ASDU is not used

Type identification		Cause of transmission																		
		1	2	3	4	5	6	7	8	9	10	11	12	13	20 to 36	37 to 41	44	45	46	47
<1>	M_SP_NA_1		x	x								x	x		x					
~~<2>~~	~~M_SP_TA_1~~			■		■						■	■							
<3>	M_DP_NA_1		x	x								x	x		x					
~~<4>~~	~~M_DP_TA_1~~			■		■						■	■							
<5>	M_ST_NA_1		x	x								x	x		x					
~~<6>~~	~~M_ST_TA_1~~			■		■						■	■							
<7>	M_BO_NA_1		x	x											x					
~~<8>~~	~~M_BO_TA_1~~			■		■														
<9>	M_ME_NA_1	x	x	x											x					
~~<10>~~	~~M_ME_TA_1~~			■		■														
<11>	M_ME_NB_1	x	x	x											x					
~~<12>~~	~~M_ME_TB_1~~			■		■														
<13>	M_ME_NC_1	x	x	x											x					
~~<14>~~	~~M_ME_TC_1~~			■		■														
<15>	M_IT_NA_1			x												x				
~~<16>~~	~~M_IT_TA_1~~			■												■				
~~<17>~~	~~M_EP_TA_1~~			■																
~~<18>~~	~~M_EP_TB_1~~			■																
~~<19>~~	~~M_EP_TC_1~~			■																
<20>	M_PS_NA_1		x	x											x					
<21>	M_ME_ND_1	x	x	x											x					
<30>	M_SP_TB_1			x								x	x							
<31>	M_DP_TB_1			x								x	x							
<32>	M_ST_TB_1			x								x	x							
<33>	M_BO_TB_1			x																
<34>	M_ME_TD_1			x																
<35>	M_ME_TE_1			x																
<36>	M_ME_TF_1			x																
<37>	M_IT_TB_1			x												x				
<38>	M_EP_TD_1																			
<39>	M_EP_TE_1																			
<40>	M_EP_TF_1																			
<45>	C_SC_NA_1						x	x			x						x	x	x	x
<46>	C_DC_NA_1						x	x			x						x	x	x	x
<47>	C_RC_NA_1						x	x			x						x	x	x	x
<48>	C_SE_NA_1						x	x			x						x	x	x	x
<49>	C_SE_NB_1						x	x			x						x	x	x	x

Type identification		Cause of transmission																	
		1	2	3	4	5	6	7	8	9	10	11	12	13	20 to 36	37 to 41	44	45	46	47
<50>	C_SE_NC_1						x	x			x						x	x	x	x
<51>	C_BO_NA_1																			
<58>	C_SC_TA_1						x	x			x						x	x	x	x
<59>	C_DC_TA_1						x	x			x						x	x	x	x
<60>	C_RC_TA_1						x	x			x						x	x	x	x
<61>	C_SE_TA_1						x	x			x						x	x	x	x
<62>	C_SE_TB_1						x	x			x						x	x	x	x
<63>	C_SE_TC_1						x	x			x						x	x	x	x
<64>	C_BO_TA_1																			
<70>	M_EI_NA_1				x															
<100>	C_IC_NA_1						x	x			x						x	x	x	x
<101>	C_CI_NA_1						x	x			x						x	x	x	x
<102>	C_RD_NA_1																			
<103>	C_CS_NA_1			x			x	x									x	x	x	x
~~<104>~~	~~C_TS_NA_1~~																			
<105>	C_RP_NA_1																			
~~<106>~~	~~C_CD_NA_1~~																			
<107>	C_TS_TA_1						x	x									x	x	x	x
<110>	P_ME_NA_1																			
<111>	P_ME_NB_1																			
<112>	P_ME_NC_1																			
<113>	P_AC_NA_1																			
<120>	F_FR_NA_1																			
<121>	F_SR_NA_1																			
<122>	F_SC_NA_1																			
<123>	F_LS_NA_1																			
<124>	F_AF_NA_1																			
<125>	F_SG_NA_1																			
<126>	F_DR_TA_1																			

2.6 Basic Application Functions (9.6)

Note that the master station sends STOPDT only in the case of channel switchover.

2.6.1 Station Initialization

(station-specific parameter)

☐ Remote initialization

2.6.2 Cyclic Data Transmission

(station-specific parameter)

☒ Cyclic data transmission

2.6.3 Read Procedure

(station-specific parameter)

☐ Read Procedure

2.6.4 Spontaneous Transmission

(station-specific parameter)

☒ Spontaneous transmission

2.6.5 Double Transmission of Information Objects with Cause of Transmission Spontaneous

(station-specific parameter)

The following type identification can be transmitted in succession caused by a single status change of an information object. The information object addresses for which double transmission is enabled are defined in a project-specific list.

☐ Single-point information M_SP_NA_1, M_SP_TA_1, M_SP_TB_1 and M_PS_NA_1
☐ Double-point information M_DP_NA_1, M_DP_TA_1 and M_DP_TB_1
☐ Step position information M_ST_NA_1, M_ST_TA_1 and M_ST_TB_1
☐ Bitstring of 32 bits M_BO_NA_1, M_BO_TA_1 and M_BO_TB_1
☐ Measured value, normalized value M_ME_NA_1, M_ME_TA_1, M_ME_ND_1 and M_ME_TD_1
☐ Measured value, scaled value M_ME_NB_1, M_ME_TB_1 and M_ME_TE_1
☐ Measured value, short floating-point number M_ME_NC_1, M_ME_TC_1 and M_ME_TF_1

2.6.6 Station Interrogation

(station-specific parameter)

☒ global

☒ group 1	☒ group 7	☒ group 13
☒ group 2	☒ group 8	☒ group 14
☒ group 3	☒ group 9	☒ group 15
☒ group 4	☒ group 10	☒ group 16
☒ group 5	☒ group 11	
☒ group 6	☒ group 12	

Information Object Address assigned to each group shall be shown in a separate table

2.6.7 Clock Synchronization

(station-specific parameter)

☒ Clock synchronization

2.6.8 Command Transmission

(object-specific parameter)

☒ Direct Command Transmission

☒ Direct set point command transmission

☒ Selected and Execute Command (Single, Double & Step Position commands)

☐ Select and execute set point command

☐ C-SE ACTTERM Used

☒ No additional definition

☒ Short pulse duration (duration determined by a system parameter in the outstation)

☒ Long pulse duration (duration determined by a system parameter in the outstation)

☒ Persistent output

☐ Supervision of maximum delay in command direction of Commands and Set Point Commands

☐ Maximum allowable delay for Commands and Set Point Commands

2.6.9 Transmission of Integrated Totals

(station or object-specific parameter)

☒ Mode A: Local freeze with spontaneous transmission

☒ Mode B: Local freeze with counter interrogation

☐ Mode C: Freeze and transmit by counter-interrogation command

☐ Mode D: Freeze by counter-interrogation command, frozen values reported spontaneously

☐ Counter read

☐ Counter freeze without reset

☐ Counter freeze with reset

☐ Counter reset

☒ General request counter

☒ Request counter group 1

☒ Request counter group 2

☒ Request counter group 3

☒ Request counter group 4

Addresses per group must be defined

2.6.10 Parameter Loading

(object-specific parameter)

☐ Threshold value

☐ Smoothing factor

☐ Low limit for transmission of measured value

☐ High limit for transmission of measured value

2.6.11 Parameter Activation

(object-specific parameter)

☐ Act/deact of persistent cyclic or periodic transmission of the addressed object

2.6.12 Test Procedure

(station-specific parameter)

☒ Test procedure

2.6.13 File Transfer

(station-specific parameter)

2.6.13.1 File Transfer in Monitor Direction

☐ Transparent file
☐ Transmission of disturbance data of protection equipment
☐ Transmission of sequences of events
☐ Transmission of sequences of recorded analogue values

2.6.13.2 File Transfer in Control Direction

☐ Transparent file

2.6.14 Background Scan

(station-specific parameter)

☒ Background scan

2.6.15 Acquisition of Transmission Delay

(station-specific parameter)

■ ~~Acquisition of transmission delay~~

2.6.16 Definition of Time Outs

Parameter	Default value	Remarks	Selected value
t_0	30 s	Time-out of connection establishment	**Configurable**
t_1	15 s	Time-out of send or test APDUs	**Configurable**
t_2	10 s	Time-out for acknowledges in case of no data messages $t_2 < t_1$	**Configurable**

t_3	20 s	Time-out of sending test frames in case of a long idle state	**Configurable**

Maximum range of values for all time-outs: 1 to 255 s, accuracy 1 s.

2.6.17 Maximum Number of Outstanding I Format APDUs *k* and Latest Acknowledge APDUs (*w*)

Parameter	Default value	Remarks	Selected value
K	12 APDUs	Maximum difference receives sequence number to send state variable	**Configurable**
W	8 APDUs	Latest acknowledge after receiving *w* I format APDUs	**Configurable**

Maximum range of values k: 1 to 32767 (2_{15}–1) APDUs, accuracy 1 APDU
Maximum range of values w: 1 to 32767 APDUs, accuracy 1 APDU (Recommendation: w should not exceed two-thirds of k).

2.6.18 Port Number

Parameter	Value	Remarks
Port number	2404	Configurable

2.6.19 RFC 2200 suite

RFC 2200 suite is an official Internet Standard that describes the state of standardization of protocols used in the Internet as determined by Internet Architecture Board (IAB). It offers a broad spectrum of actual standards used in the Internet. The suitable selection of documents from RFC 2200 defined in this standard for given projects must be chosen by the user of this standard.

- ☒ Ethernet 802.3
- ☐ Serial X.21 interface
- ☐ Other selection from RFC 2200:

List of valid documents from RFC 2200

1. .....
2. .....
3. .....
4. .....
5. .....
6. .....

MODIFICATION RECORD

VERSION	REV.	DATE	AUTHOR	CHANGE DESCRIPTION
1.00	0	2nd May, 2019	G. LaMarre	Created.

GE
Grid Solutions

MCP NERC-CIP5 Response

Product Bulletin

Date: April 21st, 2021 **Classification:** GE Information **Publication Number:** PRBT-0429

NOTICE **This document applies to the MCP family (G100/G500) unless otherwise indicated.**

Overview

The purpose of this document is to answer commonly asked questions pertaining to the features supported by the version 1.1 and further of MCP Series of Substation Gateway products. This is not a NERC-CIP document. Users of GE Grid Solutions MCP equipment may require this information for the purposes of assessment and implementation of NERC-CIP v5 processes.

Standard	Req #	Requirement	Applicable Security Measures
CIP-002-5.1 Bulk Electric System [BES] Cyber System Categorization	All	It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System (...)	Not Applicable (Responsible Entity Organizational function)
CIP-003-5 Security Management Controls	R1	Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies (...)	Not Applicable (Responsible Entity Organizational function)

imagination at work

© 2021 General Electric Company. All rights reserved.
* Trademarks of General Electric Company.

	R2	Each Responsible Entity for its assets identified in CIP-002-5, Requirement R1, Part R1.3, shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented cyber security policies that collectively address the following topics, and review and obtain CIP Senior Manager approval for those policies at least once every 15 calendar months.	Not Applicable (Responsible Entity Organizational function)
	R3	Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change.	Not Applicable (Responsible Entity Organizational function)
	R4	The Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator.	Not Applicable (Responsible Entity Organizational function)
CIP-004-5.1 Personnel & Training	R1 – R3	Awareness, Training and Personnel Risk Assessment	Not Applicable (Responsible Entity Organizational function)
	R4	Access Management Program	Not Applicable (Responsible Entity Organizational function)
	R5	Access Revocation	Responsible Entity Organizational function The MCP can help enforce this process thanks to its support for TACACS+ and LDAP, which provides a centralized administration point where users can be revoked. The MCP also supports manually deployed Certificate Revocation Lists to remove a user's access to network IEDs using SSL/TLS.

CIP-005-5 Electronic Security Perimeter	R1.1	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	Responsible Entity Organizational and Project Engineering function. MCP facilitates implementing this requirement by using different NICs.
	R1.2	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	Responsible Entity Organizational and Project Engineering function. MCP facilitates implementing this requirement by using different NICs. The MCP can constitute an EAP. User authentication is possible via login/password or certificates. For central authentication, multifactor authentication is possible with TACACS+RSA SecureID. The MCP can also be connected to an EAP – as desired.
	R1.3	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default	MCP facilitates implementing this requirement by using different NICs and an internal rule based and configurable firewall. The MCP will only enable the ports and services configured. The firewall will automatically block all other ports.
	R1.4	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	When used as an EAP, for the purpose of providing access to Cyber Assets, MCP can be configured to require name and certificate-based authentication. Authentication can be based on locally defined user or centrally managed users via LDAP or TACACS+.
	R1.5	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	The MCP logs authentication attempts, connections status, and firewall actions.
	R2.1	Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Responsible Entity Project Engineering function. MCP facilitates implementing this requirement by using different NICs and an internal rule based and configurable firewall and RBAC.
	R2.2	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	MCP can be configured to allow remote access sessions using HTTPS (TLS), SSH, and VPN.

	R2.3	Require multi-factor authentication for all Interactive Remote Access sessions	Responsible Entity Project Engineering function. For remote HMI access, MCP assists compliance by using LDAP or TACACS+ authentication which in turn can be configured to require RSA token access in the organization. For Remote Access sessions for the purpose of pass-through EAP connections ("virtual connection") – the MCP requires user names and keys/certificates.
CIP-006-5 Physical Security of BES Cyber Systems	All	All	Not applicable to MCP – Responsible Entity Organization function. MCP assists in implementing these requirements by providing a configurable real time interface to the systems which monitor Physical Access, using industry standard communication protocols (for e.g.: SNMP, MODBUS, ASCII). Events gathered can be alarmed locally or remotely via email, RSYNC over SSH, SFTP, FTP (push). Event can also be forwarded to a syslog server or a SIEM via syslog protocol.
CIP-007-5 Systems Security Management	R1.1	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device, then those ports that are open are deemed needed.	MCP facilitates implementing this requirement by using an internal firewall, rules based and configurable. The MCP will only enable the ports and services associated with the configured functionality. The firewall will automatically block all other ports. Users can further edit and customize the firewall rules as needed and close/open ports according to their needs.
CIP-007-5 Systems Security Management	R1.2	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	USB ports can be disabled. Network ports are disabled by default. Front maintenance port which can be disabled by configuration.

CIP-007-5 Systems Security Management	R2.1	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	The GE SDLC includes testing with vulnerability scanners and fuzzers tailored for the MCP. Our scanning tools are continuously updated for the latest vulnerabilities and issues and run against our devices. GE PSIRT maintains a registered users list for Cyber Security notifications. The process is setup to send notifications to registered users if a critical vulnerability is identified. Based on severity and exposure of vulnerability details, the assessment of new discovered vulnerabilities is within 30 days. MCP logs all installations of patches and this log is available to administrators.
CIP-007-5 Systems Security Management	R2.2	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	Responsible Entity Organizational function. Aided by the GE process notification of registered users.
CIP-007-5 Systems Security Management	R2.3	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Responsible Entity Organizational function. Aided by the GE process notification of registered users.
CIP-007-5 Systems Security Management	R2.4	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	Responsible Entity Organizational function.

CIP-007-5 Systems Security Management	R3.1	Deploy method(s) to deter, detect, or prevent malicious code.	Responsible Entity Organizational and Process Engineering function, for e.g. offline scanning of USB FLASH drives used for patching, control electronic access to resources. This is aided by the MCP being based on an embedded computer platform. MCP is built with in-depth security concept (access control, hardening, no backdoors, etc.). Even if an attacker finds a way to inject malicious code in the device, several other mechanisms are there to ensure security: • The device Operating system is a Linux base hardened following security best practices (ex. kernel hardening, privilege separation, etc.) • The Operating System security relies on secured containers which allow isolation between applications. • The MCP does not automatically mount USB drives when they are inserted. A user must login and manually mount the drive. Concerning the Windows hosted configuration tools such as DSAS (DS Agile Studio). We recommend the customer installs antimalware solution based on application whitelisting technology on all PCs.
CIP-007-5 Systems Security Management	R3.2	Mitigate the threat of detected malicious code.	Responsible Entity Organizational and Process Engineering function. The MCP aides by providing logs of all running application processes, with their unique ID and dependencies. The Operating System security relies on secured containers which allow isolation between applications.
CIP-007-5 Systems Security Management	R3.3	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	Responsible Entity Organizational and Process Engineering function. The MCP does not support the major delivery mechanisms of malware targeted for generic operating systems. See R3.1 answer

CIP-007-5 Systems Security Management	R4.1	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: • 4.1.1. Detected successful login attempts; • 4.1.2. Detected failed access attempts and failed login attempts;	The MCP logs successful and failed login attempts, as well as running processes with their application ID.
CIP-007-5 Systems Security Management	R4.1.3	Detected malicious code.	The MCP is an embedded computer platform, using Linux OS. The following major sources of entry of mainstream malware are simply not supported by the MCP: • Installable third-party programs using generic tools like apt-get, yum or windows installer • Auto mount and auto-run of programs on a USB stick or CD drive • Opening documents with embedded macros • Receiving emails with attachments • External web browsing • Open file shares The Responsible Entity Organizational and Process Engineering should develop procedures to control offline scanning of USB FLASH drives used for MCP patching. Also see R3.1 answer
CIP-007-5 Systems Security Management	R4.2	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): • 4.2.1. Detected malicious code from Part 4.1; and • 4.2.2. Detected failure of Part 4.1 event logging.	See R3.1 Failure of the event logging subsystem itself cannot be logged by the same failed subsystem; appropriate system architectures can be deployed, where absence of renewed logs present (uploaded) at an Enterprise Level can be detected and alarmed.

CIP-007-5 Systems Security Management	R4.3	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.	Responsible Entity Organizational and Process Engineering function. Logs in MCP are maintained by size, not by time. MCP log rotate mechanism maintains last 10 user activity log files, each 256 KB of size (2.56 MB maximum); the System Architecture should provision for the MCP to send these logs to an Enterprise Repository for long term availability.
CIP-007-5 Systems Security Management	R4.4	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Responsible Entity Organizational and Process Engineering function. Logs in MCP are maintained by size, not by time, it is up to the Responsible Entity to review them as needed.
CIP-007-5 Systems Security Management	R5.1	Have a method(s) to enforce authentication of interactive user access, where technically feasible.	All interactive user access to the MCP is subject to authentication, either local or remote (TACACS+, LDAP).
CIP-007-5 Systems Security Management	R5.2	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	Responsible Entity Organizational and Process Engineering function. MCP does not have generic accounts that cannot be changed. The following roles exist in MCP; a given user can be assigned to a role: • Administrator (full rights) • Supervisor (full access to the HMI) • Operator (can execute commands but cannot change configuration) • Observer (can only see data)
CIP-007-5 Systems Security Management	R5.3	Identify individuals who have authorized access to shared accounts.	Responsible Entity Organizational and Process Engineering function. For Local based authentication, the list of accounts is presented in the MCP configuration tools.
CIP-007-5 Systems Security Management	R5.4	Change known default passwords, per Cyber Asset capability.	Responsible Entity Organizational and Process Engineering function. MCP does not have passwords that cannot be changed.

CIP-007-5 Systems Security Management	R5.5	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: • 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and • 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	MCP complies and exceeds all R5.5 requirements for password complexity when Local based authentication is used. For Remote based authentication (TACAS+, LDAP) – the password complexity requirements must be implemented in the central servers.
CIP-007-5 Systems Security Management	R5.6	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	While the MCP alone doesn't enforce timely passwords changes, the Responsible Entity can meet this requirement by using centralized user management and procedures enforcing the timely changes.
CIP-007-5 Systems Security Management	R5.7	Where technically feasible, either: • Limit the number of unsuccessful authentication attempts; or • Generate alerts after a threshold of unsuccessful authentication attempts.	MCP complies to R5.7 requirements.
CIP-008-5 Cyber Security Incident Response	R1.1	One or more processes to identify, classify, and respond to Cyber Security Incidents.	Responsible Entity Organizational function. The MCP provides the necessary logs enabling the Responsible Entity to implement this requirement.

Plan Specifications	R1.2	One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident and notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. Initial notification to the ES-ISAC, which may be only a preliminary notice, shall not exceed one hour from the determination of a Reportable Cyber Security Incident.	Responsible Entity Organizational function. The MCP provides the necessary logs enabling the Responsible Entity to implement this requirement.
	R1.3	The roles and responsibilities of Cyber Security Incident response groups or individuals.	Responsible Entity Organizational function.
	R1.4	Incident handling procedures for Cyber Security Incidents.	Responsible Entity Organizational function.
	R2.1	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months (...)	Responsible Entity Organizational function.
	R2.2	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Responsible Entity Organizational function.
	R2.3	Retain records related to Reportable Cyber Security Incidents.	Responsible Entity Organizational function. Logs in MCP are maintained by size, not by time, it is up to the Responsible Entity to retain logs as required.
	R3.1	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response (...)	Responsible Entity Organizational function.
	R3.2	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan (...)	Responsible Entity Organizational function.

CIP-009-5 Recovery Plan Specifications	R1.1	Conditions for activation of the recovery plan(s).	Responsible Entity Organizational function.
	R1.2	Roles and responsibilities of responders.	Responsible Entity Organizational function.
	R1.3	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	Responsible Entity Organizational function. MCP assists compliance via snap-shot images which can be remotely retrieved and restored using DSAS (SFTP & SSH protocol).
	R1.4	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	Responsible Entity Organizational function. MCP assists compliance when using compressed configuration archives with integrity checks in place.
	R1.5	One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	Responsible Entity Organizational function. See R1.3
	R2.1	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	Responsible Entity Organizational function.
	R2.2	Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.	Responsible Entity Organizational function.

	R2.3	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Responsible Entity Organizational function.
	R3.1	No later than 90 calendar days after completion of a recovery plan test or actual recovery (...)	Responsible Entity Organizational function.
	R3.2	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan: • 3.2.1. Update the recovery plan; and • 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	Responsible Entity Organizational function
CIP-010-3 Configuration Change Management and Vulnerability Assessments	R1.1	Develop a baseline configuration, individually or by group, which shall include the following items: • Operating system(s) (including version) or firmware where no independent operating system exists; • Any commercially available or open-source application software (including version) intentionally installed; • Any custom software installed; • Any logical network accessible ports; and • 1.1.5. Any security patches applied.	Responsible Entity Organizational Function. MCP assists compliance by allowing users to create snapshots of the configurations used via DSAS.
	R1.2	Authorize and document changes that deviate from the existing baseline configuration.	Responsible Entity Organizational Function. DSAS Detailed Config Compare utility can help with the process based on the configurations.

	R1.3	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	Responsible Entity Organizational Function and Process.
	R1.4	For a change that deviates from the existing baseline configuration: • 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; • 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and • 1.4.3. Document the results of the verification.	Responsible Entity Organizational and Engineering Function and Process. Users should engage in necessary testing and qualification processes before installing or changing the MCP within a live BES Cyber System. MCP assists compliance by providing all configurations in XML format, which can be easily compared (via DSAS Detailed Config Compare utility).
	R1.5.1	Where technically feasible, for each change that deviates from the existing baseline configuration: • 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected;	Responsible Entity Organizational and Engineering Function and Process. Users should engage in necessary testing and qualification processes before installing or changing the MCP within a live BES Cyber System.
	R1.5.2	Where technically feasible, for each change that deviates from the existing baseline configuration: • 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	Responsible Entity Organizational and Engineering Function and Process. Users should engage in necessary testing and qualification processes before installing or changing the MCP within a live BES Cyber System.

	R2.1	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	Responsible Entity Organizational and Engineering Function and Process. MCP assists compliance by providing all configurations in XML format, which can be easily compared (via DSAS Detailed Config Compare utility).
	R3.1	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Responsible Entity Organizational and Engineering Function and Process.
	R3.2	Where technically feasible, at least once every 36 calendar months: • 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and • 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	Responsible Entity Organizational and Engineering Function and Process.
	R3.3	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	Responsible Entity Organizational and Engineering Function and Process.

	R3.4	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	Responsible Entity Organizational and Engineering Function and Process.
CIP-011-1 Cyber Security — Information Protection	R1.1	Method(s) to identify information that meets the definition of BES Cyber System Information.	Responsible Entity Organizational and Engineering Function and Process. Based on its end user application, the MCP can be a Medium or High Impact asset.
	R1.2	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	Responsible Entity Organizational and Engineering Function and Process. To further assist, the MCP offline configuration tool (DSAS) provides integrity validation for configuration archives and snapshots (when a strong password is used). The G500 SED is shipped with a default SED password (set in UEFI). The G100 SED has no password. In addition, if passwords are saved, a strong password is required.
	R2	R2.1: Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media. R2.2: Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.	Since the configuration and sensitive date exist in the MCP's removable SSD drives, it is recommended that these drives be removed before disposing the MCP or sending it for repairs. It is the Responsible Entity's responsibility to protect these drives and/or destroy the contained information accordingly.

Frequently Asked Questions (MCP)

The following NERC CIP-007-5: Frequent Asked Questions, are applicable to the MCP.

CIP-007-5 R1 – Ports and Services

Q : R1a - Provide a list of factory default open ports – tcp and udp

A : Please refer to the following table for complete list of ports. Factory default open ports are indicated by "Yes" from the "Enabled by default?" column.

Port Numbers	TCP/UDP	Enabled by default?	Used for
443	TCP	Yes	Sync to/from, Online Editor, PETC, Remote runtime HMI.
22	TCP	Yes	Snapshot save/restore, shell access to gateway, file transfer with Gateway.
922	TCP	No	Emergency administrator access, open only when remote authentication configured.
80, 8081	TCP	Yes	Settings GUI.
123	TCP	No	NTP, if configured.
Configurable, default 502	TCP	No	MODBUS, if configured.
Configurable, default 2404	TCP	No	IEC60870-5-104, if configured.
514	UDP	No	Rsyslog, if configured.
10514	TCP	No	Rsyslog, if configured.
Configurable, default 20000	TCP/ UDP	No	DNP, if configured.
Configurable, default 8001 – 8020	TCP	No	Pass-through or terminal server, if configured.
Configurable	TCP	No	TLS tunnel for pass through, terminal server or secure connection relay, if configured.
54000	TCP	No	LogicLinx, if configured.
162	UDP	No	SNMP, if configured.
Configurable, default 1194	UDP	No	OpenVPN, if configured.
51000	TCP	No	Hot Standby Sync Service, if Hot Standby configured
51001	TCP	No	Hot/Warm Standby Heart Beat, if Hot/Warm-Standby Configured.
51003	TCP	No	Standby pointing to active tunnel, if configured
51194, 51195	TCP	No	Hot/Warm Standby Tunnel, if Hot/Warm-Standby Configured

Q : R1b - Can these ports be closed via firmware or software?

A : Yes, by configuring with custom firewall rules.

Q : R1c - Can new ports be opened via firmware or software?

A : Yes, by configuring any LAN applications, Rsyslog Service, Secure Connection Relay, Terminal Server, SNMP, OpenVPN, or NTP, the associated ports will be opened.

CIP-007-5 R2 – Security Patch Management

Q : R2a - Are automated security update notifications available from the vendor via email?

A : GE Multilin™ maintains a registered users list for Cyber Security notifications. The process is setup to send notifications to registered users if a critical vulnerability is identified.

Q : Can GE provide periodic updates for the MCP that would bring software such as the operating system, web server, and database up to their current versions?

A : MCP updates are currently planned to be provided on an as-needed basis. Patch updates are signed, and signed firmware updates are under development. In the meantime, the method for at least MCP firmware v1.1 is to update the whole firmware as a single image with the configuration being backed up, upgraded, and restored by the desktop software.

CIP-007-5 R3 – Malicious software prevention

Q : R3a - Does the device support anti-malware tools?

A : No, as this is not currently technically feasible as well as the device does not run a generic OS but a tailored RTOS that is not designed to load or execute 3rd party software components or programs.

CIP-007-5 R4 – Security Status Monitoring

Q : R4a - Does the device provide support for automated security status monitoring tools, specifically for monitoring system events related to cyber security (example, syslog)?

A : Yes, the MCP logs events in SOEs can retrieve any syslog files from connected IEDs.

Q : R4b - Can the device log events, especially security related events?

A : Yes, the MCP logs successful and unsuccessful login attempts, any use of sudo, password change, SSH sessions information, and more.

Q : R4c - Can the device detect a security incident?

A : No, the MCP relies on a Security Event Manager software package to perform alerts of a security incident.

Q : R4d - Can the device send an alert upon detecting a security incident?

A : No, the MCP relies on a Security Event Manager software package to perform alerts of a security incident.

CIP-007-3 R5 – Account Management

Q : R5a - Can the device be accessed remotely via the network?

A : Yes, if configured.

Q : R5b - If yes, does the access method use login accounts?

A : Yes, the access method uses both local accounts and remote accounts via LDAP or TACACS server.

Q : R5c - Provide a list of factory default accounts and their access privileges (e.g. administrator, individual, shared, read-only, read-write)

A : Factory default User account/Username: defadmin; Access privilege: administrator. **This is an administrator account that is used only for initial IP address and admin user setup. As soon as an admin account is created and logged into, this 'defadmin' account is automatically removed.**

Serial default User account/Username: root; Access privilege: administrator. **This is present on all Linux computers, and the expectation is that the Customer will change this to a password of their choosing.**

Predix Edge Console default User/Username: admin; Access privilege: administrator. **This is present for future expansion. A default Admin user and password exist, and the expectation is that the Customer will change the password to something of their choosing.**

Q : R5d - Can new user accounts be created in addition to the factory default ones?

A : Yes.

Q : R5e - Can the privileges of the user accounts be changed for both – factory default and newly created ones?

A : No, the factory default user account privileges cannot be changed. The newly created account privileges can be changed for HMI use.

Q : R5f - Does the access require passwords?

A : Yes, access to the MCP always requires password.

Q : R5g - If yes, does the MCP enforce the password to have the minimum number of characters (combination of alpha, numeric, and special)?

A : Yes, the password must be minimum 8 characters and have at least one number and at least one special character.

Q : R5h - Can the device support a user access log?

A : Yes, the MCP support local SOE log can be accessed remotely, as well as the ability to retrieve any Syslog logs from any connected device.

Q : R5i - If yes, can the user access log be stored in the device for at least 90 days for auditing purposes?

A : Yes, the local user access log can be configured to hold enough records for normal account activity over a period of 90 days (e.g. 10,000 records).

In addition – SNMP related questions

Q : Does the device support SNMP?

A : Yes, as an SNMP client only.

Product Support

If you need help with any aspect of your GE Grid Solutions product, you can:

- Access the GE Grid Solutions Web site
- Search the GE Grid Solutions Technical Support library
- Contact GE Grid Solutions Technical Support

GE Grid Solutions Web Site

The GE Grid Solutions Web site provides fast access to technical information, such as manuals, release notes and knowledge base topics.

Visit us on the Web at: http://www.gegridsolutions.com

GE Grid Solutions Substation Automation Technical Support Library

This site serves as a document repository for post-sales requests. To get access to the Technical Support Web site, go to: http://sc.ge.com/*SASTechSupport

Contact GE Grid Solutions Technical Support

For help with any aspect of your GE Grid Solutions product, please contact our support team, 24/7, as follows:

Region	E-mail	Telephone
Global Contact Centre	ga.support@ge.com	+44 1785 250070
Central and East Asia andPacific	ga.supportCEAP@ge.com	+61 414 730 964
India	ga.supportIND@ge.com	+91 44 22648000
Middle East, North Africa andTurkey	ga.supportMENAT@ge.com	+971 42929467
Europe, Russia, CIS and Sub-Saharan Africa	ga.supportERCIS@ge.com	+34 94 4858854
North America	ga.supportNAM@ge.com	+1 877 605 6777
Latin America	ga.supportLAM@ge.com	+55 11 36187308

Copyright Notice

© 2021, General Electric Company. All rights reserved.

The information contained in this online publication is the exclusive property of General Electric Company, except as otherwise indicated. You may view, copy and print documents and graphics incorporated in this online publication (the "Documents") subject to the following: (1) the Documents may be used solely for personal, informational, non-commercial purposes; (2) the Documents may not be modified or altered in any way; and (3) General Electric Company withholds permission for making the Documents or any portion thereof accessible via the internet. Except as expressly provided herein, you may not use, copy, print, display, reproduce, publish, license, post, transmit or distribute the Documents in whole or in part without the prior written permission of General Electric Company. If applicable, any use, modification, reproduction, release, performance, display, or disclosure of the Software Product and Associated Material by the U.S. Government shall be governed solely by the terms of the License Agreement and shall be prohibited except to the extent expressly permitted by the terms of the License Agreement.
The information contained in this online publication is subject to change without notice. The software described in this online publication is supplied under license and may be used or copied only in accordance with the terms of such license.

Trademark Notice

GE and the GE monogram are trademarks and service marks of General Electric Company.

* Trademarks of General Electric Company. Other company or product names mentioned in this document may be trademarks or registered trademarks of their respective companies.

Document Revision History

Version	Revision	Date	Author	Change Description
1.00	0	Sept 30th, 2019	E. Nasi	Initial Release.
1.10	0	March 3rd, 2020	N. Ajwad	Added FAQ section.
	1	Aug 09th, 2020	N. Ajwad	Updated FAQ section.
2.00	0	Sept 30th, 2020	N. Ajwad	Updated for G500 v2.0: added information about G500 SED default password in section **CIP-011-1, R1.2.**
3.00	0	April 21st, 2021	E. Nasi	Updated for MCP family.