NAE Commissioning Guide

MS-NAE55xx-3, MS-NAE5510-2U, MS-NAE5510-3U, MS-NXE85SW-x

Building Technologies & Solutions www.johnsoncontrols.com 2022-06-03 LIT-1201519

Release 12.0



Contents

| Introduction | 7 |
|---|----|
| Summary of changes | 7 |
| Related documentation | 8 |
| NAE commissioning overview | 10 |
| Network Automation Engines (NAEs) | 10 |
| NCE25 models - Release 9.0.x | 11 |
| NAE35 models - Release 9.0.x | 11 |
| NAE45 models - Release 9.0.x | 12 |
| NAE55 models - Release 12.0 | 12 |
| NAE85 model - Release 12.0 | 12 |
| Warning banner | 13 |
| MS/TP communications bus | 14 |
| Metasys network sites | 14 |
| NAE commissioning | 16 |
| NAE configuration | 17 |
| Metasys UI on NAE85 | 19 |
| Site Management Portal user interface | 19 |
| Metasys Help Files | 22 |
| Browser recommendations for downloading Launcher | 22 |
| System Configuration Tool (SCT) | 22 |
| Controller Configuration Tool (CCT) | 23 |
| Archive databases | 23 |
| NAE disk image updates and archive database upgrades | 24 |
| Site Director | 24 |
| Computer name | 25 |
| Object name | 25 |
| Basic Access operating mode (small-capacity engines only) | 26 |
| Login user names and passwords | 26 |
| NAE connectivity | 28 |
| Time zone, date, and time management | 29 |
| Alarms and events | 29 |
| Email notification | 30 |
| Syslog DDA | 31 |
| Simple Network Management Protocol (SNMP) notification | 34 |
| Initial default NCE/NAE configuration | 35 |
| Allow HTTP | 36 |
| Advanced Security Enabled | 38 |
| FIPS and non-FIPS compliance | 39 |
| System and user preferences | 41 |
| Reset command device | 41 |
| NAE network sensitivity | 42 |

| Detailed Procedures | 42 |
|--|----|
| Installing Launcher to access the NAE | 43 |
| Establishing direct connection to an NAE | 44 |
| Preparing NAE for a network that supports DHCP and DNS | 45 |
| Preparing NAE for a network without DHCP and without DNS support when the NAE uses APIPA | 48 |
| Preparing NAE for a network without DHCP and without DNS support when the NAE uses a static IP address | 49 |
| Preparing NAE for a network that supports DHCP but not DNS | 50 |
| Preparing NAE for a network that supports DNS but not DHCP | 51 |
| Accessing Site Management Portal UI on an NAE | 51 |
| Entering basic NAE parameters in the focus screen | 52 |
| Entering NAE network parameters | 54 |
| Creating email alarm and event notifications and destinations in SMP UI at Release 11.0 and earlier | 55 |
| Configuring encrypted email | 61 |
| Configuring encrypted email with no authentication required | 61 |
| Configuring encrypted email with SMTP authentication | 62 |
| Configuring encrypted email with POP-before-SMTP authentication | 62 |
| Creating NAE SNMP alarm notifications and destinations | 63 |
| Enabling Syslog reporting | 66 |
| Setting the time, date, time zone, and time synchronization | 68 |
| Setting up NAE alarm parameters | 69 |
| Editing existing alarm parameters | 69 |
| Creating new alarms | 69 |
| Designating an NAE as a child of a Site Director | 70 |
| Changing Site Director with the SCT | 72 |
| Removing user accounts from a demoted Site Director | 72 |
| Moving security database and clearing it from demoted Site Director prior to Release 6.0 | 73 |
| Moving security database and clearing it from demoted Site Director Release 6.0 or later | 73 |
| Enabling and disabling Warning Banner | 74 |
| Adjusting NAE network sensitivity | 76 |
| Replacing an NAE | 80 |
| Enabling Expert mode | 81 |
| Troubleshooting | 81 |
| Common NAE problems | 82 |
| Corrupted NAE memory | |
| Login problems | 83 |
| Network connection related problems | 83 |
| NAE reset related problems | 84 |
| Troubleshooting guide | |
| NAE diagnostic tools | 88 |

| NAE LED status indicators | |
|--|-----|
| NCE25 LED startup sequence | 93 |
| NAE35/NAE45 LED startup sequence | 94 |
| NAE55 LED startup sequence | 94 |
| Diagnostic tab | 94 |
| Summary tab | 96 |
| Troubleshooting procedures | 97 |
| Verifying Ethernet network communications (Ping) | 97 |
| Pre-boot execution environment (PXE) | 97 |
| Determining the NAE IP address and device name for a network connection | 97 |
| Determining the NAE IP address by using the SCT Pro | 98 |
| Determining the NAE IP address and device name by using a serial port monitor | |
| Setting a computer to be compatible with APIPA | 99 |
| Technical specifications - NCE, NAE, and NIE models | 99 |
| Appendix: Time zone, date, and time management | 109 |
| Introduction | 109 |
| Time synchronization methods | 110 |
| - Windows time synchronization | 110 |
| Multicast time synchronization | 111 |
| BACnet time synchronization | 111 |
| Example network | 111 |
| Multiple time zones | 112 |
| Site time server | 113 |
| Local time and date indication on status bar | 113 |
| Selecting a time synchronization method | 114 |
| Configuring Site Director for Windows time synchronization | 114 |
| Configuring Site Director for Multicast time synchronization | 115 |
| Configuring Site Director for BACnet time synchronization (Network Engines only) | 116 |
| Configuring Site Director time to sync with external time source | 117 |
| Selecting a site time server for the Metasys Server Site Director (Windows) | 118 |
| Selecting a site time server for the Metasys Server Site Director (Multicast) | 118 |
| Selecting a site time server for the Network Engine Site Director (Windows) | 119 |
| Selecting a site time server for the Network Engine Site Director (Multicast) | 120 |
| Setting the time zone | 121 |
| Setting the time zone on the Metasys Server Site Director | 121 |
| Setting the time zone in the Network Engine Site Director | 123 |
| Setting the date and time on the Site Director | 124 |
| Setting the date and time in the Metasys Server Site Director | 124 |
| Setting the date and time in the Site Director Network Engine | 126 |
| Multicast time synchronization settings | 128 |
| Verifying the Site Director defined for an engine or server | 129 |
| Appendix: Configuring and Maintaining Preferences | 130 |
| Configuring and maintaining preferences introduction | 130 |

| Preferences Concepts | |
|---|-----|
| System and user preferences | |
| Managing preferences | |
| Detailed Procedures | |
| Configuring preferences | |
| Restoring default system preferences | |
| Copying preferences between devices | |
| Restoring default user preferences | |
| Removing user preference files | |
| Copying user preferences to another user | |
| Preserving preferences for a network engine update | |
| Appendix: Certificate Management | 136 |
| Certificate management introduction | |
| Certificate Signing Request (CSR) | 138 |
| Import certificate | |
| Export certificate | |
| Certificate list view | |
| Certificate tree view | 140 |
| Download certificate | |
| Detailed procedures | |
| Requesting a certificate | |
| Importing a certificate | |
| Exporting a certificate | |
| Downloading a certificate | |
| Uploading a certificate | |
| Deleting a certificate | |
| Deleting a certificate request | 151 |
| Replacing a self-signed certificate | |
| Backing up a certificate | |
| Appendix: Erasing Network Engine SDRAM and flash memory | 152 |
| Erasing Network Engine SDRAM and flash memory | 152 |
| Software terms | |
| Product warranty | |
| Patents | |
| Contact information | 156 |
| | |

Introduction

Important: The MS-NAE55xx-3 is the only NAE hardware engine you can upgrade to Release 12.0. The MS-NAE55xx-2 engines must remain at Release 11.0 or earlier, and the other, small capacity network engines, such as the NAE35s, NAE45s, and NCE25s, must remain at Release 9.0.x or earlier.

This document describes how to:

- commission a Network Control Engine (NCE) or a Network Automation Engine (NAE) for network connectivity in several network scenarios
- access the Metasys system Site Management Portal UI on an NAE
- configure the basic NAE parameters for initial operation on the network
- enable or disable Advanced Security and Hypertext Transfer Protocol Secure (https)
- troubleshoot an NAE
- configure the NAE DDAs for sending alarm and event messages through email and SNMP
- configure a Syslog DDA for sending events and audits to an external Syslog server

This document does not describe how to mount, wire, or power on an NAE. For more information, refer to NAE55 Installation Guide (Part No. 24-10051-43). Also, this document does not describe how to build or download an archive database for a Metasys system site or how to configure an NAE to monitor and control a building automation system (BAS). For those procedures, refer to *SCT: System Configuration Tool Help (LIT-12011964)*.

(i) Note: In this document, NAE refers to all NCE25, NAE35, NAE45, NAE45-Lite, NAE55, and NAE85 models, unless noted otherwise. Also, the term small-capacity engine refers to any NCE25, NAE35, NAE45, or NAE45-Lite model, and the term large-capacity engine refers to any NAE55 or NAE85 model.

In addition to this document, refer to the following literature for information specific to your model of NAE:

- NCE25 Series: refer to the NCE Technical Bulletin (LIT-12011267)
- NAE85 Engine: refer to the NAE85 Commissioning Guide (LIT-12011044)

For commissioning information about the newest network engine models, or for steps on how to replace an NAE with an SNE, or an NCE with an SNC, refer to the following literature:

- SNE: refer to the SNE Commissioning Guide (LIT-12013352)
- SNC: refer to the SNC Commissioning Guide (LIT-12013295)

For information about commissioning an NAE to use the built-in third-party integrations, refer to the specific network engine document that covers the integration that you want to add, listed in Table 1.

Summary of changes

The following information is new or revised:

- Updated Release 9.0.8 to 9.0.x as the latest release for affected network engines
- Added Metasys UI on NAE85
- Updated the end of the Site Management Portal user interface section with information on the SC Network Port and Update objects in the navigation tree
- Updated Troubleshooting guide

- Replaced *Determining the NAE SNE IP address by using the NCT* with Determining the NAE IP address by using the SCT Pro
- Removed references to Open Data Server (ODS) as it is discontinued at Release 12.0
- Updated Technical specifications NCE, NAE, and NIE models
- Added a note to Appendix: Certificate Management regarding BACnet/SC certificates
- Removed references to the NAE-S (MS-NAE551S-2) model as it was discontinued from July 2021
- Replaced the term Master with Manager where appropriate

Related documentation

Table 1: NAE Related documentation

| For information on | See document |
|--|--|
| Overview of the Metasys system network features and functions | Metasys System Configuration Guide (LIT-12011832) |
| Definition of terms, concepts, and acronyms commonly used to describe the Metasys System | Metasys System Extended Architecture Glossary Technical Bulletin (LIT-1201612) |
| General network and information technology definitions and concepts, and creating a printer DDA for an NAE | Network and IT Guidance Technical Bulletin (LIT-12011279) |
| Daily Operation of the Metasys system network, navigating the SMP UI or SCT UI, monitoring and | Metasys Site Management Portal Help (LIT-1201793) |
| controlling BAS networks, and connecting to cloud- based applications | SCT: System Configuration Tool Help (LIT-12011964) |
| Installation considerations and guidelines, mounting, wiring, and starting up an SNE | SNE Network Engine Installation Guide (Part No. 24-10143-01647) |
| Installation considerations and guidelines, mounting, wiring, and starting up an SNC | SNC Network Engine Installation Guide (Part No. 24-10143-01892) |
| Installation considerations and guidelines, mounting, wiring, and starting up an NCE25 | NCE25 Installation Instructions (Part No. 24-10143-63) |
| Installation considerations and guidelines, mounting, wiring, and starting up an NAE35 or NAE45 | NAE35/NAE45 Installation Instructions (Part No. 24-10050-6) |
| Installation Considerations and Guidelines, Mounting, Wiring, and Starting up an NAE55 or NIE55 | NAE55/NIE55 Installation Instructions (Part No. 24-10051-43) |
| Installation considerations and guidelines, mounting, wiring, and starting up an NAE-S | NAE55-S Installation Instructions (Part No. 24-10051-108) |
| Additional guidelines for commissioning and configuring and NCE25 Network Engines | NCE Technical Bulletin (LIT-12011267) |
| Additional guidelines for commissioning and configuring and SNE Network Engines | SNE Commissioning Guide (LIT-12013352) Additional guidelines for commissioning and configuring and SNE Network Engines |
| Additional guidelines for commissioning and configuring and SNC Network Engines | SNC Commissioning Guide (LIT-12013295) |
| Additional guidelines for commissioning NAE85 network engines | NAE85 Commissioning Guide (LIT-12011044) |

Table 1: NAE Related documentation

| For information on | See document |
|---|---|
| Additional guidelines for commissioning NxE89 | NIE89 Commissioning Guide |
| network engines | (LIT-12011920) |
| Commissioning an NAE for the Modbus protocol | Additional guidelines for commissioning |
| | and Network Engine Commissioning for |
| | Modbus Vendor Integration Application |
| Commissioning on NAE for the M Rus protocol | Note (LIT-12013130) |
| | M-Rus Integration Application Note |
| | (LIT-12013149) |
| Commissioning an NAE for the KNX protocol | Network Engine Commissioning for KNX |
| | Vendor Integration Application Note |
| | (LIT-12013148) |
| Commissioning an NAE for the C•CURE 9000 and victor | NAE Commissioning for C•CURE- |
| video management system integration | victor Integration Application Note |
| Commissioning on NAE fourth a Zottlay MV Croally C. | (L11-12013151) |
| Lommissioning an NAE for the Zettler MX Speak 6.0 | Network Engine Commissioning for Zettler MX Speak 6.0 Vendor Integration |
| | Application Note (LIT-12013269) |
| Commissioning an NAE for the OPC UA integration | Network Engine Commissioning for OPC UA |
| | Client Vendor Integration Application Note |
| | (LIT-12013545) |
| | |
| Commissioning NIEx9 network engines | NIEx9 Commissioning Guide |
| | (LIT-12011922) |
| Updating the NAE/NIE disk image to new software | NAE Update Tool Help (LIT-12011524) |
| release versions | |
| Installing the ADS and ADX software | Metasys Server Installation and Upgrade |
| | Instructions Wizard (LII-12012162) |
| Installing the ADS-Lite software | Metasys Server Lite Installation |
| | (I IT-12012258) |
| Installing the OAS software | Open Application Server Installation and |
| | Upgrade Instructions (LIT-12013222) |
| Installing the SCT software | SCT Installation and Upgrade Instructions |
| | Wizard (LIT-12012067) |
| Creating, editing, and loading archive databases with | SCT: System Configuration Tool Help |
| the SCT | (LIT-12011964) |
| Managing Trusted Certificates Created for Network | SCT: System Configuration Tool Help |
| Engines | (L11-12011964) |
| Integrating N2 Devices into the Metasys System | N2 Integration with the NAE Technical |
| Network | Duilellii (L11-1201083) |
| | Controller Tool Hole (LT 12011117) |
| Using the CCI | Controller 1001 Help (L11-12011147) |

Table 1: NAE Related documentation

| For information on | See document |
|---|---|
| NAE/NCE BACnet® protocol conformance | NAE/NCE Protocol Implementation Conformance Statement (LIT-1201532) |
| SNE/SNC BACnet® protocol conformance | SNE/SNC Protocol Implementation Conformance Statement (LIT-12013355) |
| How to set up a local or remote MS/TP communications bus | MS/TP Communications Bus Technical Bulletin (LIT-12011034) |
| Enabling NAEs to communicate with MS/TP controllers over wireless mesh networks | ZFR1800 Series Wireless Field Bus System Technical Bulletin (LIT-12011295) |
| Integrating LonWorks devices into the Metasys system network | LonWorks® Network Integration with Network Engines and LCS Technical Bulletin (LIT-1201668) |
| Migrating N1 networks to the Metasys system network | N1 Migration with the NIE Technical Bulletin (LIT-1201535) |
| Integrating local and remote BACnet/SC devices into the Metasys system network | BACnet/SC Workflow Technical Bulletin (LIT-12013959) |
| Integrating local and remote BACnet MS/TP and BACnet IP devices into the Metasys system network | BACnet Controller Integration Technical Bulletin (LIT-1201531) |
| Security issues, including adding users and roles to the system and configuring standard and basic access modes | Security Administrator System Technical Bulletin (LIT-1201528) |
| Installing the Launcher application | Launcher Installation Instructions (LIT-12011783) |
| Using the Launcher, accessing a Metasys system network through dial-up connections | Launcher Tool Help (LIT-12011742) |
| Dialing into a Metasys system network from a computer | Metasys System Direct Connection and Dial-Up Connection Application Note (LIT-1201639) |

NAE commissioning overview

Network Automation Engines (NAEs)

NAEs are web-enabled, Ethernet-based, supervisory controllers that connect BAS networks to IP networks and the web, and allow you to monitor and control BAS field devices from a computer using the Launcher application. You use the Launcher application to log in to the NAE. If the Launcher is not already installed on your machine, you are prompted to install it when you attempt to log in using a web browser. To install the Launcher, use either a supported version of Windows® Internet Explorer®, Google® Chrome[™], or Apple® Safari®. (Other web browsers may work, but are not tested or supported.) Refer to the *Launcher Installation Instructions (LIT-12011783)*.

The NAE Series of network engines is a scalable line of supervisory controllers with varying network, trunk, and field device capacities to meet the requirements of different applications.

All NAEs provide scheduling, alarm and event management, trending, energy management, data exchange, and password protection. NAEs are factory-loaded with a supported Linux operating system and the current release of the Metasys system software. The NAEs support many different vendor integrations from which you can select during commissioning, such as Modbus, M-Bus,

KNX, Tyco® C•CURE®/victor®, Zettler, OPC Unified Architecture (UA), and MQTT. Each NAE can run two integrations. To commission each protocol, refer to the appropriate document:

- Modbus Network Engine Commissioning for Modbus Vendor Integration Application Note (LIT-12013150)
- M-Bus Network Engine Commissioning for M-Bus Vendor Integration Application Note (LIT-12013149)
- KNX Network Engine Commissioning for KNX Vendor Integration Application Note (LIT-12013148)
- C•CURE/victor Network Engine Commissioning for C•CURE/victor Integration Application Note (LIT-12013151)
- Zettler Network Engine Commissioning for Zettler MX Speak 6.0 Vendor Integration Application Note (LIT-12013269)
- OPC UA Network Engine Commissioning for OPC UA Client Vendor Integration Application Note (LIT-12013545)

NCE25 models - Release 9.0.x

The NCE25 models:

- support either one field bus or one LonWorks® network trunk into a Metasys system network, specifically:
 - NCE256x-x: one BACnet® MS/TP trunk with up to 32 MS/TP controllers
 - NCE251x-x: one N2 Bus with up to 32 N2 controllers
 - NCE252x-x: one LonWorks trunk with up to 32 LonWorks devices (Release 9.0 only)
- support up to two vendor integrations, including Modbus, M-Bus, and KNX
- monitor and control up to 100 BACnet IP field devices over Ethernet at the supervisory level
- provide an integral MS/TP Field Equipment Controller with 33 Input/Output (I/O) points
- cannot serve as a Site Director for other engines except for itself
- support Domain Name Server (DNS) for resolving NAE names on the building network, but does not support NETBIOS name resolution

NAE35 models - Release 9.0.x

The NAE35 models:

- support one RS485 field bus or one LonWorks network trunk into a Metasys system network. The NAE351x models integrate one N2 Bus or one BACnet® MS/TP trunk with up to 50 field controllers. The NAE352x models (Release 9.0 only) integrate a single LonWorks trunk with up to 64 LonWorks devices.
- support up to two vendor integrations, including Modbus, M-Bus, and KNX
- monitor and control up to 100 BACnet IP devices over Ethernet at the supervisory level
- serve as a Site Director supervising a maximum of two additional network engines, which can be NCE25 or NAE35 model engines only
- support Domain Name Server (DNS) for resolving NAE names on the building network, but does not support NETBIOS name resolution

Several NAE35 models provide the Basic Access operating mode as the primary UI. See Basic Access operating mode (small-capacity engines only) for more information.

NAE45 models - Release 9.0.x

The NAE45 models:

- support either one RS485 field bus or one LonWorks network trunk into a Metasys system network. The NAE451x models integrate one N2 Bus or one BACnet MS/TP trunk with up to 100 field controllers. The NAE452x models (Release 9.0 only) integrate a single LonWorks trunk with up to 127 LonWorks devices.
- support up to two vendor integrations, including Modbus, M-Bus, and KNX.
- monitor and control up to 100 BACnet IP field devices over Ethernet at the supervisory level.
- serve as a Site Director supervising a maximum of two additional network engines, which can be NCE25, NAE35, or NAE45 model engines only.
- support Domain Name Server (DNS) for resolving NAE names on the building network, but does not support NETBIOS name resolution.

Notes:

- The NAE45-Lite supports the MS/TP bus and BACnet IP communication to third-party devices. The NAE45-Lite does not support the N2 Bus, N1 integration, VND integration, XL5K integration, LonWorks network, or wireless supervisor (N2).
- The NAE45-Lite must have an ADS-Lite-A as its Site Director, or be stand-alone. The NAE45-Lite cannot be a Site Director to other engines.

NAE55 models - Release 12.0

The NAE55 models:

- support up to two RS485 field buses into a Metasys system network. The NAE551x models integrate two N2 Buses, two BACnet MS/TP trunks, or one N2 Bus and one BACnet MS/TP trunk. Each bus or trunk may contain up to 100 field controllers. The NAE552x models can also integrate a LonWorks network trunk with up to 255 LonWorks devices. NAE55 models can also monitor and supervise a number of BACnet IP devices; the total number of BACnet IP devices depends on the number of objects each device supports.
- support up to two RS485 field buses into a Metasys system. The NIE596x model integrates two N2 Buses, two BACnet MS/TP trunks, or one N2 Bus and one BACnet MS/TP trunk. Each bus or trunk may contain up to 100 field controllers. The NIE592x model integrates a LonWorks network trunk with up to 255 LonWorks devices.
- support up to two vendor integrations, including Modbus, M-Bus, KNX, C•CURE/victor, Zettler, and OPC UA
- supervise BACnet/IP and BACnet Secure Connect (BACnet/SC) devices from Johnson Controls, such as the FAC4911 Advanced Application Field Equipment Controller, the CGE General Purpose Application Equipment Controllers, the CVE VAV Box Controllers, and the VMA1930 Variable Air Volume Modular Assembly
- serve as a Site Director supervising a maximum of two other network engines, which can be NAE55, SNE, or SNC model engines

NAE85 model - Release 12.0

Important: At Release 12.0, the NAE85 functions as a Site Director but not as a child device. To keep a NAE85 as a child device, do not upgrade it to Release 12.0.

➤ Important: A new install of an NAE85 or an upgrade of an NAE85 requires Microsoft[™] SQL Server. If you install or upgrade an NAE85 on the Microsoft Server Operating System (OS), you need the standard or enterprise edition of SQL Server and an SQL license. If you install or upgrade an NAE85 on your Windows 10 OS, SQL Server Express is loaded for you as part of the install if no other SQL Server instance is installed.

The NAE85 model:

- acts as a site director and not as a child device at Release 12.0
- hosts the Metasys UI at Release 12.0
- migrates large BACnet IP networks into a Metasys system network
- supervises BACnet/IP and BACnet/SC devices from Johnson Controls, such as the FAC4911 Advanced Application Field Equipment Controller, the CGE General Purpose Application Equipment Controllers, the CVE VAV Box Controllers, and the VMA1930 Variable Air Volume Modular Assembly
- support up to two vendor integrations, including Modbus, M-Bus, KNX, C•CURE/victor, Zettler, and OPC UA
- serves as a Site Director supervising a maximum of four other supervisory devices, which can be NCE25, NAE35, NAE45, NAE55, SNE, or SNC model engines

Refer to the *NAE85 Commissioning Guide (LIT-12011044)* for additional information specific to the NAE85 Series network engines.

Warning banner

As an option, an NAE configured as a Site Director can have a Warning Banner enabled. The Warning Banner is a statement that always appears when operators log on the Site Management Portal of the engine. By default, the network engine is configured not to display a warning banner.

For small-capacity engines, you can select to use the U.S. Department of Defense (DoD) banner. For the large-capacity engines, you have the choice of three different warning banners: U.S. Department of Defense (DoD), U.S. (General Services Administration (GSA)), or U.S. Department of Transportation (DOT) Federal Aviation Administration (FAA). The information in the text window is customized for the United Stated government agency where the Metasys system is installed. The reader must read and accept the conditions in the Warning Banner before logging on. The banner cannot be customized or its text be changed. For steps on how to enable or disable this banner, see Enabling and disabling Warning Banner.

Figure 1: United States DoD Warning Banner



MS/TP communications bus

The MS/TP communications bus is a local or remote network that connects supervisory controllers and equipment controllers to point interfaces using BACnet MS/TP protocol. The remote network, called the Remote Field Bus, requires the addition of a BACnet/IP to BACnet MS/TP Router. The MS/TP bus consists of two types of buses: the FC Bus and the SA Bus. Each bus has its own set of device addresses. For details on how to apply the local and remote MS/TP bus, refer to the *MS/TP Communications Bus Technical Bulletin (LIT-12011034*).

Metasys network sites

A small Metasys network site comprises a single NAE or multiple NAEs and SNEs with one of the NAEs designated as the Site Director (Figure 2). See Site Director for additional information on Site Director hierarchy and the number of network engines a Site Director can supervise.



Figure 2: Metasys Network with NAE55 as Site Director for multiple network engines

Larger Metasys network sites can comprise multiple NAEs and one or more ADSs or ADXs with access to multiple remote sites. On any site with one or more ADSs/ADXs, an ADS/ADX is designated as the Site Director. Figure 3 shows an example of a simple Metasys network with one SNE, one NAE55, and an ADS as the Site Director.



Figure 3: Metasys Network with ADS as Site Director for one SNE and one NAE

NAE commissioning

(i) **Note:** The NAE85 hosts the Metasys UI at Release 12.0. For steps on commissioning the NAE85 with the Metasys UI, refer to the *NAE85 Commissioning Guide (LIT-12011044)*.

NAE commissioning includes preparing the network engine for connectivity, connecting to the network engine, adding the network engine to the profile list in Launcher, and accessing and logging in to the engine's Site Management Portal UI.

Each Metasys network installation, commissioning, and configuration scenario is unique. In some scenarios, the network engines (on a Metasys network) may be commissioned and configured before they are installed and connected to the network; in other scenarios, the network engines are mounted and wired to the network before they are commissioned and configured.

(i) **Note:** Network engine installation includes locating, mounting, wiring, and powering on an NAE. See Related documentation for references to NAE installation instructions for the various models.

The commissioning tasks, the task order, and the required attribute values (at commissioning) for a network engine are determined by the specific Metasys network installation, commissioning, and configuration scenario for the site. The commissioning procedures presented in this document are the procedures required for most scenarios regardless of when commissioning occurs.

The first task in commissioning an NAE is to establish a connection with the network engine through the Launcher. If the Launcher is not already installed on your machine, you are prompted to install it when you attempt to log in using the web browser. The Launcher is a software

application installed on each client computer that lets you access any Metasys server or supervisory engine on the building network, regardless of its software version. For details, refer to the *Launcher Tool Help (LIT-12011742)* and the *Launcher Installation Instructions (LIT-12011783)*.

After a connection is established, you can then access the Site Management Portal on the NAE from the Launcher. See NAE connectivity for six typical network connection scenarios. See Site Management Portal user interface and Accessing Site Management Portal UI on an NAE for more information on accessing and navigating the Site Management Portal UI.

After you have accessed the Site Management Portal UI on an NAE, you can configure the engine:

- object name and basic device parameters
- host name (computer name), domain name, and network parameters
- trusted certificates (optional)
- time and date management parameters
- alarm and event parameters
- SNMP messages and the network management destination
- network integrations
- third-party protocol integrations
- Site Director status
- Advanced Security setting

After commissioning an NAE, you must configure the engine at the job site. The next section, NAE configuration, provides an overview of the sequence of steps needed to install, commission, and configure a new NAE.

NAE configuration

(i) **Note:** The NAE85 hosts the Metasys UI at Release 12.0. For steps on configuring the NAE85 with the Metasys UI, refer to the *NAE85 Commissioning Guide (LIT-12011044)*.

NAE configuration is preparing the engine with the Site Management Portal UI and the SCT to operate on a specific Metasys network site, and communicate with, monitor, and control specific BAS field devices on that site. Configuration also includes preparing the NAE to compile, generate, and communicate information about site status, alarms, events, and trends.

You can typically accomplish NAE configuration by downloading a pre-built archive database (from the SCT) that contains the device objects, object references, attribute values, logic, graphics, user information, and other references and data required for the NAE to perform its specific tasks on the network.

Alternatively, you can create and edit an archive database online in the Site Management Portal UI, but it may be more convenient to create and edit the NAE archive database offline in the SCT. When you download the database, the values in the archive database overwrite the existing values on the commissioned NAE. Refer to the *SCT: System Configuration Tool Help (LIT-12011964)* for information on creating and downloading archive databases.

After you configure an NAE with an archive database, you can set up the email, Syslog, and SNMP DDAs and create specific alarm and event notifications for delivery to specific email, Syslog server, and network management destinations.

Here is an overview the steps to commission and configure the NAE:

- 1. Add and configure a site. Refer to *Metasys SCT Help (LIT-12011964)*.
- 2. Add and configure the engines in the site with the SCT, including any third-party integration.

- 3. Complete building the offline archive database in the SCT. [For all of these steps, refer to *Metasys SCT Help (LIT-12011964)*].
 - a. Set Advanced Security Enabled attribute.
 - b. Add integration trunks, field devices, and field points.
 - c. Add programming logic using the Logic Connector Tool.
 - d. Configure alarm and trend extensions and audit logs.
 - e. Configure alarm destinations: email, Syslog, and SNMP DDAs.
 - f. Build graphics with User Graphics Tool.
 - g. Configure User Views and Tailored Summaries.
- 4. Install, wire, and power the engine. Refer to the appropriate installation guide for the engine model you are installing. (See Related documentation.)
- 5. Prepare the engine for connectivity to the Metasys system network. See Detailed Procedures for instructions on how to connect an engine in various network scenarios and to set up some basic engine parameters.
- 6. If the engine is not the designated Site Director, demote it from Site Director status. See Designating an NAE as a child of a Site Director.
- Change the engine's computer name value and assign an IP address, if necessary. See Computer name. The engine is now ready to receive an archive database download from the SCT.
- 8. Use the Manage Archive Wizard in SCT to download the database to the engine. For the NCE, also download the local application. Refer to the *Metasys SCT Help (LIT-12011964)*.
- 9. If there are only engines on the site, designate one of the engines as the Site Director. If the site has an ADS or ADX server, that server is automatically designated as the Site Director. Refer to the *ADS/ADX Commissioning Guide (LIT-1201645)*.
- 10. Using SCT, create a backup of the archive database, which includes the security database. Refer to the *Metasys SCT Help (LIT-12011964)*.
- 11. Log on the NAE to verify operation.

Metasys UI on NAE85

Figure 4: Metasys UI on NAE85

| Sp | aces Network Views | b ay3 | 4 | | Q 🗠 🕏 | : |
|-----|--|--|--|------------|---|----|
| | | <u>bay3 site</u> | | | Page | 1- |
| + | | DETAIL | | 2 | EQUIPMENT RELATION SHIPS | 2 |
| | bay3 site → Summary Definitions | Value: <u>Operational</u> | | High Alarm | | |
| e e | User Views Onae00d0c9ca0dd7 | Focus Diag | nostic Network | | | |
| | - Content - Cont | Object Name | bay3 | | No equipment relationships have been configured | |
| | — 🌧 SC Network Port — 🖿 Energy | Description Object Type | Click To Add Device | | | |
| | Programming Schedule | Authorization Category | System | | | |
| | Graphic1 | Model Name | MS-NAE8500 | | | 7 |
| | Automation Cursory Gl Automation GGT Curso LIGT Graphics | Local Time | 05:10 AM (HH:MM AM/PM) Monday, May 30, 2022 | | | |
| | - Z Graphic3 | Engineering Values | Monday, May 30, 2022 | | Updated:10s ago | |
| | 🖿 🖿 Sample | ID | 1734fad4-6f1f-588c-a8ab- e02ee0eb4090 | | | * |
| | | Firmware Version | 13.0.0.354 | | Operational | |
| | | Item Reference | bay3:bay3 | | | |
| | | Version Archive Date | 40.0 Monday, May 30, 2022 | | 05/29/2022 12:00 AM 05/30/2022 11:10 AM | 1 |
| | METASYS Ø Johnson Controls, Pic. 2013-2022 | Max Message | 994 bytes | • | 1 29. May 30. May | |

In addition to the Site Management Portal UI, the NAE85 software installer also installs the Metasys UI software. Metasys UI is a mobile-optimized software component that consolidates existing Metasys user interface products into a single, simplified, and easy-to-learn interface. Metasys UI provides a simple location-based navigation approach to finding information about the Metasys site, including the ability to search for any location or equipment by name and to bookmark a location or equipment in a web browser. All data displayed in the Metasys UI is organized in a dashboard format that gives you the overview of what is happening within a space, equipment, or central plant. You can also and create and manage graphics and their associations to equipment and spaces. Access the Metasys UI from any type of client device with any screen size. For more details, refer to the *Metasys UI Technical Bulletin (LIT-12012115)* and *Metasys UI Help (LIT-12011953)*.

Site Management Portal user interface

You can view and edit NAE parameters and the parameters for associated devices in the engine's Site Management Portal UI. Access the Site Management Portal UI of the NAE by using the Launcher. See Accessing Site Management Portal UI on an NAE. Figure 5 shows an example of the Site Management Portal UI.

In the Display panel on the right side of the window is a series of tabbed screens. Table 3 and Table 2 describe the information that you can view and edit in each tabbed screen. The navigation panel on the left displays the navigation tree for the BAS network integrations, field devices, field points, and their associated objects that the NAE is monitoring and supervising.

Figure 5: NAE Focus Tab in Edit Mode - Advanced

| | | _ | |
|--|--------------------------|--|---------------|
| <u>E</u> dit <u>V</u> iew <u>A</u> ction I <u>n</u> sert <u>T</u> ools <u>Q</u> ue | ery <u>H</u> eip | Last Login: Fri 05/27/2022 08:41:18 CDT Met*** | .ogout Exit |
| | | M4-SNE22 | ê O 🛛 🖉 |
| Items | | Operational Normal | |
| Site | Focus Summary Diagnostic | Network Email SNMP Syslog Alarm | Trend |
| 🛄 User Views | Save Cancel | Basi | ic 💿 Advanced |
| Summary Definitions | | (3) | |
| M4-SNE22 | Attribute | Value | Units |
| BACnet Protocol Eng | Object | | |
| Eth IP DataLink | Name | M4-SNE22 | 8 |
| B Undate | Object Type | Device | |
| | Object type | Device | 7 |
| | Authorization Category | System | <u> </u> |
| E- | Model Name | M4-SNE22001-0 | |
| 🗄 📲 🚼 BACnet IP1 | Time | | |
| ⊞ | Local Time | 09:26 AM | (HH:MM |
| | Local Date | Friday, May 27, 2022 | |
| | Engineering Values | | |
| | Firmware Version | 12.0.0.3436 | |
| | Staged Firmware Version | | |
| | Staged Files | | |
| | Item Reference | SNE00108D0C5D50:SNE00108D0C5D5 | 0 |
| | Version OS Version | 10 17 41 24 | |
| | Archive Date | Friday May 27, 2022 | |
| (6) | Max Message Buffer | QQ4 | hvtes |
| | Max APDI LL ength | 1024 | bytes |
| (0) | | 1024 | 0,000 |

Table 2: NAE Focus Tab Descriptions

| Callout | Description |
|---------|--|
| 1 | Previous and next arrows for navigating to viewed screens |
| 2 | NAE object: Double-click or drag into display panel to view and edit NAE parameters. |
| 3 | Display panel (in Edit view) |
| 4 | Editable values: type in or select the appropriate value. |
| 5 | Viewable but non-editable values in the displayed screen. |
| 6 | Navigation panel |
| 7 | Alarm and event indicator |

When you view the NAE online with the Site Management Portal UI, the border around the panels is blue (Figure 5). When you view the NAE offline with the SCT UI, the border is black (Figure 6).

| Screen Tab Designation | Purpose | Online or Offline Access |
|------------------------|--|-----------------------------|
| Focus | Provides the description and name (label) of the device object, the local time and date, the firmware version, message buffer and alarm, and audit repository sizes. The Focus tab also identifies the local Site Director and includes general site information about the ADS/ADX to which the NAE reports (if applicable). | Both |
| Communications | Establishes communication parameters, including Serial port and internal or external USB modem configuration. Newer network engines do not have this tab. | Both |
| Network | Establishes Computer Name (host name) for network identity, ADS/ADX dial-up parameters (if applicable), LAN, and BACnet Routing. The host name cannot consist of only numbers. | Both |
| Email | Establishes the NAE email alarm-notifications features common to all email messages and create unique email message destinations. | Both |
| SNMP | Establishes the NAE Simple Network Management Protocol (SNMP) features common to all SNMP notifications and create unique SNMP message destinations. | Both |
| Syslog | Provides the NAE Syslog server reporting destination information. | Both |
| Alarm | Provides the NAE alarm setup and destination information. | Both |
| Summary | Provides network and field device status information and attribute values for supervisory and field devices on the NAE field trunks. | Online |
| Diagnostic | Provides various status reports to aid in troubleshooting the NAE. | Online |
| Trend | Monitors and records the changes in the behavior of an NAE over time, assisting with diagnosing various system-wide behavioral characteristics. | Both |

Table 3: Metasys Site Management Portal UI Tabbed Screens

Menus, tab screens, attribute lists, values, and units of measure in the Site Management Portal UI are dynamic and change in the displayed screen according to the item you select from the navigation tree. Refer to the *Object and Feature Tabs* section in the *Metasys Site Management Portal Help (LIT-1201793)* for descriptions of menu items.

With the addition of the BACnet/SC integration at Release 12.0, two new objects called SC Network Port and Update now appear under the navigation trees of the Site Management Portal UI and the Metasys UI. For descriptions of the SC Network Port object, refer to <u>SC Network Port</u>. For descriptions of the Update object attributes, refer to <u>Engine Attributes</u> in the *Metasys Site* *Management Portal Help (LIT-1201793)*. For further details on BACnet/SC, refer to the *BACnet/SC Workflow Technical Bulletin (LIT-12013959)*.

Metasys Help Files

The Metasys Help files provide shared system information and individualized mode-dependent information for the Metasys Site Management Portal (SMP) or the System Configuration Tool (SCT). The *Metasys Site Management Portal Help (LIT-1201793)* provides information about alarming, commanding, auditing live data values, and other online features. The *SCT: System Configuration Tool Help (LIT-12011964)* provides information about offline operations such as managing archives, creating spaces, simulating systems, and establishing equipment and serving relationships.

In either SMP or SCT mode, the Metasys Help menu provides Help files in PDF format. Because last minute changes might occur just before product release, always refer to the Johnson Controls Knowledge Exchange for the most up-to-date version of the Metasys Help files.

Browser recommendations for downloading Launcher

To access a network engine for downloading the Launcher application, you can use Google® Chrome[™] version 91 or later, Apple® Safari® 13.1 or later, and Microsoft® Edge® version 91 or later. Other web browsers may work, but are not tested or supported. After you install the Launcher, you use the Launcher, not the web browser, to open the Site Management Portal UI.

System Configuration Tool (SCT)

SCT is an offline software tool you use to create, edit, save, and restore the various archive and security databases that configure Metasys system networks, OASs, ADSs/ADXs, NAEs, NIEs, SNEs, SNCs, and supported field devices. The SCT UI opens in its own window and has a similar appearance to the online Site Management Portal UI (Figure 6). SCT also manages trusted certificates for network engines. For details, see Appendix: Certificate Management.

SCT, if running on a 32-bit Windows operating system, allows commissioning of N2 devices by allowing HVAC PRO software, GX-Tool software, and XTM Configurator software to access the devices on the N2 Bus of an NAE. SCT also allows commissioning of equipment controllers by using the CCT software to access the devices on the field bus of an NAE.

SCT provides a Simulation feature that allows you to simulate an online supervisory device and test a database's control logic prior to downloading it to an NAE. Using the SCT, you can view and configure multiple sites in one archive.

Figure 6: SCT UI screen example

| Metasys System Configuration Tool | | | |
|---|---|---|--------------------------------|
| Item Edit View Action Insert Tools Facility Q | uery SCT Pro <u>H</u> elp | | Met*** Logout Exit |
| ۵. | | NAE55-W | <u>^</u> – 🛛 🖉 |
| All Items | Configuration Diagnostic Network F | mail SNMP Syslog Alarm | Trend |
| All Items → MyArchive8 → Ste → ME55-W (110) → ME55-W (110) → ME55-W (110) → ME55-W (110) → ME55-W (110) → MA55-W (110) → MA55-W (110) → Mother Protocol Eng → Definitions → Definitions | Configuration Diagnostic Network E Edit Attribute Object Image: Constraint of the second of the sec | Snmail SnmP Syslog Alarm Value Value Value Value NAE55-W Device System Value MS-NAE5510-2 (UTC-06:00) Central Time (US & Contral Time (US & Contra Time (US & Contra Ti | Trend Basic Advanced Canada) |
| | Enable Application Generated Audits | 80 % False | |
| | Audit Action When Full | Rollover | |
| | Audit Generate Alarm When Full | True | |
| | Enabled Audit Level | 2 | |
| × | | Serve | er: 11/20/2018, 09:37 AM CST |

Controller Configuration Tool (CCT)

CCT is a software tool that you use to configure, simulate, and commission equipment controllers that belong to the Metasys system family, such as CGMs, CVMs, FACs, FECs, IOMs, and VMAs. Among the many helpful CCT options is Supervisor Passthru, which provides you the means to download an equipment controller over the Metasys network, provided SCT 15.0 and CCT 15.0 are installed on the same computer. For more information on CCT, refer to the *Controller Tool Help (LIT-12011147)*.

Archive databases

A Metasys archive database contains the configuration information for Metasys Servers, network engines, BAS network integrations, third-party integrations, field devices, and field points that make up a single site or multiple sites on a Metasys system network. Multiple archive databases, representing multiple sites, can reside on a single ADS/ADX running the SCT. The SCT navigation panel in Figure 6 provides a graphical representation of some of the items that may be in a Metasys archive database.

An NAE archive database, which is stored in the network engine's internal memory, contains only the specific configuration information that makes up the network integrations, field devices, and field points that the NAE is supervising. Each NAE retains only its own archive database. You can also save the NAE database in a Metasys archive database on an ADS/ADX or another computer using the SCT. A graphical representation of some of the items contained in an NAE archive database is shown in Figure 5 in the Site Management Portal UI navigation panel.

You can upload an NAE archive database to the SCT where it can be saved to a hard disk or other long-term storage media. You can also edit an NAE archive database offline in the SCT and download the edited archive database to the network engine.

NAE disk image updates and archive database upgrades

The NAE operating system, Metasys system software, NAE archive database, and recent NAE operation data reside on the NAE disk image.

To update the NAE Metasys system software, use SCT Pro or the NAE Update Tool. Refer to *SCT Pro Help (LIT-12013035)* and *NAE Update Tool Help (LIT-12011524)*. For some *Metasys* releases, the NAE Update Tool is **required** to update the disk image.

When you update an NAE to a new version of the disk image for the latest release version of the Metasys system software, you must also upgrade the NAE archive database to a new release database. For an overview of the upgrade process, refer to the *SCT Installation and Upgrade Instructions (LIT-12012067)*.

Site Director

For each Metasys system network site, a single network engine or a Metasys server (ADS, ADX, or OAS) is designated as the Site Director. The Site Director provides a single point of access to the site and all of the web-enabled devices on the site. The Site Director supports functions such as user login, user administration, user views, time synchronization, and data traffic management.

On larger building control networks with one or more Metasys servers, a Metasys server is designated as the Site Director. On small network sites without a Metasys server, you must designate one of the NAEs as the Site Director.

By default, an NAE is designated as a Site Director when its firmware in loaded in the factory. You must demote any NAE that is not the designated Site Director on a site. See Designating an NAE as a child of a Site Director for more information.

If a Metasys server is on a site, an NAE cannot be the Site Director. You must demote the NAE to be a child of a Metasys server. See Designating an NAE as a child of a Site Director for more information.

(i) **Note:** The NAE45-Lite model cannot be a Site Director to other engines. The NAE45-Lite can only be a child device of an ADS-Lite-A. You must demote the NAE45-Lite to be a child of an ADS-Lite. See Designating an NAE as a child of a Site Director for more information.

The following table lists the supervisory rights of each network engine model when it serves as a Site Director.

| Site Director | Supervisory Rights |
|---------------|--|
| NAE85 | May supervise up to four additional engines on the site: NCE25s, NAE35s, NAE45s, NAE55s, SNEs, or SNCs |
| NAE55 | May supervise up to three additional engines on the site: NCE25s, NAE35s, NAE45s, NAE55s, SNEs, or SNCs. |
| NAE45 | May supervise up to two additional engines on the site: NCE25s, NAE35s, or NAE45s. |
| NAE45-Lite | Cannot supervise any additional engines on the site. |

Table 4: Supervisory Rights

Table 4: Supervisory Rights

| Site Director | Supervisory Rights |
|---------------|---|
| NAE35 | May supervise up to two additional NCE25s or NAE35s. on the site. |
| NCE25 | Cannot supervise any additional engines on the site. |

(i) **Note:** If you attempt to add an NAE to a site and the new NAE exceeds the supervisory device limit for the Site Director, the Site Director does not accept the additional device. The Site Director records an error message in the Site Director Audit Viewer each time you attempt to add a **new** device that exceeds the device limit.

Computer name

The **Computer Name** is an editable Network Identification attribute on the network engine's Network tab. Devices on the building network and the Metasys system network use the Computer Name to identify and communicate with the NAE across the network. This Computer Name is synonymous with host name on a network.

Each NAE is factory-configured with a unique initial Computer Name value NAExxxxxxxxxx, where xxxxxxxxxx is the Ethernet MAC address of the device without the hyphens. For example, if the MAC address of the NAE is 00-D0-C9-ED-E7-10, the initial computer name is NAE00D0C9EDE710. Changing the Computer Name value initiates a device reset on the NAE.

The initial computer name is often useful during commissioning for locating and connecting to an NAE before it is configured with an archive database download from the SCT. In most cases, the archive database download from the SCT overwrites the initial Computer Name value and determines the NAE Computer Name on the Metasys site.

The Computer Name of an NAE must adhere to these rules:

- Must not consist of all numbers. For example, a computer name of N1234 is acceptable but 1234 is not.
- Must end with either a letter or a number and must not consist of any special symbols (for example, @, #, or \$)
- Must not use hyphens in the first or last character of the name, but hyphens are allowed elsewhere
- Must consist of no more than 15 characters
- Important: If you change the Computer Name of an NAE with SCT, all existing references between the NAE object and other objects on the site are updated with the new name. In addition, any existing network connections to other devices are updated as well.
- ③ Note: Before building the archive database in SCT, you should consult the network administrator or Information Technology (IT) department to determine if there is an existing protocol for host names (computer names) on the network.

Object name

The **Name** is an editable Object attribute on the NAE Focus tab that the Metasys software uses to identify the NAE in the Site Management Portal UI and in the SCT. The Object Name is a label only and may not be the same as the Computer Name. Changing the Object Name merely changes the name that you see in the navigation tree, alarm messages, trend reports, and other screens in the Site Management Portal UI and SCT that refer to the NAE. Changing the Object Name **does not** impact the object references or network communication with other devices on the site. You can change the Object Name at any time. We recommend an intuitive name that clearly identifies the NAE in the Site Management Portal UI and Metasys site.

Basic Access operating mode (small-capacity engines only)

Basic Access for small-capacity engines is a mode of operation allowing users with Basic Access user accounts access to a subset of the standard user interface capabilities based on their assigned permissions. Basic Access user accounts are created by *Metasys* system administrators using the Security Administrator system. Basic Access meets the user interface requirements for most building operators. Basic Access is provided on all of the Metasys system engines and servers but is the primary user interface in the NAE35 controllers.

You cannot commission or configure an NAE35 in Basic Access mode. You must log in to the full Site Management Portal UI on the NAE35 to commission and configure the device. See Login user names and passwords for information on logging in to NAE35 Basic Access.

(i) **Note:** Network engines upgraded to Release 11.0 or later no longer offer Basic Access user accounts.

Login user names and passwords

All NAEs are configured at the factory with the same initial login user name and default password. The initial login user name is **MetasysSysAgent**, and it is not case sensitive. For the MetasysSysAgent default password, contact your local Johnson Controls® representative.

The initial user name and password is required to log in to any NAE that has never been logged in to before, including a network engine from the factory or one that has been newly updated with SCT or the NAE Update Tool Help. The Change Password dialog box appears immediately to prompt you for a new password. You must change the MetasysSysAgent default password at this point. SCT may also request you to change the password during some database operations if the network engine still has the original default password. The process for updating the password may take up to 30 seconds to complete.

The following table lists the password rules enforced by the Metasys system user's language_locale setting. Three primary user language groups are available: English, non-English (Europe), and non-English (Asia).

| Language of User | Supported | Enforced Password Rules |
|-------------------------|---|---|
| | Language_Locale | |
| English | English (en_us) | The password must include a minimum of 8 characters and a maximum of 50 characters. |
| | | The password cannot include spaces or include a word or phrase that is in the Blocked Words list. |
| | | The password and the username cannot share the same three consecutive characters. |
| | | The password must meet the four following conditions: |
| | | - Include at least one number (0–9) |
| | | Include at least one special character (-, ., @, #, !, ?, \$, %) |
| | | Note: Only the special characters listed above can be used; all other special characters are invalid. |
| | | - Include at least one uppercase character |
| | | - Include at least one lowercase character |
| Non-English (Europe) | Czech (cs_cz) German (de_de) | The password must include a minimum of 8 characters and a maximum of 50 characters. |
| | Spanish (es_es) French (fr_fr) Hungarian (hu_hu) Italian (it_it) Norwegian (nb_no) Dutch (nl_nl) Polish (pl_pl) Portuguese (Brazilian) (pt_br) Russian (ru_ru) | The password cannot include spaces or include a word or phrase that is in the Blocked Words list. |
| | | The password and the username cannot share the same three consecutive characters. |
| | | The password must meet three of the following conditions: |
| | | - Include at least one number (0–9) |
| | | Include at least one special character (-, ., @, #, !, ?, \$, %) |
| | Swedish (sv_se) | - Include at least one uppercase character |
| | TURKISN (tr_tr) | - Include at least one lowercase character |
| | | Include at least one Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase |

Table 5: Metasys System Password Rules

| Language of Licer | Supported | Enforced Descuerd Bules | | | | | | | | | | | | | | | | | | | | | | |
|------------------------------------|---|---|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
| Language of User | Supported | Enforceu Passworu Rules | | | | | | | | | | | | | | | | | | | | | | |
| | Language_Locale | | | | | | | | | | | | | | | | | | | | | | | |
| Non-English (Asia) | Chinese Simplified (zh_cn) Chinese Traditional (zh_tw) | The password must include a minimum of 8 characters and a maximum of 50 characters. | | | | | | | | | | | | | | | | | | | | | | |
| | | The password cannot include spaces or include a word or phrase that is in the Blocked Words list. | | | | | | | | | | | | | | | | | | | | | | |
| Japanese (Ja_Jp) Korean (ko_kr) | Korean (ko_kr) | The password and the username cannot share the same three consecutive characters. | | | | | | | | | | | | | | | | | | | | | | |
| | | The password must meet two of the following conditions: | | | | | | | | | | | | | | | | | | | | | | |
| | | - Include at least one number (0–9) | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | Include at least one special character (-, ., @, #, !, ?, \$, %) | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | - Include at least one uppercase character |
| | | | | | | | | | | | | | | | | | | | | | | | | |
| | | Include at least one Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase | | | | | | | | | | | | | | | | | | | | | | |

Table 5: Metasys System Password Rules

Keep in mind these important facts about network engine passwords:

- You can change the NAE login user name and password values only when an NAE is a Site Director. If you want to change the login user name or password, you must do so before demoting the NAE from Site Director status.
- When you change (or add) an NAE login user name or password, make sure to record the new user name and password and store them in a safe location. You cannot access the engine's Site Management Portal UI without a valid user name and password. Refer to the *Security Administrator System Technical Bulletin (LIT-1201528)* for details.
- The NAE35 models with Basic Access operation mode require an additional login user name and password to enable and use the Basic Access mode. The initial login user name is **BasicSysAgent**, and it is not case sensitive. You are prompted to create your own account password.

NAE connectivity

You can prepare the connection parameters of an NAE for communication over the building network using one of the following procedures:

- Preparing NAE for a network that supports DHCP and DNS
- Preparing NAE for a network without DHCP and without DNS support when the NAE uses APIPA
- Preparing NAE for a network without DHCP and without DNS support when the NAE uses a static IP address
- Preparing NAE for a network that supports DNS but not DHCP

Time zone, date, and time management

The procedure you use to set the time zone, date, and time on an NAE depends on how the NAE fits into the Metasys site hierarchy. See Appendix: Time Zone, Date, and Time Management for information and detailed procedures for setting time zone, date, and time on an NAE and on a Metasys network.

Alarms and events

Each NAE stores alarm and event messages generated by the NAE and the connected field trunk devices. You can configure an NAE to send alarm and event notifications through the NAE DDAs to email destinations and SNMP devices.

DDAs are agents that route and deliver alarm and event messages to destinations such as email addresses, Syslog servers, and SNMP management systems.

If the site has an ADS/ADX, each NAE can forward alarm and event information to the ADS/ADX for centralized notification and long-term storage.

Important:

To avoid a loss of notification if the repository becomes full, the Metasys system manages the NAE repositories according to the following criteria :

- Events forwarded to an ADS Event Repository are always removed before events that are not forwarded.
- The lowest priority event with the oldest time stamp and Acknowledge Required flag set to false is replaced first.
- If the event about to be created is of a higher priority than at least one event in the repository, the event with the oldest time stamp and the lowest priority is replaced.
- If all events are of the same priority, the event with the oldest time stamp is replaced.
- If the event about to be created is of a lower priority than all other events in the Event Repository, no event is replaced and the new event is discarded.

A loss of alarm paging, printing, or emailing can result if the NAE is not commissioned with strict adherence to these criteria. To avoid managing events in this way, move ADS/ADX and the notification DDAs to the server.

You can designate multiple alarm and event sources in an NAE and in the connected equipment devices, and then configure the conditions that trigger those alarms or events. You can also define multiple notification types and multiple notification destinations for each alarm or event.

The NAE also has several pre-configured internal diagnostic features that are factory set to generate alarms. NAE device diagnostic features with factory-set default alarm values include those listed in the following table.

Table 6: Default Network Engine Alarm Values

| Audit Rate | Event Rate | | |
|-------------------------------|----------------------|--|--|
| BACnet Broadcast Receive Rate | Flash Usage | | |
| COV Rcv Rate | Memory Usage | | |
| CPU Temperature | Samples Lost | | |
| CPU Usage | Sample Rate | | |
| Events Lost | Transfer Buffer Full | | |

You can check the status of these diagnostic features on the Diagnostic tab.

Refer to the *Introduction to Alarm and Event Management* in the *Metasys SMP Help (LIT-1201793)* for more information.

(i) **Note:** After an alarm is generated, anyone who acknowledges the alarm clears that alarm notification for all other users. If an ADS/ADX is the Site Director, you can set the ADS/ADX to deliver alarm and event notifications to a network printer.

Email notification

(i) **Note:** The NAE85 hosts the Metasys UI at Release 12.0. For steps on configuring the NAE85 to generate an alarm and event messages with the Metasys UI, refer to the *NAE85 Commissioning Guide (LIT-12011044)*.

You can configure an NAE to generate alarm and event messages by sending email to one or more email destinations using the email DDA. The steps require you to configure custom email messages and specify email message destinations in the Email tab of the Site Management Portal UI. The following figure provides an example of an email message destination that is active Monday through Friday from 6:00 A.M. to 6:00 P.M.

Figure 7: Example of defining an Email notification

| Operational Alarm Ecous Summary Diagnostic Network Email SMMP Syslog Alarm Attribute Value | $\Theta \Theta$ | PrevRelN50-3 🛍 | | | | | | | | 1000 | | |
|--|-----------------|----------------|------------|---------|-------|------------|---------------------|-----------------|-------------------|-------------|-------------------|--------------|
| Ecous Summary Diagnostic Network Email Studie Edit Attribute Value Image: Studie St | | | | | | | Oper | ational | Alarm | | | |
| Extent Artibule Yalue Shared Configuration Email Enabled True ShTP Server Host 00.00 SMTP Port 25 Authentcation Type None SMTP Port 25 Authentcation Type None SMTP Password Program Deverthesit Program Deverthesit Destination Configuration Label Destination 1 Email Address billigid com Priority Normal Stubject 3 Rethies 3 Enalted True Event Filters Email True Priority Normal Stubject 3 Rethies 3 Enalted True Event Filters Email True Priority Nersage Value Stata Day Of Week >= Monday Message Yalue Stata Day Of Week >= Monday Findaw Withorcation Category Achrowledge Reguired Proious Statas Proious Statas< | Focus | Summary | Diagnostic | Network | Email | SNMP | Syslog | Alarm | Trend | | | |
| Attribute Value Shared Configuration Image: Configuration of the second of | Edit | 1 | | | | | | | | | | |
| Attribute Value Shared Configuration Enail Enailed True Shared Configuration Shared Configuration 0.0.0 Shared Configuration 25 Authenciation Type None Shared Configuration 26 Authenciation Type None Shared Configuration 26 Authenciation Type None Shared Configuration 26 POP Stever Hostname Poperator Poperations Attribute Value Destination Configuration Label Destination 1 Label Destination Configuration Label Priority Priority Normal Subject Retrices 3 Retries 3 Enabled True End Time >2000 AM End Time >= 1200.00 AM * * Priority Yalue Stan Day Of Week >= Monday * Priority Yalue * * Priority Yalue * * * * * * * * * </td <td></td> <td>)</td> <td></td> | |) | | | | | | | | | | |
| Shared Configuration Email Enabled True SMTP Fort 25 Authentication Type None SMTP Port 25 Authentication Type None SMTP Password ************************************ | Att | ribute | | Value | | | | | | | | |
| Email Enabled True SHTP Sever Host 00.0.0 SHTP Vort 25 Authentication Type None SHTP User Name SHTP Destivation POP Sever Hostname POP Sever Hostname Port term Destination 1 Destination Configuration Label Destination 1 Email Address bill@jci.com Priority Normal Subject Retries 3 Enabled True Event Filters Hern Operator Value Eter Titlers Format Priority Value Stat Day Of Week >= Monday Forday Format Value Stat Day Of Week >= Monday Forday Format Value Stat Day Of Week >= Monday Forday Format Value Stat Day Of Week >= Monday Forday Format Forma | Sh | ared Configur | ation | | | | | | | | | |
| SMTP Server Host 0.0.0 SMTP Port 25 Authentication Type None SMTP User Name POP Server Hostname Pop Server | | Email Enable | d | True | | | | | | | | |
| SMTP Port 25 Authentication Type None SMTP Dassword POP Server Hostname Pop Server Hos | | SMTP Server H | Host | 0.0.0.0 | | | | | | | | |
| Authentication Type None SMTP User Name POP Server Hostname Postinations Attribute Value Destination 1 Email Address Priority Normal Subject Retries 3 Enabled Tue Event Filters term Start Time >= 1200:00 AM Start Time <= 1200:00 AM Start Time | | SMTP Port | | 25 | | | | | | | | = |
| SMTP User Name SMTP Password POP Sever Hostname nontime configuration Destination 1 Email Address Priority Normal Subject Retries 3 Enabled True Event Filters Item Operator Value Format Priority Format Priority Format Priority Kethes 3 Enabled Time >= 1200:00 AM Event Filters Item Operator Value Start Time >= 1200:00 AM Format Priority Kets 3 Enabled Time >= 1200:00 AM Event Filters Item Description Format Priority Message Value Site Name Item Cluster Contexet Item Subject Attribute Format Priority Message Value Site Name Item Fully Qualified Reference Attributed Reference Authorization Category Acknowledge Required | | Authentication | Туре | None | | | | | | | | |
| SMTP Password POP Server Hostname POP Server Hostname Destination s Attribute Value Destination 1 Destination Configuration Label Destination 1 Email Address Dill@ci.com Priority Normal Subject Retries 3 Enabled True Event Filters Item Operator Value Start Time >= 12200.00 AM End Time <= 1200.00 | | SMTP User Na | ame | ****** | | | | | | | | |
| POP Server Hostname Postinations Attribute Value Destination Configuration Label Destination 1 Email Address Dill@jci.com Priority Normal Subject Priority Normal Subject Enabled True Event Filters Rem Operator Value Start Time >= 1200.00 AM Configuration End Time <= 1200.00 AM Configuration Format Format Format Format Kensesage Value Start Day Of Weak <= Finday Format Kensesage Value Start Day Of Weak Enabled Format Kensesage Value Format Kensesage Kens | | SMTP Passwo | ord | ****** | | | | | | | | |
| Destinations Attribute Value Destination 1 Label Destination 1 Email Address bill@jci.com Priority Normal Subject Retries Retries 3 Enabled True Event Filters Item Operator Value Start Time >= Format Priority Format Priority Format Priority Kethessage Work Retries 3 Enabled True Event Filters Item Operator Value Start Day Of Week >= Monday Format Format Priority Message Value Site Name Item Tully Qualified Reference Authorization Category Acknowledge Required Previous Status Previous Status | | POP Server H | ostname | | | | | | | | | |
| Destinations Attribute Value Destination 1 Destination Configuration Label Destination 1 Email Address bill@ci.com Priority Normal Subject Retries Retries 3 Enabled True Event Filters Item Operator Value Start Time >= Start Day Of Week >= Monday Format Format Priority Message Value Site Name Site Name Value Site Name Item Fully Qualified Reference Authorization Category Acknowledge Required Previous Status | | | | ******* | - | | | | | | | |
| Destination 1 Label Destination 1 Email Address bill@jci.com Priority Normal Subject Betries Retries 3 Enabled True Event Filters Item Operator Value Start Time >= 12:00:00 AM Start Time <= | Destinat | ions | | | | Attribute | | | Value | | | |
| Label Destination 1 Email Address bill@jcl.com Priority Normal Subject - Retries 3 Enabled True Event Filters Item Operator Value Stat Time = Priority Normal Stat Time = Retries 3 Format Priority Value = Site Name > Value = Site Name > Item Fully Qualified Reference Acknowledge Required = Previous Status = | Destina | ation 1 | | | | Destinatio | on Configui | ation | | | | |
| Email Address bill@jci.com Priority Normal Subject | | | | | | Label | | | Destination 1 | | | |
| Priority Normal Subject | | | | | | Email A | ddress | | bill@ici.com | | | |
| Priority Normal Subject Retries Retries 3 Enabled True Event Filters Item Operator Value Start Time >= Start Time >= Start Time >= Format Priority Format Priority Message Value Site Name Site Name Hem Description Hem Fully Qualified Reference Authorization Category Acknowledge Required Previous Status Previous Status | | | | | | | | | | | | |
| Priority Normal Subject Retries Retries 3 Enabled True Event Filters Item Operator Value Start Time >= Event Filters Item Operator Value Start Time >= Event Filters Item Operator Value Start Time >= End Day Of Week >= Monday = Format Priority Value Site Name Item Fully Qualified Reference Authorization Category Acknowledge Required Previous Status | | | | | | | | | | | | |
| Subject Retries 3 Enabled True Event Filters Item Operator Value Start Time >= Start Time >= Start Day Of Week >= Monday m Format Priority Message Value Site Name Item Fully Qualified Reference Item Fully Qualified Reference Authorization Category Acknowledge Required Previous Status | | | | | | Priority | | | Normal | | | |
| Retries 3 Enabled Tue Event Filters Item Operator Value Start Time >= 12:00:00 AM End Time <= | | | | | | Subject | t | | | | | |
| Enabled True Event Filters Item Operator Value Start Time >= 12:00:00 AM End Time <= | | | | | | Retries 3 | | | | | | |
| Event Filters Item Operator Value Start Time >= 12:00:00 AM End Time <= | | | | | | Enable | d | | True | | | |
| Start Time >= 12:00:00 AM End Time <= | | | | | | | Event Filters | | Item | Operator | Value | |
| End Time <= | | | | | | | | | Start Time | >= | 12:00:00 AM | |
| Start Day Of Week >= Monday Fnd Dav Of Week <= | | | | | 4 | | | End Time | <= | 12:00:00 AM | | |
| Fnd Dav Of Week <= Fridav Format Priority Ø Message Ø Value Site Name Ø Item Description Ø Item Fully Qualified Reference Ø Authorization Category Acknowledge Required Previous Status | | | | | | | | | Start Day Of Week | >= | Monday | |
| Format Priority Message Value Site Name Item Description Item Fully Qualified Reference Authorization Category Acknowledge Required Previous Status | | | | | | | | | End Day Of Week | <= | Friday | |
| Message Value Site Name Item Description Item Fully Qualified Reference Authorization Category Acknowledge Required Previous Status | | | | | | Format | | | Priority | | | |
| ✓ Value Site Name ✓ Item Description ✓ Item Fully Qualified Reference ✓ Authorization Category Acknowledge Required Previous Status | | | | | | | V Message | | | | | |
| | | | | | | | | | Value | | | |
| State Name Item Description Item Fully Qualified Reference Authorization Category Acknowledge Required Previous Status | | | | | | | | | Cita Noma | | | |
| ✓ Item Description ✓ Item Fully Qualified Reference ✓ Authorization Category Acknowledge Required Previous Status | | | | | | | | | | | | |
| | | | | | | | | | Item Description | | | |
| Authorization Category Acknowledge Required Previous Status | | | | | | | Item Fully Qualifie | d Reference | | | | |
| Acknowledge Required Previous Status | | | | | | | Authorization Cate | gory | | | | |
| Previous Status | | | | | | | | Acknowledge Req | uired | | | |
| | | | | | | | | Previous Status | | | - | |
| | 8 | | | | | | | | | | Sonjor: 5/26/2022 | 07:56 AM CDT |

Syslog DDA

(i) **Note:** The NAE85 hosts the Metasys UI at Release 12.0. For the relevant steps on Syslog DDA with the NAE85 on the Metasys UI, refer to the *NAE85 Commissioning Guide (LIT-12011044)*.

An NAE configured as a Site Director has the optional capability of sending its configured audit log entries and alarm notifications to the central repository of an external, industry-standard, Syslog server, conforming to Internet published RFC 3164. After you save the Syslog DDA configuration, all messages are sent immediately to the configured Syslog server. You can then open a user interface at the Syslog server and use the provided filters to interrogate or apply forensic analysis on these messages. To assist in reading the log, a vertical bar symbol (|) separates individual fields of each Metasys message and a single character dash (-) replaces any blank field.

By default, the Syslog option is disabled. Changing the Syslog Reporting Enabled attribute to **True** on the Syslog window enables the Syslog function. The prerequisites to the Syslog DDA are as follows:

- The Syslog server must be installed and running on a computer server or virtual machine that is reachable by the NAE.
- The NAE must be running Release 8.0 software or later.
- No more than three Syslog destinations can be specified.
- The firewall port must be open.

The definition of the Syslog DDA requires:

- label to identify the Syslog server
- IP address of the Syslog server
- port numbers for the UDP send port and UDP receive port (for example, 514 for both)
- event and audit filters to apply against all events and audit messages. Only those events and audit messages that match the filters are passed to the Syslog server.

The Syslog DDA attribute called **Syslog Reporting Enabled** appears on the Shared Configuration section of the Syslog tab of an NAE device object (Figure 8). This attribute has two selections: True or False.

When the Syslog Reporting Enabled attribute is set to True, the feature is active and your Metasys messages (events and audits) are forwarded to your destination Syslog server according to the filtering you specified. When the Syslog Reporting Enabled attribute is set to False, the feature is inactive and no Metasys messages are forwarded to the Syslog server. The configuration example in Figure 8 is set to route to the Syslog server all High Warning alarms that require acknowledgment.

The Syslog DDA implementation is UDP, not TCP. Therefore, any audits/events generated while the Syslog server is offline are not recorded at the Syslog server, even though the Metasys system, unable to determine the current status of the Syslog server, continues to send out messages. A gap in time is present between events when the Syslog server comes back online.

Figure 8: Syslog Tab in Engine's Device Object

| System | | | | | | | | - [| × |
|--|------------------------|--------------|------------|--------------|----------|---------------------|-----------------------|-----------------------|------------|
| <u>I</u> tem <u>E</u> dit <u>V</u> iew <u>A</u> ction I <u>n</u> sert <u>T</u> ools <u>Q</u> uer | ry <u>H</u> elp | | | | | Last Login: T | hu 05/26/2022 07:46:2 | 3 CDT Met*** Logou | Exit |
| û | A A | | | Prev | ReIN50-3 | 3 | | (| 1080 |
| All Items | | | | Oper | ational | Alarm | | | |
| | Focus Summary Diagno | stic Network | Email SNMP | Syslog | Alarm | Trend | | | |
| PrevReiN50-3 | | | | | | | | | |
| Eth IP Datal ink | Edit | | | | | | | | |
| SC Network Port | | | | | | | | | _ |
| | Attribute | Value | | | | | | | |
| Energy | Shared Configuration | | | | | | | | |
| Programming | Syslog Reporting Enabl | ed True | | | | | | | |
| Schedule | | | | | | | | | |
| 🗄 📲 Field Bus MSTP1 | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | Destinations | | | | | | | | |
| | | | Attribute | | | Value | | | |
| | Syslog 1 | | Destinat | on Configu | ration | | | | |
| | | | Label | | | Syslog 1 | | | |
| | • | | Syslo | Server | (| 0.0.0 | | | |
| | | | UDP S | end Port | | 514 | | | |
| | | | UDP F | Receive Port | t e | 514 | | | |
| | | | Event | Filters | | Item | Operator | Value | |
| | | | | | | Acknowledge Require | d == | True | |
| | | | | | | Current Status | == | High Warning | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | Audit | ilters | | Item | Operator | Value | |
| | | | 4 | | | | | | |
| | | | | | | | | | |
| | | | • | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | - |
| | | | | | | | | Sopror: 5/26/2022_07 | -57 AM CDT |
| | | | | | | | • | Server: 5/26/2022, 07 | :57 AM CDT |

Figure 9 shows an example of Metasys system messages as they appear on the Kiwi Syslog® Server Console user interface. Use the console to filter the messages. If you do not have a tool, open a web browser and type the following URL:

http://<IP of the server>>:<Port>/Events.aspx

For example:

http://SysLogserver1:8088/Events.aspx

When you browse to this site, type a valid username and password when prompted to gain access to the Syslog server. A user interface appears with the captured messages.

Figure 9: Syslog User Interface

| | | | | Kiwi Syslog Server (Licensed - Version 9.4) |
|------------|-----------|---------------|---------------|--|
| File Edit | /iew Help | | | |
| 8 2 🖬 | 1 🖸 🕄 | Display 00 (D |)efault) v | |
| Date | Time | Priority | Hostname | Message |
| 09-15-2015 | 21:55:43 | User.Notice | 10.108.171.21 | Sep 16 05:55:43 Inc-jag-NAE45 Metasys: Inc-jag-NAE45:Inc-jag-NAE45/AV1 High Alarm 70 9/16/2015 5:20:15 AM AV1 11.0 User Acknowledgement - |
| 09-15-2015 | 21:55:41 | User.Notice | 10.108.171.21 | Sep 16 05:55:41 Inc-jag-NAE45 Metasys: Inc-jag-NAE45:Inc-jag-NAE45/AV1 High Alarm 70 9/16/2015 5:22:32 AM AV1 66.0 User Acknowledgement - |
| 09-15-2015 | 21:55:35 | User.Notice | 10.108.171.21 | Sep 16 05:55:35 Inc-jag-NAE45 Metasys: Inc-jag-NAE45:Inc-jag-NAE45/AV1 High Alarm 70 9/16/2015 5:27:12 AM AV1 22.0 User Acknowledgement - |
| 09-15-2015 | 21:29:38 | System3.Info | 10.108.171.21 | Sep 16 05:29:38 Inc-jag-NAE45 Metasys: Inc-jag-NAE45:Inc-jag-NAE45/AV1 9/16/2015 5:29:37 AM AV1 User Action MCE MetasysSysAgent Command Adjust 7 33 0k |
| 09-15-2015 | 21:28:35 | System3.Info | 10.108.171.21 | Sep 16 05:28:35 Inc-jag-NAE45 Metasys: Inc-jag-NAE45:Inc-jag-NAE45/AV1 9/16/2015 5:28:35 AM AV1 User Action MCE MetasysSysAgent Command Adjust 77 7 0k |

If you run into any trouble while implementing the Syslog DDA functionality, consult this following table.

| Scenario | Behavior |
|--|--|
| The engine is starting up but the SysLog DDA has not yet started. | All generated audits and events are cached and sent to Syslog DDA once it is started. The maximum size of the cache is 1,000 audits and 1,000 events per hour. |
| The Syslog server crashes. | All generated audits and events that the engine sends to the Syslog server are lost; nothing is cached. |
| The Syslog server goes offline or is unreachable. | All generated audits and events that the engine sends to the Syslog server are lost; nothing is cached. No data is sent to the Syslog server until it comes back online or becomes reachable. |
| The IP address, name, or port numbers of the Syslog server as defined in the engine's object are invalid. | All generated audits and events that the engine sends to the Syslog server are lost; nothing is cached. No data is sent to the Syslog server until you correct the invalid parameters in the Syslog DDA. |
| The Syslog Reporting Enabled parameter is set to True, but no Syslog parameters are defined. | All generated audits and events that the engine sends to the Syslog server are lost; nothing is cached. No data is sent to the Syslog server until you specify the parameters that the Syslog DDA requires. |
| The UDP Send Port or UDP Receive Port is blocked by a firewall. | All generated audits and events that the engine sends to the Syslog server are lost; nothing is cached. No data is sent to the Syslog server until the ports on the Syslog server are opened. |
| A parameter of the Syslog server changes, but the corresponding parameter in the Syslog DDA of the engine is not likewise changed. | All generated audits and events that the engine sends to the Syslog server are lost; nothing is cached. No data is received at the Syslog server until you correct the invalid parameters in the Syslog DDA. |

Table 7: Syslog Server Troubleshooting

Simple Network Management Protocol (SNMP) notification

SNMP is a protocol governing network management and the monitoring of network devices and their functions. It is not necessarily limited to TCP/IP networks. SNMP monitoring is typically used for large BAS networks with many network devices. Alarm and event notifications are sent to and stored on an SNMP management computer that monitors all devices on the network.

The NAE uses SNMP protocol to deliver network device status and conditions to a designated SNMP management computer. You must set up SNMP monitoring at the network level, and you must assign an SNMP management device on the network. (For details, see Creating NAE SNMP alarm notifications and destinations.) If you are applying a Metasys system to an existing network, consult with the network administrator or IT department that administers the network to determine if SNMP monitoring is available on the network.

Configure custom SNMP messages and specify the SNMP message destinations in the SNMP tab of the Site Management Portal UI. Perform this configuration to each NAE individually; SNMP configuration cannot be done on an ADS/ADX.

Enhanced SNMP functionality is available on Metasys systems, including a Metasys system Management Information Base (MIB) file for configuring third-party SNMP translation applications to request, receive, and translate specified SNMP trap messages generated by the Metasys SNMP DDA.

Initial default NCE/NAE configuration

NCEs and NAEs are shipped with standard initial values for many of the editable attributes. The following table lists some important initial default configuration values for the NCE25, NAE35, and NAE45 models. Table 9 and Table 10 define some important initial default configuration values for the NAE55 and NAE85 models.

(i) **Note:** This information does not apply to the NAE45-Lite.

| Attribute/Field Name | NCE25, NAE35, and NAE45 Initial Value |
|------------------------|---|
| Computer Name | NAExxxxxxxxxx or NCExxxxxxxx, where xxxxxxxxx is the Ethernet MAC address of the device without hyphens. For example, if the Ethernet MAC address is 00-80-66-05-0F-FC, the initial Computer Name is NAE08066050FFC. |
| DHCP Client | Enabled |
| Serial Port RS232C A | 115,200 baud, 8 bits, no parity, 1 stop bit (115200,8,n,1), Direct Connect IP over Point-to-Point (PTP). |
| Serial Port RS232C B | 115,200 baud, 8 bits, no parity, 1 stop bit (115200,8,n,1) |
| Site Director | A new network engine is a Site Director by default. If an NCE/NAE is not going to be the Site Director, demote the engine by specifying the Computer Name or IP address of the designated Site Director in this Site Director attribute field. |
| | Image: Note: An NCE25 should not be designated as a Site Director to any other engines than itself. |
| Initial Login Username | MetasysSysAgent (not case sensitive) |
| Initial Login Password | Contact your local Johnson Controls representative. |

Table 8: NCE25, NAE35, and NAE45 Initial Configuration Values

Table 9: NAE55 Initial Configuration Values

| Attribute/Field Name | NAE55 Initial Value |
|----------------------|--|
| Computer Name | NAExxxxxxxxxx, where xxxxxxxxx is the Ethernet MAC address of the device without the hyphens. For example, if the Ethernet MAC address is 00-80-66-05-0F-FC, the initial Computer Name is NAE008066050FFC for NAE55s. |
| DHCP Client | Enabled |
| Serial Port A | 115,200 baud, 8 bits, no parity, 1 stop bit (115200,8,n,1), Direct Connect IP over Point-to-Point (PTP). |
| Serial Port B | 9600 baud, 8 bits, no parity, 1 stop bit (9600,8,n,1) |

Table 9: NAE55 Initial Configuration Values

| Attribute/Field Name | NAE55 Initial Value |
|------------------------|--|
| Site Director | A new NAE55 is a Site Director by default. If an NAE is not a Site Director, demote the engine by specifying the Computer Name or IP address of the designated Site Director in this Site Director attribute field. |
| Initial Login Username | MetasysSysAgent (not case-sensitive) |
| Initial Login Password | Contact your local Johnson Controls representative. |

| Attribute/Field Name | NAE85 Initial Value |
|------------------------|--|
| Computer Name | NAExxxxxxxxx, where xxxxxxxxx is the Ethernet MAC address of the enabled Ethernet card without the hyphens. For example, if the Ethernet MAC address is 00-1E-EC-6E-5D-32, the initial Computer Name is NAE001EEC6E5D32. Same as the computer name defined under the system properties of the Windows operating system. |
| DHCP Client | Enabled When you commission an NAE85 for an Ethernet LAN that supports Dynamic Host Configuration Protocol (DHCP) and Domain Name Server (DNS), we recommend that you configure a DHCP reservation for the NAE85 to ensure it always receives the same IP address when its lease expires. This practice prevents address bindings between the NAE85 and other devices from breaking. |
| Site Director | A new NAE85 is shipped installed as a Site Director. If you do not want the NxE85 to be the Site Director, you must demote it by entering the Computer Name or IP address of the designated Site Director in this Site Director attribute field. |
| Initial Login Username | MetasysSysAgent (not case-sensitive) |
| Initial Login Password | Contact your local Johnson Controls representative. |

Table 10: NAE85 Initial Configuration Values

Allow HTTP

A network engine at Metasys system Release 8.1 or later has an attribute called **Allow Http** located under the **Network** tab of the engine in the SMP UI. This attribute controls if the Windows Firewall in the network engine blocks incoming network traffic over the HTTP port (port 80). By default, the **Allow Http** attribute is set to **True** for all network engines upgraded to Release 8.1 or later. Changing this attribute to **False** blocks all incoming network traffic over port 80 at the network engine. Doing so does not interfere with NAE Update Tool operations or SCT Pro.

(1) **Note:** SCT Pro is the preferred tool for flashing engines to Release 10.1 or later.
Figure 10: Allow Http attribute for network engine

| System | - c | x c |
|---|--|-------------|
| <u>I</u> tem <u>E</u> dit <u>V</u> iew <u>A</u> ction I <u>n</u> sert <u>T</u> ools | Query Help Last Login: Thu 05/26/2022 07:46:23 CDT Met*** | ut Exit |
| All Items PrevReIN50-3 BACnet Protocol Eng SC Network Port Cupdate Cinergy | PrevReIN50-3 Operational Alarm Focus Summary Diagnostic Network Email SNMP Syslog Alarm Trend Edit Attribute Value Value Value Orwork Identification Computer Name PrevReIN50-3 Domain Name Completion Domains Listo[1]-cgna.jdi.com Ethemer Mick. Address 74/EF-48-0C-48-9E | |
| ∞ Teld Bus MSTPT | Ethemet MAC Address 74:E:48:0C:A6:9E Allow Http True DHCP Enabled True JCI IP Address 172:21.13.19 IP Mask 255:255:255.0 IP Router Address Listof[1]-172:21.13.1 Obtain DNS address automatically True | |
| ▼ | Server: 5/26/2022, 07 | 7:59 AM CDT |

The **Allow Http** attribute is set on each network engine independently. A schedule or other control action can modify the value of this attribute. You can configure a tailored summary to view the value of the **Allow Http** attribute on all network engines at the site. You can also use the mass editing capability in SCT to modify the **Allow Http** attribute across multiple devices.

To provide the highest level of security, set **Allow Http** to **False** for every network engine upgraded to Release 8.1 or later. However, if the network engine is a Site Director and if you have not upgraded the child engines reporting to it to Release 8.1 or later, set **Allow Http** to **True**. For reference, the following table lists which Metasys tools, utilities, and features depend on Port 80. If the network engine uses one or more of these items that require Port 80, set **Allow Http** to **True**.

| Item | Does it require Port 80 | Notes |
|---|----------------------------|---|
| Advanced Graphics Application (AGA) | Yes | Uses an older version of Metasys data access services that requires http. |
| Advanced Reporting and Energy Essentials | Yes | Uses http for communication with engines. |
| ССТ | Yes | Uses an older version of Metasys data access services that requires http. However, CCT only requires Port 80 for upload and download operations. |
| Graphic Generation Tool (GGT) | Yes | Uses an older version of Metasys data access services that requires http. |
| Launcher 2.0 | No | Uses https for communication with engines upgraded to Release 8.1 or later, but must be set for http to communicate with engines prior to Release 8.1. |
| Metasys Export Utility | Yes | Uses an older version of Metasys data access services that requires http. |
| Metasys for Validated Environments (MVE) | No | Uses https for communication with engines upgraded to Release 8.1 or later. |
| Metasys UI | No | Uses https for communication with engines upgraded to Release 8.1 or later. |

Table 11: Port 80 requirements for tools, utilities, and features

| Item | Does it require Port 80 | Notes |
|---|----------------------------|--|
| NAE Configuration and Information Tool (NCT) | Yes | Requires port 80 for sending a file to an engine from the commissioning laptop. |
| NAE Update Tool | Yes | Allow Http is set to Requires port 80 to successfully perform a code download to the engine using the HTTP update method. If False , the NAE Update Tool temporarily opens port 80 for its operations, then closes the port after the download completes. |
| P2000 | Yes | Requires port 80 (inbound) to be open on the Windows Firewall of the Metasys server. |
| Ready Access Portal | Yes | Uses https between the Ready Access Portal server and the client, but http between the Ready Access Portal server and the engines. |
| | | Note: Ready Access Portal is no longer supported at Release 9.0 or later. |
| SMP | No | Uses https for communication with engines upgraded to Release 8.1 or later. |
| SCT/SCT Pro | No | Uses https for communication with equipment controllers and engines upgraded to Release 8.1 or later. |

Table 11: Port 80 requirements for tools, utilities, and features

Advanced Security Enabled

The Advanced Security Enabled setting, available only to Site Directors and network engines at Release 10.0 or later, indicates if the site uses the advanced security settings. This attribute provides an improved layer of security between Metasys Site Directors and network engines. With this attribute set to **True**, backward-compatible methods of communication between the Site Director and its network engines are disabled, which means a Site Director at Release 10.0 or later discards all communication attempts from network engines prior to Release 10.0. At Release 10.0, Advanced Security Enabled is defaulted to **False**. However, to provide for a higher level of security, the Advanced Security Enabled attribute is defaulted to **True** at Release 10.1 or later.

| I System | | | | _ | | × |
|---|-----------------|---------------------------------|-----------------------------|-------------------|-----------|---------|
| <u>I</u> tem <u>E</u> dit <u>V</u> iew <u>A</u> ction I <u>n</u> sert <u>T</u> ools <u>Q</u> ue | ry <u>H</u> elp | Last Lo | gin: Thu 05/26/2022 10:02:4 | 42 CDT Met*** 🛛 🛛 | ogout | Exit |
| 仓 | $\Theta \Theta$ | | Site | | <u></u> | - 🛛 🖉 |
| All Items | | | Normal | | | |
| | Site View | Authorization Categories | Custom Enumerations | | | |
| User Views | Edit | | | 🔵 Basi | c 🖲 Ad | lvanced |
| E PrevRelN50-3 | Attribu | ite ne sync metrioa | Value | | | |
| | Mu | lticast Group Address | 224.0.1.1 | | | |
| | Mu | lticast UDP Port | 123 | | | |
| | Mu | lticast TTL | 1 | | | |
| | Mu | lticast Heartbeat Interval | 5 minutes | | | |
| | Offlin | e Detection | | | | |
| | Po | I Rate | Fast | | | |
| | Opera | ational Data | | | | |
| | All | ltems Update In Progress | False | | | |
| | • On | line Archive Transfer In Progre | ss False | | | |
| | En | um Set Memory Used | 0 % | | | |
| | k Re | maining Custom Sets | 256 | | | |
| | Re | maining Auto Sets | 1000 | | | |
| | Site | e Security Level | Encrypted Only | | | |
| | Ce | rtificate Renewal Period | 60 days | | | |
| | Adv | anced Security Enabled | True | | | |
| | BACn | et | | | | |
| | BA | Cnet Site | False | | | |
| | BA | Cnet Encoding Type | ISO 10646 (UTF-8) | | | = |
| | Thi | rd party BBMDs | Listof[0] | | | |
| | DN | S Refresh Period | 20 minutes | | | |
| | Graph | ic Association | | | | |
| | Gra | aphic | Object Name: Reference: | | | |
| | Gra | aphic Alias | | | | |
| | Warn | ing Banner | | | | |
| | Wa | rning Banner | None | | | - |
| 8 | | | • | Server: 5/26/202 | 22, 10:06 | AM CDT |

Figure 11: Advanced Security Enabled attribute for Site object

Important:

This setting applies to the entire site, so change this attribute to **False** if you have any network engines on the site that are running any release prior to Metasys Release 10.0. Otherwise, these older engines go offline to the Site Director.

Whenever you change this attribute from **False** to **True**, a user message appears to indicate that all network engines prior to Release 10.0 remain online, but are disconnected from the site because they no longer communicate with the Site Director.

FIPS and non-FIPS compliance

At Metasys Release 11.0 and later, the encryption methods used for communication between the NAE and the Metasys Server have been updated to meet FIPS 140-2. FIPS 140-2 is based on the Federal Information Processing Standard (FIPS) Publication 140-2, a U.S. government computer security standard used to approve cryptographic modules.

FIPS 140-2 compliance is a standard feature on all NAE engines at Release 11.0 and later and an optional, licensed feature for the Metasys Server and NAE85/LCS85 software engines. After you update an NAE to Release 11.0 or later, the only method for removing FIPS 140-2 compliance is to reimage the engine to an earlier release. Also, there is no attribute in the user interface to indicate that a particular network engine is FIPS compliant. All NAE engines that run Release 11.0 and later firmware are FIPS compliant; all engines at any earlier release are not FIPS compliant.

For the Metasys Server at Release 11.0 or later, FIPS 140-2 compliance is a purchased and licensed feature. The attribute called **FIPS Compliance Status**, located under the Engineering Values section of the ADS device object, indicates the current FIPS status of the server. The value is either Compliant (Licensed) or Non-Compliant (Unlicensed). This read-only attribute is set to Compliant (Licensed) after you license FIPS compliance and install the FIPS compliance software on the Metasys Server. After you license the server for FIPS compliance, the server communicates **only** with other network engines that are also FIPS compliant. This restriction is necessary for a facility to be fully FIPS compliant.

Refer to the following table for an overview of how communication between the Site Director and network engines is affected using various security settings. As indicated in Table 12, a Site Director at an earlier release **cannot** communicate to a network engine that is at a later release, regardless of security settings.

| Site Director with release | Site DirectorServer FIPSAdvancedCompliance | | Network Engine communication to Site Director | | |
|---|--|--------------------|--|----------------------|-----------------------|
| | Security | | Rel. 9.0 or earlier | Rel. 10.0 or 10.1 | Rel. 11.0 or later |
| ADS/ADX Rel. 9.0 or earlier | <na></na> | <na></na> | ALLOWED | BLOCKED | BLOCKED |
| ADS/ADX | FALSE | <na></na> | ALLOWED | ALLOWED | BLOCKED |
| Rel. 10.0 or 10.1 | TRUE | <na></na> | BLOCKED | ALLOWED | BLOCKED |
| ADS/ADX | FALSE | Unlicensed | ALLOWED | ALLOWED | ALLOWED |
| Rel. 11.0 or | TRUE | Unlicensed | BLOCKED | ALLOWED | ALLOWED |
| later | TRUE or FALSE | Licensed | BLOCKED | BLOCKED | ALLOWED |
| Network Engine Rel. 9.0 or earlier | <na></na> | <na></na> | ALLOWED | BLOCKED | BLOCKED |
| Network | FALSE | <na></na> | ALLOWED | ALLOWED | ALLOWED |
| Engine Rel. 10.0 or 10.1 | TRUE | <na></na> | BLOCKED | ALLOWED | BLOCKED |
| Network Engine Rel. 11.0 or later | TRUE or FALSE | Always Licensed | BLOCKED | BLOCKED | ALLOWED |

Table 12: Network Engine security overview

System and user preferences

The Metasys system provides customized preferences for the Site Management Portal UI. The preferences allow you to configure how the UI behaves, including the sounds and colors, the startup view, and the ability to add links to external applications that can be accessed from within the UI of the network engine.

Reset command device

The Reset Device command in the Site Management Portal UI initiates an orderly reset that saves recent changes to the NAE archive database and restarts the engine's operating system. When the NAE requires a reset, the title bar of the object in the Display panel displays Reset Needed. A reset is required for new settings to take effect after making changes to the following attributes:

- APDU Retries
- APDU Segment Time-Out
- APDU Time-Out
- BACnet IP Port
- Computer Name
- Contact Person
- Domain Name
- Max APDU Length
- Network Address
- Port Number
- Read/Write Community
- SNMP DDA
- SNMP Management Device
- Serial Port 1 Cable Config
- Time Sync Period
- (i) **Note:** Changing the Computer Name value of the NAE forces a device reset.

NAE network sensitivity

On some busy building networks, equipment controllers on the BACnet/IP and MS/TP field bus may cycle online and offline to the NAE, even though the device is actually online. This behavior is most often seen with small-capacity network engines. If the building network is experiencing this issue, you can lower the sensitivity of the BACnet/IP and MS/TP field bus networks by increasing the number of seconds the network engine waits before flagging an equipment controller as offline. Three different sensitivity options, each with a different set of values, are available:

- High Sensitivity: for a system that is not showing any signs of the offline cycling issue
- **Medium Sensitivity** (default): for a system that is showing the offline cycling issue occasionally
- Low Sensitivity: for a system that is showing chronic occurrences of the offline cycling issue

Table 13 lists the items in the network engine that you can adjust to decrease network sensitivity. After changing any of these values, you need to restart the engine for the new sensitivity settings to take effect. For a description of the steps required, see Adjusting NAE network sensitivity.

| Attributes to Adjust |
|--|
| APDU Segment Timeout APDU Timeout APDU Retries |
| Internode Comm Timer |
| Poll Delay |
| Internode Comm Timer |
| APDU Segment Timeout APDU Timeout APDU Retries |
| Internode Comm Timer APDU Segment Timeout APDU Timeout APDU Retries |
| |

Table 13: Network Sensitivity Adjustments

Detailed Procedures

You need the following items to perform the detailed commissioning procedures for an NAE:

- an NAE with Release 8.1 and newer software
- an Internet browser on a laptop or desktop computer for downloading the Launcher application that is used to log on the NAE. Supported browsers include Microsoft Edge 91 or later, Google Chrome version 91 or later, or Apple Safari version 13.1 or later
 - (i) **Note:** In some scenarios, the computer must be a DHCP client or must be configured to use a static IP address appropriate for the network.
- the NAE Ethernet MAC address

You may also need:

- a new, unique IP address for each NAE on the Metasys network if DHCP cannot be used
- a copy of the NAE archive database that configures the NAE for your specific site. (The NAE archive database can be created and stored offline in the SCT.)

• SCT Release 15.0 or later loaded on the commissioning computer

Installing Launcher to access the NAE

About this task:

You use the Launcher application to access an NAE. If the Launcher application is already installed on your computer, skip to Step 4 below.

(i) **Note:** The Single Site Connection install option is available to network engines and the ADS/ ADX at Release 9.0 or earlier. For network engines and the ADS/ADX at Release 10.0 or later, only the Full Launcher Installer option is available.

If the Launcher application is not installed, follow these steps:

- 1. Open a supported web browser on the computer.
- 2. Enter this URL in the address field: **http://<NAE-computer-name>/metasys**. A link to the Launcher website displays on a blank web page. Click the link.
- 3. Select the current release for your operating system to download the Launcher installation file to a location on your computer. When complete, run the Launcher installation. For details, refer to the *Launcher Installation Instructions (LIT-12011783)* if needed.
- 4. Start the **Launcher** application.

Launcher Add Delete Edit Launch Description P/Host Name Version: Description P/Host Name Version: Description P/Host Name Version: Description P/Host Name Version:

Figure 12: Launcher window

- 5. Click Add.
- 6. Enter the host name (or IP address) of the NAE including the domain name if required, and then click **Discover**. The Launcher searches for the device on the building network. When the device is found, the Add New window refreshes to indicate the found device.

Figure 13: Add New: Launcher found device

Add New

| SN | /IP/SCT | B | lookmark |
|---|---|-----------------------------|-----------------|
| IP Address or Host Name 172.21.53.74 | : | | Discover |
| Add Version SMP ☑ 12.0.0.5988 | Default Language English (United States) | Description 172.21.53.74 | Create Shortcut |

- 7. Make sure the **Add** box next to SMP is selected. You can enter a descriptive name for the NAE in the **Description** field to make the NAE easier to find in the profile list, or you can keep the default IP address. Click **Save**. The NAE is added to the profile list on the SMP tab.
- 8. Select the NAE from the SMP profile list and click **Launch**. If the device you are adding has not yet been downloaded and installed on your computer, a **Downloading** window appears, followed by an **Installing** window. The windows close when the download and installation steps are complete.
- 9. Enter the initial Username and Password values for the NAE and click **Login**. See Login user names and passwords.
- 10. If necessary, set the time, time zone, and date.

Establishing direct connection to an NAE

About this task:

This scenario is typical for a single NAE that is not attached to a building network and can be used to set up an NAE before it is installed and connected to a site network. The following procedure requires two Ethernet cables.

- 1. Make sure that the NAE is receiving power and running. The RUN LED should flash blue and purple at a rate of one blink per second.
- 2. Connect the NAE to an Ethernet switch port with one of the cables. Connect your computer to an Ethernet switch port with the second cable. Make sure that the LAN **is not connected** to the Ethernet switch.
- 3. Verify that the 10/LINK or 100/1000 LINK LED on the NAE and Ethernet switch are lit to confirm connectivity between the computer and the NAE through the Ethernet switch.
- 4. Verify that the Local Area Connection for the Ethernet connection to the NAE is enabled and that all other network connections (including wireless connections) are disabled on the laptop, as follows:
 - a. In **Control Panel**, select **Network Connections** or **Network and Dialup Connections**.
 - b. Verify that the Local Area Connection for the Ethernet connection to the NAE is enabled. All other connections should be disabled or disconnected. To disable or enable a connection, right-click the connection and choose from the menu.
- 5. Verify that the computer has a valid IP address, as follows:
 - a. On the **Start** menu, select **Run**.

- b. Type cmd, and click **OK**.
- c. At the command prompt, type <code>ipconfig</code> and press **Enter**. If the computer IP address is all 0s, wait several minutes. Enter the <code>ipconfig</code> repeatedly until the address is established.
- 6. Access the Metasys system login screen for the network engine using the Launcher. See Accessing Site Management Portal UI on an NAE for information on accessing the NAE UI.

Preparing NAE for a network that supports DHCP and DNS

The following scenario is typical when you install an NAE on an existing building network. Your computer must be connected to the network. The computer must be a DHCP client or configured to use a static IP address appropriate for the network.

- (i) **Note:** We recommend that you configure a DHCP reservation for the NAE to ensure it always receives the same IP address when its lease expires. This practice prevents address bindings between the NAE and other devices from breaking.
- 1. Verify that your network administrator has updated the DNS server and the DHCP server with the NAE Ethernet MAC address and the NAE host name.
- 2. With your computer or commissioning laptop connected to the building network, open SCT Pro. This tool listens for and shows the IP address information of the NAE as it comes online.
- 3. Connect the NAE to the network with an Ethernet patch cable.
- 4. Connect 24 VAC supply power to the NAE. Then wait for the NAE to complete the startup and initialization sequence. SCT Pro indicates the current IP address of the network engine.
 - (1) **Note:** The startup and initialization sequence may take up to 10 minutes to complete. If the DHCP server is not online when the NAE is powered on (or if the NAE Ethernet cable is disconnected and reconnected with no DHCP server online), the NAE assumes a unique IP address between 169.254.0.1 and 169.254.255.254 and a subnet mask of 255.255.0.0. This is a feature of Automatic Private Internet Protocol Addressing (APIPA) that applies when DHCP is enabled in the NAE (factory default).
- 5. Go to Installing Launcher to access the NAE, follow all instructions, then return to the next step in this section.
- 6. After you have completed the steps in Installing Launcher to access the NAE, including the step for logging in to the NAE, select the NAE device object in the Navigation panel, and drag it to the Display panel of the Site Management Portal UI. The Focus tab for the selected NAE appears in the Display panel.

Figure 14: NAE Focus Tab - Basic

| 💷 System | - D X |
|---|---|
| Item Edit View Action Insert Tools Quer | / Help Last Login: Thu 05/26/2022 08:47:04 CDT Met*** Logout Exit |
| 企 | |
| All Items | Operational Alarm |
| PrevReIN50-3 | Focus Summary Diagnostic Network Email SNMP Syslog Alarm Trend |
| BACnet Protocol Eng | Edit Basic Advanced |
| SC Network Port | Attribute Value |
| | Object |
| Energy | Name PrevReIN50-3 |
| Programming | Description |
| 📄 Schedule | Object Type Device |
| 🖮 🔚 🛛 Field Bus MSTP1 | Authorization Category General |
| | Model Name MS-NAE5521-3 |
| | Time |
| | Local Time 09:17 AM (HH:MM AM/PM) |
| | Local Date Thursday, May 26, 2022 |
| | Time Zone (UTC-06:00) Central Time (US & Canada) |
| × | - Server: 5/26/2022, 09:17 AM CE |

7. Go to the **Network** tab and verify the Computer Name and Domain Name values. Change these values to the assigned values for your network site. Also verify the **Allow http** attribute. If trusted certificates are not deployed to the engine, communication between the engine and its clients occurs over port 80. If you need to close the network engine's incoming http communication port (port 80), select **False** for Allow http. Doing so does not interfere with NAE Update Tool operations. Otherwise, keep this attribute at its default value (True).

Figure 15: NAE Network Tab - Edit Mode

| 🗾 System | | | - 0 | \times |
|--|--|--|-------------------------------|----------|
| <u>I</u> tem <u>E</u> dit <u>V</u> iew <u>A</u> ction I <u>n</u> sert <u>T</u> ools <u>Q</u> uer | r <u>H</u> elp LastLog | gin: Thu 05/26/2022 08:47:04 CD | T Met*** Logout | Exit |
| <u>۵</u> | P P | PrevReIN50-3 | ê C |) 🛛 🖉 |
| All Items PrevReIN50-3 | Focus Summary Diagnostic Netwo | perational Alarm ork Email SNMP Syslog | Alarm Trend | |
| Eth IP DataLink | Save Cancel | 1 | [| |
| SC Network Port | Network Identification | Value | Units | - |
| ···· · Energy ···· · Programming | Computer Name Domain Name | PrevReIN50-3 | | |
| Schedule Field Bus MSTP1 | Completion Domains Ethernet MAC Address | Listof[1] - cg.na.jci.com 💌 74:FE:48:0C:A6:9E |] | = |
| | Allow Http | True |) | |
| | DHCP Enabled | True | | _ |
| | JCI IP Address | 172 21 13 19 | | |
| | IP Mask IP Router Address | 255 .255 .255 .0 Listof[1] - 172.21.13.1 | | |
| ▼ | | Ser | : rver: 5/26/2022, 09:17 / | AM CDT |

- ➤ Important: The NAE Update Tool places restrictions on the host name (Computer Name) values that you can use for an NAE. Names must start with a letter or number, and must end with either a letter or a number, and may contain dashes only in the interior of the name. Refer to the NAE Update Tool Help (LIT-12011524) for more information on host name restrictions.
- (i) **Note:** Changing the Computer Name forces a device reset on the NAE. (See Computer name and Reset command device.)
- 8. Go to the **Focus** tab and check the NAE Object Name. Change the Object Name to the descriptive label used to identify the NAE in the Site Management Portal UI and SCT.

Figure 16: NAE Focus Tab - Advanced Edit Mode

| 💷 System | | - 🗆 X |
|---------------------|----------------------------------|---|
| | <u>H</u> elp Last Logir | 1: Thu 05/26/2022 08:47:04 CDT Met*** Logout Exit |
| 企 | Pro Pro | evReIN50-3 🖰 🗆 🛛 🖉 |
| All Items | Ope | erational Alarm |
| | Focus Summary Diagnostic Network | k Email SNMP Syslog Alarm Trend |
| BACnet Protocol Eng | Edit | 🔘 Basic 💿 Advanced |
| Eth IP DataLink | | 1 |
| SC Network Port | Attribute | Value |
| Update | Object | |
| Energy | Name | PrevReIN50-3 |
| Programming | Description | |
| Schedule | Object Type | Device |
| ⊞ Hield Bus MSTP1 | Authorization Category | General |
| | Model Name | MS-NAE5521-3 |
| | Time | |
| | Local Time | 09:21:00 AM (HH:MM:SS AM/PM) |
| | Local Date | Thursday, May 26, 2022 |
| | Time Zone | (UTC-06:00) Central Time (US & Canada) |
| | Engineering Values | |
| | Firmware Version | 12.0.0.2063 |
| | Staged Firmware Version | |
| | Staged Files | |
| | Item Reference | Test123:PrevReIN50-3 |
| | Version | 37.0 |
| | BIOS Version | |
| | OS Version | 10.17.41.24 |
| | Archive Date | Thursday, May 26, 2022 |
| | Max Message Buffer | 994 bytes |
| | Max APDU Length | 1024 bytes |
| | APDU Segment Timeout | 10000 ms |
| | APDU Timeout | 10000 ms |
| | APDU Retries | 4 |
| | Internode Comm Timer | 120 💌 |
| × | | Server: 5/26/2022, 09:20 AM CDT |

Depending on the DNS server configuration, the NAE should be reachable from the subnet on which the NAE resides or from other subnets.

Preparing NAE for a network without DHCP and without DNS support when the NAE uses APIPA

About this task:

This scenario is typical when you install an NAE on a stand-alone network designated as a building control network only. Perform these steps from a computer attached to the network. The NAE uses APIPA to automatically assign an IP address. For this procedure, do not attach an Ethernet crossover cable directly to the NAE. In this scenario, a direct connection to the NAE may affect the assignment of an IP address.

- 1. Attach the NAE to the network using an Ethernet patch cable.
- 2. With your computer or commissioning laptop connected to the building network, open SCT Pro. This tool listens for and shows the IP address information of the NAE as it comes online.
- 3. Connect supply power to the NAE and wait for the NAE to complete initialization.
 - (i) **Note:** The startup and initialization sequence may take up to 10 minutes to complete.

- 4. Verify that the computer is configured to use APIPA or a static IP address and subnet mask that are compatible with APIPA. If necessary, change the computer's IP address and subnet mask to be compatible with APIPA.
- 5. Go to Installing Launcher to access the NAE, follow all instructions, and then return to the next step in this section.
- 6. After you have completed the steps in Installing Launcher to access the NAE, including the step for logging in to the NAE, demote the NAE from Site Director if the NAE is not going to be the Site Director. See Designating an NAE as a child of a Site Director.
- (Optional) Select the **Network** tab of the NAE device object. Change the Computer Name value from the factory default, if desired. See Computer name and Reset command device. Initial setup is complete. You can now log in to the NAE by starting the Launcher and entering the initial computer name of the NAE or the computer name you assigned in Step 7.

Preparing NAE for a network without DHCP and without DNS support when the NAE uses a static IP address

About this task:

This scenario is typical when you install the NAE on a stand-alone network dedicated to building control only. Do not use this scenario when the NAE uses APIPA. The steps can be performed from a computer that is attached to the network or a computer that is connected directly to the NAE with an Ethernet crossover cable. If the computer is attached to the network, the computer must be connected to the same subnet as the NAE. To connect to the NAE with this procedure, you may need to know the IP address of the NAE.

- 1. Check the network IP address and the subnet mask of the computer. If needed, change the IP address and the subnet mask of the computer so that the computer and the NAE are on the same subnet. The IP address assigned to the computer must be unique for the subnet.
- 2. With your computer or commissioning laptop connected to the building network, open SCT Pro. This tool listens for and shows the IP address information of the NAE as it comes online.
- 3. Connect supply power to the NAE and wait for the NAE to complete startup and initialization. The startup and initialization sequence may take up to 10 minutes to complete. SCT Pro indicates the current IP address of the network engine.
- 4. Go to Installing Launcher to access the NAE, follow all instructions, then return to the next step in this section.
- 5. After you have completed the steps in Installing Launcher to access the NAE, including the step for logging in to the NAE, demote the NAE from Site Director if the NAE is not going to be the Site Director.
- 6. Select the NAE device object from the Navigation panel of the Site Management Portal UI and drag it to the Display panel. The NAE device object UI opens in the Display panel.
- 7. Select the Network tab of the NAE device object and click **Edit**.
- 8. Change the Computer Name value, if desired. Change DHCP Enabled attribute value to False. This disables DHCP and APIPA. Specify the IP Address, IP Mask, IP Router Address, and the DNS Server IP Addresses. The network administrator typically assigns these values. Record the assigned IP address for the NAE for future reference. Click **Save**. The NAE automatically logs you out and resets.

| System | | | - 🗆 × |
|--|----------------------------------|---------------------------------|-------------------------------|
| <u>I</u> tem <u>E</u> dit <u>V</u> iew <u>A</u> ction I <u>n</u> sert <u>T</u> ools <u>Q</u> uer | y <u>H</u> elp Last Lo | gin: Thu 05/26/2022 08:47:04 CD | T Met*** Logout Exit |
| 企 | e 9 | PrevReIN50-3 | ê o 🛛 🖗 |
| All Items | C | perational Alarm | |
| PrevReIN50-3 | Focus Summary Diagnostic Netwo | ork Email SNMP Syslog | Alarm Trend |
| BACnet Protocol Eng | Save Cancel | | |
| - 🐝 Eth IP DataLink | | 1 | |
| SC Network Port | Attribute | Value | Units |
| Update | Network Identification | D. D. 19/50.0 | |
| Energy | Computer Name | Previce IN50-3 | |
| Schedule | Completion Domains | Listof[1] - ca na ici com 🖉 🗍 | |
| E- Hand Field Bus MSTP1 | Ethernet MAC Address | 74:EE:48:0C:46:0E | |
| | Allow Http | | |
| | LAN | line | |
| | DUCE Enabled | True | |
| | | Title | |
| | JCI IP Address | 172 21 13 19 | |
| | * IP Mask | 255 .255 .255 .0 | |
| | IP Router Address | Listof[1] - 172.21.13.1 😨 | |
| | Obtain DNS address automatically | True | |
| | DNS server IP addresses | Listof[3] 💿 📖 | |
| | BACnet Communication | | |
| | IP Communication Mode | Ethernet IP Only Mode 🔹 | |
| | Operational Certificate Status | Struct | |
| | BACnet Routing | | |
| | Routing Mode | Disabled 👻 | |
| | BACnet Integrated Objects | Include in Object List | |
| | | | |
| | | | |
| | | | |
| 8 | P | Sei | rver: 5/26/2022, 09:22 AM CD1 |

Figure 17: Network Tab - Edit Mode

- 9. Wait for the NAE to complete the startup and initialization sequence.
 - (i) **Note:** The startup and initialization sequence may take up to 10 minutes to complete.

Initial setup is complete.

(i) **Note:** If you connected your computer directly to the NAE with an Ethernet crossover cable, disconnect the crossover cable and connect the NAE to the network with an Ethernet patch cable.

You can log in to the NAE by entering its IP address in Launcher on any subnet of the network.

Preparing NAE for a network that supports DHCP but not DNS

About this task:

This scenario is common to many building networks. The NAE should only use DHCP without DNS if you have configured DHCP to always assign the same IP address after device resets and lease

renewals. If this is not the case, use static IP addresses as described in Preparing NAE for a network without DHCP and without DNS support when the NAE uses a static IP address.

- 1. Attach the NAE to the network using an Ethernet patch cable.
- 2. With your computer or commissioning laptop connected to the building network, open SCT Pro. This tool listens for and shows the IP address information of the NAE as it comes online.
- 3. Connect supply power to the NAE and wait for the NAE to complete initialization. SCT Pro indicates the current IP address of the network engine.
 - The startup and initialization sequence may take up to 10 minutes to complete.
- 4. Go to Installing Launcher to access the NAE, follow all instructions, then return to the next step in this section.
- 5. After you have completed the steps in Installing Launcher to access the NAE, including the step for logging in to the NAE, update the NAE computer name value on the Network tab. After the computer name is updated, the Site Management Portal UI automatically logs out, and the NAE automatically resets. Wait for the NAE to complete the startup and initialization sequence. (This sequence may take up to 10 minutes.)

Preparing NAE for a network that supports DNS but not DHCP

This scenario is not typical of modern networks. The steps are identical to the steps in the Preparing NAE for a network without DHCP and without DNS support when the NAE uses APIPA and Preparing NAE for a network without DHCP and without DNS support when the NAE uses a static IP address.

Using the NAE Ethernet MAC address (from the NAE label), the network administrator can update the DNS server and the assigned computer name. If this is done, you can enter **dns-name** in Launcher on any computer on the building network.

Accessing Site Management Portal UI on an NAE

About this task:

After an NAE is set up for connectivity, the Site Management Portal UI can be accessed through the Launcher.

See Site Management Portal user interface and the *Metasys Site Management Portal Help* (*LIT-1201793*) for additional information about navigating the Site Management Portal UI.

You need to know the Computer Name (or IP address) of the NAE you wish to access. If you do not know the IP address of the NAE, see Determining the NAE IP address and device name for a network connection.

If the NAE has been added to a building's DNS server, you can access it by its Computer Name.

To access the Site Management Portal UI on an NAE through the Launcher:

- 1. Start Launcher.
- 2. Select the Computer Name (or IP address) of the NAE on the SMP tab of the Launcher, and click **Launch**. The Metasys system login window appears.
- 3. Type the NAE Username and Password, and then click **Login** or press **Enter**.
- 4. To view an NAE, select the NAE object from the Navigation panel and drag it to the Display panel. The NAE object opens with the Focus tab active (Figure 18).

Entering basic NAE parameters in the focus screen

- 1. In the Site Management Portal UI, display the NAE device object and click the **Focus** tab.
- 2. Click **Edit**. Edit the NAE Object Name and Description values as required.

Figure 18: NAE Focus tab (Basic)

| III System | | > | < |
|--|----------------------|--|-----|
| <u>I</u> tem <u>E</u> dit <u>V</u> iew <u>A</u> ction I <u>n</u> sert <u>T</u> ools <u>Q</u> uer | <u>H</u> elp | Last Login: Thu 05/26/2022 08:47:04 CDT Met*** Logout Ex | at |
| 企 | 88 | PrevReIN50-3 🖺 🗆 🛛 | ø |
| All Items | | Operational Alarm | |
| PrevReIN50-3 | Focus Summary Diag | gnostic Network Email SNMP Syslog Alarm Trend | |
| BACnet Protocol Eng | Edit | 🖲 Basic 🔵 Advanc | ced |
| SC Network Port | Attribute | Value | |
| | Object | | |
| 💼 Energy | Name | PrevReIN50-3 | |
| Programming | Description | | |
| 🚞 Schedule | Object Type | Device | |
| ি∺" 🔚 🛛 Field Bus MSTP1 | Authorization Catego | ry General | |
| | Model Name | MS-NAE5521-3 | |
| | Time | | |
| | Local Time | 09:22:00 AM (HH:MM:SS AM/PM) | |
| | Local Date | Thursday, May 26, 2022 | |
| | Time Zone | (UTC-06:00) Central Time (US & Canada) | |
| 8 | | Server: 5/26/2022, 09:22 AM (| CDT |

- 3. Click Save.
- 4. Select the **Advanced** option and click **Edit.**

| System | | — C |) X |
|--|--------------------------|--|-------------|
| <u>I</u> tem <u>E</u> dit <u>V</u> iew <u>A</u> ction I <u>n</u> sert <u>T</u> ools <u>Q</u> uer | y <u>H</u> elp | Last Login: Thu 05/26/2022 08:47:04 CDT Met*** | ıt Exit |
| 企 | 89 | PrevReIN50-3 | 8000 |
| All Items | | Operational Alarm | |
| | Focus Summary Diagnostic | Network Email SNMP Syslog Alarm Tren | d |
| BACnet Protocol Eng | Save Cancel | 🔾 Basic 🧕 | Advanced |
| SC Network Port | Attribute | Value | U |
| - Dpdate | Object | | |
| Energy | Name | PrevReIN50-3 | |
| Programming | Description | | |
| Schedule | Object Type | Device | |
| 🗄 📲 Field Bus MSTP1 | Authorization Category | General | - |
| | Model Name | MS-NAE5521-3 | _ |
| | Time | | |
| | Local Time | 09:23 AM | (H |
| | Local Date | Thursday, May 26, 2022 | |
| | Time Zone | (UTC-06:00) Central Time (US & Canada) | - |
| | Engineering Values | | _ |
| | Firmware Version | 12.0.0.2063 | _ |
| | Staged Firmware Version | | |
| | , Staged Files | | _ |
| | Item Reference | Test123:PrevReIN50-3 | |
| | Version | 37.0 | |
| | BIOS Version | | |
| | OS Version | 10.17.41.24 | |
| | Archive Date | Thursday, May 26, 2022 | |
| | Max Message Buffer | 994 | byt |
| | Max APDU Length | 1024 | byt |
| | APDU Segment Timeout | 10000 | ms |
| | APDU Timeout | 10000 | ms |
| | APDU Retries | 4 | |
| | Internode Comm Timer | 120 | |
| | Graphic Association | | |
| | Graphic | Object Name: | |
| | | Beference: | |
| | Craphic Alias | Neierence. | |
| | Alarme | | |
| | Alarm Papasiton/ Siza | 1000 | Ent |
| | Alarm Spoore Time | 5 | mi |
| | Fuent Action When Full | Pollover | |
| | Event Action when Full | | 1 |
| | Ack Forward Enable | False | - I |
| L | Audit Trail | | |
| × | | Server: 5/26/2022, 09 | 9:23 AM CDT |

Figure 19: NAE Focus Tab - Advanced Edit Mode

 Edit the advanced attribute values as needed. (Refer to the NAE Device Object Help and Audit Trails Help in the Metasys Site Management Portal Help (LIT-1201793) for guidance.)
 If the NAE is on a site with an ADS/ADX, enter the ADS/ADX's IP address in Local Site Director field in the Site section of this screen. The NAE thereafter reports to the ADS/ADX as its Site Director.

Entering NAE network parameters

The NAE Computer Name and Domain Name on the Network tab identify the NAE on the network so it can be found by other computers. In many commissioning scenarios, you can use the initial Computer Name to commission the NAE. See Computer name for more information.

In most site configuration scenarios, you configure many of the Metasys network values in the NAE UI by downloading a pre-built archive database from the SCT to the commissioned NAE. The download from SCT overwrites the initial Computer Name with the new value for the Metasys network.

(i) **Note:** If you are building the NAE database online, you must establish the production network NAE Computer Name value before you establish references to objects on the NAE. After creating object references, changing the Computer Name value breaks all object references to local objects on the site.

- ➤ Important: The NAE Update Tool places restrictions on the host name (Computer Name) values that you can use for an NAE. Names must start with a letter or number, and must end with either a letter or a number, and may contain dashes only in the interior of the name. Refer to the NAE Update Tool Help (LIT-12011524) for more information on host name restrictions.
- 1. In the Site Management Portal UI, display the NAE device object, click the **Network** tab, and then click **Edit**.

| 💷 System | | - 🗆 X |
|---|----------------------------------|---|
| Item Edit View Action Insert Tools Quer | / <u>H</u> elp Last Login: Thu 0 | 5/26/2022 10:10:06 CDT Met*** Logout Exit |
| 企 | Prev R | ReIN50-3 🔒 🗆 🖉 |
| All Items | Opera | tional Alarm |
| 🗆 🕼 Site | Focus | Summary |
| User Views | Diagnostic Network Email | SNMP Syslog Alarm Trend |
| Summary Definitions | Save Cancel | |
| | Attribute | Value Units |
| | Network Identification | |
| | Computer Name | PrevReIN50-3 |
| | Domain Name | |
| | Completion Domains | Listof[1] - cg.na.jci.com 💌 📖 |
| | Ethernet MAC Address | 74:FE:48:0C:A6:9E |
| | Allow Http | True |
| | LAN | |
| | DHCP Enabled | True 👻 |
| | JCI IP Address | 172 21 13 19 |
| | IP Mask | 255 .255 .255 .0 |
| | IP Router Address | Listof[1] - 172.21.13.1 💌 |
| | Obtain DNS address automatically | True |
| | DNS server IP addresses | Listof[3] |
| | BACnet Communication | |
| | IP Communication Mode | Ethernet IP Only Mode |
| | Operational Certificate Status | Struct 💌 |
| | BACnet Routing | |
| | Routing Mode | Disabled 👻 |
| | BACnet Integrated Objects | Include in Object List |
| No. 1 | ₽ | Server: 5/30/2022, 07:36 AM CDT |

Figure 20: NAE Network Tab - Edit Mode

- 2. In the Network Identification section, type the Computer Name value.
- 3. Enter the Network Identification and LAN attribute values as needed and click **Save**.
- (i) **Note:** If you are setting up an NAE to dial out to an ADS/ADX.

Creating email alarm and event notifications and destinations in SMP UI at Release 11.0 and earlier

Important: LCS85 email configuration is no longer available with the SMP UI at Release 12.0.

A network engine can be set up to generate custom alarm and event email messages and send the messages to one or more specified email destinations.

- (i) **Note:** In most scenarios, we recommend that you set up the Email DDA and configure the email notifications and the notification destinations after the network engine is configured with an archive database that includes the user database.
- 1. In the Site Management Portal UI, display the network engine device object, click the **Email** tab, and then click **Edit**. (See the top half of the Display panel in Figure 21.)
- 2. Enter the Shared Configuration values according to Table 14. These fields establish values for attributes that are common to all email alarm notifications generated from this network engine. Refer to *Alarm and Event Management* in *Metasys Site Management Portal Help (LIT-1201793)* for additional information on setting the attribute values for alarm and event notifications.
- 3. Scroll down to the Destinations section of the Email tab.
- 4. Click **New**. The Email Destinations Configuration edit section appears.

| 🗾 System | | | | - 0 | × |
|--|--------------------------|--------------------|---------------------------|--|-----------|
| Item Edit View Action Insert Tools Query | <u>H</u> elp | | | Last Login: Thu 05/26/2022 08:47:04 CDT Met*** | Exit |
| 企 | A A | | PrevReIN50-3 | | |
| All Itoms | | | Operational Alarm | | |
| | Focus Summary Diagnostic | Network Email SNMP | Syslog Alarm Trend | | |
| | | | 1,1113 | | |
| Eth IP Datal ink | Save Cancel | | | | |
| SC Network Port | | 1 | 1 | | |
| | Attribute | Value | Units | | |
| Energy | Shared Configuration | | | | - |
| Programming | Email Enabled | True | | | |
| - Schedule | SMTP Server Host | 0.0.0.0 | | | |
| ⊞ Field Bus MSTP1 | SMTP Port | 25 | | | |
| | Authentication Type | None | | | |
| | SMTP User Name | ***** | | | |
| | SMTP Password | *** | | | |
| | POP Server Hostname | | | | • |
| | Destinations | New Delete | Attribute | Value | |
| | Destination 1 | | Destination Configuration | Value | |
| | | | Label | Destination 1 | |
| | | | Email Address | bill@ici.com | |
| | | | | | |
| | | | | | |
| | | | Priority | Normal | |
| | | | Subject | | |
| | | | Retries | 3 | |
| | | | Enabled | True | |
| | | | Event Filters | Item Operator Value | |
| | | | | Start Time >= 12:00:00 Al | |
| | | 1 | | | |
| | | | | End Time <= V 12.00.00 Ar Delete | |
| | | ſ | | Start Day Of W >= Monday 🔽 | |
| | | | Format | Priority | |
| | | | | ✓ Message | |
| | | | | ✓ Value | |
| | | | | Site Name | |
| | | | | | |
| | | | | Ren Description | |
| | | | | rem Fully Qualified Reference | |
| | | | | Authorization Category | |
| | | | | Acknowledge Required | |
| | | | | Previous Status | - |
| | <u>.</u> | | | Conver-5/06/0000_00/ | |
| | | | | Server: 5/26/2022, 09:2 | 28 AM CDT |

Figure 21: Network engine Email Configuration - Edit Mode

5. Enter the Destination values according to Table 14. (Refer to the *Alarm and Events Management* section in the *Metasys Site Management Portal Help (LIT-1201793)* for additional information on setting the attribute values for alarm and event notifications.)

| Table 14: Shared Attribut | es for All Email Destinations | |
|---------------------------|-------------------------------|--|
| | - | |

| Attribute | Description (Value Requirement/Range) | Initial Value |
|---------------------|---|----------------------|
| SMTP Server Host | Specifies the SMTP server name that handles | Fully qualified host |
| | outgoing email. (Required Value) | name |
| SMTP Port | Specifies the TCP port that the server uses to 25 | |
| | deliver email message. (Required Value/1 to | |
| | 25) | |
| Authentication Type | Specifies the Authentication Type the | None |
| | network engine uses to log in to the | |
| | outgoing email server. Select SMTP, POP | |
| | before SMTP, or None. | |
| SMTP User Name | Specifies the user name the network engine | - |
| | uses to log in to the SMTP server that | |
| | handles outgoing email messages. (Required | |
| | only if SMTP is selected for Authentication | |
| | Type.) | |
| SMTP Password | Specifies the password the network engine | - |
| | uses to log in to the SMTP server that | |
| | handles outgoing email messages. (Required | |
| | only if SMTP is selected for Authentication | |
| | Type.) | |
| POP Server Hostname | Specifies the POP server name for incoming | - |
| | email messages. (Required only if the email | |
| | server requires POP before SMTP, before | |
| | it accepts email messages from client. If | |
| | this field is left blank, POP before SMTP is | |
| | disabled.) | |
| POP User name | Specifies the POP user name. (Required only | Maximum 20 |
| | if POP Authentication is required and there is | characters |
| | a value specified for POP server host.) | |
| POP Password | Specifies the POP Password. (Required only if | Maximum 20 |
| | POP Authentication is required and there is a | characters |
| | value specified for POP server host.) | |
| From Email Address | Specifies a valid email address that is | Email address |
| | recognized and exists on the SMTP Server. | |
| | (Required Value) | |

| Attribute | Description (Value Requirement/Range) | Initial Value |
|--------------------|---|---------------|
| SSL Email Enabled | When True, emails are sent over an SSL- | False |
| | encrypted connection if the server supports | |
| | encryption with StartTLS. When this | |
| | parameter is set to True, emails are not | |
| | sent if they cannot be encrypted, regardless | |
| | of the SSL Email Ignoring Errors attribute | |
| | setting. | |
| SSL Email Ignoring | When True, the email is sent even if the | False |
| Errors | email server certificate appears to be invalid. | |
| | When False, the email is sent only if the | |
| | operating system can verify that the server | |
| | sent a valid SSL certificate. This feature is | |
| | only enabled if SSL Email Enabled is True. | |
| | In Note: Make sure that proper certificate revocation, such as Online Certificate Status Protocol (OCSP) stapling, is enabled and configured. For more information about OCSP configuration, refer to https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-ocsp/5792b4c4-c6ba-439a-9c2a-52867d12fb66 . | |
| Email Diagnostics | Displays diagnostic information regarding | - |
| | the communication between the Email | |
| | DDA (SMTP Client) and the SMTP Server. | |
| | This attribute displays both successful and | |
| | unsuccessful email message deliveries. | |

Table 14: Shared Attributes for All Email Destinations

Table 15: Attributes for Specific Email Destinations and Notifications

| Attribute | Description (Value Requirement/Range) | Initial Value |
|---------------|---|---------------|
| Label | Specifies a name for the email destination (for | - |
| | example, John Doe). | |
| Email Address | Specifies the destination email addresses (for | - |
| | example, john.doe@jci.com). (Required Value) | |
| Priority | Specifies the email message priority (High, | Normal |
| | low, or normal). | |
| Subject | Contains the body text of the email message. | - |
| | (Maximum of 256 characters.) | |
| Retries | Specifies the number of attempts at sending | 3 |
| | the email message. (0–10 Retries) | |
| Enabled | Enables or disables Email Destination. (True, | True |
| | False) | |

| Attribute | Description (Value Requirement/Range) | Initial Value |
|-----------|--|---------------|
| Filters | Enables you to specify the rules that filter | - |
| | alarm and event notifications. Each filter has | |
| | an Item, Operator, and Value. | |
| Format | Enables some predefined format | - |
| | characteristics of the notifications that are | |
| | sent to a destination. Predefined format | |
| | characteristics include: | |
| | Notification Priority | |
| | Notification Message (content) | |
| | • Value | |
| | • Site Name | |
| | Item Description | |
| | Item Fully Qualified Reference | |
| | Item Category | |
| | Acknowledge Required | |
| | Previous Status | |
| | (Enable a format by selecting the check box next to the format.) | |

Table 15: Attributes for Specific Email Destinations and Notifications

6. Click **New** to the right of Destination Email Addresses. The Email Import dialog box appears. Import user names and the associated email addresses from the list of user names for the site. (Refer to the *Metasys*® *SMP Help* [*LIT-1201793*] for more information.)

Figure 22: Import Email Addresses Dialog Box

| Metasys - Email Addresses | × |
|---|--|
| Select and/or enter the desired destinat create the email address string for the | tion email addresses. Click OK to email DDA (maximum 256 characters). |
| Metasys User Addresses John Smith (Admin@jci.com) Metasys System Agent (Admin@jci.com) Metasys Basic System Agent (AdminBasi- Jane Smith (Jane.Smith@jci.com) Metasys System Operator (Operator@jc | Destination Email Addresses Metasys User Addresses Metasys System Agent (Admin@jci.com) Metasys System Operator (Operator@j) Metasys Basic System Agent (AdminBas) Additional User Addresses Mary.Smith@jci.com Mike.Jones@jci.com John.Jones@jci.com |
| Current Calculated Length: 106 | Remove Remove All |
| Ok Cancel | |

7. To filter the email messages that are sent to a destination, click **New** next to the Filters section of the Email Destination Configuration tab. The Add Filter dialog box appears.

Figure 23: Add Filter Dialog Box

| Add Filter | | × |
|------------|----------------------|---|
| Item | Acknowledge Required | - |
| Operator | == | - |
| Value | True | - |
| | OK Cancel | |

- 8. Select the Item, Operator, and Value (from the drop-down lists) for the condition that you want to trigger the email notification. (Refer to *Event Message Routing, Filtering, and Destinations* in the *Metasys*® *SMP Help* [*LIT-1201793*] for additional information on filters.)
- 9. Click **OK**.

- 10. Enable the Format characteristics for email notifications sent to the specified destinations by selecting the check boxes next to the Format characteristic.
- 11. Add additional email destinations with filters and formats as required.
- 12. Click Save.

Configuring encrypted email

By default, Metasys software encrypts your user name and password as they are entered into the SMP UI, but the software does not automatically encrypt email messages. This feature allows embedded and server machines to send email to email servers over a secure channel (secure socket layer [SSL]). The entire email payload is encrypted, and allows our software to communicate to email servers that require SSL connections.

Consider these points when using email encryption:

- The SMTP port is different when using secure socket layer connections. This port is typically 465.
- Server-class machines and embedded devices do not have the same list of trusted Certificate Authorities. An embedded device may not trust a certificate that is trusted on a server-class machine. To increase the chances of an embedded device trusting a certificate used by a server-class machine, have the certificate signed by a major authority.
- To maximize efficiency when using this feature, set up mailing groups instead of individual users in the destination field to minimize the number of users to which the machine has to send email. This setup allows you to create different email groups and customize the type of messages that each user receives.
- To increase the chance of an embedded device or an ADS/ADX trusting the certificate the mail server uses, ensure the signed certificate is obtained by a major certificate authority.
- If you are using an embedded device as your site director, no option is available to update the Trusted Certificate Authority list at this time.
- To ensure you have the latest list of Trusted Certificate Authorities installed on your ADS/ADX, install any available certificate updates from Microsoft Windows Update.

You can configure encrypted email in three ways:

- Configuring encrypted email with no authentication required
- Configuring encrypted email with SMTP authentication
- Configuring encrypted email with POP-before-SMTP authentication

Configuring encrypted email with no authentication required

About this task:

- (i) **Note:** Encrypted Email with No Authentication Required functions only when Anonymous Authentication is enabled on the mail server.
 - 1. View a network engine.
 - 2. Click the **Email** tab.
 - 3. Click **Edit**.
 - 4. Edit the Attributes in the Shared Configuration as shown in Table 16.

Table 16: Attributes for No Authentication Required

| Attribute | Selection |
|---------------------------|---------------------------------------|
| SMTP Server Host | mail.yourdomain.com or yourdomain.com |
| SMTP Port | 465 |
| Authentication Type | None |
| SSL Email Enabled | True |
| SSL Email Ignoring Errors | False |

5. Verify that the email was sent correctly.

Configuring encrypted email with SMTP authentication

- 1. View a network engine.
- 2. Click the **Email** tab.
- 3. Click Edit.
- 4. Edit the Attributes in the Shared Configuration as shown in Table 17.

Table 17: Attributes for SMTP Authentication

| Attribute | Selection |
|---------------------------|---------------------------------------|
| SMTP Server Host | mail.yourdomain.com or yourdomain.com |
| SMTP Port | 465 |
| Authentication Type | SMTP |
| SSL Email Enabled | True |
| SSL Email Ignoring Errors | False |

5. Verify that the email was sent correctly.

Configuring encrypted email with POP-before-SMTP authentication

About this task:

(i) Note:

When SSL Email is enabled and you use POP-before-SMTP Authentication, the Metasys system uses port 995 to communicate to the mail server. Ensure that the mail server you are connecting to uses port 995 for secure socket layer connections for POP3 access.

When SSL Email is not enabled and you use POP-before-SMTP Authentication, the Metasys system uses port 110 to communicate to the mail server. Ensure that the mail server you are connecting to uses port 110 for non-encrypted POP3 access.

- 1. View a network engine or device.
- 2. Click the **Email** tab.
- 3. Click Edit.
- 4. Edit the Attributes in the Shared Configuration as shown in Table 18.

Table 18: Attributes for POP-Before-SMTP Authentication

| Attribute Selection | |
|---------------------|---------------------------------------|
| SMTP Server Host | mail.yourdomain.com or yourdomain.com |
| SMTP Port | 465 |
| Authentication Type | POP-before-SMTP |

Table 18: Attributes for POP-Before-SMTP Authentication

| Attribute | Selection |
|---------------------------|--------------------------------------|
| POP Server Hostname | yourdomain.com or pop.yourdomain.com |
| SSL Email Enabled | True |
| SSL Email Ignoring Errors | False |

5. Verify that the email was sent successfully.

Creating NAE SNMP alarm notifications and destinations

You can set up an NAE to generate and deliver alarm and event messages on a network using SNMP network monitoring.

You can typically use SNMP monitoring for large BAS networks with many network devices. Alarm notifications are sent to and stored on an SNMP management computer that monitors all devices on the network.

You must set up SNMP monitoring at the network level and an SNMP management device must be assigned on the network. If you are applying a Metasys system to any existing network, consult with the network administrator or IT department that administers the building network to determine if SNMP monitoring is available on the network.

- (i) **Note:** In most scenarios, we recommend that you set up the SNMP DDA and configure the SNMP notifications and the notification destinations after an NAE is configured with an archive database that includes the user database.
- 1. In the Site Management Portal UI, display the NAE device object and click the **SNMP** tab.
- 2. Click Edit. The SNMP Configuration Edit screen appears (Figure 24).

Figure 24: NAE SNMP configuration tab - Edit mode

| III System | | | | - | - 🗆 X |
|--|--|------------------------------|---|--|--------------------|
| Item Edit View Action Insert Tools Query | / <u>H</u> elp | | | Last Login: Thu 05/26/2022 08:47:04 CDT Met*** | Logout Exit |
| û | 00 | | PrevReIN50-3 | | ê o a 🖗 |
| All Items PrevReIN50-3 BACnet Protocol Eng Eth IP DataLink | Focus Summary Diagnostic 1 Save Cancel | Network Email SNMP | Operational Alarm Syslog Alarm Trend | | |
| SC Network Port | Attribute Shared Configuration SNMP Enabled SNMP Trap Version SNMP Management Device SNMP Request Port Contact Person Destinations New | Value False V1 V1 Delete | Units | | |
| × | | | | Server: 5/26/ | 2022, 09:28 AM CDT |

- 3. In the Shared Configuration section, set SNMP Enabled value to True if your network application uses SNMP monitoring.
- 4. Type the IP address or host name values of the SNMP Management device (computer).
- 5. In the Read Only Community and Read/Write Community fields, enter the community string used by the ENMS to retrieve data from objects maintained by managed devices (Table 19).

| Attribute | Description (Value Requirement/Range) | Initial Value |
|-------------------|--|---------------|
| SNMP Enabled | Enables or disables SNMP DDA on the NAE. (True, | False |
| | False) | |
| SNMP Trap Version | Specifies the version of SNMP used on the network SNMP Versi | |
| | on which the NAE resides. (Not required if SNMP | 1 |
| | Enabled is set to False) | |
| SNMP Management | Specifies the IP address or host name of the SNMP | - |
| Device | Management device on the network on which the | |
| | NAE resides. The direction of communication is from | |
| | the SNMP Management device to the NAE. Currently, | |
| | this function is not supported on the NAE85. (Not | |
| | required if SNMP Enabled is set to False) | |
| SNMP Request Port | Specifies the port on the SNMP server where SNMP | 161 |
| | notifications are sent. (Not required if SNMP Enabled | |
| | is set to False) | |
| Contact Person | Specifies the contact person for the SNMP | - |
| | notifications. (Not required if SNMP Enabled is set to | |
| | False) | |
| Public Community | Specifies the community name used by the NMS | public |
| Name | to modify data in objects maintained by managed | |
| | devices. (Not required if SNMP Enabled is set to | |
| | False) | |
| SNMP Trap Message | Specifies the format used to generate SNMP | String Based |
| Format | notifications. Change to MIB Based when SNMP | |
| | management application uses the Metasys MIB file to | |
| | translate SNMP notifications. (Not required if SNMP | |
| | Enabled is set to False) | |

Table 19: Shared Attributes for SNMP Destination

6. Click **New** in the Destinations section. The Destination Configuration edit screen appears (Figure 25).

| Item Edit View Action Insert Tools Query Help Last Login: Thu 05/26/2022 08:47:04 CDT Met*** Logout Image: Control Cont | Exit |
|---|--------|
| Best PrevReIN50-3 Best All Items Operational Alarm Best | |
| All Items Operational Alarm | |
| | () |
| PrevReIN50-3 Focus Summary Diagnostic Network Email SNMP Syslog Alarm Trend | |
| BACnet Protocol Eng bth IP DataLink Save Cancel | |
| SC Network Port | |
| Date Update Shared Configuration | |
| Programming SNMP Enabled False V | |
| Schedule SNMP Trap Version V1 V | |
| E-B Field Bus MSTP1 SNMP Management Device 0.0.0.0 | |
| SNMP Request Port 161 | |
| Contact Person | - |
| | |
| Atribute Value Units | |
| Uestination 1 Uestination Destination 1 | |
| Trao Community Name Dublic | |
| IP Address 0.0.0.0 | |
| Destination Port Number 162 | |
| Enabled True 👻 | |
| Event Filters Item Operator Value | |
| New | |
| Delete | |
| | |
| Format | |
| romat Priority | |
| , ₩ Message | |
| Value | - |
| Server 5/26/2022 09:3 | AM CDT |

Figure 25: SNMP Destination Configuration Tab - Edit Mode

7. Enter the Destination information for the SNMP trap (Table 20).

Table 20: Attributes for Specific SNMP Notifications

| Attribute | Description (Value Requirement/Range) | Initial Value |
|------------------|---|---------------|
| Label | Specifies a functional name for the destination | Destination # |
| | SNMP server. (Maximum 20 characters) | |
| Trap Community | Specifies the SNMP Community Name used | Public |
| Name | by the Network Management System (NMS) | |
| | group to listen to the traps. (Maximum 20 | |
| | characters) | |
| IP Address | Specifies the IP Address of the NMS system | 0.0.0.0 |
| | that receives the trap messages. | |
| Destination Port | Specifies the port on the SNMP Management | 162 |
| Number | device that receives messages from the NAE | |
| | (typically Port Number 162). The direction of | |
| | communication is from the NAE to the SNMP | |
| | Management device. | |
| Enabled | Enables or disables the SNMP destination. | True |

| Attribute | Description (Value Requirement/Range) | Initial Value |
|-----------|--|---------------|
| Filters | Enables you to specify the rules that filter | - |
| | alarm and event notifications. Each filter has | |
| | an item, operator, and value. | |
| Format | Allows you to enable some predefined format | - |
| | characteristics of the notifications that are | |
| | sent to a destination. Predefined format | |
| | characteristics include: | |
| | Notification Priority | |
| | Notification Message (content) | |
| | • Value | |
| | Site Name | |
| | Item Description | |
| | Item Fully Qualified Reference | |
| | • Item Category | |
| | Acknowledge Required | |
| | Previous Status | |
| | (Enable a format by selecting the check box next to the format.) | |

Table 20: Attributes for Specific SNMP Notifications

8. Click **Save** when finished.

Enabling Syslog reporting

An NAE can be set up to generate custom alarm and event email messages and send the messages to one or more specified email destinations.

- 1. In the Site Management Portal UI, display the NAE device object and click the **Syslog** tab.
- 2. Click **Edit**. The Shared Configuration section of the Syslog tab appears.

| System | | | | - 0 | × |
|--|---|--|---|----------------|--------|
| Item Edit ⊻iew Action I <u>n</u> sert <u>T</u> ools <u>Q</u> ue | ry ∐elp | | Last Login: Thu 05/26/2022 08:47:04 CDT Met** | * Logout | Exit |
| ŵ | 69 | PrevReIN50 | 0-3 | A (| 300 |
| All Items ProvReIN50-3 BACnet Protocol Eng Sc Network Port Update Energy Programming Schedule Field Bus MSTP1 | Focus Summary Diagnostic Network Er Save Cancel Attribute Value Ur Shared Configuration Syslog Reporting Enabled True | Operational mail SNMP Syslog Alarm | Alarm | | |
| | Destinations New Delete | Attribute Destination Configuration Label Syslog Server UDP Send Port UDP Receive Port Event Filters | Value Syslog 1 0.0.0 514 514 Acknowledge == * True * Current Status == * High Warning * Delete Item Operator Value New Delete | | |
| ▼ | | | Server: 5/3 | 26/2022, 09:30 | AM CDT |

Figure 26: NAE Syslog Configuration - Edit Mode

- 3. Click the **down** arrow for the Syslog Reporting Enabled attribute and select **True**.
- 4. In the Destinations section, click **New**. The Destination Configuration edit fields appear.
- 5. Enter the Destination Configuration values according to the following table.

Table 21: Attributes for Specific Syslog Destinations

| Attribute | Description (Value Requirement/Range) | |
|------------------|---|--|
| Label | Specifies a name for the Syslog server (for example, Syslog1). | |
| Syslog Server | Specifies the IP address or resolvable host name of the Syslog | |
| | server that is configured to receive events and audits from the NAE. | |
| UDP Send Port | Specifies the Syslog port that is used to send messages to an NAE. | |
| UDP Receive Port | Specifies the Syslog port that is used to receive messages from an | |
| | NAE. | |
| Event Filters | Specifies the rules for filtering the alarms and events that are sent | |
| | to the Syslog server. Each filter has an Item, Operator, and Value. | |
| Audit Filters | Specifies the rules for filtering the audit messages that are sent to | |
| | the Syslog server. Each filter has an Item, Operator, and Value. | |

6. In the Event Filters section, click **New**. The Add Filter dialog box appears.

Figure 27: Add Filter Dialog Box: Events

| Add Filter | × |
|------------|----------------|
| Item | Current Status |
| Operator | == |
| Value | Normal |
| | OK Cancel |

- 7. Select the item, operator, and value of the condition that you want to trigger a message to the Syslog server.
- 8. Add any additional event filters as desired.
- 9. In the Event Filters section, click **New**. The Add Filter dialog box appears.

Figure 28: Add Filter Dialog Box: Audits

| Add Filter | × |
|------------|-----------|
| Item | Item |
| Operator | == |
| Value | |
| | OK Cancel |

- 10. Select the item, operator, and value of the condition that you want to trigger a message to the Syslog server.
- 11. Add any additional audit filters as desired.
- 12. Add additional Syslog destinations and filters as desired.
- 13. Click OK.
- 14. Click Save.

Setting the time, date, time zone, and time synchronization

How you set the time zone, date, and time on an NAE depends on how the NAE fits into the Metasys site hierarchy. See Appendix: Time Zone, Date, and Time Management for information and detailed procedures on setting time zone, date, and time on an NAE and on a Metasys network.

Setting up NAE alarm parameters

NAEs ship from the factory with several pre-configured default diagnostic alarms that monitor the NAE hardware. You can edit these default alarm settings or create new alarms for the NAE hardware.

You can also create new alarms and edit existing alarms for supported field devices on the NAE field trunks.

Editing existing alarm parameters

- 1. In the Site Management Portal UI, select and drag the desired NAE object or field device object from the Navigation panel and drop it in the Display panel. The NAE or field device Focus screen opens.
- 2. Click the Alarm tab. The Alarm Configuration screen opens (Figure 29).

Figure 29: NAE Alarm Configuration Tab

| System | | | – 🗆 × |
|--|---|---|--|
| Item Edit View Action Insert Tools Quer | y <u>H</u> elp | | Last Login: Thu 05/26/2022 08:47:04 CDT Met*** Logout Exit |
| 金 | 69 | PrevReIN50-3 | ° <u>`</u> □ ⊠ Ø |
| All Items | Fogue Summon Disgonatio N | Operational Alarm | |
| PrevReIN50-3 BACnet Protocol Eng BACnet Protocol Eng SC Network Port Update Programming Schedule Field Bus MSTP1 | Select tem(s): CPU Usage Alarm Event Rate Alarm Sample Rate Alarm Edit Attribute Reference | Value | New Delete |
| | Name Description Object Type Present Value Input Alarm State Event Enable Report Delay Active Report Delay Status | Event Rate Alarm Analog Alarm Normal 0.00 per hour True False 0 seconds | |
| | Enabled Reliability Time Date Error Log Alarm/Warning Thresholds High Alarm Limit High Warning Limit Cooling Setpoint Heating Setpoint | True Reliable Unspecified Struct 200.00 per hour | |
| 8 | | | Server: 5/26/2022, 09:32 AM CDT |

- 3. Select items in the **Select Item(s)** list to edit existing alarms. (To create new alarms, see Creating new alarms.)
- 4. Click **Edit** and make changes to the desired Attributes for the NAE or field device.
- 5. Click **Save** to save the edited alarm settings.

Creating new alarms

About this task:

You can create new alarms for the NAE or any of the supported field devices on the field trunks attached to the NAE.

1. Select and drag the desired NAE or field device object from the Navigation panel into the Display panel. The NAE or field device object Focus screen opens.

2. Select the **Alarm** tab and the device's Alarm screen opens. Click **New** and the Insert Alarm Wizard opens (Figure 30).

Figure 30: Insert Alarm Wizard

| 🔝 Insert Alarm Wizard | | | | | | |
|--------------------------------|--|--|--|--|--|--|
| Start Select Attribute | Select Attribute | | | | | |
| Configure Summary Finish | Memory Usage Alarm {Alarm} Battery Condition Alarm {Alarm} Board Temperature Alarm {Alarm} Memory Usage Trend I og {Trend} | | | | | |
| | Attribute: Present Value other | | | | | |
| | Cancel A Back Next Last | | | | | |

- 3. Select the device Attribute for which you want to create an alarm.
- 4. Follow the Wizard instructions and create or edit the values for the Attribute for which you want to create an alarm.
- 5. Click **Save** when you have finished creating the desired alarm parameters for the device Attribute.

Designating an NAE as a child of a Site Director

About this task:

All NAEs have a Site object and therefore are Site Directors by default. To designate the Site Director on a new site, you must demote all the NAEs on the site that are not designated as the Site Director. You must reset an NAE when it is demoted. Also, if the NAE is at Release 10.0 or later, you must pair the NAE to its Site Director.

In many Metasys network site commissioning and configuration scenarios, the Site Director status of the NAE on the site is built into the archive database for the site. The status of these devices is established on the NAE when the archive database is downloaded from the SCT to the site devices. The SCT database download overwrites the existing values in the NAE.

(1) **Note:** If a Metasys Server is on a site, an NAE cannot be the Site Director.

Designating an NAE as Site Director is typically done offline in the SCT but can be done online in the NAE UI. The procedure in this section describes how to designate an NAE as the Site Director online in the NAE UI. To do so with the SCT, go to the Changing Site Director with the SCT section.

③ Note: If you do the site promotion or demotion online, you may lose any navigation trees built for the site. If User Views (navigation trees) have already been built, upload them to the SCT, establish the Site Director, and then download the navigation trees back to the source devices. The Site Director and NAE Computer Name values in the NAE UI must match the values in the SCT archive database.

To demote an NAE and designate its Site Director, complete the following steps:

- 1. On the Navigation panel, select the NAE that you wish to demote from Site Director.
- 2. Drag the NAE into the Display panel to open the Focus tab.
- 3. Select the **Advanced** option.
- 4. Click **Edit**. The Focus edit screen appears (Figure 31).
- 5. Scroll down to the Site attributes and select the Local Site Director field.

Figure 31: Designating the Site Director

| System | | | | – 🗆 X |
|---|-------------------------------------|-------------------------------|------------------------------------|---------------------------------|
| Item Edit View Action Insert Tools Quer | y <u>H</u> elp | | Last Login: Thu 05/26/2022 08:47:0 | 04 CDT Met*** Logout Exit |
| 企 | | PrevReIN50-3 | | |
| All Items | | Operational Alarm | | |
| | Focus Summary Diagnostic Network | Email SNMP Syslog Alarm Trend | | |
| BACnet Protocol Eng | Save Cancel | | | O Basic Advanced |
| SC Network Port | Attribute Audit Action when Full | Value Rollover | Units | |
| Energy | Audit Generate Alarm When Full | True | 7 | |
| Programming | Enabled Audit Level | 2 | | |
| Schedule | Power Management | | | |
| 🗄 📲 Field Bus MSTP1 | Power Sampling Interval | 1 | seconds | |
| | Power Consecutive Samples | 5 | | |
| | Weekly Scheduling | | | Ξ. |
| | JCI Exception Schedule | Auto Delete 31 days | | - |
| | Site | | | |
| | Site Director Online | True | | |
| | Authenticated with Site | True | | |
| | Local Site Director | 172.21.13.25 | | |
| | ADS Repository | 0.0.0.0 | | |
| | ADS Connection Type | LAN | | |
| | ADS Delivery Time | 12:15 AM | (HH:MM AM/PM) | |
| | BACnet | | | |
| | Object Name | PrevReIN50-3 | | |
| | User Name Is BACnet Obj Name | False | - | |
| | Device Object Identifier | 1 | | |
| | System Status | Operational | | |
| | Configured Network Number | 1001 | | |
| | BACnet UDP Port | 47808 | | |
| | Process Id List | Listof[0] | | |
| L | <u> </u> | (- · | 7 | |
| × | | | 9 | Server: 5/26/2022, 09:33 AM CDT |

- 6. Type the host name or IP address of the NAE or ADS/ADX that you want to designate as the local Site Director.
- 7. Click **Save**. A confirmation message box appears (Figure 32).

Figure 32: Confirmation for Demoting Site Director



- 8. If you wish to proceed, click **OK** to this confirmation message; otherwise, click **Cancel**.
- 9. Depending on the type and release level of the network engine, either the engine that you are demoting logs you out and resets, or prompts for the user credentials of the Local Site Director you specified.
 - If the engine reboots, wait several minutes for the reset to complete, then log on the Site Director. The navigation tree shows the network engine is now a child of the Site Director.
 - If the engine prompts you, enter the administrator's user name and password of the Site Director, then click **OK**. If the credentials you entered are correct, the NAE logs you out and resets. Wait several minutes for the NAE to reset, then log on the Site Director. The navigation tree shows the NAE is now a child of the Site Director, and the NAE is paired with its Site Director. If the credentials you entered are incorrect, a dialog box appears to report a failed connection. Click **OK** and try to log in again.

Changing Site Director with the SCT

About this task:

- **Note:** If you have already changed the Site Director and downloaded the site, go to Moving security database and clearing it from demoted Site Director prior to Release 6.0 or Moving security database and clearing it from demoted Site Director Release 6.0 or later.
 - 1. Start the SCT, open the archive database for the site, and choose the new Site Director from the available list in the Site Director attribute of the Site object.
 - 2. Perform a download to update all devices. During the download process, pair all Release 10.0 or later network engines with the Site Director. For more information about device pairing in SCT, refer to *Metasys SCT Help (LIT-12011964)*.

Removing user accounts from a demoted Site Director

If you demote a supervisory controller or ADS/ADX from a Site Director to a child device on the site, all user accounts that you added to the device while it was a Site Director remain in the security database. If you determine that user accounts on the demoted site should be removed after the demotion has occurred, you must move the security database and clear it from the demoted Site Director. If the demoted Site Director is at a Metasys release prior to 6.0, follow the instructions in Moving security database and clearing it from demoted Site Director prior to Release 6.0. If the
demoted Site Director is at Release 6.0 or later, follow the instructions in Moving security database and clearing it from demoted Site Director Release 6.0 or later.

Moving security database and clearing it from demoted Site Director prior to Release 6.0

- 1. Create a backup of the Security database of the demoted device, but only if you are using the same set of users on the new or existing Site Director.
- 2. Create a backup of the Security database from one of the devices (Metasys Server or network engine) on the site that has never been a Site Director and has never had a Site Director's Security database restored to it (in other words, has a clean Security database with only the default user accounts).
- 3. Restore the clean copy of the Security database that you created in Step 2 to the device that was demoted from the Site Director.
- 4. If you are using the Security database of the demoted device on the new Site Director, restore the Security database that you backed up in Step 1 to the new or existing Site Director.
- Create a backup of the Security database from the device that was demoted and restored with a clean database in Step 3.
 This step ensures that the device Security database in the SCT matches the clean Security you restored to the device in Step 3.

Moving security database and clearing it from demoted Site Director Release 6.0 or later

About this task:

- (i) **Note:** Starting at Release 6.0, the security database backup is performed as part of the SCT upload, regardless of whether or not the supervisory controller or ADS/ADX is a Site Director.
 - 1. In the SCT, go to **Tools > Security Copy**
 - (1) **Note:** If the security database does not exist, it means the controller has never been accessed from the Site Management Portal and uploaded to the SCT to verify that a security database exists for the demoted supervisory controller. This database is the security backup that was originally used by the Site Director.

If the security database does not exist, go to Step 2. If the security database does exist, go to Step 5.

- 2. Log in to the demoted controller from the Site Management Portal.
- 3. Change your password when prompted at the login.
 - (i) **Note:** Changing your password creates the security database automatically the next time the SCT database is uploaded.
- 4. Perform an SCT upload. Once the upload is complete, click **Tools > Security Copy** in SCT.
- 5. In the Security Copy Wizard, do one or both of the following:
 - to verify that a security database exists for the demoted. If the Security database of the demoted Supervisory device is required on the new Site Director, perform a security copy to the Site Director by selecting the Supervisory device that contains the correct security database.
 - If you do not want to use the Site Director Security database on the demoted Supervisory device, perform a security copy by selecting a Supervisory device that has never had users added to the Security database and copy to the demoted Supervisory device.

6. Perform an SCT upload for all Supervisory devices that have had their Security databases changed. This upload ensures that the security database backup is synchronized with the Supervisory device.

Enabling and disabling Warning Banner

- (i) **Note:** If the warning banner for a network engine's Site Director is set to appear, the selected warning banner also appears when users log in to that network engine. Therefore, you only need to follow these steps when the network engine is a Site Director.
- 1. In the Site Management Portal UI, display the NAE Site object, click the **Site View** tab, and then click **Edit**.
- 2. Scroll to the bottom of the window to locate the Warning Banner attribute.

Figure 33: Enabling and Selecting the Warning Banner - Network Engine Example

| 國 System | | | – 🗆 X |
|--|---------------------------------------|--|---------------------------|
| Item Edit View Action Insert Tools Query | <u>H</u> elp | Last Login: Thu 05/26/2022 10:05:57 CD1 | Met*** Logout Exit |
| 企 | | Site | |
| All Items | | Normal | |
| | Site View Authorization Categories Cu | stom Enumerations | |
| User Views | Save Cancel | | 🔵 Basic 💿 Advanced |
| | Attribute | Value | Units |
| | Multicast IIL | 1 | 🔺 |
| I II. | Multicast Heartbeat Interval | 5 | minutes |
| | Online Detection | | |
| | Poll Rate | Fast | |
| | Operational Data | | |
| I II. | All Items Update In Progress | False | |
| | Online Archive Transfer In Progress | False | |
| I II. | Enum Set Memory Used | 0 | % |
| | Remaining Custom Sets | 256 | |
| | Remaining Auto Sets | | |
| | Site Security Level | Encrypted Only | |
| | Certificate Renewal Period | 60 | days |
| I II | Advanced Security Enabled | True | |
| I II | BACnet | | |
| | BACnet Site | False | |
| | BACnet Encoding Type | [ISO 10646 (UTF-8) | |
| | Third party BBMDs | Listof[0] | |
| | DNS Refresh Period | 20 | minutes |
| I II | Graphic Association | | |
| | Graphic | Object Name: | |
| I II | | Reference: | |
| | Graphic Alias | | |
| | Warning Banner | | |
| | Warning Banner | None | • |
| × | None | | 6 |
| | U.S. Department o | f Defense (DoD) Warning Banner | |
| | U.S. Department o | f Transportation (DOT) Federal Aviation Administra | tion (FAA) Warning Banner |

3. Select a banner type from the Warning Banner drop-down box. For a small-capacity engine, only the DoD warning banner is available, so select **True** for the Warning Banner attribute. For a large-capacity engine, you can select from three different warning banners: U.S. Department of Defense (DoD), U.S. (General Services Administration (GSA)), or U.S. Department of Transportation (DOT) Federal Aviation Administration (FAA). **None** is selected by default.

- 4. Click **Save**. The banner change takes from 3 to 5 minutes to become effective at the network engine.
- (1) **Note:** If you want to disable the Warning Banner in the future, go back to this screen, select **False** or **None**, and save the change.

Adjusting NAE network sensitivity

About this task:

Follow the steps in this section to adjust the network sensitivity of the BACnet/IP and MS/TP field bus networks for a network engine. By increasing the number of seconds the network engine waits before flagging a field device as offline, you can minimize the number of false offline reports. Three different sensitivity options, each with a different set of values, are available: high, medium, and low. The default setting for all network engines upgraded to Release 11.0 or later is medium.

The following are the three sensitivity range options and why you might choose them:

- High Sensitivity: for critical applications or customer requirements for faster status updates
- Medium Sensitivity (default): for a system that is not showing any signs of offline cycling
- Low Sensitivity: for a system that is showing chronic occurrences of offline cycling
- (i) **Note:** If you adjust the communication parameters to low sensitivity, keep in mind the following possible effects:
 - Causes any outgoing confirmed messages to queue up for retries during the time when a remote device has stopped responding, but has not yet been detected as offline. For supervisory devices that are low on free memory, memory may become exhausted over time, which may cause the supervisory device to restart.
 - For an integrated General BACnet device, increases the possibility of missing a device restart. This scenario increases the chances of losing change of value (COV) subscriptions at remote devices for significant periods of time. In addition, commanded values might also be in unwanted states longer than normal.
 - For an integrated Johnson Controls-family device, increases the possibility that a slight delay may occur before a device restart is detected, causing extra time needed to recover COV subscriptions and commanded values. Detection of the restart event is guaranteed, but old data is present longer than normal.

Do not specify an **APDU Timeout** or **APDU Segment Timeout** value that is higher than 30000 ms, even though the system allows higher values.

Before you begin, verify that the engine is set to run in Expert Mode so that all attributes you need to adjust are available. For details, see Enabling Expert mode. Also, select the Advanced view for all attribute windows.

(i) **Note:** Be consistent with the sensitivity adjustments. For example, if you select low sensitivity, make sure you use the low sensitivity values for all items.

Follow these steps to adjust the sensitivity values:

1. Open the Focus window for the **network engine** that you want to adjust. Enter new values for the sensitivity range that you selected using the values listed in Table 22. Figure 34 shows an example.

| Attribute | High Sensitivity | Medium Sensitivity | Low Sensitivity |
|--------------|------------------|--------------------|-----------------|
| APDU Segment | 4000 ms | 10000 ms | 20000 ms |
| Timeout | | | |
| APDU Timeout | 6000 ms | 10000 ms | 20000 ms |

Table 22: Supervisory Device Network Settings

| Attribute | High Sensitivity | Medium Sensitivity | Low Sensitivity |
|---|------------------|--------------------|-----------------|
| APDU Retries | 4 | 4 | 5 |
| Internode Comm | 20 seconds | 120 seconds | 240 seconds |
| Timer | | | |
| Note: Older FxC controllers have a supervi- sory status mod- ule that times out unless the Internode Comm Timer is set to high sensitivity. | | | |

Table 22: Supervisory Device Network Settings

Figure 34: Example: Supervisory Device Network Settings

| PrevReIN50-3 | | | | | 60 | 🛛 🖉 | | | | |
|---------------------------------|------------------------|------------|---------|-----------|-----|-----|--------|-------|-------|---|
| | | | Operat | ional Al | arm | | | | | |
| Focus | Summary | Diagnostic | Network | Email | SNI | MP | Syslog | Alarm | Trend | |
| Edit | Edit O Basic Advanced | | | | | | | | | |
| Attri | bute | | | Value | | | | | | |
| Max Message Buffer 994 bytes | | | | | | | | | | |
| N | lax APDU Len | gth | | 1024 byte | s | | | | | |
| A | PDU Segmer | nt Timeout | | 10000 ms | 5 | | | | | |
| A | PDU Timeout | 1 | | 10000 ms | 5 | | | | | |
| A | PDU Retries | | | 4 | | | | | | |
| Ir | nternode Com | ım Timer | | 120 | | | | | | - |
| Server: 5/26/2022, 09:38 AM CDT | | | | | | | | | | |

- 2. Click Save.
- 3. Open the Snapshot Focus window for the **BACnet Protocol Eng** integration of the network engine that you want to adjust. Enter the Poll Delay for the sensitivity range that you selected using the value listed in Table 23. Figure 35 shows an example.

Table 23: BACnet Protocol Eng Network Settings

| Attribute | High Sensitivity | Medium Sensitivity | Low Sensitivity |
|------------|------------------|--------------------|-----------------|
| Poll Delay | 20 seconds | 60 seconds | 120 seconds |

Figure 35: Example: BACnet Protocol Eng Network Settings

| 💷 System | | | - 🗆 X |
|---|---|------------------------------|---------------------------------|
| Item Edit View Action Insert Tools Quer | y <u>H</u> elp | Last Login: Thu 05/26/2022 1 | 0:08:02 CDT Met*** Logout Exit |
| <u>命</u> | 00 | BACnet Protocol Eng | ê o 🛛 🥙 |
| All Items Site User Views | Focus Diagnostic Save Cancel | Normal | 🔵 Basic 💿 Advanced |
| Summary Definitions | Attribute Object | Value | Units |
| Eth IP DataLink SC Network Port | Name Description Object Type | BACnet Protocol Eng BACPE | |
| Energy Programming Schedule | Authorization Category Engineering Values | General | _ |
| È 🔁 Field Bus MSTP1 | Version Communication | 1.0 | 9 |
| | Poll Delay | 60 | Source 5/26/2022 40:44 AU ODT |
| | | | Server: 5/26/2022, 10:11 AM CDT |

- 4. Click Save.
- 5. Open the Snapshot Focus window for the **BACnet IP** integration of the network engine that you want to adjust. Enter new values for the sensitivity range that you selected using the values listed in Table 24. Figure 36 shows an example.

| Attribute | High Sensitivity | Medium Sensitivity | Low Sensitivity |
|----------------|------------------|--------------------|-----------------|
| APDU Segment | 8000 ms | 11000 ms | 20000 ms |
| Timeout | | | |
| APDU Timeout | 6000 ms | 12000 ms | 20000 ms |
| APDU Retries | 3 | 4 | 5 |
| Internode Comm | 30 seconds | 120 seconds | 240 seconds |
| Timer | | | |

Table 24: BACnet IP Network Settings

Figure 36: Example: BACnet IP Network Settings

| ← → BACnet IP | |
|------------------------------------|-------------------|
| Norma | l |
| Focus Engineering Diagnostic Summa | ry Snapshot Focus |
| Save Cancel | |
| Attribute | Value . |
| APDU Segment Timeout | 10000 🌥 |
| APDU Timeout | 10000 |
| APDU Retries | 4 |
| Max APDU Length | 480 |
| COV Threshold | 10 |
| Internode Comm Timer | 120 |
| COV Count | 0 |
| Peak COV Count | 0 |
| Peak COV Cache Count | 0 |
| | |

- 6. Click Save.
- 7. Open the Snapshot Focus window for the integration of the network engine that you want to adjust. Enter new values for the sensitivity range that you selected using the values listed in Table 25. Figure 37 shows an example.

| Attribute | High Sensitivity | Medium Sensitivity | Low Sensitivity |
|----------------|------------------|--------------------|-----------------|
| APDU Segment | 6000 ms | 12000 ms | 30000 ms |
| Timeout | | | |
| APDU Timeout | 8000 ms | 11000 ms | 29000 ms |
| APDU Retries | 3 | 3 | 5 |
| Internode Comm | 30 seconds | 120 seconds | 240 seconds |
| Timer | | | |

Table 25: Field Bus MS/TP Network Settings

| 💷 System | | - 🗆 X |
|---|---------------------------------------|---|
| Item Edit View Action Insert Tools Quer | Help Last Login: Thu 05 | 5/26/2022 09:45:29 CDT Met*** Logout Exit |
| 企 | Field Bus N | 1STP1 🔒 🗆 🖉 |
| All Items | Norm | al |
| 🖃 🛄 PrevReIN50-3 | Focus Engineering Diagnostic Hardware | Summary |
| BACnet Protocol Eng | Save Cancel | 🔵 Basic 💿 Advanced |
| SC Network Port | Attribute | Value |
| <mark>R</mark> Update | Alarm State | Normal |
| Energy | Communication | |
| Programming | Max Manager | 127 |
| Field Bus MSTP1 | Max Info Frames | 20 |
| | JCI Network Port APDU Timeout | 12000 ms |
| | JCI Network Port APDU Segment Timeout | 11000 ms |
| | JCI Network Port APDU Retries | 3 |
| | Periodic Update | 20 se |
| | Page Size | 1000 |
| | Poll Delay | ms |
| | Count | 2 |
| | Synchronize Time | True |
| | Synchronize Time Zone | True |
| | Discover All As General BACnet Device | False |
| | Requested Vendor ID | |
| | Internode Comm Timer | 120 |
| 8 | | Server: 5/26/2022, 09:50 AM CD1 |

Figure 37: Example: Field Bus MSTP Network Settings

- 8. Click Save.
- 9. Restart the network engine to put these new settings into effect.

Replacing an NAE

About this task:

To replace an NAE on a network site, update the site registration to ensure that devices on the site communicate with the new (replacement) engine; otherwise, devices may attempt to communicate with the network engine that was removed from the site.

If you do not remove the NAE from a site correctly, the Site Director may attempt to send messages to the old NAE, creating unnecessary network traffic.

If the NAE's trend data is stored in an ADS repository, forward the data prior to beginning the upgrade by following these steps for each engine:

- 1. Select a supervisory engine in the Navigation tree.
- 2. Select Action > Commands. A list of available commands appears.
- 3. Select Archive, then click Send. The archived trend data is sent to the ADS/ADX.

To replace the NAE:

1. Using the SCT, upload the current copy of the NAE database.

- 2. Physically replace the old NAE with the new NAE, connect the new NAE to the network, and power on the new NAE.
- 3. Do one of the following:
 - Configure the NAE with the same host name and IP address of the old NAE from the Site Management Portal.
 - (i) **Note:** This configuration lets you download the database with SCT without using the Device Change option.
 - Verify that the SCT can communicate with the NAE, then select the Device Change option when downloading the database with SCT to identify the Site Director and host name of the new NAE.
- 4. Download the existing NAE archive database to the new NAE.

Enabling Expert mode

About this task:

Follow the steps in this section to enable Expert mode in the SMP UI for a Metasys Server or network engine. Expert mode is required if you want to adjust the network sensitivity of the BACnet/IP and MS/TP field bus networks for a network engine (see Adjusting NAE network sensitivity). The Expert mode options are available to you under the Expert tab of Metasys Preferences. Expert mode is also required to enable web service logging and to view memory usage on the status bar.

- Start Windows File Explorer and verify that file extensions appear. If file extensions are hidden, click Tools > Folder Options and under the View tab, remove the check box for Hide extensions for known file types.
- With Windows File Explorer, navigate to the folder called C:\Users\<user>
 \JohnsonControls.Metasys, where <user> is the name of the user who is currently logged in to the computer.
- 3. Create a new text file called **MetasysExpertPreferences.xml** under this folder. Make sure that you are saving the file to the C:\Users\<user>\JohnsonControls.Metasys folder. If the file is already present, skip to the next step.
- 4. Log on the Metasys SMP. Click **Tools** > **Configure Preferences** to open the Metasys Preferences window. The Expert tab is now visible.
- 5. Click the Expert tab and set **Show Internal items and views** to True. Click **OK** to apply the change and close the window.
- 6. Refresh the SMP UI window to allow the Snapshot Focus windows to appear.

Troubleshooting

This section describes the most common problems you may encounter when you set up and operate NAEs. Use the general solution guidelines and procedure references in this section to avoid or resolve these problems. Table 26 provides a list of common NAE problems and their solutions.

This section is not a troubleshooting guide for Metasys system networks, customer networks, BAS networks, or the field devices connected to the NAE.

Field device troubleshooting is covered in the field device documentation. Refer to the appropriate field device documentation for additional information.

(i) **Note:** To effectively troubleshoot an NAE, it may be necessary to isolate the NAE from the Ethernet network and the associated field trunks and field devices, and then direct-connect to the NAE with a computer to browse the Site Management Portal UI.

Common NAE problems

See the following sections and Table 26 when you encounter a problem with an NAE.

Corrupted NAE memory

Corruption of nonvolatile NAE flash memory may render an NAE inoperable. Flash memory may become corrupted for a variety of reasons and is one of the most common NAE problems encountered when commissioning, configuring, updating, and operating the NAE.

A typical method to recover from corrupted NAE flash memory includes reloading the NAE disk image and downloading the NAE archive database with a compatible version of the SCT. Refer to the *NAE Update Tool Help (LIT-12011524)* for information on installing the NAE disk image. Refer to the *SCT: System Configuration Tool Help (LIT-12011964)* for information on upgrading NAE archive databases.

NAE disk image update and archive download related problems

NAE flash memory commonly becomes corrupted when an NAE disk image update or archive download is interrupted. To avoid memory corruption and data loss, follow the procedure for disk image updates and archive downloads carefully, and allow the NAE to complete the update and download without interruption.

Update and upgrade related problems may also occur when the SCT software, NAE software, and the NAE archive databases are of incompatible versions. When you update the NAE disk image, you must update the NAE archive database to match the new software version. The SCT application used to configure a *Metasys* or NAE must also be of the same software version as the NAE software.

Refer to the *NAE Update Tool Help (LIT-12011524)* and see the Related documentation section of this document for additional information on disk image updates and archive upgrades and downloads.

Data protection battery related problems

Improper shipping, handling, installing, charging, or disconnecting of the NAE data protection battery may also result in flash memory corruption and data loss.

To avoid problems related to the data protection battery, refer to the *Setup and Adjustment* sections in the appropriate network engine installation instructions for proper procedures for connecting, charging, and disconnecting the data protection battery before you connect supply power to the NAE. These instructions include:

- NCE25 Installation Instructions (Part No. 24-10143-63)
- NAE35/NAE45 Installation Instructions (Part No. 24-10050-6)
- NAE55/NIE55 Installation Instructions (Part No. 24-10051-43)
- NIE29 Installation Instructions (Part No. 24-10143-594)
- NIE39/NIE49 Installation Instructions (Part No. 24-10050-103)
- NIE59 Installation Instructions (Part No. 24-10143-608)

Data protection battery testing procedure

Use this procedure to test the integrity of the battery in the NxE55 network engine. The life expectancy of the 12 VDC battery installed in the NxE55 is 3 to 5 years. The battery monitoring circuit of the NxE55 does not load test the battery. If the battery fails to maintain a proper voltage level during a power loss, the NxE55 may not be able to complete a normal shutdown and unarchived data could be lost. Therefore, periodically field test each battery or replace a battery that is well beyond its life expectancy, even if a battery fault condition does not exist. As a best practice, establish a regular maintenance schedule to check the batteries of all NxE55s currently in service.

Follow these steps to test the sealed 12 VDC battery used on NxE55s. (This procedure does not apply to the N40-class network engines, including the NCE25, NAE35, and NAE45.) To perform the test, you need to remove the battery from the network engine and assemble the parts listed here. Test leads are required to connect the 7.5 ohm resistor to the battery.

Parts required:

- 7.5 ohm, 25 watt resistor (Ohmite® part number D25K7R5) or equivalent
- Jumper wire test leads (22 or 24 gauge)
- DC voltmeter
- Stopwatch or other time source

Follow these steps:

- 1. Verify the battery you want to test is fully charged.
- 2. Connect the 7.5 ohm load across the battery.
- 3. Wait 60 seconds, then record the voltage across the battery terminals (not across the load resistor).
- 4. Wait another 60 seconds and again record the voltage across the battery terminals.
- 5. Remove the load from the battery.
- 6. Subtract the voltage reading taken in **Step 4** from the voltage reading taken in **Step 3**. This is your difference reading.
 - If the difference reading is **less than or equal to** 0.25 VDC, the battery is good. Reinstall the battery.
 - If the difference reading is **greater than** 0.25 volts, the battery is no longer effective. Replace the battery.

Login problems

Login problems may occur when the user name or password is incorrectly entered at login. If the default user name and password fail, the initial values may have been changed by an administratorlevel user. You need the designated user name and password to log in to an NAE. If the passwords for all NAE users are forgotten, you need to reimage the network engine, which is similar to the factory reset of a smartphone.

Whenever you change the Security System database for a small-capacity network engine with Release 8.0 or later (NxE35, NxE45, or NxE25), you must issue the **Reset Device** command to ensure that the security database is archived to non-volatile memory. This step **is not** required for large-capacity engines (NxE55s). If you do not perform this step for a network engine that has a poor or dead battery, and that engine loses power, the latest changes to the Security System database are lost.

As a last resort, you can also reload the NAE with the NAE/NIE Update Tool, but that process deletes the archive database. For details, refer to the *NAE Update Tool Help (LIT-12011524*).

Network connection related problems

Many network connection and communication problems result from incorrect device names, incorrect IP addresses, or other attribute value errors entered into the Site Management Portal UI or into the UI of the associated network devices. If the NAE attribute values do not match the values entered in the devices connected to the NAE, the NAE and associated devices may not establish network connections or communications.

Check the device names, IP addresses, gateway, subnet masks, ports, baud rates, and other network parameters in the Site Management Portal UI. Also check the servers, computers, and field

devices connected to the NAE, and ensure that the attribute values are correct for each computer or device.

For example, communication between a Site Director and an NAE could be lost after downloading the network engine with SCT. This may occur on a network where device name resolution is not implemented. To resolve this communication issue, log in to the NAE after the download and change the Local Site Director field back to the IP address of the Site Director. Within minutes after you save this change, the engine comes back online to the Site Director.

See Determining the NAE IP address and device name for a network connection and Verifying Ethernet network communications (Ping).

NAE reset related problems

Certain setting changes initiated in the Site Management Portal UI do not take effect until the NAE is reset. Reset the NAE whenever you are prompted, and allow the NAE to complete the reset sequence before you try to log on. See Reset command device.

Troubleshooting guide

Table 26 provides information for troubleshooting an NAE, hereafter referred to generically as the network engine.

| Problem | Solution |
|---|--|
| The network engine does not operate when powered on (and | Corrupted flash memory or data loss are the most common causes of this problem. To resolve this problem: |
| the POWER LED is on). | If the unit has a data protection battery, ensure that the battery is connected and charged. For more information on handling, installing, and charging the data protection battery, refer to the NAE55 Installation Guide (Part No. 24-10051-43). |
| | 2. Ensure that the database does not exceed the network engine flash memory capacity. |
| | Reload the disk image and download the archive database to the network engine while the network engine is disconnected from the network. |
| The network engine does not operate after updating the disk | Corrupted flash memory and data loss are the most common causes of this problem. To resolve this problem: |
| image, downloading an archive database, or installing a patch. | Ensure that the database does not exceed the network engine flash memory capacity. Reload the disk image and download the archive database to the network engine while the network engine is disconnected from the network. |
| Only the host name or the IP address of the network engine changes, even though you changed both attributes. | In some instances, you need to make each change in separate steps. To resolve, change the host name first, reboot, then change the IP address. This scenario can occur if the network engine is placed online to a network that does not have an active DHCP server. |

| Table | 26: | Trouble | shooting | the | Network | Engine |
|-------|-----|---------|----------|-----|---------|--------|
| | | | | | | |

| Table | 26: | Troubleshooting | the Network | Engine |
|-------|-----|-----------------|-------------|--------|
|-------|-----|-----------------|-------------|--------|

| Problem | Solution | | | |
|-----------------------------------|--|--|--|--|
| The network engine does not | Specify the domain of the Site Director in the completion | | | |
| come online or populate in the | domain list of the network engine. Locate this attribute in the | | | |
| Server or the network engine Site | SMP OF under the engine's Network tab. | | | |
| Director. | If a network engine is either offline in the Site Director | | | |
| | the engine manually with the Pair Device with Site Director | | | |
| | command at the engine. Or, try SCT to manually pair the | | | |
| | engine. Then, save the configuration by uploading the affected | | | |
| | network engine and the Site Director. | | | |
| | Use the IP address of the Site Director in the Local Site | | | |
| | Director attribute instead of the host name. This attribute is | | | |
| | located under the engine's Focus tab. | | | |
| | If a network engine is not paired as indicated by the blue icon | | | |
| | use the Pair Device with Site Director command at the | | | |
| | Site Director to manually pair the engine. Then, upload the | | | |
| | impacted network engine and the Site Director to the SCT | | | |
| | archive to save the configuration. | | | |
| | From the Metasys server, try to ping the network engine by its | | | |
| | IP address or host name. If the ping request does not return | | | |
| | connections | | | |
| The network engine does not | Check to make sure that 24 VAC power is connected correctly | | | |
| communicate with any other | and that the 24 VAC and POWER LEDs are on. | | | |
| device. | Check to make sure that communication terminal blocks and | | | |
| | other communication connectors are firmly in place. | | | |
| | Check that the wiring is the correct size (18 AWG minimum | | | |
| | for power, 18 AWG for N2 Bus, 26 AWG for Ethernet | | | |
| | communication). | | | |
| | Check that you have set the correct baud rate on each | | | |
| | Chark the integrity of the wires and cables | | | |
| | Check the integrity of the wires and cables. | | | |
| | Check that NZ EOL Switches are correct. Refer to the Setting | | | |
| | Bulletin (LIT-636018) for details on N2 EOL terminations. | | | |
| N2 communication (on devices | Check that the N2 wires are connected properly and are not | | | |
| that support the N2 Bus protocol) | loose in the termination block. | | | |
| is not present | Check that the N2 LEDs indicate communication. | | | |
| | Check that the N2 EOL switches are correctly set. Refer to the | | | |
| | Setting Terminations section of the N2 Communications Bus | | | |
| | <i>Technical Bulletin (LIT-636018)</i> for details on N2 terminations. | | | |
| | Check the entire N2 Bus. Refer to <i>the N2 Communications Bus</i> | | | |
| | Technical Bulletin (LIT-636018). | | | |

| Table 2 | 26: Tro | oublesho | ooting | the | Network | Engine |
|---------|---------|----------|--------|-----|---------|--------|
|---------|---------|----------|--------|-----|---------|--------|

| Problem | Solution | | | |
|---|---|--|--|--|
| LonWorks communication | Check that the LonWorks network wires are connected | | | |
| (on devices that support the | properly and are not loose in the termination block. | | | |
| LonWorks protocol) is not present | connect the <i>Metasys</i> system Connectivity to LonWorks network Tool, the COM.PRO Tool, or a third-party LonWorks network configuration tool to the LonWorks network. Verify that it is possible to communicate with the devices on the network including the network engine. If communication is good, verify that the network engine database has been generated correctly and that the LonWorks enabled device data corresponds to the devices installed. If the network engine does not respond, verify that the network engine has been correctly installed in the LonWorks network database and that the network configuration image has been sent to the network engine. If the network engine cannot be installed, replace the network engine. Refer to the <i>LonWorks</i> ® <i>Network Integration with Network Engines and LCS Technical</i> <i>Bulletin (LIT-1201668)</i> for network engine database generation information. | | | |
| | Check the entire LonWorks network. Refer to the LonMark Guidelines - Physical Layer for details (<u>http://</u> <u>www.lonmark.org</u>). | | | |
| The network engine is showing no Ethernet communication. | Verify that you are using a patch cable for a hub or switch and a crossover cable for a single computer connection. | | | |
| | Check the port and cable integrity. Make sure that either the 10/Link, 100/Link, or 100/1000 Link LED is green or yellow (indicating an established Ethernet connection; 1000 Mbps Ethernet connection is yellow). Check that the hub or switch into which the LAN connector is plugged works and is connected correctly. | | | |
| The network engine is showing no modem communication | Beginning at Release 9.0.7, network engines no longer support modem communication. | | | |
| The USR 5637 modem connects, but garbled characters appear and eventually communication drops. The network engine does not dial in or dial out | | | | |
| | Charles to make own the batter is installed which the batter | | | |
| The network engine loses data. | Check to make sure the battery is installed and that the BATT FAULT LED is not lit. Replace, if necessary, with appropriate replacement battery. Periodically load-test the battery. The battery protection circuit in the network engine does not load test the battery, so data loss can occur even if the battery fault LED is not illuminated. | | | |
| | Do not unnecessarily press the system RE-BOOT switch. | | | |

| Problem | Solution | | | |
|---|--|--|--|--|
| The network engine runs slowly. | The amount of data you are trying to process is too much for the network engine to handle. A value of 50% or less for the CPU Usage attribute of the network engine is considered acceptable, although other performance indicators should also be assessed. Refer to the <i>SCT: System Configuration Tool</i> <i>Help (LIT-12011964)</i> or <i>Metasys Site Management Portal Help</i> <i>(LIT-1201793)</i> system for more information. Reduce the size of the database. | | | |
| The network engine is generating high CPU alarms. | Programming objects (LCT, Signal Select, Global Data) referencing analog objects with small COV values (0.5%) are the most common cause of this problem. To determine the source of the high CPU usage, follow these steps: | | | |
| | Add a Trend extension to the Last Idle Sample of the network engine. This attribute is the inverted instantaneous CPU Usage. For example, if this number is low (5%), then the CPU usage is high (95%). The CPU usage is an average over a 15–30 minute period. Locate programming objects (Control System objects [LCT] or Signal Select) that reference objects with small COV increments and disable them one at a time. Monitor the Last Idle Sample value after disabling the object. Within 30 seconds, the Last Idle Sample should significantly increase if that object was a contributing factor to the high CPU usage. When the problem object is determined, then either manually or with Mass Edit Live, update the COV increment to a larger value before re-enabling the programming object. | | | |
| All network and bus communication is disrupted. | Check for possible external interference. To reduce RF interference, do not use cell phones or handheld transceivers within 3 meters (10 feet) of the network engine. | | | |
| | Check that the power transformer secondary is not shared with another load. | | | |
| The network engine overheats. | When the internal temperature reaches the high limit, the network engine issues an alarm and lights the GENL FAULT or FAULT LED, allowing you a chance to intervene before heat- related damage results. | | | |
| | Check that the unit has been installed according to the installation instructions and that the mounting orientation is correct. | | | |
| | Make sure cables are not blocking the ventilation of the unit. | | | |
| | Clean out the dust in the unit with canned air (pressurized air used to clean computers and other sensitive devices). | | | |
| The internal modem no longer functions. | Beginning at Release 9.0.7, network engines no longer support modem communication. | | | |

| Table 26 | : Trouble | shooting | the | Network | Engine |
|----------|-----------|----------|-----|---------|--------|
|----------|-----------|----------|-----|---------|--------|

| Problem | Solution |
|--|--|
| The unit has been damaged or all external causes of failure have been checked. | Replace the network engine. |
| The following message appears in the Focus window for a network engine: Item Not Found | The network engine has become unpaired with the Site Director. This issue may occur after you set the Advanced Security Enabled option under the Site Director's Site object to True. To resolve, use the Tools > Pair NxE with Site Director option to force network engine pairing. If this action does not restore communication, either restart the Metasys Server or the network engine that has not paired. |
| During the process of replacing an NAE with an SNE, you successfully downloaded the SNE with SCT, but an NAE pairing error occurs with the status of: Unable to Login Or, you try to manually pair the engine to the Site Director, but you get the error: Unable to communicate with | When you migrate an NAE to an SNE, the SNE can get stuck into a bad pairing state. This happens when you turn power off from the NAE, but you do not remove that engine from the site's archive database. If you leave the device object in the site's database, and you add a new engine with the same name or IP address, the pairing process with the Site Director fails. To resolve, promote the SNE to Site Director status, allow the engine to reset, then demote the SNE as a child device to the Site Director. The pairing process between the Site Director and its child SNE anging should now work |

NAE diagnostic tools

The NAE hardware and UI provide tools for diagnosing and troubleshooting hardware and software problems with the NAE.

The primary NAE diagnostic tools include:

- LED status indicators
- Diagnostic tab
- Summary tab
- a serial point monitor

Other tools are also available, such as the SNMP Trap Browser and the ping command for determining the NAE IP address and the ability to communicate on the TCP/IP network. See Determining the NAE IP address and device name for a network connection and Troubleshooting procedures for information on using the Trap Browser and the ping command.

NAE LED status indicators

Figure 38, Figure 39, and Figure 40 show the location and designation of the NCE25, NAE35, NAE45, and NAE55 LEDs that indicate the status of the engines. Some models do not have all the LEDs shown in these figures. Table 27 describes their Normal Status and Function.

Figure 38: NCE25 LED Status Indicators



Figure 39: NAE35/NAE45 LED Status Indicators



Figure 40: NAE55 LED Status Indicators



| LED Label (Color) | NAE Series | Normal Status | Descriptions/Other Conditions |
|----------------------------------|-------------------------------|------------------|--|
| POWER (Green) | NCE25, NAE35, NAE45, NAE55 | On Steady | On Steady = Unit is getting power from either the battery or 24 VAC power. Also see the 24 VAC LED. Off Steady = Unit is shut down. |
| ETHERNET (Green) | NCE25, NAE35, NAE45, NAE55 | Flicker | Flicker = Data is transferring on the Ethernet connection. Ethernet traffic is general traffic (may not be for the NAE). Off Steady = No Ethernet traffic, probably indicates a dead Ethernet network or bad Ethernet connection. |
| 10/LINK (Green) | NCE25, NAE35, NAE45, NAE55 | On Steady | On Steady = Ethernet connection is established at 10 Mb/s. |
| 100/LINK (Green) | | On Steady | On Steady = Ethernet connection is established at 100 Mb/s |
| 100/1000 Link (Green/ Yellow) | | On Steady | On Steady (Green) = Ethernet connection is established at 100 Mb/s. On Steady (Yellow) = Ethernet connection is established at 1,000 Mb/s. |
| FCA (Green) | | Flicker | On Steady = Controllers are defined to FC A (Trunk 1) in the NAE55, but none are communicating. (NAE55 transmitting only) Flicker = Normal communications; FC A port is transmitting and receiving data. Flickers are generally in sync with data transmission but should not be used to indicate specific transmission times. Also, the flicker rate for the MS/TP bus is different from the rate for the N2 Bus. Off Steady = No controllers are defined to FC A (FC Bus 1 or N2 Trunk 1) in the NAE55. |

| LED Label (Color) | NAE Series | Normal | Descriptions/Other Conditions |
|----------------------------|-------------------------------|-----------------------------|---|
| | | Status | |
| FCB (Green) | NAE55 | Flicker | On Steady = Controllers are defined to FC B (Trunk 2) in the NAE55, but none are communicating. (NAE55 transmitting only) Flicker = Normal communications; FC B port is transmitting and receiving data. Flickers are generally in sync with data transmission but should not be used to indicate specific transmission times. Also, the flicker rate for the MS/TP bus is different from the rate for the N2 Bus.CR83936 Off Steady = No controllers are defined to FC B (FC Bus 2 or N2 Trunk 2) in the NAE55. |
| FC BUS or LON ¹ | NCE25, NAE35, NAE45 | | Flicker = N2 controllers are defined to FC BUS in the NAE35/45, but none are communicating. (NAE35/45 transmitting only) Fast Flicker (may appear Steady on) = Normal communications; FC BUS port is transmitting and receiving data. Flickers are generally in sync with data transmission but do not indicate specific transmission times. Off Steady = No field controllers are defined to FC BUS in the NAE35/45. |
| SA BUS (Green) | NCE25 | Blinking | Blinking - 5 Hz = Data Transmission (normal communication) Off Steady = No Data Transmission On Steady = Communication lost, waiting to join communication ring |
| PEER COMM (Green) | NCE25, NAE35, NAE45, NAE55 | Varies (see next column) | Flicker = Data traffic between NAE devices. For an NAE that is not a Site Director, this LED indicates regular heartbeat communications with the Site Director. For a Site Director NAE, flashes are more frequent and indicate heartbeat communications from all other NAE devices on the site. For a single NAE on a network without an ADS/ADX, there is no flicker. |

| LED Label (Color) | NAE Series | Normal Status | Descriptions/Other Conditions |
|-----------------------|-------------------------------|------------------|---|
| RUN (Green) | NCE25, NAE35, NAE45, NAE55 | On Steady | On Steady = NAE software is running. On 1 second, Off 1 second = NAE software is in startup mode. On 0.5 seconds, Off 0.5 seconds = NAE software is shutting down. Off Steady = Operating system is shutting down or software is not running. |
| 24 VAC (Green) | NAE55 | On Steady | On Steady = 24 VAC power present Off Steady = Loss of 24 VAC power. In the Off Steady condition, the NAE may be running on battery power. Also see the POWER LED. |
| MODEM RX ² | NCE25, NAE35, NAE45 | Flicker | Flicker indicates modem is connected and receiving data. |
| MODEM TX ² | NCE25, NAE35, NAE45 | Flicker | Flicker indicates modem is connected and transmitting data. |

| LED Label (Color) | NAE Series | Normal | Descriptions/Other Conditions |
|---------------------------|-------------------------------|------------|---|
| | | Status | |
| BATT FAULT (Red) | NCE25, NAE35, NAE45, NAE55 | Off Steady | Off Steady = Normal operation. On Steady = Battery fault. Replace the battery. Battery not connected or cannot be charged. The BATT FAULT LED may remain On for up to 24 hours after initially powering on the NAE. If the BATT FAULT LED remains on longer than 48 hours after initially powering on the NAE, check the battery connection or replace the battery. |
| GENL FAULT or FAULT (Red) | NCE25, NAE35, NAE45, NAE55 | Off Steady | Off Steady = Normal operation. On Steady = General Fault. Fault conditions are user configured in software. Pre-configured fault conditions include excessive CPU use, flash or memory use, excessive CPU or PWB temperature, or battery fault. In normal operation, the GENL FAULT LED stays on steady for the first half of the startup sequence. Blink - 2 Hz = Download or Startup in progress, not ready for normal operation. Blink Rapidly - 5 Hz = One or more defined SA Bus devices are offline. Check SA Bus devices for problems, including low batteries on wireless sensor. Note: On NCE25 and NAE35/45 models, the GENL FAULT LED label designation is FAULT. |

1 LED labeled FC BUS on models that support MS/TP Bus or N2 Bus, and labeled LON on models that support LonWorks network.

Modem LEDs are only on NCE25 models with internal modems. Modem functionality not supported at Release 9.0.7 or later.

NCE25 LED startup sequence

About this task:

During startup, the NCE25 automatically initiates an LED test to verify the operational status of the LEDs. Immediately after connecting supply power, the following LED lighting sequence occurs:

- 1. The POWER, BATT FAULT, 10 LINK, FAULT, RUN, and PEER COM LEDs turn on, indicating that the OS is starting up. (After 2 seconds, the LEDs may change states depending on site-specific network activity.)
- 2. The BATT FAULT, PEER COM, and FAULT LEDs shut off. The RUN LED flashes to indicate that the NCE software is loading.

 The LEDs display the operational status of the NCE. When the RUN LED goes on steady, startup is complete and the NCE is operational. The total time to start up the NCE25 depends on the size of the database and can take several minutes.

NAE35/NAE45 LED startup sequence

About this task:

During startup, the NAE35/NAE45 automatically initiates an LED test to verify the operational status of the LEDs.

Immediately after connecting supply power, the following LED lighting sequence occurs:

- 1. The POWER, FAULT, RUN, and PEER COM LEDs turn on, indicating that the OS is starting up. (After 2 seconds, the LEDs may change states depending on site-specific network activity.)
- 2. The PEER COM and FAULT LEDs shut off. The RUN LED flashes to indicate that the NAE35/ NAE45 software is loading.
- The LEDs display the operational status of the NAE35/NAE45. When the RUN LED goes on steady, startup is complete and the NAE35/NAE45 is operational. The total time to start up the NAE35/NAE45 depends on the size of the database and may take several minutes.

NAE55 LED startup sequence

About this task:

During startup, the NAE55 automatically initiates an LED test to verify the operational status of the LEDs.

Immediately after connecting supply power, the following LED lighting sequence occurs:

- 1. The POWER, PEER COM, RUN, and GENL FAULT LEDs turn on, indicating that the OS is starting up. For the NAE55, the N2A and N2B LEDs also turn on.
- 2. The FCA, FCB, PEER COM, and GENL FAULT LEDs shut off. The RUN LED flashes to indicate that the NAE55 software is loading.
- The LEDs display the operational status of the NAE55. When the RUN LED goes on steady, the application is running and the NAE55 is ready.
 The total time to start up the NAE55 depends on the size of the database and may take up to 15 minutes.

Diagnostic tab

The Diagnostic tab displays NAE hardware status information that may aid troubleshooting.

With the NAE object selected, click the **Diagnostic** tab to view current information about the NAE hardware status. Figure 41 shows an example.

Figure 41: NAE Diagnostic Tab

| 💷 System | | | | | | | - | - 🗆 | \times |
|---------------------------------------|--|---|--|---|------------------------|---|---------------|-------------|----------|
| <u>I</u> tem <u>E</u> dit <u>V</u> ie | ew <u>A</u> ction I <u>n</u> sert <u>T</u> ools <u>Q</u> uery | <u>H</u> elp | | Last | Login: T | hu 05/26/2022 09:45:2 | 29 CDT Met*** | Logout | Exit |
| 企 | | | | | Prev | ReIN50-3 | | ግ | - 🛛 🖾 |
| All Items | | | | | Oper | ational Alarm | | | |
| | | Focus | Summary D | iagnostic | Network | k Email SNMP | Syslog Ala | arm Trend | d |
| All Items | vReIN50-3 BACnet Protocol Eng Eth IP DataLink SC Network Port Update Energy Programming Schedule Field Bus MSTP1 | Focus Edit Attrib Devic CF Fila Es Me Ot Ot Ba CF Ba Ot Ot CF Ba Ot Ot CF | Summary D ute Ce PU Usage ash Usage stimated Flash A emory Usage oject Memory Us oject Count attery Condition PU Temperature bound Reference uplicate Reference ository Storage epository Status ansfer Buffer Full me Between Buffer amples Lost ample Rate ents Lost ent Rate dits Lost undit Rate te Detection etwork Tolerance etection Interval P Messaging ansport Failure F aximum Intermitter ret Messaging DV Rcv Rate DV Tx Rate Accet Broadcast Series Data egistration Usag ata Usage | iagnostic wailable age re ces ces ces ll ffer Reads ffer Reads se Rate thent Failure I ant Failure Pe tent Failure Pe | Period eriod ate | ational Alarm ational Alarm k Email SNMP Value 4.9 % 0.1 % 12.0 megabytes 19.2 % 0.0 % 51 Service 46 deg C 27 deg C Listof[0] Listof[0] Listof[0] 0 per hour 0 0 per hour 0 10 per hour 0 10 per hour 0 10 per hour 0 10 per nour 0 10 per min 30 seconds Listof[0] Listof[0] 0 per min 3 per min 0 per min 3 per min 0 per min 3 per min 0 per min | Syslog Ala | | |
| | | Da | ata Collection Ra | ate | | o per min | | | |
| 8 | | | | | | • | Server: 5/26 | 2022, 09:52 | 2 AM CDT |

You can also select and drag Network Protocol objects into the Display panel and click the **Diagnostic** tab to view information for the selected Network protocol (Figure 42).

Figure 42: BACnet Protocol Diagnostic Tab

| 📵 System | | - | - 🗆 × |
|--|--------------------------------------|--|---------------------|
| <u>I</u> tem <u>E</u> dit <u>V</u> iew <u>A</u> ction I <u>n</u> sert <u>T</u> ools <u>Q</u> uer | y <u>H</u> elp | Last Login: Thu 05/26/2022 09:45:29 CDT Met*** | Logout Exit |
| 企 | ⋳⋺ | BACnet Protocol Eng | 10 🛛 🖓 |
| All Items | | Normal | |
| 🗏 🗐 PrevReIN50-3 | Focus Diagnostic | | |
| BACnet Protocol Eng | Edit | | |
| Eth IP DataLink | | 1 | |
| SC Network Port | Attribute | Value | |
| Dpdate | Statistics | | - |
| Energy | Latch Statistics | False | |
| Programming | Clear Statistics | False | |
| Schedule | Reset Date | Monday, May 9, 2022 | |
| teld Bus MSTP1 | Reset Time | 07:06:53 AM (HH:MM:SS AM/PM) | |
| | Conf Req Tx | 3011 | |
| | Conf Req Rcv | 8 | |
| | Seg Conf Req Tx | 0 | |
| | Seg Conf Req Rcv | 0 | |
| | Ack Tx | 8 | |
| | Ack Rcv | 0 | |
| | Seg Ack Tx | 0 | |
| | Seg Ack Rcv | 0 | - |
| | Simple Ack Tx | 0 | |
| | Simple Ack Rcv | 0 | |
| | Segment Ack Tx | 0 | |
| | Segment Ack Rcv | 0 | |
| | Unconfirmed Tx | 25 | |
| | Unconfirmed Rcv | 974 | |
| | Error Tx | 0 | |
| | Error Rcv | 0 | |
| | Reject Tx | 0 | |
| | Reject Rcv | 0 | |
| | Abort Tx | 0 | |
| | Abort Rcv | 0 | |
| | | Server: 5/26 | /2022, 09:53 AM CDT |

Summary tab

The Summary tab (Figure 43) in the Site Management Portal UI provides a quick view of the status of the objects and items currently in your site.

Select, drag, and drop an object from the Navigation panel in the Display panel, and click the **Summary** tab. When you first click the **Summary** tab, the NAE requests the status of the items in the Display panel (Figure 43). This request may take a few minutes.

For additional information and explanations of the attributes found in the Summary and Diagnostic tabs, refer to the *Object Help* in the *SCT: System Configuration Tool Help (LIT-12011964)* or the *Metasys Site Management Portal Help (LIT-1201793)*.

Figure 43: NAE Summary Tab

| 💷 System | | | | | | | | — | | \times |
|---|--------------|--------|--|---|------------|-----------|-----------|-----------|-----------|----------|
| <u>I</u> tem <u>E</u> dit <u>V</u> iew <u>A</u> ction I <u>n</u> sert <u>T</u> ools <u>Q</u> uery | <u>H</u> elp | | Las | t Login: Th | u 05/26/20 | 22 09:45: | 29 CDT Me | t*** Log | gout | Exit |
| 企 | ⋳⋺ | | | PrevF | eIN50-3 | | | | °`` | 🛛 🖉 |
| All Items | | | | Opera | tional Ala | arm | | | | |
| RevReIN50-3 | Focus Su | Immary | Diagnostic | Network | Email | SNMP | Syslog | Alarm | Trend | |
| BACnet Protocol Eng Eth IP DataLink SC Network Port Update Energy Programming Schedule Field Bus MSTP1 | Out of S | Ser | Item BACnet Pro Eth IP Datal SC Network Update Energy Programmi Schedule Field Bus M | tocol Eng Link Port ng STP1 | Value | Descri | ption | | | |
| × | р | | | | | ۲ | Server: | 5/26/2022 | , 09:53 A | |

Troubleshooting procedures

Verifying Ethernet network communications (Ping)

You can use the ping command to verify that computers on the Ethernet network can communicate with other computers on the network.

To use the ping command, you must have a computer configured to use the TCP/IP protocol and at least one other computer connected to the network.

To verify the computers can communicate on the network using the ping command:

- 1. Open a Command Prompt window (cmd) on the computer.
- 2. Type the ping command. Use the format **ping <address>**, where <address> is the IP address or domain name of the computer you want to ping. (For example: 198.81.196.2, www.jci.com, or NAE008066050FFC.)

3. Press Enter.

If you receive a reply, the computers are communicating on the network.

If you do not receive a reply, try pinging your own computer address.

- If you can ping your own address but not any other addresses, the problem is with the network. Check the Link light on the network card.
- If you cannot get a reply from your own address, the problem is probably with the network card in your computer or with the TCP/IP properties. Check the network card in your computer, and verify the TCP/IP properties.

Pre-boot execution environment (PXE)

The NAE implements a PXE client. If your network uses a PXE server, exclude the NAE MAC address from the PXE server. If you do not exclude the NAE MAC address, the NAE may not start properly.

(i) **Note:** Consult with the system administrator or IT department to determine if the network has a PXE server.

Determining the NAE IP address and device name for a network connection

The IP address determined by this procedure is the IP address used on a building network connection, not serial or dial connections.

Determining the NAE IP address by using the SCT Pro

About this task:

You can use SCT Pro to discover the NAE. To determine the IP address of an NAE by using SCT Pro to discover the device, complete the following steps:

- 1. Open the SCT Pro dashboard.
- 2. From the **Utilities** pane, click **Discover**. The **Device Discovery**page opens.
- 3. Check the status to ensure the system is listening for device wake-up messages.
- 4. Click **Discover**. The table displays devices on the subnet. For more information, refer to *SCT Pro Help (LIT-12013035)*.

Determining the NAE IP address and device name by using a serial port monitor

When an NCE25, NAE35, or NAE45 is powered on, it sends a text string to its serial port that contains helpful information, such as its current IP address and device name. (This functionality is no longer available with the NAE55 at Release 10.0.) This data stream is sent from the RS232C or RS232C A Serial Port. The following table is an example of the data that is sent.

| Device Information | Example Output |
|-----------------------|-------------------|
| Host Name | NAE-1 |
| DHCP Enabled | Yes |
| IP Address | 159.222.8.206 |
| Subnet Mask | 255.255.252.0 |
| Default Gateway | 159.222.8.2 |
| DHCP Server | 159.222.8.9 |
| MAC Address | 00-80-66-05-0F-FC |
| Neuron® ID | 00-00-00-00-00 |
| Model Number | MS-NAE4510-2 |
| RAM Memory | 122 Mb |
| NAND Memory | 128 Mb |
| ОЅ Туре | Linux |
| COM1 | 115200n8 |
| Serial/Internal modem | no |
| USB Modem | no |
| Battery Status | Good |

| Table 28: Example NCE25 | , NAE35, NAE45 | Startup Data St | tream |
|-------------------------|----------------|-----------------|-------|
|-------------------------|----------------|-----------------|-------|

(1) Note: The IP address and device name are internal to the NAE and change if the NAE is attached to a network using DHCP, unless the DHCP server is configured to assign a static IP address. Also, if the NAE has an IP address and is then disconnected from the network, a VT100 terminal emulator sees zeros as the IP address until the NAE is restarted.

To determine the NAE IP address and device name, attach an RS232 DB9 cable between the serial ports of the computer and the NAE, then connect a computer monitor. Install a VT100 terminal emulator program on the computer that connects to the device. Check with your IT department, or technical support team, for a recommended VT100 terminal emulator program to use with your Windows operating system.

In the terminal emulator program, use the following settings:

- Baud rate=115200
- Data Bits: 8 bit
- Stop Bits: 1
- Control Flow: None

Setting a computer to be compatible with APIPA

About this task:

If you are configuring an NAE for use on an Ethernet network without DHCP or DNS support, the computer's IP address must be compatible with APIPA. View the local area connection properties of the active network connection as follows:

- 1. In Control Panel, select **Network and Internet > Network and Sharing Center > Change adapter settings**. The Network Connections window appears.
- 2. Right-click **Local Area Connection** and select **Properties**. The Local Area Connection Properties window appears.
- 3. Click Internet Protocol Version 4 (TCP/IPv4) and then click Properties.
- 4. Make sure the option **Obtain an IP address automatically** is selected. This setting allows Windows to provide the network engine with an IP address in the 169.254.x.x range when connected to a network that does not have a DCHP server.

Technical specifications - NCE, NAE, and NIE models

Table 29: NCE25 technical specifications

| Power Requirement | Dedicated nominal 24 VAC, Class 2 power supply (North America), SELV power supply (Europe), at 50/60 Hz (20 VAC minimum to 30 VAC maximum) |
|---------------------------------|--|
| Power Consumption | 25 VA maximum for NCE25 only |
| | Image: The 25 VA rating does not include any power supplied by the NCE to devices connected at the NCE BOS. BO devices connected to and powered by an NCE can require an additional 125 VA (maximum). |
| Power Source | +15 VDC power source terminals provide 100 mA total current; quantity of inputs: five, located in Universal IN terminals; for active (3-wire) input devices |
| Ambient Operating Conditions | 0 to 50°C (32 to 122°F), 10 to 90% RH, 30°C (86°F) maximum dew point |
| Ambient Storage Conditions | -40 to 70°C (-40 to 158°F), 5 to 95% RH, 30°C (86°F) maximum dew point |
| Data Protection Battery | Supports data protection on power failure. Rechargeable NiMH battery: 3.6 VDC 500 mAh, with a typical life of 5 to 7 years at 21°C (70°F); Product Code Number: MS-BAT1020-0 |
| Processors | Supervisory Controller: 192 MHz Renesas SH4 7760 RISC processor Field Controller: 20 MHz Renesas H8S2398 processor |

Table 29: NCE25 technical specifications

| Memory | Supervisory Controller: 128 MB flash nonvolatile memory for | | | | | | | |
|--|--|--|--|--|--|--|--|--|
| | operating system, configuration data, and operations data storage and | | | | | | | |
| | backup and 128 MB SDRAM for operations data dynamic memory | | | | | | | |
| | Field Controller: 1 MB flash memory and 1 MB RAM | | | | | | | |
| Operating System | Microsoft Windows Embedded CE 6.0 (Release 9.0) | | | | | | | |
| | Buildroot 2017.08.2 with Linux kernel 4.14 (Release 9.0.7 or later patch) | | | | | | | |
| Network and Serial | One Ethernet port; 10/100 Mbps; 8-pin RJ-45 connector | | | | | | | |
| Interfaces (Depending on NCE | One optically isolated RS-485 SA Bus port; with a pluggable and keyed 4-position terminal block (on all NCE25 models) | | | | | | | |
| model.) | One optically isolated RS-485 port; with a pluggable and keyed 4- position terminal block (only on NCE25 models that support an N2 Bus or MS/TP bus trunk) | | | | | | | |
| | One LonWorks port; FTT10 78 Kbps; pluggable, keyed 3-position terminal block (only on NCE25 models that support a LonWorks Network trunk). The LonWorks models are supported to run the Metasys Release 9.0 software, but not the Release 9.0.7 or later patch update. | | | | | | | |
| | One RS-232-C serial port with standard 9-pin sub-D connector that supports standard baud rates | | | | | | | |
| | One USB serial port with standard USB connector that supports an optional, user-supplied external modem. Modem functions are available with Metasys Release 9.0, but are not available after the NAE is patched with Release 9.0.7 or later. | | | | | | | |
| | Option: One telephone port for internal modem; up to 56 Kbps; 6-pin modular connector (NAE models with an optional internal modem have one RS-232-C serial port only; not supported for engine with Release 9.0.7 or later.) | | | | | | | |
| Analog Input/Analog | Analog Input Points: 16-bit resolution | | | | | | | |
| Output Point Resolution | Analog Output Points: 16-bit resolution and ±200 mV accuracy on 0-10 VDC applications | | | | | | | |
| Input/Output Capabilities | 10-Universal Inputs: Defined as 0–10 VDC, 4–20mA, 0–600k ohm, or Binary Dry Contact | | | | | | | |
| | 8-Binary Inputs: Defined as Dry Contact Maintained or Pulse/ Accumulator Mode | | | | | | | |
| | 4-Analog Outputs: Defined as 0–10 VDC or 4–20mA | | | | | | | |
| | 7-Binary Outputs: Defined as 24 VAC Triac (selectable internal or external source power) | | | | | | | |
| | • 4-Configurable Outputs: Defined as 0–10 VDC or 24 VAC Triac BO | | | | | | | |
| Dimensions (Height x Width x Depth) | 155 x 270 x 64 mm (6.1 x 10.6 x 2.5 in.), minimum mounting space required: 250 x 370 x 110 mm (9.8 x 14.6 x 4.3 in.) | | | | | | | |
| Housing | Plastic housing Plastic material: ABS and polycarbonate Protection: IP20 (IEC60529) | | | | | | | |
| Mounting | On flat surface with screws, on three mounting clips, or a single 35 mm DIN rail | | | | | | | |

Table 29: NCE25 technical specifications

| Shipping Weight | 1.2 kg (2.7 lb) |
|-----------------|---|
| Compliance | United States: UL Listed, File E107041, CCN PAZX, UL 916, Energy Management Equipment; FCC Compliant to CFR47, Part 15, Subpart B, Class A |
| | Canada: UL Listed, File E107041, CCN PAZX7, CAN/CSA C22.2 No. 205, Signal Equipment Industry Canada Compliant, ICES-003 |
| CE | Europe: CE Mark - Johnson Controls declares that this product is in compliance with the essential requirements and other relevant provisions of the EMC Directive. |
| | Australia and New Zealand: RCM Mark, Australia/NZ Emissions Compliant |
| | BACnet International: BTL 135-2012 Listed B-BC, Protocol Revision 12 |

Table 30: NAE35 and NAE45 technical specifications

| Power Requirement | Dedicated nominal 24 VAC, Class 2 power supply (North America), SELV power supply (Europe), at 50/60 Hz (20 VAC minimum to 30 VAC maximum) |
|---------------------------------|--|
| Power Consumption | 25 VA maximum |
| Ambient Operating Conditions | 0 to 50°C (32 to 122°F); 10 to 90% RH, 30°C (86°F) maximum dew point |
| Ambient Storage Conditions | -40 to 70°C (-40 to 158°F); 5 to 95% RH, 30°C (86°F) maximum dew point |
| Data Protection Battery | Supports data protection on power failure. Rechargeable NiMH battery: 3.6 VDC 500 mAh, with a typical life of 5 to 7 years at 21°C (70°F); Product Code Number: MS-BAT1020-0 |
| Processor | 192 MHz Renesas SH4 7760 RISC processor |
| Memory | 128 MB flash nonvolatile memory for operating system, configuration data, and operations data storage and backup 128 MB SDRAM for operations data dynamic memory |
| Operating System | Microsoft Windows Embedded CE 6.0 (Release 9.0) Buildroot 2017.08.2 with Linux kernel 4.14 (Release 9.0.7 or later patch) |

Table 30: NAE35 and NAE45 technical specifications

| Network and Serial | One Ethernet port; connects at 10 or 100 Mbps; 8-pin RJ-45 connector |
|--|--|
| Interfaces | One optically isolated RS-485 port; 9.6k, 19.2k, 38.4k, or 76.8k baud (depending on protocol); with a pluggable and keyed 4-position terminal block (FC Bus available on NAE351x and NAE451x models only) |
| | One LonWorks port; FTT10 78 Kbps; pluggable, keyed 3-position terminal block (LonWorks port available on NAE352x-x and NAE452x models only). The LonWorks models are supported to run the Metasys Release 9.0 software, but not the Release 9.0.7 or later patch update. |
| | One RS-232-C serial port with standard 9-pin sub-D connector that supports standard baud rates. |
| | Second serial port, on models without an internal modem, that supports an optional, user-supplied external modem. Modem functions are available with Metasys Release 9.0, but are not available after the NAE is patched with Release 9.0.7 or later. |
| | • One USB serial port with standard USB connector that supports an optional, user-supplied external modem. Modem functions are available with Metasys Release 9.0, but are not available after the NAE is patched with Release 9.0.7 or later. |
| | Option: One telephone port for internal modem; up to 56 Kbps; 6-pin modular connector (NAE models with an optional internal modem have one RS-232-C serial port only; not supported for engine with Release 9.0.7 or later.) |
| Housing | Plastic housing material: ABS polycarbonate UL94-5VB Protection: IP20 (IEC 60529) |
| Mounting | On flat surface with screws on three mounting clips or a single 35 mm DIN rail |
| Dimensions (Height x Width x Depth) | 131 x 270 x 62 mm (5-3/16 x 10-5/8 x 2-1/2 in.) Minimum space for mounting NAE35 and NAE45: 210 x 350 x 110 mm (8-3/16 x 13-13/16 x 45/16 in.) |
| Shipping Weight | 1.2 kg (2.7 lb) |
| Compliance | United States: UL Listed, File E107041, CCN PAZX, UL 916, Energy Management Equipment; FCC Compliant to CFR47, Part 15, Subpart B, Class A |
| | Canada: UL Listed, File E107041, CCN PAZX7, CAN/CSA C22.2 No. 205, Signal Equipment; Industry Canada Compliant, ICES-003 |
| CE | Australia and New Zealand: RCM Mark, Australia/NZ Emissions Compliant |
| | Europe: CE Mark – Johnson Controls declares that this product is in compliance with the essential requirements and other relevant provisions of the EMC Directive. |
| | BACnet International: BTL 135-2012 Listed B-BC, Protocol Revision 12 |

The MS-NAE5510-2U and MS-NAE5510-3U network engines with Release 8.1 software comply with UL 864 10th Edition UUKL/ORD-C100-13 UUKLC Smoke Control Listing for United States and

Canada. Refer to the *Metasys System UL 864 10th Edition UUKL/ORD-C100-13 UUKLC Smoke Control System Technical Bulletin (LIT-12012487)* for specific UL 864 UUKL listing guidelines that must be followed per UL 864.

| Power Requirement | Dedicated nominal 24 VAC, Class 2 power supply (North America) at 50/60 Hz (20 VAC minimum to 30 VAC maximum) |
|---------------------------------|---|
| Power Consumption | 50 VA maximum |
| Ambient Operating Conditions | 0 to 50°C (32 to 122°F); 10 to 90% RH, 30°C (86°F) maximum dew point |
| Ambient Storage Conditions | -40 to 70°C (-40 to 158°F); 5 to 95% RH, 30°C (86°F) maximum dew point |
| Data Protection Battery | Supports data protection on power failure. Rechargeable gel cell battery: 12 V, 1.2 Ah, with a typical life of 3 to 5 years at 21°C (70°F); Product Code Number: MS-BAT1010-0 |
| Clock Battery | Maintains real-time clock through a power failure. Onboard cell; typical life 10 years at 21°C (70°F) |
| Processor | 1.6 GHz Intel Atom® processor |
| Memory | 4 GB flash nonvolatile memory for operating system, configuration data, and operations data storage and backup. 1 GB SDRAM for operations data dynamic memory for all models |
| Operating System | Johnson Controls OEM Version of Microsoft Windows Standard 2009 |
| Network and Serial | One Ethernet port; 10/100/1,000 Mbps; 8-pin RJ-45 connector |
| Interfaces | • Two optically isolated RS-485 ports; 9,600, 19.2k, 38.4k, or 76.8k baud; pluggable and keyed 4-position terminal blocks |
| | • Two RS-232-C serial ports, with standard 9-pin sub-D connectors, that support all standard baud rates |
| | Two USB serial ports; standard USB connectors (use is not supported on Smoke Control NAEs) |
| Housing | Plastic housing with internal metal shield Plastic material: ABS + polycarbonate |
| Mounting | On flat surface with screws on four mounting feet or on dual 35 mm DIN rail |
| Dimensions (Height x | 226 x 332 x 96.5 mm (8.9 x 13.1 x 3.8 in.) including mounting feet |
| Width x Depth) | Minimum space for mounting: 303 x 408 x 148 mm (12.0 x 16.1 x 5.8 in.) |
| Shipping Weight | 2.9 kg (6.4 lb) |

| Table 31: NAE5510-2U | (Smoke | Control) | technical | specifications |
|----------------------|--------|----------|-----------|----------------|
|----------------------|--------|----------|-----------|----------------|

Table 31: NAE5510-2U (Smoke Control) technical specifications

| Compliance | United States: UL Listed, File E107041, CCN PAZX, UL 916, Energy |
|------------|---|
| | Management Equipment; FCC Compliant to CFR47, Part 15, Subpart B, |
| | Class A |
| | LIL Listed Eilo S4077 LIL 864 LILIKI /LILIKI C 10th Edition Listed Smoke |
| | OL LISTER, FILE 34977, OL 804 OOKL/OOKLC TOTH EUTION LISTER, SITIOKE |
| CE | Control Units and Accessories for Fire Alarm Systems Equipment |
| | Canada: UL Listed, File E107041, CCN PAZX7, CAN/CSA C22.2 No. 205, |
| | Signal Equipment, Industry Canada Compliant, ICES-003 |
| | LIL Listed Eilo \$4077 LIL \$64 LILIKI /OPD \$100 12 10th Edition Listed |
| | |
| | Smoke Control Units and Accessories for Fire Alarm Systems |
| | Europe : CE Mark - Johnson Controls, Inc. declares that this product |
| | is in compliance with the essential requirements and other relevant |
| | provisions of the EMC Directive |
| | |
| | Australia and New Zealand: RCM Mark, Australia/NZ Emissions |
| | Compliant |
| | BACnet International: BTL 135-2012 Listed B-BC. Protocol Revision 12 |
| | Brenet International. Bre 135 2012 Listed B-BC, Frotocor Revision 12 |

Table 32: NAE55xx-3 (Energy Management) and NAE5510-3U (Smoke Control) technical specifications

| Power Requirement | Dedicated nominal 24 VAC, Class 2 power supply (North America), SELV power supply (Europe), at 50/60 Hz (20 VAC minimum to 30 VAC maximum) |
|---------------------------------|---|
| Power Consumption | 50 VA maximum |
| Ambient Operating Conditions | 0 to 50°C (32 to 122°F); 10 to 90% RH, 30°C (86°F) maximum dew point |
| Ambient Storage Conditions | -40 to 70°C (-40 to 158°F); 5 to 95% RH, 30°C (86°F) maximum dew point |
| Data Protection Battery | Supports data protection on power failure. Rechargeable gel cell battery: 12 V, 1.2 Ah, with a typical life of 3 to 5 years at 21°C (70°F); Product Code Number: MS-BAT1010-0 |
| Clock Battery | Maintains real-time clock through a power failure. Onboard cell; typical life 10 years at 21°C (70°F) |
| Processor | 1.46 GHz Intel® Atom® Bay Trail E3815 processor for MS-NAE55xx-3 models |
| Memory | 16 GB flash nonvolatile memory for operating system, configuration data, and operations data storage and backup for MS-NAE55xx-3 models. 2 GB DDR3 SDRAM for operations data dynamic memory for all models |
| Operating System | Johnson Controls OEM Version of Microsoft Windows Embedded Standard 7 with SP1 (WES7, Release 9.0) Wind River Linux 9 (Release 10.0) |

Table 32: NAE55xx-3 (Energy Management) and NAE5510-3U (Smoke Control) technical specifications

| Network and Serial | • One Ethernet port: 10/100/1 000 Mbps: 8-pin RI-45 connector |
|----------------------|---|
| Interfaces | |
| Interfaces | Two optically isolated RS-485 ports; 9,600, 19.2k, 38.4k, or 76.8k baud; pluggable and keyed 4 position terminal blocks (RS-485 terminal blocks available on NAE55 models only) |
| | • Two RS-232-C serial ports, with standard 9-pin sub-D connectors, that support all standard baud rates |
| | Two USB 2.0 serial ports; standard USB connectors support an optional, user-supplied external modem |
| | • Options: One telephone port for internal modem; up to 56 kbps; 6- pin RJ-12 connector |
| | One LonWorks port; FTT10 78 Kbps; pluggable, keyed 3-position terminal block (LonWorks port available on NAE552x-x models only) |
| Housing | Plastic housing with internal metal shield Plastic material: ABS + polycarbonate; Protection: IP20 (IEC 60529) |
| Mounting | On flat surface with screws on four mounting feet or on dual 35 mm DIN rail |
| Dimensions (Height x | 226 x 332 x 96.5 mm (8.9 x 13.1 x 3.8 in.) including mounting feet |
| Width x Depth) | Minimum space for mounting: 303 x 408 x 148 mm (12.0 x 16.1 x 5.8 in.) |
| Shipping Weight | 2.9 kg (6.4 lb) |
| Compliance | United States : UL Listed, File E107041, CCN PAZX, UL 916, Energy Management Equipment, FCC Compliant to CFR47, Part 15, Subpart B, Class A |
| CE | UL Listed, File S4977, UL 864 UUKL/UUKLC 10th Edition Listed, Smoke Control Units and Accessories for Fire Alarm Systems Equipment (MS- NAE5510-3U model only with Release 8.1 software) |
| | Canada : UL Listed, File E107041, CCN PAZX7, CAN/CSA C22.2 No. 205, Signal Equipment, Industry Canada Compliant, ICES-003 UL Listed, File S4977, UL 864 UUKL/ORD-C100-13 10th Edition Listed, Smoke Control Units and Accessories for Fire Alarm Systems (MS- NAE5510-3U model only with Release 8.1 software) |
| | Europe : CE Mark - Johnson Controls declares that this product is in compliance with the essential requirements and other relevant provisions of the EMC Directive. |
| | Australia and New Zealand : RCM Mark, Australia/NZ Emissions Compliant |
| 1 | |

Table 33: NAE-S technical specifications (North America and Canada only)

| Power Requirements | NAE551S-2 Engine: |
|--------------------|--|
| | Dedicated nominal 24 VAC, Class 2 power supply (North America), at |
| | 50/60 Hz (20 VAC minimum to 30 VAC maximum) |
| | Internal Module with Embedded Encryption Technology: |
| | Input: Dedicated nominal 100–240 VAC, Class 1 power supply (North |
| | America), at 50/60 Hz (85 VAC minimum to 264 VAC maximum) |
| | Output: 24 VDC (22 VDC minimum to 26 VDC maximum) |

Table 33: NAE-S technical specifications (North America and Canada only)

| Power Consumption | 50 VA maximum |
|--|--|
| Power Specifications for Encryption Board | Dedicated nominal 24 VDC, input voltage range 85–264 VAC (120–375 VDC), output current 2.0A |
| Ambient Operating Conditions | 32 to 122°F (0 to 50°C); 10 to 90% RH, 86°F (30°C) maximum dew point |
| Ambient Storage Conditions | -40 to 158°F (-40 to 70°C); 5 to 95% RH, 86°F (30°C) maximum dew point |
| Data Protection Battery | Supports data protection on power failure. Rechargeable gel cell battery: 12 V, 1.2 Ah, with a typical life of 3 to 5 years at 70°F (21°C); Product Code Number: MS-BAT1010-0 |
| Clock Battery | Maintains real-time clock through a power failure. Onboard cell; typical life 10 years at 70°F (21°C) |
| Processor | 1.6 GHz Intel Atom® processor |
| Memory | 4 GB flash nonvolatile memory for operating system, configuration data, and operations data storage and backup 1 GB SDRAM for operations data dynamic memory for all models |
| Network and Serial | One Ethernet port; 10/100/1000 Mbps; 8-pin RJ-45 connector |
| Interfaces | • Two optically isolated RS-485 ports; 9600, 19.2k, 38.4k, or 76.8k baud; pluggable and keyed 4 position terminal blocks (RS-485 terminal blocks available) |
| Housing | Plastic housing with internal metal shield Plastic material: ABS + polycarbonate; Protection: IP20 (IEC 60529) |
| Mounting | Must be mounted in a locked, secure panel using four mounting feet or dual 35 mm DIN rails. |
| Dimensions (Height x Width x Depth) | 8.9 x 13.1 x 3.8 in. (226 x 332 x 96.5 mm) including mounting feet Minimum space for mounting: 12.0 x 16.1 x 5.8 in. (303 x 408 x 148 mm) |
| Shipping Weight | 10.4 lb (3.88 kg) |
| Shipping Restriction | The Bureau of Industry and Security of the U.S. Department of Commerce has regulated this shipment under 740.17(b)(2) of the EAR and restricted the shipment of this product to the following countries: Cuba, Iran, North Korea, Sudan, and Syria. |
| Compliance | United States : UL 508A and CCN NITW Industrial Control Panel Listed, FCC Compliant to CFR47, Part 15, Subpart B, Class A |
| | Canada : cUL CSA-C22.2 No. 14, CCN NITW7, Industrial Control Equipment; IC Compliant to ICES-003 Class A |
| | BACnet International: BTL 135-2012 Listed B-BC, Protocol Revision 12 |

Table 34: NAE85 software system recommendations for installation or upgrade

| Recommended | Intel® Xeon® Gold 5222 3.8G, 4C/8T, 10.4GT/s, 16.5M Cache, Turbo, HT |
|-----------------------|--|
| computer platform | (105W) DDR4-2933 |
| | |
| | or |
| | |
| | Intel® Xeon® Gold 6244 3.6G, 8C/16T, 10.4GT/s, 24.75M Cache, Turbo, HT (150W) DDR4-2933 |
| Recommended memory | 16 GB RAM minimum; 32 GB RAM recommended |
| Hard disk | 160 GB minimum |
| Supported operating | • Windows® 10 Pro and Windows 10 Enterprise Editions versions 2004, |
| systems and software | 21H1, and 21H2 (64-bit). For all future Windows 10 updates after version 21H2, we will evaluate and certify that Metasys software can support the updates before we provide guidance on support. |
| | • Windows® Server® 2019 (version 1809 or later) (64-bit) |
| | • Windows® Server® 2016 (version 1607 or later) (64-bit) |
| | ① Note: The NAE85 software requires two Windows components: |
| | Microsoft .NET Framework Version 3.5 SP1 and Microsoft .NET Framework Version 4.6.1. |
| Operating systems and | Windows 10: |
| icrosoft SQL | |
| | • SQL Server® 2019 Express with CU14 (64-bit) |
| | • SQL Server® 2017 Express with CU27 (64-bit) |
| | • SQL Server® 2016 Express with SP2 CU17 (64-bit) |
| | Note: The NAE85 installation program includes SQL Server Express 2017 CU19 (64-bit). If no SQL Server instance is present on the host computer, the NAE85 installation program installs and configures SQL Server Express 2017 CU19. |
| | Windows Server 2019: |
| | • SOL Sanvara 2019 with $CU14$ (64 hit) |
| | |
| | • SQL Server® 2017 with CU27 (64-bit) |
| | SQL Server® 2016 with SP2 CU17 (64-bit) |
| | Windows Server 2016: |
| | • SQL Server® 2019 with CU14 (64-bit) |
| | • SQL Server® 2017 with CU27 (64-bit) |
| | • SQL Server® 2016 with SP2 CU17 (64-bit) |
| Supported operating systems for Metasys client computers | • Windows® 10 Pro and Windows 10 Enterprise Editions versions 2004, 21H1, and 21H2 (64-bit). For all future Windows 10 updates after version 21H2, we will evaluate and certify that Metasys software can support the updates before we provide guidance on support. |
|--|--|
| | • Apple® macOS® 11 Big Sur |
| | • Apple® macOS® 10.15 Catalina |
| | • Apple® OS X® 10.14 Mojave |
| | Note: Apple® operating systems are supported for Metasys client computers only. In Apple® OS X®, you cannot view Graphics+ graphics in the |
| | SMP UI. |
| Recommended antivirus software | Symantec Endpoint Protection version 12 |
| Supported web browser | Microsoft® Edge® version 91 or later |
| software for Metasys | Google® Chrome[™] version 91 or later |
| | • Apple® Safari® 13.1 or later |
| | Note: Other browsers, such as Mozilla® Firefox®, may also be used but are not fully supported. |
| | Use a web browser to download the Launcher application. After you install Launcher, use Launcher, not the web browser, to log on to the SMP. |
| Supported virtual environments | Microsoft Hyper-V™, VMware® |
| Network communication | Network Interface: 1 Gbps Ethernet network interface card connects at 10 Mbps, 100 Mbps, or 1 Gbps (100 Mbps or better recommended) |
| Recommended data | UPS for NxE85 model: APC Smart-UPS SC 450VA, 280 W, 120 VAC input/ |
| protection | output, NEMA 5-15R output connections, OEM Part No. SC450RM10 |
| Compliance | FIPS 140-2 Level 1: Compliant with Federal Information Processing Standard |
| | Note: FIPS 140-2 compliance applies to an NAE85 when the FIPS 140-2 feature is licensed. |

Appendix: Time zone, date, and time management

Introduction

The goal of time synchronization is to maintain accurate time across all components within the Metasys system. In general, the Site Director is responsible for requesting time from an external time server, and the Site Director's child devices request the time from the Site Director. Requests for time are done using Network Time Protocol (NTP) requests. Network-wide time management ensures that scheduling, trending, audit trailing, data collecting, time-stamping of alarms, and

other functions that require accurate time management use the correct time zone, date, and time consistently for all system operations.

The following table summarizes the time sources for various system items. All time is in UTC and all system devices adjust to daylight savings time.

Table 35: Time Sources

| Item | Time Source |
|----------------------------------|-----------------------------|
| Trend Data, Events, and Commands | Network Engine |
| Annotations | Metasys Server ¹ |
| Event Acknowledgements | Metasys Server ¹ |

1 Includes ADS, ADX, ADS-Lite, and OAS.

To ensure that the correct time appears on the Site Management Portal user interface accessed from a client computer, apply the most recent Daylight Saving Time (DST) patch for the operating system on all clients that access the Site Director. The latest DST patch is available from the <u>Microsoft Download center</u>.

Time synchronization methods

The three methods for network time synchronization that are available to a Metasys site are:

- Windows Simple Network Time Protocol (SNTP)
- Multicast
- BACnet®

Windows time synchronization

Windows time synchronization is Microsoft Corporation's implementation of the standard Windows SNTP w32time. This method is also referred to as unicast synchronization. With this form of time synchronization, all routers manage User Datagram Protocol (UDP) traffic.

If the Site Director is a Metasys Server, the server maintains system time and broadcasts this time to all subordinate network engines. You configure Windows time synchronization by accessing the Clock and Region settings under the Control Panel of the server's operating system. There you set the Date and Time parameters to retrieve the time automatically, which enables the Network Time Protocol (NTP) service on the computer. In this configuration, time comes from a reliable time server that is accessible on the customer's network or over the Internet. The NTP service on the Metasys Server must be on; if NTP is off, the Metasys Server cannot retrieve time from the time server, and the network engines are not able to retrieve time from the Metasys Server.

(i) Note: Use Windows Time Sync for the SNx engines.

If the Site Director is a network engine, system time also comes from an external time server that is accessible on the building network or over the Internet. As the site time server, the engine provides the time zone, date, and time for all other engines on the site. All other devices are considered time clients because they receive the time zone, date, and time from the Engine Site Director. In this configuration, the Device Time Servers attribute under the Focus window of the Engine's Site object specifies the IP address or host name of the external time server. The Device Time Servers attribute under each subordinate network engine specifies the IP address or host name of the Engine Site Director.

There is yet a third selection for Windows time synchronization. You can set up the Metasys Server and each network engine to retrieve the time on their own from an external time server. This configuration is not as desirable because every supervisory device in the Metasys system is making separate time requests to the same time server and the devices might be using different time sync periods. In this configuration, the Device Time Servers attribute under the Focus window of the Metasys Server and all of its engines specifies the IP address or host name of the external time server.

(i) **Note:** If you implement an intentional time change for your site, all other devices on the site use Windows time synchronization to update the new time within 10 minutes.

Multicast time synchronization

Multicast time synchronization is the Johnson Controls implementation of SNTP w32time with Multicast capabilities and RFC-2030 compliance. Multicast is the most commonly used time synchronization option for Metasys sites. This method delivers the same features as the Windows method, but also provides improved Metasys time synchronization between the Site Director and supervisory devices. A time server provides the time to the Site Director, and the Site Director in turn multicasts the time to all supervisory devices on the Metasys network. By default, the server's operating system synchronizes with the external time server once every seven days.

When a supervisory device first reports to the Site Director, it polls the Site Director for the current time and matches its time with the Site Director time. By default, every 5 minutes the Site Director broadcasts the current time to all supervisory devices. You can change this duration, called the Multicast Heartbeat Interval, from one to 255 minutes. If a particular device time differs 1.5 seconds or more from the Site Director time, the device adjusts its time to match. Additionally, if the Site Director time changes by more than 1 to 1.5 seconds, it sends out a Multicast time message to all devices within 2 seconds of the change. This time synchronization method reduces the time interval in which devices are out of sync with the SNTP time server.

(1) Note: Use Windows Time Sync for the SNx engines.

Multicast time synchronization requires that all Ethernet routers on the site support Multicast routing (Internet Group Multicast Protocol [IGMP]) because the Multicast time message crosses routers. To implement Multicast synchronization across routers, you may require assistance from the customer's IT department.

BACnet time synchronization

BACnet time synchronization uses the BACnet protocol to synchronize with BACnet devices such as a network engine and a third-party device that needs a synchronized time. You can only use this method if the Site Director is a network engine and the engine has access to a BACnet time server. This method is **not** available if the Site Director is a Metasys Server. Lastly, the BACnet time synchronization method is available even if the network engine Site Director uses the Windows or Multicast method.

When entering BACnet time synchronization parameters, you need to specify the time synchronization recipients, which are those engines and third-party devices that receive the synchronized time. Three formats are available: ID (the BACnet device object instance number), IP Address, and Broadcast. Also, three forms of broadcast types are available: Local, Remote, and Global.

BACnet time synchronization sends the device's current time to the recipients specified in the two recipient lists: Time Sync Recipients and UTC Time Synchronization Recipients. Select one of the Site Director methods (Windows or Multicast) for setting the supervisory device's time to that of a known time server. Do not send BACnet time synchronization messages to devices that are receiving their time from a Site Director that uses the Windows or Multicast method.

Example network

Figure 44 shows an example system with a common time zone, date, and time management setup. This example is representative of the Multicast or Windows time synchronization methods.

The Metasys Server is the Site Director and is configured to receive the date and time from an intranet time server. The date and time originates at an Internet time server (such as the Naval atomic clock). Using Simple Network Time Protocol (SNTP), the intranet time server requests the time from the Internet time server. The Site Director requests the time from the intranet time server. Then, using the Metasys system automatic time synchronization, and the manually configured time zone, the Site Director automatically provides the time zone, date, and time to the other engines and Metasys Servers on the Metasys network.



Figure 44: Example of time management system

Multiple time zones

Starting at Metasys Release 8.0, multiple time zones are supported for Metasys Servers and network engines, provided that you set the time zones correctly. For network engines that are located in different time zones, the time synchronization occurs in Universal Time Coordinated (UTC) time, not in the time zone of the Site Director. For more details, see Multiple time zones.

The time zone of the Site Director defaults to (UTC-06:00) Central Time (US & Canada). If your site is not in the Central time zone, set the time zone for your location. When you set the time zone in the Site Director, it propagates the current time to all the engines and Metasys Servers on the site. You must set the time zone in the Site Director even if you select a site time server. In addition, you must set the time zone in all non-Site Director Metasys Servers after installing each server.

With Release 8.0 or later, multiple time zones are supported for network engines that are located in different regions of the world. The Default Time Zone attribute in the network engine's Site object provides this time zone capability. The attribute has a drop-down list of all available world time zones. You use it to identify the local time zone where the engine is located. Selecting a time zone means that the operator is no longer required to apply time zone math when working with Schedule objects defined at the engine. The time zone you select is also applied to Schedule objects that you define at the engine.

By default, each updated network engine continues to time-sync with the Site Director, but the time sync occurs in UTC time. For example, a Site Director in the central time zone (UTC-06:00) that syncs with an engine in the mountain time zone (UTC-07:00) does not change the engine to the central

time zone. The local time and date attributes of the Site Director show its local time and date as does the network engine. Also, consider the following important factors:

- **Scheduling:** schedules at each network engine execute relative to the local time zone of the engine, allowing you to schedule based on the local time zone, rather than the Site Director's time zone. Prior to Release 8.0, you had to take into account the local time zone of the engine, then mentally convert the time based on the time zone of the Site Director. These time zone calculations are no longer required.
- **Historical data:** alarms, audits, and trended values from engines that are viewed on the Site Director report in local UTC time. However, alarms, audits, and trended values from engines that are viewed on the engine itself report in local time.
- **Other features:** items such as Archive Date and ADS Delivery Time report in the local time of the engine.

To take advantage of the multi-time zone features, the Metasys Server Site Director and the network engines must be at Release 8.0 or later. If a site has a mixture of engines, some of which are at Release 7.0 or earlier, the older engines do not exhibit the multi-time zone behavior. For example, as Table 36 indicates, the local time of an NAE at Release 7.0 uses the Site Director's time, whereas an NAE at Release 8.0 or later uses a time specified by its Default Time Zone attribute.

| Device | Release | Time Zone | Time Zone Used |
|----------------|--------------|-----------|-------------------------------------|
| Metasys Server | 8.0 or later | Central | Central Standard Time |
| Network Engine | 6.5 | Mountain | Site Director's time zone (Central) |
| | 7.0 | Central | Site Director's time zone (Central) |
| | 8.0 or later | Pacific | Pacific Standard Time |
| | 8.0 or later | Eastern | Eastern Standard Time |

Table 36: Time Zone Examples

(i) **Note:** If your system consists of a network engine Site Director with multiple child network engines, make sure that you use the Default Time Zone attribute of the **Site** object, not the Time Zone attribute in the engine, or undesirable behavior may occur.

Site time server

As a preference to setting the date and time manually for a device, you can select a site time server. A site time server sets the date and time in the Site Director. Site time servers can be on your intranet, such as a Domain Controller/Server; or on the Internet, such as the U.S. Naval Observatory Master Clock.

For a list of Internet time servers, go to <u>https://tf.nist.gov/tf-cgi/servers.cgi</u>.

See Configuring Site Director time to sync with external time source.

Local time and date indication on status bar

The date, time, and time zone in the status bar of the SMP user interface indicates the local date, time, and time zone for that device. The date, time, and time zone in the device object to which you are browsing are the same time; however, there may sometimes seem to be a discrepancy or delay between the two. This is normal operation. See Figure 45.

System \times Item Edit View Action Insert Tools Query Help Last Login: Mon 08/10/2020 14:05:20 CDT Met*** Logout Exit 1000 SNE11000-gr1 Operational Normal All Items All Items - Expert Alarm Email SNMP Syslog Snapshot Focus Trend ۱İ) SNE11000-gr1 Focus Summary Diagnostic Network User Views Summary Definitions Edit Basic Advanced ė. 🗖 Attribute Value PEE BACnet Protocol Eng Object Eth IP DataLink Name SNE11000-ar1 Energy Programming Description Schedule Object Type Device Authorization Category General Model Name M4-SNE11000-0 Time 02:08 PM (BH:MM AM/PM) Local Time Local Date Monday, August 10, 2020 Engineering Values Memory Usage: 21.9% 0 Server: 8/10/2020 02:09 PM CDT îî.

Figure 45: Normal discrepancy between local time and server time as shown in SMP UI

For a network engine at Release 8.0 or later, the local time and date shown on the device object's focus window is based on the default time zone set for the device. If the engine is located in a different time zone than the Site Director, the current time and date shown for each differs.

Selecting a time synchronization method

About this task:

To select a time synchronization method, go to one of the following sections:

- Configuring Site Director for Windows time synchronization
- Configuring Site Director for Multicast time synchronization
- Configuring Site Director for BACnet time synchronization (Network Engines only)

Configuring Site Director for Windows time synchronization

About this task:

Follow these steps to set the time synchronization method to Windows for the Site Director, either the Metasys Server or a network engine.

- 1. Log on the server or network engine Site Director.
- 2. Drag the Site object of the Site Director to the display frame.
- 3. Select Advanced.
- 4. Click **Edit**.
- 5. In the Time section under the Time Sync Method drop-down box, select **Windows**.

Figure 46: Time Sync Method field set to Windows

| | Time | | |
|---|------------------------------|--|---------|
| | Default Time Zone | (UTC-06:00) Central Time (US & Canada) | |
| | Site Time Servers | Listof[0] | |
| | Device Time Servers | Listof[0] | |
| | Time Sync Period | 1 hour | |
| 1 | Time Sync Method | Windows | - |
| | Multicast Group Address | 224 0 1 1 | |
| | Multicast UDP Port | 123 | |
| | Multicast TTL | 1 | |
| | Multicast Heartbeat Interval | 5 | minutes |

- 6. Click Save.
- 7. If you changed the Time Sync Method from Multicast to Windows, manually start the win32time service or restart the Site Director, because this service does not restart on its own.

Configuring Site Director for Multicast time synchronization

About this task:

Follow these steps to set the time synchronization method to Multicast for the Site Director, either the Metasys Server or a network engine.

- 1. Log on the server or network engine Site Director.
- 2. Drag the Site object to the display frame.
- 3. Select Advanced.
- 4. Click **Edit**.
- 5. In the Time section under the Time Sync Method drop-down box, select **Multicast**.

Figure 47: Time Sync Method field set to Multicast

| | Time | | |
|---|------------------------------|--|---------|
| | Default Time Zone | (UTC-06:00) Central Time (US & Canada) | |
| | Site Time Servers | Listof[0] | |
| | Device Time Servers | Listof[0] | |
| | Time Sync Period | 1 hour | |
| 1 | Time Sync Method | Multicast | |
| | Multicast Group Address | 224 0 1 1 | |
| | Multicast UDP Port | 123 | |
| | Multicast TTL | 1 | |
| | Multicast Heartbeat Interval | 5 | minutes |

- 6. Retain the default values for the following Multicast attributes as follows:
 - Multicast Group Address: 244.0.1.1
 - Multicast UDP Port: 123
 - Multicast TTL: 1

- Multicast Heartbeat Interval: 5

For descriptions of these Multicast attributes, see Multicast time synchronization settings.

- 7. Click **Save**. With Multicast time synchronization enabled, the Windows win32time service in the background of the operating system is terminated. Time synchronization occurs when you change the clock locally at the Metasys Server or upon expiration of the Time Sync Period.
- 8. Click on the **Date and time** on the bottom right corner of Windows®. Click **Date and time settings** to verify that the **Set time automatically** parameter is set to **On**.

Configuring Site Director for BACnet time synchronization (Network Engines only)

About this task:

Follow these steps to set the time synchronization method to BACnet for the Site Director. This method is **only** available to a network engine Site Director. The Metasys Server does not support BACnet time synchronization.

- 1. Log on the network engine Site Director.
- 2. Drag the Device object of the Site Director to the display frame.
- 3. Select Advanced.
- 4. Click **Edit**.
- 5. Move to the bottom of the window to locate the BACnet time attributes (Figure 48).

Figure 48: BACnet time synchronization attributes

| III System | - | |
|---|--|----------------|
| <u>I</u> tem <u>E</u> dit <u>V</u> iew <u>A</u> ction I <u>n</u> sert <u>T</u> ools <u>Q</u> uery | / Help Last Login: Fri 05/27/2022 08:41:18 CDT Met*** | gout Exit |
| 企 | M4-SNE22 | 1000 |
| All Items | Operational Normal | |
| 🖂 🥼 Site | Focus Summary Diagnostic Network Email SNMP Syslog Alarm | Trend |
| User Views Summary Definitions | Edit O Basic | Advanced |
| • M4-SNE22 | Attribute Value | |
| BACnet Protocol Eng | UTC Offset 360 minutes | |
| SC Network Part | DST Status True | |
| | BACnet Communications Password | |
| Energy | Last Restart Reason Cold Start | |
| B | Time of Device Restart 07:47:35 AM Friday, May 27, 2022 | |
| 🕀 💼 Schedule | Restart Notification Recipients Listof[1] - (complex data) | |
| 🖶 📲 😫 BACnet IP1 | Time Sync Recipients Listof[0] | |
| | UTC Time Synchronization Recipients Listof[0] | |
| | Time Synchronization Interval 0 minutes | |
| | Align Intervals False | |
| | Interval Offset 0 minutes | |
| | IEIEJ Function A List Listof[0] | |
| | IEIEJ Function A Period 60 seconds | |
| | Enforce Strict BACnet Compliance False | |
| × | Server: 5/27/2022 | , 08:55 AM CDT |

6. Under the Time Sync Recipients drop-down list, specify the BACnet recipients (devices) that are to be time synchronized with the **local** time that is kept by the network engine. For each recipient, define its device ID, IP address information, or broadcast type and information.

Figure 49: Time Sync Recipient parameters

| BACnet Recipient | × | BACnet Rec | ipient | × |
|---|-------|--|--|---------------------|
| D D D D Address Broadcast OK Cancel | | ID Address Broadcast | Broadcast Type Network Number UDP Port | Local 0 47808 |
| | | | ОК | Cancel |
| BACnet Recipient | × | | | |
| ID IP Address 0 Address Network Number 0 Broadcast UDP Port 47808 | 0.0.0 | | | |
| OK Cancel |) | | | |

- 7. Under the UTC Time Synchronization Recipients drop-down list, specify the BACnet recipients (devices) that are to be time synchronized with the **UTC** time that is kept by the network engine. For each recipient, define its device ID, IP address information, or broadcast type and information.
- 8. For Time Synchronization Interval, specify the periodic interval, in minutes, at which Time Synchronization and UTC Time Synchronization requests are sent. If you set to zero, then periodic time synchronization is disabled.
- 9. For Align Intervals, specify whether clock-aligned periodic time synchronization is enabled. If periodic time synchronization is enabled and the time synchronization interval is a factor of an hour or a day (that is, the value divides without a remainder), then the beginning of the period specified for time synchronization aligns to the hour or day, respectively.
- 10. For Interval Offset, specify the offset, in minutes, from the beginning of the period defined for time synchronization until the actual time synchronization requests are set. Interval Offset has no effect when Align Intervals is False.
- 11. Click Save.

Configuring Site Director time to sync with external time

source

About this task:

Set up the Site Director to synchronize time with an external time source by following the steps particular to your synchronization method:

- Selecting a site time server for the Metasys Server Site Director (Windows)
- Selecting a site time server for the Metasys Server Site Director (Multicast)
- Selecting a site time server for the Network Engine Site Director (Windows)
- Selecting a site time server for the Network Engine Site Director (Multicast)

Selecting a site time server for the Metasys Server Site Director (Windows)

About this task:

Follow these steps to select a time server for a Metasys Server Site Director when the time synchronization method is Windows.

- 1. Log on the Metasys Server Site Director.
- 2. Drag the Site object to the display frame.
- 3. Select Advanced.
- 4. Click **Edit**.
- 5. In the Time section under the Time Sync Method drop-down box, verify the selection is set to **Windows**.

Figure 50: Time Sync Method field set to Windows

| | Time | | |
|---|------------------------------|--|---------|
| | Default Time Zone | (UTC-06:00) Central Time (US & Canada) | |
| | Site Time Servers | Listof[0] | 1 |
| | Device Time Servers | Listof[0] | |
| | Time Sync Period | 1 hour | |
| ŧ | Time Sync Method | Windows | |
| | Multicast Group Address | 224 0 1 1 |] |
| | Multicast UDP Port | 123 |] |
| | Multicast TTL | 1 | |
| | Multicast Heartbeat Interval | 5 | minutes |

- 6. Leave the Site Time Servers list blank.
- 7. In the Device Time Servers list, click the browse button and add the IP address, host name, or website of the SNTP Time Server that furnishes the time to the Metasys Server Site Director.
 - (i) **Note:** Specify a host name only if a DNS server is available to the Site Director.
 - (1) **Note:** You may need to increase the TTL setting in a heavily subnetted network.
- 8. Click Save.
- 9. Set the Internet Time Server in the Windows operating system of the Site Director to match the IP Address, host name, or time server specified for the Site Time Server as follows:
 - a. In Control Panel of the Site Director, search for **Date and Time**.
 - b. Open the Date and Time dialog box, and click the **Internet Time** tab. If the Internet Time tab is missing, the server is part of a domain and its time is controlled by a domain server. Skip these steps.
 - c. Click **Change Settings** and enter in the Server field the same IP address, host name, or time server that you defined in the Site Time Server field in Step 6. Click **OK** to apply the change.

Selecting a site time server for the Metasys Server Site Director (Multicast)

About this task:

Follow these steps to select a time server for a Metasys Server Site Director when the time synchronization method is Multicast.

1. Log on the Metasys Server Site Director.

- 2. Drag the Site object to the display frame.
- 3. Select Advanced.
- 4. Click **Edit**.
- 5. In the Time section under the Time Sync Method drop-down box, verify the selection is set to **Multicast**.

Figure 51: Time Sync Method field set to Multicast

| | Time | | |
|---|------------------------------|--|---------|
| | Default Time Zone | (UTC-06:00) Central Time (US & Canada) | |
| | Site Time Servers | Listof[0] | |
| | Device Time Servers | Listof[0] | |
| | Time Sync Period | 1 hour | |
| ŧ | Time Sync Method | Multicast 🗨 | |
| | Multicast Group Address | 224 .0 .1 .1 | |
| | Multicast UDP Port | 123 |] |
| | Multicast TTL | 1 | |
| | Multicast Heartbeat Interval | 5 | minutes |

- 6. In the Site Time Servers list, click the browse button and add the IP address or host name of the SNTP Time Server that furnishes the time to the network engine Site Director. Leave the Device Time Servers list blank.
 - (i) **Note:** Specify a host name only if a DNS server is available to the Site Director.
- 7. Click Save.

Selecting a site time server for the Network Engine Site Director (Windows)

About this task:

Follow these steps to select a time server for a network engine Site Director when the time synchronization method is Windows.

- 1. Log on the network engine.
- 2. Drag the Site object of the Site Director to the display frame.
- 3. Select Advanced.
- 4. Click **Edit**.
- 5. In the Time section under the Time Sync Method drop-down box, verify the selection is set to **Windows**.

Figure 52: Time Sync Method field set to Windows

| | Time | | |
|---|------------------------------|--|---------|
| | Default Time Zone | (UTC-06:00) Central Time (US & Canada) | |
| | Site Time Servers | Listof[0] | |
| | Device Time Servers | Listof[0] | |
| | Time Sync Period | 1 hour | |
| 1 | Time Sync Method | Windows | - |
| | Multicast Group Address | 224 .0 .1 .1 | |
| | Multicast UDP Port | 123 | |
| | Multicast TTL | 1 | |
| | Multicast Heartbeat Interval | 5 | minutes |

- 6. In the Site Time Servers list, click the browse button and add the IP address or host name of the site time server. Leave the Device Time Servers list blank.
- 7. In the Device Time Servers list, click the browse button and add the IP address or host name of the network engine Site Director.
 - (i) **Note:** Specify host names only if a DNS server is available to the Site Director.
- 8. Click Save.
- 9. Restart the network engine Site Director.

Selecting a site time server for the Network Engine Site Director (Multicast)

About this task:

Follow these steps to select a time server for a network engine Site Director when the time synchronization method is Multicast.

- 1. Log on the network engine.
- 2. Drag the Site object of the Site Director to the display frame.
- 3. Select Advanced.
- 4. Click **Edit**.
- 5. In the Time section under the Time Sync Method drop-down box, verify the selection is set to **Multicast**.

Figure 53: Time Sync Method field set to Multicast

| | Time | | |
|---|------------------------------|--|---------|
| | Default Time Zone | (UTC-06:00) Central Time (US & Canada) | |
| | Site Time Servers | Listof[0] | |
| | Device Time Servers | Listof[0] | |
| | Time Sync Period | 1 hour 🔽 | |
| ŧ | Time Sync Method | Multicast | - |
| | Multicast Group Address | 224 0 11 | |
| | Multicast UDP Port | 123 | |
| | Multicast TTL | 1 | |
| | Multicast Heartbeat Interval | 5 | minutes |

- 6. In the Site Time Servers list, click the browse button and add the IP address or host name of the site time server. Leave the Device Time Servers list blank.
 - (i) **Note:** Specify a host name only if a DNS server is available to the Site Director.
- 7. Click Save.
- 8. Restart the network engine Site Director.

Setting the time zone

Refer to one of the following sections to set the time zone:

- Setting the time zone on the Metasys Server Site Director
- Setting the time zone in the Network Engine Site Director

Setting the time zone on the Metasys Server Site Director

1. In the lower-right corner of the Metasys Server computer screen, click the time. The Date and Time Properties box appears (Figure 54). The appearance of this screen and others vary depending on the operating system.

Figure 54: Time and Date on a Metasys Server

| 2: Tuesd | 2:50:36 рм Tuesday, July 28, 2020 | | | | | |
|-------------|--------------------------------------|----|----|---------|----------------------|--------|
| July 2 | 020 | | | | ^ | \sim |
| Su | Мо | Tu | We | Th | Fr | Sa |
| 28 | 29 | 30 | 1 | 2 | 3 | 4 |
| 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 12 | 13 | 14 | 15 | 16 | 17 | 18 |
| 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| 26 | 27 | 28 | 29 | 30 | 31 | 1 |
| 2 | 3 | 4 | 5 | 6 | | 8 |
| Date a | Date and time settings | | | | | |
| | | | Ę | 도 4») - | 2:50 PM 7/28/2020 | 5 |

2. Depending on the operating system, click **Change date and time settings** or **Date and time settings**. The Date and Time window appears (Figure 55).



| Settings | - 🗆 X |
|-------------------------|---|
| ம் Home | Date & time |
| Find a setting | Current date and time |
| Time & Language | 2:58 PM, Tuesday, July 28, 2020 |
| 🗟 Date & time | Set time automatically On |
| 🚳 Region | Set time zone automatically |
| ₄ ^字 Language | Off Set the date and time manually |
| ပ္ Speech | Change |
| | Synchronize your clock Last successful time synchronization: 7/28/2020 2:54:08 PM Time server: time.windows.com Sync now |
| | Time zone |
| | (UTC-06:00) Central Time (US & Canada) |
| | Adjust for daylight saving time automatically On |

- 3. Verify that the **Set time automatically** option is set to **On**.
- 4. Select the correct time zone under the **Time zone** drop-down list box.
- 5. Select Adjust for daylight saving time automatically.
- 6. Close the window to save your changes.

Setting the time zone in the Network Engine Site Director

- 1. Log on the Site Director network engine.
- 2. Drag the Site object to the Display frame.
- 3. Click Edit.
- 4. In the Time section, in the Default Time Zone drop-down box, select the correct time zone for the device (Figure 56).

Figure 56: Default Time Zone in the Site Object

| Time | |
|---------------------|--|
| Default Time Zone | (UTC-06:00) Central Time (US & Canada) |
| Site Time Servers | Listof[0] |
| Device Time Servers | Listof[0] |
| Time Sync Period | 1 hour |

- 5. Click Save.
 - (i) **Note:** The Site object's focus window is updated immediately to indicate the current time and selected time zone, but the blue status bar in the lower right corner does not update until you log off, then log on the network engine again.
- 6. Reset the network engine for the time zone change to take effect.

Setting the date and time on the Site Director

About this task:

Refer to one of the following sections to manually set the date and time:

- Setting the date and time in the Metasys Server Site Director
- Setting the date and time in the Site Director Network Engine

Setting the date and time in the Metasys Server Site Director

About this task:

Follow these steps to set the date and time for a Metasys Server that is configured as the Site Director.

1. In the lower-right corner of the Metasys Server computer screen, click the time. The Date and Time Properties box appears (Figure 57). The appearance of this screen and the next screen vary depending on the operating system.

Figure 57: Time and Date on a Metasys Server Site Director



2. Depending on the operating system, click **Change date and time settings** or **Date and time settings**. The Date and Time window appears (Figure 58).



| Settings | _ | | × |
|-------------------------|---|--------|---|
| வ் Home | Date & time | | |
| Find a setting | Current date and time | | |
| Time & Language | 2:58 PM, Tuesday, July 28, 2020 | | |
| 🗟 Date & time | Set time automatically On | | |
| 👰 Region | Set time zone automatically | | |
| ₄ ^字 Language | Off Set the date and time manually | | |
| D Speech | Change | | |
| | Synchronize your clock | | |
| | Last successful time synchronization: 7/28/2020 2:54:08 PM Time server: time.windows.com | | |
| | Sync now | | |
| | Time zone | | |
| | (UTC-06:00) Central Time (US & Canada) | \sim | |
| | Adjust for daylight saving time automatically | | |
| | On | | |

- 3. Click **Change**. On the Change Date and Time dialog, set the date and time.
 - (i) **Note:** If your operating system has the **Change Set time automatically** option set to **On**, the date and time are controlled by an external time server.
- 4. Click **Change** to save your changes, then close the dialog box. The Site Director date and time are now set and propagate to all other child devices on the site.

Setting the date and time in the Site Director Network Engine

About this task:

Follow these steps to set the date and time for a network engine that is configured as the Site Director.

- 1. In the navigation tree, right-click the Site object and select **Command**. The Command dialog box appears.
- 2. Click **Set Time** and enter a value in the text box (Figure 59).

Figure 59: Time in Site Director Network Engine (SNE example)

| I SNE11000-gr1:SNE11000-gr1/\$site X | | |
|--|--|--|
| Select the command to issue, then click Send. (Specify command parameters, if required.) | | |
| Show Command Set All Commands | | |
| Set Time | | |
| Value 02:29:39 PM | | |
| Set Date | | |
| Update Broadcast Management | | |
| Update All Items Cache | | |
| Global Time Broadcast | | |
| | | |
| Send Cancel | | |

- 3. Click Send.
 - (i) **Note:** If you have a site time server selected, do not attempt to set the time manually. If you have one or more site time servers defined, sending this command generates an error.
- 4. In the navigation tree, right-click the Site object and select **Command**. The Command dialog box appears.
- 5. Click **Set Date** and select a date from the calendar (Figure 60).

Figure 60: Date in Site Director Network Engine (SNE example)



- 6. Click Send.
 - (i) **Note:** If you have one or more site time servers defined, sending this command produces an error. If you have a site time server defined, do not use this command to set the time manually.

The Site Director time zone, date, and time are now set and propagate to all other child devices on the site. Note that it may take up to 10 minutes for all devices to synchronize.

Multicast time synchronization settings

The following table describes the Multicast time synchronization attributes.

| Attribute | Description | |
|-------------------------|--|--|
| Multicast Group Address | Specifies the IP address used to multicast the SNTP message. This address identifies the group of devices to receive the SNTP message. The RFC-2030 defined standard address is 224.0.1.1. The address is configurable to allow site-specific use. | |
| Multicast UDP Port | Specifies the UDP port on which Multicast time synchronization polls and listens for messages. The RFC-2030 defined standard port is 123.The UDP port defined here must match the Time Server's UDP port for successful polling to occur. | |

 Table 37: Multicast Time Synchronization Fields

Table 37: Multicast Time Synchronization Fields

| Attribute | Description |
|------------------------------|--|
| Multicast TTL | Specifies the Time-to-Live (TTL) for a Multicast message. The value indicates the number of router hops allowed (number of routers to pass through) before the message is not sent. Routers must be configured to pass Multicast messages to allow the time sync message to pass. |
| | Note: A default value of 1 typically stops the Multicast message from leaving the IP subnet of the Site Director. Most routers decrease the existing TTL upon arrival of a packet, and drop the packet instead of rerouting it when the TTL reaches 0. |
| Multicast Heartbeat Interval | Specifies the number of minutes between forcing a Multicast time synchronization message from the Site Director to participating devices. |

Verifying the Site Director defined for an engine or server

About this task:

For time synchronization to work properly, all engines and servers on a site must have the correct name for the Site Director in the Local Site Director attribute. If an engine or server has the wrong Site Director specified, time synchronization on your Metasys site does not work properly. Follow these steps:

- 1. Log on the engine or server.
- 2. Drag and drop the engine or server object to the Display frame.
- 3. Select Advanced.
- 4. Scroll to the Site section and verify that the Local Site Director attribute contains the correct device (Figure 61). In this example, the Site Director is a network engine (SNE11000-gr1).
 - (i) **Note:** The Local Site Director may be entered as an IP address or host name. If entered as a host name, the name is case-sensitive (for example, SNE11000-gr1 is not the same as sne11000-gr1).

Figure 61: Site Director Field

| Site | |
|-------------------------|--------------|
| Site Director Online | True |
| Authenticated with Site | True |
| Local Site Director | SNE11000-gr1 |

5. If the Site Director field contains the wrong device or is empty, click **Edit**. Edit the Site Director entry and click **Save**.

Appendix: Configuring and Maintaining Preferences

Configuring and maintaining preferences introduction

The *Metasys* system provides customized preferences for the user interface. The preferences allow authorized users to configure how the user interface behaves, including the sounds and colors, the startup view, and the ability to add links to external applications that can be accessed from within the user interface of the NAE device.

Some steps in the following sections involve certain file operations, such as copying files and navigating to specific folders. The tool used for these operations is NxE85 the NxE Information and Configuration Tool (NCT) for the NAE. For a hardware engine, log on to the device remotely using the NCT, then use the Get File and Copy File options in the **Explorer** tab of the NCT.

For information on the NCT, refer to the *NxE Information and Configuration Tool Technical Bulletin* (*LIT-1201990*).

Preferences Concepts

System and user preferences

Preferences are divided into two categories: System preferences and User preferences.

System preferences

System preferences apply to all users who log on to the site or device. System preferences affect the performance and operation of the system. Only the MetasysSysAgent user and the BasicSysAgent user have authorization to configure system preferences. An audible alarm notification change is an example of a system preference.

Before you make system preference changes, the device reads the preferences from the DefaultSystemPreferences.xml file. Once you make system preference changes, a new file called SystemPreferences.xml is created (Figure 62). Both of these files are located in the directory on the network engine as indicated in Table 38.

| Network engine | File location |
|---|---|
| NCE25/NAE35/NAE45 NAE Device\opt\metasys\var\Preferences\ | |
| (Release 9.0.7 or later) NAE55 (Release 10.0) | NAE Device\opt\metasys\bin\UI\audio\ |
| NAE85 | C:\ProgramData\Johnson Controls\MetasysIII\Preferences C:\Program Files (x86)\Johnson Controls\MetasysIII\UI \audio |

Table 38: Location of preferences files

The procedure to synchronize system preferences within a site or to reuse the system preferences on another site is a manual copy and paste process. Use the process to copy system preferences to other devices on the site or to other sites. See Copying preferences between devices.

Figure 62: System preference files

| MAE NICTool: NAE55-W | |
|--|--|
| Connected - NAE55-W | Quit |
| Connections Tools Explorer About, Etc. | |
| Refresh Device Contents | |
| Directories | Files |
| | UserPreferences-1.xml, created 12/8/2018 12:12:50 PM, 13969 bytes DefaultSystemPreferences.xml, created 12/8/2018 12:12:50 PM, 9065 bytes DefaultUserPreferences.xml, created 12/8/2018 12:12:50 PM, 14451 bytes |
| Successful connection! Getting file list from the device Success | |
| 🔲 Always On Top | Connected - NAE55-W Advanced Mode |

- DefaultSystemPreferences.xml: This is the default system preferences file. It is installed as part of the standard installation for all network engines.
- SystemPreferences.xml: This file stores the configured system preferences. If you have not yet configured system preferences, this file does not appear in the directory.

User preferences

User preferences apply to a specific network engine user. User preferences define how the information is displayed in the user interface and do not affect the operation of the system. The colors and marker styles of a trend display are examples of user preferences. Each user is authorized to view and edit their own user preferences.

The system automatically assigns a numbered user preference file name for each user called UserPreferences-userID.xml, where userID is the identification number of the user. Using an identification number, rather than using the actual user name, serves two purposes. First, it avoids any conflicts that might arise if the user name contains special characters. Second, it allows the user to be renamed without breaking the connection to the user preferences file.

To view user identification numbers, open the Security Administrator screen and select **User Preference File Names** under the **View** menu (this option is available only to the MetasysSysAgent user). The user preference file names appear in the **Roles and Users** pane (Figure 63) and correspond to files on the *Metasys* device in the directory as indicated in Table 38. As shown by two callouts in Figure 63:

- 1: User preference file name as seen in the Security Administration in the user interface.
- **2**: User preference file as seen when accessing a network engine using the NCT.

The procedure to synchronize user preferences within a site or to reuse the user preferences on another site is a manual copy and paste process. Use the manual process to copy user preferences to other devices on the site or to other sites. See Copying preferences between devices.

Figure 63: User preference file

| Security Administration | | | | |
|--|---|--|--|--|
| File Edit Insert View Help | | | | |
| 8 | e e 2 2 | | | |
| Roles and Users Navigation Views | Access Permissions - MetasysSysAgent | | | |
| Roles ADMINISTRATOR ADMINISTRATOR ANALYSIN ADMINISTRATOR DMINISTRATOR ADMINISTRATOR ADMINISTRATOR ADMINISTRATOR A | Key Yermission comes from this user. Permission comes from a role. Permission comes from both the user and a role. Permission comes from both the user and a role. Category Second div Remain and a framework Manage them Manage them Manage them Manage them Mondifier Remain and a come them Manage the | | | |
| | HVAC Q < Q < Q < Q < Q < Q < Q < Q < Q < Q < | | | |
| | Services Q × Q × Q × Q × Q × Q × Q × Q × Q × Q × | | | |

| Connected - NAE55-W Quit Connections Tools Explorer About, Etc. Refresh Device Contents Directories Files Outer Audit Trails DefaultSystemPreferences-1 xml, created 12/8/2018 12:12:50 PM, 13969 bytes DB DefaultSystemPreferences xml, created 12/8/2018 12:12:50 PM, 9065 bytes DefaultUserPreferences xml, created 12/8/2018 12:12:50 PM, 14451 bytes DefaultUserPreferences xml, created 12/8/2018 12:12:50 PM, 14451 bytes DefaultUserPreferences xml, created 12/8/2018 12:12:50 PM, 14451 bytes State Services SQL Data TempSecurityDB TimeManagement Successful connection! | NAE NICTool: NAE55-W | |
|---|--|--|
| Connections Tools Explorer About, Etc. Refresh Device Contents Directories Files Directories Q UserPreferences-1 xml, created 12/8/2018 12:12:50 PM, 13969 bytes DefaultSystemPreferences.xml, created 12/8/2018 12:12:50 PM, 9065 bytes DefaultUserPreferences.xml, created 12/8/2018 12:12:50 PM, 14451 bytes DefaultUserPreferences.xml, created 12/8/2018 12:12:50 PM, 14451 bytes DefaultUserPreferences.xml, created 12/8/2018 12:12:50 PM, 14451 bytes DefaultUserPreferences SteServices SteServices SQLData Send Path \opt\metasys\var\Preferences\ TimeManagement Send Path \opt\metasys\var\Preferences\ Successful connection! Send File | Connected - NAE55-W | Quit |
| Refresh Device Contents Directories Image: Contents Image: Content Image: Conte | Connections Tools Explorer About, Etc. | |
| Directories Files - var 2 - Audit Trails DefaultSystemPreferences.xml, created 12/8/2018 12:12:50 PM, 13969 bytes - DB DefaultSystemPreferences.xml, created 12/8/2018 12:12:50 PM, 14451 bytes - dumps EventRepos - log N50 - PersistData Preferences - SiteServices SiteServices - SQLData Send Path \opt\metasys\var\Preferences\ - TempSecurityDB - Get File Get All Debug Files Successful connection! Send File | Refresh Device Contents | |
| Successful connection! | Directories | d Path \opt\metasys\var\Preferences\ tFie Get All Debug Files Send File |
| Getting file list from the device Success | Successful connection! Getting file list from the device Success | Connected - NAE55-W Advanced Mode |

Managing preferences

System and user preferences stored in a network engine are not saved in the archive database by SCT, and they are not part of the archive upload/download process. Additionally, preferences are not saved during a security backup when you upgrade. You must manage preferences manually.

For information on managing preferences for each preference type, see the following sections:

• System preferences

• User preferences

Detailed Procedures

Configuring preferences

About this task:

- (i) **Note:** To configure the preferences of a specific user, you must log in as that user or as a user with Administrator rights.
 - 1. On the **Tools** menu of the user interface, click **Configure Preferences**. The **Metasys Preferences** dialog box appears.
 - 2. Set the preferences according to the *Preferences* section of the *Metasys Site Management Portal Help (LIT-1201793)*.

If you specified Level 1-4 Sound Files on the **Alarm Settings** tab, place the alarm sound files into the audio folder on the network engine. **Some network engines do not permit the file copy operation because the audio folder is write-protected.** The audio folder is located in the following directory:

For NAE85:

C:\Program Files (x86)\JohnsonControls\MetasysIII\UI\audio

For NCE25/NAE35/NAE45 (Release 9.0.7or later) and NAE55 (Release 10.0 or later):

NAE Device\opt\metasys\bin\UI\audio\

(1) **Note:** If a sound file is missing from the folder, the *Metasys* system uses the default system beep for that alarm priority.

Restoring default system preferences

- 1. Using NCT, connect to the network engine on which you want to restore the default system preferences.
- 2. Click **Start SSH** on the **Connections** tab. NCT now opens a port to the engine for you to use.
- 3. Use an SSH client like PuTTY to log on to the network engine. Use the MetasysSysAgent credentials.
- 4. Navigate to the \opt\metasys\var\Preferences directory on the engine.
- 5. Delete the file with this command: rm SystemPreferences.xml.
- 6. Exit from the SSH client and disconnect the engine from NCT.

Copying preferences between devices

- 1. Using NCT, connect to the source network engine; that is, the one that contains the preferences you want to copy.
- 2. Click the **Explorer** tab, click **Refresh Device Contents**, then navigate to the Preferences directory for the device as shown in Table 38.
- 3. Use **Get File** in NCT to copy SystemPreferences.xml (system preference) or UserPreferences-userID.xml (user preference), where userID is the identification number that appears in the Security Administration tool.
- 4. Paste the file onto the desktop of your computer.
- 5. Disconnect the network engine from NCT.
- 6. Connect NCT to access the destination network engine (where you want to copy the preferences) as the MetasysSysAgent user and navigate to the Preferences directory for the device as shown in Table 38.

7. Use the Send File option in the NCT to paste the SystemPreferences.xml file or UserPreferences-userID.xml file that you copied to your computer desktop with Step 4.

Restoring default user preferences

- 1. Log on to the SMP user interface of the network engine as the MetasysSysAgent user.
- 2. On the **Tools** menu of the user interface, select **Administrator**. The Security Administration tool appears.
- 3. On the **View** menu, select **User Preference File Names**. The user preference file names appear in the **Roles and Users** pane of the Security Administration tool.
- 4. Record the file name of the user whose preferences you want to restore.
 - (i) **Note:** If the user has been removed from the system, there is no record of the user preference file name in the Security Administration tool. In this case, remove user preference files from the network engine that do not have a corresponding user preference file name in the Security Administration tool.
- 5. Close the Security Administration tool and continue with Removing user preference files.

Removing user preference files

- 1. Using the NCT, connect to the network engine from which you want to remove the user preference files and navigate to the Preferences directory for the device as shown in Table 38.
- 2. Delete files named UserPreferences-userID.xml, where userID is the identification number that appears in the Security Administration tool.
 - (i) Note: Do not delete DefaultUserPreferences.xml.

Copying user preferences to another user

- 1. Log on to the SMP user interface of the network engine as the MetasysSysAgent user.
- 2. On the **Tools** menu of the user interface, select **Administrator**. The Security Administration tool appears.
- 3. On the **View** menu, select **User Preference File Names**. The user preference file names appear in the Roles and Users pane of the Security Administration tool.
- 4. Record the file name of the user whose preferences you want to copy (Source User) and the file name of the user whom you want to share those preferences (Destination User).
- 5. Close the Security Administration tool.
- 6. Using NCT, connect to the network engine and click the **Explorer** tab.
- 7. Click **Refresh Device Contents** and navigate to the Preferences directory for the device as shown in Table 38.
- 8. Use the **Get File** option to retrieve a copy of the user preferences file (source user) that you want to duplicate for another user (destination user). Copy the file to an accessible location on your laptop.
- 9. Rename the user preferences file of the source user to match the name of the destination user.
- 10. Use the **Send File** option to send the user preference file of the destination user to the Preferences directory of the engine.

Preserving preferences for a network engine update

About this task:

Preferences do not persist after an engine update unless you take manual steps to save the settings before you begin a system upgrade.

- 1. Before you begin the engine update process, use the NCT to connect to the network engine that contains the preferences and custom files you want to copy.
- 2. Click the **Explorer** tab, click **Refresh Device Contents**, then navigate to the Preferences directory for the device as shown in Table 38.
- 3. Use the **Get File** option in NCT to copy SystemPreferences.xml (system preference) or UserPreferences-userID.xml (user preference), where userID is the identification number for each specific user with customized preferences. If you are saving preferences for multiple users, be sure to retrieve all files. Also, retrieve any special files, such as customized sound .wav files, from the location shown in Table 38.
- 4. Paste these files in a safe location on your computer or network drive, or store them on other media.
- 5. Update the network engine according to the *Metasys Server Installation and Upgrade Instructions (LIT-12012162).*
- 6. With NCT, connect to the updated network engine and use **Send File** to copy the files that you copied in Step 3 back to the appropriate location as listed in Table 38.

Appendix: Certificate Management

(i) **Note:** For details on certificate management for BACnet/SC, refer to the *BACnet/SC Workflow Technical Bulletin (LIT-12013959)*.

Certificate management introduction

Use the Certificate Management option in SCT to manage trusted certificates that are stored in network engines. Enhancements at Metasys Release 8.1 provided for improved security by enabling encrypted communication between Metasys servers and network engines. These enhancements included the option to configure encrypted and trusted communication for network engines. Beginning with Release 9.0, encrypted and trusted communication is available between the Metasys server and network engines. The Site Security Level attribute in the Site object controls this capability. For details, refer to the *ADS/ADX Commissioning Guide (LIT-1201645)*.

When you install or upgrade a Metasys site to Release 8.1 or later, self-signed certificates are installed for the Metasys Server and network engines by default. Self-signed certificates for network engines have three-year durations. Once devices are installed or upgraded, Metasys system communication is encrypted. If a customer is satisfied with encrypted communications, no Certificate Management steps are required. System components come online and communicate as they would at any Metasys software release.

Optionally, if trusted communications is desired, the customer's IT department can generate trusted certificates or obtain trusted certificates from a Certificate Authority (CA) for the Metasys server and network engines. You use the Certificate Management option in SCT to manage trusted certificates for network engines.

(i) **Note:** If you are implementing certificate management on an **existing** Metasys system, keep in mind that adding a trusted certificate may require you to add a domain name to the original host name of a server or engine. This action requires you to rename all data in the Metasys historical databases. You can perform the renaming operation within SCT, but be aware that this procedure requires intensive database operations that significantly prolong a system upgrade. Therefore, be sure to allocate extra time if you are renaming historical data as part of an upgrade to Metasys Release 9.0. For details about renaming a network engine, refer to the *Download* section in *SCT: System Configuration Tool Help (LIT-12011964)*.

The connection status currently active on the computer is indicated by a security shield icon that appears on the Metasys SMP and SCT login windows, and SMP and SCT UI main screens. If the engine is using trusted certificates, a green shield icon with a checkmark appears. If the engine is using self-signed certificates, an orange shield icon with an exclamation mark appears. And finally, if the certificate chain to the engine is broken, the certificate is misnamed, or the certificate has expired, a red shield icon with an X appears. The Metasys UI login screen does not indicate the active connection status.

To help you remember when server certificates installed on network engines expire, the Site object has an attribute called Certificate Renewal Reminder. This attribute regulates when certificate expiration reminders begin. It specifies the number of days prior to security certificate expiration before operators are notified daily that an engine certificate is about to expire. For example, if you use the default period of 60 days, and a server certificate on a network engine expires on January 1, beginning on November 1, an event requiring acknowledgement is sent to operators once a day or until the self-signed certificate is renewed or a new trusted certificate is installed.

For releases 12.0 or later, if you want to manage the BACnet/SC certificates, use the BACnet/SC Management feature that is part of Metasys UI or Johnson Controls System Configuration Tool (JCT). For more information about BACnet/SC certificates and how to manage them, refer to the *BACnet/SC Workflow Technical Bulletin (LIT-12013959)*

The sections that follow describe how to manage security certificates for network engines with SCT, including how to request, upload, and download certificates. You also use Certificate Management to add each Metasys server certificate so that SCT can push the server's root certificate to network engines. Without the root certificate, network engine communication to the Metasys server works, but it is untrusted. For setting up root, intermediate, and server certificates on an Metasys server, refer to the appropriate document: *Metasys Server Installation and Upgrade Instructions (LIT-12012162), Open Application Server (OAS) Installation Guide (LIT-12013222), or NAE85 Installation and Upgrade Instructions (LIT-12011530).*

Figure 64 shows an example of the Certificate Management window in SCT. Open it by clicking **Tools > Certificate Management**. The window has a Certificates tab that includes details about each certificate in the archive. From this window, you can request, export, or delete a certificate. You can also replace an existing certificate with a self-signed certificate.

| Metasys System Configuration Tool | | | | | | | | | |
|--|---|----------|--------------|---------------|-----------------------|-------------------|--------------|--|--|
| <u>I</u> tem <u>E</u> dit <u>V</u> iew <u>A</u> ction I <u>n</u> sert <u>T</u> ools <u>F</u> acili | w Action I <u>n</u> sert Tools Facility Query Help Met*** Logout Exit | | | | | | | | |
| 企 | Certificate Management 🖺 🗆 🛛 🖉 | | | | | | | | |
| All Items Equipment | | | | | | Import Ce | rtificates | | |
| MyArchive | Certificates | Devices | Requests (0) | | | | | | |
| SCT Summary Definitions | Status [| ls | ssued To | Туре | Device | Expiration | Details | | |
| SCT Controller Templates | V (| NAE74 | FE480CA67B | Server | NAE74FE480CA67B | 2018-09-23 | · · · | | |
| User Views | V (| y 🗌 Jcii | | Intermediate | Single | 2022-06-05 | - - - | | |
| | U (| M | 2286559 | Server | M2286559 | 2021-09-20 | • | | |
| | V (|] JC | I Root CA | Root | Single | 2022-06-05 | • | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | De | lete | Export Certificate(s) | | | | |
| | | | Request C | ertificate(s) | Replace Self-sign | | | | |
| | | | | | Sen | ver: 9/27/2016 08 | 3:17 AM CDT | | |

Figure 64: Certificate Management Main Screen

The following table explains each column in the Certificates window. Click inside a column header to sort the column.

Table 39: Description of Certificates Table

| Column Name | Description |
|---------------|--|
| Status | A security shield icon that indicates the connection status afforded by the certificate. |
| | C: encrypted and trusted |
| | U: encrypted and self-signed |
| | Sencrypted, but either the certificate chain to the site or engine is broken, the certificate has a name mismatch, or the certificate has expired. |
| Checkbox Icon | A check box to select the device that you want to work with. |
| Issued To | The name of the device to which the certificate is issued. |

Table 39: Description of Certificates Table

| Column Name | Description |
|-------------|--|
| Туре | The type of certificate: root, intermediate, or server. |
| Device | The device to which the certificate is bound (single or multiple for intermediate and root certificates). |
| Expiration | The date on which the certificate expires. The certificate management tool highlights all certificates that will expire within the number of days specified by the Certificate Renewal Period attribute of the Site object (or have already expired). Also, the Certificate Renewal Period attribute in the Site object controls when certificate expiration reminders begin. It specifies the number of days prior to security certificate expiration before the operator is notified daily that a certificate is about to expire. This attribute is synchronized to all child devices. Certificate Renewal Period applies only to devices at Release 8.1 or later. |
| Details | A clickable arrow that opens an expanded panel with more detailed information about the certificate. |

Certificate Signing Request (CSR)

SCT can generate a certificate signing request (CSR) on behalf of a network engine. However, SCT cannot act as a certificate authority (CA) for signing certificates. Requesting a certificate is a multistep process that involves specifying the following information:

- common name
- email address
- name of organization
- name of organizational unit
- city
- state or province
- name of country

Summary of steps for Network Engine:

- 1. Verify that the device name in the SCT archive and the subject common name for the device match.
- 2. Use SCT to create a CSR and an associated private key for each network engine. See Requesting a certificate.
- 3. Send the CSR for each engine to the internal IT department or CA for signing. The internal IT department or CA returns the signed certificate files.
- 4. Import the signed certificate files for each network engine into the SCT archive. See Importing a certificate.
 - (1) **Note:** You need to import the root certificate, the server certificate, and an intermediate certificate file (if provided). The combination of one root certificate, one or more intermediate certificates, and one server certificate is known as a certificate chain. The certificate chain must be complete for both the server and each network engine to successfully configure a site.

The CSR is complete and SCT removes the certificate request from the Requests table. The private key that SCT previously created is paired with the imported certificate.

- 5. Export all certificate files and store them in a safe and secure location in case you need to reimport them. See Exporting a certificate.
- (i) **Note:** You cannot request a CSR for a device if an existing CSR is still pending. You must delete the existing CSR first.
- Important: The private key that is generated when the CSR is created can be associated with the new certificate only if the device name in the SCT archive and the subject common name for the device match. Therefore, before requesting a device CSR, verify that the device name is correct. If not, the newly purchased certificate could be worthless because of the device name mismatch. A common mistake is to forget to include the company domain name with the CSR. No workaround is available that can recover the use of the new certificate.

Import certificate

Use SCT to import certificates and private keys from the local file system. Three file formats are supported: *.pem, *.cer, and *.crt. Typically, each device has two or three certificate files to import: one root, one intermediate, and one server certificate. Some devices may have more than one intermediate certificate. Whatever the case, always import every certificate file that the customer's IT department or CA provides from the CSR you sent them.

SCT supports the import of only one certificate at a time. For example, if the root and intermediate certificate information comes in a single file, you need to split it into two different files, one for the root and the other for the intermediate certificate.

When you import a server certificate, SCT pairs the imported server certificate with the private key from the associated CSR. If a server certificate is imported that contains an identical Issued To Common Name (CN) as an existing certificate, the imported certificate replaces the existing certificate, but the private key is retained; it is not replaced.

Export certificate

Use SCT to export certificates and private keys to the local file system. Exporting certificates is an optional precautionary measure that allows you to export and store certificates to a computer or removable media for safekeeping. Keep in mind that certificates with private keys are sensitive information that you should treat as highly confidential files.

Three file formats are supported: *.pem, *.cer, and *.crt. Typically, each device has two or three certificate files to export: one root, one intermediate, and one server certificate. Some devices may have more than one intermediate certificate. Whatever the case, always export every certificate file that the customer's IT department or CA provides from the CSR you sent them.

Certificate list view

Use the certificate list view to determine if all certificates required by each device reside in the archive. The certificate list view provides these features:

- Indication of an expired certificate.
- Indication of whether a certificate is required in one or more certificate chains used by a device in the archive. The list view also makes clear which certificates are not needed and may be deleted.
- Information about the certificate, including: Issued To, Type, Device Name (server certificates), Expiration Date, Details (for example, SHA1 Thumbprint).
- Clickable column headers that sort the rows by the data in that column.
- Options for importing, exporting, and deleting root, intermediate, or server certificates.

Figure 65: Viewing Certificate Details

| Metasys System Configuration Tool | | | | | | | | |
|--|--------------|---|--|--|---|------------------------------------|-------------------|-----|
| Item Edit View Action Insert Tools Facility Query Help Met*** Logout Exit | | | | | | | | it |
| û | \ominus | ⊂ ⊂ Certificate Management 🕆 🗋 🗖 🖉 | | | | | | 2 |
| All Items Equipment | | | | | | Imp | oort Certificates | |
| 🗏 🏀 MyArchive | Certificates | Devices | Requests (1) | | | | | |
| Configuration Data | Status | | Issued To | Туре | Device | Expiration | Details | |
| SCT Controller Templates | | | NAE74FE480CA67B | Server | NAE74FE480CA67B | 2018-09-23 | Þ | |
| User Views | | | JCIIssue3 | Intermediate | Single | 2022-06-05 | + | |
| | U | | M2286559 | Server | M2286559 | 2021-09-20 | • | |
| Image: Provide the state of the s | | > | JCI Root CA | Root | Single | 2022-06-05 | Θ | |
| | | Valid F Valid T Issuer Subjer AKID SKID SHA-1 | rom Mon Jun (ro Sun Jun (CN=JCI R =Milwauk ct CN=JCI R =Milwauk N/A T7C754C Thumbprint CDD6282 | 520:39:53 CDT 200 521:35:49 CDT 202 oot CA, OU=Global I se, S=WI, C=US, E=c oot CA, OU=Global I se, S=WI, C=US, E=c 5DA126B897105BD 541FE170090F08E | 96 12 Infrastructure, O=Johnson C JarkI.bobert@jci.com Infrastructure, O=Johnson C SlarkI.bobert@jci.com B8FD4BAEA2C528D994 9503062F44549D1E86 | ontrols INC., L ontrols INC., L | | |
| | | | [| Delete Export | Certificate(s) | | | |
| | | | | | | Server: 9/27/2 | 016 11:32 AM C | CDT |

Certificate tree view

Use the certificate tree view to verify the certificate chain, which is the combination of root, intermediate, and server certificates required by the device. This information is important because the certificate chain must be complete to successfully configure a site. The certificate tree view displays the following:

- **Root certificate**: the highest level certificate; only one for each device.
- **Intermediate certificate**: one level for each intermediate; there may be none, ore, or multiple.
- Server certificate: the lowest level certificate; only one for each device.

The certificate tree view indicates if the certificate chain is missing or incomplete for any device. For each certificate, the following data is shown:

- **Issued To:** the common name (CN) field. For server certificates, the common name must exactly match the device's computer name (hostname).
- **Expiration:** date when the certificate is set to expire.
- **Details:** drop-down box that contains the SHA1 Thumbprint to distinguish certificates with the same common name.

Figure 66: Certificate Chain View

| Metasys System Configuration Tool | | | | | | |
|--|------------------------------|----------|-----------|--------------------|---------------|-----------------|
| <u>Item Edit View Action Insert Tools Facility</u> | y <u>Q</u> uery <u>H</u> elp | | | | Met*** | ogout Exit |
| û | \ominus | | Certifica | ate Management | | 2 🗆 🖉 |
| All Items Equipment | | | | | Impor | t Certificates |
| 🖻 🏠 MyArchive | Certificates | Devices | Requests | | | |
| | Status | | | Device | | Details |
| | U | | | M2286559.cg.na.jci | .com | • |
| | | ŧ | | NAE74FE480CA6 | 7B | • |
| | | Issue | ed To | Expiration | Detai | Is |
| | JCI Ro | ot CA | | 2022-06-05 | 022-06-05 | |
| | JCIIs | ssue3 | | 2022-06-05 | Þ | • |
| | N/ | E74FE480 | CA67B | 2018-08-24 | + | |
| | | | | | | |
| | | | | | | |
| < | | | | Ser | ver: 9/21/201 | 16 10:20 AM CDT |

The following example shows the certificate chain view when a certificate is missing.

Figure 67: Missing Certificate Example

| ⊢[- | - Certificate Management | | | | | | | | | 2 | |
|-----|---------------------------|------------|-------------|---------|-----------|-----------|--------|----------|-----------|----------|---|
| | | | | | | | | In | nport Cer | tificate | s |
| Cer | tificates | Devices | Request | s (0) | | | | | | | |
| | Statu | 6 | | 1 | | | Device | | | | |
| | × | | | | | MAIN-ADX | | | Ŧ | | |
| | | Issue | d To | | | Expiratio | n | | | | |
| | No Server Certificate | | | ??? | | * | | | | | |
| | This certificate is missi | | | ng, and | l must be | imported | đ | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | 1.1 | Uplo | ad | |)ownloa | ad | Export | Certific | ate(s) | | |
| | | Request Ce | tificate(s) | Repl | ace Sel | lf-sign | | | | | |

Download certificate

Use the Download Certificate option to download server certificates independently from other actions. This method is much faster than if you were to download the full database with the Download To Device option under Manage Archive.

When you download certificates to a site device, SCT determines the correct set of certificates required by that device for successful site configuration. If any certificates are missing, SCT includes the set of certificates that it recognizes during the download, but the missing certificates need to be imported before trusted connections can be established. Also, no certificates are downloaded if the server certificate and private key for that device are not present in the SCT archive.

Detailed procedures

Follow these procedures to manage certificates in a network engine.

Requesting a certificate

About this task:

To request a certificate for a network engine in an archive database:

- 1. Open the archive database.
- 2. Verify that the network device name in the archive matches the subject common name of the online network engine. If not, change the network device name in the archive to match the online network engine name.
- 3. On the Tools menu, select **Certificate Management**. The Certificate Management screen appears.
- 4. Click the **Devices** tab. The Devices screen appears.

Figure 68: Request Certificate - Devices Tab



5. Click the network engine for which you want to request a certificate. Click **Request Certificate(s)**. The Request Certificate(s) form appears.

Figure 69: Request Certificate(s) Form

| Request Certificate(s) | × |
|--|---|
| Request Certificate(s) | |
| CSR information for M2286559:NAE74FE480CA67B | |
| | |
| Email Address | |
| my.name@jci.com | |
| Organization Name | |
| Johnson Controls | |
| Organization Unit Name | |
| BE | |
| City | |
| Milwaukee | |
| State/Province | |
| WI | |
| Country Name | |
| | |
| | |
| | |
| Cancel Save CSR Details | |

6. Complete all the fields on the form. Click **Save CSR Details**. An Export CSR(s) confirmation window appears.

Figure 70: Export CSR(s) Confirmation



7. Click **Yes** to continue. The Export CSR(s) - Select Folder window appears.

Figure 71: Export CSR(s) - Select Folder

| Export CSR(s) - Select Folder | | X |
|-------------------------------|---|----------------------------------|
| Look In 📄 All Users | | |
| Adobe | Application Data BeyondTrust Canneverbe Limited | Dell I Desktop I Documents |
| Apple | Cisco Corel | Favorites |
| Folder Name: | | |
| Files of <u>T</u> ype | | Export Cancel |
| | | Export |

- 8. Browse to a folder where you want to save the CSR file and click **Export**. The certificate request file with a .PEM extension is exported to the selected folder. For example, the certificate request file for a network engine called NAE-1 on a computer called ADX-1 would be **ADX-1_NAE-1_CSR.PEM** for a network engine with a fully qualified name of ADX-1:NAE-1.
- 9. Send the certificate request file to the IT department to obtain your trusted certificate. When you receive the file, go to Importing a certificate to import the certificate into SCT for the network engine.

Importing a certificate

About this task:

To import a certificate for a network engine in an archive database:

- 1. Open the archive database.
- 2. On the Tools menu, select **Certificate Management**. The Certificate Management screen appears.
- 3. Click **Import Certificates**. The Import Certificates dialog box appears.
Figure 72: Request Certificate Screen

| Metasys System Configuration Tool | | | | | | |
|--|---|---------|--------------|-----------------|-----------------------|--|
| <u>I</u> tem <u>E</u> dit <u>V</u> iew <u>A</u> ction I <u>n</u> sert <u>T</u> ools <u>F</u> acility | Item Edit View Action Insert Tools Facility Query Help Met*** Logout Exit | | | | | |
| 企 | \ominus | | Certificate | Management | | |
| All Items Equipment | | | | | Import Certificates | |
| 🖻 🏀 MyArchive | Certificates | Devices | Requests (1) | | | |
| Configuration Data | ~ | R | equested On | Device | Details | |
| SCT Controller Templates | ~ | : | 2016-09-27 | NAE74FE480CA67B | • | |
| | | | | | | |
| | | | Delete | Export PEM(s) | | |
| | | | | Server: 9 | /27/2016 09:56 AM CDT | |

4. Select the certificate file. The file has a .crt, .cer, or .pem extension. Click **Import**. The certificate for the network engine is imported.

Figure 73: Import Certificates Screen

| Import Certi | ficates | × |
|-----------------------|----------------------------------|---------------|
| Look In | All Users | / 🖆 🏠 🖀 🔳 👰 |
| SymEFA | ASI M2286559_NAE74FE480CA67B.cer | |
| Tahoo! (| Companion | |
| File <u>N</u> ame | M2286559_NAE74FE480CA67B.cer | |
| Files of <u>T</u> ype | Certificates (.crt, pem, cer) | - |
| | | Import Cancel |

5. Click the **Certificates** tab to view the newly imported certificate.

Figure 74: Newly Imported Certificate

| Metasys System Configuration Tool | | | | | | | | |
|---|---|----------------------------|-----------------|-----------------|-----------------|----------------|------------------|-----|
| Item Edit View Action Insert Tools Facility | em Edit View Action Insert Tools Facility Query Help Met*** Logout Exit | | | | | | | |
| û | \ominus | Certificate Management 🛅 🗖 | | | | | 10 🛛 | 2 |
| All Items Equipment | | | | | | Imp | ort Certificates | |
| 🗏 🌍 MyArchive | Certificates | Devices | Requests (1) | | | | | |
| SCT Summary Definitions | Status | | Issued To | Туре | Device | Expiration | Details | |
| SCT Controller Templates | V | | NAE74FE480CA67B | Server | NAE74FE480CA67B | 2018-09-23 | • | |
| □ ■ | | | | | | | | |
| | | | | Delete Export 0 | Certificate(s) | | | |
| | | | | | | Server: 9/27/2 | 016 11:32 AM | CDT |

Exporting a certificate

About this task:

To export a certificate for a network engine in an archive database:

- 1. Open the archive database.
- 2. On the Tools menu, select **Certificate Management**. The Certificate Management screen appears.
- 3. Click the **Devices** tab. A table of devices with certificates appears. Select the device whose certificate you want to export.

Figure 75: Exporting a Certificate

| Metasys System Configuration Tool | ti na sette | | | | | - • × |
|--|-------------------------------|---------|---------------|----------------|-------------------------------|-----------------------------|
| Item Edit View Action Insert Tools Facilit | ty <u>Q</u> uery <u>H</u> elp | | | | | Met*** Logout Exit |
| <u>گ</u> | ⊣→ | | | Certificate M | lanagement | |
| All Items Equipment | | | | | | Import Certificates |
| 🗏 🌀 MyArchive | Certificates | Devices | Requests (1) | | | |
| SCT Summary Definitions | Statu | S | | | Device | Details |
| SCT Controller Templates | U | | | | M2286559 | • |
| | Ų | | ţ | × | NAE74FE480CA67B | > |
| | | | Upload | 3 C | ownload Export Certificate(s) | |
| | | | Request Certi | ficate(s) Repl | ace Self-sign | |
| | | | | | Sen | ver: 9/27/2016 02:05 PM CDT |

4. Click **Export Certificate(s)**. The Export Certificates dialog box appears.

| Export Certifi | cate(s) - Select Folde | er | | × |
|---|------------------------|---|---|---|
| Look <u>I</u> n | All Users | | 🗾 🖆 🏠 🛅 | |
| 1e Adobe Altova Apple Apple Cor | mputer | Application Data BeyondTrust Canneverbe Limited Cisco Corel | Dell Desktop Documents Favorites | |
| Folder <u>N</u> ame: Files of <u>T</u> ype | C:\Users\All User | s) Expo | rt Certificate(s) Cancel | |

Figure 76: Export Certificate(s) - Select Folder Screen

5. Click **Export Certificate(s)**. The certificate file is exported to the selected folder location. For example, if the name of the NAE is NAE-1, the certificate file would be called **NAE-1.pem**.

Downloading a certificate

About this task:

To download a certificate to a network engine from an archive database:

- 1. Open the archive database.
- 2. On the Tools menu, select **Certificate Management**. The Certificate Management screen appears.

Figure 77: Downloading a Certificate

| Metasys System Configuration Tool | | | | | |
|---|-------------------------------|--------------------------|-----------------------------|--|----------------------------|
| <u>I</u> tem <u>E</u> dit <u>V</u> iew <u>A</u> ction I <u>n</u> sert <u>T</u> ools <u>F</u> acilit | ty <u>Q</u> uery <u>H</u> elp | | | | Met*** Logout Exit |
| Ê | $\Theta \to$ | | Certificate Mana | gement | 2 🗆 🖉 |
| All Items Equipment | | | | | Import Certificates |
| 🗏 🌐 MyArchive | Certificates Devices | Requests (1) | | | |
| SCT Summary Definitions | Status | | | Device | Details |
| SCT Controller Templates | U | | | M2286559 | • |
| M2286559 Summary Definitions M2286559 (8.1) NAE74FE480CA67B (8.1) NAE00D0C9B9A950 (8.0) | Ų | ŧ | V | NAE74FE480CA67B | • |
| | | Upload Request Certif | l Dowr ficate(s) Replace | nload Export Certificate(s) Self-sign | |
| | | | | Serv | er: 9/27/2016 11:39 AM CDT |

3. Select the device that has the certificate you want to download. (If you need to download the certificates of multiple engines, you can select more than one from the devices table.) Click **Download**. The Certificate Download Wizard appears.

| Certificate Download | d Wizard | | | x | | | | |
|---|--------------------------------------|--|--------|---|--|--|--|--|
| Start Site Login Specify Retries Summary Finish | Set this o Network (Note that | Site Login Set this option if the destination device is not accessible on the Local Area Network (behind a firewall, for example). Note that this option will slow the operation if used unnecessarily. | | | | | | |
| | The use Usernam Passwor | The username and passwords for each engine are required below. Username: Password: Test Login | | | | | | |
| | M22 | ice 286559:NAE74FE480CA67B | Status | | | | | |
| | Ca | ancel 🔍 Back Next 🕨 | Last | | | | | |

- 4. Specify the username and password of the network engine (or click Communicate via Site Director to use the Site Director's credentials). Click Test Login. When the login is confirmed, click Next to complete the remaining steps in the Certificate Download Wizard. The ActionQ window appears to indicate the progress of the download. A completion status of OK indicates that the certificate download process was successful.
- 5. Close the ActionQ window.

Uploading a certificate

About this task:

To upload a certificate from a network engine to an archive database:

- 1. Open the archive database.
- 2. On the Tools menu, select **Certificate Management**. The Certificate Management screen appears.

3. Click the **Devices** tab. A table of devices with certificates appears. Select the device that has a certificate you want to upload. (If you need to upload the certificates of multiple engines, you can select more than one from the devices table.)

| Metasys System Configuration Tool | | | | | | |
|--|----------------------|-------------------------|---------------------------|--|----------------------------|--|
| tem Edit View Action Insert Tools Facility Query Help Met*** Logout Exit | | | | | | |
| û | \ominus | | Certificate Mana | gement | 2020 | |
| All Items Equipment | | | | | Import Certificates | |
| MyArchive | Certificates Devices | Requests (1) | | | | |
| SCT Summary Definitions | Status | | | Device | Details | |
| SCT Controller Templates | U | | | M2286559 | | |
| □ ↓ M2286559 □ ↓ User Views □ ↓ Summary Definitions □ ↓ M2286559 (8.1) □ ↓ M4274FE480CA67B (8.1) □ ↓ NAE74FE480CA67B (8.1) □ ↓ NAE74FE480CA67B (8.1) | Ų | ŧ | Ø | NAE74FE480CA67B | > | |
| | | Upload Request Certi | Dowr ficate(s) Replace | nload Export Certificate(s) Self-sign | | |
| | | | | Serv | er: 9/27/2016 11:39 AM CDT | |

Figure 79: Uploading a Certificate

4. Click **Upload**. The Certificate Upload Wizard appears.

Figure 80: Certificate Upload Wizard

| Certificate Upload V | Vizard | × |
|---|--|--|
| Start Site Login Specify Retries Summary Finish | Set this option if the destination device is in Network (behind a firewall, for example). Note that this option will slow the operation Communicate The username and passwords for each Username: ********* Password: ******** Test Login M2286559:NAE74FE480CA67B | .ogin not accessible on the Local Area n if used unnecessarily. via Site Director engine are required below. |
| | Cancel 🖪 Back Next 🕨 | Last |

- 5. Specify the username and password of the network engine (or click **Communicate via Site Director** to use the Site Director's credentials). Click **Test Login**. When the login is confirmed, click **Next** to complete the remaining steps in the Certificate Upload Wizard. The ActionQ window appears to indicate the progress of the upload. A completion status of **OK** indicates that the certificate upload process was successful.
- 6. Close the ActionQ window.

Deleting a certificate

About this task:

To delete a network engine certificate from an archive database:

- 1. Open the archive database.
- 2. On the Tools menu, select **Certificate Management**. The Certificate Management screen appears.
- 3. Select the device whose certificate you want to delete. Click **Delete**. A confirmation message appears.
- 4. Click **OK** to delete the certificate. The certificates list refreshes indicating that the certificate is removed.

Deleting a certificate request

About this task:

Follow these steps to delete a network engine certificate request from an archive database.

- 1. Open the archive database.
- 2. On the Tools menu, select **Certificate Management**. The Certificate Management screen appears.
- 3. Select the device whose certificate request you want to delete. Click **Delete**. A confirmation message appears.

Figure 81: Delete CSR Confirmation Message

| Delete CSR | x |
|--|----------|
| Warning! If you delete this CSR, its private key will be permanently deleted which may cau problems. To delete the CSR, enter the device reference of M2286559:NAE74FE480CA678 in the area below and click the OK button | ise B |
| M2286559:NAE74FE480CA67B OK Cancel | |

4. Click **OK** to delete the certificate request. The certificate requests list refreshes indicating that the certificate request has been removed.

Replacing a self-signed certificate

About this task:

Follow these steps to replace an existing certificate with a new self-signed certificate for a network engine in the archive database. This procedure is useful if you need to replace an expired or compromised trusted certificate with a self-signed certificate.

- 1. Open the archive database.
- 2. On the Tools menu, select **Certificate Management**. The Certificate Management screen appears.
- 3. Click the **Devices** tab. A table of all devices with certificates appears.

Figure 82: Devices Tab in Certificate Management

| Metasys System Configuration Tool | | | | | | | |
|--|---|--------------------------|----------------------------|--|----------------------------|--|--|
| <u>I</u> tem <u>E</u> dit <u>V</u> iew <u>A</u> ction I <u>n</u> sert <u>T</u> ools <u>F</u> acili | em <u>E</u> dit <u>V</u> iew <u>A</u> ction I <u>n</u> sert <u>T</u> ools <u>Facility</u> <u>Q</u> uery <u>H</u> elp Met*** Logout Exit | | | | | | |
| 企 | \ominus | | Certificate Mana | gement | 2020 | | |
| All Items Equipment | | | | | Import Certificates | | |
| 🗏 🍘 MyArchive | Certificates Devices | Requests (1) | | | | | |
| SCT Summary Definitions | Status | | | Device | Details | | |
| SCT Controller Templates | | | | M2286559 | • | | |
| K M2286559 K M228655 K M228655 K M22865 K M228 K M22865 K M228 K M22865 K M228 K M22 K M22 K M22 K M22 K M22 K M2 K M K M2 K M | • | | | NAE74FE480CA67B | • | | |
| | | Upload Request Certif | i Dowr īcate(s) Replace | nload Export Certificate(s) Self-sign | | | |
| | | | | Serv | er: 9/27/2016 11:34 AM CDT | | |

4. Select the device and click **Replace Self-sign**.

Backing up a certificate

About this task:

To back up a certificate for a network engine, create a backup of the archive database using the traditional method in SCT (**Tools > Database > Create Backup**). In addition to backing up the archive database, this process also backs up the network engine certificates. For details, refer to the *Create Backup* section in *Metasys SCT Help (LIT-12011964)*. You can also back up and store certificates for safekeeping by exporting each certificate file to a computer or removable media. Refer to the *Exporting a Certificate* section in *Metasys SCT Help (LIT-12011964)*. Lastly, certificates are also backed up and stored when you export the archive database. Refer to the *Export Database* section in *Metasys SCT Help (LIT-12011964)*.

Important: As an important restriction for creating and restoring database archive backups that contain network engine certificates, you must use the same SCT computer for both operations. Do not restore the archive using a different SCT computer, or the certificate data is deleted. This is a security precaution that protects against certificate theft.

Appendix: Erasing Network Engine SDRAM and flash memory

Erasing Network Engine SDRAM and flash memory

Network engines have two types of memory: synchronous dynamic random access memory (SDRAM) and flash memory. SDRAM contains data dynamic memory for network engine operations. Flash memory stores the operating system, configuration data, and operations data storage and backup. You can erase either type of memory from the network engine.

The SDRAM memory of a network engine is cleared when the network engine loses power or is restarted through a soft boot. The on-board battery retains power to the system during the shutdown process. After all the LEDs on the engine front cover turn off, the memory is cleared.

The Flash memory of a network engine is cleared when you re-image the network engine with the NAE Update Tool using the PXE Only method. This operation removes all database and trend information, and replaces the system with the factory default image. You must use the PXE Only update, not the HTTP method, to delete all static and changed files from the network engine.

Use the following procedure to completely erase the Flash memory from any of these supported network engine models: MS-NCE25xx-0, MS-NAE35xx-2, MS-NAE45xx-2, MS-NxE55xx-0, MS-NxE55xx-1, and MS-NxE55xx-3. If you need more details than what is provided here, refer to *NAE Update Tool Help (LIT-12011524*).

- 1. Start the NAE Update Tool from the Start menu on your computer by selecting **Programs** > **Johnson Controls** > **Metasys** > **NAE Update Tool**.
- 2. If your computer has more than one network card, the **Select Ethernet Adapter** screen appears. Select the **wired** Ethernet card and click **OK**. The main screen of the NAE Update Tool appears.

Figure 83: NAE Update Tool – Main Screen



- 3. Enable verbose messaging in the message window by selecting **Advanced Mode** in the **Options** menu.
- 4. On the NCE/NAE/NIE menu, select the **Add** option, and select the type of network engine whose Flash memory you want to erase. The update target window appears.

Figure 84: Example of Adding a Network Engine Target

| General Settings | | |
|-----------------------------|--|--|
| Target device to be updated | | Enable DHCP or Fixed IP Address Information |
| Description: | NAE55-W | Enable DHCP |
| MAC address: | 00-80-66-05-05-EF | IP Address: |
| Host Name: | NAE55-W | IP Mask: |
| Status: | Enabled 🔻 | IP Router Address: |
| | | DNS Server IP Address: |
| File | Juices | Update Process To Use |
| File | | Update Process To Use |
| Disk image: | NAE55-NIE55_9.0.2.6438.dn2 | ···· PXE Only (update devices in this subnet only) ▼ |
| Login Informati | on for HTTP Update Process o | r to remotely start the update |
| User Name: | MetasysSysAgent If Test Login fails using configured values, enter the current Host Name or IP Address here | |
| Password: | •••••• | Before Update |
| | | |
| | | |

- 5. Under this General Settings tab, specify the required information for the network engine.
- 6. If the device is an NCE25, NAE35, or NAE45, you **must** select **Extended** for the Update type and select the **Add UI Resources** check-box if you need to add a user interface resource file with the update.

If the device is an NAE55, the Update type entry is not required.

- 7. In the **File** section, click the browse button and select the correct image file to use for the engine type.
- 8. In the **Enable DHCP or Fixed IP Address Information** section, specify the following values:
 - **Enable DHCP (Check Box):** Mark this check box if the network engine obtains its IP address from a DHCP server on the network (default). Do not mark **Enable DHCP** if the network engine is assigned a static IP address. If you clear this option, the next four fields become editable.
 - **IP Mask:** If DHCP is not enabled, enter appropriate values for these attributes. You can retrieve these fields from the device if you specify the engine's login credentials and click **Test Login Before Update**. These IP entries are written to the device at the end of the update, saving you the step of doing so manually.
- 9. For the update process, select **PXE Only (update devices in this subnet only)**. This is the only update method that erases all network engine Flash memory.

- 10. If you wish to test logging into the device, specify the login information for the network engine as follows:
 - **User Name** and **Password**: Specify a valid user name and a valid password to access the device. You can use the MetasysSysAgent user with its current password. Note that the default password for the MetasysSysAgent user changed at Release 6.0. For more information, contact your local Johnson Controls representative.
 - **Test Login Before Update:** Click this button to test whether you can login to the device. If Test Login fails using configured values, enter the current Host Name or IP Address here.
- 11. After you have entered all necessary fields, click **OK** to save your entries and return to the Main screen.
- 12. On the NAE Update Tool Main screen, make sure that the **Status** column entry for the network engine whose Flash memory you are erasing is **Enabled**.
 - (i) **Note:** If the **Status** entry is not **Enabled**, double-click the row for the network engine that you want to update. The **Edit update target** screen appears. In the **Status** drop-down box, select **Enabled** and click **OK**.
- 13. Verify that no one is currently logged in to the network engine. If so, log out before proceeding. Also, during the update process, make sure that you do not exit the NAE Update Tool or turn off power to the network engine. Doing so adversely affects the process.
- 14. Highlight the network engine in the Target list and click **Update Device**. The network engine receives the request and the update begins.

If the update does not start, perform a software reset of the device from the SMP UI. In the Navigation tree, right-click the network engine, then select **Commands** > **Reset Device**.

The Log window shows the update progress. An Update Complete message in the log indicates a successful update. If any errors occur, refer to the *Troubleshooting* section in *NAE Update Tool Help (LIT-12011524)*.

- 15. When the Status column for the network engine indicates **Completed**, log in to the newly updated network engine by using the IP address displayed in the log portion of the tool.
- 16. Close the NAE Update Tool. The Flash memory is erased and replaced with the factory disk image. The SDRAM is also refreshed by the restart process.

Software terms

Use of the software that is in (or constitutes) this product, or access to the cloud, or hosted services applicable to this product, if any, is subject to applicable end-user license, open-source software information, and other terms set forth at www.johnsoncontrols.com/techterms. Your use of this product constitutes an agreement to such terms.

Product warranty

This product is covered by a limited warranty, details of which can be found at www.johnsoncontrols.com/buildingswarranty.

Patents

Patents: <u>https://jcipat.com</u>

Contact information

Contact your local branch office: <u>www.johnsoncontrols.com/locations</u> Contact Johnson Controls: <u>www.johnsoncontrols.com/contact-us</u>

© 2022 Johnson Controls. All rights reserved. All specifications and other information shown were current as of document revision and are subject to change without notice.