# Contents

Introduction...................................................................................................................................... 7

Summary of changes.......................................................................................................................7

NAE commissioning overview........................................................................................................ 8

   Network Automation Engines (NAEs)................................................................................................. 8

   NCE25 models - Release 9.0.7................................................................................................... 8

   NAE35 models - Release 9.0.7................................................................................................... 9

   NAE45 models - Release 9.0.7................................................................................................... 9

   NAE55 models - Release 10.0.................................................................................................... 9

   NAE-S model - Release 8.1.......................................................................................................10

   NxE85 model - Release 10.0.................................................................................................... 10

Warning banner...................................................................................................................................11

MS/TP communications bus.............................................................................................................. 11

Metasys network sites......................................................................................................................... 12

NAE commissioning............................................................................................................................ 14

NAE configuration............................................................................................................................... 15

Site Management Portal user interface........................................................................................... 16

Metasys UI........................................................................................................................................ 18

Metasys help files............................................................................................................................. 19

Browser recommendations for downloading the Launcher............................................................19

System Configuration Tool (SCT)....................................................................................................... 19

Controller Configuration Tool (CCT).................................................................................................. 20

Archive databases............................................................................................................................... 20

NAE disk image updates and archive database upgrades.............................................................21

Site Director..........................................................................................................................................21

NAE computer name...........................................................................................................................22

NAE object name................................................................................................................................. 22

Basic Access operating mode.......................................................................................................... 22

Login user names and passwords.................................................................................................... 23
NAE connectivity.................................................................................................................................25
Time zone, date, and time management..............................................................................................25
Alarms and events..................................................................................................................................25
Email notification....................................................................................................................................26
Syslog DDA.............................................................................................................................................27
Simple Network Management Protocol (SNMP) notification...............................................................30
RADIUS overview.................................................................................................................................31
Initial default NAE configuration........................................................................................................32
Allow HTTP...........................................................................................................................................33
Advanced Security Enabled................................................................................................................35
System and user preferences..............................................................................................................35
Reset Device command......................................................................................................................35
NAE network sensitivity.......................................................................................................................36

Detailed Procedures.............................................................................................................................37
Installing Launcher to access the NAE....................................................................................................38
Establishing direct connection to an NAE............................................................................................40
Preparing NAE for a network that supports DHCP and DNS..............................................................40
Preparing NAE for a network without DHCP and without DNS support when the NAE uses APIPA.........................................................................................................................43
Preparing NAE for a network without DHCP and without DNS support when the NAE uses a static IP address....................................................................................................................44
Preparing NAE for a network that supports DHCP but not DNS.........................................................45
Preparing NAE for a network that supports DNS but not DHCP.......................................................46
Accessing Site Management Portal UI on an NAE................................................................................46
Establishing basic NAE parameters in the focus screen......................................................................47
Establishing NAE network parameters...............................................................................................48
Creating email alarm and event notifications and destinations..........................................................50
Configuring encrypted email................................................................................................................54
  Configuring encrypted email with no authentication required..........................................................54
  Configuring encrypted email with SMTP authentication.................................................................55
Configuring encrypted email with POP-before-SMTP authentication .............................................. 55
Creating NAE SNMP alarm notifications and destinations ................................................................. 56
Enabling Syslog reporting .................................................................................................................. 59
Configuring RADIUS server .............................................................................................................. 61
Adding RADIUS users ....................................................................................................................... 64
Setting the time, date, time zone, and time synchronization .......................................................... 66
Setting up NAE alarm parameters ..................................................................................................... 67
  Editing existing alarm parameters ...................................................................................................... 67
  Creating new alarms .......................................................................................................................... 68
Designating an NAE as a child of a Site Director .............................................................................. 68
Changing Site Director with the SCT ............................................................................................... 70
Removing user accounts from a demoted Site Director ..................................................................... 70
  Moving security database and clearing it from demoted Site Director prior to Release 6.0 ............ 71
  Moving security database and clearing it from demoted Site Director Release 6.0 or later ............. 71
Enabling and disabling Warning Banner .......................................................................................... 72
Adjusting NAE network sensitivity .................................................................................................... 73
Replacing an NAE ................................................................................................................................ 77
Troubleshooting .................................................................................................................................. 78
  Common NAE problems .................................................................................................................... 78
  Corrupted NAE memory .................................................................................................................... 78
  Login problems ................................................................................................................................. 80
  RADIUS errors ............................................................................................................................... 80
  Situations when Metasys system login screen appears for RADIUS users .................................. 80
  Network connection related problems ............................................................................................ 82
  NAE reset related problems ............................................................................................................. 82
  Troubleshooting guide ....................................................................................................................... 82
NAE diagnostic tools .......................................................................................................................... 86
  NAE LED status indicators ............................................................................................................... 86
Downloading a certificate ........................................................................................................ 142
Uploading a certificate ........................................................................................................... 143
Deleting a certificate ............................................................................................................ 145
Deleting a certificate request .............................................................................................. 146
Replacing a self-signed certificate ....................................................................................... 146
Backing up a certificate ........................................................................................................ 147

Appendix: Erasing Network Engine SDRAM and flash memory........................................ 147
   Erasing Network Engine SDRAM and flash memory......................................................... 147
Introduction

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
• 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. 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).

Note: In this document, NAE refers to all NCE25, NAE35, NAE45, NAE45-Lite, NAE55, and NxE85 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 NxE85 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)
• NxE85 Series: refer to the NxE85 Commissioning Guide (LIT-12011044)
• Secure NAE-S: refer to the NAE-S Commissioning Guide (LIT-12012269), a confidential Johnson Controls document

Lastly, for information about commissioning an NAE to use the four built-in third-party integrations, refer to the specific NAE/NIE document that covers the integration that you want to add, listed in Table 28.

Summary of changes

The following information is new or revised:

• Updated screens throughout the document to indicate the new or revised content.

• Updated Launcher screen examples and content throughout the document.

• Added new material on adjusting the NAE network sensitivity in two sections: NAE network sensitivity and Adjusting NAE network sensitivity.

• Added steps on how to select new Warning Banners in Enabling and disabling Warning Banner.

• Removed modem and pager capabilities from network engines. Once updated with Release 9.0.7 or 10.0, network engines are no longer able to communicate remotely using modems and paging services.

• Removed cloud-based application icon from all network diagrams.
• Removed all NIE55 content. The NIE55 is no longer supported.

• Updated NxE85 model - Release 10.0 section.

• Updated section to include steps to follow using the latest NAE Information and Configuration Tool (NCT).

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 supervisory controllers is a scalable line of appliance computers 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 four different vendor integrations from which you can select during commissioning: Modbus, M-Bus, KNX, and Tyco® C•CURE®/victor®. Each NAE can run two integrations. To commission each protocol, refer to the appropriate document:

• Modbus - NAE/NIE Commissioning for Modbus® Vendor Integration Application Note (LIT-12013150)
• M-Bus - NAE/NIE Commissioning for M-Bus Vendor Integration Application Note (LIT-12013149)
• KNX - NAE/NIE Commissioning for KNX Vendor Integration Application Note (LIT-12013148)
• C•CURE/victor - NAE Commissioning for C•CURE-victor Integration Application Note (LIT-12013151)

NCE25 models - Release 9.0.7

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, KNX, and C•CURE/victor
• 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 Site Director except in stand-alone applications
• support Domain Name Server (DNS) for resolving NAE names on the building network, but does not support NETBIOS name resolution
NAE35 models - Release 9.0.7

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, KNX, and C•CURE/victor
- 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 for more information.

NAE45 models - Release 9.0.7

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, KNX, and C•CURE/victor
- 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, XI5K 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 10.0

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, and C•CURE/victor

• supervise BACnet/IP field controllers from Johnson Controls, such as the FAC4911 Advanced Application Field Equipment Controller and the VMA1930 Variable Air Volume Modular Assembly

• serve as a Site Director supervising a maximum of four other network engines, which can be NCE25, NAE35, NAE45, or NAE55 model engines

**NAE-S model - Release 8.1**

The NAE-S model:

• supports up to two RS485 field buses into a Metasys system network. The NAE551S 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. A LonWorks network NAE-S model is not offered. The NAE-S 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.

• supervise BACnet/IP field controllers from Johnson Controls, such as the FAC4911 Advanced Application Field Equipment Controller and the VMA1930 Variable Air Volume Modular Assembly.

• communicates on an encrypted network with other encrypted NAE-S engines or unencrypted network engines. The NAE-S is a hardened version of the NAE55-series network engine. This network engine has embedded encryption technology under a securely fastened enclosure to protect and secure the building automation system at the endpoint.

• serves as a Site Director supervising a maximum of four other NAE-S engines over the encrypted network

**NxE85 model - Release 10.0**

The NAE85 model:

• migrates large BACnet IP networks into a Metasys system network

• supervises BACnet/IP field controllers from Johnson Controls, such as the FAC4911 Advanced Application Field Equipment Controller and the VMA1930 Variable Air Volume Modular Assembly

• supports multiple vendor integrations, including Modbus, M-Bus, KNX, and C•CURE/victor

• serves as a Site Director supervising a maximum of four other supervisory devices, which can be NCE25, NAE35, NAE45, NAE55, or NxE85 model engines

The NIE85 model:

• migrates large N1 networks into a Metasys system network

• supports multiple vendor integrations, including Modbus, M-Bus, or KNX

• serves as a Site Director supervising a maximum of four other supervisory devices, which can be NCE25, NAE35, NAE45, NAE55, or NxE85 model engines
Refer to the *NxE85 Commissioning Guide (LIT-12011044)* for additional information specific to the NxE85 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](image)

**MS/TP communications bus**

The MS/TP communications bus is a local or remote network that connects supervisory controllers and field 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 or 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 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 NAEs](image)

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 multiple NAEs and an ADS as the Site Director.
For customers that require a highly secure system, one or more NAE-S network engines can be part of the Metasys network. Figure 4 shows a network that features a secure NAE-S network engine with other unencrypted NAE engines reporting to an ADS/ADX Site Director. For more details, refer to the NAE-S Commissioning Guide (LIT-12012269).
NAE commissioning

NAE commissioning includes preparing the NAE for connectivity, connecting to the NAE, adding the NAE to the profile list in Launcher, and accessing and logging in to the Site Management Portal UI. To commission the NAE-S, refer to the [NAE-S Commissioning Guide (LIT-12012269)](LIT-12012269) for specific instructions that apply only to this secure NAE model (confidential Johnson Controls document).

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

**Note:** NAE installation includes locating, mounting, wiring, and powering on an NAE. See [Related documentation](LIT-12011742) for references to NAE installation instructions for the various NAE models.

The commissioning tasks, the task order, and the required attribute values (at commissioning) for an NAE are determined by the specific Metasys network installation, commissioning, and configuration scenario for the site. The NAE 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 NAE 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)](LIT-12011742) and the [Launcher Installation Instructions (LIT-12011783)](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 NAE:

- 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

After commissioning an NAE, you must configure the NAE at the job site. Figure 5 is a flowchart that provides an overview of the sequence of steps needed to install, commission, and configure a new NAE.

**NAE configuration**

NAE configuration is preparing an NAE in 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.

You can create and edit an archive database online in the Site Management Portal UI, but in almost all cases, you should 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 Metasys® SCT Help (LIT-12011964) for information on creating and downloading archive databases.

After you configure an NAE with an archive database containing user information, 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.
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 NAE Site Management Portal UI by using the Launcher. See Accessing Site Management Portal UI on an NAE. Figure 6 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 2 and Table 1 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 6: NAE Focus Tab in Edit Mode - Advanced

Table 1: NAE Focus Tab Descriptions

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

When you view the online NAE Site Management Portal UI, the border around the panels is blue (Figure 6). When you view the offline SCT UI, the border is black (Figure 7).
Table 2: Metasys Site Management Portal UI Tabbed Screens

<table>
<thead>
<tr>
<th>Screen Tab Designation</th>
<th>Purpose</th>
<th>Access Online/Offline</th>
</tr>
</thead>
<tbody>
<tr>
<td>Focus</td>
<td>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).</td>
<td>Both</td>
</tr>
<tr>
<td>Communications</td>
<td>Establishes communication parameters, including Serial port and internal or external USB modem configuration.</td>
<td>Both</td>
</tr>
<tr>
<td>Network</td>
<td>Establishes Computer Name (host name) for network identity, LAN, and ADS/ADX dial-up parameters (if applicable). The host name cannot consist of only numbers.</td>
<td>Both</td>
</tr>
<tr>
<td>Email</td>
<td>Establishes the NAE email alarm-notifications features common to all email messages and create unique email message destinations.</td>
<td>Both</td>
</tr>
<tr>
<td>SNMP</td>
<td>Establishes the NAE Simple Network Management Protocol (SNMP) features common to all SNMP notifications and create unique SNMP message destinations.</td>
<td>Both</td>
</tr>
<tr>
<td>Syslog</td>
<td>Provides the NAE Syslog server reporting destination information.</td>
<td>Both</td>
</tr>
<tr>
<td>Alarm</td>
<td>Provides the NAE alarm setup and destination information.</td>
<td>Both</td>
</tr>
<tr>
<td>Summary</td>
<td>Provides network and field device status information and attribute values for supervisory and field devices on the NAE field trunks.</td>
<td>Online</td>
</tr>
<tr>
<td>Diagnostic</td>
<td>Provides various status reports to aid in troubleshooting the NAE.</td>
<td>Online</td>
</tr>
<tr>
<td>Trend</td>
<td>Monitors and records the changes in the behavior of an NAE over time, assisting with diagnosing various system-wide behavioral characteristics.</td>
<td>Online</td>
</tr>
</tbody>
</table>

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® SMP Help (LIT-1201793) for descriptions of menu items.

**Metasys UI**

In addition to the Site Management Portal UI, the Metasys UI is installed with Metasys server software. The Metasys UI is a mobile-optimized software component that consolidates existing Metasys user interface products into a single, simplified, and easy-to-learn interface. The 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).

**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® SMP Help (LIT-1201793) provides information about alarming, commanding, auditing live data values, and other online features. The Metasys® SCT 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. For large-capacity engines running Release 10.0, the entire Metasys Help can be viewed. However, for small-capacity network engines running Release 9.0.7, a one-page PDF file opens with a link to the online version of Metasys Help.

**Browser recommendations for downloading the Launcher**

To access an NAE for downloading the Launcher application, you can use Windows Internet Explorer version 11, Google Chrome version 54 or later, Apple Safari version 10.0 or later, or Microsoft Edge version 38.14393. 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)**

The SCT is an offline software tool used to create, edit, save, and restore the various archive and security databases that are used to configure Metasys system networks, ODSs, ADSs/ADXs, NAEs, 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 7). The SCT also manages trusted certificates for network engines. For details, see Appendix: Certificate Management.

The SCT 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, and allows commissioning of FECs, VMA16s, and IOMs by using the CCT software to access the devices on the field bus of an NAE.

The 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.
Controller Configuration Tool (CCT)

Use CCT in conjunction with the Metasys system user interface to configure, simulate, and commission all field equipment controllers, such as CGMs, CVMs, FACs, FECs, IOMs, and VMAs. You must install CCT on the same computer as SCT software to use the Ethernet Passthru option in SCT. For more information on CCT, refer to the Controller Tool Help (LIT-12011147).

Archive databases

A Metasys archive database contains the configuration information for ADSs/ADXs, NAEs, 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 7 provides a graphical representation of some of the items that may be in a Metasys archive database.

An NAE archive database, which resides in the internal NAE 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 6 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 NAE.
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 disk image to the latest release version of the Metasys system software, use the SCT or the NAE/NIE Update Tool. Refer to Metasys® SCT Help (LIT-12011964) and NAE/NIE Update Tool Help (LIT-12011524). For some Metasys releases, the NAE/NIE Update Tool is required to update the disk image. Also, if you have a custom integration built by the Johnson Controls' Systems Integration Services (SIS) group, you must first back up the protocol DLL and license files with the NIEx9 Driver Manager tool before you update the disk image. If you skip that step, you are not able to restore the DLL and license files to the NAE after you update the engine. Refer to the NIEx9 Driver Manager Application Note (LIT-12011919). This DLL backup step is not necessary if you are using any of the four pre-configured integrations (Modbus, M-Bus, KNX, and C•CURE/victor).

When you update an NAE to a new 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 ODS) is designated as the Site Director. The Site Director UI 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 it is manufactured. 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.

Note: You can establish or change the login user name and password for the NAE only when the NAE is designated as a Site Director. Establish these values before demoting an NAE from the Site Director.

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.

Note: The NAE45-Lite 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 NAE to be a child of an ADS/ADX or ODS. 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.

<table>
<thead>
<tr>
<th>Site Director</th>
<th>Supervisory Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAE85</td>
<td>May supervise up to four additional engines on the site: NCE25s, NAE35s, NAE45s, NAE55s, or NxE85s</td>
</tr>
<tr>
<td>NAE55</td>
<td>May supervise up to four additional engines on the site: NCE25s, NAE35s, NAE45s, or NAE55s.</td>
</tr>
<tr>
<td>NAE45</td>
<td>May supervise up to two additional engines on the site: NCE25s, NAE35s, or NAE45s.</td>
</tr>
<tr>
<td>NAE35</td>
<td>May supervise up to two additional NCE25s or NAE35s on the site.</td>
</tr>
<tr>
<td>NCE25</td>
<td>None, an NCE25 can only be a Site Director to itself.</td>
</tr>
</tbody>
</table>
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 Trail each time you attempt to add a new device that exceeds the device limit. If you attempt to add the same device more than once, each attempt fails but no error message is recorded after the first attempt.

NAE computer name

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

Each NAE is factory-configured with a unique initial Computer Name value NAExxxxxxxxxxx, where xxxxxxxxxxx is the Ethernet MAC address of the device without the hyphens. For example, if the MAC address of the NAE is 00-80-66-05-0F-FC, the initial computer name is NAE008066050FFC. 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.

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.

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.

NAE object name

The NAE Object Name is an editable 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

Basic Access 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.
Login user names and passwords

All NAEs are shipped 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/NIE Update Tool. 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).

**Table 4: Metasys System Password Rules**

<table>
<thead>
<tr>
<th>Language of User</th>
<th>Supported LanguageLocale</th>
<th>Enforced Password Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>English</td>
<td>English (en_us)</td>
<td>• The password must include a minimum of 8 characters and a maximum of 50 characters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The password cannot include spaces or include a word or phrase that is in the Blocked Words list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The password and the username cannot share the same three consecutive characters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The password must meet the four following conditions:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Include at least one number (0–9)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Include at least one special character (–, ., @, #, !, ?, $, %)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>☑ Note: Only the special characters listed above can be used; all other special characters are invalid.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Include at least one uppercase character</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Include at least one lowercase character</td>
</tr>
</tbody>
</table>
Table 4: Metasys System Password Rules

<table>
<thead>
<tr>
<th>Language of User</th>
<th>Supported Language_Locale</th>
<th>Enforced Password Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-English (Europe)</td>
<td>Czech (cs_cz)</td>
<td>• The password must include a minimum of 8 characters and a maximum of 50 characters.</td>
</tr>
<tr>
<td></td>
<td>German (de_de)</td>
<td>• The password cannot include spaces or include a word or phrase that is in the Blocked Words list.</td>
</tr>
<tr>
<td></td>
<td>Spanish (es_es)</td>
<td>• The password and the username cannot share the same three consecutive characters.</td>
</tr>
<tr>
<td></td>
<td>French (fr_fr)</td>
<td>• The password must meet three of the following conditions:</td>
</tr>
<tr>
<td></td>
<td>Hungarian (hu_hu)</td>
<td>- Include at least one number (0–9)</td>
</tr>
<tr>
<td></td>
<td>Italian (it_it)</td>
<td>- Include at least one special character (., @, #, !, $, %)</td>
</tr>
<tr>
<td></td>
<td>Norwegian (nb_no)</td>
<td>- Include at least one uppercase character</td>
</tr>
<tr>
<td></td>
<td>Dutch (nl_nl)</td>
<td>- Include at least one lowercase character</td>
</tr>
<tr>
<td></td>
<td>Polish (pl_pl)</td>
<td>- Include at least one Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase</td>
</tr>
<tr>
<td></td>
<td>Portuguese (Brazilian) (pt_br)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Russian (ru_ru)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Swedish (sv_se)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Turkish (tr_tr)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Non-English (Asia)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Chinese Simplified (zh_cn)</td>
<td>• The password must include a minimum of 8 characters and a maximum of 50 characters.</td>
</tr>
<tr>
<td></td>
<td>Chinese Traditional (zh_tw)</td>
<td>• The password cannot include spaces or include a word or phrase that is in the Blocked Words list.</td>
</tr>
<tr>
<td></td>
<td>Japanese (ja_jp)</td>
<td>• The password and the username cannot share the same three consecutive characters.</td>
</tr>
<tr>
<td></td>
<td>Korean (ko_kr)</td>
<td>• The password must meet two of the following conditions:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Include at least one number (0–9)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Include at least one special character (., @, #, !, $, %)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Include at least one uppercase character</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Include at least one lowercase character</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Include at least one Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase</td>
</tr>
</tbody>
</table>

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 NAE’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 or ODS, each NAE can forward alarm and event information to the ADS/ADX or ODS for centralized notification and long-term storage.

Important:

If the site depends on emailing alarms, the Metasys system manages the NAE repositories according to the following criteria to avoid a loss of notification if the repository becomes full:

- Events forwarded to an ADS or ODS 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 field 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>
<thead>
<tr>
<th>Table 5: Default Network Engine Alarm Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Rate</td>
</tr>
<tr>
<td>BACnet Broadcast Receive Rate</td>
</tr>
<tr>
<td>Battery Condition</td>
</tr>
<tr>
<td>Board Temperature</td>
</tr>
<tr>
<td>COV Rcv Rate</td>
</tr>
<tr>
<td>CPU Temperature</td>
</tr>
<tr>
<td>CPU Usage</td>
</tr>
</tbody>
</table>

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.

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

Email notification

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.
Syslog DDA

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 9). 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 9 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 10 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.

If you run into any trouble while implementing the Syslog DDA functionality, consult this following table.
### Table 6: Syslog Server Troubleshooting

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>The engine is starting up but the SysLog DDA has not yet started.</td>
<td>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.</td>
</tr>
<tr>
<td>The Syslog server crashes.</td>
<td>All generated audits and events that the engine sends to the Syslog server are lost; nothing is cached.</td>
</tr>
<tr>
<td>The Syslog server goes offline or is unreachable.</td>
<td>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.</td>
</tr>
<tr>
<td>The IP address, name, or port numbers of the Syslog server as defined in the engine’s object are invalid.</td>
<td>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.</td>
</tr>
<tr>
<td>The Syslog Reporting Enabled parameter is set to True, but no Syslog parameters are defined.</td>
<td>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.</td>
</tr>
<tr>
<td>The UDP Send Port or UDP Receive Port is blocked by a firewall.</td>
<td>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.</td>
</tr>
<tr>
<td>A parameter of the Syslog server changes, but the corresponding parameter in the Syslog DDA of the engine is not likewise changed.</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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.

**RADIUS overview**

You can optionally configure the NAE to authenticate non-local user access through a Remote Authentication Dial-In User Service (RADIUS) server. RADIUS is used by the NAE to authenticate the identity of authorized non-local users of the system.

All RADIUS users must have a Metasys system user defined for which Metasys authorization is created and maintained. The NAE RADIUS implementation adheres to the following Internet RFC documents:

- RFC 2865 - Remote Authentication Dial In User Service
- RFC 2548 - Microsoft Vendor-specific RADIUS Attributes

The Metasys system implementation of RADIUS is as follows:

- Before you add a RADIUS user account to the security system of a network engine, first add the network engine as a client of the RADIUS server. If you first configure the RADIUS server settings in the network engine before you perform this prerequisite step, you may get the message *Unable to login - Unexpected Error* when you try to log in. If this error appears, reset the network engine from the SMP UI. Then try to log in again. The RADIUS server authenticates the user and login is successful.

- The Metasys system does not import authorization; all Metasys system users, both local (Metasys) and non-local (RADIUS), are authorized through user configuration done online in the SMP, then stored in the Metasys Security Database.

- The user ID must match what is expected to be authenticated by the RADIUS server, with or without the @domain as defined by the local RADIUS implementation.

- Since the Metasys system performs no local authentication of non-local users, all password functions are unavailable or ignored when creating and maintaining non-local Metasys user accounts. RADIUS passwords are never stored in the Metasys Security Database.

- Authorization for a RADIUS user may be configured as Administrator, User, Operator, Maintenance, or any custom roles created in the Metasys system.

- When a non-local user receives a number of consecutive RADIUS failures to authenticate and the account has been set up to lock after receiving that many failed login attempts, the Metasys system authorization locks, prohibiting the user from accessing the Metasys system device until a Metasys system administrator unlocks the account.

- When a non-local user is authenticated by RADIUS, and the Metasys system schedule prohibits access during the login time, the user’s login attempt fails.

When a user provides a non-local username to the Metasys system for login, after confirming the supplied password conforms to Metasys complexity rules, the controller passes the credentials, including the username and password, to the configured RADIUS server for authentication. After the RADIUS server confirms authenticated access, authorization is permitted as specified in the Metasys Security Database.
Messages reporting errors in RADIUS authentication are intentionally obscure to hinder possible intrusion from unauthorized users. See RADIUS errors for some situations that may result in error messages. Descriptive Metasys system login failure messages are presented to the user only when RADIUS is disabled. When RADIUS is enabled, local and non-local authentication failure messages are identical and obfuscated.

**Initial default NAE configuration**

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 8 and Table 9 define some important initial default configuration values for the NAE55 and NxE85 models.

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

**Table 7: NCE25, NAE35, and NAE45 Initial Configuration Values**

<table>
<thead>
<tr>
<th>Attribute/Field Name</th>
<th>NCE25, NAE35, and NAE45 Initial Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Name</td>
<td>NAExxxxxxxxxxxxx or NCExxxxxxxxxxxxx, where xxxxxxxxxxxxx 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.</td>
</tr>
<tr>
<td>DHCP Client</td>
<td>Enabled</td>
</tr>
<tr>
<td>Serial Port RS232C A</td>
<td>115,200 baud, 8 bits, no parity, 1 stop bit (115200,8,n,1), Direct Connect IP over Point-to-Point (PTP).</td>
</tr>
<tr>
<td>Serial Port RS232C B</td>
<td>115,200 baud, 8 bits, no parity, 1 stop bit (115200,8,n,1)</td>
</tr>
<tr>
<td>Site Director</td>
<td>A new NAE35/NAE45 is a Site Director by default. If an 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. <strong>Note:</strong> An NCE25 should not be designated as a Site Director to any other engines than itself.</td>
</tr>
<tr>
<td>Initial Login Username</td>
<td>MetasysSysAgent (not case sensitive)</td>
</tr>
<tr>
<td>Initial Login Password</td>
<td>Contact your local Johnson Controls representative.</td>
</tr>
</tbody>
</table>

**Table 8: NAE55 Initial Configuration Values**

<table>
<thead>
<tr>
<th>Attribute/Field Name</th>
<th>NAE55 Initial Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Name</td>
<td>NAExxxxxxxxxxxxxxx, where xxxxxxxxxxxxx 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.</td>
</tr>
<tr>
<td>DHCP Client</td>
<td>Enabled</td>
</tr>
<tr>
<td>Serial Port A</td>
<td>115,200 baud, 8 bits, no parity, 1 stop bit (115200,8,n,1), Direct Connect IP over Point-to-Point (PTP).</td>
</tr>
<tr>
<td>Serial Port B</td>
<td>9600 baud, 8 bits, no parity, 1 stop bit (9600,8,n,1)</td>
</tr>
<tr>
<td>Site Director</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Table 8: NAE55 Initial Configuration Values

<table>
<thead>
<tr>
<th>Attribute/Field Name</th>
<th>NAE55 Initial Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Login Username</td>
<td>MetasysSysAgent (not case-sensitive)</td>
</tr>
<tr>
<td>Initial Login Password</td>
<td>Contact your local Johnson Controls representative.</td>
</tr>
</tbody>
</table>

### Table 9: NxE85 Initial Configuration Values

<table>
<thead>
<tr>
<th>Attribute/Field Name</th>
<th>NxE85 Initial Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Name</td>
<td>NAExxxxxxxxxxxxx, where xxxxxxxxxxxxx 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.</td>
</tr>
<tr>
<td>DHCP Client</td>
<td>Enabled</td>
</tr>
<tr>
<td>Site Director</td>
<td>A new NxE85 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.</td>
</tr>
<tr>
<td>Initial Login Username</td>
<td>MetasysSysAgent (not case-sensitive)</td>
</tr>
<tr>
<td>Initial Login Password</td>
<td>Contact your local Johnson Controls representative.</td>
</tr>
</tbody>
</table>

### 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 whether 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/NIE Update Tool operations.
The Allow Http attribute is set independently on each network engine. 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 has one or more child engines reporting to it that have **not** been upgraded 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.

<table>
<thead>
<tr>
<th>Item</th>
<th>Requires Port 80?</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Graphics Application (AGA)</td>
<td>Yes</td>
<td>Uses an older version of <strong>Metasys</strong> data access services that requires http.</td>
</tr>
<tr>
<td>Advanced Reporting and Energy Essentials</td>
<td>Yes</td>
<td>Uses http for communication with engines.</td>
</tr>
<tr>
<td>Controller Configuration Tool (CCT)</td>
<td>Yes</td>
<td>Uses an older version of <strong>Metasys</strong> data access services that requires http. However, CCT only requires Port 80 for upload and download operations.</td>
</tr>
<tr>
<td>Dialup NAE</td>
<td>No</td>
<td>Uses the POP protocol, not http.</td>
</tr>
<tr>
<td>Graphic Generation Tool (GGT)</td>
<td>Yes</td>
<td>Uses older version of <strong>Metasys</strong> data access services that requires http.</td>
</tr>
<tr>
<td>Launcher</td>
<td>No</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Metasys Export Utility</strong></td>
<td>Yes</td>
<td>Uses older version of <strong>Metasys</strong> data access services that requires http.</td>
</tr>
<tr>
<td><strong>Metasys for Validated Environments (MVE)</strong></td>
<td>No</td>
<td>Uses https for communication with engines upgraded to Release 8.1 or later.</td>
</tr>
<tr>
<td><strong>Metasys UI</strong></td>
<td>No</td>
<td>Uses https for communication with engines upgraded to Release 8.1 or later.</td>
</tr>
</tbody>
</table>
Table 10: Port 80 Requirements for Tools, Utilities, and Features

<table>
<thead>
<tr>
<th>Item</th>
<th>Requires Port 80?</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAE Configuration and Information Tool (NCT)</td>
<td>Yes</td>
<td>Requires port 80 for sending a file to an engine from the commissioning laptop.</td>
</tr>
<tr>
<td>NAE/NIE Update Tool</td>
<td>Yes</td>
<td>Requires port 80 to successfully perform a code download to the engine using the HTTP update method. If Allow http is set to False, the NAE/NIE Update Tool temporarily opens port 80 for its operations, then closes the port after the download completes.</td>
</tr>
<tr>
<td>P2000</td>
<td>Yes</td>
<td>Requires port 80 (inbound) to be open on the Windows Firewall of the Metasys server.</td>
</tr>
<tr>
<td>Site Management Portal (SMP)</td>
<td>No</td>
<td>Uses https for communication with engines upgraded to Release 8.1 or later.</td>
</tr>
<tr>
<td>System Configuration Tool (SCT)</td>
<td>No</td>
<td>Uses https for communication with field controllers and engines upgraded to Release 8.1 or later.</td>
</tr>
</tbody>
</table>

Advanced Security Enabled

The Advanced Security setting, only available to Site Directors and devices 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 devices. 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 discards all communication attempts from network engines prior to Release 10.0.

This setting applies to the entire site, so keep this attribute set to False (default) if you have any network engines on the site that are running a Metasys release prior to Release 10.0.

When you change this attribute 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. If this message appears, click OK to continue and set the attribute to True, or Cancel to keep the attribute set to False.

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 NAE device. See Appendix: Configuring and Maintaining Preferences for information and detailed procedures on how to customize system and user preferences.

Reset Device command

The NAE 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 NAE 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

Note: Changing the NAE Computer Name value forces a device reset. Also, if you issue a Reset Device command to a small-capacity engine that has been upgraded to Release 9.0.7, you may need to wait a few extra minutes before the online device can open its focus window in the SMP UI.

Important: To avoid losing data, do not push the RE-BOOT SYSTEM switch on the NAE to initiate a device reset. Pushing the RE-BOOT SYSTEM switch initiates a CPU reset and restart of the NAE, which causes all unsaved data to be lost, including recent attribute value changes.

NAE network sensitivity

On some busy building networks, field 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 a field device 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 11 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.
Table 11: Network Sensitivity Adjustments

<table>
<thead>
<tr>
<th>Navigational Tree Item</th>
<th>Attributes to Adjust</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Engine: Focus window</td>
<td>APDU Segment Timeout</td>
</tr>
<tr>
<td></td>
<td>APDU Timeout</td>
</tr>
<tr>
<td></td>
<td>APDU Retries</td>
</tr>
<tr>
<td></td>
<td>Internode Comm Timer</td>
</tr>
<tr>
<td>BACnet Protocol Eng</td>
<td>Poll Delay</td>
</tr>
<tr>
<td>Eth IP DataLink</td>
<td>APDU Segment Timeout</td>
</tr>
<tr>
<td></td>
<td>APDU Timeout</td>
</tr>
<tr>
<td></td>
<td>APDU Retries</td>
</tr>
<tr>
<td></td>
<td>Internode Comm Timer</td>
</tr>
<tr>
<td>BACnet IP</td>
<td>Internode Comm Timer</td>
</tr>
<tr>
<td></td>
<td>APDU Segment Timeout</td>
</tr>
<tr>
<td></td>
<td>APDU Timeout</td>
</tr>
<tr>
<td></td>
<td>APDU Retries</td>
</tr>
<tr>
<td>Field Bus MSTP</td>
<td>Internode Comm Timer</td>
</tr>
<tr>
<td></td>
<td>APDU Segment Timeout</td>
</tr>
<tr>
<td></td>
<td>APDU Timeout</td>
</tr>
<tr>
<td></td>
<td>APDU Retries</td>
</tr>
</tbody>
</table>

Detailed Procedures

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

- an NAE with Release 9.0.7 or 10.0 software
- a laptop or desktop computer with Windows Internet Explorer version 11, Google Chrome version 54, or Apple Safari version 10.0 or later (for downloading the Launcher application)

⚠️ 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
- the NAE Information and Configuration Tool (NCT) installed on the commissioning laptop or computer

You may also need:

- a null modem Serial cable
- an Ethernet crossover cable
- 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
Installing Launcher to access the NAE

You use the Launcher application to access an NAE. If the Launcher application is already installed on your computer, skip to Step 5 below. 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. The Launcher Download dialog box appears, which varies slightly depending on the network engine’s release.

   Figure 12: Launcher download (Network Engines at Release 10.0 and 9.0.7)

3. Click Full Launcher Installer to reach the public Launcher download website. (Do not click Single Site Connection, it is no longer active.)

4. 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.

5. Start the Launcher application.
6. Click **Add**.

7. 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.

8. 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.
9. 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.

10. Enter the initial Username and Password values for the NAE and click Login. See Login user names and passwords.

11. If necessary, set the time, time zone, and date. See Appendix: Time Zone, Date, and Time Management.

Establishing direct connection to an NAE

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 be on steady (not blinking).

2. Connect an Ethernet switch with two Ethernet patch cables between the Ethernet port of the NAE and your computer. Make sure that the LAN is not connected to the Ethernet switch.

3. Verify that the 10/LINK or 100/1000LINK 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 ipconfig and press Enter. If the computer IP address is all 0s, wait several minutes. Enter the ipconfig 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.

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 NxE85 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, start NCT. 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. The NCT indicates the current IP address of the network engine.

   Note: Startup and initialization is complete when the NAE green RUN LED is on steady and the PEER COM LED is either off or flickering to show activity. 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 15: NAE Focus Tab - Basic

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/NIE Update Tool operations. Otherwise, keep this attribute at its default value (True).

**Figure 16: NAE Network Tab - Edit Mode**

- **Important:** The NAE/NIE 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/NIE Update Tool Help (LIT-12011524)* for more information on host name restrictions.

- **Note:** Changing the Computer Name forces a device reset on the NAE. (See NAE computer name and Reset Device command.)

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.
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

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, start NCT. 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.

   Note: Startup and initialization is complete when the NAE green RUN LED is on steady and the PEER COM LED is either off or flickering to show activity. 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.

7. (Optional) Select the Network tab of the NAE device object. Change the Computer Name value from the factory default, if desired. See NAE computer name and Reset Device command. 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.

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

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, start NCT. 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. Startup and initialization is complete when the NAE green RUN LED is on steady and the PEER COM LED is either off or flickering to show activity. The startup and initialization sequence may take up to 10 minutes to complete. The NCT 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.
9. Wait for the NAE to complete the startup and initialization sequence.

   **Note:** Startup and initialization is complete when the NAE green RUN LED is on steady and the PEER COM LED is either off or flickering to show activity. The startup and initialization sequence may take up to 10 minutes to complete.

   Initial setup is complete.

   **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**

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, start NCT. 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. The NCT indicates the current IP address of the network engine. Startup and initialization is complete when the NAE green RUN LED is on steady and the PEER COM LED is either off or flickering to show activity. 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. (Startup and initialization is complete when the NAE green RUN LED is on steady. This sequence may take up to 10 minutes. See Pre-boot execution environment (PXE) for more information.)

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

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

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 19).
Establishing 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 19: NAE Focus Tab (Basic)**

3. Click **Save**.

4. Select the **Advanced** option and click **Edit**.
5. Edit the advanced attribute values as needed. (Refer to the NAE Device Object Help and Audit Trails Help in the Metasys® SMP 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 then reports to the ADS/ADX as its Site Director.

Establishing 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 NAE 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.

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/NIE 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/NIE 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.

![Figure 21: NAE Network Tab - Edit Mode](image)

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.

Note: If you are setting up an NAE to dial out to an ADS/ADX, see Configuring an NAE to Dial Out to an ADS/ADX/ODS.
Creating email alarm and event notifications and destinations

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.

**Note:** In most scenarios, we recommend that you set up the Email DDA and configure the email notifications and the notification destinations after the NAE is configured with an archive database that includes the user database.

1. In the Site Management Portal UI, display the NAE device object, click the **Email** tab, and then click **Edit**. (See the top half of the Display panel in Figure 22.)

2. Enter the Shared Configuration values according to Table 12. These fields establish values for attributes that are common to all email alarm notifications generated from this NAE. Refer to *Alarm and Event Management* in *Metasys® SMP 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.

5. Enter the Destination values according to Table 12. (Refer to the *Alarm and Events Management* section in the *Metasys® SMP Help (LIT-1201793)* for additional information on setting the attribute values for alarm and event notifications.)
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description (Value Requirement/Range)</th>
<th>Initial Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP Server Host</td>
<td>Specifies the SMTP server name that handles outgoing email. (Required Value)</td>
<td>Fully qualified host name</td>
</tr>
<tr>
<td>SMTP Port</td>
<td>Specifies the TCP port that the server uses to deliver email message. (Required Value/1 to 25)</td>
<td>25</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>Specifies the Authentication Type the NAE uses to log in to the outgoing email server. Select SMTP, POP before SMTP, or None.</td>
<td>None</td>
</tr>
<tr>
<td>SMTP User Name</td>
<td>Specifies the user name the NAE uses to log in to the SMTP server that handles outgoing email messages. (Required only if SMTP is selected for Authentication Type.)</td>
<td>-</td>
</tr>
<tr>
<td>SMTP Password</td>
<td>Specifies the password the NAE uses to log in to the SMTP server that handles outgoing email messages. (Required only if SMTP is selected for Authentication Type.)</td>
<td>-</td>
</tr>
<tr>
<td>POP Server Hostname</td>
<td>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.)</td>
<td>-</td>
</tr>
<tr>
<td>POP User name</td>
<td>Specifies the POP user name. (Required only if POP Authentication is required and there is a value specified for POP server host.)</td>
<td>Maximum 20 characters</td>
</tr>
<tr>
<td>POP Password</td>
<td>Specifies the POP Password. (Required only if POP Authentication is required and there is a value specified for POP server host.)</td>
<td>Maximum 20 characters</td>
</tr>
<tr>
<td>From Email Address</td>
<td>Specifies a valid email address that is recognized and exists on the SMTP Server. (Required Value)</td>
<td>Email address</td>
</tr>
<tr>
<td>SSL Email Enabled</td>
<td>When True, emails are sent over an SSL-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.</td>
<td>False</td>
</tr>
<tr>
<td>SSL Email Ignoring Errors</td>
<td>When True, the email is sent even if the 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.</td>
<td>False</td>
</tr>
</tbody>
</table>
### Table 12: Shared Attributes for All Email Destinations

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description (Value Requirement/Range)</th>
<th>Initial Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Diagnostics</td>
<td>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.</td>
<td>–</td>
</tr>
</tbody>
</table>

### Table 13: Attributes for Specific Email Destinations and Notifications

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description (Value Requirement/Range)</th>
<th>Initial Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>Specifies a name for the email destination (for example, John Doe).</td>
<td>–</td>
</tr>
<tr>
<td>Email Address</td>
<td>Specifies the destination email addresses (for example, <a href="mailto:john.doe@jci.com">john.doe@jci.com</a>). (Required Value)</td>
<td>–</td>
</tr>
<tr>
<td>Priority</td>
<td>Specifies the email message priority (High, low, or normal).</td>
<td>Normal</td>
</tr>
<tr>
<td>Subject</td>
<td>Contains the body text of the email message. (Maximum of 256 characters.)</td>
<td>–</td>
</tr>
<tr>
<td>Retries</td>
<td>Specifies the number of attempts at sending the email message. (0–10 Retries)</td>
<td>3</td>
</tr>
<tr>
<td>Enabled</td>
<td>Enables or disables Email Destination. (True, False)</td>
<td>True</td>
</tr>
<tr>
<td>Filters</td>
<td>Enables you to specify the rules that filter alarm and event notifications. Each filter has an Item, Operator, and Value.</td>
<td>–</td>
</tr>
<tr>
<td>Format</td>
<td>Enables some predefined format characteristics of the notifications that are sent to a destination. Predefined format characteristics include:</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>• Notification Priority</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Notification Message (content)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Value</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Site Name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Item Description</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Item Fully Qualified Reference</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Item Category</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Acknowledge Required</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Previous Status (Enable a format by selecting the check box next to the format.)</td>
<td></td>
</tr>
</tbody>
</table>

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.)
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.

![Add Filter Dialog Box](image)

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**

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 14.
Table 14: Attributes for No Authentication Required

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Selection</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP Server Host</td>
<td>mail.yourdomain.com or yourdomain.com</td>
</tr>
<tr>
<td>SMTP Port</td>
<td>465</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>None</td>
</tr>
<tr>
<td>SSL Email Enabled</td>
<td>True</td>
</tr>
<tr>
<td>SSL Email Ignoring Errors</td>
<td>False</td>
</tr>
</tbody>
</table>

5. Verify that the email was sent correctly.

Configuring encrypted email with SMTP authentication

1. View an network engine.
2. Click the Email tab.
3. Click Edit.
4. Edit the Attributes in the Shared Configuration as shown in Table 15.

Table 15: Attributes for SMTP Authentication

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Selection</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP Server Host</td>
<td>mail.yourdomain.com or yourdomain.com</td>
</tr>
<tr>
<td>SMTP Port</td>
<td>465</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>SMTP</td>
</tr>
<tr>
<td>SSL Email Enabled</td>
<td>True</td>
</tr>
<tr>
<td>SSL Email Ignoring Errors</td>
<td>False</td>
</tr>
</tbody>
</table>

5. Verify that the email was sent correctly.

Configuring encrypted email with POP-before-SMTP authentication

- **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 an Engine or device.
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 POP-Before-SMTP Authentication

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Selection</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP Server Host</td>
<td>mail.yourdomain.com or yourdomain.com</td>
</tr>
</tbody>
</table>
Table 16: Attributes for POP-Before-SMTP Authentication

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Selection</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP Port</td>
<td>465</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>POP-before-SMTP</td>
</tr>
<tr>
<td>POP Server Hostname</td>
<td>yourdomain.com or pop.yourdomain.com</td>
</tr>
<tr>
<td>SSL Email Enabled</td>
<td>True</td>
</tr>
<tr>
<td>SSL Email Ignoring Errors</td>
<td>False</td>
</tr>
</tbody>
</table>

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.

**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 25).

   **Figure 25: NAE SNMP Configuration Tab - Edit Mode**

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 17).

**Table 17: Share Attributes for SNMP Destination**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description (Value Requirement/Range)</th>
<th>Initial Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Enabled</td>
<td>Enables or disables SNMP DDA on the NAE. (True, False)</td>
<td>False</td>
</tr>
<tr>
<td>SNMP Trap Version</td>
<td>Specifies the version of SNMP used on the network on which the NAE resides. (Not required if SNMP Enabled is set to False)</td>
<td>SNMP Version 1</td>
</tr>
<tr>
<td>SNMP Management Device</td>
<td>Specifies the IP address or host name of the SNMP 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)</td>
<td>–</td>
</tr>
<tr>
<td>SNMP Request Port</td>
<td>Specifies the port on the SNMP server where SNMP notifications are sent. (Not required if SNMP Enabled is set to False)</td>
<td>161</td>
</tr>
<tr>
<td>Contact Person</td>
<td>Specifies the contact person for the SNMP notifications. (Not required if SNMP Enabled is set to False)</td>
<td>–</td>
</tr>
<tr>
<td>Public Community Name</td>
<td>Specifies the community name used by the NMS to modify data in objects maintained by managed devices. (Not required if SNMP Enabled is set to False)</td>
<td>public</td>
</tr>
<tr>
<td>SNMP Trap Message Format</td>
<td>Specifies the format used to generate SNMP notifications. Change to <strong>MIB Based</strong> when SNMP management application uses the Metasys MIB file to translate SNMP notifications. (Not required if SNMP Enabled is set to False)</td>
<td>String Based</td>
</tr>
</tbody>
</table>

6. Click **New** in the Destinations section. The Destination Configuration edit screen appears (Figure 26).
7. Enter the Destination information for the SNMP trap (Table 18).

**Table 18: Attributes for Specific SNMP Notifications**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description (Value Requirement/Range)</th>
<th>Initial Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>Specifies a functional name for the destination SNMP server. (Maximum 20 characters)</td>
<td>Destination #</td>
</tr>
<tr>
<td>Trap Community Name</td>
<td>Specifies the SNMP Community Name used by the Network Management System (NMS) group to listen to the traps. (Maximum 20 characters)</td>
<td>Public</td>
</tr>
<tr>
<td>IP Address</td>
<td>Specifies the IP Address of the NMS system that receives the trap messages.</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Destination Port Number</td>
<td>Specifies the port on the SNMP Management device that receives messages from the NAE (typically Port Number 162). The direction of communication is from the NAE to the SNMP Management device.</td>
<td>162</td>
</tr>
<tr>
<td>Enabled</td>
<td>Enables or disables the SNMP destination.</td>
<td>True</td>
</tr>
<tr>
<td>Filters</td>
<td>Enables you to specify the rules that filter alarm and event notifications. Each filter has an item, operator, and value.</td>
<td>–</td>
</tr>
</tbody>
</table>
Table 18: Attributes for Specific SNMP Notifications

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description (Value Requirement/Range)</th>
<th>Initial Value</th>
</tr>
</thead>
</table>
| 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.) | – |

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.
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 19: Attributes for Specific Syslog Destinations**

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

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

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**.

### Configuring RADIUS server

To configure a RADIUS account, use the Security Administrator system.

1. Using *Metasys* Launcher, start and log in to the SMP with any *Metasys* system administrator account.
2. On the SMP UI screen, select **Tools > Administrator**. The Security Administrator window appears.

3. In the **Security Administration** menu, click **RADIUS**. The Configure RADIUS screen appears.

**Figure 30: RADIUS Configure Option**
4. Select the **Enable RADIUS Authentication** check box to enable the fields on the Configure RADIUS screen.

5. Fill in the fields of the Configure RADIUS screen using the information in the following table.

**Table 20: RADIUS Configuration Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable RADIUS Authentication</td>
<td>Checked or unchecked</td>
<td>Check box to configure and enable RADIUS server authentication. The check box defaults to unchecked. If it is not checked, all fields in the RADIUS Configuration screen are not editable.</td>
</tr>
<tr>
<td>RADIUS Server</td>
<td>IPv4 address or a DNS name</td>
<td>IPv4 address of the RADIUS server.</td>
</tr>
<tr>
<td>RADIUS Server Port</td>
<td>0 - 65535</td>
<td>Port on the RADIUS server to which Metasys directs messages.</td>
</tr>
</tbody>
</table>
Table 20: RADIUS Configuration Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS Client Port</td>
<td>0 - 65535</td>
<td>Port on the network engine that is used to send requests to and receive responses from the RADIUS server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>☑ <strong>Note:</strong> The default port for RADIUS is 1812.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Text string</td>
<td>A secret that is used to verify the validity of messages sent by the RADIUS server to the client. Knowing the Shared Secret does not grant access to a RADIUS server.</td>
</tr>
<tr>
<td>NAS Identifier</td>
<td>Text string</td>
<td>A RADIUS attribute that the client uses to identify itself to a RADIUS server.</td>
</tr>
<tr>
<td>Authentication Mechanism</td>
<td>MS-CHAPv2</td>
<td>Mechanism used for server authentication.</td>
</tr>
</tbody>
</table>

6. Click **Save**.
   ☑ **Note:** At any time, RADIUS may be disabled by clearing the **Enable Radius Authentication** check box and applying or saving the configuration. While RADIUS is disabled, only local users can authenticate. Login errors display when a user attempts to log in with a RADIUS account.

Adding RADIUS users

To provide access to the Metasys system for users that are authenticated by a RADIUS server:

1. Using Metasys Launcher, start and log in to the SMP with any Metasys system administrator account.

2. On the SMP UI screen, select **Tools > Administrator**. The Security Administration window appears.
3. Add a new RADIUS user in one of two ways:
   
a. In the **Insert** Menu, click **Insert RADIUS User**.
b. Right-click the **RADIUS Users** folder. Select **Insert**.

4. The User Properties dialog box appears. Enter the User Name. **Notes:**
   - Spell out the User Name the same as defined and expected by the RADIUS server.
   - Many fields appear dimmed when you add a RADIUS user account because they are controlled by a RADIUS server. These fields include: Password, Verify Password, View Blocked Words List, View Password Policy, Min Password Length, Max Password Length, User Must Change Password at Next Logon, and User Cannot Change Password.

5. Review the selections in the remaining tabs to ensure that the appropriate **Metasys** authorization is assigned to the user. Then click **OK**. Once you add a new RADIUS user, the new user account is opened to the Access Permissions page.

   **Note:** The Maximum Password Age and Password Uniqueness fields on the Account Policy tab do not apply to RADIUS users because those features are handled by the RADIUS server.

**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 34).

![Figure 34: NAE Alarm Configuration Tab](image)

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

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 35).

   ![Insert Alarm Wizard](image)

   **Figure 35: Insert Alarm Wizard**

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

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 it 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.

**Note:** If an ADS/ADX/ODS is on a site, an NAE cannot be the Site Director. If an NAE55 is the Site Director, it can supervise up to four additional supervisory devices on the site (NCE25s,
NAE35s, NAE45s, or NAE55s only). If an NAE45 is the Site Director, it can supervise up to two additional supervisory devices on the site (NCE25s, NAE35s, or NAE45s only). If an NAE35 is the Site Director, it can supervise up to two additional NCE25s or NAE35s on the site. NCE25s cannot supervise other network engines and should only be designated as the Site Director in stand-alone applications.

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.

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 NAE Focus edit screen appears (Figure 36).
5. Scroll down to the Site attributes and select the Local Site Director field.

Figure 36: Designating the Site Director

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 37).
8. If you wish to proceed, click **OK** to this confirmation message; otherwise, click **Cancel**.

9. If the NAE that you are demoting is at Release 9.0.7 or earlier, the NAE logs you out and resets. Wait several minutes for the NAE to reset, then log in to the Site Director. The navigation tree shows the NAE is now a child of the Site Director.

10. If the NAE that you are demoting is at Release 10.0 or later, you are prompted for the user credentials of the Local Site Director you specified. 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 in to 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

**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 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 your 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 your
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 (NAE/NIE/ADS/ADX) 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.

5. 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

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 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.

   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. 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.

   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 the SCT.

5. In the Security Copy Wizard, do one or both of the following:

   - 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

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 38: Enabling and Selecting the Warning Banner - NAE at Release 10.0 Example

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.
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

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 10.0 is medium.

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

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 21.

Table 21: Supervisory Device Network Settings

<table>
<thead>
<tr>
<th>Attribute</th>
<th>High Sensitivity</th>
<th>Medium Sensitivity</th>
<th>Low Sensitivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>APDU Segment Timeout</td>
<td>4000 ms</td>
<td>10000 ms</td>
<td>20000 ms</td>
</tr>
<tr>
<td>APDU Timeout</td>
<td>6000 ms</td>
<td>10000 ms</td>
<td>20000 ms</td>
</tr>
<tr>
<td>APDU Retries</td>
<td>4</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Internode Comm Timer</td>
<td>20 seconds</td>
<td>120 seconds</td>
<td>240 seconds</td>
</tr>
</tbody>
</table>
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 22.

**Table 22: BACnet Protocol Eng Network Settings**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>High Sensitivity</th>
<th>Medium Sensitivity</th>
<th>Low Sensitivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poll Delay</td>
<td>20 seconds</td>
<td>60 seconds</td>
<td>120 seconds</td>
</tr>
</tbody>
</table>
4. Click **Save**.

5. Open the Snapshot Focus window for the **Eth IP DataLink** 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 23.

**Table 23: Eth IP DataLink Network Settings**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>High Sensitivity</th>
<th>Medium Sensitivity</th>
<th>Low Sensitivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>APDU Segment Timeout</td>
<td>4000 ms</td>
<td>10000 ms</td>
<td>20000 ms</td>
</tr>
<tr>
<td>APDU Timeout</td>
<td>6000 ms</td>
<td>10000 ms</td>
<td>20000 ms</td>
</tr>
<tr>
<td>APDU Retries</td>
<td>4</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Internode Comm Timer</td>
<td>20 seconds</td>
<td>120 seconds</td>
<td>240 seconds</td>
</tr>
</tbody>
</table>
6. Click **Save**.

7. 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.

**Table 24: BACnet IP Network Settings**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>High Sensitivity</th>
<th>Medium Sensitivity</th>
<th>Low Sensitivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>APDU Segment Timeout</td>
<td>4000 ms</td>
<td>10000 ms</td>
<td>20000 ms</td>
</tr>
<tr>
<td>APDU Timeout</td>
<td>6000 ms</td>
<td>10000 ms</td>
<td>20000 ms</td>
</tr>
<tr>
<td>APDU Retries</td>
<td>4</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Internode Comm Timer</td>
<td>20 seconds</td>
<td>120 seconds</td>
<td>240 seconds</td>
</tr>
</tbody>
</table>
8. Click **Save**. Figure 42 is an example of adjusting all network parameters to set a Medium sensitivity.

9. Restart the network engine to put these new settings into effect.

**Replacing an NAE**

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

If you do not remove 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 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.
     - **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.

**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 25 provides a list of common NAE problems and their solutions. To troubleshoot the NAE-S, also refer to the *NAE-S Commissioning Guide (LIT-12012269)* for specific information that applies only to this secure NAE model.

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.

**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 25 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/NIE Update Tool Help (LIT-12011524)* for information on installing the NAE disk image. Refer to the *Metasys® SCT 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/NIE 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 administrator-level user. You need the designated user name and password to log in to an NAE.

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/NIE Update Tool Help (LIT-12011524).

RADIUS errors

This section describes some situations that may result in error messages after enabling RADIUS to authenticate user login credentials. When the NAEs are not configured for RADIUS authentication, the standard Metasys login error messages appear. When the NAEs are configured for RADIUS authentication, RADIUS errors are intentionally obscured to hinder possible intrusion from unauthorized users. If you encounter these errors and cannot resolve them, contact your local network administrator. The two figures in this section are examples of the general RADIUS error messages.

A RADIUS error message appears in any of the following scenarios:

• The RADIUS server is not online or available when the non-local (RADIUS) user tries to log in to the Metasys system.

• The server or network engine is configured to communicate with a RADIUS server, but the RADIUS server is unavailable and therefore does not respond to a login request from the non-local user.

• The non-local user's account is disabled, either in the Metasys system or in the RADIUS server.

• The non-local user's account password has expired.

• The non-local user’s account password does not meet the Metasys system password complexity requirements.

• The RADIUS server is enabled, but the Metasys local user account the operator is using is disabled, locked out, or cannot log in because the user’s timesheet does not permit login at this time.

• The RADIUS server is enabled, but the Metasys local user account the operator is using is entered incorrectly.

The RADIUS error message Invalid Credential appears if you try to log in to an NAE with a non-complex password and RADIUS is not enabled.

Situations when Metasys system login screen appears for RADIUS users

The following situations produce the Metasys system login screen for RADIUS users.

• when you log out of the Metasys Site Management Portal UI (either manually or when a user session ends)

• if RADIUS user authentication fails for any reason

• when you are logged in to the Windows OS with a RADIUS user account that is not privileged
within the *Metasys* system

- if the RADIUS server is unavailable

- when you are logged in to the Windows OS using a local Windows account and not a RADIUS user account

- when access to RADIUS server is restricted at login time through a RADIUS user time sheet (known as Logon Hours) or access is restricted to the *Metasys* system through the *Metasys* time sheet. RADIUS server Logon Hours takes precedence, so if you are restricted from operating system access, but not restricted by a *Metasys* time sheet, access to the *Metasys* system as a RADIUS user is not granted.

- if your RADIUS user account is enabled, but overridden to disabled with the *Metasys* Access Suspended property within *Metasys* Security Administration User Properties

- if you log in to a *Metasys* device such as an ADS, ADX, ODS, SCT, NAE, or NCE

- if *Metasys* authorization fails for any reason, such as when a user without System Configuration Tool permissions attempts to log in to SCT

When the *Metasys* Site Management Portal UI login window appears, and the site has RADIUS authentication enabled, RADIUS appears in the Login to field.

**Figure 43: Metasys Login Screen with RADIUS Server Domain List**

From this screen, you have the following options:

- Enter a RADIUS username and password, and click **RADIUS** in the drop-down list.

- Enter a RADIUS username in the form of domain\username and a RADIUS password. (The **Login to** drop-down list becomes disabled.)
Note: Usernames are obscured at login for RADIUS accounts. After login, usernames are partially obscured (for example, JSmith appears as JSm***).

The user credentials are strongly encrypted before being transmitted over the network for authentication. These credentials are active for the entire Metasys Site Management Portal UI session until you log out (or the user session terminates).

If the Metasys Device Manager has not fully started, and you try to log in to the network engine, a runtime status error occurs and the Metasys login screen appears. In this case, the Metasys login screen does not display the RADIUS server domain drop-down list and you are not able to log in as a RADIUS user.

To log in as a RADIUS user, you must close the login screen, wait a few moments for the Metasys Device Manager to fully start, then navigate again to the network engine. If you remain at the login screen following the startup error and do not close it, then log in with a Metasys local user account. All RADIUS menu options and functions are unavailable. To restore RADIUS options and functions, you must close the browser and navigate to the network engine again, then specify your RADIUS user credentials.

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, Determining the NAE IP address and device name by using a serial port monitor, 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. See Reset Device command.

Troubleshooting guide

Table 25 provides information for troubleshooting an NAE.
### Table 25: Troubleshooting the NAE

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The NAE does not operate when powered on (and the POWER LED is on).</td>
<td>Corrupted flash memory or data loss are the most common causes of this problem. To resolve this problem:</td>
</tr>
<tr>
<td></td>
<td>1. Ensure that the data protection battery is connected and charged. (Refer to the unit’s Installation Instructions for more information on handling, installing, and charging the data protection battery.)</td>
</tr>
<tr>
<td></td>
<td>2. Ensure that the database does not exceed the NAE flash memory capacity.</td>
</tr>
<tr>
<td></td>
<td>3. Reload the disk image and download the archive database to the NAE while the NAE is disconnected from the network.</td>
</tr>
<tr>
<td>NAE does not operate after updating the disk image, downloading an</td>
<td>Corrupted flash memory and data loss are the most common causes of this problem. To resolve this problem:</td>
</tr>
<tr>
<td>archive database, or installing a patch.</td>
<td>1. Ensure that the database does not exceed the NAE flash memory capacity.</td>
</tr>
<tr>
<td></td>
<td>2. Reload the disk image and download the archive database to the NAE while the NAE is disconnected from the network.</td>
</tr>
<tr>
<td>NAE does not communicate with any other device.</td>
<td>Check to make sure that 24 VAC power is connected correctly and that the 24 VAC and POWER LED's are on.</td>
</tr>
<tr>
<td></td>
<td>Check to make sure that communication terminal blocks and other communication connectors are firmly in place.</td>
</tr>
<tr>
<td></td>
<td>Check that the wiring is the correct size (18 AWG minimum for power, 18 AWG for N2 Bus, 26 AWG for Ethernet communication).</td>
</tr>
<tr>
<td></td>
<td>Check that you have set the correct baud rate on each connected device.</td>
</tr>
<tr>
<td></td>
<td>Check the integrity of the wires and cables.</td>
</tr>
<tr>
<td></td>
<td>Check that N2 EOL switches are correct. Refer to the Setting Terminations section of the N2 Communications Bus Technical Bulletin (LIT-636018) for details on N2 EOL terminations.</td>
</tr>
<tr>
<td>No N2 communication (on devices that support the N2 Bus protocol)</td>
<td>Check that the N2 wires are connected properly and are not loose in the termination block.</td>
</tr>
<tr>
<td></td>
<td>Check that the N2 LEDs indicate communication.</td>
</tr>
<tr>
<td></td>
<td>Check that the N2 EOL switches are correctly set. Refer to the Setting Terminations section of the N2 Communications Bus Technical Bulletin (LIT-636018) for details on N2 terminations.</td>
</tr>
<tr>
<td></td>
<td>Check the entire N2 Bus. Refer to the N2 Communications Bus Technical Bulletin (LIT-636018).</td>
</tr>
<tr>
<td>Problem</td>
<td>Solution</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>No LonWorks communication (on devices that support the LonWorks protocol)</td>
<td>Check that the LonWorks network wires are connected properly and are not loose in the termination block. Connect the <em>Metasys</em> 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 NAE. If communication is good, verify that the NAE database has been generated correctly and that the LonWorks enabled device data corresponds to the devices installed. If the NAE does not respond, verify that the NAE has been correctly installed in the LonWorks network database and that the network configuration image has been sent to the NAE. If the NAE cannot be installed, replace the NAE. Refer to the <em>LonWorks® Network Integration with NAE and LCS Technical Bulletin</em> (LIT-1201668) for NAE database generation information. Check the entire LonWorks network. Refer to the <em>LonMark Guidelines - Physical Layer</em> for details (<a href="http://www.lonmark.org">http://www.lonmark.org</a>).</td>
</tr>
<tr>
<td>No Ethernet communication</td>
<td>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.</td>
</tr>
<tr>
<td>No modem communication</td>
<td>Beginning at Release 9.0.7, network engines no longer support modem communication.</td>
</tr>
<tr>
<td>The USR 5637 modem connects, but garbled characters appear and eventually communication drops.</td>
<td>Beginning at Release 9.0.7, network engines no longer support modem communication.</td>
</tr>
<tr>
<td>The NAE does not dial in or dial out.</td>
<td>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.</td>
</tr>
<tr>
<td>Problem</td>
<td>Solution</td>
</tr>
<tr>
<td>---------</td>
<td>----------</td>
</tr>
<tr>
<td>The NAE runs slowly.</td>
<td>The amount of data you are trying to process is too much for the NAE to handle. A value of 50% or less for the CPU Usage attribute of the NAE is considered acceptable, although other performance indicators should also be assessed. Refer to the <em>Metasys® SCT Help (LIT-12011964)</em> or <em>Metasys® SMP Help (LIT-1201793)</em> system for more information. Reduce the size of the database.</td>
</tr>
</tbody>
</table>
| The NAE 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:  
1. Add a Trend extension to the Last Idle Sample of the NAE. 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.  
2. 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.  
3. 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 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 NAE.  
Check that the power transformer secondary is not shared with another load. |
| The NAE overheats. | When the internal temperature reaches the high limit, the NAE 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 25: Troubleshooting the NAE

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The unit has been damaged or all external causes of failure have been</td>
<td>Replace the NAE.</td>
</tr>
<tr>
<td>checked.</td>
<td></td>
</tr>
<tr>
<td>The following message appears in the Focus window for a network engine:</td>
<td>The network engine has become unpaired with the Site Director. This issue may occur after you set</td>
</tr>
<tr>
<td>Item Not Found</td>
<td>the Advanced Security Enabled option under the Site Director’s Site object to True. To resolve,</td>
</tr>
<tr>
<td></td>
<td>use the <strong>Tools &gt; Pair NxE with Site Director</strong> option to force network engine pairing. If this</td>
</tr>
<tr>
<td></td>
<td>action does not restore communication, either restart the <strong>Metasys</strong> Server or the network</td>
</tr>
<tr>
<td></td>
<td>engine that has not paired.</td>
</tr>
</tbody>
</table>

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:

- the **NAE LED status indicators**
- the **Diagnostic tab**
- the **Summary tab**
- a serial point monitor (see Determining the NAE IP address and device name by using a serial port 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 44, Figure 45, and Figure 46 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 26 describes their Normal Status and Function.
Table 26: NAE LED Status Indicators

<table>
<thead>
<tr>
<th>LED Label (Color)</th>
<th>NAE Series</th>
<th>Normal Status</th>
<th>Descriptions/Other Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>POWER (Green)</td>
<td>NCE25, NAE35, NAE45, NAE55</td>
<td>On Steady</td>
<td>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.</td>
</tr>
<tr>
<td>ETHERNET (Green)</td>
<td>NCE25, NAE35, NAE45, NAE55</td>
<td>Flicker</td>
<td>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.</td>
</tr>
<tr>
<td>10/LINK (Green)</td>
<td>NCE25, NAE35, NAE45, NAE55</td>
<td>On Steady</td>
<td>On Steady = Ethernet connection is established at 10 Mb/s.</td>
</tr>
<tr>
<td>100/LINK (Green)</td>
<td>On Steady</td>
<td>On Steady</td>
<td>On Steady = Ethernet connection is established at 100 Mb/s</td>
</tr>
<tr>
<td>LED Label (Color)</td>
<td>NAE Series</td>
<td>Normal Status</td>
<td>Descriptions/Other Conditions</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------</td>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 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.  
Off Steady = No controllers are defined to FC A (FC Bus 1 or N2 Trunk 1) in the NAE55.                                                                      |
| 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.  
Off Steady = No controllers are defined to FC B (FC Bus 2 or N2 Trunk 2) in the NAE55.                                                                      |
### Table 26: NAE LED Status Indicators

<table>
<thead>
<tr>
<th>LED Label (Color)</th>
<th>NAE Series</th>
<th>Normal Status</th>
<th>Descriptions/Other Conditions</th>
</tr>
</thead>
</table>
| FC BUS or LON¹    | NCE25, NAE35, NAE45 | Normal Status | 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. |
| 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. |
<table>
<thead>
<tr>
<th>LED Label (Color)</th>
<th>NAE Series</th>
<th>Normal Status</th>
<th>Descriptions/Other Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>MODEM RX¹</td>
<td>NCE25, NAE35, NAE45</td>
<td>Flicker</td>
<td>Flicker indicates modem is connected and receiving data.</td>
</tr>
<tr>
<td>MODEM TX¹</td>
<td>NCE25, NAE35, NAE45</td>
<td>Flicker</td>
<td>Flicker indicates modem is connected and transmitting data.</td>
</tr>
<tr>
<td>BATT FAULT (Red)</td>
<td>NCE25, NAE35, NAE45, NAE55</td>
<td>Off Steady</td>
<td>Off Steady = Normal operation. Off 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.</td>
</tr>
<tr>
<td>GENL FAULT or FAULT (Red)</td>
<td>NCE25, NAE35, NAE45, NAE55</td>
<td>Off Steady</td>
<td>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.</td>
</tr>
</tbody>
</table>

¹ LED labeled FC BUS on models that support MS/TP Bus or N2 Bus, and labeled LON on models that support LonWorks network.
² 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

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.

3. 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

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.

3. 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

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.

3. 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 47 shows an example.
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 48).
Summary tab

The Summary tab (Figure 49) 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 49). 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 Metasys® SCT Help (LIT-12011964) or the Metasys® SMP Help (LIT-1201793).
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.

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 NCT

You can use the Network Engine (NxE) Information and Configuration Tool (NCT) to discover the NAE. To determine the IP address of an NxE by using the NCT to discover the device, start the NCT, click Discover, and look for the NxE in the Discovered Devices list. The NxEs must be connected to the same subnet as the NCT computer for the NCT to detect them. For more information, refer to the NxE Information and Configuration Tool Technical Bulletin (LIT-1201990).

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. Table 27 provides an example of the data that is sent.

Table 27: Example NCE25, NAE35, NAE45 Startup Data Stream

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

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 these settings: baud rate=115200 bps; data length=8 bit; no parity; one stop bit.)
Setting a computer to be compatible with APIPA

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.

1. View the local area connection properties of the active network connection as follows:
   a. In Control Panel, select **Network and Internet > Network and Sharing Center > Change adapter settings**. The Network Connections window appears.
   b. Right-click **Local Area Connection** and select **Properties**. The Local Area Connection Properties window appears.

2. Click **Internet Protocol Version 4 (TCP/IPv4)** and then click **Properties**.

3. Make sure the option **Obtain an IP address automatically** is selected.

Related documentation

<table>
<thead>
<tr>
<th>For Information On</th>
<th>See Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview of the Metasys System Network Features and Functions</td>
<td>Metasys® System Configuration Guide (LIT-12011832)</td>
</tr>
<tr>
<td>Definition of Terms, Concepts, and Acronyms Commonly Used to Describe the Metasys System</td>
<td>Metasys System Extended Architecture Glossary Technical Bulletin (LIT-1201612)</td>
</tr>
<tr>
<td>General Network and Information Technology Definitions and Concepts, and Creating a Printer DDA for an NAE</td>
<td>Network and IT Guidance Technical Bulletin (LIT-12011279)</td>
</tr>
<tr>
<td>Daily Operation of the Metasys System Network, Navigating the SMP UI or SCT UI, Monitoring and Controlling BAS Networks, and Connecting to Cloud-Based Applications</td>
<td>Metasys® SMP Help (LIT-1201793) Metasys® SCT Help (LIT-12011964)</td>
</tr>
<tr>
<td>Installation Considerations and Guidelines, Mounting, Wiring, and Starting up an NCE25</td>
<td>NCE25 Installation Instructions (Part No. 24-10143-63)</td>
</tr>
<tr>
<td>Installation Considerations and Guidelines, Mounting, Wiring, and Starting up an NAE35 or NAE45</td>
<td>NAE35/NAE45 Installation Instructions (Part No. 24-10050-6)</td>
</tr>
<tr>
<td>Installation Considerations and Guidelines, Mounting, Wiring, and Starting up an NAE55 or NIE55</td>
<td>NAE55/NIE55 Installation Instructions (Part No. 24-10051-43)</td>
</tr>
<tr>
<td>Installation Considerations and Guidelines, Mounting, Wiring, and Starting up an NAE-S</td>
<td>NAE55-S Installation Instructions (Part No. 24-10051-108)</td>
</tr>
<tr>
<td>Additional Guidelines for Commissioning and Configuring and NCE25 Network Engines</td>
<td>NCE Technical Bulletin (LIT-12011267)</td>
</tr>
<tr>
<td>Additional Guidelines for Commissioning NxE85 Network Engines</td>
<td>NxE85 Commissioning Guide (LIT-12011044)</td>
</tr>
<tr>
<td>Additional Guidelines for Commissioning NxE89 Network Engines</td>
<td>NIE89 Commissioning Guide (LIT-12011920)</td>
</tr>
<tr>
<td>Commissioning an NAE for the Modbus Protocol</td>
<td>NAE/NIE Commissioning for Modbus® Vendor Integration Application Note (LIT-12013150)</td>
</tr>
<tr>
<td>For Information On</td>
<td>See Document</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Commissioning an NAE for the M-Bus Protocol</td>
<td>NAE/NIE Commissioning for M-Bus Vendor Integration Application Note (LIT-12013149)</td>
</tr>
<tr>
<td>Commissioning an NAE for the KNX Protocol</td>
<td>NAE/NIE Commissioning for KNX Vendor Integration Application Note (LIT-12013148)</td>
</tr>
<tr>
<td>Commissioning an NAE for the C&gt;CURE 9000 and victor video management system integration</td>
<td>NAE Commissioning for C&gt;CURE-victor Integration Application Note (LIT-12013151)</td>
</tr>
<tr>
<td>Commissioning NIEx9 Network Engines</td>
<td>NIEx9 Commissioning Guide (LIT-12011922)</td>
</tr>
<tr>
<td>Updating the NAE/NIE Disk Image to New Software Release Versions</td>
<td>NAE/NIE Update Tool Help (LIT-12011524)</td>
</tr>
<tr>
<td>Installing the ADS and ADX Software</td>
<td>Metasys Server Installation and Upgrade Instructions Wizard (LIT-12012162)</td>
</tr>
<tr>
<td>Installing the ADS-Lite Software</td>
<td>Metasys Server Lite Installation and Upgrade Instructions Wizard (LIT-12012258)</td>
</tr>
<tr>
<td>Installing the ODS Software</td>
<td>ODS Installation and Upgrade Instructions Wizard (LIT-12011945)</td>
</tr>
<tr>
<td>Installing the SCT Software</td>
<td>SCT Installation and Upgrade Instructions Wizard (LIT-12012067)</td>
</tr>
<tr>
<td>Creating, Editing, and Loading Archive Databases with the SCT</td>
<td>Metasys® SCT Help (LIT-12011964)</td>
</tr>
<tr>
<td>Managing Trusted Certificates Created for Network Engines</td>
<td>Metasys® SCT Help (LIT-12011964)</td>
</tr>
<tr>
<td>Integrating N2 Devices into the Metasys System Network</td>
<td>N2 Integration with the NAE Technical Bulletin (LIT-1201683)</td>
</tr>
<tr>
<td>How to Install the CCT Software</td>
<td>CCT Installation Instructions (LIT-12011529)</td>
</tr>
<tr>
<td>Using the Controller Configuration Tool</td>
<td>Controller Tool Help (LIT-12011147)</td>
</tr>
<tr>
<td>NAE/NCE BACnet® Protocol Conformance</td>
<td>NAE/NCE Protocol Implementation Conformance Statement (LIT-1201532)</td>
</tr>
<tr>
<td>How to Set Up a Local or Remote MS/TP Communications Bus</td>
<td>MS/TP Communications Bus Technical Bulletin (LIT-12011034)</td>
</tr>
<tr>
<td>Enabling NAEs to Communicate with MS/TP Controllers over Wireless Mesh Networks</td>
<td>ZFR1800 Series Wireless Field Bus System Technical Bulletin (LIT-12011295)</td>
</tr>
<tr>
<td>Integrating LonWorks Devices into the Metasys System Network</td>
<td>LonWorks® Network Integration with NAE and LCS Technical Bulletin (LIT-1201668)</td>
</tr>
<tr>
<td>Migrating N1 Networks to the Metasys System Network</td>
<td>N1 Migration with the NIE Technical Bulletin (LIT-1201535)</td>
</tr>
<tr>
<td>Integrating Local and Remote BACnet MS/TP and BACnet IP Devices into the Metasys System Network</td>
<td>BACnet® Controller Integration with NAE/NCE/ODS Technical Bulletin (LIT-1201531)</td>
</tr>
</tbody>
</table>
Table 28: NAE Related Documentation

<table>
<thead>
<tr>
<th>For Information On</th>
<th>See Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installing the Launcher Application</td>
<td>Launcher Installation Instructions (LIT-12011783)</td>
</tr>
<tr>
<td>Using the Launcher, Accessing a Metasys System Network through Dial-up Connections</td>
<td>Launcher Tool Help (LIT-12011742)</td>
</tr>
<tr>
<td>Dialing into a Metasys System Network from a Computer</td>
<td>Metasys System Direct Connection and Dial-Up Connection Application Note (LIT-1201639)</td>
</tr>
</tbody>
</table>

Technical specifications - NCE, NAE, and NIE models

Table 29: NCE25 technical specifications

<table>
<thead>
<tr>
<th>Power Requirement</th>
<th>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)</th>
</tr>
</thead>
</table>
| Power Consumption | 25 VA maximum for NCE25 only  

Note: 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). |

<table>
<thead>
<tr>
<th>Power Source</th>
<th>+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</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ambient Operating Conditions</td>
<td>0 to 50°C (32 to 122°F), 10 to 90% RH, 30°C (86°F) maximum dew point</td>
</tr>
<tr>
<td>Ambient Storage Conditions</td>
<td>-40 to 70°C (-40 to 158°F), 5 to 95% RH, 30°C (86°F) maximum dew point</td>
</tr>
<tr>
<td>Data Protection Battery</td>
<td>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</td>
</tr>
</tbody>
</table>
| Processors | **Supervisory Controller:** 192 MHz Renesas SH4 7760 RISC processor  
**Field Controller:** 20 MHz Renesas H8S2398 processor |
| 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 14.4 (Release 9.0.7 patch) |
### Table 29: NCE25 technical specifications

<table>
<thead>
<tr>
<th>Network and Serial Interfaces (Depending on NCE model.)</th>
<th><img src="https://via.placeholder.com/150" alt="Description" /></th>
</tr>
</thead>
<tbody>
<tr>
<td>• One Ethernet port; 10/100 Mbps; 8-pin RJ-45 connector</td>
<td><img src="https://via.placeholder.com/150" alt="Description" /></td>
</tr>
<tr>
<td>• One optically isolated RS-485 SA Bus port; with a pluggable and keyed 4-position terminal block (on all NCE25 models)</td>
<td><img src="https://via.placeholder.com/150" alt="Description" /></td>
</tr>
<tr>
<td>• 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)</td>
<td><img src="https://via.placeholder.com/150" alt="Description" /></td>
</tr>
<tr>
<td>• 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 <strong>not the Release 9.0.7 patch update.</strong></td>
<td><img src="https://via.placeholder.com/150" alt="Description" /></td>
</tr>
<tr>
<td>• One RS-232-C serial port with standard 9-pin sub-D connector that supports standard baud rates</td>
<td><img src="https://via.placeholder.com/150" alt="Description" /></td>
</tr>
<tr>
<td>• 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 <strong>not</strong> available after the NAE is patched with Release 9.0.7.</td>
<td><img src="https://via.placeholder.com/150" alt="Description" /></td>
</tr>
<tr>
<td>• 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.)</td>
<td><img src="https://via.placeholder.com/150" alt="Description" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Analog Input/Analog Output Point Resolution</th>
<th><img src="https://via.placeholder.com/150" alt="Description" /></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Analog Input Points: 16-bit resolution</td>
<td><img src="https://via.placeholder.com/150" alt="Description" /></td>
</tr>
<tr>
<td>• Analog Output Points: 16-bit resolution and ±200 mV accuracy on 0-10 VDC applications</td>
<td><img src="https://via.placeholder.com/150" alt="Description" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Input/Output Capabilities</th>
<th><img src="https://via.placeholder.com/150" alt="Description" /></th>
</tr>
</thead>
<tbody>
<tr>
<td>• 10-Universal Inputs: Defined as 0–10 VDC, 4–20mA, 0–600k ohm, or Binary Dry Contact</td>
<td><img src="https://via.placeholder.com/150" alt="Description" /></td>
</tr>
<tr>
<td>• 8-Binary Inputs: Defined as Dry Contact Maintained or Pulse/Accumulator Mode</td>
<td><img src="https://via.placeholder.com/150" alt="Description" /></td>
</tr>
<tr>
<td>• 4-Analog Outputs: Defined as 0–10 VDC or 4–20mA</td>
<td><img src="https://via.placeholder.com/150" alt="Description" /></td>
</tr>
<tr>
<td>• 7-Binary Outputs: Defined as 24 VAC Triac (selectable internal or external source power)</td>
<td><img src="https://via.placeholder.com/150" alt="Description" /></td>
</tr>
<tr>
<td>• 4-Configurable Outputs: Defined as 0–10 VDC or 24 VAC Triac BO</td>
<td><img src="https://via.placeholder.com/150" alt="Description" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Dimensions (Height x Width x Depth)</th>
<th><img src="https://via.placeholder.com/150" alt="Description" /></th>
</tr>
</thead>
<tbody>
<tr>
<td>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.)</td>
<td><img src="https://via.placeholder.com/150" alt="Description" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Housing</th>
<th><img src="https://via.placeholder.com/150" alt="Description" /></th>
</tr>
</thead>
<tbody>
<tr>
<td>Plastic housing</td>
<td><img src="https://via.placeholder.com/150" alt="Description" /></td>
</tr>
<tr>
<td>Plastic material: ABS and polycarbonate</td>
<td><img src="https://via.placeholder.com/150" alt="Description" /></td>
</tr>
<tr>
<td>Protection: IP20 (IEC60529)</td>
<td><img src="https://via.placeholder.com/150" alt="Description" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mounting</th>
<th><img src="https://via.placeholder.com/150" alt="Description" /></th>
</tr>
</thead>
<tbody>
<tr>
<td>On flat surface with screws, on three mounting clips, or a single 35 mm DIN rail</td>
<td><img src="https://via.placeholder.com/150" alt="Description" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Shipping Weight</th>
<th><img src="https://via.placeholder.com/150" alt="Description" /></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2 kg (2.7 lb)</td>
<td><img src="https://via.placeholder.com/150" alt="Description" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Compliance</th>
<th><img src="https://via.placeholder.com/150" alt="Description" /></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>United States:</strong> UL Listed, File E107041, CCN PAZX, UL 916, Energy Management Equipment; FCC Compliant to CFR47, Part 15, Subpart B, Class A</td>
<td><img src="https://via.placeholder.com/150" alt="Description" /></td>
</tr>
</tbody>
</table>
Table 29: NCE25 technical specifications

<table>
<thead>
<tr>
<th></th>
<th>Canada: UL Listed, File E107041, CCN PAZX7, CAN/CSA C22.2 No. 205, Signal Equipment Industry Canada Compliant, ICES-003</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Europe:</strong> CE Mark - Johnson Controls declares that this product is in compliance with the essential requirements and other relevant provisions of the EMC Directive.</td>
</tr>
<tr>
<td></td>
<td><strong>Australia and New Zealand:</strong> RCM Mark, Australia/NZ Emissions Compliant</td>
</tr>
<tr>
<td></td>
<td><strong>BACnet International:</strong> BTL 135-2012 Listed B-BC, Protocol Revision 12</td>
</tr>
</tbody>
</table>

Table 30: NAE35 and NAE45 technical specifications

<table>
<thead>
<tr>
<th>Power Requirement</th>
<th>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)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Consumption</td>
<td>25 VA maximum</td>
</tr>
<tr>
<td>Ambient Operating Conditions</td>
<td>0 to 50°C (32 to 122°F); 10 to 90% RH, 30°C (86°F) maximum dew point</td>
</tr>
<tr>
<td>Ambient Storage Conditions</td>
<td>-40 to 70°C (-40 to 158°F); 5 to 95% RH, 30°C (86°F) maximum dew point</td>
</tr>
<tr>
<td>Data Protection Battery</td>
<td>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</td>
</tr>
<tr>
<td>Processor</td>
<td>192 MHz Renesas SH4 7760 RISC processor</td>
</tr>
<tr>
<td>Memory</td>
<td>128 MB flash nonvolatile memory for operating system, configuration data, and operations data storage and backup</td>
</tr>
<tr>
<td></td>
<td>128 MB SDRAM for operations data dynamic memory</td>
</tr>
<tr>
<td>Operating System</td>
<td>Microsoft Windows Embedded CE 6.0 (Release 9.0) Buildroot 2017.08.2 with Linux kernel 14.4 (Release 9.0.7 patch)</td>
</tr>
</tbody>
</table>
### Table 30: NAE35 and NAE45 technical specifications

| Network and Serial Interfaces | • One Ethernet port; connects at 10 or 100 Mbps; 8-pin RJ-45 connector  
|                              | • 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 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.  
|                              | • 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.  
|                              | • 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.)  

| 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 4.5/16 in.)  

| Shipping Weight              | 1.2 kg (2.7 lb)  

|                             | **Canada: UL Listed, File E107041, CCN PAZX7, CAN/CSA C22.2 No. 205, Signal Equipment; Industry Canada Compliant, ICES-003**  
|                             | **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.

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

<table>
<thead>
<tr>
<th>Specification</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power Requirement</strong></td>
<td>Dedicated nominal 24 VAC, Class 2 power supply (North America) at 50/60 Hz (20 VAC minimum to 30 VAC maximum)</td>
</tr>
<tr>
<td><strong>Power Consumption</strong></td>
<td>50 VA maximum</td>
</tr>
<tr>
<td><strong>Ambient Operating Conditions</strong></td>
<td>0 to 50°C (32 to 122°F); 10 to 90% RH, 30°C (86°F) maximum dew point</td>
</tr>
<tr>
<td><strong>Ambient Storage Conditions</strong></td>
<td>-40 to 70°C (-40 to 158°F); 5 to 95% RH, 30°C (86°F) maximum dew point</td>
</tr>
<tr>
<td><strong>Data Protection Battery</strong></td>
<td>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</td>
</tr>
<tr>
<td><strong>Clock Battery</strong></td>
<td>Maintains real-time clock through a power failure. Onboard cell; typical life 10 years at 21°C (70°F)</td>
</tr>
<tr>
<td><strong>Processor</strong></td>
<td>1.6 GHz Intel Atom® processor</td>
</tr>
<tr>
<td><strong>Memory</strong></td>
<td>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</td>
</tr>
<tr>
<td><strong>Operating System</strong></td>
<td>Johnson Controls OEM Version of Microsoft Windows Standard 2009</td>
</tr>
<tr>
<td><strong>Network and Serial Interfaces</strong></td>
<td>• One Ethernet port; 10/100/1,000 Mbps; 8-pin RJ-45 connector</td>
</tr>
<tr>
<td></td>
<td>• Two optically isolated RS-485 ports; 9,600, 19.2k, 38.4k, or 76.8k baud; pluggable and keyed 4-position terminal blocks</td>
</tr>
<tr>
<td></td>
<td>• Two RS-232-C serial ports, with standard 9-pin sub-D connectors, that support all standard baud rates</td>
</tr>
<tr>
<td></td>
<td>• Two USB serial ports; standard USB connectors (use is not supported on Smoke Control NAEs)</td>
</tr>
<tr>
<td><strong>Housing</strong></td>
<td>Plastic housing with internal metal shield</td>
</tr>
<tr>
<td></td>
<td>Plastic material: ABS + polycarbonate</td>
</tr>
<tr>
<td><strong>Mounting</strong></td>
<td>On flat surface with screws on four mounting feet or on dual 35 mm DIN rail</td>
</tr>
<tr>
<td><strong>Dimensions (Height x Width x Depth)</strong></td>
<td>226 x 332 x 96.5 mm (8.9 x 13.1 x 3.8 in.) including mounting feet</td>
</tr>
<tr>
<td></td>
<td>Minimum space for mounting: 303 x 408 x 148 mm (12.0 x 16.1 x 5.8 in.)</td>
</tr>
<tr>
<td><strong>Shipping Weight</strong></td>
<td>2.9 kg (6.4 lb)</td>
</tr>
<tr>
<td><strong>Compliance</strong></td>
<td><strong>United States</strong>: UL Listed, File E107041, CCN PAZX, UL 916, Energy Management Equipment; FCC Compliant to CFR47, Part 15, Subpart B, Class A</td>
</tr>
<tr>
<td></td>
<td>UL Listed, File S4977, UL 864 UUKL/UUKLC 10th Edition Listed, Smoke Control Units and Accessories for Fire Alarm Systems Equipment</td>
</tr>
</tbody>
</table>
Table 31: NAE5510-2U (Smoke Control) technical specifications

<table>
<thead>
<tr>
<th>Country</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Canada</strong></td>
<td>UL Listed, File E107041, CCN PAZX7, CAN/CSA C22.2 No. 205, Signal Equipment, Industry Canada Compliant, ICES-003</td>
</tr>
<tr>
<td><strong>Europe</strong></td>
<td>CE Mark - Johnson Controls, Inc. declares that this product is in compliance with the essential requirements and other relevant provisions of the EMC Directive.</td>
</tr>
<tr>
<td><strong>Australia and New Zealand</strong></td>
<td>RCM Mark, Australia/NZ Emissions Compliant</td>
</tr>
<tr>
<td><strong>BACnet International</strong></td>
<td>BTL 135-2012 Listed B-BC, Protocol Revision 12</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Specification</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power Requirement</strong></td>
<td>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)</td>
</tr>
<tr>
<td><strong>Power Consumption</strong></td>
<td>50 VA maximum</td>
</tr>
<tr>
<td><strong>Ambient Operating Conditions</strong></td>
<td>0 to 50°C (32 to 122°F); 10 to 90% RH, 30°C (86°F) maximum dew point</td>
</tr>
<tr>
<td><strong>Ambient Storage Conditions</strong></td>
<td>-40 to 70°C (-40 to 158°F); 5 to 95% RH, 30°C (86°F) maximum dew point</td>
</tr>
<tr>
<td><strong>Data Protection Battery</strong></td>
<td>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</td>
</tr>
<tr>
<td><strong>Clock Battery</strong></td>
<td>Maintains real-time clock through a power failure. Onboard cell; typical life 10 years at 21°C (70°F)</td>
</tr>
<tr>
<td><strong>Processor</strong></td>
<td>1.46 GHz Intel® Atom® Bay Trail E3815 processor for MS-NAE55xx-3 models</td>
</tr>
<tr>
<td><strong>Memory</strong></td>
<td>16 GB flash nonvolatile memory for operating system, configuration data, and operations data storage and backup for MS-NAE55xx-3 models.</td>
</tr>
<tr>
<td></td>
<td>2 GB DDR3 SDRAM for operations data dynamic memory for all models</td>
</tr>
<tr>
<td><strong>Operating System</strong></td>
<td>Johnson Controls OEM Version of Microsoft Windows Embedded Standard 7 with SP1 (WES7, Release 9.0)</td>
</tr>
<tr>
<td></td>
<td>Wind River Linux 9 (Release 10.0)</td>
</tr>
</tbody>
</table>
### Table 32: NAE55xx-3 (Energy Management) and NAE5510-3U (Smoke Control) technical specifications

| Network and Serial Interfaces | • One Ethernet port; 10/100/1,000 Mbps; 8-pin RJ-45 connector  
|                              | • 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 Width x Depth) | 226 x 332 x 96.5 mm (8.9 x 13.1 x 3.8 in.) including mounting feet  
|                               | 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  
|                               | 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  
|                               | **BACnet International**: BTL 135-2016 Listed B-BC, Protocol Revision 15 at Metasys Release 10.0  

CE
## 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)  
| 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 Interfaces | • One Ethernet port; 10/100/1000 Mbps; 8-pin RJ-45 connector  
|        | • 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 |
**Table 33: NAE-S technical specifications (North America and Canada only)**

<table>
<thead>
<tr>
<th>Country</th>
<th>Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canada</td>
<td>cUL CSA-C22.2 No. 14, CCN NITW7, Industrial Control Equipment; IC Compliant to ICES-003 Class A</td>
</tr>
<tr>
<td></td>
<td>BACnet International: BTL 135-2012 Listed B-BC, Protocol Revision 12</td>
</tr>
</tbody>
</table>

**Table 34: NAE85 software system recommendations for installation/upgrade**

<table>
<thead>
<tr>
<th>Recommended Computer Platform</th>
<th>IntelXeon E5506, 2.13 GHz, 4 MB Cache</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2 x 160 GB 7.2K SATA, 8.9 cm (3.5 in.) Cabled</td>
</tr>
<tr>
<td></td>
<td>3 Gbps, RAID 1 configuration with add-in SAS6/iR (SATA/SAS Controller)</td>
</tr>
<tr>
<td>Recommended Memory</td>
<td>2 GB RAM minimum</td>
</tr>
<tr>
<td>Hard Disk</td>
<td>160 GB minimum</td>
</tr>
</tbody>
</table>

**Supported Operating Systems and Software**

- Windows® Server® 2016 (64-bit)
- Windows® Server® 2012 R2 with Update 1 (64-bit)
- Windows® Server® 2012 (64-bit)

**Note:** The NAE85 software requires two Windows components: Microsoft .NET Framework Version 3.5 SP1 and Microsoft .NET Framework Version 4.6.1.

**Supported Operating Systems for Metasys Client Computers**

- Windows® 10 Pro and Enterprise Editions with Anniversary Update (version 1607) (64-bit)
- Windows® 8.1 Pro and Enterprise Editions with Update 1 (64-bit)
- Windows® 7 Professional, Enterprise, and Ultimate Editions with SP1 (64-bit)
- Windows® 7 Professional, Enterprise, and Ultimate Editions with SP1 (32-bit)
- Apple® macOS® 10.12 Sierra
- Apple® OS X® 10.11 El Capitan

**Notes:**

- Apple® operating systems are supported for Metasys client computers only.
- In Apple® OS X®, you cannot view Graphics+ graphics in the Site Management Portal UI.

**Internal Optical Drive**

- DVD ROM, SATA

**Recommended Antivirus Software**

- Symantec Endpoint Protection version 12
### Table 34: NAE85 software system recommendations for installation/upgrade

| Supported Web Browser Software for Metasys Client Computers | • Windows® Internet Explorer® 11.0.9600.18449 Update version 11.0.35 or later  
|• Google® Chrome™ version 54 or later  
|• Apple® Safari® 10 or later  
|**Notes:**  
|• In Internet Explorer 11, select the Use Microsoft compatibility lists option, found under Tools > Compatibility View Settings, to ensure that websites appear and function correctly.  
|• Other browsers, such as Mozilla® Firefox®, may also be used but are not fully supported.  
|• You use the web browser to download the Launcher application. After you install the Launcher application, you use the Launcher, not the web browser, to log in to Metasys Site Management Portal (SMP) UI. |

| 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 Protection | UPS for NxE85 model: APC Smart-UPS SC 450VA, 280 W, 120 VAC input/output, NEMA 5-15R output connections, OEM Part No. SC450RM1U |

### Table 35: NIE85 Software system recommendations for installation/upgrade

| Product Code | MS-NXE855W-0: NIE85 or NAE85 software for 10,000 objects (new projects only software) |
| Recommended Computer Platform | Intel® Xeon® E5506, 2.13 GHz, 4 MB cache  
|2 x 160 GB 7.2K RPM SATA, 8.9 cm (3.5 in.) cabled  
|3 Gbps, RAID 1 configuration with add-in SAS6/iR (SATA/SAS Controller) |
| Recommended Memory | 2 GB RAM minimum |
| Hard Disk | 160 GB minimum |
| Supported Operating Systems and Software | • Windows® Server® 2016 (64-bit)  
|• Windows® Server® 2012 R2 with Update 1 (64-bit)  
|• Windows® Server® 2012 (64-bit)  
|**Note:** Microsoft .NET Framework 3.5 Service Pack (SP) 1 and Microsoft .NET Framework 4.6.1 are required for any of the operating systems. |
## Table 35: NIE85 Software system recommendations for installation/upgrade

| Supported Operating Systems for *Metasys* Client Computer | • Windows® 10 Pro and Enterprise Editions with Anniversary Update (version 1607) (64-bit)  
• Windows® 8.1 Pro and Enterprise Editions with Update 1 (64-bit)  
• Windows® 7 Professional, Enterprise, and Ultimate Editions with SP1 (64-bit)  
• Apple® macOS® 10.12 Sierra  
• Apple® OS X® 10.11 El Capitan  
• Apple OS X 10.10 Yosemite  
**Note:** Apple operating systems are supported for *Metasys* client computers only. Also, in Apple OS X, you cannot view Graphics+ graphics in the Site Management Portal UI. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Optical Drive</td>
<td>DVD ROM, SATA</td>
</tr>
<tr>
<td>Recommended Antivirus Software</td>
<td>Symantec Endpoint Protection Version 12</td>
</tr>
</tbody>
</table>
| Supported Web Browser Software for *Metasys* Client Computers | • Windows® Internet Explorer® 11.0.9600.18449 Update version 11.0.35 or later  
• Google® Chrome™ version 54 or later  
• Apple® Safari® 10 or later  
**Notes:**  
• In Internet Explorer 11, select the *Use Microsoft compatibility lists* option, found under *Tools > Compatibility View Settings*, to ensure that websites appear and function correctly.  
• Other browsers, such as Mozilla® Firefox®, may also be used but are not fully supported.  
• You use the web browser to download the Launcher application. After you install the Launcher application, you use the Launcher, not the web browser, to log in to *Metasys* Site Management Portal (SMP) UI. |
| Supported Virtual Environments | Microsoft Hyper-V™, VMware® |
| Network Communication | Network Interface: Single 1 Gbps Ethernet network interface card 10/100/1000 Mbps (100 Mbps or better recommended) |
| Recommended Data Protection | UPS: APC Smart-UPS SC 450 VA, 280 W, 120 VAC input/output, NEMA 5-15R output connections, OEM Part No. SC450RM1U |

## Appendix: Time zone, date, and time management

### Time zone, date, and time management introduction

The time zone, date, and time used by all devices connected to a *Metasys* site are synchronized automatically, preventing errors from manual time entry and clocks that become inaccurate over time. 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 same time zone, date, and time consistently for all system operations.

Time synchronization occurs on the *Metasys* network when an engine or server sends an **IAmLive** message to the Site Director. If the IAmLive message fails, the engine or server sends another
message to retrieve the time from the Site Director. When the time is synchronized between the devices, a second IAmLive message is successful.

For network-wide time synchronization, the network engine designated as Site Director is the device time server because it provides the time zone, date, and time for all other engines/servers on the site. All other devices are considered time clients because they receive the time zone, date, and time from the Site Director. Beginning at Release 8.0, multiple time zone support was made available for upgraded network engines. The network engine designated as Site Director remains the device time server, but for network engines at Release 8.0 or later, the time synchronization occurs in UTC time, not in the time zone of the Site Director. For more details, see Multiple time zones.

To set the date and time in the Site Director (and therefore the entire site), you can set the time manually or select a time server for the Site Director. The time server for the Site Director is referred to as the site time server and should be a reliable source that is not on the Metasys network. Regardless of how you set the date and time, you must set the time zone in the Site Director.

**Note:** Beginning at Release 8.0, the Metasys System supports Release 8.0 (or later) network engines set in different time zones.

**Important:** Edit the Device Time Servers attribute or Time Sync Period attribute in the Site object only.

**Note:** 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 Microsoft Corporation.

**Overview of time synchronization**

This section contains a summary of how time synchronizes on a site with various system components. Table 36 summarizes the time sources for various system items. All time is Universal Time Coordinated (UTC) and all system devices handle DST.

**Table 36: Time Sources**

<table>
<thead>
<tr>
<th>Item</th>
<th>Time Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAE/NIE Trend Data</td>
<td>NAE/NIE</td>
</tr>
<tr>
<td>NAE/NIE Events</td>
<td>NAE/NIE</td>
</tr>
<tr>
<td>NAE/NIE Commands</td>
<td>NAE/NIE</td>
</tr>
<tr>
<td>Annotations</td>
<td>ADS/ADX/ODS</td>
</tr>
<tr>
<td>Event Acknowledgements</td>
<td>ADS/ADX/ODS</td>
</tr>
</tbody>
</table>

**ADS/ADX/ODS Site Director with Network Engines**

On a site with an ADS/ADX/ODS Site Director and network engines, the following time synchronization steps occur:

1. Site Director comes online.
2. Network engines come online and check in with the Site Director.
3. Every 15 seconds, the network engines check for Site Director online/offline conditions. If the Site Director is offline, the network engines send an IAmLive message to the Site Director every 20 seconds.
4. When the Site Director receives the IAmLive message, it attempts to validate the security credentials of the network engines. If the time in the network engines is different than the
time in the Site Director by 5 or more minutes (also taking into account the time zone of each network engine), the engine security credentials are invalidated.

5. Network engines come online and check in with the Site Director.

6. Every 15 seconds, the network engines check for Site Director online/offline conditions. If the Site Director is offline, the network engines send an IAmLive message to the Site Director every 20 seconds.

7. When the network engine receives back an invalidated credential, the network engines request the current time from the Site Director and update the engine time to match (also taking into account the time zone of each network engine).
   
   **Note:** Time between an Site Director and network engines synchronizes only if the time differs between the Site Director and network engines by 5 or more minutes. In the worst case scenario, one network engine could be 4 minutes and 59 seconds ahead of the Site Director, and another network engine could be 4 minutes and 59 seconds behind the Site Director.

8. After time is synchronized and the Site Director is online, the network engines send IAmLive messages to the Site Director every 5 minutes (instead of every 20 seconds).
   
   **Note:** Time synchronization is affected if you change the network engine's Site Director from an Site Director in one time zone to an Site Director in a different time zone. If you make this change online, as an interim step, promote the network engine to be its own Site Director, wait several minutes, then assign to the network engine the Site Director Site Director in the new time zone. This interim step ensures proper time synchronization.

**NIE and child devices**

- **Important:**
  
  We recommend that time be synchronized carefully between the NIE and the N1 network, preferably using a common external time server. All N1 network data collected by the NIE is time stamped at the NIE (no N1 network time stamps persist in the data collected by the NIE).

  While the NIE can push time to the NCM, the preferred method of synchronization for the NIE and N1 network is to have both synchronize with an external time server.

On a site with an NIE and child devices (NCMs, for example), the following time synchronization steps occur:

1. The NIE comes online and is mapped to NCMs.

2. When the time changes in the NIE (as a result of synchronization with an ADS/ADX/ODS, for example), the NIE pushes the time change down to the NCM. This time push requires that the Synchronize Time attribute of the NIE N1 Integration object is enabled.

**Time synchronization methods**

Three methods for network time synchronization are available in the Metasys system, including Windows Simple Network Time Protocol (SNTP) time synchronization, Multicast, and BACnet® time synchronization.

You can use the Microsoft Windows and Multicast methods when an SNTP master time server is available. If the Site Director has no access to SNTP time servers, you can use the BACnet synchronization method.

To enable a time synchronization method, modify the Time Sync Method attribute for the Site. See the **Steps for successful time management** and **Setting the time synchronization method** sections.
Windows time synchronization

The 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 can route User Datagram Protocol (UDP) traffic. Windows time synchronization may have a larger time interval in which devices are out of sync with the SNTP master time server due to skewing and convergence.

If you use Windows time synchronization, you must define a device time server in the Site Director using the Device Time Servers attribute.

Note: If you implement an intentional time change for your site, in less than 5 minutes, all other devices on the site update with the new time with Windows time synchronization.

Multicast time synchronization

The Multicast time synchronization is the Johnson Controls implementation of SNTP w32time with Multicast capabilities and RFC-2030 compliance. This method delivers the same features as the Windows method, but also provides Multicast functionality. The Multicast method provides improved Metasys time synchronization between the Site Director and supervisory devices. A time server provides the master time to the Site Director, and the Site Director in turn multicasts the time to all supervisory devices on the Metasys network.

When a supervisory device first signs up with 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. 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 form of time synchronization requires that all routers on the site support Multicast routing (Internet Group Multicast Protocol [IGMP]) because the Multicast time message crosses routers. The Johnson Controls SNTP time synchronization reduces the time interval in which devices are out of sync with the SNTP master time server.

BACnet time synchronization

BACnet time synchronization uses BACnet protocol to synchronize with BACnet devices such as the network engine. Use this method when the Site Director has access to a BACnet time server. This method is not available on the ADS/ADX/ODS.

Example network

Figure 50 shows an example system with a common time zone, date, and time management setup. This example is representative of the Multicast and Windows time synchronization methods.

The ADS/ADX/ODS Site Director 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/server on the Metasys network.
Multiple time zones

The time zone of the Site Director defaults to (GMT-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/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 ADS/ADX/ODS devices after ADS/ADX/ODS software installation.

Starting at Release 8.0, multiple time zones across a site are supported. This new capability is accomplished with a new attribute on the network engine’s Site object called Default Time Zone. This attribute has a drop-down list of all available world time zones 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 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:

- **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.

The ADS/ADX/ODS Site Director and the network engines must be at Release 8.0 or later to take advantage of the multi-time zone features. If a site has a mixture of engines at different Metasys releases, the older engines do not exhibit this new feature. For example, as Table 37 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.
Table  37: Time Zone Examples

<table>
<thead>
<tr>
<th>Device</th>
<th>Release</th>
<th>Time Zone</th>
<th>Time Zone Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADS/ODS</td>
<td>8.0 or later</td>
<td>Central</td>
<td>Central Standard Time</td>
</tr>
<tr>
<td>NAE</td>
<td>6.5</td>
<td>Mountain</td>
<td>Site Director’s time zone (Central)</td>
</tr>
<tr>
<td>NAE</td>
<td>7.0</td>
<td>Central</td>
<td>Site Director’s time zone (Central)</td>
</tr>
<tr>
<td>NAE</td>
<td>8.0 or later</td>
<td>Pacific</td>
<td>Pacific Standard Time</td>
</tr>
<tr>
<td>NAE</td>
<td>8.0 or later</td>
<td>Eastern</td>
<td>Eastern Standard Time</td>
</tr>
</tbody>
</table>

Note: If your system consists of a network engine Site Director with multiple child network engines, make sure 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 an alternative to setting 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.


See the Selecting a site time server for the Site Director Network Engine or Selecting a site time server for the Site Director ADS/ADX/ODS (Windows method only) sections.

Time in device object and user interface 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 51.

Figure 51: Local Time and Date Shown in User Interface

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.
In the ADS/ADX/ODS Site Director, the time zone, date, and time in the device object of the device are set by you or by the designated site time server. In a non-Site Director network engine, the time zone, date, and time in the device object come from the Site Director. The device object then passes the time zone, date, and time along to the Status Bar for display. If the device is busy, it may take a few minutes for the time zone, date, and time to update correctly in the Status Bar.

**Steps for successful time management**

For successful time management, do the following:

1. Verify that each non-supervisory engine/server on the Metasys network has the correct Site Director defined. See the Verifying the Site Director defined for an engines/server section.

2. Set the time synchronization method for the site. See the Setting the time synchronization method section.

3. Set the default time zone of the Site object for each network engine that has Metasys software at Release 8.0 or later.

4. Set the time zone and then set the date and time or select a site time server for the site. See the Network Engine as Site Director or ADS/ADX/ODS as Site Director section. If you have a network engine as the Site Director, the time zone, date, and time are set in the engine's Site object. See the Network Engine as Site Director section. If you have non-Site Director ADSs/ADXs on the site, you must set the time zone for these servers. If you have an ADS/ADX/ODS as the Site Director, the time zone, date, and time are set in the Windows operating system of the computer where the ADS/ADX/ODS resides. See the ADS/ADX/ODS as Site Director section. If you have non-Site Director ADS/ADX/ODS devices on the site, you must set the time zone for these servers.

5. For Multicast time synchronization only, configure the SNTP Multicast attributes for the site. See the Configuring additional multicast time synchronization settings section.

6. If a P2000 Security Management System (SMS) is integrated to the ADS/ADX/ODS server, both the P2000 and ADS/ADX/ODS servers should reference the same network time server. If the two systems use different time servers, the P2000 and ADS/ADX/ODS servers are not clock synchronized, which results in intermittent or no communication between the two systems.

**Verifying the Site Director defined for an engines/server**

For time synchronization to work properly, all engines/servers on a site must have the correct name for the Site Director in the Local Site Director attribute. If an engine/server has the wrong device defined as Site Director, time synchronization may not work properly on your Metasys site.

1. Log in to the engine/server.

2. Drag and drop the engine/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 52). In this example, the Site Director is a network engine (NxE-THREE).

   **Notes:**
   
   - 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, NxE-THREE is not the same as nx-e-three). 

   **Figure 52:**
   
   ![Site Director Configuration Example]
- If the Site Director field contains the wrong device or is empty, click **Edit**. Edit the Site Director entry and click **Save**.

5. Go to **Setting the time synchronization method**.

### Setting the time synchronization method

See the Time synchronization methods section for descriptions of the methods.

1. Log in to the Site Director engine/server.
2. Drag the Site object to the Display frame.
3. Click **Edit**.
4. Select **Advanced**.
5. In the Time section, in the Time Sync Method drop-down box, select the desired time synchronization method (Windows or Multicast).

![Figure 53: Time Sync Method Field](image)

6. If you select Windows time, enter a device time server in the Device Time Servers attribute. A device time server is required for Windows time synchronization.

7. Click **Save**.

   **Important:** When the Time Sync Method is set to Multicast and the ADS/ADX/ODS computer is synchronized with a time source other than itself, the Site Time Server must be an SNTP Time Server to allow the ADS/ADX/ODS to perform time synchronization. Time synchronization occurs when a change is detected in the ADS/ADX/ODS computer local clock, or at the Site configured Time Sync Period. Enabling Multicast time synchronization terminates the Windows win32time service, but changing the Time Sync Method back
to Windows does not re-enable the service. If you change the Time Sync Method back to Windows, you must manually start the win32time service, or restart the Site Director.

- **Note:** When the Time Sync Method is set to Windows, also set the Internet Time Server in the Windows operating system of the Site Director to match the IP Address specified for the Site Time Server. In Control Panel of the Site Director, search for **Date and Time**. On the Date and Time dialog box, click the **Internet Time** tab. Click **Change Settings** and enter in the Server field the same IP address that you defined in the Site Time Server attribute. Click **OK** to apply the change.

8. Go to **Network Engine as Site Director** or **ADS/ADX/ODS as Site Director**.

**Network Engine as Site Director**

If a network engine is the Site Director, you must set the time zone first, then either set the date and time or select a time server for the Site Director network engine.

- **Note:** See the **Verifying the Site Director defined for an engines/server** and **Setting the time synchronization method** sections before following the steps in this section.

**Setting the default time zone in the Site Director Network Engine**

1. Log in to 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 54).

- **Figure 54: Default Time Zone in the Site Object**

5. Click **Save**.

- **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 in to the network engine again.

If you are also manually setting the date and time in the Site Director network engine, go to **Setting the date and time in the Site Director Network Engine**.

If you are selecting a time server for the Site Director network engine, go to **Selecting a site time server for the Site Director Network Engine**.

**Setting the date and time in the Site Director Network Engine**

Before you manually set the date and time in the Site Director network engine, follow the steps in **Setting the default time zone in the Site Director Network Engine**.

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 55).

**Figure 55: Time in a Site Director Network Engine**

3. Click **Send**.

   **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 56).
6. Click Send.
   ☑ 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 attempt to set the time manually.

   The Site Director time zone, date, and time are now set and propagate to all other engines on the site.

Selecting a site time server for the Site Director Network Engine

Before you select a site time server for the Site Director network engine, follow the steps in Setting the default time zone in the Site Director Network Engine.

1. Reset the network engine for the time zone change to take effect.
2. Log in to the network engine.
3. Drag the Site object to the Display frame.
4. Click Edit.
5. In the Time section, in the Site Time Servers field, click the browse button.
   ☑ Note: The Device Time Servers field should be blank unless you are using Windows time synchronization. Do not change the value for the Time Sync Period attribute.
6. In the screen that appears, click Add (Figure 57).

7. Enter the IP address of the SNTP server from which the Site Director receives its time (Figure 58).

   **Note:** Specify a host name only if a DNS server is available to the Site Director. If you add more than one address, the Site Director network engine tries to contact the first address. If that fails, the network engine contacts the second one, and so on. The network engine use only the first address in the list.

8. Click OK.

9. Click Save. The Site Director now requests the date and time from the selected time server and propagates it to all other engines on the site.

10. Go to Configuring additional multicast time synchronization settings, if needed.

**ADS/ADX/ODS as Site Director**

Set the time zone first, then either set the date and time or select a time server for the Site Director ADS/ADX/ODS.

**Notes:**

- See the Verifying the Site Director defined for an engines/server and Setting the time synchronization method sections before following the steps in this section.
• If you select a site time server for your Site Director ADS/ADX/ODS, and you also set the
time manually in the ADS/ADX/ODS, the manual time is overridden at the end of the time
specified in the Time Sync Period attribute (default is 1 hour).

Setting the time zone in the Site Director ADS/ADX/ODS

1. In the lower-right corner of the ADS/ADX/ODS computer screen, click the time. The Date and
Time Properties box appears (Figure 59). The appearance of this screen varies depending on
the operating system.

   Figure 59: Time and Date on a Site Director ADS/ADX/ODS

   Monday, February 15, 2016
   
   < February, 2016 >
   
   Su Mo Tu We Th Fr Sa
   31 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 1 2 3 4 5
   6 7 8 9 10 11 12
   1:45:21 PM

   Change date and time settings...

2. Click Change date and time settings, then click Change time zone. The Time Zone Settings
box appears (Figure 60).

   Figure 60: Time Zone on a Site Director ADS/ADX/ODS

3. Select a time zone from the drop-down list box.

4. Select Automatically adjust clock for Daylight Saving Time, if present.
5. If you have non-Site Director ADS/ADX devices on your site, set the time zone in those servers following the instructions in this section. If you are also manually setting the date and time in the Site Director ADS/ADX, go to the Setting the date and time in the Site Director ADS/ADX/ODS section. If you are selecting a time server for the Site Director ADS/ADX, click OK and go to the Selecting a site time server for the Site Director ADS/ADX/ODS (Windows method only) or Selecting a site time server for the Site Director ADS/ADX/ODS (Multicast method only) section.

Setting the date and time in the Site Director ADS/ADX/ODS

Before manually setting the date and time in the Site Director ADS/ADX/ODS, follow the steps in the Setting the time zone in the Site Director ADS/ADX/ODS section.

1. Click the time in the lower-right corner of the screen. Click Change date and time settings.
2. Set the time and date.
3. Click OK.

The Site Director time zone, date, and time are now set and propagate to all other engines/servers on the site.

Selecting a site time server for the Site Director ADS/ADX/ODS (Windows method only)

If you set up a site time server for your Site Director, you can set the date and time manually in the ADS/ADX/ODS, but the manual settings are overridden at the end of the Time Sync Period.

Before selecting a site time server for the Site Director ADS/ADX/ODS, follow the steps in the Setting the time zone in the Site Director ADS/ADX/ODS section.

1. On the ADS/ADX/ODS computer, press the Windows key + R. The Run dialog box appears (Figure 61).

   ![Figure 61: Run Dialog Box](image)

2. Type Net time /setsntp:"10.10.16.1 10.10.16.2 ...", where 10.10.16.1 and 10.10.16.2 are example IP addresses of time servers.
   Note: The IT department should provide the address of a suitable time server. Be sure that the quotation marks are included (especially when listing multiple time servers).
3. Click OK.

   The Site Director now requests the date and time from the selected time server and propagates it to all other engines/servers on the site.
Selecting a site time server for the Site Director ADS/ADX/ODS (Multicast method only)

Before selecting a site time server for the Site Director ADS/ADX/ODS, follow the steps in the Setting the time zone in the Site Director ADS/ADX/ODS section.

1. Log in to ADS/ADX/ODS.
2. Drag and drop the Site object to the Display frame.
3. Click Edit.
4. In the Time section, in the Site Time Servers field, click the browse button (Figure 62).
   
   ![Figure 62: Site Time Servers in the Site Object]
   
   **Note:** Leave the Device Time Servers field blank. Do not change the value for the Time Sync Period attribute.

5. In the screen that appears (Figure 63), click Add.

![Figure 63: Add Site Time Server]

6. Enter the IP address of the SNTP server from which the Site Director receives its time.
   
   **Note:** Specify a host name only if a DNS server is available to the Site Director. Leave the Device Time Servers field blank. For Multicast time synchronization, if you add more than one address, the Site Director ADS/ADX/ODS tries to contact only the first address.

7. Click OK.
8. Click Save. The Site Director now requests the date and time from the selected time server and
propagates it to all other engines/servers on the site.

9. Go to Configuring additional multicast time synchronization settings.

Configuring additional multicast time synchronization settings

In addition to selecting the Multicast time synchronization method (Setting the time synchronization method), you must define other Multicast attributes.

To configure additional Multicast time synchronization settings:

1. Log in to the Site Director engine/server.
2. Drag the Site object to the Display frame.
3. Click **Edit**.
4. Select **Advanced**.
5. In the Time section, modify the attributes listed in Table 38 (Figure 64).

**Figure 64: Multicast Time Synchronization Fields**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast Group Address</td>
<td>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.</td>
</tr>
<tr>
<td>Multicast UDP Port</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Table 38: Multicast Time Synchronization Fields**
Table 38: Multicast Time Synchronization Fields

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast TTL</td>
<td>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.</td>
</tr>
<tr>
<td>Note:</td>
<td>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.</td>
</tr>
<tr>
<td>Multicast Heartbeat Interval</td>
<td>Specifies the number of minutes between forcing a Multicast time synchronization message from the Site Director to participating devices.</td>
</tr>
</tbody>
</table>

6. 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 65). Both of these files are located in the directory on the network engine as indicated in Table 39.

<table>
<thead>
<tr>
<th>Network engine</th>
<th>File location</th>
</tr>
</thead>
<tbody>
<tr>
<td>NCE25/NAE35/NAE45 (Release 9.0.7)</td>
<td>NAE Device\opt\metasys\var\Preferences\</td>
</tr>
<tr>
<td></td>
<td>NAE Device\opt\metasys\bin\UI\audio\</td>
</tr>
<tr>
<td>NAE55 (Release 10.0)</td>
<td></td>
</tr>
<tr>
<td>NAE85</td>
<td>C:\ProgramData\Johnson Controls\MetasysIII\Preferences</td>
</tr>
<tr>
<td></td>
<td>C:\Program Files (x86)\Johnson Controls\MetasysIII\UI\audio</td>
</tr>
</tbody>
</table>

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 65: System preference files

- 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 66) and correspond to files on the Metasys device in the directory as indicated in Table 39. As shown by two callouts in Figure 66:

- 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.
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

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® SMP 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 9.0.7) and NAE55 (Release 10.0):
   NAE Device\opt\metasys\bin\UI\audio\n
   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 39.

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 39.

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.
4. Record the file name of the user whose preferences you want to restore.
   📌 **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 39.
2. Delete files named *UserPreferences-userID.xml*, where userID is the identification number that appears in the Security Administration tool.
   📌 **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.
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 39.
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**

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 39.

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 39.

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 Wizard (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 39.
Appendix: Certificate Management

Certificate management introduction

Certificate Management is an option in SCT that you use 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 ADS/ADX/ODS 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.

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 Metasys® SCT 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.

The sections that follow describe how to manage security certificates for network engines with SCT 12.0, 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 (ADS, ADX, ODS, or NxEB85), refer to the appropriate document: Metasys® Server Installation and Upgrade Instructions Wizard (LIT-12012162), ODS Installation and Upgrade Instructions Wizard (LIT-12011945), or NxEB85 Installation and Upgrade Instructions (LIT-12011530).

Figure 67 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.
The following table explains each column in the Certificates window. Click inside a column header to sort the column.

**Table 40: Description of Certificates Table**

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>A security shield icon that indicates the connection status afforded by the certificate.</td>
</tr>
<tr>
<td></td>
<td>- : encrypted and trusted</td>
</tr>
<tr>
<td></td>
<td>- : encrypted and self-signed</td>
</tr>
<tr>
<td></td>
<td>- : encrypted, but either the certificate chain to the site or engine is broken, the certificate has a name mismatch, or the certificate has expired.</td>
</tr>
<tr>
<td>Checkbox Icon</td>
<td>A check box to select the device that you want to work with.</td>
</tr>
<tr>
<td>Issued To</td>
<td>The name of the device to which the certificate is issued.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of certificate: root, intermediate, or server.</td>
</tr>
<tr>
<td>Device</td>
<td>The device to which the certificate is bound (single or multiple for intermediate and root certificates).</td>
</tr>
</tbody>
</table>
Table 40: Description of Certificates Table

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expiration</td>
<td>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.</td>
</tr>
<tr>
<td>Details</td>
<td>A clickable arrow that opens an expanded panel with more detailed information about the certificate.</td>
</tr>
</tbody>
</table>

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 multi-step 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.

   **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.

5. 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.
6. Export all certificate files and store them in a safe and secure location in case you need to re-import them. See Exporting a certificate.

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

**Figure 69: Certificate Chain View**

**Figure 70: Missing Certificate Example**

This certificate is missing, and must be imported.
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

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.
4. Click the **Devices** tab. The Devices screen appears.

   **Figure 71: 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 72: Request Certificate(s) Form**

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

**Figure 73: Export CSR(s) Confirmation**

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

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

1. Open the archive database.


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

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

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

1. Open the archive database.
3. Click the **Devices** tab. A table of devices with certificates appears. Select the device whose certificate you want to export.
4. Click **Export Certificate(s)**. The Export Certificates dialog box appears.
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**

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

1. Open the archive database.


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.

**Figure 81: Certificate Download Wizard**

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**

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

1. Open the archive database.


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.)

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

To delete a network engine certificate from an archive database:

1. Open the archive database.


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

1. Open the archive database.
3. Select the device whose certificate request you want to delete. Click Delete. A confirmation message appears.

![Delete CSR Confirmation Message](image)

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
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.
3. Click the Devices tab. A table of all devices with certificates appears.
4. Select the device and click **Replace Self-sign**.

**Backing up a certificate**

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/NIE 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/NIE Update Tool Help (LIT-12011524)**.

1. Start the NAE/NIE 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/NIE Update Tool appears.

3. Enable verbose messaging in the message window by selecting **Advanced Mode** in the **Options** menu.

4. 

5. 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.
6. Under this General Settings tab, specify the required information for the network engine.

7. 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.

9. In the **File** section, click the browse button and select the correct image file to use for the engine type.

10. 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.

11. 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.
12. 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.

13. After you have entered all necessary fields, click **OK** to save your entries and return to the Main screen.

14. On the NAE/NIE Update Tool Main screen, make sure that the **Status** column entry for the network engine whose Flash memory you are erasing is **Enabled**. 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**.

15. 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/NIE Update Tool or turn off power to the network engine. Doing so adversely affects the process.

16. 

17. 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/NIE Update Tool Help (LIT-12011524)**.

18. 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.

19. Close the NAE/NIE Update Tool. The Flash memory is erased and replaced with the factory disk image. The SDRAM is also refreshed by the restart process.