F4-SNC Commissioning Guide

F4-SNC2515x-xx,F4-SNC16121-xx, F4-SNC2515x-xx,F4-SNC25151-xxx

Building Technologies & Solutions

LIT-12013549

www.johnsoncontrols.com

2020-12-14

Contents

Document introduction

This document describes the following:

- Create a new archive database and add an SNC to the archive.
- Configure a new SNC in several scenarios.
- Commission an SNC for network connectivity in several network scenarios.
- Configure the basic SNC parameters for initial operation on the network.
- Troubleshoot an SNC.
- Configure the SNC DDA for sending alarm and event messages through email and Simple Network Management Protocol (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 an SNC. In addition, this document does not describe how to build or download an archive database for a Facility Explorer® system site, or how to configure an SNC to monitor and control a Building Automation System (BAS).

ⓘ **Note:** In this document, SNC refers to the SNC2515x-xx and SNC1612x-xx models.

Related documentation

Table 1: SNC related documentation

For information about	Refer to
The daily operation of the Facility Explorer system network, navigating the SMP UI or System Configuration Tool (SCT) UI, monitoring and controlling BAS networks, and connecting to cloud-based applications	*Facility Explorer Site Management Portal Help (LIT-12013520)*
Installation considerations and guidelines, mounting, wiring, and starting up an SNC	*F4-SNC Installation Guide (Part No. 24-10143-02031)*
Installing the SCT software	*SCT Installation and Upgrade Instructions Wizard (LIT-12012067)*
How to install the Controller Configuration Tool (CCT) software	*CCT Installation Instructions (LIT-12011529)*
Using the CCT	*Controller Tool Help (LIT-12011147)*
How to set up a local or remote MS/TP communications Bus	*FX MS/TP Communications Bus Technical Bulletin (LIT-12011670)*
Security issues, including adding users and roles to the system and configuring standard and basic access modes	*Security Administrator System Technical Bulletin (LIT-1201528)*
Installing the Launcher application	*Launcher Installation Instructions (LIT-12011783)*
Using the Launcher	*Launcher Tool Help (LIT-12011742)*

SNC Series of supervisory controllers

The F4 SNC Series are Ethernet-based, supervisory controllers that connect Building Automation System (BAS) networks to IP networks. The SNC also features onboard inputs and outputs for direct control of equipment. This device monitors and controls networks of field-level building automation devices, including HVAC equipment, lighting, security, and fire safety equipment. The SNC has certified FIPS 140-2 Level 1 Compliance, which is a United States government cybersecurity standard that approves cryptographic modules/algorithms used for encryption.

The SNC Series of supervisory controllers perform a key role in the Facility Explorer system architecture. They provide network management and system-wide control coordination over one or more networks of controllers, including the following Facility Explorer controllers:

- CG Series General Purpose Equipment Controllers
- CV Series VAV Terminal Equipment Controllers
- PCA Advanced Application Programmable Controller
- PCG General Purpose Programmable Controllers
- PCX Expansion Input/Output Modules
- PCV Programmable Variable Air Volume Box Controllers
- LX VAV Box Controllers

In addition to providing supervisory control capabilities, the SNC Series also feature onboard input and output interfaces (I/O). The SNC2515x has a total of 40 I/O points - with 25 inputs and 15 outputs. The SNC1612x has a total of 28 I/O points - with 16 inputs and 12 outputs. The first two numbers of the product code represent the number of inputs (SNC**25**15x) and the next two numbers represent the number of outputs (SNC25**15**x).

An SNC has the following features for the building controls market:

- Non-volatile solid-state Flash memory to store all programs and data
- Multi-color LEDs to indicate power, communications, and device condition
- Removable, color-coded, screw terminal blocks for 24 VAC power, communications bus, and I/O point field wiring connections
- One FC Bus/Trunk configurable as BACnet MS/TP trunks
- One SA Bus that you can connect Input/Output Modules and increase the I/O control points in your application. You can also connect NS Series network sensors and supported variable frequency drives (VFDs) to the SA Bus, and integrate state-of-the-art temperature control and motor speed control into SNC application.
- One active RJ45 8-pin modular connector for Ethernet connection for BACnet/IP networks or two Ethernet connectors which support the daisy chain configuration.

The following table compares the features of the SNC Series of network control engines:

Features	SNC25151-0 SNC25151-0H	SNC25151-04 SNC25151-04H	SNC16121-0	SNC16121-04
Onboard inputs and outputs	• 40 total onboard I/O: 14 UI, 11 BI, 4 CO, 4 AO, 7 BO • Supports SA Bus expansion		• 28 total onboard I/O: 10 UI, 6 BI, 4 CO, 4 AO, 4 BO • Supports SA Bus expansion	
Communication interfaces	• 2 Ethernet port: SNC25151-0, SNC25151-0H, SNC25151-04, SNC25151-04H, SNC16121-0, SNC16121-04 • 1 RS-485 port • 2 USB ports for connecting external integration adapters[1]			
Maximum allowed devices across all integrations. For example, MS/TP +IP. Includes VND integrations and devices brought in through routers.	96	4	60	4
BACnet/IP maximum trunks	1	1	1	1
BACnet/IP maximum devices per trunk	50	4	50	4
BACnet MS/TP maximum trunks	1	1	1	1
BACnet MS/TP maximum devices per trunk	50	4	50	4
BACnet MS/TP maximum devices per trunk (with 3rd party)	50	4	50	4
Remote Field Bus maximum trunks	3	0	3	0
Remote Field Bus maximum Johnson Controls Devices per bus	32	0	32	0
Remote Field Bus maximum devices per bus (with 3rd party devices)	16	0	16	0
Maximum objects in device[2]	2500	2500	2500	2500

Features	SNC25151-0 SNC25151-0H	SNC25151-04 SNC25151-04H	SNC16121-0	SNC16121-04
Supported integration drivers	• BACnet/IP • BACnet MS/TP			
Operating System	Wind River® Linux LTS 17 (LTS=long-term support)			
Microprocessor	NXP i.MX6 DualLite processor			
Memory	2 GB of DDR3 RAM and 16 GB of eMMC Flash			
User Interface	Site Management Portal (SMP)			

1 Only the supported USB integration adapters function with the SNC. Other integration adapters that are not supported cannot function with the SNC.

2 Suggested object limit for performance considerations.

The SNC Series is scalable with varying network, trunk, and field device capacities to meet the requirements of different applications. All SNCs provide scheduling, alarm and event management, trending, energy management, data exchange, and password protection.

You use the Launcher application to log on to the SNC. Install the Launcher application if your machine does not have it installed. Refer to *Launcher Installation Instructions (LIT-12011783)* for more information.

Warning banner

An SNC configured as a Site Director or a child reporting to a Site Director that supports the warning banner can have one of three warning banners. The warning banner is a statement that always appears when operators log on to the SMP.

You have the choice of three different warning banners with customized information for each of the following agencies: U.S. Department of Defense (DoD), U.S. General Services Administration (GSA), or U.S. Department of Transportation (DOT) Federal Aviation Administration (FAA). The default selection is **None**. The reader must read and accept the conditions in the warning banner before logging on. The banner cannot be customized or have its text changed. For steps on how to enable or disable this banner, see Enabling and disabling the warning banner.

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 and the SA Bus. Each bus has its own set of device addresses. For details on how to apply the local and remote MS/TP bus, refer to the *FX MS/TP Communications Bus Technical Bulletin (LIT-12011670)*.

Facility Explorer network site configurations

A Facility Explorer network site can comprise of the following:

- One SNC device
- One or more field controller devices on the SNC's field bus
- One or more BACnet/IP field controllers

- One of more PCX/XPM devices

See Site Director for additional information on Site Director hierarchy.

SNC preparation

Each SNC installation, commissioning, and configuration scenario is unique.

ⓘ **Note:** Refer to *F4-SNC Installation Guide (Part No. 24-10143-02031)* for information about how to install an SNC.

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

The first task in commissioning an SNC is to establish a connection with the SNC using the Launcher. If your machine does not have Launcher already installed, an install prompt appears when you attempt to log on using the web browser. For details, refer to *Launcher Tool Help (LIT-12011742)* and *Launcher Installation Instructions (LIT-12011783)*.

ⓘ **Note:** You must follow this step prior to transferring the database to the SNC. The SNC transfer fails if the device has not been logged into and the default password changed.

After a connection is established, you can access the (Site Management Portal) SMP on the SNC from the Launcher. See SMP user interface and Accessing the SMP UI on an SNC for more information about how to access and navigate the SMP UI.

After you access the SMP UI on an SNC, you can configure the following parameters:

- 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
- Site Director status

Refer to the Certificate Management Introduction of the *SCT Help (LIT-12011964)* for more information on Certificate Management and about how to request, import, export, download, upload, or delete a certificate, to delete a certificate request, replace a self-signed certificate, or back up a certificate.

After you configure an SNC, you must commission the SNC at the job site.

SNC configuration

Create a new archive to configure a new SNC.

Create and edit the SNC archive database offline in the SCT. Refer to *SCT Help (LIT-12011964)* for information about how to create archive databases.

After you configure an SNC with an archive database that contains 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.

SMP user interface

You can view and edit SNC parameters and the parameters for associated devices in the engine's SMP UI. Use the Launcher to access the SNC SMP UI. See Accessing the SMP UI on an SNC.

In the Display panel on the right side of the window is a series of tabbed screens. 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 SNC is monitoring and supervising.

When you view the online SMP UI, the border around the panels is blue. When you view the offline SCT UI, the border is black.

Table 2: SMP UI tabbed screens

Screen tab designation	Purpose	Access online/ offline
Focus	Description and name (label) of the device object, the local time and date, the firmware version, message buffer and alarm, and audit repository sizes.	Online
Network	Establishes the Computer Name (host name) for network identity and LAN if applicable. The host name cannot consist of only numbers.	Both
Email	Establishes the SNC email alarm-notifications features common to all email messages and creates unique email message destinations.	Both
SNMP	Establishes the SNC Simple Network Management Protocol (SNMP) features common to all SNMP notifications and creates unique SNMP message destinations.	Both
Syslog	SNC Syslog server reporting destination information.	Both
Alarm	SNC alarm setup and destination information.	Both
Summary	Network and field device status information and attribute values for supervisory and field devices on the SNC field trunks.	Online
Diagnostic	Various status reports to aid in troubleshooting the SNC.	Both
Hardware	The Hardware tab shows hardware-related attributes available for the object type to which the point object belongs.	Both
Trend	Monitors and records the changes in parameter values of an SNC over time, assisting with diagnosing various system-wide behavioral characteristics.	Both

Menus, tab screens, attribute lists, values, and units of measure in the SMP 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 *Facility Explorer Site Management Portal Help (LIT-12013520)* for a description of menu items.

SCT

Use SCT to import the application file and download to the SNC.

Note: The SNC has two types of logic; the application/ control which is created, modified, and simulated with CCT and supervisory logic which is created in SCT.

SCT Pro

SCT Pro is the next generation of interface for SCT. For example, you can use SCT Pro to maintain healthy backup practices for a site, including the creation of backups automatically on a recurring schedule. SCT Pro does not include the full range of features that are available in SCT, but each release adds new features; and you can use SCT for the tasks that SCT Pro does not support.

Refer to *SCT Pro Help (LIT-12013035)* for more information on using SCT Pro.

CCT

Use CCT (version 13.1 or later) to create, edit, and commission applications for the SNC. Use SCT (version 13.2 or later) to import the application file and download to the SNC.

The SNC does not support the following CCT features:

- Transfers - Boot, Main, or Application code
- Attributes are not available - such as the **Network Settings** tab when **Define Hardware** is selected
- DIS1710/MAP
- BBMD
- Advanced Controller Features such as Calendars, Global Calendar, Intrinsic Alarming, Event Log, Notifications, Schedules, Trends, SA Bus Diagnostics
- Peer to Peer

  Note: The Connections option in the AV, BV, and MV objects in the Local Application is an alternative method which may be used in the absence of Peer to Peer connections.
- Connection types: MAP 4.2+ / BACnet Router, Zigbee, Direct Ethernet

For more information on CCT, refer to *Controller Tool Help (LIT-12011147)*.

FX Help files

The FX Help files provide shared system information and individualized mode-dependent information for the FX SMP or the SCT. The *Facility Explorer Site Management Portal Help (LIT-12013520)* contains information about alarming, commanding, auditing live data values, and other online features. The FX Help menu provides an option to open the Help file in PDF format.

Browser options for downloading the Launcher

After you install the Launcher, use the Launcher, not the web browser, to open the SMP UI.

Archive databases

An SNC archive database, which resides in the SNC internal memory, contains only the specific configuration information that makes up the network integrations, field devices, and field points that the SNC is supervising. Each SNC retains only its own archive database. You can also save the SNC database in a archive database on a Server or another computer using the SCT. A graphical

representation of some of the items contained in an SNC archive database is shown in the SMP UI or SCT UI navigation panel.

You can upload an SNC archive database to the SCT where you can save it to a hard disk or other long-term storage media. You can also edit an SNC archive database offline in the SCT and download the edited archive database to the SNC.

Site Director

The Site Director UI contains a single point of access to the site. The Site Director also supports functions such as user log on, user administration, user views, time synchronization, and data traffic management.

SNC computer name

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

The initial computer name is often useful during commissioning for locating and connecting to an SNC 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 SNC Computer Name on the site.

- **Important:** If you change the Computer Name of an SNC with SCT, all existing references between the SNC 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.

SNC object name

The SNC **Object Name** is an editable attribute on the SNC **Focus** tab that the software uses to identify the SNC in the SMP UI and in the SCT. The **Object Name** is a label only and is not necessarily the same as the computer name. Changing the **Object Name** changes the name that you see in the navigation tree, alarm messages, trend reports, and other screens in the SMP UI and SCT that refer to the SNC. Changing the **Object Name** does not affect the object references or network communication with other devices on the site. You can change the **Object Name** at any time. Use an intuitive name that clearly identifies the SNC in the SMP UI and site.

Log on user names and passwords

All SNC have the same default initial log on user name and default password. The initial log on user name is , and it is not case sensitive. For the default password, contact your local Johnson Controls representative.

Use the initial user name and password to log on to any SNC the first time you commission the SNC. The **Change Password** dialog box prompts you to change the initial default password before you continue. You must change the default password when you first log on to a new SNC, or a recently updated SNC with the SCT. The process to update the password may take up to 60 seconds to complete.

You must use complex passwords to access the SNC securely on the site. Complex passwords meet the following requirements of the particular language: English, non-English, or Asian, which you can review in the **Change Password** window. For English users, the requirements are as follows:

- The password must include a minimum of 8 characters and a maximum of 50 characters.
- The password cannot include spaces or include a word or phrase that is in the Blocked Words list.
- The password and the username cannot share the same three consecutive characters.
- The password must meet the four following conditions:

  - Include at least one number (0–9)
  - Include at least one special character (-, ., @, #, !, ?, $, %)

    Note: Use only the special characters listed above; all other special characters are invalid.

  - Include at least one uppercase character
  - Include at least one lowercase character

Note: When you change or add an SNC 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 SMP UI without a valid user name and password. Refer to *Security Administrator System Technical Bulletin (LIT-1201528)* for details.

SNC connectivity

You can establish a connection between a computer and an SNC using one of the following procedures:

- Preparing an SNC for a network that supports DHCP and DNS
- Preparing an SNC for a network without DHCP and without DNS support when the SNC uses APIPA
- Preparing SNC for a network without DHCP and without DNS Support when the SNC uses a static IP address
- Preparing SNC 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 SNC depends on how the SNC fits into the site hierarchy. See Appendix: Time Zone, Date, and Time Management for information and detailed procedures for setting time zone, date, and time on an SNC and on a network.

Alarms and events

Each SNC stores alarm and event messages generated by the SNC and the connected field trunk devices. You can configure an SNC to send alarm and event notifications through the SNC 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 a Server, each SNC can forward alarm and event information to the Server for centralized notification and long-term storage.

➤ **Important:** To avoid a loss of notification when the repositories become full, the system manages the SNC repositories according to the following criteria:

- Events forwarded to a Server Event Repository are removed before unforwarded events.
- The event that is replaced first is the lowest priority event with the oldest time stamp, and with the Acknowledge Required flag set to **False**.
- If the new event is of a higher priority than at least one event in the repository, it replaces the event with the oldest time stamp and with the lowest priority.
- If all events are of the same priority, it replaces the event with the oldest time stamp.
- If the new event is of a lower priority than all other events in the Event Repository, it replaces no event and the new event is discarded.

A loss of emailing can result if you do not commission the SNC with strict adherence to these criteria. To avoid managing events in this way, move the notification DDAs to the server.

You can designate multiple alarm and event sources in an SNC 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 SNC also has several pre-configured internal diagnostic features that are factory set to generate alarms. SNC device diagnostic features with factory-set default alarm values include those listed in the following table.

Table 3: Default SNC Alarm values

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

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

Email notification

You can configure an SNC to generate alarm and event messages by sending an 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 SMP UI.

Syslog DDA

An SNC 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. 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. A vertical bar symbol (|) separates individual fields of each message and a single character dash (-) replaces any blank field to help assist in reading the log.

The Syslog option is disabled, by default. 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 SNC.
- You can specify no more than three Syslog destinations.
- The firewall port must be open.

The definition of the Syslog DDA requires the following:

- A label to identify the Syslog server.
- The 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 pass to the Syslog server.

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

When the **Syslog Reporting Enabled** attribute is set to **True**, the feature is active and forwards your messages (events and audits) 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 forwards no messages to the Syslog server.

The Syslog DDA implementation is UDP, not TCP. When the Syslog server is offline it does not record any audits or events at the Syslog server, even though the system, unable to determine the 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.

Use the console to filter the messages. If you do not have a tool, open a web browser and enter the following URL:

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

For example: http://SysLogserver1:8088/Events.aspx

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

If problems occur when you try to implement the Syslog DDA functionality, consult the following table:

Table 4: Syslog server troubleshooting

Scenario	Behavior
The SNC is starting up but the Syslog DDA has not yet started.	When started, all generated audits and events are cached and sent to Syslog DDA. The maximum size of the cache is 1,000 audits and 1,000 events.
The Syslog server crashes.	All generated audits and events that the engine sends to the Syslog server are lost and nothing is cached.
The Syslog server goes offline or is unreachable.	All generated audits and events that the engine sends to the Syslog server are lost and nothing is cached. The Syslog server receives no data until it comes back online or becomes reachable.
The IP address, name, or port numbers of the Syslog server as defined in the engine's object are invalid.	All generated audits and events that the engine sends to the Syslog server are lost and nothing is cached. The Syslog server receives no data until you correct the invalid parameters in the Syslog DDA.
The Syslog Reporting Enabled parameter is set to **True**, but do not define the Syslog parameters.	All generated audits and events that the engine sends to the Syslog server are lost and nothing is cached. The Syslog server receives no data until you specify the parameters that the Syslog DDA requires.
Your firewall is blocking the by the UDP Send Port or UDP Receive Port	All generated audits and events that the engine sends to the Syslog server are lost and nothing is cached. The Syslog server receives no data until you open the ports on the Syslog server.
A parameter of the Syslog server changes, but the corresponding parameter in the Syslog DDA of the engine is not likewise changed.	All generated audits and events that the engine sends to the Syslog server are lost and nothing is cached. The Syslog server receives no data until you correct the invalid parameters in the Syslog DDA.

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. Large BAS networks with many network devices would use SNMP monitoring. The SNMP management computer monitors all devices on the network and receives and stores all alarm and event notifications.

The SNC 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 SNC SNMP alarm notifications and destinations. If you are applying a Facility Explorer 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 SMP UI. Perform this configuration to each SNC individually

Initial default SNC configuration

SNCs come with standard initial values for many of the editable attributes. The following tables list some important initial default configuration values.

Table 5: SNC initial configuration values

Attribute/field name	SNC
Computer Name	SNCxxxxxxxxxxx, where xxxxxxxxxxx is the Ethernet MAC address of the device without hyphens. For example, if the Ethernet MAC address is 00-10-8D-05-0F-FC, the initial Computer Name is SNC00108D050FFC.
DHCP Client	Enabled
Site Director	A new SNC is a Site Director for itself by default.
Initial Login Password	Contact your local Johnson Controls representative.

Allow HTTP

An attribute called **Allow Http** is located under the **Network** tab of the engine in the SMP UI. This attribute controls if the 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 SNC. Changing this attribute to **False** blocks all incoming network traffic over port 80 at the network engine.

The **Allow Http** attribute is set independently on each SNC. 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.

Staged Firmware Version and Staged Files

The SNC has two special attributes called Staged Firmware Version and Staged Files. These attributes support the dual partition format of the device's memory chip. These fields are usually empty. They are described as follows:

- **Staged Files**: lists staged files that are set for activation at a later time. For example, if the code and archive database are set for later activation, this field would read Code, Archive Database. If this attribute is empty, no files are currently staged. Possible values: Code, Archive Database, Security Database, HTTPS Certificates.
- **Staged Firmware Version**: indicates the engine firmware version that is staged for later activation. If this field is empty, no firmware files are currently staged. This attribute is in contrast to the Firmware Version attribute, which indicates the engine's firmware version that is currently active.

Site Security Level

There is an attribute in the SNC Site object called **Site Security Level**. If the SNC is a Site Director, you use this attribute to select if you want to enable only encrypted communication or encrypted and trusted communication between the SNC Site Director and its child engines. Do not set this attribute to **Encrypted and Trusted** until you have downloaded, with trusted certificates, all SNCs reporting to the Site Director. If the site has one or more network engines with self-signed certificates and some older engines without certificates, set this attribute to **Encrypted Only**.

System and user preferences

The system contains customized preferences for the SMP 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 you can access from within the UI of the SNC device.

Reset device command

The SNC Reset Device command in the SMP UI initiates an orderly reset that saves recent changes to the SNC archive database and restarts the SNC operating system. When the SNC 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

  Changing the SNC **Computer Name** value forces a device reset. If the SNC is configured for DHCP, after the reset occurs, it may receive a different IP address from the DHCP Server.

➤ **Important:** To avoid losing data, do not push the Reset button on the SNC to initiate a device reset. Pushing the Reset button initiates a CPU reset and restart of the SNC, which causes all unsaved data to be lost, including recent attribute value and archive database changes.

SNC 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 SNC, 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

The following table 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 SNC network sensitivity.

Table 6: Network Sensitivity Adjustments

Navigational Tree Item	Attributes to Adjust
Network Engine: Focus window	APDU Segment Timeout APDU Timeout APDU Retries Internode Comm Timer
BACnet Protocol Eng	Poll Delay
Eth IP DataLink	APDU Segment Timeout APDU Timeout APDU Retries Internode Comm Timer
BACnet IP	Internode Comm Timer APDU Segment Timeout APDU Timeout APDU Retries
Field Bus MSTP	Internode Comm Timer APDU Segment Timeout APDU Timeout APDU Retries

Detailed procedures

You need the following items to perform the detailed workflow procedures for the SNC:

- An SNC.
- A laptop or desktop computer with a suitable browser to download the Launcher application.

Note: In some scenarios, the computer must be a DHCP client or configured to use a static IP address appropriate for the network.

- SCT loaded on the commissioning computer.
- CCT

  Note: Refer to the *Release Enhancements and Compatibility* section in the *Controller Tool Help (LIT-12011147)* for more information. CCT 13.1 at Release Mode 10.4 is required for this release.

- Newest Field Controller Package file

  Note: You must license the field controller package file.

- The SNC Ethernet MAC address.

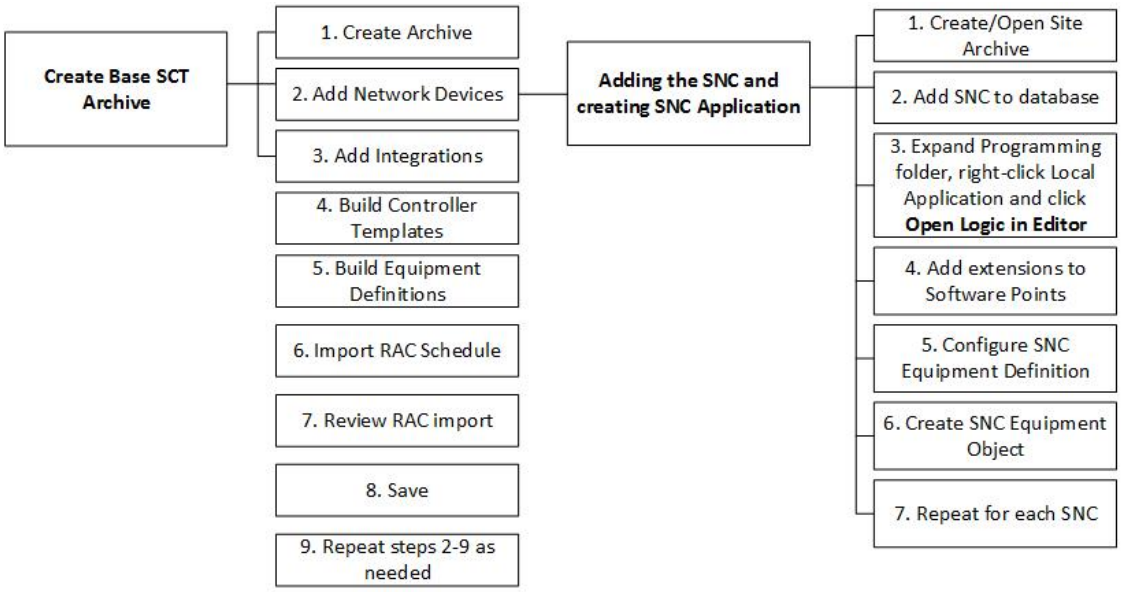
You may also need the following items:

- An Ethernet cable.
- A unique static IP address for each SNC on the network if DHCP cannot be used.

SNC application workflow

The following figure shows the workflow on how to configure a new SNC on a site.

Figure 1: Configuring a new SNC workflow



Note: If an PCX goes offline, the points mapped to the PCX do not display as offline in the Navigation Tree as the points are under the Local Hardware Folder and not the PCX.

ⓘ **Note:** The Rapid Archive Creation workflow is supported for controllers on the FC Bus of the SNC only, not the Local Application.

Creating a New Archive Database

About this task:

ⓘ **Note:** If another archive database is already open, you cannot create a new archive database. Before you create a new archive database, a prompt appears to close any open archive databases.

1. From the **Item** menu, select **New Archive**. The New Archive wizard appears.
2. Enter a name for the new archive. All archive files are created in the same directory.
   ⓘ **Note:** There are the following restrictions for archive names:

   - Archive names are not case sensitive.
   - Archive names cannot be longer than 32 characters.
   - The first character can only be an alphabetical character from a to z.
   - You cannot include special characters in the name. For example, ! @ # $ % . and & are not allowed.
   - Archive names cannot include spaces.

3. Choose the type of archive to create.
   ⓘ **Note:** To discover devices and add them to the archive, see Creating a New Archive Using Device Discovery.

Creating a New Archive Using Device Discovery

About this task:

Use the **Scan the site for engines (fast)** feature of the **New Archive** wizard, to retrieve site information from a Site Director, and quickly build an archive database that includes all of the engines in the site. Be aware that only limited information about the engines is transferred to the archive. An engine's objects, security, and certificates are not transferred.

1. In the **New Archive** wizard, click **Scan the site for engines (fast)**.
2. In the **Site Director Reference** field, enter the name of the Site Director.
   ⓘ **Note:** The **Site Director Reference** field is case sensitive.
3. **Optional:** In the **Site Director IP** field, enter the IP address of the Site Director.
   ➤ **Important:** If you are using a static IP address for your Site Director, you must enter its IP address in the **Site Director IP** field.
4. Verify that you can communicate with the Site Director by entering a valid User Name and Password that is defined in the Site Director's security database. The user must have administrative privileges on the Site Director. Click **Test Login**. If communication is established, `Login ID is OK` appears. If the message `Login ID is not OK` appears, enter the correct login details, then click **Test Login**.
5. Click **Create**. A new archive is created. The SCT creates a site in the archive that has the same name as the Site Director.

Adding an SNC to the archive

1. With the archive database open, from the **Insert** menu, select **Supervisory Device**. The Insert Device Wizard Select Object Type screen appears.
2. Select SNC .

3. Follow the prompts on the screen to configure the SNC. See the following table for details.

Table 7: Insert Device Wizard Screens

Screen	Purpose
Object Type	Select SNC.
Destination	Select the site where the SNC resides.
Identifier	Type a unique name for the SNC. A unique name is required for each SNC in an archive. By default, the name of the object being entered has a number appended to keep it unique.
Configure	Access engine features, including: **Configuration** - If **Basic** is selected, you can edit parameters such as name and description. If you select **Advanced**, you can configure additional parameters such as engineering values, alarm snooze, audit trail, and site. **Communications** - Configure the serial port. **Network** - Enter the LAN settings and configure dial-up settings for accessing the network over dial-up connections. **Email** - Set up SMTP and POP destinations. You can add email addresses for the engine to send messages. **SNMP** - Enable SNMP and add destinations.
Summary	View the basic parameters of the supervisory device just added.

4. Click **Finish**.

Configuring a new SNC

About this task:
The following steps describe how to configure a new SNC.

1. In the SNC archive, expand the Programming folder to access the Local Application.
2. Right-click the Local Application and click **Open Logic in Editor**. The CCT opens in archive-connected mode.
3. Select the appropriate SNC model and map the points under hardware for each of the control application's inputs and outputs.

   ⓘ **Note:** When you configure the control application in CCT, set the BACnet Exposed attribute to **True** for any control application data that you want to display in the SCT and SMP UI's navigation tree. When BACnet Exposed is set to **False**, SCT does not create an object under the Local Application as an interface to the application data. All points under the Inputs, Outputs, and Miscellaneous data boxes in CCT are exposed by default and cannot be turned off.

4. Save and exit the CCT.
5. Refresh the SCT.

   ⓘ **Note:** When you save the new configuration and refresh SCT UI, you can see the changes in the points with green download arrows. If the CCT is in an archive-connected mode, it connects to the archive. Anything saved in the CCT is updated in the SCT. If you try to delete a point in the SCT from a point created by the save operation in the CCT, you get an error message. To delete an exposed point that was automatically created by SCT you must change the BACnet Exposed attribute to **False** and resave the `.caf` file back into SCT.

6. Add extensions to the software points in the Local Application under Programming.

   ⓘ **Note:** The Local Application name changes to the System Name of the CCT application after saving. If project requirements need to monitor direct hardware commands, you can add extensions to the Hardware I/O.

7. To manually build the equipment definition, expand the Equipment Definitions folder and to add the points you want to include, drag and drop the points, the controller, or the SNC application.
8. To create the equipment object, in Equipment Definition click **Open in Discovery** to automatically discover the points you mapped.
9. Click **Save** to build the Equipment objects.
10. Manually add the Serving information.
11. Manually add any Served By to the equipment object, if required.
12. Click **Save**.
13. Repeat Steps 2-12 as needed.
14. Go to Downloading the archive to the SNC to download the archive to the SNC.

Duplicating a new SNC

About this task:
Complete the following steps to duplicate a similar SNC:

1. Right-click the SNC, click **Edit**, and then click **Copy**.
2. Paste the SNC.
3. To modify the local application to account for any differences, right-click the local application object in the Programming folder of the SNC and click **Open Logic in Editor**.
4. To create the equipment object, in Equipment Definition click **Open in Discovery** to automatically discover the points you mapped.
5. Click **Save** to build the Equipment objects.
6. Manually add the Serving information and the Served By to the equipment object if required.
7. Click **Save**.

Configuring a new SNC with an existing CAF file

About this task:

1. In the SNC archive, expand the Programming folder to access the Local Application.
2. Right-click the Local Application and click **Import CAF file**.
3. Browse to the location of the `.caf` file.
4. Click **Import CAF File**.
5. Refresh the SCT.
6. Add extensions to the points in the Local Application.

   ⓘ **Note:** The Local Application name changes to the System Name of the CCT application after saving.

   ⓘ **Note:** You can add extensions to the Hardware I/O if project requirements require monitoring of direct hardware commands

7. To create the equipment object, in Equipment Definition click **Open in Discovery** to automatically discover the points you mapped.
8. Click **Save** to build the Equipment objects.
9. Manually add the Serving information and the Served By to the equipment object if required.

10. Click **Save**.
11. Go to Downloading the archive to the SNC to download the archive to the SNC.

Creating a CAF file in CCT

About this task:
A Controller Application File (CAF) is a file which contains all the logic components needed to represent a system. The tool prompts you to save a controller application file for each system you create. If you save this file you can access it later to make changes or to use it for additional systems. Refer to *CCT Help (LIT-12011147)* for more information about how to create a CAF file.

Configuring a new SNC with existing logic

About this task:
The following steps describe how to configure a new SNC with already existing logic from another SNC. This procedure imports the Local Application from one SNC to the other. Extensions are not part of the import.

1. In the SNC archive, expand the Programming folder to access the Local Application.
2. In SCT, right-click the Local Application and click **Import Application Logic**. This imports the local application from one SNC to the other.
3. Select the item and click **OK**.
4. Add extensions to the software points in the Local Application under the Programming folder.

   ⓘ **Note:** The Local Application name changes to the System Name of the CCT application after saving.

   ⓘ **Note:** If project requirements need to monitor direct hardware commands, you can add extensions to the Hardware I/O.
5. To manually build the equipment definition, expand the Equipment Definitions folder and to add the points you want to include, drag and drop the points, the controller, or the SNC application.
6. To create the equipment object, in Equipment Definition click **Open in Discovery** to automatically discover the points you mapped.
7. Click **Save** to build the Equipment objects.
8. Manually add the Serving information.
9. Manually add any Served By to the equipment object, if required.
10. Click **Save**.
11. Repeat Steps 2-10 as needed.
12. Go to Downloading the archive to the SNC to download the archive to the SNC.

Downloading the archive to the SNC

1. Select the SNC and then select ***Tools*** **>** ***Manage Archive***.
2. In the **Manage Archive** Wizard under **Type**, select **Download to Device**.
3. Select **Activate Immediately** to activate the download.
4. Select **Enable SNC Logic** so the device begins operating.
5. Click **Next** until you reach the Site Login page.
6. Enter the password and click **Login**.
7. If the device is paired, click **Last**. If the device is not paired, enter the Site Director username and password and click **Login** to pair the device.
8. Click **Finish**.

Commissioning an SNC

1. In the SNC archive, expand the Programming folder to access the Local Application.
2. Right click the Local Application and click **Open Logic in Editor**. The CCT opens in archive-connected mode.

   Note: To commission the device, you must open the CCT from the SCT using **Open Logic in Editor**.
3. Click **Commission**.
4. Select **NxE Passthru** in the **Commission Device** dialog box.
5. Click **Manual** under Connection Parameters; or in an archive-connected mode you can click **Connect to Supervisory Device** and **Connect via Site Director** if the DNS is configured on the site appropriately or the SCT archive has the IP address of those devices.
6. Ensure the **Host Name/IP Address** field is correct and enter the **Password**.
7. Click **Login**. The device should be identified.
8. Click **Next**.
9. Select a device from the list and click **Next**.
10. Click **Finish**.

Editing application without downloading the SNC

1. Open the Manage Archive wizard and upload the SNC.
2. Modify the application as necessary.
3. In the Manage Archive wizard, select **Synchronize**, then click **Next**.
4. Enable the SNC logic.

   Note: Logic is disabled by default.

Installing Launcher to access the SNC

About this task:
Use the Launcher application to access the SNC.
If you have not already installed the Launcher application, complete the following steps:

1. Start the web browser.
2. Enter the following URL in the address field: https://www.johnsoncontrols.com/launcher.
3. Click the Launcher version you want to download.
4. Follow the instructions on the screen to install the Launcher. Refer to the *Launcher Installation Instructions (LIT-12011783)* if needed.
5. Start the **Launcher** application. The Launcher window appears.
6. Click **Add**. The **Add New** window appears.
7. Enter the host name (or IP address) of the SNC 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 SNC in the **Description** field to make the SNC easier to find in the profile list, or you can keep the default IP address. Click **Save**. The SNC is added to the profile list on the SMP tab.
9. Select the SNC 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 SNC and click **Login**. See Log on 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 SNC

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

1. Make sure that the SNC is receiving power and running.
2. Connect an Ethernet switch with two Ethernet patch cables between the Ethernet port of the SNC and your computer. Make sure that the LAN **is not connected** to the Ethernet switch.
3. Verify that the ETH ACTIVITY LED on the SNC and Ethernet switch are lit to confirm connectivity between the computer and the SNC through the Ethernet switch.
4. Verify that the Local Area Connection for the Ethernet connection to the SNC 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 SNC 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 system login screen for the network engine using the Launcher. See Accessing the SMP UI on an SNC for information on accessing the SMP UI.

Preparing an SNC for a network that supports DHCP and DNS

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

ⓘ **Note:** Configure a DHCP reservation for the SNC to ensure it always receives the same IP address when its lease expires. This practice prevents address bindings between the SNC and other devices from breaking.

1. Verify that your network administrator has updated the DNS server and the DHCP server with the SNC Ethernet MAC address and the SNC host name, if using DHCP reservation.
2. With your computer or commissioning laptop connected to the building network, launch SCT Pro.
3. From the Dashboard, in the Utilities pane, click **Discover**. The Device Discovery page appears.

4. Click **Discover**. All engines on the same subnet as the SCT Pro server appear in the list.
5. Connect the SNC to the network with an Ethernet cable.
6. Go to Installing Launcher to access the SNC, follow all instructions, and then return to the next step in this section.
7. After you have completed the steps in Installing Launcher to access the SNC, including the step for logging on to the SNC, select the SNC device object in the Navigation panel, and drag it to the Display panel of the SMP UI. The **Focus** tab for the selected SNC appears in the Display panel.
8. 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.
9. 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 engines incoming http communication port (port 80), select **False** for **Allow Http**.

   ⓘ **Note:** Changing the **Computer Name** forces a device reset on the SNC. See SNC computer name and Reset device command.
10. Go to the **Focus** tab and check the SNC **Object Name**. Change the **Object Name** to the descriptive label used to identify the SNC in the SMP UI and SCT.

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

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

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

1. Set your computer for DHCP, which gives an APIPA address with no DHCP server available.
2. With your computer or commissioning laptop connected to the building network, start SCT Pro.
3. From the Dashboard, in the Utilities pane, click **Discover**. The Device Discovery page appears.
4. Click **Discover**.
5. Connect supply power to the SNC and wait for the SNC to complete initialization.
6. Go to Installing Launcher to access the SNC, follow all instructions, and then return to the next step in this section.
7. After you have completed the steps in Installing Launcher to access the SNC, including the step for logging in to the SNC, demote the SNC from Site Director if the SNC is not going to be the Site Director. See Designating an SNC as a child of a Site Director.
8. **Optional.** Select the **Network** tab of the SNC device object. You can change the **Computer Name** value from the factory default. See SNC computer name and Reset device command.

Use the APIPA IP address to access the SNC; this can be shown with SCT Pro device discovery.

Preparing SNC for a network without DHCP and without DNS Support when the SNC uses a static IP address

About this task:
This scenario may occur when you install the SNC on a stand-alone network dedicated to building control only. You can perform the steps from a computer attached to the network or a computer connected directly to the SNC with an Ethernet cable. If you connect the computer to the network, connect the computer to the same subnet as the SNC. To connect to the SNC with this procedure, you need to know the IP address of the SNC.

1. Check the network IP address and the subnet mask of the computer.
2. Set your computer for DHCP, which gives an APIPA address with no DHCP server available.
3. With your computer or commissioning laptop connected to the building network, start SCT Pro.
4. From the Dashboard, in the Utilities pane, click **Discover**. The Device Discovery page appears.
5. Click **Discover**. All engines on the same subnet as the SCT Pro server appear in the list.
6. Connect supply power to the SNC and wait for the SNC to complete startup and initialization.
7. Go to Installing Launcher to access the SNC, follow all instructions, and then return to the next step in this section.
8. After you have completed the steps in Installing Launcher to access the SNC, including the step for logging on to the SNC, demote the SNC from Site Director if the SNC is not going to be the Site Director.
9. Select the SNC device object from the Navigation panel of the SMP UI and drag it to the Display panel. The SNC device object UI opens in the Display panel.
10. Select the **Network** tab of the SNC device object and click **Edit**.
11. If you want, you can change the **Computer Name**. Change DHCP Enabled attribute value to **False**. This disables DHCP and APIPA.
12. Specify the IP Address, IP Mask, and IP Router Address. The network administrator assigns these values.
13. Record the assigned IP address for the SNC for future reference.
14. Click **Save**. The SNC automatically logs you out and resets.
15. Wait for the SNC to complete the startup and initialization sequence.

    To log on to the SNC, enter the IP address in Launcher on any subnet of the network. Change your computer to a unique static IP on the same subnet as the SNC to access it.

Preparing SNC for a network that supports DHCP but not DNS

About this task:
This scenario is common to many building networks. The SNC uses DHCP only without DNS if DHCP reservation is being used. If this is not the case, use static IP addresses as described in Preparing SNC for a network without DHCP and without DNS Support when the SNC uses a static IP address.

1. Attach the SNC to the network using an Ethernet cable.
2. Ensure the computer is set for DHCP.
3. With your computer or commissioning laptop connected to the building network, start SCT Pro.
4. From the Dashboard, in the Utilities pane, click **Discover**. The Device Discovery page appears.

5. Click **Discover**. All engines on the same subnet as the SCT Pro server appear in the list.
6. Connect supply power to the SNC and wait for the SNC to complete initialization
7. Go to Installing Launcher to access the SNC, and then follow all instructions, then return to the next step in this section.
8. After you have completed the steps in Installing Launcher to access the SNC, including the step for logging on to the SNC, select the SNC device object from the Navigation panel of the SMP UI and drag it to the Display panel. The SNC device object UI opens in the Display panel.
9. Update the SNC **Computer Name** value on the **Network** tab. After you update the computer name, the SMP UI automatically logs out, and the SNC automatically resets.
10. Wait for the SNC to complete the startup and initialization sequence.

Preparing SNC for a network that supports DNS but not DHCP

This scenario is not typical of modern networks.

1. Check the network IP address and the subnet mask of the computer.
2. With your computer or commissioning laptop connected to the building network, start SCT Pro.
3. From the Dashboard, in the Utilities pane, click **Discover**. The Device Discovery page appears.
4. Click **Discover**. All engines on the same subnet as the SCT Pro server appear in the list.
5. Connect supply power to the SNC and wait for the SNC to complete startup and initialization.
6. Go to Installing Launcher to access the SNC, follow all instructions, and then return to the next step in this section.
7. After you have completed the steps in Installing Launcher to access the SNC, including the step for logging on to the SNC, demote the SNC from Site Director if the SNC is not going to be the Site Director.
8. Select the SNC device object from the Navigation panel of the SMP UI and drag it to the Display panel. The SNC device object UI opens in the Display panel.
9. Select the **Network** tab of the SNC device object and click **Edit**.
10. If you want, you can change the **Computer Name**. Change DHCP Enabled attribute value to **False**. This disables DHCP and APIPA.
11. Specify the DNS IP Address, IP Address, IP Mask, and IP Router Address. The network administrator assigns these values.
12. Record the assigned IP address for the SNC for future reference.
13. Click **Save**. The SNC automatically logs you out and resets.

Using the SNC Ethernet MAC address from the SNC label, the network administrator can update the DNS server and the assigned computer name. You can then enter `dns-name` in Launcher on any computer on the building network.

Accessing the SMP UI on an SNC

About this task:
After SNC is set up for connectivity, you can access the SMP UI through the Launcher
You need to know the **Computer Name** (or IP address) of the SNC you want to access.
To access the SMP UI on an SNC through the Launcher:

1. Start **Launcher**.
2. If the SNC is not already added to Launcher, on the Launcher screen, click the **SCT** tab to locate the device in the profile list. Select the device in the list.
3. Click **Launch**. (You may also right-click the profile in the list and select Launch from the menu that appears.) The standard system login screen appears.
4. Enter the SNC Username and Password, and then click **Login** or press **Enter**.
5. To view an SNC, select the SNC object from the Navigation panel and drag it to the Display panel. The SNC object opens with the **Focus** tab active.

Establishing basic SNC parameters in the Focus tab

About this task:
To establish basic parameter in the **Focus** tab, complete the following steps:

1. In the SMP UI, display the SNC device object and click the **Focus** tab.
2. Select the **Advanced** option and click **Edit.**
3. Edit the SNC Object Name and Description values as required.
4. Click **Save.**

   If the SNC is not a site director, enter the site director's IP in the **Site** section of this screen so the SNC can find the Site Director. Refer to for more information.

Establishing the SNC network parameters

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

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

ⓘ **Note:** If you are building the SNC database online, you must establish the production network SNC **Computer Name** value before you establish references to objects on the SNC.

To establish the network parameters, complete the following steps:

1. In the SMP UI, display the SNC device object, click the **Network** tab, and then click **Edit**.
2. In the **Network Identification** section, enter the **Computer Name** value.
3. Enter the LAN attribute values as needed and click **Save**.

Creating email alarm and event notifications and destinations

An SNC 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, set up the Email DDA and configure the email notifications and the notification destinations after you configure the SNC with an archive database that includes the user database.

1. In the SMP UI, display the SNC device object, click the **Email** tab, and then click **Edit**.

2. Enter the Shared Configuration values according to Table 8. These fields establish values for attributes that are common to all email alarm notifications generated from this SNC. Scroll down to the **Destinations** section of the **Email** tab. Refer to *Alarm and Event Management* in for additional information on setting the attribute values for alarm and event notifications.
3. Click **New**.
4. Enter the destination values according to the following table. Refer to *Alarm and Events Management* section in the for additional information on setting the attribute values for alarm and event notifications.

Table 8: Shared attributes for all email destinations

Attribute	Description (value requirement/range)	Initial value
SMTP Server Host	Specifies the SMTP server name that handles outgoing email. Required value.	0.0.0.0
SMTP Port	Specifies the TCP port that the server uses to deliver email message. Required Value of 1 to 25.	25
Authentication Type	Specifies the Authentication Type the SNC uses to log on to the outgoing email server. Select SMTP, POP before SMTP, or None.	None
SMTP User Name	Specifies the user name the SNC uses to log on to the SMTP server that handles outgoing email messages. Required only if SMTP is selected for Authentication Type.	–
SMTP Password	Specifies the password the SNC uses to log on to the SMTP server that handles outgoing email messages. Required only if you select SMTP for Authentication Type.	–
POP Server Hostname	Specifies the POP server name for incoming email messages. Required only if the email server requires POP before SMTP, before it accepts email messages from the client. If you leave this field blank, POP before SMTP is disabled.	–
POP User name	Specifies the POP user name. Required only if POP Authentication is required and there is a value specified for POP server host. Maximum 20 characters	–
POP Password	Specifies the POP Password. Required only if POP Authentication is required and there is a value specified for POP server host. Maximum 20 characters	–
From Email Address	Specifies a valid email address that is recognized and exists on the SMTP Server. Required Value.	–

Table 8: Shared attributes for all email destinations

Attribute	Description (value requirement/range)	Initial value
SSL Email Enabled	When True, emails are sent over an SSL-encrypted connection if the server supports encryption with StartTLS. When this parameter is set to **True**, you cannot send emails if they cannot be encrypted, regardless of the SSL Email Ignoring Errors attribute setting.	False
SSL Email Ignoring Errors	When set to **True**, the email is sent even if the email server certificate appears to be invalid. When set to **False**, the email is sent only if the operating system can verify that the server sent a valid SSL certificate. You can only enable this feature if SSL Email Enabled is True.	False
Email Diagnostics	Displays diagnostic information regarding the communication between the Email DDA (SMTP Client) and the SMTP Server. This attribute displays both successful and unsuccessful email message deliveries.	–

Table 9: Attributes for specific email destinations and notifications

Attribute	Description (value requirement/range)	Initial value
Label	Specifies a name for the email destination.	–
Email Address	Specifies the destination email addresses. This is a required value.	–
Priority	Specifies the email message priority as high, low, or normal.	Normal
Subject	Contains the body text of the email message. The maximum characters allowed is 256.	–
Retries	Specifies the number of attempts at sending the email message. (0–10 Retries)	3

Table 9: Attributes for specific email destinations and notifications

Attribute	Description (value requirement/range)	Initial value
Enabled	Enables or disables Email Destination. (True, False)	True
Event Filters	Enables you to specify the rules that filter alarm and event notifications. Each filter has an **Item**, **Operator**, and **Value**.	–
Format	Enables some predefined format characteristics of the notifications sent to a destination. Predefined format characteristics include: • Priority • Message (content) • Value • Site Name • Item Description • Item Fully Qualified Reference • Authorization Category • Acknowledge Required • Previous Status (Enable a format by selecting the check box next to the format.)	Show default checked items for Priority, Message, Value, Item Description, Item Fully Qualified Reference, Authorization Category

5. Click **...** to the right of Destination Email Addresses. You can import user names and the associated email addresses from the list of user names for the site.
6. To filter the email messages sent to a destination, click **New** beside the **Filters** section of the **Email Destination Configuration** tab.
7. Select the Item, Operator, and Value for the condition that you want to trigger the email notification.
8. Click **OK**.
9. Enable the Format characteristics for email notifications sent to the specified destinations by selecting the check boxes next to the Format characteristic. Add additional email destinations with filters and formats as required.
10. Click **Save**.

Configuring encrypted email

Your user name and password is encrypted by software once you enter it 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 software encrypts the entire email payload, 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 usually 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, you need to 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 an 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 trusting the certificate the mail server uses, ensure a major certificate authority obtains the signed certificate.
- If you use 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, install any available certificate updates from Microsoft Windows® Update.

You can configure encrypted email in three ways:

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

Configuring encrypted email with no authentication required

About this task:

ⓘ **Note:** Encrypted Email with No Authentication Required functions only when you **Anonymous Authentication** on the mail server.

1. View a network engine.
2. Click the **Email** tab.
3. Click **Edit**.
4. Edit the Attributes in the Shared Configuration as shown in Table 10.

Table 10: Attributes for no authentication required

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

5. Verify that you sent the email correctly.

Configuring encrypted email with SMTP authentication

1. View a network engine.
2. Click the **Email** tab.
3. Click **Edit**.
4. Edit the Attributes in the Shared Configuration as shown in Table 11.

Table 11: Attributes for SMTP authentication

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

5. Verify that you sent the email correctly.

Configuring encrypted email with POP-before-SMTP authentication

About this task:

ⓘ **Note:** When you enable SSL Email and you use POP-before-SMTP Authentication, the 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 you enable SSL Email and you use POP-before-SMTP Authentication, the 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 according to the following table:

Table 12: Attributes for POP-before-SMTP authentication

Attribute	Selection
SMTP Server Host	For example: mail.yourdomain.com or yourdomain.com
SMTP Port	465
Authentication Type	POP-before-SMTP
POP Server Hostname	yourdomain.com or pop.yourdomain.com
SSL Email Enabled	True
SSL Email Ignoring Errors	False

5. Verify that you sent the email correctly.

Creating SNC SNMP alarm notifications and destinations

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

You can use SNMP monitoring for large BAS networks with many network devices. The SNMP management computer monitors all devices on the network and receives and stores all alarm and event notifications.

You must set up SNMP monitoring at the network level and you must assign an SNMP management device on the network. If you apply a 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 you configure an SNC with an archive database that includes the user database.

1. In the SMP UI, display the SNC device object and click the **SNMP** tab.
2. Click **Edit**.
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.
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. See the following table for more information.

Table 13: Share attributes for SNMP destination

Attribute	Description (value requirement/ range)	Initial value
SNMP Enabled	Enables or disables SNMP DDA on the SNC. (True, False).	False
SNMP Trap Version	Specifies the version of SNMP used on the network on which the SNC resides. Not required if **SNMP Enabled** is set to **False**.	SNMP Version 1
SNMP Management Device	Specifies the IP address or host name of the SNMP Management device on the network on which the SNC resides. The direction of communication is from the SNMP Management device to the SNC.	–
SNMP Request Port	Specifies the port on the SNMP server where SNMP notifications go. Not required if **SNMP Enabled** is set to **False**.	161
Contact Person	Specifies the contact person for the SNMP notifications. Not required if **SNMP Enabled** is set to **False**.	–
Public Community Name	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**.	Public
SNMP Trap Message Format	Specifies the format used to generate SNMP notifications. Change to **MIB Based** when SNMP management application uses the SNC MIB file to translate SNMP notifications. Not required if **SNMP Enabled** is set to **False**.	String Based

6. Click **New** in the **Destinations** section. The window where you can edit the **Destination Configuration** appears.

7. Enter the destination information for the SNMP trap. See the following table for more information.

Table 14: Attributes for specific SNMP notifications

Attribute	Description (value requirement/range)	Initial value
Label	Specifies a functional name for the destination SNMP server. Maximum 20 characters.	Destination #
Trap Community Name	Specifies the SNMP Community Name used by the Network Management System (NMS) group to listen to the traps. Maximum 20 characters.	Public
IP Address	Specifies the IP Address of the NMS system that receives the trap messages.	0.0.0.0
Destination Port Number	Specifies the port on the SNMP Management device that receives messages from the SNC. The direction of communication is from the SNC to the SNMP Management device.	162
Enabled	Enables or disables the SNMP destination.	True
Filters	Enables you to specify the rules that filter alarm and event notifications. Each filter has an item, operator, and value.	–
Format	You can 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 SNC can be set up to generate custom alarm and event email messages and send the messages to one or more specified Syslog Servers.

1. In the SMP UI, display the SNC device object and click the **Syslog** tab.
2. Click **Edit**.
3. Click the **down** arrow for the **Syslog Reporting Enabled** attribute and select **True**.
4. In the **Destinations** section, click **New**.
5. Enter the Destination Configuration values according to the following table.

Table 15: Attributes for specific syslog destinations

Attribute	Description (value requirement)
Label	Specifies a name for the Syslog server. For example, Syslog1.
Syslog Server	Specifies the IP address or resolvable host name of the Syslog server configured to receive events and audits from the SNC.
UDP Send Port	Specifies the Syslog port used to send messages to an SNC.
UDP Receive Port	Specifies the Syslog port used to receive messages from an SNC.
Event Filters	Specifies the rules for filtering the alarms and events sent to the Syslog server. Each filter has an **Item**, **Operator**, and **Value**.
Audit Filters	Specifies the rules for filtering the audit messages sent to the Syslog server. Each filter has an **Item**, **Operator**, and **Value**.

6. In the **Event Filters** section, click **New**.
7. In the **Add Filter** dialog box, 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.
9. In the **Event Filters** section, click **New**.
10. Select the item, operator, and value of the condition that you want to trigger a message to the Syslog server. You can add additional audit filters and syslog destinations.
11. Click **OK**.
12. Click **Save**.

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

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

Setting up the SNC alarm parameters

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

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

Editing the existing alarm parameters

1. In the SMP UI, select and drag the SNC object or field device object that you want to edit the alarm parameters from the Navigation panel and drop it in the Display panel. The SNC or field device **Focus** tab opens.
2. Click the **Alarm** tab. The **Alarm** tab opens.

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

Creating a new alarm

About this task:
You can create new alarms for the SNC or any of the supported field devices on the field trunks attached to the SNC.

1. Select and drag the SNC or field device object from the Navigation panel into the Display panel.
2. Select the **Alarm** tab.
3. Click **New**.
4. In the **Insert Alarm** wizard, select the device attribute for which you want to create an alarm.
5. Follow the wizard instructions and create or edit the values for the Attribute for which you want to create an alarm.
6. Click **Save**.

Designating an SNC as a child of a Site Director

About this task:
All SNC's 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 SNC's on the site that are not the Site Director.
In many network site commissioning and configuration scenarios, the Site Director status of the SNC on the site is built into the archive database for the site. The status of these devices is established on the SNC when the archive database is downloaded from the SCT to the site devices. The SCT database download overwrites the existing values in the SNC.
You typically demote an SNC from the Site Director offline in the SCT UI, but you can complete the process online in the SNC SMP UI. The procedure in this section describes how to use the SNC SMP UI to demote an SNC from the Site Director. To do so with the SCT, go to the Changing the 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 SNC Computer Name values in the SNC UI must match the values in the SCT archive database.

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

1. On the Navigation panel, select the SNC that you want to demote from Site Director.
2. Drag the SNC into the Display panel to open the **Focus** tab.
3. Select **Advanced**.
4. Click **Edit**.
5. Scroll down to the Site attributes and select the **Local Site Director** field.
6. Type the host name or IP address of the SNC that you want to designate as the local Site Director.
7. Click **Save**. To view an image of the message box.
8. If you wish to proceed, click **OK** to this confirmation message; otherwise, click **Cancel**.

9. 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**.

    a. If the credentials you entered are correct, the SNC logs you out and resets. Wait several minutes for the SNC to reset, then log in to the Site Director. The navigation tree shows the SNC is now a child of the Site Director, and the SNC is paired with its Site Director.
    b. If the credentials you entered are incorrect, a dialog box appears to report a failed connection. Click **OK** and try to log on again.

Changing the Site Director with the SCT

About this task: Start the SCT, and add the new device to the archive database for the site. The SCT automatically makes the new device the Site Director and demotes the SNC.

Removing user accounts from a demoted Site Director

If you demote a supervisory controller or Server 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.

Moving the security database and clearing it from demoted Site Director

About this task:

ⓘ **Note:** If **Include Security** is selected (default), the security database backup is performed as part of the SCT upload, regardless of whether or not the supervisory controller or Server 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 5.

2. Log on to the demoted controller from the SMP.
3. Change your password when prompted at the log on screen.

    ⓘ **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 with security 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 the warning banner

Note: The warning banner that is set in the Site Director appears if you log on to a child device of the Site Director.

1. In the SMP UI of the Site Director, display the Site object, click the **Site View** tab, click the **Advanced** button in the top right and then click **Edit**.
2. Scroll to the bottom of the window to locate the **Warning Banner** attribute.
3. Select a banner type from the **Warning Banner** list. **None** is selected by default.

   Note: You can select one of the 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).
4. Click **Save**. The setting takes from three to five minutes to become effective at the network engine.

Adjusting SNC network sensitivity

About this task:
Follow the steps in this section to adjust the network sensitivity of the BACnet/IP and MS/TP field bus networks for a network device. 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.
Before you begin, verify that the SNC 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 the following table.

Table 16: Supervisory Device Network Settings

Attribute	High Sensitivity	Medium Sensitivity	Low Sensitivity
APDU Segment Timeout	4000 ms	10000 ms	20000 ms
APDU Timeout	6000 ms	10000 ms	20000 ms
APDU Retries	4	4	5
Internode Comm Timer	20 seconds	120 seconds	240 seconds

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 the following table.

Table 17: BACnet Protocol Eng Network Settings

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

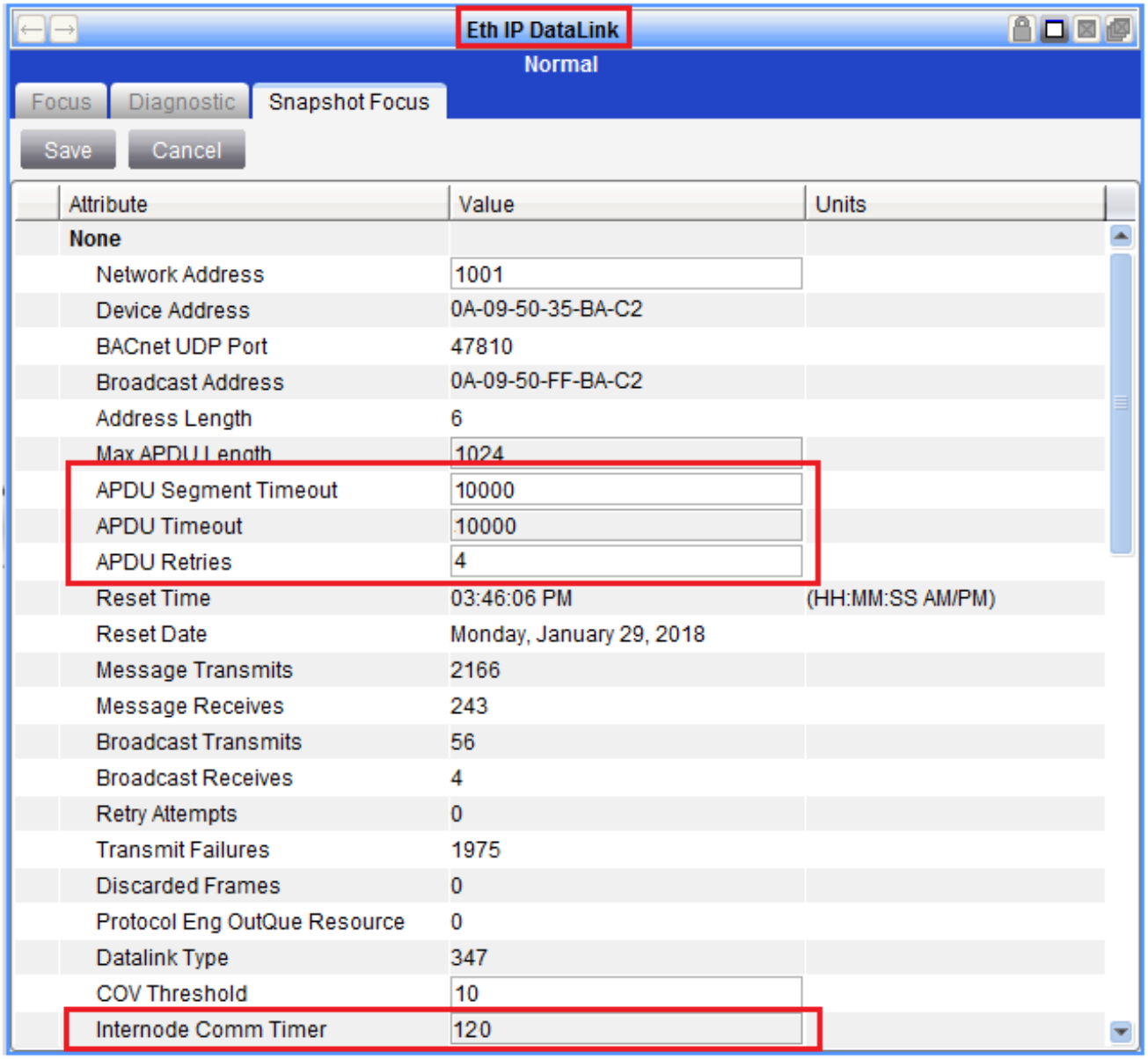
4. Click **Save**.

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 the following table.

Table 18: Eth IP DataLink Network Settings

Attribute	High Sensitivity	Medium Sensitivity	Low Sensitivity
APDU Segment Timeout	4000 ms	10000 ms	20000 ms
APDU Timeout	6000 ms	10000 ms	20000 ms
APDU Retries	4	4	5
Internode Comm Timer	30 seconds	120 seconds	240 seconds

Figure 2: Example: Eth IP DataLink Network Settings



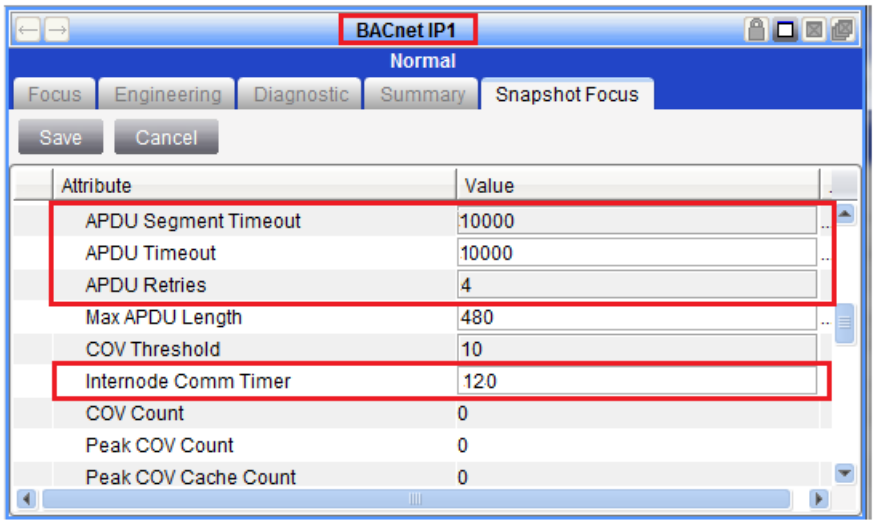
6. Click **Save**.

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 the following table.

Table 19: BACnet IP Network Settings

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

Figure 3: Example: BACnet IP Network Settings



8. Click **Save.** Figure x 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 SNC

About this task:
To replace an SNC on a network site, update the site registration to ensure that devices on the site communicate with the new (replacement) engine; otherwise, devices may attempt to communicate with the network engine that was removed from the site.
If you do not remove the SNC from a site correctly, the Site Director may attempt to send messages to the old SNC, creating unnecessary network traffic.
If the SNC'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 Site Director or Server.

To replace the SNC, complete the following steps:

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

2. Physically replace the old SNC with the new SNC, connect the new SNC to the network, and power on the new SNC.
3. Do one of the following:

   - Configure the SNC with the same host name and IP address of the old SNC from the SMP.

     Note: This configuration lets you download the database with SCT without using the Device Change option.

   - Verify that the SCT can communicate with the SNC, then select the Device Change option when downloading the database with SCT to identify the Site Director and host name of the new SNC.

4. Download the existing SNC archive database to the new SNC.

Troubleshooting

This section describes some issues you may encounter when you set up and operate an SNC. Use the general solution guidelines and procedure references in this section to avoid or resolve these problems.

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

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 SNC, it may be necessary to isolate the SNC from the Ethernet network and the associated field trunks and field devices, and then direct-connect to the SNC with a computer to browse the SMP UI.

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 SNC. If you forget the password, see Recovery button for more information.

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 SNC attribute values do not match the values entered in the devices connected to the SNC, the SNC 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.

For example, communication between a Site Director and an SNC could be lost after you download the network engine with SCT. This may occur on a network where device name resolution is not implemented. To resolve this communication issue, log on to the SNC 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.

SNC reset related problems

Certain setting changes initiated in the SMP UI do not take effect until the SNC is reset. Reset the SNC whenever you are prompted or if the SNC's status is `reset needed`, and allow the SNC to complete the reset sequence. See Reset device command.

Troubleshooting guide

The following table provides information for troubleshooting an SNC.

Table 20: Troubleshooting the SNC

Problem	Solution
The SNC does not operate when powered on	Corrupted flash memory or data loss are the most common causes of this problem. To resolve this problem: 1. Ensure that the database does not exceed the SNC flash memory capacity. 2. Reload the disk image and download the archive database to the SNC while the SNC is disconnected from the network.
The SNC does not operate after updating the disk image, downloading an archive database, or installing a patch.	Corrupted flash memory and data loss are the most common causes of this problem. To resolve this problem: 1. Ensure that the database does not exceed the SNC flash memory capacity. 2. Reload the disk image and download the archive database to the SNC while the SNC is disconnected from the network.
The SNC does not communicate with any other device.	Make sure that 24 VAC power is connected correctly and that the 24 VAC and HEARTBEAT LED is on.
	Make sure that communication terminal blocks and other communication connectors are firmly in place.
	Check that the wiring is the correct size (18 AWG minimum for power, 26 AWG for Ethernet communication).
	Check that you have set the correct baud rate on each connected device.
	Check the integrity of the wires and cables.
Ethernet communication is not present.	Verify that you are using the correct cable.
	Check the port and cable integrity. Make sure that the ETH ACTIVITY LED is flickering green. Check that the hub or switch into which the LAN connector is plugged works and is connected correctly.
The SNC runs slowly.	The amount of data you are trying to process is too much for the SNC to handle. A value of 50% or less for the CPU Usage attribute of the network engine is considered acceptable, although other performance indicators should also be assessed.

Table 20: Troubleshooting the SNC

Problem	Solution
Only the host name or the IP address of the network engine changes, even though you changed both attributes.	In some instances, you need to make each change in separate steps. To resolve, change the host name first, reboot, then change the IP address. This scenario can occur if the network engine is placed online to a network that does not have an active DHCP server.
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 network engine.
	Check that the power transformer secondary is not shared with another load.
The SNC overheats.	When the internal temperature reaches the high limit, the SNC issues an alarm and lights the 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 unit has been damaged or all external causes of failure have been checked.	Replace the network engine.
The following message appears: `Extensions from an item of type AV Mapper can only be pasted to another item of type AV Mapper.`	Extensions cannot be copied from one object to the other if the objects are not of the same object type. In this case you either need to manually create the extension or find an existing extension that is of the same object type that can be copied.
The following message appears in the Focus window for a SNC: `Item Not Found`	The SNC has become unpaired with the Site Director. This issue may occur after you set the Advanced Security Enabled option under the Site Director's Site object to True. Pair the SNC with the Site Director. If this action does not restore communication, restart the SNC that has not paired.

Pre-boot execution environment (PXE)

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

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

Setting a computer to be compatible with APIPA

About this task:
If you are configuring an SNC 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 the Control Panel, select ***Network and Sharing Center > Change adapter settings***. The **Network Connections** window appears.
   b. Right-click **Local Area Connection** and select **Properties**.
2. Right-click on **Local Area Connection** and select **Disable** followed by **Enable**.

SNC diagnostic tools

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

The primary SNC diagnostic tools include:

- LED status indicators
- Diagnostic tab
- Summary tab

LED status indicators

LEDs on the front panel of the SNC indicate its functional state. For a comprehensive list of LED functional information, see Table 21.

LED test sequence at startup

During startup, the SNC automatically initiates a self-test to verify correct operation of the unit. When you connect supply power, the following LED lighting sequence occurs:

- The **HEARTBEAT** LED flashes blue/purple when the SNC starts.
- The **FAULT** LED is solid red for approximately 30 seconds, then turns off.
- The **USB-1|2** LED flashes green when a supported device is connected to either of the USB ports. The LED turns solid red when an unsupported device is connected. The LED is off if no device is connected.

SNC LED indication table

Table 21 describes each LED on the device. The normal states are in bold. A flicker has a fast blink rate faster than one second and a flash has a much slower blink rate of one second.

Table 21: SNC LED designations, normal statuses, descriptions, and other conditions

LED name	Color	State	Description
HEARTBEAT	Multi-color: blue or purple	**Flashing blue and purple**	1 blink per second (1 Hz) = Normal operating system and all monitored processes start and the device is running
		On blue	Power is supplied by 24 VAC, but controller is non-operational
		Medium flicker, purple and blue	2 blinks per second (2 Hz) = SNC starting up
		Fast flicker, purple and blue	5 blinks per second (5 Hz) = SNC shutting down
		Off	No power
FAULT	Red	**Off**	No faults and normal operation
		On	Device fault or no application loaded. Diagnostics are running or fault conditions are detected. For example, excessive memory or flash usage, or a high CPU/PWB temperature.

Table 21: SNC LED designations, normal statuses, descriptions, and other conditions

LED name	Color	State	Description
SA BUS	Green	**Flashing**	1 blink per second (1 Hz) = indicates communication activity
		On	Devices have been defined but none are communicating (network engine transmitting only)
FC BUS	Green	**Flashing**	1 blink per second (1 Hz) = indicates communication activity
		Off	No devices are communicating or no controllers have been configured to work with this bus
		On	Controllers have been defined but none are communicating (network engine transmitting only)
ETH-1 and ETH-2	Green	**Flickering**	Data is transferring on the Ethernet connection
		Off	No communications
USB-1|2	Green or Red	**Flashing**	Flash green = 1 blink per second (1 Hz), an approved device or devices are connected and communicating correctly to either USB-1|2
		On	Solid red = an unapproved device is connected to USB 1 and/or USB 2. In this case a user needs to sequentially remove each device until the LED flashes green or the LED is turned off. ⓘ **Note:** Only approved USB adapters that have been tested and qualified function with the SNC. Non-qualified adapters do not function with the SNC.
		Off	No USB device is connected
EOL	Yellow	**On**	On Steady = end-of-line termination is enabled for the Field Bus connection
		Off	Off Steady = indicates the end of line termination network is disabled

Reset button

The SNC features a recessed Reset button that is located directly above the LEDs and to the left of the Recovery button. To force an immediate restart of the SNC engine and a reset of the processor, press and hold down the Reset button for at least four seconds with an extended paper clip or mini screwdriver. This action is otherwise known as a hard reset or processor reset. During the reset, the SNC's archive database and any data the SNC has collected are lost. The data includes all historical information, including alarm, trend, and audit trail data. If you need to reset the SNC but retain the archive and stored historical data, you can either press and immediately release the reset button, or issue a Reset Device command from the user interface. This type of reset is known as a soft reset.

Note: Press the reset button only if the SNC fails to respond and users cannot access it. Do not press the reset button unless you have tried other means to fix the problem.

Diagnostic tab

The **Diagnostic** tab displays SNC hardware status information useful for troubleshooting.

With the SNC object selected, click the **Diagnostic** tab to view current information about the SNC hardware status.

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.

Summary tab

The **Summary** tab in the SMP 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 SNC requests the status of the items in the Display panel. This request may take a few minutes.

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 SNE00108D050FFC.)
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.

Technical specifications

Table 22: Technical specifications

Specification	Description
Power requirement	Dedicated nominal 24 VAC, Class 2 power supply (North America), SELV power supply (Europe), at 50/60 Hz (20 VAC minimum to 30 VAC maximum)
Power consumption	32 VA maximum from main power supply ⓘ **Note:** The VA rating does not include any power supplied to the peripheral devices connected to Binary Outputs (BOs) or Configurable Outputs (COs), which can consume up to 12 VA for each BO or CO, for a possible total consumption of an additional 132 VA (maximum).
Power source	+15 VDC power source terminals provide 100 mA total current; quantity of inputs: five, located in Universal Input terminals; for active (3-wire) input devices
SA Bus power	15 V at 240 mA maximum
Operating System	Wind River® Linux LTS 17 (LTS=long-term support)
Processor	NXP i.MX6DualLite Processor, 1GHz 32-bit dual core Cortex A9 processor
Memory	16 GB flash nonvolatile memory for operating system, configuration data, and operations data storage and backup 2 GB SDRAM for operations data dynamic memory
Universal Input (UI) resolution	Input: 24-bit Analog to Digital converter
Analog Output (AO) accuracy	Output: +/- 200 mV accuracy in 0–10 VDC applications
Supported integrations	BACnet/IP, BACnet MS/TP
Network and serial interfaces	One supported Ethernet port (top); 1000/100/10 Mbps; 8-pin RJ45 connector One FC port (RJ12 6-pin port; connects with 1.5 m [4.9 ft] RJ12 field bus cable) One SA port (RJ12 6-pin port; connects with 1.5 m [4.9 ft] RJ12 field bus cable) One optically isolated RS-485 port; with a removable 4-pin terminal block One optically isolated SA Bus port; with a removable 4-pin terminal block Two USB A ports. All support USB 2.0 and Open Host Controller Interface [Open HCI] specification.
Transmission speeds	Ethernet communication: 1000, 100, or 10 Mbps Optically isolated, serial communication (FC Bus): 76,800, 38,400, 19,200, 9600, or 1200 bps (selectable) Sensor/actuator communication (SA Bus): 38,400 bps
Ambient temperature conditions	Operating: 0°C to 50°C (32°F to 122°F) Non-operating: -40°C to 70°C (-40°F to 158°F)

Table 22: Technical specifications

Specification	Description
Ambient humidity conditions	Storage: 5% to 95% RH, 30°C (86°F) maximum dew point conditions Operating: 0% to 90% RH, 30°C (86°F) maximum dew point conditions
Housing	Polycarbonate and Acrylonitrile butadiene styrene (ABS) blend
Mounting	On flat surface with screws on three mounting clips or a single 35 mm DIN rail
Dimensions (width x height x depth)	250 mm x 145 mm x 45.5 mm (9.84 in. x 5.71 in. x 1.79 in.)
Weight	0.65 kg (1.433 lbs)
Compliance	**United States:** UL Listed, File E107041, CCN PAZX, UL 916, Energy Management Equipment; FCC Compliant to CFR47, Part 15, Subpart B, Class A
	Canada: UL Listed, File E107041, CCN PAZX7, CAN/CSA C22.2 No. 205, Signal Equipment; Industry Canada Compliant, ICES-003
	Europe: Johnson Controls declares that this product is in compliance with the essential requirements and other relevant provisions of the EMC Directive.
CE	**Australia and New Zealand:** RCM Mark, Australia/NZ Emissions Compliant
	BACnet International: BTL 135-2016 Listed B-BC/B-RTR/B-BBMD, Protocol Revision 15

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 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 network when a device sends an `IAmLive` message fails, the device sends another message to retrieve the time from the Site Director. When the time is synchronized between the devices, a second message to the Site Director is sent if the `IAmLive` message is successful.

For network-wide time synchronization, the device 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. 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 network. Regardless of how you set the date and time, you must set the time zone in the Site Director.

➤ **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 SMP 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.

Overview of time synchronization

This section contains a summary of how time synchronizes on a site with various system components. Table 23 summarizes the time sources for various system items. All time is Universal Time Coordinated (UTC) and all system devices handle DST.

Table 23: Time sources

Item	Time source
Trend Data	SNC
Events	SNC
Commands	SNC
Annotations	*Metasys* Server
Event Acknowledgements	*Metasys* Server

Metasys Server Site Director with network engines

About this task:
On a site with a *Metasys* Server Site Director and network engines, the following time synchronization steps occur:

1. A *Metasys* Server 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 the *Metasys* Server online/offline conditions. If the *Metasys* Server is offline, the network engines send an `IAmLive` message to the *Metasys* Server every 20 seconds.
4. When the *Metasys* Server 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 *Metasys* Server by 5 or more minutes (also taking into account the time zone of each network engine), the engine security credentials are invalid.
5. When the network engine receives an invalid credential, the network engine requests the current time from the *Metasys* Server and update the engine time to match, also taking into account the time zone of each network engine.

   Note: Time between a *Metasys* Server and network engines synchronizes only if the time differs between the *Metasys* Server and network engines by five or more minutes. In the worst case scenario, one network engine could be four minutes and 59 seconds ahead of the *Metasys* Server, and another network engine could be four minutes and 59 seconds behind the *Metasys* Server.
6. After time is synchronized and the *Metasys* Server is online, the network engines send `IAmLive` messages to the *Metasys* Server every five minutes (instead of every 20 seconds).

   Note: Time synchronization is affected if you change the network engine's Site Director from a *Metasys* Server in one time zone to a *Metasys* Server 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 *Metasys* Server Site Director in the new time zone. This interim step ensures proper time synchronization.

Time synchronization methods

Three methods for network time synchronization are available in the 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 five 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 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 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 five 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.

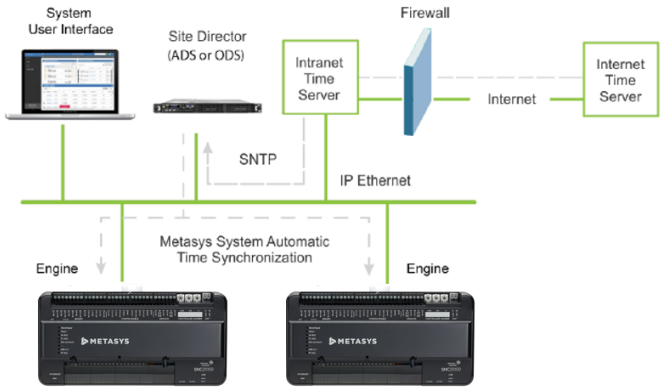
Example network

Figure 4 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 *Metasys* Server 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.

Figure 4: Time Management Sample System



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 device on the site. You must set the time zone in the Site Director even if you select a site time server.

Multiple time zones across a site are supported. This new capability is accomplished with a new attribute on the 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 device 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.
- **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.

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

For a list of Navy master clocks, go to http://tycho.usno.navy.mil.

See the Selecting a site time server for the Site Director network engine or Selecting a Site Time Server for the Site Director Metasys Server (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.

The local time and date shown on the device object's **Focus** tab is based on the default time zone set for the device. If the device is located in a different time zone than the Site Director, the current time and date shown for each differs.

In the Server 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

About this task:
For successful time management, complete the following steps:

1. Verify that each non-supervisory device on the network has the correct Site Director defined.
   See the Verifying the Site Director defined for a network engine 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 Metasys Server as a 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 *Metasys* Server on the site, you must set the time zone for these servers.
   If you have a *Metasys* Server as the Site Director, the time zone, date, and time are set in the Windows operating system of the computer where the *Metasys* Server resides. See the Metasys Server as a Site Director section. If you have non-Site Director *Metasys* Server 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 *Metasys* Server, both the P2000 and ADS/ADX/ODS/OAS servers should reference the same network time server. If the two systems use different time servers, the P2000 and *Metasys* Servers are not clock synchronized, which results in intermittent or no communication between the two systems.

Verifying the Site Director defined for a network engine

About this task:
For time synchronization to work properly, all network engines on a site must have the correct name for the Site Director in the Local Site Director attribute. If a network engine has the wrong device defined as Site Director, time synchronization may not work properly on your *Metasys* site.

1. Log on to the SNC.
2. Drag and drop the SNC 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.

   ⓘ **Notes:**

   - The Local Site Director may be entered as an IP address or host name.
   - If the Site Director field contains the wrong device or is empty, click **Edit**. Edit the Site Director entry and click **Save**.

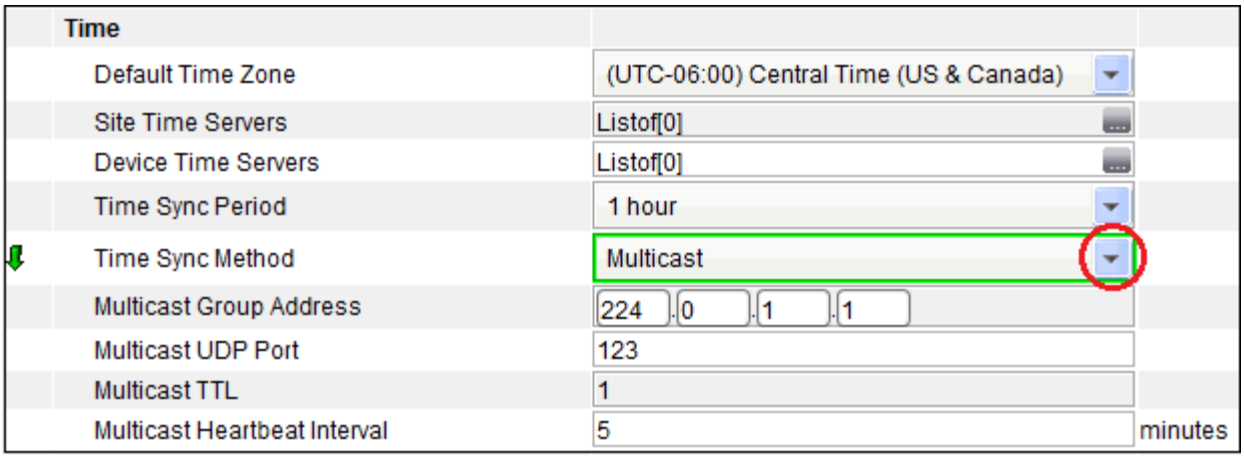
5. Go to Setting the time synchronization method.

Setting the time synchronization method

About this task:
See the Time synchronization methods section for descriptions of the methods.

1. Drag the Site object to the Display frame.
2. Click **Edit**.
3. Select **Advanced**.
4. In the **Time** section, in the **Time Sync Method** list, select the desired time synchronization method (Windows or Multicast).

Figure 5: Time sync method field



5. 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.

6. Click **Save**.

   Important: When the Time Sync Method is set to Multicast and the *Metasys* Server computer is synchronized with a time source other than itself, the Site Time Server must be an SNTP Time Server to allow the *Metasys* Server to perform time synchronization. Time synchronization occurs when a change is detected in the *Metasys* Server 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 the 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.

7. Go to Network engine as Site Director or Metasys Server as a Site Director.

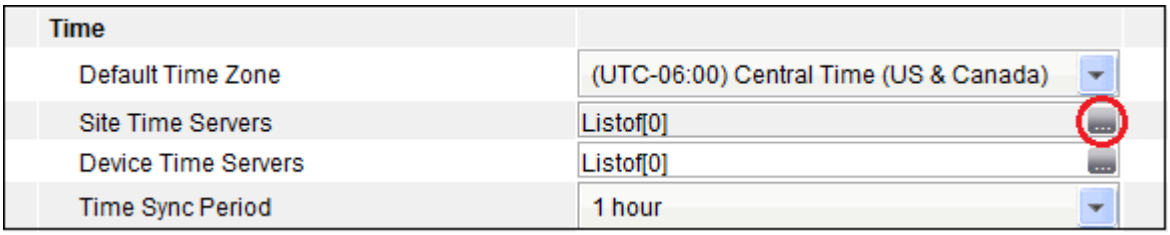
Selecting a site time server for the Site Director network engine

About this task:
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. Log on to the network engine.
2. Drag 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.

   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.

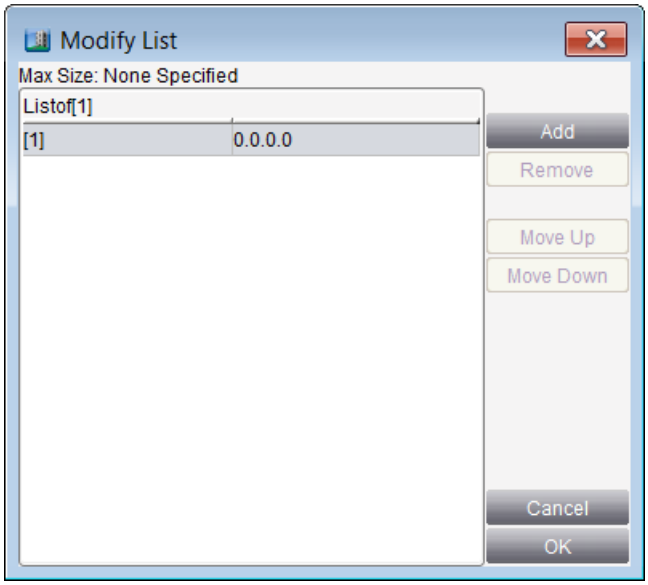
Figure 6: Site time servers in the Site Object



5. In the screen that appears, click **Add** (Figure 6).
6. Enter the IP address of the SNTP server from which the Site Director receives its time (Figure 7).

   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 uses only the first address in the list.

Figure 7: Add site time server



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 on the site.

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 a network engine and Setting the time synchronization method sections before following the steps in this section.

Setting the date and time in the Site Director network engine

About this task:
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.
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.
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.

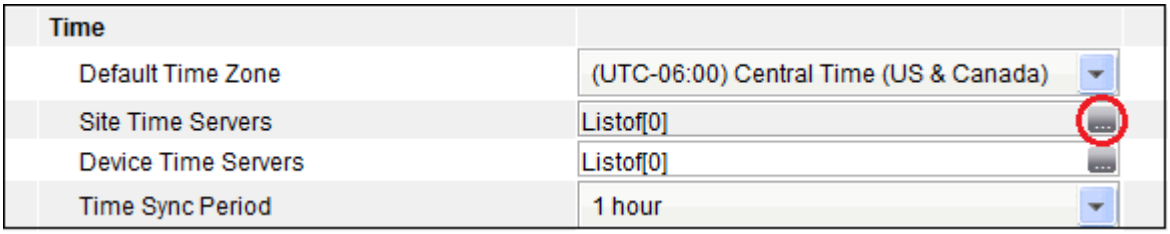
Selecting a site time server for the Site Director network engine

About this task:
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. Log on to the network engine.
2. Drag 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.

   ⓘ **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.

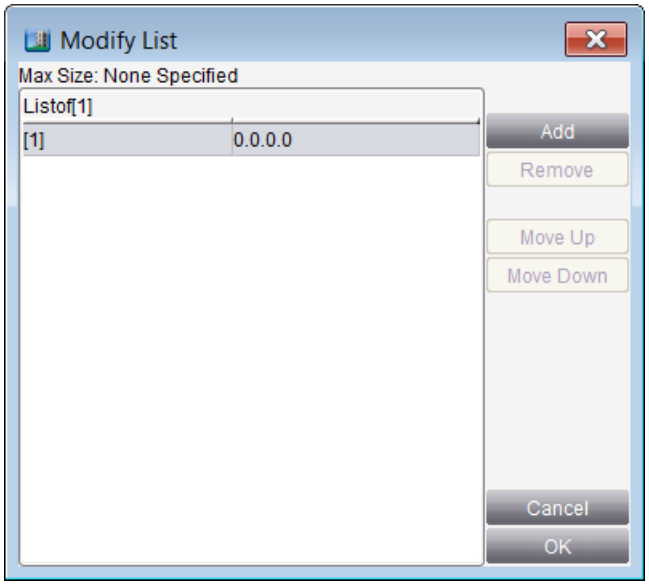
Figure 8: Site time servers in the Site Object



5. In the screen that appears, click **Add** (Figure 8).
6. Enter the IP address of the SNTP server from which the Site Director receives its time (Figure 9).

   ⓘ **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 uses only the first address in the list.

Figure 9: Add site time server

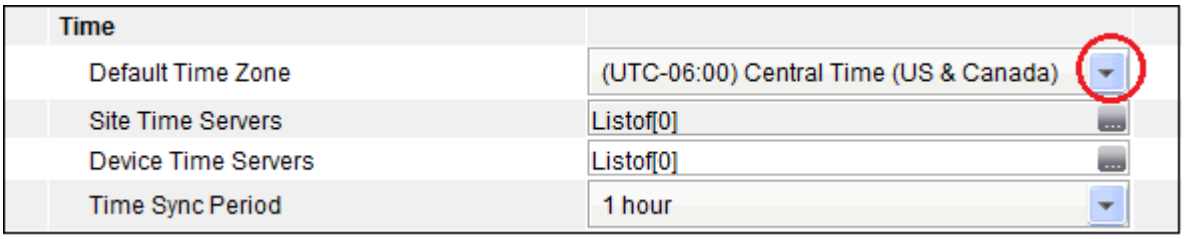


7. Click **OK**.
8. Click **Save**. The Site Director now requests the date and time from the selected time server and propagates it to all other engines on the site.

Setting the default time zone in the site director network engine

1. Log on 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** list, select the correct time zone for the device.

Figure 10: 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.

Metasys Server as a Site Director

Set the time zone first, then either set the date and time or select a time server for the Site Director *Metasys* Server.

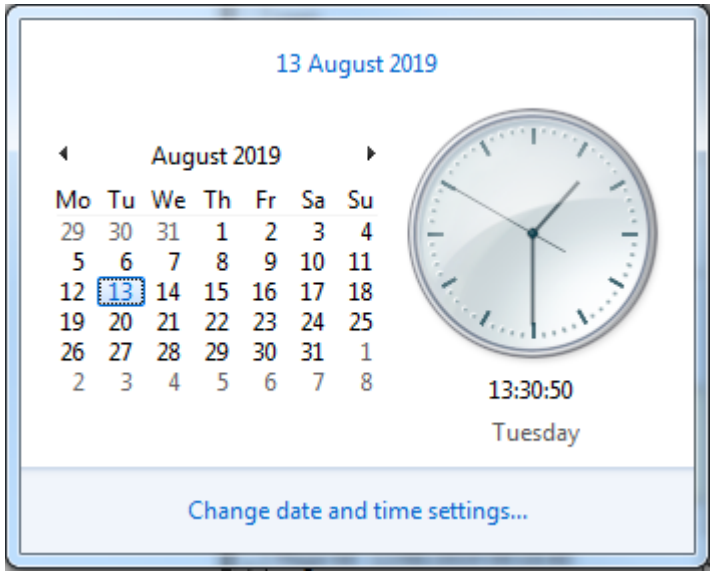
ⓘ **Notes:**

- See the Verifying the Site Director defined for a network engine 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 *Metasys* Server, and you also set the time manually in the *Metasys* Server, the manual time is overridden at the end of the time specified in the Time Sync Period attribute. The default is 1 hour.

Setting the time zone in the Site Director *Metasys* Server

1. In the lower-right corner of the *Metasys* Server computer screen, click the time. The Date and Time Properties box appears as shown in Figure 11. The appearance of this screen varies depending on the operating system.

Figure 11: Time and date on a Site Director



2. Click **Change date and time settings**, then click **Change time zone**.
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 *Metasys* Server 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 *Metasys* Server Site Director, go to the Setting the date and time in the Site Director Metasys Server section. If you are selecting a time server for the Site Director *Metasys* Server, click **OK** and go to the Selecting a Site Time Server for the Site Director Metasys Server (Windows method only) or Selecting a Site Time Server for the Site Director Metasys Server (Multicast method only)

Setting the date and time in the Site Director *Metasys* Server

About this task:
Before manually setting the date and time in the Site Director *Metasys* Server, follow the steps in the Setting the time zone in the Site Director Metasys Server 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**.

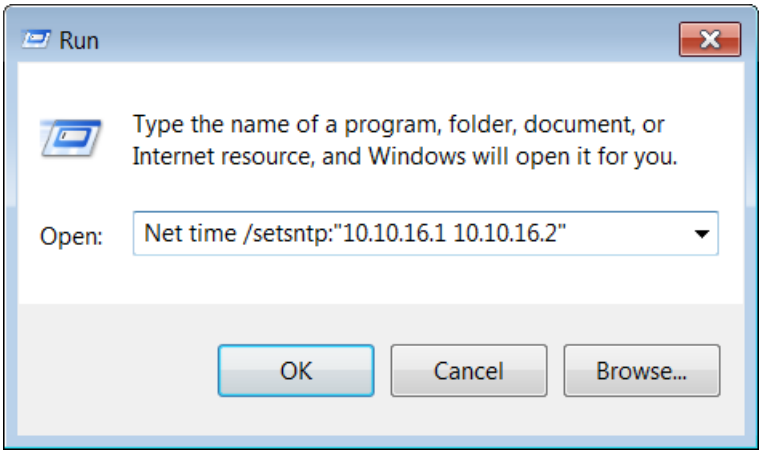
   The Site Director time zone, date, and time are now set and propagate to all other engines and servers on the site.

Selecting a Site Time Server for the Site Director *Metasys* Server (Windows method only)

About this task:
If you set up a site time server for your Site Director, you can set the date and time manually in the *Metasys* Server, but the manual settings are overridden at the end of the Time Sync Period.
Before selecting a site time server for the Site Director *Metasys* Server, follow the steps in the Setting the time zone in the Site Director Metasys Server section.

1. On the *Metasys* Server computer, press the **Windows key + R**. The **Run** dialog box appears.

Figure 12: Run dialog box



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 and servers on the site.

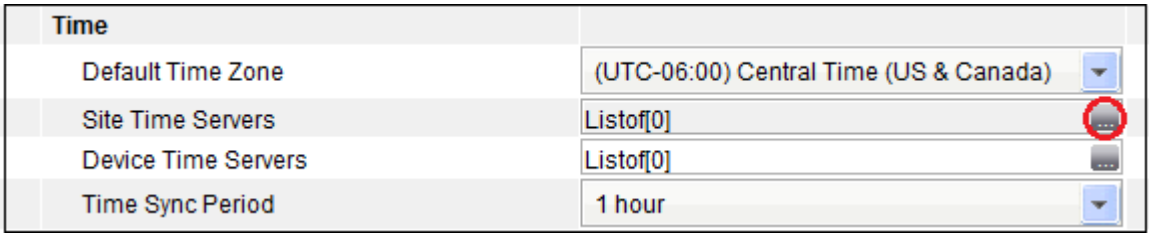
Selecting a Site Time Server for the Site Director *Metasys* Server (Multicast method only)

About this task:
Before selecting a site time server for the Site Director *Metasys* Server, follow the steps in the Setting the time zone in the Site Director Metasys Server section.

1. Log on to the *Metasys* Server.
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 shown in Figure 13.

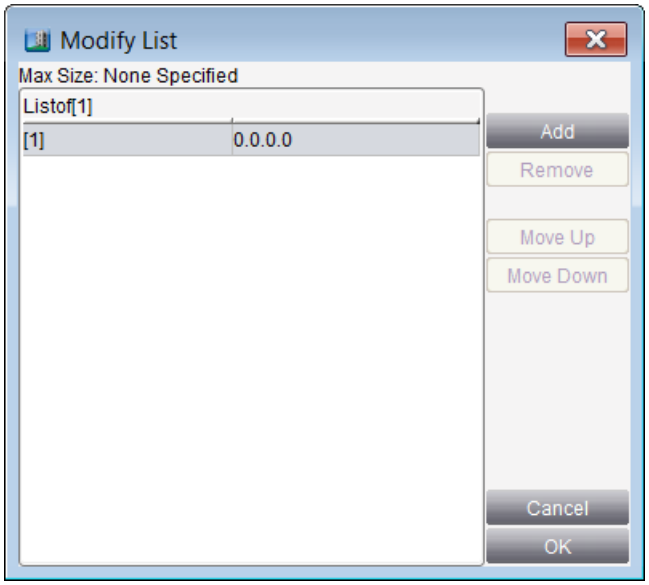
   ⓘ **Note:** Leave the **Device Time Servers** field blank. Do not change the value for the **Time Sync Period** attribute.

Figure 13: Site time servers in the Site Object



5. In the **Modify List** dialog box that appears, click **Add**.

Figure 14: 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 *Metasys* Server Site Director 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 and servers on the site.

Configuring additional multicast time synchronization settings

About this task:
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 on to the Site Director engine or 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 24 (Figure 15) and then click **Save**.

Figure 15: Multicast time synchronization fields

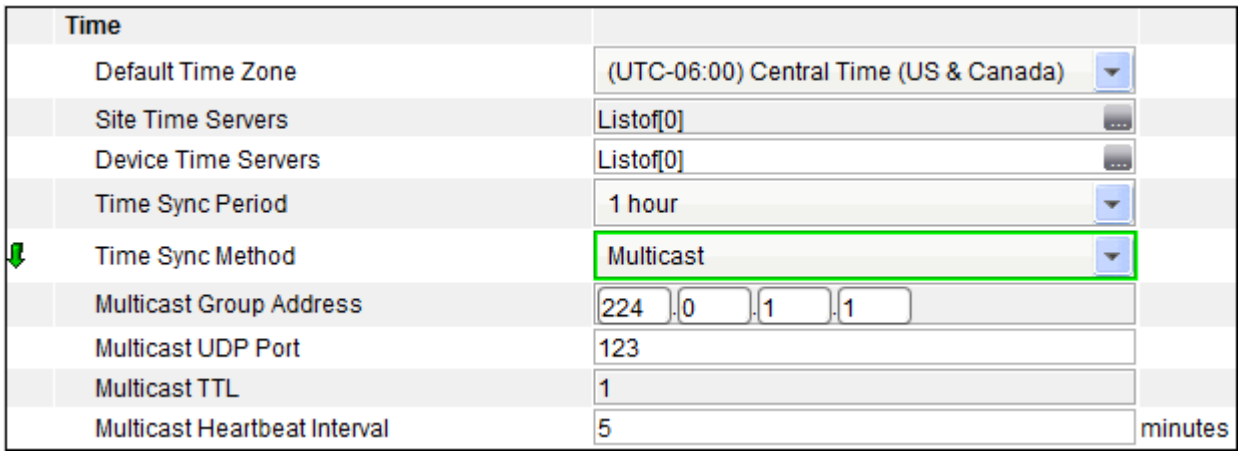


Table 24: Multicast time synchronization fields

Attribute	Description
Multicast Group Address	Specifies the IP address used to multicast the SNTP message. This address identifies the group of devices to receive the SNTP message. The RFC-2030 defined standard address is 224.0.1.1. The address is configurable to allow site-specific use.
Multicast UDP Port	Specifies the UDP port where the 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.
Multicast TTL	Specifies the Time-to-Live (TTL) for a Multicast message. The value indicates the number of router hops allowed (number of routers to pass through) before the message is not sent. Routers must be configured to pass Multicast messages to allow the time sync message to pass. ⓘ **Note:** A default value of 1 typically stops the Multicast message from leaving the IP subnet of the Site Director. Most routers decrease the existing TTL upon arrival of a packet, and drop the packet instead of rerouting it when the TTL reaches 0.
Multicast Heartbeat Interval	Specifies the number of minutes between forcing a Multicast time synchronization message from the Site Director to participating devices.