Network and IT Guidance Technical Bulletin

Building Technologies & Solutions

www.johnsoncontrols.com

2021-02-05

LIT-12011279

Release 11.0

Johnson Controls

Contents

Document introduction

This document is intended for Building Automation System (BAS) and IT professionals. In addition to this document, the *Metasys IP Networks for BACnet/IP Controllers Technical Bulletin (LIT-12012458)* provides valuable guidance on the various IP networks that are available for deploying the Metasys system into a facility. Also, for updated security and product support information from Johnson Controls®, reference the following sites:

- Cyber Solutions website
- Metasys Software Security and Support statement

➧ **Important:** Engage appropriate network security professionals to ensure that the computer hosting the Site Director is a secure host for Internet access. Network security is an important issue. Typically, the IT organization must approve configurations that expose networks to the Internet. Be sure to fully read and understand IT Compliance documentation for your site. Use care when performing steps on Metasys system components because restarts may be required that conflict with compliance requirements. For example, upgrading a Metasys Server requires the computer to be offline for a period of time. Similarly, installing new software on the Metasys Server, or installing of some Windows operating system updates, may require a computer restart.

In this document, **Metasys Server** refers in general terms to the following products (unless otherwise noted):

- Application and Data Server (ADS)
- Extended Application and Data Server (ADX)
- ADS-Lite
- Open Application Server (OAS)
- Open Data Server (ODS)

In this document, **network engine** refers in general terms to the following engine models (unless otherwise noted):

- Network Automation Engine (NAE): NAE35, NAE45, NAE55, and NAE85
- Network Integration Engine (NIE): NIE55 and NIE85

  ⓘ **Note:** NIE engines are no longer available since these integrations are now standard with NAE's and SNx's at Release 10.1

- Network Control Engine (NCE): NCE25
- Series of Network Engines (SNEs): SNE1050x, SNE1100x, SNE110Lx, and SNE2200x (where x is either 0 or 1)
- Series of Network Controllers (SNCs): SNC1612x and SNC2515x (where x is either 0 or 1)
- LonWorks® Control Server (LCS): LCS85

ⓘ **Note:** Some products in this document are available only to specific markets.

Summary of changes

The following information is new or revised:

- Removed RADIUS user account information because RADIUS servers are no longer supported at Metasys Release 11.0.

- Removed Windows 7 content because Windows 7 is no longer a supported operating system at Metasys Release 11.0. Also updated the versions of Windows 10 and Windows 8.1 that are supported.
- Removed information about BasicSysAgent (Basic Access) account as it is no longer supported from Release 11.0 and later. All users with Basic Access are converted to Standard Access users when you upgrade the archive with System Configuration Tool (SCT) Release 14.0.
- Updated Protocols and ports tables and Advanced security enabled sections.

Related documentation

Table 1: Related information

For information on	See document
General background on Metasys system features and components	*Metasys System Product Bulletin (LIT-1201526)*
Operations available to the Metasys system	*Metasys Site Management Portal Help (LIT-1201793)*
Operations available to the Metasys UI	*Metasys UI Help (LIT-12011953)*
Software products and tool available to Metasys system	*Metasys System Software Purchase Options Product Bulletin (LIT-12011703)*
Setting up system access for users and establishing user roles	*Security Administrator System Technical Bulletin (LIT-1201528)*
Backing up and restoring Security databases	*Metasys SCT Help (LIT-12011964)*
Commissioning a Metasys Server for secure communication	*ADS/ADX Commissioning Guide (LIT-1201645)*
	OAS Commissioning Guide (LIT-12013243)
	ODS Commissioning Guide (LIT-12011944)
Commissioning a network engine for secure communication	*NAE Commissioning Guide (LIT-1201519)*
	SNE Commissioning Guide (LIT-12013352)
	SNC Commissioning Guide (LIT-12013295)
	NIEx9 Commissioning Guide (LIT-12011922)
	LCS85 Installation and Upgrade Instructions (LIT-12011623)
Commissioning a secure NAE55 (NAE-S) with embedded encryption technology (available to Johnson Controls® employees only)	*NAE-S Commissioning Guide (LIT-12012269)*
Commissioning a Metasys for Validated Environments site	*Metasys for Validated Environments Extended Architecture Technical Bulletin (LIT-12011327)*
Interaction between an N1 network and the NIE at Metasys Release 9.0 or earlier	*N1 Migration with the NIE Technical Bulletin (LIT-1201535)*
Connecting a Mobile Access Portal (MAP) Gateway to your network	*Mobile Access Portal Gateway Network and IT Guidance Technical Bulletin (LIT-12012015)*
Interaction between a many-to-one wireless network and the Metasys network using the Wireless Room Temperature Sensing (WRS) system	*WRS Series Many-to-One Wireless Room Temperature Sensing System Technical Bulletin (LIT-12011095)*
Planning your Metasys network and implementing virtual networks (VLANs)	*Metasys IP Networks for BACnet/IP Controllers Technical Bulletin (LIT-12012458)*

Table 1: Related information

For information on	See document
BACnet network and a Metasys network interaction	*BACnet® Controller Integration with NAE/NCE/ODS Technical Bulletin (LIT-1201531)*
IP network planning and configuration as it applies to the Metasys system	*Metasys IP Networks for BACnet/IP Controllers Technical Bulletin (LIT-12012458)*
Monitoring SNMP for network	*Metasys Site Management Portal Help (LIT-1201793)*
	Metasys Open Data Server Help (LIT-12011942)

Network and IT considerations

Computer hardware configuration requirements

Computer minimum hardware configurations are based upon experience and testing for both client and server platforms and are published in the literature for each component of the Metasys system. Follow these requirements.

Computers running Metasys software must perform simultaneous tasks that require both hardware and network resources, and optional or advanced features require a large amount of memory for proper performance. Examples of the optional features of the Metasys system include advanced navigation and support for complex graphics, operation with the maximum number of concurrent users, complex and extended queries with the Metasys Export Utility, support for large network integrations, extensive use of trending, and large numbers of concurrent open applications.

It is important to note that operating systems and computing capabilities change rapidly. A computer that is adequate for today's applications may be inadequate in a year if additional system features and functions become required. Configuration requirements for computers running Metasys software may be upgraded on a regular basis to reflect these changes. Refer to the *Metasys System Configuration Guide (LIT-12011832)* for specific computer requirements for all Metasys software products and tools.

Metasys device IP address assignment (DHCP or manual)

See Table 2 for IP address assignment rules in the Metasys system. In this table, the term Site Director is introduced. The Site Director is the device designated to maintain the site information by holding the Site object, which contains information about the logical organization of data about your facility, user password administrative information, and overall master time and date. This function resides in an engine or in a Metasys Server on large installations. Although an engine can be a Site Director, if the site has a Metasys Server, then a Metasys Server must be the Site Director. The Site Director provides a uniform point of entry and supports functions such as user login, user administration, time synchronization, and traffic management.

Table 2: IP address assignments

Device	Dynamic addressing	Static addressing	Notes
SNE/SNC	Supported	Recommended when the SNE/SNC is the Site Director	• The SNE/SNC is a supervisory device for equipment controllers. • The SNE110Lx cannot be the Site Director. It must reside under an ADS-Lite Site Director.
NAE/NCE	Supported	Recommended when the NAE/NCE is the Site Director	• The NAE/NCE is a supervisory device for equipment controllers. • The NAE85 is installed on a server-class computer, but all other network engines are stand-alone devices on the IP network. • The NAE45-Lite cannot be the Site Director. It must reside under an ADS-Lite Site Director.
NIE	Not supported	Required	• A DHCP server can be configured to assign a particular IP address to a particular MAC address; therefore, DHCP can be used to assign a static IP address to a device. • The NIE55 is a supervisory device for equipment controllers. • The NIE85 is installed on a server-class computer, but the NIE55s and NIE59s are stand-alone network engines on the IP network.
NIEx9	Supported	Recommended when the NIEx9 is the Site Director	• A DHCP server can be configured to assign a particular IP address to a particular MAC address; therefore, DHCP can be used to assign a static IP address to a device. • The NIEx9 is a supervisory controller. • NIE89s are installed on server-class computers, but the NIE29s, NIE39s, NIE49s, and NIE59s are stand-alone devices on the IP network.

Table 2: IP address assignments

Device	Dynamic addressing	Static addressing	Notes
LCS	Supported	Recommended when the LCS85 is the Site Director	• The LCS is a supervisory device for equipment controllers. • The LCS85 is installed on a server-class computer. • DHCP is supported as long as the same address is assigned to the LCS85 after a restart or shutdown for an extended period of time. If a new address is assigned, you must reconfigure the LonWorks software driver and update settings for the LCS85 designated as the configuration server.

Table 2: IP address assignments

Device	Dynamic addressing	Static addressing	Notes
ADS/ADX OAS/ODS	Supported	Recommended when the ADS/ADX, OAS, or ODS is the Site Director	The ADS is loaded on a desktop-class computer and the ADX is installed on a server-class computer. The OAS or ODS is loaded on either a desktop-class or a server-class computer.
TEC20-3C-2	Supported for primary port only	Recommended for primary port; required for secondary port	• Enable DHCP only if your network has one or more DHCP servers. Otherwise, the TEC20-3C-2 Coordinator may become unreachable over the network. • Only the primary Ethernet connection Primary Rate Interface (PRI), such as NET and LAN1, can be enabled to use DHCP. The secondary Ethernet connection (SEC), such as NET2 and LAN2) can only use static IP addressing. • The TEC20-3C-2 Coordinator is factory-configured with an IP address of 192.168.1.12n and a submask of 255.255.255.0, where n equals the last number in the TEC20-3C-2 Coordinator serial number. When commissioning the device with the TEC Wireless Configuration Tool, do not assign your computer with the same IP address as the TEC20-3C-2 Coordinator's factory-assigned IP address.

Table 2: IP address assignments

Device	Dynamic addressing	Static addressing	Notes
WRS-RTN	Supported	Recommended if communication issues arise	• The WRS-RTN system is not supported at Metasys Release 9.0.7 or later. • If your devices use Network Address Translation (NAT) to communicate across the Internet, the NATs must provide static internal and external IP addresses. If you are using DHCP to assign addresses to devices that communicate across networks that use NATs, your DHCP server should be configured to always allocate the exact same IP address as the Metasys system devices' MAC addresses. This configuration makes these devices behave as if they have static IP addresses, although they have DHCP addresses. This behavior sometimes is called Dynamically Assigned, Statically Allocated addressing from a DHCP server. • The data transmission over Ethernet between a WRS-RTN and an engine consumes very little bandwidth (less than 1.5% of the usable bandwidth on a 10 Mbps Ethernet network, based on maximum device loading). Refer to the *WRS Series Many-to-One Wireless Room Temperature Sensing System Technical Bulletin (LIT-12011095)* for details.

Metasys device hostname resolution (DNS or hosts file)

If DHCP servers are available on the network and DHCP is enabled on the Metasys system devices, a DHCP server can automatically assign the addresses of the DNS servers to some devices. Alternatively, the DNS server addresses may be manually assigned. See Table 2 for specifics for each device.

If the network does not support DNS, then the host's file or registry entries of the Site Director must be updated with the host name/IP address pairs for all engines/servers on the Metasys site, and each child device (non-Site Director engine/server) must be updated with the host name/IP address pair of the Site Director (and any other Ethernet-based device with which it communicates).

Either DNS or local host file updates are necessary for successful communication between a Site Director and all devices on the Metasys site.

We recommend using DNS scavenging to ensure that old host records are cleaned up properly. The recommended scavenging interval is the same interval as the DHCP lease time.

For information on configuring DHCP and DNS on an engine, refer to the commissioning guide for your network engine:

- *SNE Commissioning Guide (LIT-12013295)*
- *SNC Commissioning Guide (LIT-12013352)*
- *NAE Commissioning Guide (LIT-1201519)*
- *NAE-S Commissioning Guide (LIT-12012269,* company-internal document)
- *NIEx9 Commissioning Guide (LIT-12011922)*
- *LCS85 Commissioning Guide (LIT-12011568)*

For information on configuring DHCP and DNS for a Metasys server, refer to Microsoft® Windows operating system literature. Also refer to the *TEC Series Wireless Thermostat Controller System Technical Bulletin (LIT-12011414)* and *WRS Series Many-to-One Wireless Room Temperature Sensing System Technical Bulletin (LIT-12011095)* for DHCP and DNS information on those respective devices.

DNS implementation considerations

The DNS infrastructure must be configured to do the following:

- The Metasys server and/or Metasys engine and Metasys DHCP supported devices (TEC20-3C-2 Coordinators, WRS-RTN Many-to-One Receivers) must be defined in the same DNS domain.
- The Metasys server and/or Metasys engine and Metasys DHCP supported devices (TEC20-3C-2 Coordinators, WRS-RTN Many-to-One Receivers) require that DNS servers be defined to resolve hosts in the domain they are in.
- If the DNS server and the Metasys server and/or Metasys engine are in different networks (VLANs), routing must be available between networks.

DHCP implementation considerations

For Metasys devices to function properly in a DHCP implementation, the DHCP servers must support dynamic DNS. The DHCP infrastructure must be configured to do the following:

- The DHCP server must create an A record in the defined DNS domain upon handing a lease to a Metasys device. Optionally, you can configure the DHCP server to update the PTR (pointer) record of the Metasys DHCP-supported device in the reverse zone DNS domain.
- The domain for DNS updates must be included in the DHCP server configuration. The Metasys DHCP-supported device does not specify the domain.

- The Metasys Server and/or network engine and the Metasys DHCP-supported devices (TEC20-3C-2 Coordinators and WRS-RTN Many-to-One Receivers) all must be in the same DNS domain.
- We recommend that the Metasys Server and/or network engine and the Metasys DHCP supported devices (TEC20-3C-2 Coordinators and WRS-RTN Many-to-One Receivers) be in a separate VLAN from all other devices at the Metasys site.
- If the DNS server, Metasys Server, network engine, and/or Metasys DHCP supported devices (TEC20-3C-2 Coordinators and WRS-RTN Many-to-One Receivers) are in different networks (VLANs), ensure that routing is available between networks and that a proper router is passed in the DHCP lease.
- If the DHCP server is not in the same VLAN as the Metasys devices, enable DHCP forwarding to the proper DHCP server on the VLANs on which the Metasys devices are located.

Microsoft Active Directory service overview

This section provides an overview of Active Directory services as implemented in the Metasys system. For more details, refer to the *Security Administrator System Technical Bulletin (LIT-1201528)*.

The Active Directory service feature used by the Metasys system provides an IT standard integration of the Metasys system into a customer’s existing Active Directory service infrastructure for authentication purposes. This optional component provides the convenience of Single Sign-On (SSO) access, a capability that permits users to log in to multiple, secured application User Interfaces without reentering their user name and password.

The Metasys system works in conjunction with the Active Directory Service. It allows the Active Directory Service to provide authentication for access to various Metasys software applications, including the Metasys server, Metasys UI, Metasys UI Offline, and System Configuration Tool (SCT) (but not the engines). Using the Security Administrator System menu option, you can add Active Directory users and assign them various levels of access and permissions, from read-only to administrator privileges. By using the Security Administrator System option, you can also grant SSO or Single Sign-On access to all Active Directory users for a more convenient authentication process. The Metasys UI and Metasys UI Offline does not support SSO.

The Metasys architecture uses Active Directory service for authentication. The user provides Active Directory service credentials in one of two forms:

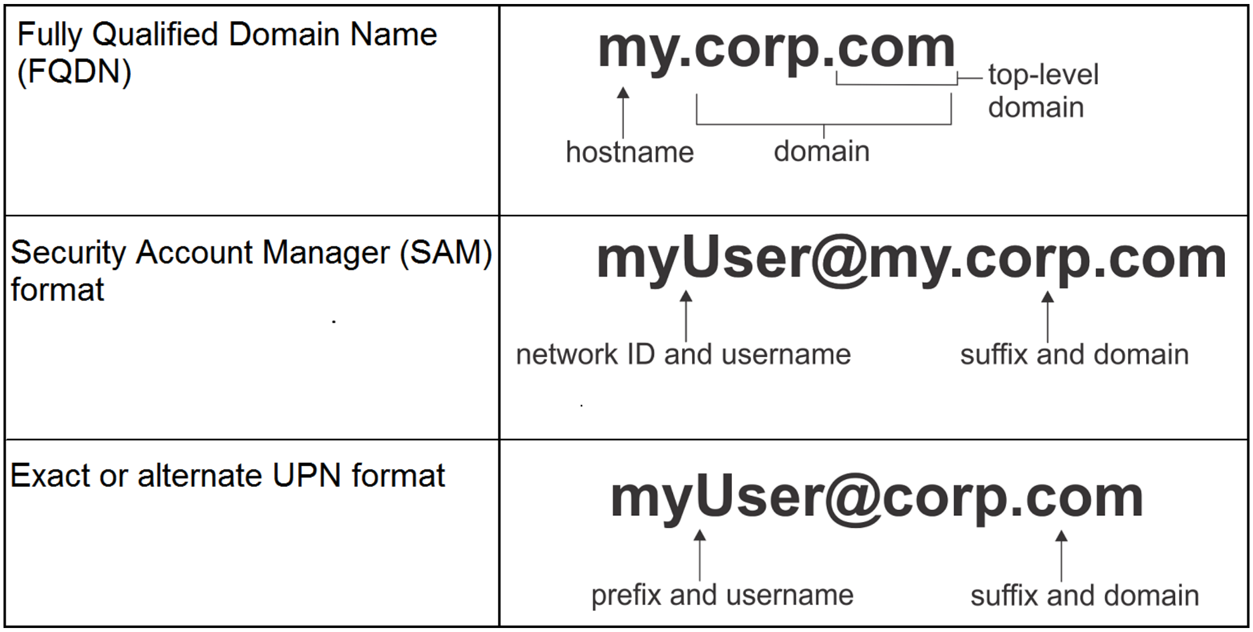
- Active Directory service credentials that are cached by Windows when the user logs in to the computer, and then automatically retrieved by the Metasys system during the Windows Integrated Authentication with IIS process on the Metasys server, or SCT.
- Active Directory service credentials (user name, password, and domain) that are specified directly on the Site Management Portal UI login screen.

An Active Directory service user name includes the specification of a domain name with the user name. For example, instead of a user name called John, the user name in Active Directory service and the Metasys system could be John@my.corp.com, which includes the domain specifier required by Active Directory service.

For releases prior to Metasys Release 8.1 and System Configuration Tool Release 11.1, Active Directory implementation with the Metasys system allows a hybrid User Principal Name (UPN) format for usernames and the Security Account Manager (SAM) format, which uses the username, password, and domain selection. The hybrid UPN format uses the username in which the full domain name is provided. The Metasys system does not support an exact or alternate match of the UPN name and instead validates the prefix portion and the suffix portion of the Active Directory username. The prefix is the username (myUser) and the suffix is the domain name (my.corp.com).

The prefix and suffix are separated by the @ symbol. For example, myUser@my.corp.com is specified instead of myUser@corp.com, where myUser@corp.com is the email UPN name.

Figure 1: Examples of Login Formats



Metasys Release 8.1 or later, and SCT Release 11.1 or later allow exact or alternate UPN authentication support for the Metasys system in compliance with Microsoft Office 365® authentication. For example, myUser@corp.com is specified, where myUser@corp.com is the exact or alternate UPN name. To enable exact or alternate UPN format user login to the Metasys system, see Enabling exact or alternate UPN authentication for a Metasys Server and Enabling exact or alternate UPN authentication for SCT.

SSO allows users to access the Metasys system without having to type in their credentials by using Windows Active Directory authentication in conjunction with the Metasys software. This feature relies on the following:

- The user has an active Windows Active Directory account.
- The user is logged into a domain computer using their Active Directory credentials.
- The user is added to the Active Directory users list in the Security Administrator System menu option.
- The SSO feature is enabled in the Security Administrator System menu option.
- The Metasys application supports SSO.

ⓘ **Note:** The Metasys system does not require any particular Active Directory service structure.

Support for Active Directory service (including single sign-on capability)

Table 3 is a summary of which Metasys system application User Interfaces support Active Directory logins and the SSO capability. If the application supports Active Directory logins, then the Metasys system can be configured to use your existing IT Active Directory Service infrastructure for authentication purposes. If the application supports SSO, then you can log in to multiple, secured applications without reentering the same user name and password.

Table 3: Products that support Active Directory logins and SSO

Application	Active Directory logins supported	Exact or alternate UPN format logins supported	SSO supported
ADS/ADX Site Management Portal UI	Yes	Yes	Yes
SCT	Yes	Yes	Yes
Metasys UI and Metasys UI Offline	Yes	Yes	No
OAS	Yes	Yes	Yes
ODS	Yes	Yes	Yes
Metasys Advanced Reporting System	No	No	No[1]
Network Engine[2]	No	No	No
Metasys for Validated Environments	Yes	Yes	No

[1] If you are using Metasys Advanced Reporting System UI on an ADX/ODS, you still can use the SSO capability to log in to the ADX Site Management Portal UI. For example, if you have an ADX/ODS with the Metasys Advanced Reporting System, you can use SSO to log in to the ADX Site Management Portal UI, but you must enter your Metasys system user name and password pair to log in to the reporting system.

[2] The engine Site Management Portal UI does not support authentication with Active Directory service. If you have an ADS/ADX/OAS/ODS Site Director, however, you can log in to the ADS/ADX/OAS/ODS Site Management Portal UI using SSO and access system information for the entire site, including details on the engine.

For more details on Active Directory and SSO interaction with Metasys system security, refer to the *Security Administrator System Technical Bulletin (LIT-1201528)*.

Implementation considerations

The Active Directory service feature as implemented on the Metasys system uses the existing Active Directory service infrastructure at the customer site. The following are important considerations:

- Active Directory service users in server-class operating system domains and read-only domains are supported.
- Use of a server-class operating system read-only domain controller is determined by the IT department that is responsible for setting up accounts for authentication against the domain controller. SSO and Active Directory service logins function with the server-class operating system read-only domain controller, whether the primary read-only domain controller is online, offline, or not accessible (as long as the Active Directory service user credentials are cached in the read-only controller). If a trust relationship exists between the read-only domain controller and another domain, the Active Directory service login functions properly as long as the trusted domain is accessible. In this case, Kerberos manages the forwarding to the correct domain. SSO does not work for an Active Directory service user in a trusted domain of a read-only domain controller because SSO uses NTLM and the message is not forwarded.
- The default Active Directory services schema is supported. For details, see Information obtained from Active Directory services.
- NTLMv2 is required to accomplish strict SSO login-free access to the Metasys system using IIS Windows Integrated Authentication. All other authentication is performed using Kerberos, which includes the Active Directory service user name, password, and domain selection at the Metasys system login screen and authentication to Active Directory services for LDAP queries.

- The Metasys system does not store or manage the passwords of Active Directory service users. Active Directory service users who are given access to the Metasys system (identified by the security identifier [SID]) are not created or managed by the Metasys system. The system maintains authorization permissions to the Metasys system only.
- Active Directory service credentials that are provided at the Metasys system login screen are strongly encrypted before they are sent over the network from the Site Management Portal UI to the Metasys server and SCT.
- To ensure that Metasys system SSO works properly, the **Network Security: LAN Manager authentication level** security policy must be configured to compatible settings on the Metasys server and SCT computer, any Site Management Portal UI client machines, and the Active Directory service domain controller.
- The Active Directory service structure may comprise one or more forests consisting of one or more domains. The Metasys system requires an Active Directory service structure that allows for the use of full domain UPN formatted names or exact or alternate UPN formatted names. Single Label Domains are one example of a directory structure that is not compatible with the Metasys system. Single Label Domains are domains that do not include .com, .edu, and so on. Users from any domain may be given access privileges to the Metasys system, as long as appropriate trust relationships and privileges exist within Active Directory services.
- The Metasys server and SCT computer should be placed in an Active Directory service organizational unit (OU) that is not affected by Group Policies (such as those typically applied to a desktop) that download software to the machine. This software may adversely affect Metasys system device operation.
- A service account in Active Directory service consisting of an Active Directory user name, password, and domain is required. For details, see Service account.

Trust relationships

- Trust relationships and privileges are dictated by the customer's IT department and are a fundamental part of a security policy. Active Directory service implementation on the Metasys system does not dictate the trusts that are established. While Active Directory services provide multiple domain support, the customer infrastructure determines whether this function is used.

Metasys Server and SCT considerations

The Metasys Server or SCT computer that is handling user authentication and authorization must follow these requirements to use the Active Directory services feature as implemented on the Metasys system:

- The Metasys Server and SCT computer must be joined to an Active Directory service domain. This is necessary for SSO login-free access to the Metasys system using Windows Integrated Authentication. If the Metasys Server and SCT are not joined to an Active Directory service domain, the Active Directory service user cannot use the login-free access to the Metasys Site Management Portal UI, but the Active Directory service user may still specify the Active Directory service user name, password, and domain at the login screen.
- The Metasys Server and SCT computer must be configured to use Windows Integrated Authentication through IIS. Windows Integrated Authentication is configured by the Metasys installation program and is necessary for SSO login-free access to the Metasys system.
- The Metasys Server and SCT computer must be configured to allow network access to the device and read/write access to the Metasys Single Sign-On web service to users of the Active Directory service.

- The hard disk on the Metasys Server or SCT computer must be formatted for the NTFS file system, not the FAT file system.
- The Metasys Server and SCT computer must not be running other third-party applications that compete with the Metasys system for computer resources.

Child device considerations

Child devices, which include network engines, do not use the Active Directory service; however, if the user logs in to a Site Director with Active Directory service credentials, they may navigate to child devices. The child devices:

- can be any combination of platforms illustrated in
- do not need to be at the same release as the Site Director
- do not need to join an Active Directory service domain

Information obtained from Active Directory services

The Active Directory service used by the Metasys system reads a set of information from the Active Directory service database, and populates and updates the user’s Properties based on those values. The following information is read, with the actual Active Directory service attribute names in parentheses:

- User name (samAccountName, userPrincipalName, CanonicalName)
- Description (Description)
- Full Name (displayName)
- Email (mail)
- Phone Number (telephoneNumber)
- Account Disabled (UserAccountControl)

In addition, the Security Identifier (ObjectSID) is obtained from the Active Directory service database and used internally to uniquely identify the Metasys user.

Enabling exact or alternate UPN authentication for a Metasys Server

About this task:
Follow the steps below to enable exact or alternate UPN authentication for a Metasys Server, including an ADS, ADX, ADS-Lite, OAS, or ODS. This procedure also enables exact or alternate UPN authentication for all Metasys software installed on the Metasys Server.

1. On the Metasys Server, open Notepad by right-clicking and selecting **Run as Administrator**. Click **Yes** if the User Account Control prompt appears.
2. In Notepad, click ***File*** > ***Open*** and browse to:

   ```
   C:\Program Files (x86)\Johnson Controls\MetasysIII\ws\
   ```

   ⓘ **Note:** By default, the Metasys software and databases are installed to the C: drive. If you have customized the installation location, specify the location. For example, if you installed on drive E, use E:\.
3. Right-click on the web.config file. Click **Open**.
4. Modify the following key under the **<configuration><appSettings>** section from false to **true**:

   ```
   <add key="enableOffice365StyleActiveDirectoryAuthentication" value="true"/>
   ```

5. Save and close the web.config file.
6. Restart the Metasys Server.

   To enable alternate or exact UPN authentication for SCT Release 11.1, see Enabling exact or alternate UPN authentication for SCT.
   For more information on creating users in the Metasys system, refer to *Security Adminstrator System Technical Bulletin (LIT-1201528)*.

Enabling exact or alternate UPN authentication for SCT

About this task:
Follow the steps below to enable exact or alternate UPN authentication for SCT. This procedure also enables exact or alternate UPN authentication for all Metasys software installed on the SCT computer.

1. On the SCT computer, open Notepad by right-clicking and selecting **Run as Administrator**. Click **Yes** if the User Account Control prompt appears.
2. In Notepad, click **File** > **Open** and browse to:

   ```
   C:\Program Files (x86)\Johnson Controls\MetasysIII\Tool
   ```

   ⓘ **Note:** By default, the Metasys software and databases are installed to the C: drive. If you have customized the installation location, specify the location. For example, if you installed on drive E, use E:\.
3. Right-click on the web.config file. Click **Open**.
4. Modify the following key under the **<configuration><appSettings>** section from false to **true**:

   ```
   <add key="enableOffice365StyleActiveDirectoryAuthentication" value="true"/
   >
   ```
5. Save and close the web.config file.
6. Restart the SCT computer.

   For more information on creating users in the Metasys system, refer to *Security Administrator System Technical Bulletin (LIT-1201528)*.

Service account

The Active Directory services, as implemented on the Metasys system, require a service account in Active Directory service consisting of a user name, password, and domain. The feature uses this service account when executing LDAP queries of Active Directory service. The Active Directory service feature allows the use of one Service Account to access all domains, or one Service Account per domain.

The service account in Active Directory service must have directory read privileges. These privileges may be open to the entire directory or limited to only those organizational units and domains that contain Metasys privileged Active Directory service users and groups. For some Active Directory service configurations, the IT department may dictate that one service account is created per domain.

The service account user name, password, and domain are defined by the customer IT department. This user should be created with a non-expiring password. If the IT department requires the modification of the Service Account password on a periodic basis, a Metasys system work process must be defined to update the password in the Security Administrator System at the time it is changed in Active Directory service. If the Service Account password in the Metasys system does not match the Service Account password in Active Directory service, Metasys system access by Active Directory service users is denied.

Service account rules

When specifying a service account with the Metasys Security Administrator System, keep these important rules in mind:

- For releases prior to Metasys Release 8.1 and SCT Release 11.1, each service account must use the full domain UPN format for the username. Provide the fully qualified domain name where the domain specifier is at the domain level. For example, use **metasys.service@my.corp.com** instead of **metasys.service@corp.com**, even though the latter is a valid form of the username.

  For Metasys Release 8.1 or later, and SCT Release 11.1 or later, each service account must use the full domain UPN format or the exact or alternate UPN for the username. Provide the full domain name where the domain specifier is at the domain level for the full domain UPN format. Provide the prefix/username and suffix/domain for the exact or alternate UPN format. For example, use **metasys.service@my.corp.com** for the full domain UPN format and **metasys.service@corp.com** for the exact or alternate UPN format.
- A blank password for a service account is prohibited.
- The ability to specify more than one service account is available. You only need to specify more than one service account if an Active Directory service trust does not exist between the domain in which the service account is created and all other domains where Metasys users reside. In this case, specify one service account per domain where the Metasys users reside.
- The Service Account should be configured with a non-expiring password; however, if the password is set to expire, you need to reset it in the Metasys Security Administrator System each time you reset it on the Active Directory service domain.

Service account permissions

The Metasys system requires that the service account in Active Directory service allow a minimal set of permissions. This section lists these permissions, but does not dictate how they should be applied; the customer's IT department determines this at the time of creation. The required permissions include the following:

- Read access to the domain object of each domain that contains Active Directory service users who are Metasys system users.
- Read access to each organizational unit that contains Active Directory service users who are also Metasys system users.
- Read access to the attributes of each User Object in Active Directory service that relates to Metasys system users or read access to only the following individual attributes on those user objects (if full read access is not allowed):

  - ObjectSID
  - samAccountName
  - displayName
  - Description
  - mail
  - userPrincipalName
  - telephoneNumber
  - UserAccountControl
  - CanonicalName

In addition, a non-expiring Service Account password is required. See Service account rules. Also, the Service Account must be able to access all domains with Metasys system users to perform LDAP queries. For example, accounts cannot be denied access to the domain controller in the domain security policy.

User account rules

The following rules apply to Active Directory service users who are added with the Metasys Security Administrator System:

- For releases prior to Metasys Release 8.1 and SCT Release 11.1, the full domain UPN format is used for the username, in which the fully qualified domain name is provided. For example, **myUser@my.corp.com** is specified instead of **myUser@corp.com**, even though the latter is a valid form of the user name. The fully qualified username appears on the main Metasys Site Management Portal UI screen to identify the currently logged in user. It also appears as the username on Metasys reports and logs.

  For Metasys Release 8.1 or later, and SCT Release 11.1 or later, the full domain UPN format or the exact or alternate UPN format is used for the username. For example, **myUser@my.corp.com** or **myUser@corp.com** is specified. The fully qualified username or exact or alternate username appears on the main Metasys Site Management Portal UI screen to identify the currently logged in user. It also appears as the username on Metasys reports and logs.
- Each specified user must exist and be enabled in Active Directory service. Properties of the user (for example, phone number and email address) are read when the user is added to the Metasys system. These items are displayed by the Metasys Site Management Portal UI under User Properties. For details, see Information obtained from Active Directory services.
- If the username for an Active Directory service user changes, you do not need to specify the new name with the Security Administrator System tool. The update of the new username occurs within the Security Administrator System when you left-click the Active Directory service user account.
- If an Active Directory service user is deleted from the Active Directory service database, delete that user from the Metasys system as well. If, for any reason, an Active Directory service user with the same username is later added to the Active Directory service database but you did not delete this user from the Metasys system, the new user cannot be added to the Metasys system until the original user is deleted.
- If an Active Directory service user is disabled in the Active Directory service database, the Metasys Access Suspended property check box under the user's Properties window is selected. Once the service user for Active Directory is re-enabled, a Metasys Administrator must manually click to clear the Metasys Access Suspended property check box before the user can log in again.
- The Metasys system follows the text case format dictated by Active Directory services. In other words, if you add a user called **MYUSER@my.corp.com**, and the Active Directory service format uses all lowercase characters, the username adjusts to **myuser@my.corp.com** when added.
- At least one defined Service Account must have the privilege to read the user's Active Directory service attributes.

User creation and permissions

In many organizations, different people need to be involved in the process of defining and maintaining Active Directory service users for the Metasys system.

IT and Active Directory service Administrators create, delete, and update accounts in Active Directory service, including the provision of a Service Account for use by the Metasys system. They manage Active Directory service user account passwords, password policies, and account policies.

Metasys Administrators add existing Active Directory service users to the Metasys system, and assign Metasys system privileges using the Security Administrator System.

Once you add an Active Directory service user to Metasys, the user is assigned privileges in the same manner as a local Metasys user. In fact, a user's local Metasys account can be disabled or deleted once their Active Directory service user account is established, unless there is an important reason for a user to have two accounts. An audit record is created whenever an Active Directory service user is added to or removed from the Metasys system.

User management in Metasys UI

The User Management feature in Metasys UI Online facilitates the creation and management of users and their roles, category-based permissions, and privileges directly in Metasys UI Online, without the need to install software on client machines. Administrators can create and manage user details for Active Directory and Metasys local users. This feature is also available in the Metasys Site Management Portal (SMP).

Only administrators can access the User Management feature. All users can view and edit certain information that relates to their specific user details in My Profile. The My Profile feature shows the user details, system privileges, and category access. The details shown in My Profile are based on your Metasys user account settings. When you edit your profile information in My Profile, your profile details automatically update in User Management.

Administrators can complete the following tasks with the User Management feature:

- Add, edit, and delete Metasys administrators.
- Add, edit, and delete Active Directory Metasys users.
- Create, edit, delete, and assign roles to Metasys users.
- Assign authorization category permissions and system privileges to users and roles.
- Navigate to Space Authorization to authorize spaces for users.
- Apply system configurations and account policies to any user.
- Filter users based on role, type, last login, and status.
- Filter roles based on system privileges, access categories, and permissions.

For Active Directory Metasys users, the control over password management and account settings remains with the respective parent portal. Also, a user will have access to the Building Network tree in the Metasys UI only if the user has the User Can View the Item Navigation Tree (Default Tree) property selected in the User Details tab in the User Management feature in Metasys UI, or in their User Properties in SMP. For more information, refer to the *Security Administrator System Technical Bulletin (LIT-1201528)*.

Syslog overview

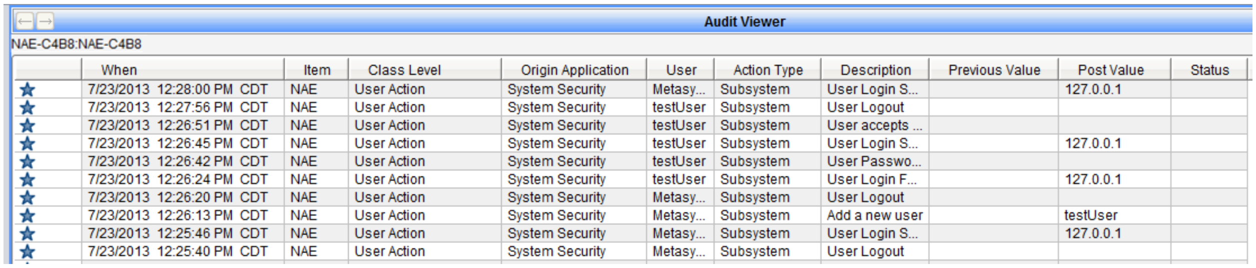
The Metasys Servers and network engines provide the optional capability of sending their configured audit log entries and event notifications to an external, customer-provided industry-standard Syslog server destination, conforming to published Internet document RFC 3164. Syslog implements a client-server application structure where the server communicates to a port for protocol requests from clients. Most commonly, the Transport Layer protocol for network logging is User Datagram Protocol (UDP). The Metasys system Syslog message provides positive indication of each field possible in the Metasys event and audit entries, replacing any blank field with the single character dash (-). Individual fields of each Metasys entry are sent to the Syslog server in the Syslog message field separated by the vertical bar symbol (|).

The Metasys system creates and maintains independent local repositories for events and audits. Existing documentation in the *Metasys System Configuration Guide (LIT-12011832)* describes their configuration. Events and audit entries are sent to the Syslog server when the entries are recorded in the servers and network engines.

When configuring the servers and network engines, confirm that the Enabled Audit Level is at the recommended setting of **2**.

When Metasys Audit messages are delivered to Syslog destinations from the Metasys SMP UI, the fields are sent in the order shown in the Metasys Audit Viewer (Figure 2). The Audit Viewer columns are labeled as follows: When | Item | Class Level | Origin Application | User | Action Type | Description | Previous Value | Post Value | Status. The Metasys audit log shows the client's IPv4 address in the Post Value column for every successful and unsuccessful login attempt.

Figure 2: Metasys Audit Viewer - SMP UI



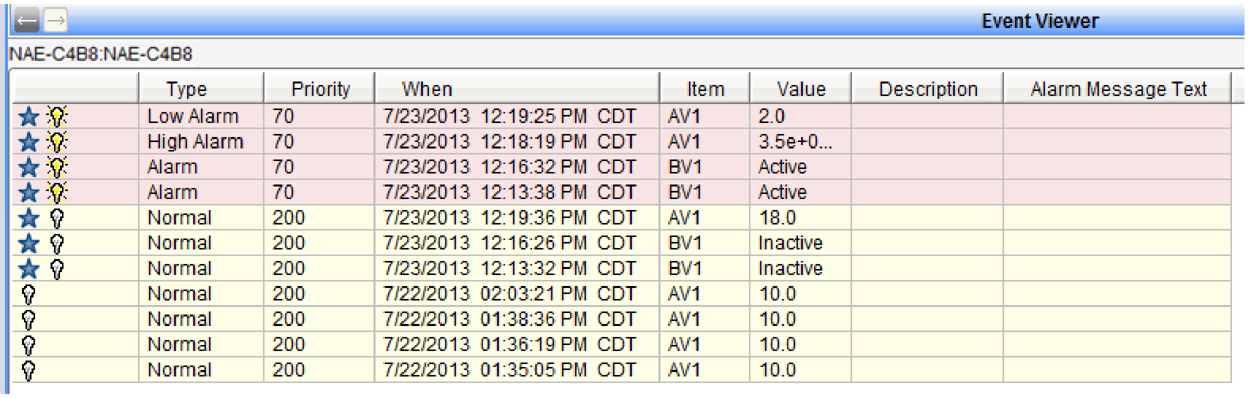
Audit Viewer

NAE-C4B8:NAE-C4B8

	When	Item	Class Level	Origin Application	User	Action Type	Description	Previous Value	Post Value	Status
★	7/23/2013 12:28:00 PM CDT	NAE	User Action	System Security	Metasy...	Subsystem	User Login S...		127.0.0.1	
★	7/23/2013 12:27:56 PM CDT	NAE	User Action	System Security	testUser	Subsystem	User Logout			
★	7/23/2013 12:26:51 PM CDT	NAE	User Action	System Security	testUser	Subsystem	User accepts ...			
★	7/23/2013 12:26:45 PM CDT	NAE	User Action	System Security	testUser	Subsystem	User Login S...		127.0.0.1	
★	7/23/2013 12:26:42 PM CDT	NAE	User Action	System Security	testUser	Subsystem	User Passwo...			
★	7/23/2013 12:26:24 PM CDT	NAE	User Action	System Security	testUser	Subsystem	User Login F...		127.0.0.1	
★	7/23/2013 12:26:20 PM CDT	NAE	User Action	System Security	Metasy...	Subsystem	User Logout			
★	7/23/2013 12:26:13 PM CDT	NAE	User Action	System Security	Metasy...	Subsystem	Add a new user		testUser	
★	7/23/2013 12:25:46 PM CDT	NAE	User Action	System Security	Metasy...	Subsystem	User Login S...		127.0.0.1	
★	7/23/2013 12:25:40 PM CDT	NAE	User Action	System Security	Metasy...	Subsystem	User Logout			

When Metasys Event messages are delivered to Syslog destinations from the Metasys SMP UI, the fields are sent in the order shown in the Metasys Event Viewer, excluding the icon column (Figure 3). The Event Viewer columns are labeled as follows: Type | Priority | When | Item | Value | Description | Alarm Message Text.

Figure 3: *Metasys* Event Viewer - SMP UI



Event Viewer

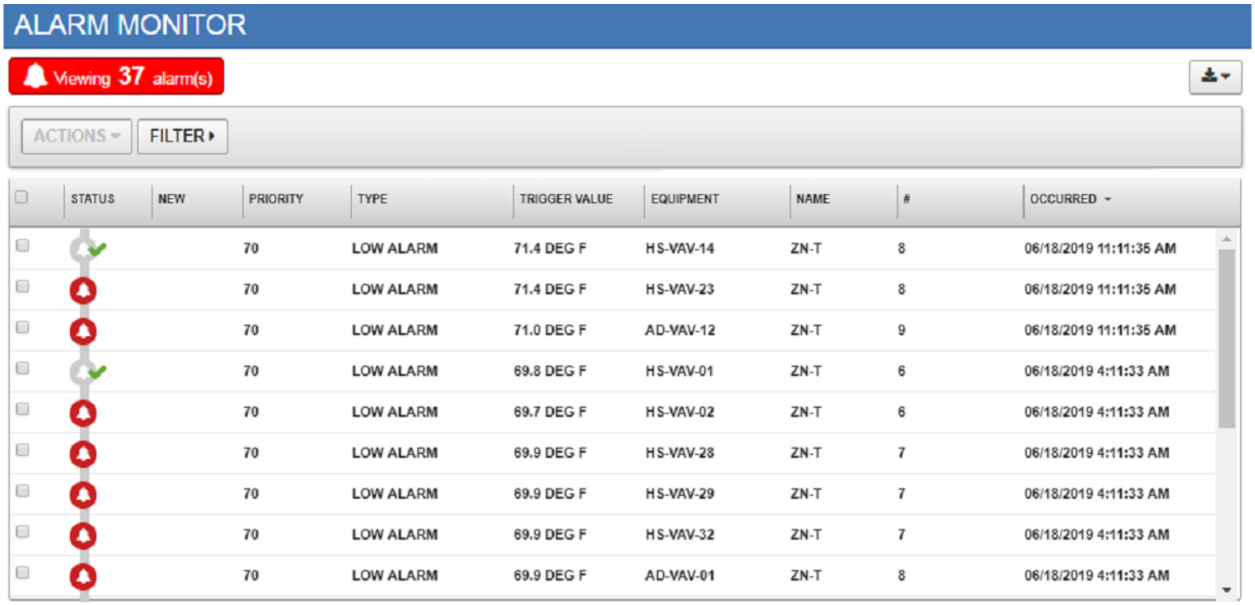
NAE-C4B8:NAE-C4B8

	Type	Priority	When	Item	Value	Description	Alarm Message Text
★ 💡	Low Alarm	70	7/23/2013 12:19:25 PM CDT	AV1	2.0		
★ 💡	High Alarm	70	7/23/2013 12:18:19 PM CDT	AV1	3.5e+0...		
★ 💡	Alarm	70	7/23/2013 12:16:32 PM CDT	BV1	Active		
★ 💡	Alarm	70	7/23/2013 12:13:38 PM CDT	BV1	Active		
★ 💡	Normal	200	7/23/2013 12:19:36 PM CDT	AV1	18.0		
★ 💡	Normal	200	7/23/2013 12:16:26 PM CDT	BV1	Inactive		
★ 💡	Normal	200	7/23/2013 12:13:32 PM CDT	BV1	Inactive		
💡	Normal	200	7/22/2013 02:03:21 PM CDT	AV1	10.0		
💡	Normal	200	7/22/2013 01:38:36 PM CDT	AV1	10.0		
💡	Normal	200	7/22/2013 01:36:19 PM CDT	AV1	10.0		
💡	Normal	200	7/22/2013 01:35:05 PM CDT	AV1	10.0		

When Metasys audit messages are delivered to Syslog destinations from Metasys UI Online, these fields are sent in the following order: Item | User | Description | Post Value | Start Day Of Week | Start Time | End Day Of Week | End Time | Spaces | Equipment.

When Metasys event messages are delivered to Syslog destinations from Metasys UI Online, these fields are sent in the following order: Current Status | Priority | Authorization Category | Acknowledge Required | Previous Status | Start Day Of Week | Start Time | End Day Of Week | End Time | Spaces | Equipment. Some of these fields appear in the following Alarm Monitor example.

Figure 4: Metasys UI Alarm Monitor



□	STATUS	NEW	PRIORITY	TYPE	TRIGGER VALUE	EQUIPMENT	NAME	#	OCCURRED ▾
□	✓		70	LOW ALARM	71.4 DEG F	HS-VAV-14	ZN-T	8	06/18/2019 11:11:35 AM
□	🔔		70	LOW ALARM	71.4 DEG F	HS-VAV-23	ZN-T	8	06/18/2019 11:11:35 AM
□	🔔		70	LOW ALARM	71.0 DEG F	AD-VAV-12	ZN-T	9	06/18/2019 11:11:35 AM
□	✓		70	LOW ALARM	69.8 DEG F	HS-VAV-01	ZN-T	6	06/18/2019 4:11:33 AM
□	🔔		70	LOW ALARM	69.7 DEG F	HS-VAV-02	ZN-T	6	06/18/2019 4:11:33 AM
□	🔔		70	LOW ALARM	69.9 DEG F	HS-VAV-28	ZN-T	7	06/18/2019 4:11:33 AM
□	🔔		70	LOW ALARM	69.9 DEG F	HS-VAV-29	ZN-T	7	06/18/2019 4:11:33 AM
□	🔔		70	LOW ALARM	69.9 DEG F	HS-VAV-32	ZN-T	7	06/18/2019 4:11:33 AM
□	🔔		70	LOW ALARM	69.9 DEG F	AD-VAV-01	ZN-T	8	06/18/2019 4:11:33 AM

For each message received from the Metasys system, the Syslog server displays three time stamps:

- the time the Syslog server received the message
- the time the Metasys system sent the message to the Syslog server (sent as part of the RFC 3164 Syslog Protocol Header)
- the time the audit or event occurred in the Metasys system as recorded in the **When** field of an Audit or Event entry

The time sent as part of the Syslog protocol header adheres to RFC 3164. The time the Metasys audit action or event occurred is recorded in standard local time and is presented in 12-hour format as part of the message field.

Metasys system use of Syslog packet format

A Syslog UPD packet contains three fields: PRI, Header, and Message.

PRI Field

The PRI field represents the two Syslog values named Facility and Severity. The Metasys system maps its messages into Syslog Facility and Severity numeric values as described in this section.

All Metasys Audit entries are sent to Syslog setting Facility to 13 (log audit) and Severity 6 (Informational).

All Metasys Events are sent at Severity 4 (Warning).

Metasys Events sent to Syslog reflect the Event Priority in the Facility part of the Syslog packet PRI field to align with the Event Notification Priority as described in Appendix M, Table M-1 of the ANSI/ASHRAE Standard 135-2012 (BACnet®), and map as follows:

Table 4: Syslog Event Facilities

Metasys Event Priority (sent to Syslog with):	Facility set to:
00 - 31	16 (Local use 0)
32 - 63	17 (Local use 1)
64 - 95	18 (Local use 2)
96 - 127	19 (Local use 3)
128 - 191	20 (Local use 4)
192 - 255	21 (Local use 5)

These BACnet ranges do not align with the Event Priority Tables 80–83 in *Metasys SMP Help (LIT-1201793)*. Metasys message groups conform to an earlier BACnet standard.

Event acknowledgments are sent to Syslog with Facility 1 (User-level messages), and Severity 5 (Notice).

Header Field

The header field sets the Hostname to the configured COMPUTER_NAME attribute of the NAE551S-2 device object.

Message Field

All Metasys system initiated Syslog messages set the Tag (first part) of the Message portion to **Metasys**. The content of the audit and event follows the tag, and each is described in the preceding section.

Refer to your Syslog server documentation for further information on how it displays information compliant with RFC3164.

ⓘ **Note:** When events are locally discarded in the Metasys system, the Event is internally acknowledged prior to being discarded. However, neither the discard nor the associated acknowledgment are sent to the Syslog server. This is standard Metasys system operation.

Syslog configurations

You configure Syslog online with a Metasys system administrator using the SMP.

Web site caching

If you cache web pages to reduce bandwidth, you may experience problems with Metasys system graphics and schedules. These features still function normally, but the User Interface may appear distorted or dimmed. We recommend you do not use web page caching.

Microsoft Message Queuing (MSMQ) technology

Recovery

About this task:
We recommend that you set MSMQ to restart after first, second, and subsequent failures.
To set recovery action:

1. In Control Panel, select **Administrative Tools**.
2. Double-click **Services**.
3. Right-click **Message Queuing** and select **Properties**. The Message Queuing Properties dialog box appears.

4. On the Recovery Tab (in the First failure, Second failure, and Subsequent failures drop-down list boxes), select **Restart the Service**.
5. Click **OK**.

   Note: RabbitMQ now replaces MSMQ. RabbitMQ is a service bus that sends notification messages to other services and for inter-process communication messages on the server.

Introduction

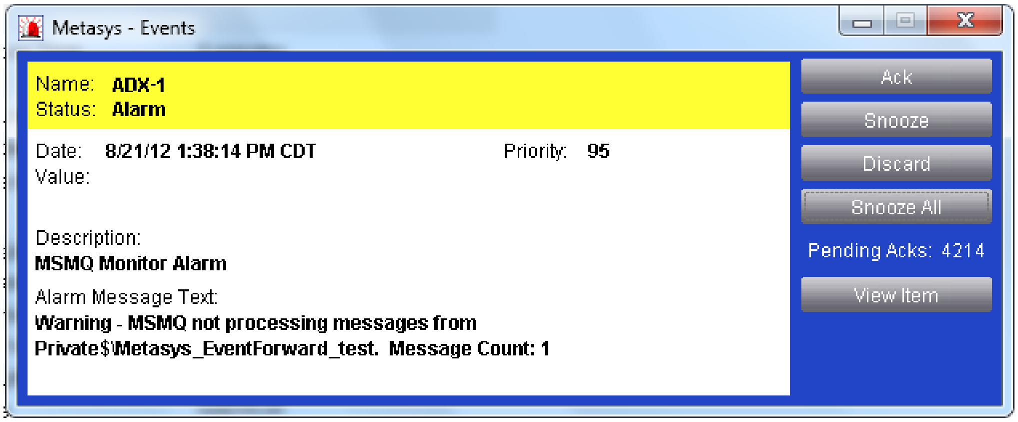
As implemented in the Metasys system, MSMQ supports trending and Site Management Portal UI navigation tree features. The Site Director queue receives trend data and navigation tree changes from other system devices. When the Site Director is busy, the messages remain in the queue until the Site Director is available to process them. Using MSMQ allows the system to avoid bottlenecks by separating the actions of receiving and processing data. All message queuing functions happen within the server itself; no messages from MSMQ broadcast over the network between the server and other devices.

MSMQ must be installed on all computers where ADS, ADX, OAS, or ODS software is installed. Once installed, do not stop or disable MSMQ. If MSMQ is stopped or disabled, the Site Director does not receive or process messages. Lost trending data may be irrecoverable. The queue fills at a rate determined by your site configuration and system use; for example, trend frequency or number of additions, changes, or deletions made to the navigation tree.

Note: Each Site Director contains all the navigation information for an entire site in a cache. This cache allows the Site Management Portal UI to display quickly without repeated requests to system devices. Updates received through the MSMQ queue keep the information current.

An alarm is generated in the Metasys system when any trend or alarm sample remains in the MSMQ for more than 10 minutes. This alarm usually indicates a problem with the Microsoft SQL Server® or that a remote forwarding destination is offline. See Figure 5 for an example of the *Metasys* alarm.

Figure 5: MSMQ Alarm



Name: **ADX-1**
Status: **Alarm**

Date: **8/21/12 1:38:14 PM CDT** Priority: **95**
Value:

Description:
MSMQ Monitor Alarm

Alarm Message Text:
Warning - MSMQ not processing messages from Private$\Metasys_EventForward_test. Message Count: 1

Pending Acks: 4214

At Release 6.5.5 and later, an alarm is generated in the Metasys system when trend samples remain in the queue after failing two bulk inserts and then fall back to a single insert mode. An alarm is generated for each trend sample that falls back to a single insert mode. XML files are created for each trend object that has a sample that cannot be processed. The XML files are located in the JCIHistorian database.

Message queue troubleshooting

Under normal operation, Metasys message queues are empty or near zero. If there is a problem with trend forwarding, the messages remain in the backlog queue and queue size increases. If this occurs, and the queues become full, permanent data loss can result.

ⓘ **Note:** This procedure requires that you have Windows Administrator access on your computer. Perform this procedure on all Metasys servers on your site. If you have a split ADX, perform this procedure on the database server computer.

To see the size of your MSMQ queue:

1. Using Windows Explorer®, right-click My Computer and select **Manage**. Depending on your operating system, the Computer Management tor Server Management screen appears.
2. In the tree in the left pane, browse to ***Services and Applications*** > ***Message Queueing*** > ***Private Queues***.
3. If the Number of Messages column for the Metasys queues (particularly metasys_trendbacklog) contains a number that is growing or not zero, you may have an issue with trend forwarding that requires further investigation. You may need to resize the window if this column is not visible.

Metasys system and virtual environments

Using software such as VMware® and Microsoft Hyper-V®, you can deploy the Metasys system in a virtual environment. When you do so, consider the following important factors.

Table 5: Virtual Environment Considerations and Requirements

Topic	Consideration or Requirement
Supported Virtual Environment Platforms	The Metasys system supports the following virtual environment platform minimum versions: • VMware vSphere Hypervisor (ESXi) 5.0 or later • VMware Workstation 10.0 • Microsoft Hyper-V® Server Allocate at least 16 Gb of memory to the virtual environment. ⓘ **Note:** There is no support for dynamic memory.
Virtual Environment Installation and Time Management	Install Hyper-V Integration Services/VMware Tools on the guest virtual machine used to host the Metasys system. Ensure the VM **does not** receive its time setting from the host server—an option that is configurable on the VM host server under the VM properties.
Prerequisite Hardware and Software	Use the same hardware specifications for the virtual machine as is stated in the Metasys server hardware requirements. Refer to the *Metasys System Configuration Guide [LIT-12011832]*). Virtual machines share hard drives, processors, network cards, and other resources. Keep this in mind when you choose and configure the server hardware for the Metasys virtual machine. If other virtual machines consume resources, the Metasys server may experience performance issues. Set the priority of the Metasys server hardware resources at the highest level.

Table 5: Virtual Environment Considerations and Requirements

Topic	Consideration or Requirement
SQL Server Software Performance	SQL Server performance is greatly affected by hard drive read/write performance. Also, applications that compete with the Metasys system for SQL Server resources may affect performance.
Dedicated Network Card	Use one dedicated network card that has a static IP address assigned for a Metasys server (physical or virtual). The network card should have a dedicated 100 Mbit/s or higher connection directly to the network. The Metasys server may experience a large amount of network traffic, depending on the size of the site. Sharing a network card with other VMs may cause the server to lose communications with connected devices such as NAEs.
Hard Disk Space and Configuration	Configure the virtual hard drive as a fixed-sized, non-expanding drive. Make sure that the virtual environment has enough disk space allocated. Do not attempt to run a system with the minimum required space. Make sure that the disk space is fully allocated, and do not configure the virtual environment to allow for drive expansion. If you have C2 Audit Tracing enabled in SQL Server, be aware that over time, the log files created can fill the hard disk. For general hardware requirements, refer to the *Application and Data Server (ADS/ADX) Product Bulletin (LIT-1201525)*, *Open Application Server (OAS) Product Bulletin (LIT-12013309)*, and *Open Data Server Product Bulletin (LIT-12011943)*.
Fail-Over and Clustering	Issues may occur if you configure the VM host server with failover or clustering. Failover occurs when a physical component of the VM server fails, causing the VM to move to another physical VM host server. A change in hardware, specifically a change in the network card or MAC Address, may cause communication issues. A reboot or reinstallation may be required.
Antivirus Software	You can employ antivirus software in a virtual environment. For a list of supported programs, see Antivirus software considerations (Metasys server, NxE85, NIE89, and LCS85 only). To understand how to configure the antivirus software on a Metasys system, see Appendix: Installing antivirus software.
Other Applications	Make sure that no other applications adversely affect the computer that is running the virtual environment. Metasys system performance degrades very quickly when other applications contend for host operating system resources.

Monitoring and managing (SNMP)

Simple Network Management Protocol (SNMP) provides IP standard SNMP functionality in the Metasys system, which enables network administrators to manage Metasys network performance, find and resolve issues related to the Metasys network, and plan for future growth of the Metasys system. SNMP uses standard SNMP Versions 1, 2C, and 3 (which excludes SNMP encryption and authentication support). The Metasys system allows delivery of unsecured SNMP traps for Metasys alarm events by using a Network Management System (NMS).

A custom Metasys system specific MIB is available and allows the NMS to monitor Metasys point objects, display attributes, and control sequence objects. The MIB also defines explicit traps and associated attributes that align with Metasys alarm messages, making data correlation (parsing/sorting) at the NMS straightforward. Traps from the Metasys system are not encrypted.

The NMS operator can perform Gets and Get Nexts (SNMP Walks) against engines through an NMS. Gets allow you to view object data but do not allow you to write to objects. To use Gets, you must query the specific engine (NAE55, for example) on which the object appears. Site Directors do not forward Get requests to other devices on the site, and you cannot perform Gets on Metasys servers. Metasys system objects are specified as a string index in a table, so the NMS must have the capability to specify an index as a string, or the NMS operator must encode the Object ID using the decimal equivalents.

The Johnson Controls® MIB is included on the product media. SNMP is offered on all supervisory devices (network engine and Metasys server).

For information on configuring SNMP traps, turning off SNMP or Gets capability, and other alarm information, refer to the *Alarm and Event Management* section of the *Metasys SMP Help (LIT-1201793)*. For information about SNMP implementation in the Metasys system, see Appendix: SNMP agent protocol implementation.

Time management (Simple Network Time Protocol [SNTP])

Three methods for network time synchronization are available in the Metasys system: Microsoft Windows SNTP time synchronization, Multicast, and BACnet time synchronization.

You can use the Multicast and Microsoft Windows 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.

ⓘ **Note:** The Multicast time synchronization is preferred over the Windows time synchronization.

Typically in the Metasys system, only the Site Director synchronizes its time with an SNTP time server. The other devices on the Metasys network synchronize with the Site Director. As a secondary method of time synchronization, configure the Metasys system to have all devices synchronize time with the Site Director as an SNTP Time Server.

If critical changes occur to time zones or time change protocols, Johnson Controls issues patches to update the Metasys system. For more details on time management, refer to the following documents:

- *ADS/ADX Commissioning Guide (LIT-1201645)*
- *OAS Commissioning Guide (LIT-12013243)*
- *ODS Commissioning Guide (LIT-12011944)*
- *NIEx9 Commissioning Guide (LIT-12011922)*
- *LCS85 Commissioning Guide (LIT-12011568)*
- *Time Zone, Date, and Time Management Appendix* found in the *NAE Commissioning Guide (LIT-1201519)*, *SNE Commissioning Guide (LIT-12013295)*, and *SNC Commissioning Guide (LIT-12013352)*

Email (SMTP)

All email capable devices in the Metasys system use only Simple Mail Transfer Protocol (SMTP) to communicate with the mail server. The Metasys system can be configured to use SMTP for notification of system events and alarms. At Release 10.1 or later, network engines continue to provide email as a notification method for alarms. For details, refer to the *NAE Commissioning Guide (LIT-1201519)*, *NIEx9 Commissioning Guide (LIT-12011922)*, *SNE Commissioning Guide (LIT-12013295)*, *SNC Commissioning Guide (LIT-12013352)*, or *LCS85 Commissioning Guide (LIT-12011568)*.

However, Metasys Servers at Release 10.1 or later no longer offer email notifications, unless MVE is installed on the Metasys Server. The email functionality is now provided by the Remote Notifications feature in Metasys UI Online. For details, refer to *Metasys UI Help (LIT-12011953)*.

Notes:

- If Symantec Enterprise Protection Version 12 is installed on a client machine with the **POP3/ SMTP Scanner** option selected, the SMTP functions and email alerts for the Metasys server software are disabled without notification. In order to use the SMTP and email alert features in the Metasys server, do not select the POP3/SMTP Scanner option during Symantec Enterprise Protection installation.
- If McAfee® VirusScan® Enterprise version 8.8 with Patch 3 or Patch 5 is installed on a client machine with the **Prevent mass mailing worms from sending mail** option selected, the SMTP functions and email alerts for the Metasys server software are disabled without notification. In order to use the SMTP and email alert functions in the Metasys server, do not select this option during the McAfee VirusScan installation.

Encrypted email

Metasys software features an email encryption capability that encrypts user names and passwords as they are entered into the SMP UI. Embedded and server machines can thereby send emails to email servers over a secure channel (secure socket layer [SSL]). The entire email payload is encrypted, and allows Metasys software to communicate to email servers that require SSL connections.

Users can configure email encryption with no authentication required, including SMTP authentication, and POP-Before-SMTP authentication.

Communication to pagers, email, printer, SNMP, or Syslog destination

The system guarantees delivery of events from engines to a Metasys server, but this delivery guarantee does not extend to the DDA destinations: pagers, email accounts, printers, or SNMP destinations.

Consider the following:

- **Pagers:** (Telocator Alphanumeric Protocol) - Delivery to the service provider is guaranteed. The service provider delivers to the final pager account as time permits. Pager functionality is not available on network engines at Release 9.0.7 or later, nor with any Metasys Server at Release 10.1 or later.
- **Email:** (Simple Mail Transfer Protocol) - Delivery to the service provider is guaranteed. The service provider delivers to the final email account as time permits. The delivery may not be made for a number of reasons, including recipient mail server spam rules, or the service provider’s inability to communicate to the recipient mail server. At Release 10.1 or later, email functionality has been moved from the Metasys Server to the Remote Notifications feature in Metasys UI Online, but is still available if MVE is installed on the Metasys Server.
- **Printers:** Information sent to a printer may not be delivered in a timely manner for a number of reasons, including printer offline or out-of-paper conditions. At Release 10.1or later, printer functionality has been moved from the Metasys Server to the Remote Notifications feature in Metasys UI Online, but is still available if MVE is installed on the Metasys Server.

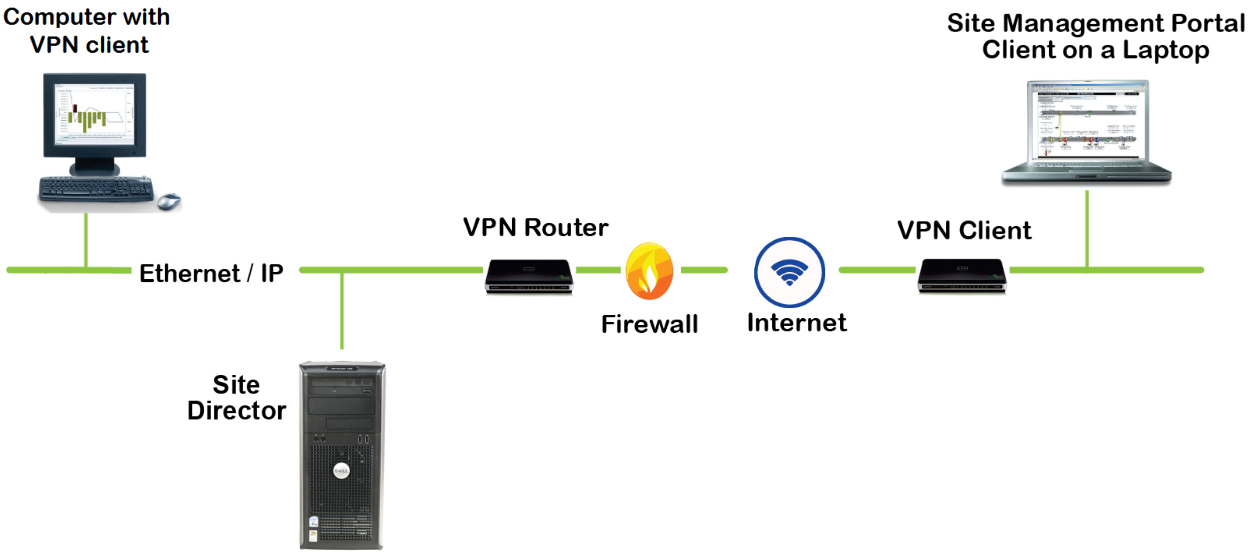
- **SNMP:** This delivery system uses UDP, which does not guarantee delivery. At Release 10.1 or later, SNMP functionality has been moved from the Metasys Server to the Remote Notifications feature in Metasys UI Online, but is still available if MVE is installed on the Metasys Server.
- **Syslog:** The Syslog DDA implementation is UDP, not TCP. Therefore, any audits/events generated while the Syslog server is offline are not recorded at the Syslog server, even though the Metasys system, unable to determine the current status of the Syslog server, continues to send out messages. A gap in time is present between events when the Syslog server comes back online. At Release 10.1 or later, Syslog functionality has been moved from the Metasys Server to the Remote Notifications feature in Metasys UI Online, but is still available if MVE is installed on the Metasys Server.

Given the non-deterministic status of delivery, we recommended that physical fail-over measures be implemented as the primary safety control for critical activities.

Remote access to the Metasys system using a VPN

The simplest method of remotely accessing the Metasys system is to use an existing VPN infrastructure. If an existing VPN infrastructure is present on the site already, the risks and security concerns have been established and addressed. Using a VPN, the Metasys system features are the same as if remote users are on the company intranet. The one restriction is that the Metasys system does not support Secure Socket Layer (SSL) VPN.

Figure 6: Metasys system Internet communication by using VPN

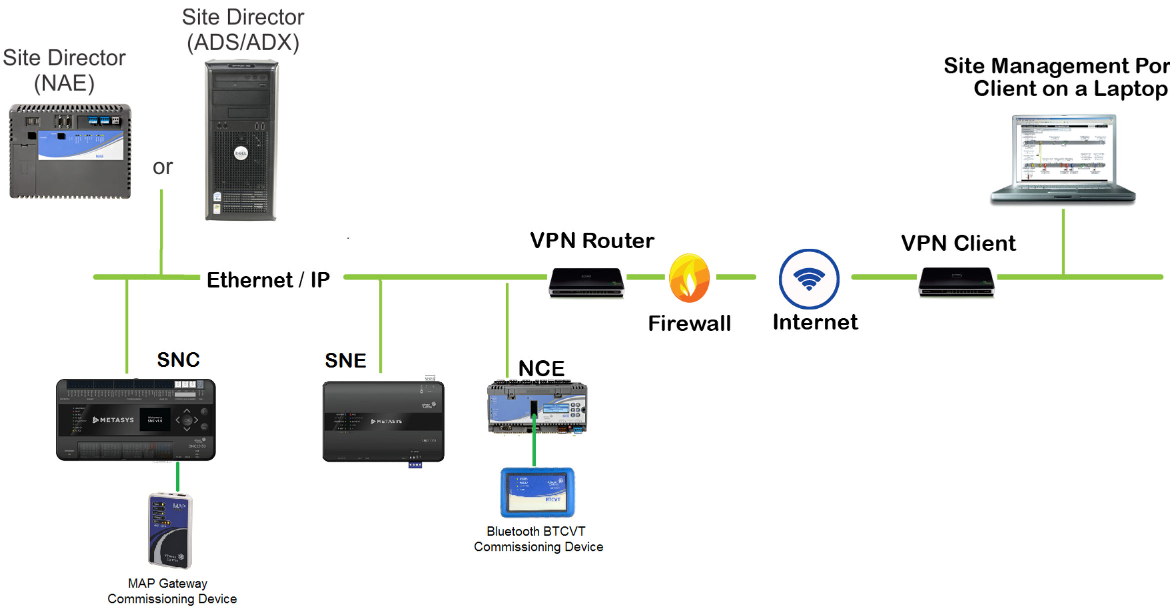


Metasys system architecture

Figure 7 shows one example of the many ways you can design the Metasys system architecture.

ⓘ **Note:** Restrictions apply to the engines supported with an ADS-Lite Site Director. Refer to the *Metasys System Configuration Guide (LIT-12011832)*.

Figure 7: Metasys System Architecture


Site Director (NAE)
Site Director (ADS/ADX)
or
Site Management Portal Client on a Laptop
Ethernet / IP
VPN Router
Firewall
Internet
VPN Client
SNC
SNE
NCE
Bluetooth BTCVT Commissioning Device
MAP Gateway Commissioning Device

Protocols, ports, and connectivity for the Metasys system

Protocols and ports tables

ⓘ **Note:** The Metasys system uses Bluetooth technology only as an option to commission a select number of devices. Bluetooth technology is not used for system communication in any way after initial commissioning. The Metasys system also uses the MAP Gateway for device commissioning. For details, refer to the *Mobile Access Portal Gateway Network and IT Guidance Technical Bulletin (LIT-12012015)*.

Table 6, Table 7 and Table 8 describe the various IP protocols and how they relate to the Metasys system.

➤ **Important:** Johnson Controls cannot be responsible for a customer's decision to open or close ports that we consider non-essential. Consult with your technical and security teams before opening or closing a port. Ports or services not described in this table are not used by the Metasys system and may be closed at the customer's discretion. Ports in this table that are not required at a customer site may also be closed at the customer's discretion. To close a port, see Closing ports.

Table 6: Ethernet Protocols and Ports

Port[1]	Protocol	Uses	Metasys Device	Description
22	SSH	TCP	Network Engine (Linux OS only)	Used to remotely access a network engine from a laptop. This function is only available for use by authorized personnel on Johnson Controls laptops.
23	Telnet	TCP	Network Engine	Telnet is no longer available for network engines at Release 10.0 or later.
25	SMTP	TCP	NAE35/NAE35/ NCE25	Provides remote access to device using the internet or local area network.
25	SMTP	TCP	ADS/ADX/OAS/ ODS	Used for alarms and events.
			Network Engine	
53	DNS	UDP	Active Directory Client	Translates domain names into numerical IP addresses. This port allows the server to receive responses to DNS queries.
			ADS/ADX/OAS/ ODS	
			Computer (Web Browser)	
			Network Engine	
67 **68**	DHCP[2]	UDP	Active Directory Client	Assigns and keeps track of dynamic IP addresses and other network configuration parameters. **Alternate Method:** Use static IP addresses.
			ADS/ADX/OAS/ ODS	
			Computer (Web Browser)	
			Network Engine	
69	TFTP[2]	UDP	Metasys SCT	Downloads new images to NAEs. ⓘ **Note:** This port is used only when the NAE is provisioned and is not used during system runtime.
			Network Engine	

Table 6: Ethernet Protocols and Ports

Port[1]	Protocol	Uses	Metasys Device	Description
80	HTTP[2]	TCP	ADS/ADX/OAS/ODS	Provides communication between peer controllers, computers, and other Internet systems using SOAP over HTTP. The ADS/ADX/ODS requires that only Port 80 be open to receive communication from client devices. Port 80 is the primary port used by the World Wide Web. ⓘ **Note:** For a higher level of security, at Metasys system Release 8.1 or later, you can close Port 80 (incoming and outgoing). See Closing ports.
			Computer (Web Browser)	
			Network Engine	
			SCT	
80	HTTP	TCP	NAE Update Tool	Used for file transfers between the client computer and the network engine.

Table 6: Ethernet Protocols and Ports

Port[1]	Protocol	Uses	Metasys Device	Description
88	Kerberos	TCP UDP	ADS/ADX/OAS/ODS (Member of Domain X)	Used by the Metasys system for Active Directory service authentication at the Metasys system login screen, and Service Account authentication prior to LDAP queries. Kerberos is a standard network authentication protocol designed to provide strong authentication for client/server applications by using secret-key cryptography. Kerberos is the primary security protocol for authentication within an Active Directory service Domain. Kerberos authentication relies on client functionality built into the Windows operating systems supported by Metasys software.
			ADX Split Web/Application Server (Member of Domain X)	
			Metasys System Client (Member of any Domain)	
			SCT (Member of Domain X)	
110	POP3	TCP	Computer (Web Browser)	Receives and holds email for downloading from your Internet server. POP3 is allowed in the Metasys system only for authentication from a SMTP server. **Note:** Firewall rules are not necessary to allow access in most cases because this server should be behind the firewall.

Table 6: Ethernet Protocols and Ports

Port[1]	Protocol	Uses	Metasys Device	Description
123	NTP	UDP	ADS/ADX/OAS/ ODS (Member of Domain X)	Used for time synchronization across a network between client computers and server-class operating system host computers.
			ADX Split Web/ Application Server (Member of Domain X)	
			Metasys System Client (Member of any Domain)	
			SCT (Member of Domain X)	
123	SNTP[2]	UDP	ADS/ADX/OAS/ ODS	Used to synchronize computer clocks over a network between a server and its clients. SNTP is not required for all systems.
			Network Engine	
135	Remote Procedure Call (RPC)	TCP	ADS/ADX/OAS/ ODS (Member of Domain X)	Used by IIS on the ADS/ ADX, OAS/ODS, and SCT during the process of authentication during SSO (Windows Integrated Authentication). If SSO is disabled in the Metasys system, this port and protocol are not used by the Metasys system; however, if the ADS/ADX, OAS/ODS, SCT, or Metasys client, or any combination are members of an Active Directory service domain, this port and protocol are used for Active Directory service functionality.
			ADX Split Web/ Application Server (Member of Domain X)	
			Metasys System Client (Member of any Domain)	
			SCT (Member of Domain X)	

Table 6: Ethernet Protocols and Ports

Port[1]	Protocol	Uses	Metasys Device	Description
161	SNMP[2]	UDP	ADS/ADX/OAS/ODS	Provides network monitoring and maintenance. Typically notifies IT department personnel of alarms that are of interest to them, such as data center environmental conditions. The site must use a network management system capable of receiving SNMP Traps. **Alternate Method:** If the system allows, use email destinations for remote alarm notification instead of SNMP.
			Metasys UI	
			Network Engine	
			SCT	
389	LDAP	TCP	ADS/ADX/OAS/ODS (Member of Domain X)	Used by the Metasys system to access user objects and attributes within Active Directory service. LDAP is a standard communication protocol for directories located on TCP/IP networks. LDAP defines how a directory client can access a directory server and how the client can perform directory operations and share directory data.
			ADX Split Web/Application Server (Member of Domain X)	
			Metasys System Client (Member of any Domain)[3]	
			SCT (Member of Domain X)	

Table 6: Ethernet Protocols and Ports

Port[1]	Protocol	Uses	Metasys Device	Description
443	Secure Sockets Layer (SSL) Transport Layer Security (TLS) HTTPS	TCP	ADS/ADX/OAS/ODS (Member of Domain X)	Required if you use SSL with your reporting ADX.
			Metasys Advanced Reporting ADX	
			Network Engine	Required if you use TLS with the Metasys UI and the Metasys UI Offline for site security. Port 443 is used for secure web browser communication. Data transferred across such connections is highly resistant to eavesdropping and interception. Moreover, the identity of the remotely connected server can be verified with significant confidence. Web servers offering to accept and establish secure connections listen on this port for connections from web browsers desiring strong communication security.
			SCT (Member of Domain X)	
			Metasys UI and Metasys UI Offline	
			Computer (web browser)	
			Background File Transfer (BFT) in SCT	With BFT, file transfers occur between the device and SCT where the device is the HTTPS client and SCT is the HTTPS server.

Table 6: Ethernet Protocols and Ports

Port[1]	Protocol	Uses	Metasys Device	Description
445	NT LAN Manager Version 2 (NTLMv2)	TCP	ADS/ADX/OAS/ ODS (Member of Domain X) ADX Split Web/ Application Server (Member of Domain X) Metasys System Client (Member of any Domain) SCT (Member of Domain X)	Used during Metasys system SSO authentication. NTLMv2 is a network authentication protocol developed by Microsoft and the secondary security protocol for authentication within an Active Directory service domain. If a domain client or domain server cannot use Kerberos authentication, then NTLM authentication is used.
465	SMTP	TCP	ADS/ADX/OAS/ ODS Network Engine	Used for alarms and events.
514	Syslog	UDP	ADS/ADX/OAS/ ODS Network Engine SCT	Provides 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.
587	SMTP	TCP	ADS/ADX/OAS/ ODS Network Engine	Used for alarms and events.
995	POP3	TCP	Computer (Web Browser)	Receives and holds email for downloading from your Internet server. POP3 is allowed in the Metasys system only for authentication from a SMTP server. The mail server uses port 995 for SSL connections for POP3 access. ⓘ **Note:** Firewall rules are not necessary to allow access in most cases because this server should be behind the firewall.

Table 6: Ethernet Protocols and Ports

Port[1]	Protocol	Uses	Metasys Device	Description
1025	Remote Procedure Call (RPC)	TCP	ADS/ADX/OAS/ODS (Member of Domain X) ADX Split Web/ Application Server (Member of Domain X) Metasys System Client (Member of any Domain) SCT (Member of Domain X)	Used by IIS on the ADS/ADX/OAS/ODS/SCT during the process of authentication during SSO (Windows Integrated Authentication). If SSO is disabled in the Metasys system, this port and protocol are not used by the Metasys system; however, if the ADS/ADX/OAS/ODS/SCT, or Metasys client, or any combination, is a member of an Active Directory service domain, this port and protocol are used for Active Directory service functionality.
1433	Microsoft SQL Server Database	TCP	ADX Metasys ADX Split Database Server (Member of Domain X)	Used between the web/ application server and database server computers when the ADX is split across two devices.
3003	PhantomJS	TCP	ADS	Involved in generating PDF files in Metasys UI Reports.
3389	Remote Desktop Protocol (RDP)	TCP	NAE55/NIE (Windows Embedded OS only)	Used to log in to the operating system of a device from a remote computer. The Remote Desktop Protocol (RDP) Service is usually disabled unless enabled by the NxE Information and Configuration Tool (NCT) operation.

Table 6: Ethernet Protocols and Ports

Port[1]	Protocol	Uses	Metasys Device	Description
4096 **4097**	N2 Protocol	UDP	NAE55 (Windows Embedded OS only)	Used for N2 tunneling over Ethernet on trunk 1. The N2 technology option provides a serial data port, allowing variable speed drives (VSDs) to link and form a network.
			NAE55 (Windows Embedded OS only)	Used for N2 tunneling over Ethernet on trunk 2. The N2 technology option provides a serial data port, allowing variable speed drives (VSDs) to link and form a network on the SA Bus.
9004	Johnson Controls Licensing Service	TCP	Software Manager	For Computer only; it may be closed.
9910	Microsoft Discovery Protocol[2]	TCP and UDP	Network Engine	Used by NCT to get diagnostic information from devices on the same network.
			SCT	
			NCT and NAE Update Tool	
9911	Metasys Private Message[2]	UDP	SCT	Used by SCT to broadcast a message to the local network segment when a user selects the device discovery menu item. Any Metasys node that receives this broadcast message will respond on UDP port 9911 with device configuration information to be displayed in the device discovery window.
10000	PhantomJS	TCP	ADS	Involved in generating PDF files in Metasys UI Reports.
10050		TCP	NAE Update Tool	Used during NAE Update Tool operations such as updating an image to a network engine. Not used with SNC and SNE engines.

Table 6: Ethernet Protocols and Ports

Port[1]	Protocol	Uses	Metasys Device	Description
11001[4]	N1 Protocol	UDP	NCM NIE5x	Provides N1 message transmission (proprietary packet encoded in UDP) for devices at Release 9.0 or earlier. If you are connecting to multiple N1 networks, the port is unique for each N1 network. Network Control Modules automatically configure themselves to use Port 11001. Start numbering other networks in the Multi-network configuration with 11003 and continue sequentially. Do not use a UDP Port Address (UDPPA) of 11002. The value 11002 is used by the Metasys Ethernet Router and should be avoided even if Metasys Ethernet Routers are not in the system. The recommended addressing for five N1s is 11001, 11003, 11004, 11005, 11006.
12000	UberDebug Service	TCP	Metasys System	Used by Metasys software for debugging and logging.
47808	BACnet/IP Protocol	UDP	NAE/NCE	Refer to the *BACnet Controller Integration with NAE/NCE Technical Bulletin (LIT-1201531)*. If you are connecting to multiple BACnet networks, the port is unique for each BACnet network. The default port number is 47808. Choose additional UDP ports that do not conflict with a port that is in use.

[1] Generally recorded by the IANA.

[2] Required for proper functionality of SCT features (for example, Device Discovery and Device Debug); this port is usually closed and is only open during operation of certain SCT features.

[3] LDAP is used by the Metasys system client only if Windows Active Directory service search tool is used (for example, Start->Search->ForPeople).

[4] This port number is registered to Johnson Controls.

The ports listed in Table 7 are Internal-Only ports. These ports do not have to be closed by the ADX server OS Firewall because the ports are open on the local device only.

Table 7: Internal-Only Ports

Port Number	Protocol	Uses	Metasys Device	Description
4369	TCP	Rabbit MQ	ADS/ADX	Erlang Port Mapping Daemon.
5291	TCP	Action Queue	ADS/ADX	Action Queue communication, processing events/audits.
5672	TCP	Rabbit MQ/Erlang	ADS/ADX	Listening port for Message Bus, communication between micro-services.
5960	TCP	Device Manager	ADS/ADX	Metasys Device Manager inter-process communication.
9003	TCP	Johnson Controls Product Update	ADS/ADX	Port to query for Johnson Controls Product Updates.
9505	TCP	Johnson Controls Rate Limit Website	ADS/ADX	Website binding to process rate limiting for requests.
9506	TCP	Johnson Controls Rewrite Website	ADS/ADX	Website binding to route API requests to appropriate micro-services.
9507	TCP	Johnson Controls Website	ADS/ADX	Main internal website binding hosting APIs.
25672	AMQP	Rabbit MQ/Erlang	ADS/ADX	Inter-node and CLI tool communication.

Table 8: Wireless Ports and Protocols

Port Number[1]	Protocol	Uses	Wireless Protocol	Metasys Device	Description
80	HTTP	TCP	802.11b/802.11g	Computer (Web Browser)	Used to synchronize computer clocks over a network between a server and its clients. SNTP is not required for all systems.
4050[1]	Wireless Many-to-One Sensing[2]	UDP	802.15.4	WRS-RTN	Used for wireless supervisor integration; recommended UDP port number.
47808	Wireless ZigBee	UDP	802.15.4	Wireless Network Coordinator (WNC)	Used for wireless supervisor integration; recommended UDP port number.

[1] If this port is in use, it **can** be reconfigured to another port.

[2] Johnson Controls proprietary protocol.

Connectivity and protocol diagrams

Figure 8 through Figure 14 are example diagrams of the various types of connectivity and protocols for the Metasys system. Not all protocols are used in all Metasys system configurations.

The configuration and network topology of the specific Metasys system installation must be considered when opening firewall ports for communication. For example, considering Figure 8 and Table 6, if the Metasys Server is not acting as a time server, then the SNTP protocol between callout 3 and callout 2 is not used. Similarly, if Metasys system alarms and events are not being monitored by IT tools, then the SNMP Trap protocol between callout 2 and callout 4, and item callout 3 and callout 4 is not used.

ⓘ **Note:** Restrictions apply to the engines supported with an ADS-Lite Site Director. Refer to the *Metasys System Configuration Guide (LIT-12011832)* to discover which engines are supported for systems using the ADS-Lite as Site Director.

Multiple engines with one ADX

The following figure is an example of the connectivity and protocols for a Metasys system using multiple engines and an ADS. Table 9describes the protocols used in Figure 8.

Figure 8: Metasys System with Multiple Engines and an ADS

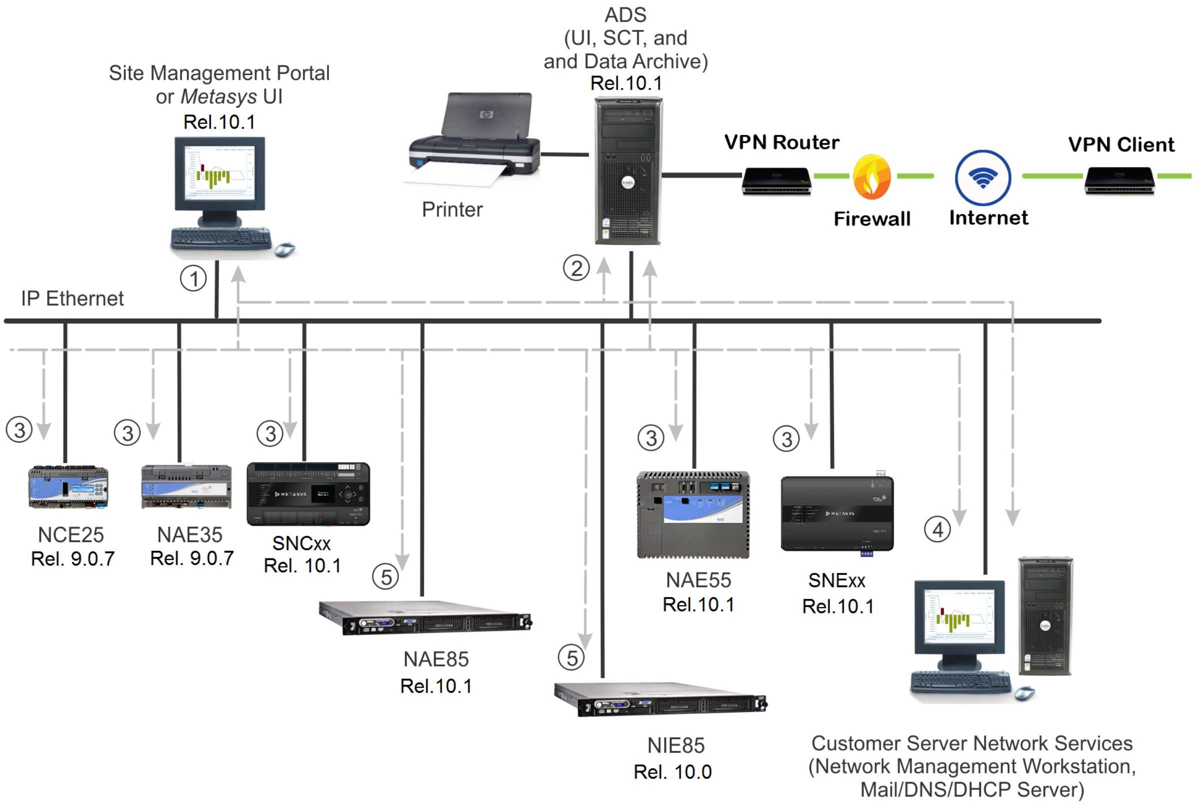


Table 9: Metasys System with Multiple Engines and an ADS

Interaction between callouts		Protocol	Communication direction
1	2,3,5	HTTP	Unidirectional[1]
1	4	Customer standard configuration	Customer standard configuration
2	3,5	HTTP	Bidirectional
2,3,5	4	DHCP, DNS, SMTP, SNMP, SNMP Trap, SNTP	Unidirectional
3,5	2	SNTP[2]	Unidirectional
3,5	3,5	HTTP, BACnet, DNS	HTTP, BACnet: Bidirectional DNS: Unidirectional

[1] In Unidirectional communication, only the originating device initiates requests (assuming synchronous response is allowed in the request).

[2] To ensure proper performance, a Web browser should never use an engine for its SNTP server.

Active Directory network

The following figure is an example of the connectivity and additional protocols used in a Metasys system that uses Active Directory service. Table 10 describes the protocols used in Figure 9.

Figure 9: Metasys system with Active Directory service

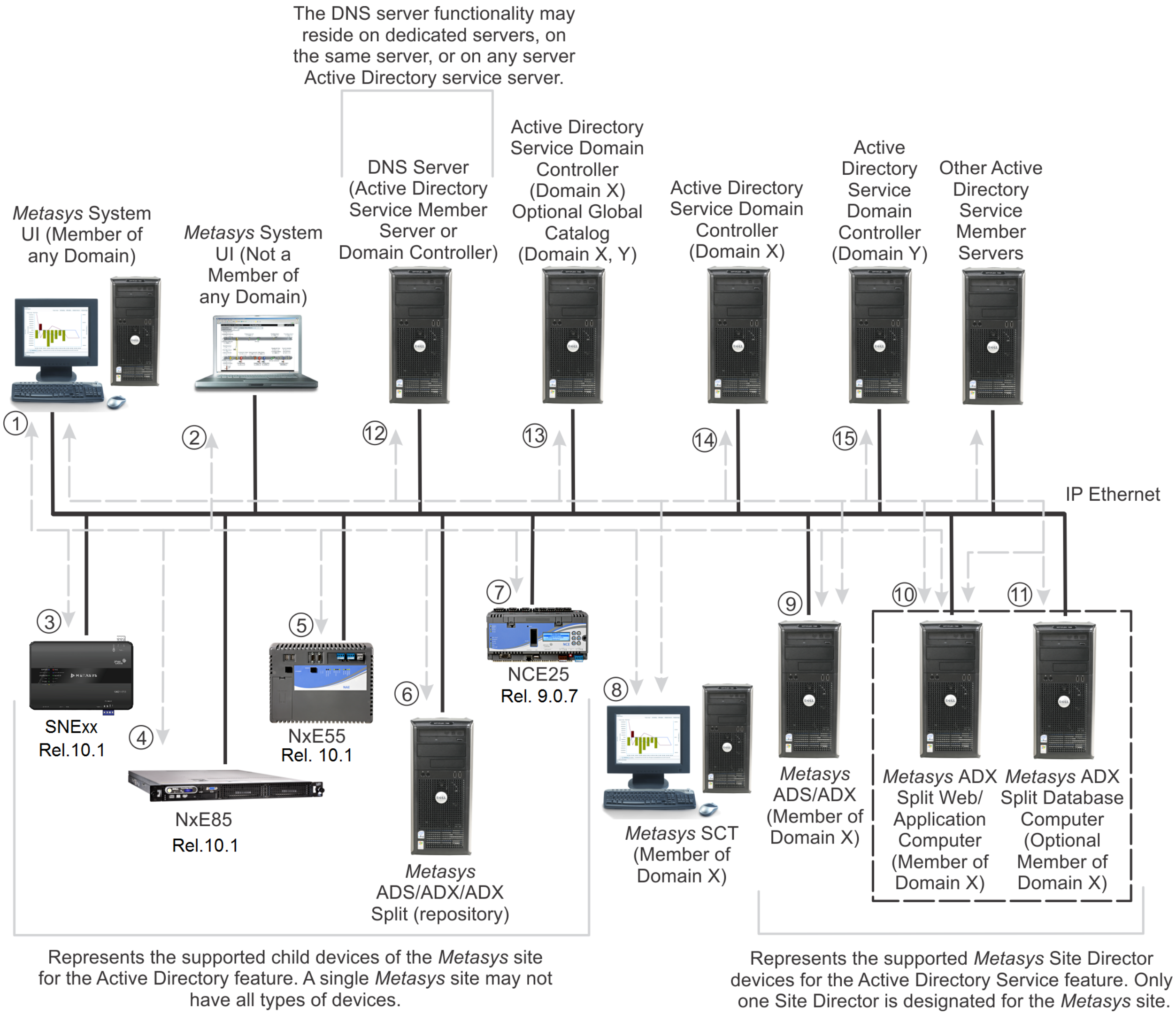

The DNS server functionality may reside on dedicated servers, on the same server, or on any server Active Directory service server.
Metasys System UI (Member of any Domain)
Metasys System UI (Not a Member of any Domain)
DNS Server (Active Directory Service Member Server or Domain Controller)
Active Directory Service Domain Controller (Domain X) Optional Global Catalog (Domain X, Y)
Active Directory Service Domain Controller (Domain X)
Active Directory Service Domain Controller (Domain Y)
Other Active Directory Service Member Servers
1
2
12
13
14
15
IP Ethernet
3
SNExx Rel.10.1
4
NxE85 Rel.10.1
5
NxE55 Rel. 10.1
6
Metasys ADS/ADX/ADX Split (repository)
7
NCE25 Rel. 9.0.7
8
Metasys SCT (Member of Domain X)
9
Metasys ADS/ADX (Member of Domain X)
10
Metasys ADX Split Web/ Application Computer (Member of Domain X)
11
Metasys ADX Split Database Computer (Optional Member of Domain X)
Represents the supported child devices of the *Metasys* site for the Active Directory feature. A single *Metasys* site may not have all types of devices.
Represents the supported *Metasys* Site Director devices for the Active Directory Service feature. Only one Site Director is designated for the *Metasys* site.

Table 10: Metasys System with Active Directory Service

Interaction between Callouts		Protocol	Communication Direction
1	**3, 4, 5, 6, 7**	No new protocols. See Figure 8 and Table 6.[1]	Unidirectional[2]
1	**8, 9, 10**	NTLMv2[3]existing protocols already defined for Metasys system; no new protocols. See Figure 8 and Table 6.[1]	Unidirectional[2]
1[4,5]	**12, 13, 14, 15**	Kerberos or NTLMv2[3], DNS, LDAP, NTP, RPC	Unidirectional[2]

Table 10: Metasys System with Active Directory Service

Interaction between Callouts		Protocol	Communication Direction
2	**3, 4, 5, 6, 7**	No new protocols. See Figure 8 and Table 6.[1]	Unidirectional[2]
2	**8, 9, 10**	No new protocols. See Figure 8 and Table 6.[1]	Unidirectional[2]
8, 9, 10[4,6,7,8]	**12, 13, 14, 15**	Kerberos or NTLMv2[3], LDAP, NTP, RPC	Unidirectional[2]

[1] *Metasys* system client in is equivalent to web browser in Figure 9.

[2] In Unidirectional communication, only the originating device initiates requests (assuming synchronous response is allowed in the request).

[3] NLTMv2 is the default and preferred version of the NTLM protocol.

[4] DNS, NTP, Kerberos, NTLM, LDAP, and RPC are protocols required as a result of the device becoming a member of an Active Directory service domain. These are standard Active Directory service protocols.

[5] The LDAP protocol may be used between the Metasys system client and domain controller when the client is using Active Directory service tools provided by the operating system and the particular domain controller is responding to the LDAP query.

[6] The Kerberos protocol is used between a Metasys Site Director and/or SCT and the Active Directory service domain controller when the Site Director is authenticating against the Active Directory service domain. For domain authentication, any domain controller within the domain may respond.

[7] The LDAP protocol is used between a Metasys Site Director and/or SCT and Active Directory service domain controller when the Site Director is querying the directory for object information.

[8] RPC is used by IIS on the ADS/ADX/OAS/ODS/SCT during the process of authentication during SSO (Windows Integrated Authentication). If SSO is disabled in the Metasys system, this port and protocol are not used by the Metasys system; however, if the ADS/ADX/OAS/ODS/SCT or Metasys system client is a member of an Active Directory service domain, this port and protocol are used for Active Directory service functionality.

M3 Workstation with N30 Controllers

The following figure is an example of the connectivity and protocols for a Metasys system using the M3 Workstation and N30 controllers. See Figure 8 with Table 6, and Figure 9 with Table 10, for the full set of protocols used by the engine, *Metasys* Server, and Site Management Portal UI.

Figure 10: Metasys System with N30 Controllers Using BACnet Protocol

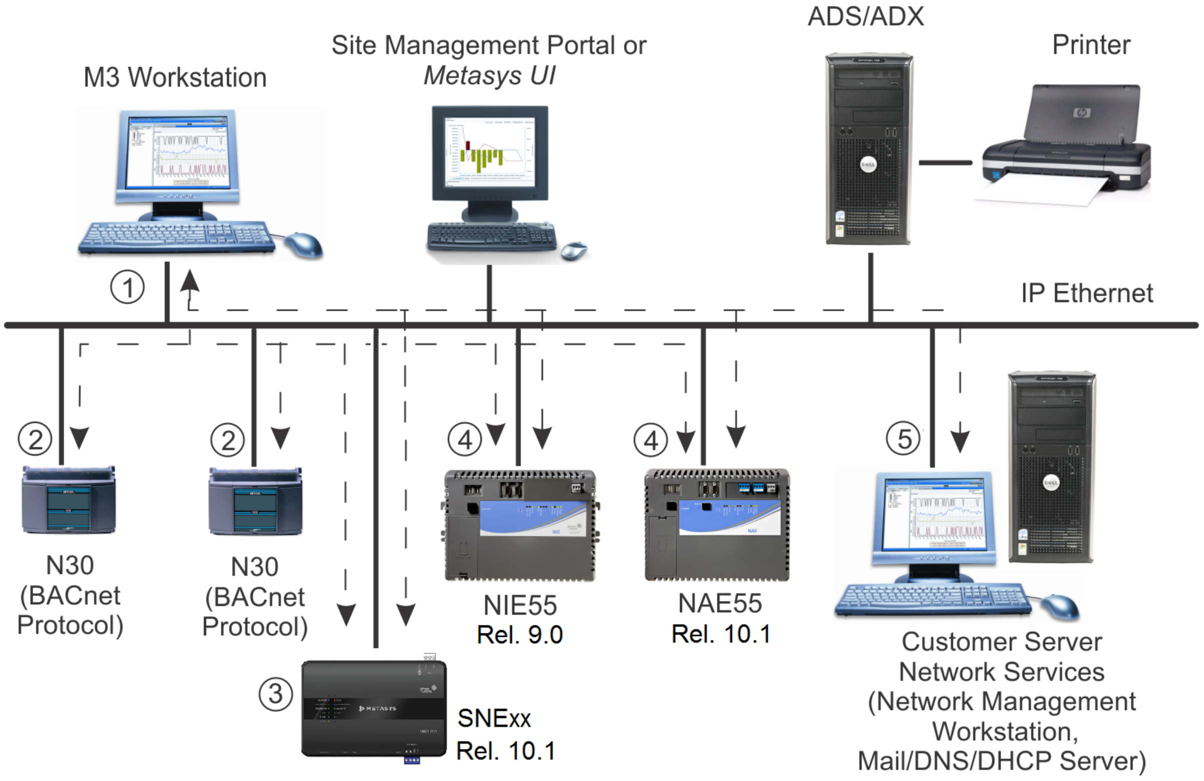


Table 11: Metasys System with N30 Controllers Using BACnet Protocol

Interaction between Callouts		Protocol	Communication Direction
1	**2**	BACnet[1]	Bidirectional[2]
1	**3**	BACnet[1]	Bidirectional[2]
1	**4**	BACnet[1]	Bidirectional[2]
1	**5**	POP3, SMTP, SNMP, SNMP Trap	Unidirectional[3]
2	**3**	BACnet[1]	Bidirectional[2]
3	**4**	BACnet[1]	Bidirectional[2]
2	**2**	BACnet	Bidirectional[2]
2	**5**	DHCP	Unidirectional[3]

[1] When using BACnet protocol with N30s, you must specify UDP Port 47808 as being used. For multiple BACnet networks, use a different port number for each network.

[2] In bidirectional communications, both devices initiate requests.

[3] In unidirectional communication, only the originating device initiates requests (assuming synchronous response is allowed in the request).

NCM legacy network

The following figure is an example of the connectivity and protocols used in a Metasys system using the OWS or M5 Workstation and NCMs. See Figure 8 with Table 6, and Figure 9 with Table 10, for the full set of protocols used by the engine, *Metasys* Server, and Site Management Portal UI.

Figure 11: Metasys System with NCMs

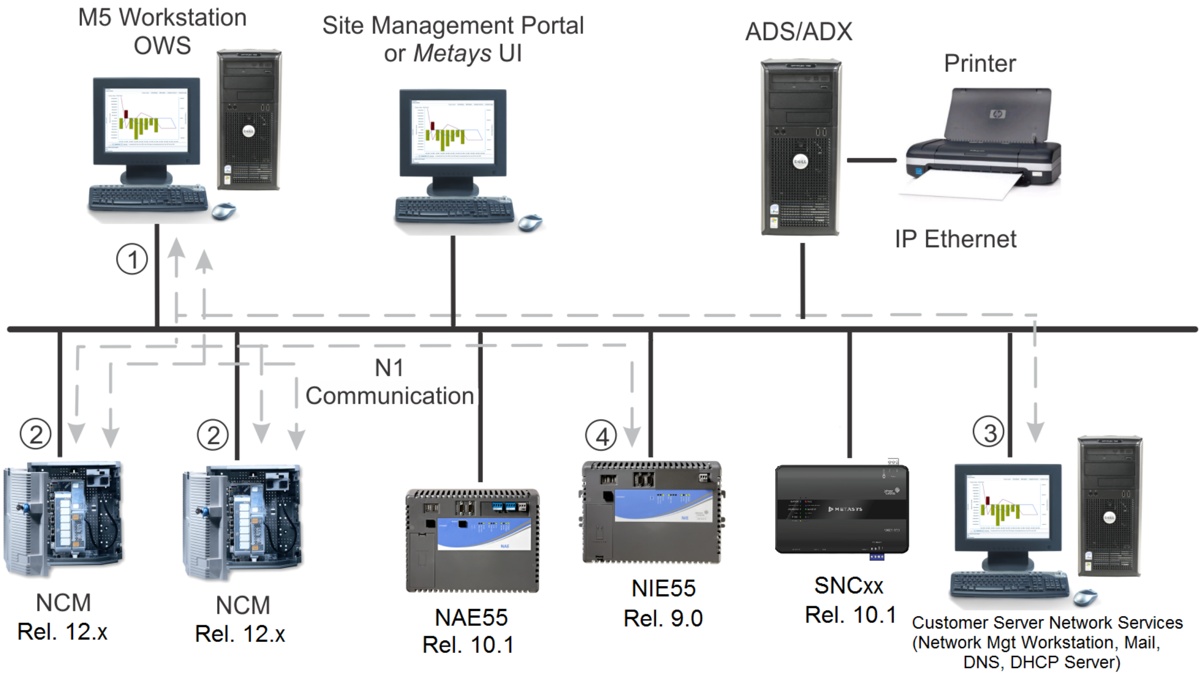


Table 12: Metasys System with NCMs

Interaction between Callouts		Protocol	Communication Direction
1	**2**	N1[1]	Bidirectional[2]
1	**3**	SNMP, SNMP Trap	Unidirectional[3]
2	**2**	N1	Bidirectional
2	**4**[4]	N1	Bidirectional

[1] When using UDP protocol with NCMs, you must specify Port 11001 as being used. For multiple N1 networks, you must use a different port number for each network.

[2] In Bidirectional communications, both devices initiate requests.

[3] In Unidirectional communication, only the originating device initiates requests (assuming synchronous response is allowed in the request).

[4] You can configure multiple N1 networks on the NIE. Refer to the *N1 Migration with NIE Technical Bulletin (LIT-1201535)* for details.

Many-to-one wireless network

The following figure is an example of the connectivity and protocols used in a Metasys network using the Many-to-One Wireless Room Temperature Sensing (WRS) application. The WRS system is supported at Metasys Release 9.0 or earlier.

Figure 12: Metasys System with Many-to-One Wireless Room Temperature Sensing Application (Release 9.0 or earlier)

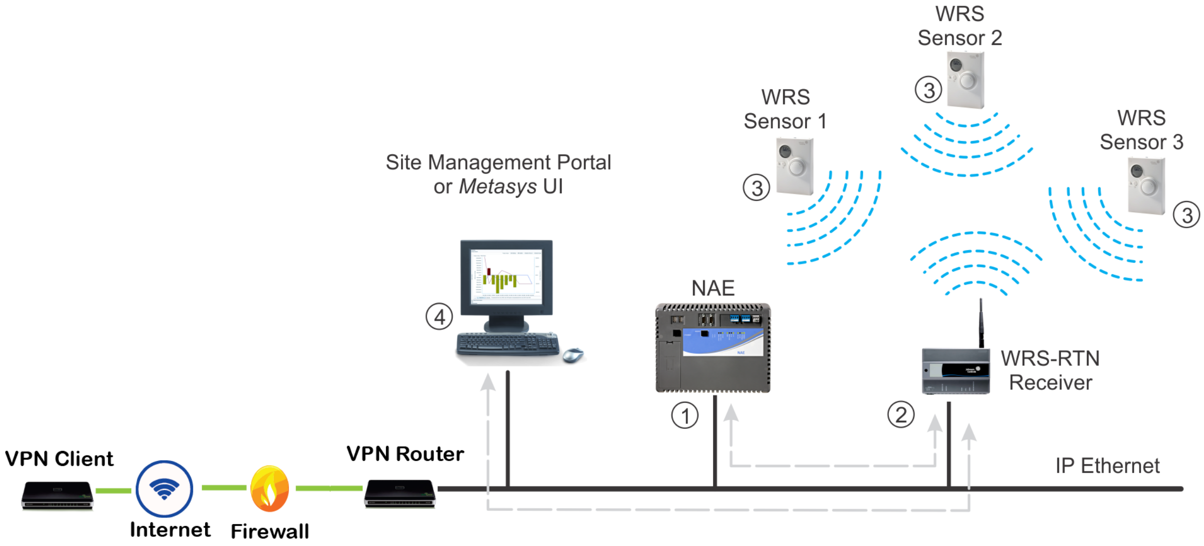


Table 13: Metasys System with Many-to-One Wireless Room Temperature Sensing Application

Interaction between Callouts		Protocol	Communication Direction
1	**2**	Tunneling over Ethernet	Bidirectional
2	**3**	Wireless Many-to-One Sensing (802.15.4)[1]	Bidirectional (2.4 GHz Channelized, 2.4 GHz DSSS Wireless Protocol)
4	**2**	HTTP	Unidirectional[2]

[1] Port 4050 is recommended for the WRS-RTN Receiver.

[2] In Unidirectional communication, only the originating device initiates requests (assuming synchronous response is allowed in the request).

The WRS Series sensors and WRS receivers operate on the 2.4 GHz Industrial, Scientific, Medical (ISM) band and use multi-frequency DSSS technology. The receiver meets the IEEE 802.15.4 standard for low power, low duty-cycle wireless transmitting systems.

The 802.15.4 standard radio is used for employing control networks within a building. This technology uses 16 different channels, allowing 802.15.4 devices, such as the WRS Series systems, to coexist with 802.11 devices.

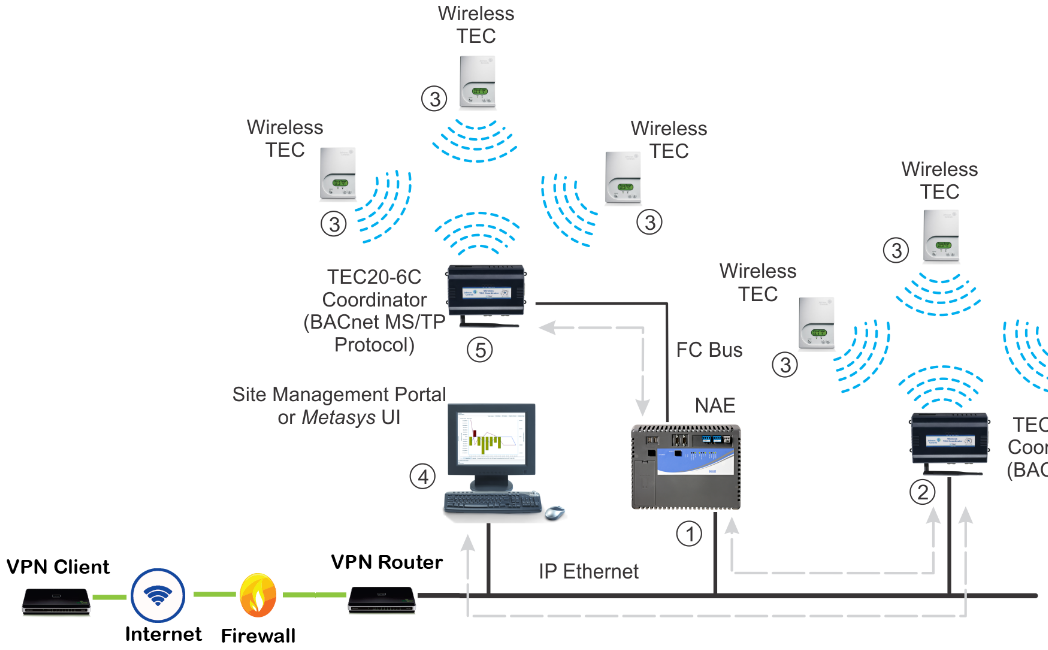
The Many-to-One system use two-millisecond multi-frequency redundant data transmissions. The sensor transmits a rapid sequence of high-speed (two millisecond) redundant data bursts to an associated receiver approximately every 60 seconds. The sensor transmits up to five redundant data bursts in rapid sequence, and each burst is transmitted on a different ZigBee frequency. When a single data burst is successfully received and acknowledged (or if all five redundant data bursts fail), the sensor goes dormant for approximately 60 seconds and then repeats the rapid transmission burst sequence.

Multi-frequency, redundant data-transmission sequences greatly enhance the success of the wireless sensing system data transmissions. Transmitting short, high-speed data bursts at 60-second intervals also reduces wireless data transmission collisions and interference with other Wi-Fi transmissions. The DSSS technology virtually eliminates accidental and unauthorized wireless interference.

TEC Series Wireless Controller network

The following figure is an example of a Metasys network using the TEC Series Wireless Thermostat Controller system.

Figure 13: Metasys Network with TEC Series Wireless Thermostat Controller System (BACnet IP and BACnet MS/TP Versions Shown)



ⓘ **Note:** A system can use either a TEC20-3C-2 Coordinator (BACnet IP) or a TEC20-6C-2 coordinator (BACnet MS/TP), but cannot use both BACnet IP and BACnet MS/TP versions.

Table 14: Metasys Network with TEC Series Wireless Thermostat Controller System

Interaction between Callouts		Protocol	Communication Direction
1	**2**	BACnet IP[1]	Bidirectional
1	**4**	HTTP	Unidirectional[2]
2	**3**	ZigBee Wireless Network (802.15.4)	Bidirectional (2.4 GHz Channelized, 2.4 GHz DSSS Wireless Protocol)

Table 14: Metasys Network with TEC Series Wireless Thermostat Controller System

Interaction between Callouts		Protocol	Communication Direction
4	**2**	HTTP	Unidirectional
1	**5**	BACnet MS/TP	Bidirectional
5	**3**	ZigBee Wireless Network (802.15.4)	Bidirectional (2.4 GHz Channelized, 2.4 GHz DSSS Wireless Protocol)

[1] When using BACnet protocol with TEC20-3C-2s, you must specify UDP Port 47808 as being used. For multiple BACnet networks, use a different port number for each network.

[2] In Unidirectional communication, only the originating device initiates requests (assuming synchronous response is allowed in the request).

The TEC Wireless Thermostat Controller System provides a wireless interface between a network engine and the TEC Wireless Thermostat Controllers, allowing the exchange of BACnet IP (TEC20-3C) or BACnet MS/TP (TEC20-6C) messages for the purpose of wireless monitoring and temperature control of building HVAC equipment.

The system consists of at least one TEC20-3C-2 Coordinator and multiple TEC Wireless Thermostat Controllers. The system uses DSSS wireless technology and operates on the 2.4 GHz ISM band. The system meets the IEEE 802.15.4 standard for low power, low duty-cycle wireless transmitting systems and are compatible with wireless mesh networks compliant with the ZigBee standard. The TEC Thermostat Controllers use a transmission power of 10 dBm.

For general information on the TEC Series Wireless system, refer to the *TEC Series Wireless Thermostat Controller System Technical Bulletin (LIT-12011414)*.

ZFR1800 Series Wireless Field Bus network

The following figure is an example of a Metasys network using the ZFR1800 Series Wireless Field Bus system.

Figure 14: Metasys Network with ZFR1800 Series Wireless Field Bus System

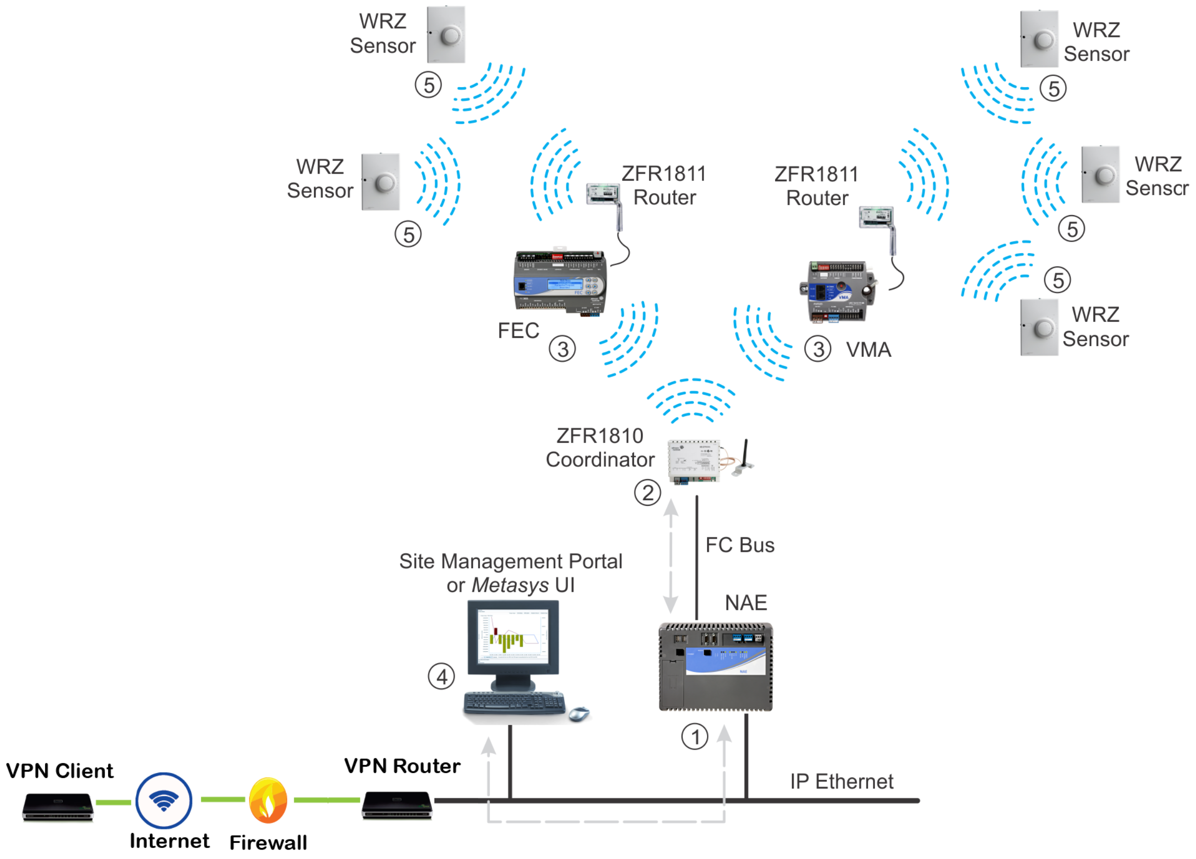


Table 15: Metasys Network with ZFR1800 Series Wireless System

Interaction between Callouts		Protocol	Communication Direction
1	**4**	HTTP	Unidirectional[1]
1	**2**	BACnet MS/TP	Bidirectional
2	**3**	ZigBee Wireless Network (802.15.4)	Bidirectional (2.4 GHz ISM bands, 802.11 b/g/n, 11/22/54 Mbps)
3	**5**	ZigBee Wireless Network (802.15.4)	Bidirectional (2.4 GHz ISM bands, 802.11 b/g/n, 11/22/54 Mbps)

[1] In Unidirectional communication, only the originating device initiates requests (assuming synchronous response is allowed in the request).

The ZFR1800 Series Wireless Field Bus System provides a wireless platform for Metasys field controllers using Johnson Controls Metasys BACnet protocol. The system consists of at least one ZFR1810 Wireless Field Bus Coordinator, connected to a network engine. It also has one or more

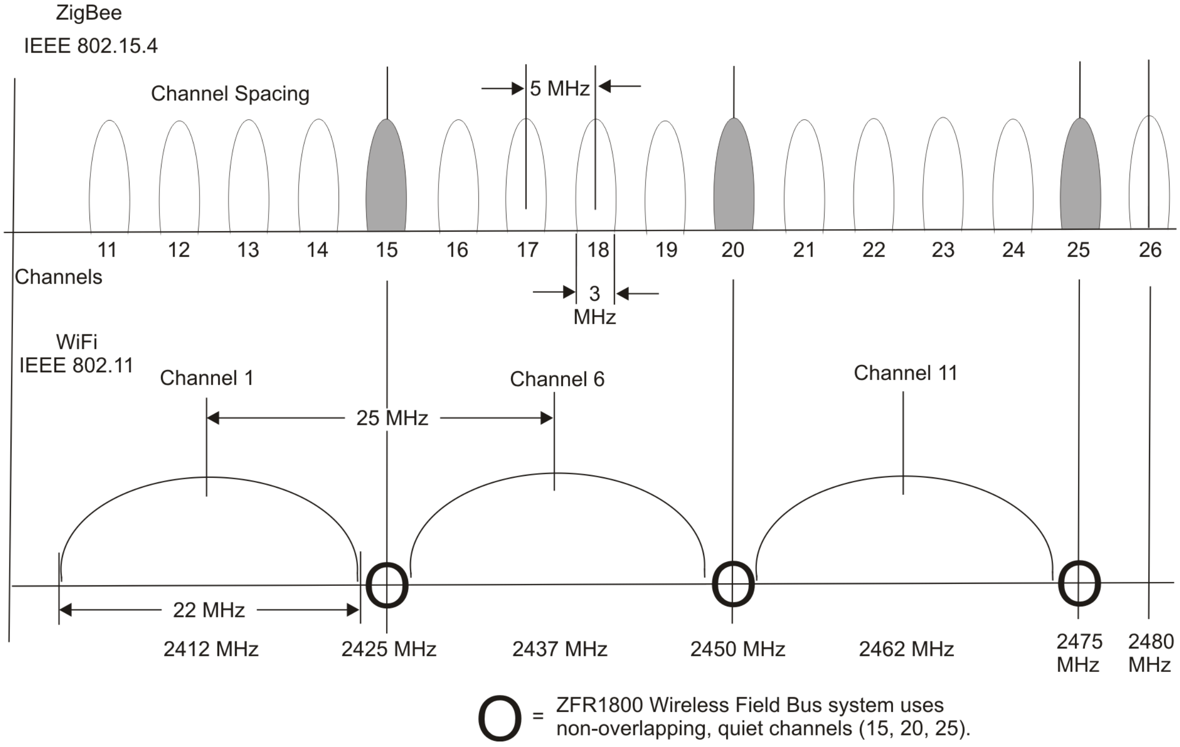
ZFR1811 Wireless Field Bus Routers, each connected to any Metasys BACnet FEC 16, FEC26, FAC26, or VMA16 Series Controller. And lastly, multiple WRZ Series Wireless Room Temperature Sensors (WRZ-TTx) in the system communicate with the routers.

As with the TEC Wireless system, the ZFR1800 Wireless Field Bus system uses DSSS wireless technology and operates on the 2.4 GHz ISM band. The system also meets the IEEE 802.15.4 standard for low power, low duty-cycle wireless transmitting systems and are compatible with wireless mesh networks compliant with the ZigBee standard. For more details on the ZFR1800 Series Wireless system, refer to the *ZFR1800 Series Wireless Field Bus System Technical Bulletin (LIT-12011295)*.

ZigBee channels

A ZigBee network has 16 channels available for use. The TEC Series Wireless Thermostat Controller system and ZFR1800 Series Wireless Field Bus system use only channels 15, 20, and 25. These channels were selected because they do not overlap with channels used on a Wi-Fi network. Figure 15 is a diagram from the *ZFR1800 Series Wireless Field Bus System Technical Bulletin (LIT-12011295)* illustrating that the ZigBee channels do not interfere with the Wi-Fi network.

Figure 15: Comparing Channel Spacing of the Systems Using ZigBee Technology Versus Wi-Fi Networks



Spanning trees

Improperly configured spanning trees cause excessive Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), or Bridge Protocol Data Unit (BPDU) traffic, which causes *Metasys* network engines to reset. Be sure all spanning trees are properly configured.

Field bus considerations

Metasys system devices that connect to Ethernet networks use various field buses to interface with the building control system. Field buses provide direct connections between field devices and the supervisory device that controls them. Field devices/buses do not interact directly with the Ethernet network, but the supervisory devices do interact with the Ethernet network. Possible field buses include the LonWorks network, MS/TP bus, and N2 Bus. For information on the buses supported by specific Metasys system devices, refer to the product literature for each device.

Pre-boot Execution Environment (PXE)

Network engines (excluding the SNE, SNC, NxE85 and LCS85) implement a PXE client. If your network uses a Pre-boot Execution Environment (PXE) server, exclude the MAC address for these devices from the PXE server. If you do not exclude the MAC addresses, these devices may not start up properly.

Network reliability requirement

Communication between the Metasys server and network engines requires a robust and reliable network. If communication throughput is not sufficient or is unreliable, false online and offline alarms from supervisory controllers may occur. In most cases, the controllers report online almost immediately, which is an indication that there is no problem with the controllers.

If they do not report online within a few seconds, or this behavior persists, contact the Johnson Controls technical support for assistance.

Metasys system security considerations

General security recommendations

For general recommendations based on the Best Practices for Enterprise Security document on Microsoft TechNet, follow this link:

http://www.microsoft.com/technet/archive/security/bestprac/bpent/bpentsec.mspx

For the most up-to-date security recommendations, we recommend discussing your site security with your local Johnson Controls field support team. High-level security recommendations include:

- Do not allow cross-frame scripting by setting X-Frame values to Deny or SAMEORIGIN.
- Ensure the appropriate cipher keys exist and are enabled.
- Ensure client and server protocols keys exist are either disabled or enabled depending on guidance from the field support team.

We recommend contacting your local field support to implement these security recommendations.

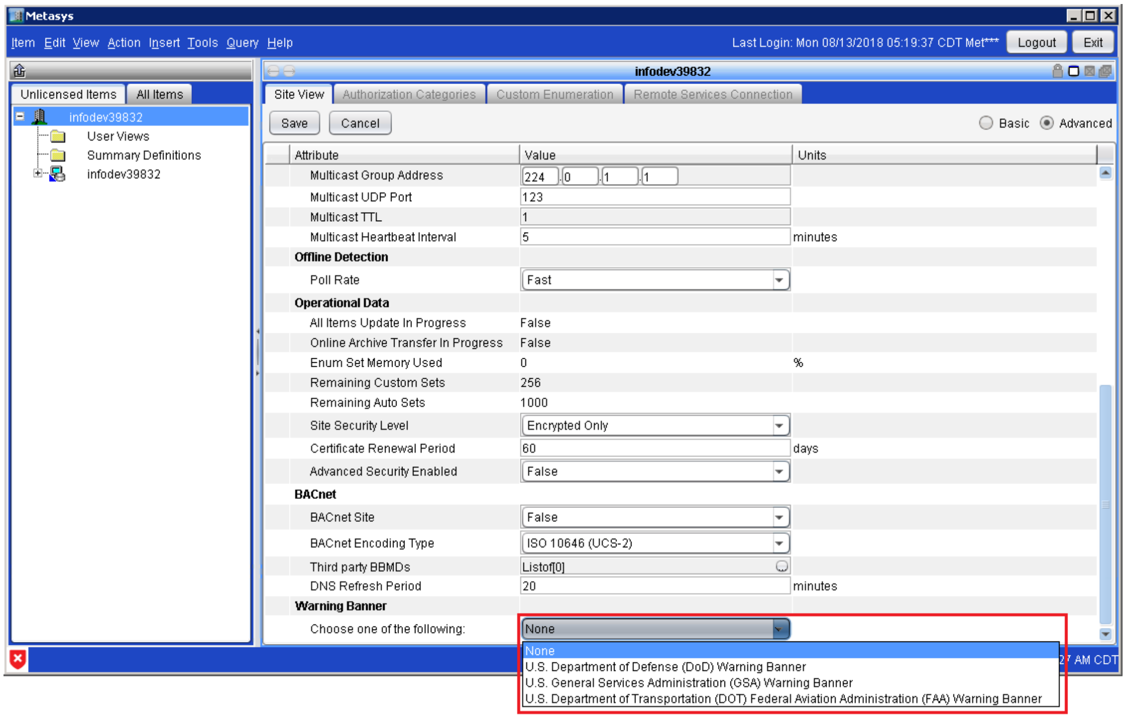
Metasys access security

Warning Banners

The Warning Banner is an optional feature of the Site Management Portal UI. The banner is a specific warning statement that appears every time you launch the SMP UI. To configure this setting, navigate to the Site object of the Site Director and click the **Site View** tab. In the **Warning Banner** section, select one of the following (Figure 16):

- U.S. Department of Defense (DoD) Warning Banner
- U.S. General Services Administration (GSA) Warning Banner
- U.S. Department of Transportation (DOT) Federal Aviation Administration (FAA) Warning Banner

Figure 16: Warning Banner Selection List on Site Object



Attribute	Value	Units
Multicast Group Address	224 . 0 . 1 . 1	
Multicast UDP Port	123	
Multicast TTL	1	
Multicast Heartbeat Interval	5	minutes
Offline Detection		
Poll Rate	Fast	
Operational Data		
All Items Update In Progress	False	
Online Archive Transfer In Progress	False	
Enum Set Memory Used	0	%
Remaining Custom Sets	256	
Remaining Auto Sets	1000	
Site Security Level	Encrypted Only	
Certificate Renewal Period	60	days
Advanced Security Enabled	False	
BACnet		
BACnet Site	False	
BACnet Encoding Type	ISO 10646 (UCS-2)	
Third party BBMDs	Listof[0]	
DNS Refresh Period	20	minutes
Warning Banner		
Choose one of the following:	None	

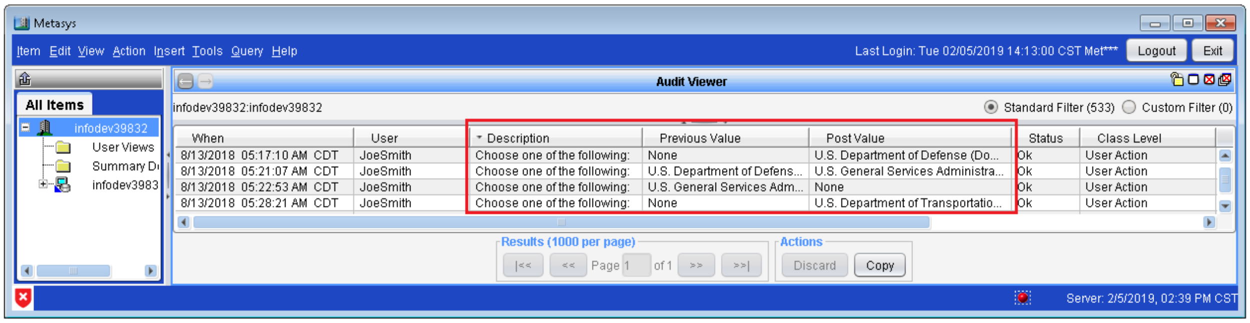
None
U.S. Department of Defense (DoD) Warning Banner
U.S. General Services Administration (GSA) Warning Banner
U.S. Department of Transportation (DOT) Federal Aviation Administration (FAA) Warning Banner

Once enabled, the Warning Banner you selected appears for all local and Active Directory service users when they log in to the SMP UI of either a Metasys Server or network engine. All local and Active Directory users must agree to the conditions on the warning statement before access is granted.

Notes:

- After you change the warning banner, the change can take up to five minutes to activate on all network engines that report to the Site Director, because the Site Director needs time to initiate the change to all its child devices.
- Whenever an operator changes the Warning Banner selection, an entry is sent to the audit log and appears in the Audit Viewer (Figure 17).
- The Warning Banner does not appear before you log in to the Metasys Advanced Reporting System, SCT UI, Metasys UI, Metasys UI Offline, or LonWorks® Control Server (LCS85).
- The only method for removing the Warning Banner from the login process is to set the Warning Banner attribute on the Site object to **None**. The Warning Banner attribute is stored in the device archive. If you download the Metasys Server from an archive that has been uploaded with the banner option enabled, the banner appears.

Figure 17: Warning Banner entry in Audit Viewer


Metasys
Item Edit View Action Insert Tools Query Help
Last Login: Tue 02/05/2019 14:13:00 CST Met***
Logout
Exit
All Items
infodev39832
User Views
Summary D
infodev3983
Audit Viewer
Results (1000 per page)
|<< << Page 1 of 1 >> >>|
Actions
Discard
Copy
Server: 2/5/2019, 02:39 PM CST

infodev39832:infodev39832

● Standard Filter (533) ○ Custom Filter (0)

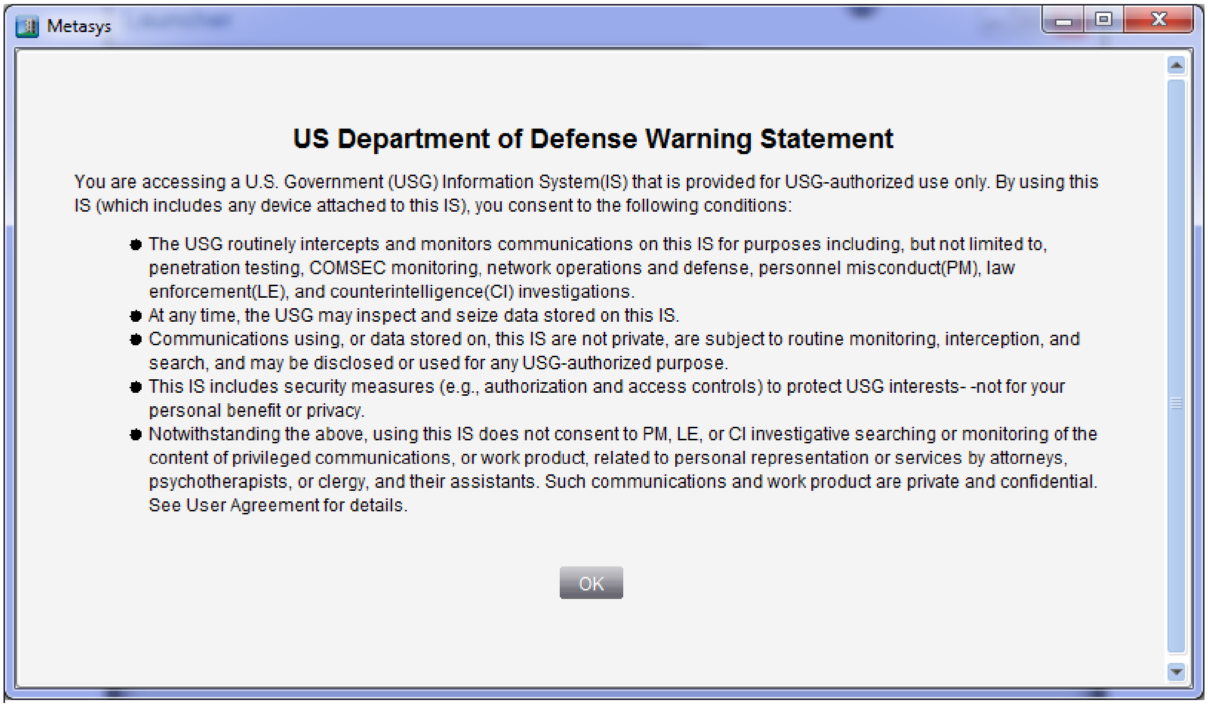
When	User	Description	Previous Value	Post Value	Status	Class Level
8/13/2018 05:17:10 AM CDT	JoeSmith	Choose one of the following:	None	U.S. Department of Defense (Do...	Ok	User Action
8/13/2018 05:21:07 AM CDT	JoeSmith	Choose one of the following:	U.S. Department of Defens...	U.S. General Services Administra...	Ok	User Action
8/13/2018 05:22:53 AM CDT	JoeSmith	Choose one of the following:	U.S. General Services Adm...	None	Ok	User Action
8/13/2018 05:28:21 AM CDT	JoeSmith	Choose one of the following:	None	U.S. Department of Transportatio...	Ok	User Action

When the Metasys system login screen appears, you have up to 30 seconds to log in. If 30 seconds passes with no user activity, the login screen closes and the Warning Banner screen returns. The Warning Banner also reappears after you log out of the Metasys system or the system logs you out because of user inactivity.

The Warning Banner remains on the screen until either you click **OK**, **I AGREE**, or you manually close the banner window. The banner does not close on its own.

Figure 18 is a representation of the Warning Banner that appears if you have selected the U.S. Department of Defense (DoD) Warning Banner.

Figure 18: United States DoD Warning Banner



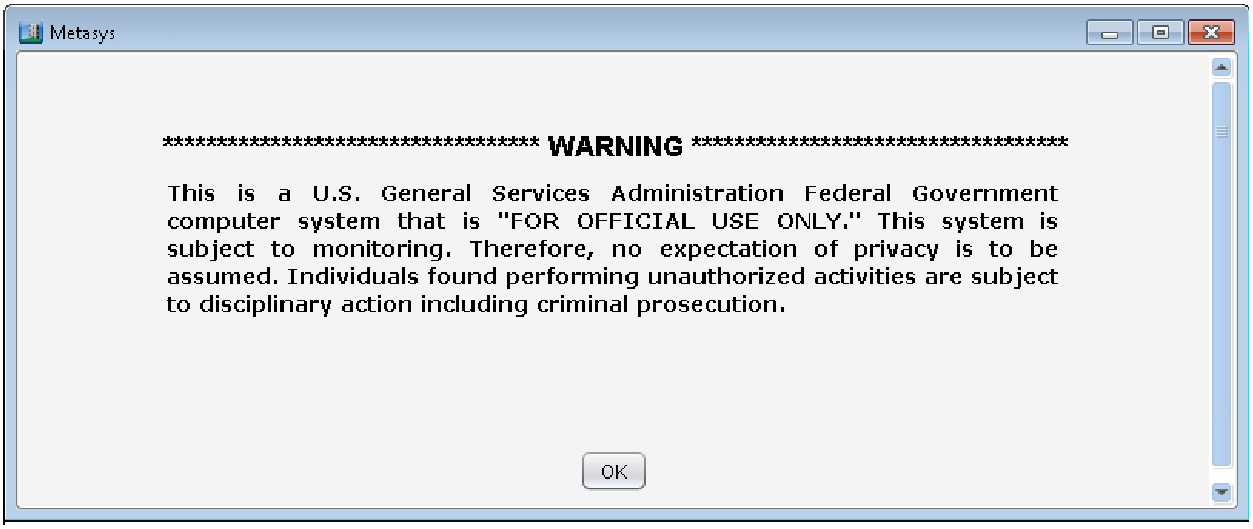
US Department of Defense Warning Statement

You are accessing a U.S. Government (USG) Information System(IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct(PM), law enforcement(LE), and counterintelligence(CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
- This IS includes security measures (e.g., authorization and access controls) to protect USG interests- -not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not consent to PM, LE, or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Figure 19 is a representation of the Warning Banner that appears if you have selected the U.S. General Services Administration (GSA) Warning Banner.

Figure 19: U.S. GSA Warning Banner

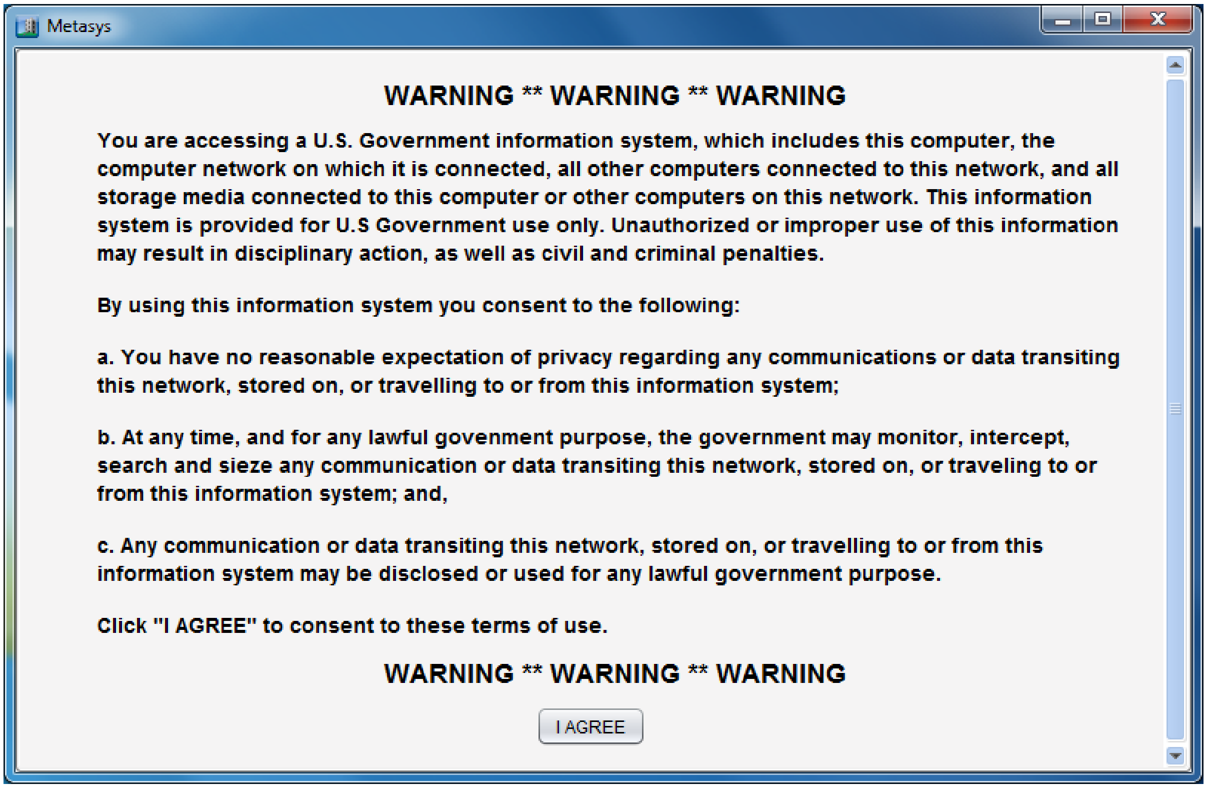


************************************ WARNING ************************************

This is a U.S. General Services Administration Federal Government computer system that is "FOR OFFICIAL USE ONLY." This system is subject to monitoring. Therefore, no expectation of privacy is to be assumed. Individuals found performing unauthorized activities are subject to disciplinary action including criminal prosecution.

Figure 20 is a representation of the Warning Banner that appears if you have selected the U.S. Department of Transportation (DOT) Federal Aviation Administration (FAA) Warning Banner.

Figure 20: U.S. DOT/FAA Warning Banner



WARNING ** WARNING ** WARNING

You are accessing a U.S. Government information system, which includes this computer, the computer network on which it is connected, all other computers connected to this network, and all storage media connected to this computer or other computers on this network. This information system is provided for U.S Government use only. Unauthorized or improper use of this information may result in disciplinary action, as well as civil and criminal penalties.

By using this information system you consent to the following:

a. You have no reasonable expectation of privacy regarding any communications or data transiting this network, stored on, or travelling to or from this information system;

b. At any time, and for any lawful govenment purpose, the government may monitor, intercept, search and sieze any communication or data transiting this network, stored on, or traveling to or from this information system; and,

c. Any communication or data transiting this network, stored on, or travelling to or from this information system may be disclosed or used for any lawful government purpose.

Click "I AGREE" to consent to these terms of use.

WARNING ** WARNING ** WARNING

Users

The Metasys system has two types of users: local users and Active Directory service users. A local user is defined in the Security Administrator system and is authenticated and authorized against the Metasys Security database. An Active Directory service user is created and stored in an Active Directory service domain and is added as a Metasys system user with the Security Administrator

System. This user is authenticated against an Active Directory service domain and authorized against the Metasys system.

Once logged in, the user is limited to actions that are permitted by the user’s assigned privileges. Refer to the *Security Administrator System Technical Bulletin (LIT-1201528)* for specific details on Metasys system access security.

Metasys system local user accounts and passwords

The user name and password are part of a Metasys local user account that controls which actions a user can perform and which parts of the system a user can see, among other access controls.

Standard policy settings apply to a Metasys system local user account: password expiration/reset, session timeout, lockout after failed attempts, and password uniqueness. You also can set the times of day a user may access the system.

Active Directory service – user accounts

Actions of an Active Directory service user within the Metasys system are controlled in the same manner as a Metasys local user, through assigned privileges. The data store for user privileges is a SQL Server database on computer/server platforms (Metasys server and SCT). For Active Directory service users, account policy settings – including maximum password age, account lockout, password uniqueness, and password complexity – are controlled outside of the Metasys system by the Active Directory service domain server. These settings are shaded when displayed in the Security Administrator System window. The Session Timeout attribute is one exception.

Default Administrator accounts

The MetasysSysAgent and Standard Access accounts, both Metasys local accounts, are the default Administrator accounts. These accounts cannot be renamed or deleted from the system. The MetasysSysAgent account retains full administrative rights, and these rights cannot be changed. The Standard Access account retains a subset of administrative rights, in that Standard Access administrators can administer only user accounts that have been assigned the **Standard Access** access type.

➤ **Important:** The first time you log in with the MetasysSysAgent account using the new default password, or the Standard Access account with the original default password, the system prompts you to change the password immediately. This new behavior enhances the overall security of the Metasys system. For details about the new default password, contact your local Johnson Controls representative.

Metasys system local user name and password pairs are stored only in the system proprietary user store, with one exception. For engines, excluding the NxE85 and LCS85, the MetasysSysAgent account is also mirrored in the operating system as a Windows account with full administrative privileges. The password of the MetasysSysAgent operating system account is controlled by the resetting of the MetasysSysAgent account through the Site Management Portal UI. Changing the account password in the Metasys system also changes the Windows operating system account password in the supervisory controller.

For the server-based network engines at Release 4.0 or later, the NIE89, and the LCS85, the MetasysSysAgent account on the Windows operating system is not linked to the MetasysSysAgent account on the Site Management Portal UI. Changing the account password in the Metasys system does not change the Windows operating system account password. The passwords are independent.

ⓘ **Note:** The Windows operating system accounts and Metasys system local accounts never have been linked on the Metasys server.

For information on hardware-based network engines operating system security, see Security on hardware-based Network Engines.

Password complexity

Complex passwords for Metasys local accounts at Release 7.0 and later are mandatory for all Metasys IP devices and for all user accounts in accord with the language locale that is selected on the computer. For details on complex passwords, refer to the *Security Administrator System Technical Bulletin (LIT-1201528)*.

The following table lists the password rules enforced by the Metasys system user's language_locale setting.

Table 16: Metasys System Password Rules

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

Table 16: Metasys System Password Rules

Supported Language_Locale	Enforced Password Rules
Chinese Simplified (zh_cn) Chinese Traditional (zh_tw) Japanese (ja_jp) Korean (ko_kr)	• 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 two of the following conditions: - Include at least one number (0–9) - Include at least one special character (-, ., @, #, !, ?, $, %) - Include at least one uppercase character - Include at least one lowercase character - Include at least one Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase

Password rules are not applicable to Active Directory users. These users are handled by the domain controller and not by the Metasys system.

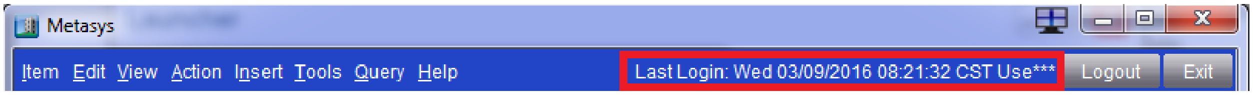
Last login

The main screen of the Metasys server or SCT user interface indicates the last time and date that the user successfully logged in. For enhanced security, only the first three letters of the user's name appear, followed by three asterisks (for example, Use***). If the user has never logged in, **Never** appears in the **Last Login** field. (See Figure 21 and Figure 22.)

➤ **Important:**

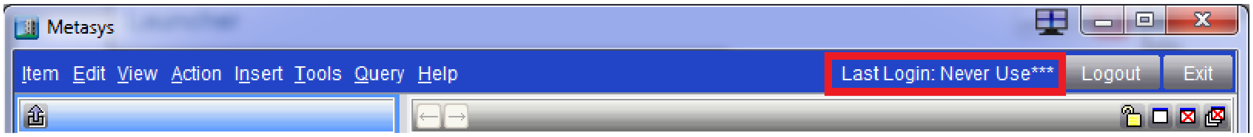
To preserve the current configuration for all Metasys system users, including last login time, always upload the device into the SCT before making changes and downloading a database. User configuration information is stored in the Security database. The Security database is restored during a device download. When an older archive is downloaded into the device, the most recent user password, properties, and login time are lost.

Figure 21: User's last login



Last Login: Wed 03/09/2016 08:21:32 CST Use***

Figure 22: User never logged in



Last Login: Never Use***

Auditing

The Metasys system offers user action auditing within the system. In other words, the software can trace each action back to the logged in user who performed the action, and list that information in the Audit Viewer. For Active Directory service users, the name recorded is the fully qualified user name (for example, **myuser@division.company.com**).

Audits are written to a proprietary data store of the Metasys system, which is a SQL Server database on computer/server platforms (Metasys Servers, including ADS/X, OAS, ODS, NxE85, and LCS85) and an XML-based file on the other engine platforms. Audits may be viewed using the Audit Viewer in the Site Management Portal UI.

Device

Intra-computer Metasys system local accounts are used to perform authentication and authorization among devices within the Metasys system. An intra-computer account is a Metasys system site account, which means the account resides in the same proprietary user store as the other Metasys users. The intra-computer account cannot be administered and cannot be used to log in to the system through the Site Management Portal UI. The intra-computer account uses a generated password that is programmatically changed once a day. Active Directory service accounts are not used for intra-computer accounts.

Network message security

Metasys software offers secured authentication challenges at login. After login, the Metasys software authenticates each SOAP message at the receiving engine. Within each encrypted SOAP message header, protection from message spoofing, message replay, and message tampering is provided.

SQL database security

The Metasys server SQL Server databases are secured using SQL Server authentication.

SQL Server software accounts used by Metasys software can be end-user defined on the Metasys server platform. Added security is possible if you separate the database server function of the ADX from the web/application server function of the ADX. In this scenario, the database server portion of the ADX can reside in a different DMZ from the web/application server portion of the ADX.

SCT is configured to use virtual service account credentials to access the SQL Server databases. The service accounts have been configured with the level of permissions required to perform the actions used by the application. Windows authentication is more secure than database authentication, as it uses a certificate based security mechanism. Windows authenticated logins pass an access token, containing a unique security ID for the user, on login. Windows authentication also means that there is no required maintenance of user passwords and accounts, as all account maintenance is handed by the Windows operating system.

Security on hardware-based Network Engines

The operating system of the hardware-based network engines, such as NAEs, SNEs, and SNCs, is secured using an account in the controller's embedded operating system. This account is the MetasysSysAgent account and is the only Windows account located on these devices. The account has administrative privileges and the password can be changed by logging in to the device directly with the Site Management Portal UI and resetting the password of the MetasysSysAgent user.

Many of the operating system features not required by Metasys software have been removed from the network engines, rendering them less vulnerable to operating system attack.

Security updates management

A Johnson Controls engineering team regularly evaluates newly released Microsoft security updates ranked Critical or Important for their effect on the Metasys system. The results of the update analysis can be obtained from Johnson Controls technical support.

For Metasys system engines, we send out applicable security updates through our support channels with instructions for applying them. For the computer-based components of the Metasys system (Metasys server, NxE85, and LCS85), we recommend that you apply Microsoft security updates and hotfixes as soon as they are released by the Microsoft Corporation.

To ensure higher security for the Site Management Portal, a private JRE is required at Release 6.0 or later that provides isolation between Metasys software and the Internet. The public Java® Runtime Environment (JRE) that was required at earlier Metasys software releases is no longer necessary for Release 6.0 or later, but it is still a requirement for any older release of Metasys software. The Launcher puts down the private JRE required by Release 6.0 or later. You install it when you first browse to the Site Management Portal UI from a client computer or when you newly install Metasys system software. Thereafter, you use the Launcher to access the Site Management Portal UI. Refer to the *Launcher Installation Guide (LIT-12011783)* for instructions about how to install the Launcher application.

ⓘ **Note:** If you use any applications from a release prior to Release 6.0 or later, you **must** continue to use the public JRE required for that particular software release.

Changing Remote Desktop settings

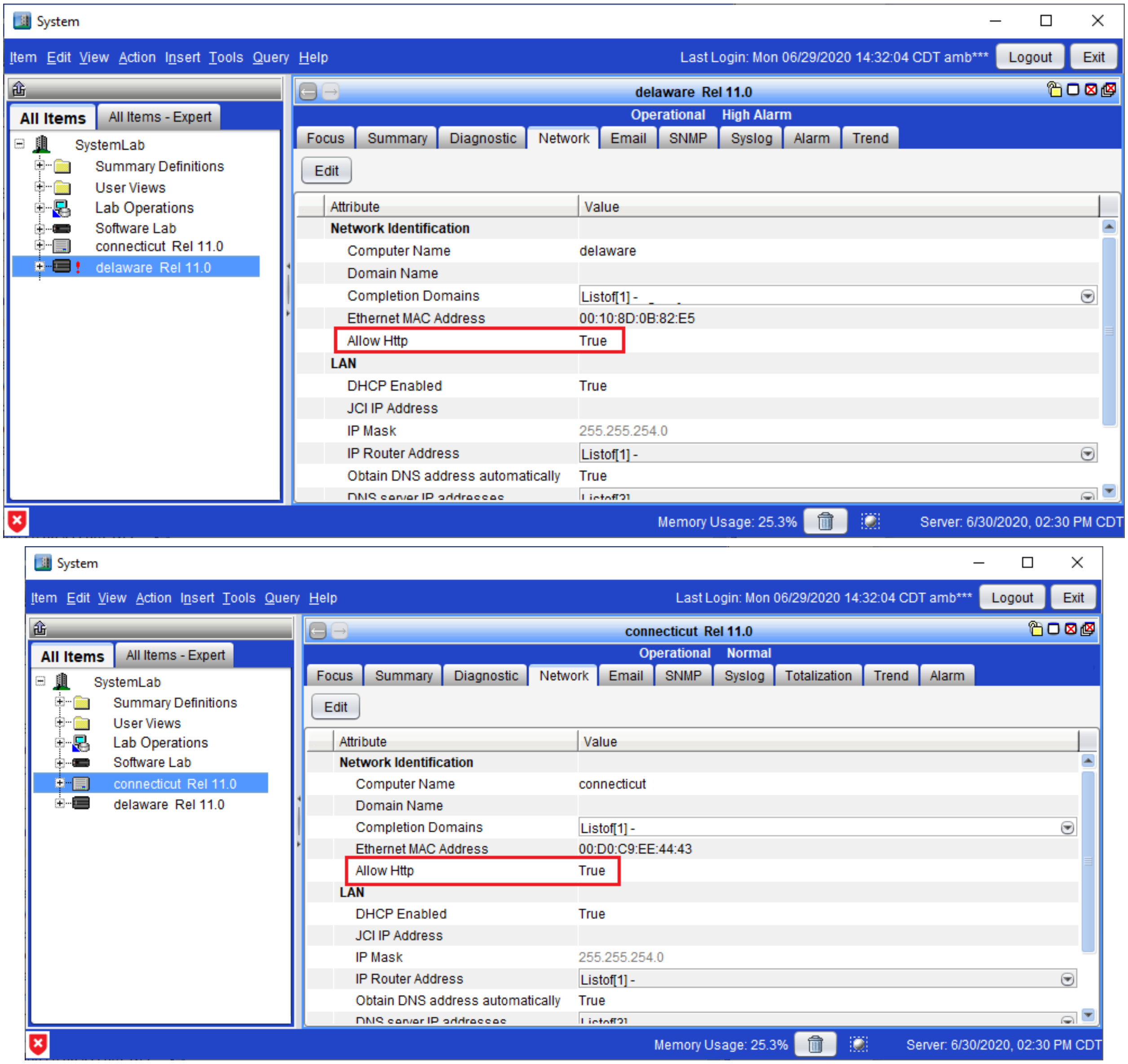
About this task:
For sites requiring remote access to devices, including Metasys servers, we recommend changing the Remote Settings on the device to allow connections only with Network Level Authentication. Use the following steps to change the setting on the device.

1. On the host computer, go to ***Control Panel*** > ***System*** > ***Remote Settings***. The System Properties window appears.
2. In the Remote Desktop section, select **Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)**.
3. Click **OK**.

Allow HTTP

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

Figure 23: Allow Http attribute for network engine



Attribute	Value
Network Identification	
Computer Name	delaware
Domain Name	
Completion Domains	Listof[1] -
Ethernet MAC Address	00:10:8D:0B:82:E5
Allow Http	True
LAN	
DHCP Enabled	True
JCI IP Address	
IP Mask	255.255.254.0
IP Router Address	Listof[1] -
Obtain DNS address automatically	True
DNS server IP addresses	Listof[2]

Attribute	Value
Network Identification	
Computer Name	connecticut
Domain Name	
Completion Domains	Listof[1] -
Ethernet MAC Address	00:D0:C9:EE:44:43
Allow Http	True
LAN	
DHCP Enabled	True
JCI IP Address	
IP Mask	255.255.254.0
IP Router Address	Listof[1] -
Obtain DNS address automatically	True
DNS server IP addresses	Listof[2]

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

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

Table 17: Port 80 requirements for tools, utilities, and features

Item	Does it require Port 80	Notes
Advanced Graphics Application (AGA)	Yes	Uses an older version of Metasys data access services that requires http.
Advanced Reporting and Energy Essentials	Yes	Uses http for communication with engines.
CCT	Yes	Uses an older version of Metasys data access services that requires http. However, CCT only requires Port 80 for upload and download operations.
Graphic Generation Tool (GGT)	Yes	Uses an older version of Metasys data access services that requires http.
Launcher 1.7	No	Uses https for communication with engines upgraded to Release 8.1 or later, but must be set for http to communicate with engines prior to Release 8.1.
Metasys Export Utility	Yes	Uses an older version of Metasys data access services that requires http.
Metasys for Validated Environments (MVE)	No	Uses https for communication with engines upgraded to Release 8.1 or later.
Metasys UI	No	Uses https for communication with engines upgraded to Release 8.1 or later.
NAE Configuration and Information Tool (NCT)	Yes	Requires port 80 for sending a file to an engine from the commissioning laptop.
NAE Update Tool	Yes	**Allow Http** is set to Requires port 80 to successfully perform a code download to the engine using the HTTP update method. If **False**, the NAE Update Tool temporarily opens port 80 for its operations, then closes the port after the download completes.
P2000	Yes	Requires port 80 (inbound) to be open on the Windows Firewall of the Metasys server.
Ready Access Portal	Yes	Uses https between the Ready Access Portal server and the client, but http between the Ready Access Portal server and the engines. ⓘ **Note:** Ready Access Portal is **no longer** supported at Release 9.0 or later.
SMP	No	Uses https for communication with engines upgraded to Release 8.1 or later.
SCT	No	Uses https for communication with field controllers and engines upgraded to Release 8.1 or later.

Advanced security enabled

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

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

When you change this attribute to **True**, a user message appears to indicate that all network engines prior to Release 10.0 remain online, but are disconnected from the site because they no longer communicate with the Site Director. If this message appears, click **OK** to continue and set the attribute to **True**, or **Cancel** to keep the attribute set to **False**. An entry to the Audit Viewer occurs whenever someone changes the Advanced security enabled attribute.

Software time bomb

Metasys software does not have a software time bomb to disable the system. Instead, a software license manager controls access to Metasys software. Software registration is mandatory after you install any Metasys application or tool. To register the software, you use a product called Software Manager and a website called the Johnson Controls License Portal. On first use of the software, the Software Manager opens for you to register the product. Log in is prevented until you have successfully registered the product. For details, refer to *Software Manager Help (LIT-12012389)*.

Antivirus software considerations (*Metasys* server, NxE85, NIE89, and LCS85 only)

Frequent virus scans of the *Metasys* server, NxE85, NIE89, and LCS85 are necessary to maintain the integrity of your system. We support virus scans on computer-based and server platform-based *Metasys* system components only (*Metasys* server, NxE85, NIE89, and LCS85). The hardware-based network engines and other *Metasys* system components not running on a computer do not support virus scans; however, many of the operating system features not required by *Metasys* software have been removed from the engines, rendering them less vulnerable to operating system attacks.

We have tested the *Metasys* server, NxE85, NIE89, and LCS85 successfully with the following antivirus software programs:

- Symantec AntiVirus Corporate Edition 12.0 or later.

  ⓘ **Note:** Symantec® Endpoint Protection software Corporate Edition version 12.0 or later is recommended for the NxE85 and LCS85.

- McAfee® VirusScan® Enterprise version 8.8 with Patch 9.

For details, see Appendix: Installing antivirus software.

Secure Sockets Layer (SSL)/Transport Layer Security (TLS)

The Metasys Advanced Reporting System, Metasys UI, and the Metasys UI Offline are the Metasys system offerings that support security certificates. We recommend that you implement SSL security for improved protection. SSL or TLS certificates may be used with the Metasys UI and Metasys UI Offline.

Implementing SSL security for the Metasys Advanced Reporting System

ⓘ **Note:** Make sure that you enable and configure proper certificate revocation, such as Online Certificate Status Protocol (OCSP) stapling. For more information about OCSP configuration refer to https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-ocsp/5792b4c4-c6ba-439a-9c2a-52867d12fb66.

To implement SSL security for the Metasys Advanced Reporting System:

1. Generate a certificate request and install the certificate.
    1. For more information on these steps, see the following address:
       http://technet.microsoft.com/en-us/library/cc771438(WS.10).aspx
2. Configure the Metasys software to use HTTPS (SSL) and HTTP protocols on the computer where you plan to install the reporting system.

    a. In Control Panel, select **System and Security**, then **Administrative Tools**. On Administrative Tools, double-click **Internet Information Services (IIS) Manager**.

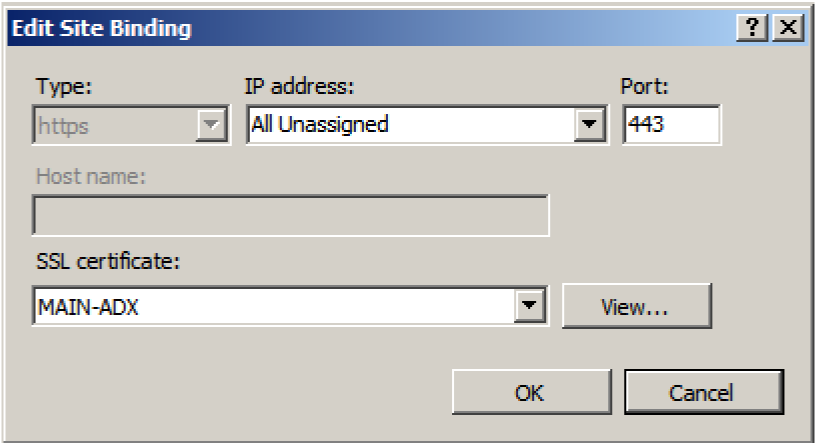
    b. In the tree in the left pane, browse to and expand **Sites** or **Web Sites**.

    c. In the right pane, right-click Default Web Site and select **Edit Bindings**. The Site Bindings box appears.

    d. Click **Edit**. Verify that the **SSL port** field contains 443 (Figure 24).

    ⓘ **Note:** Port 80 must be open on the ADX for communication from other system devices. Verify that the TCP port entry is 80.

Figure 24: SSL Port Field: 443



Type: https

IP address: All Unassigned

Port: 443

Host name:

SSL certificate: MAIN-ADX

e. Click **OK**.

f. Close the IIS Manager window.

g. Install the ADX/ODS software with Metasys Reporting.

h. Using Windows Explorer, browse to: `C:\Program Files (x86)\Johnson Controls \MetasysIII\UI\com\jci\framework`

i. Using a text editor, open **frameworkproperties.properties**.

j. Update the advancedReportingURL setting line to use **https:** instead of **http:** so it appears like the following:

```
advancedReportingURL=https://SERVERNAME/MetasysReports
```

k. Save the file.

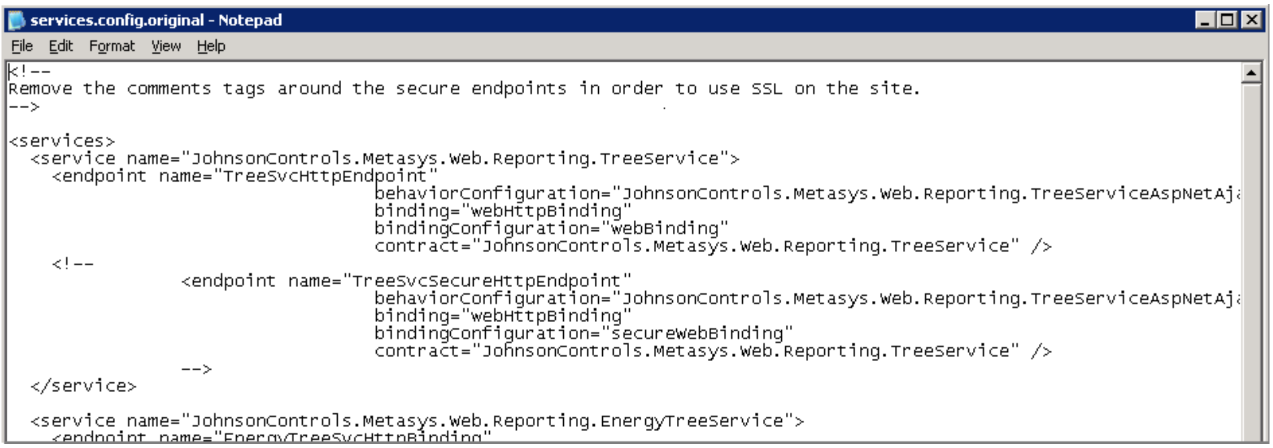
l. Using Windows Explorer, browse to: `C:\Program Files (x86)\Johnson Controls \MetasysReports`

m. Using a text editor, open **services.config**.

n. Delete the comment tags from the file. Comment markers appear as `<!-- and -->` (Figure 25).

Note: Do not delete the text between the comment tags. Delete all three sets of comment tags that appear in the file.

Figure 25: Comment Tags



services.config.original - Notepad

```
<!--
Remove the comments tags around the secure endpoints in order to use SSL on the site.
-->

<services>
  <service name="JohnsonControls.Metasys.Web.Reporting.TreeService">
    <endpoint name="TreeSvcHttpEndpoint"
                                  behaviorConfiguration="JohnsonControls.Metasys.Web.Reporting.TreeServiceAspNetAj
                                  binding="webHttpBinding"
                                  bindingConfiguration="webBinding"
                                  contract="JohnsonControls.Metasys.Web.Reporting.TreeService" />
    <!--
                <endpoint name="TreeSvcSecureHttpEndpoint"
                                  behaviorConfiguration="JohnsonControls.Metasys.Web.Reporting.TreeServiceAspNetAj
                                  binding="webHttpBinding"
                                  bindingConfiguration="secureWebBinding"
                                  contract="JohnsonControls.Metasys.Web.Reporting.TreeService" />
                -->
  </service>

  <service name="JohnsonControls.Metasys.Web.Reporting.EnergyTreeService">
    <endpoint name="EnergyTreeSvcHttpBinding"
```

o. Save the file.

p. Close all Windows Explorer windows.

q. On the Start menu, in the Run text box, type **regedit**.

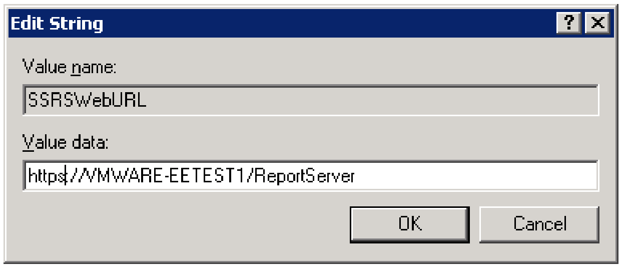
r. Click **OK**. The Registry Editor window appears.

s. In the tree on the left, browse to ***HKEY_LOCAL_MACHINE*** > ***Software*** > ***Johnson Controls*** > ***Metasys*** > ***ADS***.

t. On the right side of the screen, double-click **SSRSWebURL**. The Edit String box appears.

u. In the Value data field, add an **s** after **http**. The value should be: http**s**://(ADx Server Name)/ReportServer (Figure 26).

Figure 26: Edit String Box



Edit String

Value name: SSRSWebURL

Value data: https://VMWARE-EETEST1/ReportServer

v. Click **OK**.

w. Close the Registry Editor.

3. Restart the computer.
4. Log in to the Metasys Advanced Reporting System UI.
5. The UI should open correctly and the URL in the browser window should have the **https:** prefix.

Metasys for Validated Environments (MVE)

Metasys for Validated Environments (MVE) is an enhanced feature of the Metasys system that audits user management for critical environments to facilitate U.S. Food and Drug Administration

(FDA) electronic records and signature requirements (Title 21 Code of Federal Regulation [CFR] Part 11). MVE is also compliant with other similar agencies around the world that deal with electronic records and electronic signature requirements, such as Annex 11 of the European Union Good Manufacturing Practice (EU GMP) regulations (European Medicines Agency [EMEA] 1998).

MVE provides secure data management and reporting capabilities, traceable electronic records and signatures, and time-stamped audit trails for facilities subject to Part 11 compliance. Any action or change initiated by the user on a validated device, such as alarm acknowledgment or setpoint adjustment, requires user reauthentication and electronic signature with required annotation.

MVE can be used only on an ADX running Metasys system supported server-based operating systems. The ADX software, MVE software, and network engines at the MVE site must each be at the **same** Metasys release level, for example, Release 11.0. MVE supports access by Active Directory service users of the Metasys system from the standard login screen. SSO access is not supported because SSO is disabled for MVE installed on an ADX.

ⓘ **Note:** To use SQL Server 2014 with Metasys products, you must install Microsoft cumulative update package 3 (KB2984923) for SQL Server 2014. To download the update package, visit http://support.microsoft.com/kb/2984923/.

For more information, refer to the *Metasys for Validated Environments, Extended Architecture Technical Bulletin (LIT-12011327)*.

Metasys server considerations

ADX-specific features

See the Metasys for Validated Environments (MVE) and Metasys Advanced Reporting System UI sections for information on these two features that are available only on ADXs with specific components installed.

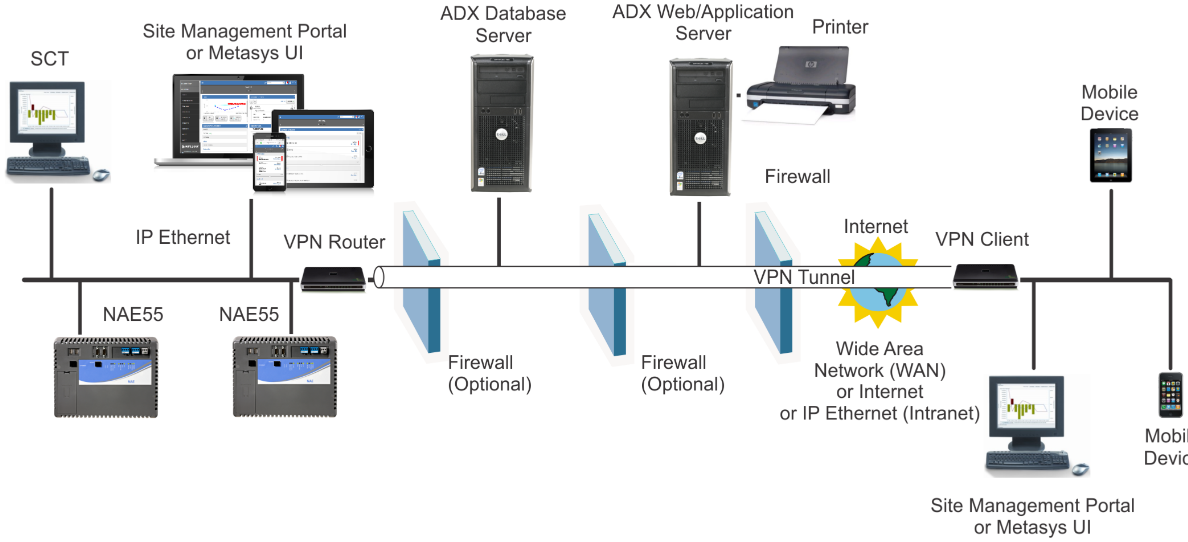
ADX split configuration

The ADX software and its associated database software are often installed on one computer (a unified ADX). However, the ADX also can be installed in a split configuration, which involves installing ADX-related software on two computers. Splitting provides enhanced security for historical data. Using the ADX in a split configuration allows you to locate the Metasys system databases behind a firewall, which reduces the risk of exposing Metasys system data to unauthorized users on the Internet. The split configuration also allows you to locate Metasys system databases on an existing SQL Server computer using existing resources (hardware, software, and technical personnel), potentially lowering the cost of installing and monitoring the Metasys system.

In an ADX split configuration, the computer running SQL Server software is known as the database server computer, and it stores historical Metasys system data. The ADX software itself and all required ADX prerequisites reside on a second computer, known as the web/application server computer. In a split configuration, the SCT must reside on a third computer. Users browse to the web/application server computer to see system data. The database server computer cannot be used as a historical data repository by more than one web/application server computer.

Metasys Network with an ADX

Figure 27: Metasys Network with an ADX in Split Configuration



ⓘ **Note:** Cloud-based applications are not available for all sites.

ADSADX log folder

The **ADSADX Log** folder in the Windows Event Viewer on the *Metasys* Server contains information related to specific Metasys server software failures or important events. The messages appear in English only.

ⓘ **Note:** In a split ADX, this folder is on the web/application server computer.

The following events may appear in the **ADSADX Log** folder:

- The Metasys server software has a failure initializing any subsystem during startup.
- The Metasys server software has a failure during runtime when it tries to write to the Microsoft SQL Server database.
- The Metasys server or SCT software has a failure during runtime for interactions with Active Directory services. For example, an Active Directory service user was denied access to the Metasys Server or SCT software, or an Active Directory service user could not be added as a Metasys server or SCT user.
- The ADSADX Log reports a message queue timeout has occurred. The message contains the text `System.Messaging.Message.QueueException: Timeout for the requested operating has expired`. This event indicates that MSMQ encountered an exception while reading an empty message queue. The sporadic appearance of this error in the ADSADX Log is normal. Because the error only occurs when the message queue is empty, all Metasys system messages have been processed successfully. However, if this error occurs constantly or continually over brief periods of time, there may be a problem with message queuing. Report this behavior to your Johnson Controls support representative.

The **ADSADX Log** folder defaults to Overwrite as Necessary. If you would like to save all events or have a certain Event Log folder size, right-click the folder in the Windows Event Log and change this property.

ⓘ **Note:** A problem exists when viewing the properties of the **ADSADX Log** in the Windows Event Viewer. Even though the folder defaults to Overwrite as Necessary when the folder is created during the first startup of the Metasys server, it appears in the Windows Event Viewer as Overwrite Events Older Than. `The file is Overwrite as Necessary.`

Additional errors write to the Windows Event Viewer Application folder. Any event in this folder is a result of information generated by or an error in the Metasys III Device Manager service (MIIIDM source).

The Windows Event Viewer is located in the Control Panel > Administrative Tools > Event Viewer.

Windows Internet Explorer web browser

➧ **Important:** We strongly advise that you do not browse to the Metasys UI, Metasys UI Offline, or any website from a Metasys server computer. Using web browsers to access web sites on the Metasys server could potentially expose your Metasys server to malicious software, including ransomware. We recommend browsing to the Metasys UI, Metasys UI Offline, or other websites on a client computer or device only.

Advanced security configuration

When the Metasys server is installed, Windows Internet Explorer Advanced Security Configuration is enabled by default. You must add any website you want to navigate to from the Metasys server Internet Explorer web browser to the list of trusted websites. This applies to all external websites.

We strongly advise that you do not browse to the Metasys Site Management Portal UI from a computer running a server class operating system. By default, Windows Internet Explorer Enhanced Security Configuration is enabled on server class operating systems and may block the Launcher download page from which you install the Launcher application for access to the Site Management Portal. Open the Site Management Portal UI from a computer that is not running a server class operating system.

SmartScreen filter

If you are using a private network, we recommend you turn off the Internet Explorer SmartScreen Filter feature. Failure to do so does not prevent Metasys software from running, but may launch multiple user interface windows unnecessarily.

Anti-spyware considerations

Anti-spyware packages alert users when changes are made to their operating systems by unidentified applications, programs, or services and may also allow the users to control these changes to their operating systems. For example, changes may occur in Internet Explorer web browser settings, running processes, or dial-up connections.

The anti-spyware software may also allow the user to designate which services can run on a Metasys server. The Metasys Device Manager, Metasys Action Queue, and Metasys Report Cache Refresh may appear on the list of services as unknown or unreliable. In these cases, in the anti-spyware tool, the Publisher attribute of the process does not identify the process as a Johnson Controls process, nor does the term Metasys appear in the name. Both of these services must be allowed to run on the Metasys server.

Additionally, anti-spyware software may not allow the Metasys server software to write to the hosts file. Some anti-spyware software warns the user that changes are to be made, and the user must accept or reject the changes. Other anti-spyware packages do not allow the change to occur at all until the software is configured.

For more information, refer to the *ADS/ADX Commissioning Guide (LIT-1201645)*, *Open Application Server (OAS) Commissioning Guide (LIT-12013243)* or *ODS Commissioning Guide (LIT-12011944)*.

Backup considerations for the Metasys Server

If a backup program changes attributes in certain Metasys Server files, the Metasys Server may shut down and then restart. To avoid this scenario, we recommend that you always avoid backing up the following files and folders, and that you exclude them from any other programs that access these directories in the Metasys Server:

- C:\Program Files (x86)\Johnson Controls\MetasysIII
- C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG
- C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config
- C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG
- C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config
- C:\Program Files (x86)\Johnson Controls\MetasysReports\bin (Metasys Advanced Reporting System only)
- C:\Program Files (x86)\Johnson Controls\MetasysReports\web.config (Metasys Advanced Reporting System only)

Supported operating system, SQL Server software, and IIS versions

Refer to the literature for the Metasys products you are installing for a list of supported operating system and SQL Server software versions. For an overview of software supported by the Metasys system, refer to the *Metasys Server Installation and Upgrade Guide (LIT-12012162)*, *SCT Installation and Upgrade Instructions (LIT-12012067)*, *Open Application Server Installation and Upgrade Instructions (LIT-12013222)*, or the *ODS Installation and Upgrade Guide (LIT-12011945)*.

As new software and service packs become available, Johnson Controls tests them for use with Metasys software. Be aware that installing other software or updating the operating system with a new service pack on a computer running Metasys software may adversely affect the system.

The following table lists the versions of IIS that can be used with Metasys products.

Table 18: Supported IIS Versions

Operating System	Supported IIS Version
Windows® 8.1 Pro and Windows 8.1 Enterprise Editions with Update (KB2919355) (64-bit)	IIS 8.5
Windows® 10 Pro and Windows 10 Enterprise Editions versions 1903, 1909, and 2004 (64-bit). For all future Windows 10 updates after version 2004, we will evaluate and certify that Metasys software can support the updates before we provide guidance on support. Windows® Server® 2016 with Update (KB4512495) (64-bit) Windows® Server® 2019 (version 1803 or later) (64-bit)	IIS 10.0

Supported network engine models and releases with security attributes

The following table lists the latest Metasys system software releases of each network engine model along with the security attributes available for each. As the security features of the *Metasys* system have improved with each new software release, the network engines have likewise been improved.

Table 19: Network engine release levels

Release with Security Attributes	**NCE25**	**NAE35, NAE45**	**NAE55, NAE85**	**NIE29, NIE39, NIE49**	**NIE59, NIE89**	**NIE55, NIE85**	**SNC, SNE**
Release 9.0 • Site Security Level • Allow Http	X	X	X	X	X	X	N/A
Release 9.0.7 • Site Security Level • Allow Http	X	X	N/A	X	N/A	N/A	N/A
Release 10.0 • Site Security Level • Allow Http • Advanced Security	N/A	N/A	X	N/A	X	X	N/A
Release 10.1 • Site Security Level • Allow Http • Advanced Security	N/A	N/A	X	N/A	N/A	N/A	X
Release 11.0 • Site Security Level • Allow Http • Advanced Security • FIPS 140-2	N/A	N/A	X	N/A	N/A	N/A	X

IIS anonymous access considerations (Metasys Server and SCT)

General information

For Metasys software to install successfully, you must provide anonymous access temporarily to the Default Web Site folder in IIS. After installation, you can disable anonymous access to the Default Web Site folder. Then, to facilitate Metasys software operations, you must enable anonymous access to the following virtual folders that are created when you install the Metasys server, SCT, Metasys Advanced Reporting feature, and the NAE Update Tool:

- **Metasys**
- **SCT**
- **MetasysIII**
- **MetasysReports**
- **NAEUpdateTool**

When you configure IIS to use Anonymous Access for an item, IIS delegates all authentication responsibilities for that item to the Metasys application. Anonymous access is required in order for the user to log in and access Metasys using Java client software and the Metasys web services. See Enabling and disabling anonymous access on the default web site.

ⓘ **Note:**

Before changing your customer's IIS anonymous access settings, consult with your customer and/or your customer's IT department to make sure the changes do not violate network security policies.

In addition, you must assign the following privileges to the Windows user account or Windows user group that is permitted to log in to the Metasys system:

- network access to the Metasys server or SCT computer
- bypass traverse checking
- batch job login capability

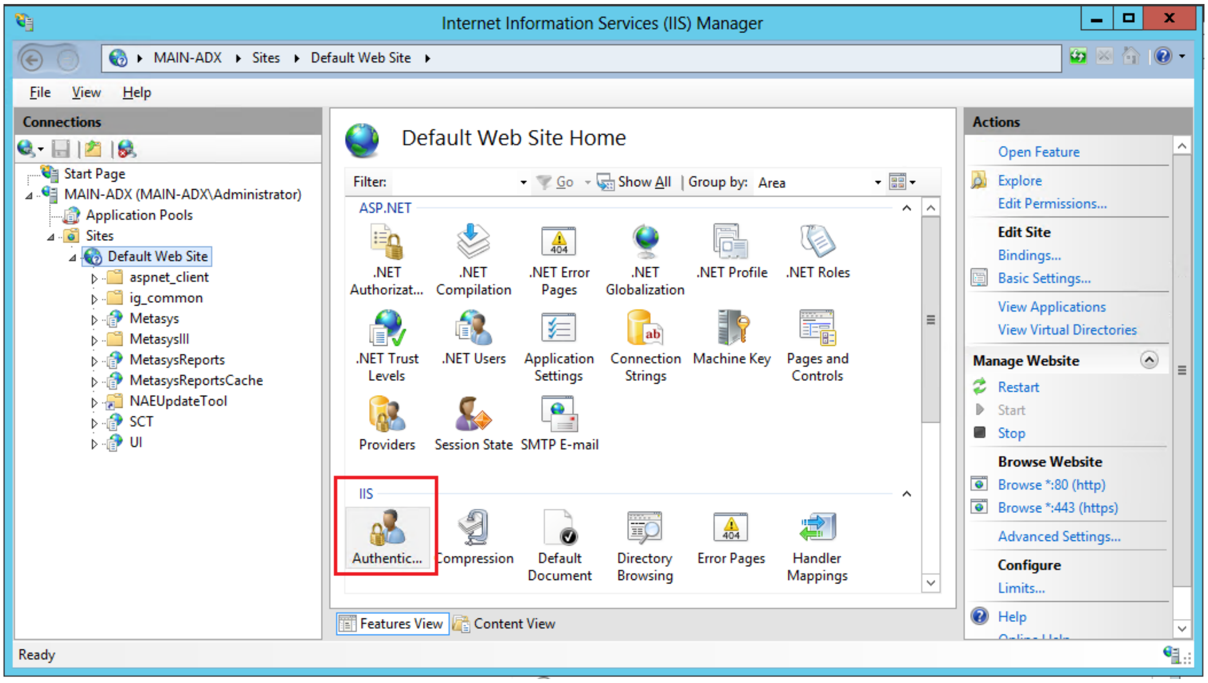
However, **do not** assign the privilege called **deny access to this computer from the network** to this same Windows user account or Windows user group.

Enabling and disabling anonymous access on the default web site

Follow these steps to enable and disable anonymous access when installing and running the Metasys server or SCT software.

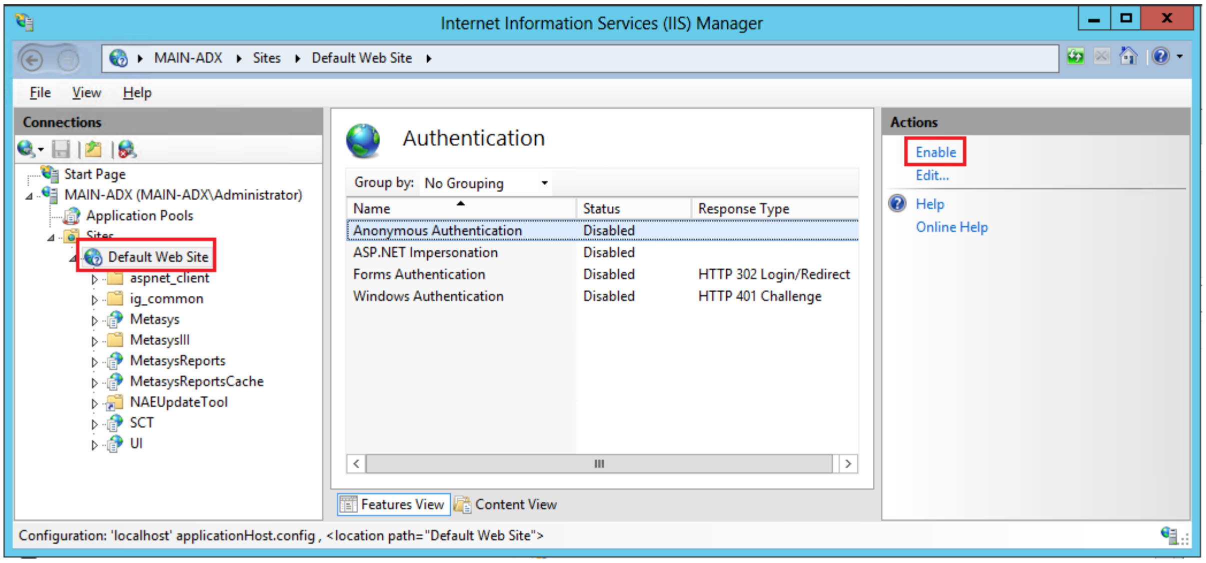
1. Open Control Panel and click ***System and Security*** > ***Administrative Tools***. Double-click **Internet Information Services (IIS) Manager**. The Internet Information Services (IIS) Manager window appears.
2. Expand the left pane to expose the Default Web Site.

Figure 28: Enabling Anonymous Access to Default Web Site



3. Select **Default Web Site** and double-click the **Authentication** icon in the middle pane. The Authentication options appear.

Figure 29: Authentication Options for Default Web Site



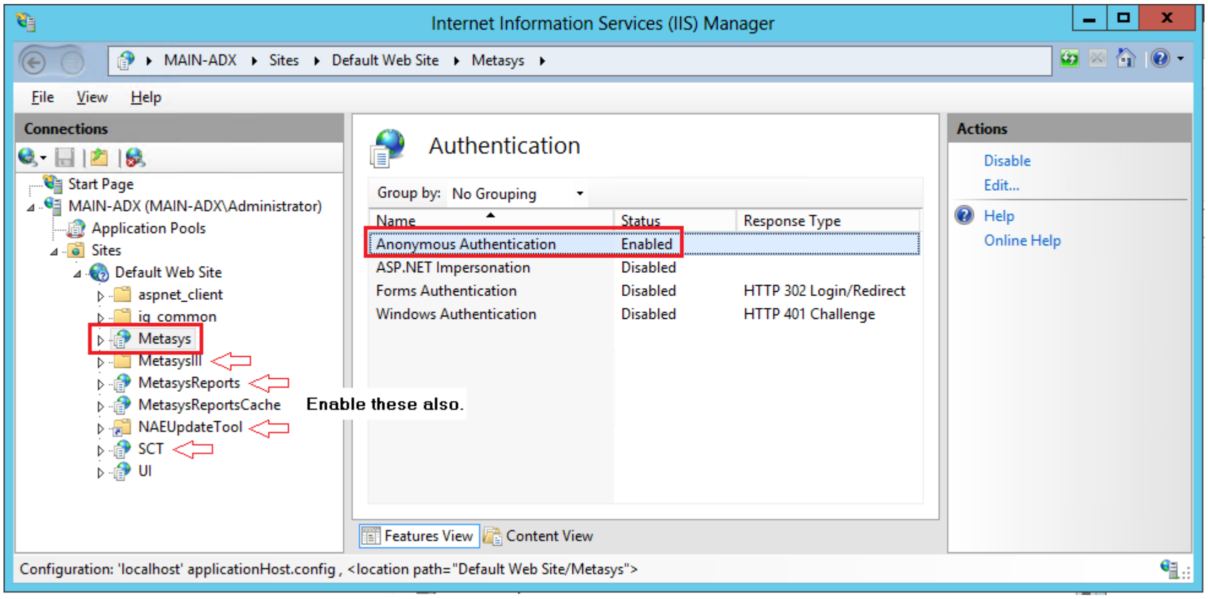
Name	Status	Response Type
Anonymous Authentication	Disabled	
ASP.NET Impersonation	Disabled	
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Disabled	HTTP 401 Challenge

Configuration: 'localhost' applicationHost.config , <location path="Default Web Site">

4. In the Actions pane, set Anonymous Access to **Enabled**.
5. Close the IIS Manager window.
6. Install the Metasys server or SCT software.
7. Reopen the IIS Manager window. Disable Anonymous Access on the Default Web site (reversing Step 4 above).

8. Expand the Default Web Site folder and enable Anonymous Access for each of the following items that might be present: Metasys, MetasysIII, SCT, MetasysReports, and NAEUpdateTool. The following figure is an example of the anonymous access setting enabled for the Metasys website.

Figure 30: Enabling Anonymous Access to Metasys Web Site



Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Disabled	HTTP 401 Challenge

Enable these also.

Configuration: 'localhost' applicationHost.config , <location path="Default Web Site/Metasys">

9. Close the IIS Manager and all other windows.

Databases

Microsoft SQL database considerations

All versions of SQL Server software must be set up in Mixed Mode Authentication and configured to use both the TCP/IP port 1433 and Named Pipes protocols. When upgrading to a new version of SQL Server software, you must preserve this configuration because the upgrade process turns off the network protocols.

Consider the following general database recommendations:

- The unified Metasys server is incompatible with server clusters. For a split Metasys server (ADX), the database server computer can be part of a server cluster.
- Run SQL Server databases in Simple Recovery mode to reduce the risk of system failure due to lack of disk space. Simple recovery mode allows you to restore from the previous night's backup only. For point-in-time recovery, run the databases in Full Recovery mode and back up your transaction log at least every 24 hours. Failure to perform Transaction log backups at this interval eventually results in system failure due to lack of available disk space.
- Confirm that SQL Server database backups are being performed correctly and consistently to prevent data corruption. Check periodically to make sure the backups are present and restorable. Create backups using the Metasys Database Manager or the tools listed in Database management: SQL Server tools. Each backup should be saved in separate locations.
- Check periodically to make sure your database indexes are healthy because fragmented indexes greatly reduce database performance. Rebuild indexes as necessary using tools available from the IT department or the Metasys Database Manager. See Database management: Metasys Database Manager and Database management: SQL Server tools.

- Do not use third-party backup programs to backup the Metasys databases. Instead, use the tools provided by SQL Server software or use the Metasys Database Manager.
- To create and manage the Metasys Server databases and SQL Server user accounts that are used during Metasys Server runtime, the Metasys Server software installation program requires a user account with administrator access to SQL Server databases during installation. The account may be either a SQL Server user account or a Windows operating system user account that has the required privileges. After the installation program creates the Metasys Server databases and SQL Server user accounts, the administrator account is no longer used. You may remove SQL Server database administrator rights from this user account.
- During runtime, the Metasys Server software uses the SQL Server user accounts that were created by the Metasys Server installation program. For information about managing the SQL Server user accounts used by the Metasys Server (account rename and password changes), contact Johnson Controls technical support.
- SCT uses virtual service accounts with integrated authentication. Windows authentication is more secure than database authentication, as it uses a certificate based security mechanism. With virtual service accounts, the management of account credentials is handled by the Windows operating system so no manual management is required.

The default location for Metasys system databases is determined by database default locations setting in SQL Server. The following table lists the databases that the Metasys system creates.

Table 20: System databases

Metasys Server historical databases	Metasys Server non-historical databases	Metasys UI databases	CCT
JCIEvents	MetasysIII	JCIReportingDB	CCT_DB
JCIAuditTrails	XMS	SpacesAuthorization	FDB_Control
JCIHistorianDB	MetasysTranslationDictionary		
JCIItemAnnotation	MetasysReporting		
JCIReportingDB			

In addition, the online archive, MetasysSCT, SCTTranslationDictionary, and any current Metasys SCT archive databases also may be present. SCT archive database names are user configured.

For information on installing SQL Server software for use with a Metasys system, refer to the *SQL Server Installation and Upgrade Instructions (LIT-12012240)*, *Metasys Server Installation and Upgrade Instructions (LIT-12012162)*, *Metasys Server Lite Installation and Upgrade Instructions (LIT-12012258)*, or *ODS Installation and Upgrade Guide (LIT-12011945)*.

Database management: Metasys Database Manager

The Metasys Database Manager allows you to purge, back up, restore, and monitor your Metasys system SQL Server databases. This tool is included on all Metasys server media and is compatible with all versions of SQL Server software supported by the installed release of Metasys software. Refer to the *Metasys Database Manager Help (LIT-12011202)* for more information.

Database management: SQL Server tools

In addition to or instead of the Metasys Database Manager, you can use the following Microsoft Corporation tools to maintain your SQL Server databases:

Table 21: SQL Server Software Maintenance Tools

SQL Server Software Family	Microsoft Corporation Database Tool	Included with SQL Server Software?[1]
SQL Server Software	SQL Server Management Studio	Yes
SQL Server Express Software	Microsoft SQL Server Management Studio Express (SSMSE)	No[2]

[1] All tools are available on http://www.microsoft.com/downloads.

[2] Available with versions that include Management Tools or Advanced Services.

For specific steps on how to back up and manage Metasys system databases using these tools, go to http://www.microsoft.com. You do not need to stop Metasys system services to perform a database backup.

Historical data storage

Network engines store a limited amount of alarm, trend, and audit trail information. After engines collect data, you can forward the data to a Metasys Server and save the data on the hard disk for long-term storage.

Historical data on engines and Metasys Servers can be copied to the clipboard and pasted into a spreadsheet, word processor, or database program. You can use Metasys Export Utility software to extract the historical data from the Metasys system to six different file formats (.xls, .txt, .csv, .mdb, .htm, .xml) for easier viewing.

Data backup/restore

For information on SQL Server software backups, see Microsoft SQL database considerations.

Use the SCT to back up and restore Metasys user accounts/privileges and to back up, restore, and create archives of Metasys configuration data. Refer to the *Metasys SCT Help (LIT-12011964)* for details.

Site Management Portal UI

The Site Management Portal UI comprises a Java application, which runs with a private JRE. See Java software and private JREs for a definition of private JREs. The Java security model allows only trusted applications to perform certain activities such as printing, connecting to the network, retrieving system information, and accessing your computer’s local file system. Trusted applications must be digitally signed and must be granted permissions by the end user.

The Metasys Site Management Portal UI is digitally signed with a certificate provided by the VeriSign® Certificate Authority (CA). The certificate verifies that the Metasys system application has not been tampered with and is distributed by Johnson Controls. A message appears stating that the security certificate was issued by a company that is trusted and indicates whether your certificate is expired.

Metasys Advanced Reporting System UI

The Metasys Advanced Reporting System offers a separate HTML-based user interface in which you can run reports on system configuration and performance. This system allows you to use a restricted access user interface and avoid Java software downloads for users with limited report and configuration needs.

The Metasys Advanced Reporting System can be used only on ADXs that are running a supported SQL Server software version with SQL Server Reporting Services. Local Metasys system users with

Standard Access access type privileges are authorized with the Advanced Reporting option in the Security Administrator System.

For more information, refer to the *Metasys Advanced Reporting System and Energy Essentials Help (LIT-12011312)*.

Java software and private JREs

The Site Management Portal (SMP) and SCT are Java applications, requiring a JRE plug-in on the local client computer. Security vulnerabilities were often discovered in the public version of the JRE, which required the developer to release updated versions and for Johnson Controls to issue patches to the SMP and SCT software. To alleviate this problem, the Metasys system no longer relies on a public JRE plug-in for Release 6.0 or later. Instead, it uses an internal private JRE that is bundled with the Metasys application and is installed locally on the computer for that application only. The private JRE is not exposed to possible security risks and is compatible with IT department policies.

To support the use of the private JRE, an application called the Launcher was developed to allow you to manage a list of all network engines, Metasys servers, SCT, LCS85, Metasys UI, Metasys UI Offline, and Metasys Advanced Reporting, or any generic website links. The Launcher is a simple software tool that launches the user interface for any Metasys release, but only manages the local Java files for Release 6.0 or later systems.

If you need to configure your proxy settings, you must do so in the Launcher tool, not in the Java control panel. For details, refer to Launcher *Help (LIT-12011742)*.

Public JRE files are still required for older versions of the Metasys system. Public JREs are installed in a public location (such as C:\Program Files\Java\) and are known by the operating system to allow certain applications, such as Internet browsers, to access that JRE.

Web browser recommendations

A supported web browser is required for downloading the Launcher.

The Launcher is a software application that is installed on each client computer that logs in to the Metasys Server, SCT, or supervisory engine. The Launcher lets you access any Metasys server or supervisory engine on the building network, regardless of its software version. You use the Launcher to reach the log in screen of the Metasys Server, SCT, or network engine. For details, refer to *Launcher Help (LIT-12011742)*.

➤ **Important:** We strongly advise that you do not browse to the Metasys Site Management Portal UI, Metasys UI, Metasys UI Offline, or any website from a computer running a server class operating system. By default, Windows Internet Explorer Enhanced Security Configuration is enabled on server class operating systems, and may block the Launcher download page from which you install the Launcher application for access to the Metasys system. In addition, accessing websites on the Metasys Server could potentially expose your server to malicious software, including ransomware. Alternatively, open the user interface from a computer that is running a Desktop operating system.

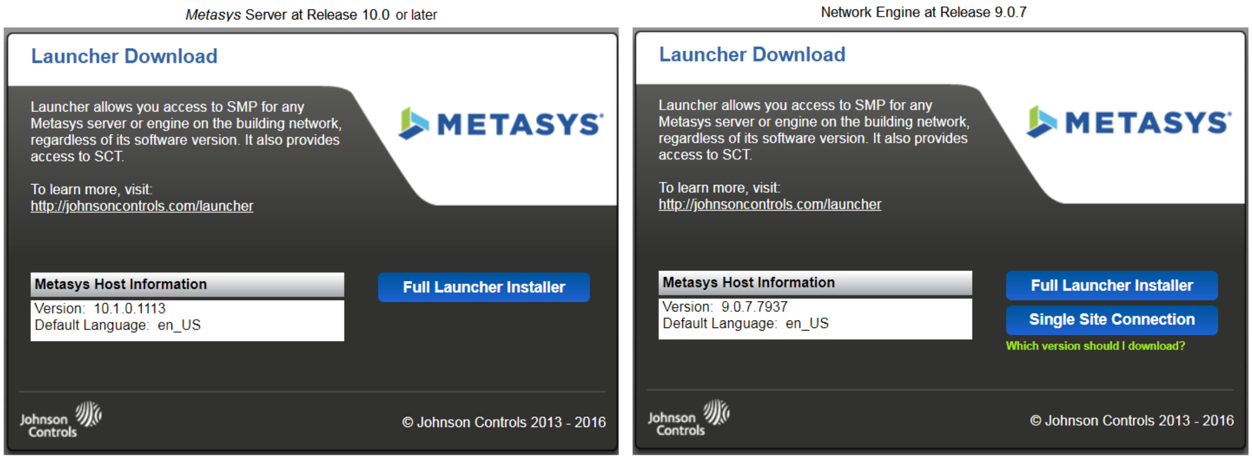
Launcher download options and proxy settings

You can use an Internet browser to download the Launcher software that the SMP UI requires. To do so, enter its URL in the address field using this format:

http://<Metasys Server or engine computer name>/metasys

One of the following Launcher Download screens appears (Figure 31).

Figure 31: Windows Launcher Download



Metasys Server at Release 10.0 or later

Launcher Download

Launcher allows you access to SMP for any Metasys server or engine on the building network, regardless of its software version. It also provides access to SCT.

To learn more, visit: http://johnsoncontrols.com/launcher

Metasys Host Information

Version: 10.1.0.1113
Default Language: en_US

© Johnson Controls 2013 - 2016

Network Engine at Release 9.0.7

Launcher Download

Launcher allows you access to SMP for any Metasys server or engine on the building network, regardless of its software version. It also provides access to SCT.

To learn more, visit: http://johnsoncontrols.com/launcher

Metasys Host Information

Version: 9.0.7.7937
Default Language: en_US

Which version should I download?

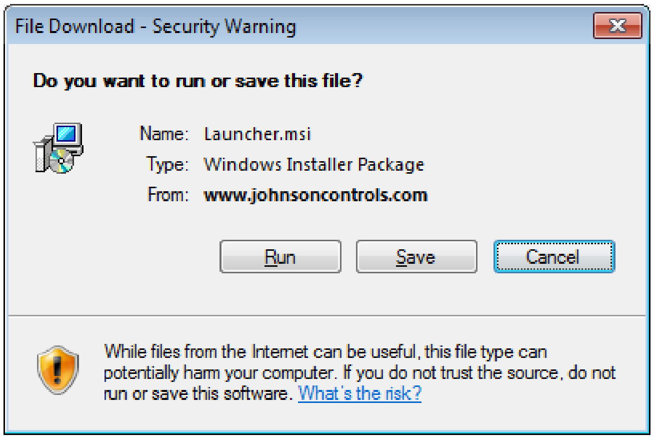
© Johnson Controls 2013 - 2016

At Release 10.0 or later, the Launcher Download screen provides one choice (Full Launcher Installer) and at Release 9.0.7, the Launcher Download screen provides two choices (Full Launcher Installer and Single Site Connection), but the Single Site Connection is no longer active.

When you click **Full Launcher Installer** for a network engine at Release 9.0.7 or later, the browser routes you to the public Launcher download website. Refer to that website for instructions on how to download the Launcher installation file to a location on your computer. When complete, run the Launcher installation. For details, refer to the *Launcher Installation Guide (LIT-12011783)*.

When you click **Full Launcher Installer** for a Metasys Server at Release 10.0 or later, a security warning screen may appear (Figure 32). This screen gives you the option to **Run** or **Save** the Launcher installation file.

Figure 32: File Download - Security Warning Screen



File Download - Security Warning

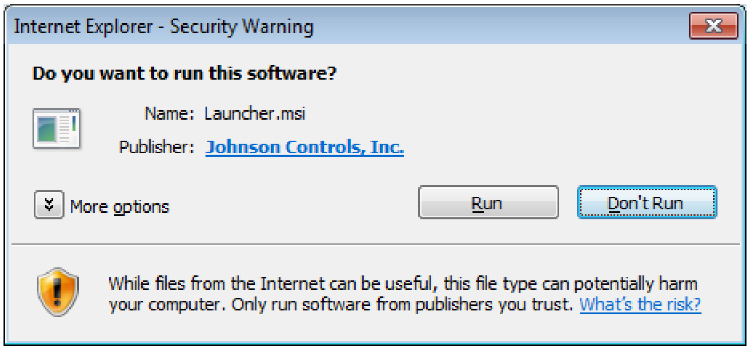
Do you want to run or save this file?

Name: Launcher.msi
Type: Windows Installer Package
From: www.johnsoncontrols.com

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

Click **Run** on the File Download - Security Warning screen. The Internet Explorer - Security Warning screen may appear (Figure 33).

Figure 33: Internet Explorer - Security Warning Screen



Internet Explorer - Security Warning

Do you want to run this software?

Name: Launcher.msi

Publisher: Johnson Controls, Inc.

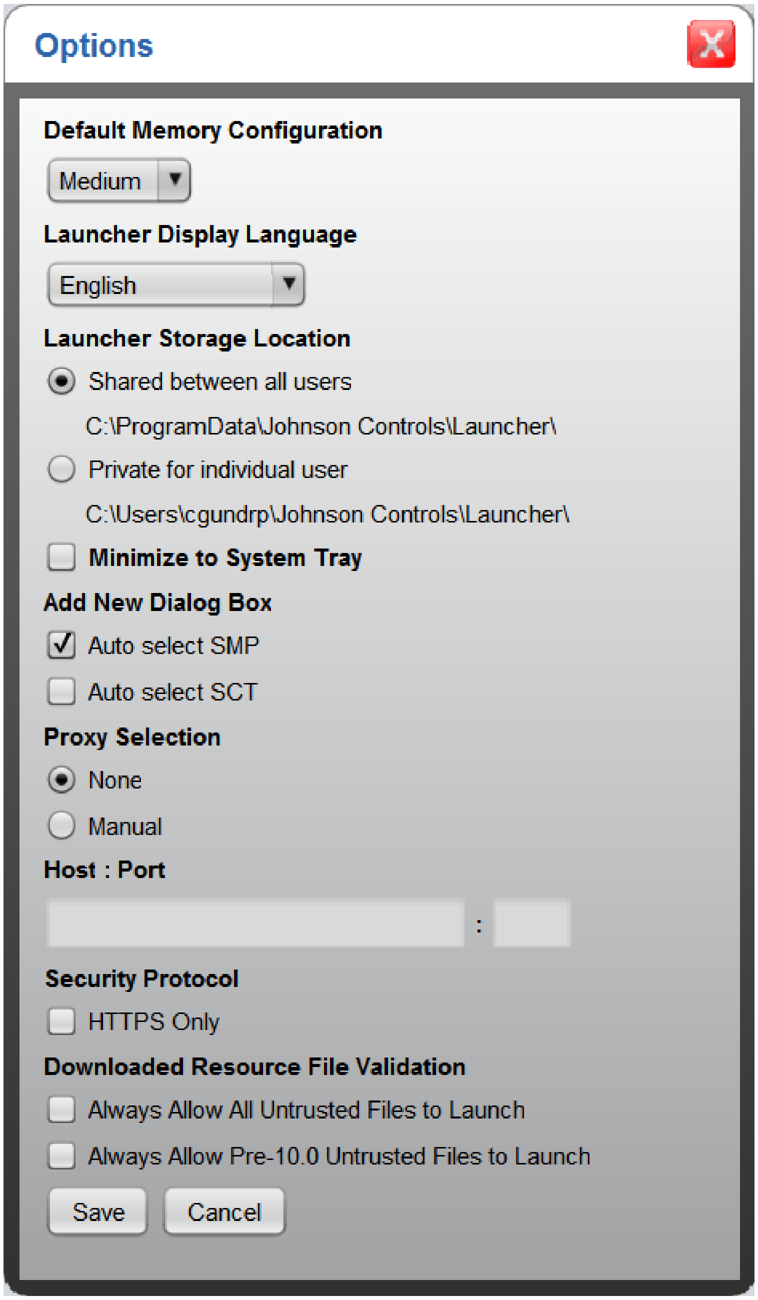
While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

For this screen, click **Run** to allow local installation of the Launcher software. For more details, refer to the *Launcher Installation Guide (LIT-12011783)*.

Launcher Proxy Settings

The full version of the Launcher tool lets you update certain options, including proxy settings (Figure 34).

Figure 34: Application Options Screen



Options

Default Memory Configuration

Medium ▼

Launcher Display Language

English ▼

Launcher Storage Location

● Shared between all users

C:\ProgramData\Johnson Controls\Launcher\

○ Private for individual user

C:\Users\cgundrp\Johnson Controls\Launcher\

□ Minimize to System Tray

Add New Dialog Box

☑ Auto select SMP

□ Auto select SCT

Proxy Selection

● None

○ Manual

Host : Port

Security Protocol

□ HTTPS Only

Downloaded Resource File Validation

□ Always Allow All Untrusted Files to Launch

□ Always Allow Pre-10.0 Untrusted Files to Launch

If the building network uses a proxy server for connection to the Internet, click **Manual** under Proxy Selection and enter the IP address or host name and port number of the proxy server.

Pop-up add blockers

You do not need to disable third-party pop-up ad blockers on the computer you use to browse to the Metasys Site Management Portal UI in order to ensure Metasys Site Management Portal UI functionality. For previous releases, you must disable pop-up ad blockers or the Login screen may not launch. To disable pop-up ad blockers, turn off the third-party pop-up ad blocker for all sites or for the address of the Metasys system Site Director. If you cannot turn off or configure the third-party pop-up ad blocker, uninstall it from the computer.

Turning off the Internet Explorer Web Browser pop-up blocker

This procedure applies to the Internet Explorer pop-up blocker. If you have third-party pop-up blockers, use the manufacturer’s instructions to disable them.

To turn off the pop-up blocker:

1. Open Internet Explorer.
2. On the Tools menu, select ***Pop-up Blocker*** > ***Turn Off Pop-up Blocker.***

ⓘ **Note:** For information on allowing pop-ups from specific sites only, refer to the Internet Explorer Help.

Sleep power option on Windows 8.1 and Windows 7 computers

If you use a computer with Windows 8.1 or Windows 7 to browse into the Metasys system, be aware that the Site Management Portal UI session information is lost if you are logged in when the operating system goes to sleep. The session terminates at the time the operating system goes to sleep, regardless of the Inactive Session Property setting that applies to your Metasys user account; for example, if Never Terminate is set for your account, the Site Management Portal UI session still terminates. The Sleep option is enabled for 2 hours by default, so you may wish to increase this setting or disable it.

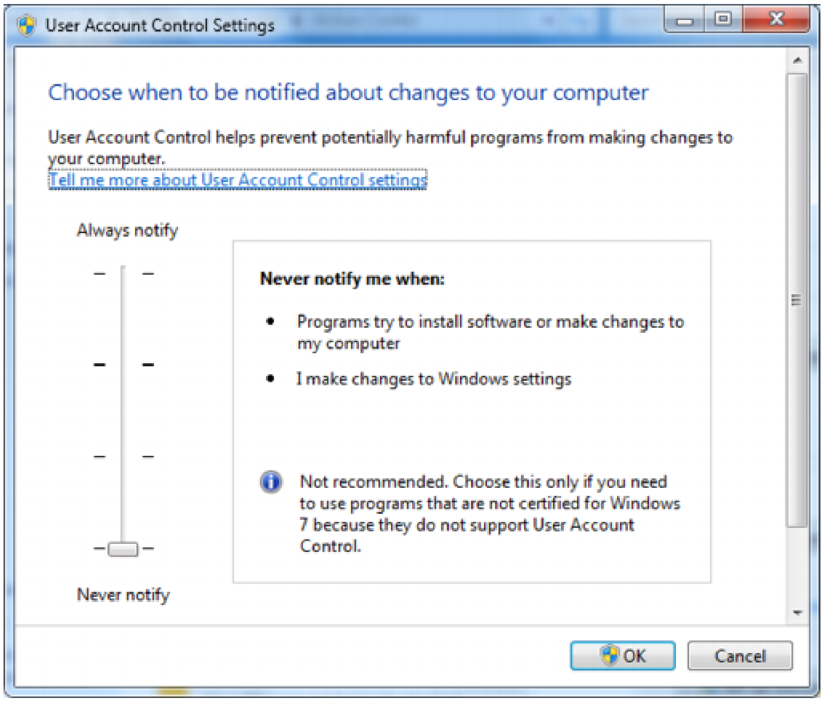
Disabling User Account Control

About this task:

ⓘ **Note:** This procedure is required if you want to use CCT software, HVAC PRO software, or GX-9100 tool software in Passthru mode from SCT on a Windows 8.1 computer. If you do not perform these steps, Passthru mode does not function. Also, follow this procedure if you need to download resource files for a VND integration into a supervisory engine.

1. In Control Panel, click ***System and Security*** > ***Action Center***. The Action Center window appears.
2. Click **Change User Account Control** settings. The User Account Control window appears (Figure 35).

Figure 35: Disabling User Account Control



User Account Control Settings

Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings

Always notify

Never notify me when:

- Programs try to install software or make changes to my computer
- I make changes to Windows settings

Not recommended. Choose this only if you need to use programs that are not certified for Windows 7 because they do not support User Account Control.

Never notify

3. Move the slider bar to the bottom position called **Never notify**.
4. Click **OK**.
5. Restart the computer to make the change effective.

Metasys dial-up networking

Point-to-Point (PPP) networking is used for all dial-up communication between the Metasys client computer (web browser) and the Metasys server and engine. Newer models of network engines and the latest release of Metasys Server software do not support communication over modems. If you have an older system, refer to the *Metasys System Extended Architecture Direct Connection and Dial-Up Connection Application Note (LIT-1201639)* for more information.

Metasys Application Programming Interface (API)

Additional enhancements to the Metasys Server software at Release 10.1 and later include a REST-compliant **Metasys Monitoring and Commanding Application Programming Interface (API)** that enables reading, writing, and commanding of one or more Metasys objects/properties to provide a secure way to bi-directionally integrate with third-party applications. As a prerequisite, you need to define a new user of type **API Access** under the Security Administrator system of the Site Management Portal that provides access to the Metasys system. For details, refer to the *Security Administrator System Technical Bulletin (LIT-1201528)*.

This is the latest in a suite of APIs that include the REST-compliant API that enables data to be securely extracted from the Metasys system and integrated with third-party data visualization tools to meet robust data analysis and reporting needs and the Metasys API for the TeleHealth Engagement Application that facilitates reliable two-way communication between the TeleHealth patient engagement application and Metasys system to provide patients direct control over their healthcare space for increased comfort and satisfaction.

Network Interface Cards (NICs)

The Metasys software supports more than one NIC on a computer running Metasys software (including Metasys server, SCT, NxE85, NIE89 and LCS85 software).

Follow the instructions in the appropriate Metasys installation literature to configure the NIC that Metasys software uses. For example, the Interface Metric for the Metasys network card must be set to 1, and all other NICs on the computer set to an Interface Metric higher than 1.

Appendix: Network and IT terminology

Active Directory Service

A network operating technology that enables IT administrators to manage enterprise-wide information from a central repository. This information includes data center policy compliance and identity management (user login accounts), which are used for both Microsoft Windows authentication (login to the Windows operating system) as well as network resource authentication (login to enterprise-wide secured applications, such as email). The Metasys system uses the LDAP integration of Active Directory.

Active Directory Service Domain/Domain Controller

A collection of Domain Controllers that can be thought of as a security boundary for network resources. A Domain Controller provides the Active Directory service to network users and computers; stores directory data; and manages user and domain interactions including the login process, authentication, and directory searches.

Active Directory Service Schema

The formal definition of all object and attribute data that can be stored in the directory; for example, user is an object type with attribute data of name, first name, last name, email, and so on. The schema is made up of object classes and attributes. The base (or default) schema contains a rich set of object classes and attributes to meet the needs of most organizations, and is modeled after the ISO X.500 standard for services.

Demilitarized Zone (DMZ)

A portion of the network located between the Internet and the intranet. It is a buffered area that is usually protected by two or more firewalls.

Domain Name System (DNS)

The method by which host domain names are translated into IP addresses. A domain name is a meaningful and easy-to-remember handle for an Internet address. DNS is the Internet standard for naming host devices and mapping host names to IP addresses.

Dynamic Host Configuration Protocol (DHCP)

A communications protocol that lets network administrators centrally manage and automate the assignment of IP addresses in an organization’s network.

DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a device is plugged into a different location on the network. DHCP can also assign dial-up users an IP address automatically when they connect to the network. Some DHCP servers can support fixed addresses for devices that need a static IP address.

The Metasys server, network engine, TEC20 Coordinator, and Many-to-One Wireless Room Temperature Sensing Receiver (WRS-RTN) can obtain their IP addresses and other network information using DHCP. Each Metasys device that can connect to the Ethernet network needs a unique IP address. Without DHCP, the IP address must be entered manually for each device; and, if the devices are moved to another subnet on the network, you must enter a new IP address. The Metasys system supports both dynamic and static IP address assignments.

Firewall

A firewall combines hardware and software to provide a security system that prevents unauthorized access from the Internet to the intranet. When engines have access to the Internet, firewalls typically are installed to prevent outsiders from accessing private data resources and to control which outside resources its own users can access. The firewall on network engines is enabled by default.

Forest

One or more domains that share a common schema and global catalog. Forests are normally organized hierarchically. The hierarchy is determined by the IT organization.

Integrated Windows Authentication

An authentication method for directory security on a web server. Integrated Windows authentication uses a cryptographic exchange with the user’s Windows Internet Explorer web browser to confirm the identity of the user, and thus authenticate the user to access the web server resource (such as a web service or a file).

Kerberos

A network authentication protocol designed to provide strong authentication for client/server applications by using secret-key cryptography. Kerberos is the primary security protocol for authentication within an Active Directory service domain.

Lightweight Directory Access Protocol (LDAP)

A standard communication protocol for directories located on TCP/IP networks. LDAP defines how a directory client can access a directory server and how the client can perform directory operations and share directory data.

Microsoft Message Queuing (MSMQ)

A technology that supports reliable, persistent storage of messages that require processing when the recipient device is temporarily offline or busy. Refer to http://www.microsoft.com for information on Microsoft Message Queuing (MSMQ).

Network Address Translation (NAT)

A protocol that enables a local area network to use one set of IP addresses for internal traffic and registered IP addresses for external traffic.

NT LAN Manager (NTLM)

A network authentication protocol developed by Microsoft Corporation. NTLM is the secondary protocol for authentication within an Active Directory service domain. If a domain client or domain server cannot use Kerberos authentication, then NTLM authentication is used.

Organizational Units (OU)

A container within Active Directory service that should be used to reflect the details of the organization’s business structure or to delegate administrative control over smaller groups of users, groups, and resources. An organizational unit (OU) inherits security policies from the parent domain and parent OU unless it is specifically disabled.

Point-to-Point Protocol (PPP)

A protocol for communication between two computers using a serial interface, typically a computer connected by phone line to a server. For example, your Internet service provider may provide you with a Point-to-Point Protocol (PPP) connection so that the provider’s server can respond to your requests, pass them on to the Internet, and forward your requested Internet responses back to you. PPP uses IP (and is designed to handle others). It is sometimes considered a member of the TCP/IP suite of protocols. Relative to the OSI reference model, PPP provides layer 2 (data-link layer) service. Essentially, it packages your computer TCP/IP packets and forwards them to the server where they can be placed on the Internet.

Ransomware

Ransomware is a type of malware that infects computer systems, restricting access to the infected systems. Ransomware variants have been observed for several years and often attempt to extort money from victims by displaying an on-screen alert. Typically, these alerts state that the systems are locked or that files are encrypted. Users are told that unless a ransom is paid, access cannot be restored. The ransom varies but is frequently $200–$400 dollars and must be paid in virtual currency, such as Bitcoin.

Ransomware is often spread through phishing emails that contain malicious attachments or through drive-by downloading. Drive-by downloading occurs when a user unknowingly visits an infected website and then malware is downloaded and installed without the user's knowledge.

Crypto ransomware, a malware variant that encrypts files, is spread through similar methods and can be spread through social media, such as Web-based instant messaging applications. Additionally, newer methods of ransomware infection were observed. For example, vulnerable Web servers were exploited as an entry point to gain access into an organization's network.

Security Identification (SID)

An alphanumeric character string that uniquely identifies Active Directory service users and groups within Active Directory service. Unlike a user name or group name, which may be renamed, the Security Identification (SID) remains constant throughout the life of the user account or group.

Service Account in Active Directory Service

A login account assigned to an application to enable the application to perform privileged actions within Active Directory service; the Metasys system requires one or more Service Accounts to be assigned to allow the system to perform directory queries and request Active Directory service authentication. Only one Service Account is allowed per domain.

Simple Mail Transfer Protocol (SMTP)

A protocol for sending email messages between servers. Most email systems that send mail over the Internet use Simple Mail Transfer Protocol (SMTP) to send messages from one server to another. The messages can then be retrieved with an email client using either POP or IMAP.

Simple Network Management Protocol (SNMP)

The primary protocol governing IP network management and the monitoring of IP network devices and their functions. It is not necessarily limited to TCP/IP networks.

Simple Network Time Protocol (SNTP)

A simplified version of NTP. These protocols allow one computer to ask another computer what time it is across a TCP/IP network, then set its own clock accordingly. A number of public Simple Network Time Protocol (SNTP) time servers keep track of time with a very high degree of accuracy that can be used to ensure that the Site Director is synced to real time. You can find lists of public SNTP time servers by performing a search on the Internet.

Syslog

Syslog is a standard for message logging. Syslog allows the separation of software that generates messages for logging, the system that stores the messages, and the software that generates reports. In the Metasys system, the servers and network engines provide the optional capability of sending its configured audit log entries and event notifications to an external, customer-provided Syslog server. A Syslog UPD packet contains three fields: PRI, Header, and Message. The Metasys system implementation of Syslog conforms to published internet document Request for Comments (RFC) 3164.

Transmission Control Protocol (TCP)

A set of rules (protocol) used along with IP to send data in the form of message units between computers over the Internet and on other networks commonly referred to as intranets or extranets. Whereas IP takes care of handling the actual delivery of the data, Transmission Control Protocol (TCP) keeps track of the individual units of data (called packets) into which a message is divided for efficient routing through the Internet.

Transport Layer Security (TLS) and Secure Sockets Layer (SSL)

Transport Layer Security (TLS) is the successor to the Secure Sockets Layer (SSL) protocol. Both communication protocols provide network security to client-server applications.

For general information on how to implement TLS or SSL, refer to https://technet.microsoft.com/en-us/library/cc784450(v=ws.10).aspx.

The Metasys software can use Secure Channel and built-in implementation of TLS or SSL included with the Microsoft Windows operating system. For more information about Secure Channel, refer to https://msdn.microsoft.com/en-us/library/windows/desktop/aa380123(v=vs.85).aspx.

User Account in Active Directory Service

A login account assigned to a user that is created, stored, and maintained only within Active Directory service; this User Account provides access to Active Directory service Network Resources. It may also provide access to the Metasys system when added and privileged using the Metasys Security Administrator System.

User Datagram Protocol (UDP)

A communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses IP. User Datagram Protocol (UDP) is an alternative to TCP. Like TCP, UDP uses the Internet Protocol to actually get a data unit (called a datagram) from one computer to another. Unlike TCP, UDP does not divide a message into packets (datagrams) and reassemble it at the other end. Specifically, UDP does not provide sequencing of the packets that the data arrives in; therefore, the application program that uses UDP must ensure that the entire message has arrived and is in the right order.

Virtual Private Network (VPN)

A private data network that uses the public telecommunication infrastructure and the Internet, maintaining privacy through the use of tunneling protocol and security procedures (encrypting data before sending it through the public network and decrypting it at the receiving end).

Appendix: Microsoft Windows operating system and SQL Server software license requirements

Windows operating system license requirements

To run SQL Server Standard Edition on the ADX you must choose from one of the following Microsoft licensing models:

- Per core
- Server + Client Access License (CAL)

For more information, refer to the *Microsoft SQL Server 2019 Licensing Models* section in the *SQL Server 2019 Licensing Datasheet* https://download.microsoft.com/download/0/5/c/05c60185-ebdd-4472-895a-3d8e8da55682/SQL_Server_2019_Licensing_Datasheet.pdf.

License requirements for servers and SQL Server

If you run SQL Server® Express on a physical or a virtual ADX, it does not require licensing. Note the following features:

- Limit of 15 connections, can be a combination of users and device connections.
- Limit of 10 GB database size.
- Install on a Window® 10 or Windows® 8 operating system.

If you run SQL Server® Standard edition, you must purchase a per core license or a server + CAL license.

- Install on a Windows Server® 2019 or Windows Server® 2016 operating system.

  ⓘ **Note:** For the majority of Metasys customers, a per core license maximizes cost savings and simplifies calculations. If you have a small ADX with very few users and a few devices, CAL licensing might suit your requirements.

Core licensing

To find the amount of cores on your system, complete the following steps:

1. Right-click the desktop taskbar, and click **Task Manager**.
2. Click the **Performance** tab.
3. In the lower section of the window, view the amount of cores on the machine and purchase core licenses accordingly.

ⓘ **Note:** When you purchase core licenses, you must license every core. Per core licenses are sold in packs of two or four. Core licensing applies to SQL Server® 2012 to SQL Server® 2019.

CAL licensing

- Purchase a server license for every server running SQL Server® software.
- You must calculate every potential user and every potential device that connects to the ADX, which could range from 1 to 100 users and 15 to 1000 engines for the ADX.

Table 22: Per core and server + CAL licensing

Type of license	License requirements	Usage example	Note
Per core: Physical environment	License all physical cores on the server.	Covers unlimited devices and users that connect to the server. If the ADX computer running SQL Server software has multiple cores in the processor, purchase one license for each physical core in the process. For a split ADX with the Metasys Advanced Reporting System. Purchase one core license for each physical core in the processor for both the database server computer and the web application server computer.	For information on how to purchase CALs, refer to the following site: http://www.microsoft.com/licensing/about-licensing/client-access-license.aspx. For information on how to calculate the number of cores in your system, refer to the following site: http://download.microsoft.com/download/4/4/5/445627B4-9AB0-4AED-BCCD-C7AC5ADAF6B2/CoreFactorTable_4_1_2014.pdf Microsoft assessment and planning toolkit https://www.microsoft.com/en-us/download/details.aspx?id=7826
Per core: Virtual environment	License all processing cores of the VM environment, not the number of servers installed on the VM.	Covers unlimited devices and users that connect to the server.	See the previous note section.

Table 22: Per core and server + CAL licensing

Type of license	License requirements	Usage example	Note
Server + CAL: Device	Purchase a server license for every server running SQL Server software. Purchase a CAL for every device that accesses the ADX server.	If you have 15 NAEs, SNCs, or SNEs connected to the ADX, you require 15 device CALs. A device CAL is the best choice if your organization has users who access the Metasys network by sharing the same computer during their work shifts.	Device CALs are independent of the number of users who access the ADX.
Server + CAL: User	Purchase a server license for every server running SQL Server software. Purchase a CAL for every user who accesses the ADX server.	If you have two users who access an ADX from different locations, you require 2 user CALs, regardless of whether they use SMP or Metasys UI for access, and regardless of the number of computers they use for that access. A user CAL is the best choice if your organization has Metasys users who need roaming access to the Metasys network using multiple computers.	User CALs are independent of the number of computers users use for that access.

Every site requires a combination of both device and user CALs.

Operating System - Device CALs: A device CAL is required for every device that accesses the ADX server, regardless of the number of users who access the ADX. A device CAL is the best choice if your organization has users who access the Metasys network by sharing the same computer during their work shifts. Additionally, each Metasys network engine (SNEs, SNCs, NAEs) requires one device CAL. For example, if 15 network engines are connected to the ADX, a total of 15 device CALs are required, on for each engine. Similarly, if 100 network engines are connected to the ADX, a total of 100 device CALs are required. Devices that do not access the server directly, such as IP controllers, do not require a CAL.

Operating System - User CALs: Every user who accesses the ADX server requires a user CAL, regardless of whether they use SMP or Metasys UI for access, and regardless of the number of computers they use for that access. A user CAL is the best choice if your organization has users who need roaming access to the Metasys network by logging into multiple Metasys Servers. For example, if two users log in to the ADX from different locations, two user CALs are required. Or if 10 users log in to the ADX, 10 user CALs are required.

Another example is a security guard station. During different shifts, security guards often use a single workstation, which requires the use of only one **device CAL**. However, if the security guards logs into multiple workstations throughout the facility, one **user CAL** per guard is required. In this example, a single user CAL is more cost-effective, because a single ADX connection requires only one user CAL.

Total Number of CALs: The total number of device and user CALs required equals the total number of devices and users connected to the ADX.

- **Example One:** If you have 100 network engines and 10 users who use different workstations to log in, you need 110 CALs (100 device CALs and 10 user CALs).
- **Example Two:** If you have 100 network engines and 10 users who use the same workstation to log in, you need 101 device CALs (100 device CALs for the SNCs and 1 device CAL for workstation).
- **Example Three:** If you have 10 network engines and 100 users who use different workstations to log in, you need 110 CALs (10 device CALs and 100 user CALs).

Table 23 lists the ADX software components and examples of what CAL combinations are required. Refer to the *Metasys® System Configuration Guide (LIT-12011832)* for the number of devices an ADX supports.

Table 23: ADX License and CAL Examples

ADX/MVE Offering	Recommended Number of CALs to Purchase	Windows Operating System CAL Examples
ADX10 and MVE (up to 10 ADX/MVE users)	5	5 CALs = 2 user CALs + 3 device CALs
		5 CALs = 3 user CALs + 2 device CALs
	15	15 CALs = 10 user CALs + 5 device CALs
		15 CALs = 8 user CALs + 7 device CALs
ADX25 and MVE (up to 25 ADX/MVE users)	30	30 CALs = 25 user CALs + 5 device CALs
		30 CALs = 10 user CALs + 20 device CALs
ADX50 and MVE (up to 50 ADX/MVE users)	60	60 CALs = 50 user CALs + 10 device CALs
		60 CALs = 10 user CALs + 50 device CALs
ADX100 and MVE (up to 100 ADX/MVE users)	110	110 CALs = 100 user CALs + 10 device CALs
		110 CALs = 10 user CALs + 100 device CALs

If you purchase Metasys system software separately from the hardware, use Table 23 to determine how many CALs you need to purchase from Microsoft. For more details, see Purchasing and designating CALs.

Purchasing and designating CALs

You need to purchase one additional device CAL for every network engine added to your Metasys system. You may also need to purchase additional user CALs as you expand the number of authorized Metasys system users. If you currently have an ADS and you expand your system to require more than 10 connections, you must upgrade to an ADX and purchase the appropriate number of CALs.

For CAL purchasing information, log in to the Johnson Controls employee portal website, go to the Tools & Applications page, then click the **Computer Price List** link in the Procurement/Purchasing section. This page contains the necessary information on how to access the Insight/Johnson Controls website (http://www.insight.com/jci) that contains information about purchasing CALs.

When you purchase CALs, you receive a paper certificate from Microsoft. There is no method in the operating system to designate or configure the number of device or user CALs. So make sure you keep the Microsoft CALs certificate in safekeeping at the customer site in case of an audit. You may be subject to a fine if a security audit reveals that your system is not correctly licensed.

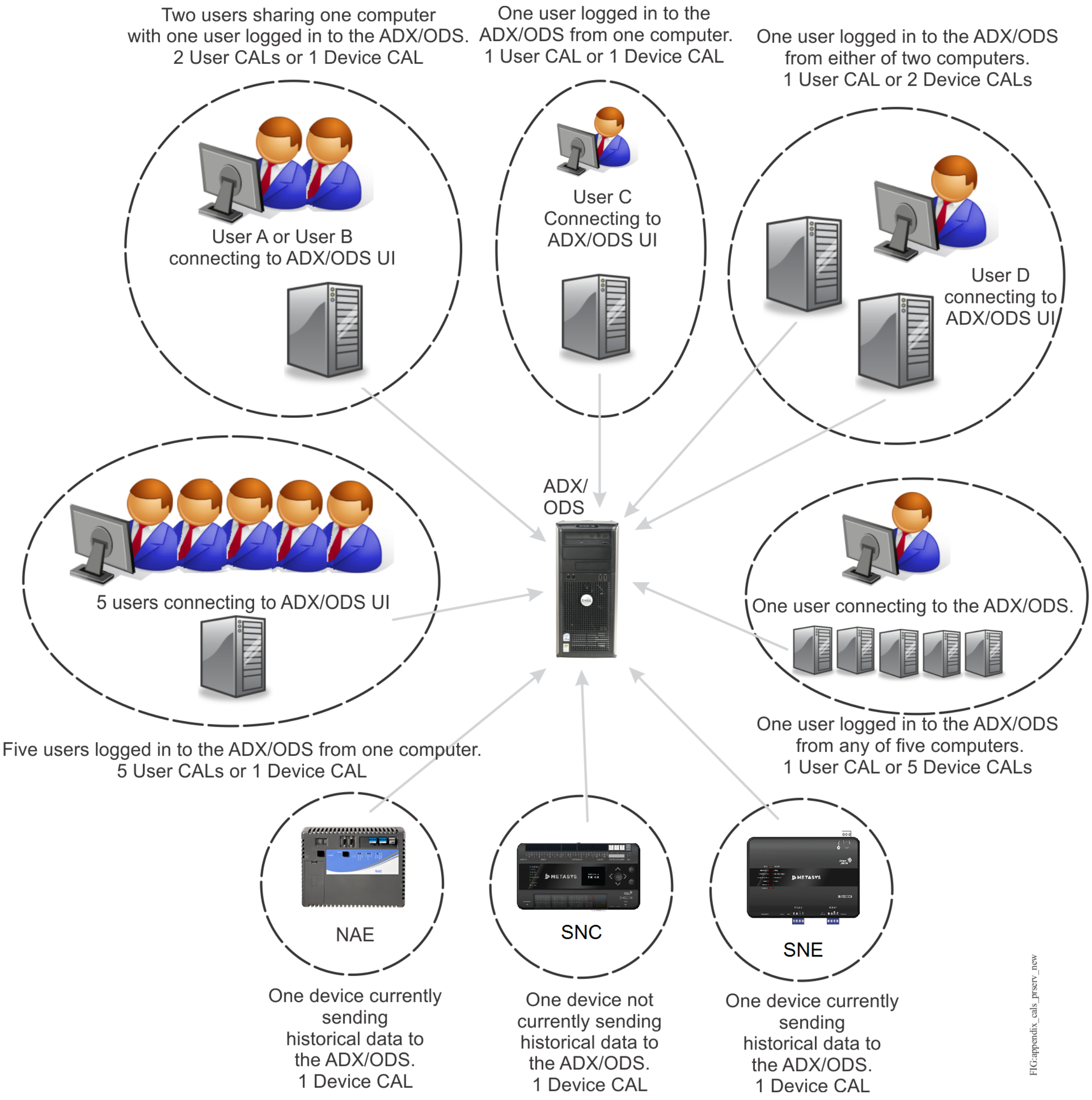
If Metasys system software is purchased separately, the customer is responsible for purchasing the correct number of CALs and for properly designating each CAL. A device CAL cannot be transferred to a user CAL, or vice versa. If a Metasys ADS/ADX Ready computer is purchased, the proper number of CALs come with the purchase, so no additional CALs are required. You must purchase additional CALs if the number of devices exceeds 5 or 10, depending on the size of the purchased Metasys system. Ultimately, the customer must determine how to split the total number of CALs between device and user.

For additional information on CALs, licensing, and downgrading operating system CALs, refer to http://www.microsoft.com/licensing/about-licensing/client-access-license.aspx.

Licensing modes and CAL examples

Figure 36 illustrates the use of CALs in a Metasys network.

Figure 36: Example Network in Per Device or Per User Operating System Licensing Mode


Two users sharing one computer
with one user logged in to the ADX/ODS.
2 User CALs or 1 Device CAL
One user logged in to the
ADX/ODS from one computer.
1 User CAL or 1 Device CAL
One user logged in to the ADX/ODS
from either of two computers.
1 User CAL or 2 Device CALs
User A or User B
connecting to ADX/ODS UI
User C
Connecting to
ADX/ODS UI
User D
connecting to
ADX/ODS UI
ADX/
ODS
5 users connecting to ADX/ODS UI
One user connecting to the ADX/ODS.
Five users logged in to the ADX/ODS from one computer.
5 User CALs or 1 Device CAL
One user logged in to the ADX/ODS
from any of five computers.
1 User CAL or 5 Device CALs
NAE
SNC
SNE
One device currently
sending
historical data to
the ADX/ODS.
1 Device CAL
One device not
currently sending
historical data to
the ADX/ODS.
1 Device CAL
One device currently
sending
historical data to
the ADX/ODS.
1 Device CAL
FIG:appendix_cals_prserv_new

ADS/ADS-Lite and non-server based OAS requirements

The ADS/ADS-Lite or non-server based OAS software does not come with, and does not require, device or user CALs. Only the server-based ADX or OAS requires CALs.

To avoid ADS/ADS-Lite or non-server based OAS connection and network communication performance issues, the number of users and the number of network engines and ADS/ADS-Lite or non-server based OAS computers that transfer trend data, event messages, and audit messages should not exceed 10. If a Metasys site with a single ADS/ADS-Lite or non-server based

OAS configured as the Site Director and default repository exceeds that number of connections, consider one of the following options:

- Configure one ADS/ADS-Lite or non-server based OAS to be the Site Director. Install and configure another ADS/ADS-Lite or non-server based OAS (or more) to provide the ADS repository function. When you install a separate ADS/ADS-Lite or non-server based OAS to provide the repository function, it allows you to dedicate five connections on the alternate ADS/OAS for system users and another five connections on the alternate ADS/ADS-Lite or non-server based OAS to network engines and ADS/ADS-Lite or non-server based OAS computers for transferring trend data, event messages, or audit messages.

ⓘ **Note:** The ADS/ADS-Lite or non-server based OAS cannot be the Site Director for another ADS/ADS-Lite or non-server based OAS of any type.

- Upgrade to an ADX or server-based OAS. Configure the Windows Server of the ADX/OAS computer with the number of CALs equal to the total number of users and devices accessing the ADX/OAS.

Refer to the *Metasys® System Configuration Guide (LIT-12011832)* for performance guidelines and limitations.

Microsoft SQL Server licensing requirements

All versions of Microsoft SQL Server Standard or Enterprise software use a **per core** licensing model. The SQL Server Express versions, however, do not require licensing. To determine the licensing needs for SQL Server Standard or Enterprise software that is installed on a Metasys Server:

- count the number of cores in the processor
- purchase the adequate number of core licenses

To assist you in counting the number of processor cores, refer to the specifications provided by the computer manufacturer or download the free Microsoft Assessment and Planning Toolkit (https://www.microsoft.com/en-us/download/details.aspx?id=7826). This toolkit may require the assistance from an IT professional. You may also consult the Microsoft Core Factor Table available at http://go.microsoft.com/fwlink/?LinkID=229882.

After you determine the number of processor cores, purchase the appropriate number of core licenses to allow the ADX computer to access the SQL Server database. If the ADX computer running SQL Server software has multiple cores in the processor, purchase one license for each physical core in the processor. For example, if the computer has a single quad-core processor, purchase four core licenses.

For a split ADX without the Metasys Advanced Reporting System, SQL Server software is installed only on the database server. You must purchase one core license for each physical core in the processor of the database server.

For a split ADX with the Metasys Advanced Reporting System, the database engine component of SQL Server software is present on the database server, and the reporting services component of SQL Server software is installed on the web/application server. You must purchase one core license for each physical core in the processor for **both** the database server and the web/application server.

Table 24 lists the number of core licenses required based on the number of physical cores in the processor.

Table 24: SQL Server license requirements

Physical Cores in the Processor	Core Licenses Required (SQL Server Standard/Enterprise software requires a minimum of four core licenses, even for processors with less than four cores.)
1	4
2	4
4	4
6	6
8	8

Appendix: SNMP agent protocol implementation

This appendix provides information for network managers to interpret the SNMP traps and Gets received by the Metasys system and provides explanations related to available agent functionalities. The Trap examples section includes several Trap message examples for your reference. The information applies to Metasys systems at Release 3.0 and later.

Overview

The Metasys SNMP agent implementation provides IP standard SNMP functionality in the Metasys system, enabling network administrators to manage Metasys network performance, find and resolve issues related to the Metasys network, and plan for future growth of the Metasys system. SNMP uses standard SNMP Versions 1, 2C, and 3 (which excludes SNMP encryption and authentication support). The Metasys system allows delivery of unsecured SNMP traps for Metasys alarm events by using a Network Management System (NMS). The Metasys SNMP agent also can monitor Metasys system point objects, select diagnostic attributes, and control sequence objects. You can configure the filter on the agent using the filtering capabilities of the DDA.

Limitations

The following are the limitations of NMS and Metasys SNMP agent functionality:

- NMS does not provide the ability to acknowledge and/or discard Alarms by using an SNMP Set message.
- NMS cannot modify the supervisory device by using an SNMP Set message.
- Metasys SNMP Agent functionality does not allow the NMS to detect when the supervisory device suffers a power failure or to initiate any action based on such detection.
- SNMP Get requests are not proxied through the site; that is, you must query the device of interest directly and not through the Site Director.
- With the SNMP Version 3 implementation, user authentication, and data encryption are not available for SNMP traps and Gets.
- The Get Bulk request, which returns data from multiple objects with one request, is not supported.

Metasys SNMP MIB files

Three Johnson Controls® MIB files are provided on the product media and on the Metasys system website for download https://my.jci.com/sites/BE/NABAS/Pages/Metasys_System_Extended_Architecture/Metasys_System_Extended_Architecture_Deployment/deployment/5_2_MIB.aspx (Table 25). The NMS software can read these MIB files, as well as the standard MIB files.

Table 25: List of Johnson Controls and Standard MIB Files

Johnson Controls MIB Files	Standard MIB Files [1]
jcicontrolsgroup.mi2	SNMPV2_MIB.mib
johnsoncontrolsinc.mi2	SNMPV2_SMI.mib
msea.mi2	SNMPV2_TC.mib

[1] Standard MIB files are available on the Internet.

These MIB files define the data available from the Metasys SNMP feature. They provide the OIDs that describe the traps and point types available in the Metasys system. For example, an OID is available to describe the alarm state of a point. Loading the MIB files into the NMS provides translation of the Metasys data.

Enterprise ID number

The assigned enterprise ID number for Johnson Controls is 4399. This number is part of all OIDs used in the Metasys system.

SNMP traps

Trap format

When an object with an alarm extension generates an event in the Metasys system, the SNMP service sends a trap to the NMS. No matter what type of event occurs, the Trap OID sends out the same set of attributes. Table 26 lists the attributes.

Configuring trap filtering

Of the available attributes listed in Table 26, configure the NMS interface to filter the attributes to be trapped. You also must select these attributes when you configure the SNMP DDA alarm notifications and destinations in the device object. For details, refer to the *NAE Commissioning Guide (LIT-1201519)*, *SNE Commissioning Guide (LIT-12013352)*, *SNC Commissioning Guide (LIT-12013295)*, *Open Application Server (OAS) Commissioning Guide (LIT-12013243)*, *ODS Commissioning Guide (LIT-12011944)*, and the *ADS/ADX Commissioning Guide (LIT-1201645)*. This list applies to Metasys alarm events only.

Table 26: Available Attributes for Trap Filtering

Field Names		
ackRequired	eventValue	itemName
eventDetectionTimestamp	evPriority	SiteName
eventMessage	itemCategory	units
eventPreviousStatus	itemDescription	
eventUniqueIdentifier	itemFullyQualifiedReference	

Agent restart trap

When an Agent Restart occurs, a coldstart trap is sent when the supervisory device (NAE, for example) powers on. Table 27 lists the attributes that are sent.

Table 27: Attributes for Coldstart Trap

Attribute Names			
hostName	ipAddress	macAddress	subnetMask

Alarm raised trap

When an object with an alarm extension generates an event in the *Metasys* system, the SNMP Agent sends the same Alarm Type that was raised in the system (*Metasys* Server or network engine). Examples include High Warning and Low Alarm. Each Trap OID also sends the attribute values that were selected for the trap (Table 26).

Alarm clear trap

When an alarm Return to Normal state occurs, the SNMP Agent reacts in the same manner as when the alarm was raised. In this way, the Alarm situation is cleared with a NormalEvent message.

Alarm synchronization

The Metasys SNMP Agent does not support Alarm Synchronization, a function that indicates to the NMS which Metasys objects went into alarm while the NMS was offline. The SNMP Agent assumes that the NMS received the alarm and, therefore, does not rebroadcast it. Even though alarm synchronization is not performed, the SNMP Agent allows the NMS to poll points and device attributes to determine their statuses. From this information, the NMS can determine which points are reporting Alarms and react accordingly.

Trap cases

Supervisory device offline/online

According to how the SNMP is configured, the Metasys Site Director sends an offline/online notification when any of its children (network engines) are considered offline or online. These events have a structure similar to the Alarm Raised structure, and reports the same set of attributes (Table 26). The eventValue attribute indicates **Offline** or **Online**.

When a supervisory device is rebooted or restored after a power failure, the SNMP Agent on the Site Director sends the offline/online notification, and the supervisory device sends the agent coldstart information.

Field device offline/online

Field devices (for example, FECs and VMAs) are treated the same way as supervisory devices. If the field device has the appropriate alarm extension defined, the controller generates online/offline alarms (Traps) as they occur.

Field device disable/enable

When the user or a process disables communication to a field device, the SNMP Agent sends a trap regarding the Disable command in a similar manner as the Alarm Raised trap. The eventValue indicates Comm Disabled.

When a Comm Enabled command to the device occurs, the SNMP Agent sends a trap regarding the Enable command as well as a separate alarm trap regarding the return to online status.

SNMP Get requests

SNMP Get requests allow the NMS to request information for a specific variable. The SNMP agent, upon receiving a Get message, issues a GET-RESPONSE message to the NMS with either the information requested or an error indication as to why the request cannot be processed.

The Metasys SNMP Agent allows you to perform SNMP Gets on pre-defined OIDs of certain objects (for example, Analog Value [AV], Binary Value [BV], and Multistate Value [MV] objects). For a list of the attributes that are available for polling, see Table 28.

ⓘ **Note:** To use Gets, you must query the specific supervisory device (NAE55, NIE55, or NCE25, for example) on which the object appears. Site Directors do not forward Get requests to other devices on the site and you cannot perform Gets on ADSs/ADXs/ODSs.

The Metasys SNMP Agent also allows you to determine the health of the device by polling the OIDs listed under Table 29. These attributes include data such as battery condition and object count.

You can poll all the points on the NAE, but realize there is a throttle on SNMP Gets, which is two requests per second on an NAE55 and one request per second on an NAE45. For example, polling 500 points on a single NAE takes about five minutes.

Get request definition

The length of the OID for a Get request has one limitation relating to the SNMP protocol: the maximum number of subidentifiers per message is 128 characters. The reference of the item or object you are requesting is contained within these subidentifiers. To determine the item reference you should use, log in to the Metasys user interface and open the Focus window of the item/object. Locate the Item Reference field under the Advanced view of the Focus window. The format of the fully qualified item reference is:

Site:Device/Item

The only part of this string that you need to specify is the Item section. Here is an example:

MyADS:NAE-1/N2-1/AHU-3/ZN-T

The only part of this item reference that is required is: **N2-1/AHU-3/ZN-T**.

Get request base OID

The Base OID for any Get Request is as follows:

1.3.6.1.4.1.4399.2.1.1.1.1.4.1.1.x.y

where **x** is an integer that represents the attribute of the point (Table 28) and **y** is an ASCII representation for the name of the Metasys point.

Table 28: Point Attributes

x	Description
.85	Present Value
.103	Reliability
.117	Units
.661	Display Precision
.1006	Alarm State
.32527	Item Reference

The two primary Get Requests are the Point Attribute Get Request and the Device Diagnostics Get Request.

Point attribute Get request

This Get Request obtains point attribute information.

Base OID

1.3.6.1.4.1.4399.2.1.1.1.1.4.1.1.x.y

where **x** is an integer that represents the attribute of the point and **y** is an ASCII representation for the name of the *Metasys* point (Table 28).

Example #1

1.3.6.1.4.1.4399.2.1.1.1.1.4.1.1.85.3.65.86.49

Returned value: present value of Metasys object called **AV1**.

In this example, the Present Value attribute breaks out as:

1.3.6.1.4.1.4399.2.1.1.1.1.4.1.1.85

The name of the Metasys point breaks out as:

3.65.86.49

where the first digit **(3)** is the length, and the remaining digits are the ASCII representations of the letters **(AV1)**.

Example #2

1.3.6.1.4.1.4399.2.1.1.1.1.4.1.1.1006.10.69.110.101.114.103.121.46.66.86.49

Returned Value: point alarm state of a Metasys object called **Energy.BV1**.

In this example, the Alarm State attribute breaks out as:

1.3.6.1.4.1.4399.2.1.1.1.1.4.1.1.1006

The name of the Metasys point breaks out as:

10.69.110.101.114.103.121.46.66.86.49

where the first digit **(10)** is the length, and the remaining digits are the ASCII representations of the letters **(Energy.BV1)**.

Device diagnostic attributes

This Get Request obtains device diagnostic information.

Base OID

1.3.6.1.4.1.4399.2.1.1.1.1.3.x

where **x** is an integer that represents the attribute of the point (Table 29).

Table 29: Device Diagnostic Attributes

x	Description
.647	Battery Condition
.650	Change of Value Receives Per Minute
.651	Change of Value Transmits Per Minute
.844	Object Count
.2395	Estimate Flash Available
.2579	CPU Temp (Not Available on NAE-45)
.2580	Board Temperature
.2581	Memory Usage
.2582	Object Memory

Table 29: Device Diagnostic Attributes

x	Description
.2583	CPU Usage
.2584	Flash Usage
.32565	Pager Dial Status

Example

1.3.6.1.4.1.4399.2.1.1.1.1.3.2580

Returned value: board temperature

In this example, the Board Temperature attribute breaks out as:

1.3.6.1.4.1.4399.2.1.1.1.1.3.2580

Translating attribute values

As highlighted in the Trap Examples section, each Trap OID sends the same set of attributes. You can translate attributes values (evPreviousState) using the key values in the following table.

Table 30: Device Diagnostic Attributes

Key	Text	Key	Text
0	Normal	**68**	Alarm
1	Fault	**69**	Trouble
2	Off Normal	**70**	Status
3	High Limit	**71**	Offline
4	Low Limit	**72**	Shutdown
64	Low Warning	**73**	Unreliable
65	High Warning	**75**	Online
66	Low Alarm	**65535**	Unknown Previous State
67	High Alarm		

Example

The difference between the SNMP Trap generated for a binary point that goes into Alarm and one whose status transitions to Return to Normal is outlined in the following table.

Table 31: SNMP Trap Attribute Example

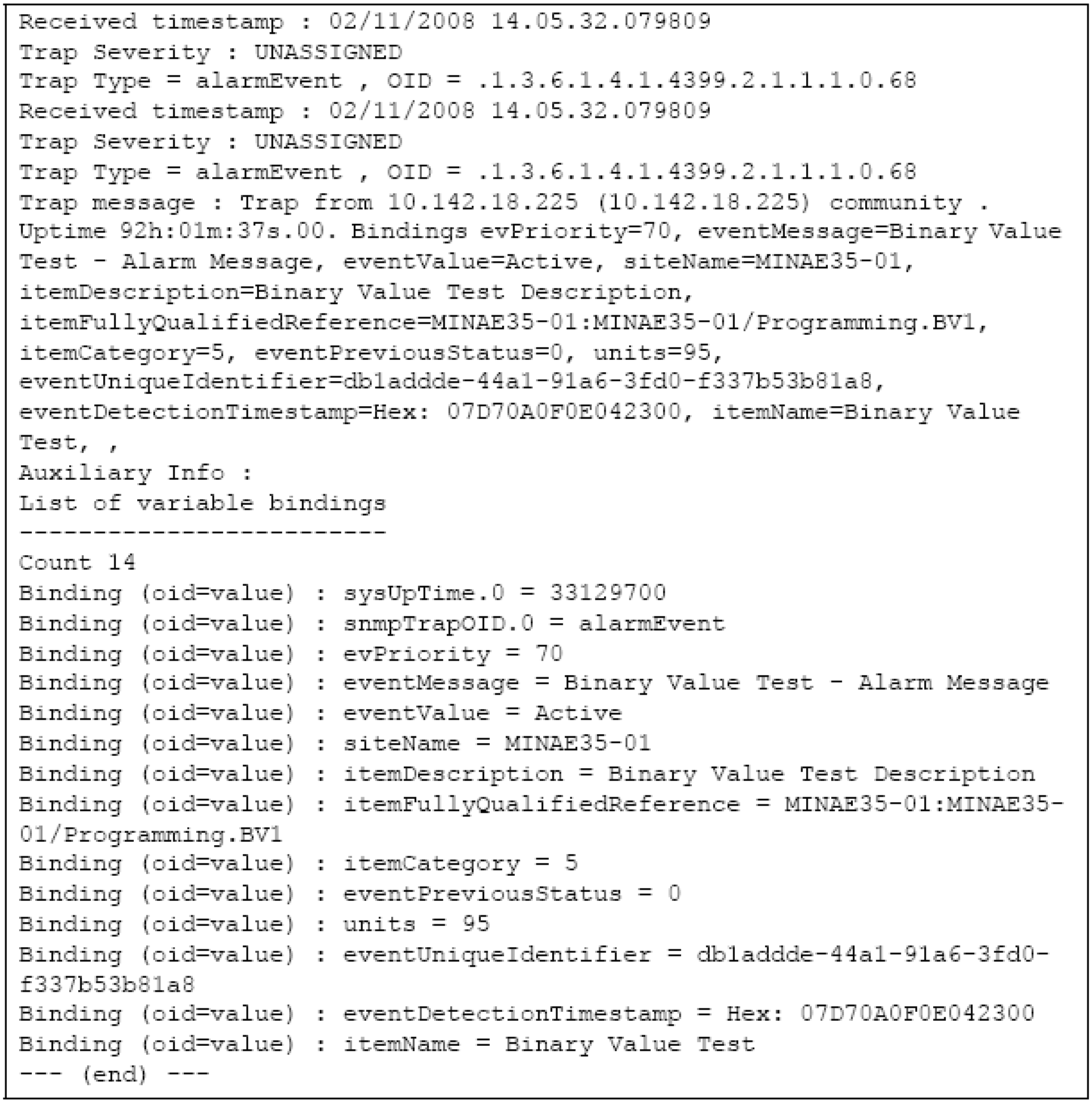
SNMP Trap Attribute	Alarm Value	Normal Value
snmpTRAPOID.O	alarmEvent	normalEvent
EventValue	Active	Inactive
EventPreviousStatus	0	68
EventMessage	Alarm message defined in the Metasys Site Management Portal UI	Return to Normal message defined in Metasys Site Management Portal UI

Trap examples

The following sections shows several trap example captured from a live system.

Binary point alarm

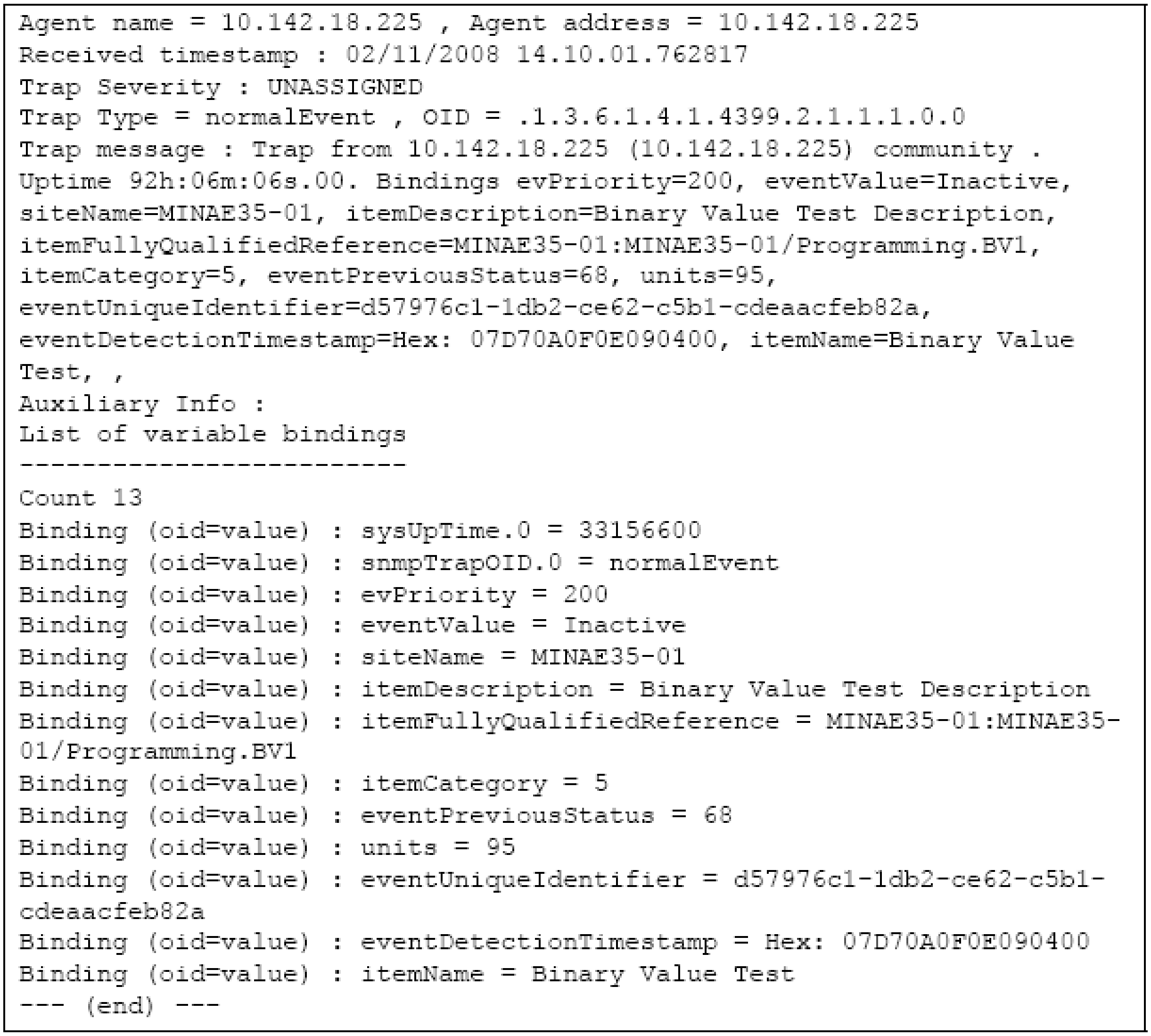
Figure 37: Binary Point Alarm Example



```
Received timestamp : 02/11/2008 14.05.32.079809
Trap Severity : UNASSIGNED
Trap Type = alarmEvent , OID = .1.3.6.1.4.1.4399.2.1.1.1.0.68
Received timestamp : 02/11/2008 14.05.32.079809
Trap Severity : UNASSIGNED
Trap Type = alarmEvent , OID = .1.3.6.1.4.1.4399.2.1.1.1.0.68
Trap message : Trap from 10.142.18.225 (10.142.18.225) community .
Uptime 92h:01m:37s.00. Bindings evPriority=70, eventMessage=Binary Value
Test - Alarm Message, eventValue=Active, siteName=MINAE35-01,
itemDescription=Binary Value Test Description,
itemFullyQualifiedReference=MINAE35-01:MINAE35-01/Programming.BV1,
itemCategory=5, eventPreviousStatus=0, units=95,
eventUniqueIdentifier=db1addde-44a1-91a6-3fd0-f337b53b81a8,
eventDetectionTimestamp=Hex: 07D70A0F0E042300, itemName=Binary Value
Test, ,
Auxiliary Info :
List of variable bindings
-------------------------
Count 14
Binding (oid=value) : sysUpTime.0 = 33129700
Binding (oid=value) : snmpTrapOID.0 = alarmEvent
Binding (oid=value) : evPriority = 70
Binding (oid=value) : eventMessage = Binary Value Test - Alarm Message
Binding (oid=value) : eventValue = Active
Binding (oid=value) : siteName = MINAE35-01
Binding (oid=value) : itemDescription = Binary Value Test Description
Binding (oid=value) : itemFullyQualifiedReference = MINAE35-01:MINAE35-
01/Programming.BV1
Binding (oid=value) : itemCategory = 5
Binding (oid=value) : eventPreviousStatus = 0
Binding (oid=value) : units = 95
Binding (oid=value) : eventUniqueIdentifier = db1addde-44a1-91a6-3fd0-
f337b53b81a8
Binding (oid=value) : eventDetectionTimestamp = Hex: 07D70A0F0E042300
Binding (oid=value) : itemName = Binary Value Test
--- (end) ---
```

Binary point return to normal

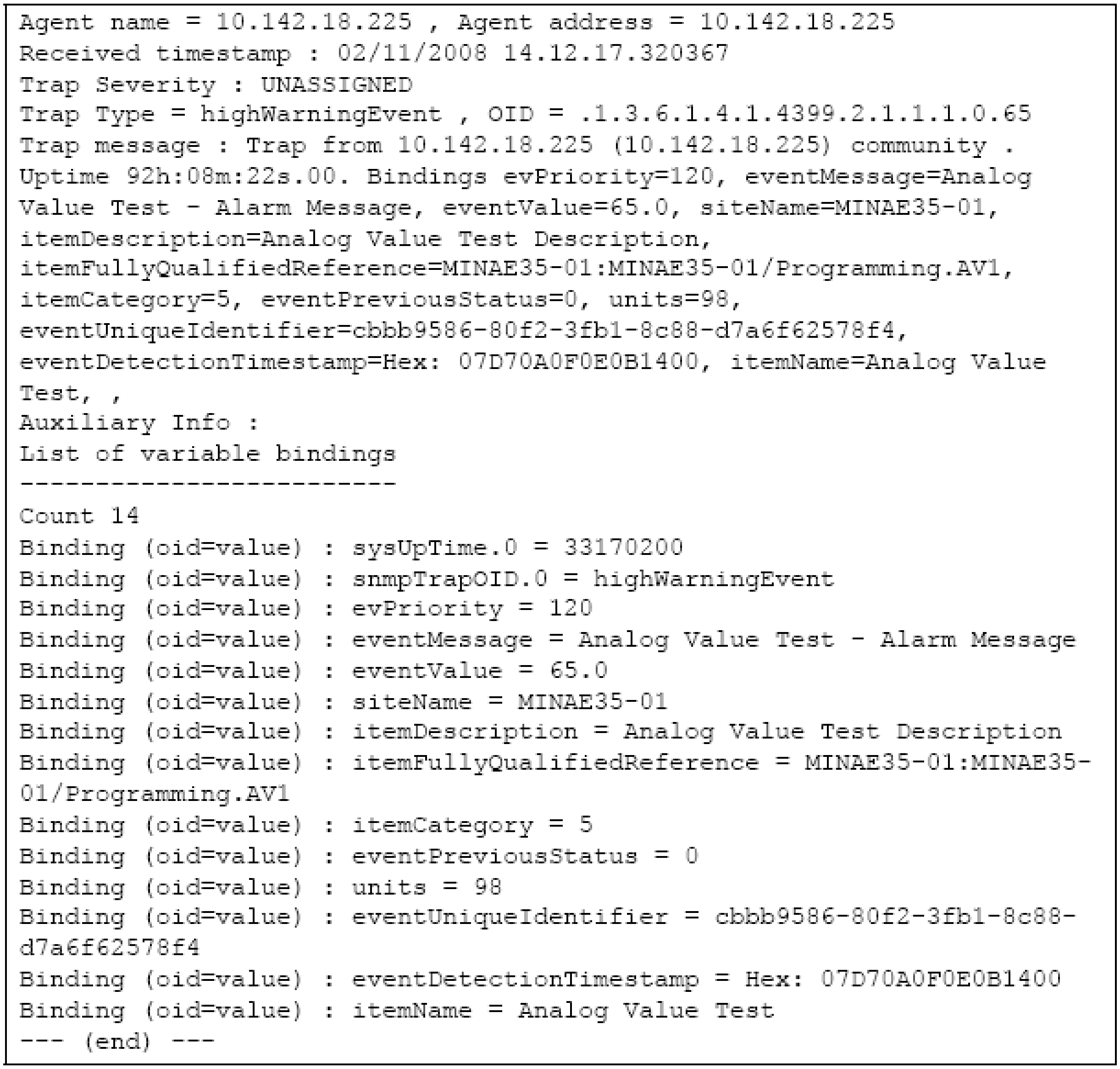
Figure 38: Binary Point Return to Normal



```
Agent name = 10.142.18.225 , Agent address = 10.142.18.225
Received timestamp : 02/11/2008 14.10.01.762817
Trap Severity : UNASSIGNED
Trap Type = normalEvent , OID = .1.3.6.1.4.1.4399.2.1.1.1.0.0
Trap message : Trap from 10.142.18.225 (10.142.18.225) community .
Uptime 92h:06m:06s.00. Bindings evPriority=200, eventValue=Inactive,
siteName=MINAE35-01, itemDescription=Binary Value Test Description,
itemFullyQualifiedReference=MINAE35-01:MINAE35-01/Programming.BV1,
itemCategory=5, eventPreviousStatus=68, units=95,
eventUniqueIdentifier=d57976c1-1db2-ce62-c5b1-cdeaacfeb82a,
eventDetectionTimestamp=Hex: 07D70A0F0E090400, itemName=Binary Value
Test, ,
Auxiliary Info :
List of variable bindings
-------------------------
Count 13
Binding (oid=value) : sysUpTime.0 = 33156600
Binding (oid=value) : snmpTrapOID.0 = normalEvent
Binding (oid=value) : evPriority = 200
Binding (oid=value) : eventValue = Inactive
Binding (oid=value) : siteName = MINAE35-01
Binding (oid=value) : itemDescription = Binary Value Test Description
Binding (oid=value) : itemFullyQualifiedReference = MINAE35-01:MINAE35-
01/Programming.BV1
Binding (oid=value) : itemCategory = 5
Binding (oid=value) : eventPreviousStatus = 68
Binding (oid=value) : units = 95
Binding (oid=value) : eventUniqueIdentifier = d57976c1-1db2-ce62-c5b1-
cdeaacfeb82a
Binding (oid=value) : eventDetectionTimestamp = Hex: 07D70A0F0E090400
Binding (oid=value) : itemName = Binary Value Test
--- (end) ---
```

Analog point high warning

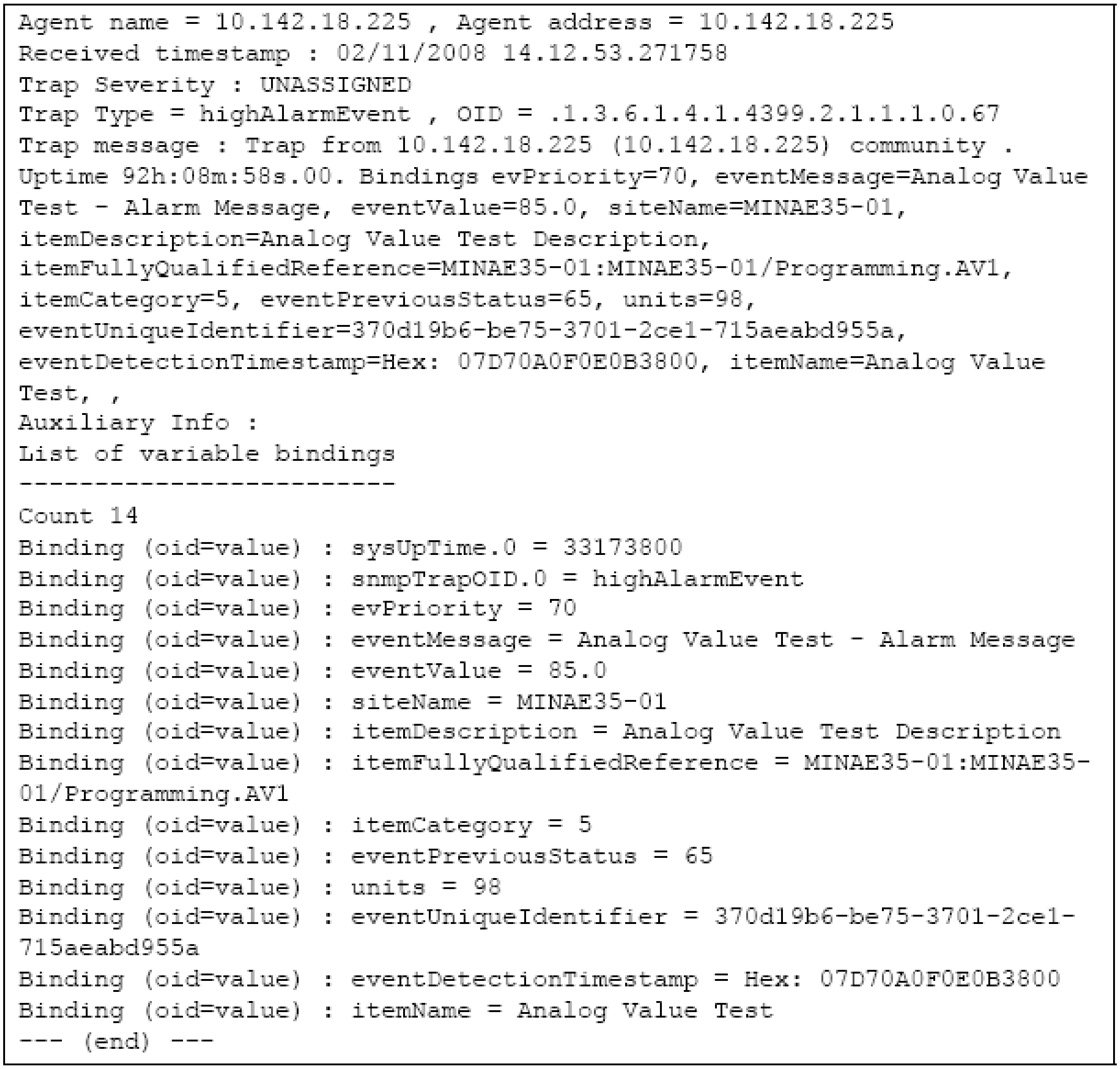
Figure 39: Analog Point High Warning



```
Agent name = 10.142.18.225 , Agent address = 10.142.18.225
Received timestamp : 02/11/2008 14.12.17.320367
Trap Severity : UNASSIGNED
Trap Type = highWarningEvent , OID = .1.3.6.1.4.1.4399.2.1.1.1.0.65
Trap message : Trap from 10.142.18.225 (10.142.18.225) community .
Uptime 92h:08m:22s.00. Bindings evPriority=120, eventMessage=Analog
Value Test - Alarm Message, eventValue=65.0, siteName=MINAE35-01,
itemDescription=Analog Value Test Description,
itemFullyQualifiedReference=MINAE35-01:MINAE35-01/Programming.AV1,
itemCategory=5, eventPreviousStatus=0, units=98,
eventUniqueIdentifier=cbbb9586-80f2-3fb1-8c88-d7a6f62578f4,
eventDetectionTimestamp=Hex: 07D70A0F0E0B1400, itemName=Analog Value
Test, ,
Auxiliary Info :
List of variable bindings
-------------------------
Count 14
Binding (oid=value) : sysUpTime.0 = 33170200
Binding (oid=value) : snmpTrapOID.0 = highWarningEvent
Binding (oid=value) : evPriority = 120
Binding (oid=value) : eventMessage = Analog Value Test - Alarm Message
Binding (oid=value) : eventValue = 65.0
Binding (oid=value) : siteName = MINAE35-01
Binding (oid=value) : itemDescription = Analog Value Test Description
Binding (oid=value) : itemFullyQualifiedReference = MINAE35-01:MINAE35-
01/Programming.AV1
Binding (oid=value) : itemCategory = 5
Binding (oid=value) : eventPreviousStatus = 0
Binding (oid=value) : units = 98
Binding (oid=value) : eventUniqueIdentifier = cbbb9586-80f2-3fb1-8c88-
d7a6f62578f4
Binding (oid=value) : eventDetectionTimestamp = Hex: 07D70A0F0E0B1400
Binding (oid=value) : itemName = Analog Value Test
--- (end) ---
```

Analog point high alarm

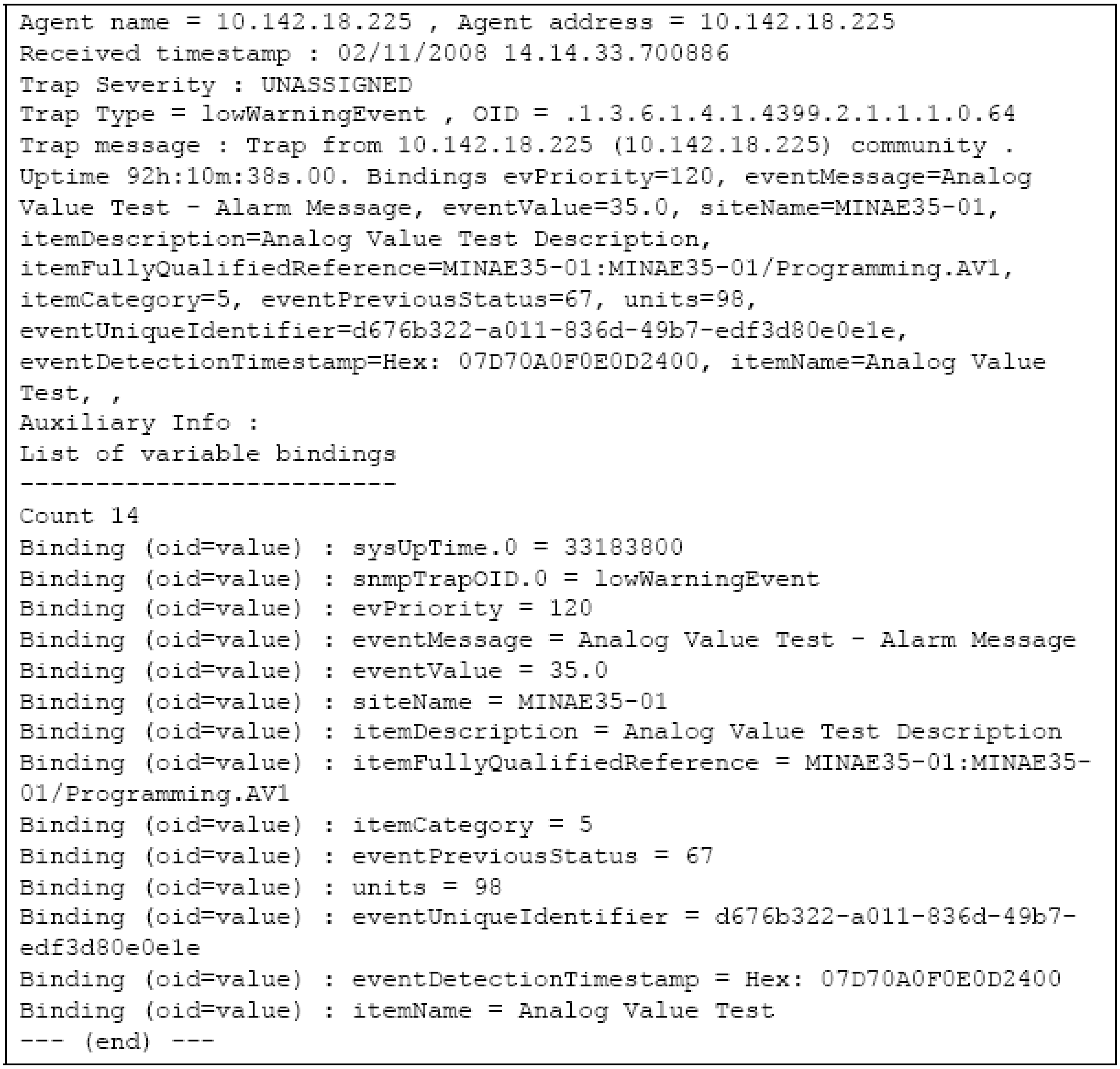
Figure 40: Analog Point High Alarm



```
Agent name = 10.142.18.225 , Agent address = 10.142.18.225
Received timestamp : 02/11/2008 14.12.53.271758
Trap Severity : UNASSIGNED
Trap Type = highAlarmEvent , OID = .1.3.6.1.4.1.4399.2.1.1.1.0.67
Trap message : Trap from 10.142.18.225 (10.142.18.225) community .
Uptime 92h:08m:58s.00. Bindings evPriority=70, eventMessage=Analog Value
Test - Alarm Message, eventValue=85.0, siteName=MINAE35-01,
itemDescription=Analog Value Test Description,
itemFullyQualifiedReference=MINAE35-01:MINAE35-01/Programming.AV1,
itemCategory=5, eventPreviousStatus=65, units=98,
eventUniqueIdentifier=370d19b6-be75-3701-2ce1-715aeabd955a,
eventDetectionTimestamp=Hex: 07D70A0F0E0B3800, itemName=Analog Value
Test, ,
Auxiliary Info :
List of variable bindings
-------------------------
Count 14
Binding (oid=value) : sysUpTime.0 = 33173800
Binding (oid=value) : snmpTrapOID.0 = highAlarmEvent
Binding (oid=value) : evPriority = 70
Binding (oid=value) : eventMessage = Analog Value Test - Alarm Message
Binding (oid=value) : eventValue = 85.0
Binding (oid=value) : siteName = MINAE35-01
Binding (oid=value) : itemDescription = Analog Value Test Description
Binding (oid=value) : itemFullyQualifiedReference = MINAE35-01:MINAE35-
01/Programming.AV1
Binding (oid=value) : itemCategory = 5
Binding (oid=value) : eventPreviousStatus = 65
Binding (oid=value) : units = 98
Binding (oid=value) : eventUniqueIdentifier = 370d19b6-be75-3701-2ce1-
715aeabd955a
Binding (oid=value) : eventDetectionTimestamp = Hex: 07D70A0F0E0B3800
Binding (oid=value) : itemName = Analog Value Test
--- (end) ---
```

Analog point low warning

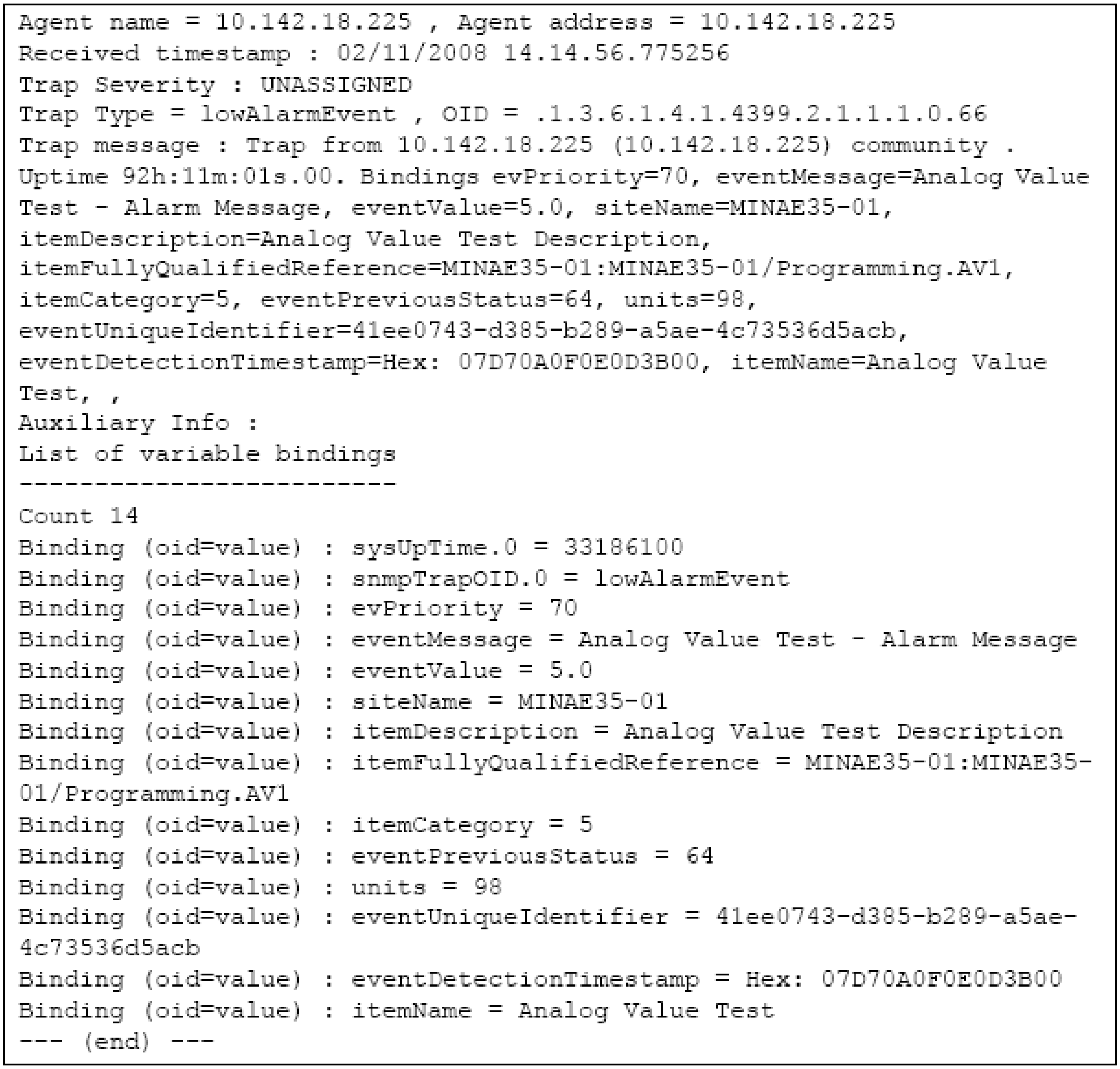
Figure 41: Analog Point Low Warning



```
Agent name = 10.142.18.225 , Agent address = 10.142.18.225
Received timestamp : 02/11/2008 14.14.33.700886
Trap Severity : UNASSIGNED
Trap Type = lowWarningEvent , OID = .1.3.6.1.4.1.4399.2.1.1.1.0.64
Trap message : Trap from 10.142.18.225 (10.142.18.225) community .
Uptime 92h:10m:38s.00. Bindings evPriority=120, eventMessage=Analog
Value Test - Alarm Message, eventValue=35.0, siteName=MINAE35-01,
itemDescription=Analog Value Test Description,
itemFullyQualifiedReference=MINAE35-01:MINAE35-01/Programming.AV1,
itemCategory=5, eventPreviousStatus=67, units=98,
eventUniqueIdentifier=d676b322-a011-836d-49b7-edf3d80e0e1e,
eventDetectionTimestamp=Hex: 07D70A0F0E0D2400, itemName=Analog Value
Test, ,
Auxiliary Info :
List of variable bindings
-------------------------
Count 14
Binding (oid=value) : sysUpTime.0 = 33183800
Binding (oid=value) : snmpTrapOID.0 = lowWarningEvent
Binding (oid=value) : evPriority = 120
Binding (oid=value) : eventMessage = Analog Value Test - Alarm Message
Binding (oid=value) : eventValue = 35.0
Binding (oid=value) : siteName = MINAE35-01
Binding (oid=value) : itemDescription = Analog Value Test Description
Binding (oid=value) : itemFullyQualifiedReference = MINAE35-01:MINAE35-
01/Programming.AV1
Binding (oid=value) : itemCategory = 5
Binding (oid=value) : eventPreviousStatus = 67
Binding (oid=value) : units = 98
Binding (oid=value) : eventUniqueIdentifier = d676b322-a011-836d-49b7-
edf3d80e0e1e
Binding (oid=value) : eventDetectionTimestamp = Hex: 07D70A0F0E0D2400
Binding (oid=value) : itemName = Analog Value Test
--- (end) ---
```

Analog point low alarm

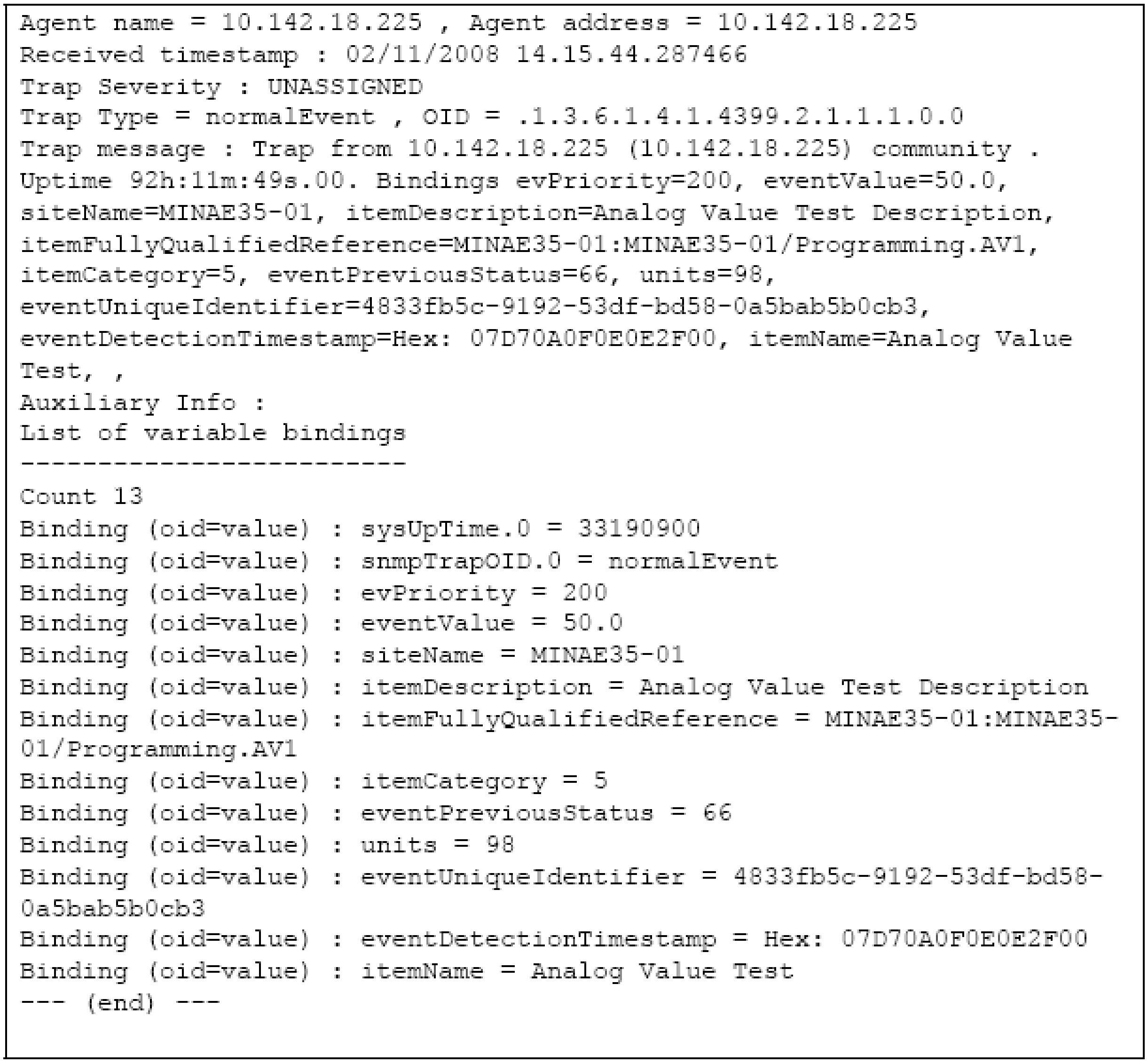
Figure 42: Analog Point Low Alarm



```
Agent name = 10.142.18.225 , Agent address = 10.142.18.225
Received timestamp : 02/11/2008 14.14.56.775256
Trap Severity : UNASSIGNED
Trap Type = lowAlarmEvent , OID = .1.3.6.1.4.1.4399.2.1.1.1.0.66
Trap message : Trap from 10.142.18.225 (10.142.18.225) community .
Uptime 92h:11m:01s.00. Bindings evPriority=70, eventMessage=Analog Value
Test - Alarm Message, eventValue=5.0, siteName=MINAE35-01,
itemDescription=Analog Value Test Description,
itemFullyQualifiedReference=MINAE35-01:MINAE35-01/Programming.AV1,
itemCategory=5, eventPreviousStatus=64, units=98,
eventUniqueIdentifier=41ee0743-d385-b289-a5ae-4c73536d5acb,
eventDetectionTimestamp=Hex: 07D70A0F0E0D3B00, itemName=Analog Value
Test, ,
Auxiliary Info :
List of variable bindings
-------------------------
Count 14
Binding (oid=value) : sysUpTime.0 = 33186100
Binding (oid=value) : snmpTrapOID.0 = lowAlarmEvent
Binding (oid=value) : evPriority = 70
Binding (oid=value) : eventMessage = Analog Value Test - Alarm Message
Binding (oid=value) : eventValue = 5.0
Binding (oid=value) : siteName = MINAE35-01
Binding (oid=value) : itemDescription = Analog Value Test Description
Binding (oid=value) : itemFullyQualifiedReference = MINAE35-01:MINAE35-
01/Programming.AV1
Binding (oid=value) : itemCategory = 5
Binding (oid=value) : eventPreviousStatus = 64
Binding (oid=value) : units = 98
Binding (oid=value) : eventUniqueIdentifier = 41ee0743-d385-b289-a5ae-
4c73536d5acb
Binding (oid=value) : eventDetectionTimestamp = Hex: 07D70A0F0E0D3B00
Binding (oid=value) : itemName = Analog Value Test
--- (end) ---
```

Analog point return to normal

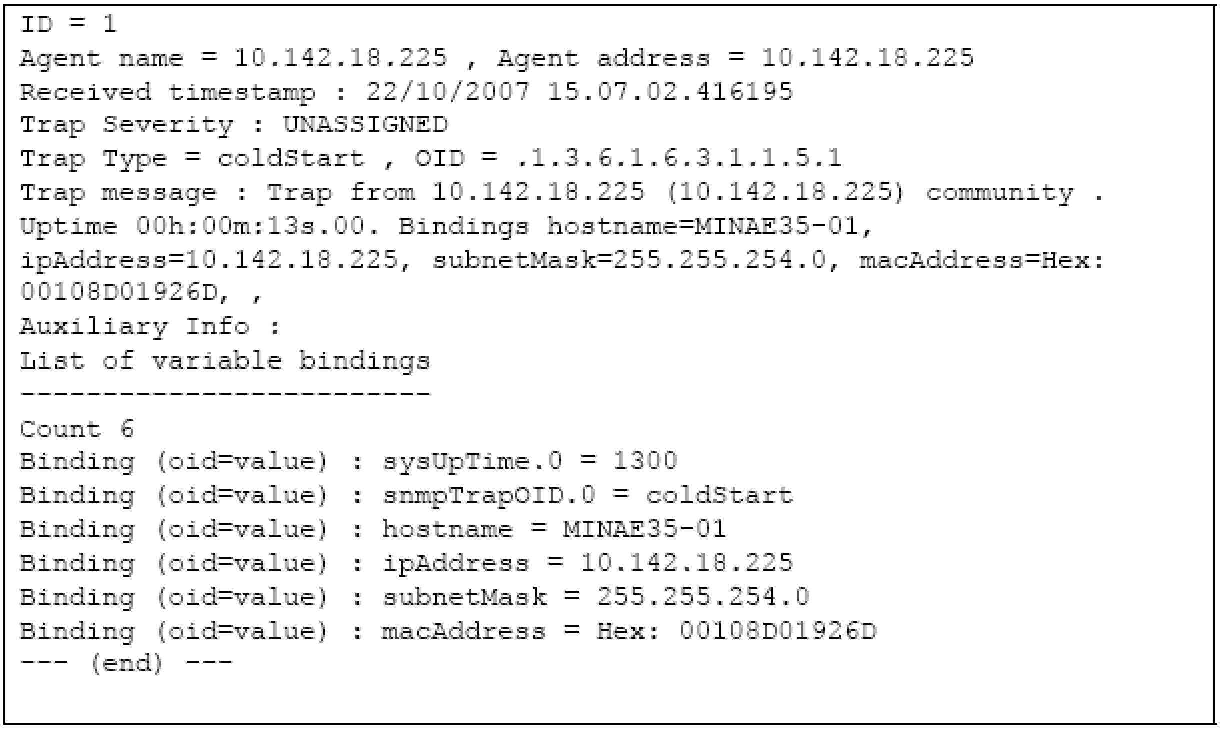
Figure 43: Analog Point Return to Normal



```
Agent name = 10.142.18.225 , Agent address = 10.142.18.225
Received timestamp : 02/11/2008 14.15.44.287466
Trap Severity : UNASSIGNED
Trap Type = normalEvent , OID = .1.3.6.1.4.1.4399.2.1.1.1.0.0
Trap message : Trap from 10.142.18.225 (10.142.18.225) community .
Uptime 92h:11m:49s.00. Bindings evPriority=200, eventValue=50.0,
siteName=MINAE35-01, itemDescription=Analog Value Test Description,
itemFullyQualifiedReference=MINAE35-01:MINAE35-01/Programming.AV1,
itemCategory=5, eventPreviousStatus=66, units=98,
eventUniqueIdentifier=4833fb5c-9192-53df-bd58-0a5bab5b0cb3,
eventDetectionTimestamp=Hex: 07D70A0F0E0E2F00, itemName=Analog Value
Test, ,
Auxiliary Info :
List of variable bindings
-------------------------
Count 13
Binding (oid=value) : sysUpTime.0 = 33190900
Binding (oid=value) : snmpTrapOID.0 = normalEvent
Binding (oid=value) : evPriority = 200
Binding (oid=value) : eventValue = 50.0
Binding (oid=value) : siteName = MINAE35-01
Binding (oid=value) : itemDescription = Analog Value Test Description
Binding (oid=value) : itemFullyQualifiedReference = MINAE35-01:MINAE35-
01/Programming.AV1
Binding (oid=value) : itemCategory = 5
Binding (oid=value) : eventPreviousStatus = 66
Binding (oid=value) : units = 98
Binding (oid=value) : eventUniqueIdentifier = 4833fb5c-9192-53df-bd58-
0a5bab5b0cb3
Binding (oid=value) : eventDetectionTimestamp = Hex: 07D70A0F0E0E2F00
Binding (oid=value) : itemName = Analog Value Test
--- (end) ---
```

Supervisory device agent restart (ColdStart)

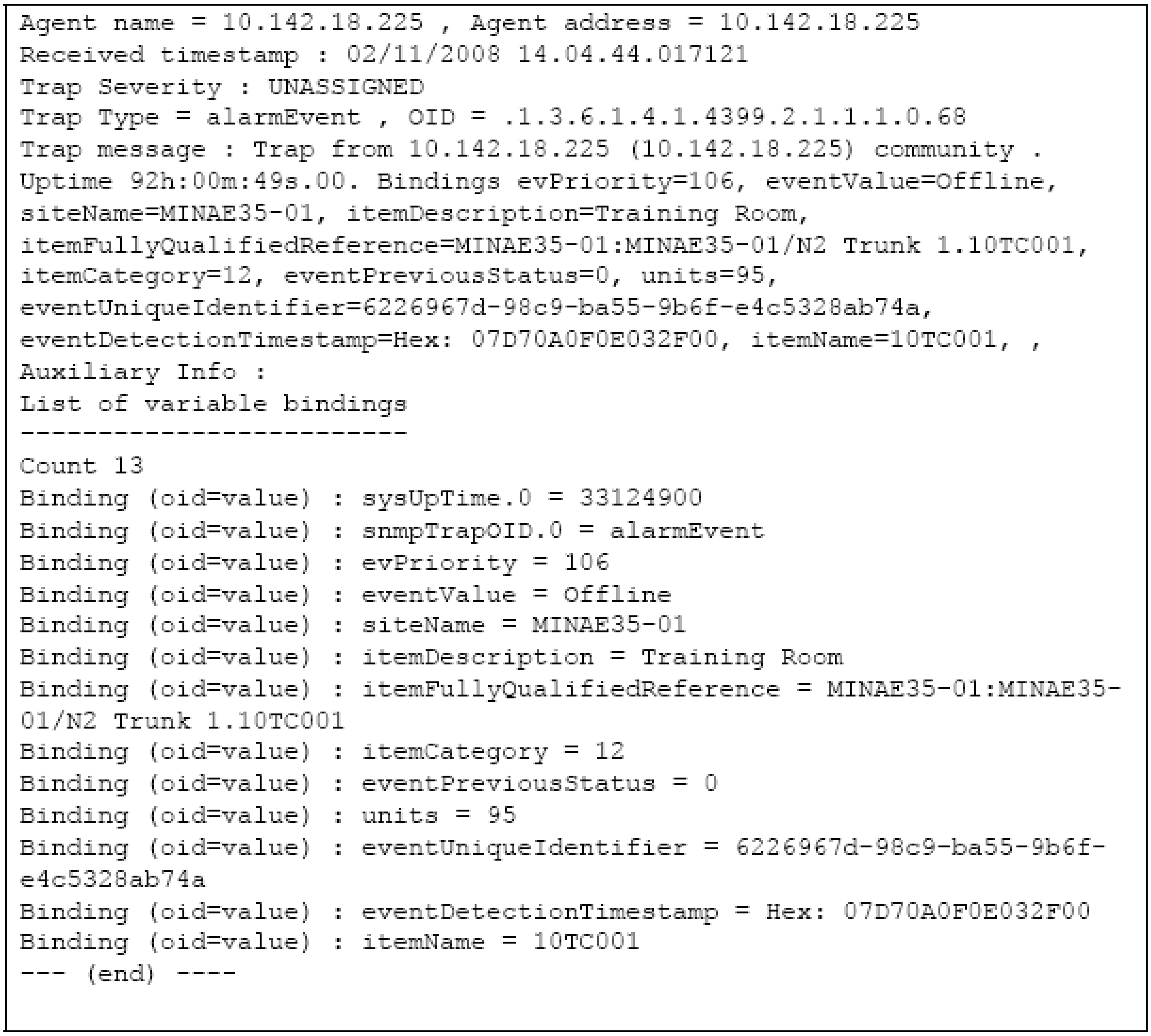
Figure 44: Supervisory Device Agent Restart (ColdStart)



```
ID = 1
Agent name = 10.142.18.225 , Agent address = 10.142.18.225
Received timestamp : 22/10/2007 15.07.02.416195
Trap Severity : UNASSIGNED
Trap Type = coldStart , OID = .1.3.6.1.6.3.1.1.5.1
Trap message : Trap from 10.142.18.225 (10.142.18.225) community .
Uptime 00h:00m:13s.00. Bindings hostname=MINAE35-01,
ipAddress=10.142.18.225, subnetMask=255.255.254.0, macAddress=Hex:
00108D01926D, ,
Auxiliary Info :
List of variable bindings
-------------------------
Count 6
Binding (oid=value) : sysUpTime.0 = 1300
Binding (oid=value) : snmpTrapOID.0 = coldStart
Binding (oid=value) : hostname = MINAE35-01
Binding (oid=value) : ipAddress = 10.142.18.225
Binding (oid=value) : subnetMask = 255.255.254.0
Binding (oid=value) : macAddress = Hex: 00108D01926D
--- (end) ---
```

Field device offline

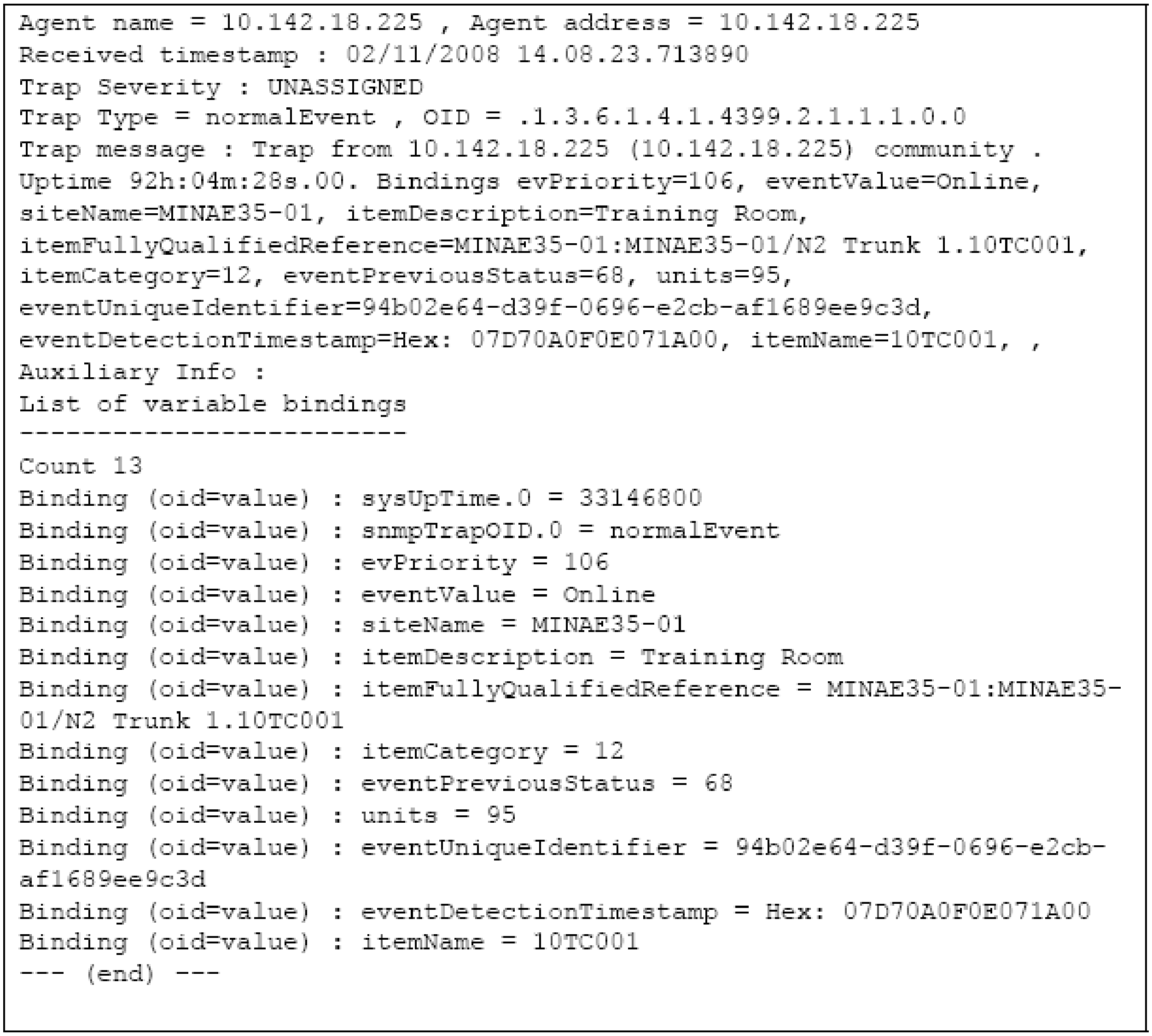
Figure 45: Field Device Offline



```
Agent name = 10.142.18.225 , Agent address = 10.142.18.225
Received timestamp : 02/11/2008 14.04.44.017121
Trap Severity : UNASSIGNED
Trap Type = alarmEvent , OID = .1.3.6.1.4.1.4399.2.1.1.1.0.68
Trap message : Trap from 10.142.18.225 (10.142.18.225) community .
Uptime 92h:00m:49s.00. Bindings evPriority=106, eventValue=Offline,
siteName=MINAE35-01, itemDescription=Training Room,
itemFullyQualifiedReference=MINAE35-01:MINAE35-01/N2 Trunk 1.10TC001,
itemCategory=12, eventPreviousStatus=0, units=95,
eventUniqueIdentifier=6226967d-98c9-ba55-9b6f-e4c5328ab74a,
eventDetectionTimestamp=Hex: 07D70A0F0E032F00, itemName=10TC001, ,
Auxiliary Info :
List of variable bindings
-------------------------
Count 13
Binding (oid=value) : sysUpTime.0 = 33124900
Binding (oid=value) : snmpTrapOID.0 = alarmEvent
Binding (oid=value) : evPriority = 106
Binding (oid=value) : eventValue = Offline
Binding (oid=value) : siteName = MINAE35-01
Binding (oid=value) : itemDescription = Training Room
Binding (oid=value) : itemFullyQualifiedReference = MINAE35-01:MINAE35-
01/N2 Trunk 1.10TC001
Binding (oid=value) : itemCategory = 12
Binding (oid=value) : eventPreviousStatus = 0
Binding (oid=value) : units = 95
Binding (oid=value) : eventUniqueIdentifier = 6226967d-98c9-ba55-9b6f-
e4c5328ab74a
Binding (oid=value) : eventDetectionTimestamp = Hex: 07D70A0F0E032F00
Binding (oid=value) : itemName = 10TC001
--- (end) ----
```

Field controller online

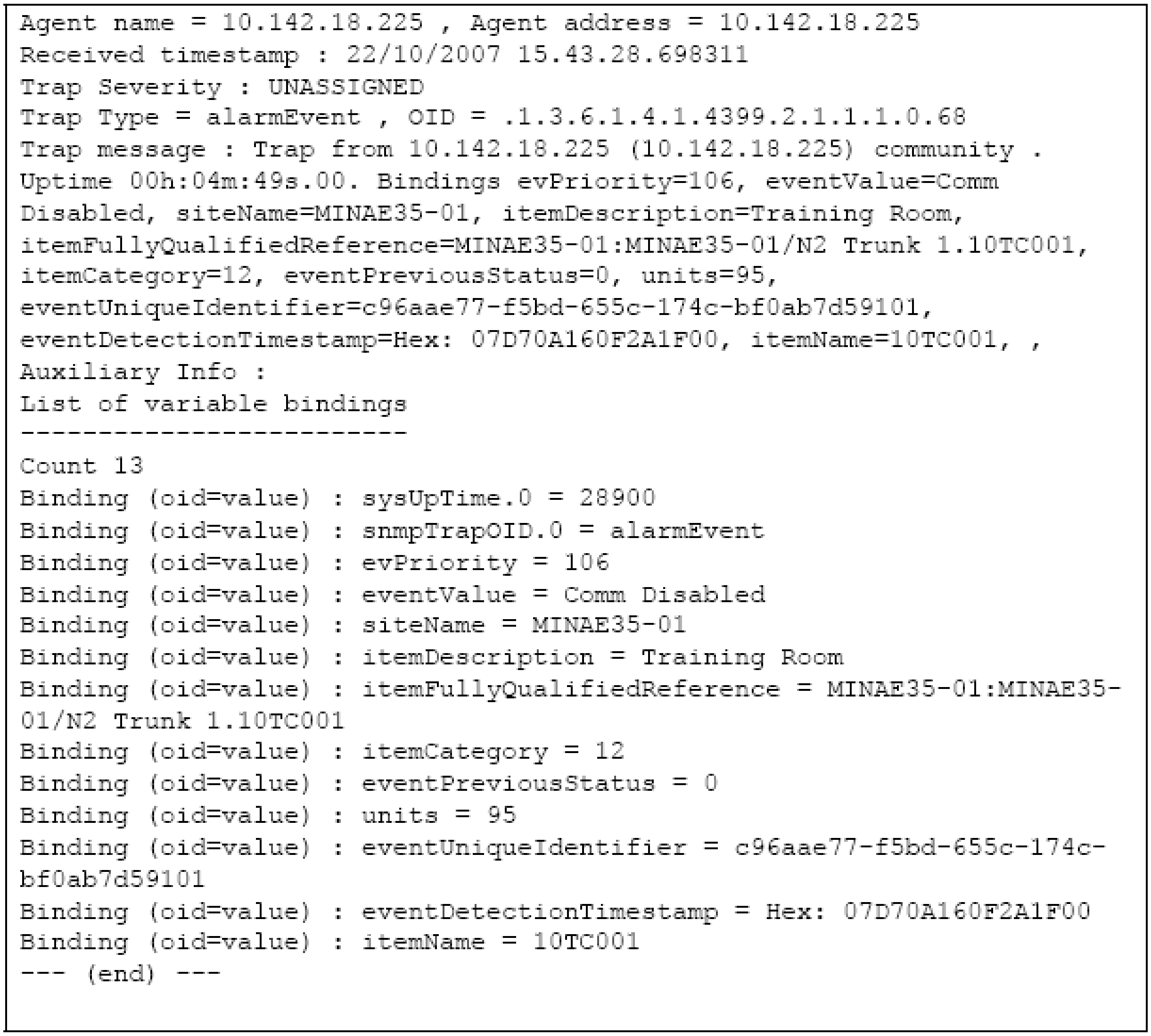
Figure 46: Field Controller Online



```
Agent name = 10.142.18.225 , Agent address = 10.142.18.225
Received timestamp : 02/11/2008 14.08.23.713890
Trap Severity : UNASSIGNED
Trap Type = normalEvent , OID = .1.3.6.1.4.1.4399.2.1.1.1.0.0
Trap message : Trap from 10.142.18.225 (10.142.18.225) community .
Uptime 92h:04m:28s.00. Bindings evPriority=106, eventValue=Online,
siteName=MINAE35-01, itemDescription=Training Room,
itemFullyQualifiedReference=MINAE35-01:MINAE35-01/N2 Trunk 1.10TC001,
itemCategory=12, eventPreviousStatus=68, units=95,
eventUniqueIdentifier=94b02e64-d39f-0696-e2cb-af1689ee9c3d,
eventDetectionTimestamp=Hex: 07D70A0F0E071A00, itemName=10TC001, ,
Auxiliary Info :
List of variable bindings
-------------------------
Count 13
Binding (oid=value) : sysUpTime.0 = 33146800
Binding (oid=value) : snmpTrapOID.0 = normalEvent
Binding (oid=value) : evPriority = 106
Binding (oid=value) : eventValue = Online
Binding (oid=value) : siteName = MINAE35-01
Binding (oid=value) : itemDescription = Training Room
Binding (oid=value) : itemFullyQualifiedReference = MINAE35-01:MINAE35-
01/N2 Trunk 1.10TC001
Binding (oid=value) : itemCategory = 12
Binding (oid=value) : eventPreviousStatus = 68
Binding (oid=value) : units = 95
Binding (oid=value) : eventUniqueIdentifier = 94b02e64-d39f-0696-e2cb-
af1689ee9c3d
Binding (oid=value) : eventDetectionTimestamp = Hex: 07D70A0F0E071A00
Binding (oid=value) : itemName = 10TC001
--- (end) ---
```

Field controller disabled

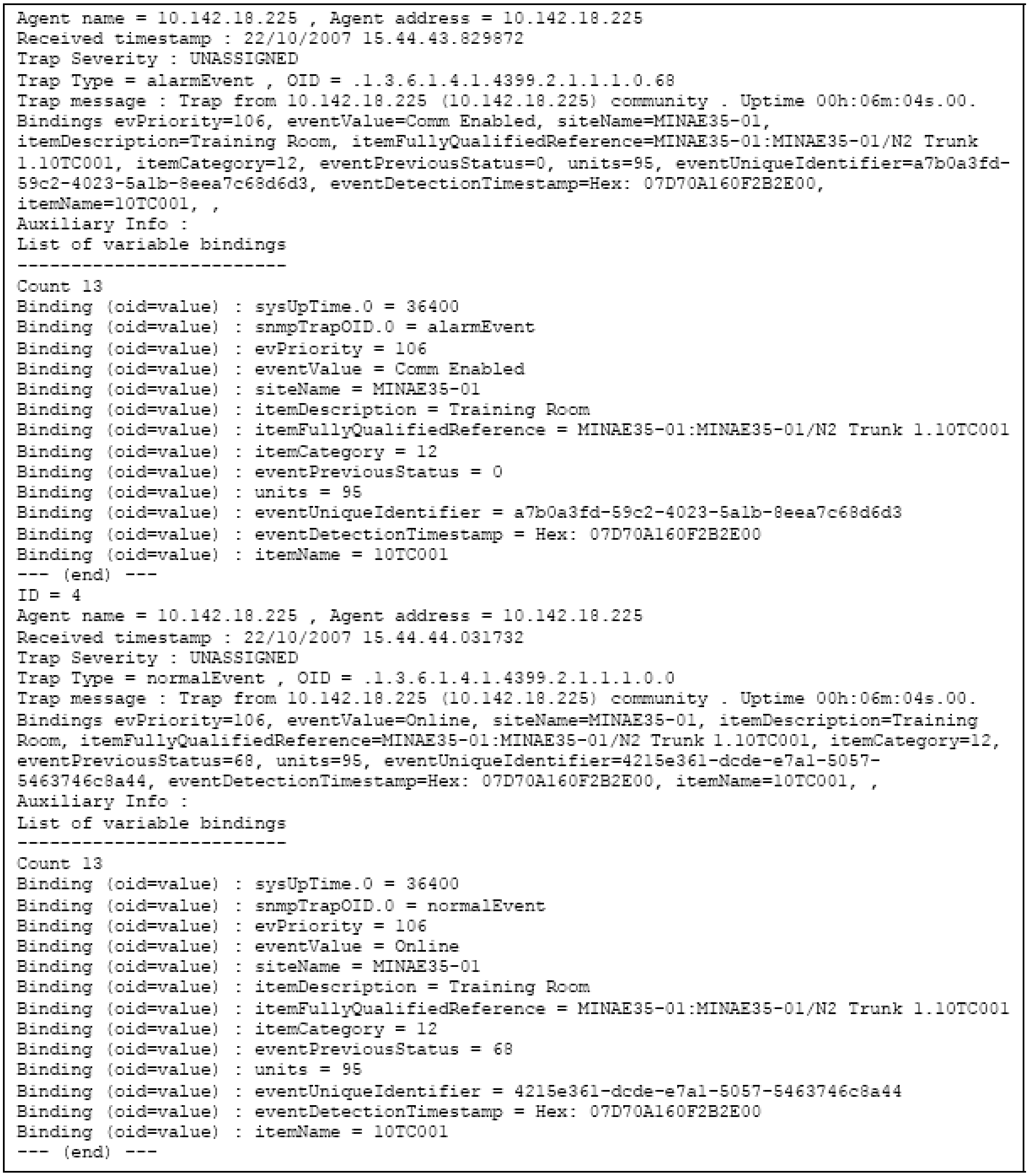
Figure 47: Field Controller Disabled Example



```
Agent name = 10.142.18.225 , Agent address = 10.142.18.225
Received timestamp : 22/10/2007 15.43.28.698311
Trap Severity : UNASSIGNED
Trap Type = alarmEvent , OID = .1.3.6.1.4.1.4399.2.1.1.1.0.68
Trap message : Trap from 10.142.18.225 (10.142.18.225) community .
Uptime 00h:04m:49s.00. Bindings evPriority=106, eventValue=Comm
Disabled, siteName=MINAE35-01, itemDescription=Training Room,
itemFullyQualifiedReference=MINAE35-01:MINAE35-01/N2 Trunk 1.10TC001,
itemCategory=12, eventPreviousStatus=0, units=95,
eventUniqueIdentifier=c96aae77-f5bd-655c-174c-bf0ab7d59101,
eventDetectionTimestamp=Hex: 07D70A160F2A1F00, itemName=10TC001, ,
Auxiliary Info :
List of variable bindings
-------------------------
Count 13
Binding (oid=value) : sysUpTime.0 = 28900
Binding (oid=value) : snmpTrapOID.0 = alarmEvent
Binding (oid=value) : evPriority = 106
Binding (oid=value) : eventValue = Comm Disabled
Binding (oid=value) : siteName = MINAE35-01
Binding (oid=value) : itemDescription = Training Room
Binding (oid=value) : itemFullyQualifiedReference = MINAE35-01:MINAE35-
01/N2 Trunk 1.10TC001
Binding (oid=value) : itemCategory = 12
Binding (oid=value) : eventPreviousStatus = 0
Binding (oid=value) : units = 95
Binding (oid=value) : eventUniqueIdentifier = c96aae77-f5bd-655c-174c-
bf0ab7d59101
Binding (oid=value) : eventDetectionTimestamp = Hex: 07D70A160F2A1F00
Binding (oid=value) : itemName = 10TC001
--- (end) ---
```

Field controller enabled

Figure 48: Field Controller Enabled Example



```
Agent name = 10.142.18.225 , Agent address = 10.142.18.225
Received timestamp : 22/10/2007 15.44.43.829872
Trap Severity : UNASSIGNED
Trap Type = alarmEvent , OID = .1.3.6.1.4.1.4399.2.1.1.1.0.68
Trap message : Trap from 10.142.18.225 (10.142.18.225) community . Uptime 00h:06m:04s.00.
Bindings evPriority=106, eventValue=Comm Enabled, siteName=MINAE35-01,
itemDescription=Training Room, itemFullyQualifiedReference=MINAE35-01:MINAE35-01/N2 Trunk
1.10TC001, itemCategory=12, eventPreviousStatus=0, units=95, eventUniqueIdentifier=a7b0a3fd-
59c2-4023-5a1b-8eea7c68d6d3, eventDetectionTimestamp=Hex: 07D70A160F2B2E00,
itemName=10TC001, ,
Auxiliary Info :
List of variable bindings
-------------------------
Count 13
Binding (oid=value) : sysUpTime.0 = 36400
Binding (oid=value) : snmpTrapOID.0 = alarmEvent
Binding (oid=value) : evPriority = 106
Binding (oid=value) : eventValue = Comm Enabled
Binding (oid=value) : siteName = MINAE35-01
Binding (oid=value) : itemDescription = Training Room
Binding (oid=value) : itemFullyQualifiedReference = MINAE35-01:MINAE35-01/N2 Trunk 1.10TC001
Binding (oid=value) : itemCategory = 12
Binding (oid=value) : eventPreviousStatus = 0
Binding (oid=value) : units = 95
Binding (oid=value) : eventUniqueIdentifier = a7b0a3fd-59c2-4023-5a1b-8eea7c68d6d3
Binding (oid=value) : eventDetectionTimestamp = Hex: 07D70A160F2B2E00
Binding (oid=value) : itemName = 10TC001
--- (end) ---
ID = 4
Agent name = 10.142.18.225 , Agent address = 10.142.18.225
Received timestamp : 22/10/2007 15.44.44.031732
Trap Severity : UNASSIGNED
Trap Type = normalEvent , OID = .1.3.6.1.4.1.4399.2.1.1.1.0.0
Trap message : Trap from 10.142.18.225 (10.142.18.225) community . Uptime 00h:06m:04s.00.
Bindings evPriority=106, eventValue=Online, siteName=MINAE35-01, itemDescription=Training
Room, itemFullyQualifiedReference=MINAE35-01:MINAE35-01/N2 Trunk 1.10TC001, itemCategory=12,
eventPreviousStatus=68, units=95, eventUniqueIdentifier=4215e361-dcde-e7a1-5057-
5463746c8a44, eventDetectionTimestamp=Hex: 07D70A160F2B2E00, itemName=10TC001, ,
Auxiliary Info :
List of variable bindings
-------------------------
Count 13
Binding (oid=value) : sysUpTime.0 = 36400
Binding (oid=value) : snmpTrapOID.0 = normalEvent
Binding (oid=value) : evPriority = 106
Binding (oid=value) : eventValue = Online
Binding (oid=value) : siteName = MINAE35-01
Binding (oid=value) : itemDescription = Training Room
Binding (oid=value) : itemFullyQualifiedReference = MINAE35-01:MINAE35-01/N2 Trunk 1.10TC001
Binding (oid=value) : itemCategory = 12
Binding (oid=value) : eventPreviousStatus = 68
Binding (oid=value) : units = 95
Binding (oid=value) : eventUniqueIdentifier = 4215e361-dcde-e7a1-5057-5463746c8a44
Binding (oid=value) : eventDetectionTimestamp = Hex: 07D70A160F2B2E00
Binding (oid=value) : itemName = 10TC001
--- (end) ---
```

Appendix: Windows Server OS considerations

This appendix covers important considerations regarding the use of Metasys system software on Windows Server operating systems.

Release 10.0 of the Metasys system supports the following server operating systems: Windows 2016 (64-bit), Windows Server 2012 R2 with Update 1 (64-bit), and Windows Server 2012 (64-bit).

➧ **Important:** We strongly advise that you do not use a computer running a Windows server class operating system to manually browse to the Metasys Site Management Portal UI. By default, Windows Internet Explorer Enhanced Security Configuration is enabled on server class operating systems and may block the Launcher download page from which you install the Launcher application for access to the Site Management Portal. Open the Site Management Portal UI from a computer that is not running a server-class operating system. See Internet Explorer enhanced security configuration.

For information on firewall settings required for Metasys system communication, see Appendix: Windows firewall.

Administrator rights

Depending on your operating system login privileges, you may need to perform the steps listed in Table 32 to use Metasys software (including logs) or access Windows operating system features and SQL Server software on your Windows Server operating system.

Table 32: Login Privileges and Steps

Login Privileges	Steps to Run Software
Not Logged in as the Windows Account with username of Administrator.	To run the software: 1. Right-click the software icon on your desktop or software name in a menu. 2. Select **Properties**. 3. Select **Run As Administrator**. 4. Click **Allow**. Refer to the documentation for the specific Metasys software you are using for more information on how to perform tasks that require Administrator privileges.
Logged in as the Windows Account with the user name of Administrator.	Run the software without additional steps.

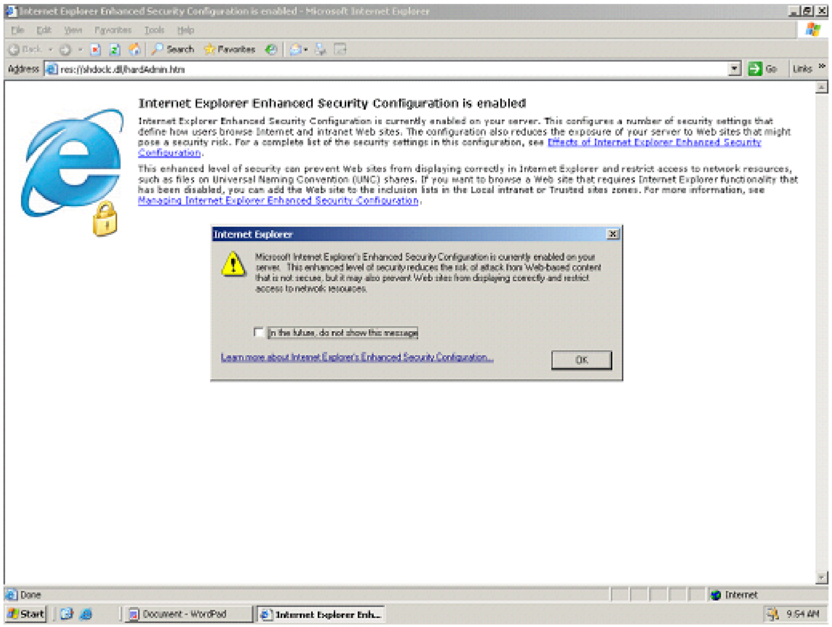
Services

Metasys server software installs and uses the Metasys III Device Manager Service and Metasys III Action Queue Service. Both Services must be run on the Local System account.

Internet Explorer enhanced security configuration

This section applies to the web browser on any computer running a supported server-class operating system. By default, Internet Explorer Enhanced Security Configuration is enabled on this operating system. When you start the Internet Explorer web browser, the `Internet Explorer Enhanced Security Configuration is enabled` message appears (Figure 49).

Figure 49: Internet Explorer Enhanced Security Configuration is Enabled Message


Internet Explorer Enhanced Security Configuration is enabled - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address res://shdoclc.dll/hardAdmin.htm
Go Links
Done
Internet
Start
Document - WordPad
Internet Explorer Enh...
9:54 AM

Internet Explorer Enhanced Security Configuration is enabled

Internet Explorer Enhanced Security Configuration is currently enabled on your server. This configures a number of security settings that define how users browse Internet and intranet Web sites. The configuration also reduces the exposure of your server to Web sites that might pose a security risk. For a complete list of the security settings in this configuration, see Effects of Internet Explorer Enhanced Security Configuration.

This enhanced level of security can prevent Web sites from displaying correctly in Internet Explorer and restrict access to network resources, such as files on Universal Naming Convention (UNC) shares. If you want to browse a Web site that requires Internet Explorer functionality that has been disabled, you can add the Web site to the inclusion lists in the Local intranet or Trusted sites zones. For more information, see Managing Internet Explorer Enhanced Security Configuration.

Internet Explorer

Microsoft Internet Explorer's Enhanced Security Configuration is currently enabled on your server. This enhanced level of security reduces the risk of attack from Web-based content that is not secure, but it may also prevent Web sites from displaying correctly and restrict access to network resources.

□ In the future, do not show this message

Learn more about Internet Explorer's Enhanced Security Configuration...

OK

The Internet Explorer Enhanced Security Configuration establishes a configuration for your computer and for the Internet Explorer web browser. This configuration decreases the exposure of your server to potential attacks that may occur through web content and application scripts. As a result, some websites may not display or perform as expected. For example, the Enhanced Security Configuration may prevent the download of the Launcher application.

To disable Enhanced Security Configuration, start Server Manager and select Local Server. Locate the IE Enhanced Security Configuration setting. Click **On** to open the Internet Explorer Enhanced Security Configuration window. Click **Off** for administrators and users, as recommended by the IT administrator.

Software supported on Windows Server platforms

- ADX
- ODS
- OAS
- Metasys Advanced Reporting System

ⓘ **Note:** Metasys Advanced Reporting supports installation on a computer with SQL Server software. However, Energy Essentials reports does not support installation on a computer with SQL Server 2017 or SQL Server 2016.

- Metasys Database Manager
- Metasys Export Utility
- Metasys System Secure Data Access
- Metasys UI
- Metasys UI Offline
- SCT
- Site Management Portal UI client computer (computer browsing to the Site Management Portal UI)

- NAE85
- LCS85

Software and technologies not listed here are not supported. Refer to the appropriate technical literature for the technology that you are using to verify compatibility with Windows Server operating systems.

Configuring computer as Application server for use as ADX

For information on configuring the computer as an application server, refer to the installation instructions for the Metasys software that you are using (for example, Metasys server or SCT).

Appendix: Windows Desktop OS considerations

This appendix covers important considerations regarding the use of Metasys system software on Windows desktop operating systems.

Release 11.0 of the Metasys system supports the following desktop operating systems: Windows® 10 Pro and Windows 10 Enterprise Editions (version 1903) (64-bit) and Windows 8.1 Pro and Windows 8.1 Enterprise Editions with Update (KB2919355) (64-bit).

These Windows desktop operating systems offer increased network security that affects Internet and intranet communication, including communication between Metasys system components.

For information on firewall settings required for Metasys system communication, see Appendix: Windows firewall.

Administrator rights

Administrative privileges may function differently on Windows 10 and Windows 8.1. Depending on your operating system login privileges, you may need to perform additional steps to use Metasys software (including logs) or access Windows operating system features and SQL Server software.

Table 33: Login Privileges and Steps

Login Privileges	Steps to Run Software
Not logged in as the Windows account named Administrator	To run the software when the Windows operating system is using the standard interface: 1. Right-click the application icon on your desktop or software name in a menu. 2. Select **Run As Administrator** or **More** > **Run As Administrator**. 3. If prompted, enter your credentials. 4. Click **Yes**. To run the software when the Windows operating system is using the Tile interface: 1. Right-click the application tile on the Start screen. 2. Select **Run As Administrator** on the bottom of the screen. 3. If prompted, enter your credentials. 4. Click **Yes**. Refer to the documentation for the specific Metasys software you are using for more information on how to perform tasks that require Administrator privileges.
Logged in as the Windows account named Administrator	Run the software without additional steps.

Services

Metasys server software installs and uses the Metasys III Device Manager Service, MetasysIII SCT Action Queue Service, and Metasys III Action Queue Service. All three services must be run on the local system account.

Internet Explorer web browser settings

ActiveX controls are not required to access sites, such as SMP and SCT.

Operating system administrator rights are required to download and install the Launcher Tool.

If you do not follow the Administrator guidelines here, you may not be able to adjust the Internet Explorer web browser settings or you may not be able to save the changes you make for the next browser session. If you experience problems similar to these, check your access rights.

Note: In Internet Explorer 11, select the **Use Microsoft compatibility lists** option, found under ***Tools*** > ***Compatibility View Settings***, to ensure that websites appear and function correctly.

Software supported

Supported desktop operating systems support the following Metasys software and technologies:

- ADS

- ODS
- OAS
- CCT
- Metasys Database Manager
- Metasys Export Utility
- Metasys System Secure Data Access
- Metasys UI
- Metasys UI Offline
- Site Management Portal UI client computer (computer browsing to the Site Management Portal UI)
- SCT

Software and technologies not listed here are not supported. Refer to the appropriate technical literature for the technology you are using to verify compatibility with the operating system.

Windows features not supported by Metasys software

Metasys software does not support the following Windows features:

- Sleep. If you install a Metasys server or SCT on Windows 10 or Windows 8.1, you must turn off the Sleep feature. Failure to turn off this feature can result in communication problems when the Metasys server or SCT goes to sleep.
- Fast User Switching. Users must log off instead of switching users.

Windows scheduled features

Some features of Windows 10 or Windows 8.1 should be rescheduled depending on the load for the Metasys server. By default, the Windows Defender security tool scans the operating system at 2 A.M. every day, and the Disk Defragmentation tool runs every Wednesday at 1 A.M. If the Metasys server is busy at these times, you should reschedule the process for a time when the Metasys server is less busy.

Appendix: Active Directory service

This appendix provides additional information to network managers for configuring the Active Directory service for use with the *Metasys* system on a computer that has the *Metasys* server or SCT software installed.

Overview

This appendix lists questions and actions that help facilitate the interaction with the customer’s IT department for configuration of the Metasys system for use with Active Directory services. You need to obtain this information and complete the configuration before the feature is enabled and Active Directory service users are added to the Metasys system. Keep in mind that these actions are most likely performed by the customer’s IT department. Furthermore, several IT teams may need to be involved; for example, assistance from the Active Directory Service Team, IT Security

Team, Infrastructure Team, and Network Team may be needed. Make sure you allow time for any necessary team interaction. Also, keep in mind that:

- These questions focus only on the IT needs of the Active Directory service feature and not on the Metasys system. The Metasys system should be properly configured with a version of the Metasys server (and SCT) software that supports the Active Directory feature. Example logistics that fall outside these questions include:

    - administrative access to the Metasys server
    - proper SQL Server rights to install or upgrade the Metasys server software
    - firewalls between Metasys system devices

- These questions assume that the person gathering the information is familiar with the Active Directory service feature.

Infrastructure questions

Table 34 is a worksheet that outlines the questions that need to be answered as part of the Active Directory service implementation on the Metasys system. For many of the actions listed in the table, you must be using an Active Directory service user account with sufficient privileges to search for users within Active Directory service. These privileges must span all domains that contain users who have SSO access to the Metasys system. Also, Active Directory service groups are normally managed by the IT department. A process must be enacted for managing the addition and removal of Metasys system users who are also Active Directory service users.

Table 34: Active Directory Service Worksheet

Question	Answer	Action Steps
How many Active Directory service domains contain users who are to be added as Metasys system users?	1	Join the Metasys server or SCT computer to the domain. Create only one Service Account under that domain. Specify the Service Account under Metasys Security Administration. For details, see Service account.
	More than 1	If trusts exist between all domains that contain Metasys system users, the Metasys server or SCT can be in any domain. Use a single Service Account within Active Directory service with access to all domains with Metasys system users.
		If trusts **do not** exist between all domains, the Metasys server can still be joined to any domain. However, if an Active Directory service user is in a domain that does not trust the domain that the Metasys server is in, the user is not able to take advantage of SSO login-free access to the Metasys system. The user can still use the Active Directory service user name, password, and domain at the Metasys login screen. Create one Service Account per domain that contains *Metasys* system users. For details, see Service account rules and Service account permissions.

Table 34: Active Directory Service Worksheet

Question	Answer	Action Steps
Are there any firewalls between the Metasys server and the Active Directory service domain?	Yes	Firewalls must be correctly configured to allow Active Directory service port and protocol access between the Metasys server and domains. This is a Microsoft prerequisite for joining a domain. For details, see Protocols, ports, and connectivity for the Metasys system.
	No	No action required.
Is every client computer that can run the Site Management Portal UI joined to an Active Directory service domain that is in the same domain as the Metasys server or in a trusted domain?	Yes	Verify that the Active Directory service is configured to allow the user to log in to the Windows Desktop with Active Directory service credentials.
	No	Can the client computers be added to the domain that the Metasys server is joined to or to some other trusted domain? • **Yes** - SSO login-free access is available. • **No** - SSO login-free access is unavailable, but the user can still specify Active Directory service credentials on the Metasys system login screen.

Primary requirements

The following is a list of requirements for using Active Directory service with the Metasys system at the customer's site. The steps for setting up Active Directory service are primarily the responsibility of the customer's IT department. Installation of the Metasys software is usually performed by others, but often supervised by IT personnel. These requirements are based on answers given for the questions posed in Table 34, though not all requirements apply to every installation.

Metasys server computer

The computer with the Metasys server software (ADS, ADX, MVE, OAS, or ODS) must be:

- joined to an Active Directory service domain (or trusted domain) where the Metasys system users are located
- added to an Active Directory service domain where the computer is not affected by group policies

In addition, configure any firewalls to allow appropriate Active Directory service communication.

SCT computer

The computer with the SCT software must be joined to an Active Directory service domain (or trusted domain) where the Metasys system users are located.

In addition, configure any firewalls to allow appropriate Active Directory service communication.

Client computer

The client computer used to run the Metasys server or SCT UI must be joined to an Active Directory service domain where the Metasys server and SCT are located or to a trusted domain.

Additional requirements

The following are additional requirements:

- Obtain the fully qualified domain names for all domains that are to contain Metasys system users. The name must be the domain level (and not the forest level or some other level).

ⓘ **Note:** This information is necessary at the time when Active Directory service users are added to the Metasys system with the Security Administrator System tool. For details, see User account rules.

- Obtain the corresponding pre-Windows 2000 domain names (short format of the domain name). This information is useful because the Metasys system user can specify this format at the login screen of the Site Management Portal UI.

For additional requirements, see Service account.

Appendix: Windows firewall

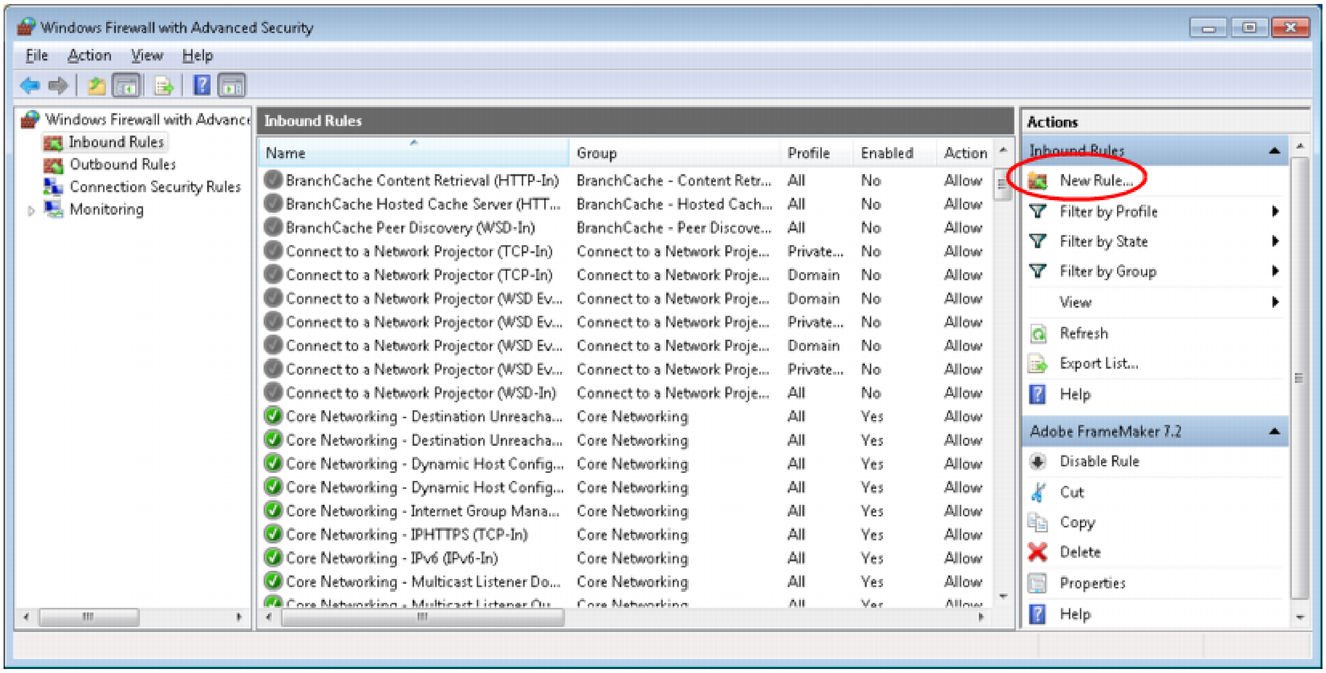
As a best practice, enable the Windows Firewall as indicated in this section, but always follow the recommendation of the customer's local IT staff. Some customers may not require enabling the Windows Firewall.

Configuring the Windows firewall

About this task:
As a best practice, enable the Windows Firewall as indicated in this section, but always follow the recommendation of the customer's local IT staff.

1. In Control Panel, click **System and Security**, then click **Windows Firewall**. The Windows Firewall window appears.
2. In the Windows Firewall window, make sure the firewall is **On**. If not, turn on the Windows Firewall.
3. Click **Advanced Settings**. The Windows Firewall with Advanced Security window appears.
4. In the left pane, click **Inbound Rules**. The Inbound Rules pane appears.

Figure 50: Windows Firewall - Inbound Rules



Inbound Rules

Name	Group	Profile	Enabled	Action
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	Allow
BranchCache Hosted Cache Server (HTT...	BranchCache - Hosted Cach...	All	No	Allow
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No	Allow
Connect to a Network Projector (TCP-In)	Connect to a Network Proje...	Private...	No	Allow
Connect to a Network Projector (TCP-In)	Connect to a Network Proje...	Domain	No	Allow
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Domain	No	Allow
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Private...	No	Allow
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Domain	No	Allow
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Private...	No	Allow
Connect to a Network Projector (WSD-In)	Connect to a Network Proje...	All	No	Allow
Core Networking - Destination Unreacha...	Core Networking	All	Yes	Allow
Core Networking - Destination Unreacha...	Core Networking	All	Yes	Allow
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow
Core Networking - Internet Group Mana...	Core Networking	All	Yes	Allow
Core Networking - IPHTTPS (TCP-In)	Core Networking	All	Yes	Allow
Core Networking - IPv6 (IPv6-In)	Core Networking	All	Yes	Allow
Core Networking - Multicast Listener Do...	Core Networking	All	Yes	Allow
Core Networking - Multicast Listener Qu...	Core Networking	All	Yes	Allow

5. In the Actions pane, select **New Rule**. The New Inbound Rule Wizard opens and the Rule Type window appears.
6. Select **Port** and click **Next**. The Protocol and Ports window appears.
7. Select **TCP**, and in the **Specific Local Ports** field, enter the port numbers (25, 80, 88, 110, 135, 389, 443, 445, 465, 587, 995, 1025, 1433, 2103, 2105, 3389, 5291, 5960, 9910, 10050, 12000).

Table 35: Ports to Open for TCP Protocol

Protocol	Port
SMTP	25
HTTP	80
Kerberos	88
POP3	110
Remote Procedure Call (RPC)	135
LDAP	389
HTTPS (TLS)	443
NT LAN Manager Version 2 (NTLMv2)	445
SMTP over TLS	465
SMTP	587
POP3 over TLS	995
Remote Procedure Call (RPC)	1025
Microsoft SQL Server Database	1433
RPC over TCP	2103
RPC over TCP	2105
Microsoft Terminal Server	3389
(Unassigned)	5291

Table 35: Ports to Open for TCP Protocol

Protocol	Port
(Unassigned)	5960
Microsoft Discovery Protocol	9910
Zabbix Agent	10050
(Unassigned)	12000

8. Click **Next**. The Action window appears.
9. Select **Allow the connection**. Click **Next**. The Profile window appears.
10. Keep all profile check boxes selected (default). Click **Next**. The Name window appears.
11. Specify **Metasys (TCP Protocol)** as the name. Optionally, you can add a description to identify this new rule. Click **Finish**.

    The Inbound Rules table refreshes to indicate the new rule called Metasys (TCP Protocol). Ports 25, 80, 88, 110, 135, 389, 443, 445, 465, 587, 995, 1025, 1433, 2103, 2105, 3389, 5291, 5960, 9910, 10050, 12000 are now open and ready for use.
12. Repeat Step 5 through Step 11 to add a new Metasys inbound rule for the UDP protocol. When the Protocol and Ports window appears, select **UDP**, and in the Specific Local Ports field, enter the port numbers (25, 53, 67, 68, 69, 88, 123, 161, 162, 9910, 9911, 47808).

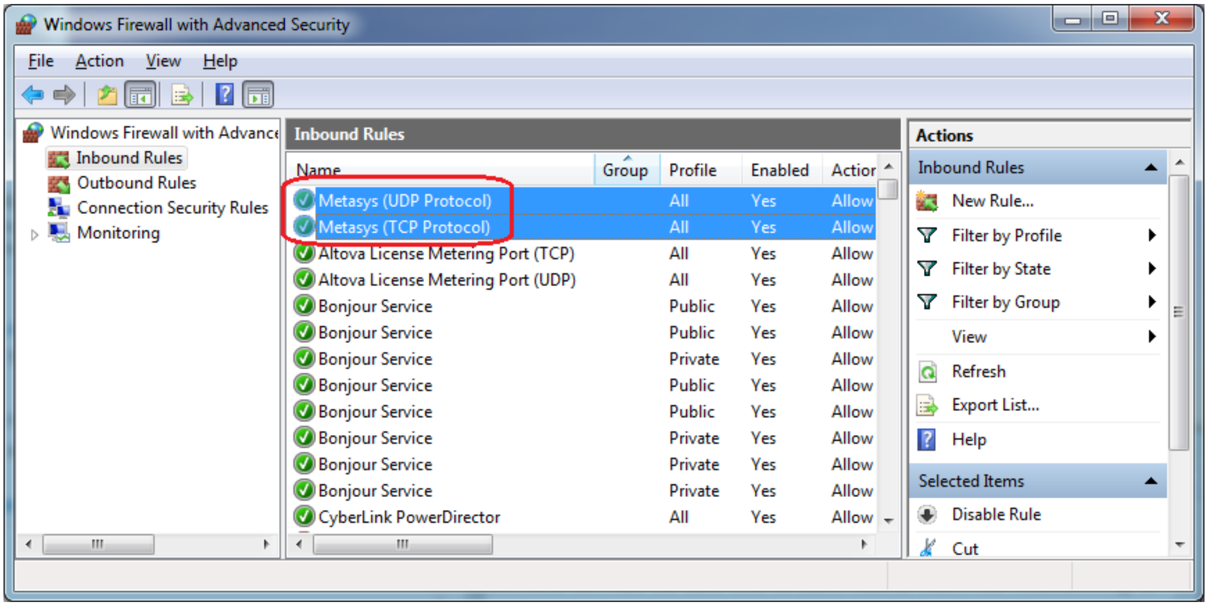
Table 36: Ports to Open for UDP Protocol

Protocol	Port
SMTP	25
DNS	53
DHCP	67
DHCP	68
Trivial File Transfer Protocol (TFTP)	69
Kerberos	88
Network Time Protocol (NTP)	123
SNMP	161
SNMP Trap	162
Microsoft Discovery Protocol	9910
SYPE-Transport	9911
BACnet®	47808, Configured for each supervisory device, including OAS, ODS and the NAE8500, in the the Network Port Ethernet IP Datalink object

13. Complete the steps to add the new inbound rule. Name the new rule **Metasys (UDP Protocol)**.

    When finished, the **Windows Firewall with Advanced Security** window appears and the Inbound Rules table refreshes to indicate the new rule called **Metasys (UDP Protocol)**. Ports 25, 67, 68, 69, 53, 88, 123, 161, 162, 9910, 9911, and 47808 are now open and ready for use.
14. In the **Windows Firewall with Advanced Security** window, verify that the two new Metasys inbound rules are defined and enabled.

Figure 51: Metasys Inbound Rules Defined and Enabled



Name	Group	Profile	Enabled	Actior
Metasys (UDP Protocol)		All	Yes	Allow
Metasys (TCP Protocol)		All	Yes	Allow
Altova License Metering Port (TCP)		All	Yes	Allow
Altova License Metering Port (UDP)		All	Yes	Allow
Bonjour Service		Public	Yes	Allow
Bonjour Service		Public	Yes	Allow
Bonjour Service		Private	Yes	Allow
Bonjour Service		Public	Yes	Allow
Bonjour Service		Public	Yes	Allow
Bonjour Service		Private	Yes	Allow
Bonjour Service		Private	Yes	Allow
Bonjour Service		Private	Yes	Allow
CyberLink PowerDirector		All	Yes	Allow

15. Close the **Windows Firewall with Advanced Security** window.
16. Close all windows.

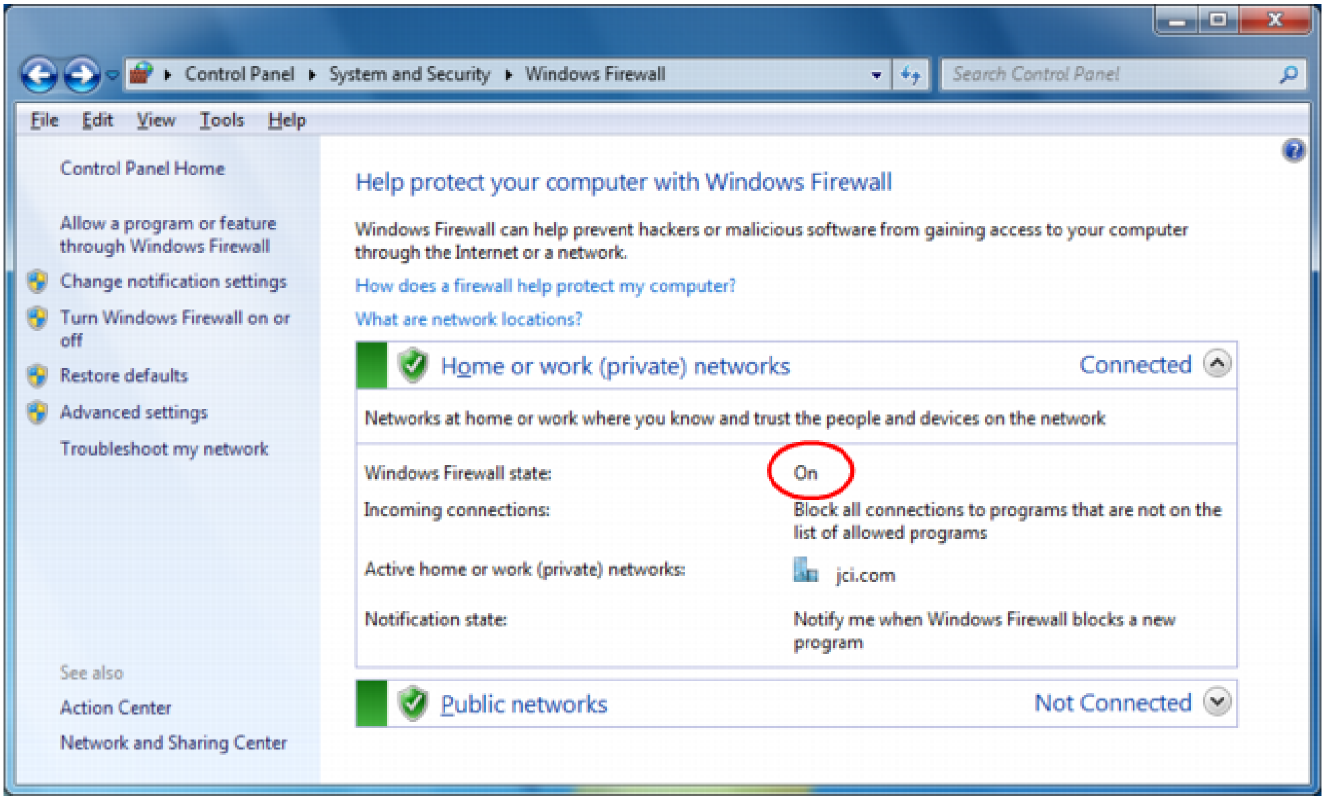
Closing ports

About this task:
This section provides an overview on how to close ports if desired. Note that closing ports can have unforeseen effects on other parts of your system. The example in this section shows blocking inbound Port 80; you can block outbound Port 80 as well by defining an outbound rule, although the ADS/ADX/ODS and network engines do not communicate out of Port 80.

ⓘ **Note:** The latest available version of the ODS is Release 10.1. The ODS is not available for upgrade to Metasys Release 11.0.

1. In Control Panel, click **System and Security**, then click **Windows Firewall**. The Windows Firewall window appears.
2. In the Windows Firewall window, make sure the firewall is **On**. If not, turn on the Windows Firewall.

Figure 52: Windows Firewall


Control Panel ▸ System and Security ▸ Windows Firewall
Search Control Panel
File Edit View Tools Help
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Action Center
Network and Sharing Center

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?

What are network locations?

Home or work (private) networks — Connected

Networks at home or work where you know and trust the people and devices on the network

Windows Firewall state: On

Incoming connections: Block all connections to programs that are not on the list of allowed programs

Active home or work (private) networks: jci.com

Notification state: Notify me when Windows Firewall blocks a new program

Public networks — Not Connected

3. Click **Advanced Settings** in the left pane. The Windows Firewall with Advanced Security window appears.
4. In the left pane, click **Inbound Rules**. The Inbound Rules pane appears.
5. In the Actions pane, select **New Rule**. The New Inbound Rule Wizard opens and the Rule Type window appears.
6. Select **Port** and click **Next**. The Protocol and Ports window appears.
7. Select **TCP**, and in the Specific Local Ports field, enter the port numbers you want to close. This example shows Port 80.
8. Click **Next**. The Action window appears.
9. Select **Block the connection** and click **Next**.
10. Complete the steps to add the new inbound rule. Name the new rule **Metasys (TCP Protocol Closed Ports), BCM (TCP Protocol Closed Ports)**.

    When finished, the Windows Firewall with Advanced Security window appears and the Inbound Rules table refreshes to indicate the new rule called **Metasys (TCP Protocol Closed Ports) BCM (TCP Protocol Closed Ports)**. The ports you specified in **Step 7** are now closed to inbound traffic.

11. In the Windows Firewall with Advanced Security window, verify that the new inbound rule is defined and enabled.
12. If you also need to close UDP ports, select **New Rule** from the **Actions** menu and repeat steps 5 through 11, substituting UDP for TCP in **Step 7**. You can also create a new outbound rule if you want to block outgoing traffic over a particular port. In that case, select the Outbound Rules option in **Step 4**.
13. Close the Windows Firewall with Advanced Security window.
14. Close any additional windows.

Appendix: Certificate management and security

Follow the steps in this appendix for managing the trusted certificates on the Metasys Server or SCT computer, and for selecting security levels for the site. The Metasys server, SCT computer, and network engines are installed with self-signed certificates, which enables encrypted network communication between the devices. Optionally, the customer can deploy trusted certificates at the Metasys server or SCT computer and enable encrypted and trusted communication between the Metasys server and network engines. Trusted certificates, installed on the client computer and the Metasys SMP or SCT computer, are either provided by the customer's IT department or a Certificate Authority (CA). A security shield icon on the Metasys server or SCT login and user interface screens indicate the encryption state:

- **Green Shield**: the connection is encrypted and trusted
- **Orange Shield**: the connection is encrypted, but not trusted
- **Red Shield**: the connection is encrypted, but the security level cannot be verified

To deploy a trusted server certificate at the Metasys server or SCT computer, follow **Steps 1-3** referenced below. Then, if the IT department or CA has provided separate files for the root and intermediate certificates, follow **Step 4**. Also follow **Step 4** if you need to establish a trusted relationship between the client computer and the Metasys server and SCT computer. If you want to establish **encrypted and trusted** communication between the Metasys server and network engines, follow **Step 5**, which explains how to set the Site Security Level. Lastly, perform **Step 6** if you want to verify all certificates are in place.

1. Requesting a server certificate
2. Completing a server certificate request
3. Binding the secure certificate
4. Importing root and intermediate certificates
5. Setting the Site Security Level to Encrypted and Trusted
6. Verifying the server certificate chain

For details on how to remove or rebind a secure certificate, see Removing or rebinding the secure certificate. For details about how to remove a self-signed certificate from the certificate store, see Removing the self-signed certificates in the certificate store. For details about managing certificates on network engines, refer to *Metasys SCT Help (LIT-12011964)*.

Lastly, this appendix describes how to use two special security attributes that you set in the site object of the Site Director: Site Security Level and Advanced Security Enabled. See the following sections for details:

Setting the Site Security Level to Encrypted and Trusted

Changing Advanced Security Enabled to False

Requesting a server certificate

1. In Control Panel, select ***System and Security*** > ***Administrative Tools*** and double-click **Internet Information Services (IIS) Manager**. The IIS main screen appears.
2. Under the IIS section in the middle pane, double-click **Server Certificates**. The Server Certificates panel appears.
3. On the Actions pane, click **Create Certificate Request**. The Distinguished Name Properties screen appears.

4. Fill out all the fields in the form. For Common name, specify the full computer name, which you can determine from ***Control Panel*** > ***System and Security*** > ***System***. The full name may also include a domain name (for example, MAIN-ADX.mycorp.com). Click **Next**. The Cryptographic Service Provider Properties screen appears.
5. Select an appropriate service provider and bit length. Click **Next**. The File Name screen appears.
6. Click the **Browse (...)** button to select a location where to save the certificate request file. The Specify Save as File Name window appears.
7. Type in a file name and click **Open**. The File Name window appears with the file name specified.
8. Click **Finish**. The certificate request file with a .txt extension is created in the selected folder. For example, the certificate request file for a server called MAIN-ADX would be **MAIN-ADX.txt**.
9. Send the certificate request file to the IT department or CA to obtain your trusted certificate. When you receive the file, go to Completing a server certificate request to import the certificate into the server.

Completing a server certificate request

About this task:
To complete a certificate request for a Metasys server or SCT computer:

1. In Control Panel, select ***System and Security*** > ***Administrative Tools*** and double-click **Internet Information Services (IIS) Manager**. The IIS main screen appears.
2. Under the IIS section in the middle pane, double-click **Server Certificates**. The Server Certificates panel appears.
3. On the Actions pane, click **Complete Certificate Request**. The Specify Certificate Authority Response screen appears.
4. Use the browse button to locate the certificate that your IT department provided. Specify a friendly name for the server. Select **Personal** under **Select a certificate store for the new certificate** if this field appears. Click **OK** to complete the certificate request. The Server Certificates window appears indicating the new certificate has been imported.
5. Next, you need to bind the certificate. See Binding the secure certificate.

Binding the secure certificate

About this task:
To bind a secure certificate for a Metasys server or SCT computer:

1. In Control Panel, select ***System and Security*** > ***Administrative Tools*** and double-click **Internet Information Services (IIS) Manager**. The IIS main screen appears.
2. Expand the Connections in the left pane so that Default Web Site appears. Click **Default Web Site**.
3. On the Actions pane, click **Bindings** under Edit Site. The Site Bindings screen appears.
4. Click **Add**. The Add Site Bindings screen appears.
5. Under Type, select **https**. Under SSL certificate, select the name of the server certificate you imported in Completing a server certificate request. Click **OK**.

ⓘ **Note:** Make sure that proper certificate revocation, such as Online Certificate Status Protocol (OCSP) stapling, is enabled and configured. For more information about OCSP configuration refer to https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-ocsp/5792b4c4-c6ba-439a-9c2a-52867d12fb66

6. If you need to import root and intermediate certificates of the Metasys Server or SCT computer at a client computer, go to Importing root and intermediate certificates. This step is necessary if you want the green shield icon to appear on Metasys SMP and SCT login and user interface screens.

   If you want to skip that step and you want to verify the certificate chain you created in the previous sections, see Verifying the server certificate chain.

Importing root and intermediate certificates

About this task:
Follow these steps to import root and intermediate certificates of a Metasys server or SCT computer at the client computer (that is, the computer that remotely logs in to SMP or SCT). Also perform these steps to import certificates when the IT department or CA provided separate files for the root and intermediate certificates.

1. Start the Microsoft Management Console at the client computer by typing `mmc` in the Search bar and pressing **Enter**. The Microsoft Management Console screen appears.
2. Click ***File*** > ***Add/Remove Snap-ins***. The Add or Remove Snap-ins screen appears.
3. Under the Available snap-ins list, select **Certificates** and click **Add**. The Certificate Snap-in screen appears.
4. Select **Computer account** and click **Next**. The Select Computer screen appears.
5. Click **Local computer** and click **Finish**. The Add or Remove Snap-ins screen appears indicating the Certificates addition.
6. Click **OK.** The Microsoft Management Console window appears with the Certificates snap-in.
7. Select **Trusted Root Certification Authorities**. Under More Actions, click ***All Tasks*** > ***Import***. The Certificate Import Wizard appears.
8. With Local Machine pre-selected, click **Next**. The next screen prompts you for the location of the certificate file request. Select the certificate request file, using the Browse button to help locate the file. Click **Next**.
9. Select **Trusted Root Certificate Authorities** as the location where to store the certificate. Click **Next**.
10. Click **Finish** to complete the certificate import.
11. Under ***Trusted Root Certificate Authorities*** > ***Certificates***, verify the root certificate has been imported.
12. Repeat the steps in this section for importing any required intermediate server certificates as necessary, but in Step 7, select the **Intermediate Certification Authorities** as the certificate type.

Verifying the server certificate chain

About this task:
To verify a certificate chain for a Metasys server or SCT computer:

1. In Control Panel, select ***System and Security*** > ***Administrative Tools*** and double-click **Internet Information Services (IIS) Manager**. The IIS main screen appears.
2. Highlight the name of the web server.

3. Under the IIS section in the middle pane, double-click **Server Certificates**. The Server Certificates panel appears.
4. On the Actions pane, click **View**. The Certificate screen appears.
5. Click the **Certification Path** tab. The certificate chain appears.
6. Click **OK** to close the certificate view.

Setting the Site Security Level to Encrypted and Trusted

About this task:
You can set the **Site Security Level** offline with SCT or online with the Site Management Portal UI. To use the online method to set the Site Security Level to **Encrypted and Trusted**, follow these steps:

1. Log on the Site Management Portal of the Site Director.
2. Open the **Site View** for the Site Director.
3. With Advanced selected, click **Edit**.
4. Locate the **Site Security Level** attribute under the **Operational Data** section.
5. Click the down arrow and select **Encrypted and Trusted**.

   ⓘ **Note:** When you set the Site Security Level attribute in the Site object to **Encrypted and Trusted**, all network engines reporting to the Site Director are modified to change their Site Security Level attribute to Encrypted and Trusted. If a network engine Site Security Level attribute is set to Encrypted and Trusted but does not have a trusted certificate, communication between the Site Director and the network engine is lost because the Site Director now requires the engine to communication with a trusted certificate. Also, if sometime later you want to change a network engine's Site Security Level back to Encrypted Only, you need to log on the network engine directly.

   Before you set the Site object Site Security Level attribute to **Encrypted and Trusted**, verify that all network engines reporting to the Site Director have trusted certificates. If the network engines do not have trusted certificates, keep this attribute set to **Encrypted Only**.
6. Click **Save**. The server and engines across the entire site now use encrypted and trusted communication.
7. As an option, use SCT to upload the Site Director so that this change is reflected in the database archive.

   If you want to later change the site to use encrypted only communication, repeat these steps but select **Encrypted Only**, then use SCT to upload the change to the archive.

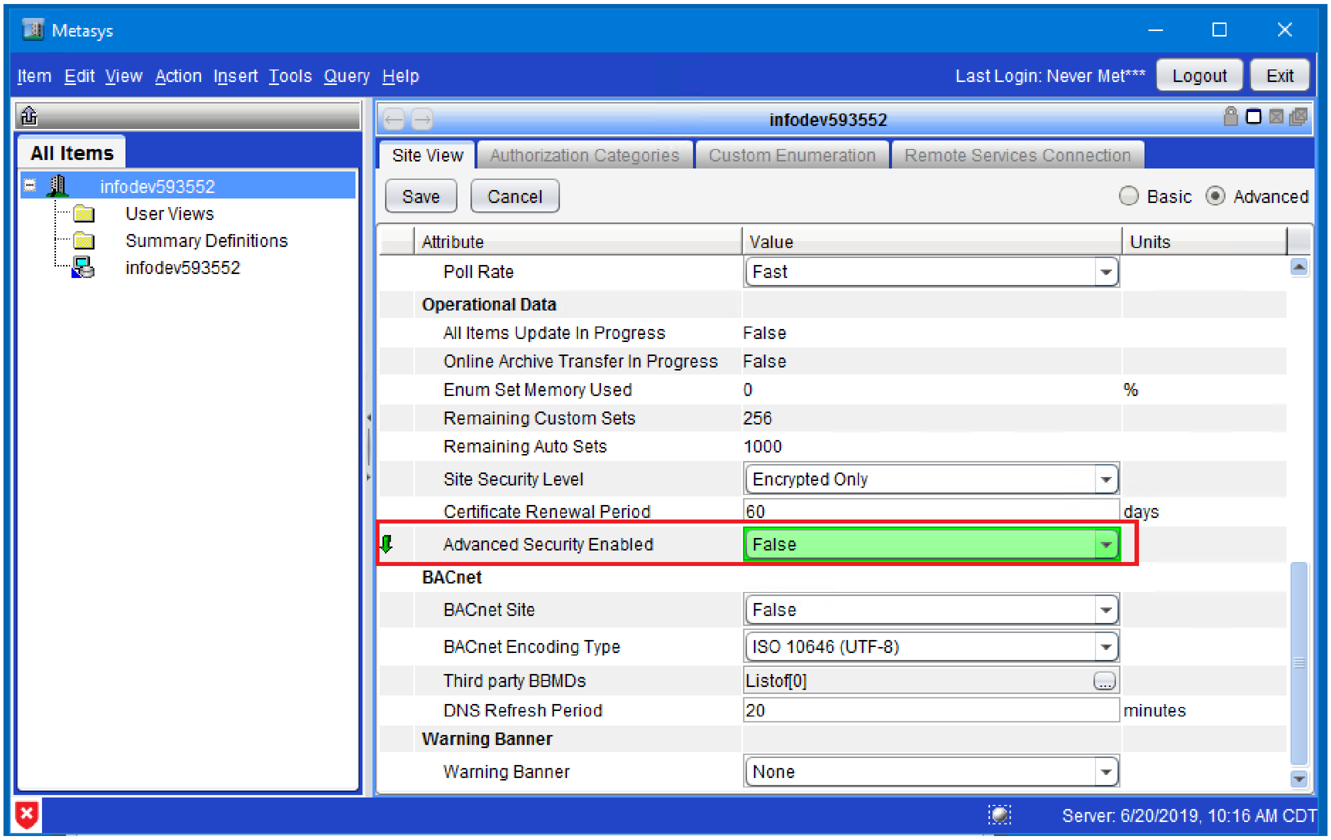
Changing Advanced Security Enabled to False

About this task:
By default, the **Advanced Security Enabled** attribute on the Site object is set to **True** for the Metasys system installed at or upgraded to Release 11.0. This attribute provides an improved layer of security between Metasys Site Directors and devices. With this attribute set to true (default), older methods of secure communication between the Site Director and its network engines are disabled, which means a Site Director at Release 10.0 or later discards all communication attempts from network engines prior to Release 10.0. This setting applies to the entire site, so if you have any network engine on the site that is running a Metasys release prior to Release 10.0, use the steps in this section to change this Site object attribute to **False**. You can use either SCT (offline method) or the Site Management Portal UI (online method). To use the online method, follow these steps:

1. Log on the Site Management Portal of the Site Director.

2. Open the **Site View** for the Site Director.
3. With Advanced selected, click **Edit**.
4. Locate the **Advanced Security Enabled** attribute under the **Operational Data** section (Figure 53).
5. Click the down arrow and select **False**.

Figure 53: Changing the Advanced Security Enabled attribute



Attribute	Value	Units
Poll Rate	Fast	
Operational Data		
All Items Update In Progress	False	
Online Archive Transfer In Progress	False	
Enum Set Memory Used	0	%
Remaining Custom Sets	256	
Remaining Auto Sets	1000	
Site Security Level	Encrypted Only	
Certificate Renewal Period	60	days
Advanced Security Enabled	False	
BACnet		
BACnet Site	False	
BACnet Encoding Type	ISO 10646 (UTF-8)	
Third party BBMDs	Listof[0]	
DNS Refresh Period	20	minutes
Warning Banner		
Warning Banner	None	

6. Click **Save**. The server and engines across the entire site no longer use advanced security.
7. As an option, use SCT to upload the Site Director so that this change is reflected in the database archive.

   ⓘ **Note:** If sometime later you change the **Advanced Security Enabled** attribute from False to True, a user message appears to indicate that all network engines prior to Release 10.0 are disconnected from the site because they can no longer communicate with the Site Director using advanced security. Do not set **Advanced Security Enabled** to True until all network engines are upgraded to Release 10.0 or later.

Removing or rebinding the secure certificate

About this task:
Follow these steps to remove a certificate binding from a Metasys server or SCT computer or to change a certificate binding. If you are changing a binding, the binding must already exist on the server from which to select.

1. In Control Panel, select ***System and Security*** > ***Administrative Tools*** and double-click **Internet Information Services (IIS) Manager**. The IIS main screen appears.
2. Expand the Connections in the left pane so that Default Web Site appears. Click **Default Web Site**.

3. On the Actions pane, click **Bindings** under Edit Site. The Site Bindings screen appears.
4. To remove the site binding, select it from the list and click **Remove**. A user prompt appears to verify that you want to remove the selected binding. Click **Yes** to remove or **No** to cancel.

   To rebind the certificate, select it from the list and click **Edit**. The Edit Site Binding screen appears.

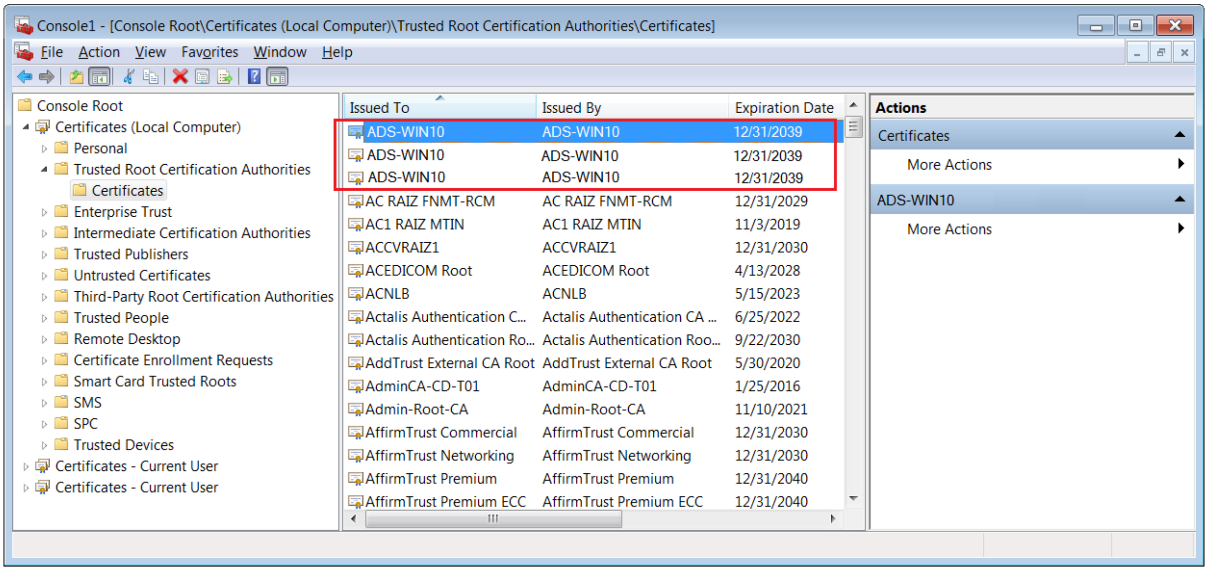
5. Click **Select** to open a table that lists all certificates available for binding.
6. Select the binding from the table and click **OK**. The Edit Site Binding screen appears with the newly selected binding.
7. Click **OK** to save the binding change.

Removing the self-signed certificates in the certificate store

About this task:
Follow this procedure to manually remove self-signed certificates before upgrading Metasys server software or SCT software for a computer that has been renamed as part of the upgrade.

1. Start the Microsoft Management Console at the Metasys server or SCT computer by typing **mmc** in the Search bar and pressing **Enter**. The Microsoft Management Console screen appears.
2. Click > ***File*** > ***Add/Remove Snap-ins***. The Add or Remove Snap-ins screen appears.
3. Under the Available snap-ins list, select **Certificates** and click **Add**. The Certificate Snap-in screen appears.
4. Select **Computer account** and click **Next**. The Select Computer screen appears.
5. Click **Local computer** and click **Finish**. The Add or Remove Snap-ins screen appears indicating the Certificates.
6. In the Add or Remove Snap-ins window, click **Add** again. The Certificate Snap-in screen appears again. This time, click ***My user account*** > ***Next*** > ***Finish***. The Add or Remove Snap-ins screen appears showing the two snap-ins you just added.
7. Click **OK**. The Microsoft Management Console window appears with the Certificates snap-in.
8. Expand **Trusted Root Certification Authorities**. Look for a certificate that matches the old name of the computer. Several identical certificates may be listed. In this example, three certificates for the computer called ADS-WIN10 are listed.

Figure 54: Removing Certificate - Selecting Certificates to Delete



Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]

- Console Root
  - Certificates (Local Computer)
    - Personal
    - Trusted Root Certification Authorities
      - Certificates
    - Enterprise Trust
    - Intermediate Certification Authorities
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Authorities
    - Trusted People
    - Remote Desktop
    - Certificate Enrollment Requests
    - Smart Card Trusted Roots
    - SMS
    - SPC
    - Trusted Devices
  - Certificates - Current User
  - Certificates - Current User

Issued To	Issued By	Expiration Date
ADS-WIN10	ADS-WIN10	12/31/2039
ADS-WIN10	ADS-WIN10	12/31/2039
ADS-WIN10	ADS-WIN10	12/31/2039
AC RAIZ FNMT-RCM	AC RAIZ FNMT-RCM	12/31/2029
AC1 RAIZ MTIN	AC1 RAIZ MTIN	11/3/2019
ACCVRAIZ1	ACCVRAIZ1	12/31/2030
ACEDICOM Root	ACEDICOM Root	4/13/2028
ACNLB	ACNLB	5/15/2023
Actalis Authentication C...	Actalis Authentication CA ...	6/25/2022
Actalis Authentication Ro...	Actalis Authentication Roo...	9/22/2030
AddTrust External CA Root	AddTrust External CA Root	5/30/2020
AdminCA-CD-T01	AdminCA-CD-T01	1/25/2016
Admin-Root-CA	Admin-Root-CA	11/10/2021
AffirmTrust Commercial	AffirmTrust Commercial	12/31/2030
AffirmTrust Networking	AffirmTrust Networking	12/31/2030
AffirmTrust Premium	AffirmTrust Premium	12/31/2040
AffirmTrust Premium ECC	AffirmTrust Premium ECC	12/31/2040

9. Select trusted certificates with the old computer name and click the **Delete** button or select ***Action*** > ***Delete***. The trusted certificates are removed. The next step is to remove personal certificates.
10. Expand **Personal**. Look for a certificate that matches the old name of the computer. Several identical certificates may be listed.
11. Select personal certificates with the old computer name and click the **Delete** button or select ***Action*** > ***Delete***.
12. Close the Microsoft Management Console, optionally saving the Console settings.

Certificate management troubleshooting

The following table lists troubleshooting topics for certificate management.

Table 37: Certificate management troubleshooting

Error Message or Scenario	Solution or Workaround
When you set the Site object Site Security Level attribute to **Encrypted and Trusted** and then download the Site Director, all network engines reporting to the Site Director are modified to change their Site Security Level attribute to Encrypted and Trusted. If a network engine Site Security Level attribute is set to Encrypted and Trusted and does not have a trusted certificate, the network engine does not communicate to the Site Director.	To resolve this issue: 1. Login to the network engine's Site Management Portal in Expert mode. 2. Open the Focus tab of the network engine object. 3. Click **Edit**. 4. For the Site Security Level attribute, select **Encrypted Only**. 5. Click **Save**. 6. Verify the network engine comes online at the Site Director.

Appendix: Installing antivirus software

To install antivirus software on computers that run Metasys software, complete the steps in this appendix. Use one of the following antivirus software programs:

- Symantec® Endpoint Protection software Corporate Edition version 12.x or later.
- McAfee® VirusScan® Enterprise version 8.8 with Patch 9 or later.
- Windows® Defender Antivirus® built into Windows® 10, Windows® Server® 2016, and Windows® Server® 2019.

Installing and configuring Symantec® Endpoint Protection software

Symantec Endpoint Protection software at version 12.0 or later is permitted on computers that run Metasys software.

However, within the SEP software configuration, select only the anti-virus and anti-spyware features. The other two features, **Proactive Threat Protection** and **Network Threat Protection**, can interfere with communication between Metasys software and supervisory devices. Follow the steps in this section to properly install and configure this software.

During and after installation of the Symantec Endpoint Protection software on the Metasys, we recommend the following settings and best practices:

- Select **Install an unmanaged client**. A question box appears regarding installation as an unmanaged client. Click **Yes** to continue.

  The Symantec Endpoint Protection software at version 14.0 installation wizard no longer has the option to install an unmanaged client. To do so with this version of software, refer to Symantec's proprietary support here: http://support.symantec.com/en-us/article.HOWTO101759.html.

- Select **Unmanaged client** for the Client Type.

  ⓘ **Note:** Do not select **Managed client**. If your network is managed by a Symantec server, selecting the Managed Client option changes the custom settings and could prevent the Metasys user interface from working correctly.

- Select the **Custom** setup type.
- Disable the installation of these options: Advanced Download Protection, Outlook Scanner, Notes Scanner, POP3/SMTP Scanner, Proactive Threat Protection, and Network Threat Protection. To disable, click the **down arrow** and select **Entire feature will be unavailable**.
- Select **Enable Auto-Protect**, **Run LiveUpdate**, and **Disable Windows Defender** (if the option is available) for Protection Options.
- Do not select the File Reputation Data Submission check box.
- Do not select the check box under Data Collection -- Installation Options.
- Allow the LiveUpdate process to complete after installation of the Symantec Endpoint Protection software.
- Double-click the **Symantec Endpoint Protection** icon in the Windows task bar. The Status screen appears. Verify that the Proactive Threat Protection and Network Threat Protection features are not installed. If they do not appear on the Status screen, they are not installed.

If the Proactive Threat Protection and Network Threat Protection features are installed, they appear on the Status screen. You must remove them from your computer.

a. In Control Panel, select **Programs > Programs and Features**. Click **Symantec Endpoint Protection** in the list of installed programs.
b. Click **Change** to start the InstallShield Wizard for Symantec Endpoint Protection.
c. When you reach the Program Maintenance screen, select **Modify**. Click **Next**. The Custom Setup screen appears.
d. Click the feature icon and select **Entire feature will be unavailable** for both Proactive Threat Protection and Network Threat Protection. An X appears in front of those features. Click **Next**. Complete the steps in the installation wizard.

Installing and configuring McAfee VirusScan Enterprise software

McAfee® VirusScan® Enterprise version 8.8 with Patch 9 is permitted on computers that run Metasys software.

We recommend installing McAfee VirusScan Enterprise software using the recommendations cited below. If you deviate from these recommendations, Metasys software may not work correctly. If you must enable higher security settings from what is recommended, gradually add changes and check for system reliability as you do so.

During and after installation of the McAfee VirusScan Enterprise software on the Metasys, we recommend the following settings and best practices:

- Select the **Typical** or **Custom** setup type.
- Select **Standard Protection** for the Access Protection Level.
- Select **Run On-Demand Scan** when the installation is complete. We recommend that you take the time now to run a full scan to ensure the computer is prepared for Metasys software. This process can take from 30 to 60 minutes to complete.
- Open the **VirusScan Console**, click **Task** > **Properties**. The Access Protection Properties window appears. Under Categories, select **Anti-virus Standard Protection**. In the protection rules table, remove the **Block and Report** check marks for **Prevent Mass Mailing Worms From Sending Mail**. Leave all other category settings at their defaults.
- Right-click **Full Scan** in the VirusScan Console, and select **Properties**.

  Click the **Performance** tab. Under System utilization, slide the bar pointer to the **Low** setting.

  Click **Schedule**, and with the assistance of your local IT staff, define a daily scan schedule. Do not scan at midnight because the Metasys system performs a daily archive at that time. Click **OK** to save the schedule. Click **OK** on the On-Demand Scan Properties-Full Scan window.
- Click **Task** > **On-Access Scanner Properties** in the VirusScan Console. The On-Access Scanner Properties window appears.

  Click the **All Processes** icon, then select **Configure** different scanning policies for high-risk, low-risk, and default processes. The left pane refreshes to show additional icons.

Click **Low-Risk Processes**. Click **Add** and add **Sqlservr.exe** and **Sqlwriter.exe** to the list of low-risk processes. (If the files do not appear in the list box, click **Browse** and locate them under the Microsoft SQL Server folder.) Click **OK** to save the changes.

Appendix: VPN with a Cisco Meraki MX Security Appliance configuration

This appendix describes how to configure a virtual private network (VPN) with Cisco Meraki™ MX Security Appliance. A VPN is a private data network that uses the public telecommunication infrastructure and the Internet, maintaining privacy through the use of a tunneling protocol and security procedures. Data is encrypted before it is sent through the public network and then decrypted at the receiving end.

To purchase a Meraki MX Security Appliance, use the Cisco Partner Locator to find a Cisco Meraki distributor in your area. The use of the Cisco Meraki™ MX Security Appliance is a good choice for customers who do not have an internal IT department.

All Meraki products require licensing to operate. Meraki licenses are available in one, three, five, seven, or ten year increments. Refer to Meraki MX Security Appliance licensing options. Additional information is available at this link.

Use the instructions in this appendix as an example. Consult your IT department and Cisco proprietary documentation for detailed information. See https://meraki.cisco.com/ for more information.

➧ **Important:** Engage appropriate network security professionals to ensure that the computer hosting the **BCPro Data Server (BDS) Site Director** is a secure host for Internet access. Network security is essential and of the highest importance. Typically, the IT organization must approve configurations that expose networks to the Internet. Be sure to fully read and understand the IT Compliance documentation for your site.

The Cisco Meraki MX Security Appliance supports provisioning and commissioning through the cloud application only. The MX Security Appliance must be pre-provisioned using the device's serial number through the Meraki dashboard. When the device is turned on and connected to the internet, the configuration is retrieved from the cloud application. Configuring the MX Security Appliance by directly connecting to the device is not supported.

To provision MX Security Appliances through the Meraki dashboard, you must first create a Meraki dashboard account. One or more organizations can be associated with a Meraki dashboard account (see Step 1 and Step 2 in Configuring a VPN Tunnel with a Cisco Meraki MX Security appliance).

To grant other users access to the Meraki MX Security Appliance owned or managed by the organization, other members must be added to the organization in the Meraki dashboard (see Step 3 in Configuring a VPN Tunnel with a Cisco Meraki MX Security appliance).

Once an organization is created through the Meraki dashboard, the MX Security Appliance to be provisioned must be added to the organization's inventory, and then the MX Security Appliance must be added to a specific network within the organization (see Step 4 and Step 5 in Configuring a VPN Tunnel with a Cisco Meraki MX Security appliance).

The MX Security Appliance must be physically deployed to the site and connected to the network (see Step 6 in Configuring a VPN Tunnel with a Cisco Meraki MX Security appliance).

When the MX Security Appliance is added to a network, the configuration for the MX Security Appliance can be created (see Step 7 in Configuring a VPN Tunnel with a Cisco Meraki MX Security appliance).

After the MX Security Appliance is deployed to the network through the Meraki dashboard, configure the MX Security Appliance, then the MX Security Appliance can provide VPN access.

Generally, you must connect the Meraki MX Security Appliance to the network that the MX Security Appliance is providing VPN access to and then connect the MX Security Appliance to the modem providing internet access. Consult your IT department and network administrator for further guidance. For more information about the Meraki MX Security Appliance, refer to https://documentation.meraki.com/MX/Installation_Guides/Z3_Installation_Guide.

Once the MX Security Appliance is deployed on the network, a VPN connection can be established to the MX Security Appliance using standard VPN client software that is included with supported Windows® operating systems, Apple® operating systems, or Android™ operating systems (see Step 8 in Configuring a VPN Tunnel with a Cisco Meraki MX Security appliance).

Before adding the MX Security Appliance to the network, provision and commission the device by completing the following steps. You can complete Steps 1-5 before physically adding the MX Security Appliance to the site network.

Configuring a VPN Tunnel with a Cisco Meraki MX Security appliance

About this task:
To configure the MX Security Applicance, complete the following steps:

1. In a web browser, go to https://dashboard.meraki.com. Create a portal user account.
2. In the Meraki dashboard, create and manage your Organization or Organizations. When you first log in, an organization with your company's name is automatically created. You can manage and rename this organization and create additional organizations in the Organization menu.

   In the Cisco Meraki user interface, a single dashboard administers one or more organizations. An organization represents a customer or customer site. Each organization contains one or more networks. A network typically consists of the MX Security Appliances on that common network. For more information about creating and managing organizations, refer to Meraki's **Creating a Dashboard Account and Organization** page.
3. Add portal users to your organization. In the Meraki dashboard, go to ***Organization* > *Configure* > *Administrator***. For more information about adding and managing portal users and administrators, refer to this Meraki's **Managing Dashboard Administrators and Permissions** page.

   After you add a user to your organization, they receive an email with a dashboard access link.
4. Add Cisco Meraki MX Security Appliances to your organization. In the Meraki dashboard, go to ***Organization* > *Configure* > *Inventory***. For more information, refer to this Meraki's **Using the Organization Inventory** page.
5. Create a new network and add the MX Security Appliance to the network. In the Meraki dashboard, go to ***Organization* > *Configure* > *Create network***. For more information, refer to this Meraki reference: here.
6. Deploy the MX Security Appliance to the site. The MX Security Appliance is placed between broadband router/modem providing connectivity to the internet and the IP-based devices.

   a. Configure the router/modem into bridge mode. The user interface of the modem or router is specific to the manufacturer and your Internet Service Provider (ISP). Consult the modem/router and your ISP documentation for further details.
   b. Connect an Ethernet cable from the Internet port of the MX Security Appliance to the router/modem.

    c. Connect the IP devices to the LAN ports of the MX Security Appliance. If there are more than four IP devices, they need to be connected to a separate switch and the switch needs to be connected to one of the LAN ports of the MX Security Appliance.
    d. Power on the MX Security Appliance. Verify that the front LED lights of the MX Security Appliance are solid white.

7. Configure the client VPN by following these steps:

    a. In the Meraki dashboard, hover over **Network** in the left pane. Select the desired network.
    b. Go to ***Teleworker* > *Monitor* >*Appliance*** Status. Record the public IP address that appeared in the WAN field or the dynamic hostname in the Hostname field. You can use the IP address or the hostname when configuring the VPN client.
    c. Go to ***Teleworker Gateway* > *Configure* > *Addresses & VLANs***. Configure the internal BAS network. For a simple BAS network, enter the existing subnet information by clicking on the default network entry under the **Routing** section.

        ⓘ **Note:** The MX IP address should be an available static IP address within the existing BAS network and the MX IP address should be used as the default gateway for all MX Security Appliances, including the network engines and the / ODS.

    d. Go to ***Teleworker Gateway* > *Configure* > *Client VPN***. Enable the Client VPN Server. In a simple BAS network, ensure the Client VPN subnet used here is in a different subnet range than the internal BAS network used previously. The Client VPN subnet should be unique with respect to all other BAS network subnets. For more information about the client VPN settings including VPN user management, refer to Meraki's **Client VPN Overview** page.

8. Setup and configure user MX Security Appliances for VPN access using Meraki's **Client VPN OS Configuration** page.

    ⓘ **Note:** A VPN connection can be established to the MX Security Appliance using standard VPNclient software that is included with supported Windows® operating systems, Apple® operating systems, or Android™ operating systems.

    If you encounter the Windows 809 error in the Windows Event log on a Windows client MX Security Appliance, you may need to add the following key to the Registry:
    Key: Server:HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PolicyAgentRegValue: AssumeUDPEncapsulationContextOnSendRule
    Type: DWORD
    Data Value: 2
    After you create this key, you may need to reboot the Windows client MX Security Appliance.

Configuring the Modem/Router into Bridge mode

To configure the modem/router into bridge mode, complete the following steps:

1. Log in to your modem/router. You must configure your modem or router into bridge mode. The user interface of the modem or router is particular to the manufacturer documentation and your Internet Service Provider (ISP). The steps included here are general. Consult the modem/router and your ISP documentation for further details.
2. Select ***Home Network* > *Subnets & DHCP*** and record the DHCPv4 End Address.

3. Select the ***Firewall >IP Passthrough*** and set the parameters as follows:

    - Set the Allocation Mode to **Default Server**.
    - Set the Default Server Internal Address to the DHCPv4 End Address recorded in Step 2.
    - Set the Passthrough Mode to **DHCP-fixed**.
    - Set the Passthrough Fixed MAC Address to the MAC Address on the MX Security Appliance. The MAC Address is typically listed on the product label on the bottom panel of the device.

Product warranty

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

Software terms

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

Patents

Patents: https://jcipat.com

Contact information

Contact your local branch office: www.johnsoncontrols.com/locations

Contact Johnson Controls: www.johnsoncontrols.com/contact-us