Network and IT Guidance for the IT Professional Technical Bulletin

Code No. LIT-1201578

Software Release 8.0

July 2016

Document Introduction

This document contains important information about connecting a *Metasys*® system to your network. From an IT perspective, a *Metasys* system device is simply a node on the network. But, the *Metasys* system uses communication protocols, security methods, and other technologies that you should consider.

This document is intended for the IT professional. Refer to the *Network and IT Guidance for the BAS Professional Technical Bulletin (LIT-12011279)* if you need expanded concepts and definitions related to the information in this document.

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 an ADS/ADX/ODS requires the computer be offline for a period of time. Similarly, installing new software on the ADS/ADX/ODS may require a computer restart.

Note: In this document, **engine** refers to all models of Network Automation Engine (NAE) 35, NAE45, NAE55, Network Integration Engine (NIE) 55, Network Control Engine (NCE) 25, NxE85, NxEx9, and LonWorks® Control Server (LCS) 85, unless noted otherwise.

Some products in this document are available only to specific markets.

Summary of Changes

The following information is new or revised in July 2016:

- Added a note recommending that you not use your ADS/ADX or ADS-Lite computer to browse to web sites, including *Metasys* UI or *Metasys* UI Offline. We recommend using client computers and devices for browsing to web sites.
- Corrected figures that include VPN tunnels. The VPN Router should be inside the firewall.

The following information was new or revised in June 2016:

- Added *Metasys* UI Offline throughout the document, including the *Microsoft Active Directory® Service Overview*, *Table 4*, *Secure Sockets Layer (SSL)/Transport Layer Security (TLS)*, and *Appendix: Security Certificate Implementation* sections.
- Added Windows 10 Professional and Enterprise operating system and removed unsupported operating systems throughout the document.
- Added *RADIUS Overview*.
- Added UberDebug service, removed N30, removed SNMP Trap, and revised protocol and port information in *Table 7*.
- Added *Syslog Overview*.
- Added the Last Login feature in SMP and SCT in *Last Login*.
- Updated Launcher screens in *Launcher Download Options and Proxy Settings*.
- Added VPN Tunnels to all *Metasys* diagrams throughout the document.
- Updated *Metasys* databases in *Microsoft SQL Database Considerations*.
- Add *Appendix: Configuring a VPN Tunnel with a NETGEAR® ProSAFE® 8-Port Gigabit VPN Firewall/Router*.

Related Documentation

Table 1: Related Information

For Information On	See Document
The *Metasys* System	*Metasys® SMP Help (LIT-1201793)*
Access Settings and Users/Roles in the System	*Security Administrator System Technical Bulletin (LIT-1201528)*
Security Database Backup/Restore	*Metasys® SCT Help (LIT-12011964)*

Table 1: Related Information

For Information On	See Document
Time, Date, Time Zone, and Time Synchronization	*NAE Commissioning Guide (LIT-1201519)*
	ADS/ADX Commissioning Guide (LIT-1201645)
	ODS Commissioning Guide (LIT-12011944)
	NIEx9 Commissioning Guide (LIT-12011922)
	LCS85 Installation and Upgrade Instructions (LIT-12011623)
Interaction between an N1 Network and the NIE	*N1 Migration with the NIE Technical Bulletin (LIT-1201535)*
BACnet® Network and a *Metasys* Network Interaction	*BACnet® Controller Integration with NAE/NCE Technical Bulletin (LIT-1201531)*
SNMP for Network Monitoring	*Metasys® SMP Help (LIT-1201793)*
	Open Data Server Help (LIT-12011942)

1 This LIT number represents a print-friendly version of the Help.

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 windows.

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 are required. Configuration requirements may be upgraded on a regular basis to reflect these changes.

Refer to the *Metasys System Configuration Guide (LIT-12011832)* for specific computer requirements.

Metasys Device IP Address Assignment (DHCP or Manual)

See *Table 2* for IP address assignment rules in the *Metasys* system.

Table 2: IP Address Assignments

Device	Dynamic Addressing	Static Addressing	Comments
NAE/NCE	Supported	Recommended when the NAE/NCE is the Site Director[1]	• The NAE/NCE is a supervisory controller/engine. • NAE85s are installed on server-class computers, but all other models 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 Dynamic Host Configuration Protocol (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 NIE is a supervisory controller/engine. • NIE85s are installed on server-class computers, but the NIE55s and NIE59s are stand-alone devices 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.
LCS	Supported	Recommended when the LCS85 is the Site Director[1]	• The NAE/NCE is a supervisory controller/engine. • LCS85s are installed on server-class computers. • 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.
ADS/ADX/ODS	Supported	Recommended when the ADS/ADX/ODS is the Site Director[1]	The ADS is loaded on a desktop-class computer and the ADX is installed on a server-class computer. The ODS is loaded on either a desktop-class computer or a server-class computer.

Table 2: IP Address Assignments

Device	Dynamic Addressing	Static Addressing	Comments
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 PRI (NET1, LAN1) can be enabled to use DHCP. The secondary Ethernet connection SEC (NET2, LAN2) can only use static IP addressing. • A new 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.
WRS-RTN	Supported	Recommended if communication issues arise	• If your network uses 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.

[1] 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 manager time and date. This function resides in an engine or in an ADS/ADX on large installations. Although an engine can be a Site Director, if the site has an ADS/ADX, then an ADS/ADX 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.

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 domain name system (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 hosts 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 *NAE Commissioning Guide (LIT-1201519)*, *NIEx9 Commissioning Guide (LIT-12011922)*, or *LCS85 Commissioning Guide (LIT-12011568)*. For information on configuring DHCP and DNS for an ADS/ADX/ODS, 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 *Metasys* 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 *Metasys* 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, *Metasys* 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.

Metasys devices require that you configure the DHCP options in *Table 3* in the DHCP server in addition to the IP address and subnet mask.

Table 3: DHCP Options

Option	Description
Option 003	Router
Option 006	DNS Servers
Option 015	DNS Domain Name

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), 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 ADS/ADX/ODS, *Metasys* UI, *Metasys* UI Offline, and SCT (but not the engines). Using the *Metasys* Administrator Tool 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 *Metasys* Administrator Tool, you can also grant SSO or Single Sign On access to all Active Directory users for a more convenient authentication process.

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 ADS, ADX, ODS, 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.

SSO allows users to access any *Metasys* User Interface 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 a Windows Active Directory account that is active.
- 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 *Metasys* Administrator Tool.
- The SSO feature is enabled in the *Metasys* Administrator Tool.
- The Active Directory user is added in the local MESA-SSO group on the ADX/ADS/ODS.

Support for Active Directory Service (Including Single Sign-On Capability)

Table 4 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 4: Products That Support Active Directory Logins and SSO

Application	Active Directory logins Supported	SSO Supported
ADS Site Management Portal UI	Yes	Yes
ADX Site Management Portal UI	Yes	Yes
SCT	Yes[1]	Yes
***Metasys* UI and *Metasys* UI Offline**	Yes	No
ODS	Yes	Yes
***Metasys* Advanced Reporting System**	No	No[2]
Ready Access Portal	Yes (Computer) No (Handheld)	No[3]
Engine[4]	No	No
***Metasys* for Validated Environments**	Yes	No

[1] If you are using the SCT Manager to switch between SCT versions, do not use the Active Directory service. SCT versions managed this way do not support the integration of the *Metasys* system with the Active Directory service.

[2] 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.

[3] If you are using Ready Access Portal UI on an ADS/ADX/ODS, you still can use the SSO capability to log in to the ADS/ADX/ODS Site Management Portal UI. For example, if you have an ADX/ODS with the Ready Access Portal software installed, 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 Ready Access Portal UI.

[4] The engine Site Management Portal UI does not support authentication with Active Directory service. If you have an ADS/ADX/ODS Site Director, however, you can log in to the ADS/ADX/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 Windows Server® 2012 R2, Windows Server 2012, Windows Server 2008 R2 with SP1, or Windows Server 2008 SP2 domains and read-only domains are supported.
- Use of a Windows Server 2012 R2, Windows Server 2012, or Windows Server 2008 R2 SP1 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 Windows Server 2014, Windows Server 2012 R2, Windows Server 2012, or Windows Server 2008 R2 SP1 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 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 ADS/ADX/ODS and SCT. Before login, RSA exchange of an RC2 key occurs. For details, see *Network Message Security*.
- 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 ADS/ADX/ODS 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 fully qualified UPN formatted names. Single Label Domains are one example of a directory structure that is not compatible with the *Metasys* system. 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 ADS/ADX/ODS 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*.

ADS/ADX/ODS/SCT Considerations

The ADS/ADX/ODS 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 ADS/ADX/ODS 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 ADS/ADX/ODS 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 ADS/ADX/ODS 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 ADS/ADX/ODS 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 ADS/ADX/ODS or SCT computer must be formatted for the NTFS file system, not the FAT file system.
- The ADS/ADX/ODS 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 such as engines or ADXs 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, including engines. The child devices:

- can be any combination of platforms illustrated in *Figure 14*
- 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.

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 Lightweight Directory Access Protocol (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 each service account, use the user principal name (UPN) format for the user name. 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 user name.
- 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 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:

- The UPN format is used for the user name, 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 user name appears on the main *Metasys* Site Management Portal UI screen to identify the currently logged in user. It also appears as the user name 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 user name for an Active Directory service user changes, you do not need to specify the new name with the *Metasys* System Administrative tool. The update of the new user name 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 user name 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 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 user name 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.

RADIUS Overview

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

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

- RFC 2865 - Remote Authentication Dial In User Service (RADIUS)
- RFC 2548 - Microsoft Vendor-specific RADIUS Attributes
- RFC 2759 - Microsoft PPP CHAP Extensions, Version 2

The *Metasys* system implementation of RADIUS is as follows:

- The *Metasys* system does not import authorization; all *Metasys* system users, both local (*Metasys*) and non-local (RADIUS), are authorized through user configuration done online in the SMP, then stored in the *Metasys* security database.
- The user ID must match what is expected to be authenticated by the RADIUS server, with or without the @domain as defined by the local RADIUS implementation.
- Since the *Metasys* system performs no local authentication of non-local users, all password functions are unavailable or ignored when creating and maintaining non-local *Metasys* user accounts. RADIUS passwords are never stored in the *Metasys* security database.
- Authorization for a RADIUS user may be configured as Administrator, User, Operator, Maintenance, or any custom roles created in the *Metasys* system.
- When a non-local user receives a number of consecutive RADIUS failures to authenticate and the account has been set up to lock after receiving that many failed login attempts, the *Metasys* system authorization locks, prohibiting the user from accessing the *Metasys* system device until a *Metasys* system administrator unlocks the account.
- When a non-local user is authenticated by RADIUS, and the *Metasys* system schedule prohibits access during the login time, the user's login attempt fails.

When a user provides a non-local user name to the *Metasys* system for login, after confirming the supplied password conforms to *Metasys* complexity rules, the controller passes the credentials, including the user name and password, to the configured RADIUS server for authentication. Only after the RADIUS server confirms authenticated access is authorization then permitted as specified in the *Metasys* security database.

Messages reporting errors in RADIUS authentication are intentionally obscure to hinder possible intrusion from unauthorized users. See *RADIUS Errors* for some situations that may result in error messages. Descriptive *Metasys* system login failure messages are presented to the user only when RADIUS is disabled. When RADIUS is enabled, local and non-local authentication failure messages are identical and obfuscated.

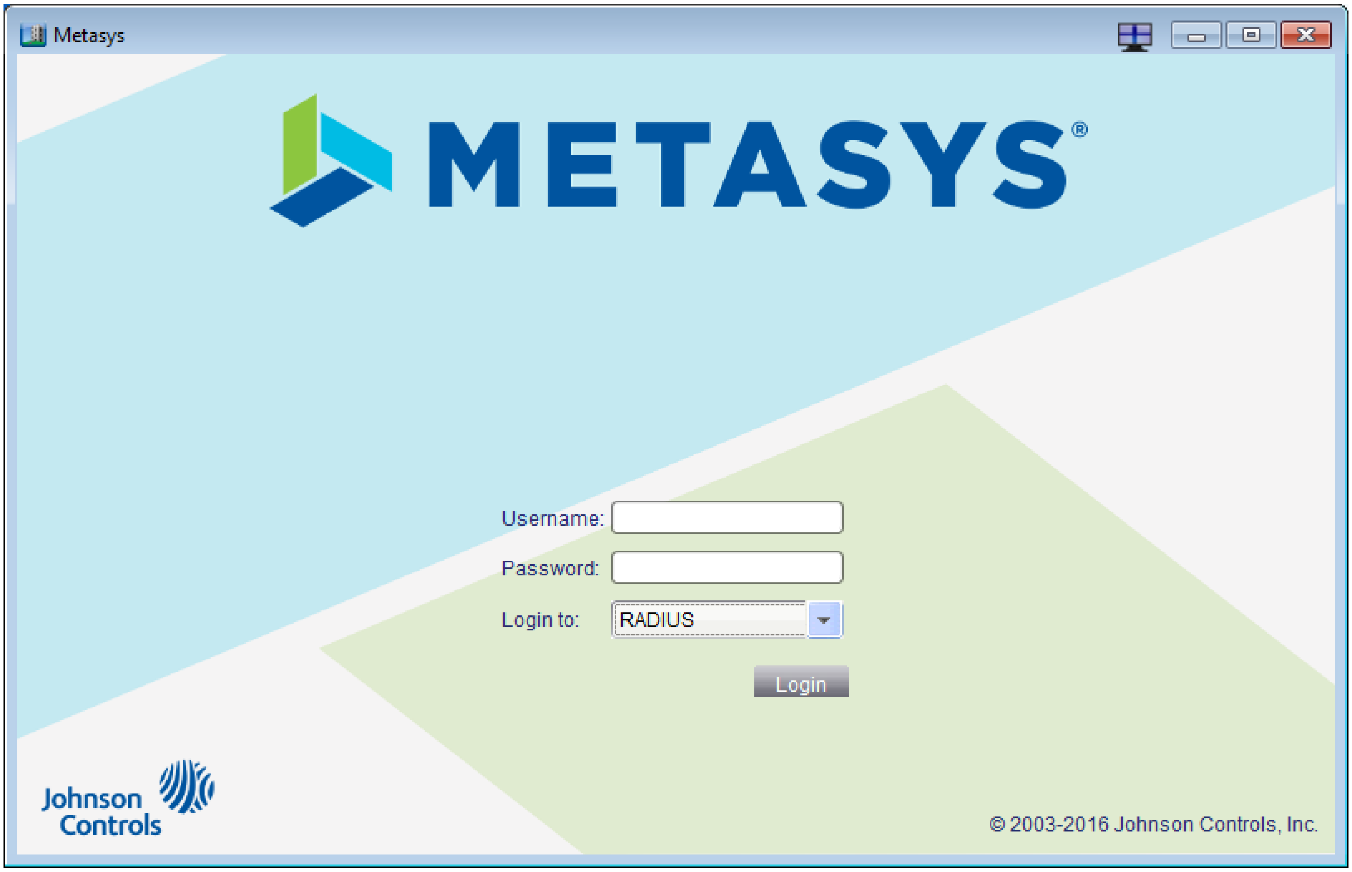
Situations When *Metasys* System Login Screen Appears for RADIUS Users

The following situations cause the RADIUS user to be presented with the *Metasys* system login screen.

- when you log out of the *Metasys* Site Management Portal UI (either manually or when a user session ends)
- if RADIUS user authentication fails for any reason
- when you are logged in to the Windows operating system (OS) with a RADIUS user account that is not privileged within the *Metasys* system
- if the RADIUS server is unavailable
- when you are logged in to the Windows OS using a local Windows account and not a RADIUS user account
- when access to RADIUS server is restricted at login time through a RADIUS user time sheet (known as Logon Hours) or access is restricted to the *Metasys* system via the *Metasys* time sheet. RADIUS server Logon Hours takes precedence, so if you are restricted from operating system access, but not restricted by a *Metasys* time sheet, access to the *Metasys* system as a RADIUS user is not granted.
- if your RADIUS user account is enabled, but overridden to disabled with the *Metasys* Access Suspended property within *Metasys* Security Administration User Properties
- if you log in to a *Metasys* device such as an ADS, ADX, ODS, SCT, NAE or NCE
- if *Metasys* authorization fails for any reason, such as when a user without System Configuration Tool permissions attempts to log in to System Configuration Tool (SCT)

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

Figure 1: *Metasys* Login Screen with RADIUS Server Domain List



Login to: RADIUS

From this screen, you have the following options:

- Enter a RADIUS user name and password, and click RADIUS in a drop-down list.
- Enter a RADIUS user name in the form of domain\username (sometimes called the pre-Windows 2000 format) and a RADIUS password. (The **Login to** drop-down list becomes disabled.)

Note: User names are obscured at login for RADIUS accounts. After login, user names are partially obscured (for example, JSmith appears as JSm***).

The user credentials are strongly encrypted before being transmitted over the network for authentication. (For details on the encryption process used, refer to the *Network Message Security* section of the *Network and IT Guidance for the IT Professional Technical Bulletin (LIT-1201578)*. These credentials are active for the entire *Metasys* Site Management Portal UI session until you log out (or the user session terminates).

If the *Metasys* Device Manager has not fully started, and you try to log in to the Application and Data Server/Extended Application and Data Server (ADS/ADX), a runtime status error occurs and the *Metasys* login screen appears. In this case, the *Metasys* login screen does not display the RADIUS server domain drop-down list and you are not able to log in as a RADIUS user.

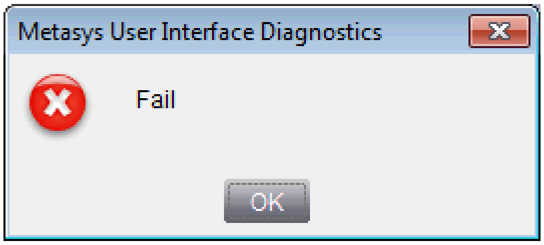
To log in as an RADIUS user, you must close the login screen, wait a few moments for the *Metasys* Device Manager to fully start, then navigate again to the ADS/ADX. If you remain at the login screen following the startup error and do not close it, then log in with a *Metasys* local user account. All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

RADIUS Errors

This section describes some situations which may result in error messages after enabling RADIUS to authenticate some user login credentials. When the servers or network engines are configured to not enable RADIUS authentication, the standard *Metasys* login error messages appear. Realize that RADIUS errors are intentionally obscure to hinder possible intrusion from unauthorized users. If you encounter these errors and cannot resolve them, contact your local network administrator. The figures in this section illustrate the RADIUS error messages.

1. If the RADIUS server is not online or available, then non-local users cannot log in to the *Metasys* system and an error message appears (see *Figure 2*).
2. If the servers or network engines is configured to communicate with a RADIUS server, and the RADIUS server does not respond to a login request by a non-local user, the message the non-local user sees indicates failure to log in without identifying that the RADIUS server is unavailable. See *Figure 2*.
3. If the non-local user's account is disabled either in the *Metasys* system or in the RADIUS server, the error message shown in *Figure 3* appears.
4. If the non-local user's account password is expired, the error message shown in *Figure 4* appears.
5. If the non-local user's account password does not meet the *Metasys* system password complexity requirements, the error message shown in *Figure 5* appears.
6. If you try to log in to a servers or network engines with a non-complex password and RADIUS is not enabled, the error message shown in *Figure 6* appears.

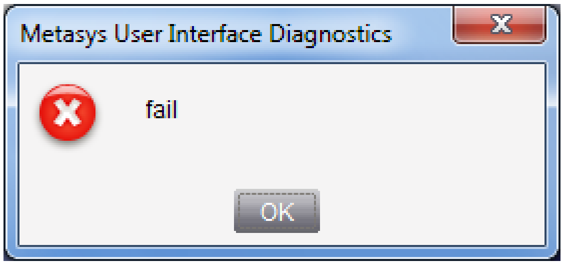
Figure 2: Login RADIUS Failure Message 1



Metasys User Interface Diagnostics

Fail

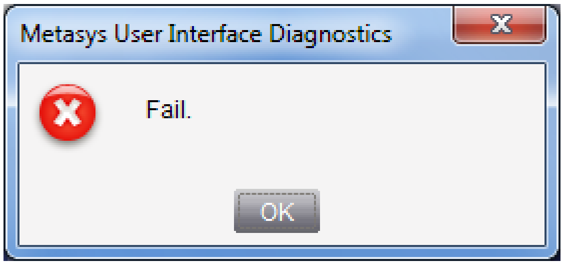
Figure 3: RADIUS Failure Message 2



Metasys User Interface Diagnostics

fail

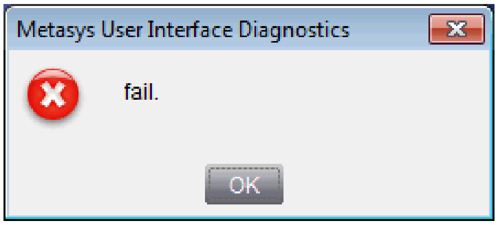
Figure 4: RADIUS Failure Message 3



Metasys User Interface Diagnostics

Fail.

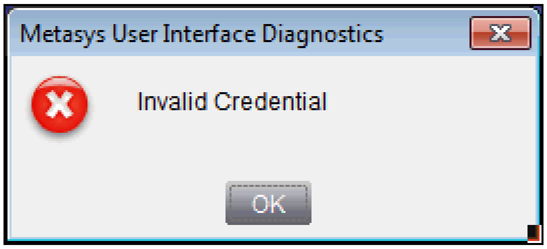
Figure 5: RADIUS Failure Message 4



Metasys User Interface Diagnostics

fail.

Figure 6: Non-Complex Password Error - RADIUS Disabled



Metasys User Interface Diagnostics

Invalid Credential

Additionally, when RADIUS is enabled, error messages for **local users** are modified as follows:

- If the user's account is disabled, locked out, or cannot log in because the user's timesheet does not permit login at this time, the error message shown in *Figure 3* appears.
- If the user's password is entered incorrectly, the error message shown in *Figure 2* appears.
- If the user's password is expired, the standard prompt for changing the user's password appears.

Syslog Overview

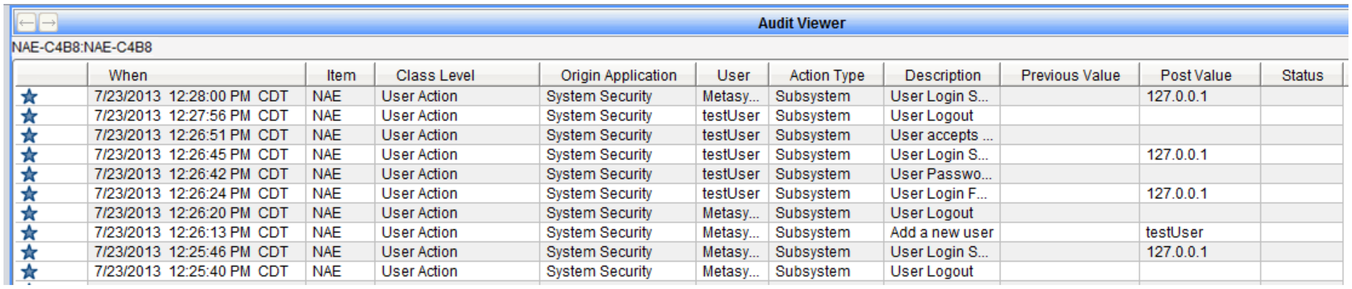
The servers and network engines provide the optional capability of sending their configured audit log entries and event notifications to an external, customer-provided industry-standard Syslog server destination, conforming to published Internet document RFC 3164. Syslog implements a client-server application 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. Using the UDP/IP protocol, the NAE551S-2 cannot guarantee the delivery of messages to the Syslog server.

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, the fields are sent in the order shown in the *Metasys* Audit Viewer (*Figure 7*). 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 7: *Metasys* Audit Viewer



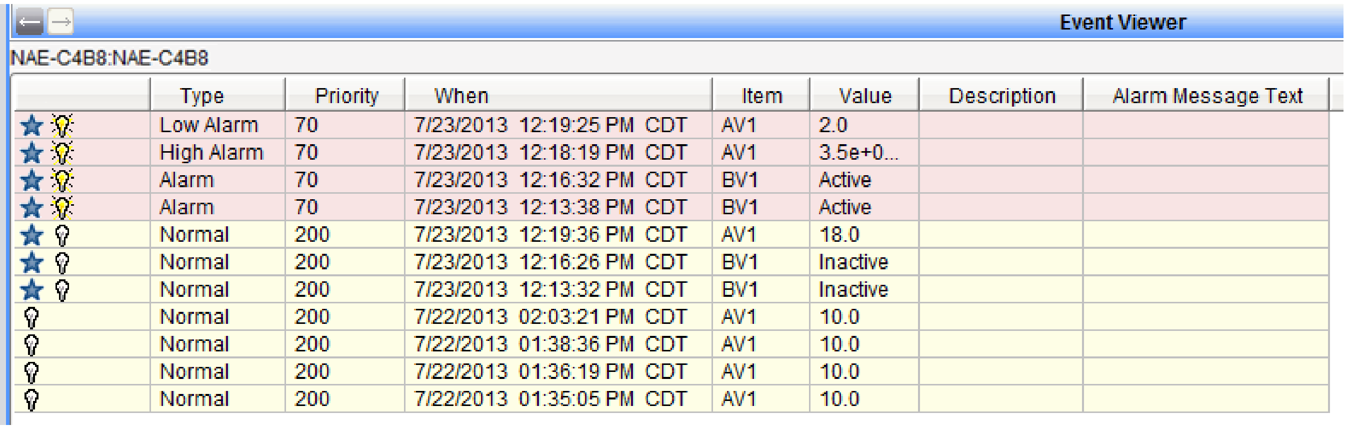
Audit Viewer

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, the fields are sent in the order shown in the *Metasys* Event Viewer, excluding the icon column (*Figure 8*). The Event Viewer columns are labeled as follows: Type | Priority | When | Item | Value | Description | Alarm Message Text.

Figure 8: *Metasys* Event Viewer



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		

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 5: 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 the *Metasys SMP Help (LIT-1201793)* PDF. *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.

RADIUS and Syslog Configurations

RADIUS and Syslog may be configured only online by a *Metasys* system administrator using the SMP.

Important: If the RADIUS configuration is not restored into the servers or network engines during a download, all previously added RADIUS users do not appear in the users list and remain hidden until RADIUS is enabled.

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

Introduction

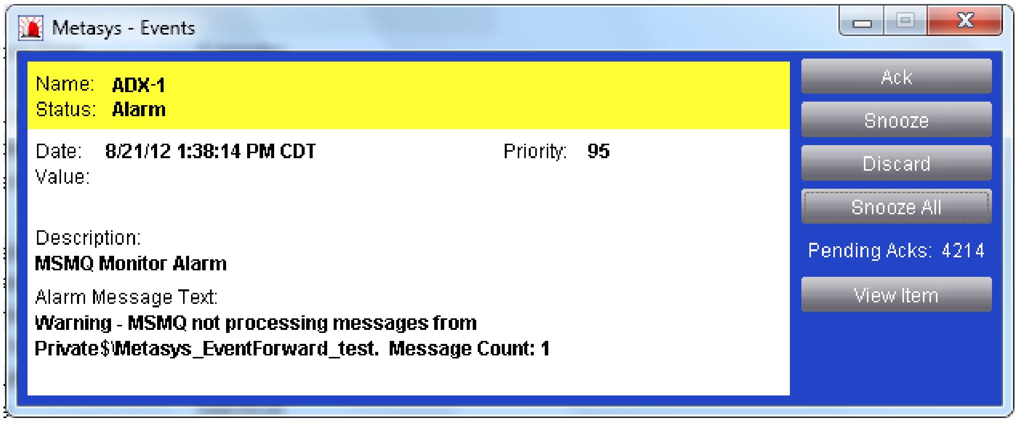
As implemented in the *Metasys* system, MSMQ supports trending and Site Management Portal UI navigation tree features. The Site Director queue receives trend data and navigation tree changes from other system devices. When the Site Director is busy, the messages remain in the queue until the Site Director is available to process them. Using MSMQ allows the system to avoid bottlenecks by separating the actions of receiving and processing data.

MSMQ must be installed on all computers where ADS, ADX, ODS, and Ready Access Portal software is installed. Once installed, do not stop or disable MSMQ. If MSMQ is stopped or disabled, the Site Director does not receive/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 and Ready Access Portal computer contain all the navigation information for an entire site in a cache known as the Navigation Tree 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 Navigation Tree Cache 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 9* for an example of the *Metasys* alarm.

Figure 9: 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.

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 ADSs/ADXs/ODSs 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 6: Virtual Environment Considerations and Requirements

Topic	Consideration or Requirement
Supported Virtual Environment Platforms	The *Metasys* system supports the following virtual environment platforms: • VMware vSphere Hypervisor (ESXi) 5.0 or later • VMware Workstation 10.0 • Microsoft Hyper-V™ Server
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 *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 ADX may experience performance issues. Set the priority of the ADS/ADX hardware resources at the highest level.
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.

Table 6: Virtual Environment Considerations and Requirements

Topic	Consideration or Requirement
Dedicated Network Card	Use one dedicated network card that has a static IP address assigned. The ADS/ADX 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 ADX 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. For general hardware requirements, refer to the *Application and Data Server (ADS/ADX) Product Bulletin (LIT-1201525)* 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 (ADS/ADX, 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)

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 via a Network Management System (NMS).

A custom *Metasys* system specific management information base (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 ADSs/ADXs/ODSs. *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 (engine and ADS/ADX/ODS).

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])

There are three methods for network time synchronization available in the *Metasys* system, including Microsoft Windows SNTP time synchronization, Multicast, and BACnet time synchronization.

You can use the Multicast and Microsoft Windows methods when an SNTP manager 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 *Time Zone, Date, and Time Management Appendix* found in the *NAE Commissioning Guide (LIT-1201519)*, *LCS85 Commissioning Guide (LIT-12011568)*, *ODS Commissioning Guide (LIT-12011944)*, *NIEx9 Commissioning Guide (LIT-12011922)*, and the *ADS/ADX Commissioning Guide (LIT-1201645)*.

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.

For information about using email as a notification method for alarms, refer to the *NAE Commissioning Guide (LIT-1201519)*, *NIEx9 Commissioning Guide (LIT-12011922)*, or *LCS85 Commissioning Guide (LIT-12011568)*.

Notes:

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

Encrypted Email

Metasys software features an email encryption capability that encrypts your user name and password as they are entered into the SMP UI. This feature allows embedded and server machines to send email to email servers over a secure channel (secure socket layer [SSL]). The entire email payload is encrypted, and allows *Metasys* software to communicate to email servers that require SSL connections.

Email encryption can be configured with no authentication required, SMTP authentication, and POP-Before-SMTP authentication.

Communication to Pager, Email, Printer, SNMP, or Syslog Destination

The system guarantees delivery of events from engines to an ADS/ADX/ODS, but this delivery guarantee does not extend to the Destination Delivery Agent (DDA) destinations: pagers, email accounts, printers, or SNMP destinations.

See the following:

- **Pagers:** (Telocator Alphanumeric Protocol) - Delivery guaranteed to the service provider. The service provider delivers to the final pager account as time permits.
- **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.
- **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.
- **SNMP:** This delivery system uses User Datagram Protocol (UDP), which does not guarantee delivery.
- **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.

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

Location of a Site Director in a Demilitarized Zone (DMZ) or on the Internet

Important: Do not place the Site Director and any *Metasys* components in the DMZ or on the Internet. If offsite access is necessary, use a VPN. Access to any component of the *Metasys* system should be strictly controlled.

The Site Director provides access to all the devices on the site using only one public IP address (the address of the Site Director). Only the Site Director requires access through the firewall to the Internet. All other devices on the site are exposed through the Site Director. See *Figure 10* for an example of a DMZ.

Communication between a *Metasys* client computer on the Internet (web browser in *Figure 10*) and the Site Director within a DMZ uses HTTP only. *Metasys* software requires that only TCP Port 80 be opened at the firewall.

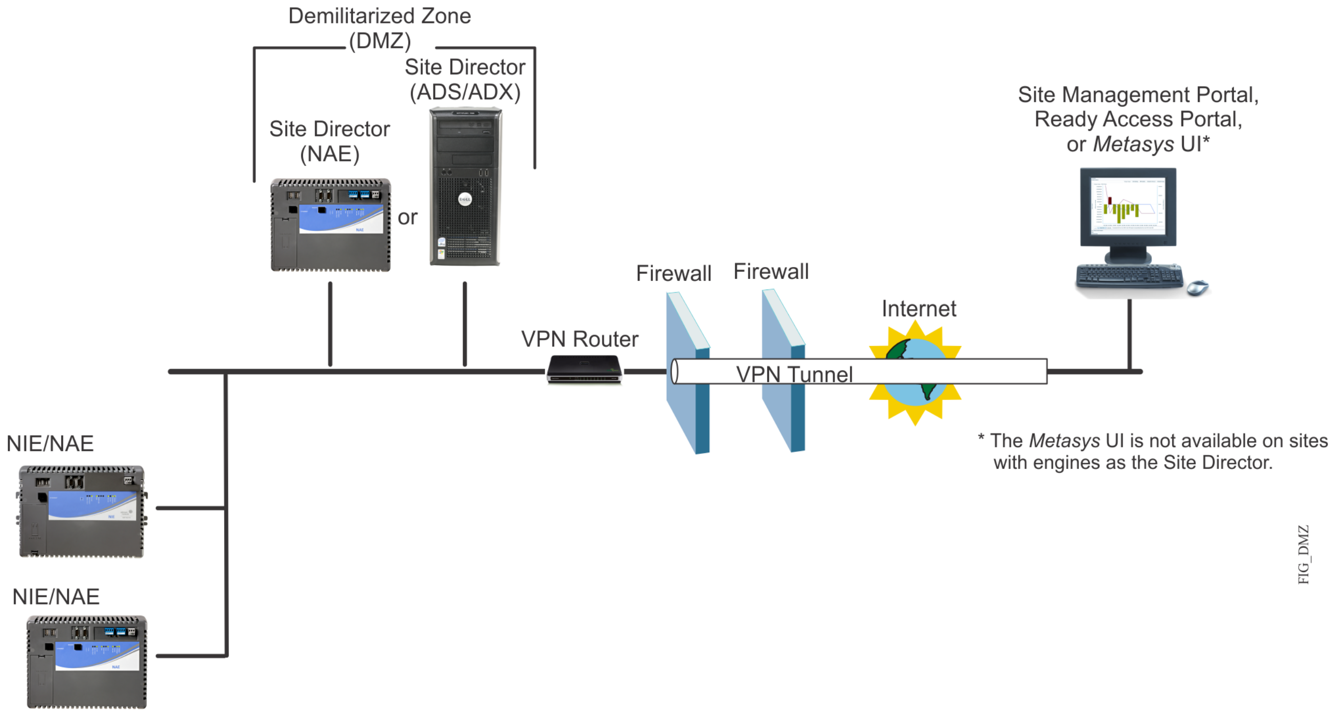
If you are using NAT to communicate between a browser and the *Metasys* site over the Internet, all *Metasys* system devices exposed to the Internet (normally only the Site Director) must have static internal and external IP addresses. Dynamic NAT is not a supported *Metasys* system configuration. If you are using DHCP to assign addresses to devices that communicate across networks that use NAT, your DHCP server should be configured to always allocate the same IP address to each *Metasys* system device. This is done in the DHCP server by assigning IP addresses to the MAC addresses of the *Metasys* system devices. 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 addresses from a DHCP server.

Note: Supervisory devices in a *Metasys* system site (the Site Director and its child devices) cannot be separated by NATs. All devices on a site must be addressable via local IP addresses. However, if a site is forwarding historical data (such as alarms, events, and trends) to an ADS/ADX/ODS repository that is not part of the site, NATs can be used if the ADS/ADX/ODS repository is assigned static internal and external IP addresses.

If the Active Directory service is implemented for *Metasys* system use, all involved devices (the ADS/ADX/ODS/SCT computer and Site Management Portal UI clients) must be directly addressable on the LAN. The client cannot make a direct connection to the Site Director over the Internet. For example, if the user is connected remotely to the Site Director, a VPN or extranet connection must be used. This is a restriction of the Active Directory service and is not unique to the *Metasys* system implementation of the service. The existing customer infrastructure determines VPN and extranet connectivity; the *Metasys* system implementation of the Active Directory service does not require a particular connectivity method.

At Release 6.0 or later, Remote Desktop for engines is only available through the NxE Information and Configuration Tool (NCT). If you intend to apply upgrades or patches over the Internet instead of locally at the site, you must open additional ports to the Internet.

Figure 10: Site Director in a DMZ Example



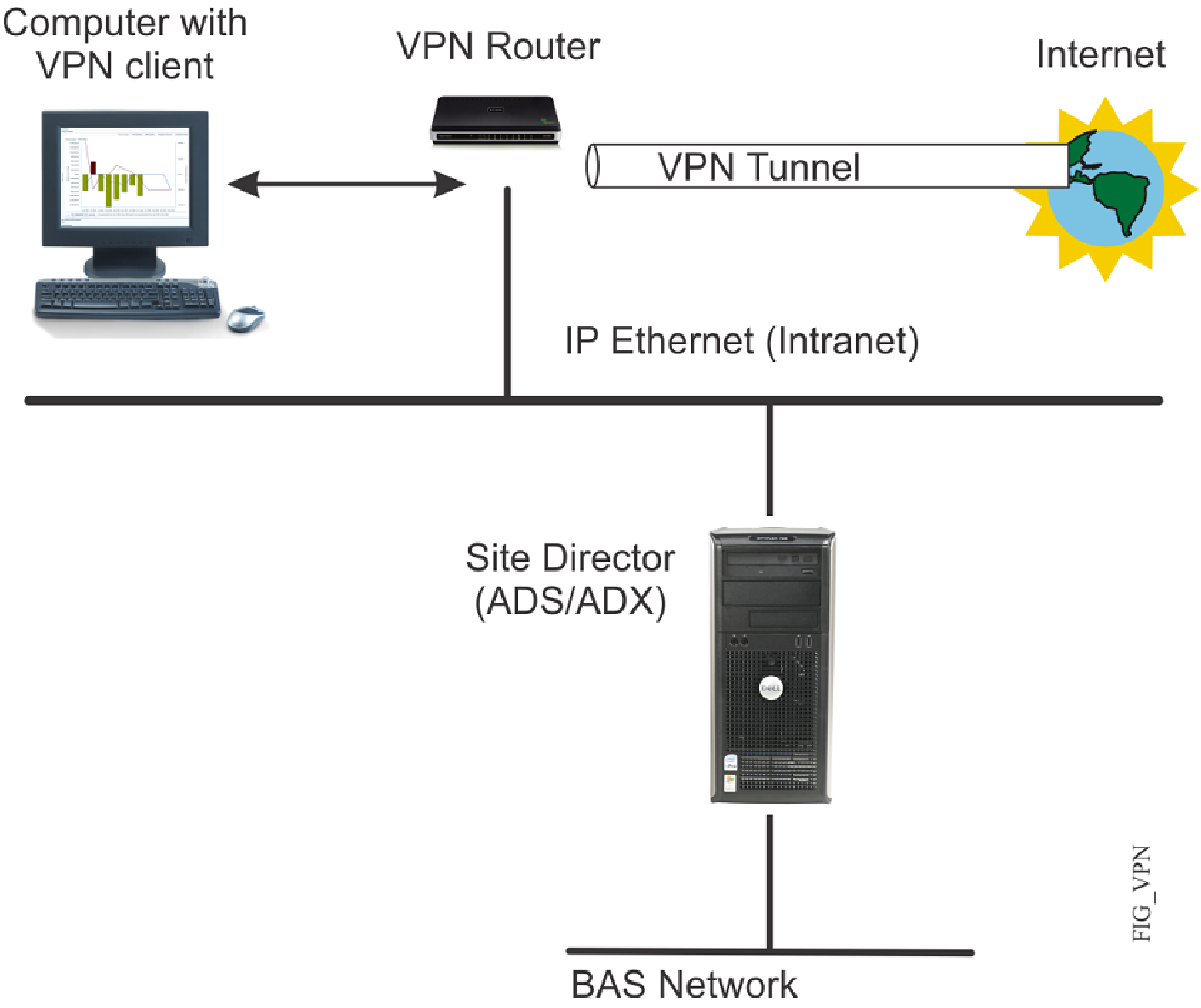
Remote Access to the Metasys System Using a VPN

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.

Note: Johnson Controls does not supply VPN infrastructure.

Note: The *Metasys* system does not support Secure Socket Layer (SSL) VPN.

Figure 11: *Metasys* System Internet Communication via VPN

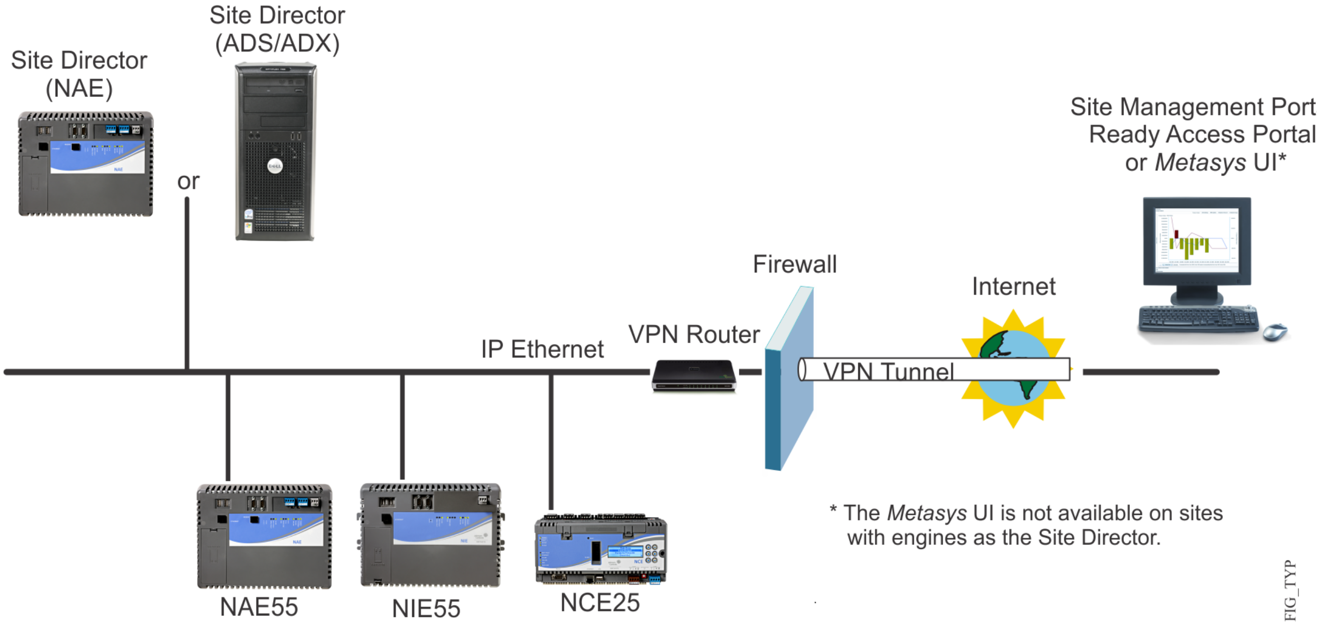


Metasys System Architecture

Figure 12 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 12: *Metasys* System Architecture



* The *Metasys* UI is not available on sites with engines as the Site Director.

Protocols, Ports, and Connectivity for the Metasys System

Protocols and Ports Tables

Note: Bluetooth® technology is used by the *Metasys* system 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.

Table 7 and *Table 8* describe the various IP protocols and how they relate to the *Metasys* system. See *Connectivity and Protocol Diagrams* for information on how protocols are used in various network layouts.

Table 7: Ethernet Protocols and Ports

Protocol	Uses	Port[1] Number	*Metasys* Device	Description
DHCP [4]	UDP	67 68	Engine ADS/ADX/ODS Computer (Web Browser) Active Directory Client *Metasys* SCT	Assigns and keeps track of dynamic IP addresses and other network configuration parameters. **Alternate Method:** Use static IP addresses.
Trivial File Transfer Protocol (TFTP) [4]	UDP	69	Engine *Metasys* SCT	Downloads new images to NAEs.
DNS	UDP	53	Engine ADS/ADX/ODS Computer (Web Browser) Active Directory Client	Translates domain names into IP addresses.
HTTP [4]	TCP	80	Engine ADS/ADX/ODS Computer (Web Browser) *Metasys* SCT	Provides communication between peer controllers, computers, and other Internet systems using Simple Object Access Protocol (SOAP) over HTTP. The ADS/ADX/ODS requires that only Port 80 be open to receive communication from client devices. **Note:** TCP Port Forwarding is supported on Port 80 only.
Post Office Protocol 3 (POP3)	TCP	110 995	Computer (Web Browser)	Usually, POP receives and holds email for downloading from your Internet server. POP3 is allowed in the *Metasys* system only for authentication from a Simple Network Management Protocol (SNMP) server. **Note:** Firewall rules are not necessary to allow access in most cases because this server should be behind the firewall.
SMTP	TCP	25 465	Engine ADS/ADX/ODS	Alarms and events.

Table 7: Ethernet Protocols and Ports

Protocol	Uses	Port[1] Number	*Metasys* Device	Description
SNMP [4]	UDP	161	Engine	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:** Use pager or email destinations for remote alarm notification instead of SNMP.
			ADS/ADX/ODS	
			Metasys SCT	
Simple Network Time Protocol (SNTP) [4]	UDP	123	Engine	Used to synchronize computer clocks over a network between a server and its clients. SNTP is not required for all systems.
			ADS/ADX/ODS	
	TCP	80	ADS/ADX/ODS	
			Computer (Web Browser)	
			Metasys System Client (Client not on any Domain)	
RADIUS	UDP	1812	Engine	Provides a secured server and network engines to authenticate non-local user access through a Remote Authentication Dial-In User Service (RADIUS) server. RADIUS is used by the server and network engines to authenticate the identity of authorized non-local users of the system.
			ADS/ADX/ODS	
			Metasys SCT	
Syslog	UDP	514	Engine	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.
			ADS/ADX/ODS	
			Metasys SCT	

Table 7: Ethernet Protocols and Ports

Protocol	Uses	Port[1] Number	*Metasys* Device	Description
N1 Protocol	UDP	11001[2]	NIE5x	Provides N1 message transmission (proprietary packet encoded in UDP). 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 Multinetwork 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.
			Network Control Module (NCM)	
BACnet/IP Protocol	UDP	47808	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.
			TEC20-3c-2	
Microsoft SQL Server Database	TCP	1433	ADX	Used between the web/application server and database server computers when the ADX is split across two devices.
			Metasys ADX Split Database Server (Member of Domain X)	
Remote Desktop Protocol (RDP)	TCP	3389	NAE55/NIE	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 7: Ethernet Protocols and Ports

Protocol	Uses	Port[1] Number	*Metasys* Device	Description
Kerberos	TCP UDP	88	*Metasys* System Client (Member of any Domain)	Kerberos is an authentication protocol 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.
			Metasys SCT (Member of Domain X)	
			Metasys ADS/ADX/ODS (Member of Domain X)	
			Metasys ADX Split Web/Application Server (Member of Domain X)	
NT LAN Manager Version 2 (NTLMv2)	TCP	445	*Metasys* System Client (Member of any Domain)	NTLMv2 is the protocol used during *Metasys* system SSO (login free) 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.
			Metasys SCT (Member of Domain X)	
			Metasys ADS/ADX/ODS (Member of Domain X)	
			Metasys ADX Split Web/Application Server (Member of Domain X)	
Secure Sockets Layer (SSL)/Transport Layer Security (TLS)/HTTPS	TCP	443	*Metasys* Advanced Reporting ADX	Required if you use SSL with your reporting ADX. See *Implementing SSL Security for the Metasys Advanced Reporting System*.
			Ready Access Portal	
			Metasys UI	Required if you use SSL with the *Metasys* UI and the *Metasys* UI Offline for site security. See *Appendix: Security Certificate Implementation*.
			Metasys UI Offline	
LDAP	TCP	389	*Metasys* System Client (Member of any Domain)[3]	LDAP is 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.
			Metasys SCT (Member of Domain X)	
			Metasys ADS/ADX/ODS (Member of Domain X)	
			Metasys ADX Split Web/Application Server (Member of Domain X)	

Table 7: Ethernet Protocols and Ports

Protocol	Uses	Port[1] Number	*Metasys* Device	Description
Network Time Protocol (NTP)	TCP	123	*Metasys* System Client (Member of any Domain)	Time synchronization across a network between Windows 10, Windows 8.1, or Windows 7 client computers and Windows Server 2012 R2, Windows Server 2012 or Windows Server 2008 R2 SP1.
			Metasys SCT (Member of Domain X)	
			Metasys ADS/ADX/ODS (Member of Domain X)	
			Metasys ADX Split Web/Application Server (Member of Domain X)	
Remote Procedure Call (RPC)	TCP	135 1025	*Metasys* System Client (Member of any Domain)	Used by IIS on the ADS/ADX/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/ODS/SCT and/or *Metasys* client is a member of an Active Directory service domain, this port and protocol are used for Active Directory service functionality.
			Metasys SCT (Member of Domain X)	
			Metasys ADS/ADX/ODS (Member of Domain X)	
			Metasys ADX Split Web/Application Server (Member of Domain X)	
N2 Protocol	UDP	4096	NAE55	For N2 tunneling over Ethernet (NAE5512 and NAE5513) on trunk 1.
		4097	NAE55	For N2 tunneling over Ethernet (NAE5512 and NAE5513) on trunk 2.
Microsoft Discovery Protocol [4]	TCP and UDP	9910	Engine	Used to get diagnostic information from devices on the same network.
			Metasys SCT	
			NCT and NAE/NIE Update Tool	
***Metasys* Private Message** [4]	UDP	9911	*Metasys* 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.
UberDebug Service	TCP	12000	*Metasys* System	Used by *Metasys* software for debugging and logging.

[1] Generally recorded by the Internet Assigned Numbers Authority (IANA).

[2] This port number is registered to Johnson Controls, Inc.

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

[4] 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.

Table 8: Wireless Ports and Protocols

Protocol	Uses	Wireless Protocol	Port[1] Number	*Metasys* Device	Description
Wireless Many-to-One Sensing[2]	UDP	802.15.4	4050[3]	WRS-RTN	Recommended UDP port number used for wireless supervisor integration.
Wireless ZigBee®	UDP	802.15.4	47808	TEC20-3C Coordinator	Recommended UDP port number used for wireless supervisor integration.
HTTP	TCP	802.11b/802.11g	80	Computer (Web Browser)	TCP Port Forwarding is supported on Port 80 only.

[1] Generally recorded by the IANA.
[2] Proprietary protocol.
[3] If this port is in use, it **can** be reconfigured to another port.

Connectivity and Protocol Diagrams

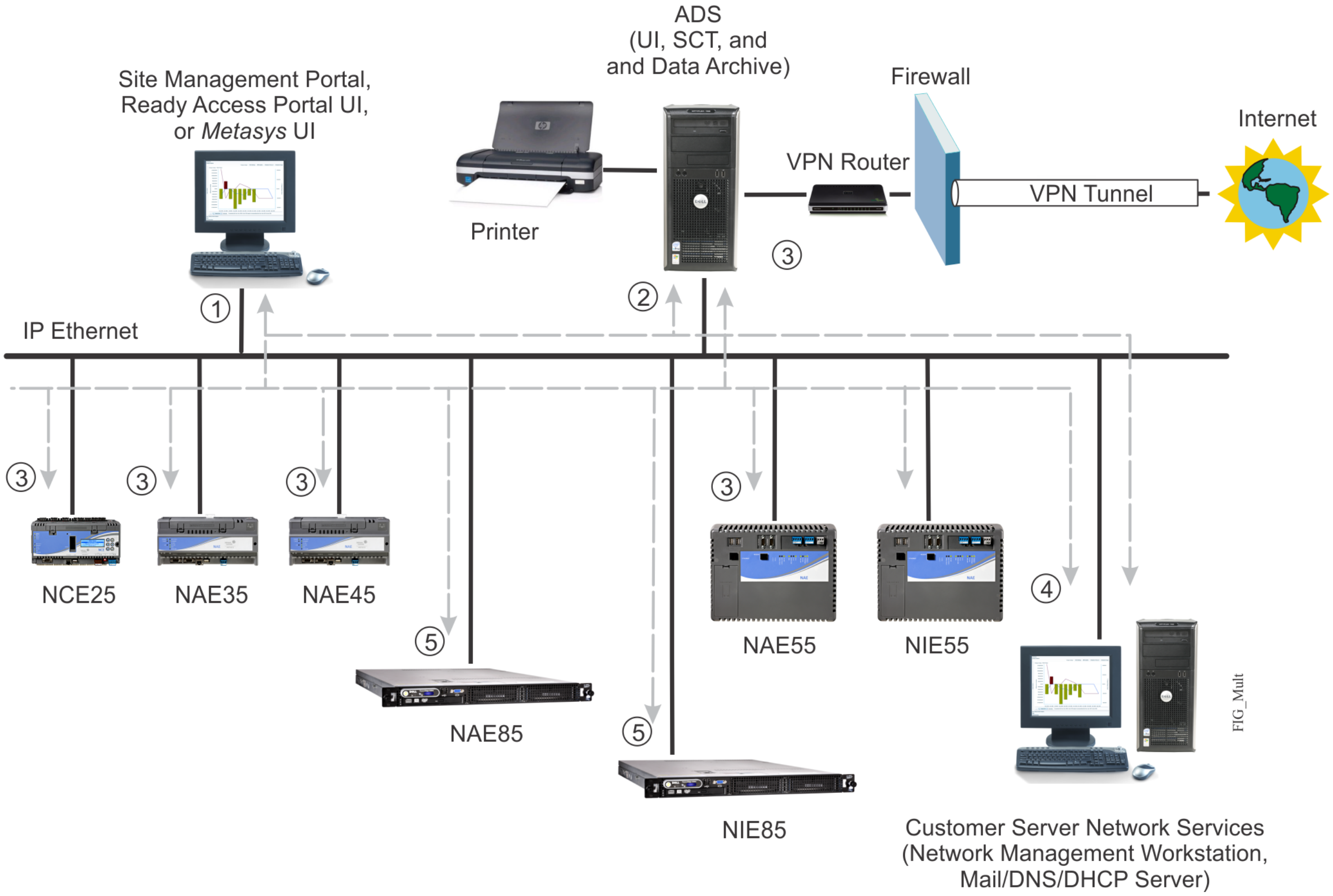
Figure 13 through *Figure 19* are example diagrams of the various types of connectivity and protocols for the *Metasys* system. Not all protocols are used in all *Metasys* system configurations.

The configuration and network topology of the specific *Metasys* system installation must be considered when opening firewall ports for communication. For example, considering *Figure 13* and *Table 7*, if the ADS is not acting as a time server, then the SNTP protocol between 3 and 2 is not used. Similarly, if *Metasys* system alarms and events are not being monitored by IT tools, then the SNMP Trap protocol between 2 and 4, and 3 and 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.

Figure 13 is an example of the connectivity and protocols for a *Metasys* system using multiple engines and an ADS.

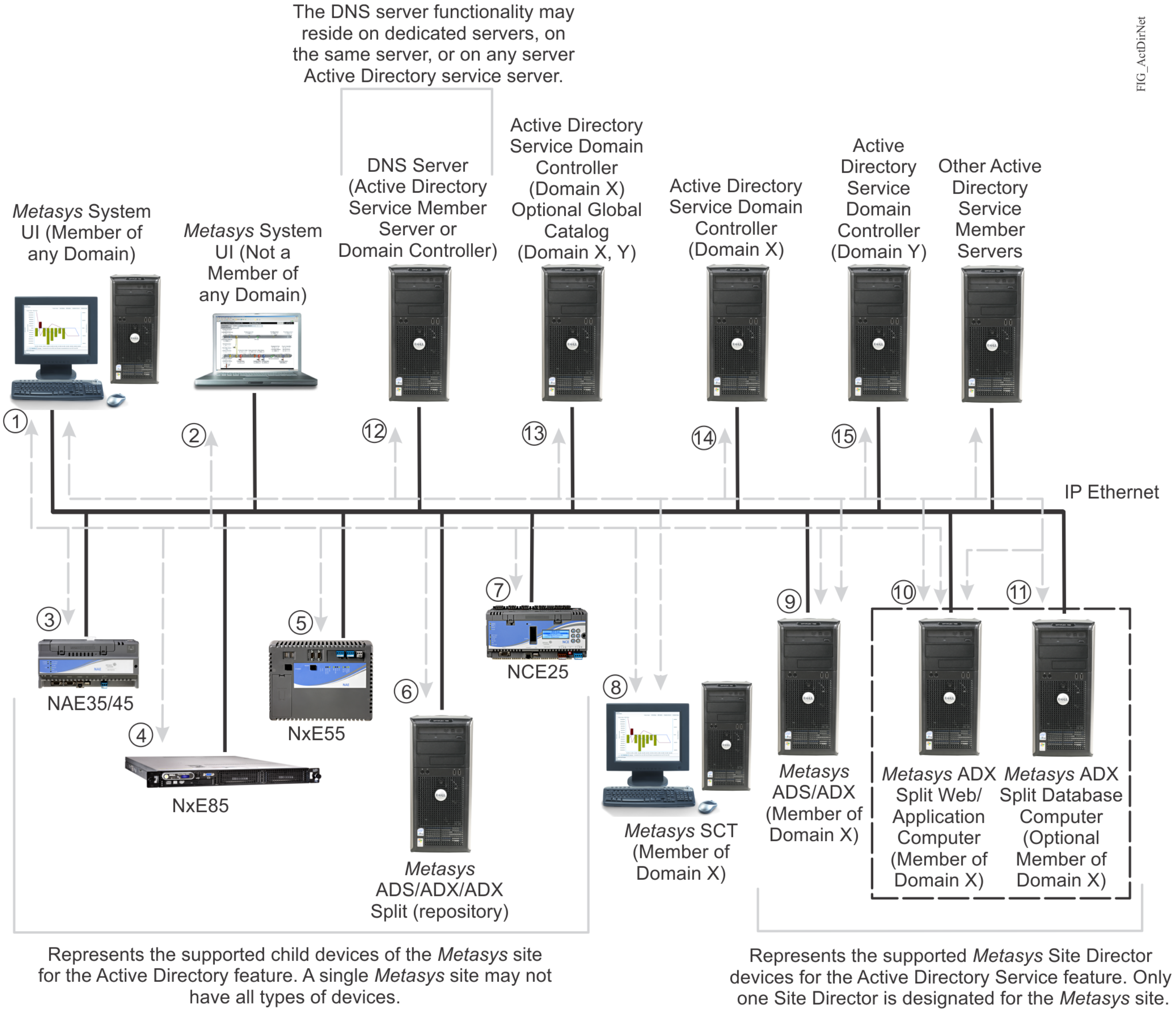
Figure 13: *Metasys* System with Multiple Engines and an ADS



Note: *Figure 13* does not show the interaction between the NCM and NIE using the N1 protocol. See *Figure 16*.

Figure 14 is an example of the connectivity and additional protocols used in a *Metasys* system that uses Active Directory service. *Table 9* describes the protocols used in *Figure 14*. Furthermore, *Figure 13* and *Table 7* describe the base protocols used by the *Metasys* system.

Figure 14: *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.
FIG_ActDirNet
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
NAE35/45
4
NxE85
5
NxE55
6
Metasys ADS/ADX/ADX Split (repository)
7
NCE25
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.

Note: *Figure 14* does not show the interaction between the NCM and NIE using the N1 protocol. See *Figure 16*.

Table 9: *Metasys* System with Active Directory Service

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

Table 9: *Metasys* System with Active Directory Service

Interaction between Callouts		Protocol	Communication Direction
2	**8, 9, 10**	No new protocols. See *Figure 13* and *Table 7*.[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 *Figure 14* is equivalent to web browser in *Figure 13*.

[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.

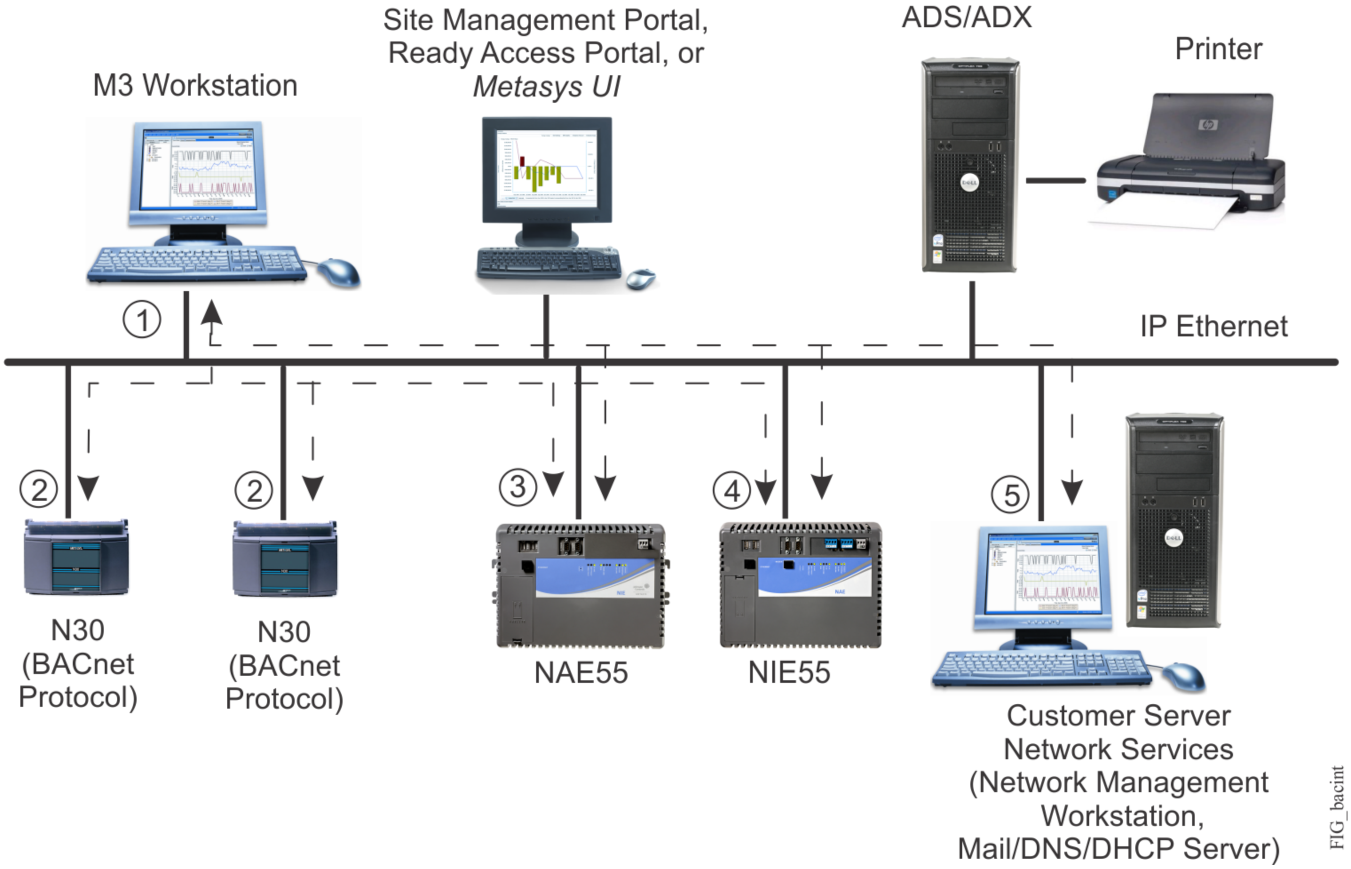
[6] The Kerberos protocol is used between a *Metasys* Site Director and/or SCT and the Active Directory service domain controller when the Site Director is authenticating against the Active Directory service domain. For domain authentication, any domain controller within the domain may respond.

[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/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/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.

Figure 15 is an example of the connectivity and protocols for a *Metasys* system using the M3 Workstation and N30 controllers. See *Figure 13* with *Table 7*, and *Figure 14* with *Table 9*, for the full set of protocols used by the engine, ADS/ADX, and Site Management Portal UI.

Figure 15: *Metasys* System with N30 Controllers Using BACnet Protocol



See *Table 10* for details on the callout numbers in *Figure 15*.

Table 10: *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[1]
2	**3**	BACnet[1]	Bidirectional[2]
3	**4**	BACnet[1]	Bidirectional[2]
2	**2**	BACnet	Bidirectional
2	**5**	DHCP	Unidirectional

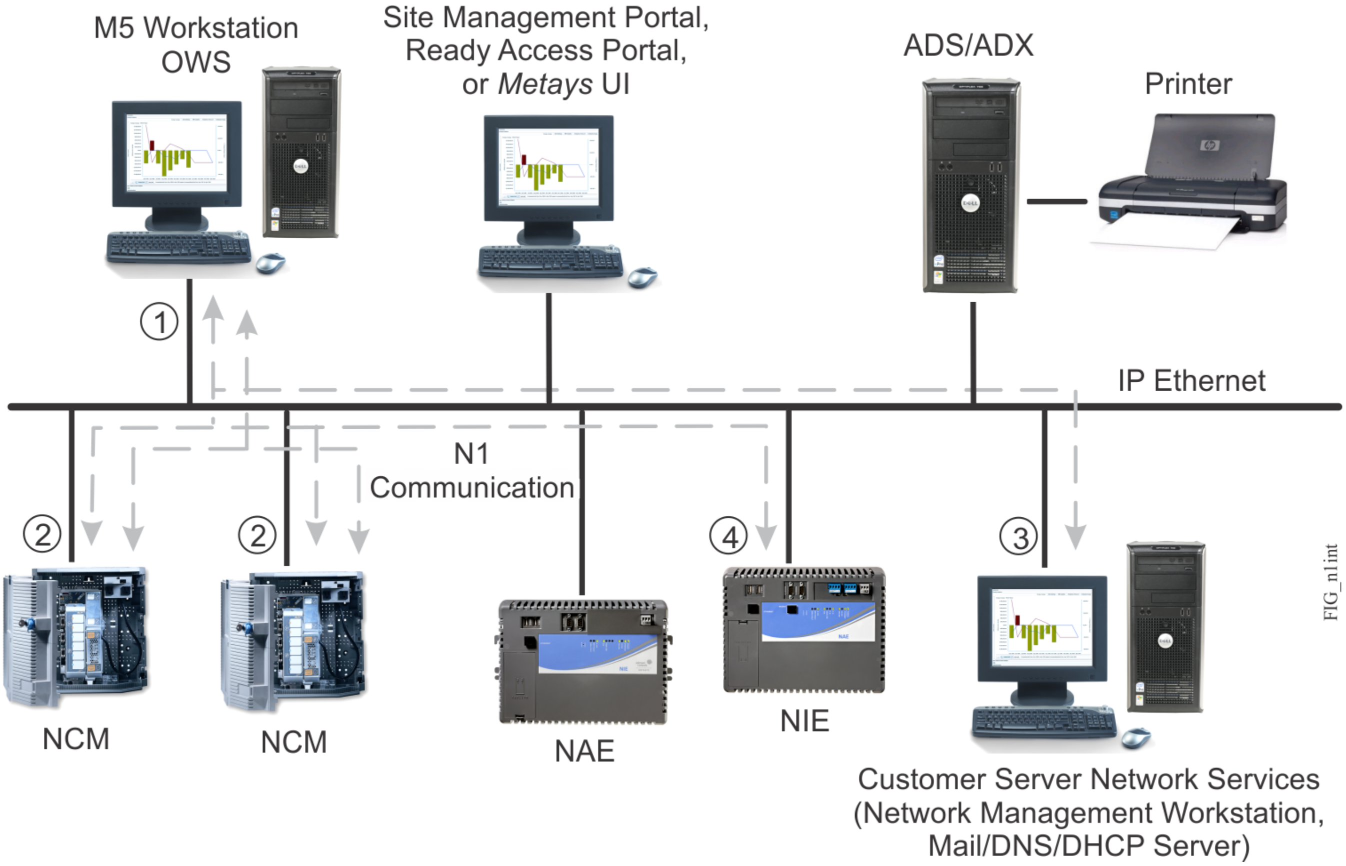
[1] When using BACnet protocol with N30s, you must specify UDP Port 47808 as being used. For multiple BACnet networks, use a different port number for each network.

[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).

Figure 16 is an example of the connectivity and protocols used in a *Metasys* system using the operator workstation (OWS) or M5 Workstation and NCMs. See *Figure 13* with *Table 7*, and *Figure 14* with *Table 9*, for the full set of protocols used by the engine, ADS/ADX, and Site Management Portal UI.

Figure 16: *Metasys* System with NCMs



See *Table 11* for information on the number callouts in *Figure 16*.

Table 11: *Metasys* System with NCMs

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

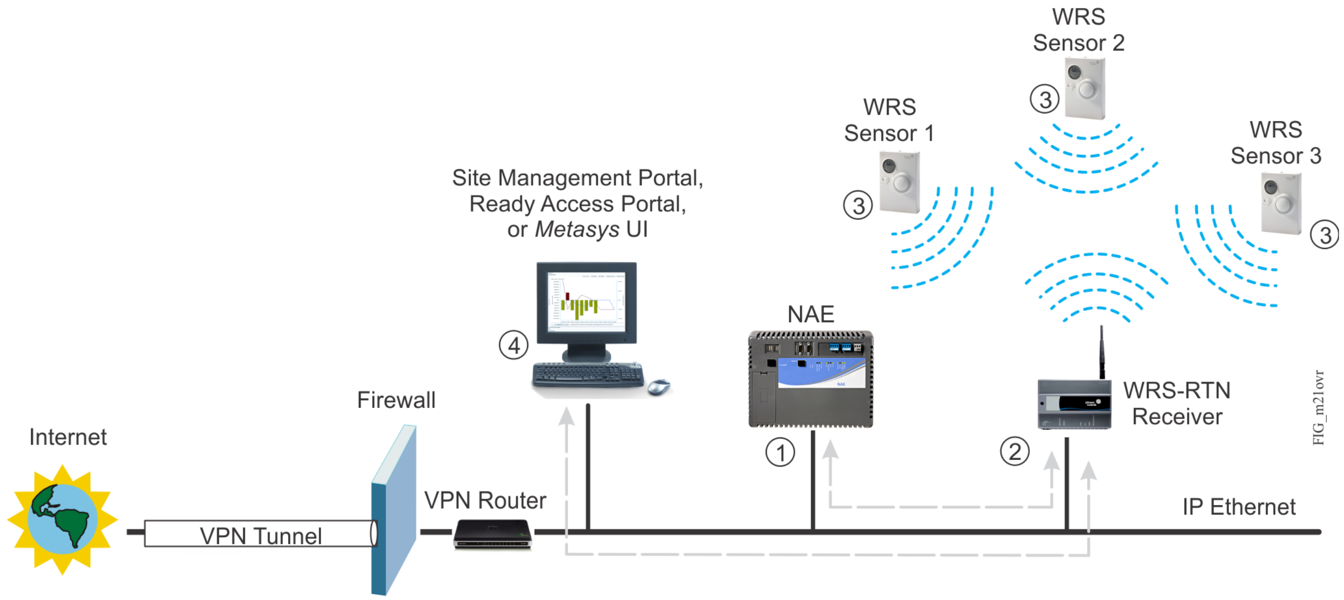
[2] In Bidirectional communications, both devices initiate requests.

[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.

Figure 17 is an example of the connectivity and protocols used in a *Metasys* network using the Many-to-One Wireless Room Temperature Sensing Application.

Figure 17: *Metasys* System with Many-to-One Wireless Room Temperature Sensing Application



See *Table 12* for information on the number callouts in *Figure 17*.

Table 12: *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[1]

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, Science, Medical (ISM) band and use multi-frequency direct sequence spread spectrum (DSSS) technology. The receiver meets the Institute of Electrical and Electronic Engineers, Inc. (IEEE) 802.15.4 standard for low power, low duty-cycle wireless transmitting systems.

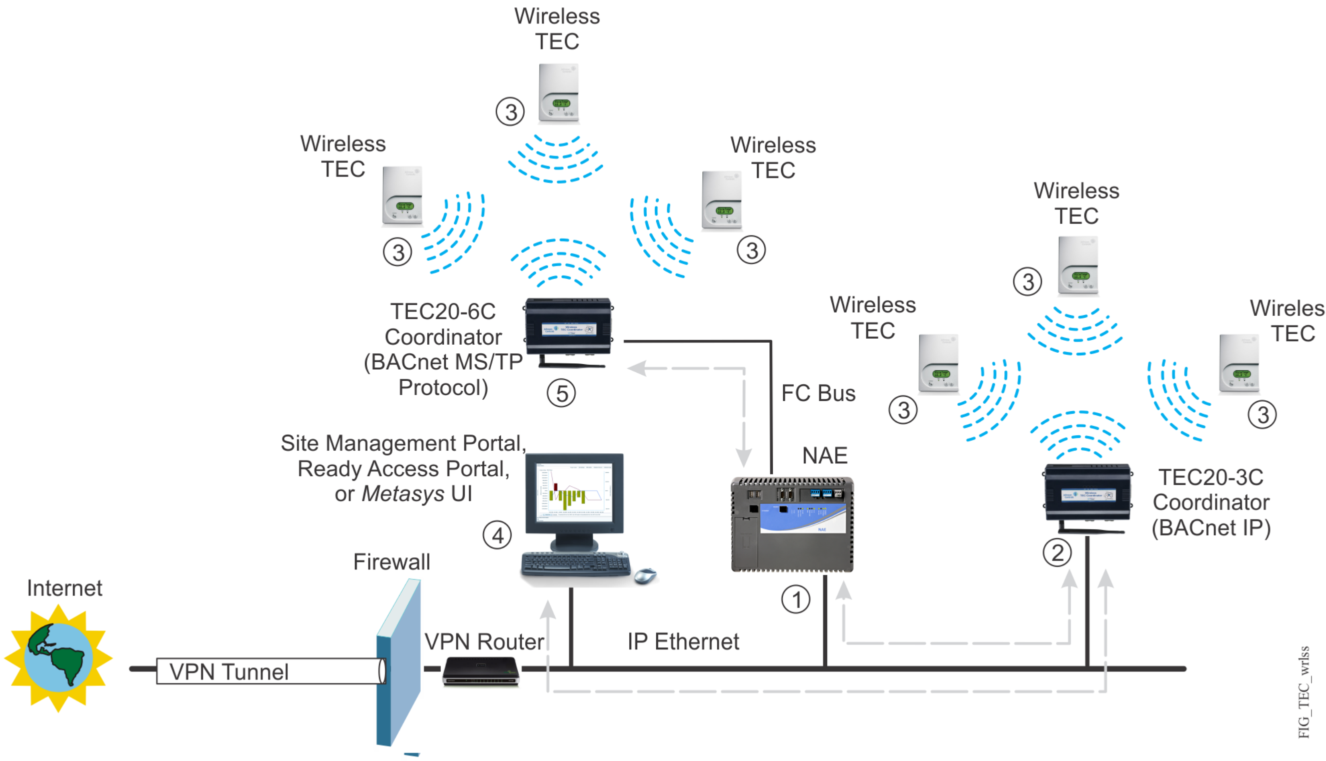
The 802.15.4 standard radio is used for employing control networks within a building. This technology uses 16 different channels, allowing 802.15.4 devices, such as the WRS Series systems, to coexist with 802.11 devices.

The Many-to-One system use 2 milliseconds 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.

Figure 18 is an example of a *Metasys* network using the TEC Series Wireless Thermostat Controller system.

Figure 18: *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 Multidrop Serial Bus/Token Passing [MS/TP]), but cannot use both BACnet IP and BACnet MS/TP versions.

Table 13: *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[1]
2	**3**	ZigBee Wireless Network (802.15.4)	Bidirectional (2.4 GHz Channelized, 2.4 GHz DSSS Wireless Protocol)
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).

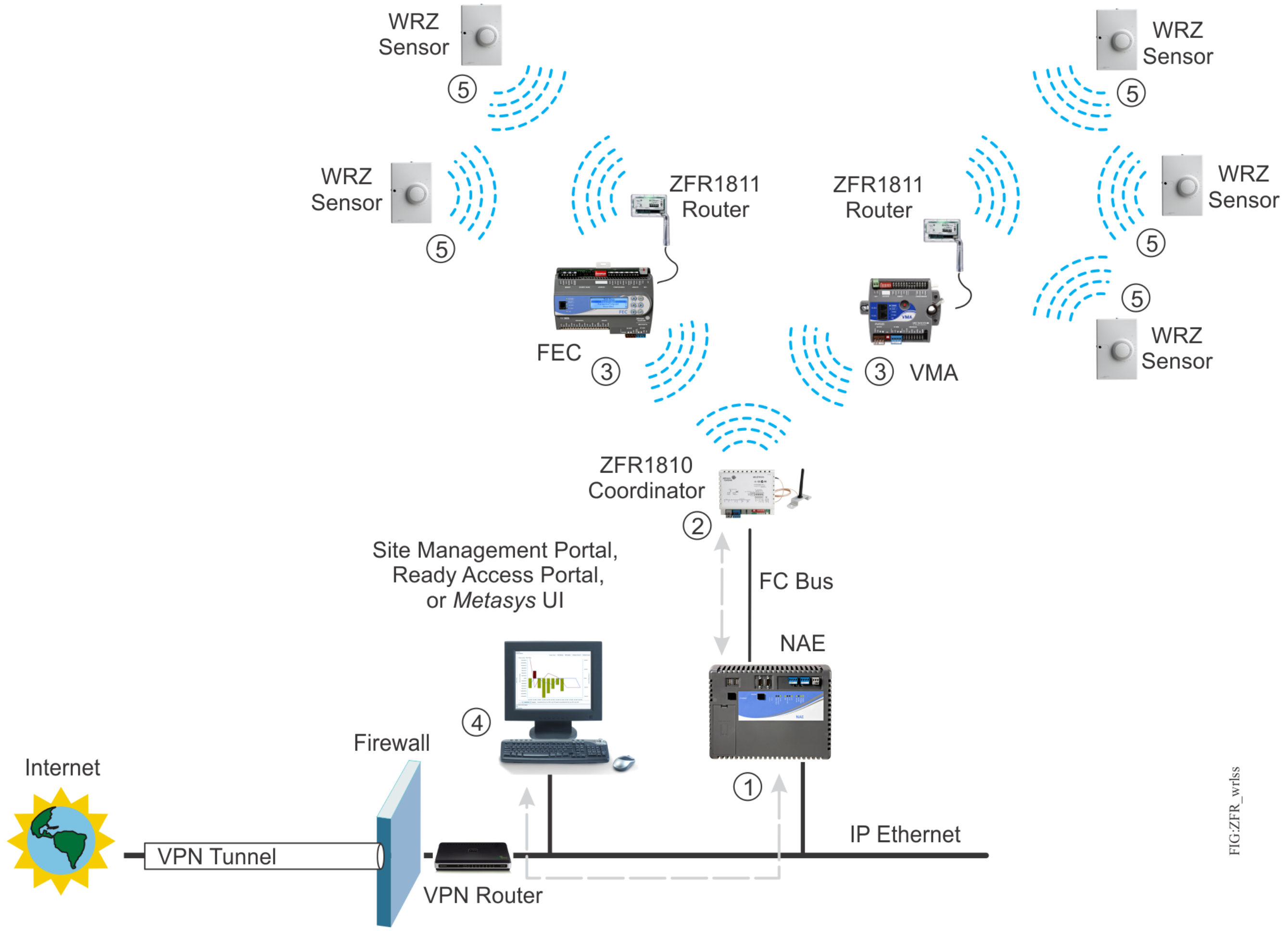
The TEC Wireless Thermostat Controller System provides a wireless interface between an NAE25/NAE35/NAE45/NAE55/NCE and the TEC Wireless Thermostat Controllers, allowing the exchange of BACnet IP (TEC20-3C) or BACnet MS/TP (TEC20-6C) messages for the purpose of wireless monitoring and temperature control 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)*.

Figure 19 is an example of a *Metasys* network using the ZFR1800 Series Wireless Field Bus system.

Figure 19: *Metasys* Network with ZFR1800 Series Wireless Field Bus System



See *Table 14* for details on the number callouts in *Figure 19*.

Table 14: *Metasys* Network with ZFR1800 Series Wireless System

Interaction between Callouts		Protocol	Communication Direction
1	**4**	HTTP	Unidirectional[1]
1	**2**	BACnet MS/TP	Bidirectional

Table 14: *Metasys* Network with ZFR1800 Series Wireless System

Interaction between Callouts		Protocol	Communication Direction
2	**3**	ZigBee Wireless Network (802.15.4)	Bidirectional (2.4 GHz Channelized, 2.4 GHz DSSS Wireless Protocol)
3	**5**	ZigBee Wireless Network (802.15.4)	Bidirectional (2.4 GHz Channelized, 2.4 GHz DSSS Wireless Protocol)

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

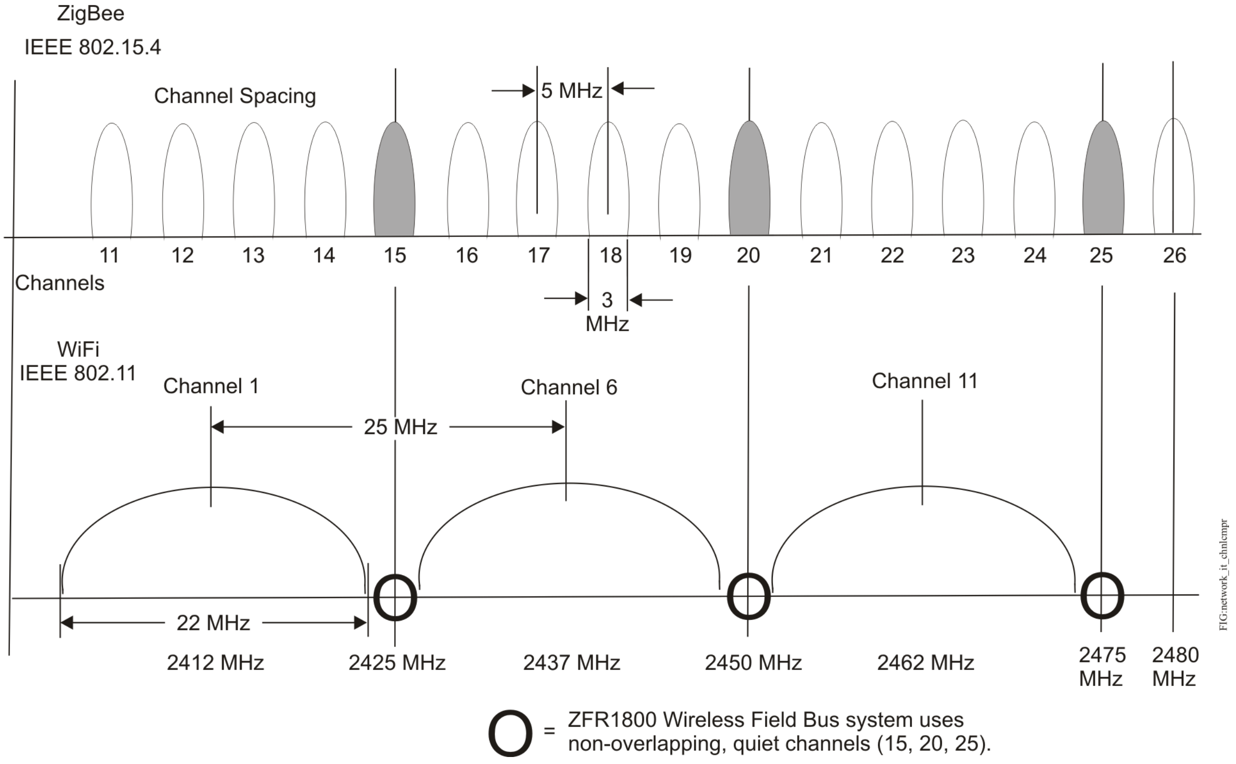
The ZFR1800 Series Wireless Field Bus System provides a wireless platform for *Metasys* field controllers using Johnson Controls *Metasys* BACnet protocol. The system consists of at least one ZFR1810 Wireless Field Bus Coordinator, connected to an NAE25/NAE35/NAE45/NAE55 or NCE. It also has one or more ZFR1811 Wireless Field Bus Routers, each connected to any *Metasys* BACnet Field Equipment Controller (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 20* 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 20: 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, Multidrop Serial Bus/Token Passing (MS/TP), 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)

Engines (excluding the 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 ADS/ADX/ODS and 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.

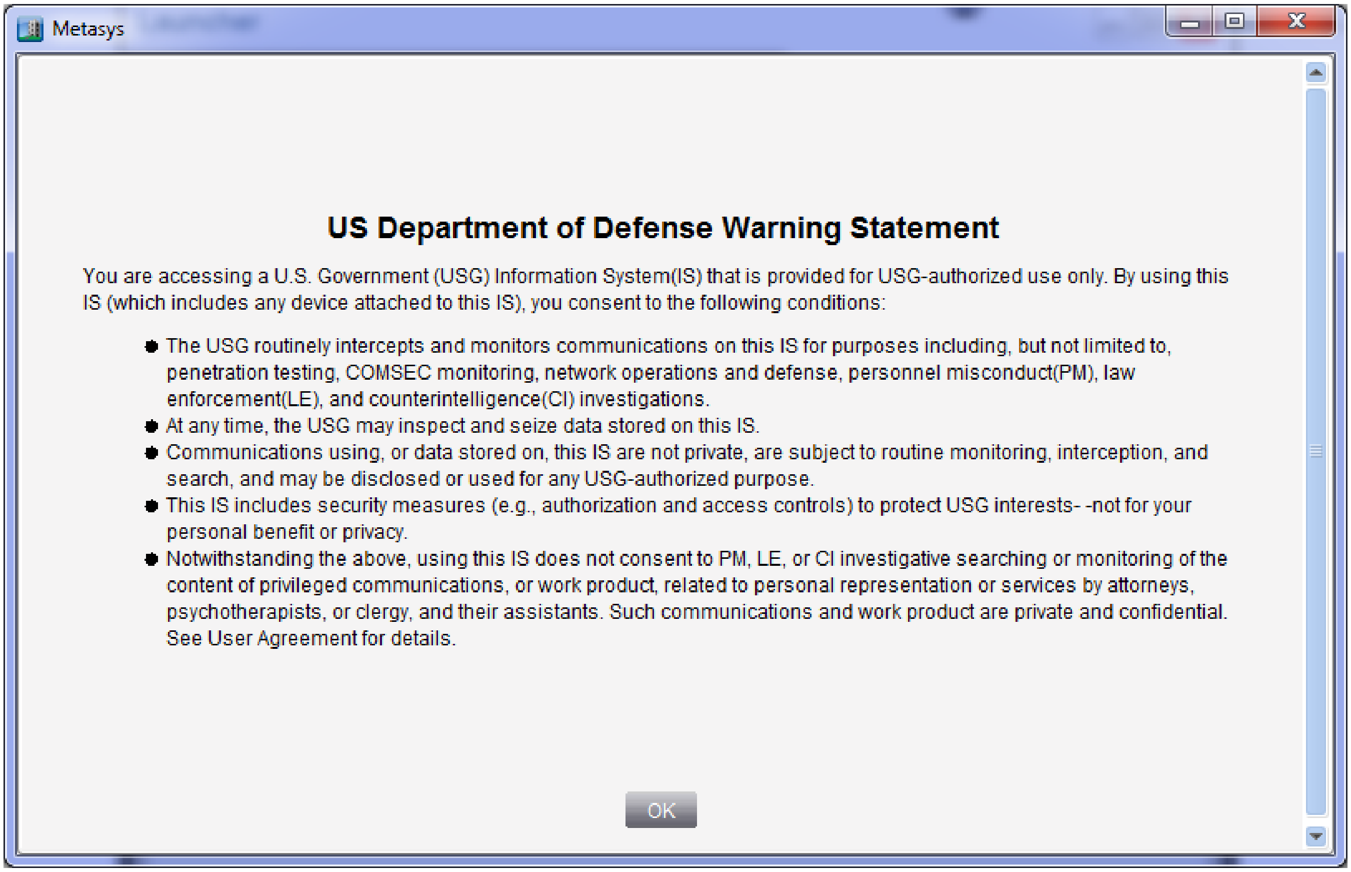
Metasys System Security Considerations

Metasys Access Security

Department of Defense Banner

If the custom United States Department of Defense (DoD) banner is enabled on the Site object for the ADS/ADX/ODS and network engines, a warning statement appears each time you access the *Metasys* Site Management Portal UI. The statement contains information important to *Metasys* users who access the building automation system at a Department of Defense facility. You must click **OK** to indicate that you consent to the stated conditions in order to reach the login screen. If your network uses the Active Directory service with Single Sign-On capability, the DoD banner appears, but the *Metasys* login screen is bypassed, and the Site Management Portal appears.

Figure 21: United States DoD Warning Statement



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.

The DoD banner remains on the screen until either you click OK or you manually close the banner window. The banner does not close on its own.

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 DoD banner screen returns. The banner also reappears after you log out of the *Metasys* system or the system logs you out because of user inactivity.

Note: The DoD banner does not appear before you log in to the *Metasys* Advanced Reporting System, Ready Access Portal user interface, supervisory engine, SCT UI, *Metasys* UI, or LONWORKS® Control Server (LCS85).

Note: The only method for removing the DoD Banner from the login process is to disable the United States Department of Defense (DoD) Banner on the Site object. The DOD banner option is stored in the device archive. If you download the ADX from an archive that has been uploaded with the banner option enabled, the banner appears.

Users

The *Metasys* system has three types of users: local users, Active Directory service users, and RADIUS 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. A RADIUS user is created and stored in the RADIUS server and is added as a *Metasys* system user with the *Metasys* Security Administrator tool. This user is authenticated against the RADIUS server.

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 (ADS/ADX/ODS 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 BasicSysAgent 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 BasicSysAgent account retains a subset of administrative rights, in that Basic Access administrators can administer only user accounts that have been assigned the **Basic Access** access type.

> **Important:** The first time you log in with the MetasysSysAgent account using the new default password, or the BasicSysAgent 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 ADS/ADX/ODS.

For information on hardware-based network engines operating system security, see *Security on Non-Server Based 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 that have the English-American (en_US) language locale selected. For details on complex passwords, refer to the *Security Administrator System Technical Bulletin (LIT-1201528)*.

Password rules are enforced for English (en_US) users only. The password rules are as follows:

- The password must include a minimum of 8 characters and a maximum of 50 characters.
- The password cannot include spaces or include a word or phrase that is in the Blocked Words list.
- The password and the user name 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

Password expiration is set in the SMP. By default, passwords expire every 60 days.

Note: Active Directory user account and RADIUS user account complex passwords are handled by the domain controller and not by the *Metasys* system.

Note: You cannot avoid using complex passwords if your user account language is set to English-American (en_us).

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**).

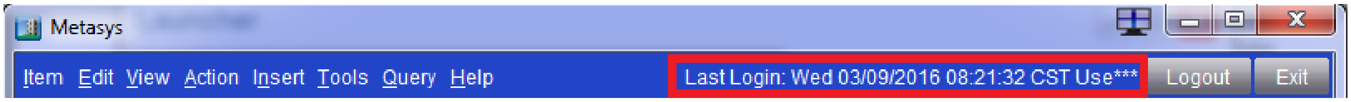
Audits are written to a proprietary data store of the *Metasys* system, which is a SQL Server database on computer/server platforms (ADS/ADX/ODS, NxE85, and LCS85) and an XML-based file on the other engine platforms (NAE35/NAE45/NAE55/NIE55/NIE59/NCE25). Audits may be viewed using the Audit Trail feature of the Site Management Portal UI.

Last Login

The main screen of the SMP, SCT, or ODS user interface indicates the last time and date that the user successfully logged in. If the user has never logged in, **Never** appears in the **Last Login** field.

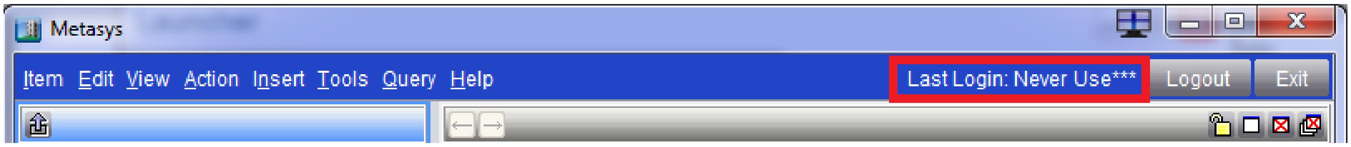
Important:	To preserve the current configuration for all *Metasys* system users, including last login time, always upload the device into the SCT before making changes and downloading a database. User configuration information is stored in the Security database. The Security database is restored during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

Figure 22: Last Login



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

Figure 23: Never Login



Last Login: Never Use***

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.

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

The *Metasys* Advanced Reporting System, *Metasys* UI, *Metasys* UI Offline, and the Ready Access Portal UI are the *Metasys* system offerings that support security certificates. We recommend that you implement SSL security for improved protection of user passwords when using the *Metasys* Advanced Reporting System (including when you use the reporting system on ADXs with MVE). SSL security is required for the Ready Access Portal UI. SSL or TLS certificates may be used with the *Metasys* UI and *Metasys* UI Offline.

For information on how to implement security certificates with the *Metasys* UI and the *Metasys* UI Offline, see *Appendix: Security Certificate Implementation*.

Implementing SSL Security for the *Metasys* Advanced Reporting System

To implement SSL security for the *Metasys* Advanced Reporting System:

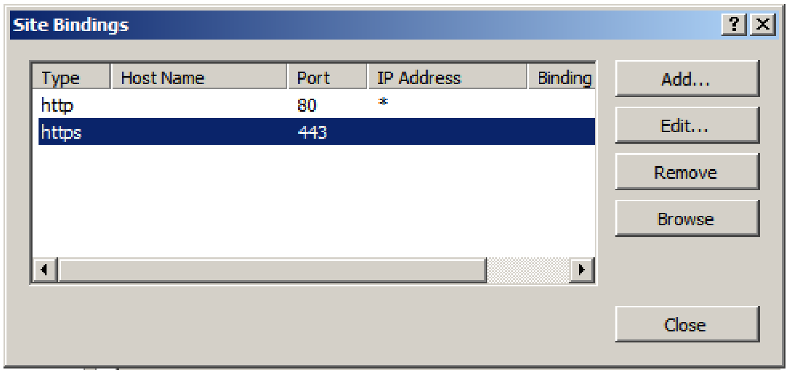
1. Generate a certificate request and install the certificate.
   For more information on these steps, see the following address:

   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:
      - In Windows Server 2012 R2, Windows Server 2012, or Windows Server 2008 R2 with SP1, 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.

Figure 24: Site Bindings

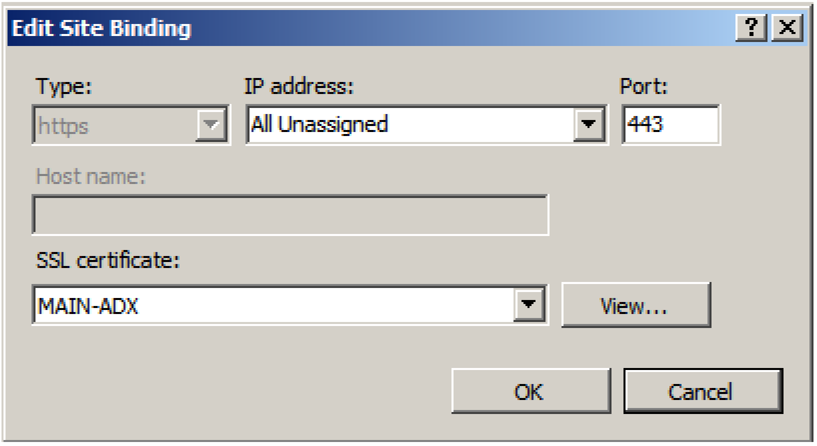


Site Bindings

Type	Host Name	Port	IP Address	Binding
http		80	*	
https		443		

d. Click **Edit**. Verify that the **SSL port** field contains 443 (*Figure 25*).
Note: Port 80 must be open on the ADX for communication from other system devices. Verify that the TCP port entry is 80.

Figure 25: SSL Port Field: 443



Edit Site Binding

Type: https

IP address: All Unassigned

Port: 443

Host name:

SSL certificate: MAIN-ADX

e. Click **OK**.

f. Close the Internet Information Services (IIS) Manager window.

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

h. Using Windows Explorer, browse to:
C:\Inetpub\wwwroot\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.

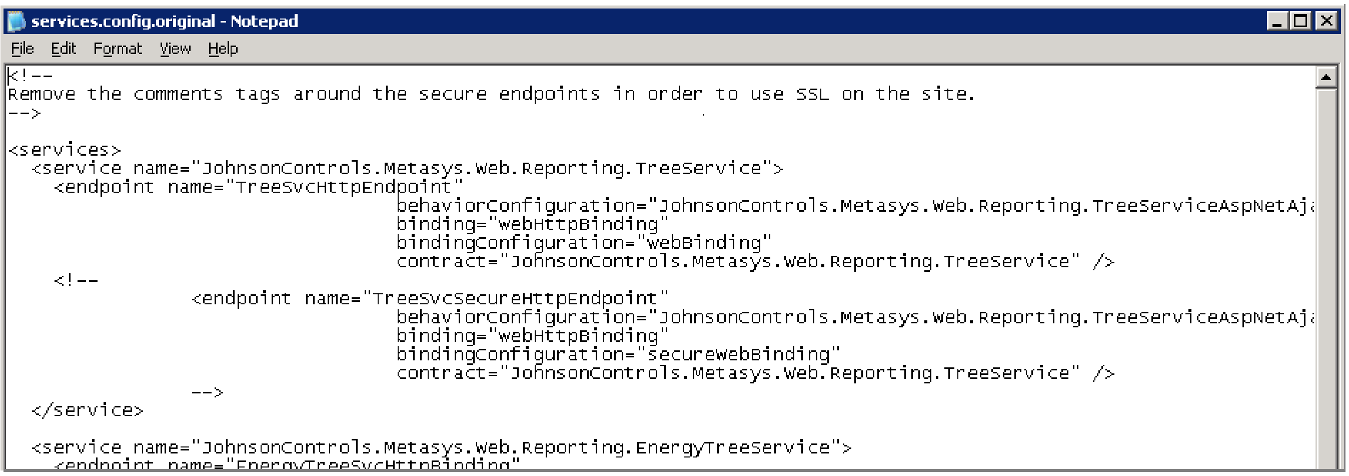
l. Using Windows Explorer, browse to:
C:\Inetpub\wwwroot\MetasysReports

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

n. Delete the comment tags from the file. Comment markers appear as `<!-- and -->` (*Figure 26*).

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

Figure 26: Comment Tags


services.config.original - Notepad
File Edit Format View Help

```
<!--
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**.

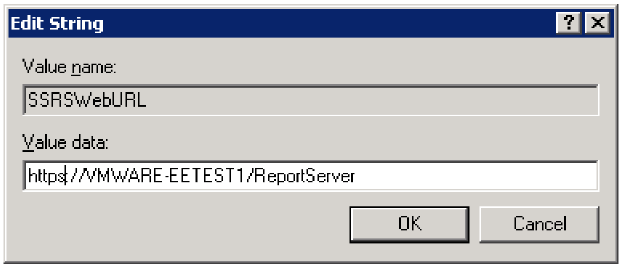
r. Click **OK**. The Registry Editor window appears.

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 27*).

Figure 27: Edit String Box



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.
   The UI should open correctly and the URL in the browser window should have the **https:** prefix.

Implementing SSL for Ready Access Portal UI

To implement SSL security for the Ready Access Portal UI, follow the steps during installation of the software. You can add SSL for the login only or for the entire Ready Access Portal UI. The options for SSL certificates include the following:

- Third-Party – Coordinate with the customer IT department before installing the Ready Access Portal software to configure IIS correctly.
- Self-Signed – Follow the installation process that allows you to generate a self-signed certificate.

Note: We do not recommend a self-signed certificate for networks exposed directly to the Internet (no firewall or VPN).

You also must have Port 80 (TCP) and Port 443 (SSL) open on the computer where the Ready Access Portal software is installed. To open Port 443 on the computer where you are going to install the Ready Access Portal:

1. In Control Pane, select **System and Security**, then **Administrative Tools**. On Administrative Tools, double-click **Internet Information Services (IIS) Manager**. The IIS Manager window appears.
2. In the tree in the left side of the screen, browse to and expand **Sites** or **Web Sites**.
3. On the right side of the screen, right-click Default Web Site and select **Properties**. The Default Web Site Properties box appears.
4. On the Web Site tab, verify that the **SSL port** field contains 443 (*Figure 25*).
   Note: Port 80 must be open on the ADX for communication from other system devices. Verify that the TCP port entry is 80.
5. Click **OK**.
6. Close the IIS Manager window.

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. MVE supports access by Active Directory service users of the *Metasys* system from the standard login screen. SSO login-free 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)*.

Network Message Security

Metasys software offers secured authentication challenges at login.

After login, the *Metasys* software authenticates each SOAP message at the receiving engine. Authentication is based on RC2 encrypted credentials, which may be a session token or user name and password pair. Within each encrypted SOAP message header, there is protection against message spoofing, message replay, and message tampering.

SQL Database Security

SQL Server databases are secured using SQL Server authentication.

SQL Server software accounts used by *Metasys* software can be end-user defined on the ADS/ADX 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.

Security on Non-Server Based Engines

The operating system of the hardware-based network engines 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 *Metasys* system user MetasysSysAgent.

Many of the operating system features not required by *Metasys* software have been removed from the 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 (ADS/ADX, 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 Instructions (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.

Software Time Bomb

Metasys software does not have a software time bomb to disable the system. For the *Metasys* system, a software time bomb disables the software and prevents login to the system if the software is not licensed after installation. The software time bomb only applies to the ODS and NxE85 software. For other *Metasys* software, the software does not disable and prevent you from logging in; however, it does remind you periodically if you do not license the product. Reminders appear as pop-up messages when you are using the Site Management Portal UI and as a special tab within the user interface that appears until you license the product.

Antivirus Software Considerations (ADS/ADX, NxE85, NIE89, and LCS85 Only)

Frequent virus scans of the ADS/ADX/ODS, 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 (ADS/ADX, 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 ADS/ADX, NxE85, NIE89, and LCS85 successfully with the following antivirus software programs:

- Symantec AntiVirus Corporate Edition 12.1.6 software or later (recommended for the NxE85 and LCS85)
- McAfee® VirusScan® Enterprise version 8.8 with Patch 5 (Patch 4 is **not** compatible).

For details, see *Appendix: Installing Antivirus Software*.

ADS/ADX/ODS Considerations

ADX-Specific Features

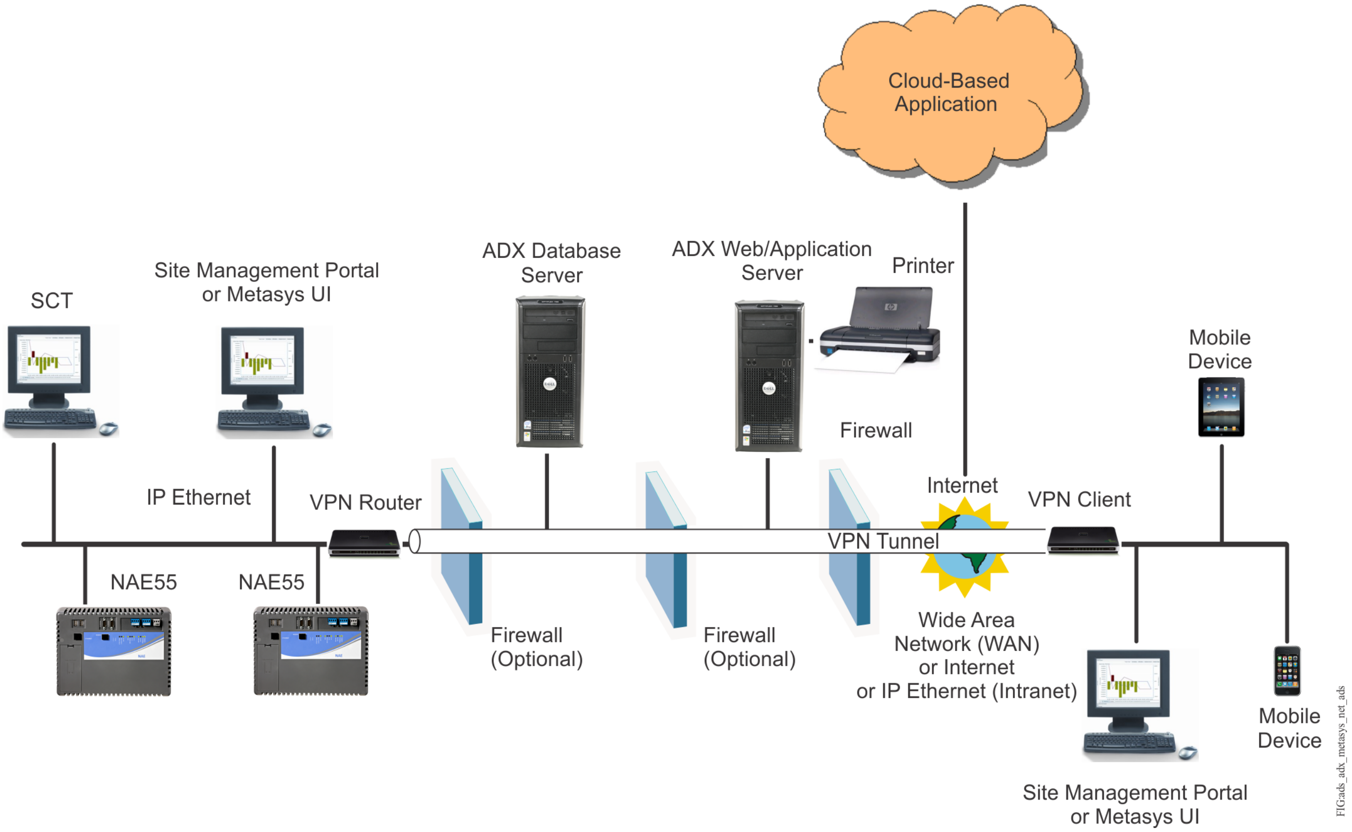
See the *Metasys for Validated Environments (MVE)* and *Metasys Advanced Reporting System UI* sections for information on these two features that are available only on ADXs with specific components installed.

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

Figure 28: *Metasys* Network with an ADX in Split Configuration


Cloud-Based Application
SCT
Site Management Portal or Metasys UI
ADX Database Server
ADX Web/Application Server
Printer
Mobile Device
Firewall
IP Ethernet
VPN Router
Internet
VPN Client
VPN Tunnel
NAE55
NAE55
Firewall (Optional)
Firewall (Optional)
Wide Area Network (WAN) or Internet or IP Ethernet (Intranet)
Mobile Device
Site Management Portal or Metasys UI
FIGads_adx_metasys_net_ads

ADSADX Log Folder

The **ADSADX Log** folder in the Windows Event Viewer on the ADS/ADX/ODS contains information related to specific ADS/ADX/ODS 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 ADS/ADX/ODS software has a failure initializing any subsystem during startup.
- The ADS/ADX/ODS software has a failure during runtime when it tries to write to the Microsoft SQL Server database.
- The ADS/ADX/ODS 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 ADS/ADX/ODS or SCT software, or an Active Directory service user could not be added as an ADS/ADX/ODS 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 ADS/ADX, 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.

Web Browsers

Important: We strongly advise that you do not browse to the *Metasys* UI, *Metasys* UI Offline, or any website from an ADS/ADX or ADS-Lite computer. Using web browsers to access web sites on the ADS/ADX or ADS-Lite could potentially expose your ADS/ADX or ADS-Lite 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 an ADX/ODS is installed, Windows Internet Explorer Advanced Security Configuration is enabled by default. You must add any website you want to navigate to from the ADS/ADX/ODS 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.

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 an ADS/ADX/ODS. 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 ADS/ADX/ODS.

Additionally, anti-spyware software may not allow the ADS/ADX/ODS 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)* or the *ODS Commissioning Guide (LIT-12011944)*.

Backup Considerations for the ADS/ADX/ODS

If a backup program changes attributes in certain ADS/ADX/ODS files, the ADS/ADX/ODS 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 ADS/ADX/ODS:

- C:\Inetpub\wwwroot\MetasysIII\GLOBAL.ASAX
- C:\Inetpub\wwwroot\MetasysIII\WEB.CONFIG
- C:\Inetpub\wwwroot\MetasysIII\BIN

- C:\<WINNT or Windows>\Microsoft.NET\Framework\v1.1.4332\CONFIG
- C:\<WINNT or 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:\Inetpub\wwwroot\MetasysReports\bin (*Metasys* Advanced Reporting System only)
- C:\Inetpub\wwwroot\MetasysReports\web.config (*Metasys* Advanced Reporting System only)

Supported Operating System and SQL Server Software 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 Instructions Wizard (LIT-12012162)*, *SCT Installation and Upgrade Instructions (LIT-12012067)*, or the *ODS Installation and Upgrade Instructions Wizard (LIT-12011945)*.

As new software and service packs become available, Johnson Controls tests them for use with *Metasys* software. We do not recommend installing software or a service pack on a computer running *Metasys* software unless it has been tested and qualified.

Internet Information Server (IIS) Anonymous Access Considerations (ADS/ADX/ODS 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 ADS/ADX/ODS, SCT, *Metasys* Advanced Reporting feature, and the NAE/NIE 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 ADS/ADX/ODS or SCT computer
- bypass traverse checking
- batch job login capability

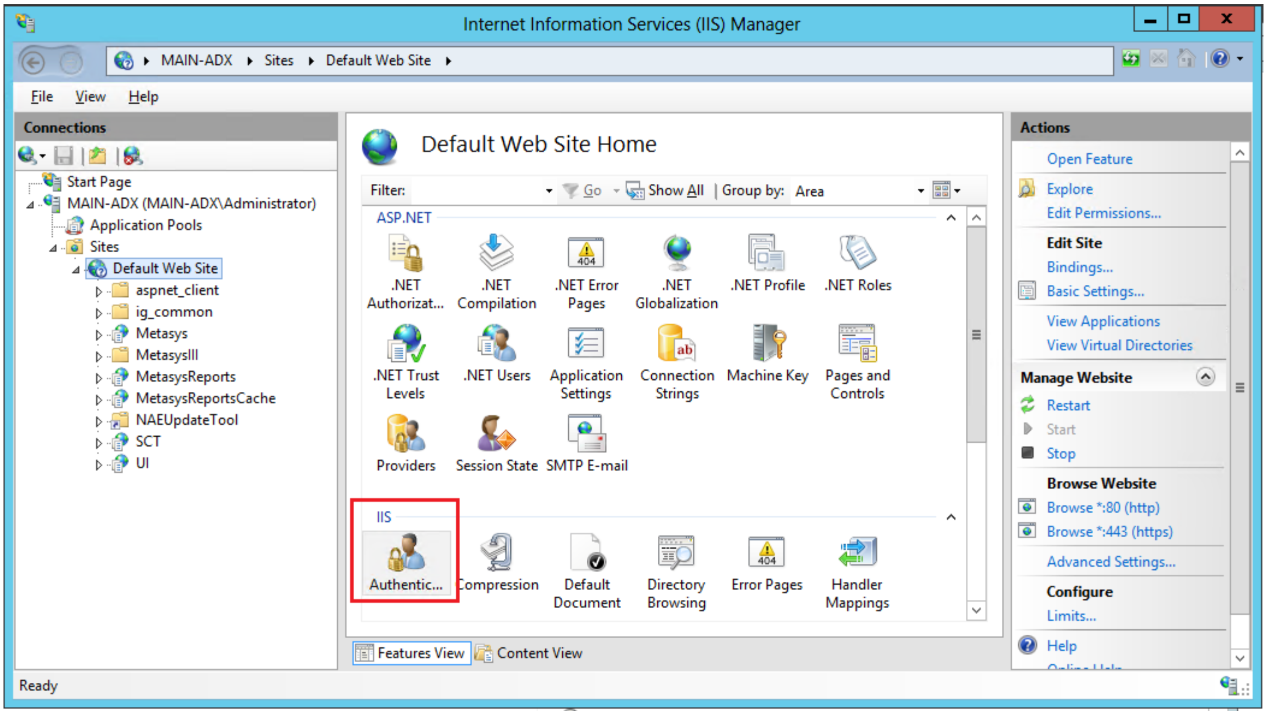
However, **do not** assign the privilege called **deny access to this computer from the network** to this same Windows user account or Windows user group.

Enabling and Disabling Anonymous Access on the Default Web Site

Follow these steps to enable and disable anonymous access when installing and running the ADS/ADX/ODS or SCT software.

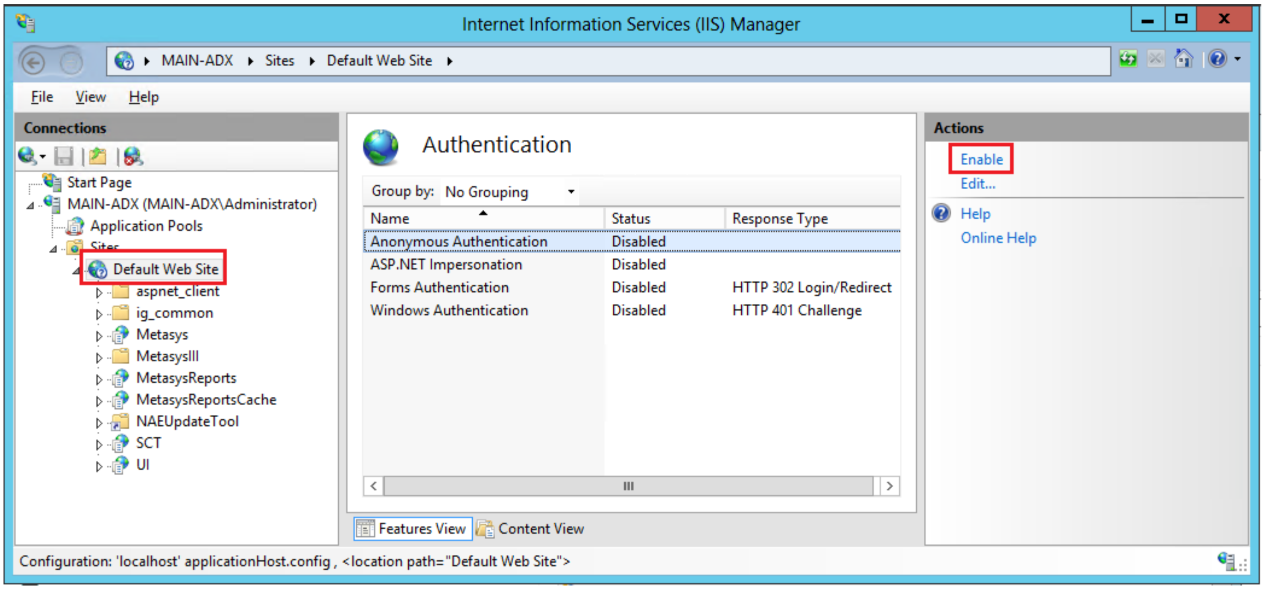
1. Open Control Panel and click System and Security > Administrative Tools. Double-click Internet Information Services (IIS) Manager. The Internet Information Services (IIS) Manager window appears.
2. Expand the left pane to expose the Default Web Site.

Figure 29: 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 30: Authentication Options for Default Web Site

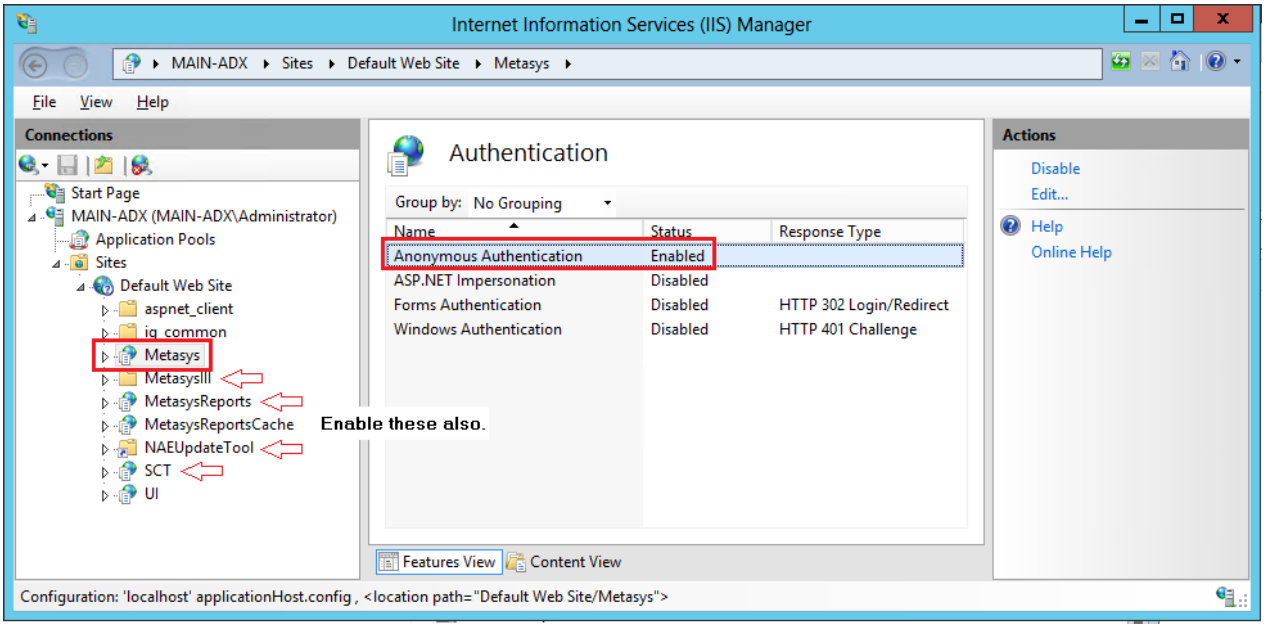


Name	Status	Response Type
Anonymous Authentication	Disabled	
ASP.NET Impersonation	Disabled	
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Disabled	HTTP 401 Challenge

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 ADS/ADX/ODS 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 31: Enabling Anonymous Access to *Metasys* Web Site



Enable these also.

Name	Status	Response Type
Anonymous Authentication	Enabled	
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/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 ADS/ADX/ODS is incompatible with server clusters. For a split 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 ADS/ADX/ODS databases and SQL Server user accounts that are used during ADS/ADX/ODS runtime, the ADS/ADX/ODS 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 ADS/ADX/ODS 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 ADS/ADX/ODS software uses the SQL Server user accounts that were created by the ADS/ADX/ODS installation program. For information about managing the SQL Server user accounts used by the ADS/ADX/ODS (account rename and password changes), contact Johnson Controls technical support.

The default location for *Metasys* system databases is determined by database default locations setting in SQL Server.

The historical databases for the ADS/ADX/ODS are JCIEvents, JCIAuditTrails, JCIHistorianDB, JCIItemAnnotation, and JCIReportingDB. Non-historical databases for the ADS/ADX include MetasysIII, XMS, MetasysTranslationDictionary, and MetasysReporting. The *Metasys* UI create the JCIReportingDB and the SpacesAuthorization database. CCT creates the CCT_DB and FDB_Control databases. The NavTreeCache, MetasysSCT databases, 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 Instructions Wizard (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 ADSs/ADX/ODS 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 15: 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

NAE35s/NAE45s/NAE55s/NIE55s/NCE25s store a limited amount of alarm, trend, and audit trail information. After engines collect data, you can forward the data to an ADS/ADX/ODS and save the data on the hard disk for long-term storage.

Historical data on engines and ADSs/ADXs/ODSs 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 as many as six different file formats (such as Microsoft Excel) for easier viewing.

Data Backup/Restore

For information on SQL Server software backups, see the *Microsoft SQL Database Considerations* section.

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, Inc. 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 SQL Server 2014, SQL Server 2012 SP3, or SQL Server 2008 R2 SP3 software 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. Currently, Active Directory service users cannot access the *Metasys* Advanced Reporting 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 an 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, a new application called the Launcher was developed to allow you to manage a list of all engines, ADS, ADX, ODS, SCT, LCS85, NIE, *Metasys* UI, *Metasys* UI Offline, Ready Access Portal, *Metasys* Advanced Reporting, or any generic website links. The Launcher is a simple user interface that launches the user interface for any *Metasys* release, but only manages the local Java files for Release 6.x systems.

Note: *Metasys®* System UL 864 9th Edition UUKL/ ORD-C100-13 UUKLC Smoke Control System network engines at Release 5.2 or earlier do not support the Launcher.

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

The Windows Internet Explorer web browser version 11 is required for downloading the Launcher. Other web browsers may work but are not fully tested.

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.

The Launcher is a software application that is installed on each client computer that logs in to the *Metasys* ADS/ADX/ODS 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. Starting at Release 6.0, you use the Launcher, not a web browser, to reach the log in screen of the NAE. For details, refer to *Launcher Help (LIT-12011742)*.

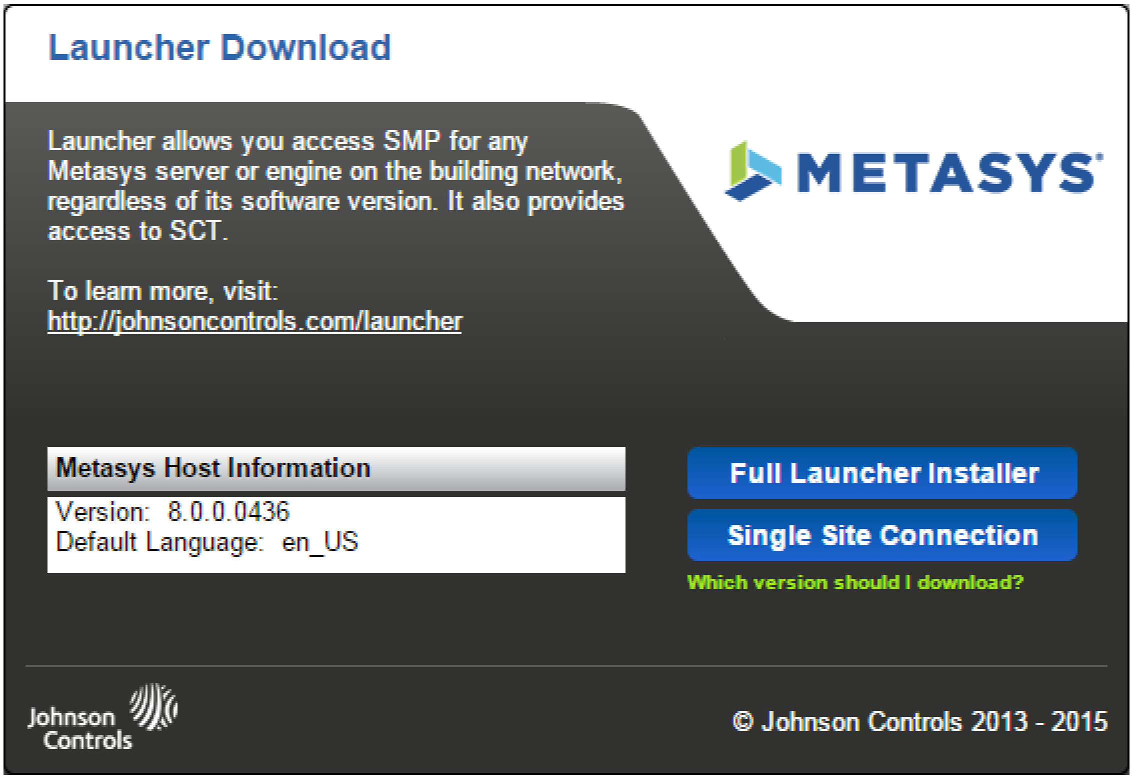
Note: We strongly advise that you do not browse to the *Metasys* Site Management Portal UI from a computer running a server class operating system. By default, Windows Internet Explorer Enhanced Security Configuration is enabled on server class operating systems, and may block the Launcher download page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

Important: We strongly advise that you do not browse to the *Metasys* UI, *Metasys* UI Offline, or any website from an ADS/ADX or ADS-Lite computer. Using web browsers to access web sites on the ADS/ADX or ADS-Lite could potentially expose your ADS/ADX or ADS-Lite 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.

Launcher Download Options and Proxy Settings

When the SMP is downloaded for the first time at Release 8.0, the Windows Launcher Download screen (*Figure 32*) appears.

Figure 32: Windows Launcher Download



Launcher Download

Launcher allows you access 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

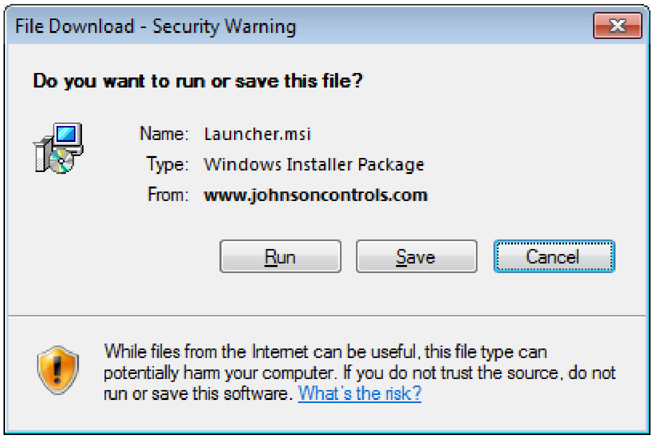
Version: 8.0.0.0436
Default Language: en_US

The Launcher Download screen provides two choices: Full Launcher Installer and Single Site Connection.

Full Launcher Installer Download

If you click **Full Launcher Installer**, a security warning screen appears (*Figure 33*). This screen gives you the option to Run, Save, or Cancel.

Figure 33: File Download - Security Warning Screen



File Download - Security Warning

Do you want to run or save this file?

Name: Launcher.msi

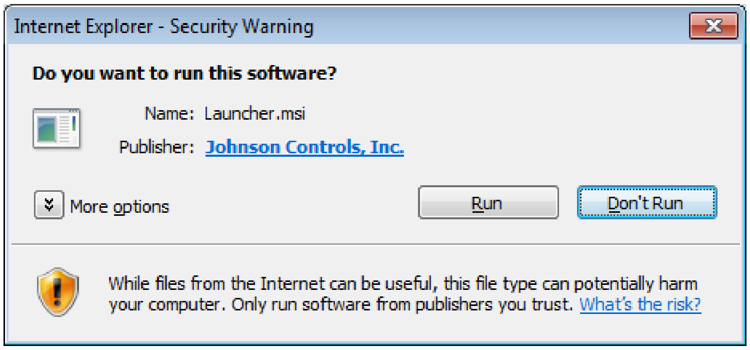
Type: Windows Installer Package

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 34*).

Figure 34: Internet Explorer - Security Warning Screen



Internet Explorer - Security Warning

Do you want to run this software?

Name: Launcher.msi

Publisher: Johnson Controls, Inc.

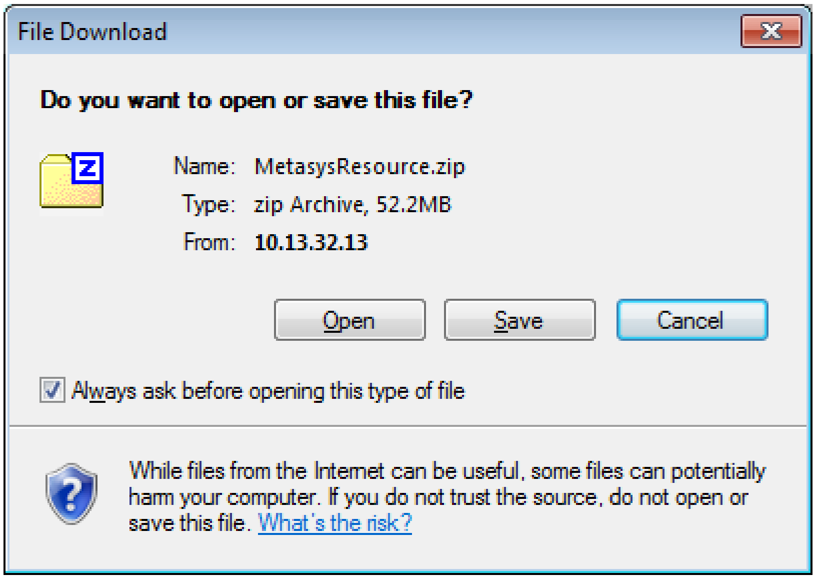
While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

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

Single Site Connection Download

If you click **Single Site Connection**, a file download screen appears (*Figure 35*).

Figure 35: File Download - Single Site Connection



File Download

Do you want to open or save this file?

Name: MetasysResource.zip

Type: zip Archive, 52.2MB

From: 10.13.32.13

☑ Always ask before opening this type of file

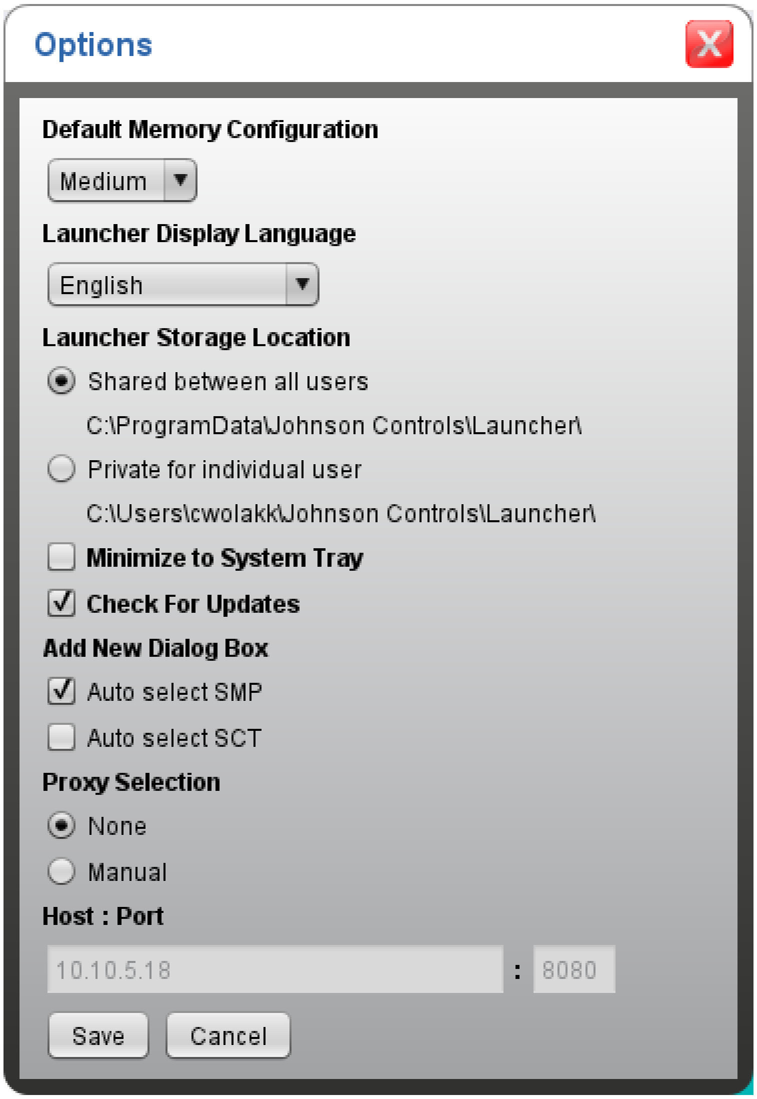
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

The File Download screen gives you the option to Open, Save, or Cancel. Click **Save** and save the MetasysResource.zip file to a location on your computer. Refer to the *Launcher Installation Instructions (LIT-12011783)* for details on how to unzip the files and run the Launcher.

Launcher Proxy Settings

The full version of the Launcher tool lets you update certain options, including proxy settings (*Figure 36*).

Figure 36: 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\cwolakk\Johnson Controls\Launcher\

□ Minimize to System Tray

☑ Check For Updates

Add New Dialog Box

☑ Auto select SMP

□ Auto select SCT

Proxy Selection

● None

○ Manual

Host : Port

10.10.5.18 : 8080

You need to configure the proxy host if the building network uses a proxy server for connection to the Internet:

Host: Port IP address of the proxy server.

Pop-up Ad 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.

Sleep Power Option on Windows 8.1 and Windows 7 Computers

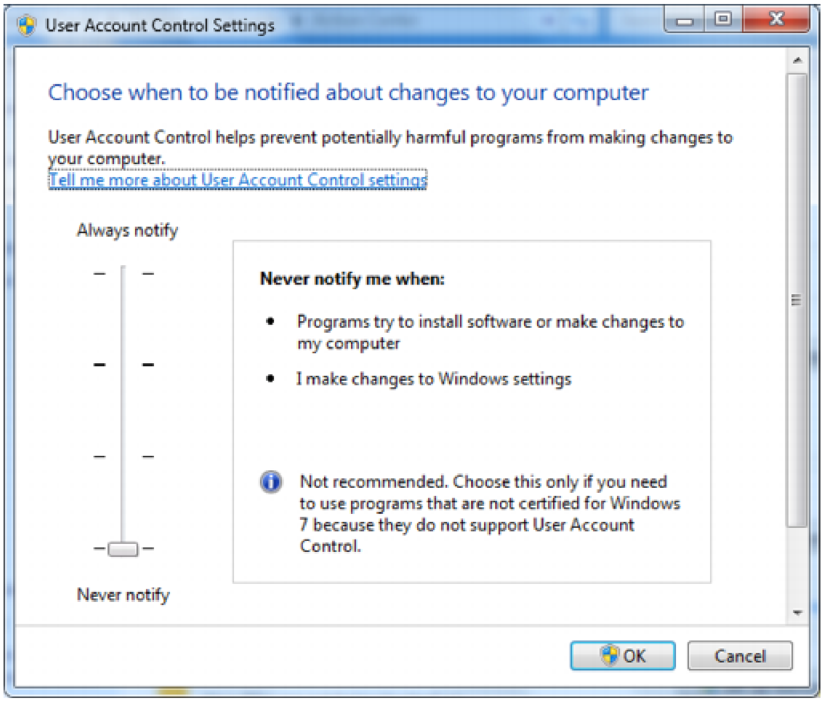
If you use a computer with Windows 8.1 or Windows 7 to browse into the *Metasys* system, be aware that the Site Management Portal UI session information is lost if you are logged in when the operating system goes to sleep. The session terminates at the time the operating system goes to sleep, regardless 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

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 or Windows 7 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 37*).

Figure 37: 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

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.

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 Protocol (PPP) is used for all *Metasys* network dial-up communication between the *Metasys* client computer (web browser) and the ADS/ADX/ODS and engine. Refer to the *Metasys System Extended Architecture Direct Connection and Dial-Up Connection Application Note (LIT-1201639)*.

Data Sharing with Published Web Services

Johnson Controls provides published web services for third-party applications to access a limited set of *Metasys* system functions. Access is tied to access controls within the *Metasys* system using local *Metasys* system user accounts only. Refer to the *Metasys System Extended Architecture Secure Data Access DLL Technical Bulletin (LIT-1201663)* for details on the web services and access controls associated with them.

Network Interface Cards (NICs)

The *Metasys* software supports more than one NIC on a computer running *Metasys* software (including SCT, ADS/ADX/ODS, NxE85, NIE89 and LCS85 software).

Follow the instructions in the appropriate *Metasys* installation documentation to enable all additional NICs on your computer running *Metasys* software so that only one NIC is enabled.

Appendix: Microsoft® Windows® Operating System and SQL Server® Software License Requirements

Windows Operating System License Requirements

The Microsoft Server operating system software used by the ADX/ODS requires licenses called Client Access Licenses (CALs). A CAL is a license that gives you the right to access the services of the server. Two types of Microsoft operating system CALs are available: a device-based CAL and a user-based CAL. These Microsoft CALs are purchased separately from the ADX/ODS software as described in *Purchasing and Designating CALs*.

Note: The ADS/ODS running on a Windows Desktop (non-server) operating system does not require purchased operating system CALs.

Operating System CALs

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/ODS server, regardless of the number of users who access the ADX/ODS. 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. Each NAE requires one device CAL. For example, if 15 NAEs are connected to the ADX/ODS, a total of 15 device CALs are required. Or if 100 NAEs are connected to the ADX/ODS, a total of 100 device CALs are required.

Operating System - User CALs: A user CAL is required for every user who accesses the ADX/ODS server, 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. For example, if two users log in to the ADX/ODS from different locations, two user CALs are required. Or if 10 users log in to the ADX/ODS, 10 user CALs are required.

Another example is a security guard station. During different shifts, security guards often use a single workstation, requiring the use of only one **device CAL**. However, if the security guards use 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/ODS 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/ODS.

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

Table 16 lists the ADX/ODS 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/ODS supports.

Table 16: ADX/ODS License and CAL Examples

ADX/ ODS Offering	Optional MVE Offering	Recommended Number of CALs to Purchase	Windows Operating System CAL Examples
ODS Server **(up to 5 users)**	**None**	10	10 CALs = 5 user CALs + 5 device CALs
			10 CALs = 3 user CALs + 7 device CALs
ADX10 **(up to 10 users)**	**MVE5** **(up to 5 users)**	5	5 CALs = 2 user CALs + 3 device CALs
			5 CALs = 3 user CALs + 2 device CALs
	MVE10 **(up to 10 users)**	15	15 CALs = 10 user CALs + 5 device CALs
			15 CALs = 8 user CALs + 7 device CALs
ADXSWO **(up to 25 users)**	**MVE25** **(up to 25 users)**	30	30 CALs = 25 user CALs + 5 device CALs
			30 CALs = 10 user CALs + 20 device CALs
ADX50 **(up to 50 users)**	**MVE50** **(up to 50 users)**	60	60 CALs = 50 user CALs + 10 device CALs
			60 CALs = 10 user CALs + 50 device CALs
ADX100 **(up to 100 users)**	**None**	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 16* to determine how many CALs you need to purchase from Microsoft. If you purchase *Metasys* system software as part of an ADS/ADX Turnkey or ADS/ADX Ready product, the appropriate number of CALs is included in the purchase. For more details, see *Purchasing and Designating CALs*.

Purchasing and Designating CALs

You need to purchase one additional device CAL for every NAE 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/ODS and you expand your system to require more than 10 connections, upgrade to an ADX or a server-based ODS, you will need more 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 (ADS/ADX Turnkey Info)** link in the Procurement/Purchasing section. The Computer Price List page appears. Review this page to learn 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.

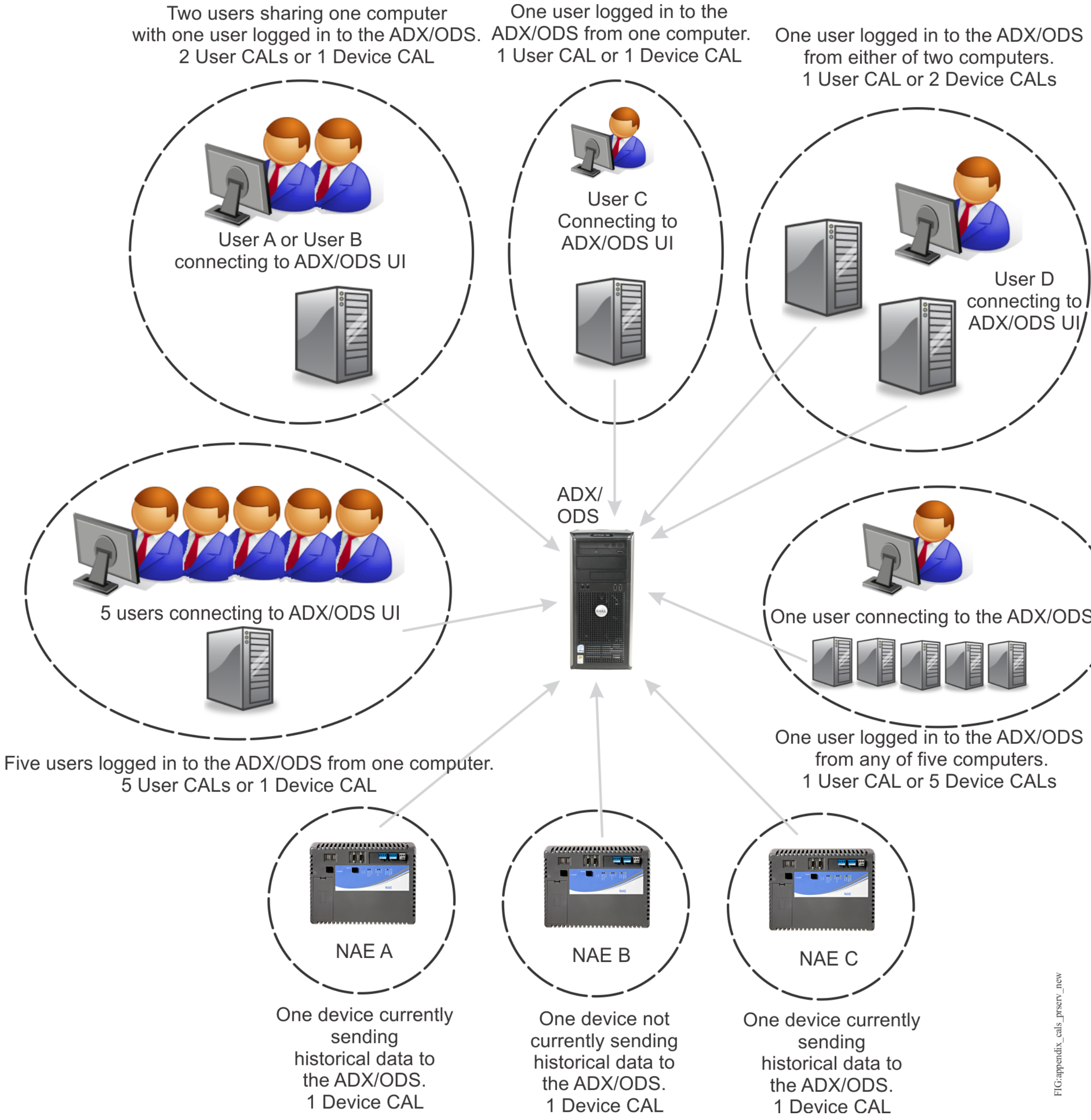
If *Metasys* system software is purchased separately, the customer is responsible for purchasing the correct number of CALs and for properly designating each CAL. A device CAL cannot be transferred to a user CAL, or vice versa. If a *Metasys* Ready or Turnkey computer is purchased, the proper number 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 38 illustrates the use of CALs in a *Metasys* network.

Figure 38: 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
User A or User B
connecting to ADX/ODS UI
One user logged in to the
ADX/ODS from one computer.
1 User CAL or 1 Device CAL
User C
Connecting to
ADX/ODS UI
One user logged in to the ADX/ODS
from either of two computers.
1 User CAL or 2 Device CALs
User D
connecting to
ADX/ODS UI
ADX/
ODS
5 users connecting to ADX/ODS UI
Five users logged in to the ADX/ODS from one computer.
5 User CALs or 1 Device CAL
One user connecting to the ADX/ODS.
One user logged in to the ADX/ODS
from any of five computers.
1 User CAL or 5 Device CALs
NAE A
One device currently
sending
historical data to
the ADX/ODS.
1 Device CAL
NAE B
One device not
currently sending
historical data to
the ADX/ODS.
1 Device CAL
NAE C
One device currently
sending
historical data to
the ADX/ODS.
1 Device CAL
FIG:appendix_cals_prserv_new

SQL Server 2014 and SQL Server 2012 Licensing Requirements

SQL Server 2014 Standard or Enterprise software and SQL Server 2012 Standard or Enterprise software use a **per core** licensing model instead of the **per processor** licensing model that SQL Server 2008 R2 uses. The cost of four core licenses in SQL Server 2014 or SQL Server 2012 SP2 is equivalent to the cost of one processor license in SQL Server 2008 R2. And just as with SQL Server 2008 R2 Express, no CALs are required for SQL Server 2012 Express software.

To determine the licensing needs for SQL Server 2014 or SQL Server 2012 software:

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

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, go to http://support.microsoft.com/kb/2984923/.

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 (http://www.microsoft.com/sam/en/us/map.aspx). 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 an unlimited number of users, NAE/NIE/NCE devices, and ADX/ODS computers to access the SQL Server database on that computer. If the ADX/ODS 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 computer. You must purchase one core license for each physical core in the processor of the database server computer.

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

Table 17 lists the number of core licenses required based on the number of physical cores in the processor.

Table 17: SQL Server 2014 or SQL Server 2012 License Requirements

Physical Cores in the Processor	SQL Server 2014 or SQL Server 2012 Core Licenses Required[1]
1	4
2	4
4	4
6	6
8	8

[1] SQL Server 2014 or SQL Server 2012 software requires a minimum of four core licenses, even for processors with less than four cores.

SQL Server 2008 R2 Licensing Requirements

The SQL Server 2008 R2 software used by the ADX or server-based ODS product requires CALs. However, the SQL Server 2008 Express R2 software edition used by the ADS or non-server based ODS product does not require CALs.

If your ADX/ODS computer has a single processor, we recommend that you purchase one Processor License to allow an unlimited number of users, NAE/NIE/NCE devices, and ADX/ODS computers to access the SQL Server 2008 R2 database on that computer. If your ADX/ODS computer is running SQL Server 2008 R2 software and has multiple processors, purchase Processor Licenses for all of the processors on that computer. Licensing is based on the number of physical CPUs in the computer, not the number of core processors. For example, if the computer has a single quad-core processor, only one processor license is required.

For a split ADX, SQL Server 2008 R2 software is installed on the database server computer. You must purchase a single processor license for the database server computer if the computer has a single processor. If the database server computer has more than one processor, you must purchase one SQL Server 2008 R2 processor license for each processor.

For a split ADX with the *Metasys* Advanced Reporting System, the database engine component of SQL Server 2008 R2 software is present on the database server computer, and the reporting services component of SQL Server 2008 R2 software is installed on the web/application server computer. You must purchase a single processor license for **both** the database server computer and the web/application server computer.

Table 18 lists the ADX/ODS software components and the operating system license types that they require.

Table 18: SQL Server 2008 License Requirements

ADX/ODS Offering	Optional MVE Offering	SQL Server 2008 Software Currently Supported	SQL Server 2008 Processor License
ODS Server (up to 5 users)	**None**	SQL Server 2008 R2 Software	1 Processor License
ADX10 (up to 10 users)	**MVE5 (up to 5 users)**	SQL Server 2008 R2 Software	1 Processor License
	MVE10 (up to 10 users)		
ADXSWO (up to 25 users)	**MVE25 (up to 25 users)**		
ADX50 (up to 50 users)	**MVE50 (up to 50 users)**		
ADX100 (up to 100 users)	**None**		

ADS/ADS-Lite or Non-Server Based ODS Requirements

The ADS/ADS-Lite or non-server based ODS software does not come with, and does not require, device or user CALs. Also, the ADS/ADS-Lite or non-server based ODS uses the free version of SQL Server Express software, so you do not need to purchase SQL Server CALs.

To avoid ADS/ADS-Lite or non-server based ODS connection and network communication performance issues, the number of users and the number of NAE/NIE/NCE devices and ADS/ADS-Lite or non-server based ODS 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 ODS 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 ODS to be the Site Director. Install and configure another ADS/ADS-Lite or non-server based ODS (or more) to provide the ADS repository function. When you install a separate ADS/ADS-Lite or non-server based ODS to provide the repository function, it allows you to dedicate five connections on the alternate ADS/ADS-Lite or non-server based ODS for system users and another five connections on the alternate ADS/ADS-Lite or non-server based ODS to NAE/NIE/NCE devices and ADS/ADS-Lite/ODS computers for transferring trend data, event messages, or audit messages.

  Note: The ADS/ADS-Lite or non-server based ODS cannot be the Site Director for another ADS/ADS-Lite/ODS of any type.
- Upgrade to an ADX or a server-based ODS. Configure the Windows Server of the ADX/ODS computer with the number of CALs equal to the total number of users and devices accessing the ADX/ODS. In addition, configure the SQL Server database with one SQL Server Processor license.

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

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 via 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 via an SNMP Set message.
- NMS cannot modify the supervisory device via 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 (*Table 19*). The NMS software can read these MIB files, as well as the standard MIB files.

Table 19: 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 object identifier (OID) 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 20* lists the attributes.

Configuring Trap Filtering

Of the available attributes listed in *Table 20*, 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)*, *ODS Commissioning Guide (LIT-12011944)* and the *ADS/ADX Commissioning Guide (LIT-1201645)*. This list applies to *Metasys* alarm events only.

Table 20: 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 21* lists the attributes that are sent.

Table 21: 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 (NAE/ADS/ODS). Examples include High Warning and Low Alarm. Each Trap OID also sends the attribute values that were selected for the trap (*Table 20*).

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 (NAEs as supervisory devices) are considered offline or online. These events have a structure similar to the Alarm Raised structure, and reports the same set of attributes (*Table 20*). 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 22*.

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 23*. 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 22*) and **y** is an ASCII representation for the name of the *Metasys* point.

Table 22: 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 22*).

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 23*).

Table 23: 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
.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 *Table 24*.

Table 24: 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 *Table 25*.

Table 25: SNMP Trap Attribute Example

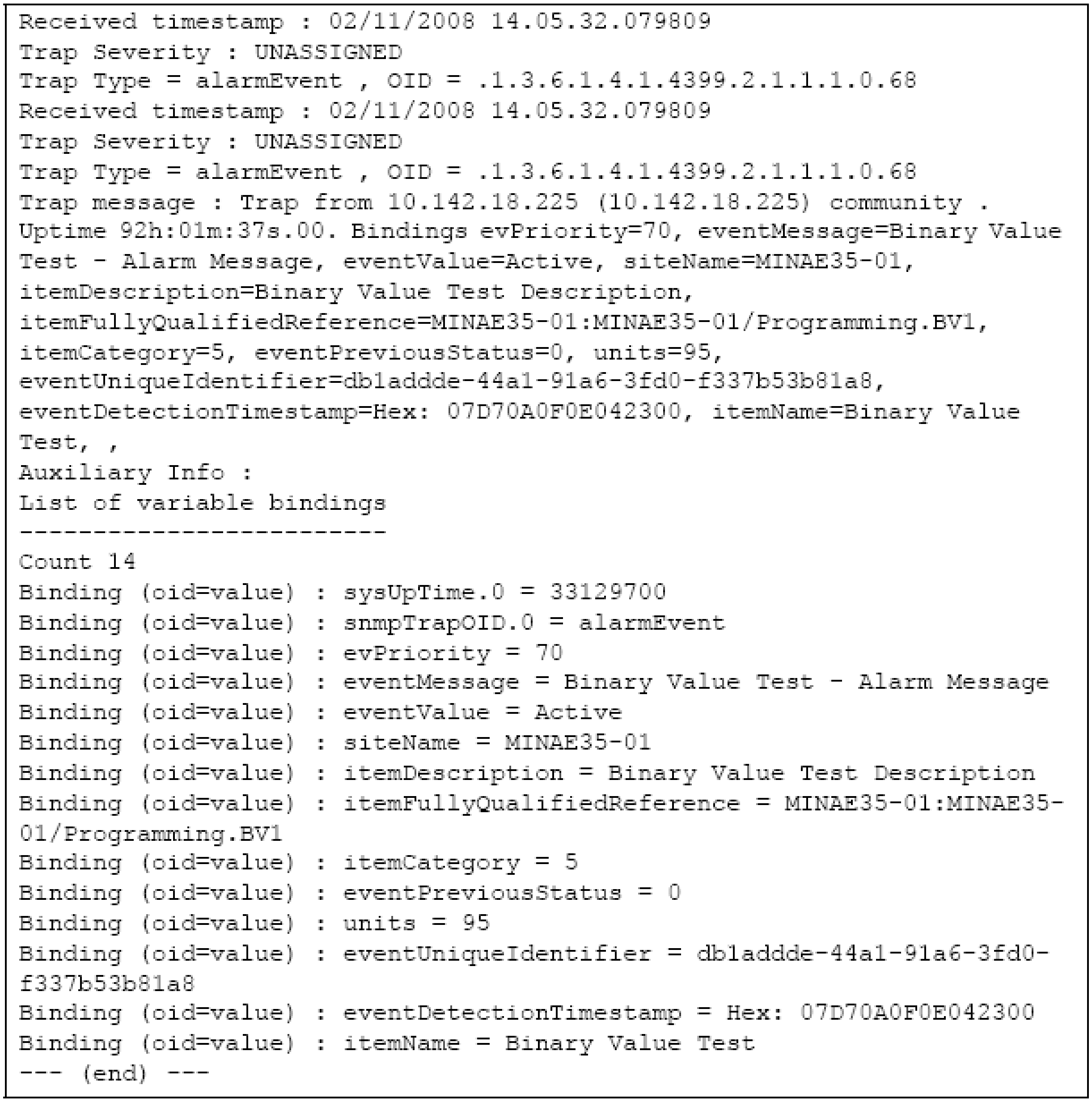
SNMP Trap Attribute	Alarm Value	Normal Value
snmpTRAPOID.O	alarmEvent	normalEvent
EventValue	Active	Inactive
EventPreviousStatus	0	68
EventMessage	Alarm message defined in the *Metasys* Site Management Portal UI	Return to Normal message defined in *Metasys* Site Management Portal UI

Trap Examples

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

Binary Point Alarm

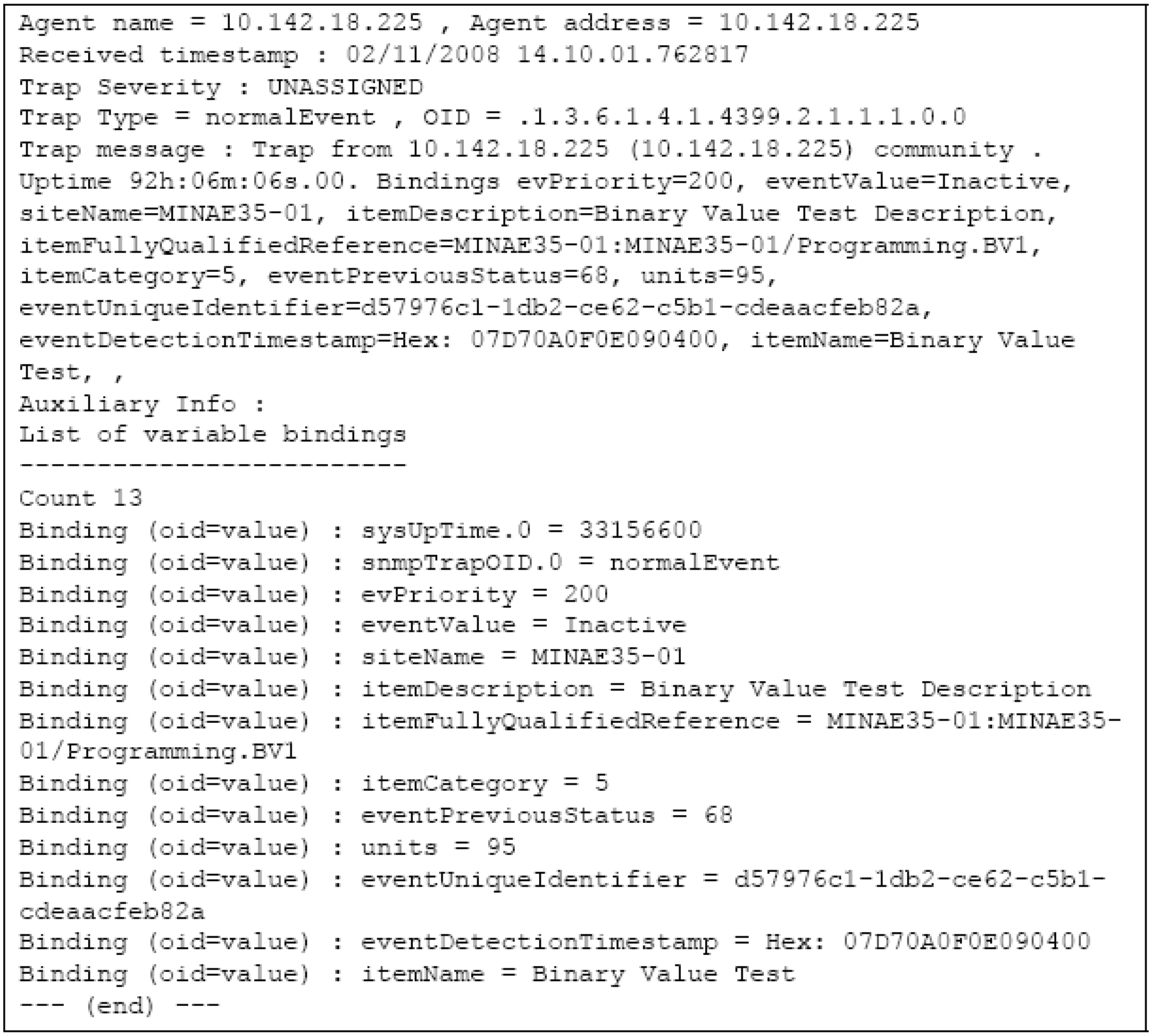
Figure 39: Binary Point Alarm Example



```
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

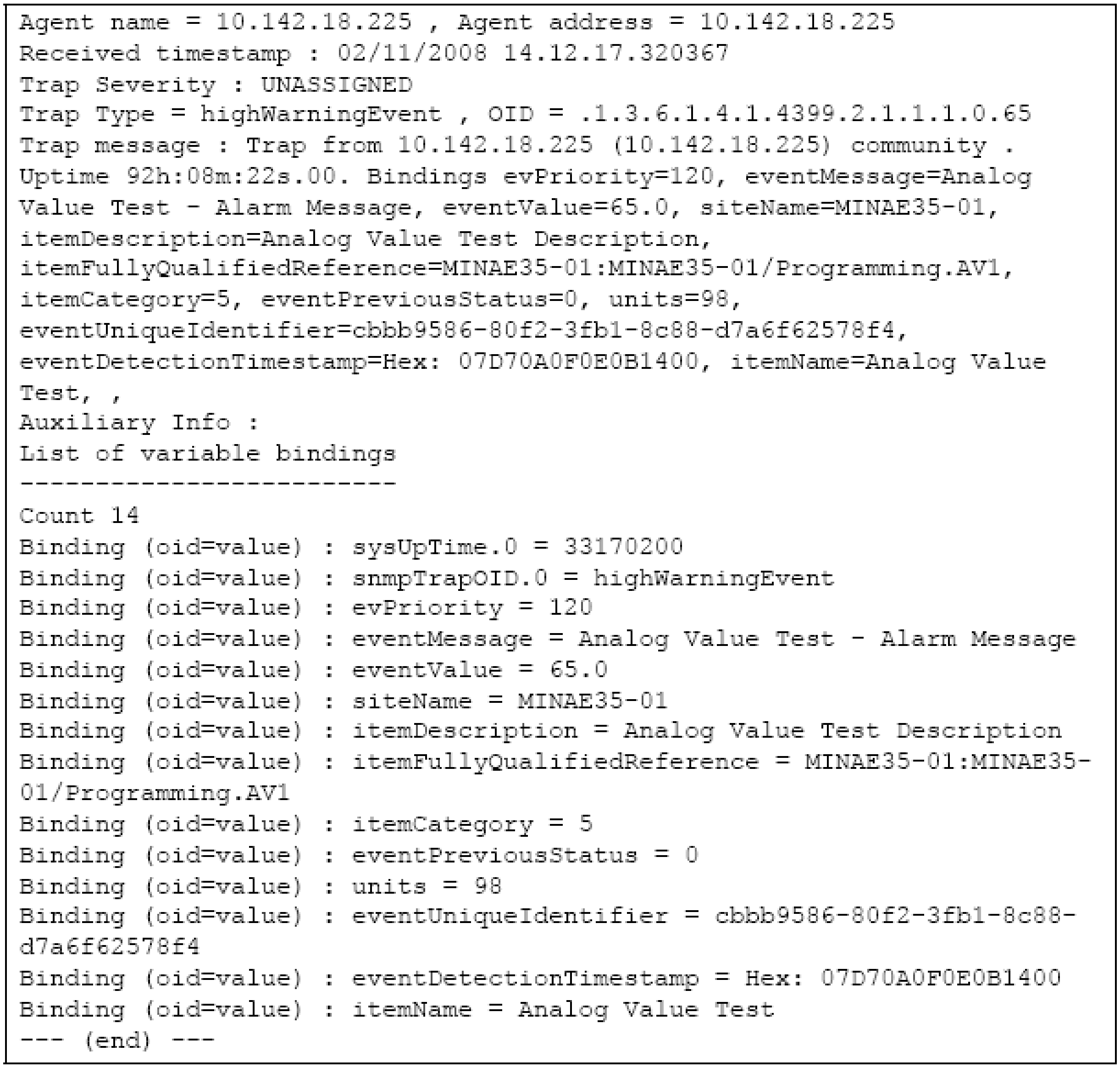
Figure 40: Binary Point Return to Normal



```
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

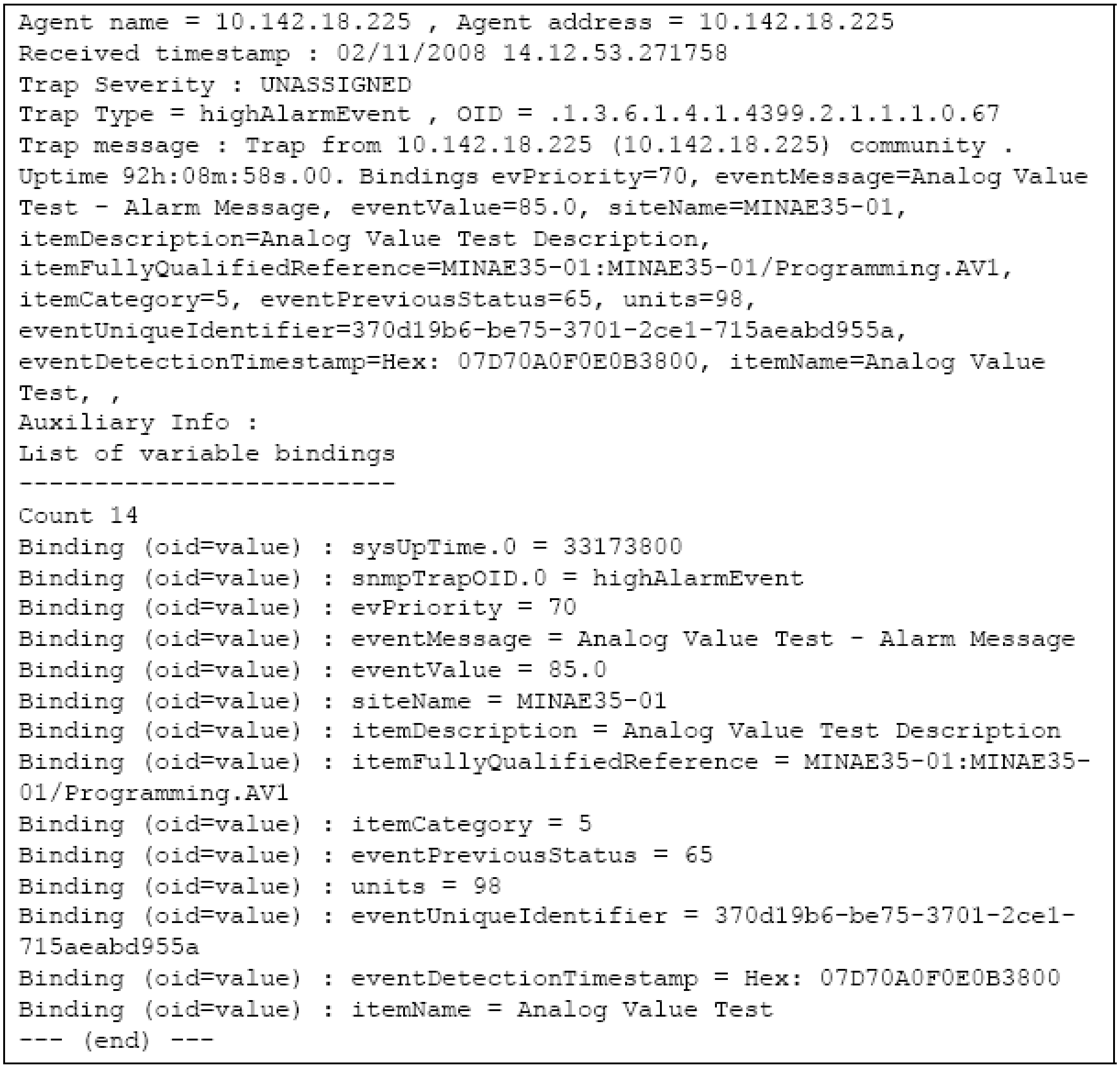
Figure 41: Analog Point High Warning



```
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

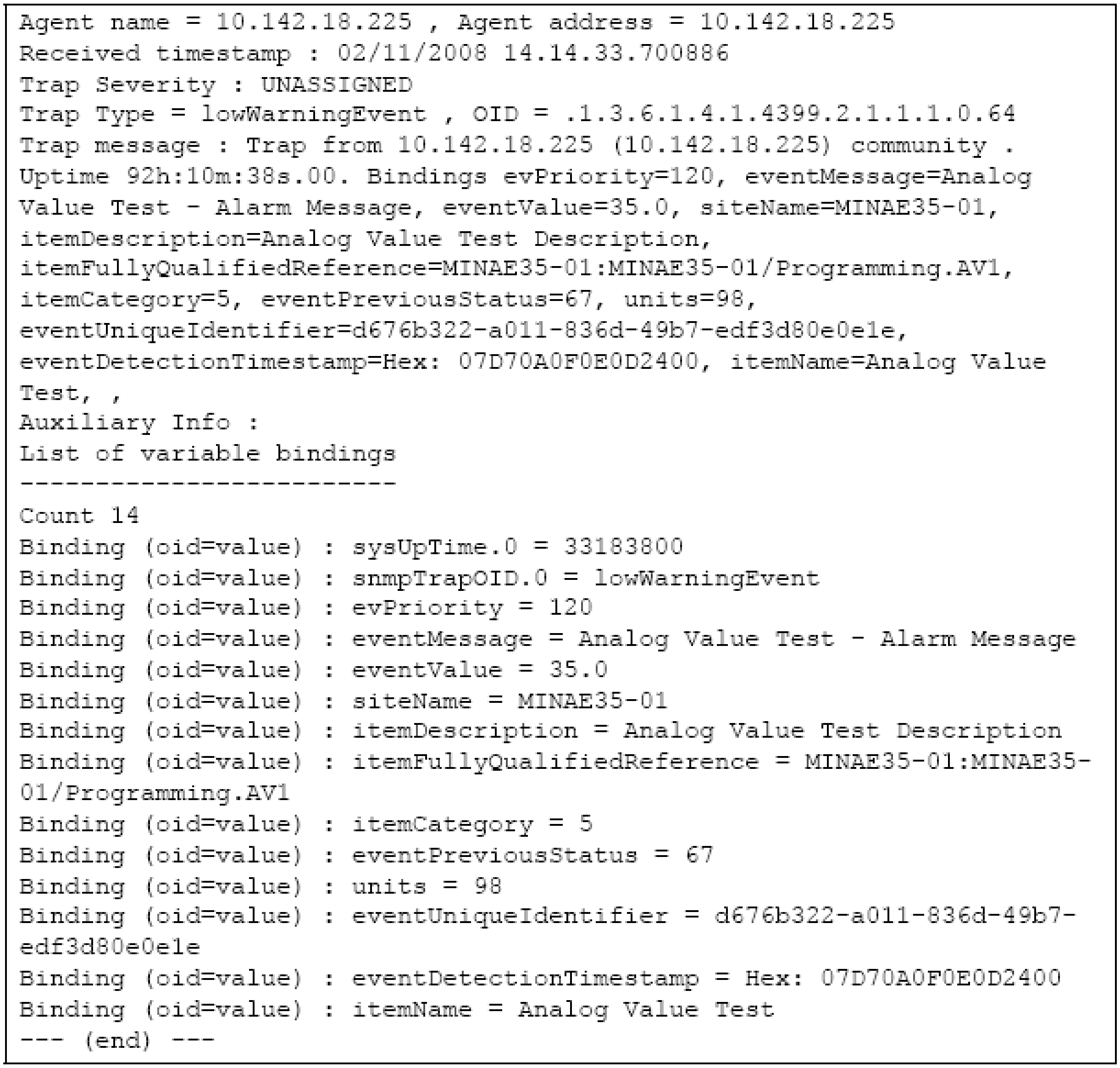
Figure 42: Analog Point High Alarm



```
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

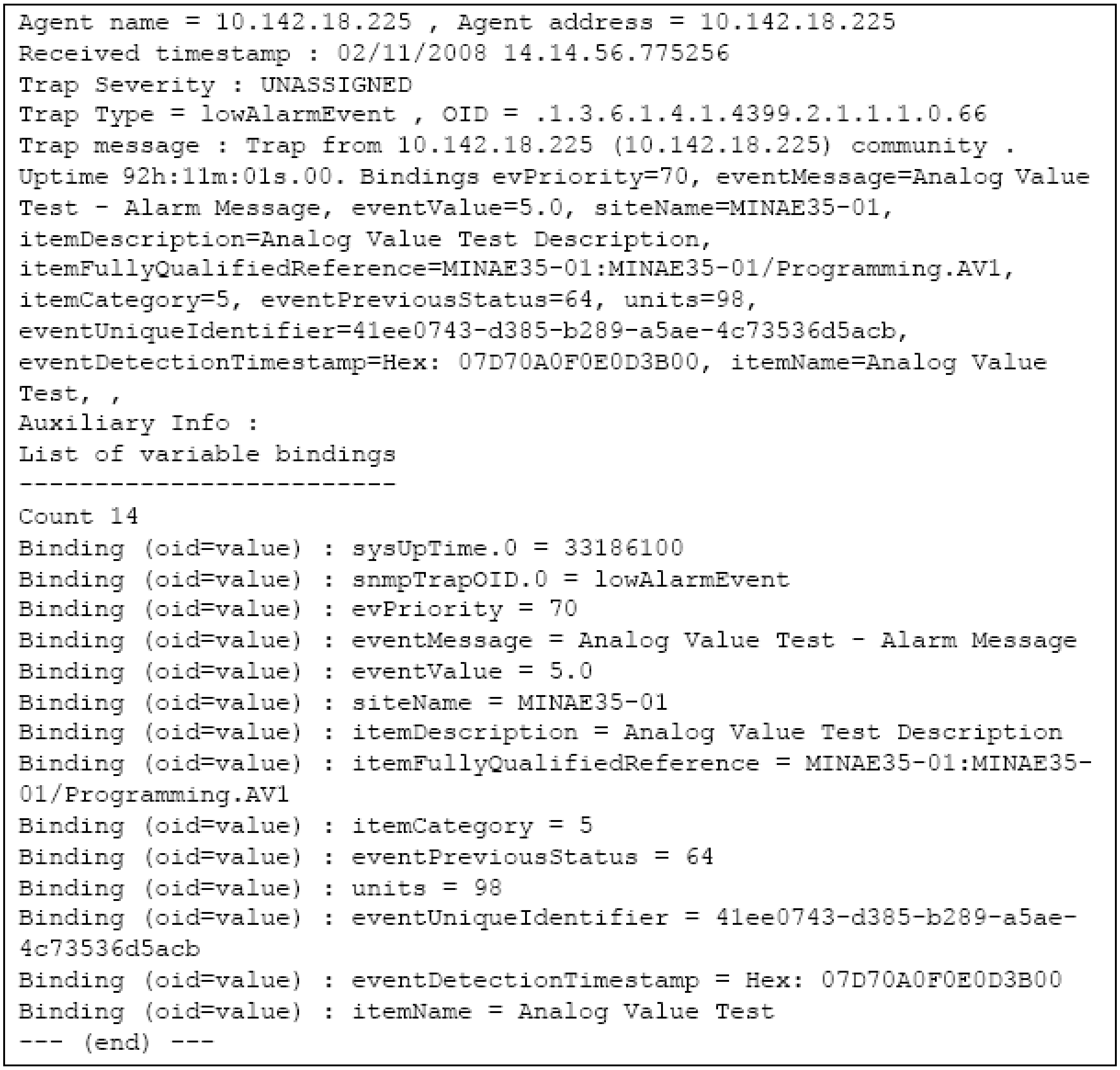
Figure 43: Analog Point Low Warning



```
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

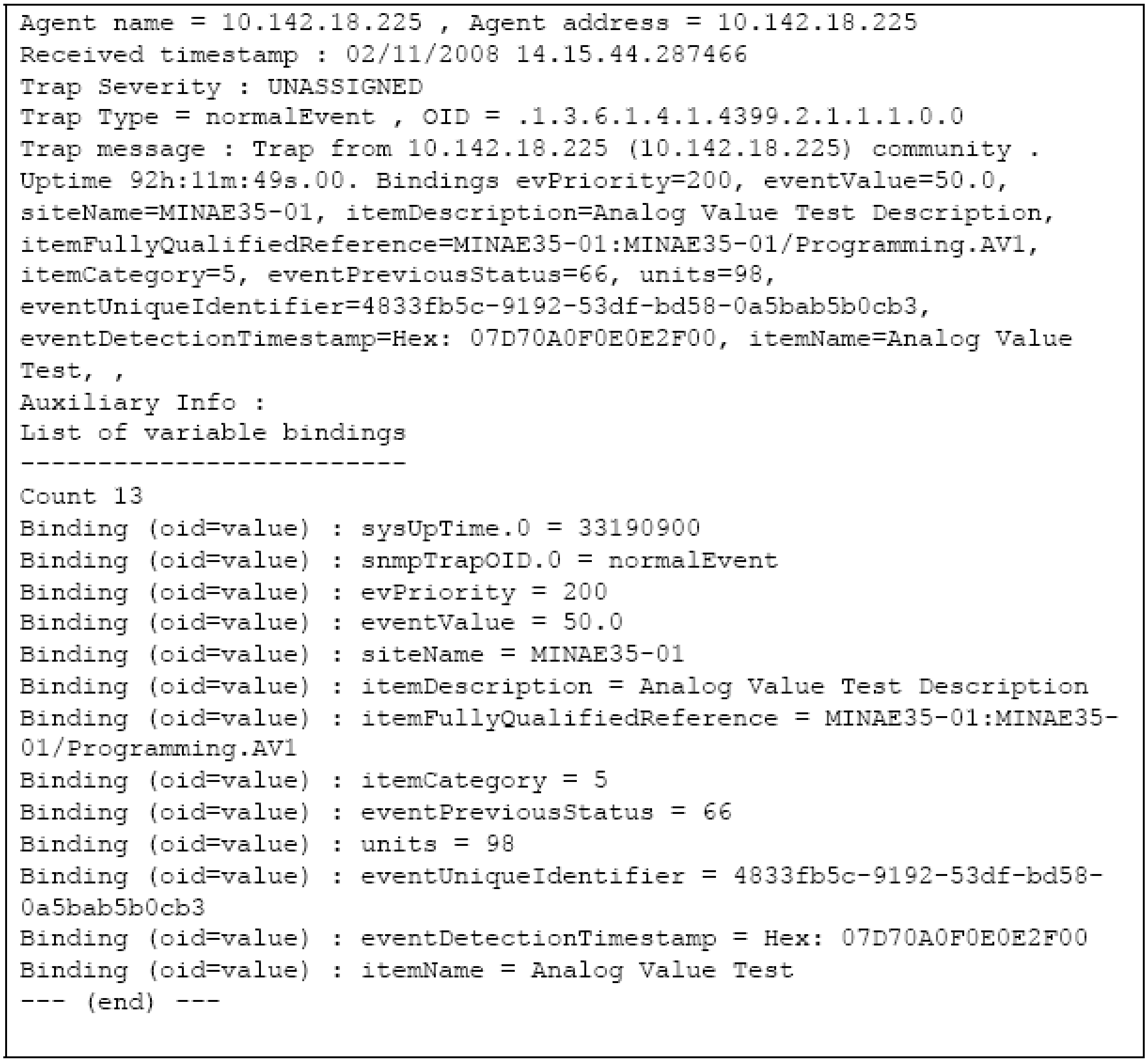
Figure 44: Analog Point Low Alarm



```
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

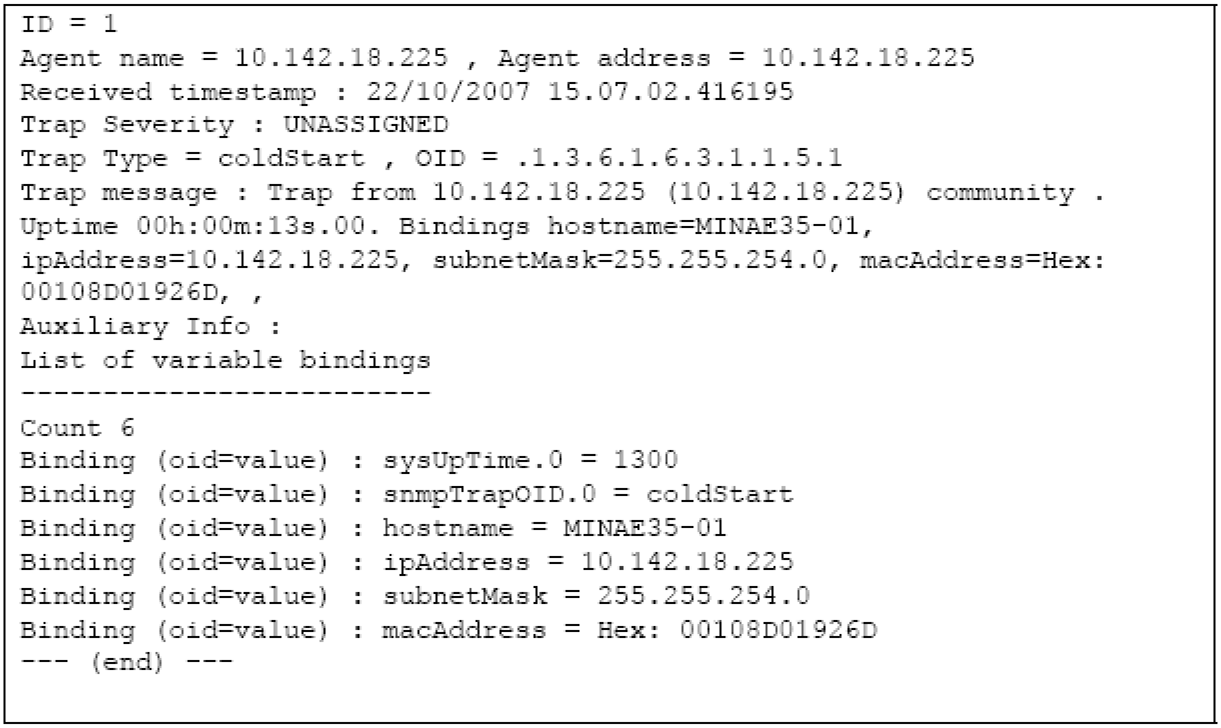
Figure 45: Analog Point Return to Normal



```
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)

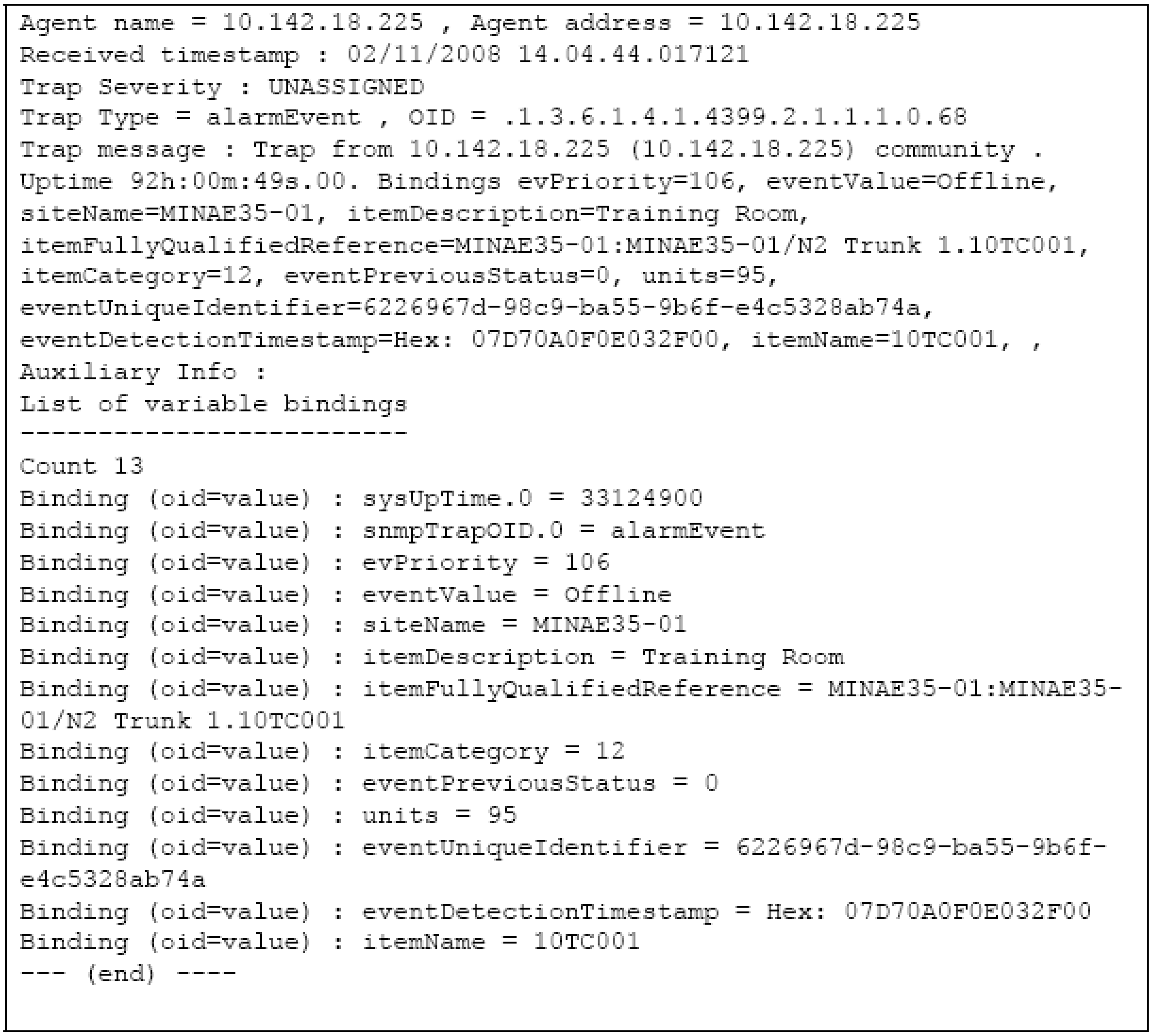
Figure 46: Supervisory Device Agent Restart (ColdStart)



```
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

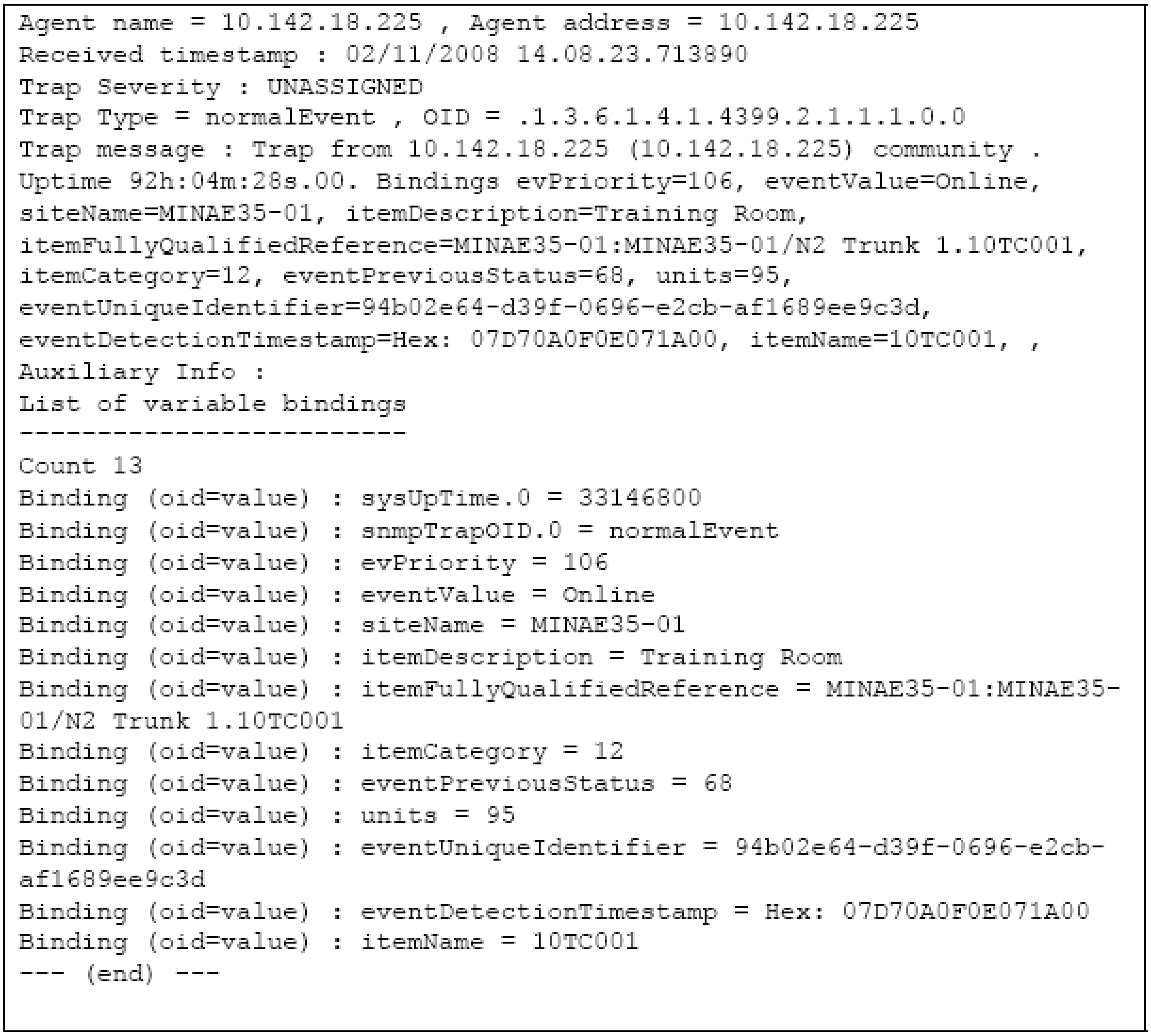
Figure 47: Field Device Offline



```
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

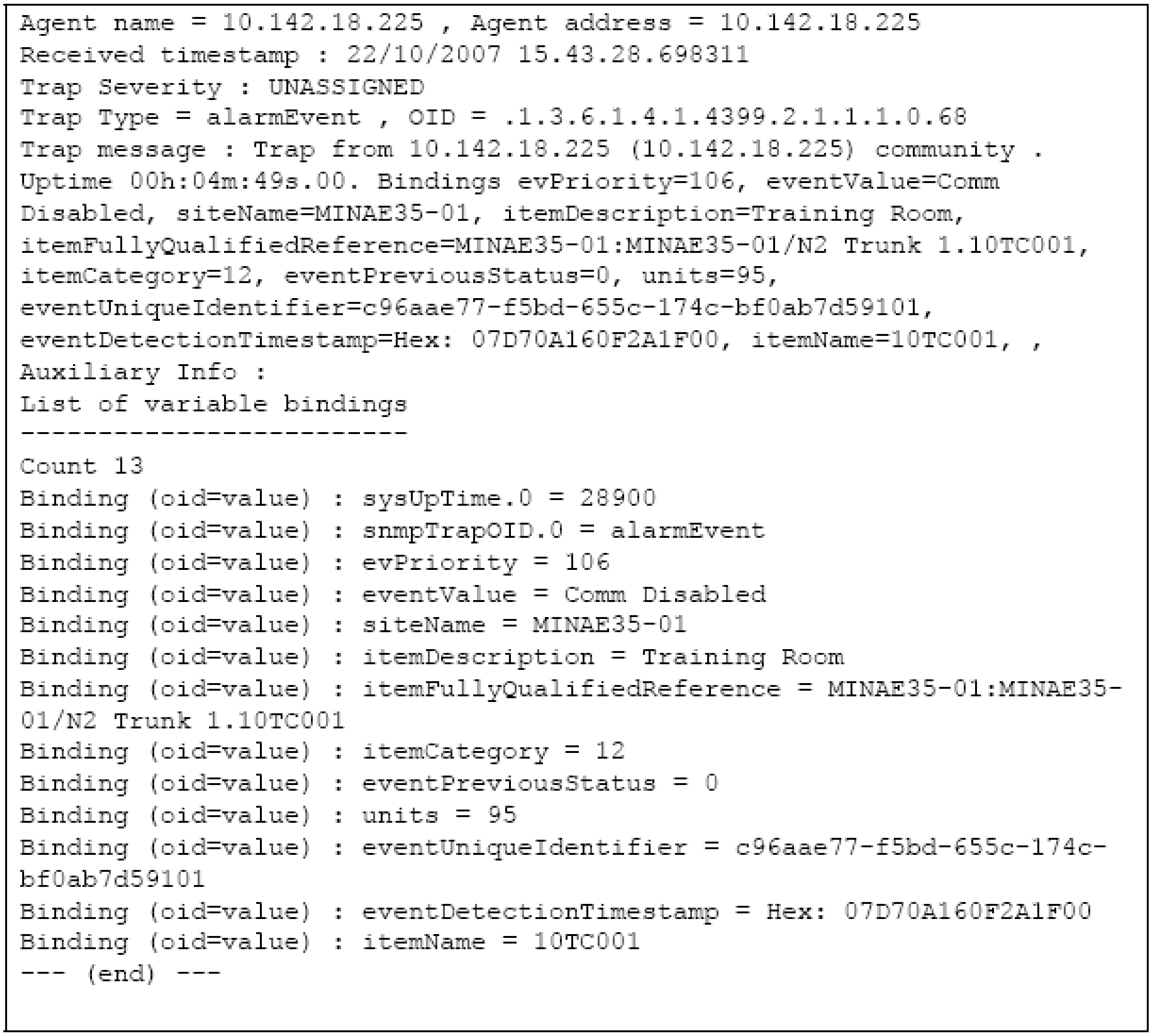
Figure 48: Field Controller Online



```
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

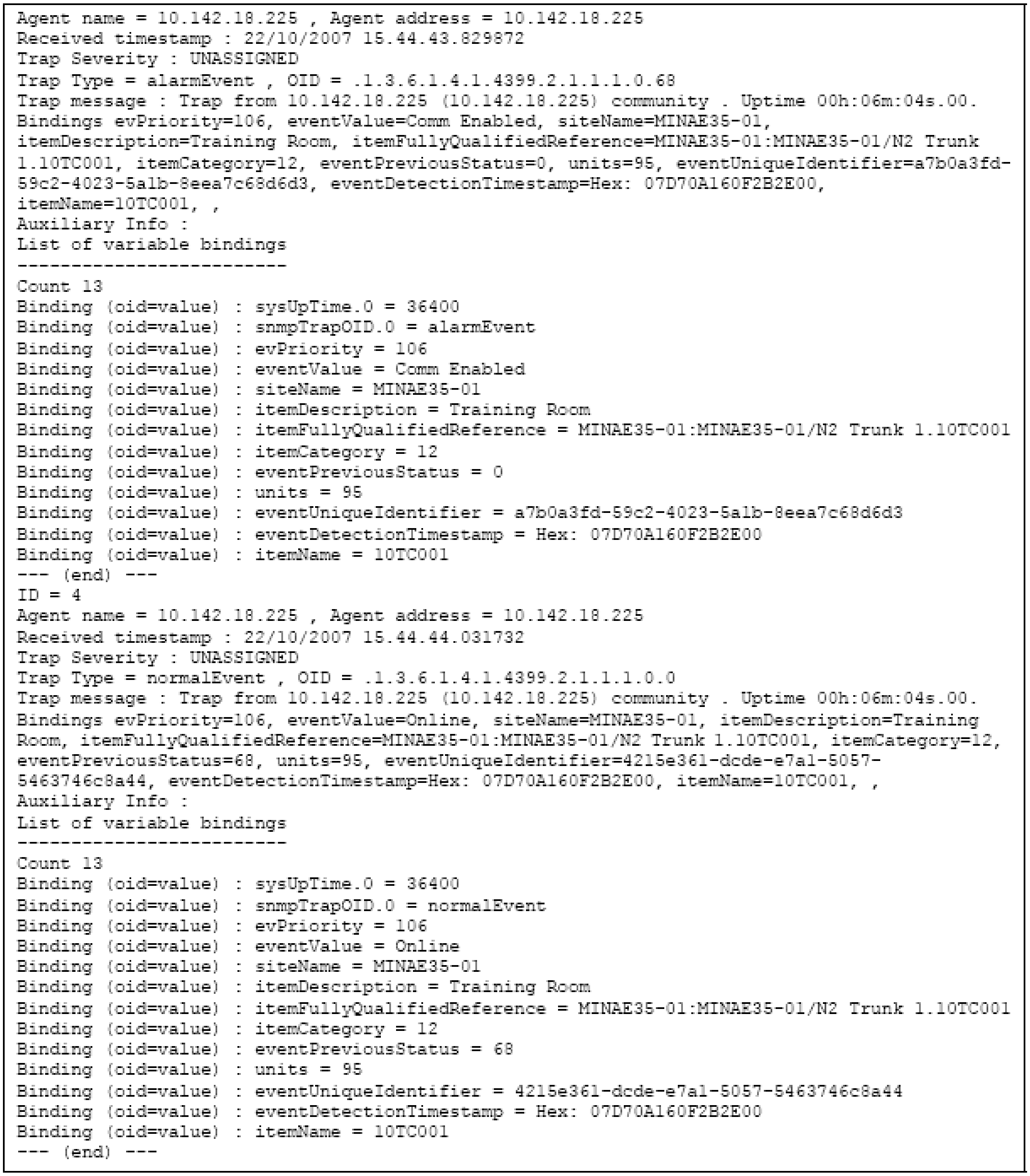
Figure 49: Field Controller Disabled Example



```
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 50: 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: 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 ADS/ADX/ODS 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 ADS/ADX/ODS (and SCT) software that supports the Active Directory feature. Example logistics that fall outside these questions include:
  - administrative access to the ADS/ADX/ODS computer
  - proper SQL Server rights to install or upgrade the ADS/ADX/ODS 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 26 is a worksheet that outlines the questions that need to be answered as part of the Active Directory service implementation on the *Metasys* system.

Table 26: 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 ADS/ADX/ODS 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 ADS/ADX/ODS 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 ADS/ADX/ODS 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 ADS/ADX/ODS 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*.
Are there any firewalls between the ADS/ADX/ODS and the Active Directory service domain?	Yes	Firewalls must be correctly configured to allow Active Directory service port and protocol access between the ADS/ADX/ODS 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.

Table 26: Active Directory Service Worksheet

Question	Answer	Action Steps
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 ADS/ADX/ODS 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 ADS/ADX/ODS 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.

[1] In order to perform this step, 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.

[2] Active Directory service groups are normally managed by the IT department. A process for managing the addition and removal of *Metasys* system users who are also Active Directory service users must be enacted.

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 26*, though not all requirements apply to every installation.

ADS/ADX/ODS Computer

The computer with the ADS, ADX, or ODS software 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 ADS/ADX/ODS or SCT UI must be joined to an Active Directory service domain where the ADS/ADX/ODS 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 Administration 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: Security Certificate Implementation

This section covers the process of purchasing a security certificate (SSL or TLS) from a public certificate authority and installing the certificate for use with the *Metasys* User Interface (UI) or the *Metasys* UI Offline.

Note: Ready Access Portal does not support the current SSL implementation included in this appendix.

The benefits of using a certificate from a public certificate authority include:

- Increased client security due to pre-established trust of a certificate authority
- Improved user experience with no browser warnings or need for client device configuration

Notes:

- A security certificate only encrypts communication between the client browser and the ADS/ADX or ADS-Lite web server. The security certificate does not encrypt communication between other *Metasys* servers or network engines.
- The certificate does not dictate which protocol version (SSL or TLS) is used, and the same certificate can generally be used for both SSL and TLS.

Prerequisites

Before using the steps outlined in this document, you must install the *Metasys* server and the *Metasys* UI or SCT with *Metasys* UI Offline software and establish the site address.

As a prerequisite to purchasing a third-party security certificate through a public certificate authority, you must base the *Metasys* UI or *Metasys* UI Offline site address on a registered Internet domain name. This may require purchasing a domain name and configuring it to point to the *Metasys* site IP address. An example domain name is used in a portion of the instructions included in this document. For an example of purchasing a domain name, see *Purchasing a Domain Name*.

Important Considerations

Consider the following when you implement third-party security certificates:

- The steps to purchase a domain name and a security certificate vary according to the registrar. Use these instructions as an example. You may choose a different registrar to purchase a domain name and security certificate.
- The domain name and security certificate costs are not included as part of the purchase cost of the *Metasys* software.
- Coordinate with the customer IT department to configure IIS correctly before you install the *Metasys* software.
- Once the third-party security certificate is implemented on the server hosting the *Metasys* software, a certificate reissue is required if the server is re-imaged or is upgraded. The steps vary according to the security certificate registrar. A certificate reissue does not have additional costs. Refer to your security certificate registrar for more information.
- Domain names and third-party security certificates expire. We recommend registering domain names and third-party certificates for the longest duration available (typically 3 years). Plan to renew domain names and security certificates before they expire.

Detailed Procedures

Purchasing a Domain Name

If the *Metasys* server that hosts the *Metasys* UI or the SCT computer that hosts the *Metasys* UI Offline requires a security certificate from a public certificate authority, a public domain name is required. You can purchase a domain name from a wide variety of registrars. This section includes instructions using the vendor https://www.namecheap.com/, a popular seller of domain names.

Note: The *Metasys* UI or *Metasys* UI Offline does not need to be exposed to the Internet to use a public domain name as shown in this example.

Note: The steps to purchase a domain name vary according to the registrar. Use these instructions as an example.

1. In a web browser, browse to https://www.namecheap.com/.
2. Select **Domains** > **Register**.
3. In the **Find your new domain name** field, enter a domain name to determine whether the domain name is available for purchase. An example of a domain name is metasys1405.link. Click **Search**.
4. If the desired domain name is available, click the shopping cart icon next to the domain name in the search results.
5. Click **View Cart**. The content of your shopping cart appears.
6. Select **3 Years** from the drop-down list. We recommend that you purchase the domain name for a 3-year period to match with the lifetime of the security certificate you purchase in *Purchasing the Security Certificate from a Public Certificate Authority*.

   Note: The AUTONEW function attempts to automatically renew the domain name at the end of this period. The WHOISGUARD (or privacy protection) feature is optional. This feature protects the contact details you enter from being publicly listed. If you select this feature, the domain registrar handles any inquiries about the domain on your behalf and then forwards these to you.

   Click **Confirm Order**.
7. Complete the purchase by logging in or creating an account and then entering the payment information.
8. When the purchase is complete, click the Your Domains/Products link (visible when you are logged into your account). Your domain name is listed on the page.
9. Click the domain name to manage the domain.
10. On the left side of the page under Host Management, click **All Host Records**. The **Modify Domain: [your domain name]** section appears.
11. In the top row, where @ is listed in the Host Name column, enter the IP address of the *Metasys* UI or *Metasys* UI Offline in the IP Address/URL column. In the Record type column, select **A (Address)**.
12. In the second row, where www is listed in the Host Name column, enter your domain name with https:// preceding the domain name in the IP Address/URL column. For example, enter https://metasys1405.link. In the Record type column, select **URL Redirect**.
13. Click **Save Changes**.

    The changes may take a few hours to take effect.

Implementing Security Certificates for Metasys UI or Metasys UI Offline Software

To implement a third-party or self-signed security certificate for *Metasys* UI or *Metasys* UI Offline software, follow the steps included here.

The options for security certificates include the following:

- Third-Party – To configure IIS correctly for a site, coordinate with the customer IT department before installing the *Metasys* software for the site. See *Third-Party Security Certificates*.
- Self-Signed – Follow the installation process that allows you to generate a self-signed certificate. See *Self-Signed SSL Certificates*.

Verify that Port 443 (SSL) is open on the server computer where the *Metasys* UI and *Metasys* UI Offline software for the site is installed.

1. Open Control Panel and click **System and Security** > **Administrative Tools.** The Administrative Tools window appears.
2. In Administrative Tools, double-click **Internet Information Services (IIS) Manager**. The IIS Manager window appears.
3. In the tree in the left pane of the screen, expand Sites or Web Sites and select **Default Web Site**.

4. Right-click Default Web Site and select **Edit Bindings**. The Site Bindings box appears.
5. Click **Edit**. Verify that the SSL port field contains 443.

   Note: Verify that the TCP Port 80 is open for *Metasys* software at the firewall.
6. Click **OK**.
7. Close the IIS Manager window.

Third-Party Security Certificates

Creating the Certificate Request

Follow these steps to create a certificate request through Microsoft IIS, which submits the properties of your security certificate to the certificate authority.

Table 27: Creating the Certificate Request (CSR)

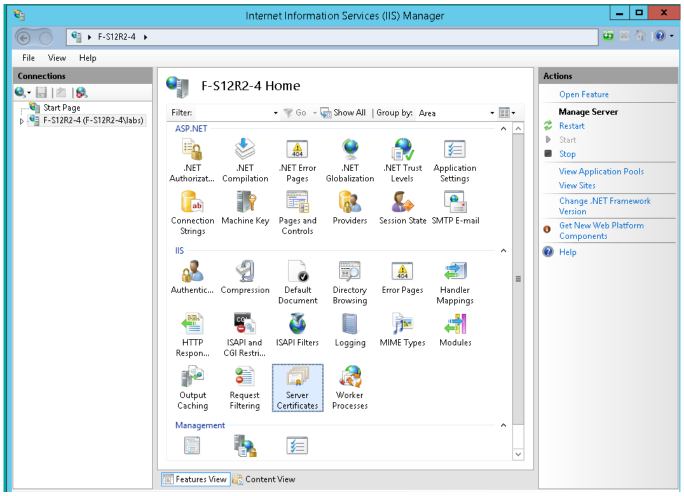
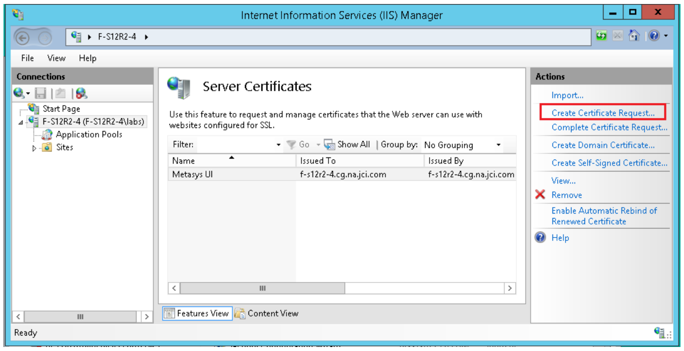
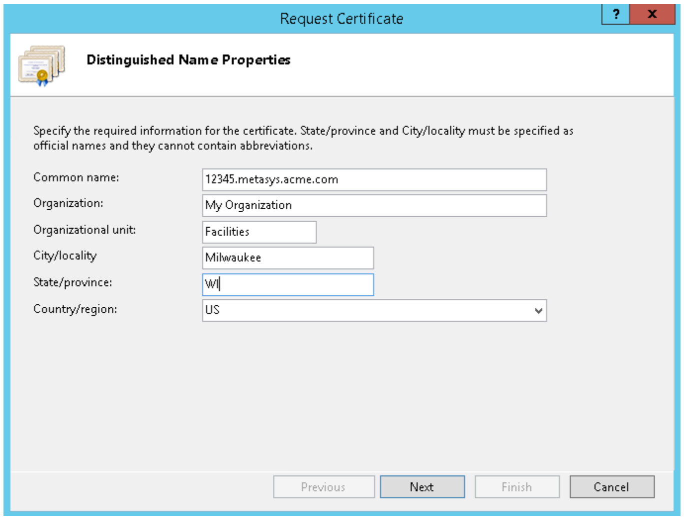
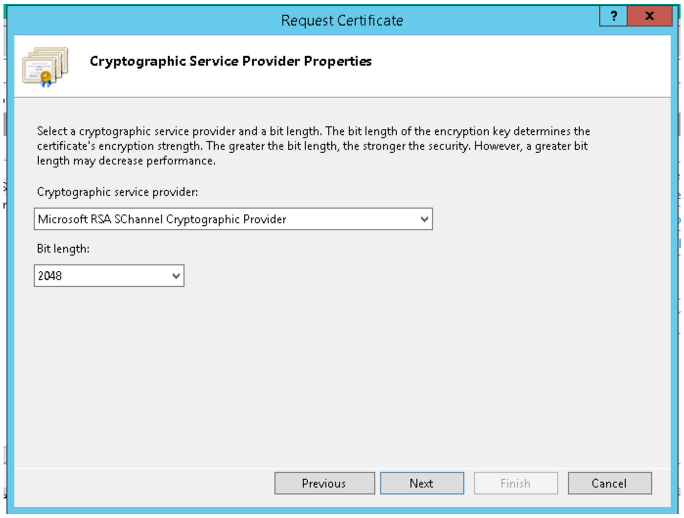
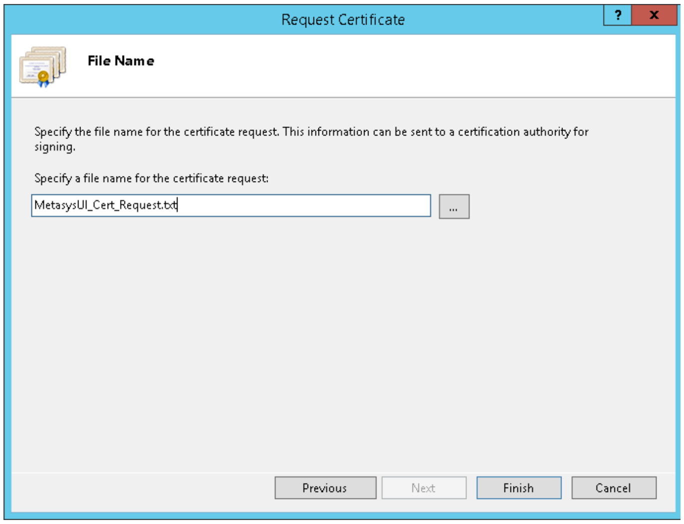
1.	**Figure 51: IIS Server Certificates**  Internet Information Services (IIS) Manager F-S12R2-4 Home	On the *Metasys* server hosting the *Metasys* UI, or the SCT computer hosting the *Metasys* UI Offline, open Control Panel and click **System and Security** > **Administrative Tools**. The Administrative Tools window appears. In Administrative Tools, double-click **Internet Information Services (IIS) Manager**. The IIS Manager window appears. **Note:** *Metasys* software supports IIS version 7 and version 8. Double-click **Server Certificates**.
2.	**Figure 52: Create Certificate Request**  Server Certificates Use this feature to request and manage certificates that the Web server can use with websites configured for SSL. Name: Metasys UI; Issued To: f-s12r2-4.cg.na.jci.com; Issued By: f-s12r2-4.cg.na.jci.com	In the right pane under Actions, click **Create Certificate Requests**. The Request Certificate wizard opens.
3.	**Figure 53: Distinguished Name Properties**  Request Certificate Distinguished Name Properties Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations. Common name: 12345.metasys.acme.com Organization: My Organization Organizational unit: Facilities City/locality: Milwaukee State/province: WI Country/region: US	In the Distinguished Name Properties window, enter the following information: • **Common name:** the domain name without https://, /ui, or /uioffline. The domain name should be the site used to browse to the *Metasys* UI or *Metasys* UI Offline. • **Organization:** the name of your organization • **Organizational unit:** the name of your department within the organization • **City/locality:** the city in which your organization is located • **State/province:** the state in which your organization is located • **Country/region:** the country in which your organization is located Click **Next**.

Table 27: Creating the Certificate Request (CSR)

4.	**Figure 54: Cryptographic Service Provider Properties**  Request Certificate **Cryptographic Service Provider Properties** Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance. Cryptographic service provider: Microsoft RSA SChannel Cryptographic Provider Bit length: 2048 	In the Cryptographic Service Provider Properties window, keep the default cryptographic service provider option. From the Bit length drop-down list, select **2048**. Click **Next**.
5.	**Figure 55: File Name**  Request Certificate **File Name** Specify the file name for the certificate request. This information can be sent to a certification authority for signing. Specify a file name for the certificate request: MetasysUI_Cert_Request.txt 	In the File Name window, specify a name for the certificate request file. Click the browse button to select the location to save the file. You can save the file anywhere; it is only needed temporarily. Click **Finish**. Go to *Purchasing the Security Certificate from a Public Certificate Authority*.

Purchasing the Security Certificate from a Public Certificate Authority

If the *Metasys* server that hosts the *Metasys* UI, or the SCT computer that hosts the *Metasys* UI Offline, requires a security certificate from a public certificate authority, acquire a basic Class 1 SSL certificate, also called a domain-verified certificate. You can purchase a security certificate from any public certificate authority. The instructions in this section use the vendor https://www.namecheap.com/, a popular reseller of SSL certificates from several of the largest certificate authorities, including GeoTrust, Inc. The RapidSSL™ product from GeoTrust, Inc. is used as an example.

Note: The steps to purchase a security certificate vary according to the registrar. Use these instructions as an example.

1. In a web browser, browse to https://www.namecheap.com/.
2. Navigate to the SSL certificate products.

3. Choose the RapidSSL option used in these instructions and select the longest duration available for the certificate. Click **Add to Cart**. The Order Confirmation page appears.
4. Click **Confirm Order**.
5. You are prompted to create an account with https://www.namecheap.com/. If you already have an account, log in. If you do not have an account, enter your account information and click **Create Account and Continue**. The Order Review page appears.
6. Review your order and select your payment option. Complete your purchase.
7. Click **Manage My Account** to view your purchased certificate.
8. On your Manage My Account page, a message appears alerting you to activate your SSL certificate. Click **SSL Certificates page**.
9. In the Status column, click **Activate Now**. The Digital Certificate Order Form page appears.
10. In the Select web server drop-down list, select **Microsoft Internet Information Server**.
11. Open the .txt file you created in Step 5 from *Creating the Certificate Request*. Select all of the text from the .txt file and paste the text into the **Enter CSR** field on the Digital Certificate Order Form page.
12. Click **Next**.
13. Select the approver email address to verify ownership of the domain name. You must be able to access the mailbox of the email address selected. A message containing a validation code is sent to this email address. Click **Next**. A confirmation page appears.
14. Confirm that the administrator contact information is correct. Click **Submit Order**. The Digital Certificate Order Process Summary appears.
15. Wait for the email message to approve the certificate.
16. When you receive the email message to approve the certificate, click the link to approve the certificate. When you click the link, you are directed to an order review and approval page. Verify that the information on the page is correct. Click **I Approve**. The order is successfully approved. Wait for the email message that contains the encoded certificate text.

    Go to *Installing the Security Certificate* to complete the process.

Installing the Security Certificate

Table 28: Installing the Security Certificate

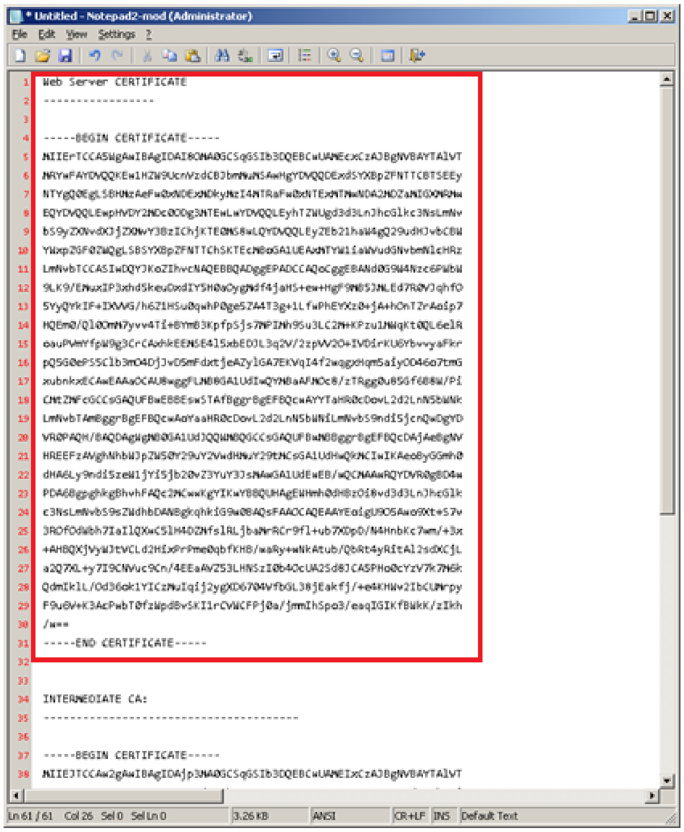
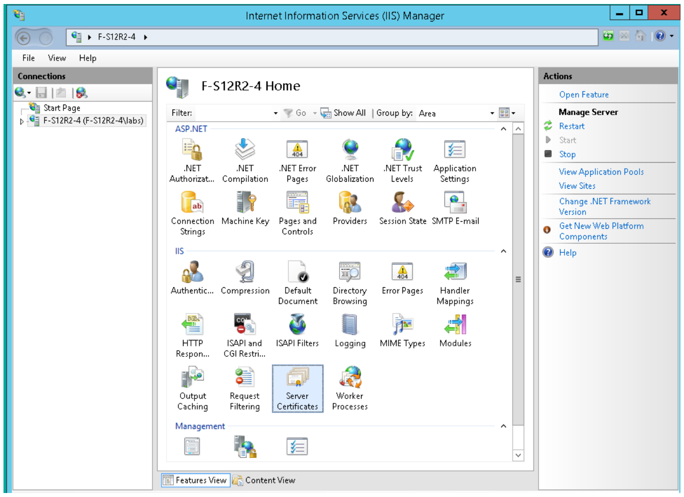
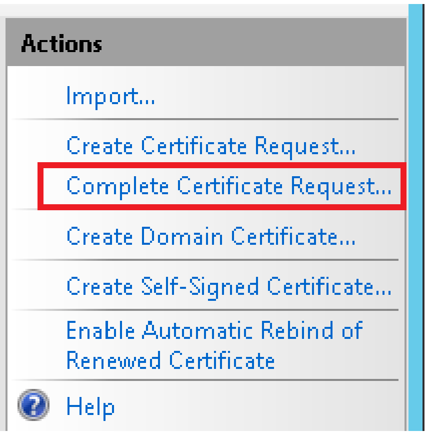
1.		When you receive the email message from the last step in *Purchasing the Security Certificate from a Public Certificate Authority*, click the link to install the certificate.
2.	**Figure 56: SSL Certificate Text to Copy**  * Untitled - Notepad2-mod (Administrator) File Edit View Settings ? Web Server CERTIFICATE ----------------- -----BEGIN CERTIFICATE----- MIIErTCCA5WgAwIBAgIDAI8OMA0GCSqGSIb3DQEBCwUAMEcxCzAJBgNVBAYTAlVT MRYwFAYDVQQKEw1HZW9UcnVzdCBJbmMuMSAwHgYDVQQDExdSYXBpZFNTTCBTSEEy NTYgQ0EgLSBHMzAeFw0xNDExNDkyMzI4NTRaFw0xNTExMTMwNDA2MDZaMIGXMRMw EQYDVQQLEwpHVDY2NDc0ODg3NTEwLwYDVQQLEyhTZWUgd3d3LnJhcGlkc3NsLmNv bS9yZXNvdXJjZXMwY3BzIChjKTE0MS8wLQYDVQQLEyZEb21haW4gQ29udHJvbCBW YWxpZGF0ZWQgLSBSYXBpZFNTTChSKTEcMBoGA1UEAxMTYW1iaWVudGNvbmNlcHRz LmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANd0G9W4Nzc6PWbW 9LK9/EMuxIP3xhd5keuOxdIY5H0aOygMdf4jaH5+ew+HgF9M05JNLEd7R0VJqhfO 5YyQYkIF+IXVVG/h6Z1HSu0qwhP0ge5ZA4T3g+1LfwPhEYXz0+jA+hOnTZrAoip7 HQEm0/Ql0OmM7yvv4Ti+8Ym83KpfpSjs7MPIMh9Su3LC2M+KPzu1MWqKt0QL6elR oauPVmYfpW9g3CrCAxhkEEM5E4l5xbEDJL3q2V/2zpVV2O+IVDirKU6YbvvyaFkr pQ5G0eP5SClb3mO4DjJvD5mFdxtjeAZylGA7EKVqI4f2wqgxHqm5aiyOD46o7tmG xubnkxECAwEAAaOCAU8wggFLMB8GA1UdIwQYMBaAFMOc8/zTRgg0u85Gf688W/Pi CMtZMFcGCCsGAQUFBwEBBEswSTAfBggrBgEFBQcwAYYTaHR0cDovL2d2LnN5bWNk LmNvbTAmBggrBgEFBQcwAoYaaHR0cDovL2d2LnN5bWNiLmNvbS9ndi5jcnQwDgYD VR0PAQH/BAQDAgWgMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAeBgNV HREEFzAVghNhbWJpZW50Y29uY2VwdHMuY29tMCsGA1UdHwQkMCIwIKAeoByGGmh0 dHA6Ly9ndi5zeW1jYi5jb20vZ3YuY3JsMAwGA1UdEwEB/wQCMAAwRQYDVR0gBD4w PDA6BgpghkgBhvhFAQc2MCwwKgYIKwYBBQUHAgEWHmh0dHBzOi8vd3d3LnJhcGlk c3NsLmNvbS9sZWdhbDANBgkqhkiG9w0BAQsFAAOCAQEAAYEoigU9OSAwo9Xt+S7v 3ROfOdWbh7IaIlQXwC5lH4DZNfslRLjbaMrRCr9fl+ub7XDpD/N4HnbKc7wm/+3x +AHBQXjVyWJtVCLd2HixPrPme0qbfKHB/waRy+wNkAtub/QbRt4yRItAl2sdXCjL a2Q7XL+y7I9CNVuc9Cn/4EEaAVZ53LHNSzI0b4OcUA25d8JCASPHo0cYzV7k7M6k QdmIklL/Od36ok1YICzMuIqij2ygXD6704VfbGL38jEakfj/+eAKHWv2IbCUMrpy F9u6V+K3AcPwbT0fzWpdBvSKI1rCVWCFPj0a/jmmIhSpo3/eaqIGIKfBWkK/zIkh /w== -----END CERTIFICATE----- INTERMEDIATE CA: --------------------------------------- -----BEGIN CERTIFICATE----- MIIEJTCCAw2gAwIBAgIDAjp3MA0GCSqGSIb3DQEBCwUAMEIxCzAJBgNVBAYTAlVT Ln 61 / 61 Col 26 Sel 0 Sel Ln 0 3.26 KB ANSI CR+LF INS Default Text	From the link to install the certificate, copy the certificate text starting at *Web Server CERTIFICATE* to *—END CERTIFICATE—* and paste the text into a Notepad file. Save and name the Notepad file as **certificates.cer**. Save a copy of this file to C:\temp\ on the *Metasys* server that hosts the *Metasys* software.
3.	**Figure 57: IIS Server Certificates**  Internet Information Services (IIS) Manager F-S12R2-4 File View Help Connections Start Page F-S12R2-4 (F-S12R2-4\labs) F-S12R2-4 Home Filter: Go Show All Group by: Area ASP.NET .NET Authorizat... .NET Compilation .NET Error Pages .NET Globalization .NET Trust Levels Application Settings Connection Strings Machine Key Pages and Controls Providers Session State SMTP E-mail IIS Authentic... Compression Default Document Directory Browsing Error Pages Handler Mappings HTTP Respon... ISAPI and CGI Restri... ISAPI Filters Logging MIME Types Modules Output Caching Request Filtering Server Certificates Worker Processes Management Features View Content View Actions Open Feature Manage Server Restart Start Stop View Application Pools View Sites Change .NET Framework Version Get New Web Platform Components Help	On the *Metasys* server hosting the *Metasys* UI, or the SCT computer hosting the *Metasys* UI Offline, browse to open Control Panel. On Control Panel, click **System and Security** > **Administrative Tools**. In Administrative Tools, double-click **Internet Information Services (IIS) Manager**. The IIS Manager window appears. Double-click **Server Certificates**.

Table 28: Installing the Security Certificate

<table>
<tr><td>4.</td><td>

Figure 58: Complete Certificate Request


Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Enable Automatic Rebind of Renewed Certificate
Help

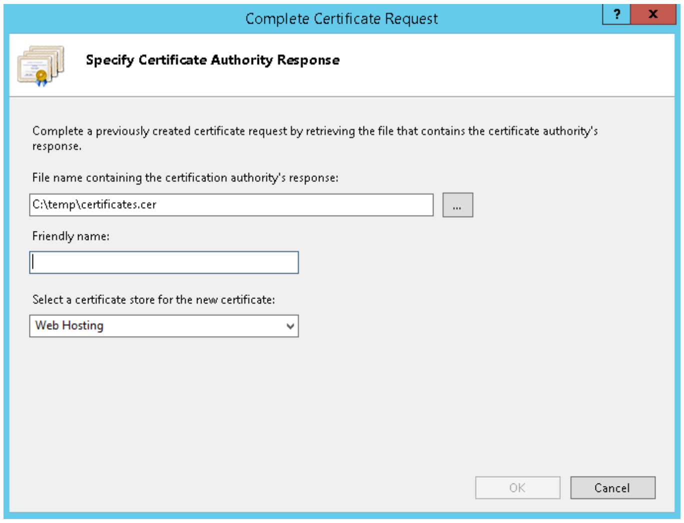
</td><td>

In the Actions pane, click **Complete Certificate Request**.

The Complete Certificate Request wizard opens.

</td></tr>
<tr><td>5.</td><td>

Figure 59: Specify Certificate Authority Response



Specify Certificate Authority Response

Complete a previously created certificate request by retrieving the file that contains the certificate authority's response.

File name containing the certification authority's response: C:\temp\certificates.cer ...

Friendly name:

Select a certificate store for the new certificate: Web Hosting

</td><td>

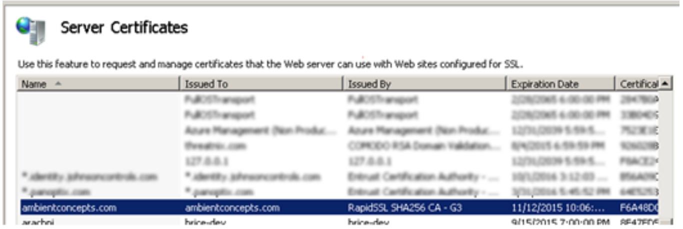
In the Specify Certificate Authority Response window, enter the following information:

- **File Name containing the certification authority's response:** click the browse button to select the certificates.cer file you saved in Step 5 of *Creating the Certificate Request*.
- **Friendly name:** enter the Common Name you entered in Step 3 from *Creating the Certificate Request*.
- **Select a certificate store for the new certificate:** choose Web Hosting from the drop-down list.
Note: The Personal option is typically used for client certificates and is not applicable to this certificate implementation.

Click **OK**. The Complete Certificate Request wizard closes.

</td></tr>
<tr><td>6.</td><td>

Figure 60: Server Certificates Listed



Server Certificates

Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.

<table>
<tr><th>Name</th><th>Issued To</th><th>Issued By</th><th>Expiration Date</th><th>Certifica</th></tr>
<tr><td></td><td>FullOSTransport</td><td>FullOSTransport</td><td>2/28/2065 6:00:00 PM</td><td>[illegible]</td></tr>
<tr><td></td><td>FullOSTransport</td><td>FullOSTransport</td><td>2/28/2065 6:00:00 PM</td><td>[illegible]</td></tr>
<tr><td></td><td>Azure Management (Non Produc...</td><td>Azure Management (Non Produc...</td><td>12/31/2039 5:59:5...</td><td>7523E1E</td></tr>
<tr><td></td><td>threatnix.com</td><td>COMODO RSA Domain Validation...</td><td>8/4/2015 6:59:59 PM</td><td>[illegible]</td></tr>
<tr><td></td><td>127.0.0.1</td><td>127.0.0.1</td><td>12/31/2039 5:59:5...</td><td>F9ACE2</td></tr>
<tr><td>*.identity.johnsoncontrols.com</td><td>*.identity.johnsoncontrols.com</td><td>Entrust Certification Authority - ...</td><td>10/1/2016 3:12:03 ...</td><td>[illegible]</td></tr>
<tr><td>*.panoptix.com</td><td>*.panoptix.com</td><td>Entrust Certification Authority - ...</td><td>3/31/2016 5:45:52 PM</td><td>[illegible]</td></tr>
<tr><td>ambientconcepts.com</td><td>ambientconcepts.com</td><td>RapidSSL SHA256 CA - G3</td><td>11/12/2015 10:06:...</td><td>F6A48D</td></tr>
<tr><td>arachni</td><td>brice-dev</td><td>brice-dev</td><td>9/15/2015 7:00:00 PM</td><td>8E47FD</td></tr>
</table>

</td><td>

Verify that the Server Certificate now appears in the list of Server Certificates.

The next step is to bind the security certificate to the default website.

</td></tr>
</table>

Table 28: Installing the Security Certificate

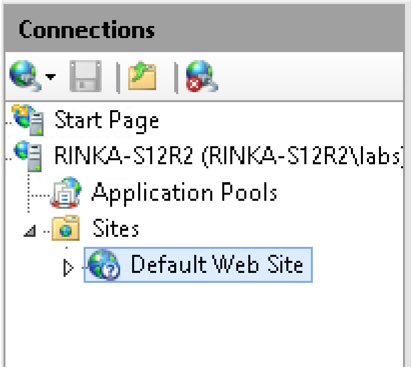
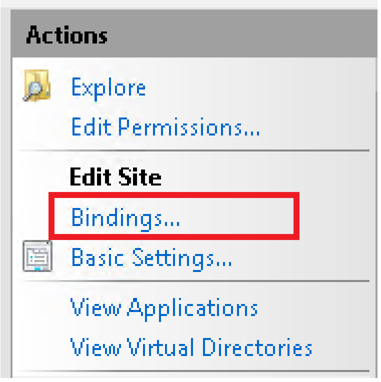
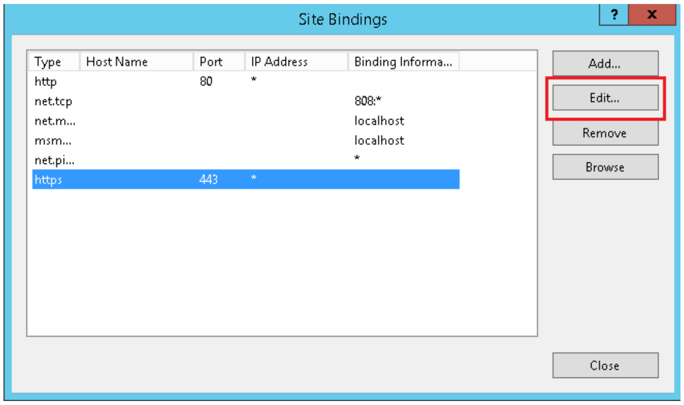
7.	**Figure 61: Default Web Site Selected**  Connections Start Page RINKA-S12R2 (RINKA-S12R2\labs) Application Pools Sites Default Web Site	In the IIS window, expand the tree in the left pane and select Default Web Site.
8.	**Figure 62: Bindings**  Actions Explore Edit Permissions... Edit Site Bindings... Basic Settings... View Applications View Virtual Directories	In the right pane under Actions, click **Bindings**. The Site Bindings window appears.

Table 28: Installing the Security Certificate

<table>
<tr><td>9.</td><td>

Figure 63: Edit Site Bindings



Site Bindings

<table>
<tr><th>Type</th><th>Host Name</th><th>Port</th><th>IP Address</th><th>Binding Informa...</th></tr>
<tr><td>http</td><td></td><td>80</td><td>*</td><td></td></tr>
<tr><td>net.tcp</td><td></td><td></td><td></td><td>808:*</td></tr>
<tr><td>net.m...</td><td></td><td></td><td></td><td>localhost</td></tr>
<tr><td>msm...</td><td></td><td></td><td></td><td>localhost</td></tr>
<tr><td>net.pi...</td><td></td><td></td><td></td><td>*</td></tr>
<tr><td>https</td><td></td><td>443</td><td>*</td><td></td></tr>
</table>

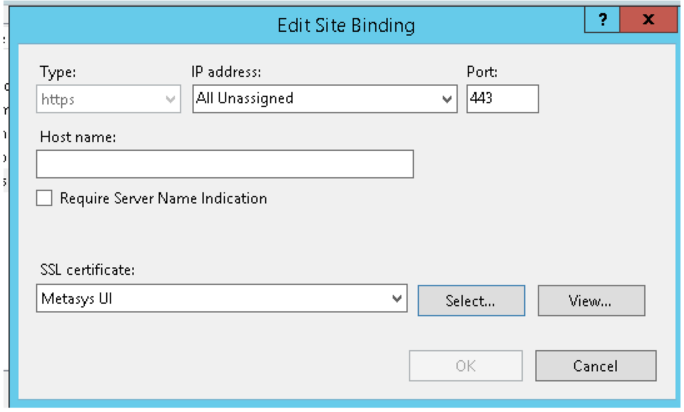
</td><td>

In the Site Bindings window, select the https entry for Port 443.

Click **Edit**.

</td></tr>
<tr><td>10.</td><td>

Figure 64: Select SSL Certificate



Edit Site Binding

Type: https

IP address: All Unassigned

Port: 443

Host name:

□ Require Server Name Indication

SSL certificate: Metasys UI

</td><td>

In the SSL certificate drop-down list, select the security certificate. Click **OK**.

Note: Ensure that you select the certificate that lists the Friendly Name you specified in *Step 5*.

You should now be able to browse to your *Metasys* UI or *Metasys* UI Offline without certificate warnings.

</td></tr>
</table>

Self-Signed SSL Certificates

Implementing A Self-Signed Certificate on Client Devices

Follow these instructions to install a self-signed certificate on client devices.

Creating a Self-Signed Certificate

1. On a Windows OS, open Control Panel and click **Network and Security** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.
2. In the left pane, select the computer name.
3. Double-click **Server Certificates**.
4. In the Actions panel, click **Create Self-Signed Certificate**. The Create Self-Signed Certificate wizard appears.
5. In the Specify Friendly Name window, enter a friendly name for the certificate and select a certificate store for the new certificate (Personal or Web Hosting).
6. Click **OK**.

Exporting a Self-Signed Certificate for Client Devices

1. In the Actions Panel of the Internet Information Services (IIS) Manager, click **Export**. The Export Certificate window appears.

2. Select a location to export the certificate.
3. Enter and confirm a password for the certificate.
4. Click **OK**.

Importing a Self-Signed Certificate on an Android OS Device with Google® Chrome™

1. Ensure that you have access to the exported Self-Signed SSL certificate from your device (for example, a microSD card, as an attachment in an email, in cloud-based storage, or in another location).
2. Go to **Settings** > **System** > **Security** on your Android device.
3. In the Credential Storage section, tap **Install from phone storage**.

Importing a Self-Signed Certificate on an iOS® Device on Apple® Safari®

Note: If you browse to the *Metasys* UI or *Metasys* UI Offline site before you implement a security certificate on your iOS device, we recommend that you do not tap or click the Continue option in the **Cannot Verify Server Identity** window in Safari. Doing so adds an exception that prevents Safari from warning you about the site in the future.

1. Ensure that you have access to the exported Self-Signed certificate from your device as an attachment in an email.
2. Open the email message that has the Self-Signed certificate attached.
3. Install the certificate. You can verify that the certificate installed by going to **Settings** > **General** > **Profiles**.

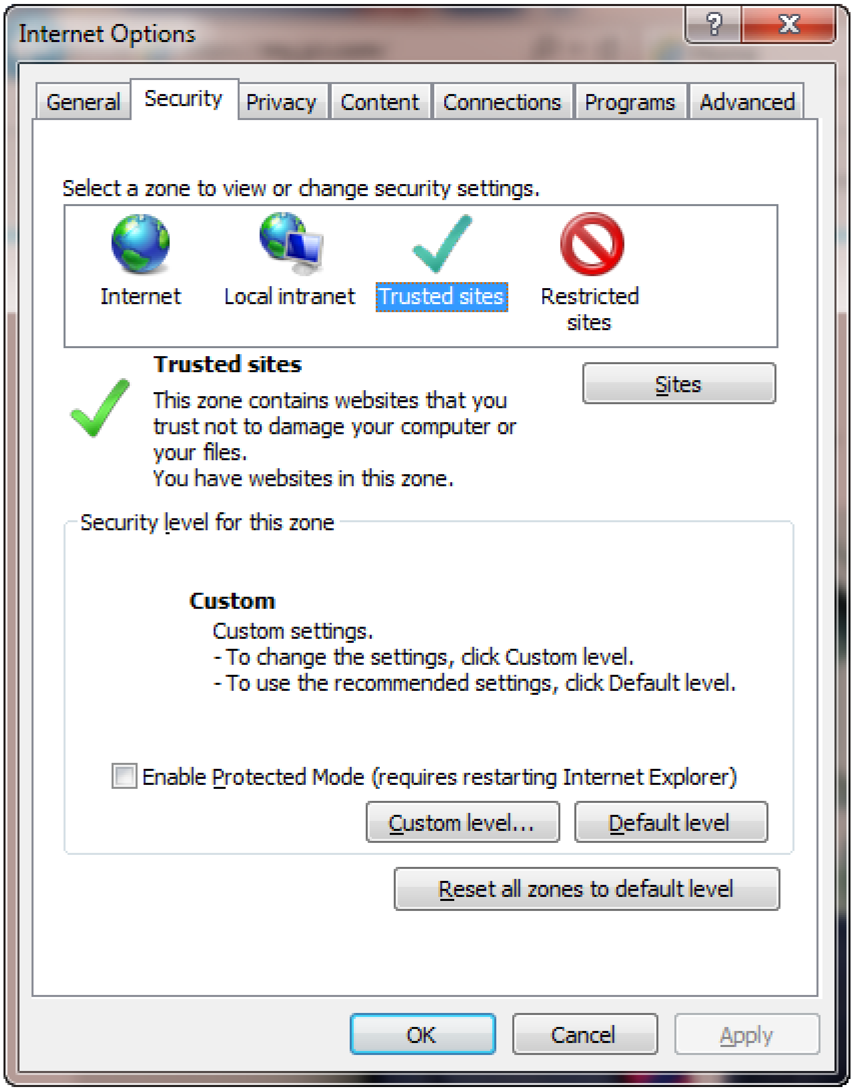
Trusted Sites

Adding the *Metasys* UI or *Metasys* UI Offline as a Trusted Site – Internet Explorer

To add the *Metasys* UI or *Metasys* UI Offline as a trusted site for Windows® Internet Explorer® 10 or 11:

1. Open Internet Explorer. Click ⚙ (Tools menu).
2. Click **Internet options**.
3. Select the Security tab.
4. Select Trusted Sites and click **Sites**.

Figure 65: Internet Options



Select a zone to view or change security settings.

Trusted sites

This zone contains websites that you trust not to damage your computer or your files.
You have websites in this zone.

Security level for this zone

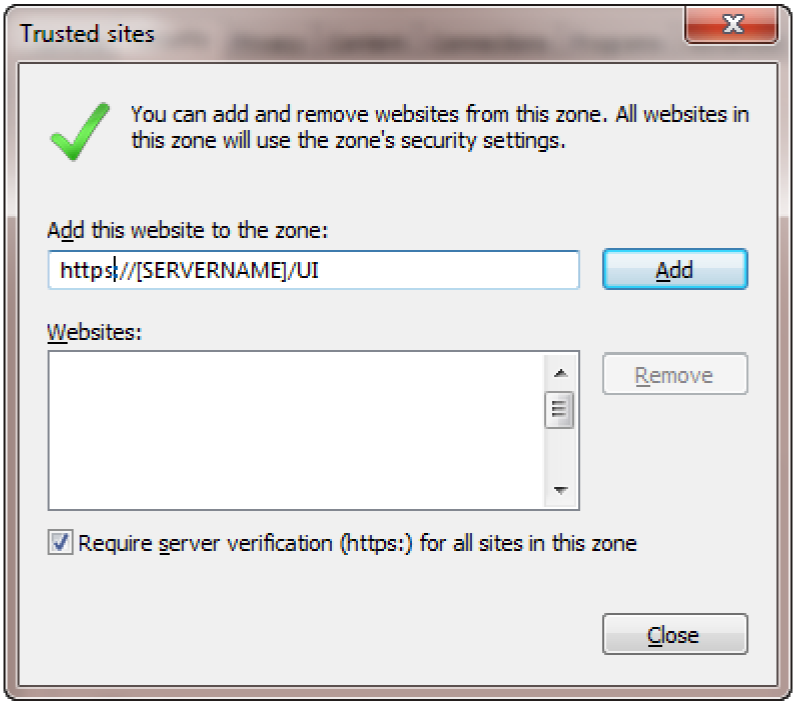
Custom

Custom settings.
- To change the settings, click Custom level.
- To use the recommended settings, click Default level.

☐ Enable Protected Mode (requires restarting Internet Explorer)

5. In the **Add this website to the zone** field, enter the *Metasys* UI or *Metasys* UI Offline site address.

Figure 66: Trusted Sites



Trusted sites

You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone: https://[SERVERNAME]/UI

Websites:

☑ Require server verification (https:) for all sites in this zone

6. Click **Add**.
7. Click **Close**.
8. Click **OK**.

Adding the *Metasys* UI or *Metasys* UI Offline as a Trusted Site – Google Chrome

To add the *Metasys* UI or *Metasys* UI Offline as a trusted site for Google Chrome:

1. Open Google Chrome. Click ≡.
2. Click **Settings**.
3. Scroll to the bottom of the page and click **Show advanced settings**.
4. Under the Network section, click **Change proxy settings**. The Internet Options window appears.
5. Select the Security tab.
6. Select Trusted Sites and click **Sites**.
7. In the **Add this website to the zone** field, enter the *Metasys* UI or *Metasys* UI Offline site address.
8. Click **Close**.
9. Click **OK**.

Adding the *Metasys* UI or *Metasys* UI Offline Sites as a Top Site – Apple Safari

To add the *Metasys* UI or *Metasys* UI Offline as Top Sites (trusted site) for Apple Safari 8 or later:

1. Open Apple Safari and browse to the *Metasys* UI or *Metasys* UI Offline.
2. Tap or click **Bookmarks**.
3. Select **Add Bookmark**.
4. Choose Top Sites.

5. Click **Add**.

Appendix: Installing Antivirus Software

Follow the steps in this appendix for installing antivirus software on computers that run ADS/ADX or SCT software. We recommend one of the following antivirus software programs:

- Symantec® Endpoint Protection software Corporate Edition version 12.0 or later
- McAfee® VirusScan® Enterprise version 8.8 with Patch 3 or Patch 5 (Patch 4 is **not** compatible).

Note: Windows Defender, provided by some Microsoft operating systems, **is not** supported on a computer that is running ADS/ADX or SCT software. Make sure you turn off Windows Defender before bringing the system online.

Installing and Configuring Symantec® Endpoint Protection Software

Symantec Endpoint Protection software at version 12.0 is permitted on computers that run ADS/ADX or SCT software. You may install Symantec Endpoint Protection software on a *Metasys* system in a unified, split, or virtual machine 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 software and supervisory devices. Follow the steps in this section to properly install and configure this software.

Table 29: Symantec Endpoint Protection Installation

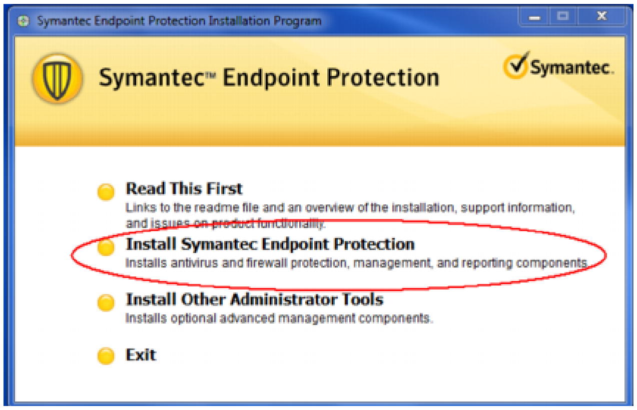
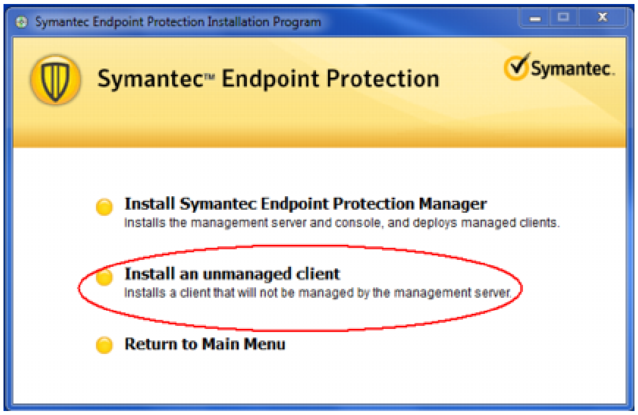
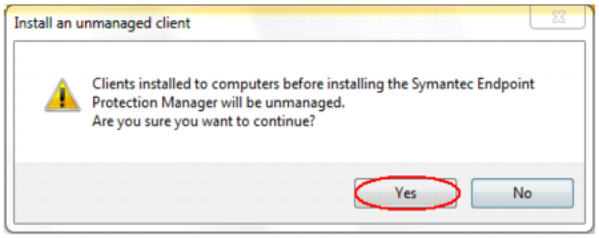
1.	**Start**	If you have already installed Symantec Endpoint Protection, go to Step 16. If you have not yet installed Symantec Endpoint Protection software, start the Symantec Endpoint Protection software installation. The Symantec Endpoint Protection welcome screen appears.
2.	**Figure 67: Welcome Screen**  Symantec Endpoint Protection Installation Program Symantec™ Endpoint Protection Symantec. Read This First Links to the readme file and an overview of the installation, support information, and issues on product functionality. Install Symantec Endpoint Protection Installs antivirus and firewall protection, management, and reporting components. Install Other Administrator Tools Installs optional advanced management components. Exit	Select **Install Symantec Endpoint Protection**.
3.	**Figure 68: Install an Unmanaged Client**  Symantec Endpoint Protection Installation Program Symantec™ Endpoint Protection Symantec. Install Symantec Endpoint Protection Manager Installs the management server and console, and deploys managed clients. Install an unmanaged client Installs a client that will not be managed by the management server. Return to Main Menu	Select **Install an unmanaged client**. A Question box appears regarding installation as an unmanaged client. Click **Yes** to continue. **Figure 69: Question About Installing an Unmanaged Client**  Install an unmanaged client Clients installed to computers before installing the Symantec Endpoint Protection Manager will be unmanaged. Are you sure you want to continue? Yes No

Table 29: Symantec Endpoint Protection Installation

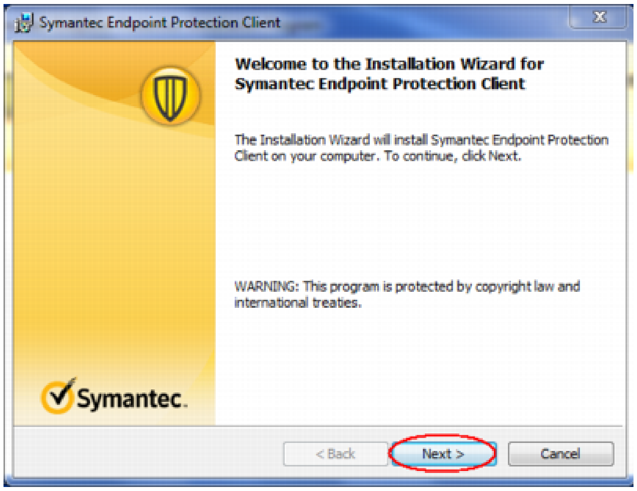
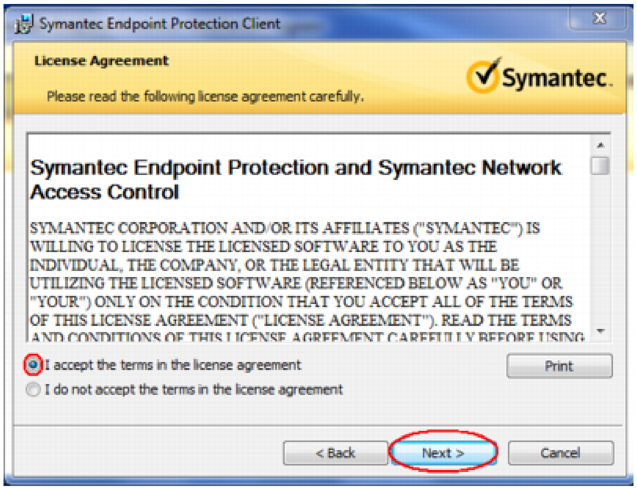
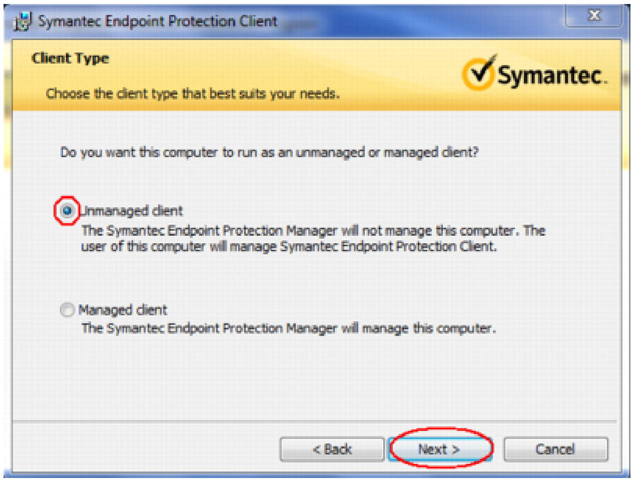
4.	**Figure 70: Installation Wizard Welcome Screen**  Symantec Endpoint Protection Client **Welcome to the Installation Wizard for Symantec Endpoint Protection Client** The Installation Wizard will install Symantec Endpoint Protection Client on your computer. To continue, click Next. WARNING: This program is protected by copyright law and international treaties. 	Click **Next**.
5.	**Figure 71: License Agreement Screen**  Symantec Endpoint Protection Client **License Agreement** Please read the following license agreement carefully. Symantec Endpoint Protection and Symantec Network Access Control SYMANTEC CORPORATION AND/OR ITS AFFILIATES ("SYMANTEC") IS WILLING TO LICENSE THE LICENSED SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE LICENSED SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT ("LICENSE AGREEMENT"). READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING ● I accept the terms in the license agreement ○ I do not accept the terms in the license agreement 	Review and accept the license agreement. Click **Next**.
6.	**Figure 72: Client Type Screen**  Symantec Endpoint Protection Client **Client Type** Choose the client type that best suits your needs. Do you want this computer to run as an unmanaged or managed client? ● Unmanaged client The Symantec Endpoint Protection Manager will not manage this computer. The user of this computer will manage Symantec Endpoint Protection Client. ○ Managed client The Symantec Endpoint Protection Manager will manage this computer. 	Select **Unmanaged client** and click **Next**. **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 user interface from working correctly.

Table 29: Symantec Endpoint Protection Installation

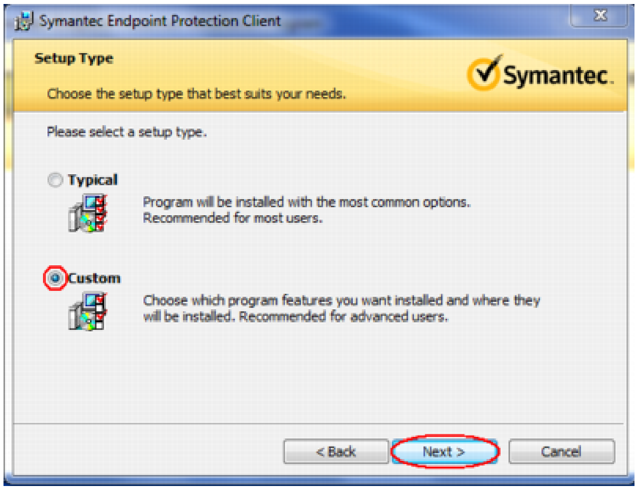
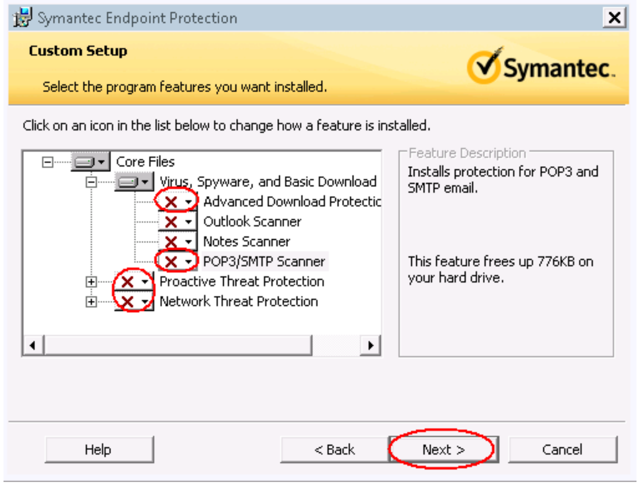
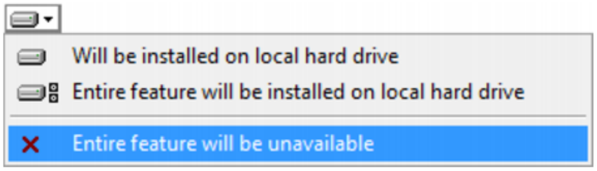
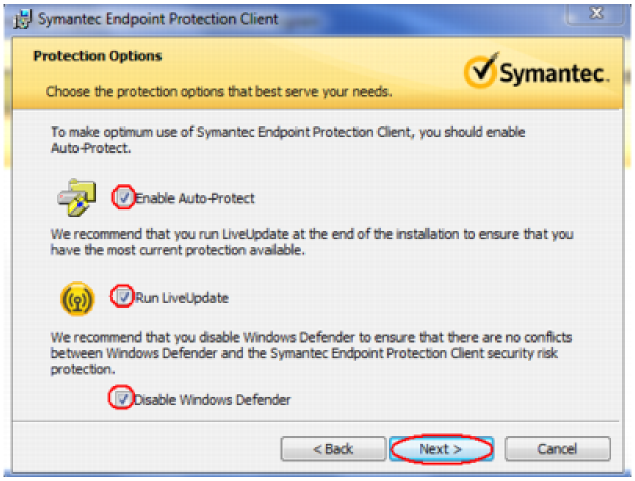
7.	**Figure 73: Setup Type Screen**  Symantec Endpoint Protection Client **Setup Type** Choose the setup type that best suits your needs. Please select a setup type. ○ **Typical** Program will be installed with the most common options. Recommended for most users. ● **Custom** Choose which program features you want installed and where they will be installed. Recommended for advanced users. 	Select **Custom** and click **Next**.
8.	**Figure 74: Custom Setup Screen**  Symantec Endpoint Protection **Custom Setup** Select the program features you want installed. Click on an icon in the list below to change how a feature is installed. Core Files Virus, Spyware, and Basic Download ✗ Advanced Download Protectic ✗ Outlook Scanner ✗ Notes Scanner ✗ POP3/SMTP Scanner ✗ Proactive Threat Protection ✗ Network Threat Protection Feature Description Installs protection for POP3 and SMTP email. This feature frees up 776KB on your hard drive. 	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**. Click **Next**. **Figure 75: Disabling Features**  Will be installed on local hard drive Entire feature will be installed on local hard drive ✗ Entire feature will be unavailable
9.	**Figure 76: Protection Options Screen**  Symantec Endpoint Protection Client **Protection Options** Choose the protection options that best serve your needs. To make optimum use of Symantec Endpoint Protection Client, you should enable Auto-Protect. ☑ Enable Auto-Protect We recommend that you run LiveUpdate at the end of the installation to ensure that you have the most current protection available. ☑ Run LiveUpdate We recommend that you disable Windows Defender to ensure that there are no conflicts between Windows Defender and the Symantec Endpoint Protection Client security risk protection. ☑ Disable Windows Defender 	Select all three protection options and click **Next**.

Table 29: Symantec Endpoint Protection Installation

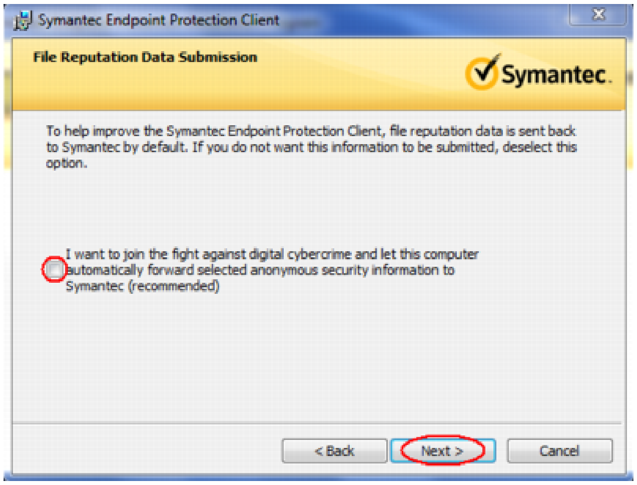
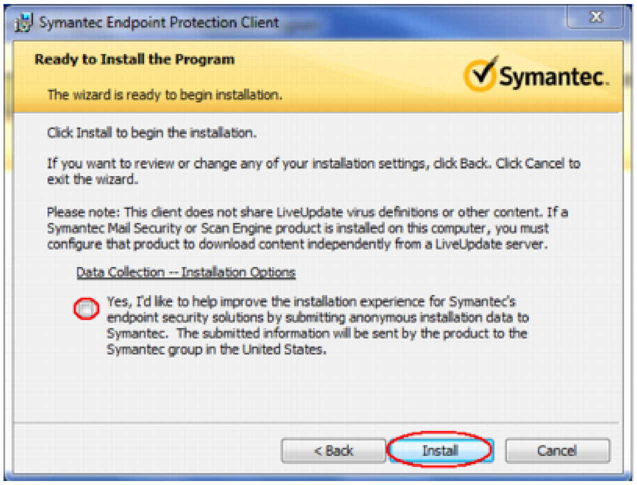
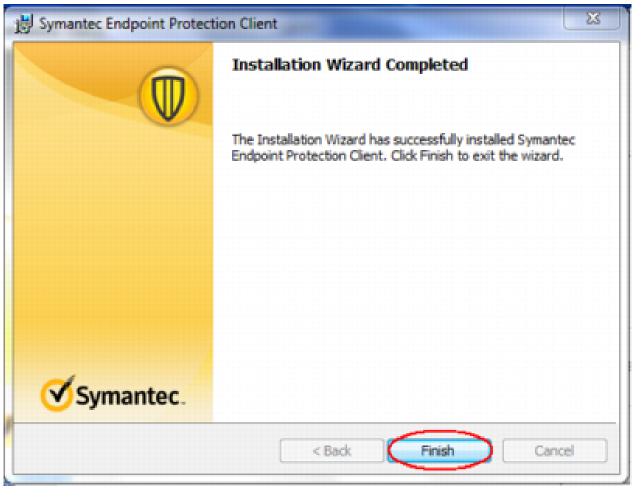
10.	**Figure 77: File Reputation Data Submission Screen**  Symantec Endpoint Protection Client **File Reputation Data Submission** To help improve the Symantec Endpoint Protection Client, file reputation data is sent back to Symantec by default. If you do not want this information to be submitted, deselect this option. □ I want to join the fight against digital cybercrime and let this computer automatically forward selected anonymous security information to Symantec (recommended) 	Do not select the File Reputation Data Submission check box. Click **Next**.
11.	**Figure 78: Data Collection Screen**  Symantec Endpoint Protection Client **Ready to Install the Program** The wizard is ready to begin installation. Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard. Please note: This client does not share LiveUpdate virus definitions or other content. If a Symantec Mail Security or Scan Engine product is installed on this computer, you must configure that product to download content independently from a LiveUpdate server. Data Collection -- Installation Options □ Yes, I'd like to help improve the installation experience for Symantec's endpoint security solutions by submitting anonymous installation data to Symantec. The submitted information will be sent by the product to the Symantec group in the United States. 	Do not select the check box under Data Collection -- Installation Options. Click **Install**.
12.	**Figure 79: Wizard Completed Screen**  Symantec Endpoint Protection Client **Installation Wizard Completed** The Installation Wizard has successfully installed Symantec Endpoint Protection Client. Click Finish to exit the wizard. 	Click **Finish**.

Table 29: Symantec Endpoint Protection Installation

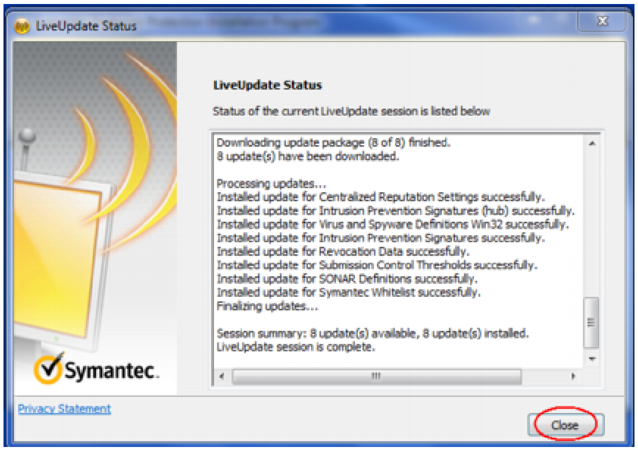
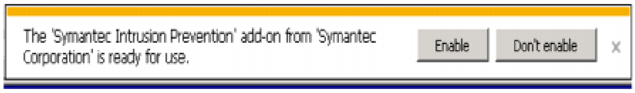
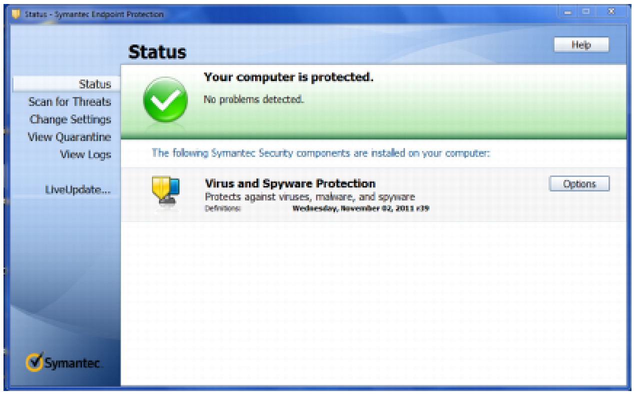
13.	**Figure 80: LiveUpdate Status Screen**  LiveUpdate Status Symantec. Privacy Statement Close **LiveUpdate Status** Status of the current LiveUpdate session is listed below Downloading update package (8 of 8) finished. 8 update(s) have been downloaded. Processing updates... Installed update for Centralized Reputation Settings successfully. Installed update for Intrusion Prevention Signatures (hub) successfully. Installed update for Virus and Spyware Definitions Win32 successfully. Installed update for Intrusion Prevention Signatures successfully. Installed update for Revocation Data successfully. Installed update for Submission Control Thresholds successfully. Installed update for SONAR Definitions successfully. Installed update for Symantec Whitelist successfully. Finalizing updates... Session summary: 8 update(s) available, 8 update(s) installed. LiveUpdate session is complete.	After the installation completes, the LiveUpdate process starts. The update process may take several minutes to complete. Do not stop the process. When the **Live Update session is complete** message appears in the status window, click **Close**.
14.		Restart the computer.
15.	**Figure 81: Symantec Intrusion Prevention Pop-up Message**  The 'Symantec Intrusion Prevention' add-on from 'Symantec Corporation' is ready for use. 	Open the Internet Explorer® web browser. A Symantec Intrusion Prevention message appears. Click **Don't enable**. Go to Step 27.
16.	**Figure 82: Symantec Endpoint Protection Icon** 	Double-click the Symantec Endpoint Protection icon in the Windows task bar. The Status screen appears.
17.	**Figure 83: Proactive Threat Protection and Network Threat Protection Not Installed**  Status - Symantec Endpoint Protection Status Help Status Scan for Threats Change Settings View Quarantine View Logs LiveUpdate... Options Symantec. **Your computer is protected.** No problems detected. The following Symantec Security components are installed on your computer: **Virus and Spyware Protection** Protects against viruses, malware, and spyware Definitions: **Wednesday, November 02, 2011 r39**	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. Go to Step 27.

Table 29: Symantec Endpoint Protection Installation

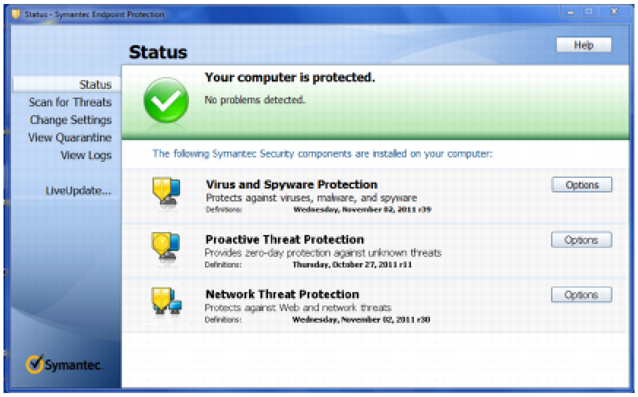
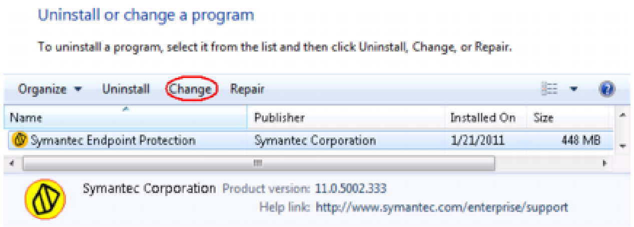
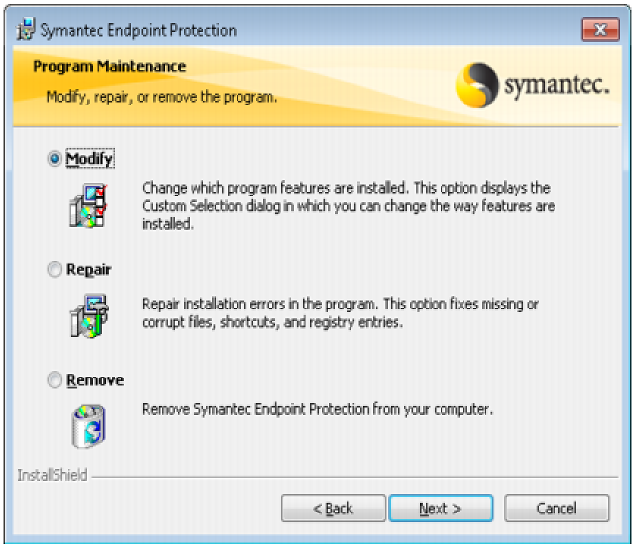
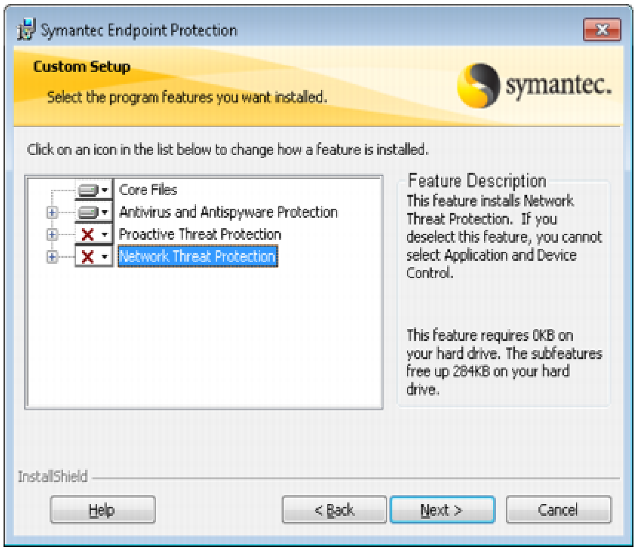
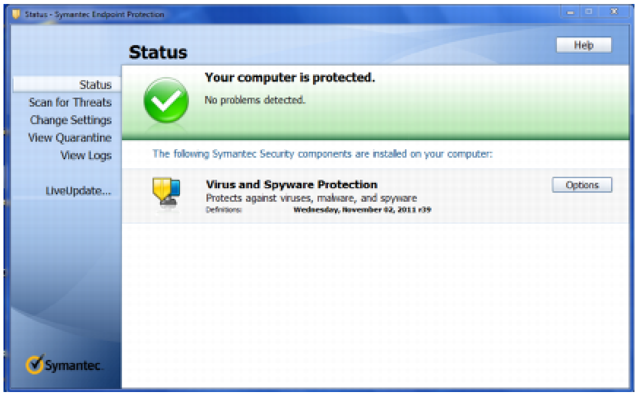
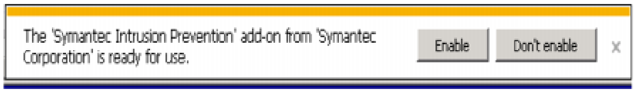
18.	**Figure 84: Proactive Threat Protection and Network Threat Protection Incorrectly Installed**  Status - Symantec Endpoint Protection Status Your computer is protected. No problems detected. The following Symantec Security components are installed on your computer: Virus and Spyware Protection Protects against viruses, malware, and spyware Definitions: Wednesday, November 02, 2011 r39 Proactive Threat Protection Provides zero-day protection against unknown threats Definitions: Thursday, October 27, 2011 r11 Network Threat Protection Protects against Web and network threats Definitions: Wednesday, November 02, 2011 r30 Help Status Scan for Threats Change Settings View Quarantine View Logs LiveUpdate... Options Options Options Symantec	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. Go to Step 19.
19.		In Control Panel, select Programs > Programs and Features. Click **Symantec Endpoint Protection** in the list of installed programs.
20.	**Figure 85: Change Program**  Uninstall or change a program To uninstall a program, select it from the list and then click Uninstall, Change, or Repair. Name / Publisher / Installed On / Size Symantec Endpoint Protection / Symantec Corporation / 1/21/2011 / 448 MB Symantec Corporation Product version: 11.0.5002.333 Help link: http://www.symantec.com/enterprise/support 	Click **Change** to start the InstallShield Wizard for Symantec Endpoint Protection.
21.	**Figure 86: Program Maintenance**  Symantec Endpoint Protection Program Maintenance Modify, repair, or remove the program. ● Modify Change which program features are installed. This option displays the Custom Selection dialog in which you can change the way features are installed. ○ Repair Repair installation errors in the program. This option fixes missing or corrupt files, shortcuts, and registry entries. ○ Remove Remove Symantec Endpoint Protection from your computer. 	When you reach the Program Maintenance screen, select **Modify**. Click **Next**. The Custom Setup screen appears.

Table 29: Symantec Endpoint Protection Installation

22.	**Figure 87: Custom Setup**  Symantec Endpoint Protection **Custom Setup** Select the program features you want installed. Click on an icon in the list below to change how a feature is installed. Core Files Antivirus and Antispyware Protection Proactive Threat Protection Network Threat Protection Feature Description This feature installs Network Threat Protection. If you deselect this feature, you cannot select Application and Device Control. This feature requires 0KB on your hard drive. The subfeatures free up 284KB on your hard drive. symantec. InstallShield Help < Back Next > Cancel	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.
23.		Click **Next**. Complete the steps in the installation wizard.
24.		Restart the computer.
25.	**Figure 88: Proactive Threat Protection and Network Threat Protection Not Installed**  Status - Symantec Endpoint Protection **Status** **Your computer is protected.** No problems detected. The following Symantec Security components are installed on your computer: **Virus and Spyware Protection** Protects against viruses, malware, and spyware Definitions: Wednesday, November 02, 2011 r39 Help Status Scan for Threats Change Settings View Quarantine View Logs LiveUpdate... Options Symantec.	When the computer restarts, log in and open the Symantec Endpoint Protection Status screen to verify that the Proactive Threat Protection and Network Threat Protection features do not appear.
26.	**Figure 89: Symantec Intrusion Prevention Pop-up Message**  The 'Symantec Intrusion Prevention' add-on from 'Symantec Corporation' is ready for use. 	Open the Internet Explorer web browser. A Symantec Intrusion Prevention message appears. Click **Don't enable**.
27.	**Done.**	

Installing and Configuring McAfee VirusScan Enterprise Software

McAfee VirusScan Enterprise version 8.8 with Patch 3 or Patch 5 is permitted on computers that run ADS/ADX or SCT software. You may install McAfee anti-virus software on a *Metasys* system in a unified, split, or virtual machine configuration.

Important:	Use only McAfee VirusScan Enterprise software version 8.8 with **Patch 3 or Patch 5** on your Windows 10, Windows 8.1, Windows 7, Windows Server 2012 R2, Windows Server 2012, or Windows Server 2008 R2 computer. McAfee VirusScan Enterprise software version with Patch 4 causes software operational issues.

We recommend installing McAfee VirusScan Enterprise software using the steps in *Table 30*. If you deviate from these steps, 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.

Table 30: McAfee Virus Scan Enterprise Installation

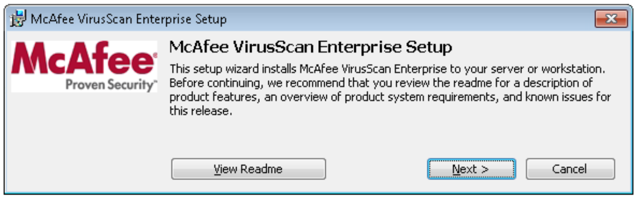
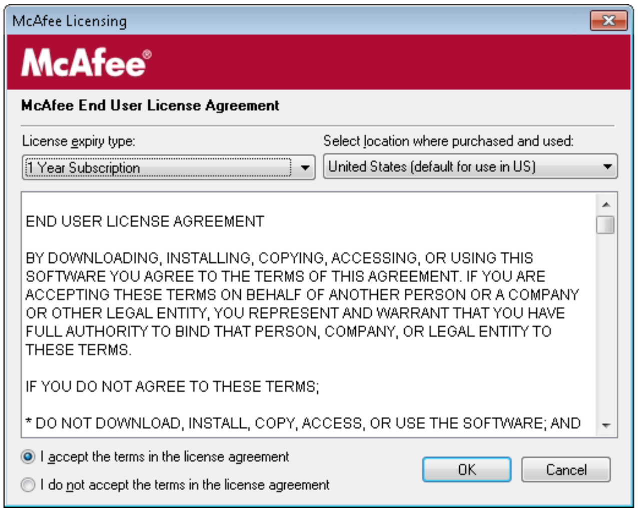
1.	**Start**	Start the McAfee Virus Scan Enterprise software installation. The McAfee VirusScan Enterprise Setup screen appears.
2.	**Figure 90: McAfee VirusScan Setup**  McAfee VirusScan Enterprise Setup McAfee VirusScan Enterprise Setup This setup wizard installs McAfee VirusScan Enterprise to your server or workstation. Before continuing, we recommend that you review the readme for a description of product features, an overview of product system requirements, and known issues for this release. McAfee Proven Security View Readme Next > Cancel	Click **Next**.
3.	**Figure 91: McAfee End User License Agreement**  McAfee Licensing McAfee End User License Agreement License expiry type: 1 Year Subscription Select location where purchased and used: United States (default for use in US) END USER LICENSE AGREEMENT BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, OR USING THIS SOFTWARE YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF ANOTHER PERSON OR A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND THAT PERSON, COMPANY, OR LEGAL ENTITY TO THESE TERMS. IF YOU DO NOT AGREE TO THESE TERMS; * DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, OR USE THE SOFTWARE; AND ● I accept the terms in the license agreement ○ I do not accept the terms in the license agreement 	Accept the licensing agreement and click **OK**.

Table 30: McAfee Virus Scan Enterprise Installation

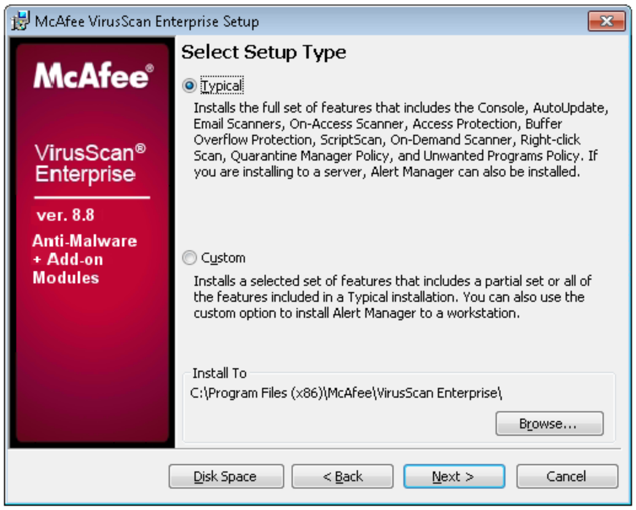
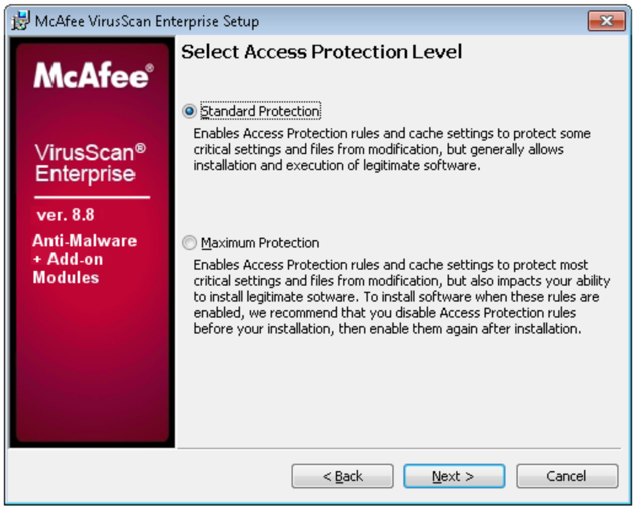
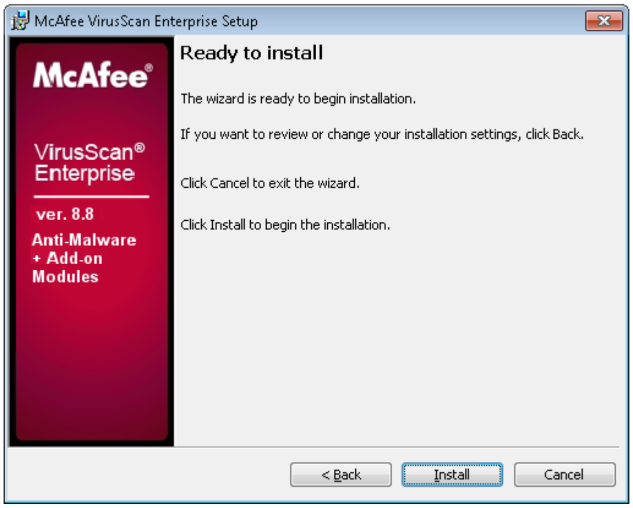
4.	**Figure 92: Select Setup Type**  McAfee VirusScan Enterprise Setup Select Setup Type ● Typical Installs the full set of features that includes the Console, AutoUpdate, Email Scanners, On-Access Scanner, Access Protection, Buffer Overflow Protection, ScriptScan, On-Demand Scanner, Right-click Scan, Quarantine Manager Policy, and Unwanted Programs Policy. If you are installing to a server, Alert Manager can also be installed. ○ Custom Installs a selected set of features that includes a partial set or all of the features included in a Typical installation. You can also use the custom option to install Alert Manager to a workstation. Install To C:\Program Files (x86)\McAfee\VirusScan Enterprise\\ McAfee VirusScan® Enterprise ver. 8.8 Anti-Malware + Add-on Modules Browse... Disk Space < Back Next > Cancel	Select **Typical**. Click **Next**.
5.	**Figure 93: Select Access Protection Level**  McAfee VirusScan Enterprise Setup Select Access Protection Level ● Standard Protection Enables Access Protection rules and cache settings to protect some critical settings and files from modification, but generally allows installation and execution of legitimate software. ○ Maximum Protection Enables Access Protection rules and cache settings to protect most critical settings and files from modification, but also impacts your ability to install legitimate sotware. To install software when these rules are enabled, we recommend that you disable Access Protection rules before your installation, then enable them again after installation. McAfee VirusScan® Enterprise ver. 8.8 Anti-Malware + Add-on Modules < Back Next > Cancel	Select **Standard Protection**. Click **Next**.
6.	**Figure 94: Ready to Install**  McAfee VirusScan Enterprise Setup Ready to install The wizard is ready to begin installation. If you want to review or change your installation settings, click Back. Click Cancel to exit the wizard. Click Install to begin the installation. McAfee VirusScan® Enterprise ver. 8.8 Anti-Malware + Add-on Modules < Back Install Cancel	Click **Install** to begin McAfee VirusScan Enterprise installation.

Table 30: McAfee Virus Scan Enterprise Installation

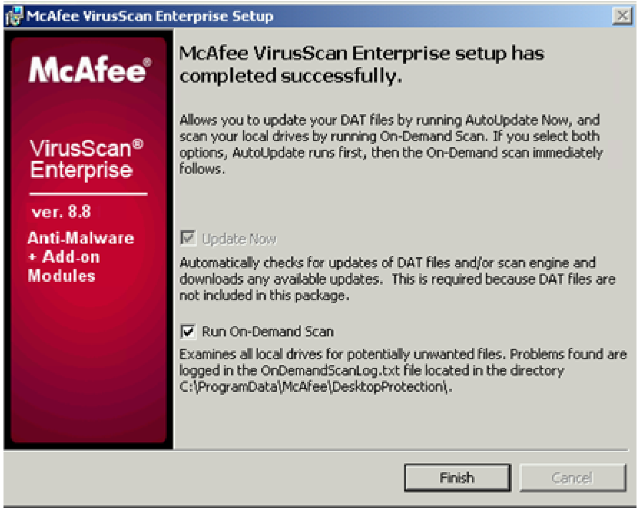
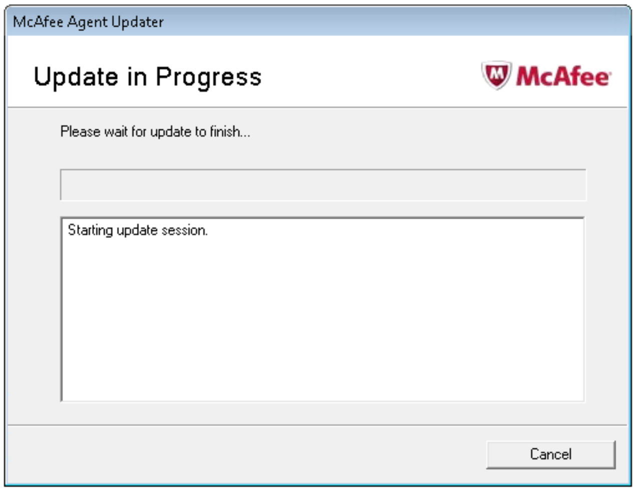
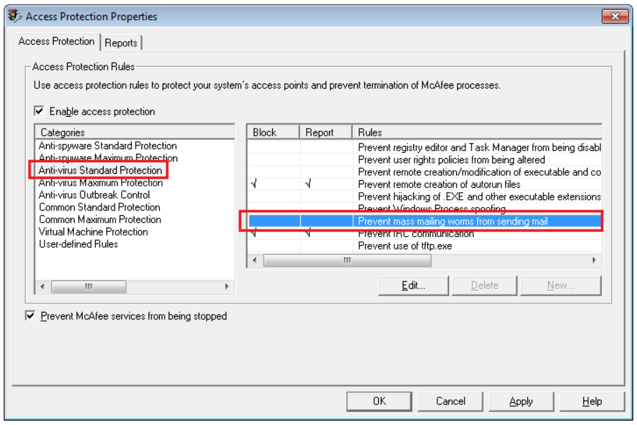
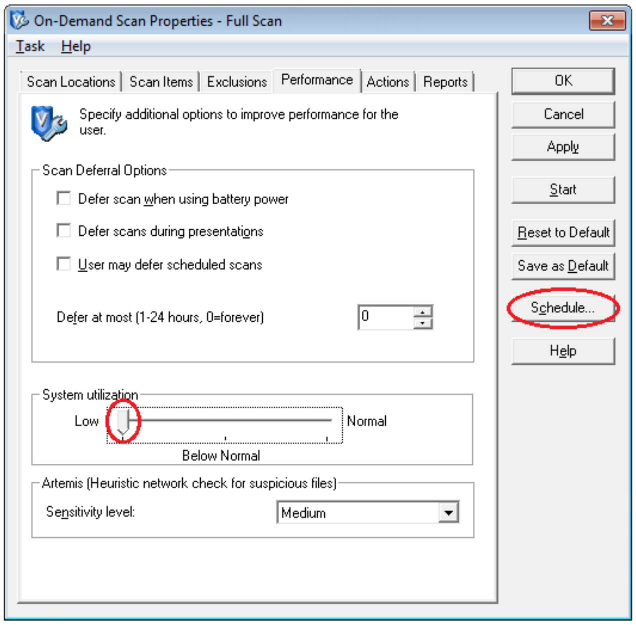
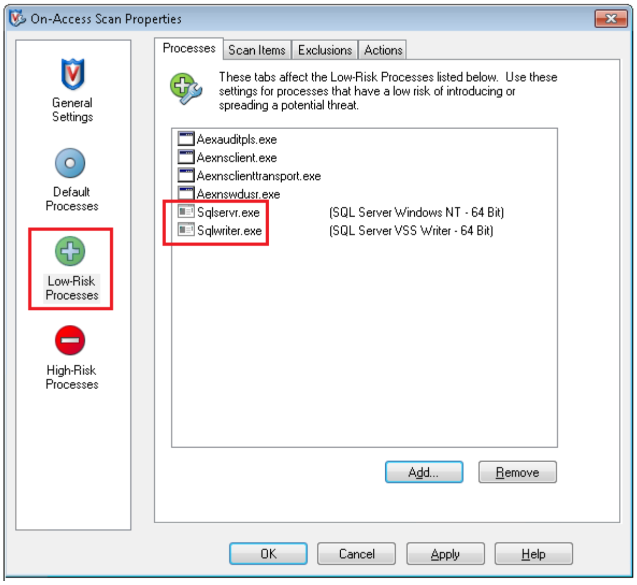
7.	**Figure 95: McAfee VirusScan Enterprise Setup Complete**  McAfee VirusScan Enterprise Setup McAfee® VirusScan® Enterprise ver. 8.8 Anti-Malware + Add-on Modules McAfee VirusScan Enterprise setup has completed successfully. Allows you to update your DAT files by running AutoUpdate Now, and scan your local drives by running On-Demand Scan. If you select both options, AutoUpdate runs first, then the On-Demand scan immediately follows. ☑ Update Now Automatically checks for updates of DAT files and/or scan engine and downloads any available updates. This is required because DAT files are not included in this package. ☑ Run On-Demand Scan Examines all local drives for potentially unwanted files. Problems found are logged in the OnDemandScanLog.txt file located in the directory C:\ProgramData\McAfee\DesktopProtection\. 	When setup is done, the completed successfully screen appears. Select **Run On-Demand Scan**. We recommend that you take the time now to run a full scan to ensure the computer is prepared for software. This process can take from 30 to 60 minutes to complete. Click **Next**.
8.	**Figure 96: McAfee Agent Updater**  McAfee Agent Updater Update in Progress Please wait for update to finish... Starting update session. 	The McAfee Agent Updater runs. Wait until the updater finishes. Click **Finish** on the McAfee setup complete window (*Figure 95*).
9.	**Figure 97: Access Protection Properties**  Access Protection Properties Access Protection Rules Use access protection rules to protect your system´s access points and prevent termination of McAfee processes. ☑ Enable access protection Categories Anti-spyware Standard Protection Anti-spyware Maximum Protection Anti-virus Standard Protection Anti-virus Maximum Protection Anti-virus Outbreak Control Common Standard Protection Common Maximum Protection Virtual Machine Protection User-defined Rules Block / Report / Rules Prevent registry editor and Task Manager from being disabl Prevent user rights policies from being altered Prevent remote creation/modification of executable and co √ √ Prevent remote creation of autorun files Prevent hijacking of .EXE and other executable extensions Prevent Windows Process spoofing Prevent mass mailing worms from sending mail √ √ Prevent IRC communication Prevent use of tftp.exe ☑ Prevent McAfee services from being stopped 	Right-click the McAfee icon in the task bar and click **VirusScan Console**. The VirusScan Console appears. Click **Task** > **Properties**. The Access Protection Properties window appears (*Figure 97*). 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. Click **OK**.

Table 30: McAfee Virus Scan Enterprise Installation

10.	**Figure 98: System Utilization**  On-Demand Scan Properties - Full Scan Task Help Scan Locations | Scan Items | Exclusions | Performance | Actions | Reports Specify additional options to improve performance for the user. Scan Deferral Options □ Defer scan when using battery power □ Defer scans during presentations □ User may defer scheduled scans Defer at most (1-24 hours, 0=forever) 0 System utilization: Low — Below Normal — Normal Artemis (Heuristic network check for suspicious files) Sensitivity level: Medium OK | Cancel | Apply | Start | Reset to Default | Save as Default | Schedule... | Help	On the VirusScan Console, right-click **Full Scan** and select **Properties**. The On-Demand Scan Properties-Full Scan window appears. Click the **Performance** tab. Under System utilization, slide the bar pointer to the **Low** setting (*Figure 98*). Click **Schedule**, and with the assistance of your local IT staff, define a daily scan schedule. Do not scan at midnight because the 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.
	Figure 99: Adding SQL Server as a Low-Risk Process  On-Access Scan Properties General Settings | Default Processes | Low-Risk Processes | High-Risk Processes Processes | Scan Items | Exclusions | Actions These tabs affect the Low-Risk Processes listed below. Use these settings for processes that have a low risk of introducing or spreading a potential threat. Aexauditpls.exe Aexnsclient.exe Aexnsclienttransport.exe Aexnswdusr.exe Sqlservr.exe (SQL Server Windows NT - 64 Bit) Sqlwriter.exe (SQL Server VSS Writer - 64 Bit) Add... | Remove OK | Cancel | Apply | Help	On the VirusScan Console, click **Task** > **On-Access Scanner Properties**. 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. Close the VirusScan Console.
12.	**Done.**	

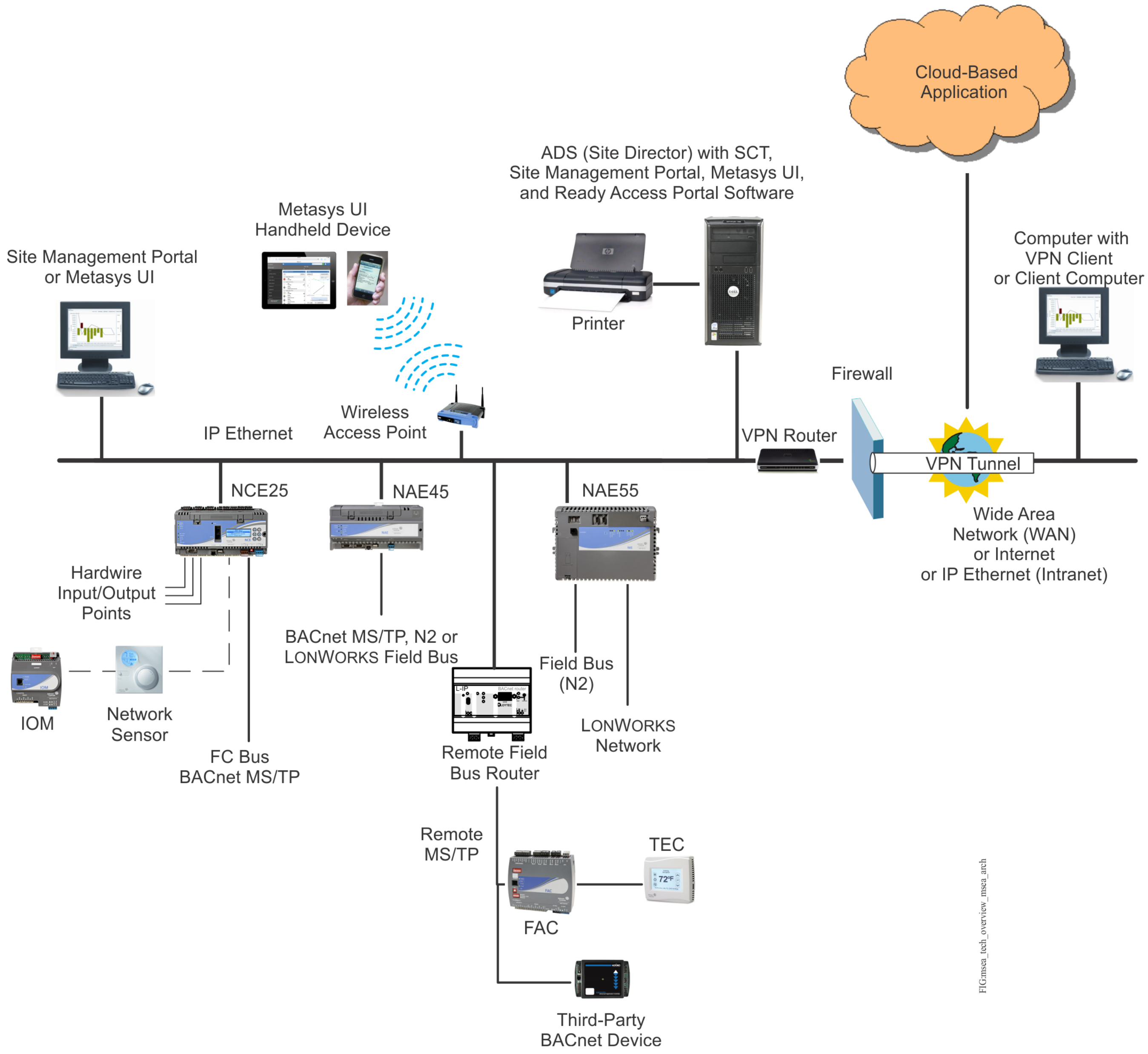
Appendix: Configuring a VPN Tunnel with a NETGEAR® ProSAFE® 8-Port Gigabit VPN Firewall/Router

This appendix describes how to configure a VPN tunnel with a NETGEAR® ProSAFE® 8-Port Gigabit VPN Firewall/Router. A VPN tunnel 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.

Use these instructions as an example. Consult your IT department and NETGEAR proprietary documentation for detailed information.

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 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 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 an ADS/ADX/ODS requires the computer be offline for a period of time. Similarly, installing new software on the ADS/ADX/ODS may require a computer restart.

Figure 100: *Metasys* System with VPN


Cloud-Based Application
ADS (Site Director) with SCT, Site Management Portal, Metasys UI, and Ready Access Portal Software
Metasys UI Handheld Device
Site Management Portal or Metasys UI
Computer with VPN Client or Client Computer
Printer
Firewall
Wireless Access Point
IP Ethernet
VPN Router
VPN Tunnel
NCE25
NAE45
NAE55
Wide Area Network (WAN) or Internet or IP Ethernet (Intranet)
Hardwire Input/Output Points
BACnet MS/TP, N2 or LONWORKS Field Bus
Field Bus (N2)
IOM
Network Sensor
LONWORKS Network
FC Bus BACnet MS/TP
Remote Field Bus Router
Remote MS/TP
TEC
FAC
Third-Party BACnet Device
FIG:msea_tech_overview_msea_arch

Preparation for Configuration of a VPN Tunnel

Before you begin configuring a VPN Tunnel with a NETGEAR® ProSAFE® 8-Port Gigabit VPN Firewall/Router device, you must complete the following steps:

1. Document the public IP address of the network that you are tunneling. See *Discovering the Public IP Address*.
2. Document the WAN IP Address of your NETGEAR® ProSAFE® 8-Port Gigabit VPN Firewall/Router device. See *Discovering the WAN IP Address of the NETGEAR® ProSAFE® 8-Port Gigabit VPN Firewall Device* .
3. Know the login information to your broadband router. See *Login Credentials for the Broadband Router*.
4. Download VPN Client Software. We recommend you download the proprietary NETGEAR VPN client software. The proprietary NETGEAR VPN client software offers a 30-day trial.
5. Follow the procedures in the *Detailed Procedures* of this appendix.

Discovering the Public IP Address

1. On a computer connected to the router that serves the network that you want a tunnel, open a web browser.
2. Browse to https://www.google.com.
3. In the search field, type **what is my ip address**. The search results display your public IP address. Write down this information.

Discovering the WAN IP Address of the NETGEAR® ProSAFE® 8-Port Gigabit VPN Firewall Device

1. Connect an Ethernet cable from a LAN port of the router to the Wide Area Network (WAN) port of the NETGEAR® ProSAFE® 8-Port Gigabit VPN Firewall/Router device.
2. Connect another Ethernet cable from your computer to a LAN port on the NETGEAR® ProSAFE® 8-Port Gigabit VPN Firewall/Router device.
3. In a web browser, type the default access IP address that is printed on the bottom of the NETGEAR® ProSAFE® 8-Port Gigabit VPN Firewall/Router device. The default setting is http://192.168.1.1.
4. Enter the default user name and password. The default user name is **admin** and the default password is **password**. We recommend you change the default password. The NETGEAR® ProSAFE® configuration UI appears.
5. Click **Monitoring**. Under the Broadband Configuration section, the IP address listed in the IP Address filed is the WAN IP Address. Write down this information.

Login Credentials for the Broadband Router

You must know the login credentials to the broadband router (the device behind the firewall you want to connect to).

Typically, the default user name and password are printed on the back of or under the broadband router device. However, the default login credentials may be available on the router manufacturer's website. If the default login credentials have been changed, use those login credentials. If necessary, you can restore the factory settings and login credentials by depressing the Reset or Factory Default button on the device with a paperclip or pen.

Detailed Procedures

Configuring the NETGEAR® ProSAFE® 8-Port Gigabit VPN Firewall/Router (Gateway Side)

For more information, refer to the NETGEAR® ProSAFE® 8-Port Gigabit VPN Firewall proprietary documentation.

1. In a web browser, enter the IP address of your NETGEAR ProSAFE 8-Port Gigabit VPN Firewall device.
2. To prevent dual-net conflicts, you may need to change the default LAN IP address of your NETGEAR® ProSAFE® 8-Port Gigabit VPN Firewall device. If the IP addresses that the router hands out on the LAN side are 192.168.1* addresses, then follow Steps 3 through 6. If not, skip to *Step 7*.
3. Click the **Network Configuration** tab.
4. Click the **LAN Settings** tab.
5. In the LAN TCP/IP Setup section, change the IP Address to 192.168.2.1 with a Subnet Mask of 255.255.255.0.
6. In the DHCP section, change the Starting IP Address to 192.168.2.2 and the Ending IP Address to 192.168.2.100
7. Click the **VPN** tab. Then select the **VPN Wizard** tab.
8. In the About VPN section, select the **VPN Client** option.
9. In the Connection Name and Remote IP Type section, enter the site specific information in the following fields:
   - **What is the new Connection Name**: Enter a Connection name.
   - **What is the preshared key?**: Enter a strong password.

   The wizard automatically creates a VPN Policy and an IKE Policy that interacts with the VPN Client software. Write down the Remote Identifier Information and the Local Identifier Information. The default values given by the wizard are arbitrary. However, we recommend keeping the default values. Furthermore, the Remote ID and the Local ID values are necessary to configure the VPN Client.
10. Click **Apply**. The wizard opens the Policies tab. Write down the information presented in the VPN Policy tab and the IKE Policy tab. The information presented in these tabs is necessary for configuring the client.

Configuring the NETGEAR® ProSAFE® 8-Port Gigabit VPN Firewall/Router (Client Side)

For more information, refer to NETGEAR® ProSAFE® 8-Port Gigabit VPN Firewall proprietary documentation.

1. After downloading and installing the NETGEAR® ProSAFE® VPN Client Professional software package, launch the executable file.
2. In the Configuration tab, select **Wizard**. The Choice of the remote equipment window appears.
3. Select **A router or a VPN gateway**. Click **Next**. The VPN tunnel parameters window appears.
4. Enter the following information:
   - **IP or DNS public (external) address of the remote equipment**: Enter the public IP address.
   - **Preshared key**: Enter the preshared key.
   - **IP private (internal) address of the remote network**: Enter the configured IP address from *Step 5* of *Configuring the NETGEAR® ProSAFE® 8-Port Gigabit VPN Firewall/Router (Gateway Side)*.

   Click **Next**. The Configuration Summary window appears.
5. Verify the information is correct. Click **Finish**.

Configuring the Ikev1Gateway Authentication

1. Click the **Ikev1Gateway directory**. The Ikev1Gateway Authentication window appears.
2. Click the **Authentication** tab.
3. In the Addresses section, enter the public IP address in the Remote Gateway field.
4. In the Authentication section, enter the preshared key in the Preshared Key and Confirm fields.

5. Keep the default values in the IKE section, unless other settings are required by your site.
6. Click the **Advanced** tab.
7. In the Local and Remote ID section, enter the following information:

   - **Local ID**
     - **Type of ID**: DNS
     - **Value for the ID**: Enter the Local ID.
   - **Remote ID**
     - **Type of ID**: DNS
     - **Value for the ID**: Enter the Remote ID.

Configuring the Ikev1Tunnel IPsec

1. Click the **Ikev1Tunnel directory**.
2. Click the **IPSec** tab.
3. In the ESP section, ensure that the Encryption is set to **3DES** and Authentication is set to **SHA-1**.
4. In the PFS section, select the **PFS** option and set the Group to **DH2**.

Configuring the Modem/Router Upstream from the NETGEAR® ProSAFE® 8-Port Gigabit VPN Firewall/Router

To complete the setup of the VPN tunnel that is between the public Internet and the private network hosting your site, 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.

1. Log into your modem/router.
2. Select the **Firewall** settings.
3. Select **IP Passthrough**.
4. In the **Default Server Internal Address** field, enter the WAN IP address of the NETGEAR® ProSAFE® 8-Port Gigabit VPN Firewall.
5. Ensure the following settings are in place:
   - **Allocation Mode**: Default Server
   - **Passthrough Mode**: DHCPS-dynamic

When your network is appropriately wired and configured, launch the VPN Client software on a remote device (laptop, smart phone, or tablet). Choose the configuration you saved and open the tunnel. You should be able to access the network through the VPN tunnel.

Index

Building Efficiency
507 E. Michigan Street, Milwaukee, WI 53202

Published in U.S.A.

www.johnsoncontrols.com