



Metasys Hardening Guide



GPS0034-CE-EN
Version 12.0
Rev A
Revised 2023-03-14

Introduction



Our solution provides peace of mind to our customers with a holistic cyber mindset beginning at initial design concept, continues through product development, and is supported through deployment. Johnson Controls also includes a rapid incident response process to meet the comprehensive and evolving cybersecurity environments.

The Hardening Guide intends to provide cybersecurity guidance used in planning, deployment, and maintenance periods.

As cybersecurity threats affect all connected devices, it is important to ensure that cybersecurity is considered throughout the planning, deployment and maintenance phases associated with a solution's functional operation.

This guide provides hardening guidance specifically for the Metasys application, including Metasys software, configuration, hardware, user accounts, permissions, roles, backup, restore, and patch management. While we do provide the supported platforms, hardening of the client / server operating system, and SQL is out of scope for this document.

This Johnson Controls **Metasys Hardening guide** is broken down into three main sections depicting the overall process for hardening:

1. Planning	2. Deployment	3. Maintain
Provides an introduction, general knowledge, and overall guidance for you to prepare your system for security and hardening	Guides you through the execution and hardening steps based on the products and security features of the target system components	Provides a checklist for future checkpoints to keep your system safe and secure

Appendixes are included at the end for additional Metasys literature, acronyms used within this document, and frequently asked questions (FAQs).

Legal disclaimer

The cybersecurity practices described in this guide are recommended practices to facilitate the secure installation and configuration of the products described herein. However, Johnson Controls cannot guarantee that the implementation of the cybersecurity practices or recommendations described in this guide will ensure the security of the relevant product or system, or prevent, or alter the potential impact of, any unauthorized access or damage caused by a cybersecurity incident. This guide is provided “as is”, and Johnson Controls makes no representation or warranty, express or implied, as to the efficacy of the cybersecurity practices or recommendations described in this guide. Johnson Controls disclaims all liability for any damages that may occur because of, or despite, reliance on this guide or compliance with any cybersecurity practices or recommendations set forth herein.

Table of Contents

Introduction.....	2
Legal disclaimer.....	3
Table of Contents	4
1 Planning.....	7
1.1.0 Metasys overview	7
1.1.1 Deployment architecture.....	7
1.1.2 Metasys Components.....	10
1.1.3 Supporting Components.....	11
1.1.4 Additional Deployment architecture examples	11
1.1.5 Metasys Releases	11
1.2.0 Security feature set.....	12
1.2.1 Security Dashboard.....	13
1.2.2 Supervisory Device safeguards	14
1.2.3 User password policy	14
1.2.4 FIPS Compliant Secure Communication on the building network	16
1.2.5 User Account Support	16
1.2.6 Encryption ciphers:.....	18
1.2.7 Updates.....	19
1.2.8 Disable insecure web traffic.....	19
1.2.9 Last Login monitoring	19
1.2.10 Performance Verification tool.....	20
1.2.11 BACnet Secure Connect (SC)	21
1.2.12 Certificate renewal period alarm event	22
1.3.0 Intended environment	23
1.3.1 Internet connectivity	23
1.3.2 Integration with IT networks.....	23
1.3.3 Integration with external systems	24
1.4.0 Patch policy	24
1.5.0 Hardening methodology.....	25
1.6.0 Communication	25
1.6.1 Communication port configuration	25
1.6.2 Communication certificates	31
1.7.0 Network planning	32
1.7.1 Trust boundaries overview	32
1.8.0 Hardware and software requirements	34
2 Deployment	35
2.1.0 Deployment overview.....	35
2.1.1 Physical installation considerations	35

2.1.2	Getting started.....	35
2.1.3	Resetting to the factory default settings.....	36
2.1.4	Considerations for commissioning.....	36
2.1.5	Recommended knowledge level.....	36
2.2.0	Hardening.....	36
2.2.1	Hardening checklist.....	37
2.2.2	Disable TLS 1.0 and 1.1.....	37
2.2.3	Disable unused Ports.....	37
2.3.0	User management best practices.....	37
2.3.1	Metasys User Roles and Permissions.....	38
2.3.2	Metasys Local User Accounts.....	40
2.3.3	Metasys LDAP Active Directory User Accounts:.....	42
2.3.4	No shared accounts.....	42
2.3.5	Change default passwords.....	42
2.3.6	Least privilege.....	42
2.3.7	Separation of duties.....	43
2.3.8	Centralized user account management.....	43
2.3.9	Password policy.....	44
2.3.10	Kiosk Service Accounts.....	44
2.3.11	User management best practices.....	44
2.4.0	Update Metasys to latest Release.....	45
2.5.0	Adding BACnet/SC as an option.....	45
2.6.0	Communication hardening.....	46
2.6.1	Least functionality.....	46
2.6.2	Communication certificate support.....	46
2.6.3	FIPS 140-2 support.....	47
2.7.0	Configuring security monitoring features.....	47
2.7.1	Audit Logs.....	47
2.8.0	Availability hardening.....	48
2.8.1	Backup/restore.....	48
2.8.2	Web Server.....	48
3	Maintain.....	50
3.1.0	Cybersecurity maintenance checklist.....	50
3.1.1	Backup historical data.....	52
3.1.2	Backup configuration data.....	52
3.1.3	Test backup data.....	52
3.1.4	Disable user accounts of terminated employees.....	52

3.1.5	Remove or “lock” inactive user accounts	53
3.1.6	Update user account roles and permissions	53
3.1.7	Disable unused features, ports, and services	53
3.1.8	Check for and prioritize advisories or product notices	54
3.1.9	Plan and execute advisory recommendations	54
3.1.10	Check and prioritize patches and updates	54
3.1.11	Plan and execute software patches and updates.....	54
3.1.12	Review TLS communication certificate expiration dates	55
3.1.13	Review updates to organizational policies	55
3.1.14	Review updates to regulations.....	55
3.1.15	Conduct security audits	56
3.1.16	Update password policies.....	56
3.1.17	Update as-built documentation	56
3.1.18	Update standard operating procedures	56
3.1.19	Update MUI logon banners.....	57
3.1.20	Renew licensing agreements.....	57
3.1.21	Renew support contracts.....	57
3.1.22	Check for end-of-support / discontinuation information and plan for replacements.	57
3.1.23	Periodically delete sensitive data in accordance with policies or regulations	57
3.1.24	Monitor for cyber attacks	58
3.2.0	Metasys Release schedule	59
Appendix A - Additional Metasys Literature.....		60
Appendix B - Acronyms		61
Appendix C – FAQs		63

1 Planning

This section helps plan for the implementation of security best practices for a Metasys system installation.

1.1.0 Metasys overview

Metasys® Building Automation System is the foundation of modern building energy management efficiency. This intelligent, world-class technology system connects your commercial HVAC, lighting, security, and protection systems – enabling them to communicate on a single platform to deliver the information you need, allowing you to make smarter, savvier decisions while enhancing your occupants' comfort, safety, and productivity.

A field engineer, or a service technician can use this document to harden a Metasys system. This document describes how to configure and use the following:

- Create unique user accounts
- Give the user sufficient permissions
- TLS/SSL and certificate management for communication between the Metasys server and the engine, or from the Metasys UI or Metasys Launcher to the Metasys device
- VPNs for remote access
- Other configurable settings

1.1.1 Deployment architecture

The Metasys system comprises various hardware and software components that work closely together to provide coordinated control over a site's HVAC and other building systems. More details are included in the next section - Metasys system architecture.

The Metasys system architecture is a distributed architecture. This means that the system components can be located as closely as possible to the equipment they are controlling, to provide optimum performance and reliability. The distributed Metasys components with their data sources and the equipment they control are connected by:

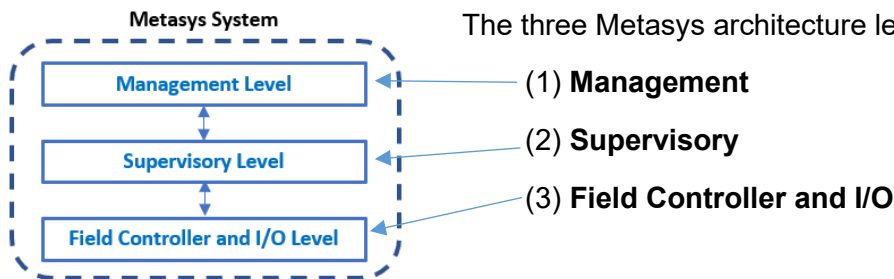
- Direct wiring
- Network wiring
- Wireless networking

The distributed Metasys components and various connection methods ensure system-wide data sharing, coordination, and remote access.

The Metasys system architecture is scalable. This means that you can add components as required to:

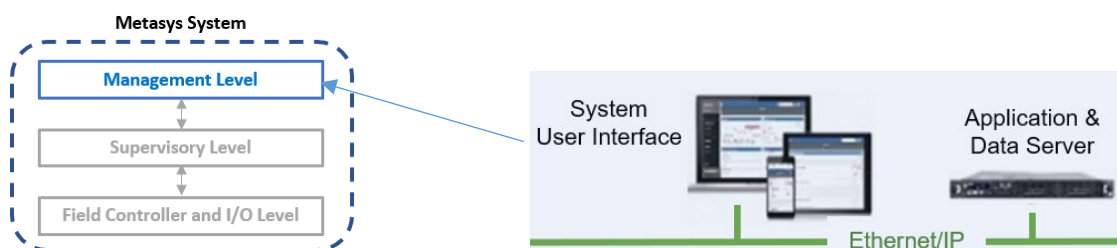
- Control buildings and systems of varying complexity, size, and scope
- Integrate third-party devices to unify their operation with the Metasys system
- Integrate earlier generations of Metasys components to modernize and unify their operation

It is important to note that every installation is unique. However, each installation can be broken down into basic building blocks or "Levels" which make up every Metasys installation.

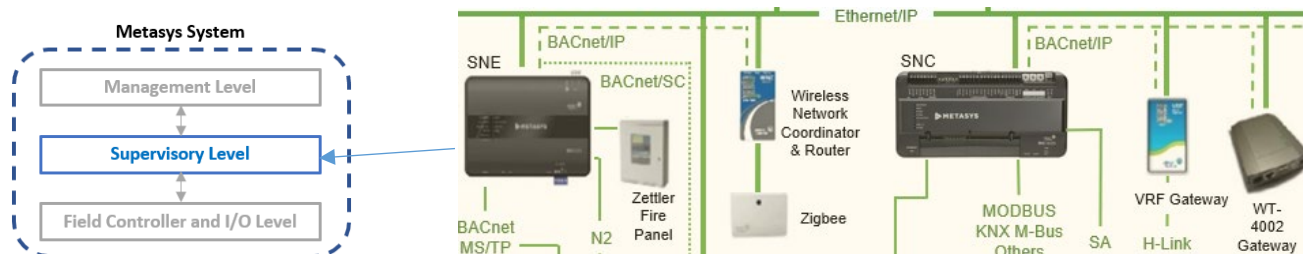


The management level resides on an Ethernet network which connects the engines. Within the supervisory level, engines route to the field controller network which can be IP-based as well as serial-based networks, while I/O devices often connect to field controllers using a standard electrical interface (e.g., voltage, current, pulse, or contact). However, some I/O devices are communication using a protocol interface.

Management Level. The Management level includes the system user interface and the server (or multiple servers) that hosts the application and database. These are core components and will be discussed further in the deployment architecture section.



Supervisory Level. The Supervisory or Engine level coordinate communications between the Management level and the Field controller and I/O level.

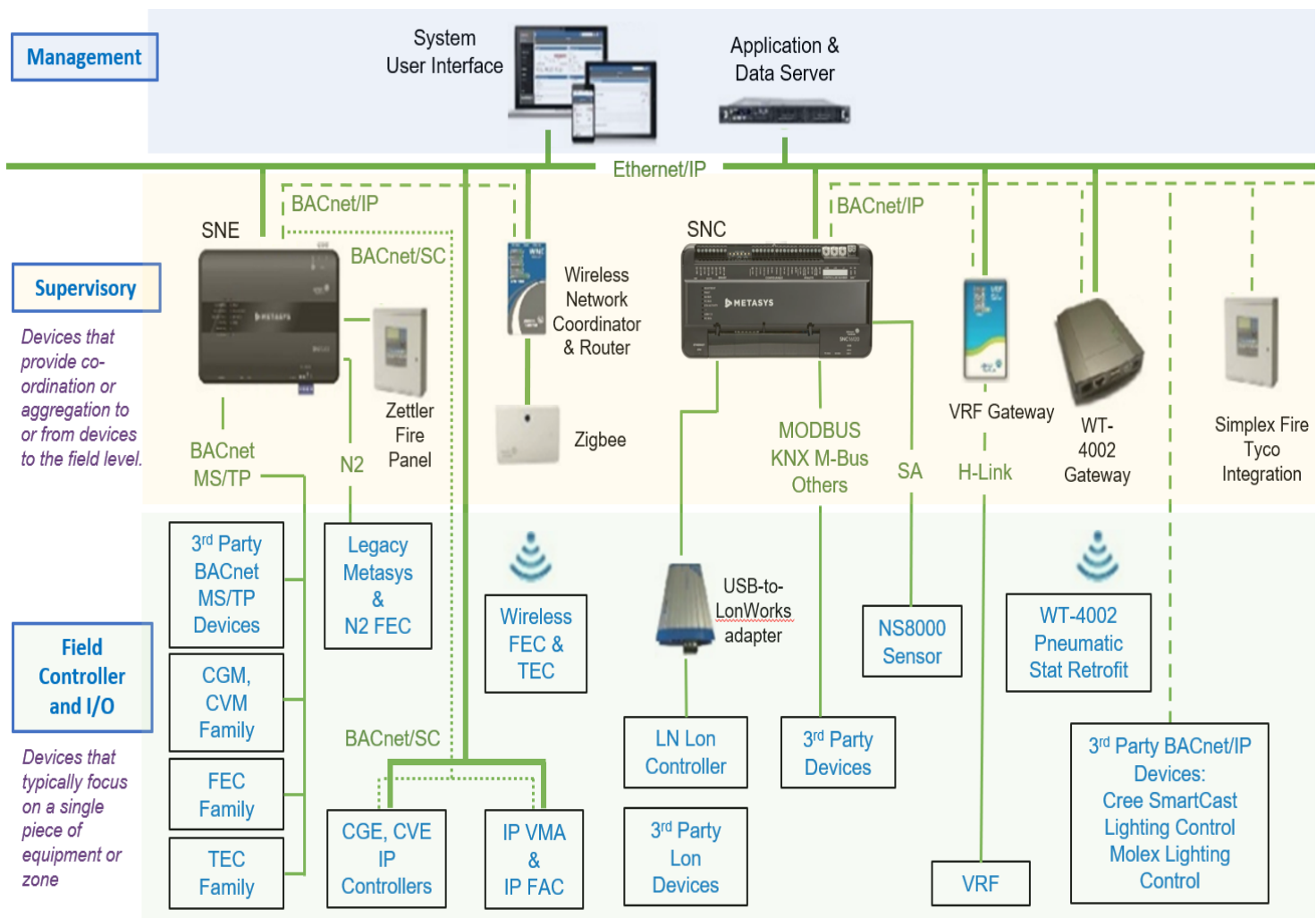


Field Controller and I/O Level. The Field Controller and I/O level includes the equipment controllers and communicates back to the Supervisory Level



Section 1.1.2 Metasys Components describes the components that make up each level in further detail

Figure 1.1.2.1: Metasys system architecture example



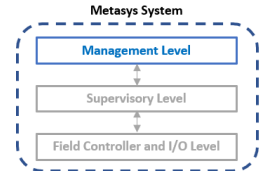
1.1.2 Metasys Components

The Metasys System configuration includes one to many Server, Network and Field components, which work together to provide a custom solution. The sections below contain a subset of the many components that may be included in a custom solution. For more comprehensive listing of devices and documentation of components Metasys supports, refer to **Appendix A - Additional Literature**.

1.1.2.1 **Management Level** – A site can optionally have one or more Metasys servers—computer-based devices that add long-term data storage and support for larger Metasys networks.

Metasys server products include:

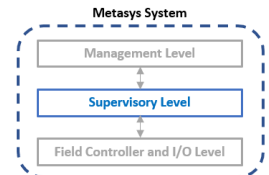
- a. Application and Data Server (ADS)
- b. ADS-Lite (available only in specific markets)
- c. Extended Application and Data Server (ADX)
- d. Open Application Server (OAS)



1.1.2.2 **Supervisory Level** – Network Engines provide network management and system-wide control coordination over one or more networks of equipment controllers.

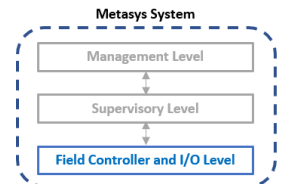
Network components include:

- a. Network Automation Engine (NAE)
- b. Network Control Engine (NCE)
- c. Network Integration Engine (NIE)
- d. Series Network Engine (SNE)
- e. Series Network Control Engine (SNC)
- f. Device gateway
- g. Server based engines such as NAE8500 or LCS8520



1.1.2.3 **Field Controller and I/O Level** – Metasys includes several model series of equipment controllers, including Various equipment controllers

- a. Application Controller (CGM/CGE)
- b. VAV Box Controller (CVM)
- c. Advanced Application Field Equipment, Controller (FAC)
- d. Field Equipment Controller (FEC)
- e. Variable Air Volume Modular Assembly (VMA)*
- f. Terminal Equipment Controller (TEC)
- g. Input/Output Modules (IOMs)
- h. Expansion Modules (XPMs)
- i. Sensor Actuator (SA) bus devices
 - a. Network sensors (NS8000s)
 - b. Actuators
 - c. Generic SA bus device
 - d. VFD on the SA bus
- j. Legacy Metasys controller, such as Unitary (UNT) controller**, Variable Air Volume Assembly (VAV)** and Air Handling Unit (AHU)**
- k. Legacy Extension Modules (XTMs)** and Expansion Modules (XPs)**



* Denotes a legacy item with some models still supported and can communicate to Metasys

** No longer manufactured and considered legacy items, but can still communicate to Metasys

1.1.3 Supporting Components

Metasys is designed to be compatible with standard protocols. With built-in support for BACnet, LON, Modbus, and other Johnson Controls systems, it is possible to interoperate with devices which support those protocols that were not specifically developed for Metasys. Networking components are also often included as part of the deployment architecture. Some components such as a Router and/or Smart Switch may be pre-existing, on site, supplied by the customer.

NOTE: Details on hardening Supporting Components are out of scope not included within this guide.

Management Level

- a. Third party management system which Metasys integrates to (BACnet, OPC UA, M-Bus, KNX, Modbus)

Supervisory Level

- b. BACnet Building Controller (B-BC) - Controllers conforming with BACnet Building Controller device profile

Field Controller and I/O Level

- a. N2 Field Controller - The N2 Field Equipment Controller legacy family comprises a group of versatile controllers and accessories designed to monitor and operate a wide variety of commercial HVAC equipment and can be networked together using the N2 Open Communications protocol (Serial network).
- b. BACnet Field Controller – BACnet IP or BACnet MS/TP serial controllers
- c. LON Field Controller – Controllers that utilize the standard LONTalk protocol
- d. Other protocol controller
- e. Input/Output (I/O) Devices – IP or Serial I/O devices which communicate to other system components using a protocol (BACnet, LON, N2, Modbus, etc.)

Networking

- a. Router (i.e., Edge router, Loytec BACnet/IP, BACnet/SC, remote field bus, etc.)
- b. Smart Switch (i.e., Smart ethernet switch, Netgear, Cisco, CCSI, etc.)
 - a. Ring Manager – IE2000 and IE4000 with Media Redundancy Protocol (MRP) for IP controllers

1.1.4 Additional Deployment architecture examples

Figure 1.2, above in section 1.1.1, showed one example deployment with various components.

See the Metasys System Configuration Guide for Metasys Release 12.0 (LIT-12011832) for additional details and configuration options.

1.1.5 Metasys Releases

Johnson Controls advises Metasys customers to upgrade to the latest release which would ensure you have the latest features and most secure installation. If you have a system that requires the ADX as a server, it must be at the highest release number. Its child engines can be at Release 12.0 or mixed with a lower Release (not below 5.2). Because you should take advantage of cybersecurity features, it is recommended that all engines are at Release 10.1 and higher.

Note: Some engines cannot go above Release 9.0.x and should be part of an upgrade plan. See Metasys Server Installation and Upgrade Instructions (LIT-12012162) for additional details.

Specific Series Network Engine models for Metasys Release 12.0 (newest release at the time this guide was written) are:

Supported Hardware	SNE2200x	SNE1100x	SNE1050x	SNE110Lx
Succeeds	NAE55 series	NAE45 series	NAE35 series	NAE45-Lite

Specific Series Network Controller models for Metasys Release 12.0 (newest release at the time this guide was written) are:

Supported Hardware	SNC2515x-0 SNC2515x-0H	SNC2515x-04 SNC2515x-04H	SNC1612x-0 SNC1612x-0H	SNC1612x-04 SNC1612x-04H
Succeeds	NCE25 Series	NCE25 Series	NCE25 Series	NCE25 Series

See Metasys System Product Bulletin (LIT-1201526) for additional details.

1.2.0 Security feature set

The Metasys UI supports the security features shown in the table below. The column titled “Feature Available” shows the first release when this feature became available. For example, if you are running Metasys Release 9.0 and a certain feature you are looking to deploy started with Release 10.0, you must update to Release 10.0 or higher to use this feature.

Table 1.2.0.1

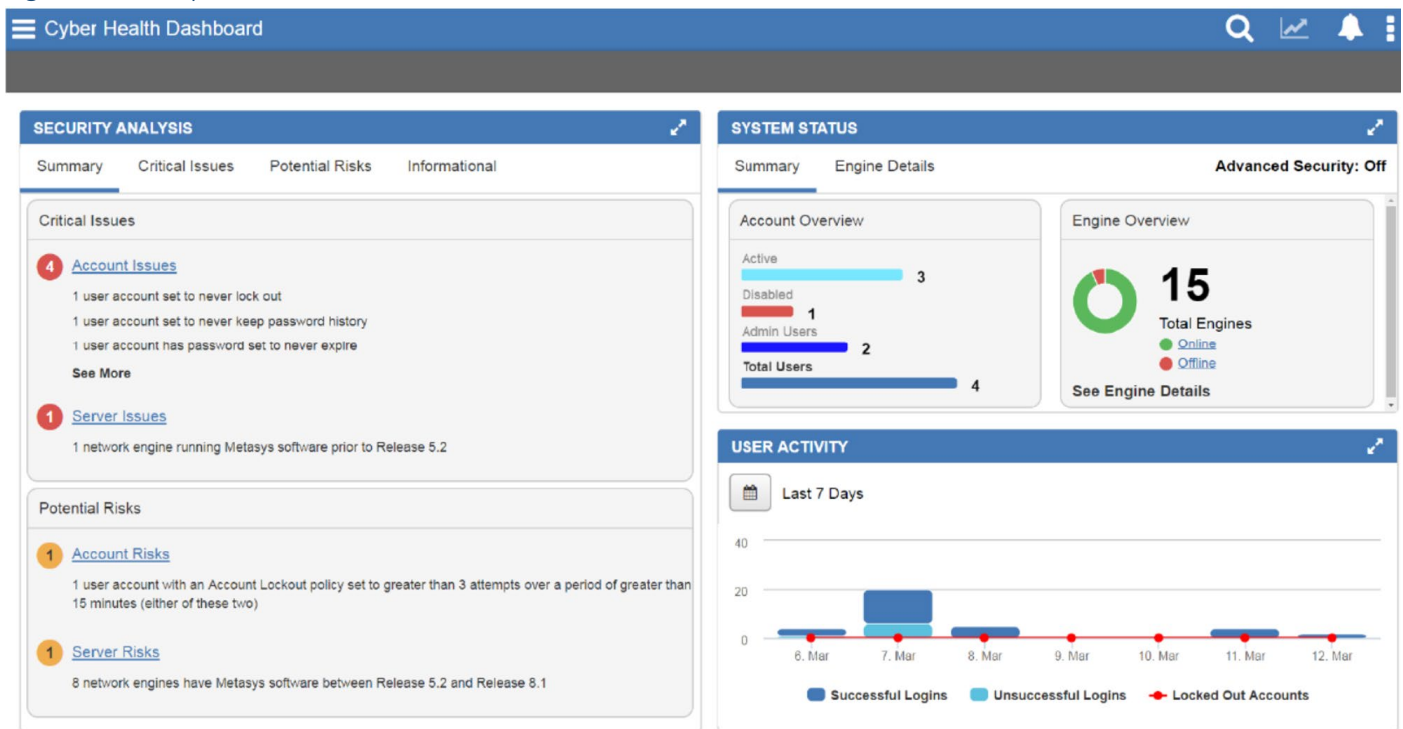
Section	Type	Feature name	Feature Available
1.2.1	Cybersecurity Dashboard (Metasys User Interface MUI only)	Security Analysis widget	10.1
		System Status	10.1
		User Activity widget	10.1
1.2.2	Supervisory Device safeguards	Advanced Security Enabled	10.0
		Engine Pairing	10.0
1.2.3	User password policy	User account control	
1.2.4	Secure Communication on the building network	FIPS 140-2 Compliance	11.0
1.2.5	User Account Support	Identify Dormant or unused user accounts	8.0
		User account management	7.0
		Warning Banner for unauthorized users	8.0
		Inactive Sessions	7.0
1.2.6	Encryption ciphers	Cipher support	
1.2.7	Updates	Update messages	
1.2.8	Disable insecure web traffic	Allow HTTPS	8.1
1.2.9	Monitor	Audit Log	1.0
		Last Login	8.0
		DDA using Syslog	7.0
1.2.10	Performance and Updates	Performance Verification Tool (PVT)	7.0
1.2.11	BACnet/SC Data Link	BACnet/SC (Secure Connect)	12.0
1.2.12	Countdown Reminder	Certificate Renewal Period	8.1

Note: Some of these features require configuration and/or licensing to be activated. See section 2 for additional details.

1.2.1 Security Dashboard

The Cyber Health dashboard provides a Metasys Administrator with a centralized view of potential security related issues or system issues which are detectable by an OAS, ADS and ADX, which may not surface as part of general system alarms. The administrator can also view if any software needs to be updated.

Figure 1.2.1.1 Cyber Health Dashboard



Security Analysis widget. This feature Provides a detailed breakdown of the Critical Issues and Potential Risks present with accounts and servers, along with an Informational tab showing the number of total user's accounts and more. The Metasys UI makes it easy to view items such as:

- The status of all user accounts (active, dormant, locked, temporary, disabled, administrator)
- Out-of-date software
- Certificate expiration, version, and status of engines

System Status Widget. Shows an account overview in the form of a bar chart and an engine overview in the form of a doughnut chart. The Engine Details tab lists the name, IP address, certification expiration, firmware version, and status of the engines.

User Activity Widget. The User activity widget shows in a dashboard view important events, such as:

- Successful user login occurrences during a specified period.
- Unsuccessful user login occurrences during a specified period.
- Account lock-out occurrences during a specified period

1.2.2 Supervisory Device safeguards

The Advanced Security Enabled and Engine Pairing provide an improved level of security between Metasys Site Directors and devices

Advanced Security Enabled. When enabled on a Site Director at Metasys 10.0 or later, the Advanced Security Enabled attribute rejects all communication attempts from network engines that have not been paired. The setting applies to the entire site, and only works with engines at Release 10.0 or later. When this attribute is set to True, a user message appears to indicate that all network engines prior to Release 10.0 remain functional but are disconnected from the site because they are no longer allowed to communicate with the Site Director.

Engine Pairing. Beginning at Metasys Release 10.0, a more secure authentication process has been implemented between updated engines and the Site Director that involves device pairing. After you pair an NxE with a Site Director, the two devices use unique credentials to authenticate communication between them. Engines at 10.x and greater must be paired to communicate with a Site Director. Unpaired engines are not able to communicate with a Site Director.

Encrypted Communication. Once devices are installed with or upgraded to Release 8.1 or later, Metasys system communication between ADX/ADS/NxE/SNx/OAS/SMP UI/Metasys UI is encrypted. Child devices at Release 8.0 or prior can be used on a Release 8.1 or later site, but communications will remain partially unencrypted. Optionally, the customer's IT department can generate trusted certificates for the Metasys Site Director. These certificates provide encrypted and trusted communication between the Site Director and the client. Trusted certificates from a Certificate Authority (CA) can be used on a new Metasys system, to provide encrypted and trusted communication between the Site Director and the Metasys SMP.

1.2.3 User password policy

Using Metasys user interface (MUI) and the Site Management Portal (SMP) UI you can apply a role-based account.

PBKDF2/salt for local accounts. Metasys local user account passwords are salted using a salt that is unique to that account and PBKDF2 before storing the password.

User account control. User accounts control user access to the Metasys system. An account defines which portions of the Metasys data a user can access (for example, all HVAC data or all lighting data from a particular area of the building) and which functions the user can perform on that data, from view-only access to configuring new databases. Always use the Principle of Least Privilege which states each user account should be given only those privileges needed to complete their tasks. The Metasys system provides the ability to divide the data into 163 unique categories, including HVAC, Fire, and Security; and has 10 different levels of user functionality.

Users can further limit user accounts to operate only at specified times on specified days of the week. The System Administrator creates all account settings.

Each account can also have associated preferences, such as which graphic or trend to display when a user logs in to the SMP UI, or which User Views appear in the Navigation Tree.

Basic Access is a feature through which users can create limited operator access to SMP features based on the user's assigned permissions in the Security Administrator. Users can avail of Basic Access on all the Metasys system engines and servers.

Microsoft Active Directory

The SMP and Metasys UI can use Microsoft Active Directory® LDAP accounts.

Table 1.2.3 shows the products which support Active Directory (AD) logins and Single Sign On (SSO).

Table 1.2.3.1 Metasys products AD & SSO logins

Application	AD login support	Exact or alternate UPN format login support	SSO Support
ADS/ADX Site Management portal UI	Yes	Yes	Yes
SCT*	Yes	Yes	Yes
SCT Pro	Yes	Yes	No
Metasys UI and JCT**	Yes	Yes	No
OAS	Yes	Yes	Yes
Metasys Advanced Reporting System	No	No	No
Network Engine (H/W and Server Release)	No	No	No
Metasys for Validated Environments	Yes	Yes	No

* SCT 15 has AD LDAP capability and AD SSO (but no ADFS integration)

** JCT – Johnson Controls System Configuration Tool, supports the configuration of the BACnet/SC configuration

See section 2.3 for additional details about user account management guidelines.

Active Directory Federation Service (ADFS) two-factor authentication

Two-factor or multi-factor authentication (MFA) is a method to login after the user has presented two or more pieces of evidence. In addition to their username, a user will provide an additional identification verification such as scanning a fingerprint, or a code received from a mobile device.

Integration with two-factor authentication is an ADFS add-on, licensed feature to add support for Metasys using ADFS, a single sign-on solution developed by Microsoft®. ADFS can then, in turn, be used to provide two-factor authentication for access to Metasys. ADFS, a centralized user account management feature, helps prevent unauthorized access to Metasys, which if not prevented, could result in data, financial, and reputational loss, system disruption, and other negative consequences.

Notes:

- ADFS is available in Metasys UI for the ADX, mobile phones and tablets
- ADFS is not available to Metasys SMP user
- The ADFS single sign-on and two-factor authentication are configured on the customer's ADFS system
- Refer to the Metasys System Configuration Guide Release 12.0 (LIT-12011832) for details
- Metasys supports ADFS 4.0
- Lightweight Directory Access (LDAP) for directory services authentication is discussed below in section 2.3.3

Table 1.2.3.2

Application	ADFS login support	SSO Support
MUI	X	X

1.2.4 FIPS Compliant Secure Communication on the building network

1.2.4.1 FIPS 140-2 Standard and Definition

The Federal Information Processing Standard (FIPS) publication 140-2 is a U.S. government standard that specifies the security requirements that will be satisfied by a cryptographic module, providing four increasing, qualitative levels intended to cover a wide range of potential applications and environments. The areas covered, related to the secure design and implementation of a cryptographic module, include specification; ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.

NOTE: on a FIPS enabled site, engines earlier than Release 11.0 will not be able to communicate with the site director.

See this NIST link for more details - FIPS 140-2, Security Requirements for Cryptographic Modules | CSRC (nist.gov).

1.2.4.1 FIPS 140-2 and Metasys

FIPS 140-2 is a licensed add-on feature to the Metasys Server software products, including ADS, ADX, NAE8500, and OAS and provides FIPS 140-2 compliance. When FIPS 140-2 is used, any engines on the site must also be upgraded to Release 11.0 or later.

FIPS 140-2 compliance is automatically available on engine-based sites at Release 11.0 and requires that all child-engines are also upgraded to Release 11.0 FIPS 140-2 certification can be obtained by using the SNx at Metasys Release 11.0 or later for the site director and child engines.

For the server class products ADX/ADS/OAS/NAE8500, one must purchase the FIPS-140-0 product code and license it. The specific product code is M4-FIPS-0.

Here is a list of the Metasys devices that support FIPS 140-2:

1.2.4.1.1 – FIPS 140-2 Compliant devices

Metasys Device	Device Type	FIPS Compliant	FIPS Certified
ADX / ADS	Server	Yes	No
OAS	Server	Yes	No
NAE8500	Engine	Yes	No
NAE55	Engine	Yes	No
SNE/SNC	Engine	Yes	Yes
CGE	IP Controller	Yes	No
CVE	IP Controller	Yes	No
FAC4911-0	IP Controller	Yes	No
VMA1930-0	IP Controller	Yes	No

For information on wolfCrypt FIPS Certificate #3389 (NIST) visit this [Link](#).

1.2.5 User Account Support

Dormant accounts. The Potential Risks tab on the Cyber Health dashboard in Metasys UI provides a Metasys administrator with a centralized view of account users, including Dormant User Accounts.

The Dormant Account User Report in SMP is used to identify and deactivate accounts designated as inactive or disabled. The report shows Active Directory, and local dormant accounts for supervisory devices (NxE/ADX/OAS) at Metasys Release 8.0 or later. See Metasys Release 12.0 Security Administrator

System Technical Bulletin (LIT-1201528 Account Policy Tab) for details how to ensure this feature is enabled.

An optional alarm can be set to identify dormant accounts on an ADS/ADX/OAS. While the alarm does not include engines, this information can be gathered by running a report on demand. When a dormant account is detected, you may choose to lock out the account, receive an alarm or both.

User account policies. Administrators manage the settings of each individual user account to match their preferred settings. Adjustments can be done for inactive sessions, account lockout, dormant accounts, and password policies. Each feature provides protection from unauthorized users.

Password History. Keeps history and ensures password cannot be reused

Password Aging. Configurable time before a user is required to change their password

Warning Banners. Warning banners are a special login feature that consists of a text window that appears to the user during login. The banner provides a definitive warning towards any possible intruders that may want to access your system that certain types of activity are illegal. At the same time, it also advises authorized and legitimate users of their obligations relating to acceptable use of the computerized or networked environment(s). The information in the text window may be customized for a United States government agency where the Metasys system is installed. Three different warning banners are available:

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

During the login process, and with one Warning Logon Banner active, Metasys can capture the client IP address of the machine a user logs in with. For higher security, user logins can be recorded from a camera to link the image of the person logging on with the user credentials to aid forensics for any suspected illegal activities. This higher security and camera would be provided outside of Metasys.

Inactive Sessions. Timed logout automatically logs you out of the Metasys system after a predefined time of inactivity. The system closes open databases, discards unsaved changes and view settings, and logs out the user. The session time out is noted in the Metasys audit log.

1.2.6 Encryption ciphers:

For Metasys Hardware engines these ciphers have been valid since Release 8.1. There are more cipher suites available with PC and Server Operating systems, but they are subject to negotiations when a HTTPS session is initiated. In that case, the hardware NAE/SNx would drive the cipher suites towards the ones that they support.

For Metasys ADX servers we use ciphers that are provided by Microsoft SChannel for each operating system listed in the System Configuration Tool Catalog Page (LIT-1900198). Metasys Release 12.0 recommends disabling TLS 1.0 and TLS 1.1 as these are both deprecated due to known vulnerabilities.

Table 1.2.6.1 – Encryption Ciphers

	Cipher	Usage	Engines	Release introduced
1	TLS_AES_256_GCM_SHA384	TLS 1.3	NAE55/SNx	11.0
2	TLS_AES_128_GCM_SHA256	TLS 1.3	NAE55/SNx	11.0
3	TLS_AES_128_CCM_8_SHA256	TLS 1.3	NAE55/SNx	11.0
4	TLS_AES_128_CCM_SHA256	TLS 1.3	NAE55/SNx	11.0
5	ECDHE-RSA-AES128-GCM-SHA256	TLS 1.2	NAE55/SNx	11.0
6	ECDHE-RSA-AES256-GCM-SHA384	TLS 1.2	NAE55/SNx	11.0
7	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	TLS 1.2	NxE25/35/45/55, SNx	8.1,11.0
8	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	TLS 1.2	NxE25/35/45/55, SNx	8.1,11.0
9	TLS_RSA_WITH_AES_128_GCM_SHA256	TLS 1.2	NxE25/35/45/55, SNx	8.1,11.0
10	TLS_RSA_WITH_AES_256_GCM_SHA384	TLS 1.2	NxE25/35/45/55, SNx	8.1,11.0
11	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TLS 1.2	NxE25/35/45/55, SNx	8.1,11.0
12	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	TLS 1.2	NxE25/35/45/55, SNx	8.1,11.0
13	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLS 1.2	NxE25/35/45/55, SNx	8.1,11.0
14	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLS 1.2	NxE25/35/45/55, SNx	8.1,11.0
15	TLS_RSA_WITH_AES_128_CBC_SHA256	TLS 1.2	NxE25/35/45/55, SNx	8.1,11.0
16	TLS_RSA_WITH_AES_256_CBC_SHA256	TLS 1.2	NxE25/35/45/55, SNx	8.1,11.0

1.2.7 Updates

Updates tab overview

The Updates tab displays information about the available updates for installed Johnson Controls software. You can download the files you need to complete the update from the Updates tab. To open the tab, click on the Updates tab.

Click the Refresh icon on the Updates tab to complete a manual refresh and get new updates if available. From the time you click the refresh icon on the Updates tab until the refresh is in progress and the system is establishing a connection with the server, you cannot change the connection setting, change the proxy details, download, resume a download, or cancel a download. Note: When you turn on the machine, the Software Manager checks when the scheduled refresh last occurred on that machine. If the scheduled refresh has not occurred in the past 12 hours and is not set up within 30 minutes when the user turns on the machine, the system runs the scheduler automatically to get the latest updates.

The following messages may display in the Updates tab based on different scenarios:

- No updates are available in the system: No new available updates. The latest Release is installed.
- Online connection setting is set to None (Offline): Software Updates are not available when the online connection setting is None (Offline).
- Installed Release of the product is EOL, and no updates are available: This product has been discontinued. Please contact your Johnson Controls office for further details.
- Installed Release of the product is EOL, but some updates are available: The installed product has been discontinued. Please download and install the latest Release.

For additional information see the following:

- Software Manager Help (LIT-12012389) for additional information
- Section 3.1.12 Plan and execute software patches and updates
- Section 1.3.1 Internet connectivity, which is required for Software Manager. There is a manual procedure if you cannot open a port at the site.
- See your Field Support Center (FSC), or Local Support Center portal

Metasys uses secure HTTP with Transport Layer Security (TLS) 1.3 between the SCT computer, all Metasys servers, and network engines that are upgraded to Metasys Release 8.1 and later. The encrypted HTTPS communications apply to the Metasys servers, Metasys UI, network engines, and SCT. This ensures that unauthorized users and computer hackers cannot view the contents of communications sent between Metasys equipment and user interface clients.

1.2.8 Disable insecure web traffic

Metasys uses secure HTTP with Transport Layer Security (TLS) 1.3 between the SCT computer, all Metasys servers, and network engines that are upgraded to Metasys Release 8.1 and later. The encrypted HTTPS communications apply to the Metasys servers, Metasys UI, network engines, and SCT. This ensures that unauthorized users and computer hackers cannot view the contents of communications sent between Metasys equipment and user interface clients.

1.2.9 Last Login monitoring

The main screen of the Metasys server or SCT user interface indicates the last time and date that user successfully logged in. The Metasys username displayed on the Site Management Portal (SMP) and MUI user interface is partially obscured after a successful login. For enhanced security, only the first three characters of the username are displayed, followed by three asterisks. If the user has never logged in, "Never" appears in the Last Login field. See figures 1.2.9.1 and 1.2.9.2.

Figure 1.2.9.1

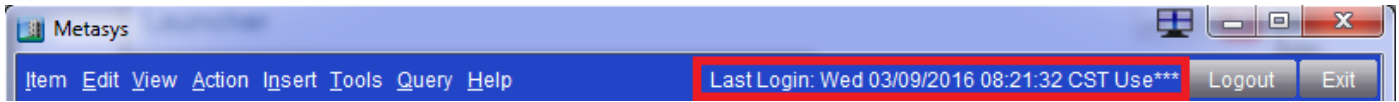





Figure 1.2.9.2



When a user logs on to either Metasys interface, the color of the lock will indicate Level and trust.

Indicator	Description	Status
	Green shield with check mark	Security level between the client computer and the Metasys Server or network engine is encrypted and trusted.
	Orange shield with exclamation point	Security level between the client computer and the Metasys Server or network engine is encrypted, but not trusted.
	Red shield with X symbol	Security level between the client computer and the Metasys Server or network engine cannot be verified because the certificate has expired, is not valid, or is not present. However, if the client computer is using Launcher 1.6 and the Metasys Server or network engine is at Release 8.1, communication is still encrypted.

1.2.10 Performance Verification tool

The Metasys Performance Verification Tool (PVT) is a tool that was developed by Johnson Controls to help document hardware inventory, identify outdated items, assist with upgrades, and help with cybersecurity.

The following tasks can be easily performed using the PVT:

- Overall
 - Determine the overall health of the Metasys system
 - Identifies whether all points are categorized the same
- Equipment
 - Scan one server at a time to identify an inventory list of all the controls hardware
 - Identify the equipment the system controls
- User accounts
 - Identifies whether the MetasysSysAgent Default user and password are being used
 - List user accounts who possess administrator privileges
 - Identifies user accounts that have not logged into Metasys within the last six months

For additional information see Metasys Performance Verification Tool (PVT) User Guide (LIT-12012406).

Note: PVT is only compatible with Metasys Release 7.0 or later.

1.2.11 BACnet Secure Connect (SC)

Metasys Release 12.0 supports BACnet/SC, which is a recent update to the BACnet interoperability standard aimed at improving cybersecurity and network infrastructure integrity. BACnet/SC integration enables the supported supervisory controllers to provide supervisory control and monitoring functions for objects integrated from connected BACnet controllers. BACnet controllers can integrate with a supervisory controller using either BACnet/IP, BACnet/SC or MS/TP communications.

Many Release 12.0 Metasys components are field updated to, or factory shipped with BACnet/SC. The SNE, SNC, and NAE55xx-3 models can act as a Primary Hub, Failover Hub, or a Node in the BACnet/SC network. See Metasys System Product Bulletin (LIT-1201526) for additional details.

BACnet/SC License. You need to purchase the M4-BACNETSC-0 add-on license to use BACnet/SC on the ADS, ADS-Lite, ADX, OAS, NAE85, or LCS85.

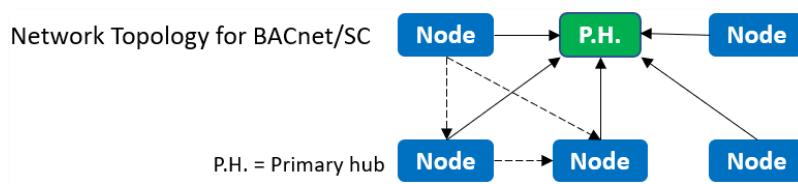
Acquiring a Certificate Authority (CA) for your site. A CA is an entity that issues the operational certificates to use for communication on a site. You must decide what will be the certificate authority used to generate the operational certificates. At Metasys Release 12.0, there are two options for the CA:

- **Option 1:** Instruct the customer's IT department to act as the CA. This is done by submitting a request to the customer by completing a Request for Information (RFI), or by sending an email to the customer.
Note: A third-party vendor of BACnet/SC devices could also act as the CA.
- **Option 2:** Purchase a CA and certificates through Johnson Controls from a third party, in which case Johnson Controls acts as the CA backed by the third party. To purchase a CA and certificates through Johnson Controls from a third party, order the following product codes:

Product code number	Description
M4-JCCA-0	<ul style="list-style-type: none"> • Johnson Controls Customer Certificate Authority (CA) for BACnet/SC ECC certificates only • Expires in 30 years
M4-JCCERT1-0	<ul style="list-style-type: none"> • Johnson Controls ECC Certificate – one (1) total • Expires in three years

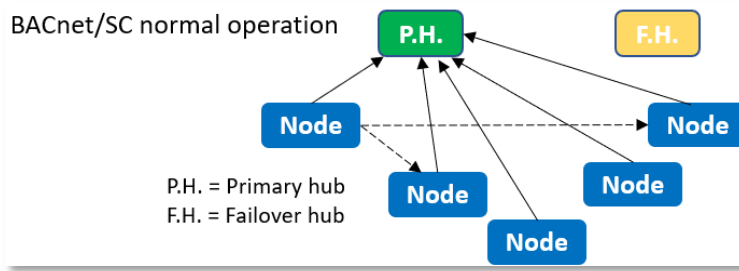
Additional Notes about BACnet/SC

- It is a new BACnet datalink ASHRAE 135-2020 Annex AB that provides secure message transport
- BACnet/SC implementations support **TLS version 1.3** for establishing communication connections between devices. Support of other versions of TLS or cipher suites beyond those required by TLS 1.3 is a local matter.
- BACnet/SC uses a virtual **hub-and-spoke** topology. The central Hub Function performs message forwarding for all broadcast messages and for point-to-point messages for devices that do not support more efficient direct connections. All Metasys devices support direct connections (optional) shown as the dashed line.

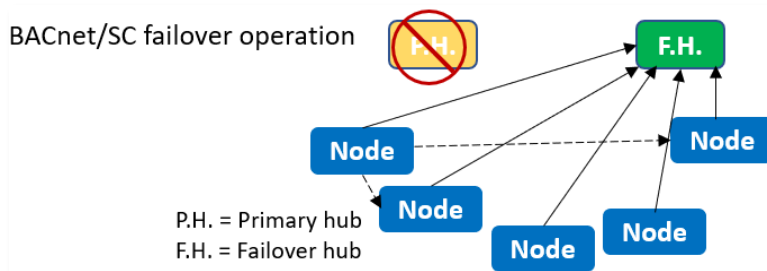


- A **Primary Hub** device has both a node and a Hub Function. The node on the Primary Hub device connects to the Hub Function, as if it was a different device. The Primary Hub is expected to

perform the Hub Function when reachable and always accepts WebSocket connections. A BACnet/SC site supports one Primary Hub only.



- A **Failover Hub** device has both a node and a Hub Function. The Failover Hub's node connects to the Primary Hub Function. If the Primary Hub Function is offline, then all nodes, including the Failover Hub's node, connect to the Failover Hub Function. A BACnet/SC site supports one Failover Hub only. While it is optional to have a Failover Hub, it is best practice to configure a Failover Hub so as not to leave a site with a single point of failure.



- A **Node** is a network port that implements a BACnet/SC Virtual Link Layer (BVLL) entity for link control and Network Protocol Data Unit (NPDU) transport, and the hub connector for connecting the hub function to participate in the BACnet/SC network.

Topic for additional information	Refer to the following document
BACnet/SC product details and usage	Metasys System Product Bulletin (LIT-1201526)
BACnet/SC workflow and certificates	Metasys BACnet/SC Workflow Technical Bulletin (LIT-12013959)
BACnet/SC ports	Network and IT Guidance Technical Bulletin (LIT-12011279)

1.2.12 Certificate renewal period alarm event

Metasys Release 12.0 includes a configurable attribute that gives a notification alert if a certificate is about to expire. When the certificate expiration reaches the defined range, a warning shows that a Metasys HTTPS certificate ADS/ADX for the BACnet/SC certificates will expire on a certain date.

Some important details:

- To ensure uninterrupted operation, it is imperative to renew BACnet/SC certificates before they expire
- The default period is 60 days and can be configured between 1-180 days
- Use the **Certificate Renewal Period** property of the **Detail widget** of the Site Object to configure the launch of the Event reminders
- You will be reminded with a daily Metasys Event until the certificates are replaced
- These events will be logged in the SMP UI and MUI System Activity feature

Follow the IT policies and guidelines for the following communication certificates:

- You should understand if you're able to provide RSA communication certificates for Metasys Release 12.0 ADS/ADX Server and engine(s)
- To install and configure the communication certificates in the IIS default website, see Metasys Release 12.0 Network and IT Guidance Technical Bulletin (LIT-12011279)
- If BACnet/SC feature (optional) is running onsite, you will need to get clarification on who is able to provide the ECC certificates

See section 1.6.2 for additional details on communication certificates

1.3.0 Intended environment

Physical access and installation of Metasys devices can greatly impact cybersecurity. Many Metasys components are designed to be operated in an indoor, dry environment. However, components at each level will possess varying degrees of access.

Management Level – The Metasys server is to be installed on location within an equipment rack in a secured, temperature-controlled location, such as within a data center or IT Server room with restricted access.

Supervisory Level – These components are designed to be installed in a user supplied panel or enclosure in an upright orientation. In most cases devices should also be physically secure, i.e., mechanical, and electrical rooms. The panel or enclosure should also be locked. Install in areas free of corrosive vapors and where the ambient temperature stays below 122 degrees F (50 degrees C).

I/O Field controller Level – This level has a vast listing of components that may be included in your system. Because of this, we can offer broad environmental information. For example:

- Components may be mounted horizontally or vertically
- It is recommended that the installation location is dry, away from corrosive vapors, away from electromagnetic emissions
- If possible, do not mount on surfaces prone to vibration
- Provide sufficient space for cover removal, cabling and wired connections

For more information, review the specific installation instructions of your Metasys components.

1.3.1 Internet connectivity

Connecting any Operational Technology (OT) system to the internet always increases cybersecurity risk. To harden your system, Johnson Controls recommends that you do not connect Metasys directly to the internet. For Metasys this could mean

- Opening the web server to the internet
- Allowing inbound access to the ADX (high-risk)

1.3.2 Integration with IT networks

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 for existing building installations, the IT organization must approve configurations that expose networks to the Internet. For new building installations follow the JCI recommendations. Be sure to fully read and understand IT Compliance documentation for your site.

1.3.3 Integration with external systems

Microsoft Active Directory LDAP or ADFS services

This section provides an overview of Active Directory LDAP services as implemented in the Metasys system. For more details, refer to the Security Administrator System Technical Bulletin Release 12.0 (LIT-1201528).

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

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

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

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

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

1.4.0 Patch policy

The policy documented here sets forth the current internal operating guidelines and process regarding Metasys, which may change from time to time at the sole discretion of Johnson Controls. Johnson Controls employs commercially reasonable efforts to pursue the operating guidelines and process described herein. However, other mitigating factors may prevent complete adherence to this policy, as determined by Johnson Controls at its discretion. Regardless, Johnson Controls endeavours to address issues that arise within Metasys with the severity that they warrant.

- When CRITICAL security vulnerabilities are discovered within Metasys, Johnson Controls will use commercially reasonable efforts to issue a critical patch for the current Release of Metasys.

When non-CRITICAL vulnerabilities are discovered within Metasys, Johnson Controls will use commercially reasonable efforts to:

- Apply fixes for HIGH severity vulnerabilities in the next immediate Release of Metasys
- Johnson Controls will assess MEDIUM vulnerabilities and plan accordingly

1.5.0 Hardening methodology

While Metasys provides many onboard security safeguards, including secure-by-default settings, we recommend that the device is hardened according to the guidance outlined in section 2, Deployment.

Generally, a defense-in-depth strategy employing standard IT hardening methods and compensating controls is needed to compliment the base security features of each component.

1.6.0 Communication

1.6.1 Communication port configuration

In a Metasys system, when you use a feature that requires a communication protocol, ensure that the corresponding port is open. Hardening your system involves closing any port that is not used. The tables on the following pages provide information on ports and protocols for Metasys to function properly.

Over the next several pages, you'll find the following three tables that relate to Metasys ports.

- Table 1.6.1.1 - Internal and External TCP/IP Port numbers and protocols
- Table 1.6.1.2 - Internal Only Port numbers and protocols
- Table 1.6.1.3 - Wireless Port numbers and protocols

Table 1.6.1.1: Internal and External TCP/IP Port numbers and protocols

Port	Protocol	Use	Devices	In bound/ Out bound	Description
25	SMTP	TCP	ADS/ADX/OAS NAE55/SNx/NAE85	O	Used for alarms and events.
53	DNS	UDP	Active Directory Client ADS/ADX/OAS Web Browser Network Engine	I/O	Translates domain names into numerical IP addresses. This port allows the server to receive responses to DNS queries.
67, 68	DHCP	UDP	Active Directory Client ADS/ADX/OAS Web Browser Network Engine	I/O	Assigns and keeps track of dynamic IP addresses and other network configuration parameters. Alternate Method: Use static IP addresses.
69	TFTP ¹	UDP	Metasys SCT NCE25/NAE35/NAE 45/NAE55	I/O	Downloads new images to NAEs (Legacy) Note: This port is used only when the NAE is provisioned (Not used during system runtime).
80	HTTP ¹	TCP	ADS/ADX/OAS Web Browser Network Engine SCT	I	Provides communication between peer controllers, computers, and other Internet systems using SOAP over HTTP. The ADS/ ADX requires only Port 80 be open to receive communication from client devices. Port 80 is the primary port used by WWW. Note: For a higher level of security, at Metasys Release 8.1 or later, you can close Port 80 (in and out).
80	HTTP	TCP	NAE Update Tool	I	File transfer between the client computer and the network engine.
88	Kerberos	TCP/ UDP	ADS/ADX/OAS ADX Split Web/Application Server Metasys System Client SCT	I/O	AD service authentication at the Metasys system login screen, and Service Account auth prior to LDAP queries. Kerberos is a standard network authentication protocol designed to provide strong auth for client/ server applications by using secret-key cryptography. Kerberos is the primary security protocol for auth within an AD service Domain. Kerberos auth relies on client functionality built into supported Windows operating systems.
110	POP3	TCP	Computer (Web Browser)	O	Receives and holds email for downloading from your Internet server. POP3 is allowed in the Metasys system only for auth from a SMTP server. Note: Firewall rules are usually unneeded for access as this server should be behind the firewall.
123	NTP	UDP	ADS/ADX/OAS ADX Split Web/Application Server	I/O	Used for time sync across a network between client computers and server class operating system host computers.

Port	Protocol	Use	Devices	In bound/ Out bound	Description
			Metasys System Client SCT		
123	SNTP ¹	UDP	ADS/ADX/OAS Network Engine	I/O	Used to sync computer clocks over a network between a server and its clients. Not required for all systems.
135	Remote Procedure Call (RPC)	TCP	ADS/ADX/OAS ADX Split Web/Application Server Metasys System Client SCT	I/O	Used by IIS on the ADS/ADX, OAS, and SCT during the process of authentication during SSO. If SSO is disabled in Metasys, this port and protocol are not used; however, if the ADS/ADX, OAS, SCT, or Metasys client, or any combination are members of an Active Directory service domain, this port and protocol are used for Active Directory service functionality.
161	SNMP	UDP	ADS/ADX/OAS Metasys UI Network Engine SCT	O O O I	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.
162	SNMP Trap	UDP	SCT Pro/NCT Tool	I	Used by Metasys devices at start up, this port announces discovery-related information.
389	LDAP	TCP	ADS/ADX/OAS ADX Split Web/Application Server Metasys System Client SCT	I/O	Used by the Metasys system to access user objects and attributes within Active Directory service.
443	SSL	TCP	ADS/ADX/OAS Metasys Advanced Reporting ADX	I/O I	Metasys 8.1 - 12.x uses HTTPS. Required if you use SSL with your reporting ADX.
443	TLS	TCP	NAE55/SNx/NAE85 Network Engine SCT & SCT Pro Metasys UI and JCT Computer (Web Browser)	I/O I I O	Required if you use TLS with the Metasys UI and the Metasys UI Offline for site security. Port 443 is used for secure web browser communication. Data transferred across such connections is highly resistant to eavesdropping and interception. Moreover, the identity of the remotely connected server can be verified with significant confidence. Web servers offering to accept and establish secure connections listen on this port for connections from web browsers desiring strong communication security.
443	HTTPS	TCP	Background File Transfer (BFT) in	I	With BFT, file transfers occur between the device and SCT where

Port	Protocol	Use	Devices	In bound/ Out bound	Description
			SCT		the device is the HTTPS client and SCT is the HTTPS server.
445	NT LAN Manager Version 2 (NTLMv2)	TCP	ADS/ADX/OAS ADX Split Web/Application Server Metasys System Client SCT	I/O	Used during Metasys system SSO authentication. NTLMv2 is a network authentication protocol developed by Microsoft and the secondary security protocol for authentication within an Active Directory service domain. If a domain client or domain server cannot use Kerberos authentication, then NTLM authentication is used.
465	SMTP	TCP	ADS/ADX/OAS Network Engine	O	Used for alarms and events
514	Syslog	UDP	ADS/ADX/OAS Network Engine SCT	O	Provides capability of sending its configured audit log entries and alarm notifications to the central repository of an external, industry-standard, Syslog server, conforming to Internet published RFC 3164.
587	SMTP	TCP	ADS/ADX/OAS Network Engine	O	Used for alarms and events
995	POP3	TCP	Computer (Web Browser)	O	Receives and holds email for downloading from your Internet server. POP3 is allowed in the Metasys system only for authentication from a SMTP server. The mail server uses port 995 for SSL connections for POP3 access. Note: Firewall rules are not necessary to allow access in most cases because this server should be behind the firewall.
1025	Remote Procedure Call (RPC)	TCP	ADS/ADX/OAS ADX Split Web/Application Server Metasys System Client SCT	I/O	Used by IIS on the ADS/ADX/OAS/SCT during the process of authentication during SSO (Windows Integrated Authentication). If SSO is disabled in the Metasys system, this port and protocol are not used by the Metasys system; however, if the ADS/ADX/OAS/SCT, or Metasys client, or any combination, is a member of an Active Directory service domain, this port and protocol are used for Active Directory service functionality.
1433	Microsoft SQL Server Database	TCP	ADX Metasys ADX Split Database Server	I/O	Used between the web/ application server and database server computers when the ADX is split across two devices.
1443	BACnet/SC	TCP	ADS/ADS-Lite/ADX/NAE85/LCS85/OAS	I/O	This is the default port. However, an Administrator can configure BACnet/SC for an alternate port using Metasys UI or JCT.

Port	Protocol	Use	Devices	In bound/ Out bound	Description
9004	Johnson Controls Licensing Service	TCP	Software Manager	I/O	For Computer only, it may be closed.
9910	Microsoft Discovery Protocol ¹	TCP/ UDP	Network Engine SCT NCT and NAE Update Tool	I	Used by NCT to get diagnostic information from devices on the same network.
9911	Metasys Private Message ¹	UDP	SCT	O	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.
10050	Turbo Boot	HTTP/ TCP/ PXE	NAE Update Tool	I/O	Used during NAE Update Tool operations such as updating an image to a network engine. Not used with SNC and SNE engines prior to Release 10.1.
11001	N1 Protocol	UDP	NCM NIE5X	I/O	Provides N1 message transmission (proprietary packet encoded in UDP) for devices at Release 9.0 or earlier. If 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. 11002 is used by the Metasys Ethernet Router and should be avoided even if Metasys Ethernet Routers are not in the system. The recommended addressing for five N1s is 11001, 11003, 11004, 11005, 11006.
12000	UserDebug Service	TCP	Metasys System	I/O	Used by Metasys software for debugging and logging.
47808	BACnet/IP Protocol	UDP	NAE/NCE/ IP Field controllers ² /SNx/NAE85/OAS/S CT	I/O	Refer to the BACnet Controller Integration with NAE/NCE Tech Bulletin (LIT-1201531). If connecting to multiple BACnet networks, the port is unique for each. The default port is 47808. Choose additional UDP ports that don't conflict with a port in use.

¹ 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

² IP controllers (IP) refers in general terms to the following controllers: M4-CGE09090-0, M4-CGE04060-0, M4-CVE03050-0P, MS-FAC4911-0, MS-VMA1930-0

Table 1.6.1.2: Internal Only Port numbers and protocols

Port	Protocol	Use	Devices	Description
3003	PhantomJS	TCP	ADS	Involved in generating PDF files in Metasys UI Reports.
4369	Rabbit MQ	TCP	ADS/ADX	Erlang Port Mapping Daemon.
5291	Action Queue	TCP	ADS/ADX	Action Queue communication, processing events/audits.
5672	Rabbit MQ/Erlang	TCP	ADS/ADX	Listening port for Message Bus, communication between microservices.
5960	Device Manager	TCP	ADS/ADX	Metasys Device Manager inter-process communication.
9003	Johnson Controls Product Update	TCP	ADS/ADX	Port to query for Johnson Controls Product Updates.
9505	Johnson Controls Rate Limit Website	TCP	ADS/ADX	Website binding to process rate limiting for requests.
9506	Johnson Controls Rewrite Website	TCP	ADS/ADX	Website binding to route API requests to appropriate micro-services.
9507	Johnson Controls Website	TCP	ADS/ADX	Main internal website binding hosting APIs.
10000	PhantomJS	TCP	ADS	Involved in generating PDF files in Metasys UI Reports.
25672	Rabbit MQ/Erlang	AMQP	ADS/ADX	Inter-node and CLI tool communication.

Table 1.6.1.3: Wireless Port numbers and protocols

Port	Protocol	Use	Devices	Inbound / Outbound	Description
80	HTTP 802.11b/802.11g	TCP	Computer (Web Browser)	I	Used to access local UI
443	HTTPS	TCP	Web Browser	I	Used to access local UI
4050 ¹	Wireless Many-to-One Sensing	UDP	WRS-RTN	I/O	Used for wireless supervisor integration; recommended UDP port number.
47808	Wireless ZigBee	UDP	Wireless Network Coordinator (WNC)	I/O	Used for wireless supervisor integration; recommended UDP port number.

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

1.6.2 Communication certificates

Certificates are important and discussed in all three sections of this hardening guide. They play a critical part in cybersecurity by allowing encrypted connections to validate the entity/entities with which they are communicating, while reducing the likelihood of bad actors.

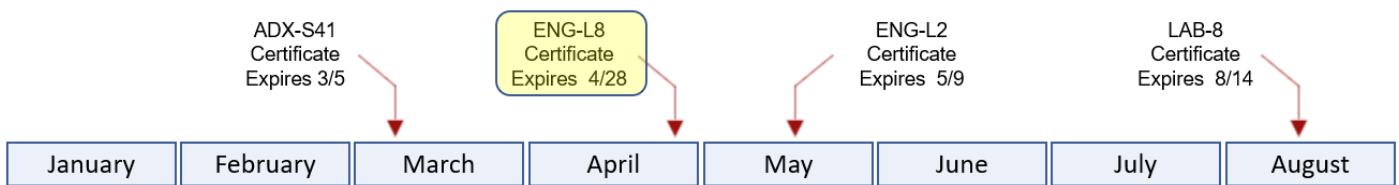
- Section 1.2.12 - Metasys configurable attribute called the **Certificate Renewal Period**
- Section 2.6.2 - How to load TLS certificates
- Section 3.1.12 - Building a maintenance routine for renewals

Most installations have multiple certificates installed, each with a different expiration depending on when they were installed.

Example:

Figure 1.6.2.1 depicts an example with 4 certificates expiring on different dates. Let's follow certificate **ENG-L8** as this will teach us how to plan for and correctly set the Certificate Renewal Period.

Figure 1.6.2.1

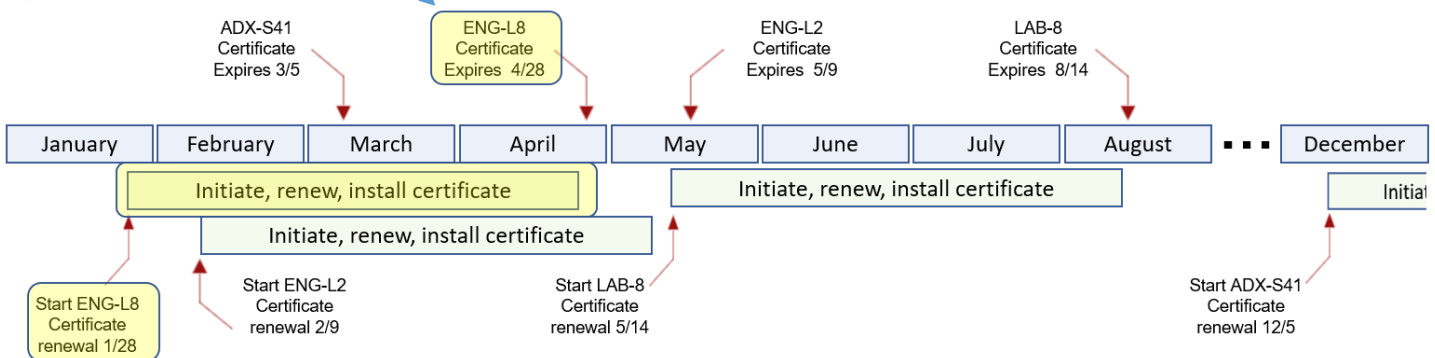


Each organization will have a varied process and timeline to renew certificates. Consult with the local IT department and review related policies to learn how long this task will take. This timeline must be identified, then added to your plan. In this example assume it takes an organization 90 days to initiate, renew and install each certificate.

We now know this task must be started a minimum of 90 days before a certificate expires.

Figure 1.6.2.2 takes **ENG-L8** expiration date of 4/28 and works backwards, adding a 90-day, light green box to discover our **Start** date of 01/28.

Figure 1.6.2.2



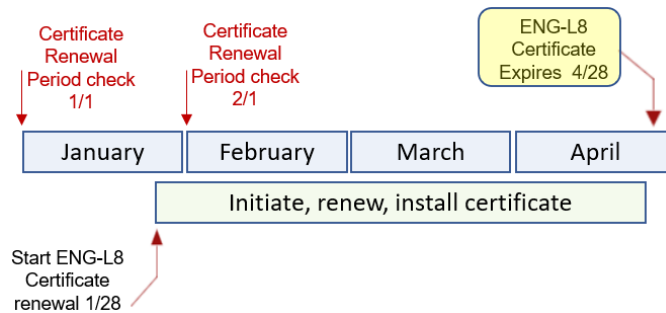
To keep all certificates current, configure the **Certificate Renewal Period** attribute to 120 days minimum (90-days for the process + 30-day buffer).

Note: For additional assurance, set the attribute higher (Max is 180).

The reason we need to include a buffer is illustrated below in figure 1.6.2.3:

- Assume certificates are set to be checked the first day of every month
- The task to renew **ENG-L8** in this example takes this organization 90 days (01/28 – 04/28)

Figure 1.6.2.3



For certificate **ENG-L8**:

- On January 1st, a 90-day review will report all certificates that expire through ~March 31st
- On February 1st, a 90-day review first reports certificate **ENG-L8** expiring on 04/28, which is too late for a 90-day processing time. Setting a reminder for ≥ 120 days will capture this task in time.

1.7.0 Network planning

This section describes network planning including infrastructure protection.

For additional network planning information on:

- How to plan your Metasys network and implementing virtual networks (VLANs) see document Metasys IP Networks for BACnet/IP Controllers Technical Bulletin (LIT-12012458)
- BACnet/SC controllers, see document Metasys BACnet/SC Controllers BACnet/SC Workflow Bulletin (LIT-12013959)

1.7.1 Trust boundaries overview

A trust boundary within a system is the boundary in which data is passed between components that do not share an equal level of trust. Products that are not part of the Metasys system or do not provide methods to sufficiently authenticate a component or user may be regarded as having a lower level of trust. Networks may also have different levels of trust. For example, an isolated network with only video cameras and NVRs is usually trusted more than a shared use network such as the corporate IT network or a remote network.

When the trust deviation is beyond the risk tolerance, it is best to control the flow of data between trusted and untrusted network using a switch or router with data flow control capabilities, such as a firewall.

1.7.1.1 Isolated LAN

The Isolated Network architecture is applicable in cases where there is no common IT network (for example, all tenants within a building build out their own private IT networks) or when the BAS network is

not allowed to connect to the IT network. An Isolated Metasys BACnet/IP network can also be deployed as a provisional network for new construction prior to the availability of the IT network. The Isolated Metasys BACnet/IP network can then be converted to a Connected Metasys BACnet/IP network once the IT network is available.

1.7.1.2 DMZ

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

We do not recommend putting any Metasys equipment in the DMZ.

1.7.1.3 Firewalls

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

Different types of firewalls that can be used with Metasys:

Proxy firewall

An early type of firewall device, a proxy firewall serves as the gateway from one network to another for a specific application. Proxy servers can provide additional functionality such as content caching and security by preventing direct connections from outside the network. However, this also may impact throughput capabilities and the applications they can support.

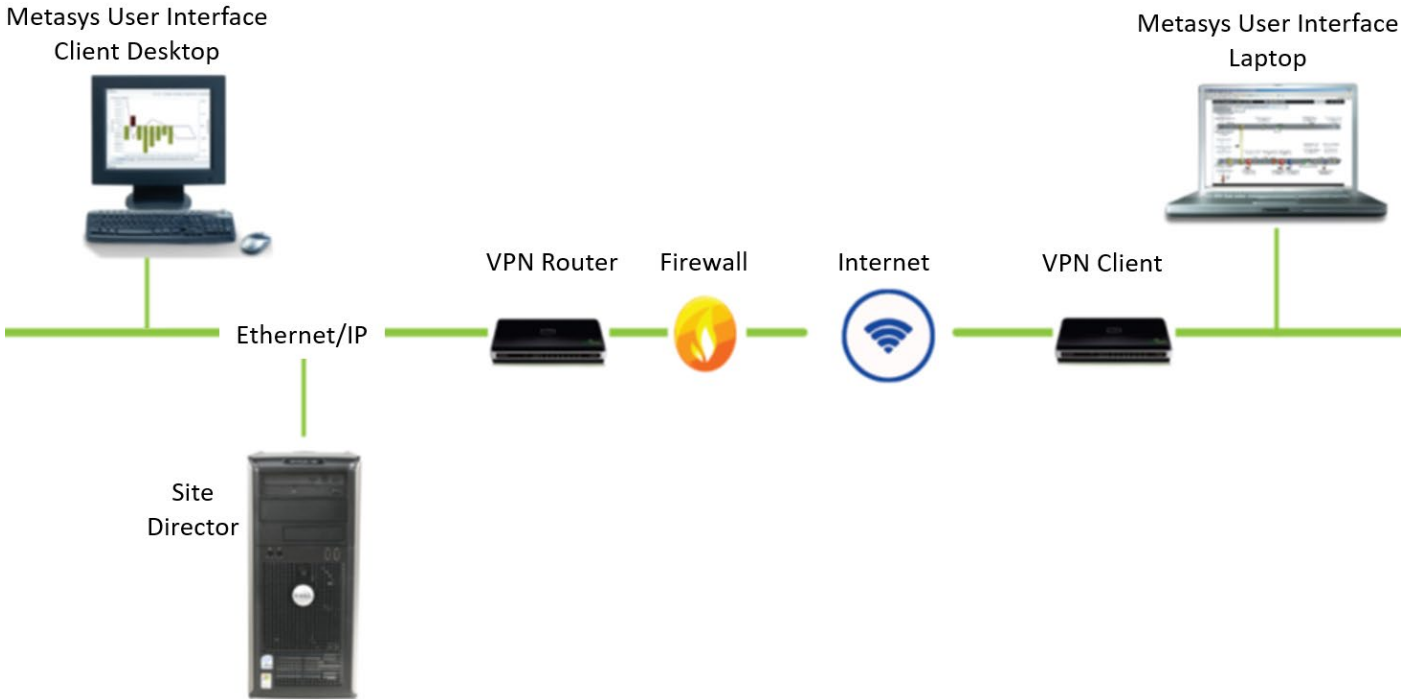
Stateful inspection firewall

Now thought of as a “traditional” firewall, a stateful inspection firewall allows or blocks traffic based on state, port, and protocol. It monitors all activity from the opening of a connection until it is closed. Filtering decisions are made based on both administrator-defined rules as well as context, which refers to using information from previous connections and packets belonging to the same connection.

1.7.1.4 Secure Remote access and VPN

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

Figure 1.7.1.4.1: Metasys system Internet communication by using VPN



1.8.0 Hardware and software requirements

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

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

It is important to note that operating systems and computing capabilities change rapidly. A computer that is adequate for today's applications may be inadequate in a year if additional system features and functions become required. Configuration requirements for computers running Metasys software may be upgraded on a regular basis to reflect these changes.

Refer to the Metasys System Configuration Guide (LIT-12011832). See section: Technical specifications and requirements (Pages 74 through 95), for specific computer requirements for all Metasys software products and tools.

Note: Certain installations will require additional storage capacity on the system or the ability to offload files to another location. For example: DoD auditing requirements for SQL and IIS. Department of Defense (DoD) auditing requirements for SQL and IIS will require additional storage capacity on the system or the ability to offload files to another location. As an option, Metasys can be configured to send audits / Event alarms to up to three external Syslog servers.

2 Deployment

The contents within this section address how to initiate secure deployment for new installations, how to harden Metasys and additional steps after commissioning required before turning over Metasys to runtime operations.

2.1.0 Deployment overview

Security hardening of Metasys begins prior to deployment with careful planning as outlined in Section 1 of this guide. It is a good practice to review that section prior to deployment to fully understand the security feature set of Metasys, its architecture, data flow and requirements before physically installing and making application specific configuration changes.

In this section more details are provided to help the installer prepare for deployment:

- Physical installation considerations
- Default security behavior
- Resetting factory defaults
- Considerations for commissioning
- Recommended knowledge level

The Metasys Server setup is a comprehensive utility that installs the Metasys Server, third-party components required by the Metasys Server software, and many of the Microsoft® Windows® components required by the Metasys system.

2.1.1 Physical installation considerations

Physical installation considerations of components within your Metasys solution are covered in section 1.3.0 – Intended Environment.

When installing Metasys software, use the instructions provided in the installation guide. Keep in mind that both the physical access and physical installation of the device can impact cybersecurity.

Physical server access enables actions that cannot be authenticated and logged electronically through the capabilities of Metasys. To prevent unauthorized access, be sure to place the device in a room, on a metal panel, cabinet or enclosure that can restrict access (for example, mechanical lock or physical access control). When communication wiring goes through areas of lower trust, consider using protective electrical wire conduit.

2.1.2 Getting started

Before installing Metasys, consider the following guidance. Certain products are installed during the installation process while others are optional and not installed. To help you better understand, please review the Metasys Server Installation and Upgrade Guide Release 12.0 document (LIT-12012162).

Operating system patches. You may decide to patch your system before installation of Metasys or after. Please see section 2.4.0 to update Metasys to latest Release. Please consult Microsoft for patches available for your server OS.

2.1.3 Resetting to the factory default settings

If a Metasys component was previously used as part of another installation or used in a test environment, the engines should be reset to factory defaults before being put into service in a new deployment. In the case that an engine would need to be sent for repairs, it is advised to first wipe the device clean. To perform the reset, you must use the System Configuration Tool (SCT).

2.1.4 Considerations for commissioning

In some applications the default settings may not be sufficient to fully commission the system. Functions that will not be used during the commissioning process should be disabled.

In the commissioning phase, a less secure configuration may be used before the full infrastructure is available to speed up the deployment process (for example, using wireless). Once the commissioning phase is complete, be sure to remove the temporary infrastructure and harden the system further before turning over to full runtime operations.

2.1.5 Recommended knowledge level

The person confirming that the proper hardening steps are executed should be experienced in Metasys administration and networking technologies. Completion of the Metasys basic and advanced installation courses is recommended. Please consult the JCI Learning and Development site for course registration.

Helpful training links which require credentials from JCI employees to logon:

- <https://johnsoncontrols.edcast.com/>
- <https://my.jci.com/sites/BESalesOpsLearn/BESalesOpsTech/Pages/welcome.aspx>
- <https://my.jci.com/sites/Training-and-Operations-Support/L&D>

2.2.0 Hardening

While Metasys has several secure-by-default safeguards, we recommend additional hardening to meet the security requirements of the target environment.

In this section configuration settings labelled as “minimum baseline protection” are provided as general guidance; However, the minimum baseline protection may not be sufficient for the target application. It is important to apply to the correct level of protection as warranted by policies and regulations that may govern the application security settings for a deployment instance of Metasys.

NOTE for US Government installations: U.S. government agencies may have additional hardening requirements. For example, the DoD requires installing SQL and IIS on different drives or partitions. Be sure to reference the applicable Security Technical Implementation Guide (STIG) which list out all the specific software requirements. STIGs can be downloaded from the following public web site:

<https://public.cyber.mil/stigs/>

2.2.1 Hardening checklist

- [Hardening Step 1: Disable TLS 1.0 and 1.1](#)
- [Hardening Step 2: Disable unused Ports](#)
- [Hardening Step 3: User Account Settings](#)
- [Hardening Step 4: Update Metasys to latest Release](#)
- [Hardening Step 5: Adding BACnet/SC as an option](#)
- [Hardening Step 6: Load TLS certificates](#)
- [Hardening Step 7: Configure Audit log](#)
- [Hardening Step 8: Backup and Restore](#)
- [Hardening Step 9: Web Server maxQueryStringLength setting](#)

2.2.2 Disable TLS 1.0 and 1.1

Metasys uses secure HTTP with Transport Layer Security (TLS) 1.2 between the SCT computer, all Metasys servers, and network engines that are upgraded to Metasys Release 9.0 and later. When using the optional BACnet/SC in your implementation, you will use TLS 1.3. The Windows registry of your computer is used to see which versions of TLS are being used.

Hardening Step 1: Disable TLS 1.0 and 1.1.

If your system does not need to use TLS 1.0 and TLS 1.1 and your customer's IT policy allows the change, we recommend disabling these two versions. Keep TLS version 1.2 and later enabled. For general information on how to implement TLS or SSL, refer to <https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings>.

Note: Ensure that you have all patches of SQL server applied which do not support TLS 1.0 and TLS 1.1.

2.2.3 Disable unused Ports

Unused ports should be closed unless they are specifically needed for Metasys or another approved use / application to function. In section 1.6.1 we reviewed the ports and protocols that need to be open based on the features being used.

Hardening Step 2: Disable unused ports

Ensure that the ports corresponding to your Metasys system from section 1.6.1.x are open. To harden your system, block all ports that are not in use.

2.3.0 User management best practices

Following best practices for managing user accounts, account credentials and authorizations (permissions) can greatly improve the security for the system. Some guidance is presented in this section. For additional guidance, NIST standards such as SP 800-63 Digital Identity Guidelines may be consulted.

Do not share accounts. It is best practice to create unique user accounts for each administrator for the Metasys system. The proper configuration of individual user accounts assures that security best practices are followed and that all user actions are audited.

Table 2.3.0.1

Feature	Description
User account password length	8-50 characters <i>Note: If you're using AD LDAP or ADFS, limitations apply. See specific Metasys or Microsoft documentation.</i>
Inactive Sessions	5 minutes timeout (30 is the default)
Password history	10 (default)
Maximum Password Age	365 days for user level accounts (default is 90) 60 days for admin level user accounts
Timesheet	The Time Sheet tab allows administrators to place time-of-day restrictions on user login. Users may log in to the system during the selected hours but denied access when they try to log in during unselected hours
Temporary user account	Allows the user to access the system as a temporary user. The user can access the account if it has not expired. When expired, the user is logged out of the system.

2.3.1 Metasys User Roles and Permissions

Only Metasys administrators can access the User Management feature. Administrators add existing Active Directory service users to the Metasys system and assign Metasys system privileges using the Security Administrator System.

Roles

You can assign a minimum of one of the following roles to the local or Active Directory LDAP user account.

- User: Read only access
- Operator: Assigned privileges from a list in the User Assigned Dialog Box
- Maintenance: Assigned privileges from a list in the User Assigned Dialog Box
- Administrator: Access to the full Security Administrator system using the Metasys system online user interface and the SCT

Permissions

Add the proper permissions for each user account. Each user can have one type of permission.

- Standard Access: The Metasys local system user or Active Directory service user can access all authorized features of the online SMP UI and the SCT. Users can also access the Metasys UI. Note: If you have Standard Access and the Advanced Reporting privilege, you can use the Metasys Advanced Reporting System.
- Tenant Access: The Metasys local system user or Active Directory service user can access all authorized features of the Metasys UI.
- API Access: API access is required to use the Metasys Application Programming Interface (API) and for API calls to function. With API access, users can retrieve information from the Metasys system network. Use API access to read and write Metasys system data from a custom application with the same high level of security as when you access system data through the SMP UI. The Metasys local system user or Active Directory user can access the Metasys API, all authorized features of the Metasys UI and can also access limited features of the SMP UI.
NOTE: We do not recommend that users with API access are given the administrator role as that user will have full administrator rights in the Metasys UI and limited administrator rights in the SMP UI. See Security Administrator System Technical Bulletin (LIT-1201528) for more details.

Note: When you assign a role and permission to a user's account, apply the principal of least privilege. See section 2.3.6 for more information on applying the least privilege.

Figure 2.3.1.1 – Security Administrator System Screen

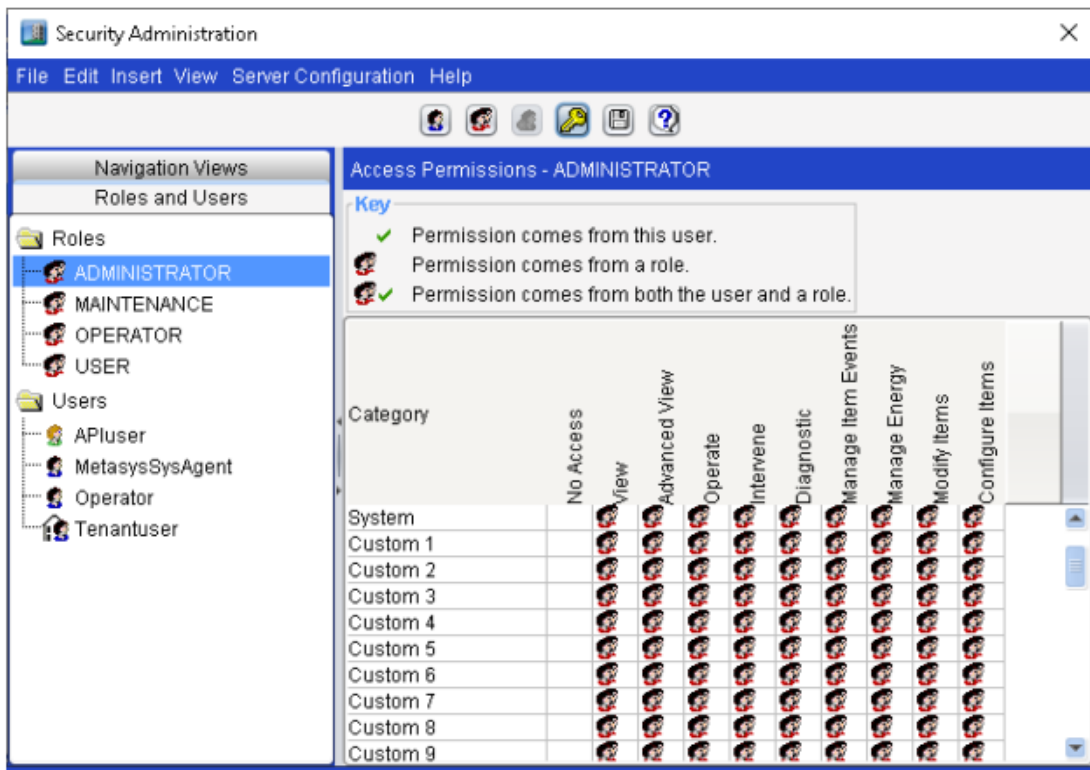
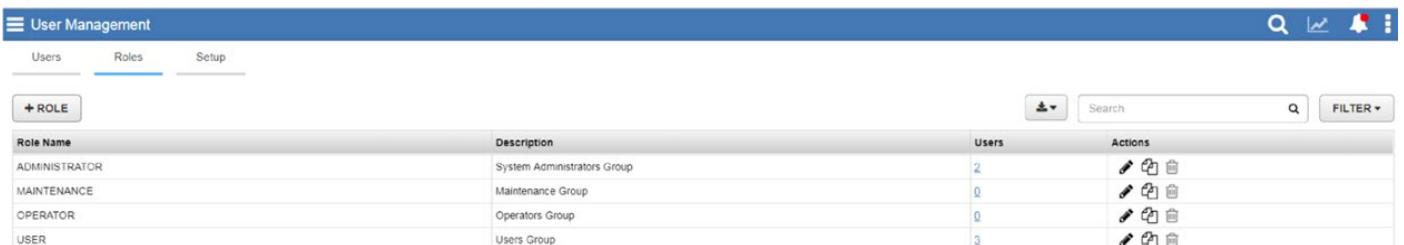


Figure 2.3.1.2 – Metasys UI (MUI) User Management: Users Tab



Figure 2.3.1.3 – Metasys UI (MUI) User Management: Roles Tab



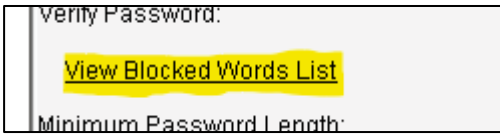
2.3.2 Metasys Local User Accounts

Metasys Local Users must use strong or complex passwords, comprised of the criteria shown in table 2.3.1 at a minimum. We recommend suggestions in the right column for further hardening.

Hardening Step 3: User Account Settings

To harden your system, update the following settings for user account attributes and policies:

Table 2.3.2.1 – User Account Passwords criteria

Attribute	Minimum requirement	Recommended for further hardening
Password total length	8 characters	Create passwords of at least 12-15 characters (max 50)
Special characters	1 character such as -, ., @, #, !, ?, \$, %. All other special characters are invalid, including spaces.	Include 2 or more non-succession special characters
Upper Case characters	1 character	Include 2 or more
Lower Case characters	1 character	Include 2 or more
Numbers	1 character	Include 1 or more
Blocked Words List	Add list of words as suggested from an online Blocked Words List 	Add company and product names associated with project (e.g., JCI, Metasys, OpenBlue, etc.)
Special rule	The password cannot contain three consecutive characters from the user account name.	

* Note: For additional details about the Blocked Words List, view details at his link - <https://docs.johnsoncontrols.com/bas/r/Metasys/en-US/Security-Administrator-System-Technical-Bulletin/12.0>

Figure 2.3.2.1 SMP UI User Properties Tab

User Properties | User Profile | Roles | Time Sheet | Account Policy

User Name: Operator
 Description: Metasys System Operator
 Password: *****
 Verify Password: *****

[View Blocked Words List](#) | [View Password Policy](#)

Minimum Password Length: 8
 Maximum Password Length: 50

Single Access User
 Temporary User

Expires On: Monday, October 29, 2018

User Must Change Password at Next Logon
 User Cannot Change Password
 Account Disabled
 Account Locked Out
 User Can Modify Own Profile
 User Can View the Item Navigation Tree (Default Tree)
 User Can Disable Alarm Pop-Ups

Access Type: Standard Access

Figure 2.3.2.2 MUI User Operator Tab

Operator

[Back](#)

Full Name
Operator
Username
Operator
Email
Role
OPERATOR
Access
Standard
Last Login
04/13/2022 9:35 AM
Status
Active
Type
Metasys

User Details | Account Settings | Timesheet | Category Access

Full Name
Operator
Description
Metasys System Operator
Username *
Operator
Email
Phone Number

Actions
 Unlock Account
 Force Password Change
 Disable Account
 User Can View The Item Navigation Tree (Default Tree)

Single Access User
 Single Access User
 User Can Modify Own Profile
 User Cannot Change Password
 Temporary User

Expires On
04/13/2022

Role *
SELECT...
OPERATOR

System Privileges
SELECT...

From Role(s):
Discard Acknowledged Events

Minimum Password Length * 8
Maximum Password Length * 50

Access Type
Standard

Language
English (United States)

CANCEL | SAVE

2.3.3 Metasys LDAP Active Directory User Accounts:

Metasys supports the following implementation of Active Directory:

- Active Directory Federation Services (ADFS) was covered back in section 1.2.3
- Lightweight Directory Access Protocol (LDAP) discussed below

You can log on using your Active Directory username and password if the Active Directory login feature is set up in the Metasys system. Metasys uses LDAP (Lightweight Directory Access Protocol) for directory services authentication. This optional component provides the convenience of Single Sign-On (SSO) access, a capability that permits users to log on to multiple, secured application User Interfaces without re-entering their username and password.

The authentication of the Metasys Active Directory LDAP account happens outside of Metasys. However, when the Domain controller does provide the authentication of the LDAP user account, then the account is granted access to Metasys with the given Metasys permissions set up for that AD LDAP account.

Using the Active Directory LDAP account, you can configure the account's session time out, and the optional timesheet to restrict which days of the weeks and hours of the day the user is allowed to access Metasys. For more information on Active Directory and the Metasys system, refer to the Network and IT Guidance Technical Bulletin (LIT-12011279).

2.3.4 No shared accounts

Unique accounts should be used during all phases of operation for Metasys. Installers, technicians, auditors, and other deployment phase users should never share common user accounts to ensure audit trails of their actions.

When user accounts are shared, it no longer becomes possible to determine which specific operator performed actions. We recommend that all users have named accounts, including JCI technicians.

However, there is one Metasys exception to this rule. During a new Metasys deployment, employing multiple installers, you will need to share the **MetasysSysAgent** account. The MetasysSysAgent password should be stored within a password manager so that it can be securely shared with other members of the installation team.

2.3.5 Change default passwords

Default passwords should be changed as these published defaults are easily guessed by unauthorized users and automated scripts can use them to gain access.

Note: Since Metasys 6.0, you will be prompted to change your password after first logon.

2.3.6 Least privilege

The principal of least privilege means the following:

- Only the minimum necessary rights should be assigned to a user that requests access to Metasys
- Access rights should be in effect for the shortest duration necessary to do their job

Granting permissions to a user beyond the scope of the necessary rights of an action can allow that user to obtain or change information in unwanted ways. The best practice when assigning Metasys access rights is to only give an individual user the necessary role and permissions to their job and nothing more.

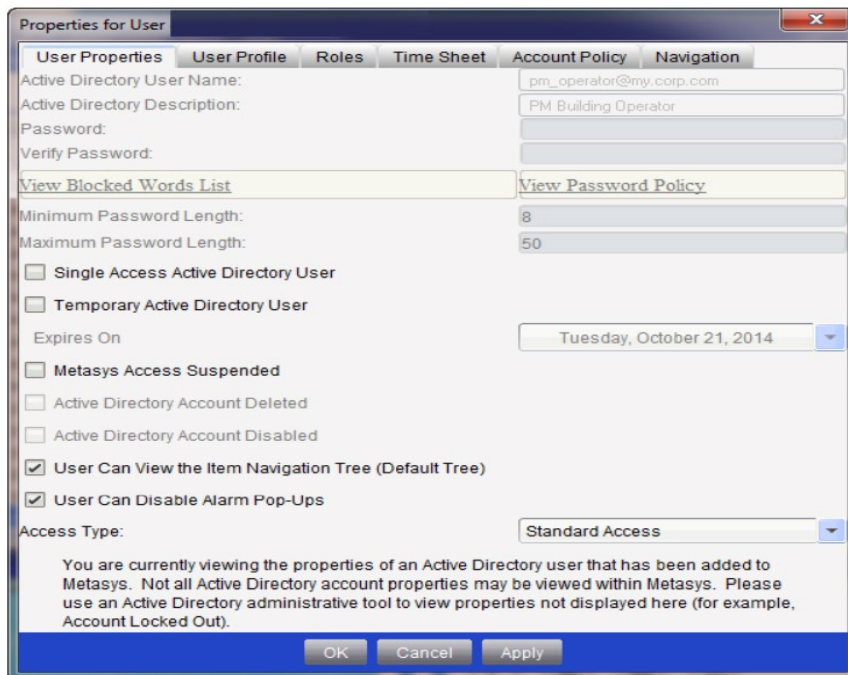
2.3.7 Separation of duties

No single user should have full access rights to perform all administrative actions. By separating duties among multiple operators, the amount of power held by a single person is restricted and aids in preventing fraud. Examples of separation of administrative duties - by site, building, sub-system (Fire, HVAC, security), building owner vs. integrator role, functions (operations vs network management vs. backup). This reduces the risk of insiders successfully committing fraud.

2.3.8 Centralized user account management

Identity Management Systems (IDMS) offer enhanced security over the local management of users within Metasys. An IDMS, such as Microsoft Active Directory or a Lightweight Directory Access Protocol (LDAP) capable IDMS, can provide user account management for multiple devices or systems. By centrally managing user accounts, an administrator can assure consistency throughout the domain the IDMS manages. This assures that when an account is disabled in the domain, access by that user is disabled everywhere in the domain. Furthermore, IDMS provides a centralized location to manage password policies which dictates password formation rules including, length, capitalization, reuse, and expiration. See Security Administrator System Technical Bulletin (LIT-1201528) for more details.

Figure 2.3.8.1



	Required field	Optional field
AD Username	X	
Metasys Session Timeout	X	
Timesheet		X
Single access Active Directory user		X
Temporary Active Directory user		X
Metasys access suspended		X
User can view the item navigation tree		X
User can disable alarm pop-ups		X
Dormant User account feature		X

2.3.9 Password policy

Customers often have password policies that all systems must support. Make sure to define the password requirements and the procedures your organization must follow to manage passwords and set a high level of security. Here are some guidelines to follow:

- Passwords are to be treated as sensitive and confidential
- Do not write down passwords where it can be discovered such as on paper, chalkboard, or dry erase boards
- Do not share your passwords with anyone
- Do not use the same passwords for personal use and at work

2.3.10 Kiosk Service Accounts

Metasys does not have a user account specifically used for Kiosks. However, the recommendation is to set up a new user account for the Kiosks and allow only view only information with no session timeout.

Recommendations

- Name this account a Kiosk account
- A Kiosk account must use a **User** role. Never use an **Administration** role.

2.3.11 User management best practices

Following best practices for managing user accounts, their credentials, and authorizations (permissions) can improve the security for the solution.

2.3.11.1 *Centralized user account management*

With Metasys you can use Active Directory LDAP user accounts (See section 2.3.3). A benefit of using Active Directory LDAP accounts is that a customer's IT department can manage Active Directory LDAP Metasys user accounts. While the Active Directory LDAP authentication is done outside of Metasys, each Active Directory LDAP session is given a username in Metasys with the session timeout, dormant user account settings, and timesheets configuration.

Metasys does not store the Active Directory LDAP password. When a user logs on to a computer, Windows caches their Active Directory service credentials and the Metasys system automatically retrieves them during the Windows Integrated Authentication with IIS process on the Metasys server, or SCT.

2.3.11.2 *Strong passwords*

Strong passwords should be used to minimize the risk of password guessing. Automated forms of password guessing such as "dictionary attacks" and "rainbow tables" can run through commonly used passwords and can be successful if strong passwords are not used. You can strengthen a password with length and complexity. The length of a password has the biggest impact on making password guessing difficult.

2.3.11.3 *Password aging*

Password aging is a technique used to reduce to possibility of password exploitation. The **Maximum password age** applies to Metasys Local User accounts. Set the account policy to define a period in days that a user can use a password for before they are prompted to change it. You can set passwords to expire after any number of days between 1 and 180 (See note below). To specify that passwords never expire, click **Never Set to Expire**.

Note: The Metasys system defaults the Maximum Password Age for an admin user account to 60 days, and the non-admin user accounts to 90 days. Starting with patch 11.04 and 12.02, the maximum configurable setting is increased to 365. See table 2.3.0.1 for hardening recommendations.

2.3.11.4 Password history

Password histories are used to mitigate against password reuse. Metasys user accounts must abide by the configured password history, with at least 11 previous passwords remembered. For further hardening, refer to the Metasys customer's IT policy on password history. If no such policy exists, leave the password history set to 11 as best practice.

2.4.0 Update Metasys to latest Release

It is always best practice to harden Metasys by updating to the latest patch Release. Patches often contain fixes which strengthen the security of the application.

Hardening Step 4: Update Metasys to latest Release

Patches and updates can include cybersecurity enhancements, as well as fixes to known issues. Review the release notes and prioritize the benefits of the patch or update.

Check for updates and patches of third-party components such as networking equipment and operating systems by consulting with the respective vendor and update these accordingly.

2.5.0 Adding BACnet/SC as an option

Section 1.2.11 discusses the planning behind adding BACnet/SC, including features, licensing requirements, certificates, and functionality. Adding BACnet/SC will harden your system

Hardening Step 5: Adding BACnet/SC as an option

Purchase product code M4-BACNETSC-0 (See section 1.2.11) and license it for your Metasys system.

Acquire and apply certificates. Section 3.1.12 discusses the importance of regularly checking certificate expiration dates. Do not let your certificates expire as some ECC certificates may take > 90 days to renew.

Engines. Metasys Engines will have a Self-signed RSA certificate for the communication between Metasys devices (Engine / Server / etc.) and will also have an ECC certificate specific to BACnet/SC.

Servers. For Metasys Release 12 servers it will be the same if the server is a BACnet/SC primary or failover Hub. If it is not a BACnet/SC primary or failover Hub, then it will have an RSA certificate. You will see instructions how to generate the CSR using the Windows server OS S-channel tool. For additional details see Network and IT Guidance Technical Bulletin (LIT-12011279) and the Metasys BACnet/SC Workflow Technical Bulletin (LIT-12013959).

Running Johnson Controls IP Controllers.

If you're using the Johnson Controls IP Controllers CVEs and CGE's, you will use the JCT tool to create the CSR file and sign your certificates.

Running third party BACnet/SC devices.

The CSR file will be created by the third party using their specified tool. However, we will take their CSR PEM files, get these signed and returned for download into the devices with their tool.

If third party devices are present, ask if it is a Primary or Failover Hub, otherwise called a BACnet/SC Node.

Running BACnet/IP and BACnet/SC. For larger sites, it is common to leave BACnet/IP running with BACnet.SC.

Important Note: If you mix SC and IP on a site, it must be done with care, especially at the supervisory level. From a BACnet point of view it can be viewed as two different sites. All the devices that talk

BACnet/IP are one site and they can communicate to each other as well as broadcast to each other, if BBMDs are set up correctly. Likewise, all the BACnet/SC devices can communicate with each other and see each other's broadcasts. Supervisory devices that are in dual communication mode participate in these two different sites, but they do not route between them. If you have an IP equipment controller in Secure Connect Only Mode it can talk to its supervisor if the supervisor is in Dual SC and IP Mode, or Secure Connect Only Mode. An IP equipment controller in Secure Connect Only Mode can only talk to peer equipment controllers that are in Secure Connect Only Mode. A supervisory device in Secure Connect Only Mode can only talk to other supervisory devices in Secure Connect Only Mode or Dual SC and IP Mode. This includes broadcasts.

Refer to Appendix C – FAQs for additional details on BACnet/SC

2.6.0 Communication hardening

Communication hardening limits an attacker's ability to gain access to Metasys. Attackers look for weakness in communication protocols, and communications that is left on encrypted and unauthenticated include the risk that the attacker will be successful in their efforts. Employ techniques to harden the communication interfaces and the transmission of data within this section.

2.6.1 Least functionality

Least functionality is a security measure designed to limit functions only to those that are required for the target application and communication sessions used at a given time. In configuring components in this manner, the attack surface is reduced and with it the risk of a cybersecurity breach is minimized.

2.6.1.1 Wireless ZFR configuration

The ZFR wireless system extends ZigBee wireless capability to the Metasys BACnet Field Bus. Depending on the model you have, consult the specific configuration guide (such as the ZFR18xx series) to further harden security on this device.

For example, the security features available on the ZFR1830 are:

- Wireless devices can only be added to ZFR mesh network when manually "opened"
- Pre-defined timers automatically close the network to prevent accidental openings
- Standard Zigbee random network keys
- Proprietary key exchange*
- Standard Zigbee AES 128-bit encryption security
- Proprietary ZFR183x messaging structures
- Signed FW Update packages

** Uses multiple JCI Proprietary keys unique to each PAN rather than single public Zigbee key*

For more information see the Metasys WRG18xx/ZFR1x3x Pro Series Technical Bulletin (LIT-12013553).

2.6.2 Communication certificate support

[Hardening Step 6: Load TLS certificates](#)

General information. HTTPS encrypts communications traffic but does not verify the identity of the remote host without a properly configured digital certificate.

For Metasys Releases 8.1 and higher, a certificate is used between the Metasys application Servers and Engines, and any Metasys client to the Metasys application servers or Metasys engines.

A Self-signed certificate (default certificate) is created at the time of the server installation unless one exists. Group certificates or Certificate Authority (CA) signed certificates are also supported for the Metasys application server and engines.

For more information see the Metasys Release 12.0 Network and IT Guidance Technical Bulletin (LIT-12011279) - Appendix: Certificate management and security.

Note: Wildcard certificates are not supported on Metasys.

Metasys application server specific. Default certificates are self-signed and can only be used for encryption. Privately trusted certificates or CA signed certificates are also supported for the Metasys application server and engines.

See the Metasys Release 12.0 Network and IT Guidance Technical Bulletin (LIT-12011279) - Appendix: Certificate management and security for details how to install the certificates on the Metasys application server.

Metasys engine specific. Use the Certificate Management option in SCT to manage trusted certificates that are stored in network engines. For details, refer to the SNE Commissioning Guide (LIT-1201645) Appendix: Certificate Management.

2.6.3 FIPS 140-2 support

FIPS 140-2 was defined by the U.S. government with a purpose of defining how a cryptographic module will protect unclassified, yet sensitive information.

See section 1.2.4 for the standard, definition and how it relates to Metasys online devices. FIPS 140-2 is an optional feature for sites where it is specified as a requirement. For the server class products ADX/ADS/OAS/NAE8500/LCS8500, one must purchase the M4-FIPS-0 product code and license it.

If you have purchased this add-on option, follow the installation instructions to enable this functionality.

See Metasys Server Installation and Upgrade Instructions (LIT-12012162) for additional details.

2.7.0 Configuring security monitoring features

In this section you can find information on configuring security monitoring features.

2.7.1 Audit Logs

[Hardening Step 7: Configure Audit log](#)

The Metasys system creates and maintains independent local repositories for events and audits. Metasys System Configuration Guide (LIT-12011832) describes their configuration. Events and audit entries from Metasys can be optionally configured and sent up to three customer Syslog servers where a customer may elect to look at audits and / or events for logins at odd times, logins from odd locations, or failed login attempts.

MUI Specific. The MUI Cyber Health Dashboard's **User Activity** widget can give you the number of unsuccessful, successful, and locked user accounts on a daily, weekly, or monthly period. Note: If you're using MUI, then you would go to **System Activity** to view your audits and alarms in a list sorted by date and time.

SMP UI Specific. The Metasys Audit Log, called the **Audit Viewer**, will show logged audits along with the IP address of the client that was logged in with. The **Event Viewer** will display the alarms and system events listed by date and time.

2.8.0 Availability hardening

Availability hardening is important to keeping your system up and running.

The three letters in "CIA triad" stand for confidentiality, integrity, and availability. The CIA triad is a common, respected model that forms the basis for the development of security systems and policies. For BAS systems, the main items is the Availability (is the system up and running) then Integrity (are the BAS communications messages unchanged and still intact) and lastly is the confidentiality still intact for the BAS communications.

2.8.1 Backup/restore

[Hardening Step 8: Backup and Restore](#)

SCT's existing functionality for uploading the archive and security database for an engine and Metasys application server provides the ability to save the Metasys configuration information and even export that data for offsite storage. Engine certificates can also be backed up. Server certificates must be backed up using the Windows Certificate Management features (the Metasys HTTPS certificates). Metasys online server databases (e.g., Historian, Audit, etc.) must be backed up using the Metasys Database Manager (MDM) tool.

More details on the process and tools needed to completely backup and restore a Metasys application server can be found in the Out of Place Upgrade procedure documentation for the Metasys application server.

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

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

See Network and IT Guidance Technical Bulletin (LIT-12011279) for additional guidance.

2.8.2 Web Server

Based on your IT policies and guidelines, you may want to update the **maxQueryStringLength** setting. The Metasys default setting is 32768. However, some organizations opt to make it the smallest value which is 4096.

Important notes:

- Before making the changes below, it is strongly recommended that these files are backed up.
- Execution of the hardening steps below is OPTIONAL and will require a server restart.
- These changes will only be applicable to ADS, ADX, OAS, NAE85, and LCS85 servers.

[Hardening Step 9: Web Server maxQueryStringLength setting](#)

The **maxQueryStringLength** setting can be updated in the following configuration files manually post installation. The setting is located within multiple files because of the three additional websites which make up our reverse proxy.

- 1) C:\inetpub\wwwroot\web.config
- 2) C:\inetpub\Johnson Controls\web.config
- 3) C:\inetpub\Johnson Controls Rate Limit\web.config
- 4) C:\inetpub\Johnson Controls Rewrite\web.config

Change the settings to:

```
<configuration>
  <system.web>
    <httpRuntime maxRequestLength="1048576" maxQueryStringLength="4096"
maxUrlLength="65536" />
  </system.web>
  <system.webServer>
    <security>
      <requestFiltering>
        <requestLimits maxAllowedContentLength="1073741824"
maxQueryString="4096" />
      </requestFiltering>
    </security>
  </system.webServer>
</configuration>
```

After the four files above are updated, and saved, the Metasys server must be restarted for the changed settings to take place.

3 Maintain

In section 1 we learned that many components work together to provide a custom solution. This section addresses how to monitor for potential cybersecurity issues and maintain protection levels as conditions change for several solutions. This means that some items in the checklist may not be part of your solution and/or within your contract. From the research you gathered in Section 1, and the terms within your contract, determine the items in table 3.1.0 that apply to your system and focus on only those items.

An audit that produces a report indicating low cybersecurity risk is a very positive result and suggests that the deployment was conducted with a high degree of care and consideration. However, new attack vectors, combined enhanced hacking tools and more advanced testing techniques may, in the future, disclose vulnerabilities with the technologies used.

The impacted technologies and their implementation may have been previously well regarded by cybersecurity experts. The discovery of vulnerabilities post the final deployment audit may not reflect the quality of the audit at the time. You may require a higher degree of protection for the environment that Metasys is serving as policies and regulations change over time.

3.1.0 Cybersecurity maintenance checklist

Continuously or periodically practice the following cybersecurity maintenance items. The frequency of their execution will depend on the policies and regulations which govern the site. The typical maintenance periods provided are a starting point and adjusted to best suit the target conditions of the deployed environment

See Table 3.1.0.1 Cybersecurity maintenance checklist on the following page.

Table 3.1.0.1 – Cybersecurity Maintenance Checklist

Item	Description	Immediate	Base on Priority	Daily	Weekly	Monthly	Quarterly	Annual
1	Backup historical data			✓				
2	Backup configuration data	✓						
3	Test backup data						✓	
4	Disable user accounts of terminated employees	✓					✓	
5	Remove inactive user accounts					✓		
6	Update user account roles and permissions						✓	
7	Disable unused features, ports, and services						✓	
8	Check for and prioritize advisories or product notices				✓			
9	Plan and execute advisory recommendations		✓					
10	Check and prioritize software patches and updates				✓			
11	Plan and execute software patches and updates		✓					
12	Review TLS communication certificate expiration dates					✓		
13	Review updates to organizational policies							✓
14	Review updates to regulations							✓
15	Conduct security audits							✓
16	Update password policies							✓
17	Update as built documentation	✓						✓
18	Update standard operating procedures							✓
19	Update MUI logon banners							✓
20	Renew licensing agreements							✓
21	Renew support contracts							✓
22	Check for end-of-life announcements and plan for replacements							✓
23	Periodically delete sensitive data in accordance with policies or regulations	✓					✓	
24	Monitor for cyber attacks	✓		✓				

3.1.1 Backup historical data

Historical data, or SQL data for Metasys, can be the most valuable asset within the Metasys system. You can replace or reconstruct everything else. It is recommended that backups are performed frequently, such as daily. With the recent trend of rising ransomware cases, it is also best practice to utilize off-site backups.

Action	Details	Suggested frequency
Backup historical data	Backup / Restore historical SQL files from Metasys	Daily

3.1.2 Backup configuration data

If you need to restore or replace a Metasys component it is important to have a backup of its configuration data to minimize the time required to restore its functions.

Action	Details	Suggested frequency
Backup configuration data	Backup / Restore device configuration data	Immediate

3.1.3 Test backup data

After completing steps 3.1.1 and 3.1.2, and if your job requires this per the contract, test your backup data on an “Out of Place Upgrade” Metasys application server. This will provide assurance that the data backups contain the expected data and integrity.

Action	Details	Suggested frequency
Test Backup data	Load data from backup media into a non-production Metasys	Quarterly

3.1.4 Disable user accounts of terminated employees

Disable user accounts of personnel who voluntarily or non-voluntarily are terminated from employment immediately.

When using Active Directory (AD) services (section 2.3.3), accounts deleted from AD are automatically disabled from Metasys.

Action	Details	Suggested frequency
Lock accounts	Refer to the Metasys System Administrator System Technical Bulletin Release 12.0 – User properties section.	Immediate

Account Disabled

Account Locked Out

Note: In section 1.2.5 we introduced the **Dormant User Account** standalone feature under the Cyber Health Dashboard. When this feature is enabled, it is useful for managing accounts considered dormant or have not been logged into Metasys for a set period, such as 90 days. From the dashboard, run the **Dormant User Account** report. This will create a report showing the status of Metasys users as either active or dormant.

3.1.5 Remove or “lock” inactive user accounts

Once your Metasys installation is up and running, it is up to our customers to remove or lock any inactive user accounts. For larger installations, it is recommended to lock accounts rather than deleting them.

For example: While employee “X” may still be employed by an organization in which the system is owned, managed, serviced, or used by, “X” may not have utilized their account for a long period. This suggests that independent of being authorized to use the system, “X” does not have a need to use the system and you should remove the user account “X”. This is sometimes referred to as a **use it or lose it** policy.

This best practice reduces the amount of active user accounts in the system and therefore lowers the potential attack footprint. We suggest this be performed monthly at a minimum. Check with your local policy to determine if this should be performed more frequently.

Action	Details	Suggested frequency
Remove inactive accounts	Refer to the Metasys System Administrator System Technical Bulletin Release 12.0 – User properties section.	Monthly

3.1.6 Update user account roles and permissions

While an employee may still be employed by an organization in which the system is owned, managed, serviced, or used by, they may have changed roles or have increased or decrease their need to utilize the system. When adding a role or a permission to a user's account when that user is granted new authorizations due to an organizational role change, be sure to remove Metasys' roles and permissions no longer required or utilized in their new role.

Action	Details	Suggested frequency
Update user account roles	Refer to the Metasys System Administrator System Technical Bulletin Release 12.0 – User properties section.	Quarterly

3.1.7 Disable unused features, ports, and services

Reassess the need for optional features, ports, and services that you do not require, and disable them. This practice will lower the attack surface of Metasys resulting in a higher level of protection.

I.e., Feature – Alarm monitor

Action	Details	Suggested frequency
Disabled unused features	Refer to your product Installation or User manuals. Also refer to sections 1.6.1 and 2.2.3 to disable unused ports	Quarterly

3.1.8 Check for and prioritize advisories or product notices

Find cybersecurity advisories for Metasys at <https://www.johnsoncontrols.com/cyber-solutions/security-advisories> with a registered user account (create a username and password). User account registration is open to JCI customers and authorized representatives. Some Key points to consider:

- Determine if Metasys is impacted by the conditions outlined in the advisories
- Based on how the Metasys system is deployed, configured, and used, will help determine if the advisory may or may not be of concern
- Referring to as-built documentation of the Metasys system will help with this assessment. A well good set of as-built documentation will identify the number of components impacted and their location.
- While advisories call attention to a cybersecurity issue, it is not always possible to take immediate action or execute the full recommendation described in the advisories. If so, prioritization will aid in your planning to ensure that any issue impacting your system is fully and appropriately addressed in order of priority.

Check for advisories or product notices from third party components such as networking equipment and operating systems by consulting with the respective vendor.

Action	Details	Suggested frequency
Check for and prioritize advisories	Refer to the link above that hosts Metasys advisories and explore each week	Weekly

3.1.9 Plan and execute advisory recommendations

Follow the plan determined in maintenance step 3.1.8. Consult with all parties who may be impacted by an advisory or downtime and choose the best time for deployment.

Action	Details	Suggested frequency
Plan and execute advisory recommendations	Plan and execute advisory recommendations	Based on priority

3.1.10 Check and prioritize patches and updates

While a Metasys patch or update may or may not relate to a security advisory, it is always best practice to apply the most current patches and updates. These patches and updates can include cybersecurity enhancements also fixes to known issues. Review the release notes and prioritize the benefits of the patch or update. The overall benefit should include the improved protection that will aid in lowering the cybersecurity risk. Be sure also to check for updates and patches of third-party components such as networking equipment and operating systems by consulting with the respective vendor.

Action	Details	Suggested frequency
Check for and prioritize patches and updates	Explore available patches and updates each week	Weekly

3.1.11 Plan and execute software patches and updates

Follow the plan determined in maintenance step 3.1.10. Consult with all parties who may be impacted by patches, updates or downtime and choose the best time for deployment. Contact your local branch office or Authorized Building Controls Specialist (ABCS) for assistance.

Action	Details	Suggested frequency
--------	---------	---------------------

Plan and execute software patches and updates	Plan and execute advisory recommendations	Base on priority
--	---	------------------

3.1.12 Review TLS communication certificate expiration dates

Metasys uses two main types of communication certificates:

- **Web:** Used in the MUI, SMP and Metasys to Metasys device communications
- **BACnet/SC** (optional in Metasys Release 12.0 installations)

Certificates will expire at different intervals. Because of this we recommend that you validate that certificates on your system are reviewed monthly and renewed accordingly.

To view and change Metasys web certificates, see the following table 3.1.12.1

Table 3.1.12.1

Certificate Type	Device(s)	Update tool
Web	Metasys Engine	SCT
Web	Metasys Server	Use standard Microsoft instructions
BACnet/SC	Any	JCT, MUI or SMP

Note: For viewing under MUI, use the browser's settings under Privacy and Security.

See Network and IT Guidance Technical Bulletin (LIT-12011279) for additional guidance.

Action	Details	Suggested frequency
Review TLS communication certificate expiration dates	Review the Web (MUI, SMP and Metasys) and the BACnet/SC communication certificates to determine when renewals are needed	Monthly

Note: Do not let your certificates expire as the process for some certificates may take > 90 days to renew.

Reminder: Review section 1.6.2 **Communication certificates**.

3.1.13 Review updates to organizational policies

Organizations may update their policies which include cybersecurity requirements. Changes to these policies can impact systems which complied prior to the change. Periodically check to see if policy changes were made and re-assess compliance with those policies.

Action	Details	Suggested frequency
Review organizational policy updates	Collect most recent security policies for your organization	Annual

3.1.14 Review updates to regulations

If Metasys is deployed in a location that is governed by regulation, it is important to check to see if there are any updates to those regulations. In some cases, new regulations are introduced. Whether it is a review of an updated regulation to maintain compliance and a new regulation, an assessment of the changes should be conducted periodically.

Action	Details	Suggested frequency
--------	---------	---------------------

Review updates to regulations	Collect most recent copies of regulations as applicable. Perform a gap analysis against the deployed configuration.	Annual
--------------------------------------	---	--------

3.1.15 Conduct security audits

Periodic security audits are necessary as cybersecurity guidance, organizational policies, regulations, auditing processes, system use, and configuration and threats have likely changed since the last audit. By conducting periodic security audits, you can apply the latest knowledge and reveal gaps in protection previously undetected or created by changes in system use of configuration.

Action	Details	Suggested frequency
Conduct security audits	Perform the tasks listed on your Security audit checklist	Annual

3.1.16 Update password policies

Guidance on password policies is evolving. Password policies should be re-assessed periodically to make sure the right policy is in place for the target environment based on current organizational policies, regulations, and guidance from standards organizations such as NIST.

Update password policies as necessary to keep your system secure that are set forth in the Security Administrator System Technical Bulletin (LIT-1201528) local IT policies, and governing bodies.

Action	Details	Suggested frequency
Update password policies	See section 2.3.9 Password policy	Annual

3.1.17 Update as-built documentation

Be certain to keep the as-built documentation up to date if the Metasys system architecture or component configuration significantly changes. Updates are also usually required if you modify the Metasys database or modify equipment. After every change, evaluate if the as-built documentation is out of date enough to initiate the documentation process.

The task of updating as-built documentation may or may not be included within your current contract. Check your Metasys contract to determine the following:

1. Yes - Updating as-built documentation is included
If so, the contract should describe the frequency (ex. major hardware upgrades, yearly, etc.)
2. No – Updating as-built documentation requires a separate contract

Some installations may require updating the as-built documentation on a more frequent, periodic basis. Work with your account executive if you have questions.

Action	Details	Suggested frequency
Update as-built documentation	Update if the Metasys system architecture or component configuration significantly changes	As changes are made or annual

3.1.18 Update standard operating procedures

Including best practices for cybersecurity within standard operating procedures can complement the protection that the system can deliver on its own. Depending on the procedures an operator uses, they can create, prevent, or close a gap in protection. Therefore, it is important to update standard operating procedures periodically.

Action	Details	Suggested frequency
--------	---------	---------------------

Update standard operating procedures	Collect standard operating procedures for use of Metasys within the organization	Annual
---	--	--------

3.1.19 Update MUI logon banners

The system use policy details included on logon banners can change over time. Review and update as required.

Action	Details	Suggested frequency
Update logon banners	Review and modify the MUI logon banner as necessary	Annual

3.1.20 Renew licensing agreements

Assure that your Metasys software license supports the necessary functions required for your installation.

Action	Details	Suggested frequency
Renew licensing agreements	Collect active licensing details.	Annual

3.1.21 Renew support contracts

Assure Metasys software support agreement (SSA) and Product Service Agreement (PSA) are up to date.

Action	Details	Suggested frequency
Renew support contracts	Collect SSA and PSA details	Annual

Note: **Site subscription services.**

Site subscription services ensure that the subscriber automatically receives every major and minor Metasys release upgrade for either 1 year or 3 years after purchasing the site subscription. The upgrade software on media or disks is no longer sent automatically to the customer when the next release is available. Software is now available for download and licensing through the License Portal. For customer sites that do not have Internet access, an offline method for obtaining a license is available.

For details, refer to Software Manager Help (LIT-12012389).

3.1.22 Check for end-of-support / discontinuation information and plan for replacements.

Check with your local Johnson Controls branch for end-of-support announcements a.k.a. discontinuation information and plan for replacements or upgrades, including all Metasys application server operating systems, Metasys SQL supported version databases, network engines, field controllers, I/O level devices and sensors.

Action	Details	Suggested frequency
Check for discontinuation information and plan for replacements	Collect end-of-support details for your Metasys products through your local office	Annual

3.1.23 Periodically delete sensitive data in accordance with policies or regulations

Most Metasys components do not collect or store sensitive data. However, in the case that an engine would need to be sent for repairs, it is customary to first wipe the device clean. You should also collect details on policies and regulations that apply to your installation and specific to your local governing bodies.

Action	Details	Suggested frequency
Periodically delete sensitive data in accordance with policies or regulations	When components are removed from the site, ensure that they are first wiped clean	As required

3.1.24 Monitor for cyber attacks

Monitoring site perimeters, networks and endpoints for cyber-attacks is a part of good cybersecurity operation. Ultimately it is the site owner's responsibility to:

- Review the many tools available to assist with real-time analytics-based detection
- Decide on and fully test the tool in a non-production environment
- Verify that Metasys continues to operate properly after you have installed any security monitoring tools (Johnson Controls can only assist within the guidelines set forth within contractual agreements in force)
- Never install software (or hardware) unless it aligns with the policies of the environment's owner

Action	Details	Suggested frequency
Monitor for cyber attacks	Determine which security monitoring tools and services to implement	Run continuously once implemented

3.2.0 Metasys Release schedule

An update to Metasys including new features, feature updates, bug fixes and / or security fixes is released approximately every 3 - 12 months depending on the content.

Each Metasys update undergoes extensive quality assurance testing before being released.

Here are some definitions of terms to help you.

- **Major release.** A major Metasys software release includes significant new products, features, and enhancements. Major releases are indicated by a new major release number followed by a dot zero (x.0). For example, Release 10.0 and Release 12.0 are major releases. Upgrading Release 9.x or 10.x software to Release 12.0 is a major upgrade.
- **Minor release.** A minor Metasys software release provides minor product and feature enhancements. Minor releases are indicated by a new minor release number following the associated major release number. For example, Release 10.1 is a minor release. Therefore, in this example, upgrading Release 10.0 software to Release 10.1 is a minor upgrade.
- **Software license.** A Metasys software package and end-user license agreement is required for each ADS/ADX, ADSLite, OAS, MVE, NAE85, and LCS85 on a Metasys system site. Each computer or server package on a site must be licensed after a new installation and re-licensed after any major upgrade to the current release. Also, every ADS/ADX that is migrated must be re-licensed after the migration. Many other software applications and tools require licensing. See Licensing information for more details.
- **Metasys for Validated Environments.** Refer to Metasys for Validated Environments, Extended Architecture Catalog Page (LIT-1900466)
- **Metasys upgrade software.** Upgrade software is current-release Metasys software for upgrading products, such as the ADS/ADX, ADSLite, OAS, MVE, NAE85, and LCS85, at sites that have a previous major release of the Metasys software already installed (for example, upgrading Release 10.x or earlier software to Release 12.0). Metasys upgrade software packages are identified by a -6 suffix on the product code number.

For additional details, see Metasys System Software Purchase Options Product Bulletin (LIT-12011703).

Appendix A - Additional Metasys Literature

Description	Literature Number	Release
Security Administrator System Technical Bulletin	LIT-1201528	12.x
Metasys System Configuration Guide for Metasys	LIT-12011832	12.x
NAE Commissioning Guide	LIT-1201519	12.x
Metasys Server Installation and Upgrade Guide	LIT-12012162	12.x
Network and IT Guidance Technical Bulletin	LIT-12011279	12.x
Metasys IP Networks for BACnet/IP Controllers Technical Bulletin	LIT-12012458	12.x
Metasys User Interface (MUI) Help	LIT-12011953	6.x
Software Manager Help	LIT-12012389	4.x
System Configuration Tool Catalog Page	LIT-1900198	15.x
BACnet Controller Integration Technical Bulletin	LIT-1201531	12.x
Metasys Performance Verification Tool (PVT) User Guide	LIT-12012406	4.1
Metasys System Product Bulletin	LIT-1201526	12.x
Metasys WRG1830/ZFR183x Pro Series Wireless Field Bus System Technical Bulletin	LIT-12013553	-
Metasys BACnet/SC Workflow Technical Bulletin	LIT-12013959	12.x
SNE Commissioning Guide	LIT-1201645	12.x
Metasys for Validated Environments, Extended Architecture Catalogue Page	LIT-1900466	12.x
Metasys System Software Purchase Options Product Bulletin	LIT-12011703	12.x

[Product Documentation | Johnson Controls](#)

[Homepage • OpenBlue, Building Automation and Controls Knowledge Exchange \(johnsoncontrols.com\)](#)
(Internal Link)

Appendix B - Acronyms

Acronym	Description
ABCS	Authorized Building Controls Specialist
AD	Active Directory
ADFS	Active Directory Federation Services
ADS	Application Data Server
ADX	Extended Application Data Server
AHU	Air Handler Unit
API	Application Programming Interface
BAC	Building Automation Control/Controller
BFT	Background File Transfer
CA	Certificate Authority
CCT	Controller Configuration Tool
CGE	General Purpose Application Controller (ethernet)
CGM	General Purpose Application Controller (MS/TP)
CVM	VAV Box Controller
DoD	Department of Defense
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FAC	Field Application Controller
FAA	Federal Aviation Administration
FEC	Field Equipment Controller
FIPS	Federal Information Processing Standard
GGT	Graphic Generating Tool
GSA	General Services Administration
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDMS	Identity Management System
IOM	Input/Output Modules
IP	Internet Protocol
JCT	Johnson Controls Configuration Tool
LDAP	Lightweight Directory Access Protocol
MDM	Metasys Database Manager tool
MFA	Multi-Factor Authentication
MRP	Media Redundancy Protocol
MS/TP	Master-Subordinate Token Passing
MUI	Metasys User Interface
MVE	Metasys for Validated Environments
NAE	Network Automation Engine
NCE	Network Control Engine
NCT	NAE information and Configuration Tool
NIE	Network Integration engine
NMS	Network Management System
OAS	Open Application Server
ODS	Open Data Server
PSA	Product Service Agreement
RDP	Remote Desktop Protocol
RNI	Remote Network Interface
RPC	Remote Procedure Call
SA	Sensor Actuator

SC	Secure Connect (BACnet/SC)
SCT	Software Configuration Tool
SMP	Site Management Portal
SNC	Series Network Control Engine
SNE	Series Network Engine
SNMP	Simple Network Management Protocol
SSA	Software Service Agreement
SSL	Secure Socket Layer
SSO	Single Sign On
STIG	Security Technical Implementation Guide
TCP	Transmission Control Protocol
TEC	Terminal Equipment Controller
TLS	Transport Layer Security
UDP	User Datagram Protocol
UI	User Interface
UNT	Unitary Controller
VAV	Variable Air Volume
VLAN	Virtual Local Area Network
VMA	Variable air volume Modular Assembly
VSD	Variable Speed Drives
WNC	Wireless Network Coordinator
XPM	Expansion Modules

Appendix C – FAQs

The following examples are the types of hardening/security settings and questions IT departments ask about or put in place.

- Q1 Disabling HTTP OPTIONS and Trace commands in IIS?
A1 This is already done in MUI. This cannot be set globally in IIS.
- Q2 Can X-Frame headers be set to Deny globally in IIS?
A2 This is already done in MUI. X-Frame cannot be set globally in IIS because in MUI, the PPA/Fault widget runs under its own web application/distinct Angular in an Iframe.
- Q3 Can strict transport security (HSTS) be enabled globally in IIS?
A3 HSTS – Metasys SOAP and REST APIs return this response header. This cannot be globally set in IIS because IIS doesn't support multiple layers adding the same header.
- Q4 Can the SA Account be completely disabled in SQL?
A4 This can be done, nothing in Metasys uses the SQL sa account.
(Note: A sysadmin account will still exist, which should be disabled when not in use, as this name is well known for Metasys)
- Q5 How is Kerberos used in AD LDAP?
A5 From the Metasys process we use the .NET component System.DirectoryServices to facilitate the LDAP query to Active Directory. Customers can enable/disable LDAP protocols independent of Metasys.
- Q6 Can the public role in SQL be locked down?
A6 Yes, Metasys does not use SQL public role for any purpose.
- Q7 Can MSEA_AppPool in IIS run under an application pool identity instead of Local System?
A7 Yes, starting at Metasys Release 12.0.
- Q8 Can the site specify/manage the list of local administrators on the machine via group policy or will this conflict/create problems for Metasys?
A8 Metasys does not use local administrators' group in any way.
- Q9 Does Metasys support API Keys for email authentication?
A9 Metasys does not currently support API Keys or email authentication.
- Q10 Does Metasys support wildcard SSL certificates?
A10 No. Wildcard SSL certificates are not supported.
- Q11 Does Metasys use Group Managed Service Accounts for MSSQLSERVER or SSO?
A11 Metasys does not use local groups, domain groups, or SQL Server groups for any purpose.
- Q12 What is BACnet/SC?
A12 BACnet Secure Connect (BACnet/SC) is a new BACnet datalink ASHRAE 135-2020 Annex AB that provides secure message transport.
- Q13 Do we support BACnet Addendum CD to Standard 135-2020?
A13 Yes, Metasys Release 12.0 supports BACnet Addendum CD TLS v1.3 Cipher Suite Application Profile for BACnet/SC, which covers the minimum cipher suites that BACnet/SC supports for interoperability with other BACnet/SC devices.

Q14 Does BACnet/SC use Broadcast Management Devices (BBMDs)?

A14 No. BACnet/SC eliminates BBMDs and their configuration.

Q15 Which version of TLS is supported?

A15 BACnet/SC implementations support TLS version 1.3 for establishing communication connections between devices. Note: Although TLS 1.2 is compatible with BACnet/SC but is not recommended with Metasys Release 12.0.

Q16 What are the two types of BACnet/SC certificates?

A16 To establish a connection, each device needs to determine that it trusts the device it is trying to establish a connection with. For example, if Device A and Device B want to establish a connection between them, each device sends its operational certificate to the other device to authenticate.

- An **operational certificate** is a term that BACnet uses for the certificate that a device uses for BACnet/SC communication. Operational certificates are also known as TLS certificates or identity certificates. The operational certificate is simply a file of information about the device, along with the device's public key and a digital signature by the Certificate Authority (CA) that issued the certificate.
- BACnet/SC also requires that all devices have at least one **signing certificate** associated with it. Normally, a site uses one signing certificate, but BACnet/SC supports a second signing certificate for each device to facilitate switch-over to a different signing certificate for the site. A device uses the signing certificates to determine if it can trust the operational certificate presented to it by other devices that want to connect to it. All devices on the site have a copy of the same one or two signing certificates, so that they can mutually trust each other.

Q17 How do I manage my BACnet/SC certificates?

A17 Use the BACnet/SC Management feature that is part of Metasys UI or Johnson Controls System Configuration Tool (JCT).

Q18 What is a public key?

A18 A public key is the public portion of a cryptographic system's public-private asymmetric key pair.

Q19 What is a Certificate Authority (CA) and how does it sign the certificate?

A19 A CA is an entity that issues the operational certificates to use for communication on a site.

- When the CA creates the operational certificate for each device on the site, it places information in the operational certificate about the CA, or issuer. All BACnet/SC devices on a site need to have the certificate for the CA(s) they trust. BACnet/SC requires that all devices can trust up to two CA certificates.
- All devices on a site that communicate through BACnet/SC must have a certificate signed by one of the two CAs that are trusted by other devices on the site.

Q20 What is the difference between a certificate chain or trust chain and a signing certificate?

A20 When a CA generates each operational certificate, it will likely include all the certificates that make up a certificate chain, starting with a trust anchor or root certificate.

Each operational certificate issued contains the Common Name of the issuer or signing CA. You can decode an operational certificate with several different tools available to see the issuer information. In this way, you can distinguish the issuing or signing certificate from possibly multiple CA certificates that make up a chain.

Q21 What needs to be in the import .zip file of operational certificates?

A21 When you receive operational certificates from the IT department, they may not be packaged in a way that enables you to directly use the Import functionality in the BACnet/SC Management feature. The basic requirements are that the certificates must be in .pem format and that the issuing or signing certificate that signed them must be present in the .zip file. You can assemble

the operational certificates in the .zip file to ensure a successful import.

Q22 What is a Certificate Signing Request (CSR)?

A22 A certificate signing request is generated by a device as the first step to obtain a new operational certificate. The CSR contains information about the device and the public key from a newly generated public-private key pair. The information in the CSR becomes part of the operational certificate, along with information about the CA that created the operational certificate. After the operational certificate is issued and saved to the device, the CSR that was used is no longer needed.

Q23 How are certificates persisted?

A23 To provide enhanced security, BACnet/SC certificates and their matching private key are only persisted on the device that generated the public-private key pair during the CSR step.

Q24 Do you need a license for BACnet/SC?

A24 Yes, a license is needed for BACnet/SC (M4-BACNETSC-0) if BACnet/SC is used on a Server site. However, a license is not needed for Engine-only sites. If two Metasys server class devices, such as ADS and NAE85, are used as a Primary Hub and Failover Hub respectively, two licences are required.

Q25 What does the Number of Active WebSocket connections attribute of the SC Network Port object mean?

A25 The Number of Active WebSocket connections attribute indicates the number of WebSocket connections that are currently active. A WebSocket connection is considered active if the following conditions apply:

- The connection is established
- The connection has been created, but has not reached the established state, such as when the connection handshake is being negotiated
- The connection is being disconnected, but not yet destroyed

Q26 Does communication traffic go through the hub or directly from device to device?

A26 A device uses the hub initially to obtain information about another device that it wants to communicate with. While the BACnet/SC specification supports routing all communication between two devices through the hub, for best performance, all Metasys devices support the use of direct connections for peer communication and do not route peer communication through the hub. Broadcast messages always go through the Hub Function

Q27 How do I choose a Primary Hub and Failover Hub for my Metasys system?

A27 See BAC/net LIT-12013959 for additional details and examples.

Q28 Can I add other protocols and services to sites that use BACnet/SC?

A28 Yes, BACnet/SC supports the addition of standard messaging protocols and services, such as MQ Telemetry Transport (MQTT).

Q29 Why do I need BACnet/SC on an ADS/ADX?

A29 You need BACnet/SC on an ADS/ADX if you want the ADS/ADX to perform the Hub Function. The ADS/ADX does not use BACnet/SC for other purposes.

Q30 Do I have to use BACnet/SC for the entire site?

A30 No, you can selectively choose which devices communicate BACnet/SC, so you can integrate BACnet/SC devices gradually.

Q31 Can I use BACnet/SC and BACnet/IP on the same subnet?

- A31 Yes, but devices that communicate through BACnet/SC cannot communicate with devices that communicate through BACnet/IP only, regardless of the subnet they are on.
Note: From a cybersecurity standpoint, a network with only BACnet/SC devices is the most secure. Mixing BACnet/IP and BACnet/SC devices on the same network can compromise the security of the network. A bad actor could send commands over BACnet/IP and have them execute on BACnet/SC controllers.
- Q32 Can BACnet/SC devices be distributed across subnets/VLANs?
- A32 Yes, if the network is configured to route messages between the subnets/VLANs, the nodes and BACnet/SC hubs can reside on different subnets/VLANs.
- Q33 Can I connect BACnet/SC networks together?
- A33 Yes, you can connect BACnet/SC networks together with a third-party BACnet/SC to BACnet/SC router. There is no limit to the number of routers you can use to connect BACnet/SC networks together.
- Q34 Where does the field technician connect to the network to install the certificates on the BACnet/SC devices?
- A34 To use the BACnet/SC Management feature, you need to connect to the Site Director to install certificates for all supported Metasys devices on a site or connect to an engine to install certificates on the engine and its integrated equipment controllers.
- Q35 Can I use Domain Name System (DNS) to specify the Primary and Failover Hub Uniform Resource Identifier (URI)?
- A35 Yes, but you cannot use a URI with the full DNS name of the devices as the Primary Hub or Failover Hub URI. Ensure that the DNS Server is configured to allow the short host name to be used.
- Q36 Who is responsible for the long-term storage and safe keeping of certificates?
- A36 Each Metasys BACnet/SC device securely stores its own operational certificate and the matching private key. The certificate is kept in a secure location on each device and is maintained even if the device has its firmware or archive changed. For security purposes, there is no mechanism to upload the private key for a device.
- Q37 What is the level of support that we offer to third-party devices on a Metasys BACnet/SC configuration?
- A37 The level of support offered is the same as we offer to third-party devices on a Metasys BACnet/IP configuration. Additionally, third-party devices need to use their own tool to put a certificate onto them as there is no standardized way to do this in BACnet until devices support Addendum CC of the ASHRAE 135-2020 BACnet protocol standard.
- Q38 Can I use Metasys BACnet/SC devices on a third-party BACnet/SC configuration?
- A38 Yes. Use the BACnet/SC Management feature in Metasys UI or JCT to configure a supervisory device for use in a third-party system.
- Q39 Does an ADS or ADX that performs the Hub Function continue to perform broadcast management for BACnet/IP devices?
- A39 Yes, an ADS or ADX that performs the Hub Function continues to perform broadcast management for BACnet/IP devices.
- Q40 How can I determine the expiration status of my certificates?
- A40 Both the operational certificates and the longer-lived signing certificates can expire. You can use the information displayed on the Devices tab of the BACnet/SC Management feature to determine the status of your certificates.

For engines and IP equipment controllers you can also open the Device object or Mapper Device object and go to the Detail widget to see information about the operational certificate status.

Q41 Will I receive a reminder before my certificates expire?

A41 Yes, you will receive certificate expiration reminders that start a configurable number of days before a certificate expires for a device, and then daily until you renew the certificate. The reminder takes the form of an alarm in System Activity, Alarm Manager, and Alarm Monitor. Use the Certificate Renewal Period property of the Detail widget of the Site Object to configure the launch of the reminders.

Q42 Will BACnet/SC work on the Media Redundancy Protocol (MRP) Ring?

A42 IP controllers in BACnet/SC mode will work in an MRP Ring although the IP Network Wizard tool used to configure the Ring Manager switches (that is the Cisco IE 2000 switches) for BACnet/IP does not yet support BACnet/SC.

Q43 How do I deal with an existing MRP Ring if I want to use BACnet/SC?

A43 Until BACnet/SC is supported on the IP Network Wizard tool, manual changes are required to the Ring Manager switches' Access Control Lists (ACLs) configuration to allow the BACnet/SC-related protocols, as well as to account for the BACnet/SC Hubs (Primary and Failover). Specific Cisco switch configuration knowledge is required to do this, so it is recommended to continue to use BACnet/IP until the BACnet/SC support on the IP Network Wizard tool is officially released.