



Metasys Hardening Guide



GPS0028-CE-EN
Version 14.1
Rev A
Revised 2025-08-12

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 document 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 Metasys overview.....	7
1.1.1 Deployment architecture.....	7
1.1.2 Metasys Components.....	11
1.1.3 Supporting Components.....	12
1.1.4 Additional Deployment architecture examples	13
1.1.5 Managed Metasys	13
1.1.6 Metasys Releases	13
1.2 Security feature set	14
1.2.1 Cyber Health Dashboard	15
1.2.2 Supervisory Device safeguards	15
1.2.3 User password policy	16
1.2.4 FIPS Compliant Secure Communication on the building network	18
1.2.5 User Account Support	19
1.2.6 Encryption ciphers.....	21
1.2.7 Updates.....	22
1.2.8 Secure web traffic support.....	23
1.2.9 Last Login monitoring	23
1.2.10 Performance Verification tool.....	23
1.2.11 BACnet Secure Connect (BACnet/SC)	24
1.2.12 Certificate renewal period alarm event	25
1.2.13 Authentication	26
1.3 Intended environment.....	26
1.3.1 Internet connectivity	26
1.3.2 Integration with IT networks.....	26
1.3.3 Integration with external Identity Providers	27
1.4 Patch policy.....	27
1.5 Hardening methodology	28
1.6 Communication	28
1.6.1 Communication port configuration	28
1.6.2 Communication certificates	34
1.7 Network planning.....	35
1.7.1 Trust boundaries overview	36
1.8 System requirements.....	37
2 Deployment	39

2.1	Deployment overview	39
2.1.1	Physical installation considerations	39
2.1.2	Getting started.....	39
2.1.3	Resetting to the factory default settings	40
2.1.4	Considerations for commissioning	40
2.1.5	Recommended knowledge level.....	40
2.2	Hardening.....	40
2.2.1	Hardening checklist	41
2.3	Disable TLS 1.0 and 1.1	41
2.4	Disable unused ports.....	41
2.5	User management.....	41
2.5.1	Metasys User Roles and Permissions	42
2.5.2	Metasys Local User Accounts	43
2.5.3	Metasys External User Accounts:	44
2.5.4	No shared accounts	45
2.5.5	Least privilege	45
2.5.6	Separation of duties	45
2.5.7	Centralized user account management	45
2.5.8	Password policy	45
2.5.9	Kiosk Service Accounts.....	46
2.5.10	User management best practices	46
2.6	Update Metasys to latest Release	46
2.7	Communication hardening.....	47
2.7.1	Least functionality.....	47
2.7.2	Communication certificate support.....	47
2.7.3	FIPS 140-2 support	47
2.8	Configuring security monitoring features.....	47
2.8.1	Audit Logs	48
2.9	Backup/restore	48
2.10	Web Server	48
3	Maintain	50
3.1	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 former employees	52
3.1.5	Remove inactive user accounts.....	52
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 applicable 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	Renew support contracts	56
3.1.20	Check for end-of-support / discontinuation information	57
3.1.21	Delete sensitive data in accordance with policies or regulations	57
3.1.22	Monitor for cyber attacks	57
3.2	Metasys Release schedule.....	57
Appendix A - Additional Metasys Literature		58
Appendix B - Acronyms		59
Appendix C – FAQs.....		61

1 Planning

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

1.1 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
- Secure 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

Metasys Release 14 servers can be deployed using two different methods:

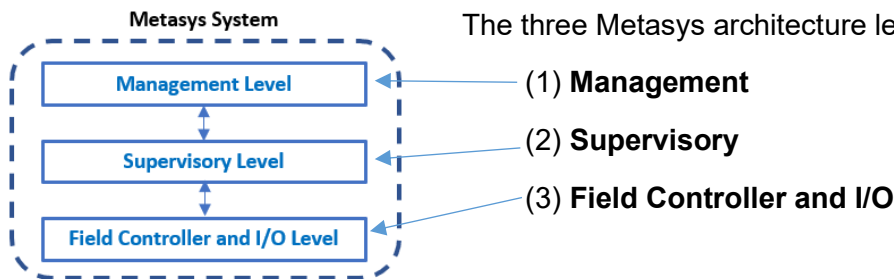
- **On-premises:** Servers are on site hosted by the customer
- **Managed Metasys:** Servers are hosted in the Johnson Controls cloud environment
See section 1.1.5 for additional details on this option

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

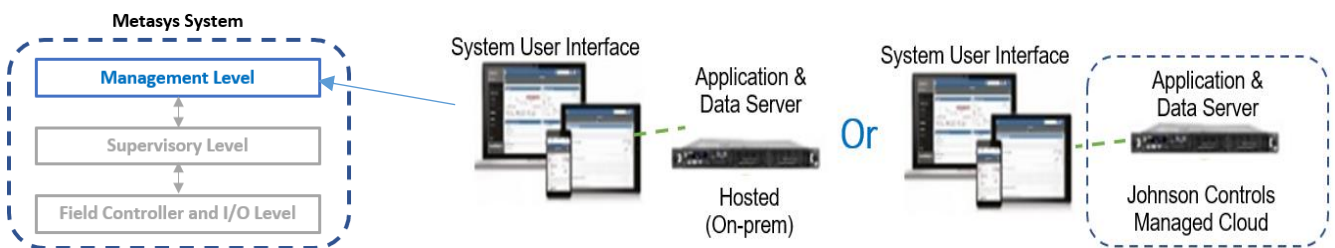
It is important to note that every installation is unique. However, each installation can be broken down into basic building blocks or "Levels" which make up every Metasys installation.



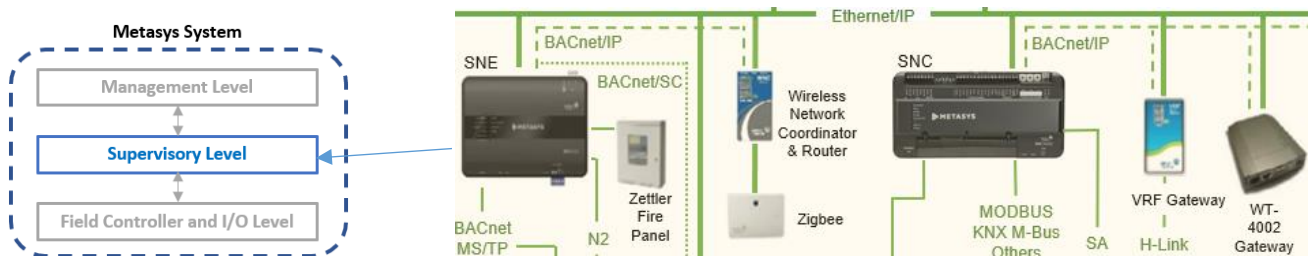
The management level resides on an Ethernet network which connects the engines. Within the supervisory level, engines route to the field controller network which can be IP-based as well as serial-based networks, while I/O devices often connect to field controllers using a standard electrical interface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

Management Level. SCT. These are core components and will be discussed further in the deployment architecture section.

Note: At Release 14, Metasys can integrate IP devices directly into the server.



Supervisory Level. The Supervisory or Engine level coordinates 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 1.1.1.1 - Metasys system on premises architecture example

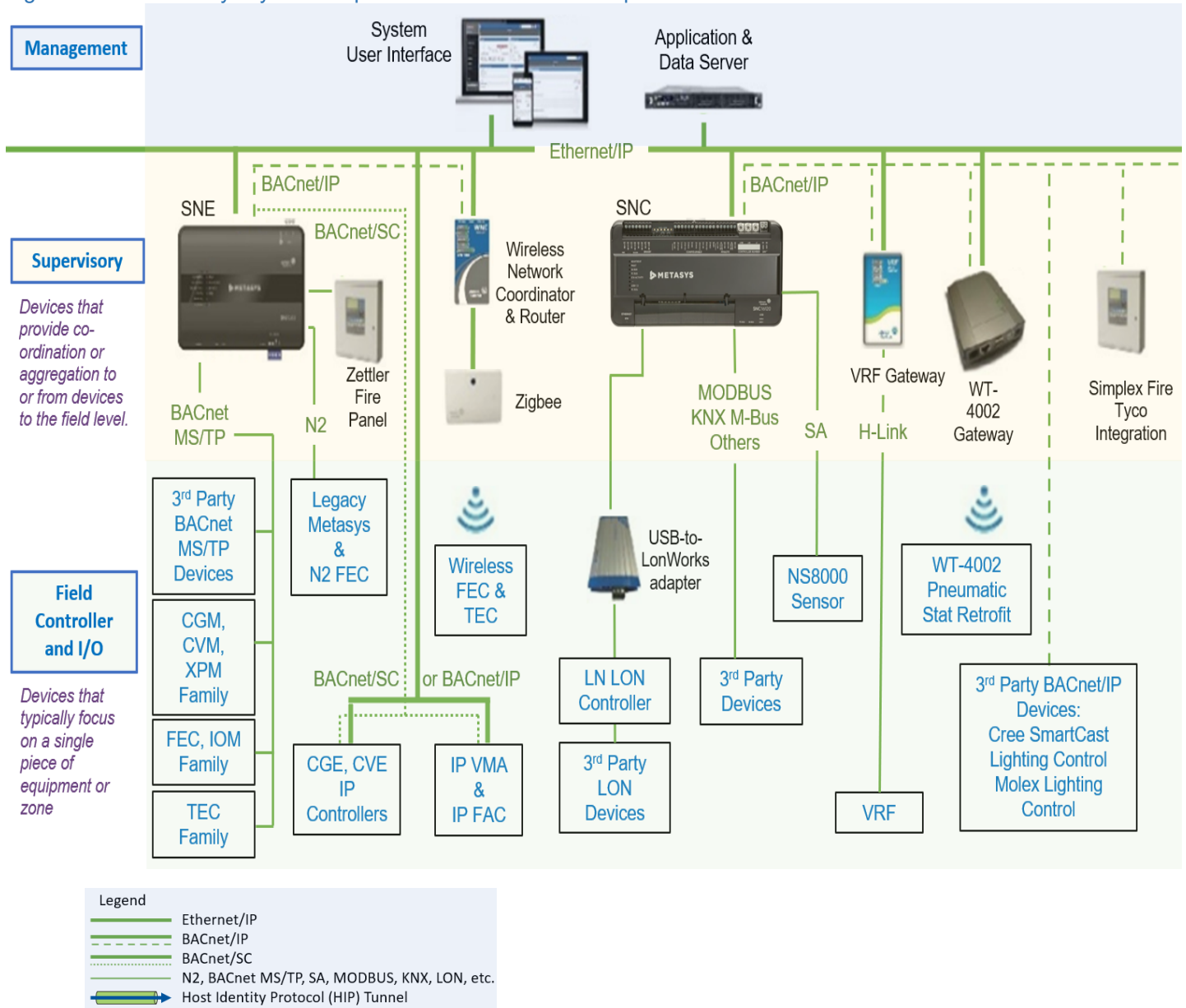
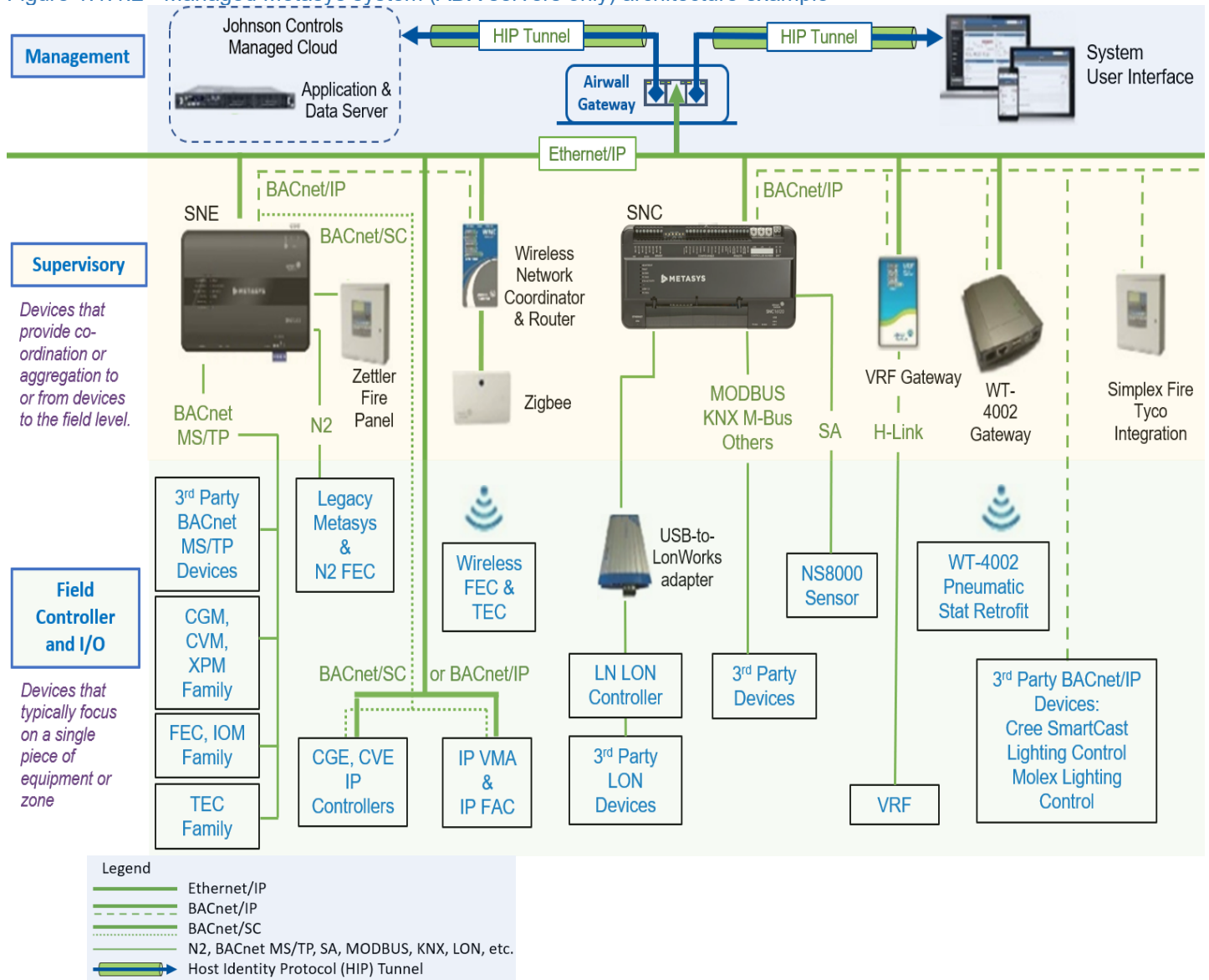


Figure 1.1.1.2 - Managed Metasys system (ADX servers only) architecture example



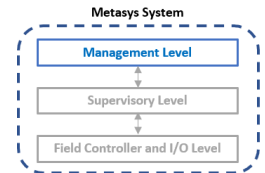
Note: For Managed Metasys installations, only the ADX server is hosted in MS Azure and protected by Johnson Controls Airwall technology.

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**.

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:

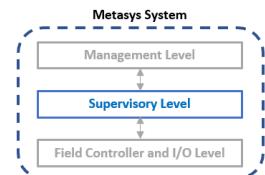
- a. Application and Data Server (ADS)
- b. Extended Application and Data Server (ADX)



Supervisory Level – Network Engines provide network management and system-wide control coordination over one or more networks of equipment controllers. The Metasys User Interface (UI) is embedded on all engine devices, providing a device-agnostic, modern web interface.

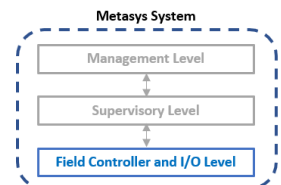
Network components include:

- a. Series Network Engine (SNE)
- b. Series Network Control Engine (SNC)
- c. Device gateway (BACnet Router / Modbus Gateway)
- d. Server based engines such as NAE8500 or LCS8520



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/CVE)
- 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

Features within Servers and Engines

Metasys User Interface (UI). A tool available on servers and engines, that enables you to set up and maintain your building management system by interacting with Metasys engines and Metasys servers to perform functions such as:

- Navigating a site that includes Navigating to an Item, Modifying an Item, and Commanding Items.
- Creating a calendar and exception schedules for events and holidays.

- Creating trends, alarms, or totalizations extensions on points.
- Creating reports to monitor data about your system.
- Customizing the navigation tree with a user view.
- Viewing graphical displays using the User Graphics Tool (UGT) and Graphics+™.
- Creating, viewing and editing Metasys UI graphics with Graphics Manager

For additional information about Metasys UI see LIT-12011953.

Site Management Portal (SMP). This feature is End of Life (EOL) and can no longer be licensed for Metasys 14.1 and higher. SMP has been succeeded by the HTML5-compliant Metasys UI.

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 and not included within this guide.

Management Level

- Third party management systems which Metasys integrates into (BACnet, OPC UA, M-Bus, KNX, Modbus)
- Metasys Validated Environments (MVE) feature – A validated MVE site director is a Metasys Server where the MVE software has been installed and licensed. The associated engines must be at a compatible MVE version. For additional information see LIT-1901214.

Supervisory Level

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

Field Controller and I/O Level

- 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).
- BACnet Field Controller – BACnet/IP, BACnet/SC or BACnet MS/TP serial controllers
- LON Field Controller – Controllers that utilize the standard LonTalk protocol
- Other protocol controller
- 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

- OpenBlue Bridge with Airwall
- Router (i.e., Edge router, BACnet/IP, BACnet/SC, remote field bus, etc.)
- Smart Switch (i.e., Smart ethernet switch, Netgear, Cisco, CCSI, etc.)
 - Ring Manager – Cisco IE2000, IE3100 and IE4010 with Media Redundancy Protocol (MRP) for IP controllers

1.1.4 Additional Deployment architecture examples

Figure 1.1.1.1 and

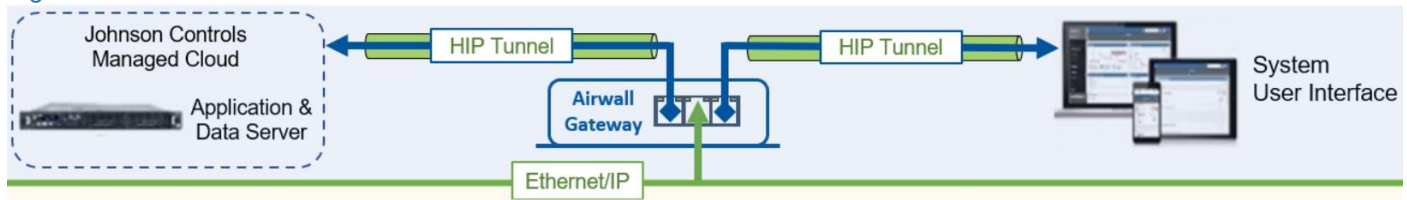
Figure 1.1.1.2 show example deployments with various components.

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

1.1.5 Managed Metasys

Managed Metasys Overview. Customers in North America have the option of having a **Managed Metasys** installation, where an ADX server is hosted in MS Azure, while all the tier 2 supervisory and tier 3 field controller devices remain on site. Communications are protected by an Airwall Gateway, which is a technology that enables the creation of secure, private, easy-to-manage software defined networks called Overlay networks, which are built upon zero-trust policies.

Figure 1.1.5.1



The Johnson Controls Remote Operations Center (ROC) will setup the hosted server(s) on behalf of the branch, hardens the solution, and applies the appropriate Metasys updates to the server only as required. The ROC offers multiple and custom levels of remote services including: 24/7 monitoring, troubleshooting, and resolution of HVAC building operation issues, security and fire systems, and elevators, along with additional custom offerings such as public-private partnership call center services.

Managed Metasys Availability. Managed Metasys is a Building Solutions North America (BSNA) offering only available on installations with an ADX server and requires a planned service agreement sold to the end customer by your local Johnson Controls branch or customer account executive.

Note: For technical support with BSNA Managed Metasys, contact BE-ROCServerHosting@jci.com.

1.1.6 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. It is recommended to upgrade all child engines to Release 14.1 (as supported by the hardware). To facilitate phased updates, it is possible to have a mix of lower Release engines. While basic compatibility is maintained down to Release 5.2, older releases may no longer be supported (see patch policy) and will lack the cybersecurity features introduced in later Releases.

The minimum recommended cybersecurity feature set is provided with Release 10.1. Current FIPS 140-2 compliance requires Release 11 or 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 14.1 (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 14.1 (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 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 1.2.1

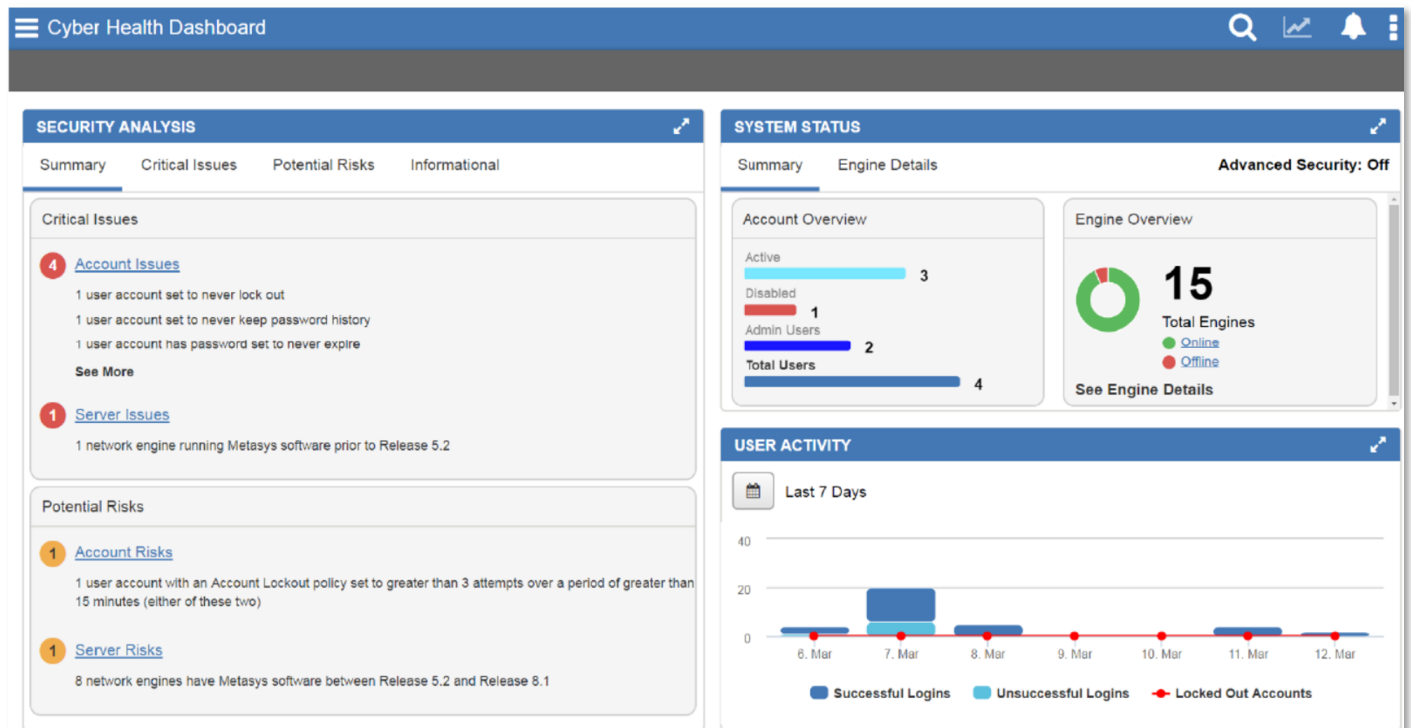
Section	Type	Feature name	Feature Available
1.2.1	Cyber Health Dashboard (Metasys UI only)	Security Analysis widget	10.1
		System Status widget	10.1
		User Activity widget	10.1
1.2.2	Supervisory device safeguards	Advanced security enabled	10.0
		Engine pairing	10.0
		Secure Boot	10.1
1.2.3	User password policy	User account control Mandatory password change	6.0
1.2.4	Secure communications	FIPS 140-2 compliance	11.0
		IEEE 802.1X	14.0
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
		Role based access control	5.2
1.2.6	Encryption ciphers	Cipher support, AES-256	
1.2.7	Updates	Update messages	
1.2.8	Secure web traffic support	Allow HTTPS	8.1
		TLS 1.3	
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
		Renewal period configuration	12.0
1.2.13	Authentication	Active Directory via LDAPS	14.0
		ADFS	11.0
		OAuth 2.0 support	14.0

Note: Certain features require configuration and/or licensing to be activated. See section 2 for details.

1.2.1 Cyber Health 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 ADS and ADX, which may not surface as part of general system alarms. The administrator can also see 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/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 UI.

1.2.3 User password policy

Using the Metasys UI you can apply a role-based account for users.

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 Metasys UI, or which User Views appear in the Navigation Tree.

Microsoft Active Directory

The Metasys UI can use Microsoft Active Directory® LDAP / LDAPS 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	Yes	Yes	Yes
Metasys JCT**	Yes	Yes	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.

OAuth 2.0 Identity provider support

Metasys Release 14 and greater supports OAuth identity providers generically as well as implicit and authorization code flow. Below is an example of an OAuth identity provider.

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
- The ADFS single sign-on and two-factor authentication are configured on the customer's ADFS system
- Refer to the Metasys System Configuration Guide (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
Metasys UI	Yes	Yes

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

Table 1.2.3.3 is a summary of which Metasys system application User Interfaces support Active Directory logins and the SSO capability. If the application supports Active Directory logins, then the Metasys system can be configured to use your existing IT Active Directory Service infrastructure for authentication purposes. If the application supports SSO, then you can log in to multiple, secured applications without reentering the same username and password.

Table 1.2.3.3 Products that support Active Directory/LDAP logins and SSO

Application	Active Directory login supported	Exact or alternate UPN format logins supported	SSO supported
SCT	Yes	Yes	Yes
Metasys UI and Johnson Controls System Configuration Tool (JCT)	Yes	Yes	No
Network Engine	No	No	No
Metasys for Validated Environments	Yes	Yes	No

For more details on Active Directory and SSO interaction with Metasys system security, refer to the Security Administrator System Technical Bulletin (LIT-1201528) or (LIT-12011279).

Support for Active Directory Federation Services (including two-factor authentication capability)

Active Directory Federation Services integration with two-factor authentication is a licensed feature to add ADFS support to the Metasys Server. ADFS is a single sign-on solution developed by Microsoft®. Use ADFS to provide two-factor authentication for access to Metasys. ADFS helps prevent unauthorized access to Metasys, which, if not prevented, could result in data, financial, and reputational loss, system disruption, and other negative consequences.

For added security, Microsoft administrators can disable the KMSI prompt. For additional details see section 2.3.3.

Table 1.2.3.4 Active Directory Federation Services

Application	ADFS login supported	KMSI on ADFS server	Two-factor Authentication on ADFS server
SCT	No	No	No
Metasys UI (ADS/AD)	Yes	Yes	Yes
Johnson Controls System Configuration Tool (JCT)	No	No	No
Network Engine	No	No	No
Metasys for Validated Environments	No	No	No

Mandatory password change. Metasys prompts users to change their password at first login.

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). <https://csrc.nist.gov/pubs/fips/140-2/upd2/final>.

1.2.4.2 FIPS 140-2 and Metasys

FIPS 140-2 is a licensed add-on feature to the Metasys Server software products, including ADS, ADX, and NAE8500, 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 greater.

FIPS 140-2 compliance is automatically available on engine-based sites at Release 11.0 or greater and requires that all child-engines are also upgraded to Release 11.0 or greater.

For the server class products ADX/ADS/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 Johnson Controls / Metasys devices that support FIPS 140-2:

Table 1.2.4.2.1 – FIPS 140-2 Johnson Controls / Metasys compliant devices

Device	Type	FIPS Compliant
ADX / ADS	Server	Yes
NAE8500	Engine	Yes
NAE55	Engine	Yes
SNE/SNC	Engine	Yes
CGE	IP Controller	Yes
CVE	IP Controller	Yes
FAC4911-0	IP Controller	Yes
VMA1930-0	IP Controller	Yes
JC-RTR1102-0	Router	Yes
JC-GTW11002-0	Gateway	Yes

1.2.4.3 IEEE 802.1X

Metasys Servers and network engines support Institute of Electrical and Electronics Engineers (IEEE) 802.1X authentication, which provides protected authentication for secure network access. For more information, see Metasys System Configuration Guide (IEEE 802.1X authentication configuration).

1.2.5 User Account Support

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

Figure out screen cap here next time

User Details	Account Settings	Timesheet
Inactive Sessions <input type="radio"/> Never Terminate <input checked="" type="radio"/> Terminate In <input type="text" value="30"/> Minutes		Maximum Password Age <input type="radio"/> Password Never Expires <input checked="" type="radio"/> Expires In <input type="text" value="60"/> Days
Account Lockout <input type="radio"/> No Account Lockout <input checked="" type="radio"/> Lockout After Bad <input type="text" value="10"/> Attempts Lockout In <input type="text" value="15"/> Minutes		Password History <input type="radio"/> Do Not Keep Password History <input checked="" type="radio"/> Remember Last <input type="text" value="10"/> Passwords
Dormant Account <input type="radio"/> Do Not Check User Account For Dormancy <input checked="" type="radio"/> Make Account Dormant After <input type="text" value="365"/> Days <input checked="" type="checkbox"/> Create Dormant User Account Event <input checked="" type="checkbox"/> Lock Out The User Account When Dormant		

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.

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 is used to identify and deactivate accounts designated as inactive or disabled. The report shows Active Directory, and local dormant accounts for supervisory devices (Nx E/ADX) at Metasys Release 8.0 or later. See Metasys Security Administrator System Technical Bulletin (LIT-1201528 Account Policy Tab) for details on how to ensure this feature is enabled.

An optional alarm can be set to identify dormant accounts on an ADS/ADX. 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.

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

Password History. Keeps history and ensures password cannot be reused

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 a camera would be provided outside of Metasys.

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). Encryption cyphers that are specific to the Microsoft operating system are independent from the Metasys application and must be hardened separately. See section 2.3 Disable TLS 1.0 and 1.1 for additional details.

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. Files needed to complete an update may be downloaded from the Updates tab. To open the tab, click on the Updates tab.

Note: Updates to **Managed Metasys** systems are automatically included with the service, so the software manager features do not apply to the end user. Managed Metasys users, please skip to the next section.

Figure 1.2.7.1 – Sample Updates Tab

Software Manager

LICENSES

UPDATES 

Metasys Server

Released On: 2023-Jul-07

Installed Version: 12.0.50.724

No new available updates. The latest version is installed.

Controller Configuration Tool (CCT)

Released On: 2022-Nov-17

Installed Version: 15.0.2.4

No new available updates. The latest version is installed.

System Configuration Tool (SCT)

Released On: 2023-Jun-06

Installed Version: 15.0.4.5

No new available updates. The latest version is installed.

Performance Verification Tool (PVT)

Released On: 2022-Aug-10

Installed Version: 4.1.0.373

Your system may have some or all the modules shown in figure 1.2.7.1, depending on your configuration. Click the **Refresh** icon on the **Updates** tab to complete a manual refresh and view new updates only if available. From the time the refresh icon on the **Updates** tab is clicked until the refresh is in progress (while 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 the **Software Manager** is launched, it 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 (end of life), 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 (end of life), 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 1.3.1 Internet connectivity, which is required for Software Manager.
There is a manual procedure if the port cannot be open at the site.
- Section 3.1.12 Plan and execute software patches and updates
- See your Field Support Center (FSC), or Local Support Center portal

1.2.8 Secure web traffic support

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

Metasys UI Administrators can view the last login information of each user by navigating to the **User Management**, then **Users** tab.

User Management							
Users Roles Setup							
+ User							
Username	Full Name	Email	Role	Authentication Type	Last Login	Status	Actions
MetasysSysAgent	Metasys System Agent		2 Roles	Metasys Local	04/08/2025 1:39 PM	Active	
Operator	Metasys System Operator		USER	Metasys Local		Active	

When a user logs on to SCT with Launcher, the color of the lock will indicate Level and trust.

Table 1.2.9.3

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.

Because the PVT is more frequently updated with new features, we encourage reviewing the Metasys Performance Verification Tool (PVT) User Guide (LIT-12012406) for the latest list. The following is a sample of tasks which can be easily performed using the PVT:

- Determine the overall health of the Metasys system
- Identifies whether all points are categorized the same
- Scan one server at a time to identify an inventory list of all the controls hardware
- Identify the equipment the system controls
- 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

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

1.2.11 BACnet Secure Connect (BACnet/SC)

Metasys Release 12.0 and greater 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.

For additional details see Network and IT Guidance Technical Bulletin (LIT-12011279) and the Metasys BACnet/SC Workflow Technical Bulletin (LIT-12013959).

Many Release 13.0 Metasys components are field updated to, or factory shipped with BACnet/SC. The SNE, and SNC 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. The M4-BACNETSC-0 add-on license must be purchased to use BACnet/SC on the ADS, ADX, NAE85, or LCS85.

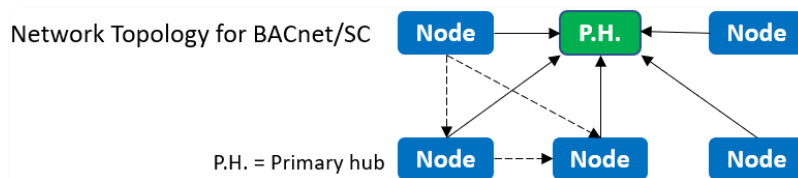
Acquiring a managed Certificate Authority (CA) for your site. A CA is an entity that issues the operational certificates to use for communication on a site and should be managed by a trusted entity. Decide which certificate authority will be used to generate the operational certificates*. The customer's IT department can act as the CA**, which should be included in the Request for Information (RFI) for new construction, or by coordinating with the customer for existing installations. A third-party vendor of BACnet/SC devices could also act as the CA.

* Note: Because there are different levels of validation, Johnson Controls recommends choosing a CA that performs either **Organization validation** or **Extended validation**. While **Domain validation** is available, it does not validate the organization and is not recommended.

** Note: This process could take ~30 days. Refer to the BACnet/SC literature for additional details.

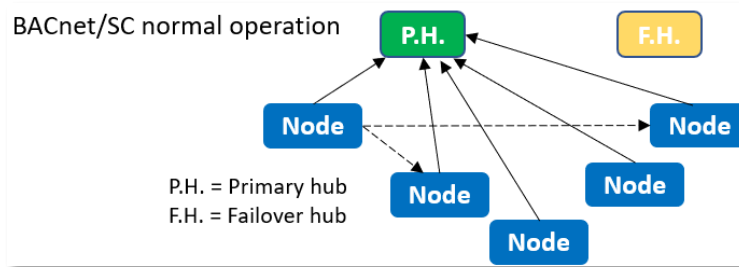
Additional Notes about BACnet/SC.

- 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.

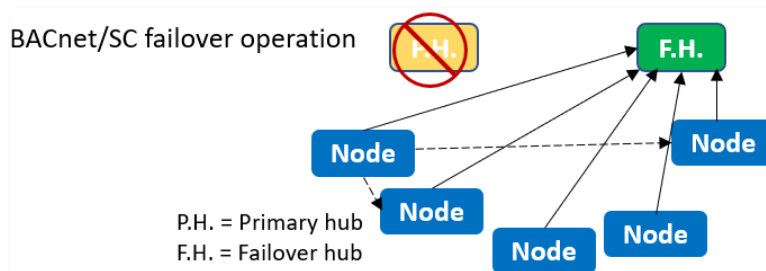


- A **Primary Hub** device has both a node and a Hub Function. The node on the Primary Hub device connects to the Hub Function, as if it was a different device. The Primary Hub is expected to perform the Hub Function when reachable and always accepts WebSocket connections. A

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 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 Metasys UI System Activity feature

See [section 1.6.2](#) for additional details on communication certificates.

1.2.13 Authentication

For customers who use the **Active Directory** integration for user management, LDAPS is an optional security protocol, offered in Release 14.0 and greater, which can be used during authentication. LDAPS encrypts the user attributes between the domain controller and Metasys server. For details to enable this feature see section 2.



1.3 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 without having protective security measures in place such as an Airwall Gateway or a customer managed VPN. For Metasys this means:

- Do not expose the web server to the internet
- Do not allow inbound access to the ADX / ADS server (This is a 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 network access. Network security is an important issue. Typically for existing building installations, the IT organization must approve intranet configurations. For new building installations follow Johnson Controls recommendations. Be sure to fully read and understand IT Compliance documentation for your site.

1.3.3 Integration with external Identity Providers

Microsoft Active Directory LDAP or OAuth 2.0 identity providers, e.g. ADFS.

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 (LIT-1201528). Metasys Release 14.0 and greater optionally provides support for LDAPS.

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 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 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 Metasys 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.

Group-To-Role. Metasys Release 14.0 and greater includes a new feature named **Group-To-Role** which enables Metasys administrators to streamline the time it takes to set up external user accounts by allowing administrators to map groups in external identity providers to Metasys roles. External users that belong to one or more mapped external groups can log in to Metasys and have a Metasys account automatically created and assigned to the mapped roles. On a future login, the newly created account will have roles reassigned based on changes in either external group assignment and/or group-to-role mapping.

1.4 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 endeavors to address issues that arise within Metasys with the severity that they warrant.

Security Patches are provided for the latest version of the current release and the latest version of the prior software release of Metasys as follows:

- When **CRITICAL** severity 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** severity vulnerabilities and plan accordingly

1.5 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 complement the base security features of each component.

1.6 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 1.6.1.4 – (Optional) Outbound internet Port numbers and protocols

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

Port ¹	Protocol	Use	Metasys Device	Inbound/ Outbound	Description
25	SMTP	TCP	ADS/ADX NAE55/SNx/NAE85	O	Used for alarms and events.
53	DNS	UDP	Active Directory Client ADS/ADX 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 ²	UDP	Active Directory Client ADS/ADX 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 ²	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 ²	TCP	ADS/ADX 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,

Port ¹	Protocol	Use	Metasys Device	Inbound/ Outbound	Description
					at Metasys Release 8.1 or later, you can close Port 80 (I and O).
80	HTTP	TCP	NAE Update Tool	I	File transfer between the client computer and the network engine pre Release 10.1.
88	Kerberos	TCP/ UDP	ADS/ADX ADX Split Web/Application Server Metasys System Client SCT	I/O	Used by the Metasys system for Active Directory service authentication at the Metasys system login screen, and Service Account authentication prior to LDAP queries. Kerberos is a standard network authentication protocol designed to provide strong authentication for client/server applications by using secretkey cryptography. Kerberos is the primary security protocol for authentication within an Active Directory service Domain. Kerberos authentication relies on client functionality built into the Windows operating systems supported by Metasys software
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 ADX Split Web/Application Server Metasys System Client SCT	I/O	Used for time sync across a network between client computers and server class operating system host computers.
123	SNTP ²	UDP	ADS/ADX 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 ADX Split Web/Application Server Metasys System Client SCT	I/O	Used by IIS on the ADS/ADX, 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, 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 ²	UDP	ADS/ADX 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

Port ¹	Protocol	Use	Metasys Device	Inbound/ Outbound	Description
					capable of receiving SNMP Traps. Alternate Method: If the system allows, use email destinations for remote alarm notification instead of SNMP.
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 ADX Split Web/Application Server Metasys System Client ³ SCT	I/O	Used by the Metasys system to access user objects and attributes within Active Directory service. LDAP is a standard communication protocol for directories located on TCP/IP networks.
443	SSL	TCP	ADS/ADX Metasys Advanced Reporting ADX	I/O I	Metasys 8.1 and higher 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 SCT	I	With BFT, file transfers occur between the device and SCT where the device is the HTTPS client and SCT is the HTTPS server.
445	NT LAN Manager Version 2 (NTLMv2)	TCP	ADS/ADX 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 Network Engine	O	Used for alarms and events
502	Modbus	TCP	Network Engine	O	Used for receiving Modbus messages from a vendor device
514	Syslog	UDP	ADS/ADX 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,

Port ¹	Protocol	Use	Metasys Device	Inbound/ Outbound	Description
					conforming to Internet published RFC 3164.
587	SMTP	TCP	ADS/ADX Network Engine	O	Used for alarms and events
636	LDAPS	TCP	ADS/ADX ADX Split Web/Application Server Metasys System Client ³ SCT	I/O	Used by the Metasys system to access user objects and attributes within Active Directory service. LDAPS is a secure communication protocol for directories located on TCP/IP networks.
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 ADX Split Web/Application Server Metasys System Client SCT	I/O	Used by IIS on the ADS/ ADX/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/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.
1443	BACnet/SC	TCP	ADS/ADX/NAE85/ LCS85	I/O	This is the default port. However, an Administrator can configure BACnet/SC for an alternate port using Metasys UI or JCT.
1833	MQTT	TCP	Network Engine	O	Used for communicating with vendor devices that use MQTT messaging over a non-secure connection.
8883	MQTT	TCP	Network Engine	O	Used for communicating with vendor devices that use MQTT messaging over a secure connection (TLS).
9004	Johnson Controls Licensing Service	TCP	Software Manager	I/O	For Computer only, it may be closed.
9005	Johnson Controls Licensing Service	TCP	Software Manager	I	For Computer only, it may be closed.
9910	Microsoft Discovery Protocol ²	TCP/ UDP	Network Engine SCT NCT and NAE	I	Used by NCT to get diagnostic information from devices on the same network.

Port ¹	Protocol	Use	Metasys Device	Inbound/ Outbound	Description
			Update Tool		
9911	Metasys Private Message ²	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.
11001⁴	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 ⁵ / SNx/NAE85/SCT	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 Generally recorded by the IANA.

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

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

⁴ This port number is registered to Johnson Controls.

⁵ In this document, 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
4050 ¹	Wireless Many-to-One Sensing ²	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.

² Johnson Controls proprietary protocol.

Table 1.6.1.4: (Optional)¹ Outbound internet Port numbers and protocols

Port	Protocol	Use	Devices	Inbound / Outbound	Description
53	DNS	UDP	Server	O	Domain Name System. 9.9.9.9 (Quad9 security-focused DNS).

					49.112.112.112 (Quad9 security-focused DNS)
123	NTP	UDP	Server	O	Network Time Protocol
443	HTTPS	TCP	Server	O	Application messages over HIP on WebSocket <ul style="list-style-type: none"> • *.tempered.network (Airwall related mgmt. and relaying of application messages) • *.openbluesec.cloud (Airwall's new management domain being migrated to from *.tempered.network over time) • *.openbluecloud.ai (certificates and other security-related data loaded from here during cloud onboarding) • mybuildinglifecycle.johnsoncontrols.com (product registration) • *.metasys-access.johnsoncontrols.com (heartbeat and sync of SRA accounts)

¹ In section 1.3.1, Johnson Controls recommended that you do not connect Metasys directly to the internet without having protective security measures in place. However, to set up the server's built-in Airwall for secure remote access by your BAS service provider, the ports and hosts above will need to be accessible for outbound communications only.

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.

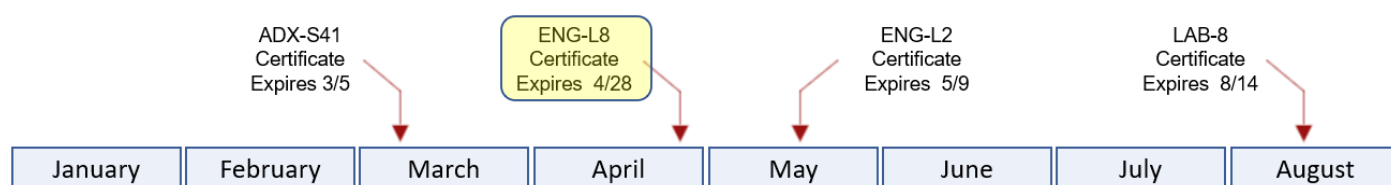
- Section 1.2.12 - Metasys configurable attribute called the **Certificate Renewal Period**
- Section 2.7.2 - How to load TLS certificates
- Section 3.1.12 - Review TLS communication certificate expiration dates

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

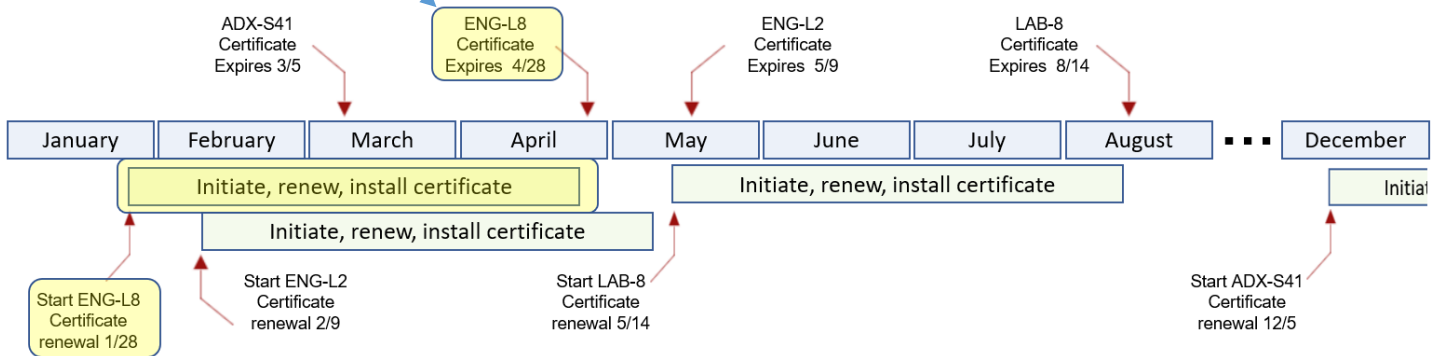


Each organization will have a varied process and timeline to renew certificates. Consult with the local IT department and review related policies to learn how long this task will take. This timeline must be identified, then added to your plan. In this example assume it takes an organization 90 days to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



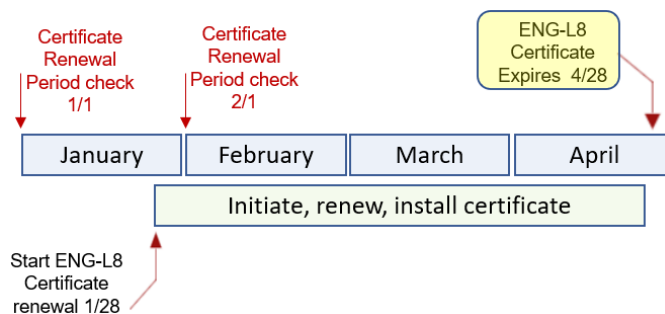
To keep all certificates current, configure the **Certificate Renewal Period** attribute to 120 days minimum (90-days for the process + 30-day buffer).

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 on 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 Network planning

This section describes network planning including infrastructure protection.

For additional network planning information on:

- How to plan your Metasys network and implement 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 their 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 which belong to the same connection.

1.7.1.4 Secure Remote access

The recommended method to remotely access Metasys is by using an Airwall Gateway or a customer managed VPN.

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 an Airwall Gateway

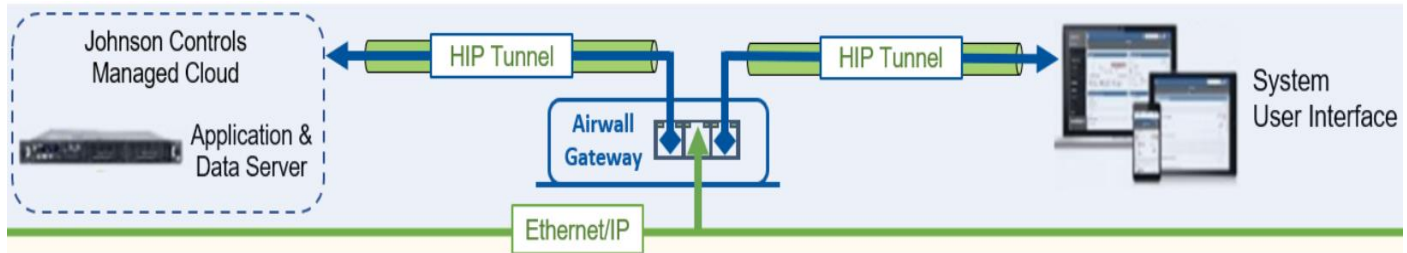
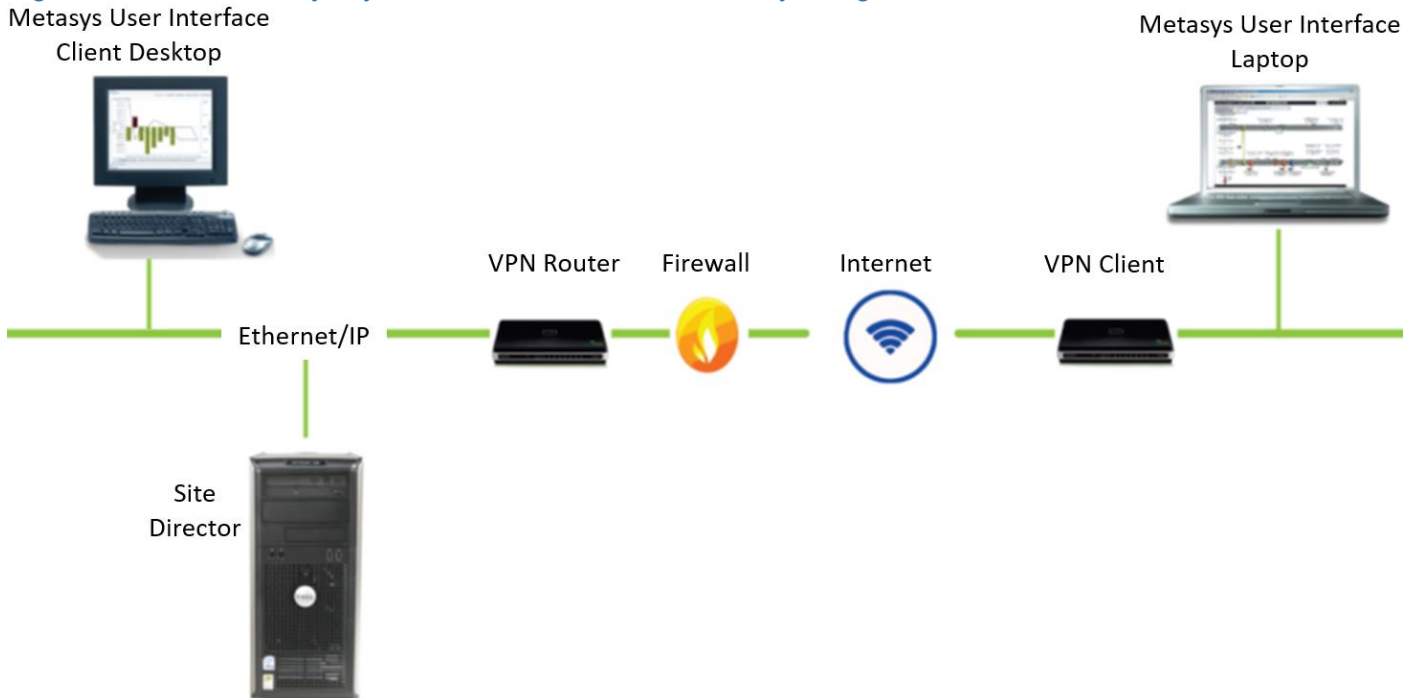


Figure 1.7.1.4.2- Metasys system Internet communication by using VPN



1.8 System requirements

Hardware and software. 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.

Metasys Server Operating System. 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, for specific computer requirements for all Metasys software products and tools.

Third-party components. During the installation, third-party components (such as SQL server, RabbitMQ, .NET, etc.) are installed on the customer's machine for Metasys to function properly.

Note on Vulnerability scans: If a vulnerability scan of a Metasys server suggests any third-party component should be updated or removed, the customer should perform the following before acting:

- Explore available Metasys patches and updates – See [section 3.1.11](#)
- Refer to the Metasys System Configuration Guide (LIT-12011832) to determine the correct third-party version required for your Metasys Release and patch level. See “sample” figure 1.8.1
- Ensure that the latest upgrade is working properly
- Ensure that other applications within your organization do not require the older version

Figure 1.8.1 Sample ADS specific requirements

Supported Operating Systems ⁴ and Database Software	<p>Windows® 11 Pro and Windows® 11 Enterprise versions 22H2, 21H2 (64-bit) General Availability Channel (GAC)</p> <p>Windows® 10 Pro and Windows 10 Enterprise Editions versions 21H2, 22H2 (64-bit).</p> <p>Windows® 10 Enterprise LTSC (1809, 21H2) (64-bit)</p> <p>Supports:</p> <ul style="list-style-type: none">• SQL Server® 2022 Express with CU9 (64-bit)• SQL Server® 2019 Express with CU18 (64-bit) <p>ⓘ Note: SQL Server 2019 or later may cause the configuration service cache that builds stored procedures to time out. This causes the user's logon to Metasys UI to fail. To resolve this issue, set SQL Server 2019 or later databases to run in 2017 compatibility mode. For more information, refer to docs.microsoft.com</p> <ul style="list-style-type: none">• SQL Server® 2017 Express with CU31 (64-bit) <p>ⓘ Note: If no SQL Server is present on the computer, the ADS software automatically installs SQL Server Express.</p>
--	---

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. The 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 Deployment overview

On-site deployment

Security hardening of Metasys begins prior to deployment with careful planning as outlined in Section 1 of this guide. It is 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.

Managed Metasys deployment

When using Managed Metasys, the hardening of the server is provided as part of the service. See section 1.1.5 Managed Metasys for additional details.

2.1.1 Physical installation considerations

Physical installation considerations of components within your Metasys solution are covered in section 1.3 – 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, in 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 document (LIT-12012162).

Operating system patches. You may decide to patch your system before installation of Metasys or after. Please see section 2.4 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 default before being put into service in a new deployment. In the event 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). For additional information see the Engine (SNC / SNE) Commissioning Guides, Recovery instructions - Recovery to same partition.

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 beyond the commissioning process should be disabled.

When configuring a new system, prior to the customer requirements being provided, default to a zero-trust network configuration. Once the commissioning phase is complete, be sure to remove any temporary infrastructure and consider further hardening of the system before transitioning to production.

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>
- **Metasys Security Features eTool** – Created to provide a place where employees could identify the security features added to Metasys and at what release. While employee facing, there is a download option in the upper right corner of the home page that leads to a document that can be shared with customers.
- [Working with FIPS 140-2 Level 1 Compliance & Certification Job Aid](#)
- Security Certificate Options @ Metasys 8.1 -
https://JCI.sumtotal.host/core/pillarRedirect?relyingParty=LM&url=app%2Fmanagement%2FLMS_ActDetails.aspx%3FActivityId%3D243424%26UserMode%3D0
- [Metasys Secured Access Job Aid](#) (C-6980-L1-EN)
- [Single Sign On using OAuth 2.0 & LDAP](#) (job aid)
- [Metasys & Cyber Security video](#) - ~2020.

2.2 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/>

General CIS Cybersecurity Guidelines. "...The CIS Controls (formerly known as Critical Security Controls) are a recommended set of prioritized cyber defense best practices. They provide specific and actionable ways to protect against today's most pervasive and dangerous attacks. SANS provides CIS Controls v8 training, research, and certification..."

Reference: SANS Institute, CIS Controls v8, <https://www.sans.org/blog/cis-controls-v8/>

Note: The primary focus of this hardening guide is on application-level hardening, while not all hardening mechanisms have been tested with Metasys functionality and compatibility, there are no notable conflicts in implementing the standard CIS Controls guidance provided by the SANS institute.

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 \(On-premises Hosted only\)](#)
- ☐ [Hardening Step 5: Load TLS certificates](#)
- ☐ [Hardening Step 6: Audit logs](#)
- ☐ [Hardening Step 7: Backup and Restore](#)
- ☐ [Hardening Step 8: Web Server maxQueryStringLength setting](#)

2.3 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.

2.4 Disable unused ports

Unused ports should be blocked 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.

2.5 User management

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 2.5.1

Feature	Description
User account password length	8-50 characters <i>Note: If you're using AD LDAP(S) or OAuth 2.0 identity providers, limitations apply. See specific Metasys, Microsoft, or OAuth documentation.</i>
Blocked Words List	Metasys includes a list of blocked words that cannot be used in creating passwords. For additional details about the Blocked Words List, view details at this link - https://docs.johnsoncontrols.com/bas/r/Metasys/en-US/Security-Administrator-System-Technical-Bulletin/14.0
Inactive Sessions	5 minutes timeout (30 is the default)
Password history	Can be set between 1-12 (10 is the default)
Maximum Password Age	365 days for user level accounts (default is 60) 60 days for admin level user accounts (default)
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 the account expires, the user is logged out of the system.

2.5.1 Metasys User Roles and Permissions

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

Roles

You must assign a minimum of one default or custom role to each local or external user account.

The following are the Metasys default user roles:

- 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 external user can access all authorized features of the online Metasys UI and the SCT.
- Tenant Access: The Metasys local system user or external 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 Metasys UI. The Metasys local system user or Active Directory user can access the Metasys API and all authorized features of the Metasys 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. 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 2.5.5 for more information on applying the least privilege.

Figure 2.5.1.1 – Metasys UI User Management: Users Tab

Username	Full Name	Email	Role	Authentication Type	Last Login	Status	Actions
MetasysSysAgent	Metasys System Agent		2 Roles	Metasys Local	05/14/2024 10:53 AM	Active	
Operator	Metasys System Operator		USER	Metasys Local		Active	

Figure 2.5.1.2 – Metasys UI User Management: Roles Tab

Role Name	Description	Group Name	Users	Actions
ADMINISTRATOR	System Administrators Group	Administrators	1	
MAINTENANCE	Maintenance Group		0	
OPERATOR	Operators Group		0	
USER	Users Group		2	

2.5.2 Metasys Local User Accounts

Metasys Local Users must use strong or complex passwords, comprised of the criteria shown in table 2.5.2.1 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 organizational policies:

Table 2.5.2.1 – User Account Passwords criteria

Attribute	Minimum requirement	Recommended for further hardening
Password total length	8 characters	Create passwords of at least 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

Special rule	The password cannot contain three consecutive characters from the user account name.	
---------------------	--	--

Figure 2.5.2.2 Metasys UI User Details Tab

The screenshot displays the Metasys UI for user management. The top navigation bar shows the user's name, 'Warren Johnson'. The left sidebar contains a 'Back' button and a list of user details: Full Name (Metasys System Agent), Username (Warren Johnson), Email (Metasys System Administrator), Role (ADMINISTRATOR), Access (Standard), Last Login (05/14/2024 2:04 PM), Status (Active), and Authentication Type (Metasys Local). The main content area has four tabs: User Details, Account Settings, Timesheet, and Category Access. The 'User Details' tab is selected, showing fields for Full Name, Username, Email, Role, Access, Last Login, Status, and Authentication Type. The 'Account Settings' tab is also visible, showing fields for New Password, Confirm New Password, Password Length, Access Type, and Language. The 'Category Access' tab shows system privileges and role settings. The 'User Details' tab includes a 'Full Name' field with the value 'Warren Johnson', a 'Username' field with the value 'Warren Johnson', an 'Email' field with the value 'Metasys System Administrator', a 'Role' dropdown menu set to 'ADMINISTRATOR', an 'Access' dropdown menu set to 'Standard', a 'Last Login' field showing '05/14/2024 2:04 PM', a 'Status' dropdown menu set to 'Active', and an 'Authentication Type' dropdown menu set to 'Metasys Local'. The 'Account Settings' tab includes a 'New Password' field, a 'Confirm New Password' field, a 'Password Length' section with 'Minimum Password Length' set to 8 and 'Maximum Password Length' set to 50, an 'Access Type' dropdown menu set to 'Standard', and a 'Language' dropdown menu set to 'English (United States)'. The 'Category Access' tab includes a 'Single Access User' checkbox, a 'User Can Modify Own Profile' checkbox, a 'User Cannot Change Password' checkbox, an 'Allow Expert Navigation' checkbox, an 'Allow Expert Object Views' checkbox, a 'Temporary User' checkbox, an 'Expires On' date field set to '05/14/2024', a 'Role' dropdown menu set to 'ADMINISTRATOR', and a 'System Privileges' section with buttons for 'MANAGE DEVICES & SITES', 'VIEW METASYS STATUS', 'DISCARD ACKNOWLEDGED EVENTS', and 'DISCARD ALL EVENTS'. The bottom right corner of the main content area has 'CANCEL' and 'SAVE' buttons.

2.5.3 Metasys External User Accounts:

Metasys supports the following implementation of external account types:

- OAuth, including Active Directory Federation Services (ADFS) See [section 1.2.13](#) for more information
- Lightweight Directory Access Protocol (LDAP) is discussed below
- Lightweight Directory Access Protocol over SSL (LDAPS) See [section 1.2.13](#) for more information

Users 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.

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).

2.5.3.1 Microsoft Keep Me Signed In (KMSI).

Microsoft ADFS provides a "Keep Me Signed In" feature to extend user login sessions securely beyond the current session. By accepting the "Stay signed in?" prompt during sign in, the KMSI feature is activated to provide the user with a 24-hour cookie that allows for logins to persist across browser sessions for up to one day. See the Microsoft website for additional details on KMSI.

NOTE: When KMSI is enabled, it becomes more important for users to log out of Windows with the completion of each session to ensure that other users are not able to access resources granted 24-hour access using a KMSI cookie.

2.5.4 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.

2.5.5 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. When adding a role or a permission to a user's account, be sure to remove Metasys' roles and permissions no longer required or utilized in their new role.
- 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.

2.5.6 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.

2.5.7 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.

2.5.8 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 a password 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

2.5.9 Kiosk Service Accounts

Metasys does not include a user account specifically used for Kiosks. If a Kiosk display is desired, our recommendation is to set up a new user account for the Kiosk(s) and assign a role with **view only** permission, and with no session timeout. Note: Never assign this user account to the **Administrator** role.

2.5.10 User management best practices

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

2.5.10.1 *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 (such as SSO) with IIS process when using SCT.

2.5.10.2 *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.

2.5.10.3 *Password aging*

Password aging is a technique used to reduce the 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 365 (default is 60).

2.5.10.4 *Password history*

The system securely stores hashes of the last 10 passwords per user to prevent reuse of passwords when creating a new one. To maintain strong password hygiene and reduce the risk of credential reuse, administrators should ensure this setting remains at the default value or is increased.

2.6 Update Metasys to latest Release

As stated previously, updates to Managed Metasys systems are automatically included with the service. Managed Metasys users, please skip to the next hardening step. See section 1.1.5 for additional details.

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.

2.7 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 unencrypted 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.

2.7.1 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.

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

2.7.2 Communication certificate support

Follow your organization's IT policies and guidelines for replacing the default self-signed certificates with trusted CA Signed certificates on Metasys Server and engines.

Hardening Step 5: Load TLS certificates

Follow your IT organization's policies to request trusted CA signed certificates for your Metasys application server and engines. Note: Wildcard certificates are not supported by Metasys.

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

Metasys engine. 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-12013352) Appendix: Certificate Management.

2.7.3 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/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.

2.8 Configuring security monitoring features

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

2.8.1 Audit Logs

Hardening Step 6: 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.

Metasys UI. The Metasys UI 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. From the Metasys UI, select **System Activity** to view your audits and alarms in a list sorted by date and time.

2.9 Backup/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.

For Metasys configuration data (archive DB) Backup & Restore processes refer to the "Database" section for backup and restore in the System Configuration Tool Help, (LIT-12011964).

For Metasys Historical SQL Databases Backup & Restore processes refer to the In Place or Out of Place upgrade sections in the Metasys Server Installation & Upgrade Instructions (LIT-12012162).

Hardening Step 7: Backup and Restore

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

Note: Depending on the installed features, some of the files above may not exist on all Metasys installations. See Network and IT Guidance Technical Bulletin (LIT-12011279) for additional guidance.

2.10 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, NAE85, and LCS85 servers

Hardening Step 8: 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 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 3.1.1 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 after 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 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 3.1.1 **Cybersecurity maintenance checklist** on the following page.

Table 3.1.1 – Cybersecurity Maintenance Checklist

Item	Description	Immediate	Priority based	Daily	Weekly	Monthly	Quarterly	Annual
1	Backup historical data			✓				
2	Backup configuration data	✓						
3	Test backup data						✓	
4	Disable user accounts of former 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 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 applicable regulations							✓
15	Conduct security audits							✓
16	Update password policies							✓
17	Update as-built documentation	✓						✓
18	Update standard operating procedures							✓
19	Renew support contracts							✓
20	Check for end-of-support / discontinuation information							✓
21	Delete sensitive data in accordance with policies or regulations	✓					✓	
22	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, also known as the Metasys Archives (SCT / SCT Pro)	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.

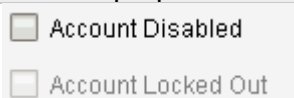
Action	Details	Suggested frequency
Test Backup data	Load data from backup media into a non-production Metasys	Quarterly

3.1.4 Disable user accounts of former employees

Disable user accounts of former employees immediately.

When using Active Directory (AD) services or external OAuth (section 2.5.3), accounts deleted from AD or an external identity provider will not be able to login to Metasys.

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



☐ Account Disabled
☐ Account Locked Out

3.1.5 Remove 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: If a user does not use their account for a long period, this may suggest that they do not have a need to use the system, and you should consider locking or removing their user account. 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 – User properties section.	Monthly

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.

User Details

Account Settings

Timesheet

Category Access

Inactive Sessions

☐ Never Terminate
 ☒ Terminate In Minutes

Account Lockout

☐ No Account Lockout
 ☒ Lockout After Bad Attempts

Lockout In Minutes

Dormant Account

☐ Do Not Check User Account For Dormancy
 ☒ Make Account Dormant After Days
 ☒ Create Dormant User Account Event
 ☐ Lock Out The User Account When Dormant

Maximum Password Age

☐ Password Never Expires
 ☒ Expires In Days

Password History

☐ Do Not Keep Password History
 ☒ Remember Last Passwords

3.1.6 Update user account roles and permissions

Users may change roles or their need to utilize the system. See section 2.5.5 for additional details

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

3.1.7 Disable unused features, ports, and services

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

e.g., features such as Alarm Monitor or services such as email notifications

Action	Details	Suggested frequency
Disabled unused features	Refer to your product Installation or User manuals. Also refer to sections 1.6.1 and 2.4 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/trust-center/cybersecurity/security-advisories> with a registered user account (create a username and password). User account registration is open to JCI customers and authorized representatives. At the bottom of the page, register to receive Metasys product security advisories via email. Some Key points to consider:

- Determine if your Metasys deployment is impacted by the conditions outlined in the advisories
- Referring to as-built documentation of the Metasys system will help with this assessment. A good set of as-built documentation will help identify the 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 the previous maintenance step. 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	Priority based

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 as well as 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 the previous maintenance step. 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	Priority based

3.1.12 Review TLS communication certificate expiration dates

Metasys uses two main types of communication certificates:

- **Web:** Used in the Metasys UI and Metasys to Metasys device communications
- **BACnet/SC** (optional in Metasys Release 12.0 or greater 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)	Documentation
Web	Metasys Engine	SCT: System Configuration Tool Help LIT-12011964
Web	Metasys Server (Windows)	See Appendix: Certificate management and security in the Network and IT Guidance Technical Bulletin LIT-12011279
Web	Metasys Server (Linux)	Metasys Server Installation and Upgrade Guide LIT-12012162
BACnet/SC	Any	BACnet/SC Workflow Technical Bulletin LIT-12013959.

For viewing web certificates, browse to the device and use the browser to look at the certificate. Use the BACnet/SC management feature in Metasys to view BACnet/SC certificates.

Action	Details	Suggested frequency
Review TLS communication certificate expiration dates	Review Web server and 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 recent security policies for your organization	Annual

3.1.14 Review applicable regulations

When Metasys is deployed in a location that is governed by regulation, it is important to check for any new or updated regulations. An assessment of the changes should be conducted periodically.

Action	Details	Suggested frequency
Review updates to regulations	Collect the 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, system 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 or 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. 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 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. 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).

3.1.20 Check for end-of-support / discontinuation information

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

3.1.21 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.

For additional details, see section 2.1.3 Resetting to the factory default settings.

Action	Details	Suggested frequency
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

3.1.22 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)
- Only install software (or hardware) which aligns with the policies of the environment's owner
- Monitor users who are logged into the system, then validate these with entries in either the **System Activity Log** in Metasys UI or review the **Cyber Health Dashboard** using the **User Activity Widget** (Section 1.2.1) in Metasys UI.

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

3.2 Metasys Release schedule

An update to Metasys including new features, feature updates, bug fixes, or security fixes is released approximately every 3 - 6 months depending on the content.

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

Appendix A - Additional Metasys Literature

Description	Literature Number
Security Administrator System Technical Bulletin	LIT-1201528
Metasys System Configuration Guide	LIT-12011832
NAE Commissioning Guide	LIT-1201519
SNC Commissioning Guide	LIT-12013295
SNE Commissioning Guide	LIT-12013352
Metasys Server Installation and Upgrade Guide	LIT-12012162
Network and IT Guidance Technical Bulletin	LIT-12011279
Metasys IP Networks for BACnet/IP Controllers Technical Bulletin	LIT-12012458
Metasys User Interface Help	LIT-12011953
Software Manager Help	LIT-12012389
System Configuration Tool Catalog Page	LIT-1900198
BACnet Controller Integration Technical Bulletin	LIT-1201531
Metasys Performance Verification Tool (PVT) User Guide	LIT-12012406
Metasys System Product Bulletin	LIT-1201526
Metasys WRG1830/ZFR183x Pro Series Wireless Field Bus System Technical Bulletin	LIT-12013553
Metasys BACnet/SC Workflow Technical Bulletin (Includes FAQs)	LIT-12013959
ADS/ADX Commissioning Guide	LIT-1201645
Metasys for Validated Environments, Extended Architecture Catalog Page	LIT-1900466
Metasys System Software Purchase Options Product Bulletin	LIT-12011703
Metasys for Validated Environments on Metasys UI	LIT-1901214

Note: When searching for Metasys LIT documents, using either link below, choose the most recent release associated with your software version.

[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
HIP	Host Identity Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDMS	Identity Management System
IEEE	Institute of Electrical and Electronics Engineers
IOM	Input/Output Modules
IP	Internet Protocol
KMSI	Keep Me Signed In
JCT	Johnson Controls Configuration Tool
LDAP	Lightweight Directory Access Protocol
LDAPS	Lightweight Directory Access Protocol over SSL
MDM	Metasys Database Manager tool
MFA	Multi-Factor Authentication
MRP	Media Redundancy Protocol
MS/TP	Master-Subordinate Token Passing
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
PSA	Product Service Agreement
RDP	Remote Desktop Protocol
RNI	Remote Network Interface
RPC	Remote Procedure Call
SA	Sensor Actuator
SA	System Administrator (Built-in SQL Server account)

SC	Secure Connect (BACnet/SC)
SCT	Software Configuration Tool
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 Metasys UI. This cannot be set globally in IIS without removing the configuration from each web.config file included in Metasys, because IIS doesn't support multiple layers adding the same header.
- Q2 Can strict transport security (HSTS) be enabled globally in IIS?
 A2 HSTS – Metasys SOAP and REST APIs return this response header. This cannot be globally set in IIS without removing the configuration from each web.config file included in Metasys, because IIS doesn't support multiple layers adding the same header.
- Q3 Can X-Frame headers be set to Deny globally in IIS?
 A3 In Metasys UI this is already set to "SameOrigin" which is required to facilitate certain Metasys features. X-Frame cannot be set globally in IIS because in Metasys UI, the PPA/Fault widget runs under its own web application in an iFrame.
- Q4 Can the SQL Server System Administrator (sa) account be disabled?
 A4 Yes. Metasys doesn't require the SQL sa account, which should be disabled when not in use.
- Q5 Can the public role in SQL be locked down?
 A5 Yes, Metasys does not use SQL public role for any purpose.
- Q6 How is Kerberos used in AD LDAP?
 A6 From the Metasys process we use .NET to facilitate the LDAP query to Active Directory. Customers can enable/disable LDAP protocols independent of Metasys.
- Q7 Can the site specify/manage the list of local administrators on the machine via group policy or will this conflict / create problems for Metasys?
 A7 Metasys does not use local administrators' group in any way.
- Q8 Does Metasys support API Keys for email authentication?
 A8 Metasys does not currently support API Keys for email authentication.
- Q9 Does Metasys support wildcard SSL certificates?
 A9 No. Wildcard SSL certificates are not supported.
- Q10 Does Metasys use Group Managed Service Accounts for MSSQLSERVER or SSO?
 A10 Metasys does not require the use of local groups, domain groups, or SQL Server groups for any purpose. For additional details see section 1.3.3.
- Q11 Can I disable CLR in SQL Server?
 A11 Yes, if Metasys reporting is not used and SCT is not running on the same server.