Cyber Solutions Universal Hardening Guide

GPS0026-CE-EN
Version 2.0
Rev A
Revised 04-02-2025

Johnson Controls

Introduction

Our practices provide peace of mind to our customers with a holistic cyber mind set beginning at initial project design concept, and is supported through deployment, including a rapid incident response to meet comprehensive and evolving cybersecurity environments.

This Universal Hardening Guide intends to provide cybersecurity guidance used in planning, deployment, and maintenance periods for building solutions without a dedicated hardening guide.

If the target solution can be connected electronically via a wired or wireless network, this guide should be consulted to plan for cybersecurity hardening of the components and the whole system. As the guidance provided is not product specific, it can be used with most solutions independent of brand or application.

As you review the guidance provided within, determine if the solution supports the recommended hardening step for the intended application. If it does, proceed to implement that hardening step by referring to the respective product documentation for details on how to execute. In some cases, there may be product limitations that prevent the full implementation. It is often better to proceed with partial controls then to skip that control entirely without any protection. If you are unsure about the best approach to take, seek assistance from a cybersecurity professional, such as a Security Champion or Cybersecurity Solution Architect.

As cybersecurity threats affect all connected devices, it is important to ensure that cybersecurity is considered throughout the planning, deployment and maintenance phases associated with a solution's functional operation. This guide provides hardening guidance for configuration and maintenance, including the operating system, user accounts, permissions and roles, backup and restore, redundancy, and patch management.

This Johnson Controls **Universal Hardening Guide** is broken down into three sections depicting the overall process for hardening:

1. Planning	2. Deployment	3. Maintain
Define the scope, and identify security features, along with the characteristics of the associated components	Select the required hardening steps based on the products and security features of the target system components	Build a maintenance checklist of ongoing tasks for the operational phase of the solution

Before you begin…

First confirm that a solution specific guide is not available for the target product before proceeding with the universal guidance.

- **Johnson Controls products:** A comprehensive list of available hardening can be found on the public website at https://www.johnsoncontrols.com/trust-center/cybersecurity/resources
- **Third-party products:** Consult with the respective supplier's support representatives to identify which hardening resources are available
- **Hybrid approach:** If hardening resources are available, you may consider using an existing hardening guide along with this Universal Hardening Guide for more comprehensive hardening

If hardening resources are not available, then refer to this **Universal Hardening Guide**.

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, expressed or implied, as to the efficacy of the cybersecurity practices or recommendations described within. 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.

Contents

1 Planning

The Planning section is designed to help organize the deployment of smart building solutions. The contents within this section are useful in several planning stage functions:

- Establishing the scope of the solution to be hardened
- Assuring compliance with the cybersecurity criteria that governs the target environment
- Designing the deployment architecture
- Providing a reference for settings made during deployment

1.1.0 Solution scoping

The first step in planning the solution hardening is determining the components in scope. If the component is to operate independently, then the scope of hardening steps may be isolated to a single device (See scope 1, 2, or 3 in Figure 1.1.1). However, you must widen the scope when a system includes multiple components or entire systems (Scope 4 in figure 1.1.1). Be sure to check for dependencies the solution requires to operate as you will want to consider for inclusion within the targeted scope.

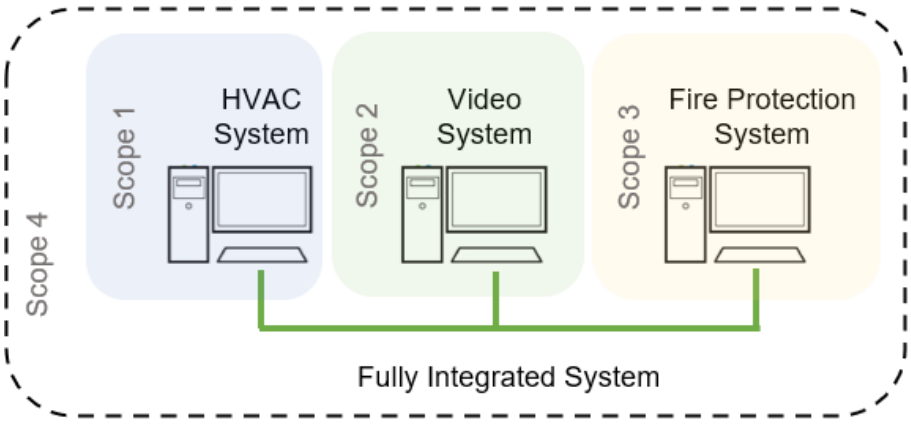
For example, one use case may detail a chiller panel used to configure a chiller independent from external connections. In a second use case, it may be necessary to connect a laptop via a web browser to configure the chiller, while a third may have that chiller interoperate with the building management system. In the later use cases, remote service access may need to be considered as in-scope.

If external components or systems already have their own hardening guide, utilize these as the primary source for hardening the external elements. How you enable the connection of external components within the local interfaces are in scope a single hardening exercise.

1.1.1 Scoping integrated solutions

It is best practice to set your scope into manageable “chunks”. While modern smart buildings often incorporate multiple systems into a single integrated solution, it is often easiest to address the hardening of each system, level, or segment within a system independently.

Figure 1.1.1



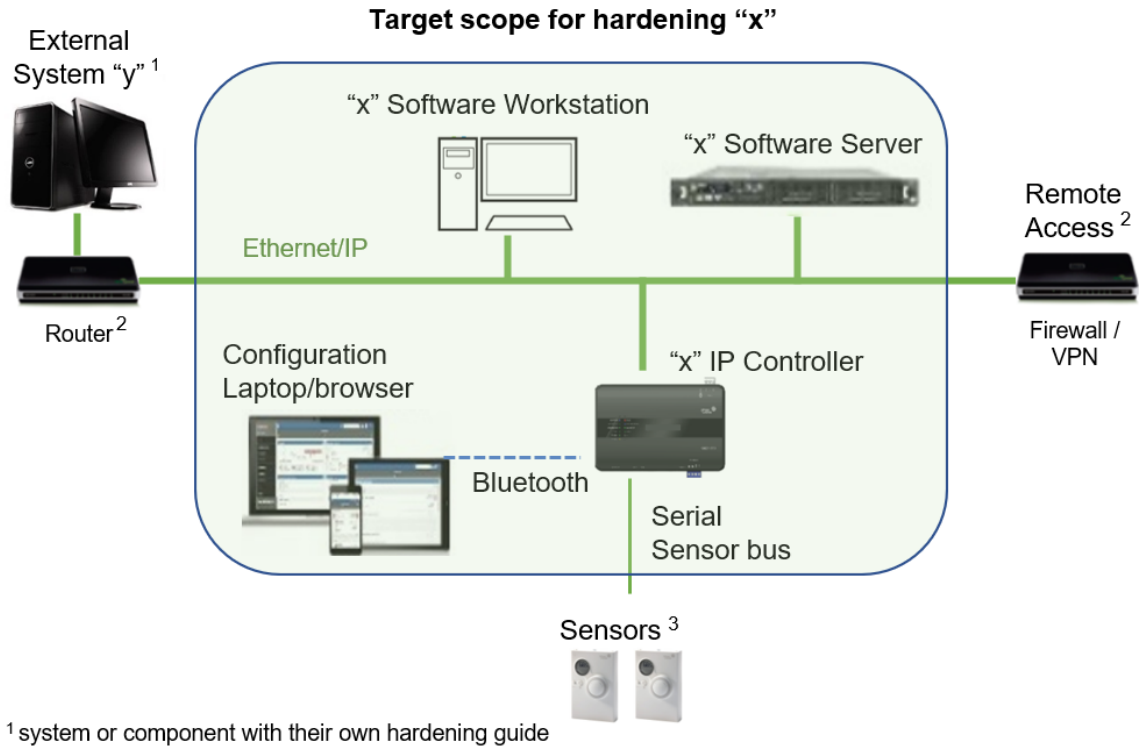
In figure 1.1.1, you’ll see three separate systems as scope 1, 2 and 3. Once the hardening of each individual system is finished, continue to harden the integrated solution (Scope 4).

1.1.2 Deployment architecture

With a solution scope in mind, draw a simple diagram to depict the devices, computers and mobile devices which will interact with each other (i.e., communicating via a wired or wireless network). In some cases, you may want to include non-IP serial networks. For simplicity, you may group similarly configured components together (e.g., cameras, controllers, workstations, servers, remote connections).

To establish a comprehensive understanding of the target scope, it is recommended to include connected devices and systems which are immediately outside the scope (but usually not deeper). When out-of-scope components are included, be sure to identify them as such. One technique is to draw a box around the in-scope components to clearly indicate the target hardening scope.

Figure 1.1.2 – Example generic architecture referred to as "x"



[1] system or component with their own hardening guide

[2] system or component with hardening steps influenced by target scope

[3] system or component with no configuration of communications or security

1.1.3 Components

Identify the components which focus on what you want to protect or “harden” against security threats for this collection of hardening actions (those which are “in-scope”). These are typically the components that perform the following actions:

- Acquire – such as a sensor, or camera
- Process - such as a server or controller
- Store – usually a database
- Present data - user interface
- Take a control action within a system - such as valves, locks, lights, or triggers.

Often you may identify additional, essential components that operate independently and are not part of the system. These supporting components are explained further in the next section.

Figure 1.1.3 –System Components

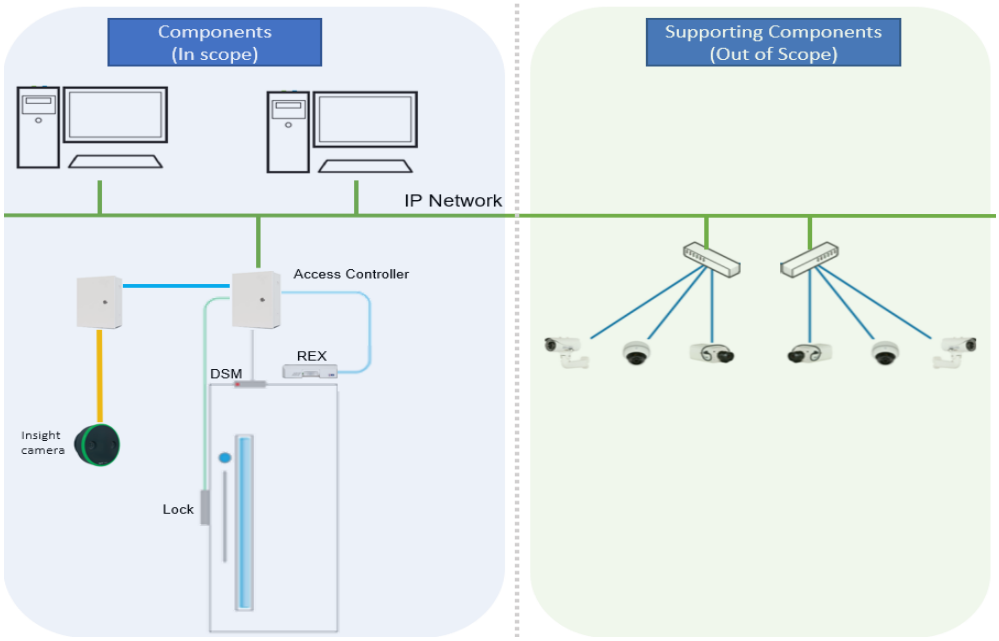


Figure 1.1.3 shows examples of both components (blue shaded) and supporting components (green shaded). It is important to note that certain devices, such as a camera can be either a component or a supporting component depending on the focus of the hardening scope.

1.1.4 Supporting components

Supporting components are those which are necessary for system operations but are not within the targeted scope. Typically, these are devices and software which are from a different supplier or sub-system, with their own distinct hardening steps. As stated in the scoping section, these often have their own hardening documentation.

Typically, all the networking equipment is addressed as a separate hardening exercise as “in-scope” components.

For example, a video surveillance system can take advantage of existing on-site cameras by connecting them to the target video management server, which is designed to be compatible with standard IP video and networking components.

1.2.0 Security feature set

Johnson Controls products are designed with built-in cybersecurity features. Some features are included and not set up by default, while other features require the reader to perform steps for advanced hardening. Refer to your system, engine, and component documentation to collect the security features for your solution.

The table below lists examples of some common security features that may apply to your installation. After collecting features specific to your solution, review each row, then do the following:

- Check either Available or Not Available
- Write in any additional features not listed but applicable on the blank lines

Table 1.2.0 – Sample security features

	Security Functional Area	Security Feature / Description	Available	Not Available
1	Human user accounts	Re-nameable built-in accounts	[ ]	[ ]
2		_____	[ ]	[ ]
3	Human user passwords	User changeable passwords	[ ]	[ ]
4		_____	[ ]	[ ]
5	Password policy	Definable password policy	[ ]	[ ]
6		_____	[ ]	[ ]
7	User authentication	Multifactor Authentication (MFA)	[ ]	[ ]
8		System usage banner	[ ]	[ ]
9		Invalid logon attempts (maximum)	[ ]	[ ]
10		Inactive account lockout	[ ]	[ ]
11		Inactivity logout	[ ]	[ ]
12		_____	[ ]	[ ]
13	Centralized user authentication	Active Directory support	[ ]	[ ]
14		OAUTH support	[ ]	[ ]
15		LDAP support	[ ]	[ ]
16		Remote Authentication Dial-In User Service (RADIUS) support	[ ]	[ ]
17		Single Sign On (SSO)	[ ]	[ ]
18		_____	[ ]	[ ]
19	User authorization	Configurable permissions	[ ]	[ ]
20		Role Based Access Control (RBAC)	[ ]	[ ]
21		Object level permissions	[ ]	[ ]
22		Database partitioning (multi-tenant)	[ ]	[ ]
23		_____	[ ]	[ ]

24	Communications	Configurable network interfaces	[ ]	[ ]
25		Configurable web server (enable/disable)	[ ]	[ ]
26		Configurable IT protocols (TLS, SSH, FTPS, SMTP, SMTPS, NTP)	[ ]	[ ]
27		Configurable OT protocols (BACnet/SC, OPC-UA, OSDP v2, ZigBee)		
28		Configurable network ports	[ ]	[ ]
29		Configurable remote access controls	[ ]	[ ]
30		Configurable firewall	[ ]	[ ]
31		_____	[ ]	[ ]
32	Wireless security	Configurable wireless interfaces	[ ]	[ ]
33		Configurable wireless password	[ ]	[ ]
34		Configurable wireless protocol (WEP,WPA1, WPA2, WPA3)	[ ]	[ ]
35		_____	[ ]	[ ]
36	Digital certificate management	View Certificates	[ ]	[ ]
37		Generate Self-signed Certificates	[ ]	[ ]
38		Load Trusted Certificates	[ ]	[ ]
39		Distribute Certificates	[ ]	[ ]
40		_____	[ ]	[ ]
41	Audit logs	Audit log support	[ ]	[ ]
42		Configurable audit log (State)	[ ]	[ ]
43		Configurable audit log (Storage)	[ ]	[ ]
44		Time synchronization support	[ ]	[ ]
45		_____	[ ]	[ ]
46	Availability assurance	Redundancy failover	[ ]	[ ]
47		Backup and restore	[ ]	[ ]
48		_____	[ ]	[ ]
49	Software updates	Field installable updates	[ ]	[ ]
50		_____	[ ]	[ ]

1.3.0 Intended environment

Physical access and installation of devices can greatly impact cybersecurity. Many components are designed to be operated in a controlled, indoor, dry environment, while others specify harsh usage outside, in dust, high humidity, rough vibration or extreme temperatures. In any instance, components at each level will possess varying degrees of access. Here is some general guidance based on typical environments per component type:

Server Level components – A server or server appliance is to be installed on-premises within an equipment rack in a secured, temperature-controlled location, such as within a data center, locked closet, or IT Server room with restricted access.

Supervisory Level components – These components are designed to be installed within a user supplied panel or enclosure usually in an upright orientation. 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 components – These components are usually designed for use in more rugged areas such as a warehouse, or outside. Components may be mounted horizontally or vertically. It is recommended that the installation location is dry (if possible), away from corrosive vapors, away from electromagnetic emissions and not 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 components.

1.3.1 Internet connectivity

Check product documentation to see if your product, a specific feature, or integration requires internet access. Internet access increases your cybersecurity footprint and attack area which requires additional hardening steps. As a rule of thumb, do not connect your product to the internet unless specifically required.

Note: Some systems that were not originally intended to be connected to the internet are connected through misconfigured firewall rules. Be sure to check with IT personnel to ensure the correct rules are in place.

If internet access is deemed required for this installation, consult your IT department for steps to take to limit external access. An example of some hardening steps you will want to include are removing unnecessary version of TLS and installing a trusted certificate.

1.3.2 Integration with IT networks

Server components may be deployed on a dedicated and isolated network or on a non-dedicated, shared network. Zero-trust architectures, and to a lesser level of protection, VLANs, may be used to share infrastructure but maintain isolation. It is typical for clients to be installed on shared IT networks. Consult with the appropriate network security professionals within your IT department to ensure your reduce system exposure. Be sure to fully read and understand IT Compliance documentation for your site.

1.3.3 Integration with external systems

Your system may integrate with components within external systems such as other Microsoft Active Directory, Identity management systems, and NTP servers.

1.4.0 Hardening methodology

While most building automation products provide onboard security safeguards, including many secure-by-default settings, we recommend that the device is hardened according to the guidance outlined in section 2, deployment.

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

1.4.1 User management best practices

Following best practices for managing user accounts, their 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.

On most systems, you can create unique user accounts for each user / operator. If your system employs role-based access control (RBAC), you can further control the operator functions. With RBAC, a user is assigned a role in which they acquire the permissions associated with that role. It is a best practice to assign only the minimum permissions necessary for users to perform their duties. Apply the administrator role sparingly. Note: In section 3, you will be advised to review this list of administrators to ensure those who have changed roles or have exited the company no longer have elevated permissions.

The proper configuration of individual user accounts assures that security best practices are followed and that all user actions cannot be repudiated. Best practices for account management include:

1.4.1.1 No shared accounts

Unique accounts should be used during all phases of operation. Installers, technicians, auditors, and other deployment phase users should never share common user accounts to assure a non-reputable audit trail of their actions.

When user accounts are shared, it no longer becomes possible to determine which specific operator performed actions. While most systems are configured to log user's actions, the user can repudiate that they logged in at that time. Furthermore, sharing of user accounts makes the application of least privilege and separation of duties more challenging.

1.4.1.2 Remove or rename default user accounts (as permitted)

By removing or renaming default user accounts, the ability to gain unauthorized access to the system will be reduced as those attempting to do so will need to enter an unpublished username which is much harder to gain knowledge of. When a default user account cannot be removed or renamed, the best practice is to at least change their default passwords (see Change default passwords).

1.4.1.3 Change default passwords

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

1.4.1.4 Least privilege

When assigning access rights users should only be given access to what they need to access to do their job. This way, users may be assigned only responsibilities required for their function.

1.4.1.5 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 include:

- Sites
- Buildings
- Sub-system (Fire, HVAC, security)
- Building owner vs. integrator role
- Functions (operations vs network management vs. backup)

Active Directory groupings can facilitate this separation, which in turn reduces the risk of insiders successfully committing fraud.

1.4.1.6 Centralized user account management

Identity Management Systems (IDMS) offer enhanced security over the local management of users. The IDMS can utilize standard protocols such as OAuth2 (Open Authorization) and Lightweight Directory Access Protocol (LDAP), open standards including Security Assertion Markup Language (SAML) or proprietary protocols, such as Active Directory Domain Services, which is used by Microsoft Active Directory. Microsoft Azure AD supports open standards such as SAML and OAuth2. IDMS solutions 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.

Centralized user account management can be further expanded through by federating management via Single-Sign-On (SSO) capabilities as facilitated by Active Directory Federated Services (ADFS) and Okta which integrate to other platforms using OAuth, OAuth2, and SAML.

1.4.1.7 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. Many systems now provide a configurable password policy which you can use to achieve the desired level of password strength. Password policies are often governed by local policies.

1.4.1.8 Password aging

Password aging is a technique used to reduce to possibility of password exploitation. When enabled the user is forced to change their password after a set time-period has elapsed.

1.4.1.9 Password history

Password histories are used to mitigate against password reuse.

1.4.1.10 Password policy

It is important to have a password policy. Customers often have password policies that all systems must support.

1.4.1.11 Account expiration

Accounts should be set to automatically expire for known temporary usage, such as consultants, or maintenance personnel.

1.5.0 Data flow diagram

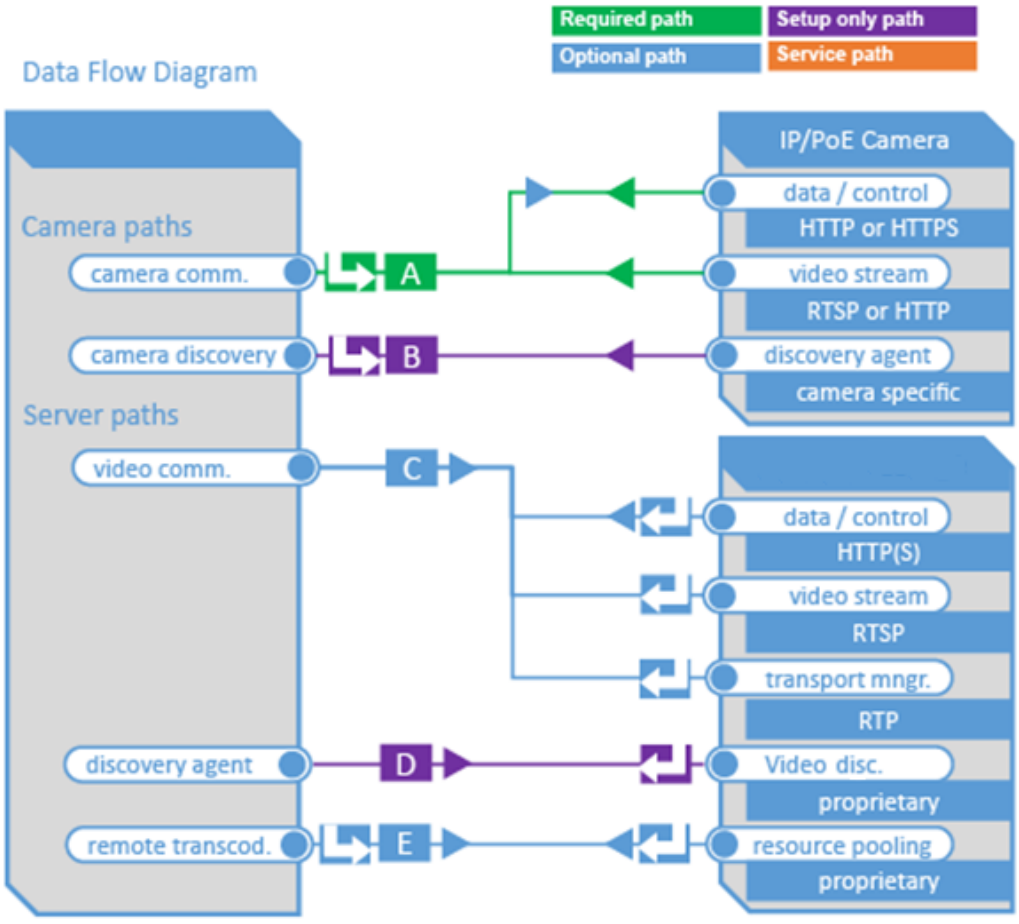
A data flow diagram is a detailed view of the architecture which will show each communication path and flow direction. This resource will be used to aid in the configuration of network security settings (rules) within routers, firewalls, and zero-trust architectures.

The use requirements of each path should be identified as:

- Required – this path must be established for the solution to function for all supported applications.
- Optional – this path is optionally required depending on the functions that will be enabled (e.g., webserver, email)
- Setup only – this path is only needed during the setup and configuration and disabling during normal operations is recommended. Note: This may also be referred to as the Commissioning path.
- Service – this path is only needed for service. A service path is typically a temporary remote service connection which is disabled during non-service periods.

It is useful for someone who is not as familiar with the process to break the communication paths to understand the processes for the basic to the more complex applications. It is helpful to group paths by function. Communication paths should be labelled so they can be referenced within the document.

Figure 1.5.0 Sample Data Flow Diagram



1.5.1 Communication paths table

A communication paths table should be created to define the ports and protocols used by each communication path as outlined in the data flow diagram that was referenced in section 1.5.0.

Communication paths table should include the following elements:

- Path identifier and/or name
- Functions within each path (e.g., data, control, stream)
  - A-Side details (local to the target component)
    - Interface (e.g., API, HTTP client, device discovery, NTP client, SNMP server, BACnet, OSDP)
    - Network port
    - Default state
    - Connection type (constant, on-demand, scheduled, manual)
  - B-Side details (remote target component)
    - Network port
    - Protocol type (i.e., UDP, TCP)
    - Internet access (if used should be indirect and managed through a firewall)
  - Flow direction
    - Initiating side (A, B or both)
  - Additional configuration notes

Figure 1.5.1 Sample Communications Path Table

Path	VideoEdge					Direction / use requirement[2]	Connecting Component			Notes
	Function	Interface	Default Port Assignment	Default Port State[1, 2]	Port Activity (if enabled)		Default Port Assignment[1, 3]	Protocol	Internet access[4]	
A	**Camera communications**					**Required**	**IP/PoE Camera**			
	data and control (non-secure)	HTTP Client	Dynamic	*if standard mode*	∞	↳ ▶[5] ◀	80	TCP	-	*select between HTTP or HTTPS[4,6]*
	data and control (secure)	HTTPS Client	Dynamic	Enabled	∞	↳ ▶[5] ◀	443	TCP	-	
	video stream	RTSP Client	Dynamic	Enabled	∞	↳ ◀	554	TCP	-	*select between RTSP or HTTP[6]*
	video stream	HTTP Client	Dynamic	Enabled	∞	↳ ◀	80	TCP	-	
B	**camera discovery**					**Commissioning only**	**IP/PoE Camera**			
	veAutoDiscSSDP	camera discovery	32200-65535	Enabled	On demand	↳ ◀	1900	UDP	-	
	nvrupnpn	camera discovery	32200-65535	Disabled	On demand	↳ ◀	1900	UDP	-	

1.6.0 Network planning

Building automation systems transmit, collect, process and, store sensitive data that will disclose sensitive information if accessed by unauthorized users. While most have several security controls in place to limit access to authorized users, it is best practice for the network design to provide additional layers of defense.

When designing your network, first determine which components will be included in the full scope of the system required to provide all the planned functions for that system.

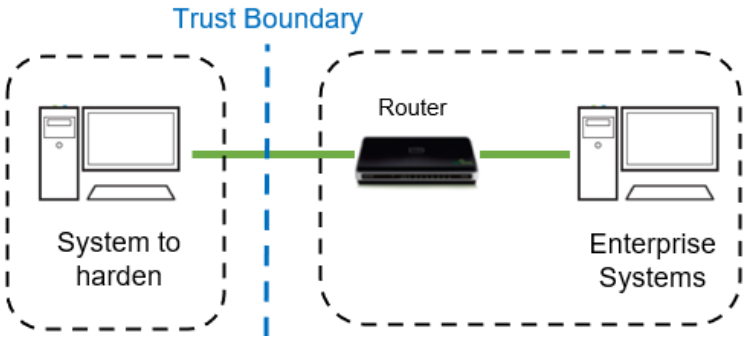
For example, planning out your network should include all the components associated with the following areas:

- Building automation and controls
- HVAC Equipment
- Refrigeration
- Fire and Special hazards
- Water and mechanical
- Fire detection
- Security
- Retail
- Other OT areas (not included above) specific to your network which require hardening

With the full scope of components and functions in mind you can build a target level of protection into the network design to protect both the network and endpoints. Keep in mind that some of the system components, while fully compatible, may not support the desired level of protection. In those cases, compensating controls may be utilized within the network design to reduce risk.

1.6.1 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. Conceptually, the trust boundary will guide your focus on these areas which are more prone to vulnerabilities.



Products that are not part of the target system or those systems which do not provide methods to sufficiently authenticate a component, or user may be regarded as having a lower of level of trust. Networks may also have different levels of trust. For example, an isolated network with only video cameras and Network Video Recorders (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.

1.6.2 Network protection

Isolating your system from networks of lower trust is recommended.

1.6.2.1 Zero-Trust Architecture

Zero-Trust networking solutions elevate the protection of remote access required for modern building services. Not only does the zero-trust technology encrypt communication, but its capabilities can also enable granular access controls and micro-segmentation to reduce the attack surface. This technology provides protection against unauthorized access, lateral movement, and malware propagation.

Zero-trust can be used in a defense-in-depth approach to isolate the smart building equipment and controls.

1.6.2.2 Demilitarized Zone (DMZ)

When communications to or from your system is required from an untrusted network (from the perspective of your system), such as a corporate LAN, a demilitarized zone (DMZ) may be established to provide a high degree of data flow control and prevent direct access to resources on the network.

Use of a DMZ is strongly recommended with providing remote connectivity in conjunction with other safeguards such as a VPN and multi-factor authentication.

1.6.2.3 VLANs

A Virtual Local Area Network (VLAN) provides the ability to share the networking infrastructure while maintaining separation between trusted and untrusted networks. The use of VLANs reduce deployment costs by removing the need to run dedicated cabling and networking equipment for the system.

If physical access to the cabling used for the VLAN is possible by authorized users, it is recommended that the VLAN switches are configured for to protect eavesdropping by employing encryption technology.

1.6.2.4 Firewalls

Routers and switches which are used to bridge trust boundaries should employ firewalls.

1.6.2.5 Remote access

Remote access points should be protected and always treated as access from an untrusted network.

1.6.2.6 VPN

A Virtual Private Network (VPN) should always be used to provide encrypted and authenticated communication for remote access connections. VPN technologies that are enabled for multi-factor authentication are recommended. Any application intended for an internal network but used over the internet, must be done through a VPN connection.

1.6.3 Endpoint protection support

Check to see if the operating system of your device includes a firewall that you can enable and configure.

1.7.0 Anti-virus

Some building solution products come with pre-installed Anti-virus software while others do not. Consult your product literature to see if there are specific setup requirements to follow or recommendations for a product to use. Below is a starter list of considerations you should look for in your product literature and from your virus software provider.

Example list of considerations

- Target server / desktop operating system type / Version (Windows, Linux, etc.)
- Antivirus memory requirement
- Antivirus CPU overhead requirement
- Compatibility with other protection services such as Windows defender
- Default or custom installation
- Update frequency
- Permissions

Some products can interfere with the communication between building automation systems. As general guidance, if you are installing anti-virus software, be sure that it is first tested in a controlled, non-production environment. An adverse reaction is rarely welcome in your production environment.

1.8.0 Hardware and software requirements

Some products are sold as pre-configured appliances while others are designed to be installed on hardware that you provide on-premises, in a data center or within the cloud. Most products designed for installation on your own desktop, server or mobile device, etc. come with an installation guide. Look through respective product installation guides to plan what you need to make your installation successful.

The table below shows areas you want to review in advance to ensure that hardware and software does not cause any faults during installation.

Hardware		
Footprint	Desktop, Server, Mobile device, or pre-configured appliance	Follow the recommendations from your installation guide
Location	On-premises, Hosted or Cloud	Consider the best location for your solution
Central processing unit (CPU)	Review the minimum requirement and the recommended requirement.	We recommend you purchase the recommended CPU or higher. Consider future expansion and upgrades when making this decision.
Memory	Review the minimum requirement and the recommended requirement.	We recommend you purchase the recommended memory or higher. As future updates are installed, you'll want headroom to expand your system. If you are installing VM, you can adjust the memory as needed.
Disk storage	Review the literature for hard disk requirements	We recommend you purchase a hard disk with plenty of room for expansion. Take note if RAID is recommended Look for any external storage requirements
Operating system	Windows, Linux, iOS, Android, etc.	Always use the recommended operating system. For the most up to date cyber security, aim for the most recent, and validated build.
Network	Take note of the interface, protocols, and speed requirements	Always match the network specifications during installation and upgrades

Software		
Operating system	Windows, Linux, iOS, Android, etc.	Refer to your installation guide
Versions	Current or last stable version	Your installation guide should provide you with information to select the appropriate OS version. Note: This may not always be the most current version. For example: Windows 10 may be recommended although Windows 11.0 is released but not validated for certain features

2 Deployment

This section is designed to help execute the deployment phase of your system. The contents within this section address how to initiate secure deployment for new installations, how to harden your attack surface and additional steps after commissioning required before the new or upgraded system is turned over to runtime operations.

2.1.0 Deployment overview

Security hardening begins prior to deployment with careful planning as outlined in section 1 of this guide. It is a good practice to review sections prior to deployment to fully understand the security feature set, 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

2.1.1 Getting started

Before you start the installation of your solution, consider the guidance in the following sections.

2.1.2 Physical installation considerations

Install hardware using the instructions provided in the installation guide. Keep in mind that the physical access to the device and physical installation of the device can impact the cybersecurity.

Physical access to certain devices enable actions that cannot be authenticated and logged electronically through the capabilities of this product. To prevent unauthorized access, be sure to place the device in a room, cabinet or enclosure that can restrict access (for example, mechanical lock or physical access control).

Some products are equipped with an optical tamper switch that you can use to send and log electronic alerts regarding physical tampering of the installation. Consider using protective electric wire conduits when communication wires with paths through areas of lower trust. If an installation requires or uses a locking enclosure, be sure the closure is kept locked when not being serviced and the key is not left in plain sight.

2.1.3 Default security behavior

On the initial startup, certain functions will be enabled to facilitate the most common commissioning tasks. Examples may include

- Automatic device discovery (example: Cameras)
- A configuration webpage
- User account settings (example: changing password on first login)

- Enhanced password validation

2.1.4 Resetting factory defaults

If this device was previously used as part of another installation or test environment, or has become unresponsive, the unit should be reset to factory defaults before being put into service in a new deployment.

See the installation or administration guide for details on how to reset to factory defaults.

2.1.5 Considerations for commission

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

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

2.1.6 Recommended knowledge level

The person confirming that the proper hardening steps are executed should be experienced in your product's administration and networking technologies. If training for your product(s) exist, completion of the basic installation course is required, and any advanced installation course is recommended.

2.2.0 Hardening

While many products include secure-by-default safeguards, additional hardening is usually required 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 the customer policies and government regulations that may govern the application security settings for this deployment.

2.2.1 Hardening checklist

This checklist provides an example list of hardening steps you may select to go through. The actual steps you will take is based upon the features included within your specific environment as gathered in Section 1.3.0.

- For steps that are not applicable to your instance, check off the “N/A” column
- As you complete the remaining steps, check off or include the date these were completed

Hardening Step	Status	
	Complete	N/A
1: Configure BIOS	-	-
1.1: Enable BIOS password	☐	☐
1.2: Prevent USB boot	☐	☐
2: Configure user accounts	-	-
2.1: Verify that only the required accounts are active	☐	☐
2.2: Rename built-in accounts	☐	☐
2.3: Change default user account passwords	☐	☐
2.4: Configure password formation policies	☐	☐
2.5: Set login invalid attempt lockout policy	☐	☐
2.6: Set the inactivity lockout policy	☐	☐
2.7: Set the inactive account log out policy	☐	☐
2.8: Set password history policy	☐	☐
2.9: Create user account groups and roles	☐	☐
2.10: Configure application for centralized authentication	☐	☐
2.11: Map application roles to authentication server groups	☐	☐
2.12: Create unique user accounts for each user	☐	☐
2.13: Assign roles, groups, and permissions for each user	☐	☐
2.14: Repeat steps (2.1 - 2.13) as required for each component	-	-
Server	☐	☐
Clients	☐	☐
Devices	☐	☐
3: Configure the system use banner	☐	☐
4: Update software	-	-
4.1: Update operating software	☐	☐
4.2: Update application software	☐	☐
4.3: Update device firmware	☐	☐
5: Configure communications	-	-
5.1: Configure network interfaces	☐	☐
5.2: Configure network ports and protocols	☐	☐
5.3: Configure FIPS 140-2 options	☐	☐
5.4: Configure IP addresses	☐	☐
5.5: Configure remote access services	☐	☐
5.6: Configure firewall and routers	☐	☐
5.7: Configure multi-factor authentication	☐	☐
6: Configuring wireless features (Wi-Fi, Bluetooth, Zigbee, Cellular, etc.)	☐	☐
6.1: Configure wireless password or pin	☐	☐
6.2: Turn off wireless broadcasting	☐	☐
6.3: Set or adjust the Bluetooth bonding interval	☐	☐
7: Configure certificate support	☐	☐

Checklist is continued on the next page

Hardening Step	Status	
	Complete	N/A
8: Configure security monitoring features	-	-
8.1: Configure audit log (state and storage)	☐	☐
8.2: SIEM integration	☐	☐
8.3: SNMP	☐	☐
8.4: Configure time synchronization	☐	☐
9: Configure availability features	-	-
9.1: Configure backups for configuration and data	☐	☐
9.2: Configure redundancy	☐	☐
10: Security audits and documentation	☐	☐
10.1: Security documentation	☐	☐
10.2: Security audit checklist	☐	☐
11: Remove unused software	☐	☐

2.2.2 Introduction to hardening

Before you begin, it is important to keep these points in mind:

- This is a universal guide and does not provide product specific configuration steps
- General guidance will be provided on the recommended action(s)
- You will need to gather documentation for the respective product and its operating system as you plan for and execute hardening steps.
- As you go through the hardening steps, refer to the checklist in section 1.2.0 which indicates the features your product supports to determine their applicability.

The following pages provides guidance on each of the items within the hardening checklist from section 2.2.1. When you encounter a step that is not applicable or not supported, skip to the next section.

NOTE: The hardening steps and sections below are written with the assumptions that all capabilities exist.

2.2.3 Configure BIOS

It is important to protect the BIOS configuration from being modified by unauthorized users.

Hardening step 1.1: Enable BIOS password

Enable password protection of the computer's BIOS and set the password. This password should only be known to administrators that have been authorized.

Note: You will need the administrator password when any BIOS changes are made.

Hardening step 1.2: Prevent USB boot

The boot sequence should prevent boot up by USB devices as it is a possible for USB devices to inject malicious code without warning.

Go into your BIOS and ensure that USB is not part of the boot sequence.

2.2.4 Configure user accounts

In this section you can find information on user management. Before executing the steps in this section, determine how the target application manages users. Here are the types of user management you may encounter:

- Independent accounts - Application and operating system has their own set of user accounts. You must manage both operating system and application user accounts separately.

- Linked accounts - Application and operating system share user accounts. The application allows users to sign on the application automatically using the active operating system user account of that computer or device.

- No accounts – Some devices such as thermostats may have a simple interface or no-interface. Their functions may be considered "public" without any sensitive data or control and may not require authentication. However, if a device provides access to sensitive data or control without authentication, you must implement compensating controls or consider replacement.

User Management of components may be decentralized or centralized. Knowing if management is centralized will determine if you need to configure users on all similar components or just the central server:

- Decentralized – each device has its own set of user accounts with no centralized management

- Centralized - a central server manages user accounts which are either distributed throughout the network for local authentication or require remote authentication by the central server. Standard methods such as Microsoft Active Directory (AD), LDAP, Oauth2, RADIUS are often utilized. Applications sometimes employ proprietary methods for centralize management without the use of a standard protocol. See hardening step 2.10 for additional guidance.

NOTE: Some solutions have components that support centralized users for the operating system, but decentralized accounts for the application.

The hardening steps (2.1 - 2.13) will apply differently based on whether management is shared, independent, centralized, or decentralized. These steps will not apply to devices without user accounts. Refer to the following table for applicability guidance.

Hardening Steps (2.1 - 2.13) Component Applicability:

Management Type	Operating System (OS)	Application	Hardening steps (2.1 - 2.13) applicability
Independent	Centralized	Centralized	Configure for both OS and application central servers
Independent	Centralized	Decentralized	Configure OS central server and repeat for the application in each component
Independent	Decentralized	Decentralized	Repeat configuration for each component for both OS and application
Independent	Decentralized	Centralized	Configure application central server and repeat for OS in each component
Shared	Centralized		Configure once for the OS central server
Shared	Decentralized		Configure once for each component
No user accounts	N/A	N/A	Skip steps 2.1-2.13

Hardening step 2.1: Verify that only the required accounts are active

Go through your list of active users and deactivate any accounts you do not plan to use. Each human user should have their own dedicated account. Unless required for non-interactive (e.g., automated backup account) system operation, all other accounts should be disabled.

Hardening step 2.2: Rename built-in accounts

Review the accounts on your system and rename any built-in accounts as they are often documented and publicly known.

Hardening step 2.3: Change default user account passwords

Review the accounts on your system and change the default passwords for any built-in accounts as they are often documented and publicly known. Changing default user account passwords and making them unique enhances the security of the product.

Hardening step 2.4: Configure password formation policies

If the component operating system or application is configured to utilize centralized authentication, then the password policy will be defined within the authentication server, such as an Active Directory server or an application specific user distribution server. Otherwise, a local password policy should be configured. Use the following guidance when configuring password policies:

Attribute	Minimum requirement	Recommended for further hardening
Password total length	8 characters	Create passwords of at least 15 characters
Special characters	1 character such as -, ., @, #, !, ?, $, %. All other special characters are invalid, including spaces.	Include 2 or more non-succession special characters
Upper Case characters	1 character	Include 2 or more
Lower Case characters	1 character	Include 2 or more
Numbers	1 character	Include 1 or more
Blocked Words List	Add list of words as suggested from an online Blocked Words List	Add company and product names associated with project (e.g., JCI, Metasys, OpenBlue, etc.)

Hardening step 2.5: Set login invalid attempt lockout policy

Configure the login invalid attempt lockout policy to limit credential theft through password guessing.

The options for lockout policy will vary per operating system or application. Here are some options you may be presented with:

Invalid attempt lockout – is engaged when a configurable number of invalid login attempts are attempted within a client interface.

- Reset mode – what action is required to reset an account lockout
  - Admin reset - requires administrator to reset lockout
  - Time delayed reset - automatically reset lockout after a configurable time-period
- Retry limit – how many invalid login attempts will trigger an account
- Retry delay – time duration before retry count is reset and use can attempt login again as their first try

Hardening guidance for invalid attempt lockout is as follows:

Policy Setting	Minimum baseline protection	To strengthen protection
Lockout Policy	Time delayed reset automatically resets lockout	Admin reset forces manual reset by administrator

Retry Limit	3*	lower retry limit
Retry Delay (minutes)	10*	increase retry delay

* These values should be set to practical limitations based on risk (I.e., what are the consequences if an operator is locked out during an emergency?).

Hardening step 2.6: Set the inactive account lockout policy

Inactive account lockout - Accounts may be set to automatically lock if not used within a set time-period, to ensure users not actively using application are disabled (Example: 30, 60 or 90 days). When login is attempted after this time-period, the account is locked and may only be unlocked by an administrator.

Policy Setting	Minimum baseline protection	To strengthen protection
Lockout Interval (Days)	90 days	Lower lockout interval period

Hardening step 2.7: Set the inactivity log out policy

Configure the session inactivity log out policy to reduce risk of unattended user sessions.

Policy Setting	Minimum baseline protection	To strengthen protection
Auto log out	☑ (enabled)	☑ (enabled) is the strongest setting
Auto log out interval (minutes)	10	Lower auto log out interval

Note: The inactivity lockout interval may be limited for certain accounts and roles such as administrator and system accounts.

Hardening step 2.8: Set the Password History policy

The password history setting prevents a user from changing their password to a recently used password.

Policy Setting	Minimum baseline protection	To strengthen protection
Password history	3	Increase the password history restriction number

Note: Reducing the value of the password history setting may cause the password history to be cleared from memory.

Hardening step 2.9: Create user account groups and roles

User account groups and roles simplify permissions assigned to users and can be applied to both the operating systems and application level. This type of management is known as Role Based Access Control (RBAC)

Operating System user groups provide a means to establish baseline permissions for operating system functions. Application roles establish permissions for the application. It may be possible to add explicit grant or

deny permission to specific user to increase or decrease a user's authorizations from the baseline defined by their assigned role.

Hardening step 2.10: Configure application for centralized authentication

Centralized authentication improves security for application-level user authentication. The application may need to be configured to support centralized authentication using a standard protocol such as LDAP, RADIUS, or OAuth2, or a proprietary method specific to the solution. These technologies can also be used to enable Single Sign On (SSO) authentication.

When integrating with a central authentication server, a secure connection using a Certificate Authority certificate for the authentication server is recommended.

Policy Setting	Minimum baseline protection	To strengthen protection
Use centralized authentication	☑ (enabled)	☑ (enabled) is the strongest setting
Use security certificate to validate connection	☑ (enabled)	☑ (enabled) is the strongest setting

Once an authentication server has been configured for use by an application, it may be possible to link groups (e.g., LDAP groups) to application roles to further simplify administration.

Hardening step 2.11: Map application roles to authentication server groups

Map each role within the application to the respective group defined in the authentication server.

Hardening step 2.12: Create unique user accounts for each user

Each user should have their own dedicated account to access the operating system and application. An operator must not use built-in accounts.

Hardening step 2.13: Assign roles, groups, and permissions for each user

If groups or roles are available use those to assign the base authorizations to each user; otherwise assign individual permissions to each user.

It is important to understand the effective permissions when a user is assigned to multiple roles or group. Some solutions have permission rules which permit the most permissive sum of authorizations from each membership while others will treat an explicit deny within any group or role they belong to as overriding to block an authorization.

Permissions, groups and roles should be assigned to users to assure the best practices for user management are followed. The assignment of the role to users sets their authorizations. Therefore, the assigned authorizations should consider what a user "needs to have access to" following the principles of least privilege and separate of duties.

Some solutions support the configuration of object level permissions for more granular authorization which further supports least privilege assignment of authorizations. Database partitioning is a technique that can be useful in separating multi-tenant users who share a common database. Database partitioning ensures that cross-tenant access to data is prevented.

Hardening step 2.14: Repeat steps (2.1-2.13) as required for each component

Ensure that all components within the system have the user accounts managed according to hardening steps 2.1 through 2.13. Inspection should include all levels and types of components – servers, clients and devices.

2.2.5 System use banner

A System Use Banner provides the operator with details on the system use policy they must comply with in other to use the system. The banner message text needs to be consistent with applicable laws, executive orders, directives, polices, regulations, standards, and guidance that governs the system use.

This message is displayed prior to the user logon. By logging on to the system the user is acknowledging their acceptance of the policy outlined in the banner

Hardening step 3: Configure the system use banner

System use banners can be applied to some operating systems and some applications. Applying to the application's user interface (local or web based) is often the most ideal location as it can to be tailored specifically for the use of that application versus the entire computer environment.

2.2.6 Software updates

Installing the latest operating system and application versions and patches ensures that the most current security features are available and vulnerability fixes are applied. It is important that any known issue is addressed, even during the commissioning process.

Create backups of the configuration and data prior to performing any update. See hardening step 9.1 for details

Hardening step 4.1: Update operating system software

The operating system should be updated to the current released version with all applicable patches applied during and after the commissioning process. In some cases, a version or patch may be incompatible. Before updating the operating system, consult with the supplier of the application it will run to confirm compatibility.

Hardening step 4.2: Update applications software

Update the application software according to the supplier's instructions. Ensure that all pre-requisites are satisfied.

Hardening step 4.3: Update device firmware

Firmware updates for devices may need to be executed from a central server which distributes the updates to the devices it manages. In other cases, firmware is installed via a device's webpage interface, proprietary interface or through removable media such as a USB memory device or compact flash.

NOTE: Older computers, applications and devices may become incompatible with the solution or lack the capability to support security features needed for compliance (e.g., processor, storage, networking, and encryption resources). If presented with non-compliant devices, plan to replace those devices with solutions that can better enable conformance.

2.2.7 Configure communications

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

Communication to and from each component should be configured according to the principal of least functionality. Least functionality is a security measure designed to limit functions only to those 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.

To fully address communication security, it may be necessary to configure setting on both the operating system and application.

NOTE: Should a mis-configuration result in the inability to communicate with support tools, you may need to physically connect to the component to re-enable or manually reset that component to factory defaults. See section 2.1.4.

Hardening Step 5: Configure communications

In this section you can find information on configuring communications for security. When hardening the communications refer to the system architecture, data flow diagrams and communication path tables you created in section 1. These resources will help you identify the require interfaces, ports, protocols, and services required for the operation of the solution as designed.

Hardening step 5.1: Configure network interfaces

A computer or device may support multiple network interfaces (Ethernet, USB, wireless, RS232, etc.). Some physical interfaces can support multiple network interfaces. It is important to disable any network interface (physical or virtual) that is not required by the solution. Several products include specific steps to disable an unused network interface in their product manual. See your specific product manual for additional details.

NOTE: for more details of wireless configuration see Hardening Step 6.

Hardening step 5.2: Configure network ports and protocols

When configuring network ports and protocols be sure to disable insecure options when a secure option is available. Secure options made simply add encryption or also provide authentication as with TLS. For example, disable use of HTTP in preference to HTTPS communications, which provides encryption and authentication via TLS, when HTTPS is supported.

Be sure to consider both Information Technology (IT) and Operation Technology (OT) protocols such as BACnet, OPC, OSDP and Zigbee. Secure versions of OT protocols can be available (BACnet/SC, OPC-UA, OSDP v2, and Zigbee security), but if they are not, compensating controls should be used to provide security.

Wireless interface configuration often includes protocol choices. Be sure to enable wireless security such as Wi-Fi Protected Access (WPA), Version 2 (WPA2), and Version 3 (WPA3). While a component may include Wired Equivalent Privacy (WEP) as an option, that security protocol has been deprecated since 2004 and should be disabled if WPA, WPA2, or WPA3 are available.

Also disable the use of other older protocol versions such as TLS 1.1 and older. Before disabling deprecated security protocols, it is important to ensure that all components utilizing are first configured to support the newer protocol version to avoid a disruption in communications.

For additional protection default ports numbers can be changed (e.g., change HTTPS default port of 443 to one that is not documented.)

Federal Information Processing Standard 140-2
The Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), is a U.S. government computer security standard used to approve cryptographic modules. The title is Security Requirements for Cryptographic Modules.

A FIPS module is a cryptographic module which may be comprised of hardware, firmware or software that implements cryptographic functions such as encryption, decryption, digital signatures, authentication techniques and random number generation.

Hardening step 5.3: Configure FIPS 140-2 Options

Solutions that support FIPS 140-2, often provide as a separate option and may require a separate license. Its configuration may require compatibility with other components within the solutions and special steps to configure.

Hardening step 5.4: Configure IP Addresses

In most cases, components should not be directly accessible from the internet. When assigning IP addresses not prescribed by the governing IT organization, the use of non-routable IP addresses is preferred. Non-routable IP addresses include:

- 10.0.0.0/8 (Range: 10.0.0.0 – 10.255.255.255)
- 172.16.0.0/12 (Range: 172.16.0.0 – 172.31.255.255)
- 192.168.0.0/16 (Range: 192.168.0.0 – 192.168.255.255)

Hardening step 5.5: Configure remote access services

Remote access should be managed for each component. Unless explicitly required for the solutions design, disable remote access services, web services and mobile access.

In particular, the following remote support services should be reviewed:

SSH (Secure Shell) - is an encrypted network protocol for text-based sessions on remote machines from another machine that has network access. 'PuTTY' is a common piece of software used to access remote Linux based machines via SSH.

RDP (Remote Desktop Protocol) - is a graphical desktop sharing protocol developed by Microsoft. It allows control of remote machines from another machine that has network access. Using the 'Remote Desktop Connection' available in Windows, service personal and administrators can access remote machines.

Other remote desktop – Applications such as TeamViewer and LogMeIn also provide a means to remotely service a computer running a desktop operating system (Windows, MAC, Linux).

Johnson Controls recommends the use of zero-trust solutions for remote service as it offers better security.

Webservers can also be used to provide remote access to data and user interfaces. It may be possible to limit the availability of webservers as well for improved security. Consider the following configuration options:

Disable webserver: Disabling external access is the most restrictive configuration. Disabling external access prevents the external web-based administration of a component. It may also disable functions that are required for normal runtime operations.

Disable UI webserver access only: Solutions may provide the ability to disable web-based users interfaces without disrupting other web services.

Disable Mobile Device Web UI Access only: Solutions may provide the ability to disabled mobile web users interface without disrupting other web services.

Concurrent Web UI Sessions: Disabling concurrent web UI sessions means that only one login for each web UI account is allowed at a time.

HTTPS is the secure version of HTTP, the protocol over which data is sent between your browser and the website that you are connected to. The 'S' at the end of HTTPS stands for 'Secure'. It means all communications between your browser and the website are encrypted. It is recommended that you use HTTPS only. It is also recommended that you change default ports to help defend against non-targeted attacks.

Hardening step 5.6: Configure firewalls and routers

Configure firewalls and routers to only allow communication paths as defined in the system architecture, data flow diagrams and communication path tables established in section 1.

Hardening step 5.7: Configure Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) is highly recommended for remote access connections. Configure MFA if remote access is required.

2.2.7 Configuring wireless features

Hardening step 6: Configuring wireless devices (Wi-Fi, Bluetooth, Zigbee, Cellular, etc.)

In hardening step 5, wireless network interfaces were either enabled for communication or disabled (turned off). For wireless interfaces that are enabled, step 5 also set the wireless protocol that is utilized. In addition to those steps, it is important to establish a password specific to that interface.

Hardening step 6.1: Configure wireless password or pin

A password should be established for each wireless interface that transmits non-public data. Be sure this password is kept safely in a tool such as 1Password and not shared freely. For example, a wireless host can be set to enter a passphrase to pair with a device, while a Bluetooth client device can be set to utilize a pin for authorization. Not all wireless protocols will support the use of a password.

Hardening step 6.2: Turn off wireless broadcasting

Several wireless protocols support turning off broadcasting of their wireless network IDs. Only authorized personnel should have access to wireless networks. Turning off broadcasting makes it less visible to bad actors and more secure to your organization.

Turn off the SSID, network name, Bluetooth ID, or other wireless broadcast ID. See your product manual for additional details on how to turn off broadcasting.

Hardening step 6.3: Set or adjust the Bluetooth bonding interval

The Bluetooth bonding interval is a timed assignment of a pairing of two devices. After pairing, the devices remember each other and can reconnect automatically in the future without needing to pair again.

- Set the Bluetooth bonding interval times to be in effect for the shortest duration necessary. This should be balanced with usability. For example: If work is planned for a single day, the lease should be set to expire after working hours.

See your product manual for settings which are available on your specific wireless device.

2.2.8 Configuring certificate support

HTTPS encrypts web traffic but does not verify the identity of the remote host without a properly configured digital certificate. Some solutions can create certificates that are unique to the individual component so a web browser or other clients can verify its identity. The certificate can be self-signed, or for more security-conscious customers, a trusted certificate authority can sign it.

Hardening step 7: Configure Communication Certificate

Determine the type of communication certificate to utilize - automatically generated or from a trusted certificate authority (CA). If using CA generated certificate disable automatic generation and install the CA generated certificate.

Table 18

	MINIMUM BASELINE PROTECTION	TO STRENGTHEN PROTECTION
AUTOMATIC GENERATION	Enabled ■	Disabled ■ *(must install signed certificate from trusted certificate authority if disabled)*

It is recommended to verify that a certificate was successfully installed. View the installed certificates details to confirm that the date range encompasses the current date.

NOTE: Some systems can distribute certificates to the devices it manages.

2.2.9 Configuring security monitoring features

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

Hardening step 8.1: Configure audits logs

Ensure that audits logs are enabled.

Solutions can track important types of system events and system operation and stores the data in logs which are useful for troubleshooting and incident investigation. Log data can contain administrative changes, device alerts, configuration changes, and system events.

Operating systems can also generate several different log files specific to each function such as general system operation, web server operation, web server errors, and Network time Protocol (NTP) operation.

Applications can generate application-specific log files to aid in diagnosing areas such as communication and functional events.

These audit trails keep track of system configuration operations including the configuration of information security controls. An audit log viewer may be included as part of the operating system or application.

If the component can define a storage location, ensure that the storage size can accommodate the storage of logs that satisfy the period in which logs must be retained for the solution. In some cases, it will be possible to set the log location to a remote storage device.

Hardening step 8.2: Configure SIEM integration

Using a third-party System Information and Event Monitoring (SIEM) tool, it is possible to collect syslog data from a device.

Hardening step 8.3: Configure SNMP

Simple Network Management Protocol (SNMP) governs network management and monitors network devices. It is sometimes used within a solution for health monitoring and failover functionality.

If not already configured as part of hardening step 5, go back and enable SNMP if its use is planned in support of security monitoring. It is highly recommended that the community string used is not a public value. If possible, disable the ability to respond to SNMP “set” commands.

Hardening step 8.4: Configure time synchronization

If not already configured in hardening step 5, enable the time synchronization protocol that will be utilized on each component. Net Time Protocol (NTP) is the most supported protocol for this purpose.

To support the integrity of log data, it is important that all components within a system that logs report on are synchronized to a common time. Both proprietary and industry protocols (e.g., Network Time Protocol (NTP), BACnet Time Synchronization Services) are available to perform time synchronization across a network. I some cases a combination of services will be used to ensure system wide time synchronization across a variety of devices.

2.2.10 Configure availability features

The solutions Johnson Controls supports provide critical operational function and their continuous operation can be essential for the safety of the building occupants, protection of assets and the compliant control of production environments. Therefore, it is important that these systems are continuously available for operation.

The backup and restore, and failover server features help to assure that the system is continuously available.

Hardening step 9.1: Configure backups for configuration and data

Making frequent backups of the system configuration during the commissioning phase can be beneficial if an error is made or lost due to a hardware failure. Once the system is made operational, being able to restore from a good backup minimizes the downtime of the system.

Backups should encompass both configuration and log for operating system and application as well as runtime data from applications.

Copies for the backup files should be stored externally from the server and ideally in a remote location to assure all the necessary backup files will still be available if there is a hardware failure or disaster at the site. Backup should be protected from unauthorized access using encryption.

Hardening step 9.2: Configure System with a failover server

For critical applications, redundant failover solutions can be investigated. Redundancy options are more common at the server level but can exist for components lower in the architecture is some cases. Redundancy can address failures in storage (e.g., RAID), power supplies, entire servers, or networks.

Consult the supplier for options available for the target solution along with respective documentation.

Note: SNMP, SSH or other protocols may be required for monitoring and control as part of failover solution.

2.2.11 Security audits and documentation

A well-documented deployment of the solution will be useful in security audits, and a security audit can expose errors in the system documentation and identifying gaps in protection. Each task feeds the other and it may be necessary to repeat hardening step 19, after an audit is complete and the gaps are addressed.

Hardening step 22: Security documentation

Document deployment once hardening is sufficient for run-time operations. When updates are released, or security advisories are published this documentation will be useful. The documentation will allow for quick assessment to determine if the deployment is impacted by the issues described in a security advisory and requires a configuration change, software update or patch.

Include the following details in creating as-built security documentation:

- As-built architecture drawing of system
- For all system components record:
  - Component identification
    - Name
    - Description
    - Device Type
    - Location
    - Vendor
    - Model
    - IP address
    - MAC address
  - Support details
    - Software version
    - Hardware version
    - Licenses
    - Installation date

- Communication configuration details
  - Enabled Ports and protocols
  - Encryption settings

Hardening step 23: Perform a security configuration audit

An audit of the security configuration will help reveal any missed steps and will allow for further hardening of the system. This will be particularly important if a less secure configuration was utilized to facilitate efficient deployment before the full infrastructure was available. Use the security gaps identified with the audit to tighten security to the appropriate levels of protection for the target environment before turning over the system to run-time operations.

The security audit must be conducted by someone who was not involved with the initial hardening of the system. An independent reviewer is more likely to find the security gaps the audit is intended to reveal.

The Hardening checklist outlined in this section must be used as the basis for the security audit checklist. (Section 2.2.1 Hardening checklist).

2.2.12 Disable unused features, services, and software

If your solution offers optional features and services, but you do not require them for your installation, you are strongly urged to disable them. This lowers the attack surface of your solution.

Remove Unused Software. Any new release, version, service patch or hotfix may use specific versions of software to function. Eventually, these older versions of software may become prone to vulnerabilities. After an upgrade, it is possible that older versions of third-party dependencies (such as .NET) are no longer required and can be removed. Check your release notes or product support to remove older versions if they reside on your system and are no longer needed after the upgrade.

Important note: Before removing any older version(s) of software:

- Ensure the software is not needed for any other function
- Ensure the system has been backed up in the event a restore is necessary
- Ensure all data was properly migrated to the new instance

3 Maintain

The contents within this section address how to monitor for potential cybersecurity issues and maintain protection levels because conditions change.

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 with enhanced hacking tools and more advanced testing techniques may, in the future, disclose vulnerabilities with the technologies used.

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

3.1.0 Cybersecurity maintenance checklist

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

The cybersecurity maintenance checklist is designed to see all the line items on the left which need to be performed during regular intervals. On the right you can quickly see which tasks need to be performed right away or daily, all the way up to yearly tasks.

The cybersecurity maintenance checklist is Table 3.1.0 on the following page.

Table 3.1.0 – Cybersecurity maintenance checklist

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

Customize this table to your solution:

- Cross off items that do not apply
- Add additional items in the blanks spaces at the bottom that apply

3.1.1 Backup runtime data

Runtime data can be the most valuable asset within your system. You can replace or reconstruct everything else. Confirm that the following backup steps are being executed:

Action	Details	Suggested frequency
Backup runtime data	Configure “Backup / Restore runtime data” within your system	Daily

3.1.2 Backup configuration data

If you need to restore or replace a component it is important to have a backup of its configuration data to minimize the time required to restore its functions. If you are using self-encrypting drives, please note that a manual record of the configuration will help assure that the system can be reconstituted should a drive need to be restored.

Action	Details	Suggested frequency
Backup configuration data	device configuration data	Weekly

3.1.3 Test backup data

After competing steps 3.1.1-Backup runtime data and 1.1.2-Backup configuration data, you should test your backups. This will provide assurance that the data backups contain the expected data and integrity.

Action	Details	Suggested frequency
Test Backup data	Restore data from backup media onto a non-production system and validate	Quarterly

3.1.4 Disable user accounts of terminated employees

Immediately disable user accounts of personnel who are terminated from employment voluntarily or non-voluntarily.

Note: If your system uses Active Directory (AD) services, accounts deleted from AD are usually removed automatically.

Action	Details	Suggested frequency
Lock accounts	Refer to your product Installation or User manuals for the procedure to lock user accounts. Also refer to any organizational policies that include user account handling.	Immediate

3.1.5 Remove inactive user accounts

While an employee may still be employed by an organization, they may not have utilized their system account for some time. This suggests that independent of being authorized to use the system, they do not have a need to use the system and their account access should be removed. This is sometimes referred to as a **use it or lose it policy**. This applies to all systems which are owned, managed, serviced, or used.

This best practice reduces the amount of active user accounts in the system and therefore lowers the potential attack footprint.

Action	Details	Suggested frequency
Remove inactive accounts	Refer to your product Installation or User manuals for the procedure to remove user accounts. Also refer to any organizational policies that include user account handling.	Monthly

Notes:

- Check with your local policy to determine if this should be performed more frequently
- Some systems have reports available to help this process

3.1.6 Update user account roles

Employees frequently change roles, causing their needs within a system to increase or decrease. Periodically review the roles assigned to users to ensure they are adequate and assigned only those responsibilities required for their function. See section 1.4.1.4 on Least privilege.

When adding a role or a permission to a user's account when that user has been granted new authorizations due to an organizational role change, be sure to remove the roles and permissions no longer required or utilized in their new role.

Action	Details	Suggested frequency
Update user account roles	Refer to your product Installation or User manuals for the procedure to update or change user accounts.	Quarterly

3.1.7 Disable unused features, ports, and services

Reassess the need for optional features, ports, and services that are no longer required, and disable them. This practice will lower the attack surface of your system resulting in a higher level of protection.

Action	Details	Suggested frequency
Disabled unused features	Refer to your product Installation or User manuals	Quarterly

3.1.8 Check for and prioritize advisories

You can usually find security advisories on a product's support website. Your product literature can inform you if you need to either receive account registration from a company representative or register a user account with that site. Some Key points to consider:

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

Check for advisories 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 product documentation for a specific website link that hosts advisories and explore each week	Weekly

3.1.9 Plan and execute advisory recommendations

Follow the plan determined in the previous maintenance step.

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

3.1.10 Check and prioritize patches and updates

While a patch or update may or may not relate to a security advisory, it is always best practice to apply the most current patches and updates. These patches and updates can include cybersecurity enhancements also fixes to known issues. Review the release notes and prioritize the benefits of the patch or update. The overall benefit should include the improved protection that will aid in lowering the cybersecurity risk.

Be sure also to check for updates and patches of third-party components such as networking equipment and operating systems by consulting with the respective vendor.

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

3.1.11 Plan and execute software patches and updates

Follow the plan determined in maintenance step 3.1.10. Consult with all parties who may be impacted by patches, updates or downtime and choose the best time for deployment.

Action	Details	Suggested frequency
Plan and execute software patches and updates	Plan and execute advisory recommendations as determined in maintenance step 10. Follow your update process	Base on priority

3.1.12 Review organizational policy updates

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

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

3.1.13 Review updates to regulations

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

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

3.1.14 Update as-built documentation

Update as-built documentation if the deployment architecture or component configuration changes. Some configuration changes happen without a formal project or plan and if such cases it may be common to negate updating the as-built documentation. Schedule a full update of the as-built documentation on a regular basis to ensure that all changes are documented.

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

3.1.15 Conduct security audits

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

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

3.1.16 Update password policies

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

Action	Details	Suggested frequency
Update password policies	Identify updated or modified password policy changes to User accounts, roles or permissions and make the changes to your system	Annual

3.1.17 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, a gap in protection can be created, prevented, or closed. 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 your system within the organization	Annual

3.1.18 Update logon banners

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

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

3.1.19 Renew licensing agreements

Assure that your system’s software license supports the necessary functions required for your installation.

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

3.1.20 Renew support contracts

Assure that your software support agreement (SSA) is up to date.

Action	Details	Suggested frequency
Renew support contracts	Collect SSA details	Annual

3.1.21 Check for end-of-life announcements and plan for replacements

Review product announcements to determine if any of the components have a planned end-of-life announcement, including all server operating systems, databases, supervisory controllers, field controllers and devices.

Action	Details	Suggested frequency
Check for end-of-life announcements and plan for replacements	Collect end-of-life details for all your products	Quarterly

3.1.22 Periodically delete sensitive data in accordance with policies or regulations

Action	Details	Suggested frequency
Periodically delete sensitive data in accordance with **policies or regulations**	Collect details on policies and regulations that apply to your location	As required

3.1.23 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 your system continues to operate properly after you have installed any security monitoring tools *(Johnson Controls can only assist within the guidelines set forth within contractual agreements in force)*
- Never install software (or hardware) unless it aligns with the policies of the environment's owner

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

There are many rootkits and malware detection tools available for operating systems, however some place significant load upon the system and may interfere with performance. It is your responsibility to verify that the system continues to operate properly after you have installed any security monitoring tools.

3.2.0 Patch policy

Review your product's patch policy. It will document the current internal operating guidelines and process, which may change from time to time. Ensure your provider employs commercially reasonable efforts to pursue the operating guidelines and process.

A policy will address all types of vulnerabilities such as critical, non-critical, high, medium, and low.
As an example:

> *When **CRITICAL** security vulnerabilities are discovered, your provider should use commercially reasonable efforts to issue a Critical Service Pack for the current version as soon as is reasonably practicable.*
>
> *When **non-CRITICAL** vulnerabilities are discovered, your provider should use commercially reasonable efforts to:*
>
> - *Apply fixes for **HIGH** severity vulnerabilities in the next immediate release*
> - *Apply fixes for **LOW** and **MEDIUM** vulnerabilities within one of the next two available releases*

3.3.0 Release schedule

Review when updates including new features and security fixes are released (i.e., Every x# months).

Review how often will interim updates that include only updates for the operating system will be released.

3.4.0 Recovery and factory reset

If a recovery is necessary, see if your product supports resetting to factory defaults. In some cases, an additional tool is required for this function.