exacqVision Hardening Guide

GPS0037-CE-EN
Version 23.09
Rev B
Revised 2024-04-09

Johnson Controls

Introduction

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

The exacqVision Hardening Guide provides cybersecurity guidance used in planning, deployment, and maintenance periods.

Because cybersecurity threats have become a risk impacting 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. It 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

An appendix is included at the end for acronyms used within this document.

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 as a result of, or despite, reliance on this guide or compliance with any cybersecurity practices or recommendations set forth herein.

Contents

1. Planning

This section helps plan for the implementation of security best practices for an exacqVision system installation.

1.1 exacqVision Overview

Exacq video management solution is a video management system (VMS) that includes video servers, and network video storage servers. exacqVision VMS can be used on factory-installed hybrid, IP, and commercially available servers. Use exacqVision to manage live and recorded video, from small stand-alone systems to large enterprise applications.

Compatible with thousands of IP camera models and dozens of access control, intrusion, and point-of-sale systems, exacqVision's integrations make it one of the most robust end-to-end security solutions in the industry.

exacqVision is offered two ways:

- A bundled hardware and software version
- VMS software only version you can operate on your own hardware or virtualized platform

For additional details and a full catalogue of our offerings visit the Exacq website through the following link - https://exacq.com/catalog/.

1.1.1 Deployment Architecture

Below are two sample architecture drawings of exacqVision. Each installation will vary based upon the components selected for your specific installation. Figure 1.1.1.1 depicts on-premise, cloud and client communications for Windows and Linux, while figure 1.1.1.2 focuses on the camera edge server.

Figure 1.1.1.1 exacqVision Architecture – Windows & Linux Host

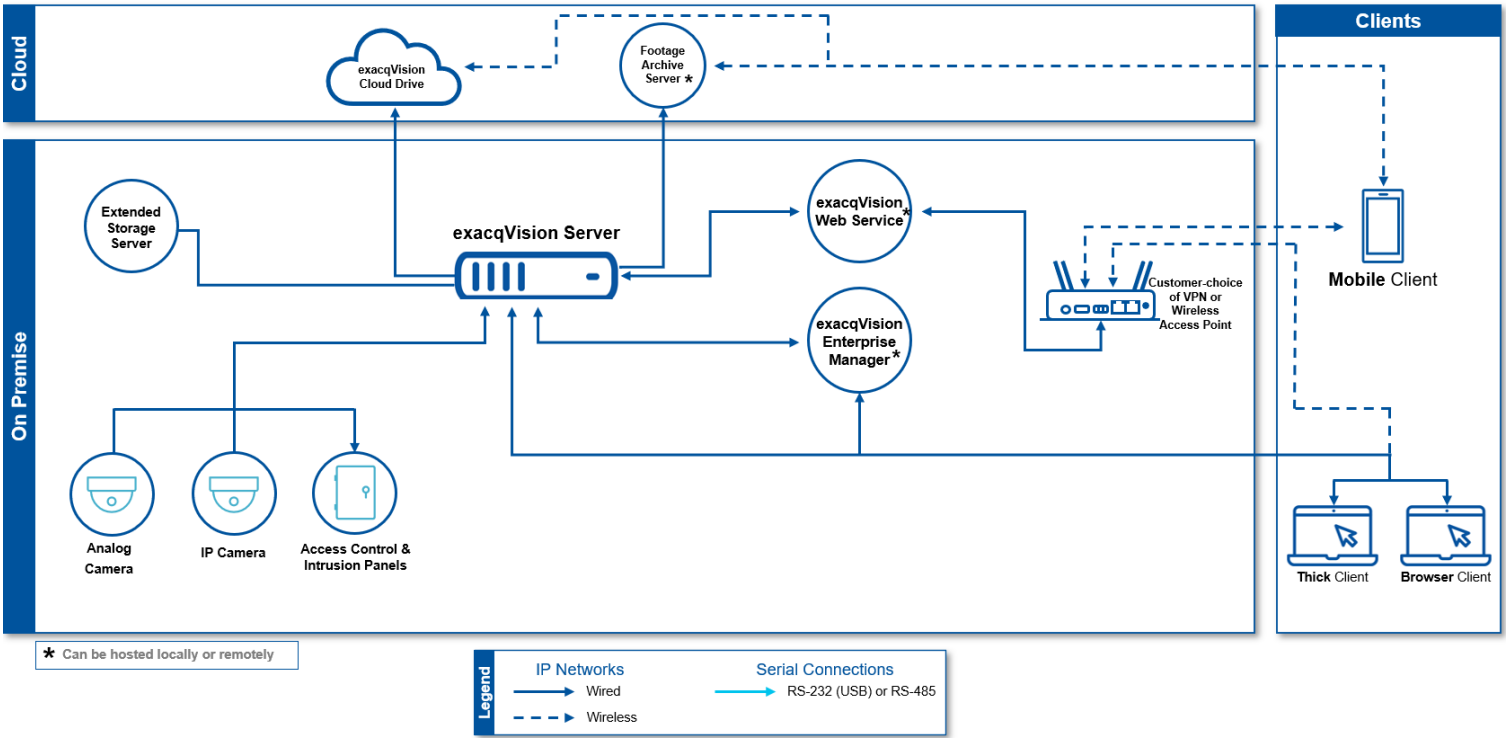
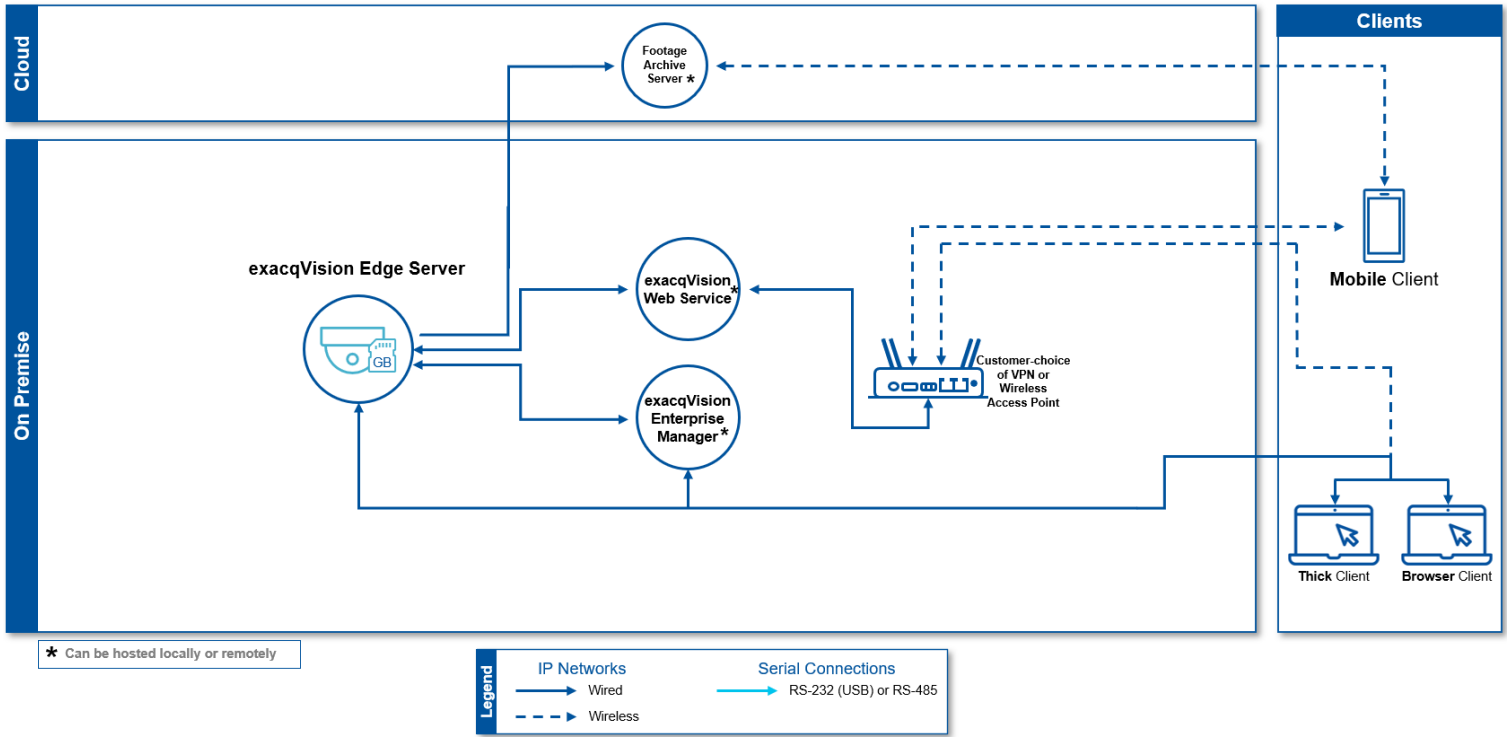


Figure 1.1.1.2 exacqVision Architecture – Camera Edge Server



1.1.2 ExacqVision Components

exacqVision Server and exacqVision client – exacqVision Professional VMS software can run in different environments depending on specific needs.

The exacqVision Professional VMS software can support Windows Linux or Mac operating systems.

	Windows	Linux	Mac
Server	Yes	Yes	No
Client	Yes	Yes	Yes
Web Service	Yes	Yes	No

For additional information, see the following link:
exacqVision Professional Video Management System Software | Exacq from Tyco Security Products

Web Service – This service hosts the exacqVision user interfaces (browser and mobile) and HTTP API.

Web Browser client – The exacqVision user interface, also referred as the Web Client. For additional details on supported Web Browsers see the following link:
exacqVision Professional Video Management System Software | Exacq from Tyco Security Products

Enterprise Manager – An exacqVision component, featuring a web-based dashboard that provides at-a-glance status of the environment's health, extensive scheduling capabilities, and intuitive VMS software.

1.1.3 Supporting Components

Cameras – exacqVision supports both Analog and IP Cameras. An IP camera is a surveillance camera that communicates over the Ethernet using IP addressing. Third party IP Cameras are supported. Illustra IP cameras offer enhanced functionality when coupled with exacqVision VMS. (Refer to Illustra Security Hardening Guide for more details). For a complete listing of supported cameras see the following link:
https://exacq.com/integration/ipcams/

IP Encoder - An IP encoder converts an analog surveillance camera signal to a digital signal and can stream the resulting signal over Ethernet using an IP address.

PoE Camera - An IP enabled surveillance camera that receives its power from the Ethernet cable – Power over Ethernet (PoE).

Network Switch - A exacqVision system can utilize standard off the shelf networking switches that are rated for the communication speeds of the IP video streams.

PoE Switch - PoE Camera may be powered by a standard off the shelf PoE Switch rated for the speed and power requirements of the PoE.

Edge server – A subset of the exacqVision server running on the camera.

Mobile App – The exacqVision mobile user interface which utilizes the Web service.

exacqVision IO Module – USB connected device to provide digital input/output signals.

exacqVision keyboard – USB connected joystick with a keyboard and number pad, which can control the exacqVision client.

Integrations – exacqVision integrates with several third-party solutions such as access controls, intrusion, and video analytics. For a complete list, see this link: https://exacq.com/integration/all/

1.2 Security feature set

This section describes exacqVision's many security features.

Table 1.2.1 – Security features

Section	Type	Feature name	Feature Available
1.2.1	Easy security configuration	Security Dashboard	✓
1.2.2	User Management	Config mode protection for non-OS admin users	✓
		Expiring or locking accounts	✓
		Support for password expiration	✓
		Restrict default account	✓
		Prevent use of common passwords.	✓
		No default admin account on new deployments.	19.12.0
	Session Control	Allow setting session cookie timeout Randomness of session IDs. Validate logins by day, time, and dates	20.12.0 ✓ ✓
1.2.3	User Authentication Safeguards	LDAP/Active Directory support	✓
		User account password policy including lockout and complexity	✓
	Passwords	User Password Support Validation against common passwords Strengthen EM and server passwords Complexity Rules Encrypted stored credentials Encrypted device passwords	✓ ✓ ✓ ✓ ✓ 19.03
		Logout all connections for a user when their password is changed.	✓
		Passphrase support	✓
1.2.4	Audit Log support	Full audit log support	✓
		Audit logging capabilities for EM	22.09.4
1.2.5	Secure Communications	Supports HTTPS configuration for configuring and streaming cameras	✓
		Support for verifiers and salted hash security.	✓
		Client-side option to validate SSL certificates	✓
		TLS version and cipher suites enhanced security	✓
		Support database encryption	19.09.0
1.2.6	Secure Storage	Password protect and encrypt exacqVision proprietary exports.	21.09
		Encrypt device passwords in configuration files	v21.12.8

Note: backup files are always encrypted by exacqVision using 128-bit AES.

1.2.1 Easy security configuration

Security Dashboard – One easy page to configure security settings for exacqVision. This features is set by default upon initial installation with a supporting license.

1.2.2 User Management

Configuration mode – When Configuration mode protection is enabled, configuration changes are restricted to users with the Operating System (OS) Admin Role.

User account password policy – exacqVision contains rules which govern password formation, expiration, reuse, and other restrictions including password length, history, complexity, and includes a blocked password list and expiration.

Inactivity Timeout – exacqVision can set a time frame for how long a user account is active within a session.

Default account – exacqVision default account is restricted and not included on new deployments.

Session Control – exacqVision can set a cookie to control the session timeout. Users can also be authenticated on selected day, time and or dates as desired.

1.2.3 User Authentication Safeguards

Microsoft Active Directory support – enables centralized authentication using a Microsoft Active Directory server for the management of user accounts and logon authentication by LDAP (see LDAP support).

LDAP support – LDAP enables centralized authentication using a Lightweight Directory Access Protocol (LDAP) compliant authentication server for the management of user accounts and logon authentication. Configure invalid attempt lockout policy to prevent the use of a user account when the lockout is engaged to protect against brute force attacks.

Provides support for password complexity requirements.

1.2.4 Audit Log Support

Audit logs – Activity and events from exacqVision are stored in audit log records that administrators can access to view evidence of the activities that have affected the system and indicate the timestamped operation, procedure, or event.

1.2.5 Secure Communications

Cameras – exacqVision supports HTTPS configuration for configuring and streaming cameras.

Salted Hash – exacqVision includes support for verifiers and salted hash security for passwords and configuration files.

Desktop client – Client-side option to validate SSL certificates.

Encryption – Ability to configure TLS version and cipher suites providing enhanced security.

Database security – exacqVision supports database encryption for higher security.

1.2.6 Secure Storage

Encrypted files – exacqVision's proprietary exports can be password protected and encrypted.

Encrypted devices – Device passwords in configuration files are encrypted.

1.3 Intended environment

The exacqVision server is installed on premise within a data center equipment rack with restricted access.

1.3.1 Internet connectivity

Connecting any Operational Technology (OT) system to the internet always increases cybersecurity risk. This product does not require Internet access.

1.3.2 Integration with IT networks

The server components for this system are often deployed on a dedicated and isolated network. VLANs or Tempered Airwall may be used to a share infrastructure but maintain isolation. It is typical for clients to be installed on shared IT networks.

1.3.3 Integration with external systems

Optionally, exacqVision may be integrated with Microsoft Active Directory and/or exacqVision Enterprise Manager.

1.4 Patch Policy

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

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

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

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

Release schedule

- An update to exacqVision including new features and security fixes is released approximately every 3 months.

- No exacqVision update will be released without undergoing extensive quality assurance testing.

1.5 Hardening Methodology

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

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

1.6 Communication

1.6.1 Communication port configuration

In an exacqVision 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.

Table 1.6.1.1

Port/ Range	Protocol	Direction *	Destination (To)	Destination (From)	Process/ Service	Description	Required	Optional	Situational	Notes
25	TCP	O/B	User Defined	server	NotifyPI	SMTP client connection		X		E-mail communication
69	UDP	O/B	Device	server	Arecont discovery	discovery receive port			X	If using Arecont Devices
80	TCP	O/B	Internet	Client	edvrclient	Checking for updates	X	X		Finds updates for Client
80	TCP	O/B	Internet	server	UpdatePI	download server installers	X	X		Allows self-updating but if disabled will not cause issues
80	TCP	O/B	Internet	Web service	wfe	Exacq Version Check Service	X	X		Finds updates for Web Service (Required if using Web Service)
80	TCP	I/B	Web Service	Server	wfe	HTTP (Default port)	X	X		Default Option
80	TCP	O/B	Relay Server	Web Service	frpc	Web Relay Client		X		Remote Connection
85	TCP	O/B	Device	server	Illustra3 plugin	Default metadata port			X	If using Illustra3 Devices with metadata
88	TCP	O/B	AD Server	server	StreamPI	Kerberos client connection		X		Active Directory
123	UDP	O/B	NTP Server	server	StreamPI	NTP client connection		X		Time management
389	TCP	O/B	AD Server	Client	edvrclient	LDAP (Default port)		X		LDAP
389	TCP	O/B	AD Server	server	StreamPI	LDAP client connection		X		LDAP
443	TCP	Bidirectional	Web Service	Client/Browser	EV Server	https		X		If using webservice
443	TCP	I/B	Web Service	Server	wfe	HTTPS (Default port)		X		Recommended Option
445	TCP	O/B	User Defined	server	ArchivePI	SMB archive connection		X		Transport Video Data to archive (should be local)
445	TCP	O/B	Server	Client	edvrclient	SMB to archive targets		X		if using archiving
465	TCP	O/B	User Defined	server	NotifyPI	SMTPS client connection		X		E-mail communication
554	TCP	O/B	Device	server	Camera plugins	To start rtsp media session			X	If using RTSP
587	TCP	O/B	User Defined	server	NotifyPI	SMTPS client connection		X		E-mail communication
636	TCP	O/B	AD Server	Client	edvrclient	LDAPS (Default port)		X		LDAPS
636	TCP	O/B	AD Server	server	StreamPI	LDAPS client connection		X		LDAP
1818	TCP	I/B	Server	Device	PanasonicPI	receive alarm XML from cameras			X	If using Panasonic Devices
1900	UDP	I/B	Server	Device	UPnP discovery	discovery receive port	X			UPnP

2380	UDP	MC	Device	server	Sony discovery	discovery scan/receive ports			X	If using Sony Devices
3000	TCP	O/B	Device	server	illustra3 plugin	default audio out port			X	If using Illustra Devices
3260	TCP	O/B	User Defined	server	ArchivePI	iSCSI storage connection		X		Transport Video Data to archive (should be local)
3702	UDP	MC	Device	server	ws-discovery	discovery scan port			X	Websocket against devices
3702	UDP	MC	Client	server	DiscoveryPI	ws-discovery		X		To view a list of servers for discovery
3702	UDP	MC	Server	Client	edvrclient	ws-discovery		X		Finds instances of server
3702	UDP	I/B	Client	Server	edvrclient	ws-discovery		X		Finds instances of server
4001	WSS	O/B	Device	server	tycodlpi	TycoAI events		X		Video Analytic
4554	UDP	I/B	Device	server	Arecont discovery	discovery send port			X	If using Arecont Devices
5354	UDP	MC	Device	server	mdnsresponder	discovery for mdns**	X	X		If needed for camera discovery
6000	TCP	O/B	Device	server	UDP plugin	default audio out port			X	if using UDP Technology Devices
6005	TCP	O/B	Device	server	Acti plugin	Default control/discovery port		X		For finding Acti Devices on the network
6006	TCP	O/B	Device	server	Acti plugin	Default stream port			X	If using Acti Devices
7070	TCP	O/B	Device	server	Acti plugin	Default rtsp port			X	If using Acti Devices with rtsp
7364	UDP	MC	Device	server	Stardot discovery	discovery scan/receive ports			X	If using Stardot Devices
7701	UDP	MC	Device	server	Samsung discovery	discovery scan port			X	If using Samsung Devices
7711	UDP	MC	Device	server	Samsung discovery	discover receive port			X	If using Samsung Devices
8080	HTTPS	O/B	Device	server	tycodlpi	TycoAI configuration		X		Video Analytic
8181	TCP	listen	Device	server	Panasonic plugin	Default metadata port			X	If using Panasonic Devices with metadata
8554	TCP/ UDP	I/B	server/RTSP server	Client	RTSP server/RTSP server plugin	Default listen port		X		If using RTSP
9766	UDP	MC	Device	server	IOImage discover	discovery			X	If using IOImage Devices
10000	UDP	MC	Device	server	Sanyo discovery	discovery scan/receive ports			X	If using Sanyo Devices
10669	UDP	MC	Device	server	Panasonic discovery	discovery scan port			X	If using Panasonic Devices
10670	UDP	MC	Device	server	Panasonic discovery	discover receive port			X	If using Panasonic Devices
22609	TCP	I/B	Server	Client EM or ISP	StreamPI	inbound client connections	X			
22609	TCP	O/B	Server	Client	edvrclient	Outbound client to server connection (Default port)	X			Main connection from Client to server
22610	TCP	O/B	Server	server	StreamPI	Internal IPC	X			Only over localhost

28774	TCP	I/B	Server	Server	UpdatePI/vfba	failback agent (default port)		X		Fallback
28780	TCP	listen	Device	server	Pelco plugin	Default event arbiter event port			X	If using Pelco Devices
35111	TCP	O/B	ISP	server	EM Importer	Listens for NVR connections			X	Needed if using Integrator Services Portal
43282	UDP	MC	Device	server	IQEye discovery	discovery scan port			X	If using IQEye Devices
43283	UDP	MC	Device	server	IQEye discovery	discovery receive port			X	If using IQEye Devices
52220	UDP	MC	Device	server	Canon discovery	discovery			X	If using Canon Devices
61449	UDP	MC	Device	server	UPnP discovery	discovery scan port.	X			UPnP
user-defined	TCP	O/B	EM	Client	edvrclient	Communication with EM			X	If using EM
user-defined	TCP	O/B	AD Server	Client	edvrclient	LDAP / LDAPS		X		LDAP/LDAPS
user-defined	TCP	O/B	Client	server	StreamPI	outbound client connections	X			
user-defined	TCP	O/B	Server	Client	edvrclient	Outbound client to server connection	X			
user-defined	TCP	O/B	Device	server	BentelPI, BoschsecPI, HoneywellPI, SerialPI, KantechPI	POS and intrusion panel connections			X	

* Direction key: I/B = Inbound, O/B = Outbound, MC = Multicast
** MDNS = Multi-cast DNS

Note: Some devices are deliberately marked as both required and optional. See the notes column to the far right for additional details.

1.6.2 Communications Path Table

Path		exacqVision				Direction / use requirement[1]	Connecting Component			Notes
	Function	Interface	Default Port Assignment	Default Port State	Port Activity (if enabled)		Default Port Assignment	Protocol	Internet access [2]	
A	**Camera communications**					**Required**	**IP/PoE Camera**			
	data and control (non-secure)	HTTP Client	80	*if standard mode*	∞	↳ ▶[5] ◀	80	TCP	-	*select between HTTP or HTTPS [2]*
	data and control (secure)	HTTPS Client	443	Enabled	∞	↳ ▶[5] ◀	443	TCP	-	
	video stream	RTSP Client	554	Enabled	∞	↳ ◀	554	TCP	-	*RTSP or HTTP*
	video stream	HTTP Client	80	Enabled	∞	↳ ◀	80	TCP	-	
	meta data	HTTP Client	85	Enabled	∞	↳ ◀	85	TCP	-	*For certain Illustra cameras*
	alarm meta data	HTTP Client	1818	Enabled	∞	↳ ◀	1818	TCP	-	*For certain Panasonic*
	audio meta data	HTTP Client	3000	Enabled	∞	↳ ◀	3000	TCP	-	*For certain Illustra cameras*
	audio meta data	HTTP Client	6000	Enabled	∞	↳ ◀	6000	TCP	-	*For certain UDP cameras*
	video stream	HTTP Client	6006	Enabled	∞	↳ ◀	6006	TCP	-	*For certain ACTi cameras*
	video stream	HTTP Client	7070	Enabled	∞	↳ ◀	7070	TCP	-	*For certain ACTi cameras*
	meta data	HTTP Client	8181	Enabled	∞	↳ ◀	8181	TCP	-	*For certain Panasonic*
	event meta data	HTTP Client	28780	Enabled	∞	↳ ◀	28780	TCP	-	*For certain Pelco cameras*
B	**camera discovery**					**Commissioning only**	**IP/PoE Camera**			
	UPnP	camera discovery	61449	Enabled	On demand	↳ ◀	1900	UDP	-	Required
	websocket	camera discovery	3702	Enabled	On demand	◀ ↰	3702	UDP	-	Situational
	multicast dns	camera discovery	5354	Enabled	On demand	◀ ↰	5354	UDP	-	Required/Optional
	Arecont	camera discovery	4554	Enabled	On demand	↳ ◀	69	UDP	-	Situational
	Sony	camera discovery	2380	Enabled	On demand	◀ ↰	2380	UDP	-	Situational
	Acti	camera discovery	6005	Enabled	On demand	↳ ◀	6005	TCP	-	Optional
	Stardot	camera discovery	7364	Enabled	On demand	◀ ↰	7364	UDP	-	Situational
	Samsung	camera discovery	7701	Enabled	On demand	◀ ↰	7711	UDP	-	Situational
	ioimage	camera discovery	9766	Enabled	On demand	◀ ↰	9766	UDP	-	Situational
	Sanyo	camera discovery	10000	Enabled	On demand	◀ ↰	10000	UDP	-	Situational
	IQEye	camera discovery	43282	Enabled	On demand	◀ ↰	43283	UDP	-	Situational
	Canon	camera discovery	52220	Enabled	On demand	◀ ↰	52220	UDP	-	Situational
	Panasonic	camera discovery	10669	Enabled	On demand	◀ ↰	10770	UDP	-	Situational

Path		exacqVision				Direction / use requirement[1]	Connecting Component			Notes
	Function	Interface	Default Port Assignment	Default Port State	Port Activity (if enabled)		Default Port Assignment	Protocol	Internet access [2]	
C	**exacqVision server**					**Optional**	**exacqVision Client**			
	e-mail communication	SMTP	25	Enabled	∞	▶ ↵	25	TCP	Optional	
	update PI	exacq.com	80	Enabled	∞	▶ ↵		TCP	Yes	
	data and control	HTTP(S) Server	443	Enabled	∞	▶ ◀↵	Dynamic	TCP	-	
	archive PI	SMB	445	Enabled	∞		445	TCP	-	
	e-mail communication	SMTPS	465	Enabled	∞	▶ ↵	25	TCP	Optional	
	video stream	RTSP Server	554	Enabled	∞	▶ ↵	Dynamic	TCP	-	
	e-mail communication	SMTPS	587	Enabled	∞	▶ ↵	25	TCP	Optional	
	discovery	bonjour	3702	Enabled	∞	▶ ↵	3702	UDP	-	
	archive PI	iSCSI	3260	Enabled	∞	↳ ◀	3260	TCP	-	
	discovery	bonjour	3702	Enabled	∞	↳ ◀	3702	UDP	-	
	RTSP Server PI	RTSP Server	8554	Enabled	∞	▶ ↵	8554	TCP / UDP	Optional	
	data and control	proprietary	Dynamic	Enabled	∞	↵	22609	TCP	-	
	data and control	proprietary	22610	Enabled	∞	↳	-	-	-	
	Video failback	proprietary	28774	Enabled	∞		28774	TCP	Optional	*Partially handled by update PI*
D	**exacqVision Client**					**Required**	**Client**			
	updates	edvrclient	80	Enabled	∞	▶ ↵	80	TCP	Required	
	SMB	edvrclient	445	Enabled	∞	▶ ↵	445	TCP	-	*Optional*
	server connection	streamPI	22609	Enabled	∞	▶ ◀↵	22609	TCP	Optional	
E	**exacqVision Webservice**					**Optional**	**Client or Relay service**			
	exacqVision Web Service	HTTP Server	80	Enabled	∞	▶ ◀↵	80	TCP	Optional	*Mobile app or Web Browser*
	Web Service Relay	frpc service	80	Enabled	∞	▶ ◀↵	80	TCP	Required	*Optional*
	exacqVision Web Service	HTTPS Server	443	Enabled	∞	▶ ◀↵	443	TCP	Optional	*Mobile app or Web Browser*
F	**exacqVision EM**					**Optional**	**Mail Server**			
	exacqVision EM	HTTP Server	80	Enabled	∞	▶ ◀↵	80	TCP	Optional	*Web Browser*
	exacqVision EM	HTTPS Server	443	Enabled	∞	▶ ◀↵	443	TCP	Optional	*Web Browser*
	server connection	streamPI	22609	Enabled	∞	▶ ◀↵	22609	TCP	Optional	

Path		exacqVision				Direction / use requirement[1]	Connecting Component			Notes
	Function	Interface	Default Port Assignment	Default Port State	Port Activity (if enabled)		Default Port Assignment	Protocol	Internet access [2]	
G	**Time sync**					**Optional**	**NTP Server**			
	Time sync	NTP Client	123	Disabled	On demand	↳ ▶ ◀	123	UDP	Optional	StreamPI
H	**Identity Management**					**Optional**	**LDAP Server**			
	LDAP	directory services	389	Disabled	On demand	▶ ↵	389	TCP	Optional	Client / Edvrclient
	LDAP	directory services	389	Disabled	On demand	▶ ↵	389	TCP	Optional	Server / StreamPI
	LDAPS (Secure)	directory services	636	Disabled	On demand	▶ ↵	636	TCP	Optional	Client / Edvrclient
	LDAPS (Secure)	directory services	636	Disabled	On demand	▶ ↵	636	TCP	Optional	Server / StreamPI
	Kerberos	directory services	88	Disabled	On demand	▶ ↵	88	TCP	Optional	Server / StreamPI

[1] Application requirements are represented by the following color codes and symbols:

■	Green = required path
■	Blue = optional path
■	Purple = Commissioning-only path
■	Orange = Service path
↳ or ↵	These arrows indicate that the component can initiate communication in the direction of the arrow
▶ or ◀	These arrows indicate that the component can send data in this direction of the arrow
⊙	This symbol indicates that the component only consumes data from this path.

[2] Any Internet access, if used, should be indirect and managed through a firewall

2. Deploying exacqVision securely

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

2.1 Deployment overview

Security hardening of exacqVision begins prior to deployment with careful planning as outlined in section 1 of this guide. It is a good practice to review that section prior to deployment to fully understand the security feature set of exacqVision, 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 to factory defaults
- Considerations for commissioning
- Recommended knowledge level

2.1.1 Physical installation considerations

Physical installation considerations of components within your exacqVision solution are covered in section 1.3 – Intended Environment.

Keep in mind that both the physical access and physical installation can impact cybersecurity.

To prevent unauthorized access, be sure to place the device in a secured rack or room that can restrict access (for example, mechanical lock or physical access control).

2.1.2 Resetting hardware to the factory default settings

If an exacqVision system was previously used as part of another installation or used in a test environment, it should be reset to factory defaults before being put into service in a new deployment.

2.1.3 Considerations for commissioning

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

2.1.4 Recommended knowledge level

The person confirming that the proper hardening steps are executed should be experienced in exacqVision administration and networking technologies. Completion of the following training courses is recommended:

- Exacq Fundamentals - https://exacq.com/support/training/
- Exacq Enterprise training - https://exacq.com/support/training/

- Exacq MasterTech – https://support.exacq.com/

2.2 Hardening

While exacqVision 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 exacqVision.

2.2.1 Hardening Checklist

- ☐ Hardening step 1a: exacqVision systems
- ☐ Hardening step 1b: Windows systems
- ☐ Hardening step 2: Strengthen server passwords
- ☐ Hardening step 3: Enable TLS
- ☐ Hardening step 4: Enforcement of SMB Protocol
- ☐ Hardening step 5: Run exacqVision Web Service locally
- ☐ Hardening step 6: Optional – Advanced hardening / Add Proxy Server
- ☐ Hardening step 7: Backup and Restore of the System
- ☐ Hardening step 8: Failover Groups feature
- ☐ Hardening step 9: Factory reset
- ☐ Hardening step 10: Enable HTTPS (If using Enterprise Manager)

2.3.0 Server – desktop platforms

Harden the exacqVision Server and desktop platforms including supported Windows, and Ubuntu versions. Note: the exacqVision Server can run on both vendor hardware or customer owned platforms (hardware and virtual). For the latest updates on which platform is supported, see the exacqVision website – https://exacq.com/products/enterprise/.

System Configuration	Hardening Step	Description
Ubuntu	Step 1a	Hardening exacqVision systems (such as Network Video Recorder (NVR) or other hardware) version 9.8 or earlier running Linux.
Windows	Step 1b	Hardening exacqVision systems running Windows

Note: Hardening steps 1a and 1b are designed for two different system configuration options. You should only need to perform step 1a or 1b, depending on your system configuration, but not both.

2.3.1 Hardening exacqVision systems (such as an NVR or other hardware) running Linux.

To maintain all software functionality while de-elevated, upgrade to exacqVision Server version 19.03 or later. To harden, complete the following steps:

1. If you are utilizing the archive features, perform steps ‘a’ through ‘c’, otherwise move to step 2
    a. If / when using CloudDrive for archiving: To recreate the cloud archive target, you must have your credentials for your Exacq cloud drive account.
    b. Delete existing archive targets.
    c. Create new archive targets. If you do not complete these steps, archive targets will not connect after transitioning to de-elevation or inversely.
2. Open the terminal.
3. In the terminal, type the following command: `sudo dpkg-reconfigure -p low edvrserver`
4. To de-elevate, select **Yes**.
5. To re-elevate, select **No**. The service automatically restarts.
6. To verify that the **core** and **exacqd** processes, are both running as the **edvrserver** user instead of the **root** user, in the terminal type the following command: `ps agux| grep exacq`
   Note: Confirm the leftmost entry shows as “edvrserver” as shown in figure 2.3.1.1 and not “root” as shown in figure 2.3.1.2

figure 2.3.1.1 – edvrserver

figure 2.3.1.2 – root

Note: The NVR can still record and search, and a local client running as non-administrative OS user is able to search, because permissions have been set properly.

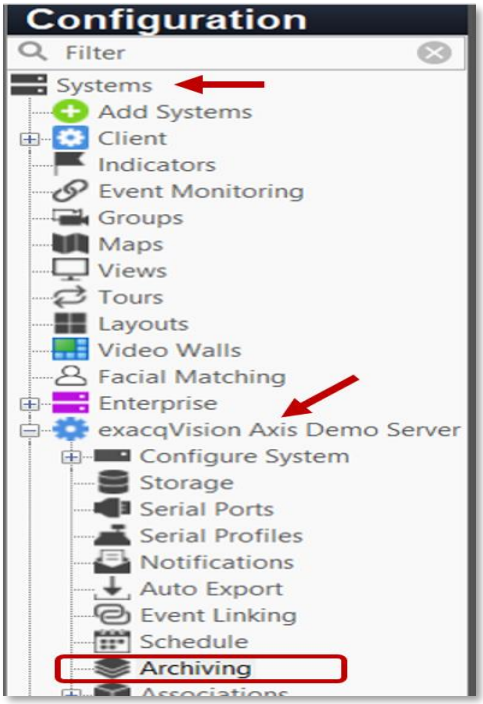
Note: For additional information on Cloud Drive, see the following link - https://www.exacq.com/products/cloud-drive/

Result: Now you can create new Server Message Block (SMB), Network File System (NFS), and cloud archive target.

Hardening a Windows system

You can continue to use existing SMB or NFS archive targets after you transition to de-elevation or inversely. This is due to fundamental differences between the Windows security model and the Linux security model. However, this is not true for cloud archiving targets.

To harden a Windows system, navigate to **Configuration**, expand **exacqVision server**, then open **Archiving.** Now complete the following steps:



1. Delete existing archive targets
2. Create new archive targets
3. In the Windows toolbar right-click **Command Prompt** and click **Run as administrator**
4. In the command prompt window, type the following command: `icacls d:\ /grant "Network Service:f" /t`
5. In the command prompt window, type the following command: `icacls d:\ /grant "Users:rx" /t`
6. Stop the service.
    a. To stop the service, click the Windows **Start** menu and type *Service*
    b. Click the Services desktop application icon
    c. In the Service list right-click **exacqVision Server** and click **Restart**
7. Modify the `PluginList.ini` file
    a. Open Notepad.exe (or another editor) and **Run as administrator**
    b. Open C:\Program Files\exacqVision\Server\PluginList.ini
    c. Add the following line: `deelevate=true` to the end of the file
8. Start the service
9. Press CTRL+ALT+DELETE and click **Task Manager**.
10. Confirm that the following processes are both running as network service user and not SYSTEM user: **core** and **exacqd**

Note: The NVR can still record and search because you have manually granted permission for the Network Service user to be able to read, write, and delete files on all relevant local recording drives. Local clients running as non-administrative OS users can search because you have manually granted read and execute permissions for all valid OS users to all relevant local recording drives.

Note: For additional information relating to archive targets, see the exacqVision User Manual at the following link: [Homepage • Exacq Knowledge Exchange (johnsoncontrols.com)]

Result: You can create new SMB, NFS, and cloud archive targets.

2.3.2 Enabling Password Strengthening and Augmented Authentication

Introduced in exacqVision Server version 9.0, this feature enables a more secure communication protocol between the client and server, meaning the server can enforce stricter authentication controls.

After an upgrade to version 9.0 or higher, machines running earlier versions of exacqVision client are no longer compatible with the server. This is desirable because client versions 9.0 or higher forces users to set strong passwords.

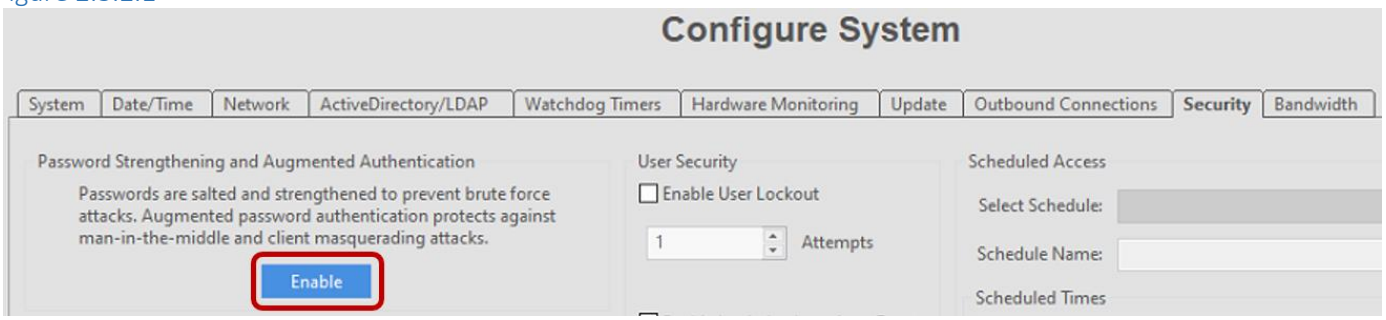
When the feature **Password Strengthening and Augmented Authentication** is enabled, the system will no longer store actual passwords. It will now use a strong algorithm to generate a secure identifier that combines a salt and hash with the Argon2 key extension algorithm and additional encryption. This secure identifier is stored. If you enable the secure identifier, passwords that are salted and hashed cannot be converted into cleartext. The use of a key extension algorithm strengthens security against dictionary or brute-force attacks.

Hardening step 2: Strengthen server passwords

Use the Security tab to enable this feature in client and server versions 9.0 or higher.

Note: Once enabled, Password Strengthening and Augmented Authentication is not reversible.

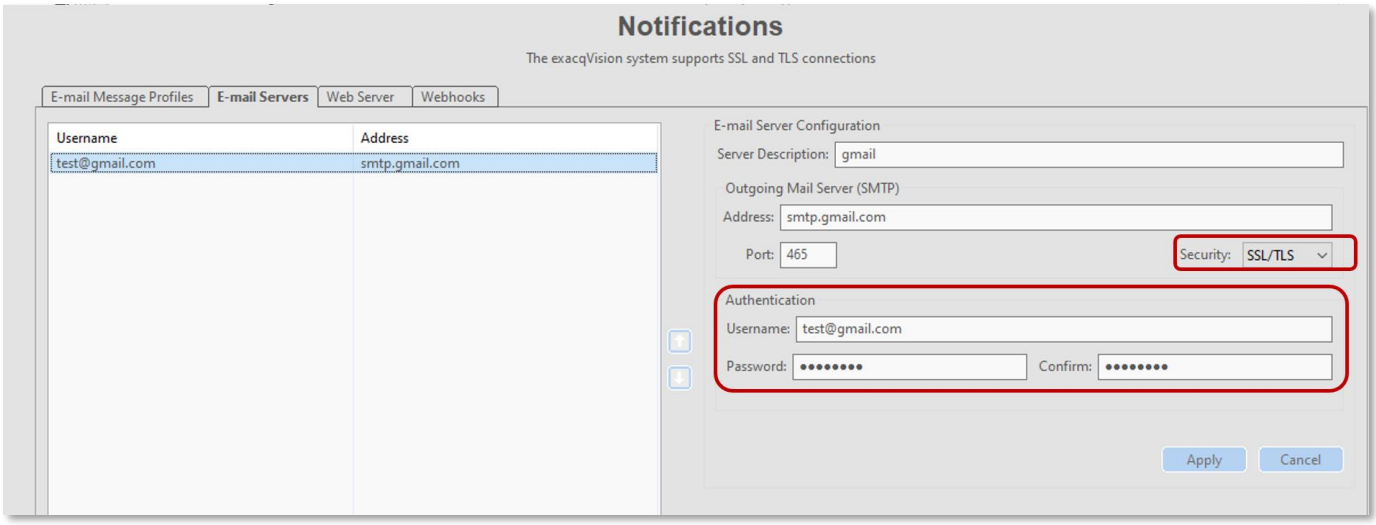
Figure 2.3.2.1



2.3.3 Discontinue using external systems that do not require authentication

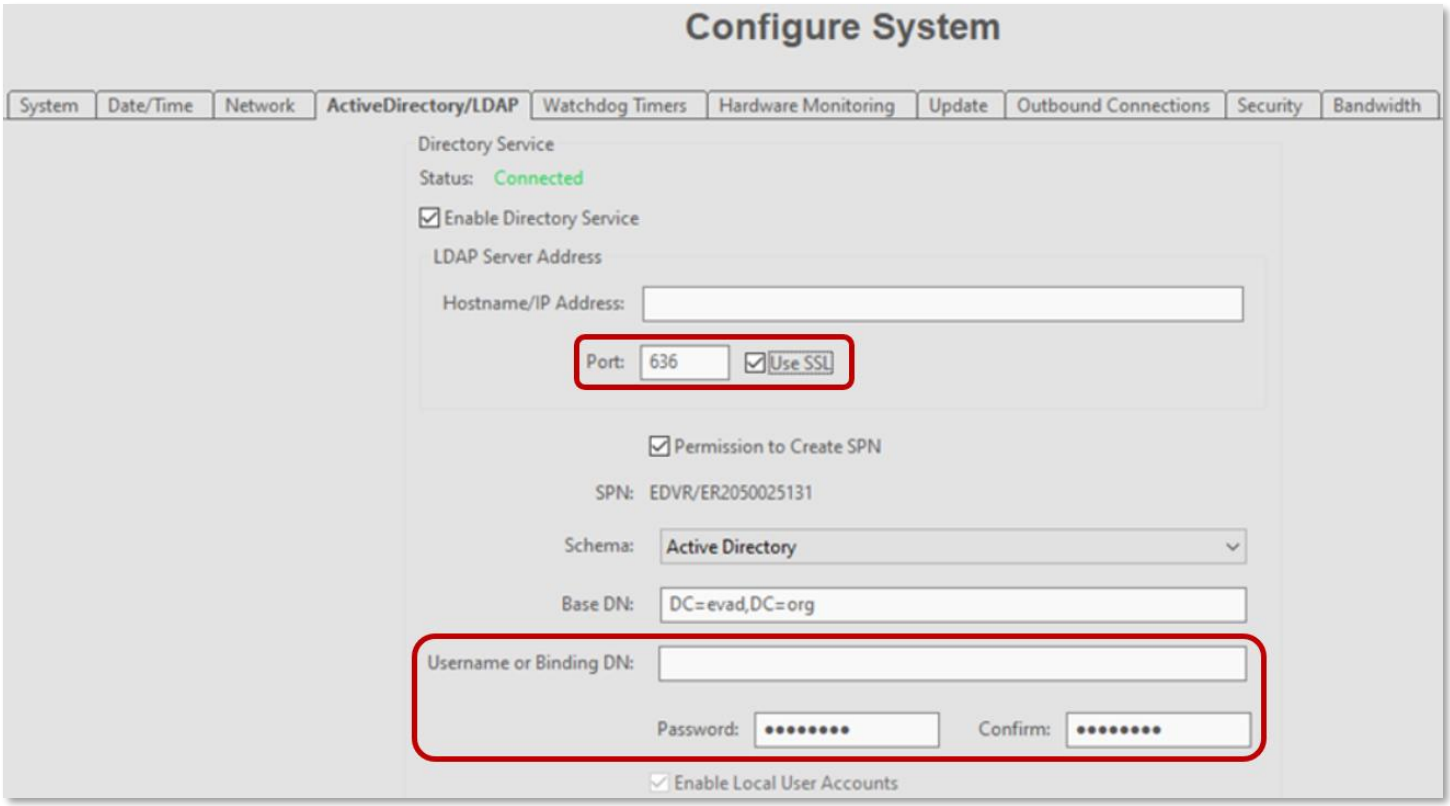
When using the **E-mail Servers** tab, use only an SMTPS server requiring password authentication and SSL.

Figure 2.3.3.1



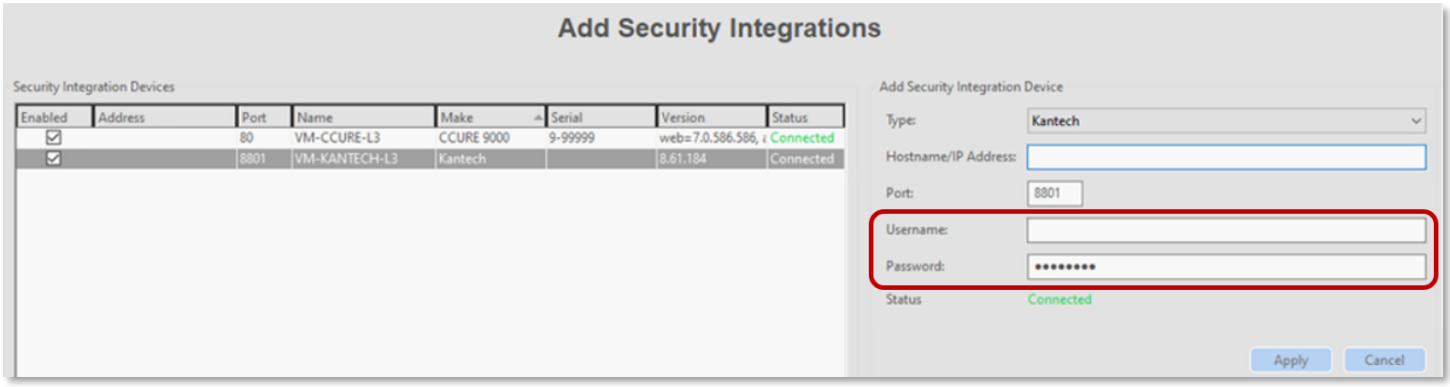
When using the **Active Directory/LDAP** integration feature, use only an LDAP server requiring SSL.

Figure 2.3.3.2



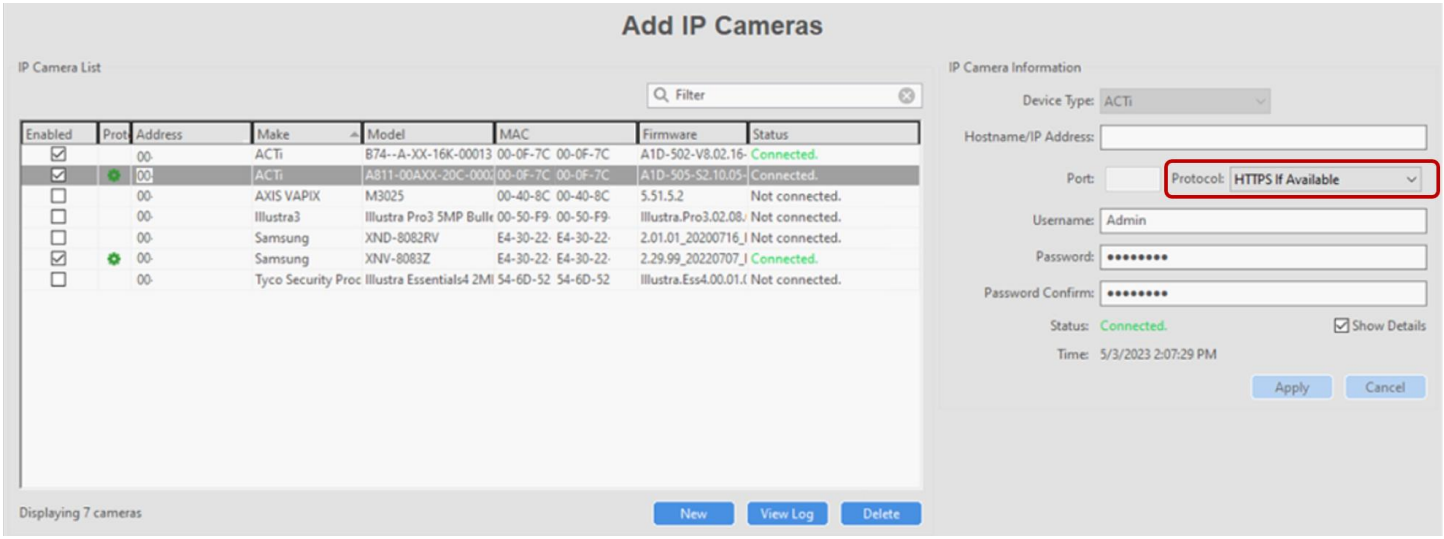
When connecting an intrusion panel or an access control system, ensure these systems require password authentication or a type of secret key mechanism on the **Add Security Integrations** tab.

Figure 2.3.3.3



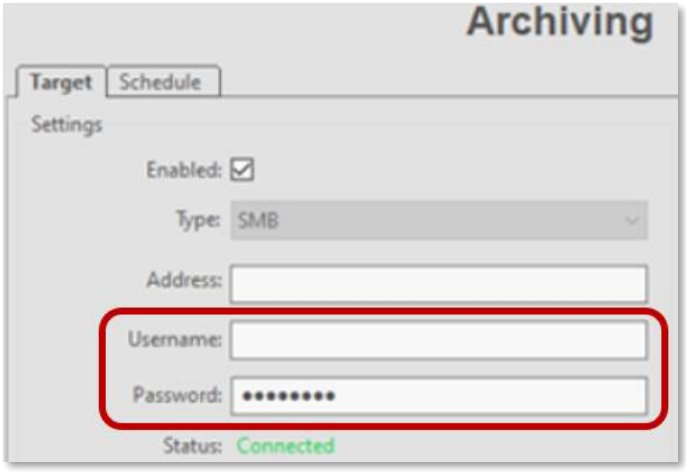
When connecting IP cameras or encoders on the **Add IP Cameras** tab, ensure all connected devices require password authentication and SSL.

Figure 2.3.3.4



When using the **Archiving** feature, only connect to SMB targets that require password authentication.

Figure 2.3.3.5



2.4 Hardening exacqVision Web Service

This section describes how to harden exacqVision Web Service on desktop platforms.

2.4.1 Enable TLS (HTTPS):

TLS connections require a user-specific certificate which must be manually configured to be enabled. Use TLS in all web communication because it actively prevents reading and manipulation of communication between the client and the web service. TLS connections are provided in the Web Service through two mechanisms:

- **Let's Encrypt/ACME**: A free service to provide TLS certificates with minor restrictions. The web service must be internet accessible with port 80 open, and a domain name must be associated with the web service.

- **External (Recommended)**: User-supplied certificates for TLS. Purchase certificates from a certificate authority, such as VeriSign, DigiCert, or Network Solutions. Alternatively, a Certificate can be issued by your organization's Active Directory Certification Authority.

Hardening step 3: Enable TLS

From the web service and end-user perspectives, there is no functional difference between the two types of configuration. To configure TLS in the web service, complete the following steps:

1. On the web service landing page, click the **Web Service Configuration** link. If this link is not displayed, the **Restrict to localhost** setting is enabled. To disable this setting access the web service directly from the machine.
2. From the navigation menu click **Configuration** and then click **HTTPS**.
3. Click **Configure**.
4. From the drop down select an encryption type, **Let's Encrypt** or **External**.
5. Enter the information and click **Apply**.
6. Restart the web service when prompted. The web service is now reachable using HTTPS.

2.4.2 SMB Protocol

ExacqVision's default method for archiving recorded data uses the SMB protocol. Using an ExacqVision S-Series storage system makes configuring archiving simple. Users may also archive to SMB shares configured on their own third-party systems, but installing and configuring Samba or SMB Shares on non-Exacq built systems is outside the scope of Exacq Support.

There have been several iterations of SMB since the protocol was first introduced. Devices wishing to communicate via SMB must first perform a negotiation to determine which version they will use. The version and dialect of SMB chosen will determine what features are used.

Version. How to check the version of Samba installed on your S-series or other Linux system:

1. Open a Terminal window, by pressing **CTRL+ALT+T**
2. Type `samba --version`, and press Enter.

Hardening step 4: Enforcement of SMB Protocol

To manually configure SMB:

1. On the S-Series server, open a Terminal window by pressing **CTRL+ALT+T**
2. Use sudo permissions to edit /etc/samba/smb.conf
3. Locate the [global] settings section.
4. Beneath the [global] tag, add the following lines:
   server signing = mandatory
   server min protocol = SMB3_11
   server max protocol = SMB3_11
5. Save your changes, then exit the file.
6. Restart Samba by entering
   sudo /etc/init.d/samba restart

The entries given for Step 4 above enforce server signing as well as SMB dialect 3.1.1. Attempts to connect with anything else would fail. A list of possible options for these three entries is given below.

server signing = [default, auto, mandatory, disabled]

server min protocol = [SMB2, SMB2_02, SMB2_10, SMB3, SMB3_00, SMB3_02, SMB3_11]

server max protocol = [SMB2, SMB2_02, SMB2_10, SMB3, SMB3_00, SMB3_02, SMB3_11]

Note: 'server min protocol' should be the same or lower than 'server max protocol'. If these are different values the client and server must support a dialect in between these values. If these are the same value, they must support that specific dialect.

Note: Without editing the configuration at all, the default behavior when these fields are excluded from the smb.conf file are the same as entering the following:
server signing = auto
server min protocol = SMB2_02
server max protocol = SMB3

For additional details on SMB, see the following link - https://support.exacq.com/#/knowledge-base/article/1306

2.4.3 Modify system settings (Windows only)

If your exacqVision instance has the Web Service enabled, perform the following step to harden the Web Service.

Hardening step 5: Run exacqVision Web Service locally

To modify system settings, you must reconfigure the exacqVision Web Service to run as **Local Service**. The Web Service always installs as **Local System**, which grants unlimited OS administrative privileges to the software. This may be a security risk if the OS itself becomes compromised. The Local Service account is more secure for a long-running Windows Service that accepts incoming network connections. To modify system settings, complete the following steps:

1. Stop the exacqVision Web Service and exacqVision Web Server services.
    a. To stop the service, click the Windows **Start** menu and type *`Service`*.
    b. Click the Services desktop application icon.
    c. In the Service list right-click **exacqVision Web Service** and click **Stop**.
2. Right-click on each service and select **Properties**.
3. Navigate to the **Log On** tab, select **This Account** and enter *`Local Service`*.
4. Clear both password controls.
5. Click **Apply**.
6. In the **Services Control** panel, confirm that the service is now running as **Local Service**.
7. Start the services.
8. Press CTRL+ALT+DELETE and click **Task Manager**.
9. Confirm that the following processes are both running as **Local Service** : **evws** processes and a **wfe** process.

2.4.4 Unavailable functionality after hardening

The following functions become unavailable when you apply certain hardening steps:

- Updates (Windows): If you attempt to update the web service through the service configuration the following message appears: **An error occurred while installing the update.** You must manually update the web service.
- Restarting (Windows): If you attempt to restart the web service through the service configuration, the following message appears: **There was an error during restart.** Use the Windows Services utility or Start menu shortcuts to manually restart the web service utility.

Hardening step 6: Optional – Advanced hardening / Add Proxy Server

If your Web Server installation requires any additional security beyond the built-in options, we recommend that you run a Proxy Pass Server.

For information on how to configure Nginx or Apache as a Web Service Gateway, see the following link: https://support.exacq.com/#/knowledge-base/article/963

2.5 Server - configuration backups

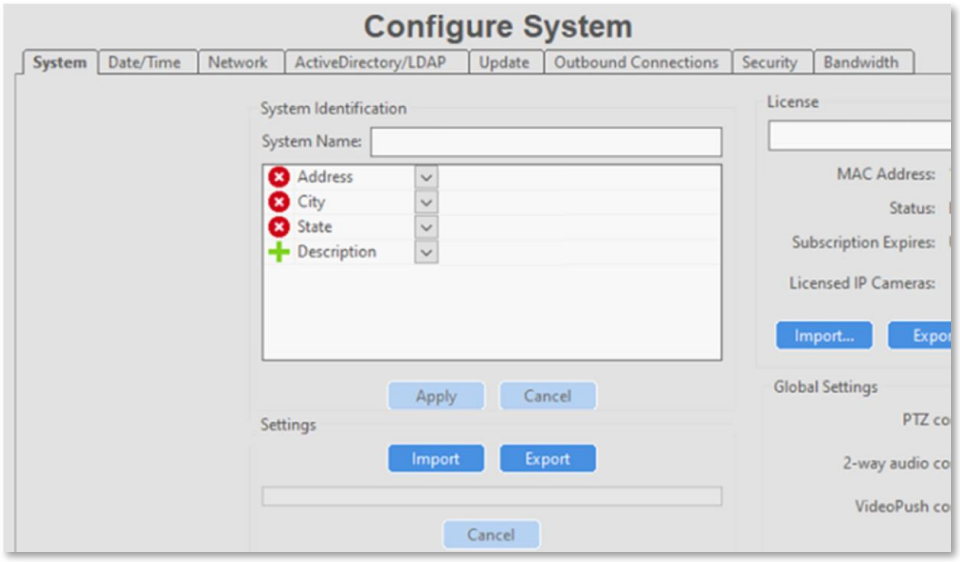
Making frequent backups of the ExacqVision configuration during the commissioning phase can be beneficial if an error is made or lost due to a hardware failure. Once the system is made operational, being able to restore from a good backup minimizes the downtime of the system.

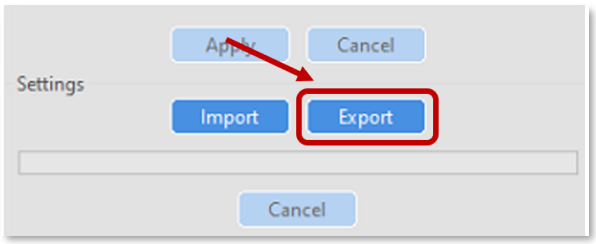
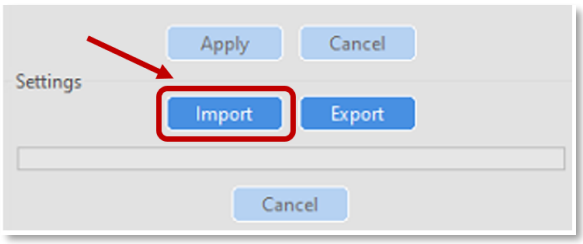
ExacqVision has a built-in utility to backup and restore the NVR server configuration data. In the event of a system failure, the NVR may be restored to the saved configuration.

Hardening step 7: Backup and Restore of the System

Navigate to the **System** tab on the **Configure System** page as shown in figure 2.5.1

Figure 2.5.1



Performing a Backup	*Performing a Restore*
• To access the built-in ExacqVision Backup utility click the **Export** button	• To access the built-in ExacqVision Restore utility click the **Import** button.
	

For additional details on Backup and Restore, see the following link:
https://support.exacq.com/#/knowledge-base/article/2795

Best practices for backup storage

Copies of 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.
Note: backup files are always encrypted by exacqVision.

Video data

Video data, which is not backed up through the built-in utility, should be backed up using archiving (refer to ExacqVision Installation and User Manual).

RAID storage

While there is no hardening step associated with RAID storage, we encourage you to review details how to configure RAID Drives, manage RAID drives, and other storage options that may harden your installation. (Refer to Storage section of ExacqVision Installation and User Manual).

2.5.1 Failover Groups

If you are using Enterprise Manager, then we recommend utilizing the **Failover Groups** feature. Configure failover groups to ensure that recorded video information is available in the event of a hardware failure. Failover groups consist of associated protected servers and spare servers.

Hardening step 8: Failover Groups feature

For additional details, see the exacqVision Enterprise Manager User Manual:
https://docs.johnsoncontrols.com/exacq/r/Exacq/en-US/exacqVision-Enterprise-Manager-User-Manual/23.06/Failover-groups

Hardening step 9: Factory reset (Optional for decommissioning or recommissioning)

Operating system Configuration

ExacqVision systems include a special partition to allow for quick and easy system restoration to factory default conditions. This recovery will only affect your operating system drive.
Note: If this process is followed using the previously exported NVR Configuration data (hardening step 6), your video data will not be impacted. (See section 2.5.0 – Backup and Restore)

For this step, it is recommended that you contact your system integrator.

2.6.0 Enterprise Manager

This section has information on how to harden exacqVision Enterprise Manager on desktop platforms including Windows 7 or later, Windows Server 2008 or later, and Ubuntu 12.04 or later.

Hardening step 10: Enable HTTPS (Enterprise Manager)

When using exacqVision Enterprise Manager, it is recommended to enable HTTPS. In Section 1, you learned about the specific details and planned for this installation.

For a trusted certificate, it is recommended that you purchase a third-party intermediate certificate from one of many online providers.

It is also possible to use a self-signed certificate. If you are using a self-signed certificate or one from a private/internal certificate authority, be aware that web browsers may warn users that the certificate is untrusted.

For additional details and steps to incorporate a certificate, see this link:
https://support.exacq.com/#/knowledge-base/article/12804

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 that exacqVision is serving 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.

Item	Description	Immediate	Base on Priority	Daily	Weekly	Monthly	Quarterly	Annual
1	*Validate backups are running*					✓		
2	*Assure failover solutions are operating*						✓	
3	*Lock user accounts of terminated employees*	✓						
4	*Remove inactive user accounts*					✓		
5	*Update user account roles*						✓	
6	*Disable unused ports*						✓	
7	*Check for and prioritize advisories*				✓			
8	*Plan and execute advisory recommendations*		✓					
9	*Check and prioritize software patches and updates*					✓		
10	*Plan and execute software patches and updates*		✓					
11	*Review updates to organizational policies*							✓
12	*Review updates to regulations*							✓
13	*Update as built documentation*	✓						✓
14	*Conduct security audits*							✓
15	*Update password policies*							✓
16	*Update standard operating procedures*							✓
17	*Renew licensing agreements*							✓
18	*Check for end-of-life announcements and plan for replacements*						✓	
19	*Periodically delete sensitive data in accordance with policies or regulations*		✓					
20	*Monitor for cyber attacks*			✓				

3.1.1 Validate backups are running

Configuration data, and **Failover Groups** were setup in section 2.5 and are important if an error is made or data is lost due to a hardware failure. Confirm that the backup steps in section 2.5 are being executed.

Table 3.1.1.1

Action	Details	Suggested frequency
Configuration backups	See section 2.5.0	Monthly

3.1.2 Assure failover solutions are operating

Backup solutions that provide continuity of operations through a hardware failure, such as redundant server failover and RAID, should be inspected to assure that they are operating properly.

Table 3.1.2.1

Action	Details	Suggested frequency
Failover Groups	See section 2.5.1 and validate that you are using the **Failover Groups** feature	Quarterly
RAID storage	See Section 2.5.0 RAID storage	Quarterly

3.1.3 Lock accounts on termination of employment

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

Table 3.1.3.1

Action	Details	Suggested frequency
Disable (Lock) accounts	See the User manual for this specific procedure	Immediate

3.1.4 Remove inactive user accounts

While an employee may still be employed by an organization in which the system is owned, managed, serviced, or used by, they may not have utilized it for a long period. This suggests that independent of being authorized to use the system, they do not have a need to use the system and you should remove 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.

One final note: exacqVision is less of a traditional Information Technology (IT) system and more of an Operational Technology (OT) system. This means that it may be acceptable for employees, contractors, and/or service technicians to not sign into this system as often as they would traditional business systems such as email. OT Systems are designed to be used on an as-needed basis, meaning access may be sporadic. Use discretion when defining “inactive accounts”.

Table 3.1.4.1

Action	Details	Suggested frequency
Remove inactive accounts	See the User manual for this specific procedure	Monthly

3.1.5 Update user account roles

While an employee may still be employed by an organization in which the system is owned, managed, serviced, or used by, they may have changed roles or have increased or decreased their need to utilize the system. 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 exacqVision roles and permissions no longer required or utilized in their new role.

Table 3.1.5.1

Action	Details	Suggested frequency
Update user account roles	See the User manual for this specific procedure	Quarterly

3.1.6 Disable unused ports

Reassess the need for ports that are not required and disable them. For example, if software was reinstalled or new features were added, ensure that any ports originally disabled remain disabled. This practice will lower the attack surface of exacqVision resulting in a higher level of protection.

Table 3.1.6.1

Action	Details	Suggested frequency
Disabled unused features	See section 1.6.1 for Communication ports	Quarterly

3.1.7 Check for and prioritize advisories

You can find security advisories for exacqVision on the Cyber Protection website Link - https://support.exacq.com/#/home. Access is provided once you have registered a user account with that site. User account registration is open to JCI customers and authorized representatives. Determine if exacqVision is impacted by the conditions outlined in the advisories. Based on how the exacqVision system is deployed, configured, and used, the advisory may or may not be of concern. Referring to as-built documentation of the exacqVision system will help with this assessment. A good set of as-built documentation will help you identify the number of components impacted and where they are located. 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.

Table 3.1.7.1

Action	Details	Suggested frequency

Check for and prioritize advisories	Refer to https://www.johnsoncontrols.com/cyber-solutions/security-advisories	Weekly

3.1.8 Plan and execute advisory recommendations

Follow the plan determined in maintenance step 9. Consult with all parties who may be impacted by an advisory or downtime and choose the best time for deployment.

Table 3.1.8.1

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

3.1.9 Check and prioritize patches and updates

While an exacqVision 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 cameras, networking equipment and operating systems by consulting with the respective vendor.

Note: exacqVision software has a built-in feature which will automatically check for updates to the server software. Review your software regularly to be notified of specific updates.

Table 3.1.9.1

Action	Details	Suggested frequency
Check for and prioritize advisories	Refer to the exacqVision downloads page https://exacq.com/support/downloads.php or the exacqVision **Update** tab	Monthly

3.1.10 Plan and execute software patches and updates

Follow the plan determined in maintenance step 9. Consult with all parties who may be impacted by patches, updates or downtime and choose the best time for deployment.

Table 3.1.10.1

Action	Details	Suggested frequency
Plan and execute software patches and updates	Plan and execute advisory recommendations	Base on priority

3.1.11 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.

Table 3.1.11.1

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

3.1.12 Review updates to regulations

If exacqVision 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.

Table 3.1.12.1

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

3.1.13 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 in 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.

Table 3.1.13.1

Action	Details	Suggested frequency
Update as-built documentation	Update as-built documentation of your system as needed	As changes are made or annual

3.1.14 Conduct security audits

Periodic security audits are necessary as cybersecurity guidance, organizational policies, regulations, auditing processes, system use, 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 or configuration. Consult with your IT department for guidance toward security audits.

Table 3.1.14.1

Action	Details	Suggested frequency
Security audits	Conduct yearly security audits	Annual

3.1.15 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.

Table 3.1.15.1

Action	Details	Suggested frequency
Update password policies	Review exacqVision system level user accounts (interactive) and roles	Annual

3.1.16 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.

Table 3.1.16.1

Action	Details	Suggested frequency
Update standard operating procedures	Collect standard operating procedures for use of exacqVision within the organization	Annual

3.1.17 Renew licensing agreements

Assure that your exacqVision software license supports the necessary functions.
Note: A software license is necessary to receive the most current updates to the exacqVision Server software.

Table 3.1.17.1

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

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

Review product announcements to determine if any of the components of exacqVision have a planned end-of-life announcement, including cameras.

Table 3.1.18.1

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

3.1.19 Periodically delete sensitive data in accordance with policies or regulations.

Check with your local exacqVision representative or integrator if you have any questions about sensitive data.

Table 3.1.19.1

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

3.1.20 Monitor for cyber attacks

Monitoring site perimeters, networks and endpoints for cyber-attacks is a part of good cybersecurity operation.

Table 3.1.20.1

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

3.2 Recovery and resetting to factory defaults

If a recovery is necessary, see section 2.1.2 Resetting to factory defaults

3.3 exacqVision testing process

As part of the requirements of the Product Security Program, exacqVision receives regular vulnerability and penetration testing from both our internal product security engineers. exacqVision is also subjected to both internal engineering team and third-party penetration testing annually and for major releases.

Vulnerability assessment

Vulnerabilities discovered in exacqVision proprietary software are assessed on the CVSS v3 score.

CVSS v3 Score, Assessment

≥ 9, Critical

≥ 7, High0

< 7, Medium

Vulnerability assessment – third party components

Vulnerabilities discovered in exacqVision proprietary software are assessed on the CVSS v3 score.

CVSS v3 Score	Assessment
≥ 9	Critical

≥ 7	High
< 7	Medium

Vulnerability assessment – third party software

exacqVision must use commercially reasonable efforts to monitor third party and open-source software included within the exacqVision ecosystem for disclosed vulnerabilities from the product vendors and open-source communities. Vulnerabilities that are discovered and disclosed will be assessed first on its assigned CVSS v3 score from the product vendor or the National Vulnerability Database and then on the ability to be exploited within exacqVision.

CVSS v3 Score	Exploitability	Assessment
≥ 9	Exploitable	Critical
≥ 9	Not Exploitable	High
≥ 7	Exploitable	High
≥ 7	Not Exploitable	Medium
< 7	Exploitable	Medium
< 7	Not Exploitable	Low

If a patch is not available to correct the vulnerability, Johnson Controls will use commercially reasonable efforts to mitigate the vulnerability within its capabilities.

exacqVision vulnerability reporting

To better protect our customers and honor the trust they put in us, we are firm believers in responsible coordinated disclosure. Security Researchers, consultants and others who believe they may have found a potential security vulnerability in a Security Product can make immediate notice to our Cyber Protection Team through email to **productsecurity@jci.com** or by the **Building Products Vulnerability Reporting** webpage at https://www.johnsoncontrols.com/cyber-solutions/security-advisories to make immediate notice to our Product Security Incident Response Team (PSIRT).

Those working directly on behalf of a Security Products customer should also notify their local Security Products representative. Thank you for your partnership with us in creating a smarter, safer more sustainable world.

Appendix A – Acronyms

Acronym	Description
AD	Active Directory
EM	Enterprise Manager
HTTP / HTTPS	Hypertext Transfer Protocol / Secure
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
LSA	LSA Server
LSI	LSI Storage
MS DS	Microsoft Directory Services
NFS	Network File System
NIC	Network Interface Card
NVR	Network Video System
PoE	Power over Ethernet
OS	Operating System
OT	Operational Technology
PSIRT	Product Security Incident Response Team
RBAC	Role Based Access Control
SMB	Server Message Block
SMTP	Simple Messaging Transfer Protocol
SSL	Secure Socket Layer
TLS	Transport Layer Security
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VMS	Video Management System