smt tyco | Software House

C•CURE 9000 Hardening Guide

GPS0029-CE-EN
Version 3.00.3
Rev B
Revised 2024-07-16

Johnson Controls

Introduction

C•CURE 9000 provides peace of mind to our customers with a holistic cyber mind-set beginning at initial design concept, continuing through product development, and is supported through deployment, including a rapid incident response to meet the comprehensive and evolving cybersecurity environments.

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

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

This guide provides hardening guidance for configuration and maintenance, including the operating system, user accounts, permissions and roles, backup and restore, redundancy, and patch management.

This Johnson Controls C•CURE 9000 **Hardening guide** is broken down into three main sections depicting the overall process for hardening:

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

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 a C•CURE 9000 system installation.

1.1 C•CURE 9000 overview

Software House C•CURE 9000 is one of the industry's most powerful and flexible security management systems. Version 3.0 can perform the following actions directly from the PC with the full C•CURE client, the web client or on the move with C•CURE Go mobile application:

- Monitor events
- Manage personnel
- Create reports
- Display dynamic views
- Monitor system activity
- View video
- Manage visitors anywhere in the world

C•CURE 9000 provides the ultimate in scalability from a single standalone server supporting up to 5,000 readers and 1,000,000 credentials to an advanced distributed enterprise architecture that supports a master server with up to 60 satellite application servers. Whether an organization consists of one facility with a few doors or many that span the globe, this solution scales as a company grows. C•CURE 9000 brings over 150 integrated solutions including video, intrusion, intercom, fire alarm management, and Physical Security Information Management (PSIM). The integrations are thoroughly tested and delivered through the intuitive C•CURE 9000 interface.

C•CURE 9000 Enterprise architecture is a licensable option that allows the user to configure multiple C•CURE 9000 servers to communicate with a Master Application Server (MAS). The MAS provides a platform for global management of personnel, video, and access security objects on two or more Satellite Application Servers (SAS). This architecture provides the capability for central monitoring and reporting for the entire enterprise. Global data such as personnel records, clearances, and operators is located on the MAS and is synchronized to each SAS. The MAS does not have direct connection to controllers or video servers but can be used to remotely monitor and manage devices connected to a SAS within the enterprise. A C•CURE 9000 installation connected to the MAS can view events, activities, and the status on every SAS in the enterprise, while local installations can connect to a SAS will have visibility only to devices connected to that server.

SQL Option

Offered as an option, C•CURE 9000 version 3.0 and later supports SQL database hosted by Amazon Relational Database Services (RDS)™powered by Amazon Web Services (AWS)™.

1.1.1 Deployment architecture – Examples of a Standalone or Enterprise system

Figure 1.1.1.1: Standalone System

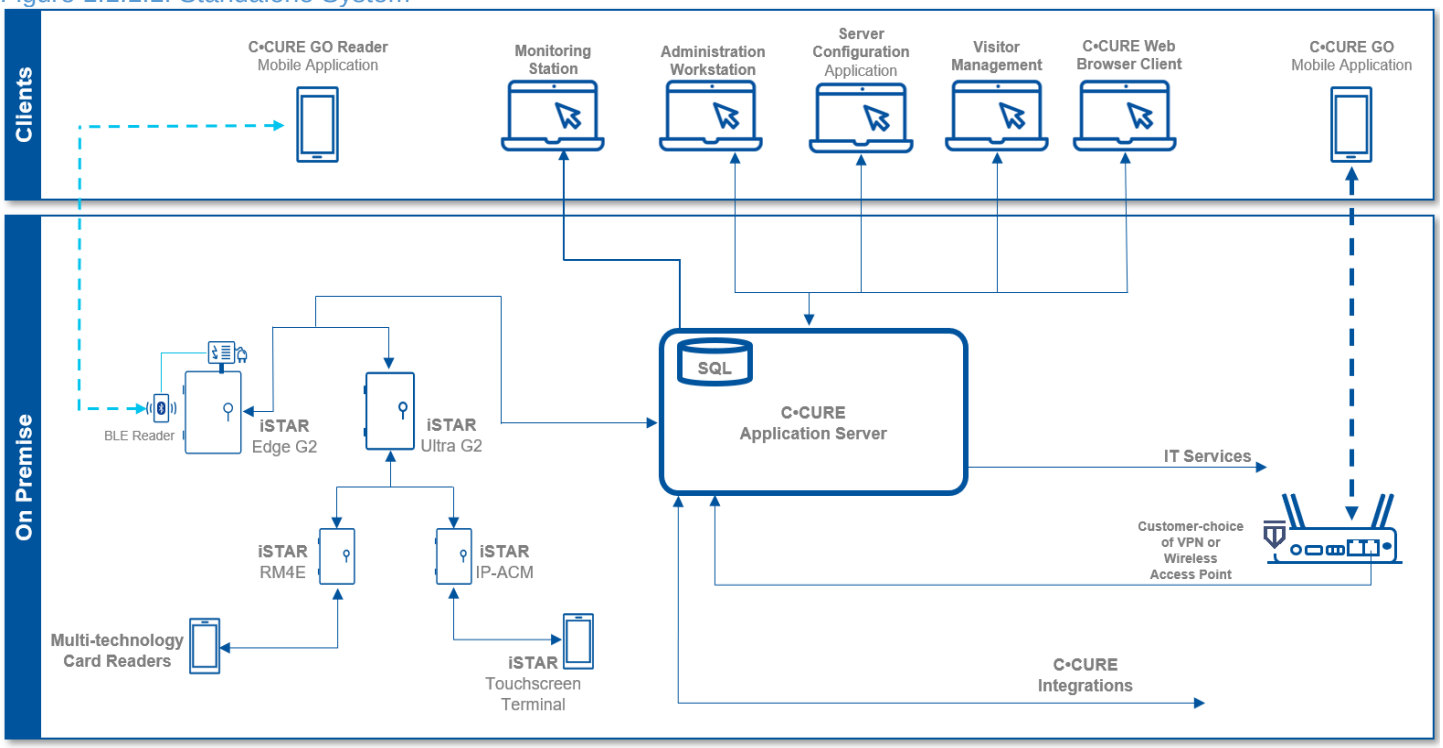
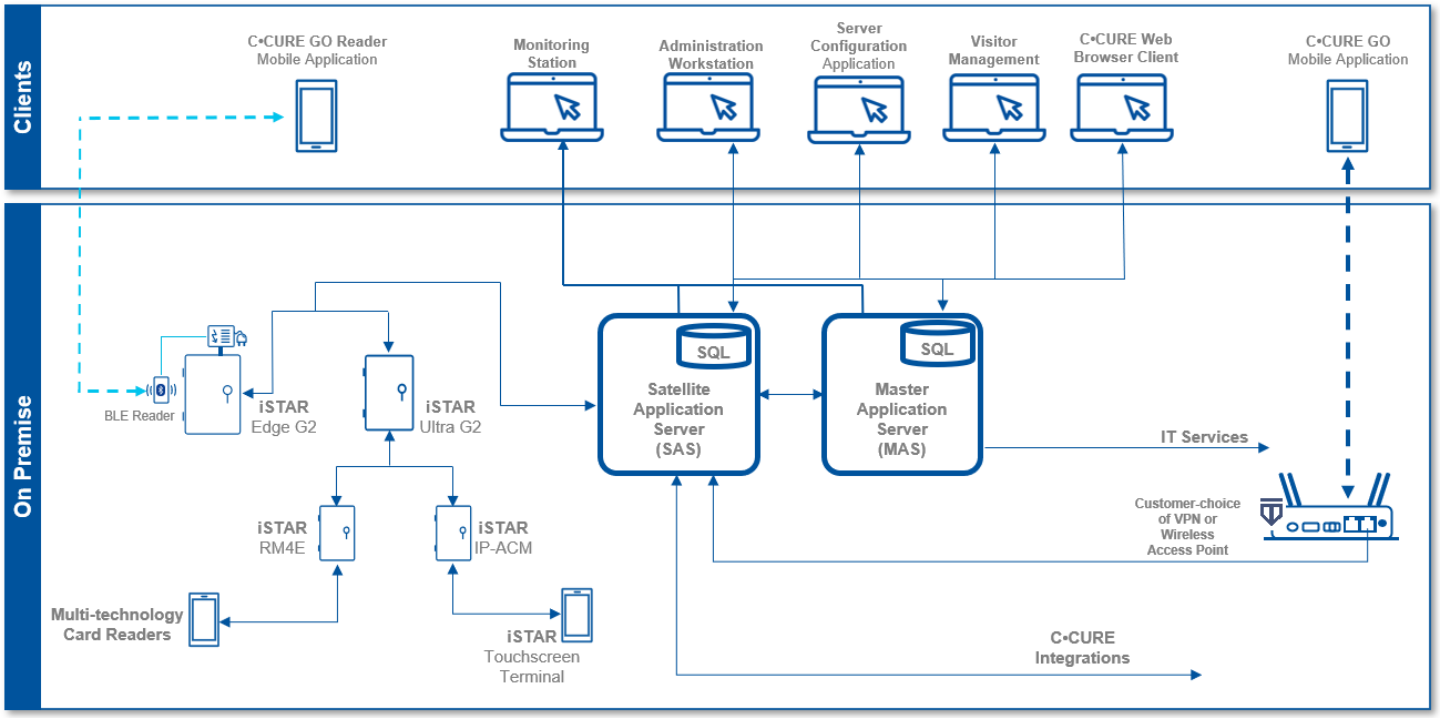


Figure 1.1.1.2: Enterprise System



1.2 Security feature set

This section describes C•CURE's many security features and how to configure them.

1.2.1 User authentication and authorization

C•CURE 9000 offers the following user authentication and authorization features:

Table 1.2.1: User authentication and authorization features

Feature	Description
No backdoor passwords	C•CURE 9000 does not have a backdoor password.
Hidden password entry	A typed password is hidden from view.
No hardcoded password	No hard-coded passwords/credential used in C•CURE 9000 code, configuration, and log files.
Encrypted password	The C•CURE 9000 database contains encrypted credential passwords.
User changeable passwords	The C•CURE user can change their account password without the assistance of an administrator.

User account password policy	User accounts are a combination of Windows AD and C•CURE 9000 rules.
	• C•CURE 9000 contains rules which govern password formation, expiration, reuse, and other restrictions including password length, history, and complexity.
	• All Windows accounts prompt a password change the next logon.
	• Johnson Controls recommends using a password of 15 characters or more from three or more of the following groups:
	  ○ Upper Case
	  ○ Lower Case
	  ○ Numerals
	  ○ Special characters

Password rules	The local Microsoft Windows operating system or the domain controller manages policies such as predefined number of logon attempts, character length, use of alphanumeric characters, and user-defined lockouts except in the case of SiteServer.
Windows login credentials	C•CURE 9000 uses the Windows login credentials to manage permissions but does not store or have any visibility of the credentials. The local Microsoft Windows operating system or the domain controller manages password rules and policies such as predefined number of login attempts, character length, use of alphanumeric characters, and user-defined lockouts.
Maximum log on attempts	Restrict the user to the configured number of consecutive authentication attempts allowed before that account is locked from further authentication retries.

SiteServer Password Policy	After 20 password attempts, the user cannot perform another attempt for 10 minutes. After 10 minutes, the user can retry as if no previous password attempts were made. Note: These are fixed values.
Microsoft Active Directory support	To enable centralized authentication, use a Microsoft Active Directory server for the management of user accounts and log on authentication. C•CURE 9000's user authentication is designed for seamless deployment in an Active Directory domain environment utilizing Windows Single Sign-On (SSO). C•CURE uses Windows log on credentials by default. At the Windows logon, users are automatically logged on to the Administration and Monitoring Stations.
Single-use password	When the iSTAR controller boots for the first time it prompts to change the password before proceeding to any other screens.
Role Based Access Control (RBAC) authorizations	C•CURE 9000 offers Role Based Access Control (RBAC) authorizations. Roles are defined in C•CURE 9000 as operator privileges with different object level permissions. C•CURE 9000 administrators can assign authorizations to individual operators and objects within C•CURE.
Operator Auto Log Off	Starting in v2.90 SP3, operators with inactivity time limit will be automatically logging out. The time limit can be configured using two new System Variables: Monitoring Shift Duration and Session Timeout.

1.2.2 Data encryption

This section describes data in transit and data at rest.

Table 1.2.2.1: Data in transit

Description	Connection type	Encryption
Communication between iSTAR Edge G2, iSTAR Ultra G2 and C•CURE Application Server	TCP/IP	TLS1.3 with 256-bit AES Encryption Also support secure update with security violation reports to C•CURE
Communication between iSTAR Ultra and C•CURE Application Server	TCP/IP	TLS1.2 with 256-bit AES Encryption Also support TLS 1.3 with AES_256_GCM starting in firmware v6.9.0.
Communication between iSTAR Pro and C•CURE Application Server	TCP/IP	128-bit RC4 Encryption. Optional. Default setting is off.
Communication between iSTAR Classic and C•CURE Application Server	TCP/IP	128-bit RC4 Encryption. Optional. Default setting is off.
Communication between iSTAR Edge and C•CURE Application Server	TCP/IP	TLS1.2 with 256-bit AES Encryption
Communication between IP-ACM2 and iSTAR Ultra Controller	TCP/IP	TLS1.2 with 256-bit AES Encryption

Communication between the C•CURE client workstation and C•CURE application server	TCP/IP	Standard Microsoft Windows Communication Foundation (WCF) transport level security encryption (SSL). The End-to-End Message Level Encryption option is in the Server Configuration Application on the Settings tab
Communication between the C•CURE Web client and C•CURE Web server	HTTPS	Support all standard IIS encryptions over HTTPS (SSLv3.0/TLS1.3)
Communication between the C•CURE application server and C•CURE Database SQL Server	TCP/IP	Standard Microsoft SQL Encryption (TLS1.3). To configure C•CURE Encrypted Connection Strings complete the following steps: 1. Navigate to **Server Configuration Application.** 2. Click **Databases.** 3. Select **Connection String Encrypted**.
Communication between the C•CURE application server and C•CURE Web/IIS Server	TCP/IP	Support standard Microsoft WCF transport level security encryption (SSL)
Communication between the Business Intelligence Reporting Suite (BIRS) and C•CURE DB Server	TCP/IP	Support all native Microsoft SSRS encryption methods (SSL, TDE).
Communication between the C•CURE Master Application Server and Satellite Application Server	TCP/IP	Standard Microsoft WCF transport level security encryption.
Communication between OSDP RM4E and iSTAR	OSDP	High-end AES-128 encryption

Table 1.2.2.2: Data at rest

Description	Encryption
iSTAR Edge G2 and iSTAR Ultra G2	Encryption/security are built-in features of firmware and operation procedures at manufacture. For example, firmware partition uses Linux LUKS disk partition encryption, and each iSTAR Edge G2 is manufactured with an encrypted eMMC card encrypted.
IP-ACM2	None, but it does not store credential info by default.
iSTAR Edge G2 and iSTAR Ultra G2	LUKS with argon2i

iSTAR Ultra	LUKS with PBKDF2 (6.6.B and later FW)
C•CURE Database Server	Standard Microsoft SQL Encryption (TDE)
C•CURE Web Server	Application-level encryption with 256-bit Encryption.

iSTAR Ultra also supports **Database Stored in RAM Only** mode. When this mode is enabled, the database of the iSTAR Ultra is no longer stored in persistent memory. In **Database Stored in RAM Only** mode, the database is erased when power is removed from the controller.

1.2.3 Transaction and activity tracking

This section describes transaction and activity tracking.

Table 1.2.3.1: Audit Logs

Feature	Description
Audit log	The audit log is a history of changes to C•CURE 9000 configurations. Field level auditing can also be enabled.
Activity journal	The activity journal maintains a record of activity monitored by the system. Records in the activity journal provide a historical view of system activity, statistical information on resource usage, and personnel and asset location information.
Audit log enabled by default	C•CURE 9000 system diagnostic log, trace log, journal, and audit logs, are enabled by default.
Audit log time synchronized	Audit log timestamps are synchronized to a common reference clock for the system.
Audit log delete protected	Audit logs are protected from deletion with deletion attempts logged.

1.2.4 High availability and disaster recovery assurance

C•CURE 9000 supports **Stratus everRun** for high availability and **Stratus ARCserve** for disaster recovery (DR) redundancy solutions for reduced system downtime.

everRun protects customers from server hardware failures or other system or network component failures. The **ARCserve** provides disaster recovery from site disasters. Customers usually have an **everRun** system in a primary site and a Windows system running on a single physical or virtual machine in the DR site. **ARCserve** is used to provide DR between the primary and DR site (also called the master and replica).

Some customers also have an **everRun** system at the DR site, to ensure high availability after they execute a disaster recovery scenario.

1.2.5 Backup and restore

C•CURE 9000 uses three databases that can be backed up at any time using the System Backup feature.

- The Core database is a component of the management platform upon which C•CURE 9000 is built. It is the central repository for configuration details describing objects created, monitored, and maintained.
- The Audit Log provides a history of changes to configurations managed by C•CURE 9000.
- The Activity Journal maintains a record of activity monitored by the system. Records in the Activity Journal provide a historical view of activity that has occurred in the system, statistical information on resource usage, and personnel and asset location information.

In the event of a system failure or corruption of these databases, restoration is easily obtained from a backup.

The C•CURE 9000 Server Configuration Application Guide describes how to perform a system backup and restore. User access to the System Backup feature is controlled through the user configuration.

1.2.6 Alarms and alerts

C•CURE 9000 supports real-time alarms and alerts for many types of events. All iSTAR controllers include tamper detection that prompts an alarm if someone opens the enclosure. The iSTAR Ultra includes an optional installation of a back tamper that can detect if the controller is removed from the wall.

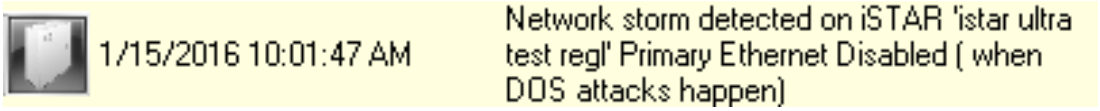
Authorization change notification – use journal auditing to verify individual authorization against other databases to verify location. To notify users of change in authorizations, generate an alert for changes in daily run journals.

1.2.7 Denial of Service (DoS) protection

The iSTAR controllers provide Denial of Service protection. When iSTAR detects unusual network traffic, the controller temporarily disables the network ports. After a period, the ports reopen, but if the unusual traffic is still present, it repeats the process, going offline for a longer period. During this time, the iSTAR continues to perform its access control functions.

When an iSTAR goes into hiding due to a DoS attempt, C•CURE 9000 alerts the monitoring station with a **Network storm detected** alert.

Figure 1.2.7.1: Alert



1.3 Intended environment

Physical access and installation of devices can greatly impact cybersecurity. Components are designed to be operated in an indoor, dry environment. However, components at each level will possess varying degrees of access. Here is some general guidance based on typical environments per component type:

Server Level – An on-site server or server appliance is to be installed within an equipment rack in a secured, temperature-controlled location, such as within a data center or IT Server room with restricted access. Note: this does not apply to cloud-based deployments.

Supervisory Level – Components 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).

Field controller Level – Components 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 installation instructions of that specific component.

1.3.1 Internet connectivity

Internet access increases your cybersecurity footprint and attack area which requires additional hardening steps. When required, C•CURE components should be protected against direct internet traffic (e.g. using a firewall, Zero-Trust, VPN, etc.).

C•CURE has additional **Security Intelligence** features, such as **Last Known Location** and **Virtual Headcount.** These features provide knowledge that can help detect anomalies. Their functionality will rely on your web browser utilizing an established internet connection.

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.

1.4 Patch Policy

The policy documented here sets forth the current internal operating guidelines and process regarding C•CURE 9000, which may change from time to time at the sole discretion of Johnson Controls. It is best practice to apply the latest C•CURE 9000 service packs and updates to all components to get the latest security fixes for your system. When applying updates, always refer to company policies.

C•CURE 9000 support is provided for the latest version of the current release. Support will also be given for 2 major versions back of the prior software release for a duration of 6 months. When we discover a critical security vulnerability, we use commercially reasonable efforts to:

- Issue a **critical update** for the current version of the product as soon as is reasonably practicable
- Subsequently issue a **critical update** or **critical service pack** for previous supported versions.

When we discover non-critical security vulnerability, we use commercially reasonable efforts to:

- Apply fixes for high severity vulnerabilities in the next immediate release
- Apply fixes for medium severity vulnerabilities in the next major release

1.5 Hardening methodology

While C•CURE 9000 provides many 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, a defence-in-depth strategy employing standard IT hardening methods and compensating controls as needed to compliment the base security features of each component.

1.6 Communication

1.6.1 Communication port configuration

In a C•CURE 9000 system, when you use a protocol, ensure that the corresponding port is open. Hardening your system involves closing any port that is not used.

NOTE: This document does not list ports used internally by each device. Ports are listed by the device that has the port open. Please see the document **C•CURE 9000 and iSTAR Port Assignments** at the following website - https://www.johnsoncontrols.com/cyber-solutions/resources for the latest revision of this C•CURE 9000 and iSTAR Port Assignment information document.

The tables below provide detailed information about on which ports and protocols you must leave open for C•CURE 9000 to function properly, valid for:

- C•CURE 9000 v2.90 SP5 (and above)
- iSTAR Ultra G2 firmware v6.8.9 (and above)
- iSTAR Ultra family firmware v6.8.0 (and above)
- iSTAR Pro firmware v5.2.x
- iSTAR Edge/eX firmware v6.2.x
- iSTAR Edge G2 firmware
- C•CURE 9000 integrations.
- C•CURE 9000 SiteServer series

Table 1.6.1.1 - C•CURE 9000 Server (victor Application Server)

Port/ Range	Protocol	Direction	Initiator	Process/ Service	Description
80	TCP	Inbound Listening	Client	IIS for HTTP (inetinfo.exe)	Port for IIS, C•CURE web client. If IIS is installed on a different server, please make sure this Inbound listening port is opened for the IIS server. This port is also used for VideoEdge Administration/Alarm.
443	TCP	Inbound Listening	Client	IIS for HTTPS	Port for IIS, C•CURE web client. If IIS is installed on a different server, please make sure this Inbound listening port is opened for the IIS server.
2800	UDP and TCP	Inbound Listening	iSTAR	Host port for iSTAR driver (SoftwareHouse.NextGen; iSTAR_DriverService.exe; SoftwareHouse.NextGen.iST, stunnel.exe)	Host port for incoming non-encrypted iSTAR (Pro and Ultra) connections.
2801	TCP	Inbound Listening	iSTAR	iSTAR Fast personnel download host port	HOST port for non-encrypted fast personal

				(SoftwareHouse.NextGen; iSTAR_DriverService.exe; SoftwareHouse.NextGen.iST, stunnel.exe)	download to iSTAR (Pro and Ultra) panels.
2802	TCP	Inbound Listening	iSTAR	Fast image download host port (iSTAR Pro only) (iSTAR_DriverService.exe)	Location = vAS, Traffic Direction from vAS = inbound, Connection Initiate from iSTAR panels. Nonencrypted image download for iSTAR Pro. This port can be closed if using host-based certificate in TLS 1.3.
2804	TCP	Inbound Listening	iSTAR Ultra (unencrypted or in Ultra SE Pro Mode)	Fast SQLite personal database download (SoftwareHouse.NextGen.iST)	HOST port for unencrypted fast SQLite personal download to iSTAR Ultra and Ultra SE (in Pro Mode) panels.
2816	TCP	Inbound Listening	iSTAR Ultra	Panel uploads personnel database file to host (iSTAR_DriverService.exe)	Host port for unencrypted uploading SQLite personnel database file.
3000	TCP	Inbound Listening	C•CURE web	HTTP for C•CURE Web (node JS – local only)	This port is needed if C•CURE web server is installed on the same PC with C•CURE server.
3001	TCP	Inbound Listening	C•CURE web	HTTPs for C•CURE Web (node JS – local only)	This port is needed if C•CURE web server is installed on the same PC with C•CURE server.
5984	TCP	Inbound Listening	C•CURE Web couch DB	HTTP for C•CURE Web DB (Couch DB – local only)	This port is needed if C•CURE web server is installed on the same PC with C•CURE server.
7144-7145	TCP	Inbound Listening	EMC Replistor	EMC Replistor (N/A)	For EMC Replistor failover/redundancy.
8042-8045	TCP	Inbound Listening	EMC Autostart	EMC AutoStart (N/A)	For EMC AutoStart failover/redundancy.
8080	TCP	Inbound Listening	Client	Tomcat6.exe	Communication from Assa Abloy DSR to C•CURE server.
8085	TCP	Inbound Listening	Client	Auto Update (autoupdate.exe)	C•CURE9000 software Auto Update for clients and SAS from MAS
8985	TCP	Inbound Listening	iSTAR/vAS	Base address of driver service (iSTAR_DriverService.exe)	location = Server Base for drivers for iSTAR, VideoEdge, Intellex, etc. used to drive communication
8995	TCP	Inbound Listening	SAS	Installation, upgrade, and repair operations on MAS and SAS (SoftwareHouse.CrossFire.S)	Required for SAS to communicate with MAS during install/upgrade. MAS listens, SASs initiates the communication.
8996	TCP	Inbound Listening	Client	Crossfire service of web client session	Required for the connection between the legacy C•CURE9000 web

				(SoftwareHouse.NextGen; iSTAR_DriverService.exe; SoftwareHouse.NextGen.iST, stunnel.exe)	client and the Crossfire service of C•CURE9000 server.
8997	TCP	Inbound Listening	Client	Admin / Monitor Client stream (SoftwareHouse.NextGen; iSTAR_DriverService.exe; SoftwareHouse.NextGen.iST, stunnel.exe)	Required for the connection between C•CURE9000 Administration client/ C•CURE9000 Monitoring Station client and the Crossfire service of C•CURE9000 server.
8998	HTTP	Inbound Listening	Client	Crossfire service of HTTP client session (SoftwareHouse.NextGen; iSTAR_DriverService.exe; SoftwareHouse.NextGen.iST, stunnel.exe)	Required for the C•CURE9000 server to listen for HTTP requests for web service connections from the C•CURE legacy Web Client, C•CURE Mobile, and Web Service.
8999	TCP	Inbound Listening	Client	Crossfire service of TCP client session (SoftwareHouse.NextGen; iSTAR_DriverService.exe; SoftwareHouse.NextGen.iST, stunnel.exe)	Required for the connection between TCP client session of C•CURE9000 Administration client/ C•CURE9000 Monitoring Station client and the Crossfire service of C•CURE9000 server. Configuration data exchanged between C•CURE client and C•CURE server.
9090	TCP	Inbound Listening	DSR	CrossFireAssaAbloyDriverService	Communication from C•CURE to DSR server.
9701	TCP	Inbound Listening	iSTAR Ultra	LightTPD.exe	iSTAR Ultra download firmware. **NOTE:** iSTAR Ultra G2 does not use this port. iSTAR Ultra G2 uses panel port 21050 for firmware download.
27000	TCP	Inbound Listening	vAS	TycoESS License software ((lmgrd.exe, TYCOESS.exe)	Required for the license validation between C•CURE 9000 clients and the license server manager on C•CURE 9000 server.
27010	TCP	Inbound Listening	vAS	TycoESS – License Vendor Daemon (TYCOESS.exe, ACVS.Enterprise.Server.Co)	Required for the system feature license validation between C•CURE9000 server and the TycoESS license vendor daemon.

					Services and applications that utilize TycoESS are vAS, C•CURE9000License.exe, LicenseManager.exe and Crossfire Framework Service.
28001	TCP	Inbound Listening	iSTAR	iSTAR Driver - iSTAR eX/Edge/Ultra Fast personnel download connection (stunnel.exe)	Location = vAS, traffic direction from vAS = inbound, Connection initiate from encrypted iSTAR panels
28002	TCP	Inbound Listening	iSTAR	iSTAR Driver - iSTAR eX/Edge firmware download and for TLS 1.2 host certificate download. (stunnel.exe)	location = vAS, traffic direction from vAS = inbound, Connection initiate from encrypted iSTAR panels. This port is used for TLS 1.2 host certificate and firmware download (for iSTAR eX, Edge, and Ultra).
28003	TCP	Inbound Listening	iSTAR	iSTAR Driver - iSTAR eX/Edge/Ultra Used by host to accept eX or Edge request for certificate signing (SoftwareHouse.NextGen.iST)	location = vAS, traffic direction from vAS = inbound, Connection initiate from encrypted iSTAR panels.
28004	TCP	Inbound Listening	iSTAR	iSTAR Driver - Encrypted iSTAR Ultra SQL Lite database download (stunnel.exe)	location = encrypted iSTAR Panels, traffic direction from vAS = outbound, connection initiate from vAS.
28010	TCP	Inbound Listening	iSTAR	iSTAR Driver - Host port for incoming encrypted iSTAR connections (stunnel.exe)	Port used by Stunnel on server for incoming iSTAR panel connection. Stunnel is the secure encrypted wrapper for communication between C•CURE9000 server and iSTAR panels.
28016	TCP	Inbound Listening	iSTAR Ultra	iSTAR Driver - Panel uploads personnel database file to host when using TLS 1.2. (stunnel.exe)	Host port for encrypted uploading SQLite personnel database file when using TLS 1.2.
28110	TCP	Inbound Listening	iSTAR Edge G2 iSTAR Ultra G2	iSTAR Driver – Port for Connection with: iSTAR Edge G2 iSTAR Ultra G2	Port used by Stunnel on server for incoming iSTAR panel connection. Stunnel is the secure encrypted wrapper for communication between C•CURE 9000 server and iSTAR panels.
28104	TCP	Inbound Listening	iSTAR Edge G2 iSTAR Ultra G2	iSTAR Driver – Fast download port for: iSTAR Edge G2 iSTAR Ultra G2	Host opens the port. Panel connects to this port to receive SQLite personnel DB (i.e. Fast personnel download).

28013	TCP	Inbound Listening	iSTAR Edge G2 iSTAR Ultra G2	iSTAR Driver – Certificate Sign Request for: iSTAR Edge G2 iSTAR Ultra G2	TLS 1.3 Certificate Sign Request (CSR) port. Host opens the port. Panel sends certificate signing request.
28116	TCP	Inbound Listening	iSTAR Edge G2 iSTAR Ultra G2	ISTARUltraUploadConnectionG2V6 Panel uploads personnel database file to host using TLS 1.3.	C•CURE port for iSTAR Ultra (f/w v6.9.0 and above), Ultra G2, and Edge G2 to upload personnel database using TLS 1.3.
33002	TCP	Inbound Listening	iSTAR/Innometriks High Assurance Reader	Stunnel (Innometriks-only)	C•CURE 9000 software supporting communication with Innometriks High Assurance reader. For communication in TLS 1.2.
33003	TCP	Inbound Listening	iSTAR/Innometriks High Assurance Reader	Stunnel (Innometriks-only)	C•CURE 9000 software supporting data downloads to Innometriks High Assurance reader. For download in TLS 1.2
33050	TCP	Inbound Listening	iSTAR/Innometriks High Assurance Reader	Stunnel (Innometriks-only)	C•CURE 9000 software supporting the transaction log from Innometriks High Assurance reader. For transaction log in TLS 1.2
33102	TCP	Inbound Listening	iSTAR/Innometriks High Assurance Reader	Stunnel (Innometriks-only)	C•CURE 9000 software supporting communication with Innometriks High Assurance reader. For communication in TLS 1.3.
33103	TCP	Inbound Listening	iSTAR/Innometriks High Assurance Reader	Stunnel (Innometriks-only)	C•CURE 9000 software supporting data downloads to Innometriks High Assurance reader. For download in TLS 1.3.
33150	TCP	Inbound Listening	iSTAR/Innometriks High Assurance Reader	Stunnel (Innometriks-only)	C•CURE 9000 software supporting the transaction log from Innometriks High Assurance reader. For transaction log in TLS 1.3.

*Port 33050 is a legacy port and should be closed.

Table 1.6.1.2 - NodeJS (use for legacy C•CURE web, C•CURE IQ, and C•CURE Portal)

Port/ Range	Protocol	Direction	Initiator	Process/ Service	Description
3000	TCP	Inbound Listening	C•CURE web	HTTP for C•CURE Web	This is a NodeJS port used for C•CURE Web (prior to v3.0). This port is needed to be opened on the PC where C•CURE Web service is installed. For example, if C•CURE Web service is installed on the same PC with C•CURE server, this port is needed to be opened for the C•CURE server.
3001	TCP	Inbound Listening	C•CURE web	HTTPs for C•CURE Web	This is a NodeJS port using for C•CURE Web (prior to v3.0). This port is needed to be opened on the PC where C•CURE Web service is installed. For example, if C•CURE Web service is installed on the same PC with C•CURE server, this port is needed to be opened for the PC of C•CURE server.
4000	TCP	Inbound Listening	C•CURE IQ	HTTP for C•CURE IQ	This is a NodeJS port using for C•CURE IQ (v2.90 and later). This port is needed to be opened on the PC where C•CURE web service is installed. For example, if C•CURE web service is installed on the same PC with C•CURE server, this port is needed to be opened for the PC of C•CURE server.
4001	TCP	Inbound Listening	C•CURE IQ	HTTPs for C•CURE IQ	This is a NodeJS port using for C•CURE IQ (v2.90 and later). This port is needed to be opened on the PC where C•CURE web service is installed. For example, if C•CURE web service is installed on the same PC with C•CURE server, this port is needed to be opened for the PC of C•CURE server.
4002	TCP	Inbound Listening	C•CURE Portal	HTTP for C•CURE Portal	This is a NodeJS port using for C•CURE Portal. This port is needed to be opened on the PC where C•CURE web service is installed. For example, if C•CURE web service is installed on the same PC with C•CURE server, this port is needed to be opened for the PC of C•CURE server.
4003	TCP	Inbound Listening	C•CURE Portal	HTTPs for C•CURE Portal	This is a NodeJS port using for C•CURE Portal. This port is needed to be opened on the PC where C•CURE web service is installed. For example, if

					C•CURE web service is installed on the same PC with C•CURE server, this port is needed to be opened for the PC of C•CURE server.

Table 1.6.1.3 - iSTAR Edge/eX

Port/ Range	Protocol	Direction	Initiator	Process/ Service	Description
80	TCP	Inbound Listening	Web	HTTP	Web connection used for diagnostic website. Port is closed in FIPS mode and is only necessary for diagnostics.
137	UDP	Inbound Listening	vAS	NetBIOS-NS	NetBIOS Name Service. This is a Windows function and cannot be closed but is not required for iSTAR operation.
138	UDP	Inbound Listening	vAS	NetBIOS-DS	NetBIOS Datagram Service. This is a Windows function and cannot be closed but is not required for iSTAR operation. This port can be blocked using a network firewall.
161	UDP	Inbound Listening	vAS	SNMP	Protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.
1025	UDP	Inbound Listening	vAS	Windows DNS	Windows DNS resolves domain names. This port cannot be closed but is not part of the iSTAR function. This port can be blocked using a network firewall.
1999	TCP	Inbound Listening	iSTAR members, ICU	Configuration	iSTAR port for incoming ICU requests.
2001	UDP	Inbound Listening	ICU	Discovery	iSTAR port for ICU broadcasts.
2008	TCP	Inbound Listening	PC running iWatch	iWATCH	iWATCH connection port. Not open by default but can be enabled via webpage diagnostic settings.
28003	TCP	Inbound Listening	Encrypted iSTAR members	encryption	Used to accept signed certificate for encryption.
28009	TCP	Inbound Listening	Encrypted iSTAR	Cluster member	iSTAR port for incoming encrypted member requests
1025 - 5000	TCP	Outbound	iSTAR Edge/eX	iSTAR to C•CURE communication	This port number is generated during bootup and is the Stunnel

					communication for C•CURE9000 server [port 28010 (Stunnel)]. Stunnel is the secure encrypted wrapper for communication between C•CURE 9000 server and iSTAR panels.

Table 1.6.1.4 - iSTAR Pro

Port/ Range	Protocol	Direction	Initiator	Process/ Service	Description
80	TCP	Inbound Listening	Web	HTTP	Web connection used for diagnostic website. Port is closed in FIPS mode. Necessary only for diagnostics.
161	UDP	Inbound Listening	vAS	SNMP	SNMP Protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.
1025	UDP	Inbound Listening	vAS	Windows DNS	Windows DNS. This is a Windows function and cannot be closed but is not required for iSTAR operation. This port can be blocked using a network firewall.
1999	TCP	Inbound Listening	iSTAR members, ICU	Master	iSTAR master port for incoming non-encrypted member connections, plus incoming ICU requests.
2008	TCP	Inbound Listening	PC running iWatch	iWATCH	iWATCH connection port. Not open by default but can be enabled via webpage diagnostic settings.
2001	UDP	Inbound Listening	ICU	Discovery	iSTAR port for ICU broadcasts.
1025 - 5000	TCP	Outbound	iSTAR Pro	iSTAR to C•CURE communication	This port number is generated during bootup.

Table 1.6.1.5 - iSTAR Ultra, iSTAR Ultra SE, iSTAR Ultra LT

Port/ Range	Protocol	Direction	Initiator	Process/ Service	Description
68	UDP	Inbound Listening	DHCP server	DHCPC	Obtaining dynamic IP address (DHCP).
161	UDP	Inbound Listening	vAS	SNMP	Protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.
443	TCP	Inbound Listening	Web	HTTPs	Secure web connection used for diagnostic website. Port is

					closed in FIPS mode. Only necessary for diagnostics.
1999	TCP	Inbound Listening	Non-encrypted iSTAR members, ICU	Master	iSTAR master port for incoming non-encrypted member connections, plus incoming ICU requests.
2001	UDP	Inbound Listening	ICU	Discovery	iSTAR port for ICU to discover iSTAR controllers, and member iSTAR controllers to discover its primary controller. The primary iSTAR controller also uses this port to receive members service requests.
2900	TCP	Inbound Listening	IP-ACM	Communication	iSTAR Ultra GCM listening port for IPACM proprietary encrypted connection.
2901	TCP	Inbound Listening	IP-ACM2	iSTAR IP-ACM	iSTAR Ultra GCM listening port for IPACM2 SSL encrypted connection with default certificate/key.
2902	TCP	Inbound Listening	IP-ACM2	iSTAR IP-ACM	iSTAR Ultra GCM listening port for IPACM2 SSL encrypted connection with default certificate/key.
2910	UDP	Inbound Listening	IP-ACM2	iSTAR IP-ACM	Used for IP-ACM discovery.
28004	TCP	Inbound Listening	C•CURE	iSTAR Ultra signed certificate download port	TLS 1.2 Signed Certificate delivery port. iSTAR Ultra opens the port. Host delivers the signed certificates.
28009	TCP	Inbound Listening	Encrypted iSTAR	iSTAR Member	iSTAR Ultra incoming encrypted member connection port.
21050	TCP	Inbound Listening	C•CURE or web	iSTAR Ultra Firmware download	Secure firmware download.
28014	TCP	Inbound Listening	C•CURE	iSTAR Ultra in TLS 1.3 signed certificate download port	TLS 1.3 Signed Certificate delivery port. iSTAR Ultra opens the port. Host delivers the signed certificates.
33002	TCP	Listening	C•CURE	Innometriks	For communication in TLS 1.2
33003	TCP	Listening	C•CURE	Innometriks	For download in TLS 1.2
33050	TCP	Listening	C•CURE	Innometriks	For transaction log in TLS 1.2
33102	TCP	Listening	C•CURE	Innometriks	For communication in TLS 1.3
33103	TCP	Listening	C•CURE	Innometriks	For download in TLS 1.3
33150	TCP	Listening	C•CURE	Innometriks	For transaction log in TLS 1.3

NOTE: iSTAR Ultra SE Pro Mode does not support encryption.

Table 1.6.1.6 - iSTAR Ultra G2

Port/ Range	Protocol	Direction	Initiator	Process/ Service	Description

161	UDP	Inbound Listening	vAS	SNMP	Protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.
443	TCP	Inbound Listening	Web	HTTPs	Secure web connection.
2001	UDP	Inbound Listening	Cluster master	Communication	iSTAR port for member iSTAR controllers to discover its master controller. The master iSTAR controller also uses this port to receive its members' service requests.
2901	TCP	Inbound Listening	IP-ACM2	iSTAR IP-ACM	iSTAR Ultra G2 GCM listening port for IP-ACM2 SSL encrypted connection with default certificate/key.
2902	TCP	Inbound Listening	IP-ACM2	iSTAR IP-ACM	iSTAR UItra G2 GCM listening port for IP-ACM2 SSL encrypted connection with default certificate/key.
2910	UDP	Inbound Listening	IP-ACM/IP-ACM2	iSTAR IP-ACM	For IP-ACM discovery.
21050	TCP	Inbound Listening	C•CURE or web	iSTAR Ultra G2 Firmware download	Secure firmware download.
28009	TCP	Inbound Listening	Cluster member	Communication	Master port for incoming encrypted member connection.
28014	TCP	Inbound Listening	C•CURE	iSTAR Ultra G2 signed certificate download port	TLS 1.3 Signed Certificate delivery port. iSTAR Ultra G2 opens the port. Host delivers the signed certificates.
33002	TCP	Listening	C•CURE	Innometriks	For communication in TLS 1.2
33003	TCP	Listening	C•CURE	Innometriks	For download in TLS 1.2
33050	TCP	Listening	C•CURE	Innometriks	For transaction log in TLS 1.2
33102	TCP	Listening	C•CURE	Innometriks	For communication in TLS 1.3
33103	TCP	Listening	C•CURE	Innometriks	For download in TLS 1.3
33150	TCP	Listening	C•CURE	Innometriks	For transaction log in TLS 1.3

*Port 33050 is a legacy port and should be closed

Table 1.6.1.7 - iSTAR Edge G2

Port/ Range	Protocol	Direction	Initiator	Process/ Service	Description
161	UDP	Inbound Listening	vAS	SNMP	Protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.
443	TCP	Inbound Listening	Web	HTTPs	Secure web connection.

2001	UDP	Inbound Listening	Cluster master	Communication	Member port to handle autoconfig from master on the same subnet.
21050	TCP	Inbound Listening	C•CURE or web	iSTAR Edge G2 Firmware download	Secure firmware download.
28009	TCP	Inbound Listening	Cluster member	Communication	Master port for incoming encrypted member connection.
28014	TCP	Inbound Listening	C•CURE	iSTAR Edge G2 signed certificate download port	TLS 1.3 Signed Certificate delivery port. iSTAR Edge G2 opens the port. Host delivers the signed certificates.

Table 1.6.1.8 - iSTAR Ultra Video

Destination System	Port/ Range	Protocol	Direction	Initiator	Process/ Service	Description
VideoEdge	25	TCP	Inbound Listening	Mail server	SMTP	SMTP
VideoEdge	68	UDP	Inbound Listening	DHCP server	DHCPC	Obtaining dynamic IP address (DHCP).
iSTAR Ultra Video VideoEdge iSTAR Ultra	80	TCP	Inbound Listening	iUV Web client, VideoEdge web client	HTTP	Web service for the iSTAR diagnostic site, iSTAR Ultra Video site and VideoEdge remote client.
VideoEdge	123	UDP	Inbound Listening	NTP (time server)	NTP	NTP (time server).
VideoEdge	161	UDP	Inbound Listening	SNMP manager	SNMP	SNMP
VideoEdge	162	UDP	Inbound Listening	SNMP manager	SNMP	SNMP Trap
iSTAR Ultra Video VideoEdge	443	TCP	Inbound Listening	iUV Web client, VideoEdge web client	HTTPS	Protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.
VideoEdge	554	TCP	Inbound Listening	Camera	RTSP	Camera video streaming connections.
VideoEdge	623	UDP	Inbound Listening	Remote control (should be closed)	RPC	RPC - standard Linux open port.
iSTAR Ultra	1999	TCP	Inbound Listening	Non-encrypted iSTAR members, ICU	Master	iSTAR master port for incoming nonencrypted member connections, plus incoming ICU requests.
iSTAR Ultra	2900	TCP	Inbound Listening	IP-ACM	Communication	Communication between the IP-ACM and iSTAR Ultra family GCM.

iSTAR Ultra	2001	UDP	Inbound Listening	ICU	discovery	iSTAR port for ICU broadcast
iSTAR Ultra	2008	TCP	Inbound Listening	PC running iWatch	iWATCH	iWATCH connection port
iSTAR Ultra	2901	TCP	Inbound Listening	IP-ACM2	Communication	Used for SSL encrypted communication between the IP-ACM2 and iSTAR Ultra family GCM.
iSTAR Ultra	2902	TCP	Inbound Listening	IP-ACM2	Communication	Reserved for enhanced SSL communication between the IP-ACM2 and iSTAR Ultra family GCM.
VideoEdge	3389	TCP	Inbound Listening	RCP client	RDP	XRDP
VideoEdge	55555	TCP	Inbound Listening	Internally Used	Transmit Manager	Transmit manager - not used externally.
VideoEdge	1900	UDP	Inbound Listening	Any	UPnP	UPnP
VideoEdge	1900	SSDP	Inbound Listening	Any	AD discovery	veAutoDiscSSDP - Discovery of devices, close after setup.
VideoEdge	2980	UDP	Inbound Listening	Any	AD discovery	veAutoDiscScan - Discovery of devices, close after setup.
VideoEdge	3702	UDP	Inbound Listening	Web Server/Any	AD discovery	veAutoDiscovery WSDicovery - Discovery of devices, close after setup.
VideoEdge	5353	UDP	Inbound Listening	Any	AD discovery	veAutoDiscMDNS - Discovery of devices, close after setup.
VideoEdge	5432	TCP	Inbound Listening	SQL	Postgresql	Postgresql
VideoEdge	5800-5803	TCP	Inbound Listening	remote unit	VNC	Java-enabled web browser VNC server.
VideoEdge	5900-5903	TCP	Inbound Listening	remote unit	VNC	VNC server
VideoEdge	8848	UDP	Inbound Listening	Any	AD discovery	veAutodiscoveryADPort - Discovery of devices, close after setup.
VideoEdge	8992	UDP	Inbound Listening	Any	AD discovery	veAutoDiscADScanPort - Discovery of devices, close after setup.
VideoEdge	12345	UDP	Inbound Listening	Any	AD discovery	veAutoDiscADPo - Discovery of devices, close after setup.
iSTAR Ultra	28003	TCP	Inbound Listening	Encrypted iSTAR Ultra members	Certificate signing	Used to accept signing for certificate for encryption.
iSTAR Ultra	28004	TCP	Inbound Listening	C•CURE	Certificate signing	Signed Certificate delivery port. iSTAR Ultra opens the port. Host delivers the signed certificates
iSTAR Ultra	28009	TCP	Inbound Listening	Encrypted iSTAR	iSTAR Member	iSTAR Ultra incoming encrypted member connection port.

VideoEdge Client	32200-38199	UDP	Outbound	VideoEdge server	victor Client UDP communication	Default VideoEdge UDP port range (for victor client connections).
VideoEdge Client	32200-38199	UDP	Outbound	VideoEdge server	AD discovery	veAutoDiscMDNS - Discovery of devices, close after setup.
VideoEdge Client	32200-38199	UDP	Outbound	VideoEdge server	AD discovery	veAutoDiscScan - Discovery of devices, close after setup.
VideoEdge Client	32200-38199	UDP	Outbound	VideoEdge server	AD discovery	veAutoDiscSSDP - Discovery of devices, close after setup.
VideoEdge Client	32200-38199	UDP	Outbound	VideoEdge server	UPnP	VideoEdgeupnpn
VideoEdge Client	32200-38199	UDP	Outbound	VideoEdge server	AD discovery	veAutoDiscSSD - Discovery of devices, close after setup.
VideoEdge Client	32200-38199	UDP	Outbound	VideoEdge server	AD discovery	veAutoDiscWSDi - Discovery of devices, close after setup.
VideoEdge Client/Camera	6000-7999	UDP	Outbound	VideoEdge server	RTP/RTCP	RTP/RTCP
VideoEdge Client/Camera	9000-9511	UDP	Outbound	VideoEdge server	Multicast	multicast port range
Failover NVR	9000-9128	TCP	Outbound	NVR	Remote Transcoding and Failover	Remote Transcoding and Failover

Table 1.6.1.9 - IP-ACM

Port/ Range	Protocol	Direction	Initiator	Process/ Service	Description
80	TCP	Inbound Listening	Web	HTTPS	Web connection used for configuration and diagnostics.

Table 1.6.1.10 - IP-ACM2

Port/ Range	Protocol	Direction	Initiator	Process/ Service	Description
443	TCP	Inbound Listening	Web	HTTPS	Secure Web connection used for configuration and diagnostics.

Table 1.6.1.11 – Innometriks High Assurance/FICAM Readers

Destination System	Port/ Range	Protocol	Direction	Initiator	Process/ Service	Description

ID Server♦	443	TCP	Inbound Listening Outbound	Red Hat sysctl	TLS 1.2 with certificates and HTTPS	Incoming enrollments from Enrollment Client(s) on ID server. PKI updates from the Internet.
Panel Service*	5002	TCP	Inbound Listening	vAS	InnometriksHA.PanelServer.exe	Single card updates from Panel Service to GCM.
Panel Service*	5003	TCP	Inbound Listening	vAS	InnometriksHA.PanelServer.exe	Multiple card updates from Panel Service to GCM.
Panel Service*	5050	TCP	Inbound Listening	vAS	InnometriksHA.PanelServer.exe	Multiple card updates from Panel Service to GCM. For logging function.
Enrollment Server	8000	TCP	Inbound Listening	Enrollment Server	InnometriksHA.EnrollmentServer.exe	Incoming enrollments from ID server to C•CURE. User configurable.
Enrollment Server	8001	TCP	Inbound Listening	Enrollment Server	Encryption	Same as above when used with encryption. User configurable.
Panel Service*	33002	TCP	Inbound Listening	vAS	Encryption	Same as 5002 when used with encryption.
Panel Service*	33003	TCP	Inbound Listening	vAS	Encryption	Same as 5003 when used with encryption.
Panel Service*	33050	TCP	Inbound Listening	vAS	Encryption	Same as 5050 when used with encryption.
C•CURE 9000 Server	33102	TCP	Inbound Listening	Innometriks High Assurance Reader	InnometriksCommunicationsG2	C•CURE 9000 software supporting communication with Innometriks High Assurance reader.
C•CURE 9000 Server	33103	TCP	Inbound Listening	Innometriks High Assurance Reader	InnometriksDownloadG2	C•CURE 9000 software supporting data downloads to Innometriks High Assurance reader.

C•CURE 9000 Server	33150	TCP	Inbound Listening	Innometriks High Assurance Reader	InnometriksTransactionLogG2	C•CURE 9000 software supporting the transaction log from Innometriks High Assurance reader.

*Port 5050 and 33050 are legacy ports and should be closed. When encryption is used, port 5002 should only remain open to localhost.

♦The ID Server is a separate machine from the C•CURE host. This machine is usually located on the same network as the C•CURE machine. Ports shown for Enrollment Server/ID Service are default and can be changed if the configuration is updated appropriately.

Table 1.6.1.12 - SQL Server

Destination System	Port/ Range	Protocol	Direction	Initiator	Process/ Service	Description
SQL Server	1433	TCP	Inbound listening	VAS or other SQL Clients	SQL Server (stunnel.exe)	SQL Server default port used for communication between the C•CURE Application Server and the Database Server. For enterprise system, SAS needs to access both SAS SQL DB and MAS SQL DB. MAS only needs to access MAS SQL DB. Please contact your Database Administrator for the exact ports used.
SQL Server	1434	UDP	Inbound listening	VAS or other SQL Clients	SQL Server Browser (sqlbrowser.exe)	SQL Server Browser Service default port for Dynamic port discovery on the Database Server only if SQL Browsing Services are being used. Please contact your Database Administrator for the exact ports used.

Table 1.6.1.13 - iSTAR Configuration Utility (ICU)

Port/ Range	Protocol	Direction	Initiator	Process/ Service	Description
2001	UDP	Inbound Listening	iSTAR	Discovery (ICU.exe)	Listening port for iSTAR broadcast.

2801	TCP	Inbound Listening	iSTAR	Configuration (stunnel.exe; SoftwareHouse.NextGen.iST)	ICU host port for iSTAR configuration updates (this port can be changed in ICU).
2910	UDP	Inbound Listening	IP-ACM and IP-ACM2	Discovery (ICU.exe)	Listening port for IP-ACM broadcast and IP-ACM2 broadcast.
9701	TCP	Inbound Listening	iSTAR	ICU/LightTPD (LightTPD.exe)	Server port for FW download to iSTAR Ultra. **NOTE:** iSTAR Ultra G2 does not use this port. iSTAR Ultra G2 uses panel port 21050 for firmware download.

Table 1.6.1.14 - C•CURE 9000 SiteServer v2.90

Port/ Range	Protocol	Direction	Action	Description
80	TCP	Inbound	Allow	IIS / VideoEdge NVR Admin/Alarm Port
123	UDP	Inbound	Allow	vAS/C•CURE client time synchronization
123	UDP	Outbound	Allow	vAS/C•CURE client outgoing time synchronization
389	TCP	Inbound	Allow	LDAP
443	TCP	Inbound	Allow	C•CURE Web
554	TCP	Inbound	Allow	VENRLive
1025	UDP	Inbound	Allow	Windows DNS
1025-5000	TCP	Outbound	Allow	iSTAR Edge/eX iSTAR to C•CURE communication
1433	TCP	Inbound	Allow	SQL 1433 TCP
1433	UDP	Inbound	Allow	SQL 1433 UDP
1434	UDP	Inbound	Allow	SQL 1434 UDP
1999	TCP	Inbound	Allow	iSTAR master port for incoming secondary communication
2001	UDP	Inbound	Allow	iSTAR port for ICU broadcasts
2001	TCP	Inbound	Allow	ICU broadcast
2800	TCP	Inbound	Allow	iSTAR host port for iSTAR driver
2800	TCP	Outbound	Allow	iSTAR host port for iSTAR driver out
2800	UDP	Inbound	Allow	iSTAR ICU host port iSTAR driver
2800	UDP	Outbound	Allow	iSTAR ICU host port iSTAR driver out
2801	TCP	Inbound	Allow	iSTAR fast personnel download host port
2802	TCP	Inbound	Allow	iSTAR fast image download host port **Note:** This is used in unencryption mode and can be closed if the port is not used for firmware image download and if there is no host-based certificate in TLS 1.3.
2803	TCP	Inbound	Allow	iSTAR encryption port (iSTAR Pro only)
2804	TCP	Inbound	Allow	iSTAR Ultra fast SQLite personnel database download.
2816	TCP	Inbound	Allow	iSTAR Ultra panel uploads personnel database file to host.
2900	TCP	Inbound	Allow	iSTAR Ultra to IP-ACM
2910	UDP	Inbound	Allow	IP-ACM
2901	TCP	Inbound	Allow	iSTAR Ultra SSL to IP-ACM 2
2902	TCP	Inbound	Allow	Reserved for enhanced SSL IP-ACM 2 to iSTAR Ultra.
2980	UDP	Inbound	Allow	veAutoDiscScan – Discovery of devices, can close after setup.
3000	TCP	Inbound	Allow	HTTP for C•CURE Web
5000	TCP	Inbound	Allow	Intellex Server
5001	TCP	Inbound	Allow	Intellex Live
5002 / 5050	TCP	Inbound	Allow	Innometriks communication between ID server and iSTAR.
5003	TCP	Inbound	Allow	Intellex Alarm

5432	TCP	Inbound	Allow	VideoEdge Postgresql
5984	TCP	Inbound	Allow	HTTP for C•CURE Web database
6000 – 7999	UDP	Inbound	Allow	VideoEdge UDP Ports
6000 – 7999	UDP	Outbound	Allow	VideoEdge Client/Camera RTP/RTCP
8000	TCP	Inbound	Allow	Innometriks incoming enrollments from C•CURE FICAM client.
8005	TCP	Inbound	Allow	System Trace URI
8006	TCP	Inbound	Allow	Remote hardware interface list URI.
8085	TCP	Inbound	Allow	AutoUpdate
8848	UDP	Inbound	Allow	VideoEdge discovery of devices (can close after setup).
8985	TCP	Inbound	Allow	Base Address of Driver Service
8995 – 8999	TCP	Inbound	Allow	C•CURE 9000 host
8995 – 8999	TCP	Outbound	Allow	C•CURE 9000 host
9000 – 9511	UDP	Outbound	Allow	VideoEdge client/camera multicast port range.
9000 – 9128	TCP	Outbound	Allow	NVR remote transcoding and failover.
9701	TCP	Inbound	Allow	iSTAR Ultra download firmware
12345	UDP	Inbound	Allow	VideoEdge discovery of devices (can close after setup).
22609	TCP	Inbound	Allow	VideoEdge HDVR admin/line/alarm port.
27010	UDP	Inbound	Allow	TycoESS License Vendor Daemon.
27000	TCP	Inbound	Allow	TycoESS License Service
28000	TCP	Inbound	Allow	iSTAR host port for iSTAR driver
28001	TCP	Inbound	Allow	iSTAR Edge/Ultra/eX fast download connection.
28002	TCP	Inbound	Allow	iSTAR Edge/Ultra/eX fast image download
28003	TCP	Inbound	Allow	C•CURE 9000 accept iSTAR Edge/Ultra/eX requests for certificate signing.
28004	TCP	Inbound	Allow	iSTAR Edge/Ultra/Ex : Accept a signed certificate
28005	TCP	Inbound	Allow	iSTAR Ultra/eX for connection made to host 2nd IP/name with dual IP configured.
28006	TCP	Inbound	Allow	iSTAR Edge/Ultra/eX for member connection to alternate master.
28007	TCP	Inbound	Allow	iSTAR Edge/Ultra/eX for alternate master host connection.
28008	TCP	Inbound	Allow	iSTAR Edge/Ultra/eX master port for incoming member connections.
28010	TCP	Inbound	Allow	iSTAR Edge/Ultra/eX communication
28016	TCP	Inbound	Allow	Host port for encrypted uploading SQLite personnel database file. Used for TLS 1.2 encryption mode.
28110	TCP	Inbound	Allow	iSTAR driver port for connection with iSTAR Edge G2 and iSTAR Ultra G2.
28104	TCP	Inbound	Allow	iSTAR driver fast download port for iSTAR Edge G2 and iSTAR Ultra G2.
28013	TCP	Inbound	Allow	iSTAR driver certificate sign request for iSTAR Edge G2 and iSTAR Ultra G2.
28116	TCP	Inbound	Allow	C•CURE upload personnel database from panel for use with the iSTAR Edge G2 and iSTAR Ultra G2. Used for TLS 1.3 encryption mode.
32200 – 38199	UDP	Outbound	Allow	Default VideoEdge UDP port range (for victor client connections).
33102	TCP	Inbound	Allow	C•CURE support communication with Innometriks High Assurance reader.

33103	TCP	Inbound	Allow	C•CURE support data downloads to Innometriks High Assurance reader.
33150	TCP	Inbound	Allow	C•CURE support transaction log from Innometriks High Assurance reader.

Table 1.6.1.15 - Other Components

Destination System	Port/ Range	Protocol	Direction	Initiator	Process/ Service	Description
Stratus everRun® Server	22	TCP	Inbound Listening	Stratus everRun® client	SSH Stratus everRun® Customer Support node access.	This port is open so that the Stratus redundancy solution support can access the system via a collaboration session during a support call.
Stratus everRun® Server	53	UDP	Inbound Listening	Stratus everRun® client	SSH/ Stratus everRun® Active Directory	Connection to the active directory for Stratus everRun redundancy solution.
Stratus everRun® Server	80	TCP	Inbound Listening	Stratus everRun® client	everRun® IIS	Stratus everRun® IIS port (required to be open) for Stratus redundancy solution.
American Dynamics VideoEdge© NVR	80	TCP	Inbound Listening	vAS, VideoEdge© Client	VideoEdge© NVR Admin/Alarm Port	VideoEdge© NVR Admin/Alarm Port.
Dedicated Micro Recorder	80	TCP	Inbound Listening	vAS	Dedicated Micro	Dedicated Micro video recorder
Bosch© Recorder	80	TCP	Inbound Listening	vAS	Bosch© Video	Bosch© video recorder
NTP server	123	UDP	Inbound Listening, Outbound	vAS/C•CURE Client	Network Time Protocol Synchronization.	For network time synchronization.
Stratus everRun® Server ArcServe® server	135	UDP	Inbound Listening	Stratus everRun® client ArcServe® client	ArcServe® RHA Control service server and the engine server	Used by: RHA for remote installer. Microsoft EPMAP (End Point Mapper) which is the DCE/RPC locator service used to remotely manage services like DHCP servers for Stratus® redundancy solutions.

Stratus everRun® Server ArcServe® server	137	UDP	Inbound Listening	Stratus everRun® client ArcServe® client	ArcServe® RHA Control service server and the engine server.	NetBIOS Name Service - Windows CIFS/SMB protocol family – used by RHA remote installer. This is for Stratus® redundancy solution.
Stratus everRun® Server ArcServe® server	138	UDP	Inbound Listening	Stratus everRun® client ArcServe® client	ArcServe® RHA Control service server and the engine server.	NetBIOS Datagram Service - Windows CIFS/SMB protocol family – used by RHA remote installer. This is for Stratus® redundancy solution.
LDAP Server	389	TCP	Inbound Listening	vAS, LDAP Clients	LDAP	LDAP which is used to synchronize C•CURE database with other databases (non-C•CURE) and facilitates other databases, such as human resources information databases, to download information.
Stratus everRun® Server	443	TCP	Inbound Listening	everRun® Web client	everRun® HTTPS Communications	HTTPS Port for SSL connections with C•CURE Go and Stratus everRun® communication. If IIS is installed on a different server, ensure this Inbound listening port is opened for the IIS server. This is for the Stratus® redundancy solution.
VideoEdge© NVR	554	TCP	Inbound Listening	vAS, VideoEdge © Client	RTSP stream	VideoEdge© NVR Live Port
ArcServe® server	1025	TCP	Inbound Listening	ArcServe® client	ArcServe® RHA control service center Windows DNS	Windows active directory port, RHA connects to AD to discover Windows domain

						configuration/settings and resources to be replicated (Exchange servers, DNS server, etc.).
Sur-Guard	1025	TCP	Inbound Listening	vAS	Sur-Guard	Sur-Guard communication
KONE Elevator	2004-2005	TCP	Inbound Listening	vAS	KONE Elevator	KONE Elevator
Stratus everRun® Server	2188-2189	TCP	Inbound Listening	Stratus everRun® client	everRun® quorum service computers and XenServer hosts	Stratus everRun® redundancy solution quorum service computers and XenServer hosts.
ASSA ABLOY DSR	2571	TCP	Inbound Listening	vAS	CrossFireAssaAbloyDriverService	ASSA ABLOY Lock communication to the DSR.
Commend Intercom server	3001	TCP	Inbound Listening	vAS	Commend Intercom server	Commend Intercom server
DSC PowerSeries	3072	TCP	Inbound Listening	vAS	ITV2	ITV2 – DSC PowerSeries Neo
American Dynamics Intellex Server	5000	TCP	Inbound Listening	vAS	Intellex Base	Intellex Base
American Dynamics Intellex Server	5001	TCP	Inbound Listening	vAS	Intellex Live	Intellex Live
American Dynamics Intellex Server	5003	TCP	Inbound Listening	vAS	Intellex Alarm	Intellex Alarm
Inner Range ISC	5000	TCP	Inbound Listening	vAS	ISC Controller communication	ISC Controller communication, alternative 6000 port. ISC is not supported in C•CURE 9000 v2.30 or later.
Inner Range ISC	5001	TCP	Inbound Listening	vAS	ISC Controller communication	ISC Controller communication, alternative 6001 port. ISC is not supported in C•CURE 9000 v2.30 or later.
TOA server	5001	TCP	Inbound Listening	vAS	TOA	TOA Intercom server
Inner Range ISC	5002	TCP	Inbound Listening	vAS	ISC Controller communication	ISC Controller communication, alternative 6002 port. ISC is not supported in

						C•CURE 9000 v2.30 or later.
Inner Range ISC	5003	TCP	Inbound Listening	vAS	ISC Controller communication	ISC Controller communication, alternative 6003 port. ISC is not supported in C•CURE 9000 v2.30 or later.
Inner Range ISC	5025	TCP	Inbound Listening	vAS	ISC Point Change Port	ISC Point Change Port. ISC is not supported in C•CURE 9000 v2.30 or later.
Inner Range ISC	5026	TCP	Inbound Listening	vAS	ISC Version Attendance Port	ISC Version Attendance Port. ISC is not supported in C•CURE 9000 v2.30 or later.
Mastermind System	5050	TCP	Inbound Listening	vAS	Mastermind	Mastermind Alarm Management
Stratus everRun® server	5900	TCP	Inbound Listening	Stratus everRun® client	VNC with Linux VMs	Stratus everRun® redundancy solution communication for failover/redundancy.
Bosch	7800	UDP	Inbound Listening	vAS	Bosch	Bosch receiver port
Bosch	7900	UDP	Inbound Listening	vAS	Bosch	Bosch receiver port
Matrix Recorder	8016	TCP	Inbound Listening	vAS	Matrix Video	Matrix video recorder
ThyssenKrupp Elevator	8038-8041	UDP	Inbound Listening	vAS	ThyssenKrupp Elevator	ThyssenKrupp Elevator
Identiv© 3VR Recorder	8080	TCP	Inbound Listening	vAS	Identiv© 3VR	3VR video recorder
Stratus everRun® server	8080-8081	TCP	Inbound Listening	everRun client	Stratus everRun® eAC	Stratus everRun® redundancy solution - eAC communication for failover/redundancy.
ASSA ABLOY DSR	9090	TCP	Inbound Listening	vAS	CrossFireAssaAbloyDriverService	Communication from C•CURE to DSR server.
Lantronix	10001-10002	TCP	Inbound Listening	DSC serial through Lantronix and Simplex 4100U serial through Lantronix	Serial	DSC serial through Lantronix and Simplex 4100U serial through Lantronix

Honeywell© Galaxy panel	10001 - 10002	TCP	Inbound Listening	vAS	Honeywell© Galaxy	Honeywell Galaxy Panel
HDVR	22609	TCP	Inbound Listening	vAS	HDVR Admin/Line/Alarm Port	HDVR Admin/Line/Alarm Port
Zettler® MZX	47808	UDP	Inbound Listening	vAS	Zettler® MZX	MZX fire detection integration
Otis Elevator	45303 45307 45308 46307 46308 47307	UDP	Inbound Listening	vAS	Otis Elevator	Otis Elevator
BACnet controller	47808	TCP	Inbound Listening	vAS	BACnet	BACnet Building Management
Elpas®	1001	TCP	Inbound Listening	vAS	Elpas®	Elpas® real time location
Schindler Elevator	4040, 5050	TCP	Inbound Listening	vAS	Schindler Elevator	Schindler Elevator
CEM Systems CDC Server	30000	TCP	Inbound Listening	vAS	CEM Systems	CEM Systems Access Control
EntraPass Server	8801	TCP	Inbound Listening	vAS	EntraPass	EntraPass Access Control

2 Deployment

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

2.1 Deployment overview

The contents in this section describe a typical deployment and how to harden the C•CURE 9000 system.

2.1.1 Physical installation considerations

To install the C•CURE 9000 software and iSTAR hardware refer to the installation guide.

Note: the physical access to the device and physical installation of the device can impact the cybersecurity.

Physical access to a component or device enables actions that cannot be authenticated and logged electronically through the capabilities of this product. To prevent unauthorized access, install the device in a room, cabinet or enclosure that can restrict access (for example, mechanical lock or physical access control). Use a tamper switch 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.

2.1.2 Knowledge level

The person responsible for hardening must be experience in C•CURE 9000 administration and networking technologies. Completion of the C•CURE 9000 basic and advance installation courses is recommended.

2.2 C•CURE 9000 System Hardening

While C•CURE has several secure-by-default safeguard, you must harden C•CURE to meet the security requirements of the target environment.

2.2.1 Hardening Checklist

- ☐ Hardening Step 1: Enable BIOS password
- ☐ Hardening Step 2: Disable USB Boot
- ☐ Hardening Step 3: Set Basic Authentication to false
- ☐ Hardening Step 4: Update your operating system
- ☐ Hardening Step 5: Disable unused ports
- ☐ Hardening Step 6: Disable unused features, services and software
- ☐ Hardening Step 7: Exclude files from end-point protection

- Hardening Step 8: Update iSTAR firmware
- Hardening Step 9: Disable iSTAR diagnostic webpage
- Hardening Step 10: Disable SNMP
- Hardening Step 11: Enable iSTAR dark mode
- Hardening Step 12: Update Firmware for the OSDP RM4E board
- Hardening Step 13: Enable the OSDP Tamper Switch
- Hardening Step 14: Disabling the Installation Mode
- Hardening Step 15: Enabling the OSDP Secure Channel
- Hardening Step 16: Enable MS SQL database encryption
- Hardening Step 17: Configure encrypted connection strings

2.2.2 BIOS hardening

Harden the BIOS to restrict unauthorized reconfiguration of the computer which could impact the operation of C•CURE 9000.

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

Note: BIOS menus can vary between versions and models of computers.

2.2.2.1 Enable BIOS password

Hardening Step 1: Enable BIOS password

Enable password protection of all Windows computers running C•CURE 9000 applications BIOS and set the password. This password should be known only to authorized administrators.

Change the BIOS password on the computer where you intend to install C•CURE 9000. To set a BIOS password follow your systems instructions.

2.2.2.2 Prevent USB boot

Hardening Step 2: Disable USB Boot

The boot sequence should prevent USB boot as it is a possible for USB devices to inject malicious code without warning. Change the setting in your BIOS if boot from USB is an option.

You can restrict booting from plug and play devices. The USB port is an important technical interface that would allow for a malicious user to upload corrupted files or download information.

2.2.3 User management

To harden the security of C•CURE 9000, it is best practice to only create Domain Users. Do not create Basic Users. Log on using Windows in a domain joined device.

To use Windows based authentication, a Windows domain server must be accessible from the target computer and the target computer must join that domain.

2.2.3.1 Configure Windows to log on to the domain

Execute the configuration of the Windows domain server and ensure that the target computer joins the domain according to Microsoft guidance.

2.2.3.2 Set Basic Authentication to false

Hardening Step 3: Set Basic Authentication to false

To set Basic Authentication to false, complete the following steps:

1. Open the C•CURE 9000 client application.
2. Click **System Variables**.
3. Navigate to **Allow Web Portal Basic Authentication** and select **False**.

2.2.3.3 Disable accounts on termination of employment

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

2.2.3.4 Remove inactive user accounts

If an employee did not use the system for a long duration, they may not have a need for a user account. If they do not need to use it, remove their account as it is best practice to reduce the number of active user accounts lowering the potential attack footprint.

2.2.3.5 Update user account roles and permissions

If an employee changes roles, you may need to update or remove their account permissions.

2.2.3.6 Recommended User Account Authorization Configurations

When installing C•CURE 9000, to avoid possible permission issues, it is best practice create a user that has access to a local or remote SQL database server. After installation ensure that you grant access only to necessary information or resources.

For example, to harden you can configure a different user account with least privileges to run C•CURE 9000 CrossFire Framework Services instead of the local system account.

The user account does not need sysadmin privileges in SQL server. The user must have a db_owner role for the following databases: ACVSCore, SWHSystem, SWHSystemAudit, SWHSystemJournal.

Configure C•CURE 9000 operators to have the least privileges based on their roles. For example, if an operator only monitors and acknowledges alarms, do not assign privileges to add, remove, or modify database

objects. Refer to the C•CURE 9000 manual for more information on how to configure different role and privileges for C•CURE operators.

2.3 Operating system updates

To date, the Software House Technical Support and Quality Assurance teams have not reported any conflicts or issues with C•CURE 9000 and Microsoft Windows Service Packs and security updates.

Software House is a Microsoft Certified Gold Partner. Qualification of all C•CURE 9000 releases, including service packs and critical updates, is performed using the latest Microsoft Windows Service Packs and security updates. Software House Technical Support can identify when new updates and patches are approved.

It is best practice to apply the latest Microsoft Windows updates. We recommend that you configure C•CURE to require a manual restart of the server to prevent automatic shut down during use.

Hardening Step 4: Update your operating system

Reviewing the current operating system against the most recent update available. Apply the update after testing on a non-production system and within a window which does not conflict with normal operations.

2.4 Communication hardening

Communication hardening limits an attacker's ability to gain access to C•CURE. Attackers look for weakness in communication protocols, and unauthenticated communications without encryption. To harden the communication interfaces and the transmission of data complete the following steps:

2.4.1 Configure communication ports

Hardening Step 5: Disable unused ports

To decide what ports to open refer to the C•CURE 9000 and iSTAR Port Assignments in section 1.6.1. Disable all unused ports. For example, if you no longer need to discover VideoEdge devices and are not using port 12354 for any other use, disable port 12345.

2.5 Disable unused features, services, and software

Hardening Step 6: Disable unused features, services, software

If you do not require optional features and services, disable them. This lowers the attack surface of C•CURE 9000. For example, if you do not need the SNMP for the iSTAR controller, disable it.

Remove Unused Software. Each C•CURE 9000 release uses specific versions of software to function. After an upgrade, it is possible that older versions of third-party dependencies (such as .NET) are no longer required and can be removed. See the table the below and 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 SQL data was properly migrated to the new SQL Server instance

Table 2.5.0.1

C•CURE 9000 3.00.3	Database support	.NET support
Standalone server series L, M, N, P	• SQL Server 2014 (SP3 or later) Express (64-bit) • SQL Server 2016 Express/Standard/Enterprise SP1 and higher (64-bit) • SQL Server 2017 Express (64-bit) • SQL Server 2019 Express/Standard/Enterprise (64-bit)	• .Net 6 and .Net 7
Standalone server series Q, R, R+, S, S+, T SAS server series L, M, N,	• SQL Server 2016 Standard & Enterprise SP1 and higher (64-bit) • SQL Server 2019 Standard & Enterprise (64-bit)	• .Net 6 and .Net 7
SAS server series Q, R, R+, S, S+, T MAS server	• SQL Server 2016 Standard/Enterprise SP1 and higher (64-bit) • SQL Server 2019 Standard & Enterprise (64-bit)	• .Net 6 and .Net 7

2.6 Configure end-point protection

Hardening Step 7: Exclude files from end-point protection

Anti-Virus/Anti-Malware software should apply the following exclusions for the C•CURE 9000 application server:

- The complete Tyco directory for example, `C:\Program Files (x86)\Tyco`
- The Microsoft SQL Server directory for example, `C:\Program Files\Microsoft SQL Server\MSSQL11.SQLEXPRESS\MSSQL\DATA`

These directory exclusions prevent a conflict when C•CURE 9000 reads or writes a file.

Note: No directory exclusions are necessary for C•CURE 9000 Client workstations. C•CURE 9000 systems are critical to operation. It is also important to disable any ability to force a restart of the C•CURE 9000 server or client workstations.

2.7 Hardening iSTAR controllers

While iSTAR has several secure-by-default safeguard, you must harden iSTAR to meet the security requirements of the target environment.

2.7.1 Firmware updates

Hardening Step 8: Update iSTAR firmware

A user with the correct permissions must perform firmware updates from the Monitoring Station, or iSTAR Diagnostic webpage (iSTAR Ultras, Edge G2, and Ultra G2). The firmware is downloaded to the controller, which continues to operate during the download process. When the controller receives the proper checksum, which validates the firmware, the controller restarts. When communication to the server is restored, the C•CURE 9000 server downloads the latest database to the controller.

Firmware updates to the iSTAR controllers are available on the Software House Support website: www.swhouse.com/Support. The site also contains the release notes that detail the changes made to the firmware, including security updates.

2.7.2 Disabling iSTAR diagnostic

Hardening Step 9: Disable iSTAR diagnostic webpage

You may use the iSTAR Diagnostic webpage to change network configuration and get diagnostic information. If you do not use this page, be sure to disable it. To disable iSTAR diagnostic complete the following steps:

1. Navigate to the C•CURE Administration Station.
2. Open the **Admin** window.
3. Open **iSTAR Dynamic View**.
4. Right-click the iSTAR controller.
5. Click **Disable Web Diagnostic**.

2.7.3 Disabling SNMP

Hardening Step 10: Disable SNMP

SNMP is enabled by default on iSTAR controllers to provide statistics of DoS attacks. For security purposes, the libraries are read-only and contain only the name of the controller. You can disable SNMP using ICU, or iSTAR Ultra webpage, or C•CURE9000 Admin window:

Figure 2.7.3.1: SNMP

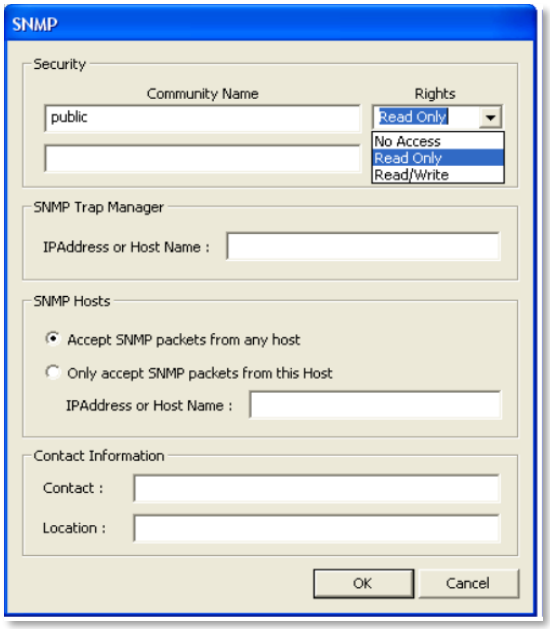
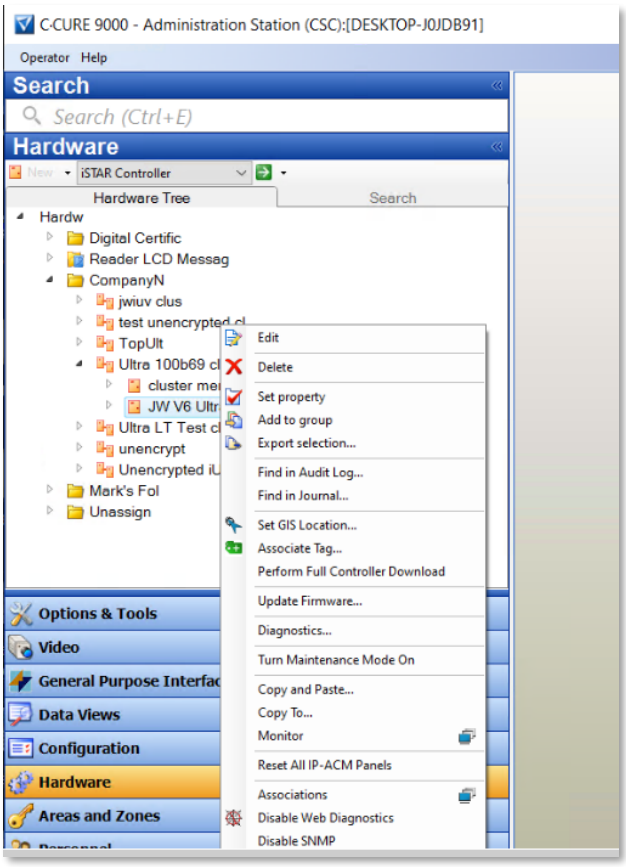


Figure 2.7.3.2: Administration station



2.7.4 Tamper detection

All iSTAR controllers include tamper detection that prompt an alarm if the enclosure opens. The iSTAR Ultra includes an optional installation of a back tamper that can detect if the controller is removed from the wall.

To enable the tamper detection, enable the Tamper input when you configure the iSTAR Ultra controller, then attach a C•CURE 9000 event to the tamper input trigger. When the controller is tampered the event activates to trigger appropriate action configured in the event.

2.7.5 Resetting factory default before connecting to a new C•CURE 9000 system

If a component or device was previously used as part of another installation or test environment, the unit should be reset to factory defaults before you use it in a new deployment. Refer to the device user manual for information on how to perform factory reset for the device.

2.8 Hardening the Communication Between C•CURE 9000 and iSTAR controllers

While C•CURE has several secure-by-default safeguard, you must harden C•CURE to meet the security requirements of the target environment.

2.8.1 Dark mode

This section describes the Dark Mode feature. Dark mode (besides requiring non-default certs) turns off the web diagnostic page, SNMP, and the local LCD on the controller. You can move to dark mode for the communication between iSTAR and C•CURE Server, and between iSTAR master to member.

FIPS or dark mode disables communication between the iSTAR Configuration Utility (ICU) and the iSTAR controller. When in FIPS-approved (dark mode), the iSTAR controllers disable all access except direct communications from C•CURE 9000. iSTAR controllers configured with a cluster password (through C•CURE 9000) require that you type your password before ICU can configure the controller. You can set all iSTAR controllers for ICU block. This prevents sending ICU commands to the controller. To troubleshoot the iSTAR controller use the diagnostic web page. The web server is password-protected. You can configure the password through a system variable in C•CURE 9000. You can disable the server either using C•CURE 9000 system variables or by placing the iSTAR into FIPS or dark mode. The encryption between C•CURE 9000 and the iSTAR Ultra and iSTAR Edge controllers has FIPS 140-2 and FIPS 197 validation. You can use host-based, controller-based, a third-party certificate or you can move to ECC asymmetric encryption.

Hardening Step 11: Enable iSTAR dark mode

To move to dark mode for iSTAR to C•CURE, complete the following step:

1. Edit the cluster and choose dark mode.

To move to ECC asymmetric encryption, complete the following step:

A. Navigate to the C•CURE Administration Station.
B. Click **Options and Tools.**
C. Click **Encryption Options**.
D. Select an encryption option. More menu tabs appear.
E. Click **Certificate Strength**.
F. Click the **Encryption** menu and select **ECC**.

2.8.2 iSTAR 256-bit AES encryption

C•CURE 9000 offers several encryption modes in the network communication with iSTAR controllers to secure the controller from potential network threats. The encryption setting applies to all iSTARs and IP-ACMv2s in the cluster.

When communicating, C•CURE 9000 and an iSTAR encrypted controller exchange a session key. Exchanging a session key requires a pair of public and private keys. A trusted entity signs the public key and generates the digital certificate from the public key. The trusted entity acts as a Certificate Authority (CA). When the CA signs the public key, the public key becomes the digital certificate. The Certificate Authority can be either a commercial service, such as VeriSign, or a locally installed CA service, for example, C•CURE 9000 or a Windows OS.

If you generate a pair of public and private keys for the CA itself, you can use the CA's own private key to sign its own public key, which then becomes a self-signed digital certificate. It is a common practice for a root CA to sign itself.

When configuring custom encryption, you must create the following:

- Certificate Authority
- Host Certificate
- Controller Certificates

Unless you specify the use of third-party certificates, C•CURE 9000 acts as the trusted entity. The system automatically generates the required certificates. You can modify the identifying information associated with each certificate, but you cannot generate the certificate manually. If you use third-party certificates, you must download each certificate from its source.

To configure encryption for an iSTAR cluster, see Appendix A.1.0 Steps for configuring encryption for iSTAR Cluster.

Default FIPS 197 256-bit AES Encryption

C•CURE 9000 offers the FIPS 197 256-bit AES encryption by default in communication with iSTAR controllers. This default encryption method is used at sites that require secure communications in the security system. UL evaluated the default 256-bit AES (FIPS-197) mode.

Enhanced FIPS 140-2 256-bit AES encryption

For sites that require additional and higher government regulation and security requirements, C•CURE 9000 offers the support of FIPS 140-2 256-bit encryption. This FIPS 140-2 encryption feature provide enhanced levels of encryption by allowing you to create or download custom digital certificates on either the C•CURE 9000 host or on iSTAR encrypted controllers. These certificates provide the public and private keys used to provide higher levels of communication encryption.

Encryption options

This section describes C•CURE 9000's encryption options. For more information refer to the C•CURE 9000 installation guide.

2.8.2.1 *Default encryption mode*

In Default Encryption Mode, C•CURE 9000 generates digital certificates internally. The C•CURE 9000 host sends the default host certificate to iSTAR encrypted controller. The iSTAR encrypted controller responds sending the default Controller certificate to the host. The controller also generates the session key. The session key is used for encryption of a single message or communication session.

2.8.2.2 *Controller based encryption mode*

Controller-based key management is the most secure of the three encryption modes available in C•CURE 9000. Software House recommends this mode if FIPS 140-2 is a requirement.

Controller-based encryption requires the intervention of an individual to manually approve the certificate by signing it at the C•CURE 9000 Monitoring Station. In this context, the individual is referred to as the Cryptographic Officer. You can configure a C•CURE 9000 system variable to allow the system to automatically

sign the certificate. In this instance, C•CURE 9000 serves as the Cryptographic Officer and no intervention by a system operator is required. For more information, see Updating System Variables for the iSTAR Driver.

When using Controller-based key management, C•CURE 9000 creates the host and CA certificates at the C•CURE 9000 host computer, and then directs the iSTAR encrypted controller to generate new public and private keys. The iSTAR encrypted controller responds by sending the public key back to the host for signature. Depending on system configuration, the key is signed at the C•CURE 9000 Monitoring station by a system operator acting as the Cryptographic Officer, or automatically signed by C•CURE 9000 (automatic signature is not recommended if there is any concern about unauthorized attempts to simulate an iSTAR controller). The host sends the signed controller certificate and the Certificate Authority (CA) certificate to the controller. Upon receipt of the certificates, the iSTAR encrypted controller restarts.

2.8.2.3 *Host based encryption mode*

Host-based key management is not as secure as controller-based key management because it transmits a private key. However, no operator intervention is required for certificate approval, and the system can use a third-party Certificate Authority.

When you use host-based key management, the system maintains all controller certificates on the host computer. Recovery from an error state may require exporting third party certificates from the host, and then physically transporting the certificates to the failing controller.

When operating in Host-based Key Management Mode, the system creates the Host, Controller, and CA certificates on the host computer, and then downloads the Controller Public key, the Controller Private key, and the CA certificate to iSTAR encrypted controller. When the download is complete, the iSTAR encrypted controller reboots.

2.8.2.4 *Certificate strength*

The certificate strength determines how the seed or key for the AES algorithm is created. Managing encryption keys allows you to manage how communication between the C•CURE 9000 host and iSTAR encrypted controllers is encrypted. C•CURE 9000 offers two certificate strengths:

RSA 1024
RSA 1024 is the default legacy certificate strength.

ECC
ECC is the stronger and preferred option, but it requires version 6.0.0.0 or greater iSTAR firmware.

Starting in firmware v6.6.5 and C•CURE 9000 v2.70 SP2, ECC certificates are supported on the IP-ACM v2 through the controller it is attached to.

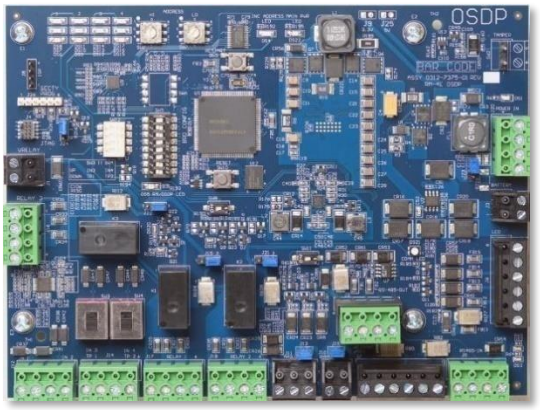
If you have ECC certificates configured from a previous version of C•CURE or firmware, you must regenerate the certificates after upgrading to firmware v6.6.5 and C•CURE 9000 v2.70 SP2. Otherwise, the ECC certificate will not download to the IP-ACM v2. See the iSTAR Configuration Utility User Guide for additional configuration information.

2.9 Hardening OSDP RM4E devices

Open Supervised Device Protocol (OSDP) RM4E boards provide encrypted bi-directional communication between iSTAR controllers and all access control hardware components on or connected to this board

(readers, inputs, outputs) via RS485 ports and OSDP protocol. This protocol is highly reliable and offers encrypted communication between the devices.

Figure 2.9.1 OSDP RM4E board



2.9.1 Firmware update

Hardening Step 12: Update Firmware for the OSDP RM4E board

Apply the latest security updates for OSDP RM4E boards. A user with the correct permissions must perform firmware updates from the Monitoring Station. OSDP RM4E firmware is downloaded to iSTAR controller. When the controller receives the OSDP RM4E firmware with proper checksum, it will then dispatch the firmware to ACM/IP-ACM boards to all connected OSDP RM4E boards. During this firmware downloading, each OSDP RM4E board will continue to operate until the downloading is completed. At this time, the OSDP RM4E board will reboot and then resume operations within a few seconds.

Firmware updates for OSDP RM4E are available on the Software House Support website:

www.swhouse.com/Support

2.9.2 Tamper switch

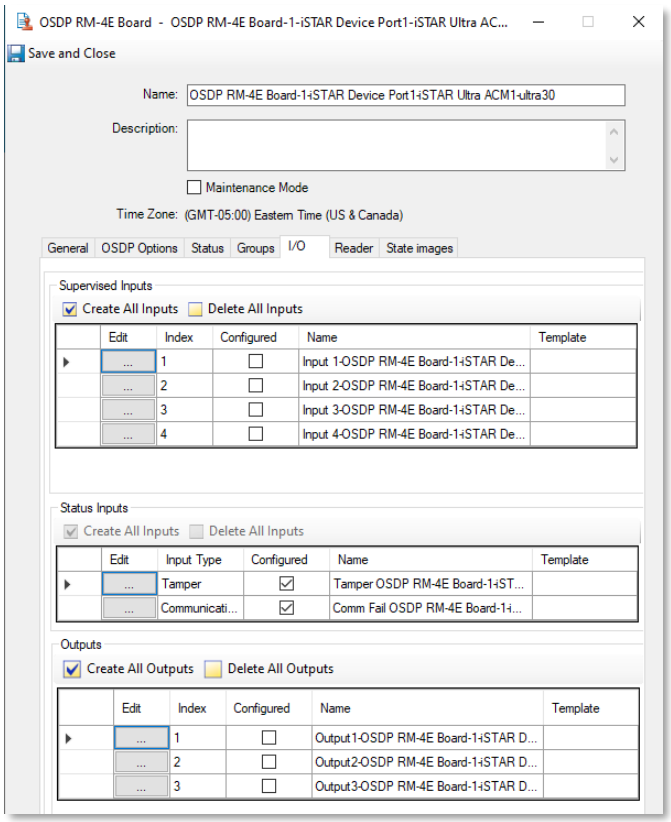
OSDP RM4E board provides a tamper switch as part of the enclosure. The switch is normally closed so that when the door is closed, no alarms are triggered. If the door is forced, the switch will open causing an alarm event.

Hardening Step 13: Enable the Tamper Switch

Configure the Tamper switch to the “On” setting.

To enable the tamper detection, enable the Tamper input when you configure the OSDP RM4E device, then attach a C•CURE 9000 event to the tamper input trigger. When the controller is tampered the event activates to trigger appropriate action configured in the event.

Figure 2.9.2.1 – OSDP RM4E board configuration



2.10 Hardening Communication between OSDP RM4E devices and iSTAR controllers

2.10.1 Use Short Temporary Cable to Connect to the iSTAR Controller During Initial Pairing Devices

During the initial pairing of OSDP RM4E devices with iSTAR controllers using the Installation Mode, new encryption keys are sent to the OSDP device after a secure channel session is started using the known Installer key. If an attacker happens to insert a listening device on the RS485 wiring, and then tamper the reader so that a new reader needs to be installed, and then listen in as the new reader gets the new keys, the attacker could impersonate that reader and steal badge numbers.

The OSDP standard recommends, and the researchers acknowledge, that the initial pairing of a device to a controller should happen using a short temporary cable connection to the controller. Once initialized, then the reader can be properly installed in the field, and the Keyset capture vulnerability will have been mitigated during the initial installation.

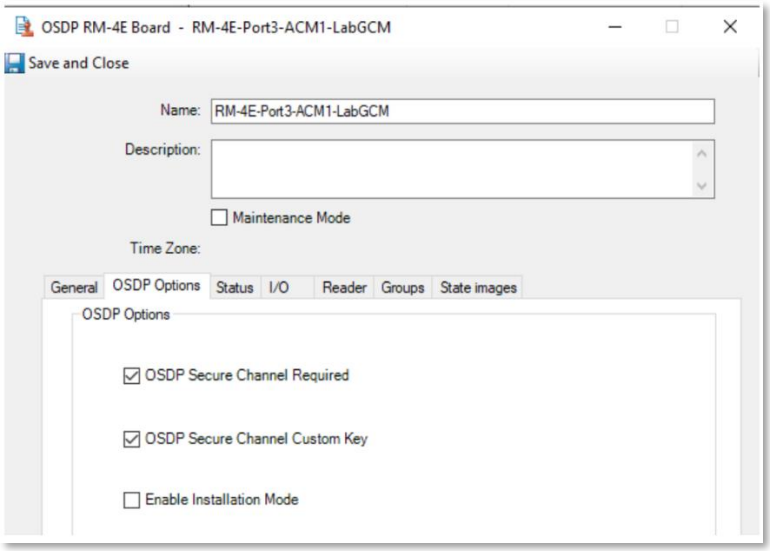
2.10.2 Disable OSDP Installation Mode after the device goes online

OSDP RM4E devices offer the OSDP Installation Mode feature. This helps to bring up OSDP device faster and easier by using a published encryption base key. If the Installation Mode is left on after the device has been brought online, attackers could impersonate a new device and ask for a new key, and possibly be able to come online. It is recommended to disable the OSDP Installation Mode after the device installation is done.

Hardening Step 14: Disabling the Installation mode

The OSDP Installation Mode can be enabled/disabled from the OSDP Options of OSDP RM4E editor screen:

Figure 2.10.2.1



2.10.3 Enable OSDP Secure Channel and Using OSDP Secure Channel Custom Key

For more secure, it is recommended to enable OSDP Secure Channel using custom key. This option can be enabled/disabled from the OSDP Options of OSDP RM4E editor screen. Once it is enabled, iSTAR controllers support using a unique, randomly generated AES-128 key for each OSDP device.

Hardening Step 15: Enabling the OSDP Secure Channel

It is also recommended to refresh the key periodically, to provide even further security, through a manual operator command, or, on a scheduled basis.

2.11 Database Stored in RAM Only

When you activate the **Database Stored in RAM Only** mode on the iSTAR Ultra the database is no longer stored in persistent memory.

Warning: Removing power from the device in this mode erases the database.

2.12 Hardening the Communication Between C•CURE 9000 Server and SQL Database Server

2.12.1 Deploy C•CURE with Microsoft SQL Enterprise

Install Microsoft SQL Enterprise according to Microsoft guidance and in alignment with the recommended settings outlined in the C•CURE 9000 installation guides.

2.12.2 Configure C•CURE Database Encryption

Hardening Step 16: Enable MS SQL database encryption

To protect the data-at-rest you must encrypt the C•CURE 9000 database. Microsoft SQL Enterprise databases supports encryption. To enable database encryption, complete the following steps from Microsoft:

https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/sql-server-encryption?view=sql-server-2017

2.12.3 Configure C•CURE Application Server with encrypted connection strings

Hardening Step 17: Configure encrypted connection strings

To configure the C•CURE Application Server with encrypted connection strings complete the following steps:

1. Open the C•CURE 9000 Server configuration application.
2. Click **Database**.
3. Select **Connection Strings Encrypted**.

2.12.4 Hardening recommendations for SQL on AWS – RDS:

When constructing RDS instances, secure ports in security groups using for RDS instances to only necessary ports such as SQL port 1433. You can also use existing encryption features of RDS to secure your data.

Please review guidance from Amazon Web Services (AWS)™ for more details.

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.html

https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingEncryption.html

2.13 Additional hardening recommendations for SQL Server

Please review the guidance from the Microsoft website

1. Should set the SQL server system's "Database Mail XPs" option to 0 to prevent Database Mail from starting
2. Ensure SQL Server is configured to use non-standard ports
3. Ensure 'Hide Instance' option is set to 'Yes' for Production SQL Server instances
4. Ensure 'Ad Hoc Distributed Queries' Server Configuration Option is set to '0'
5. Ensure 'CLR Enabled' Server Configuration Option is set to '0'
6. Ensure 'Ole Automation Procedures' Server Configuration Option is set to '0'
7. Ensure 'Remote Access' Server Configuration Option is set to '0'
8. Ensure 'Remote Admin Connections' Server Configuration Option is set to '0': The remote admin connections option controls whether a client application on a remote computer can use the Dedicated Administrator Connection (DAC).
9. Note: You can keep this option enabled only for failover clusters in Microsoft SQL Server
10. Ensure 'Trustworthy' database property is set to 'Off'
11. Ensure the 'sa' Login Account is set to 'Disabled'
12. Ensure 'xp_cmdshell' Server Configuration Option is set to '0'
13. Ensure the public role in the msdb database is not granted access to SQL Agent proxies
14. Ensure Latest SQL Server Service Packs and Hot fixes are Installed that are supported by C•CURE
15. Ensure 'MUST_CHANGE' Option is set to 'ON'4 for All SQL Authenticated Logins
16. Ensure the 'sa' login account has been renamed
17. Ensure 'CLR Assembly Permission Set' is set to 'SAFE_ACCESS' for All CLR Assemblies
18. Disable 'SQL Server Browser Service' if not required
19. Ensure 'Scan For Startup Procs' Server Configuration Option is set to '0'

20. Ensure 'CHECK_EXPIRATION' Option is set to 'ON' for All SQL Authenticated Logins Within the Sysadmin Role: Password expiry policy should be same for Windows and SQL Server
21. Ensure only the default permissions specified by Microsoft are granted to the public server role
22. Ensure 'Maximum number of error log files' is set to greater than or equal to '12'

2.14 Hardening the Communication Between C•CURE 9000 Server and clients

With transport level security the HTTPS protocol provides communication confidentiality and integrity protection. The main benefit of transport level security is performance. SSL implementations are widely used and tend to be highly optimized. SSL hardware accelerators further boosts performance. The disadvantage of transport level security is that it only provides point to point security over a network connection. As soon as the message is removed from the network the protection is lost. This is problematic in many scenarios where messages are routed through intermediate nodes or where messages are persisted in databases and other stores. In these scenarios we recommend End-to-End Message Level Encryption.

End-to-end encryption, encrypts and signs messages and authenticates the call through a windows account. End-to-end encryption protects the message. For example, end-to-end encryption may encrypt the entire message payload or the sensitive portions to ensure confidentiality. End-to-end encryption may also sign messages to prevent an attacker from modifying the message without detection by the recipient. The advantage of using message level security is that it protects the messages while traveling over the network, while routing through intermediary nodes, and while persisting the messages in databases. The disadvantage is performance as end-to-end encryption requires additional processing. You can improve performance by only encrypting sensitive parts of larger messages.

To enable end-to-end encryption, complete the following steps:

1. Open the C•CURE 9000 Server configuration application
2. Click **Settings**
3. Select **Enable End-to-End Message Level Encryption**

2.15 Hardening C•CURE 9000 Server/IIS Server, C•CURE IQ Portal, and C•CURE IQ web clients

The installer defaults to use HTTPS. It is strongly recommended not to switch to use HTTP due to security risk and HTTP may be deprecated in a future release.

It is also recommended to remove the HTTP Site Binding if you do not use HTTP. To remove HTTP Site Binding, complete the following steps:

1. Open the Internet Information Service (IIS) Manager
2. On the left menu, expand the Sites
3. Right-click on the Default Web Site and select Edit Bindings…
4. On the Site Bindings window, select http and click Remove

Use HTTPS to encrypt communication between C•CURE 9000 server/IIS server, C•CURE IQ Portal, and C•CURE IQ Web Clients. To enable the encryption for C•CURE Web communication complete the following steps:

1. Install the C•CURE web client according to the instructions in the installation guide
2. Select HTTPS as the protocol
3. To add a Server Certificate. Configure SSL for the IIS and create a self-signed certificate. For more information refer to chapter 1 of the C•CURE web installation guide.

Notes: It is also recommended to generate and use a strong-signed 3rd party certificate instead of the default self-signed certificate supplied by the installation. This default self-signed certificate only helps users to start using HTTPS and have a limited expiration time.

IIS Cookie settings. In IIS, ensure **cookie protection mode** is always set to encrypt and validate Forms Authentication cookies.

2.16 Hardening victor Web Service Server and C•CURE GoReader devices

C•CURE GoReader communicates with C•CURE 9000 server using victor Web Service. victor Web Service must have a verifiable and trusted server certificate signed by a globally trusted certification authority. Devices that run the GoReader application must have a trusted root certificate installed. This enables the client device to establish a secure connection and complete the transport layer security (TLS) handshake.

Note: the default selection on the GoReader app is SPP mode.

2.17 Hardening the Communication Between C•CURE 9000 Master Application Server and Satellite Application Servers Hardening Consideration

Windows Communication Foundation (WCF) is used for communications between C•CURE Master Application Server and Satellite Application Server. Use X.509 certificates to configure WCF to use TLS 1.2 or higher according to Microsoft guidance.

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 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 (Journal) 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*			✓				

3.1.1 Backup runtime data

Runtime data can be the most valuable assets 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 (Journal) data	Configure Backup / Restore runtime (Journal) 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	**Error! Reference source not found.**Backup device configuration data	Weekly

3.1.3 Test backup data

After competing steps 3.1.1 and 1.1.2, 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	Load data from backup media into a non-production system and test	Quarterly

3.1.4 Disable user accounts of terminated employees

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

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 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.

Check with your local policy to determine if this should be performed more frequently.

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

Note: Some systems have reports available which show

3.1.6 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 decrease 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 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 not 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-build 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-built 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 Operating 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, door controllers, readers, and I/O level 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 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 Linux, however some place significant load upon the system and may interfere with system performance. It is your responsibility to verify that the system continues to operate properly after you have installed any security monitoring tools.

Cybersecurity testing. Cybersecurity tests may be conducted on Johnson Controls solutions. We recommend that test are conducted in a non-production test environment to protect against disruption to operations.

A security test may produce field correctable findings if the steps outlined in this Hardening Guide are not followed.

Before conducting security tests, fully execute steps in the Hardening Guide. The following hardening steps, if not conducted, are known to result in addressable security findings:

- Update all components in scope to the most current supported version, including latest patches
    - All Johnson Controls' applications

    - All supporting Microsoft software, such as Windows, SQL Server, and .NET (see compatibility matrix, table 2.5.0.1)
- Remove components not required by the Johnson Controls applications (e.g. old versions of Microsoft .NET Core). See section 2.5 for additional information.
- Install PKI certificates for applicable interfaces that are either:
    - Provided by the local IT PKI administrator
    - Acquired from a public Certificate Authority (CA)

  Non-existent or self-signed PKI certificates will usually generate security findings.

If a test tool detects potential issues with a Johnson Controls component, you may share the results with Johnson Controls at this link - https://www.johnsoncontrols.com/cyber-solutions/security-advisories#ContactUs.

Potential false positives

Johnson Controls treats shared security reports seriously and can validate a finding or determine if a finding is not applicable to the Johnson Controls application. Scanners will use general knowledge from published CVEs to attempt to identity potential vulnerabilities within the system under test. The published CVEs may not apply to the product or present the same level of risk for all applications. If applicable, then the actual risk will vary depending on conditions such as the configuration, deployment environment and how a component was utilized in the code. For example, the vulnerability may exist in a sub-component that the Johnson Controls application does not distribute, or utilize, or has not been configured, or enabled for use.

Appendix A

This section contains detailed steps for configuring encryption for the iSTAR cluster.

Appendix A.1.0 Steps for configuring encryption for iSTAR Cluster

When communicating, C•CURE 9000 and an iSTAR encrypted controller exchange a session key. Exchanging a session key requires a pair of public and private keys. A trusted entity signs the public key and generates the digital certificate from the public key. The trusted entity acts as a Certificate Authority (CA). When the CA signs the public key, the public key becomes the digital certificate. The Certificate Authority can be either a commercial service, such as VeriSign, or a locally installed CA service, for example, C•CURE 9000 or a Windows OS.

If you generate a pair of public and private keys for the CA itself, you can use the CA's own private key to sign its own public key, which then becomes a self-signed digital certificate. It is a common practice for a root CA to sign itself.

When configuring custom encryption, you must create the following:

- Certificate Authority
- Host Certificate
- Controller Certificates

Unless you specify the use of third-party certificates, C•CURE 9000 acts as the trusted entity. The system automatically generates the required certificates. You can modify the identifying information associated with each certificate, but you cannot generate the certificate manually. If you use third-party certificates, you must download each certificate from its source.

Use this section to configure certificates including host-based, or controller based, third party certificates, and ECC.

Appendix A.1.1 Configuring FIPS 140-2 Encryption for an iSTAR Encrypted Cluster

To configure FIPS 140-2 encryption for an iSTAR encrypted cluster, complete the following tasks:

1. Click the **Options and Tools** pane.
2. Click **Encryption Options** to open the dialog box.
3. Select from the following options:
    a. **Controller-Based Encryption Mode** modifies the system-wide Key Management Policy to Custom - Controller supplied. The controller supplies public and private keys, and the host signs public keys.
    b. **Host-Based Encryption Mode** modifies the system-wide Key Management Policy to Custom - Host supplied.
    c. **Default Encryption Mode** is where the Host supplies all public and private keys.

Note: To use FIPS 140-2 mode, we recommend that you use the Controller-Based Encryption Mode for two reasons:

- Host-based Encryption requires a private key to be transmitted to the controllers non-encrypted. Controller-based Encryption does not. The trade-off is that the controller-based method requires a signature at the host that recognizes the iSTAR to be valid.
- The second reason is that it is much easier to recover from a controller-based error situation than to recover from a host-based area. Host based recovery of encryption keys is more difficult.

4. Click the **Hardware** pane.
5. In the **Hardware** tree double-click the iSTAR Cluster.
6. In the iSTAR Cluster dialog box, click the **Encryption** tab.
7. Select from the following options:
    a. Non-FIPS 140-2 or FIPS 140-2
    b. Validate mode for iSTAR Ultra, iSTAR Edge, iSTAR eX, and IP-ACM.
8. Navigate to the **Triggers** tab or click **Save and Close**.

Note: FIPS 140-2 compliant mode is not evaluated by UL.

Appendix A.1.2 Creating a digital certificate for a certificate authority

The Creating the Digital Certificate for the Certificate Authority section is not evaluated by UL and cannot be used in UL applications.

Configuring custom encryption requires a digital certificate for the Certificate Authority. C•CURE 9000 can serve as a trusted entity to generate a digital certificate for the Certificate Authority. In this case, the system automatically generates a new root certificate.

First you must select a custom encryption key management mode. For details, refer to the C•CURE System Maintenance Guide.

1. In the Administration Station, on the **Options and Tools** pane, select **Encryption Options**.
2. Click **Certificate Authority**.
    - When a custom CA root certificate does not exist, the system selects the **Create New Root Certificate** check box and displays the selection as read-only.
    - The system populates the **Certificate Name**, **Country Code**, and **Expiration Date** fields. You can modify these system-supplied values as required. All other fields in the Certificate Details section are editable, but optional.
3. Click **Save and Close**. The certificate is generated with the values provided by the system.

After generating the CA certificate, the system populates the fields in the Certificate Lifetime section, as follows:

Certificate created on: The day and date when the certificate was created.

Certificate expires on: The day and date the certificate expires.

Both fields are read-only. These fields are blank until a CA certificate is generated in the system.

Appendix A.1.2.1 Creating the digital certificate for the controller

To create the digital certificate for the controller, complete the following steps:

1. In the Administration Station, on the **Options and Tools** pane, select **Encryption Options**.
2. Select the **Controller** tab.

When a custom controller certificate does not exist, the system selects the **Create New Controller Certificate** check box and displays the selection as read-only. The system populates the **Certificate Name**, **Country**

Code, and **Expiration Date** fields. You can modify these system-supplied values. You can edit all other fields in the certificate details section.

3. Navigate to **Certificate Creation** and do one of the following:
    - To apply the new certificate to all iSTAR encrypted controllers in the system, select **Apply to All Controllers**.
    - To apply the new certificate to a specific iSTAR encrypted controller, in the **Apply to Single Controller** field, browse to locate, and select the controller.
4. Click **Save and Close**.

The certificate is generated with the values the system provides. After generating the controller certificate, the system populates the fields in the Certificate Lifetime section, as follows:

Certificate created on: The day and date when the certificate was created.

Certificate expires on: The day and date the certificate expires.

Both fields are read-only. These fields are blank until a controller certificate is generated in the system.

Appendix A.1.2.2 Creating the digital certificate for the host

The Creating the Digital Certificate for the host section is not evaluated by UL and cannot be used in UL applications.

Configuring custom encryption requires a digital certificate for the host. C•CURE 9000 can serve as a trusted entity to generate a digital certificate for the host. In this case, the system automatically generates a host certificate.

First you must select a custom encryption mode. For details, refer to the C•CURE System Maintenance Guide. To create a digital certificate for the host, complete the following steps:

1. In the Administration Station, on the **Options and Tools** pane, click **Encryption Options**.
2. Click **Host**.

When a custom host certificate does not exist, the system selects the **Create New Host Certificate** box, and displays the selection as read-only. The system populates the **Certificate Name**, **Country Code**, and **Expiration Date** fields. You can modify these system-supplied values. You can edit all other fields in the certificate details section.

3. Click **Save and Close**.

The certificate is generated with the values provided by the system. After the controller certificate is generated, the system populates the fields in the Certificate Lifetime section, as follows:

Certificate created on: The day and date when the certificate was created.

Certificate expires on: The day and date the certificate expires.

Both fields are read-only. These fields are blank until a host certificate is generated in the system.

Appendix A.1.2.3 Custom encryption using third-party certificates

The custom encryption using third-party certificates section is not evaluated by UL and cannot be used in UL applications.

Although C•CURE 9000 can serve as a trusted entity to create custom digital certificates, you have the option to use certificates from commercial trusted entities. If you choose to use third-party certificates when configuring custom encryption, you must download certificates for the Certificate Authority, Controller, and Host to C•CURE 9000.

Note: The iSTAR Pro controller does not support the use of third-party certificates.

Appendix A.1.2.4 Downloading the digital certificate for the certificate authority

Configuring custom encryption requires a digital certificate for the Certificate Authority. You can use certificates from a trusted third-party certificate supplier. You must download the certificate from the trusted source and import the CA public key, a `.PEM` file, and import it into C•CURE 9000. Use the Encryption Options function to load the certificate into the C•CURE 9000 database and configure custom encryption key management.

First select a custom encryption key management mode and specify the use of third-party certificates. For details, refer to the C•CURE System Maintenance Guide.

To load the digital certificate for the certificate authority, complete the following steps:

1. In the Administration Station, on the **Options and Tools** pane, select **Encryption Options**.
2. Select the **Controller** tab.

If you specified the use of third-party certificates, In the Certificate Creation section, the system selects **Load New Controller Certificate**, and displays the selection as read-only.

3. In the **File** field, browse to find the public key. The public key is identifiable as a .PEM file.
4. In the **Certificate Details** section, enter information that identifies and describes the third-party certificate.

The **Certificate Name**, **Country Code**, and **Expiration Date** fields are required fields. You can edit all other fields in the certificate details section.

5. Click **Save and Close**.

The digital certificate for the Certificate Authority uses the values provided by the third-party certificate.

After the CA certificate is loaded, the system populates the fields in the Certificate Lifetime section, as follows:

Certificate created on: The day and date when the certificate was created.

Certificate expires on: The day and date the certificate expires.

Both fields are read-only. These fields are blank until a CA certificate is loaded into the system.

Appendix A.1.2.5 Downloading the digital certificate for the controller

Configuring custom encryption requires a digital certificate for iSTAR encrypted controllers operating in dark mode. However, you can operate using custom controller key management mode and not necessarily go dark. You can use one certificate for all controllers in dark mode or create certificates for individual controllers. You can use certificates from a trusted third-party certificate supplier. You must download the certificates from the trusted source. Use the Encryption Options function to load them into the C•CURE 9000 database and configure custom encryption.

First select a custom encryption key management mode and specify the use of third-party certificates. For details, refer to the C•CURE System Maintenance Guide.

To load the digital certificate for the controllers

1. In the Administration Station, on the **Options and Tools** pane, select **Encryption Options**.
2. Select the **Controller** tab.

The Third-Party Certificates section lists available iSTAR encrypted controllers. For each controller, you can select a third-party certificate file and a private key.

3. For each controller that you want to configure in dark mode, do the following:
    a. In the **Certificate File to Load** field, browse to find the public key. The public key is identifiable as a `.PEM` file.
    b. In the **Private Key File** field, browse to find a private key that you want to use. The private key is identifiable as a `.KEY` file.
4. Click **Save and Close**.

The digital certificates for the various controllers use the values provided by the third-party certificates. After one or more certificates are loaded, the system populates the fields in the Certificate Lifetime section, as follows:

Certificate created on: The day and date when the certificate was created.

Certificate expires on: The day and date the certificate expires.

Both fields are read-only. These fields are blank until a controller certificate is loaded into the system.

Appendix A.1.2.6 Downloading the digital certificate for the host

Configuring custom encryption requires a digital certificate for the host. You can use certificates from a trusted third-party certificate supplier. You must download the certificates from the trusted source. Use the Encryption Options function to load them into the C•CURE 9000 database and configure custom encryption.

First select a custom encryption mode and specify the use of third-party certificates. For details, refer to the C•CURE System Maintenance Guide.

To load the digital certificate for the host, complete the following steps:

1. In the Administration Station, on the **Options and Tools** pane, click **Encryption Options**.
2. Click **Host**.

If you specified the use of third-party certificates, In the Certificate Creation section, the system selects **Load New Controller Certificate**, and displays the selection as read-only.

3. In the **Certificate File to Load** field, browse to find the public key. The public key is identifiable as a `.PEM` file.
4. In the **Private Key File** field, browse to find a private key that you want to use. The private key is identifiable as a `.KEY` file.
5. In the **Certificate Details** section, type the information that identifies and describes the third-party certificate.

The **Certificate Name**, **Country Code**, and **Expiration Date** fields are required fields. All other fields in the Certificate Details section are editable, but optional.

6. Click **Save and Close**.

The digital certificate for the host uses the values provided by the third-party certificate.

After the host certificate is loaded, the system populates the fields in the Certificate Lifetime section, as follows:

Certificate created on: The day and date when the certificate was created.

Certificate expires on: The day and date the certificate expires.

Both fields are read-only. These fields are blank until a host certificate is loaded into the system.