tyco | Software House

C•CURE 9000 v2.9 Hardening Guide

GPS0003-CE-20202905-EN
Rev A

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.

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 guaranty 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

Use this section to plan your deployment.

1.1.0 C•CURE 9000 overview

Software House C•CURE 9000 is one of the industry's most powerful and flexible security management systems. You can monitor events, manage personnel, create reports, display dynamic views, monitor system activity, view video and manage visitors anywhere in the world directly from your PC with the full C•CURE client, the web client or on the move with C•CURE Go mobile app. C•CURE 9000 provides the ultimate in scalability from a single standalone server supporting up to 5,000 readers and 500,000 credentials to an advanced distributed enterprise architecture that supports a master and up to 40 satellite application servers. Whether your organization consists of one facility with a few doors or many that span the globe, this solution scales as your company grows. C•CURE 9000 brings you over 150 integrated solutions including video, intrusion, intercom, fire alarm management, and PSIM. The integrations are thoroughly tested and delivered to you 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.

1.1.1 Deployment architecture

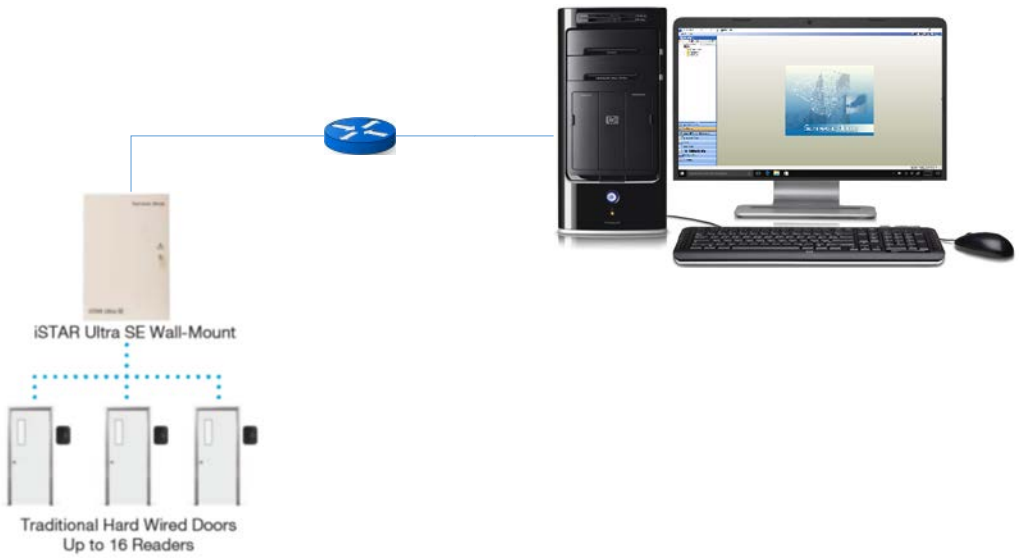

Figure 1: Standalone System

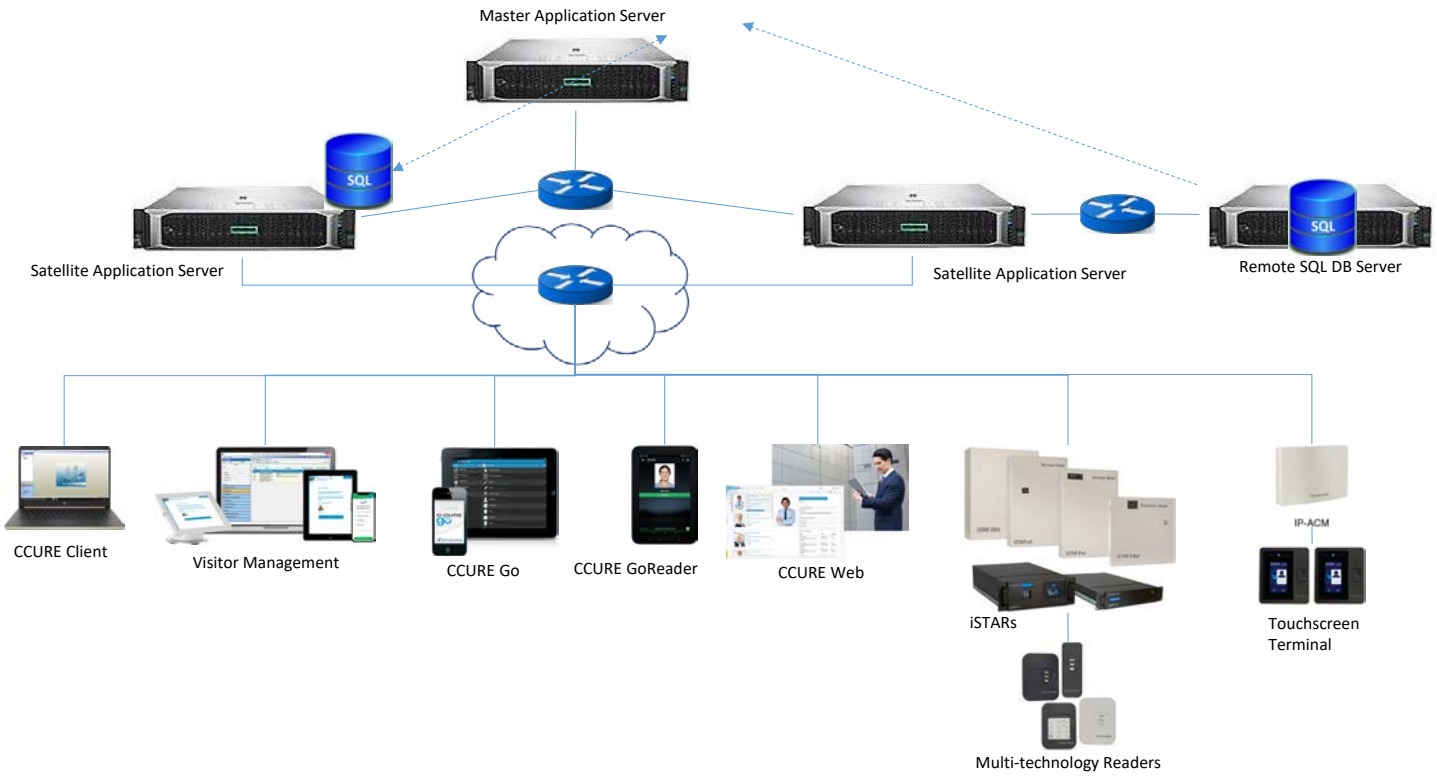

Figure 2: Enterprise System

1.2.0 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: User authentication and authorization features

Feature	Description
No backdoor passwords	C•CURE 9000 does not have a backdoor password.
Hidden password entry	When a user types a password it 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	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 time you log on.
Password rules	The local Microsoft Windows operating system or the domain controller manages policies such as predefined number of log on 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.
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. Upon logging on to Windows you are automatically logged on to the Administration and Monitoring Stations.
Single-use password	When the iSTAR controller boots for the first time it prompts you to change the password before you can proceed to any other screens.
Role Based Access Control (RBAC) authorizations	C•CURE 9000 offers role Based Access Control (RBAC) authorizations. You can define roles 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.

1.2.2 Data encryption

This section describes data in transit and data at rest.

Table 2: Data in transit

Description	Connection type	Encryption
Communication between iSTAR Edge 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
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 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/TLS1.2)
Communication between the C•CURE application server and C•CURE Database SQL Server	TCP/IP	Standard Microsoft SQL Encryption (TLS1.2). 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 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.

Table 3: Data at rest

Description	Encryption
iSTAR Edge 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	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 Theft Protection CPNI mode. When you enable customer proprietary network information (CPNI) mode the database of the iSTAR Ultra is no longer stored in persistent memory. In this mode, if you remove power from the controller, the database is erased.

1.2.3 Transaction and activity tracking

This section describes transaction and activity tracking.

Table 4: Transation and activity tracking

Feature	Description
Audit log	The audit log is a history of changes to C•CURE 9000 configurations. You can also enable field level auditing.
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 you can back up at any time using the System Backup feature.

- The Core database is a core 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 in C•CURE 9000.
- 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 the Core, Audit Log or Activity Journal database, you can restore one or more of these databases 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 you can 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 of time, the ports reopen, but if the unusual traffic is still present, it repeats the process, going offline for a longer period of time. 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 3: Alert

2 Deploying and Hardening the C•CURE 9000 System

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.

2.1.0 Deployment overview

The contents in this section describe a typical deployment.

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.

2.2.0 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 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.

2.2.1.1 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 intent to install C•CURE 9000. To set a BIOS password follow your systems instructions.

2.2.1.2 Prevent USB boot

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

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.

2.2.2 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.

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

2.2.2.1 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.

2.2.2.2 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**.

2.2.2.3 Disable accounts on termination of employment

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

2.2.2.4 Remove inactive user accounts

If an employee did not use the system for a long period 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.

2.2.2.5 Update user account roles and permissions

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

2.2.2.6 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.

2.3.0 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.

2.4.0 Service packs and critical updates

It is best practice to apply the latest C•CURE 9000 service packs and critical updates to get the latest security fixes for your system.

When we discover a critical security vulnerability we use commercially reasonable efforts to:

- Issue a critical service pack for the current version of the product as soon as is reasonably practicable
- Subsequently issue a 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 low-medium vulnerabilities in the next major release

2.5.0 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:

2.5.1 Configure communication ports

To decide what ports to open refer to the C•CURE 9000 and iSTAR Port Assignments document. Disable all unused ports. For example, if you do not need the SNMP feature, disable UDP port 161 for SNMP.

2.6.0 Disable unused features and services

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.

2.7.0 Configure 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.

3 Hardening iSTAR controllers

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

3.1.0 Firmware updates

A user with the correct permissions must perform firmware updates from the Monitoring Station, or iSTAR Diagnostic webpage (iSTAR Ultras and Edge 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.

3.2.0 Disabling iSTAR diagnostic

You can use the iSTAR Diagnostic webpage to change network configuration and get diagnostic information. If you do not use it 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**.

3.3.0 Disabling SNMP

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

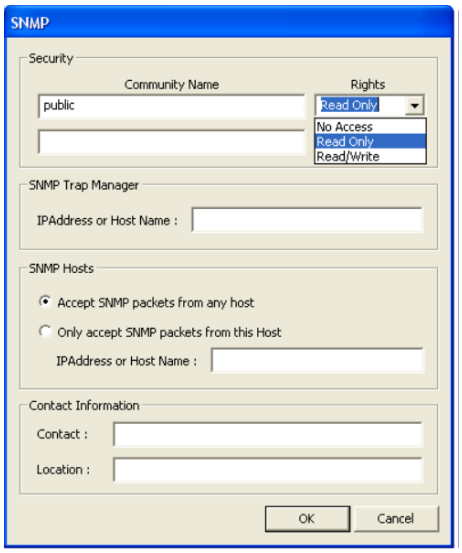

Figure 4: SNMP

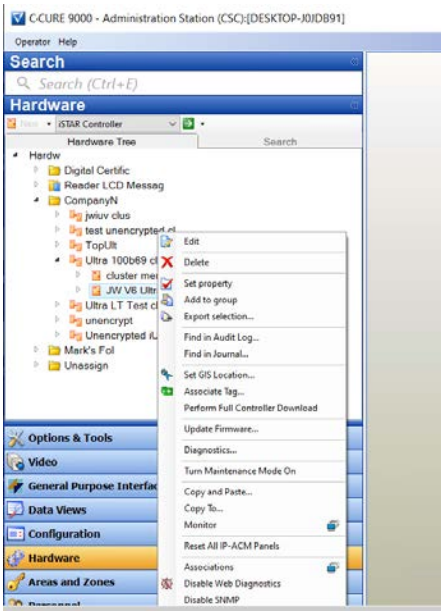

Figure 5: Administration station

3.4.0 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.

3.5.0 Resetting factory default before connect 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.

4 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.

4.1.0 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.

When in FIPS-approved (dark mode), the iSTAR controllers disable all access except direct communications from C•CURE 9000. FIPS or dark mode disables communication between the ICU and the iSTAR controller. 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.

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**.

4.2.0 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 Configuring encryption for iSTAR Cluster.

4.2.1 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.

4.2.2 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.

4.2.3 Encryption options

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

4.2.3.1 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.

4.2.3.2 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.

4.2.3.3 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.

4.2.3.4 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 more preferable 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.

4.3.0 CPNI – Data privacy management

When you activate the CPNI mode on the iSTAR Ultra the database is no longer stored in persistent memory.

Warning: Removing power from the database in CPNI mode erases the database.

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

5.1.0 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.

5.2.0 Configure C•CURE Database Encryption

In order 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

5.3.0 Configure C•CURE Application Server with 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**.

6 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**.

7 Hardening C•CURE 9000 Server/IIS Server and C•CURE web clients

Use HTTPS to encrypt communication between C•CURE 9000 server/IIS server and C•CURE 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.

8 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.

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

We use WCF for communications between CCURE Master Application Server and Satellite Application Server. Microsoft allows end users to configure WCF with Transport Security using a X.509 Certificate.

The encryption level is also depended on the operating system. For example, Microsoft documents TLS 1.2 is supported on Windows Server 2019.

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.