tyco | Software House

C•CURE IQ Server

Hardening Guide

GPS0036-CE-EN
Version 3.00.2
Rev B
Revised 2023-12-12

Johnson Controls

Introduction

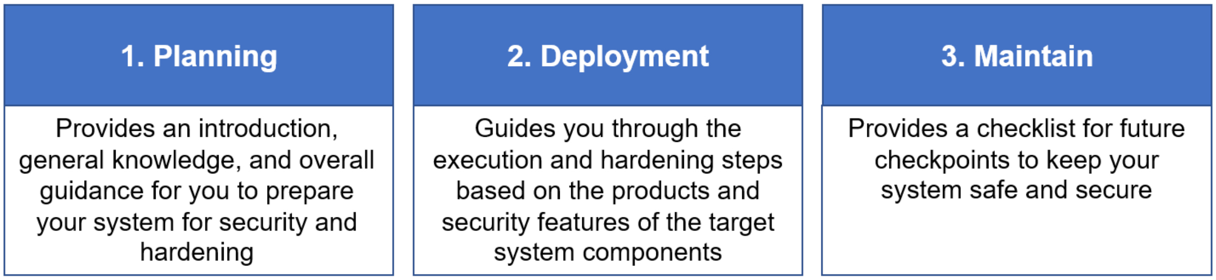
C•CURE IQ Server provides peace of mind to our customers with a holistic cyber mind set beginning at initial design concept, continuing through product development, and is supported through deployment, including a rapid incident response to meet the comprehensive and evolving cybersecurity environments.

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

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

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

This **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 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 resulting of, or despite, reliance on this guide or compliance with any cybersecurity practices or recommendations set forth herein.

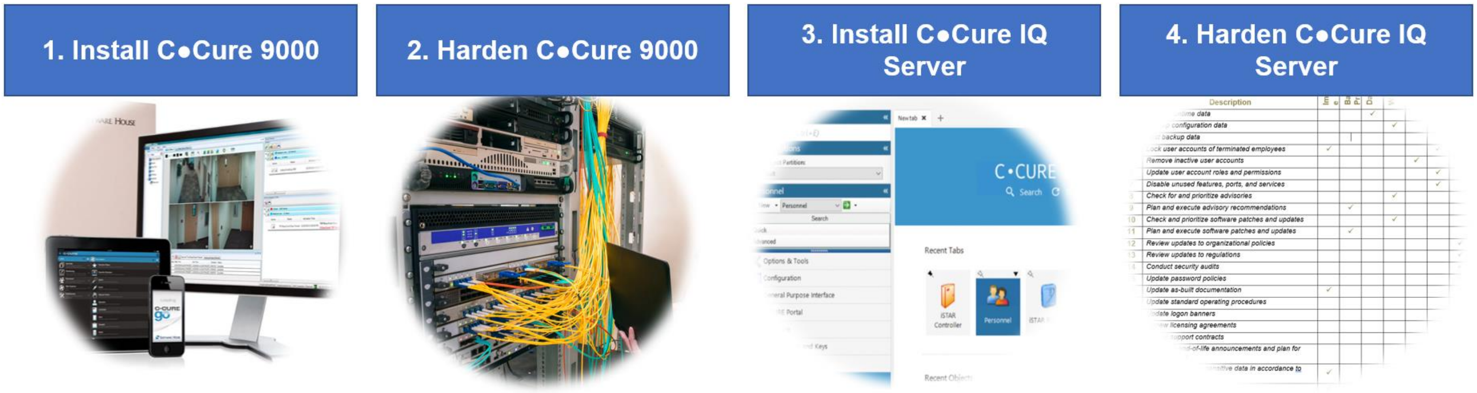
Contents

1.0 Planning

C•CURE IQ Server is an extension to the C•CURE 9000 product line. This section helps plan for the implementation of security best practices for a C•CURE IQ Server system installation.

Features covered in the C•CURE 9000 product line, iSTAR Controllers and related hardening steps will not be covered in this guide. For this and additional related information, see the C•CURE 9000 Hardening guide.

Note: Before going through this C•CURE IQ Server hardening guide, first complete steps 1 through 3 below; Installation of C•CURE 9000, hardening of C•CURE 9000 and installation of C•CURE IQ Server.



This hardening guide is designed to start at step 4 – Harden C•CURE IQ Server.

1.1.0 C•CURE IQ Server overview

The C•CURE IQ Server platform is based on a containerized architecture to incorporate the latest technologies for improved security and expanded deployment options while shortening the time it takes to bring updates to market. With the containerized architecture, C•CURE IQ Server leverages the latest containerization solutions for managing the lifecycle, packaging, and monitoring of its applications.

It is built to run in multiple on-premises deployment scenarios, including offline (air-gapped) and online environments.

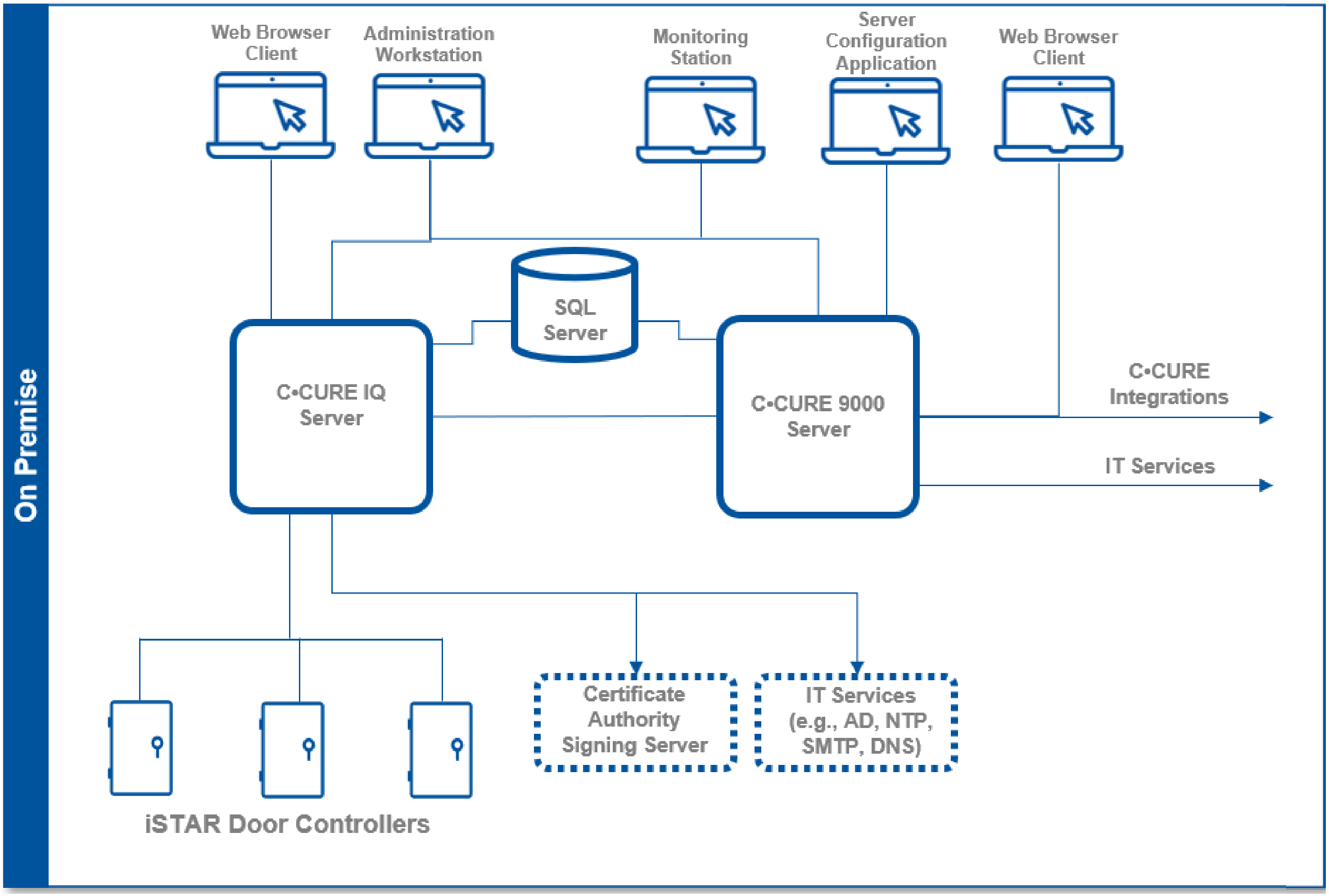
C•CURE IQ Server is a licensable add-on to C•CURE 9000 allowing for scaling across larger deployments, handling access control. For example, customers can easily scale to more iSTAR door controllers (see the C•CURE IQ Server Installation Guide for additional details).

The C•CURE IQ Server solution does not require:

- upgrading of standalone application server to an enterprise deployment.
- increasing Satellite Application Server (SAS) instances if an enterprise deployment already exists.

1.1.1 Deployment architecture

Figure 1.1.1.1: Standalone System connected to C•CURE IQ Server.



Note: Devices such as Readers are not shown in figure 1.1.1.1

C•CURE IQ Server 3.00.2 is deployed as a single Linux server attached to the existing C•CURE 9000 and iSTAR Door Controllers as shown.

1.2.0 Security feature set

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

Table 1.2.0 – Security features

Section	Type	Feature name
1.2.1	User authentication and authorization	No backdoor passwords Hidden password entry No hardcoded password Encrypted passwords User account password policy Password rules with a supported third-party Third party Identity Provider Integration Centralized authentication system Maximum log on attempts Operator Auto Log Off Segregation of duties
1.2.2	Data encryption	Data encrypted in Transit Data encrypted at Rest
1.2.3	Secure communications	TLS 1.3
1.2.4	Digital certificate management	Support for C•CURE IQ Server digital certificates
1.2.5	Audit logs	Secure container logs
1.2.6	Automated hardening	Hardening enabled by default

1.2.1 User authentication and authorization

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

Table 1.2.1: User authentication and authorization features

Feature	Description
No backdoor passwords	C•CURE IQ Server does not have a backdoor password.
Hidden password entry	All typed passwords are hidden from view.
No hardcoded password	No hard-coded passwords/credential used in C•CURE IQ Server code, configuration, and log files.
Encrypted passwords	The C•CURE IQ Server database contains encrypted credential passwords. The jump host used to setup C•CURE IQ Server also contains encrypted passwords to allow for saving passwords during the update process without compromising security.
User account password policy	C•CURE IQ Server contains rules which govern password formation, expiration, reuse, and other restrictions including password length, history, and complexity.
Password rules with a	C•CURE IQ Server has the option to delegate to a supported third-party identity provider (e.g., Microsoft Active Directory) which would delegate password policies. Features such as

supported third-party	predefined number of logon attempts, character length, use of alphanumeric characters, and user-defined lockouts are all configurable through this provider.
Third party Identity Provider Integration	C•CURE IQ Server has the option to delegate to a supported third-party identity provider such as Microsoft Active Directory (AD). This feature allows single sign-on (SSO) with your corporate Identity Management System (IDMS).
Centralized authentication system	C•CURE IQ Server uses a centralized, operator authentication system.
Maximum log on attempts	The authentication system restricts the user to the configured number of consecutive authentication attempts allowed before that account is locked from further authentication retries.
Operator Auto Log Off	Operators inactive longer that the inactivity time limit (default 1 hour) will be automatically logged out.
Segregation of duties	Administrative users for back-end functions are managed separately from operators.

1.2.2 Data encryption

This section describes data in transit and data at rest.

Table 1.2.2.1: Data encrypted in transit

Description of the communication path	App Layer	Connection type	Encryption
Communication between victor Application Server and RabbitMQ in C•CURE IQ Server	AMQP	TCP/IP	TLS1.3 with 256-bit AES-GCM Encryption (TLS_AES_256_GCM_SHA384)
Communication between the C•CURE client workstation and RabbitMQ in C•CURE IQ Server	AMQP	TCP/IP	TLS1.3 with 256-bit AES-GCM Encryption (TLS_AES_256_GCM_SHA384)
Communication between a web browser and ingress termination point in the C•CURE IQ Server cluster	HTTP	TCP/IP	TLS1.3 with 256-bit AES-GCM Encryption (TLS_AES_256_GCM_SHA384)
Communication between C•CURE IQ Server and victor Application Server	WCF	TCP/IP	RSA encryption with 1024-bit keys
Communication between the C•CURE IQ Server and SQL Server Database	SQL	TCP/IP	Microsoft SQL Server Encryption (TLS1.3 for SQL Server 2023 and TLS1.2 for earlier versions with appropriate Windows updates)
Communication from cert-manager in C•CURE IQ Server to the ACME server	HTTP	TCP/IP	TLS1.x, exact version depends on the configuration of the ACME server.

Communication from iSTAR door controller to C•CURE IQ Server	Binary	TCP/IP	TLS1.3 with 256-bit AES Encryption
Communication from tools on jump host (kubectl, helm, setup.sh) to Kubernetes API Server	HTTP	TCP/IP	TLS1.3 with 256-bit AES Encryption

Table 1.2.2.2: Data encrypted at rest

Feature	Description
Setup password protection	The passwords are protected at rest using AES 256-bit encryption and stored within a vault.
Secrets, certificates, and Keys protection	The secrets, certificates and keys are protected at rest using AES 256-bit encryption and stored within a vault.
Key Rotation	Key rotation is supported.
Basic authentication password protection	Basic authentication passwords are stored at rest with a salted hash using SHA-384.
iSTAR Passwords Encrypted by the passphrase	The iSTAR controller passwords, stored by the iSTAR Personnel service, are encrypted via the C•CURE 9000 Encryption Key Passphrase which is the passphrase initially configured in C•CURE 9000 and re-entered in C•CURE IQ Server during setup. See the C•CURE 9000 Hardening Guide for more information on the algorithm used.

1.2.3 Secure communications

All communications into C•CURE IQ Server are secured by TLS 1.3.

Red Hat Enterprise Linux 7 (RHEL) provides “firewalld” which is enabled by our installation with only the necessary inbound ports opened.

Outbound communications, to the extent possible, are secured by the highest TLS version possible, based on what is supported by the external server.

1.2.4 Digital certificate management

C•CURE IQ Server contains many different certificates, including:

- **Ingress certificates** – all inbound HTTPS connections to C•CURE IQ Server are secured by one or more certificates known as “ingress certificates”. Setup of C•CURE IQ Server provides two options for issuing/signing these certificates through your preferred internal certificate authority.
- **Kubernetes API server certificates** – the various components of Kubernetes (kubelet, kube-scheduler, kube-proxy, etc.) communicate with the kube-apiserver via HTTPS using a certificate created at setup time. This certificate can be rotated periodically using scripts provided with C•CURE IQ Server.
- **Inter-pod certificates** – the communication between pods uses a certificate managed by the cert-manager component and distributed using Kubernetes secrets.
- **ACME server certificate** – C•CURE IQ Server (specifically, cert-manager) when configured to issue ingress certificates via an ACME server, must communicate with the ACME server over HTTPS. As such, C•CURE IQ Server must be given the root CA certificate used to sign the ACME server’s certificate.
- **SQL Server certificate** – C•CURE IQ Server (specifically the auth and istar-personnel services) are required to communicate with SQL Server over TLS. As such, they must be provided with the root CA certificate used to sign the SQL Server certificate.
- **RabbitMQ certificate** – while the services running in pods on the same server are not using TLS to communicate with RabbitMQ, the external clients (such as victor Application Server, Administration Workstation, and Monitoring Station) are using TLS. The certificate used for this communication is communicated through Vault to the clients.

1.2.5 Audit Logs

All containers in the platform use standard container logging, the output of which is collected and stored in an isolated Log container for privileged access. Container log files are read-only to all users except those with “root” access. C•CURE services create log files that are mounted on their local volume of the node they are on. These JCI service Logs are then collected into repository which can be searched, viewed, and graphed via the Grafana user interface. Please see the C•CURE IQ Server Installation and Maintenance Guide for more detailed instructions and details.

1.2.6 Automated hardening

The C•CURE IQ Server setup program includes a hardening step that is enabled by default. This hardening step uses the Security Content Automation Protocol (SCAP) via the OpenSCAP tool provided through Red Hat Enterprise Linux. The mitigations taken by the hardening step have been tested with C•CURE IQ Server to ensure that those mitigations provide an additional layer of strong protection while not interfering with the operation of the platform.

1.3.0 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:

<u>Server Level</u> – 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.

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 specific installation instructions of your components.

1.3.1 Internet connectivity

The C•CURE IQ Server system does not require inbound or outbound internet access for normal operations. Internet access increases your cybersecurity attack surface which requires additional hardening steps. For those who require remote access and cloud-hosted services, Johnson Controls recommends using a zero-trust solution such as Tempered Airwall to harden your solution as this provides a secure overlay and tunnel to any internet facing device or component residing on an untrusted network.

Inbound

As a best practice, we strongly recommend not exposing products on the internet unless that product specifically requires internet accessibility.

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

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

Outbound

The C•CURE IQ Server is designed to be able to run in an offline/air-gapped environment where outbound connectivity to the internet is not available. While an air-gapped configuration will be required for some customers, it’s not a security requirement in all scenarios. Allowing outbound internet connectivity (especially port 443) will simplify the installation and update procedure of the operating system packages and hence may be desirable.

1.3.2 Integration with external systems

This solution requires integration with C•CURE 9000 including the victor Application Server, Monitoring Station, and Administration Workstation. Integration with iSTAR Controllers is optional.

1.4.0 Patch policy

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 point release 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 vulnerabilities within the next available major release

1.5.0 Hardening methodology

While C•CURE IQ Server provides many onboard security safeguards, including many secure-by-default settings and automated hardening steps, we recommend that the device is hardened according to the guidance outlined in section 2, Deployment.

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

1.6.0 Communication

1.6.1 Communication port configuration

In a C•CURE IQ Server system, when using a protocol, ensure that the corresponding port is open. Hardening your system involves closing any port that is not used. The tables on the following pages provide information on which ports and protocols must be left open for C•CURE IQ Server to function properly.

The C•CURE IQ Server has automated the enabling of the default firewall on your RHEL system, *firewalld*, and only opening inbound ports from table 1.6.2.1 below. Outbound ports on the RHEL system are left open by default in this version of the C•CURE IQ Server setup program.

If your installation or site has additional firewall software running on your Linux VM or on the physical hypervisor server, please ensure that the inbound and outbound ports listed in the next two sections are opened.

1.6.2 Inbound ports which are required to be opened

The following inbound ports are required to be opened by firewalls and/or intrusion software surrounding the Linux server for proper functioning of C•CURE IQ Server.

Table 1.6.2.1: Inbound Ports

Port	Protocol	Use
22	TCP	SSH/SCP used for RKE setup and for basic command line/shell use during install and ongoing operation of C•CURE IQ Server
80	TCP	Unencrypted HTTP traffic used sparingly: • to return a “307 Internal Redirect” back to the browser with “https” (port 443) thereby forcing traffic to be encrypted • to respond to ACME challenges on port 80
443	TCP	HTTPS TLS-encrypted traffic to Web UIs and REST/gRPC APIs.
1514	TCP	Harbor syslog port.
2377	TCP	Docker networking used by Harbor on the jump host requires this port so that the various harbor containers can communicate with each other.
4443	TCP	HTTPS TLS-encrypted traffic to Notary image signing API on Harbor running on jump host.
6443	TCP	Kubernetes API (over HTTPS) exposed on the control nodes
7946	TCP	Docker networking used by Harbor on the jump host requires this port so that the various harbor containers can communicate with each other.
8472	UDP	VXLAN Tunneling between worker nodes
8443	TCP	HTTPS TLS-encrypted traffic to local Harbor artifact registry
10250	TCP	Kubelet API (over HTTPS) exposed on the worker nodes
28013	TCP	iSTAR Controller Certificate Signing Request (CSR)
28104	TCP	iSTAR Fast Download Channel
28110	TCP	iSTAR Controller Primary Connection
28116	TCP	iSTAR Panel Data Upload - Used for diagnostic purposes; only open when debugging
28220	TCP	iSTAR Driver gRPC Port - Used for diagnostic purposes; only open when debugging
30705	TCP	AMQPS (RabbitMQ over TLS) used to connect from the victor Application Server and C•CURE Windows applications to the queueing system in C•CURE IQ Server

1.6.3 Outbound ports which are required to be opened

The following outbound ports are required to be opened by firewalls and/or intrusion software surrounding the Linux servers for proper functioning of C•CURE IQ Server.

Table 1.6.3.1: Outbound Ports

Port	Protocol	Use
22	TCP	SSH/SCP used for RKE setup from the jump host during the install and ongoing operation of the cluster
25	TCP	SMTP for sending alerts from Grafana (and other potential email traffic in the future)
53	UDP & TCP	DNS lookups
80	TCP	Unencrypted HTTP traffic used sparingly.
123	UDP	Network Time Protocol (NTP) Synchronization
443	TCP	HTTPS TLS-encrypted traffic outbound from the various servers
1433	TCP	SQL Server Connections from C•CURE IQ Server to C•CURE's SQL Server default instance. If this installation is not using the default SQL Server port, open your instance's port instead.
2377	TCP	Docker networking used by Harbor on the jump host requires this port so that the various harbor containers can communicate with each other.
4443	TCP	HTTPS TLS-encrypted traffic outbound from the worker to Notary endpoint of Harbor on the jump host.
6443	TCP	Requests to the Kubernetes API from kubectl on the jump host and from kubelet and the Kubernetes dashboard on the worker nodes
7946	TCP	Docker networking used by Harbor on the jump host requires this port so that the various harbor containers can communicate with each other.
8443	TCP	HTTPS TLS-encrypted traffic from worker/control nodes out to Harbor artifact registry
8472	UDP	VXLAN Tunneling between worker nodes
8997	TCP	WCF Stream Binding from C•CURE IQ Server to victor Application Server
8999	TCP	WCF Session Binding from C•CURE IQ Server to victor Application Server
10250	TCP	Requests to the Kubelet API from kube-apiserver on the control nodes
28014	TCP	iSTAR outbound CSR response

1.7.0 Hardware Requirements

The minimum machine size specifications are shown in the table below. The host can be either a physical server or a VM. For additional information, see the document Installation and Maintenance Guide.

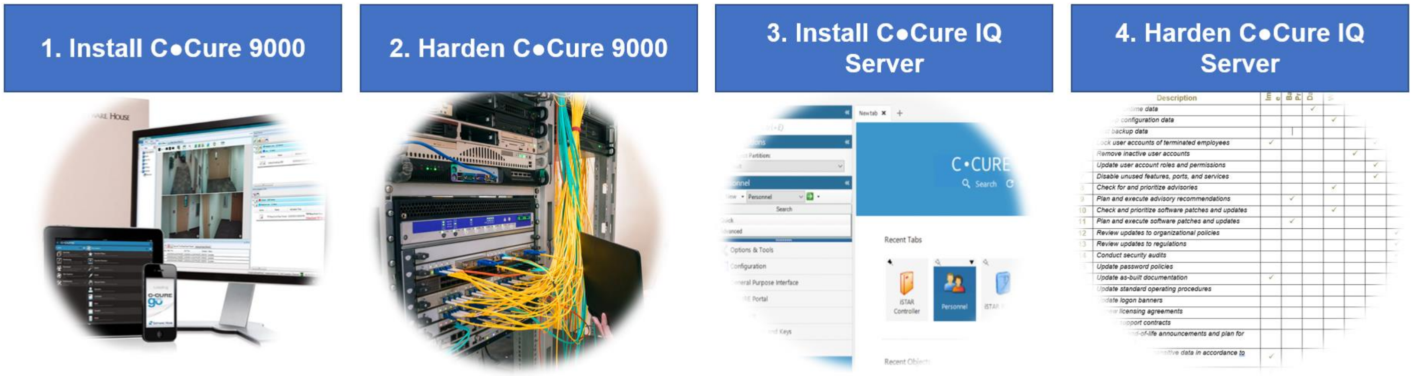
Host role	Size of host
Combined jump host, Kubernetes control node and Kubernetes worker node	• RAM: 32GB • CPU: 12 logical cores • Disk: 500GB

2 Deployment

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

2.1.0 Deployment overview

Reminder: At this juncture, C•CURE 9000 should be installed, hardened, and C•CURE IQ Server installed.



1. Install C•Cure 9000

2. Harden C•Cure 9000

3. Install C•Cure IQ Server

4. Harden C•Cure IQ Server

2.1.1 Physical installation considerations

To continue, the C•CURE 9000 installation and hardening must already be completed. The C•CURE 9000 Hardening Guide recommended that the server be installed in a locked room, cabinet, or enclosure to restrict access. The same applies to any additional hardware for C•CURE IQ Server.

2.1.2 Knowledge level

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

2.1.3 IQ Server updates

C•CURE IQ Server updates will be supplied on a regular basis between major and minor releases. These updates will contain security patches of third-party open-source software as it becomes available. See section 1.4.0 for additional details.

It is best practice to apply the latest C•CURE IQ Server **critical updates** and **point releases** to get the latest security fixes for your system.

2.2.0 C•CURE IQ Server System Hardening

While C•CURE IQ Server has several secure-by-default safeguards, C•CURE IQ Server must be hardened 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: Disable basic password authentication for all operators

□ Hardening Step 4: Update your operating system

□ Hardening Step 5: Disable unused ports

- □ Hardening Step 6: Disable unused features and services
- □ Hardening Step 7: Exclude files from endpoint protection
- □ Hardening Step 8: Backup and restore
- □ Hardening Step 9: Time synchronization
- □ Hardening Step 10: Reissue and sign TLS ingress certificates

2.2.2 BIOS hardening

During the installation of C•CURE 9000 the BIOS of the physical machine that it is running on should have already been hardened to the steps below. If C•CURE IQ Server was installed on a separate physical machine (bare metal/VM on a hypervisor server) follow these steps again for the additional physical machine.

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

2.2.3 Enable BIOS password

Hardening Step 1: Enable BIOS password

Enable password protection of the BIOS and set the password on the physical server running C•CURE IQ Server by following the manufacturer’s specific system instructions. This BIOS password should be known only to authorized administrators.

2.2.4 Prevent USB boot

Booting from USB devices can be restricted within the BIOS. The USB port is an important technical interface that would allow for a malicious user to upload corrupted files or download information.

Hardening Step 2: Disable USB Boot

Disable the USB boot setting in the BIOS if boot from USB is an option.

2.2.5 User management

C•CURE 9000 and C•CURE IQ Server both recommend using third-party Identity Management Systems (IDMSs) for authentication of operators.

NOTE: We use the terms Identity Management System (IDMS) and Identity Provider (IdP) interchangeably. Both are third-party systems that are installed in your enterprise for managing the identity of people associated with your organization. We support OIDC / OAuth2.

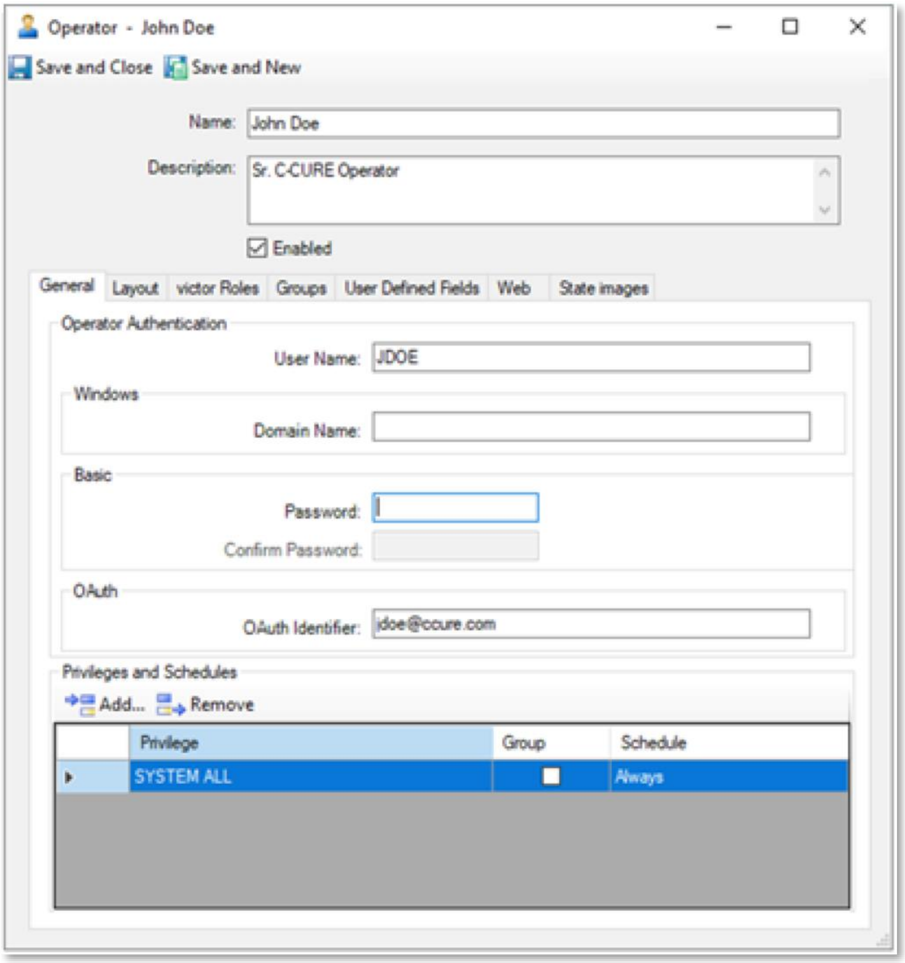
IDMSs offer enhanced security over the local management of users. An IDMS, such as Microsoft Active Directory or Okta can provide user account management for multiple applications, devices, or systems. By centrally managing user accounts, an administrator can assure consistency throughout the domain the IDMS manages. This assures that when an account is disabled in the domain, access by that user is disabled everywhere in the domain that is governed by the IDMS. Furthermore, an IDMS provides a centralized location to manage password policies which dictates password formation rules including, length, capitalization, reuse, and expiration.

C•CURE IQ Server includes the “Auth Service” that has a web user interface known as C•CURE IQ Identity Management. Through this, we can enable C•CURE IQ to use Single Sign On (SSO) via one or more of your third-party IdPs. Once enabled, take steps to remove any operator with a basic username and password to avoid those users from being able to login after they have been removed from the IDMS.

Hardening Step 3: Disable basic authentication for all operators

1. Configure and enable one or more External Identity Providers through the C•CURE IQ Identity Management user interface as described in the C•CURE IQ Server Installation and Maintenance Guide.
2. Using the C•CURE 9000 Administration Workstation, create or modify one or more operators with OAuth identifiers matching the identifiers in the IDMS.
3. Test signing onto the applications such as the Monitoring Station, the Administration Workstation and/or the C•CURE IQ Web Application using the third-party IDMS.
4. When the integration is configured and working correctly, go back into C•CURE 9000 Administration Workstation and remove all passwords from all operators.

Figure 2.2.5.1



Name: John Doe

Description: Sr. C-CURE Operator

☑ Enabled

User Name: JDOE

Domain Name:

Password:

Confirm Password:

OAuth Identifier: jdoe@ccure.com

	Privilege	Group	Schedule
▸	SYSTEM ALL	□	Always

2.3.0 Operating system updates

As of the writing of this document, the Software House Technical Support and Quality Assurance teams have not reported any conflicts or issues with C•CURE IQ Server and Red Hat Enterprise Linux 7 operating system and package updates.

It is best practice to apply the latest Red Hat Enterprise Linux 7 and Red Hat package updates.

Note: The operating system and all packages are updated each time the setup script is run (first time and during upgrades); therefore, it is not necessary to run this manually.

Hardening Step 4: Update your operating system

To optional update RHEL 7 with all the latest patches, run this command:

```
sudo yum update
```

2.4.0 Communication hardening

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

2.4.1 Configure communication ports

Unused ports should be closed unless they are specifically needed for C•CURE IQ Server, another approved use, or the application to function. In section 1.6 we reviewed the ports and protocols that need to be open based on the features being used. The C•CURE IQ Server setup program enables the Linux firewall and only opens inbound ports as described in section 1 of this document. However, outbound ports are left open by default.

Hardening Step 5: Disable unused ports

Ensure that the ports corresponding to your C•CURE IQ Server system from section 1.6.2 are open. To harden your system, be sure to disable/close any outbound ports not listed in section 1.

For additional information, see the C•CURE IQ Server Installation and Maintenance Guide

2.5.0 Disable unused features and services

Hardening Step 6: Disable unused features and services

If optional features are installed and not required in this instance, disable them. This lowers the attack surface of C•CURE IQ Server.

The config.yml file provides three places to disable rarely used User Interfaces (UIs) that can help reduce the attack surface:

```
config_enable_rabbitmq_ui: true
config_enable_kubernetes_dashboard: true
config_enable_grafana: true
```

Set these to `false` to disable the respective UIs, **but only if they are not in use**. Be sure to rerun `setup.sh` to apply the changes. If any of these UIs are needed later, set them back to `true` and rerun `setup.sh`.

There may be features of Linux that can be disabled after installation such as `vim` or `cron`. Consult the Linux vendor documentation for more information on disabling unused Linux features.

2.6.0 Recommended endpoint protection

Hardening Step 7: Exclude files from endpoint protection

We do not recommend any specific endpoint protection software. However, when using endpoint protection software, the following exclusions (directories that should not be scanned) must be made:

- `/var/lib/docker`

2.7.0 Encrypt or delete secrets

The C•CURE IQ Server installation process (including the troubleshooting process) requires that certain secrets be written to disk. Leaving secrets on the disk for an extended period increases risk. We recommend either encrypting or deleting those secrets. A script is provided with the installation (encrypt.sh) to encrypt all secrets (see the Maintenance chapter of the C•CURE IQ Server Installation and Maintenance Guide for details of using this script). If using this script, remember (or store securely) the password. Whether encrypting or deleting the secrets, always back them up in a secure location.

Here is a list of the secrets on the drive (where ~ represents the home directory of the user that was used to install the C•CURE IQ Server).

- `~/.kube/config` – contains secrets that allow login and control the Kubernetes cluster. This is used by the kubectl and helm commands, so encrypting/deleting it will impact your ability to run those commands.
- `/root/.docker/config.json` – this file *may* contain the credentials used to login to the local harbor to push artifacts during the install. A successful install will logout of harbor, which removes those credentials. However, it's a good idea to encrypt/remove this file if something went wrong during the installation process.
- `/root/.docker/trust` – this directory contains several secrets used to sign container images.
- `/data/certs` – this directory contains the certificate signing keys used for a few internal processes.
- `~/jci-k8s-setup/files/cert/ingress.key` – this file contains the secret key for TLS on the ingress endpoints into the Kubernetes cluster (only if chosen to manually sign the certificates and not use ACME… if using ACME, this file will not exist).

Important Reminders

- The passwords for the installation are already encrypted and aren't included in this list. The "always encrypted" passwords are in `~/jci-k8s-setup/passwords`. And can be deleted if they are backed up first.
- To run any of the following, restore the secrets first:
  - `kubectl`
  - `helm`
  - `setup.sh`
  - `view-secrets.sh`
  - `rotate-certificates.sh`
- To run any of the following, restore the passwords directory first (or provide all the same passwords via environment variables):
  - `setup.sh`
  - `view-secrets.sh`
  - `rotate-certificates.sh`

2.8.0 Backup and restore

The data stored within C•CURE IQ Server are copies of data that exists in other places. Therefore, in the case of a disaster, the best approach is to restore the system to a snapshot taken prior to installation, restore the configuration and reinstall the system.

Hardening Step 8: Backup and restore

To expedite a reinstall, backup the following files:

- `~/jci-k8s-setup.tgz (the last tarball used to deploy)`
- `~/jci-k8s-setup/config.yml (the configuration file used from the last install)`

- `~/jci-k8s-setup/passwords/* (the encrypted passwords from the last install)`
- `~/jci-k8s-setup/files/certs/* (The ingress certificate and key; only needed when using manual certificate signing)`

See the C•CURE IQ Server Installation and Maintenance Guide for details about when to take a snapshot/checkpoint of the system, how to backup and restore important files and how to reseed the iSTAR Personnel database.

2.9.0 Time synchronization

The time on the Linux server must be in-sync with the time on the Windows client(s) and Windows server(s) for the entire system to operate properly and to keep the system secure.

See the time synchronization section in the Prerequisite chapter of the C•CURE IQ Server Installation and Maintenance Guide for more details on why this is important and how to pick NTP server(s) to use with C•CURE IQ Server.

Hardening Step 9: Time synchronization

Follow these steps to ensure the time is in-sync on your Linux server:

- From a command prompt, enter `timedatectl` and ensure the response has `NTP enabled: yes` and `NTP synchronized: yes`.
- From a command prompt, enter `chronyc tracking` and ensure the response shows only a small difference to NTP time (within 0.1 seconds).
- From a command prompt, enter `watch -n .1 date` and, at the same time, bring up your C•CURE 9000 Windows server clock and ensure the times on both servers match to the second.

If any of these steps show an issue or difference in the time, please follow the steps in the Troubleshooting chapter of the C•CURE IQ Server Installation and Maintenance Guide.

2.10.0 Reissue and sign TLS ingress certificates

This process is part of the original install of C•CURE IQ Server. Confirm that certificates are still valid on your system and reissue only if necessary.

If the ingress certificates used for C•CURE IQ Server are manually signed, re-issue (renew) them before they expire. Regenerate the CSR before renewing the certificate so that the private key is rotated in this process.

Hardening Step 10: Reissue and sign TLS ingress certificates

See the Maintenance chapter of the C•CURE IQ Server Installation and Maintenance Guide for instructions on regenerating the CSR, re-issuing the certificates and re-deploying.

Note: This is not applicable when using ACME certificate signing in your environment.

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 after the final deployment audit may not reflect the quality of that audit. You may require a higher degree of protection for the environment because policies, regulations and guidance may change over time.

3.1.0 Cybersecurity maintenance checklist

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

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

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

Table 3.1.0 – Cybersecurity maintenance checklist

Item	**Description**	**Immediate**	**Priority Based**	**Daily**	**Weekly**	**Monthly**	**Quarterly**	**Annually**
1	*Backup configuration data*	✓			✓			
2	*Disable unused features, ports, and services*						✓	
3	*Check for and prioritize advisories*				✓			
4	*Plan and execute advisory recommendations*		✓					
5	*Check and prioritize patches and updates*				✓			
6	*Plan and execute patches and updates*		✓					
7	*Review organizational policy updates*							✓
8	*Review updates to regulations*							✓
9	*Update as-built documentation*	✓						✓
10	*Conduct security audits*							✓
11	*Update password policies*							✓
12	*Update standard operating procedures*							✓
13	*Update login banner*							✓
14	*Renew licensing agreements*							✓
15	*Renew support contracts*							✓
16	*Check for end-of-life announcements and plan for replacements*						✓	
17	*Periodically delete sensitive data in accordance with policies or regulations*		✓					
18	*Monitor for cyber attacks*	✓				✓		
19	*Check time synchronization*					✓		
20	*Rotate Kubernetes certificates*						✓	
21	*Reissue and sign TLS ingress certificates*							✓
22	*Rotate vault password*						✓	
23	*Rotate Kubernetes encryption key*						✓	

3.1.1 Backup configuration data

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.

See the Maintenance chapter of the C•CURE IQ Server Installation & Maintenance Guide for details on backing up the configuration data.

Frequency: After each change and weekly.

3.1.2 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.

Note: See the Johnson Controls Cyber security learning website for port assignment information and other hardening guides at this link - Resources | Johnson Controls.

Refer to the Maintenance chapter of the C•CURE IQ Server Installation and Maintenance Guide for information on disabling certain features of the platform when they are not needed.

Frequency: Quarterly.

3.1.3 Check for and prioritize advisories

Security advisories are usually found on a product’s support website. Product literature can inform the 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.

Frequency: Weekly.

3.1.4 Plan and execute advisory recommendations

Follow the plan determined in the previous maintenance step.

Frequency: Based on priority.

3.1.5 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.

Note: 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.

Frequency: Weekly.

3.1.6 Plan and execute software patches and updates

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

To update the C•CURE IQ Server and dependent Linux packages, please see the Maintenance chapter in C•CURE IQ Server Installation and Maintenance Guide.

Frequency: Based on priority.

3.1.7 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.

Frequency: Annually.

3.1.8 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 or a new/upcoming regulation to determine gaps in compliance, an assessment of the changes should be conducted periodically.

Collect most recent copies of regulations as applicable. Perform a gap analysis against the deployed configuration.

Frequency: Annually.

3.1.9 Update as-built documentation

Update as-built documentation if the deployment architecture or component configuration changes. Some configuration changes happen without a formal project or plan and if such cases occur, it may be necessary to update the as-built documentation. Schedule a full update of the as-built documentation on a regular basis to ensure that all changes are documented. C•CURE IQ Server is an add-on to C•CURE 9000. We recommend that keeping the as-built documentation for both systems together and updated at the same frequency.

Frequency: As changes are made or annually.

3.1.10 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. We recommend that performing an audit for C•CURE 9000 and C•CURE IQ Server at the same time for effectiveness.

Frequency: Annually - synchronized with your annual C•CURE 9000 audit.

3.1.11 Update password policies

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

If your organization updates its policies, ensure account passwords are updated to comply with those policies.

Frequency: Annually.

3.1.12 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 used, a gap in protection can be created, prevented, or closed. Therefore, it is important to update standard operating procedures periodically.

Frequency: Annually.

3.1.13 Update login banner

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

To update the Linux login banner, please see the Maintenance chapter in C•CURE IQ Server Installation and Maintenance Guide.

Frequency: Annually.

3.1.14 Renew licensing agreements

Assure that your system's licenses support the necessary functions required for your installation, including but not limited to C•CURE IQ Server, operating systems, connected systems, hypervisors, and hardware. Collect active license details and ensure compliance. Act as necessary.

Frequency: Annually.

3.1.15 Renew support contracts

Assure that your support agreements are up to date, including but not limited to C•CURE IQ Server, operating systems, connected systems, hypervisors, and hardware. Collect active support agreement details and renew as necessary.

Frequency: Prior to support agreement expiration date or annually.

3.1.16 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 but not limited to C•CURE IQ Server, server operating systems, connected systems, hypervisors, and hardware. Collect end-of-life details for all your products and substitute with a replacement product prior to end-of-life date.

Frequency: Quarterly.

3.1.17 Periodically delete sensitive data in accordance with policies or regulations

Collect details on policies and regulations that apply to your location. Based on those policies and regulations, be sure to delete sensitive data.

NOTE: C•CURE IQ Server hold a minimum amount of personal data. Such data is a copy of the data held in C•CURE 9000. Therefore, any data deleted in C•CURE 9000 will be deleted in C•CURE IQ Server.

Frequency: As required.

3.1.18 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 any security monitoring tools are installed *(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

Note: 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 installation of security monitoring tools.

Frequency: Run continuously once implemented then validate the solution is operating monthly.

3.1.19 Check Time synchronization

The time on the Linux server must be in-sync with the time on the Windows client(s) and Windows server(s) for the entire system to operate properly and to keep the system secure.

See section 2.9.0 to ensure the time is in-sync on your Linux server.

If any of these steps show an issue or difference in the time, please follow the steps in the Troubleshooting chapter of the C•CURE IQ Server Installation and Maintenance Guide.

Frequency: Monthly.

3.1.20 Rotate Kubernetes certificates

The Kubernetes certificates (and corresponding private keys) are generated at setup time. They are used internally by Kubernetes to communicate via mTLS between the Kubernetes components (e.g., Kubelet, Kubernetes API server, and etcd). They have been configured to expire after 10 years, but we recommend rotating them more frequently.

The C•CURE IQ Server provides a script for rotation of these certificates. Please refer to the Maintenance chapter of the C•CURE IQ Server Installation and Maintenance Guide for instructions on rotating these certificates.

Frequency: Quarterly.

3.1.21 Reissue and sign TLS ingress certificates

As discussed in 2.10.0, if the ingress certificates used for C•CURE IQ Server are manually signed, re-issue (renew) them before they expire. Regenerate the CSR before renewing the certificate so that the private key is rotated in this process.

Frequency: Annually, at least 1 month prior to expiration (or earlier if your organization has a long lead-time for obtaining certificates), if using manual certificate signing.

3.1.22 Rotate vault password

The encrypted passwords and secrets in `~/jci-k8s-setup/passwords` are protected by ansible-vault with the password provided during the initial installation. Think of this as the master key to all the passwords needed during an install (and future upgrades). To rotate the ansible-vault password for those files, run `ansible-vault rekey ~/jci-k8s-setup/passwords/*` and enter the old and new password. Make sure to save this password in a secure location as your old ansible-vault password can no longer be used.

If other secrets are encrypted on C•CURE IQ Server host using encrypt.sh as described in section 2.7.0, rotate the encryption password by first running decrypt.sh and then running encrypt.sh providing the new password.

See the Maintenance chapter of the C•CURE IQ Server Installation and Maintenance Guide for more details around the rotation process.

Frequency: Quarterly.

3.1.23 Rotate Kubernetes at-rest encryption key

Kubernetes secrets are encrypted at-rest with a private key managed by RKE. To rotate that key, run `./rke encrypt rotate-key` as the rke user from `/home/rke/rke` directory.

See the Maintenance chapter of the C•CURE IQ Server Installation and Maintenance Guide for more details around this rotation process.

Frequency: Quarterly.