



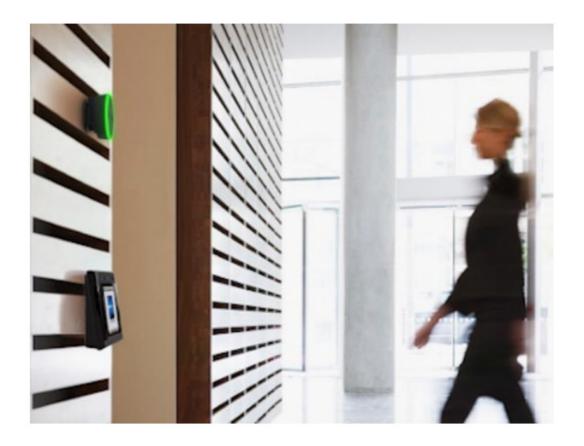
# Home » Johnson Controls » Johnson Controls CEM AC2000 Security Management System User Guide 📆

### Contents [ hide ]

- 1 Johnson Controls CEM AC2000 Security Management System
- 2 Product Specifications
- 3 Product Information
- 4 Product Usage Instructions
  - 4.1 Deployment Architecture
- 5 Introduction
- 6 Legal disclaimer
- 7 Support
- 8 Planning
  - 8.1 Deployment architecture
- 9 Deployment
  - 9.1 Password configuration options
- 10 Maintain
  - 10.1 Cybersecurity maintenance checklist
- 11 FAQ
- 12 Documents / Resources
  - 12.1 References



Johnson Controls CEM AC2000 Security Management System



### **Product Specifications**

• Product: CEM AC2000

• Version: GPS0032-CE-EN Version 12.1 Rev A

• Release Date: 2025-02-26

### **Product Information**

The CEM AC2000 is an access control system designed to provide secure access to facilities. It consists of core components such as the Central Database Computer (CDC), Real Time Computer (RTC), Layer 3 Switch, and AC2000 Workstation, along with supporting components for seamless integration with external systems.

### **Product Usage Instructions**

### **Planning**

After selecting your AC2000 solution, there are three options for running the AC2000 system components:

- 1. Separate Real Time Computer (Separate Central Database Computer (CDC)
- 2. Combined RTC and CDC

3. VMware Cluster infrastructure environment

**Note:** CEM failover is not supported when a VM server is used. Redundancy should be provided by the VMware infrastructure.

#### **Deployment Architecture**

### Components

A typical system's access control system includes both core and supporting components.

### **Core Components**

- Central Database Computer (CDC): The CDC serves each client workstation and reader controller. It processes and stores system data.
- Real Time Computer (RTC): The RTC is a software controller for use with Ethernetbased CEM readers and devices.
- Layer 3 Switch: Provides VLAN management and connects workstations, servers, and readtointo the network.
- AC2000 Workstation: Supports up to three types of Workstation applications on one machine.

### **Supporting Components**

An AC2000 access control system can integrate with external systems like Video Surveillance, Intrusion Detection, Fire systems, and more.

### Introduction

- Our solution provides peace of mind to our customers with a holistic cyber mind set beginning at initial design concept, continues through product development, and is supported through deployment, including a rapid incident response to meet comprehensive and evolving cybersecurity environments.
- The Hardening Guide intends to provide cybersecurity guidance used in planning, deployment, and maintenance periods.
- As cybersecurity threats affect all connected devices, it is important to ensure that cybersecurity is considered throughout the planning, deployment, and maintenance phases associated with a solution's functional operation.

This guide provides hardening guidance for configuration and maintenance, including
the operating system, user accounts, permissions and roles, backup and restore,
redundancy, and patch management. It is broken down into three main sections
depicting the overall process for hardening:

### 1. Planning

Provides an introduction, general knowledge, and overall guidance for you to prepare your system for security and hardening

### 2. Deployment

Guides you through the execution and hardening steps based on the products and security features of the target system components

#### 3. Maintain

Provides a checklist for future checkpoints to keep your system safe and secure

### Legal disclaimer

The cybersecurity practices described in this guide are recommended practices to facilitate the secure installation and configuration of the products described herein. However, Johnson Controls cannot guarantee that the implementation of the cybersecurity practices or recommendations described in this guide will ensure the security of the relevant product or system, prevent or mitigate the potential impact of any unauthorized access or damage caused by a cybersecurity incident. This guide is provided "as is", and Johnson Controls makes no representation or warranty, expressed or implied, as to the efficacy of the cybersecurity practices or recommendations described within. Johnson Controls disclaims all liability for any damages that may occur because of, or despite, reliance on this guide or compliance with any cybersecurity practices or recommendations set forth herein.

### **Support**

• If you require technical assistance using CEM products, contact the CEM Support team using one of the following options:

• **Telephone:** +44(0)2890 456656

• Email: cem.support@jci.com

• Website: https://www.cemsys.com

• Provide our support engineers with the following information:

- The site name
- The product name and model
- The CEM software version
- A description of the problem

### **Planning**

#### **CEM AC2000 Overview**

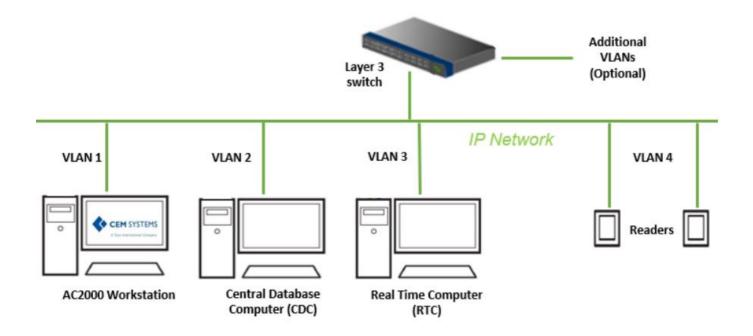
- The AC2000 solution is a powerful and reliable enterprise access control and integrated security management system. As CEM manufactures both the AC2000 hardware and software, AC2000 is renowned in the industry as one of the most comprehensive and flexible security systems available.
- A business or organization can scale its single-site AC2000 access control system to a multi-site enterprise solution.
- With a wide range of features and functionality, AC2000 is available in two solution options, providing reliable and innovative access control for any sized site.
  - AC2000 Standard An enterprise access control and integrated security
    management system that goes beyond access control and has been successfully
    installed at some of the largest facilities around the world where security is
    paramount.
  - AC2000 Airport Used by many of the world's leading airports for over 25 years,
     AC2000 Airport is an aviation-specific access control and integrated security
     management system, with a proven record as one of the most reliable and
     resilient security solutions available.
- After selecting your AC2000 solution, there are three options for running the AC2000 system components:
  - 1. Separate Real Time Computer (RTC) and Central Database Computer (CDC)
  - 2. Combined RTC and CDC
  - VMware Cluster infrastructure environment

**Note:** CEM failover is not supported when a VM server is used. Redundancy should be provided by the VMware infrastructure.

This document guides how to harden and operate an AC2000 system securely.

#### **Deployment architecture**

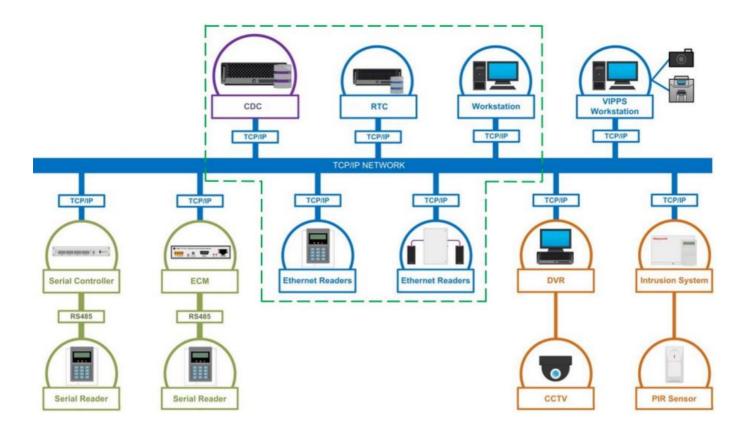
Figure 1.2: Typical reader deployment architecture



### **Components**

A typical CEM system's access control system includes both core and supporting components.

Figure 1.2.1: CEM Core and supporting components



### **Core Components**

Shown above in figure 1.2 and figure 1.2.1 (within the dotted green lines)

### Central Database Computer (CDC)

The CDC serves each client workstation and reader controller. The CDC processes and stores the alarms, transactions, and other data the system generates. In some systems, there can be multiple CDC servers, with one designated as the primary CDC and the other as a hot standby. The CDC is the central store for all data.

### Real Time Computer (RTC)

The AC2000 RTC is a software controller designed for use with Ethernet-based CEM readers and devices. You can use each RTC with up to 256 CEM master readers and devices. Each installation has one or more RTC's. For single RTC systems, the CDC and RTC can reside on the same computer. Each CDC supports up to 256 RTCs.

#### Layer 3 Switch

A network switch with layer 3 routing capabilities provides VLAN management and connects workstations, servers, and the readers into your network. It is best practice to segment this network to isolate readers on a dedicated local area network (LAN) or Virtual LAN (VLAN). You can use a networking switch that has Power-Over-Ethernet (PoE) ports to power Emerald readers. Other types of reader require a dedicated 12VDC power supply.

#### Card Readers

The CEM range of intelligent card readers are the most advanced in the industry and are designed for use with the powerful AC2000 access control and security management system CEM Systems can support and supply a range of third-party solution card readers. A card reader will read data from the user's card and delivers the information read back via TCP/IP. Typical card readers include Serial readers and Ethernet readers.

Note: Sections 2.10.1 and 2.11 detail specific card reader hardening steps

#### AC2000 Workstation

Up to three types of Workstation applications may be installed on one machine if required.

#### AC2000 Workstation

The AC2000 Workstation is a Windows application that manages the access control system for general administration and running reports.

### Visual Imaging Pass Production System (VIPPS)

The CEM Visual Imaging Pass Production System (VIPPS) allows users to produce and administer permanent and temporary ID badges. VIPPS can also be

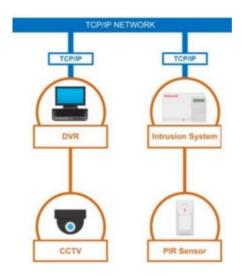
used to enroll fingerprint biometric templates directly onto the AC2000 access control system for integrated biometric enrollment.

### Security Hub Workstation

Used for viewing Alarm events, monitoring alarms, and events on a graphical display

#### **Supporting Components**

An AC2000 access control system can seamlessly integrate with external systems, Video Surveillance, Intrusion, Perimeter Detection, Fire, and more. Here are some of the most common supporting components:



### Digital Video Recorder (DVR)

A device used to make and store digital video recordings, supporting a variety of search and playback functions. Video/DVR servers are connected to video surveillance applications, such as AD Video or ExacqVision, that integrate with AC2000. AC2000 receives alarm and event notifications from the DVR servers.

### • Intrusion System

The intrusion detection system is designed to display, monitor, and control alarm/event signals from individual or multiple perimeter sensor systems, on a single site or group of sites using configured Zones and Sensor Lines.

#### Video Surveillance

View live and recorded footage within the AC2000 system. If external video surveillance systems are also integrated, the AC2000 Video alarm pop-up feature, based on priority or time, can be activated.

### Passive Infrared Sensor (PIR)

PIR motion detection.

### **Deployment**

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

### **Deployment Overview**

- Security hardening of AC2000 begins prior to deployment with careful planning as outlined in section 1 of this guide. It is a good practice to review section prior to deployment to fully understand the security feature set, its architecture, data flow and requirements before physically installing and making application specific configuration changes.
- In this section, more details are provided to help the installer prepare for deployment.

### Hardening CEM AC2000

While CEM AC2000 has several secure-by-default safeguards, we recommend additional hardening to meet the security requirements of the target environment.

### **Hardening Checklist**

- Hardening Step 1: Internet and firewall protection
- Hardening Step 2: Block all ports that are not in use
- Hardening Step 3: Enforce regular password changes
- Hardening Step 4: Account deactivation limit
- Hardening Step 5: Account lockout attempts
- Hardening Step 6: Account set Allow third-party application settings
- Hardening Step 7: Update software
- Hardening Step 8: Disable TLS 1.0 and 1.1 when not using an Emerald card reader
- Hardening Step 9: Change the default password on the Emerald card reader

#### **Networks**

While CEM AC2000 has several secure-by-default safeguards, we recommend additional hardening to meet the security requirements of the target environment.

### Hardening Step 1: Internet and firewall protection.

The network cannot be internet facing and must have the appropriate firewall and network protections in place. You must install the AC2000 access control system on a secure network.

#### **Ports**

Hardening Step 2: Block all ports that are not in use.

In an AC2000 system, when you use a protocol, ensure that the corresponding port is open.

For additional information on ports and protocols, see Table 1:

Po rt	Protocol	Devices	
22	SSH	CDC server/RTC client and RTC server/CDC client, and CDC s erver/Workstation client	
80	HTTP	CDC server/V3 portable client	
12 3	NTP	NTP server/CDC client	
44	HTTPS	CDC server/workstation client  The V3 portable client uses this port.	
44 5	Samba SMB	CDC server/workstation client	
50 10	CEM Comms	CDC server/RTC client and CDC server/workstation client	
50 60	OpenSips	CDC Server and Workstation/Reader Client	

54 05	Corosync UD P	CDC server/CDC client  Note: This port is only for fail-over systems.			
54 32	ODBC/Postgr es	CDC server/workstation client			
55 53	MDC	RTC server/reader client			
55 54	PBP	Reader server/RTC client			
55 55	PBP	Secondary reader server/RTC client  Note: Only the EDCM in master/master mode, and the 90×0 ser ver/CDC client use this port.			
55 56	90×0	90×0 server/CDC client			
66 66	Reader diagn ostics	Reader server/diagnostic client			
77 89	DRBD	CDC server/CDC client  Note: This port is only for fail-over systems.			
99 99	TCP	RTC server/Aperio client			

### Personal data

- Store only personal information that is necessary for security and access control purposes.
- For example, it may not be necessary to store the date of birth or home address of a

cardholder.

### **Password configuration options**

This section describes password configuration options, including enforcing regular password changes, setting the account deactivation limit, and setting the account lockout attempts limit.

#### 1. Enforcing regular password changes

Hardening Step 3: Enforce regular password changes

To encourage users to change their passwords regularly, complete the following steps:

- Log on to AC2000.
- Open the configured application.
- From the Parameters list, select the parameter passwd force change days.
- In the Configured Parameters pane, in the Value field, type the number days after which the system enforces the user to change their password. For example, if you type 90 into the Value field, the system enforces a password change after 90 days.
- Click Save.

### 2. Setting the account deactivation limit

Hardening Step 4: Account deactivation limit

In AC2000, you can set the system to automatically deactivate a user account that is inactive for a designated period. To set the account deactivating limit, complete the following steps:

- Log on to AC2000.
- Open the configured application.
- · Click Add.
- In the Configured Parameters pane, in the Name field, enter user\_lock\_days.
- In the Value field, type the number of days after which the system automatically deactivates a user account. For example, if you type 365 into the Value field, the system deactivates the account after 365 days.
- In the Comment field, enter automatic account lockout
- Click Save.

### 3. Setting the account lockout attempts limit

Hardening Step 5: Account lockout attempts

The automatic account lockout feature locks out a user account from AC2000 after a set number of unsuccessful logon attempts. To set the account lockout attempts limit, complete the following steps:

- Log on to AC2000 WEB.
- Click AC2000 Setup and click Web Login Config.
- In the Account Login Attempts field, select how many times you want a user to attempt to log on before they are locked out of the system.
- Click Update.

**Note:** After the system locks a user out of AC2000, the account can be reset only by a system administrator. For more information, refer to User Options in the Setup Guide.

### 4. Hardening Guide Account Locked alarm.

Use the "enable\_lockout\_alarm" setting to generate an alarm on the Security Hub application each time an account is locked out.

To enable the account locked alarm, complete the following steps:

- On the AC2000 Floatbar, click Advanced Configuration, and click Configured.
- Select the enable\_lockout\_alarm setting.
- In the Value field, type Y to enable the alarm.
- Click Save.

Any time an account is locked out, the system generates an alarm in Security Hub. You must acknowledge and cancel the alarm manually.

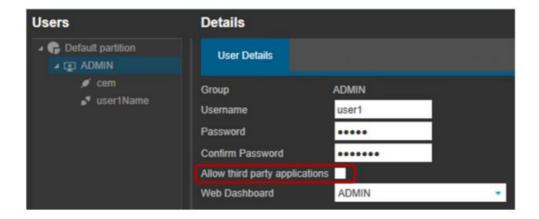
### Account settings – allow or disallow third-party applications.

When creating or updating a user, notice the Allow third-party applications box, which is unchecked by default to enhance security.

- When this box is left unchecked, users have access to the AC2000 database only via AC2000 applications.
- When this box is checked, the user has unrestricted access to the database.
   Hardening Step 6: Account set Allow third-party applications

### Setting unchecked:

Ensure any new users have the Allow third-party applications box of their profile unchecked.



### Setting checked:

Determine if a user needs unrestricted database access and that this access is approved by the appropriate personnel.

- For only this user, check the Allow third-party applications box. Notice that the Read-Only field appears. It is highly recommended that you check this box, unless write privileges are also approved.
- Security Warning: Check these settings only when necessary



### Software updates

Hardening Step 7: Update software

Always update to the latest software version. For more information, see Support.

### **System Configuration**

**Note:** Hardening steps 8 and 9 are designed for two different system configuration options —whether you are using emerald readers or not. You should only need to perform step 8 or 9, depending on your system configuration.

Table 2.10: Final hardening step

System Configuration	Hardening Step	Description
----------------------	----------------	-------------

Not using the Emerald card r eaders	Step 8 – Section 2.1 1.0	Disable older TLS versions				
Using the Emerald card read ers	Step 9 – Section 2.1 2.0	Change the Emerald default password				

### **Transport Layer Security (TLS) Settings**

- If you are using Emerald card readers, then you must also use TLS 1.0 for them to function properly. If you are using an Emerald card reader, please skip to the next section.
- Hardening Step 8: Disable TLS 1.0 and 1.1 when not using an Emerald card reader
- For an AC2000 system that does not use Emerald card readers, use TLS 1.2 or higher.

**Note:** To harden an AC2000 system that does not use Emerald card readers, contact CEM support to disable TLS 1.0 and TLS 1.1 from the system.

### Changing the default password on an Emerald card reader.

- On most systems TLS is active by default but take a moment to ensure TLS 1.x is enabled before moving on to the next step.
- It is best practice to change the default password on all Emerald readers as shown below:

Hardening Step 9: Change the default password on the Emerald card reader

To change the default password on an Emerald reader, complete the following steps:

- 1. Log onto the AC2000 Floatbar, click Device Configuration, and click Devices.
- 2. From the navigation tree, select the Emerald realm for which you want to change the password.
- 3. Click the Properties tab and click Advanced View.
- 4. Click the Other tab and click Admin Settings.
- 5. In the Admin Settings pane, select the Enable Remote SSH check box, and click Save.
- 6. Log onto the AC2000 CDC server using the CEM user profile and password.
- 7. Connect to the selected emerald reader with the IP address of the reader. For

example, if the emerald has an IP address of 192.168.1.125, enter the following on the CDC: tsrssh root@192.168.1.25

**Note:** If you are not on the AC2000 CDC server, use an SSH client, such as PuTTY, and the IP address of the Emerald reader.

- 8. In the Password field, enter the root password. The default password is "GBest 1946".
- 9. To change the password, enter the password
- 10. On the New Password line, enter the new password.
- 11. On the Retype Password line, enter the new password again.
- 12. Type logout in the Emerald Reader, type logout
- 13. Log onto AC2000 Floatbar, click Device Configuration, and click Devices.
- 14. From the navigation tree, select the Emerald read-on for which you changed the password.
- 15. Click the Properties tab and click Advanced View.
- 16. Click the Other tab and click Admin Settings.
- 17. In the Admin Settings pane, clear the Enable Remote SSH check box, and click Save. Note: It is best practice that you enable SSH access only when strictly necessary.

### **Encryption at rest**

If you require data to be encrypted at rest, run the AC2000 system on servers that provide this functionality at the hardware level.

### **External systems**

Where possible, ensure that you authenticate connections to external systems that involve sensitive information or critical functions.

#### **Maintain**

- The contents within this section address how to monitor for potential cybersecurity issues and maintain protection levels as 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

in technologies used.

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

#### 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 are adjusted to best suit the target conditions of the deployed environment:

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

#### Backup data

If you need to restore or replace your AC2000 system, it is essential to have a backup of

its data. Backup your system daily and check that the backup succeeds.

### Lock the user accounts of terminated employees.

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

#### Remove inactive user accounts.

While an employee may still be employed by an organization in which the system is owned, managed, serviced, or used by them, they may not have utilized it for a long period. This suggests that, independent of being authorized to use the system, they do not have a need to use the system, and you should remove their user account. This is sometimes referred to as a 'use it or lose it policy'. This best practice reduces the number of active user accounts in the system and therefore lowers the potential attack footprint.

#### Update user accounts, roles, and permissions...

While an employee may still be employed by an organization that owns, manages, or services the system, their role may change, requiring an increase or decrease in what they can do via the AC2000 system. When a person's role changes, make sure that the appropriate permissions are added and any that are no longer required are removed.

### Disable unused features, ports, and services

If you no longer require optional features, ports, and services, disable them. This practice lowers the attack surface of CEM AC2000, resulting in a higher level of protection.

#### Check for and prioritize advisories.

You can find security advisories for CEM AC2000 on the Cyber Protection website. Access is provided once you have registered a user account with that site. User account registration is open to JCI customers and authorized representatives. Determine if CEM AC2000 is impacted by the conditions outlined in the advisories. Based on how the CEM AC2000 system is deployed, configured, and used, the advisory may not be of concern. Referring to the as-built documentation of the CEM AC2000 system will help with this assessment. A good set of as-built documentation will help you identify the number of components impacted and where they are located. While advisories call attention to a

cybersecurity issue, it is not always possible to take immediate action or execute the full recommendation described in the advisories. If so, prioritization will aid in your planning to ensure that any issue impacting your system is fully and appropriately addressed in order of priority. Check for advisories from third-party components such as networking equipment and operating systems by consulting with the respective vendor.

#### Plan and execute advisory recommendations.

If CEM AC2000 is impacted by the conditions outlined in the advisories, including those from third party components, then action must be taken to mitigate the issues raised. The specific action is based upon the content of the advisories distributed and depends upon the environment CEM AC2000 is deployed into. Plans for executing the advisory recommendations must consider the Hosting platform and environment.

#### Check and prioritize patches and updates..

While an AC2000 patch or update may or may not relate to an advisory, it is always best practice to apply the most current patches and updates. These patches and updates can include cybersecurity enhancements and 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 lowers the cybersecurity risk. Check for updates and patches of third-party components such as networking equipment and operating systems by consulting with the respective vendor.

#### Plan and execute software patches and updates.

Create a plan to apply software updates on a regular basis. This plan should include provisions for the unlikely event of service impact. Make considerations regarding schedule and deployed environment to minimize service disruptions.

#### Review updates to organizational policies.

Organizations may update their policies, which include cybersecurity requirements.

Changes to these policies can impact systems that complied before the change.

Periodically check to see if policy changes were made and reassess compliance with those policies.

#### Review updates to regulations.

If CEM AC2000 is deployed in a location that is governed by regulations 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 regulation, an assessment of the changes should be conducted periodically.

#### Conduct security audits.

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

### **Update password policies**

Guidance on password policies has been evolving. Password policies should be reassessed 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.

### 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 it is possible that the as-built documentation may not be updated accordingly. Schedule a full update of the as-built documentation regularly to ensure that all changes are documented.

### Update standard operating procedures..

Including best practices for cybersecurity within standard operating procedures can complement the protection that the system can deliver on its own. Depending on the procedures an operator uses, a gap in protection can be created, prevented, or closed. Therefore, it is important to update standard operating procedures periodically.

### **Update logon banners**

This system includes a policy on logon banners that can change over time. Review and update as required.

### Renew licensing agreements

Assure that your CEM AC2000 software license supports the necessary functions.

### **Renew support contracts**

Assure that your CEM AC2000 software support agreement (SSA) is up to date.

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

Review product announcements to determine if any of the components of CEM AC2000 have a planned end-of-life announcement.

### Periodically delete sensitive data by policies or regulations.

Collect details on policies and regulations that apply.

### Monitor for cyber attacks.

Monitoring site perimeters, networks, and endpoints for cyberattacks is a part of good cybersecurity operations. Many tools are available to assist with real-time analytics-based detection.

#### **FAQ**

- Can the AC2000 system support multiple CDC servers?
   Yes, some systems can have multiple CDC servers with one designated as the primary CDC and the others as hot standbys.
- What is the maximum number of RTCs supported by each CDC?
   Each CDC supports up to 256 RTCs.
- How many types of Workstation applications can be installed on one machine?
   Up to three types of Workstation applications may be installed on one machine if required.

# **Documents / Resources**



# Johnson Controls CEM AC2000 Security Management System [pdf] User

Guide

CEM AC2000 Security Management System, CEM AC2000, Security Management System, Management System

### References

- User Manual
- Johnson

Controls

◆ CEM AC2000, CEM AC2000 Security Management System, Johnson Controls, Management System, Security Management System

# Leave a comment

Your email address will not be published. Required fields are marked \*

Save my name, email, and website in this browser for the next time I comment.

Comment *	
Name	
Email	
Website	

# **Post Comment**

### Search:

e.g. whirlpool wrf535swhz

**Search** 

Manuals+ | Upload | Deep Search | Privacy Policy | @manuals.plus | YouTube

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.