CEM AC2000 v10.5

Hardening Quick Start Guide

GPS0020-CE-20210625-EN
Rev C

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 Quick Start 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.

Legal disclaimer

The cybersecurity practices described in this guide are recommended practices to facilitate the secure installation and configuration of the products described herein. However, Johnson Controls cannot guarantee that the implementation of the cybersecurity practices or recommendations described in this guide will ensure the security of the relevant product or system, or prevent, or alter the potential impact of, any unauthorized access or damage caused by a cybersecurity incident. This guide is provided “as is”, and Johnson Controls makes no representation or warranty, 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

Contents

Introduction ... 2
Legal disclaimer ... 3
Support ... 4
1. Overview ... 6
1.1 Deployment architecture ... 7
1.1.1 Components ... 7
1.1.2 Core Components ... 8
1.1.3 Supporting Components ... 9
2. Hardening CEM AC2000 ... 9
2.1.0 Hardening Checklist ... 9
3. Networks ... 9
3.1.0 Ports ... 10
4. Personal data ... 10
5. Password configuration options ... 11
5.1 Enforcing regular password changes ... 11
5.2 Setting the account deactivation limit ... 11
5.3 Setting the account lock out attempts limit ... 11
6. Software updates ... 12
7. Adobe® Flash Player ... 12
8. Transport Layer Security (TLS) settings ... 12
8.1 AC2000 System not using Emerald card reader(s). ... 12
8.2 AC2000 System using Emerald card reader(s). ... 13
9. Changing the default password on an Emerald card reader. ... 13
10. Encryption at rest ... 13
11. External systems ... 14

1. Overview

The AC2000 solution is a powerful and reliable enterprise access control and integrated security management system. As CEM manufacturers 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 three solution options, providing reliable and innovative access control for any sized site.

- **AC2000 Lite** – A feature rich yet cost-effective access control and security management system for small to medium sized sites. AC2000 Lite offers a complete IP access control solution. Using CEM intelligent IP card readers and CEM's leading Power over Ethernet access control solution, IT and Security administrators can take improve cost effectiveness by taking advantage of existing Ethernet network infrastructure.

- **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.

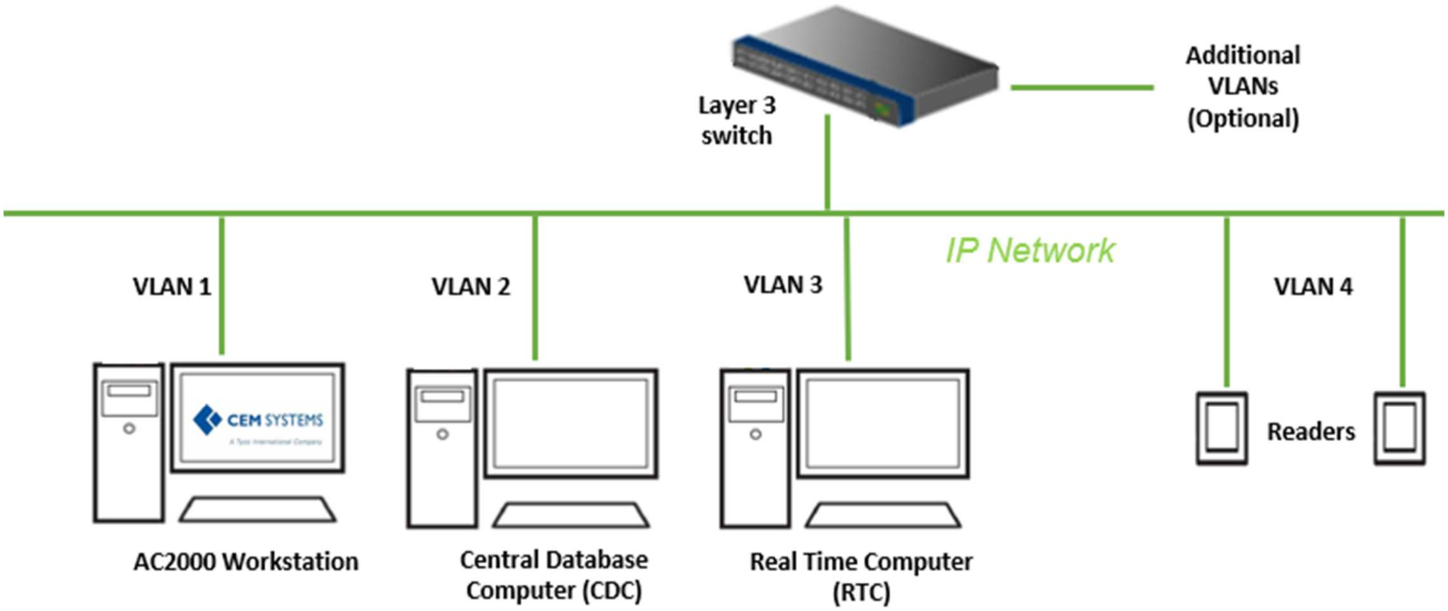
After selecting your AC2000 solution, there are three options for running the AC2000 system components:

1. Separate Real Time Computer (RTC) and 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*

This document provides guidance on how to harden and operate an AC2000 system securely.

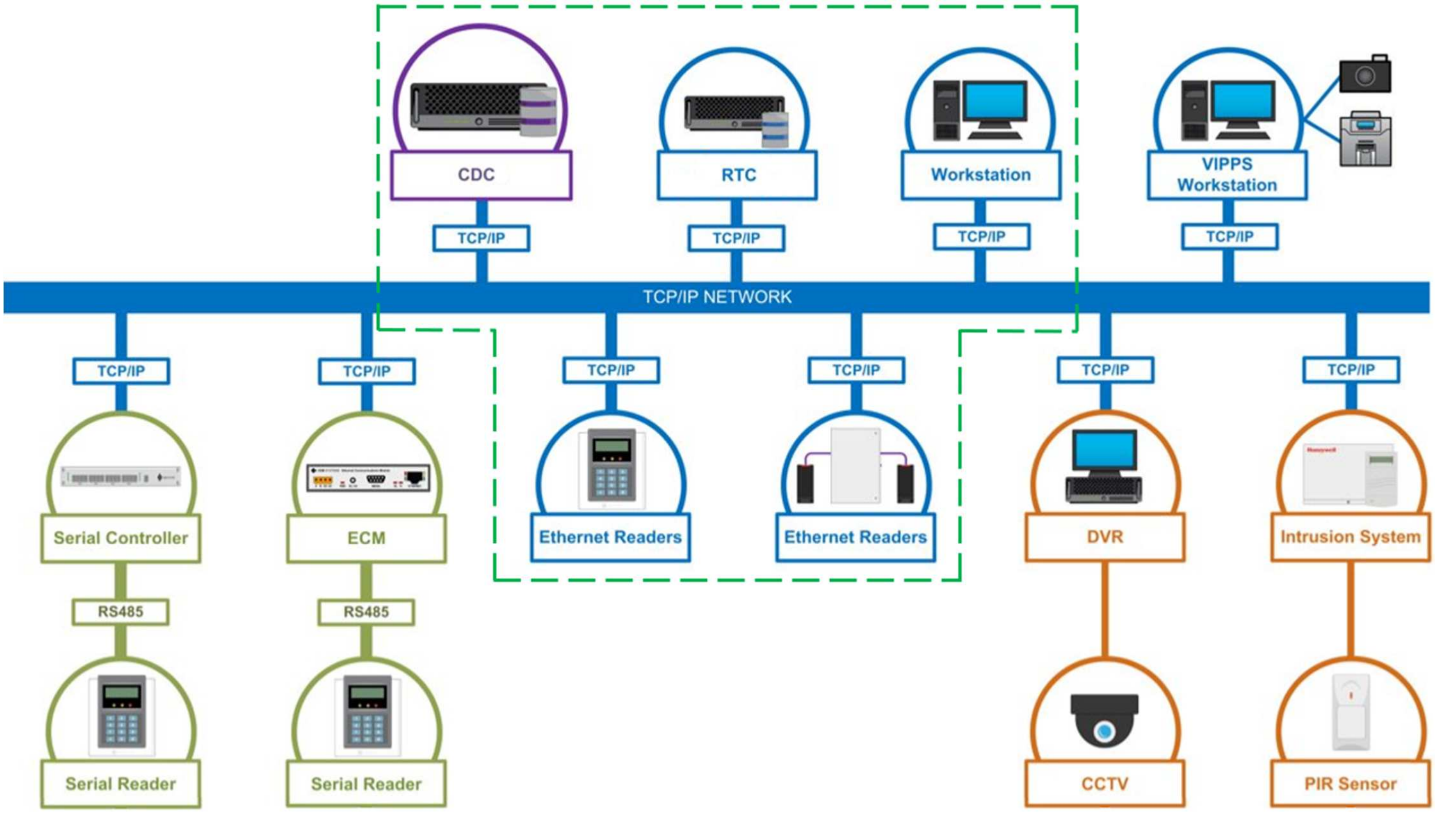
1.1 Deployment architecture

Figure 1: Typical reader deployment architecture



1.1.1 Components

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



1.1.2 Core Components

Shown above 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 can be used 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 TCPIP. Typical card readers include Serial readers and Ethernet readers.

Note: Sections 8.0 and 9.0 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.

- **AED Workstation**
  Used for viewing Alarm events, monitoring alarms and events on a graphical display

1.1.3 Supporting Components

An AC2000 access control system can seamlessly integrate with external systems; CCTV, 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. CCTV/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.

Closed Circuit Television (CCTV)

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

Passive Infrared Sensor (PIR)

PIR motion detection.

2. 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.

2.1.0 Hardening Checklist

Hardening Step 1: Internet and firewall protection. 9

Hardening Step 2: Block all ports that are not in use. 10

Hardening Step 3: Enforce regular password changes 11

Hardening Step 4: Account deactivation limit 11

Hardening Step 5: Account lock out attempts 11

Hardening Step 6: Update software 12

Hardening Step 7: Remove TLS 1.0 & 1.1 when not using an Emerald card reader 133

Hardening Step 8: Change default password on Emerald card reader 13

3. 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.

3.1.0 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:

Table 1: Port numbers and protocols

Port	Protocol	Devices
22	SSH	CDC server/RTC client and RTC server/CDC client
80	HTTP	CDC server/V3 portables client
123	NTP	NTP server/CDC client
137	Samba SMB	CDC server/workstation client
138	Samba SMB	CDC server/workstation client
139	Samba SMB	CDC server/workstation client
443	HTTPS	CDC server/workstation client The V3 portables client uses this port.
445	Samba SMB	CDC server/workstation client
5010	CEM Comms	CDC server/RTC client and CDC server/workstation client
5060	OpenSips	CDC Server and Workstation/Reader Client
5405	Corosync UDP	CDC server/CDC client **Note:** This port is only for fail-over systems.
5432	ODBC/Postgres	CDC server/workstation client
5553	MDC	RTC server/reader client
5554	PBP	Reader server/RTC client
5555	PBP	Secondary reader server/RTC client **Note:** Only the EDCM in master/master mode, and the 90x0 server/CDC client use this port.
5556	90x0	90x0 server/CDC client
9999	TCP	RTC server/Aperio client
6666	Reader diagnostics	Reader server/diagnostic client
7789	DRBD	CDC server/CDC client **Note:** This port is only for fail-over systems.

4. 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 card holder.

5. 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.

5.1 Enforcing regular password changes

Hardening Step 3: Enforce regular password changes

To enforce users to change their password on a regular basis, complete the following steps:

a. Log on to AC2000.
b. Open the Configured application.
c. From the **Parameters** list, select the parameter passwd_force_change_days.
d. 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.
e. Click **Save**.

5.2 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 time period. To set the account deactivating limit, complete the following steps:

a. Log on to AC2000.
b. Open the Configured application.
c. Click **Add**.
d. In **Configured Parameters** pane, in the **Name** field, enter user_lock_days.
e. 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.
f. In the **Comment** field, enter automatic account lock out.
g. Click **Save**.

5.3 Setting the account lock out attempts limit

Hardening Step 5: Account lock out attempts

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

a. Log on to AC2000 WEB.
b. Click **AC2000 Setup** and click **Web Login Config**.
c. 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.
d. 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*.

Account Locked alarm. When an account is locked out, the system generates ad alarm on the Security Hub application is enabled.
To enable the account locked alarm, complete the following steps:

a. On the AC2000 Floatbar, click **Advanced Configuration**, and click **Configured**.
b. Select the **enable_lockout_alarm** setting.
c. In the **Value** field, type **Y** to enable the alarm.
d. 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.

6. Software updates

Hardening Step 6: Update software

Always update to the latest software version. For more information, see ***Error! Reference source not found.***.

7. Adobe® Flash Player

The AC2000 system does not require Adobe® Flash Player for any application. It is best practice that you do not install it on your workstation.

Note: Adobe no longer supports Flash Player after December 31, 2020 and blocked Flash content from running in Flash Player January 12, 2021. For more information see the “Adobe Flash Player EOL General Information Page” - https://www.adobe.com/products/flashplayer/end-of-life.html

8. Transport Layer Security (TLS) settings

The AC2000 system can be configured with or without using Emerald card readers. If you are using Emerald card readers, then you must also use TLS 1.0 for them to function properly.

Table 2: Final hardening step

System Configuration	Hardening Step	Description
Not using Emerald card readers	Step 7 – Section 8.1	Remove older TLS versions
Using Emerald card readers	Step 8 – Section 9.0	Change Emerald default password

Note: Hardening steps 7 and 8 are designed for two different system configuration options. You should only need to perform step 7 or 8, depending on your system configuration.

8.1 AC2000 System not using Emerald card reader(s).

For an AC2000 system that does not use Emerald card readers, use TLS 1.2 or higher.

Note: If you are using an Emerald card reader, please skip to section 9.0.

Hardening Step 7: Remove TLS 1.0 & 1.1 when not using an Emerald card reader

To harden an AC2000 system that does not use Emerald card readers, contact CEM support to remove TLS 1.0 and TLS 1.1 from the system. For more information, see ***Error! Reference source not found.***.

8.2 AC2000 System using Emerald card reader(s).

AC2000 systems that use Emerald Card readers must support TLS 1.0 to work properly.
Please ensure that TLS version 1.0 is installed on your system prior to moving to section 9.0.

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

It is best practice to change the default password on all emerald readers as shown below

Hardening Step 8: Change default password on 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 reader that you want to change the password on.
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:
    - ssh 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 passwd
10. On the **New Password** line, enter the new password.
11. On the **Retype Password** line, enter the new password again.
12. To logout of the emerald reader, type logout
13. Log onto AC2000 Floatbar, click **Device Configuration**, and click **Devices**.
14. From the navigation tree, select the emerald reader that you changed the password on.
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.

10. Encryption at rest

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

11. External systems

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