# CAM+ Best Practice Guide (for Customer Admins)

**Version 1**

**12/2025**

## Contents

## 1. Introduction

CAM+ is a cloud-based environmental monitoring system used to continuously measure temperature, humidity, $CO_2$, $O_2$, differential pressure, and other critical environmental conditions across controlled environments.

CAM+ consists of the following components:

- **Wireless sensors**: which measure parameters such as temperature, CO2, 02, etc
- **The WARP**: which receives and stores data from sensors, sends a copy of the data to the cloud, and triggers an alarm if a sensor goes out of range or a device cannot communicate with the cloud
- **Signal repeaters**: which relay data from sensors to the WARP if there is poor signal due to distance or obstructing items
- **The CAM+ Website**: a cloud portal that allows you to view sensor data, reports, and documents; complete incident audits (recording what was done to resolve an alarm); and manage users and account settings.

This guide provides clear best practices for operating CAM+ effectively and compliantly.

## 2. Onboarding New Staff

Follow the steps below when onboarding new staff to ensure they have access to the system, know what their responsibilities are, and know how to complete them.

### Permissions Required

- You must be a Customer Admin to add users.
- You must have the Manage Contacts permission to add contacts and allocate them to contact lists.

*Note*: You can check your permissions by clicking the Edit Profile button on the CAM+ Website homepage. If you can't see the Edit Profile button, that means you're a Customer Admin and have all permissions enabled.

### Best Practice

- Clearly define and communicate the tasks new staff members are responsible for (e.g. completing incident audits, approving incident audits, managing contact lists, managing isolations, managing setpoints, signing reports, etc.).
- Create new user accounts for new staff members on the CAM+ Website and ensure they have the correct permissions to perform the tasks they are responsible for.

  *Note*: If your account uses Single Sign-On, your IT department must add users to the Checkit App in your identity provider account (e.g., Microsoft Entra, Google Workspace, Okta, etc.) before you can create the user on the CAM+ Website.
- If you want the new staff members to receive alarm notifications, add them as a contact and allocate them to contact lists.
- Use the onboarding email template on page 3 to formally communicate access, responsibilities, and required learning resources.

## Email Template

Dear [**add name**],

A user account has been created for you on CAM+ (the system we use to monitor environmental conditions such as temperature and humidity).

You are a [**Standard User / Customer Admin**].

Your responsibilities include:

- [**Add responsibilities e.g. completing incident audits, approving incident audits, managing contact lists, etc.**]

You can access your account at camplus.checkit.net

In order to learn about the CAM+ System, please:

- Watch the CAM+ Training Videos
- Read the CAM+ Best Practice Guide
- Download the CAM+ Quick-Start Guide and save it on your desktop
- Save the Help Centre link to your bookmarks

Kind regards,

[**Add name]**

## 3. User Management

There are 2 types of users: Customer Admins & Standard Users.

- **Customer Admins** have all permissions enabled and are the only users who can manage user accounts, including creating users, editing permissions, and reactivating passwords and PINs.
- **Standard Users** are granted a custom set of permissions assigned per department (for example, completing incident audits or managing isolations within a specific department). See User Permissions for details.

Both Standard Users' and Customer Admin's passwords and PINs expire after a configurable period, up to a maximum of 365 days.

When a password or PIN expires, the user cannot log in to the CAM+ Website. If access is still required, a Customer Admin must reactivate the password and PIN. Reactivation unlocks the existing credentials; the user is not required to create a new password or PIN.

Customer Admins cannot reactivate their own password or PIN and must request reactivation from another Customer Admin.

*Note*: If your account uses Single Sign-On, Customer Admins only need to reactivate PINs. Passwords are managed by your Identity Provider (e.g., Microsoft Entra, Google Workspace, Okta, etc.)

---

### Permissions Required

- You must be a Customer Admin to manage users.

*Note*: You can check your permissions by clicking the Edit Profile button on the CAM+ Website homepage. If you can't see the Edit Profile button, that means you're a Customer Admin and have all permissions enabled.

---

### Best Practice

- Clearly define and communicate ownership of tasks (such as completing and approving incident audits, managing contact lists, isolations, setpoints, and signing reports, etc.) and ensure users have the correct permissions to perform them.

  *Note*: Customer Admins can edit a user's permissions if necessary, see Modify a User for instructions. See User Permissions for a full description.

- Ensure there are at least two Customer Admins on the system at all times.
- Review user accounts quarterly to confirm users still require access and that permissions align with their current responsibilities.
- Proactively reactivate passwords and PINs before they expire if users still require access.
- Immediately delete users when staff leave.

  *Note*: If your account uses Single Sign-On, users must also be deleted from your identity provider (e.g. Microsoft Entra, Google Workspace, Okta).

## 4. Alarms & Incident Audits

An alarms is triggered if a sensor goes out of range, a device cannot communicate with the cloud, a device has low battery, or a signal repeater/ the WARP is disconnected from the mains power.

Alarms triggered by sensors require the completion of an incident audit, recording what was done to resolve the issue.

### Permissions Required

- You must have the manage Incidents permission to complete the first 3 fields of an incident audit.
- You must have the Approve Incidents permission to complete the 4th and final field of an incident audit "Supervisor Sign-Off".

*Note*: You can check your permissions by clicking the Edit Profile button on the CAM+ Website homepage. If you can't see the Edit Profile button, that means you're a Customer Admin and have all permissions enabled.

### Best Practice

- Ensure your organisation has an SOP in place for alarm response and incident audit handling, ensure relevant staff are trained on these procedures, and upload the SOPs to the Documents Library for reference and audit evidence.
- Clearly define and communicate who is responsible for completing and approving incident audits and ensure they have the appropriate permissions to do so.

  *Note*: Customer Admins can edit a user's permissions if necessary, see Modify a User for instructions.
- Respond to alarms immediately to protect products and maintain compliance.
- Only accept an alarm if you can dealt with it promptly (no further contacts will not be notified of the alarm if you accept it).
- If you receive a monitoring alarm, resolve it as soon as possible (see WARP Troubleshooting). We are unable to notify contacts of alarms while the WARP is offline.

- If you receive a probe failure alarm, resolve it as soon as possible (see Probe Troubleshooting) No readings will be recorded while the probe is disconnected from the transmitter.
- If you receive a transmitter offline alarm, resolve it as soon as possible (see Transmitter Troubleshooting). Readings will be stored on the sensor until the device is back online, but the sensor will not be able to trigger alarms if it goes out of range and data will be overwritten after 7 days.
- If you receive a battery low alarm, replace the battery in the transmitter as soon as possible.
- If you receive a signal repeater offline alarm, resolve it as soon as possible (see Signal Repeater Troubleshooting). Readings will be stored on the sensor until the device is back online, but , but the sensor will not be able to trigger alarms if it goes out of range and data will be overwritten after 7 days.
- Complete & approve incident audits promptly (same day where possible).
- Complete each field of an incident audit as you deal with the issue so that other staff are aware of its status (don't complete all fields at the end once the issue has been resolved).
- Use standard comments when completing incident audits for consistent reporting.

  *Note*: Customer Admins should contact us if you want to modify your standard comments.

# 5. Reporting

You can generate a range or reports on sensor data, alarms, setpoints, user activity, and isolations and save them to your device or the Documents Library.

### Permissions Required

- You must have the General Access permission to generate reports.
- You must have the Manage Libraries permission to save reports to the Documents Library.
- You must have the Sign Reports permission to add a second signature to a report.

*Note*: You can check your permissions by clicking the Edit Profile button on the CAM+ Website homepage. If you can't see the Edit Profile button, that means you're a Customer Admin and have all permissions enabled.

### Best Practice

- Clearly define and communicate who is responsible for generating reports, who is responsible for adding a second signature to reports, how often they should do so, and ensure they have the correct permissions to do so

  *Note*: Customer Admins can edit a user's permissions if necessary, see Modify a User for instructions. See User Permissions for a full description.
- Save reports to the Documents Library, rather than storing them locally, to maintain a central audit record.
- Add a second signature to applicable reports to ensure they are reviewed by an authorised user.
- Generate a Check Readings Report daily (or per shift, where required) to verify current conditions.
- Customer Admins should review the monthly Alarm KPI Report in order to identify recurring excursions or faults and download a copy of it before the end of every month.
- Customer Admins should periodically save a copy of the User Audit Report.
- Contact us if data is missing from sensor data reports due to a sensor having been offline and we will retrieve the missing data.

# 6. Documents Library

The Documents Library is a central repository where you can store and access system-generated reports, user-uploaded documents, and files provided by Checkit.

### Permissions Required

- You must have the Manage Libraries permission to save and upload files.
- You must have the Sign Reports permission to add a second signature to a report.
- You must be a Customer Admin to delete files and create and delete folders.

*Note*: You can check your permissions by clicking the Edit Profile button on the CAM+ Website homepage. If you can't see the Edit Profile button, that means you're a Customer Admin and have all permissions enabled.

### Best Practice

- Clearly define and communicate who is responsible for managing the library (i.e., saving reports, signing reports, uploading and deleting files, etc.) and ensure they have the correct permissions to do so.

  *Note*: Customer Admins can edit a user's permissions if necessary, see Modify a User for instructions. See User Permissions for a full description.
- Save reports to the Documents Library, not to local devices.
- If you download a file from the library, ensure that it is saved to a secure location.
- Add a second signature to reports promptly where required.
- Upload relevant SOPs (for example, procedures for handling service interruptions) and reference documents such as equipment or refrigeration unit user manuals to the Documents Library so they are centrally available for staff and audits.
- Do not delete documents unless you are certain they are no longer required (outdated documents may be required to demonstrate past compliance).
- Use standard naming conventions when uploading files.

- If you create a folder and its contents are:
    - Only relevant to a specific department, create a local folder
    - Relevant to all departments, create a global folder
- Review the library quarterly to ensure proper organisation and completeness.

## 7. Contacts

Contacts are people who receive alarm notifications via phone call, SMS, and email.

They are allocated to contact lists: a group of contacts who receive alarm notifications triggered by a sensor group at designated times such as during working hours, non-working hours, weekends, public holidays.

### Permissions Required

- You must have the Manage Contacts permission to create, allocate, modify, disable, and delete contacts and modify a contact list's start and end date/time.

*Note*: You can check your permissions by clicking the Edit Profile button on the CAM+ Website homepage. If you can't see the Edit Profile button, that means you're a Customer Admin and have all permissions enabled.

### Best Practice

- Clearly define and communicate who is responsible for managing contacts and ensure they have the correct permission to do so.

  *Note*: Customer Admins can edit a user's permissions if necessary, see Modify a User for instructions. See User Permissions for a full description.

- Ensure each contact list has at least 8 contacts for adequate coverage.
- When allocating contacts, configure the contacts to receive notifications by all 3 methods: phone call, SMS, and email.
- If a contact is not configured to receive notifications via phone call, place them at the bottom of the list.
- If a contact's phone number is direct dial during the day but routes through a switchboard at night, create the contact twice, for example, "John Smith (Day)" and "John Smith (Night)".
- For public holidays such as New Year's Day, configure a start and end date/time on the special-occasion contact list (e.g. 01/Jan/2026 00:00 – 02/Jan/2026 09:00) and ensure the appropriate contacts who will be working during the public holiday are assigned to the special-occasion contact list. This will override the regular contact list for that period.

- Review contact lists quarterly to ensure they are up to date.
- Delete contacts when staff leave your organisation.

# 8. Isolations

An isolation is a period during which a sensor's alarms are suspended.

You may want to create an isolation if a unit is going to be temporarily out of use or undergoing scheduled maintenance.

During the isolation period, the sensor will not trigger an alarm if it exceeds its high setpoint/ falls below its low setpoint, but it will continue to take readings.

You can create a one-time isolation or a recurring isolation on a specific day of the week.

The isolation will end automatically at the end of the time period and the sensor will resume triggering alarms.

---

**Permissions Required**

- You must have the Manage Isolations permission enabled to create, modify, and disable isolations.

*Note*: You can check your permissions by clicking the Edit Profile button on the CAM+ Website homepage. If you can't see the Edit Profile button, that means you're a Customer Admin and have all permissions enabled.

---

**Best Practice**

- Clearly define and communicate who is responsible for managing isolations and ensure they have the correct permission to do so.

  *Note*: Customer Admins can edit a user's permissions if necessary, see Modify a User for instructions. See User Permissions for a full description.

- Create isolations in advance before the unit is out of service.
- After the isolation period has ended, ensure the sensor is back in range before returning products to the unit.
- Keep isolation windows as short as possible.
- When creating isolations, add clear comments describing the reason for the isolation.
- Use recurring isolations only for predictable, routine tasks (e.g., weekly maintenance).

- Modify recurring isolations if scheduled maintenance times change.
- Disable isolations if they are no longer necessary.
- Review isolation activity quarterly to ensure they are being used correctly.

# 9. Setpoints

A setpoint is the acceptable range (for example, temperature range, humidity range, etc.) and alarm delay period of a sensor.

For example, a temperature sensor in a blood transfusion fridge may be configured to trigger an alarm if it exceeds 6°C or falls below 1°C for more than 10 minutes.

You may want to modify a setpoint if the contents of a unit changes and requires a different acceptable range.

---

**Permissions Required**

- You must have the Manage Settings permission to modify a setpoint.

*Note*: You can check your permissions by clicking the Edit Profile button on the CAM+ Website homepage. If you can't see the Edit Profile button, that means you're a Customer Admin and have all permissions enabled.

---

**Best Practice**

- Clearly define and communicate who is responsible for managing setpoints and ensure they have the correct permission to do so.

  *Note*: Customer Admins can edit a user's permissions if necessary, see Modify a User for instructions. See User Permissions for a full description.

- Modify a setpoint if a unit's contents changes and requires a different acceptable range.
- Record a clear reason for each setpoint change.
- Review setpoints quarterly or following equipment or process changes.
- Avoid excessive alarm delays that could mask real issues.

## 10. When Staff Leave

Follow the steps below when staff leave to ensure their access is removed

### Permissions Required

- You must be a Customer Admin to delete users.
- You must have the Manage Contacts permission to delete contacts.

*Note*: You can check your permissions by clicking the Edit Profile button on the CAM+ Website homepage. If you can't see the Edit Profile button, that means you're a Customer Admin and have all permissions enabled.

### Best Practice

- Delete users when they leave your organisation to ensure they no longer have access to CAM+.

  *Note*: If your account uses Single Sign-On, users must also be deleted from your identity provider (e.g. Microsoft Entra, Google Workspace, Okta).

- Delete contacts when they leave your organisation to ensure they no longer receive alarm notifications.

## 11. Service Interruptions

CAM+ is designed to be highly reliable and is available 99.9% of the time. However, there may be rare occasions where the system is temporarily unavailable due to either planned maintenance or unplanned outages.

### Planned Outages

From time to time, scheduled maintenance may be required to maintain system performance and security. We aim to keep planned outages as infrequent and as short as possible.

- Planned outages are communicated at least 30 days in advance.

### Unplanned Outages

In rare cases, an unexpected outage may occur.

- You will be notified as soon as possible if an unplanned outage occurs.
- Our teams will work to restore service as quickly as possible.

### What Happens During an Outage

CAM+ has a robust architecture with redundancy built in to protect your data.

- Sensors continue to take readings as normal.
- Readings are stored locally on the WARP while the cloud service is unavailable.
- You will not receive alarm notifications during the outage.
- You may not be able to log in to the CAM+ Website.
- You can continue to view live sensor readings and monitor alarms directly on the WARP display panel.

### What Happens When CAM+ Comes Back Online

Once the service is restored:

- You will be notified as soon as CAM+ is back online.
- You will be able to log in to the CAM+ Website as normal.
- Alarm notifications will resume.
- All sensor data stored on the WARP will be automatically uploaded to the cloud, within a maximum of 48 hours.

- No data is lost during the outage.

---

**Best Practice**

- Ensure your organisation has an SOP in place for operating during CAM+ service interruptions, ensure relevant staff are trained on these procedures, and upload the SOPs to the Documents Library for audit and operational reference.
- During an outage, use the WARP display panel to monitor conditions sensor readings and alarms.
- After the outage, contact us if you need missing data urgently (i.e. you cannot wait up to 48 hours).

## 12. General Upkeep

Regular system upkeep helps ensure your CAM+ system remains compliant and reflects current operational responsibilities. Periodic reviews also reduce the risk of missed alarms, incorrect escalation, or unauthorised changes.

---

### Permissions Required

- Customer Admins should perform general upkeep.

*Note*: You can check your permissions by clicking the Edit Profile button on the CAM+ Website homepage. If you can't see the Edit Profile button, that means you're a Customer Admin and have all permissions enabled.

---

### Best Practice

- Review user accounts to ensure access and permissions remain appropriate. Modify and delete users if necessary.

  *Note*: If your account uses Single Sign-On, users must also be deleted from your identity provider (e.g. Microsoft Entra, Google Workspace, Okta).

- Ensure there are at least two Customer Admins registered on your account. Add Customer Admins if necessary.
- Proactively reactivate passwords and PINs before they expire if users still require access.
- Review contact lists to ensure there are at least 8 contacts allocated. Allocate additional contacts if necessary.
- Review setpoints to ensure they still align with operational requirements. Modify setpoints if necessary.
- Review isolations to confirm they are being used appropriately and are not left active unnecessarily. Disable isolations if necessary.
- Review alarm trends and recurring incidents to identify underlying issues.
- Refresh staff training and confirm users understand their responsibilities.

# 13. Audit Preparation

CAM+ provides a range of reports and documents that you can save and download to evidence system configuration, user governance, alarm management, and incident handling for internal reviews and external audits.

When generating reports, you can select a date range of up to 2 months and view data from the previous 2 years.

### Permissions Required

- Customer Admins should prepare for audits.

*Note*: You can check your permissions by clicking the Edit Profile button on the CAM+ Website homepage. If you can't see the Edit Profile button, that means you're a Customer Admin and have all permissions enabled.

### Best Practice

- Generate a Sensor Summary Report to evidence the minimum, maximum and average readings of all sensors during the audit period.
- Generate a Sensor Incident List Report to evidence incidents that occurred during the audit period.
- Generate a User Audit Report to evidence user activity on the CAM+ Website (e.g. logins, changes to setpoints, etc.) during the audit period.
- Generate an Isolation History Report to evidence reasons for pausing alarms during the audit period.
- Generate an Alarm Settings Report to evidence current alarm setpoints.
- Download Check Readings Reports from the Documents Library  (filed under *Documents Library> System Users>Check Readings Record*) to evidence sensor readings during the audit period.
- Download the Operational Qualification from the Documents Library (filed under *Documents Library>System Installation*) to evidence that Checkit meets required standards and regulations.
- Download the Installation Qualification from the Documents Library (filed under *Documents Library>System Installation)* to evidence that Checkit meets required standards and regulations.

- Download Calibration Certificates from the Documents Library (filed under *Documents Library>System Installation)* to evidence that Checkit meets required standards and regulations.
- Download Website Validation Documents from the Documents Library (filed under *Documents Library>Website Validation)* to evidence that Checkit meets required standards and regulations.

## 14. Recommended Optional Feature

CAM+ includes optional features that can improve alarm response, security, and workflow efficiency. These can be enabled on request.

### Recommended Enhancements

- **Alarm Dashboard**
  Consider upgrading to the Alarm Dashboard to view live alarms across your department or site in real time.
- **Single Sign-On (SSO)**
  Consider enabling Single Sign-On for improved security and simpler authentication for all staff.
- **Password/PIN Expiry Reminder Service**
  Consider enabling automatic password/PIN expiry reminders to reduce login problems and admin workload.
- **Targeted Alarm Notification Routing**
  Consider using Automatic Notifications so specific alarm types notify specific team members automatically.
- **Cleared Alarms Notifications**
  Consider enabling Cleared Alarms so staff are notified when conditions return to normal.
- **Asset Intelligence (Advanced Analytics)**
  Consider upgrading to Asset Intelligence for insights into equipment performance and long-term trends.
- **Sensor Alerts (Early Warning Thresholds)**
  Consider using Sensor Alerts for early warnings before alarms occur, reducing product and compliance risk.