checkit

CAM+ Best Practice Guide (for Standard Users)

Version 1

12/2025

checkit

Contents

1. Introduction 1
2. Alarms & Incident Audits 2
3. Reporting 4
4. Documents Library 5
5. Contacts 6
6. Isolations 7
7. Setpoints 8
8. Service Interruptions 9

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. 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

- 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.

3. 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

- 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.
- Contact us if data is missing from sensor data reports due to a sensor having been offline and we will retrieve the missing data.

4. 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

- 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.
- Use standard naming conventions when uploading files.

5. 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

- 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.

6. 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

- 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.

7. 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

- 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.

8. 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 will 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

- Follow your organisation's standard operating procedures.
- 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).