Verkada

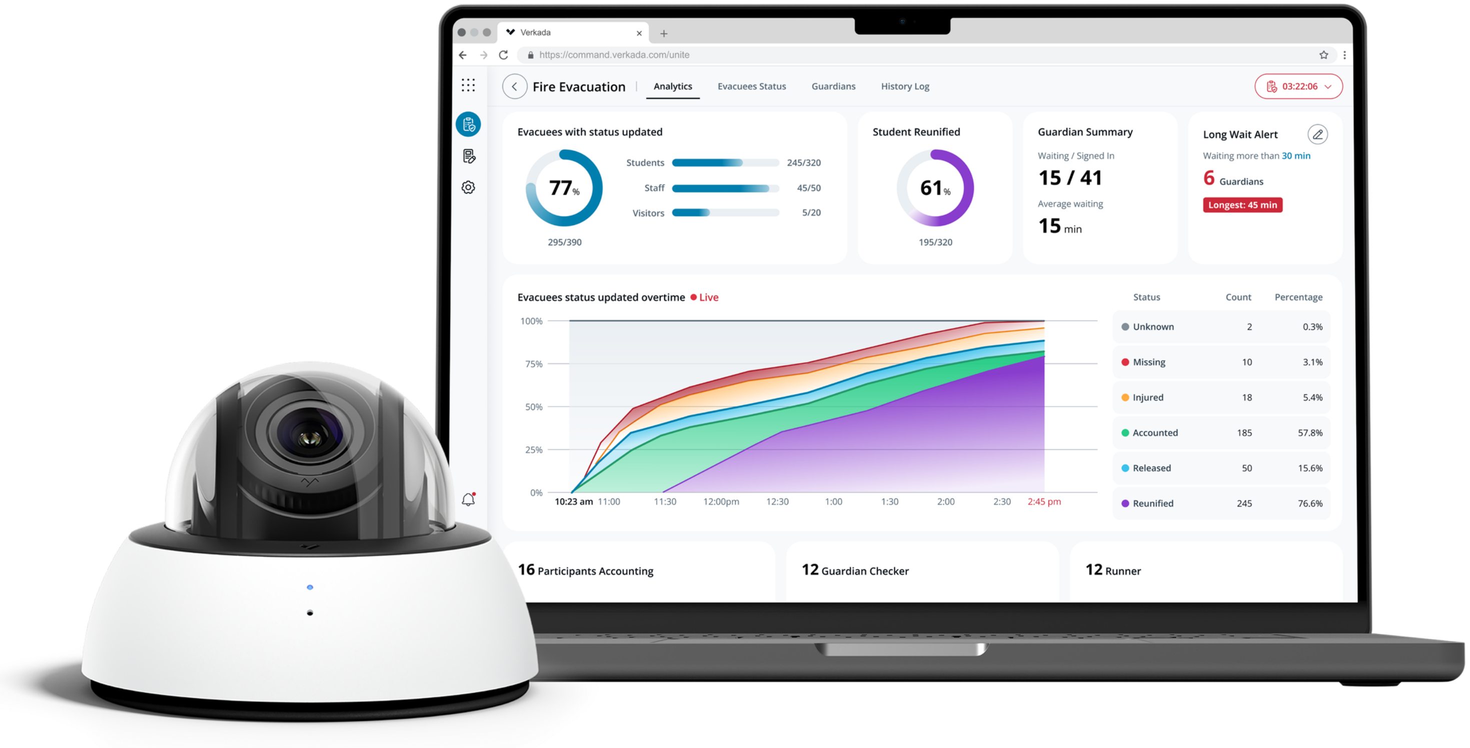
Incident Response User Guide

Table of contents

01. Overview

Verkada Incident Response provides a unified platform to manage daily campus operations and critical incidents, leveraging Verkada Guest to streamline visitor management and offer a specialized module for student reunification. This feature helps organizations account for employees and visitors and track the well-being and location of people during an emergency.

The platform is designed for a secure, traceable, and orderly response, modeled after the Standard Reunification Method (SRM) developed by The "I Love U Guys" Foundation. The system simplifies preparing for, managing, and investigating any type of incident through customizable response plans.



Evacuees with status updated

77%

295/390

Students	245/320
Staff	45/50
Visitors	5/20

Student Reunified

61%

195/320

Guardian Summary

Waiting / Signed In
15 / 41
Average waiting
15 min

Long Wait Alert

Waiting more than 30 min
6 Guardians
Longest: 45 min

Evacuees status updated overtime ● Live

Status	Count	Percentage
● Unknown	2	0.3%
● Missing	10	3.1%
● Injured	18	5.4%
● Accounted	185	57.8%
● Released	50	15.6%
● Reunified	245	76.6%

16 Participants Accounting

12 Guardian Checker

12 Runner

02. How to get started: setup and configuration

Incident Response is a product designed to help organizations track the status and location of people during an incident. It allows organizations to account for employees and visitors, and for schools, it supports the reunification of students with their guardians. Incident Response is included with the Workplace license at no additional cost.

2.1 Prerequisites and licensing

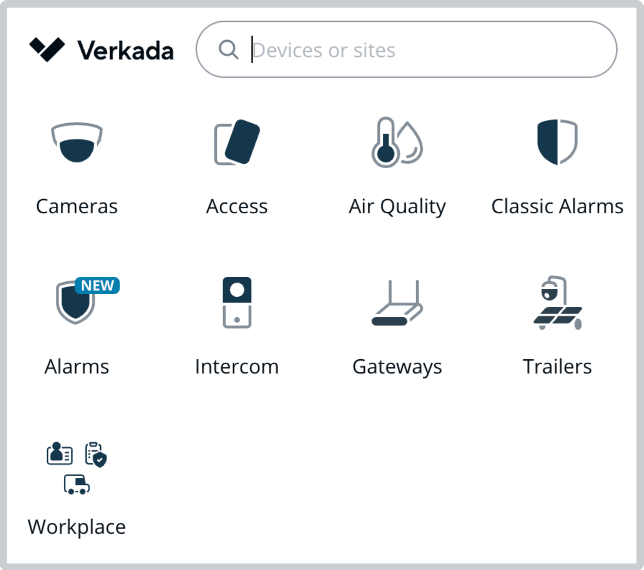
Incident Response is included with the Workplace license at no additional cost. However: Incident Response is only available in sites that *already* have Verkada Guest configured. Specifically, one Workplace license covers one Incident Response site.

2.2 Initial setup and configuration

To begin configuring Incident Response, you must be an org admin in Verkada Command.

01. Configuring the initial site

1. To activate Incident Response for your first Workplace site:
2. In Verkada Command, navigate to **All Products > Workplace > Incident Response**.
3. Click **Import Existing Guest Sites**.
4. Select your desired site and click **Import Site**.



02. Configuring additional sites

After successfully setting up your initial Workplace site for Incident Response, you can configure subsequent sites:

1. In Verkada Command, go to **All Products > Workplace > Incident Response**.
2. On the left navigation pane, click **Incident Response Settings**.
3. At the top of the settings page, select **Organization > Sites**.
4. Click **Import Site**.

2.3 Managing employee lists

Employees who are assigned to an Incident Response site are automatically shared across all Workplace products for that site, including Guest, Mailroom, and Incident Response. These employees are the individuals who can participate in any active response launched at that site.

Employee list management is split by role:

- Org admins hold permissions to manage the organization-level employee list.
- Workplace site admins are necessary to manage site-level employee lists.

To manage the employee list:

1. In Verkada Command, go to **All Products > Incident Response**.
2. On the left navigation, click **Settings**.
3. At the top, select **Sites > Employees**.
4. Select **View Employees**.
5. At the top, select **Manage Employees**.

It is best practice to maintain separate employee lists by site. This way, organizations can ensure that only the appropriate staff are involved in responding to location-specific incidents.

2.4 Connecting your SIS (K12-specific)

For schools, having accurate student and guardian information is critical. Connecting a student information system (SIS) to Verkada Guest ensures this data is ready without requiring duplicate work to maintain up-to-date contact information.

Available SIS syncs

Verkada Guest currently syncs with:

- Clever
- Classlink

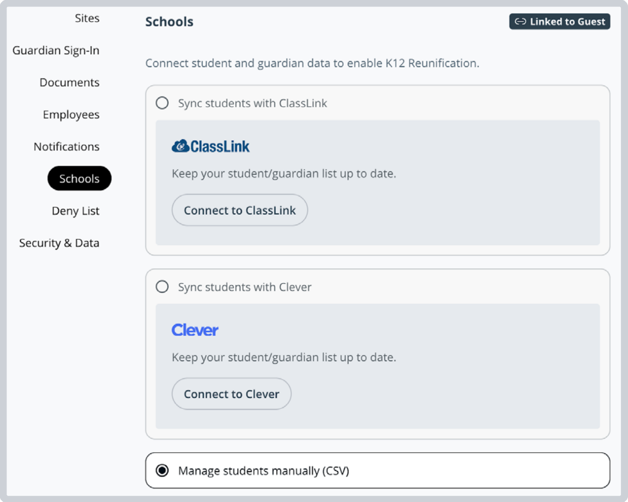
What gets synced

Once connected, Verkada Guest pulls key information from the connected SIS:

- Student information, like name, ID, and associated guardians.
- Guardian information, like name and contact details.
- Teacher, course, and section roster data (only available via SIS syncs with Clever and ClassLink. This information is not available when student lists are maintained manually.)

Connecting Incident Response with an SIS provider

To set it up, pick a sync for your school district in Guest Settings, in the Organization Tab, under Schools. See these articles on setting up SIS syncs.



Schools

Connect student and guardian data to enable K12 Reunification.

○ Sync students with ClassLink

Keep your student/guardian list up to date.

○ Sync students with Clever

Keep your student/guardian list up to date.

● Manage students manually (CSV)

Manually uploading student lists

Guest allows schools to manage student and guardian data through a manual CSV upload by following these steps:

1. Navigate to All Products > Workplace > Guest.
2. On the left navigation, click Guest Settings.
3. At the top, select Sites > [your site].
4. Under Student List, click Manage Student List.
5. In the top right corner, select Replace with CSV to upload a new file.

2.5 Workplace permissions

Action	Organization Admin	Workplace Site Admin	Workplace Employee
Opt in a site for Incident Response	✓		
Set up an SIS sync	✓		
Create response templates	✓	✓	
Configure site settings	✓	✓	
Manage site-level employee lists	✓	✓	
Launch/end a response	✓	✓	
Review active response progress from Command	✓	✓	
Contribute to an active response	✓*	✓*	✓

*Admins must be designated as Workplace employees to contribute to an active response.

03. Creating response templates for incidents

Workplace site admins can curate relevant response templates for different types of incidents. These templates ensure an organized, efficient, and traceable response by using pre-configured information tailored for potential scenarios.

Response templates are site-specific.

A response template defines the framework of an Incident Response protocol, it tracks:

- Who needs to be accounted for (evacuees).
- What statuses can be assigned to evacuees (e.g., **Safe**, **Unaccounted for**).
- Where evacuees can be marked as present, designated as locations.
- For schools, templates can also be configured for reunification.

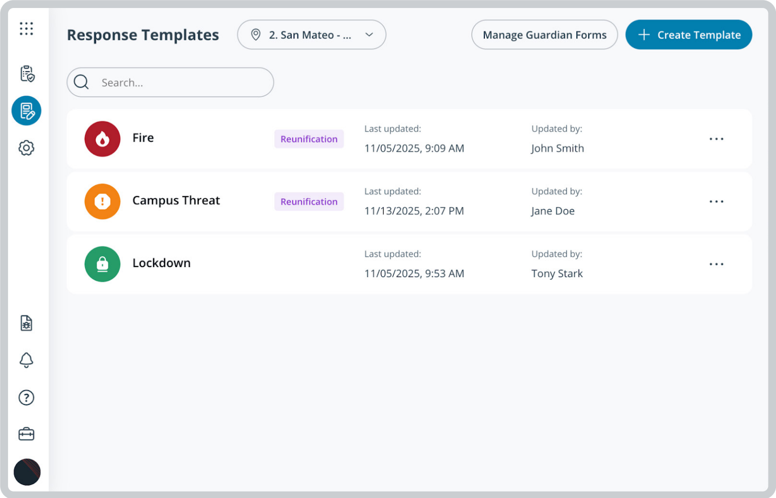
3.1 Steps to create a response template

1. In Verkada Command, go to **All Products > Incident Response**.
2. On the left navigation, click **Response Templates**.
3. At the top, select your site.
4. Select **Create Template**.

3.2 General template configuration

The initial setup requires filling out descriptive details for the template:

- Enter a unique template name.
- Choose a template color.
- Choose a template icon.
- Enter a descriptive template description.



Fire	Reunification	Last updated: 11/05/2025, 9:09 AM	Updated by: John Smith
Campus Threat	Reunification	Last updated: 11/13/2025, 2:07 PM	Updated by: Jane Doe
Lockdown		Last updated: 11/05/2025, 9:53 AM	Updated by: Tony Stark

3.3 Defining affected people (evacuees)

This critical setting defines who will be tracked and accounted for when the template is launched. Admins must identify all personnel types who should be managed during the emergency. You can select from these groups:

- **Staff** – All employees assigned to the site.
- **Visitors (profiles pulled from Guest)** – All visitors signed in and present on site the day the response is launched.
- **Students** – All students in the school linked to the site.
    - » For K12 customers, Student Information System (SIS) integrations (including Clever and Classlink) ensure student and guardian information is readily available, thus eliminating the need to manually create and continuously update rosters.

3.4 Customizing statuses and locations

Statuses and locations define how staff and responders track the people involved in an incident.

- **Evacuee statuses:**
  Define statuses that can be assigned to evacuees to accurately mark their current state. While customizing statuses is allowed, the unknown status is required. When reunification is enabled for a response template, there will also be a status called reunified. Additional statuses are fully customizable and must be configured when setting up a response template.
- **Location names:**
  Define assembly points, or locations where evacuees and guardians (if reunification is enabled) are expected to assemble.

3.5 Enabling reunification (K12-specific)

For K12 users, enabling the reunification feature integrates the principles of the Standard Reunification Method (SRM) to Incident Response. This allows for the safe and controlled release of students to guardians post-incident.

3.6 Configuring guardian forms for reunification (K12-specific)

Incident Response provides tools for schools to manage every step of a reunification event. Guardian forms are an essential component, allowing schools to collect required information from guardians before releasing students.

Admins can create either global forms, which can be used across multiple sites, or site-specific forms.

01. Global guardian forms

1. Global guardian forms require Command org admin permissions for creation.
2. In Verkada Command, go to **All Products > Workplace > Incident Response**.
3. On the left navigation, click **Incident Response Settings**.
4. Under Guardian Sign-In, select **Manage Guardian Forms**.
5. In the top right, select **Add Guardian Form**.
6. Enter a unique name and click **Save**.

02. Site-specific guardian forms

Site-specific guardian forms require at least Workplace site admin permissions for creation, but can also be created by org admins.

1. In Verkada Command, go to **All Products > Workplace Incident Response**.
2. On the left navigation, click **Incident Response Settings > your site**.
3. Under **Guardian Sign-In**, select **Manage Guardian Forms**.
4. In the top right, select **Add Guardian Form**.
5. Enter a unique name and click **Save**.

Configuration details

All guardian forms have mandatory and optional fields.

Required information	Optional fields
All guardian forms must collect the following information: • The guardian's name. • The names of the students they are requesting.	Organizations can choose to include the following optional steps in the form configuration: • Contact info (email and/or phone number). • Guardian photo • Security screening • Open response questions • Multiple choice questions • Questionnaires • Videos • PDFs • Documents

The security screening step is configured to require capturing an image of the guardian's ID at check-in. This process is used to extract the legal name and date of birth from the ID for verification purposes.

Assigning guardian forms to a response template

Once created, the guardian form must be assigned to a response template that is enabled for reunification. Staff must select the desired form when configuring the response template.

Employees who access the Incident Response portal (unite.my.verkada.com) during an active response will see the sign in guardians page for response templates where reunification is enabled. Workplace site admins can also view all signed-in guardians and their details on the guardians page in an active response in Command.

04. Launching and ending an active response

An active response is the operational phase of incident management where staff uses the predetermined response template to account for affected individuals and begin the process of control and potential reunification.

4.1 Launching a response

Only Workplace site admins and Command org admins have the necessary permissions to initiate a response.

Steps to launch a response

1. In Verkada Command, go to **All Products > Workplace >Incident Response**.
2. On the **Incident Response Home** page, click **Launch Response**.
3. Select the desired **Response Template**.

Optional: Using drill mode for practice

When launching, you have the option to toggle on drill mode to simulate the event for practice.
If drill mode is enabled, you may also toggle on notify staff to send notifications that include magic links to employees, allowing them to participate in the simulation.
Drills enable users to practice response protocols using the exact interface and instructions they would see in an actual emergency.

Initiating the response

- When a response is officially launched, all employees associated with the site will be sent notifications. These notifications include magic links to the Incident Response portal.
- At the beginning of a response, all evacuees (people defined in the template) are initially designated with a status and location of unknown.
- Staff can access the Incident Response portal via the magic link, without needing to sign-in to Command
- The event response dashboard, which is web-based and mobile-friendly, automatically syncs with Verkada Guest.

4.2 Ending a response

Ending a response is a measure taken once the incident has concluded. Note: Only Workplace site admins or org admins have the right permissions to end a response.

Steps to end a response

1. In Verkada Command, go to **All Products > Incident Response**.
2. On the Incident Response home page, click on the **Active Response**.
3. In the top right corner of an Incident Response, click on the timer.
4. Select the **End** button.
5. In the confirmation message that appears, select **End Incident.**

Post-incident notification

For non-drill responses, all employees are notified that the response has ended.

4.3 Running drills

Regular drills help your team build confidence and familiarity with emergency protocols.

See the following steps to set up:

1 **Create response templates**

Before running your first drill, set up response templates for different incident types. These templates define:
Who needs to be accounted for (students, staff, visitors)

- Available status options (safe, unaccounted for, reunited, missing, needs help)
- Assembly locations for evacuees and guardians

For K-12: Enable reunification and configure your guardian form

2 **Launch the drill**

Only Workplace site admins can launch a response:

- In Verkada Command, select your response template
- Toggle on Drill Mode
- Optional: Enable Notify Staff to send magic links to employees via email or SMS

3 **Staff participation**

When the drill launches, employees receive a magic link to access the Incident Response portal:

- Staff can join from any browser by clicking the magic link shared with them, or by going to unite.my.verkada.com to log in.
- All evacuees start with an "unknown" status and location

4 **Practice reunification (K-12)**

If reunification is enabled, staff can practice the full Standard Reunification Method (SRM):

- Access student and guardian data, including teacher and section assignments
- Check in guardians through the sign in guardians page
- Mark students as reunified once released to authorized guardians
- Practice designated roles: accountants, greeters, and reunifiers

5 **End and review**

- A Workplace site admin ends the drill, which locks further changes
- Review the drill from Command to see tracking logs and activity
- Debrief immediately with staff to gather feedback and identify improvements

05. The Incident Response portal & reunification flow

The Incident Response portal serves as the unified, operational interface for managing an active incident, specializing in the accountability and controlled release of individuals following a crisis. The portal utilizes processes modeled after the Standard Reunification Method (SRM) developed by The "I Love U Guys" Foundation.

5.1 Accessing the Incident Response portal

The Incident Response portal is a web page where employees can account for evacuees for an active Response.

When a response is launched (in either Incident or Drill mode), all Workplace employees in the site are sent a magic link via email and/or SMS. An employee can log into the portal directly at unite.my.verkada.com anytime.

5.2 Employee actions

Employees interact with the active response by updating critical information on affected people (evacuees) using the people status page.

1. **Updating status and location:** Employees can view, search for, and update the status and location of any evacuee.
2. **Tracking information:** Filters on the people status page allow employees to quickly find specific evacuees based on evacuee status, evacuee location, teacher & section (available only for K12 customers utilizing an SIS integration).

5.3 Controlled and secure reunification flow

The Incident Response feature facilitates a controlled release of students to their guardians post-incident. This process aligns with the SRM, which defines specific roles to ensure order.

Phase 1: Accountability Students are first assembled and accounted for. Staff responsible for this action are referred to as accountants.

Phase 2: Guardian check-in and verification As students are being accounted for, the system also manages the secure intake of parents/guardians.

1. **Guardian check-in:** Employees use the sign in guardians page on the portal. Staff can check in guardians on their behalf from their device.
2. **Guardian list monitoring:** The sign in guardians page defaults to showing all waiting guardians. Employees can filter the list to see all guardians (who have been checked in), denied guardians, or reunified guardians. Clicking on a guardian allows employees to see which student(s) the guardian requested to release and which employee processed the check-in.

Temporary guardians

Temporary guardian exceptions are a feature available when the guardian & student name step is enabled on a school guest type and the 'allow temporary guardian exceptions' option is selected. If a visitor selects a student they are not linked to, staff will be prompted to review the request on the Incident Response portal. There, staff can choose to either allow or deny the temporary guardian exception.

Note: Manual overrides are still possible. If a guardian exception is denied, staff can still manually allow entry by selecting the log and choosing Allow entry. If this occurs, the visitor is considered approved and students can be reunified with that individual. The visit details and audit logs will reflect whether the visitor was approved as a temporary guardian.

Phase 3: Release

- **Staging separation:** After successful verification, guardians can be directed to a separate staging area from the waiting guardians and students.
- **Reunification:** Designated reunifiers—trusted school staff or certified first responders — coordinate the student-guardian pairings.
  - » The **reunify students + guardians** page is used for this process. By default, this page shows student/guardian pairings where the student's current status is not unknown and not reunified. Reunifiers can use filters on this page to further refine the list of eligible student and guardian pairs.

5.4 Notifications to guardians

When a guardian successfully checks in at a reunification site, they immediately receive a text message confirming:

1. Check-in confirmation

When a guardian successfully checks in at a reunification site, they immediately receive a text message confirming:

- Their check-in has been recorded
- Staff are now coordinating their reunification with their student(s)

2. Reunification complete

Once staff mark the student as reunified and released to the guardian, a second text is sent confirming:

- The reunification process is complete
- Their student has been successfully released to their care

Note: In order for guardians to receive these notifications, organizations must ensure the guardian form collects contact information and the SIS sync shares phone number and email information.

06. Viewing and auditing past responses

The Verkada Incident Response platform is engineered to facilitate a secure and traceable response, allowing organizations to thoroughly review and audit actions taken during both drills and live emergencies.

6.1 Viewing active responses from Command

During an active incident or drill, Workplace site admins maintain a read-only view of the response directly from Command.

6.2 Auditing past responses

Once an incident is resolved, ending the response action locks further changes on the Incident Response portal. Past responses can then be audited directly from Command.

The Command interface provides comprehensive analytics designed to assess efficiency and accountability, including:

Key metrics and statuses

The audit view presents graphical data on accountability and reunification efficiency, such as:

- Evacuees with status updated (e.g., percentage of students, staff, and visitors accounted for)
- Students reunified (the percentage of students successfully reunified with a guardian).
- Evacuee statuses over time.
- Detailed status breakdowns (count and percentage) for status categories

Guardian and personnel summary

For templates utilizing the reunification feature, the audit view also includes a guardian summary:

- Metrics such as the number of guardians checked in and average waiting time.
- Tracking of staff involvement by defined roles (accountants, guardian checkers, and reunifiers).

6.3 Reviewing responses for improvement

The goal of auditing past responses is to support a cycle of continuous improvement.

- **Post-incident review:** After an event is resolved, organizations should review how the response went to better understand what transpired, identify areas that functioned well, and determine opportunities for improvement.
- **Updating plans:** Insights derived from the review process should be used to update response templates as needed, strengthening future readiness and response capabilities.

07. FAQs

Q: What is Incident Response?

A: Incident Response is a specialized response plan focused on tracking the location and well-being of people during an incident. For schools, it also includes a reunification feature for the safe and controlled release of students to their guardians, modeled after the 'I Love U Guys' Foundation's Standard Reunification Method.

Q: How does Incident Response ensure student rosters are accurate?

A: Through integrations with Student Information Systems (SIS) Clever and Classlink, student and guardian information can be automatically synced, eliminating the need to manually create and update rosters. Manual CSV uploads are also possible.

Q: Can I practice before a real emergency?

A: Yes. Incident Response scenarios can be converted into drills for practice using the exact interface used in an actual emergency by toggling on **Drill Mode** when launching a response.

Q: Is there an extra charge?

A: No. Incident Response is included with the Workplace license at no additional cost.