

Kio Staff Safe

Complete Guide

Table of Contents

Intro to Kio Staff Safe	4
Why Kontakt.io?	4
The components: a connected framework of IoT devices and apps	5
Kio Staff Safe app concepts and terminology	8
About staff duress alerts	10
Things to know	10
About the alert lifecycle	10
Alert notifications	12
Setup guide	13
Prerequisites	13
Required setup tasks	13
Advanced setup	15
Quick start guide	17
Sign in to Kio Cloud	17
Navigating Kio Staff Safe	18
Guide to activate a staff duress alert	27
Things to know	27
Signal for help: how to activate a duress alert	27
Wearing your badge	28
Additional resources	30
Staff Safe web: Respond to and manage alerts	32
Things to know	32
Respond to and view active alerts	32
Email and text alert notifications: respond to an active alert	33
Resolve an alert	35
Alert details and history	36
Staff Safe Alerts mobile: Respond to and resolve active alerts	40
Things to know about staff duress alerts	40
Get the app	40
Sign in to app	40
Set your location	42
Respond to and acknowledge an active alert	43
Resolve an active alert	44
Log out of the app	45
Alert details and history	47
View the details of an alert	47
About the alert details	47
Download alert incident report	49
Download alert incident report	51
Analytics and metrics	52



Safety Summary	52
Staff locations	58
Search and locate staff	58
View staff within a specific location	58
View staff location history	58
Staff management	60
Things to know	60
Add a Staff Role	61
Add Staff Groups	61
Add staff	62
Add multiple staff at one time (bulk add)	62
Staff badge management	64
Things to know	64
Assign badge to staff	64
Replace a staff's badge	65
Power on or off a Smart Badge	66
Smart Badge insert reference card	67
Additional resources	68
Alert Rule management	70
Alert Rule settings	70
Create an alert rule	71
Edit an alert rule	72
Alert Rules and Webhooks	73
Prerequisites	73
Assign a Webhook to an alert rule	73
View an alert's Webhook events	74
User access management	75
Things to know	75
About user profiles	75
Staff Safe: roles and permissions	76
Add a user and assign their roles	77
Edit a user's assigned roles	77
Remove a user's access to Kio Cloud	78



Intro to Kio Staff Safe

In today's dynamic healthcare environments, ensuring the safety and security of staff and patients is paramount. Kontakt.io's Kio Staff Safe solution, one of many applications within the Kio Cloud Platform, leverages its AI-enabled Real-time Location System (RTLS) to enhance people safety. It provides a discreet alerting system and rapid incident response to support an organization's duress protocols.

Why Kontakt.io?

A fast-to-deploy, easy-to-use, and scalable cloud platform

- **Fast time to deployment:** Implement safety measures quickly with minimal disruptions using Kontakt.io's cloud-based infrastructure. Our team of experts ensures swift installation and integration into your existing environment.
- **Easy to use:** Intuitive and seamless operation for both staff and responders, requiring minimal training and support.
- **Scalable:** Easily expand coverage and functionality as your needs grow. The modular infrastructure ensures scalability by leveraging existing BLE-enabled Wi-Fi infrastructure.

The platform advantage

One badge, many use cases

The same Smart Badge used for staff safety duress alerts can also serve multiple other needs across your operations, such as:

- **Asset tracking:** Find and locate equipment closest to you, ensuring quick access to necessary tools and improving operational efficiency.
- **Nurse call cancellation:** Automate nurse call alert cancellation when entering the patient room, saving time and reducing alert fatigue among staff.
- **Hand hygiene compliance:** Automate staff hand hygiene activities to improve infection control.
- **Patient credential display:** When entering a room, automatically show staff credentials on a patient display or TV screen, enhancing transparency and patient trust.
- **Other use cases:** Expand the badge's functionality to cover additional applications, such as patient flow and resource orchestration.

Infrastructure modularity: 100% room-level certainty with Beam Minis

The **Kio Staff Safe solution** leverages **Beam Minis** for **100% room-level certainty** at low latency (< 3 seconds). Unlike Bluetooth-only location systems that provide only pod or zone-level accuracy, Kontakt.io's modular infrastructure allows you to deploy Beam Minis only where needed, providing precise location data when it matters most, ensuring quick and accurate responses in duress situations.



Integrate with existing IT infrastructure and systems

The Kio Staff Safe solution seamlessly integrates with various existing systems to enhance its functionality and fit into your organization's technology landscape. These existing integrations include:

- **Wi-Fi Access Points:** Leverage providers, like Cisco Spaces, to extend BLE connectivity using your current network infrastructure.
- **Emergency Notification Systems:** Integrate with leading platforms, such as Singlewire and Spok, to streamline and automate emergency notifications.
- **Nurse Call Cancellation Systems:** Integrate with systems, such as Rauland Borg and Hillrom, to allow staff to cancel alerts quickly and efficiently.
- **EHRs:** Connect with your existing EHR systems to ensure a comprehensive, integrated approach to staff and patient safety.

The benefits and features

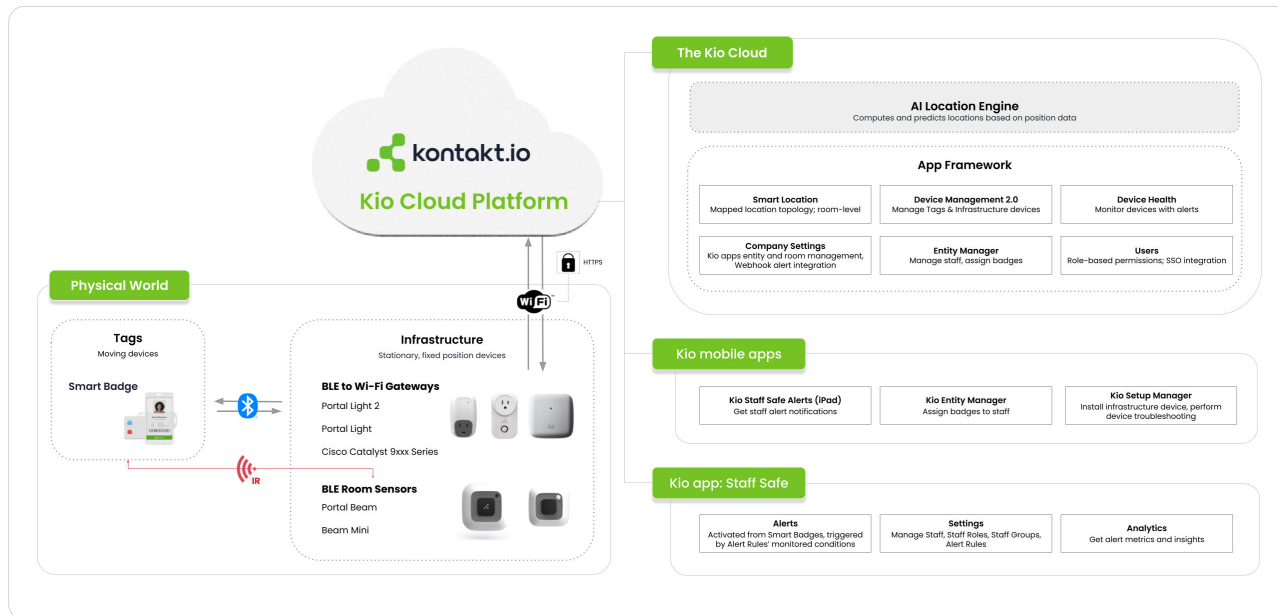
- **Staff feel valued and safe:** When staff encounter an emergency, they can discreetly press a button on their Smart Badge to call for help. This activates an alert and notifies responders of their real-time location.
- **Empowered responders:** Responders receive detailed alert notifications, including the staff's real-time location, enabling swift and effective interventions.
- **Room-level certainty:** Thanks to the modular Beam Minis, responders can be dispatched precisely to the room where help is needed, providing location accuracy in critical moments.
- **Alert state awareness:** Alerts go through various statuses from activation to resolution, ensuring complete visibility into the current state of all incidents.
- **Alert metrics and insights:** Gain actionable insights from comprehensive alert metrics to optimize safety protocols.
- **Alert Webhooks:** Instantly send alerts to designated third-party systems for seamless integration.
- **Role-based permissions:** Control access based on user roles, ensuring secure and tailored use of the system.

The components: a connected framework of IoT devices and apps

The Kio Staff Safe framework consists of IoT tag and Infrastructure devices and the Kio Cloud platform, providing a robust, reliable solution for staff safety.

The following illustration highlights the framework and architecture.





The physical world

This consists of IoT devices deployed to support the Kio Staff Safe solution.

• Tags: moving devices

- **Smart Badges:** These are wearable devices worn by people for staff duress alerts and location awareness. Badges continuously broadcast data via Bluetooth Low Energy (BLE) and empower staff with instantaneous alert activation from two easy-access buttons.

• Infrastructure devices: stationary devices

BLE-enabled Access Points: These devices leverage the Wi-Fi network you already have in place, such as Cisco Catalyst 9100s Access Points and Cisco Spaces, to enhance BLE connectivity and optimize deployment without the need for additional infrastructure.

Portal Lights (BLE to Wi-Fi Gateway): These devices aggregate data from Kontakt.io BLE devices and send the data to Kio Cloud over the Wi-Fi network. They also provide the over-the-air (OTA) device firmware and configuration updates for BLE-only Infrastructure and Tag devices.

Beam Mini: Adds room-level certainty with its built-in IR transmitter, ensuring precise location accuracy.

The Kio Cloud

The Kio Cloud is a suite of apps designed to manage Kontakt.io's IoT devices, the location topology, user management, and the Kio solution-based apps shared components,

- **AI Location Engine:** Computes accurate, room-level data for Kontakt.io's RTLS, occupancy, and indoor navigation solutions.



- **Smart Location:** Manage the mapping of the physical locations where Kontakt.io solutions and IoT devices are deployed. Smart Location consists of the following:

Mapped location topology: A hierarchical mapping consisting of campuses, buildings, floors along digital floorplans, and rooms. This topology is used by the Kio Cloud Location and Occupancy Engine that computes accurate, room-level data for Kontakt.io's RTLS, occupancy, and indoor navigation solutions.

Departments: Group rooms for use within the Kio solution-based apps. A Department can be shared between buildings, but it can not be shared between campuses.

Spaces: Group rooms or seats for use with the Kio Workspace Insights app.

Footfall: Locations that identify the floors where people footfall occupancy is measured by a Kontakt.io Portal Beam. For use with the Kio Workspace Insights app and the Kontakt.io Location and Occupancy API.

- **Company Settings:** Manage the shared components for the Kio solution-based apps.

Entity Management (people safety and workflow app): Manage Entity Types (staff roles) and entities (staff).

Room Management (shared with all Kio solution-based apps): Define room types, set room type rules by entity types, and match Smart Location rooms to their room type.

- **Users:** Manage who has access to the Kio Cloud suite of apps.

User permissions are role-based, with each role having a specific permissions. If a user is not assigned a role within an app, the app is not available to them from their Kontakt.io Launchpad.

- **Device Management 2.0:** Manage Kontakt.io IoT devices.

This includes claiming Kontakt.io orders, managing device settings, getting insights into device inventory, and keeping devices up-to-date with the latest firmware.

- **Device Health:** Monitor the health of Kontakt.io IoT devices.

Get alerts when devices may need attention. The alerting features include three available alert types, optional alert delivery mediums, and elective monitoring of devices by specific devices, device types, or by locations.

The Kio mobile apps

- **Kio Setup Manager:** A mobile app used to install Kontakt.io infrastructure devices, including the Portal Light, Portal Beam, and Beam Mini. It also offers device troubleshooting capabilities.
- **Kio Staff Safe Alerts for the iPad: [40]** A mobile version of the Kio Staff Safe web app "Simple View". This app provides responders with access to active alerts at their selected location, as well as the ability to acknowledge and resolve alerts.
- **Kio Entity Manager:** A mobile companion to the Kio Cloud Entity Manager web app, providing users a method to assign Smart Badges to staff.
- **Kio Proximity:** A mobile app that locates nearby Kontakt.io BLE Tag devices commonly attached to tracked assets or worn by people. Using Bluetooth signal strength (RSSI), it determines the proximity of Tags to your real-time location. The app is especially useful for locating Tags that may be out of range of a Portal Light or other BLE-to-WiFi gateway device.



Kio Staff Safe app concepts and terminology

The Kio Staff Safe app is designed for scalability and ease of use while providing a comprehensive tool for administrators, stakeholders, and personnel responsible for responding to staff duress incidents.

The following provides an overview of the concepts and terminology unique in the Kio Staff Safe app.

- **Staff**

The people wearing Kontakt.io Smart Badges. Each staff member has a unique profile, which includes their assigned Staff Role and Smart Badge (tag). Staff are Entities within Company Settings.

- **Staff Roles**

A Staff Role is a method to categorize staff by their roles within your organization. Staff Safe provides metrics by roles, and roles can also be assigned to Alert Rules. Staff Roles are Entity Types within Company Settings.

- **Staff Groups**

Staff Groups provide an additional method to segment staff. Unique to groups, staff can be assigned to one or multiple groups,

Staff Groups are required for the "response time" metric. When configuring an Alert Rule, a specific Staff Group is assigned to the Incident Responder setting. The response time is measured by the system tracking which responder - a staff member wearing a smart badge and assigned to the group - first enters the room location where an alert was activated.

- **Alert Rules**

Alert Rules define the monitored conditions that trigger staff duress alerts and the notifications sent when staff activate an alert from their Kontakt.io Smart Badge. Each Alert Rule's configuration includes the monitored locations, the button event that triggers an alert (blue, red, or any button), the staff the rule applies to, and who receives alert notifications and the notification methods. The notification methods include email, SMS text, or through a Webhook that delivers alerts to a third-party system. Webhooks are configured in Company Settings and assigned to Alert Rules.

Alert Rules can also be configured to track first-response time metrics by assigning a Staff Group to the Include Responder setting. When a member of this group first enters the location where the alert was activated, the system acknowledges the alert and logs the response time. This data contributes to the calculation of the Average Time to Respond, viewable in the Safety Summary Dashboard and at the individual alert level.



- **Alerts**

Alerts are the duress alerts activated by staff from their Kontakt.io Smart Badge. Responders receive alert notifications with the staff's real-time location, enabling them to respond and de-escalate the alerting incidents.

Your organization has the ability to customize the button event that activates an alert, including the buttons and the number of presses.

Alert Rule configuration: . Specifies which button - blue, red, or any - triggers an alert.

Smart Badge configuration: By **factory default**, alerts are activated by pressing a badge button **three times in quick succession** . Optionally, a badge can be configured for single-press activation, though this is not recommended due to the increased likelihood of false alerts.

- **Users**

A User is someone with access to the Kio Cloud platform suite of apps. User access is managed from the Kio Cloud Users app, which employs role-based permissions to ensure appropriate access is granted to users based on their responsibilities.

Kio Staff Safe users typically include those managing the app's settings, alert responders, and stakeholders requiring insights into analytics and metrics.



About staff duress alerts

Staff duress alerts, activated from a Kontakt.io Smart Badge, are the heart of the Kio Staff Safe solution. When an alert is activated, designated responders are notified of the alerting incident.

Things to know

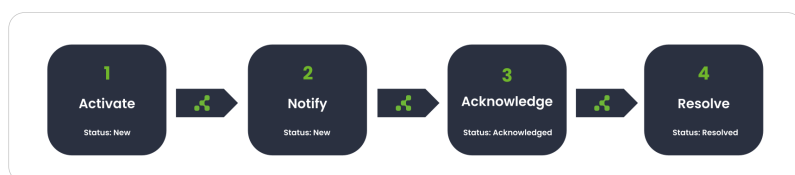
At anytime, staff can discretely call for help by pressing a button on their Smart Badge that activates an alert and sends notifications to responders with the staff's real-time location and alert details. Be sure to educate staff on your organization's Alert Rule and Smart badge configuration, which is explained below.

- **Alert Rule configuration:** . Specifies which button - blue, red, or any - triggers an alert.
- **Smart Badge configuration:** By **factory default**, alerts are activated by pressing a badge button **three times in quick succession** . Optionally, a badge can be configured for single-press activation, though this is not recommended due to the increased likelihood of false alerts.

About the alert lifecycle

The alert lifecycle represents the various stages, workflow, and statuses that an alert goes through from activation to resolution.

Within Kio Staff Safe, the state of an alert is identified by its status — New, Acknowledged, and Resolved — providing users with an instant overview of each alert's current state and enabling data-driven metrics. This structured approach ensures a standard, predictable alert progression workflow, starting from the moment an alert is activated to its resolution.

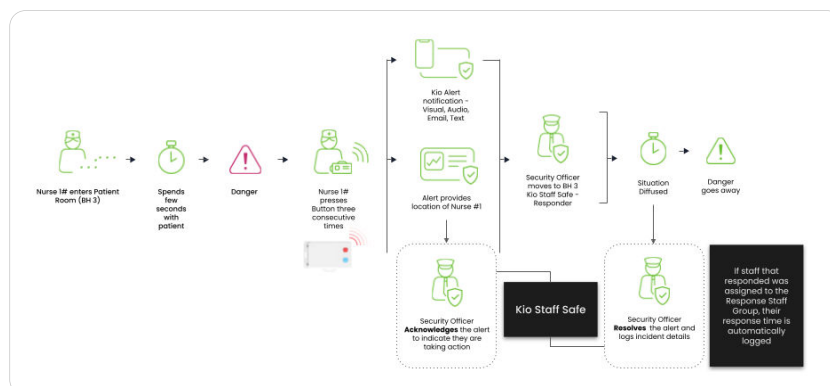


Alert Stage	Alert Workflow	Alert Status
Activate	<ol style="list-style-type: none"> 1. Staff: When faced with a duress or emergency situation needing help, they press a button on their Smart Badge three consecutive times (factory default). 2. Kio Staff Safe Alert Rule: Condition set in an alert rule is reached. 	New



Alert Stage	Alert Workflow	Alert Status
Notify	<ol style="list-style-type: none"> Kio Staff Safe: <ul style="list-style-type: none"> Triggers a new alert and sends alert notifications to responders. <p>The alert notification method(s) are set in the rule; email, SMS text message, or to a third-party system via a Webhook.</p> <p>An alert notification includes: (1) identity of the staff that activated the alert (2) time of activation (3) name and type of alert (4) location of the alert (campus, building, floor, and room).</p> <ul style="list-style-type: none"> Alerts with a critical severity level: additional Kio Staff Safe in-app visual and audio alert is activated. Responders: Receive alert notifications. 	New
Acknowledge	<ol style="list-style-type: none"> Responder: Sets the alert to "Acknowledge" to indicate they are taking action. Kio Staff Safe: When a responder, assigned to a Staff Group in the "Include Responder" setting of the Alert Rule that triggered the alert, enters the room where the alert was activated, the system automatically acknowledges the alert and logs the response time. This information is reflected in the "Average Time to Respond" metric, which can be viewed in both the Safety Summary Dashboard and at the individual alert level. 	Acknowledged
Resolve	<ol style="list-style-type: none"> Responder: Sets the alert to "Resolve" to indicate the alerting incident is resolved, assigns a Resolution Code, and enters notes related to the incident. Kio Staff Safe: Permanently stores all alert details along with an activity timeline for historical reporting and metrics.. 	Resolved

Example: alert activation to resolution



Alert notifications

How responders receive alert notifications, either through email, SMS text, or a third-party system, is configured within Kio Staff Safe Alert Rules. Additionally, Kio Staff Safe provides in-app visual and audio notifications for alerts with a severity level of critical.

When a staff duress alert is activated, its notification provides the following details:

- **Who:** staff that activated the alert.
- **Where:** the real-time location where the alert was activated; campus, building, floor, and room.
- **What:** the type of alert; Critical, High, Medium, Low, or Info.
- **When:** date/time the alert was activated.



Setup guide

This guide is intended for those responsible for the setup of the Kio Staff Safe app - a key phase in the Kio Apps deployment journey.

Prerequisites


To complete this setup, the following requirements are must be met.

- **Assigned User roles:** You are assigned to the **Administrator** role for **Staff Safe** and **Company Settings** .
- **Infrastructure devices installed:** This will vary by your deployment, but commonly includes the BLE to Wi-Fi gateways being either Kontakt.io Portal Lights or third-party BLE Access Points, and Beam Minis or Portal Beams for 100% room-level certainty.
- **Kontakt.io order claimed:** The order with the Smart Badges is claimed in Kio Cloud Device Management 2.0.

Required setup tasks

We recommend completing the tasks in the following order.



Task	Related article
<p>Create Staff Roles and Staff Groups and Add Staff</p> <ul style="list-style-type: none"> • Staff Roles: A categorization of staff that commonly mirrors the types of roles or positions within your organization. <p>Staff Roles apply to metrics, can be assigned to Alert Rules, and staff are required to be assigned to a Staff Role. Staff Roles are the Entity Types within Company Settings.</p> <ul style="list-style-type: none"> • Staff Groups (optional): An additional method to categorize staff. <p>If your deployment requires the "average time to respond metric" that is computed by an alert's first responder, you will need to create Staff Groups. This metric requires responders to be added as Staff and assigned to a Staff Group and badge, and wear their assigned badge onsite at all times. A Staff Group is assigned to the Include Responder setting within Alert Rules.</p> <ul style="list-style-type: none"> • Staff: Each person within your organization that will wear a Kontakt.io Smart Badge must be added to Kio Staff Safe. <p>Staff are assigned to their Kontakt.io Smart Badge (tag), a Staff Role, and optionally a Staff Group. Staff will always be those that require the ability to activate a staff duress alert from their assigned Smart Badge. Staff will not have permissions to sign in to the Kio Cloud platform, which requires a User account.</p> <p>If your deployment includes the "average time to respond metric", that requires responders to also wear a Smart Badge they are required to be added as a Staff, and will also be added as a User that allows them to sign in to the Kio Cloud platform.</p> <div style="background-color: #f0f0f0; padding: 10px; margin-top: 20px;"> <p> Staff Roles and Staff can also be created and managed from the Kio Cloud Company Settings app. Within Company Settings, Staff Roles are Entity Types and Staff are Entities. For first-time setup, Kontakt.io recommends use of the Company Settings app.</p> <p>Staff Groups are only managed from the Kio Staff Safe app.</p> </div>	<p>Staff management [60]</p>



Task	Related article
<p>Create Alert Rules</p> <p>An Alert Rule defines when an alert is activated by a Smart Badge button press event including the blue, red, or any button, who the alert applies that identifies the staff wearing badges, the location including one to multiple Campuses and Buildings, and the alert notification recipients that identifies the responders. Based on the scope of your deployment, you may have one to multiple Alert Rules.</p> <p>If your deployment includes sending alerts to a third-party system, you will also need to complete the Webhooks advanced setup [16].</p>	<p>Alert Rule management [70]</p>
<p>Add Users</p> <p>A user is someone that requires access to Kio Staff Safe and the Kio Cloud platform. This includes those responsible for the Staff Safe setup and administration, who will be responding to staff alerts, and users that require access to metrics and analytics.</p>	<p>User access management [75]</p>
<p>Assign staff to their Kontakt.io Smart Badges</p> <p>Each badge has a unique MAC address and Unique ID that is linked to the staff assigned to the badge.</p>	<p>Staff badge management [64]</p>
<p>Onboard responders and users</p> <p>Responders are those responsible for responding to staff duress alerts. It's important for them to know how to respond to and manage staff duress alerts.</p> <p>Users are commonly stakeholders interested in alert analytics and metrics.</p>	<p>Quick start guide [17]</p> <p>Staff Safe web: Respond to and manage alerts [32]</p> <p>Staff Safe Alerts mobile: Respond to and resolve active alerts [40]</p>
<p>Onboard staff wearing badges for staff duress alerts</p> <p>It's important for staff to know how to activate an alert, how to properly wear a badge, and how it all works.</p> <p>The Smart Badge button that activates an alert is dependent on your Alert Rules - that being either the blue, red, or any button.</p>	<p>Guide to activate a staff duress alert [27]</p>

Advanced setup

This setup is dependent on the scope of your deployment and is completed from the Kio Cloud Company Settings app.

Company Settings: Room Management

If your deployment includes the tracking the status of staff by their real-time room locations, you will also need to set up Room Management within Company Settings.



Complete the tasks in the following order.

Task	Related article
Create Room Types	Room Types management
Create Room Type rules by Entity Types (Staff Roles)	Room type rule management
Match Smart Location rooms to their Room Type	Room Matching

Company Settings: Webhooks

If your deployment includes sending new alerts to a third-party system, this requires the set up of Webhooks. This is commonly performed by your IT staff or integration team.

Complete the tasks in the following order.

Task	Related article
Create and configure Webhooks This task is commonly performed by your IT department or integration team.	Webhooks setup and management
Assign Webhooks to Kio Staff Safe Alert Rules This results in alerts being sent to the third-party system configured within the Webhook.	Alert Rules and Webhooks [73]



Quick start guide

If you're new to Kio Staff Safe or just need a refresher, this is a great place to start. Whether you're responding to alerts, responsible for the app administration, or want to get insights into alert metrics, you'll get a quick overview about the features most important to your role.

Sign in to Kio Cloud

Kio Cloud is a cloud-based platform accessible through a web browser. Your organization's Kio Cloud administrator will provide you with the specific URL for signing in. Your access and permissions to the Kio Cloud suite of apps is determined by your assigned app roles, which is managed by those assigned to the Users app Administrator role.

To sign in, use one of supported web browsers listed below. We recommend the browser is at the most current version.

- Google Chrome™ (recommended)
- Mozilla Firefox®
- Apple® Safari®

Sign in with your email and password

This method is required when your organization has not set up Single sign-on (SSO) with Kio Cloud.



First-time sign-in: You should have received an activation email from Kontakt.io to set up your user profile. If you didn't, check your spam/junk folder or contact your Kio Cloud administrator.

1. From a **web browser**, go your organization's **Kio Cloud URL** > enter your **email address** and **password** > select **Sign In**.
2. Enter your **email address** and **password** > select **Sign In**.

Your **Kontakt.io Launchpad** displays the apps for which you have an assigned role. If an app doesn't appear, it means you haven't been assigned a role in that app.

Sign in with your Single sign-on (SSO) credentials

If your organization has set up Single sign-on (SSO) with Kio Cloud, you'll use your organization's identity provider to sign in.

1. From a **web browser**, go to your organization's **Kio Cloud URL**.



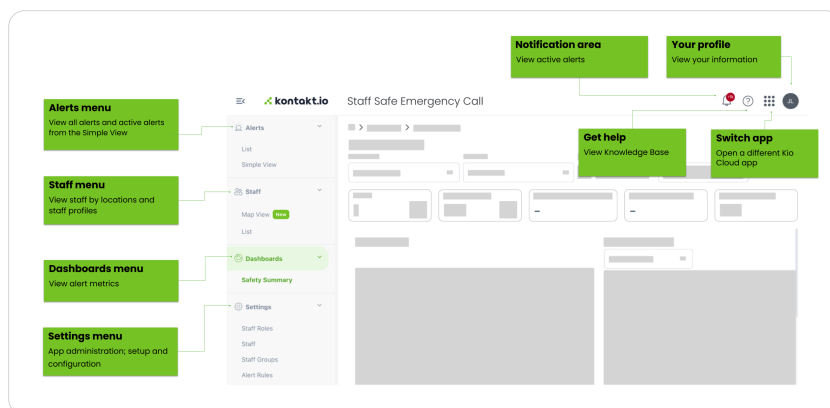
- Select the available **SSO method** and enter your credentials.

Your **Kontakt.io Launchpad** displays the apps for which you have an assigned role. If an app doesn't appear, it means you haven't been assigned a role in that app.

Navigating Kio Staff Safe

Once signed in to Kio Cloud, from your **Kontakt.io Launchpad** select **Staff Safe Emerg. Call**.

It's important to be familiar with the app menus and their features. The menus available to you are determined by your assigned role within the Kio Staff Safe app.



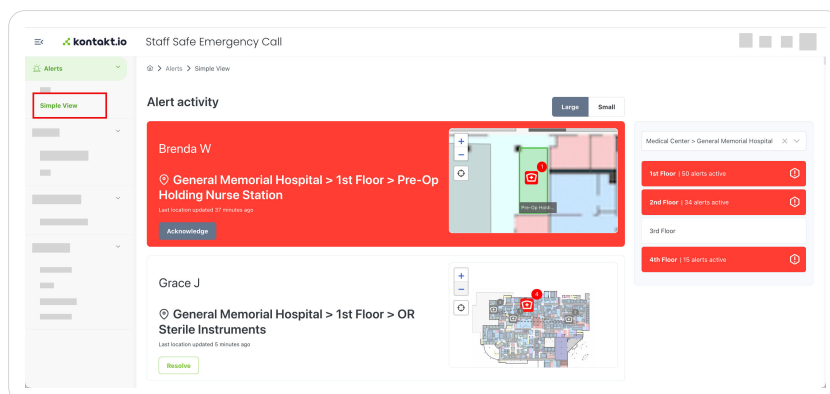
Alerts menu

The Alerts menu, including the List and Simple View, is where the staff duress alerts are located and provides the current status [21] and details of each alert. The Simple View is designed for use by responders - providing them only active staff alerts with enhanced visuals. The List view provides all alerts, along with access to the details of each alert.



Simple View

The Simple View is the most important view for those responsible for responding to alerts. This view provides all active alerts, those in a new or acknowledged status, along with a map pinpointing the real-time location of staff with an active alert.

Alerts are sorted in descending order, the most recent first.



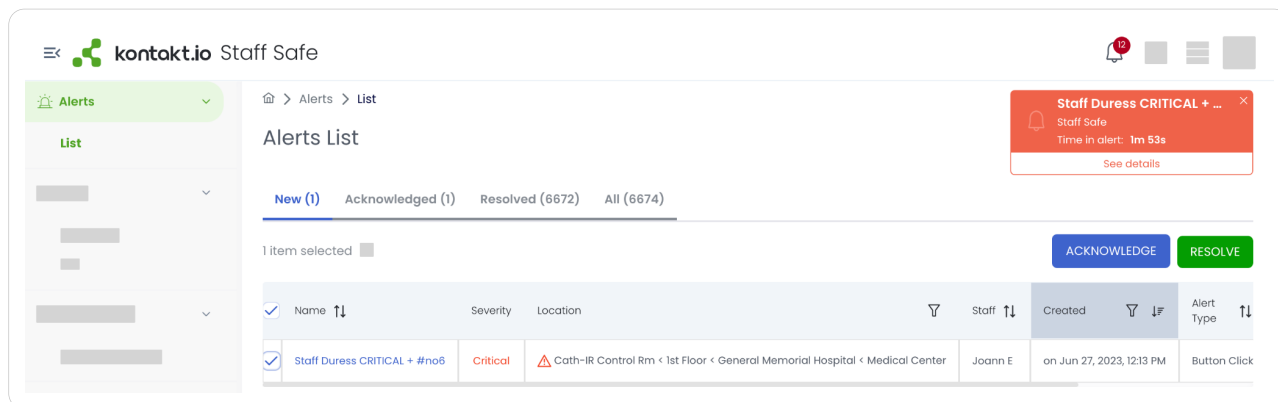
Key features:

- **Location specific alerts.** Filter active alerts to a specific Building location within a Campus. The selected location also includes a floor-level count of alerts in RED that have not been acknowledged or resolved - providing a key visual indicator of the alerts that need immediate attention.
- **Visual colored alert status indicators.** Alerts that have not been acknowledged have a RED colored background and those that have been acknowledged have a WHITE colored background.
- **Map view with staff location details.** The map includes unique icons to identify the real-time location,
- **Last location detail:** Provides when the staff's last location was received. A warning icon is displayed when the last location received has exceeded the lost tag threshold time period.
 -  > Identifies the staff's most recent real-time location.
 -  > Identifies a room location change, including a numbered sequence and visual movement path.
- **Acknowledge and Resolve alerts.** Alert responders can change an alert's status and log all activity from this single view.

List view

The List view includes all staff alerts categorized by their current status - New, Acknowledged, Resolved - to provide an instant overview of the current state of all alerting incidents. You can select an alert to view its profile and historical activity timeline.

From this view, you can view the details of each alert by selecting the alert.



The screenshot shows the 'kontakt.io Staff Safe' interface. The main content area is titled 'Alerts List' and includes a filter bar with 'New (1)', 'Acknowledged (1)', 'Resolved (6672)', and 'All (6674)'. Below the filter bar, there is a table of alerts. The table has columns for 'Name', 'Severity', 'Location', 'Staff', 'Created', and 'Alert Type'. One alert is listed: 'Staff Duress CRITICAL + #no6' with a severity of 'Critical' and a location of 'Cath-IR Control Rm < 1st Floor < General Memorial Hospital < Medical Center'. The staff member is 'Joann E' and the alert was created on 'Jun 27, 2023, 12:13 PM'. The alert type is 'Button Click'. There are 'ACKNOWLEDGE' and 'RESOLVE' buttons at the top right of the table. A notification banner at the top right of the interface shows 'Staff Duress CRITICAL + ...' with a 'See details' link.

Name	Severity	Location	Staff	Created	Alert Type
Staff Duress CRITICAL + #no6	Critical	Cath-IR Control Rm < 1st Floor < General Memorial Hospital < Medical Center	Joann E	on Jun 27, 2023, 12:13 PM	Button Click

An alert profile includes:

- **Alert Details:** Includes all alert information along with key metrics.

The Responded By and Response Time are only generated at the time the first responder, those assigned to the Incident Responder Group within the Alert Rule that triggered the alert, enters the room location where the alert was activated.



- **Activity Timeline:** Includes each activity and a timestamp for all actions taken when an alert is active.

Activity includes when the alert was activated, acknowledged, and resolved, the user notes entered during a status change, and staff room-level location changes. In addition, if the Alert Rule that triggered the alert is configured with a Webhook, each webhook event and its details are logged within the Activity Timeline.

Assistance Needed + #no419

Severity: Medium | Status: **RESOLVED** | Responded by: - | Response Time: - | Duration: 42m

Time	Activity	Note
May 23, 2024, 03:22 PM	Resolved by User: Julie Lininger	Example of a resolution note - follow your organizations policies.
May 23, 2024, 03:19 PM	Acknowledged by User: Julie Lininger	
May 23, 2024, 02:57 PM	Location changed from Nurse Offices to 210-216 Corridor	

- **Alert Report.** Download a PDF report that provides the alert's details and activity.

kontakt.io
Incident Report
Powered by kontakt.io

Location: 210-216 Corridor (2nd Floor > General Memorial Hospital > Medical Center)

Date: May 23, 2024, 7:39:44 PM UTC

Duration: 42 minutes

Severity: Medium

Status: Resolved

Resolution code: Low

Staff: Crystal B (0a:59:8a:5b:77:a9)

INCIDENT
On May 23, 2024, 7:39:44 PM UTC, Crystal B (0a:59:8a:5b:77:a9) triggered an alert by pushing Blue button on Kontakt.io device to report an incident at 210-216 Corridor (2nd Floor > General Memorial Hospital > Medical Center).

This incident was resolved in 42 minutes.

NOTES
Example of a resolution note - follow your organizations policies.

FOR MORE INFORMATION
Please contact Julie Lininger.



About the alert statuses

An alert is comprised of a series of statuses it undergoes from activation to resolution — New, Acknowledged, and Resolved — providing an instant overview the current state of an alert and enabling data-driven metrics. This structured approach ensures a standard, predictable alert progression workflow, starting from the moment an alert is activated to its resolution.

Status	Description
New	Alert has not acknowledged a Staff Safe user (responder).
Acknowledged	<p>A Staff Safe user (responder) set the alert to Acknowledge to indicate that action is being taken.</p> <p>If the Alert Rule that triggered the alert has an assigned Staff Group within its Include Responder setting, when the first responder (wearing a Smart Badge and assigned to this group) enters the room location where the alert was activated, the alert is automatically set to Acknowledge.</p>
Resolved	<p>A Staff Safe user (responder) set the alert to Resolve to indicate the alerting incident has ended.</p> <p>When to to resolve, the user is required to set a Resolution code and can optionally add notes to log additional details about the incident.</p>

Dashboards menu

The Dashboard menu provides alert analytics delivering actionable insights, helping organizations monitor alert trends, response times, and alert resolutions. You can interact with the dashboard metrics by clicking on bars, locations, or segments in the charts to get detailed insights or filter the data further.

Filters

Safety Summary

Alert Rules

All existing rules ▼

Location

General Memorial Hospital ▼

Date Range

Last 30 days ▼ Mar 21 2024 - Apr 19 2024

Customize metrics by selecting filters for:

- **Resolution Code:** View metrics by specific codes or all codes.
- **Alert Rules:** Filter metrics by specific alert rules.
- **Location:** View metrics by campus, building, or floor.
- **Date range:** Analyze metrics over preset time frames or a custom date range.

Overall metrics

Alerts

221 ↓

Avg. Alerts/Day

7.4 ↓

Avg Time to Acknowledge

56m ↑

Avg Time to Respond

-

Avg Alert Duration

3h 40m ↑



- **Alerts:** Total number of alerts, showing trends in alert frequency.
- **Average alerts per day:** Daily average of activated alerts.
- **Average time to acknowledge:** Time from alert activation to acknowledgment, measure response speed.
- **Average time to respond:** Time from alert activation to responder arrival at the location, provided responders are wearing badges and assigned to incident responder groups.
- **Average alert duration:** The average duration of alerts from activation to resolution, helping to understand the typical lifespan of alerts and identify trends that may require attention.

Additional metrics

- **Alerts by role:** Segments alerts by staff roles, identifying which roles activate the most alerts.
- **Alerts by location:** Groups alerts by room, floor or building, helping identifying high-risk areas.
- **Alerts by day/week and time:** Track alerts by the day of the week and time of day to spot peak incident times.
- **Response time:** Segments alerts based on response times, which options to group by hour, floor, or building.

Staff menu

The Staff menu includes both a Map and List view that provides visibility into the location and profiles of all staff. The profiles of staff includes their settings, last known location, and their location history.

Map view

The Map view provides staff locations by floors within a building and an interactive floor plan map that includes staff room-level locations and active alerts.

Key features include:

- **Location navigation:** Quickly navigate by campus and each building and floor.
- **Staff:** View staff room-level locations within a floor, along with filtering capabilities by staff role.
- **Rooms:** View staff located within specific rooms.
- **Alerts:** View active alerts by floor.



kontakt.io Staff Safe Emergency Call

Map View > Medical Center > General Memorial Hospital > 1st Floor

Map View

1st Floor

Staff (32) Rooms Alerts (30)

Search

Andrea R
Looking For Supplies | Nurse | Respiratory Storage

Anita F
Nurse Station | Nurse Manager | ER Fast Track Nurs...

Anita R
With Patient | Nurse | SDS Rm 8

Carlos F
With Patient | Nurse Manager | Cath-IR Control Rm

Dawn K
Nurse Station | Nurse | Pre-Op Holding Nurse Station

Denise T
Nurse Station | Nurse | MICU Nurse Station

Elisabeth W
Nurse Station | Nurse | Endoscopy Nurse Station

Nurse 22 Nurse Manager 10

1st Floor

List view

The List view organizes staff a list format that provides a quick glimpse into staff details. From this view, you can view each staff's unique profile that includes their setting details, assigned Smart Badge (Tag), and their last received real-time location and location history,

This list is **searchable** and provides **column filtering** - making it easy to find specific staff. You can also set the columns displayed to view what's most important to you.



kontakt.io Staff Safe Emergency Call

Staff > List

Staff

Search by ID, Display Name, Attributes and Tag ID

All Columns

Staff ID	Name	Staff Type	Associated Apps	Groups	Attributes	Staff Status	Last Location	Tag Status	Tag Id	Actions
Joann E	Joann E	Nurse	Staff Safe Em...		Unit: ED	Nurse Station	Endoscopy N...	Ok	57:18:a4:56:1...	
Margaret R	Margaret R	Nurse	Staff Safe Em...		Unit: Pediatric	Nurse Station	Main Nurse S...	Ok	7d:fe:df:97:7a...	
Susan W	Susan W	Nurse Manager	Staff Safe Em...		Unit: SICU	Looking for s...	ER Medicatio...	Ok	d6:4e:42:a9:...	
Wendy T	Wendy T	Nurse Manager	Staff Safe Em...		Unit: LDRP	Looking for s...	Soiled Utility ...	Ok	e7:93:2d:f1:8...	
Anita F	Anita F	Nurse Manager	Staff Safe Em...		Unit: Radiology	Nurse Station	ER Fast Track...	Ok	2f:a3:c9:22:6...	
Rebekah E	Rebekah E	Nurse	Staff Safe Em...		Unit: Endosco...	With Patient	OR 10 > 1st Fl...	Ok	a4:73:a2:02:9...	
Trisha J	Trisha J	Nurse Manager	Staff Safe Em...		Unit: PACU	With Patient	MICU 11 > 1st...	Ok	5c:f7:c9:10:ef...	
Anita R	Anita R	Nurse	Staff Safe Em...		Unit: ED	With Patient	SDS Rm 8 > 1...	Ok	e5:44:b6:19:...	
Nancy W	Nancy W	Nurse	Staff Safe Em...		Unit: LDRP	Nurse Station	Nurse Offices...	Ok	ac:10:f8:eae1...	
Hilda B	Hilda B	Nurse	Staff Safe Em...		Unit: Radiology	Looking for s...	ER Fast Track...	Ok	24:56:9f:b6:8...	

Showing 1 to 10 of 157 entries

To view a **staff's profile**, select their **Staff ID**, **Name** or the **edit icon** located in the Actions column.

kontakt.io Staff Safe Emergency Call

Staff > List > Detailed View

Joann E

Details Location History

Staff ID
Joann E

Name
Joann E

Staff Role
Nurse

Created by
Pawel Stokowiec

Created at
Sep 20, 2022, 08:57 AM

Last Updated by
Pawel Stokowiec

Last Updated at
Dec 11, 2023, 06:33 AM

Staff Status

Staff Status Available: Nurse Station

Time in Status
56m

Assigned tag

Smart Badge | 12fW08f | 57:18:a4:56:1f:6c

Applications

Associated Applications
Staff Safe Emergency Call

Excluded Applications
-

Groups

No groups assigned

Location

Last Seen
May 08, 2024, 07:05:47 AM

Campus Name
Medical Center

Building Name
General Memorial Hospital

Floor Name
1st Floor

Room Name
Endoscopy Nurse Station

Attributes

Settings menu

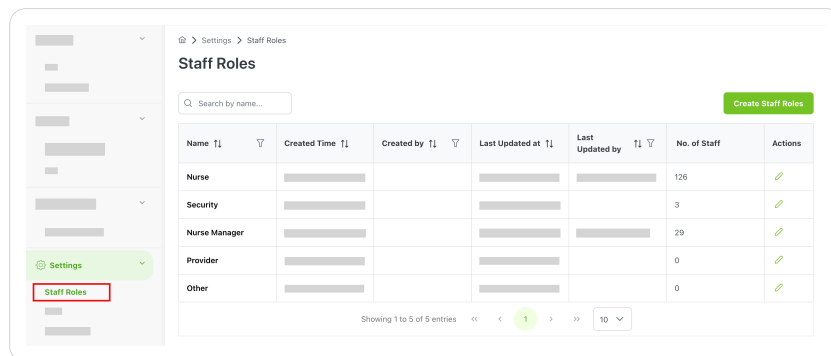
The Settings Menu contains all administrative capabilities. Only users assigned the Kio Staff Safe Administrator role have access to the Settings Menu and its sub-menus.



Staff Roles

Staff Roles are a categorization of staff that commonly mirrors the types or roles or positions within your organization. All staff are required to be assigned to a Staff Role. Staff Roles are included in alert metrics and can also be assigned to Alert Rules.

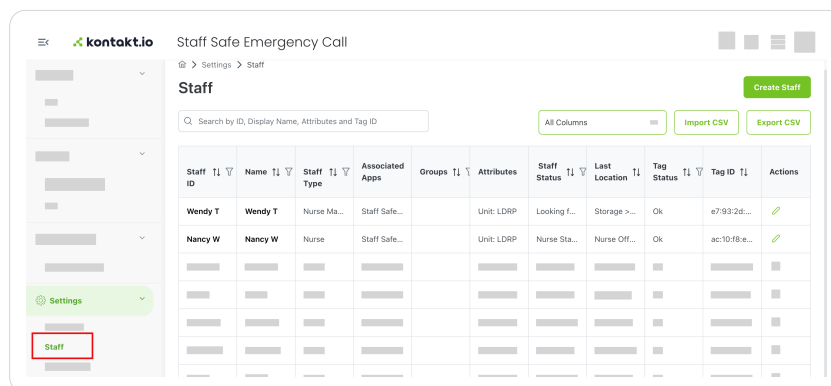
You can also manage Staff Roles from Company Settings, where they are identified as Entity Types.



Staff

Staff are the people that are assigned to and wearing Kontakt.io Smart Badges.

You can also manage staff from Company Settings, where they are identified as Entities.



Staff Groups

Staff Groups offer a way to segment staff beyond their Staff Roles. Staff can be assigned to multiple groups, but can only be assigned to one Staff Role. You can also use groups in Alert Rules to specify which staff the alerts apply to, and assign groups to the Include Responder setting for automated alert acknowledgments and response time metrics.

Staff Groups are created and managed exclusively from the Kio Staff Safe app.



Alert Rules

Alert Rules define the monitored conditions that trigger staff duress alerts and the notifications sent when staff activate an alert from their Kontakt.io Smart Badge. Each Alert Rule's configuration includes the monitored locations, the button event that triggers an alert (blue, red, or any button), the staff the rule applies to, and who receives alert notifications and the notification methods. The notification methods include email, SMS text, or through a Webhook that delivers alerts to a third-party system. Webhooks are configured in Company Settings and assigned to Alert Rules.

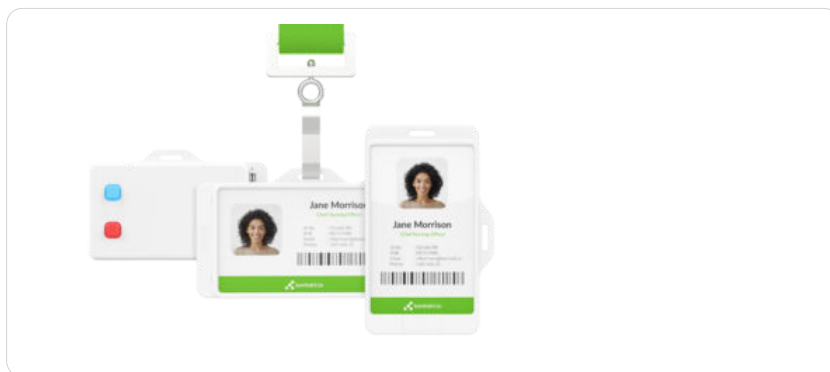
Alerts Rules are created and managed exclusively from the Kio Staff Safe app.



Guide to activate a staff duress alert

Kio Staff Safe is a discreet alerting and rapid incident response solution that supports your organization's duress response protocols. Your **Kontakt.io Smart Badge** empowers you to quickly activate an alert to signal for help when faced with a duress event or need assistance.

When you activate an alert from your Smart Badge, this signal for help immediately sends alert notifications to security and nearby staff. These notifications provide responders with your real-time location allowing them to intervene, de-escalate, and provide assistance when it matters the most.



Things to know

A Kontakt.io Smart Badge only functions within your organization's designated coverage areas. Designated coverage areas are defined by your organization and managed within Kontakt.io's Kio Cloud platform. The BLE to Wi-Fi infrastructure gateway devices, such as Kontakt.io Portal Lights, are installed throughout the coverage areas that provide the required wireless connectivity and communication to the Kio Staff Safe solution. Your badge cannot activate alerts outside of your organization's designated coverage areas. For example, if you are at home or not within a designated coverage area, your location will not be known and alerts cannot be activated.

Signal for help: how to activate a duress alert

- ❗ Follow your organization's instructions to activate an alert. Each Smart Badge colored button may be associated with specific alert types as determined by your organization.

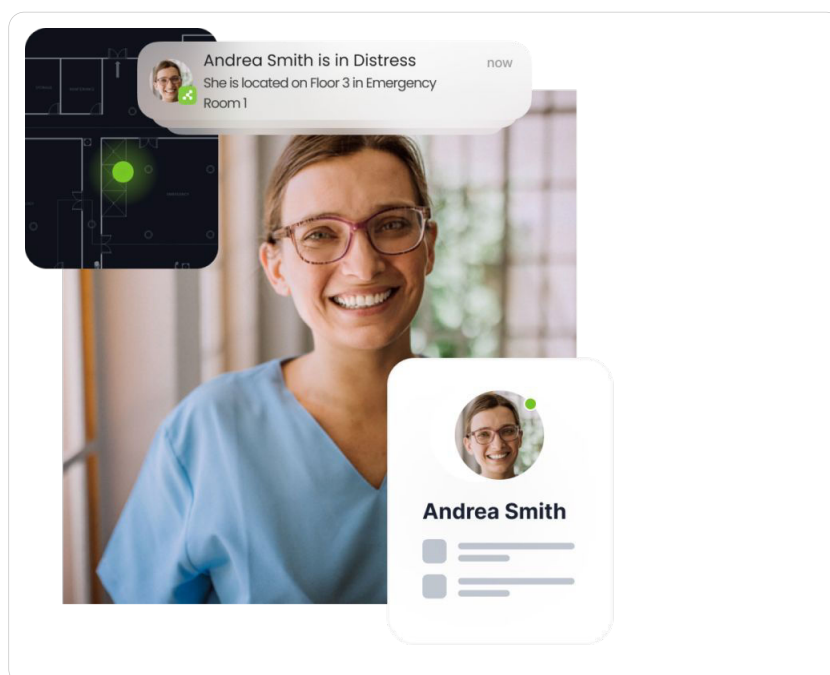
By factory default, an alert is activated by pressing a button three times. This triple-press action ensures intentional use to signal for help and reduces the chance of an accidental alert. Alternatively, badges can be configured by your organization to activate an alert with a single button press.

Press a **button** (defined by your organization) on your Smart Badge **three times in quick succession**





From the instant alert notifications, responders can quickly find you by knowing your real-time location, even when you are on the move.



Wearing your badge

It's important to wear your badge at all times when onsite.

Placement guidelines

- **Button facing body**

With the buttons facing your body, this helps to prevent accidental activation and ensures you can discreetly press a button in an emergency.

- **Clear of other items**

When the badge is not placed behind other accessories or obscured by clothing, this allows its wireless communication and ensures it's easily accessible to activate a call for help.



- **IR Sensor visibility**

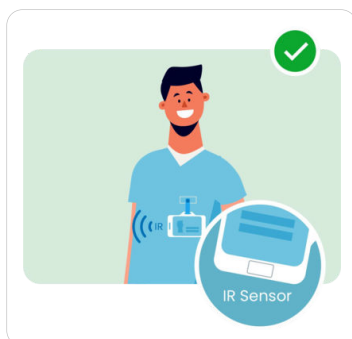
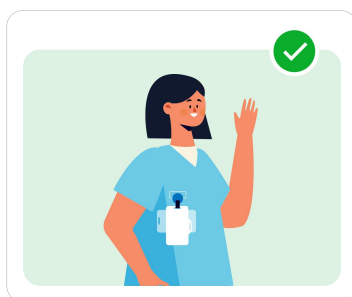
The IR Sensor, either located on the front, non-button side or the corner of the badge (Smart Badge 3), must always be visible and not covered by other items. During an active alert, this little sensor allows responders to receive your real-time location with room-level certainty.

Example: Wear the badge horizontally behind a vertical badge to ensure the IR Reader is always visible.

Smart Badge 3: IR sensor is located in the corner and is visible regardless of the button side placement.

Placement good examples

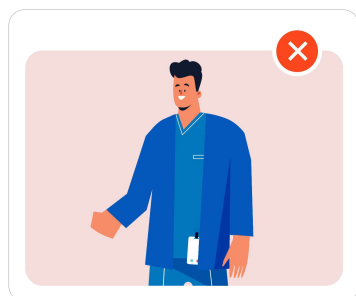
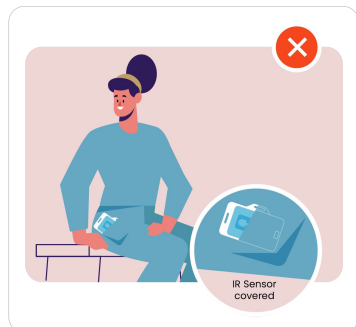
- Buttons facing body
- IR Sensor is fully visible and unobstructed
- Clear of other items
- Attached to the outside of your clothing



Placement bad examples

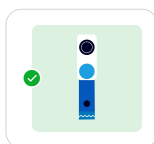
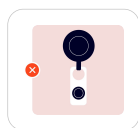
- Badge covered by clothing - placed in pocket or hidden under a jacket or shirt
- Badge obscured by other items - placed behind other objects makes it difficult to see or access
- Incorrect badge orientation - worn with buttons facing outward or IR Sensor covered





Tip

Avoid attaching the badge to a clip that could rotate the badge.



Additional resources

The following provide learning resources for staff wearing Kontakt.io Smart Badges.

- Kio Staff Safe Quick Start Guide

Provides instructions for activating a duress alert by **pressing any button three times in quick succession**, along with guidelines for **wearing a badge**.

The buttons that activate an alert, either the blue, red, or any button, and the number of presses may vary by your organization's deployment.



- Kio Staff Safe explainer video. Get a 2 minute overview of how it all works.

This video highlights a Portal Light infrastructure along with Smart Badges. Your deployment may vary to include third-party BLE to Wi-Fi gateways such as Cisco Access Points, and Kontakt.io Beam Minis or Portal Beams.

Scan the QR Code



Staff Safe web: Respond to and manage alerts

Staff duress alerts, activated by staff from their Kontakt.io Smart Badge, are the core of the Kio Staff Safe solution. These alerts provide responders with the real-time location of staff - allowing them to intervene and de-escalate the incident and provide assistance when it matters the most.

As a responder, the following provides the steps to respond to and manage alerts from the Kio Staff Safe web app.

Things to know

At anytime, staff can discretely call for help by pressing a button on their Smart Badge that activates an alert and sends notifications to responders with the staff's real-time location and alert details. Be sure to educate staff on your organization's Alert Rule and Smart badge configuration, which is explained below.

- **Alert Rule configuration:** . Specifies which button - blue, red, or any - triggers an alert.
- **Smart Badge configuration:** By **factory default**, alerts are activated by pressing a badge button **three times in quick succession** . Optionally, a badge can be configured for single-press activation, though this is not recommended due to the increased likelihood of false alerts.

Respond to and view active alerts

When you receive an alert notification, the most important step is to **take action and locate the staff to intervene, de-escalate, and provide assistance**. When you receive an alert, from Kio Staff Safe app you can quickly view the staff's real-time location and acknowledge the alert to indicate that action is being taken. Acknowledging an alert will provide responders and other staff with the visibility into the current state of the alerting incident.

Kio Staff Safe provides multiple methods to respond to and view active alerts. In particular, the **Simple View**, available in both the Kio Staff Safe web app and mobile app, has been **specifically designed for responders**. The Simple View provides the quickest and easiest way to view active alerts and provides the real-time location of staff with an active alert.

Kio Staff Safe web: respond from the Simple View

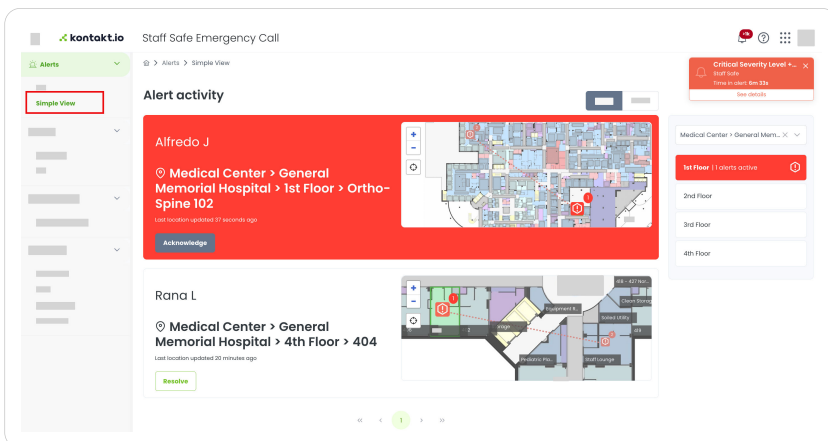
1. From your **Kontakt.io Launchpad**, select **Staff Safe Emerg. Call**.
2. From the **Alerts** menu, select **Simple View**.



3. From the **Alert Activity** locate the **alert**.

An alert pinpoints the staff's last known location with a pulsing icon. If the staff moves to a different room after activating the alert, the location details and map view dynamically update to reflect their current location

The map view updates in real-time to pinpoint each location change as the staff moves. Each movement is marked by an updated icon, showing the staff's path as they change locations.



Last location detail: Provides when the staff's last location was received. A warning icon is displayed when the last location received has exceeded the lost tag threshold time period.

 > Identifies the staff's most recent real-time location.

 > Identifies a room location change, including a numbered sequence and visual movement path.

4. To indicate you are taking action and responding to the alert, select **Acknowledge**. This option only appears if another staff member (user) has not acknowledged the alert.



The location notification area, displays the count of alerts in red that have not been acknowledged by floor-level.

In the example above, there is one alert, "Alfredo j", on the 1st floor that has not been acknowledge.

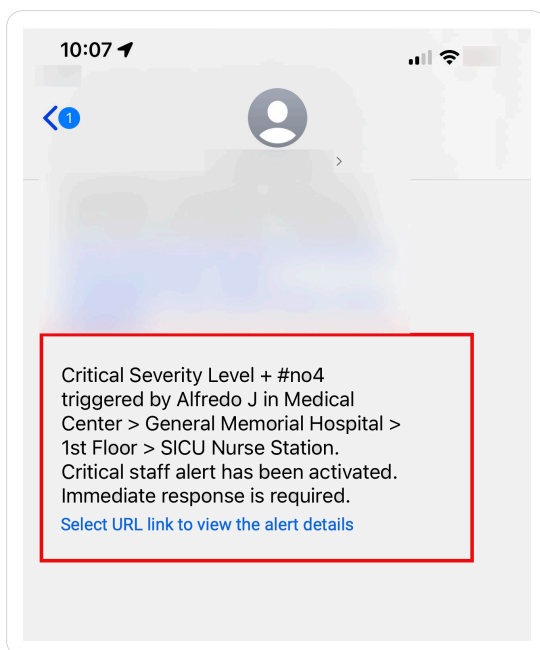
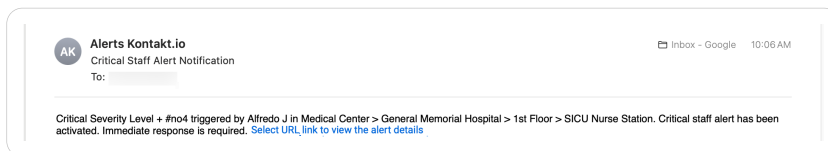
Email and text alert notifications: respond to an active alert

Both **email** and **text alert notifications** provide users with the following details related to an alert:

1. **Alert details:** A brief description of the nature of the alert, ensuring users understand the urgency or type of incident.
2. **URL link:** A direct link to view additional information about the alert in the Kio Cloud platform. This allows users to access the system for more context.

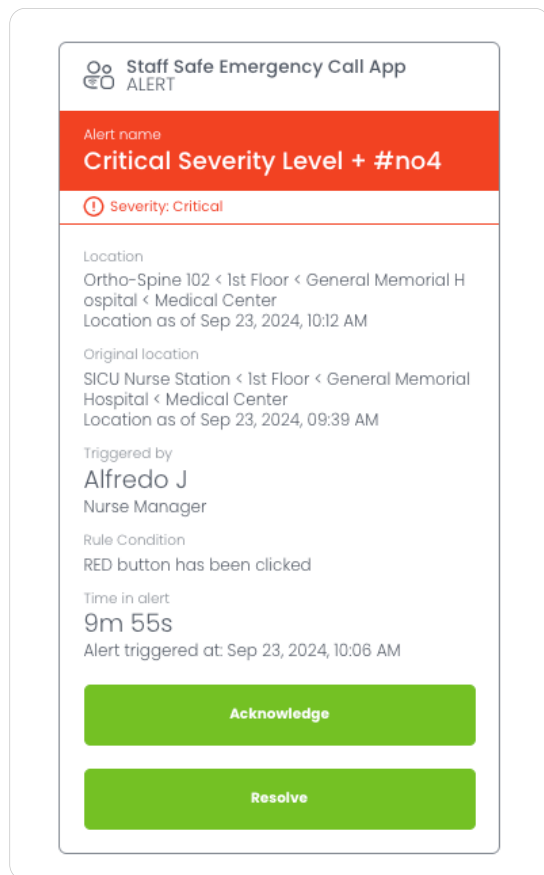


- 3. **Acknowledge/Resolve options:** Buttons to acknowledge the alert to indicate they are taking action, as well as option to resolve the alert if applicable.



Selecting the alert link provided in the notification displays the alert details.





Resolve an alert

Resolving an alert indicates that the staff incident resulting in the alert has been responded to and de-escalated. Essentially, all necessary actions have been taken to ensure the safety and well-being of the staff member that activated the alert.

Things to know

- To resolve an alert, it must first be in the Acknowledged status. If applicable, you can acknowledge the alert and then proceed to resolve it.
- To resolve an alert, you will be required to select a Resolution Code. The available options are: Duplicate, Handled by security, Handled before security arrived, Accidental, Test, Other.
- When you resolve an alert, it is removed from the Simple View in both the web and iPad mobile app. This ensures immediate visibility into only active alerts.

Resolve an alert from the Simple View

1. From your **Kontakt.io Launchpad**, select **Staff Safe Emerg. Call**.
2. From the alert, select **Resolve**.



3. Select the applicable **Resolution Code** > enter **Notes** related to the alerting incident > select **Resolve**.

Notes provided should follow your organization's policies and procedures.

The alert is removed from the Simple View.

To view the details of a resolved alert, navigate to the List View within the Alerts menu and select the alert's name.

Resolve an alert from List View

1. From your **Kontakt.io Launchpad**, select **Staff Safe Emerg. Call**.
2. From the **Alerts** menu, select **List**. This view filters the alerts by their current status - New, Acknowledged, Resolved.

Commonly, an alert is in an Acknowledged status prior to being resolved. Although from the List View, you can Resolve an alert without it being acknowledged.

3. From the alert, select the **checkbox** next to its **Name** > from the upper-right corner, select **Resolve**.
4. Select the applicable **Resolution Code** > enter **Notes** related to the alerting incident > select **Resolve**.

Notes provided should follow your organization's policies and procedures.

Alert details and history

Each alert maintains a detailed profile with a log of all activities. An alert's activity timeline includes the details of each status change, alert notification details, and notes entered by users. From an alert, you can also download an alert incident report that provide a complete record of all activities.

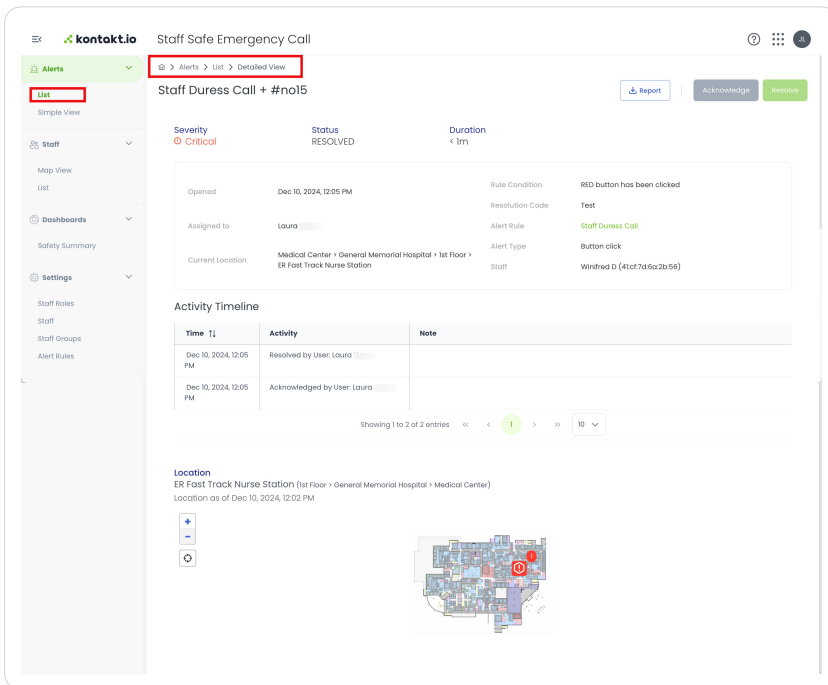
View the details of an alert

1. From your **Kontakt.io Launchpad**, select **Staff Safe Emerg. Call**.
2. From the **Alerts** menu, select **List**. This view filters the alerts by their current status - New, Acknowledged, Resolved.



3. Once you locate the alert, select its **Name**.

From the alert's profile, you can view the following details and activity.



About the alert details

Detail	Description
Severity	Identifies the severity of the alert. The severity is configured within the Alert Rule that triggered the alert. A rule's severity can be either be Critical, High, Medium, Low, or Info.
Status	The current state of the alert. Within Kio Staff Safe, the state of an alert is identified by its status — New, Acknowledged, or Resolved — providing users with an instant overview of each alert's current state and enabling data-driven metrics.
Responded by	Only displayed if the Include Responder is set in the Alert Rule that triggered the alert. Responded by is the name of the user (responder), assigned to the Incident Responder Staff Group, that first entered the room-level location of where the alert was activated.
Response Time	Only displayed if the Include Responder is set in the Alert Rule that triggered the alert. The Response Time is the duration of time from when the alert was activated to when the first responder (Responded by) entered the room-level location where the alert was activated.



Detail	Description
Duration	The duration of an alert is the total time between when the alert is first triggered (activated) and when it is resolved. This duration measures how long the alert remained in an active state, providing a timeline from activation to resolution.
Opened	Date and timestamp of when the alert was triggered (activated by staff from their Smart Badge).
Assigned to	The name of the user that created the Alert Rule that triggered the alert.
Current Location	The last received location of the staff at the time the alert was activated.
Original Location	The location where the alert was initially activated. This is only displayed if the staff member has moved to a different room-level location from where the alert was originally activated. This feature, along with the current location, helps track both the origin and current location of the staff, which can be critical for safety and response purposes.
Rule Condition	The Alert Rule's button event that activated the alert. The button event is set within the Alert Rule, which can be set to either the blue button, red button, or any button.
Resolution Code	The value selected when a user changed the alert's status to resolved.
Note	The value entered by a user when they changed the alert's status to resolved.
Alert Rule	The name of the Alert Rule that activated the alert.
Alert Type	The Alert Rule type; this value will always be Button click.
Staff	Who activated the alert from their Smart Badge, including the badge's 12 character MAC address.

Activity Timeline

The Activity Timeline includes each activity and a timestamp of all actions taken during from alert activation to resolution.

- Each alert status change - when the alert was activated, acknowledged, and resolved.
- Alert notifications details.
- Who made a status change and the notes entered during a status change.
- Staff room-level location changes that occurred during the duration of the alert.
- If the Alert Rule that triggered the alert is configured with a Webhook, includes the Webhook event and its details.



Location details

Provides the staff's last received location during the duration of the alert, along with any room-level movements recorded during the alert. This information allows you to track the staff's location movements that displays the sequence of locations from a map view.

Download alert incident report

For any alert in a resolved status, you can download the alert's incident report.

1. From your **Kontakt.io Launchpad**, select **Staff Safe Emerg. Call**.
2. From the **Alerts** menu, select **List**. This view filters the alerts by their current status - New, Acknowledged, Resolved.
3. Select the **Resolved** tab > locate the alert > select its **Name**.
4. From the alert, select **Report**. The PDF file is saved to your computer's default download folder.

Example of an incident report.



Incident Report

Powered by



Location: 210-216 Corridor (2nd Floor > General Memorial Hospital > Medical Center)

Date: May 23, 2024, 7:39:44 PM UTC

Duration: 42 minutes

Severity: Medium

Status: Resolved

Resolution code: Low

Staff: Crystal B (0a:59:8a:5b:77:a9)

INCIDENT

On May 23, 2024, 7:39:44 PM UTC, Crystal B (0a:59:8a:5b:77:a9) triggered an alert by pushing Blue button on Kontakt.io device to report an incident at 210-216 Corridor (2nd Floor > General Memorial Hospital > Medical Center).

This incident was resolved in 42 minutes.

NOTES

Example of a resolution note - follow your organizations policies.

FOR MORE INFORMATION

Please contact Julie Lininger.



Staff Safe Alerts mobile: Respond to and resolve active alerts

The **Kio Staff Safe Alerts for the iPad** offers a mobile experience of the Kio Safe Safe "**Simple View**". The Simple View is designed for use by responders - providing them only active staff duress alerts with enhanced visuals. Each active alert provides the location of the staff that activated the alert - allowing responders to intervene and de-escalate the incident and provide assistance when it matters the most.

Things to know about staff duress alerts

At anytime, staff can discretely call for help by pressing a button on their Smart Badge that activates an alert and sends notifications to responders with the staff's real-time location and alert details. Be sure to educate staff on your organization's Alert Rule and Smart badge configuration, which is explained below.

- **Alert Rule configuration:** . Specifies which button - blue, red, or any - triggers an alert.
- **Smart Badge configuration:** By **factory default**, alerts are activated by pressing a badge button **three times in quick succession** . Optionally, a badge can be configured for single-press activation, though this is not recommended due to the increased likelihood of false alerts.

Get the app

To install **Kio Staff Safe Alerts**, search for it from the **Apple App Store**.

App requirements: iPad at iOS version 16 or later | Bluetooth enabled (on) | Internet connection

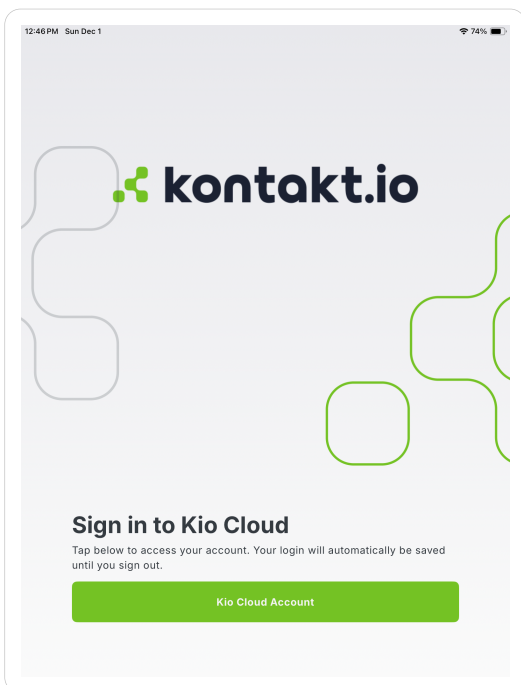
For optimal use it's recommended to set the iPad to Kiosk (Single App) Mode, a configuration typically managed by your organization's IT staff. This mode restricts the device to a single application, enhancing focus and security.

Sign in to app

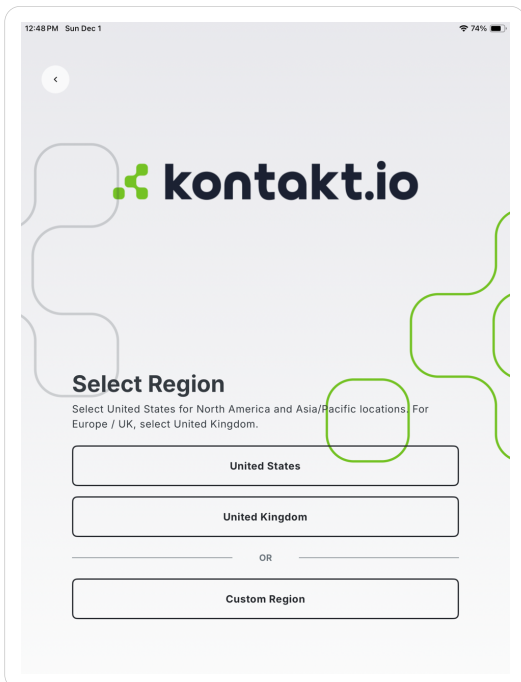
1. From your **iPad**, tap **Kio Alerts**.



- From **Sign in to Kio Cloud**, tap **Kio Cloud Account**.



- From **Select Region**, tap **United States** if your Kio Cloud account is located in **North America** or **Asia/Pacific**, or tap **United Kingdom** if located in **Europe** or the **UK**.



- From **Enter Tenant ID**, enter your organization's ID > tap **Continue**.

Don't know your organization's Tenant ID? This can be found in your organization's Kio Cloud URL (example: [https://\[your Tenant ID\].app.cloud.\[us or uk\].kontakt.io](https://[your Tenant ID].app.cloud.[us or uk].kontakt.io)).



5. **Sign in to your Kio Cloud account.** Ensure you follow the same sign-in method used when you sign into Kio Cloud from a web browser.

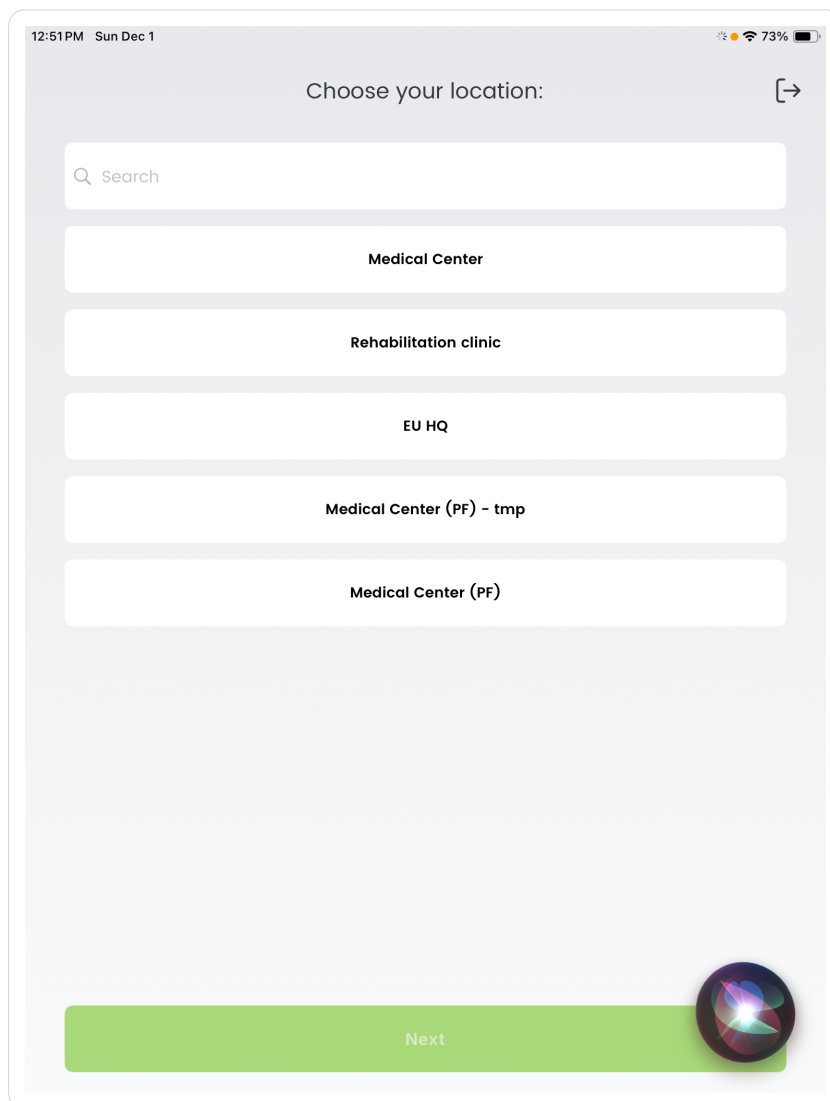
If your organization's Kio Cloud account is set up for Single sign-on (SSO), tap the SSO method displayed and enter your credentials.

Set your location

By setting your campus and building location, you have instant access to only active alerts at these locations. This is helpful if you are required to respond to alerts that occur in specific locations.

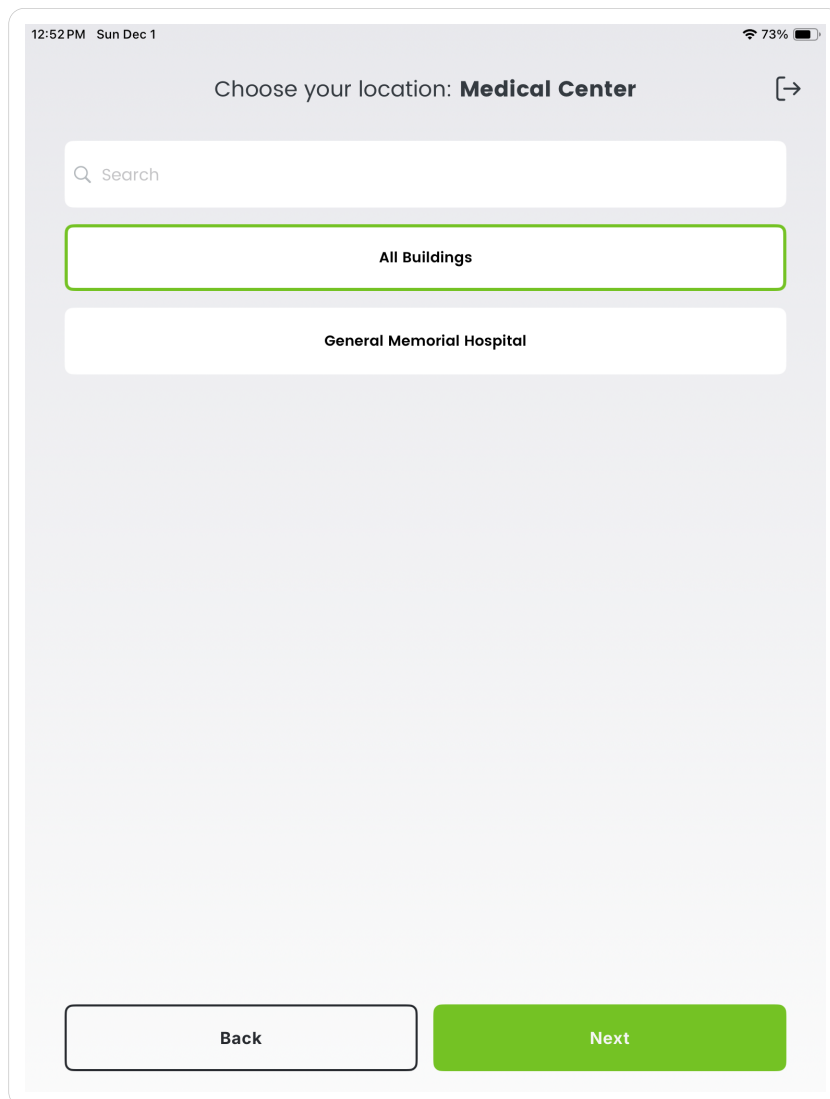
During your first-time sign in, you are prompted to first choose your Campus location and then the building location. You can select one or multiple buildings.

Example: Set your Campus location

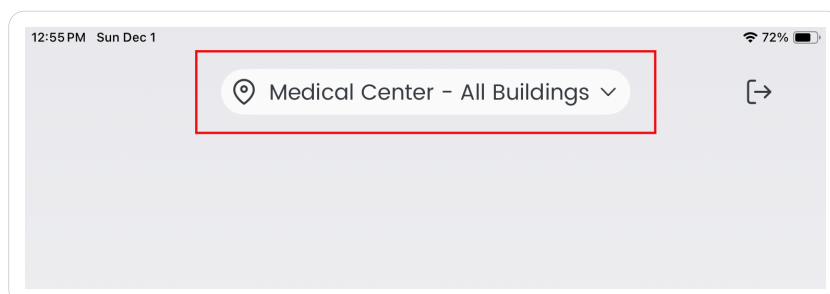


Example: Choose your building location. You can set one or more buildings.





When needed, you can change your location at anytime. From the top of the screen, tap on current set location as shown below.



Respond to and acknowledge an active alert

When you receive an alert notification, the most important step is to **take action and locate the staff to intervene, de-escalate, and provide assistance.**

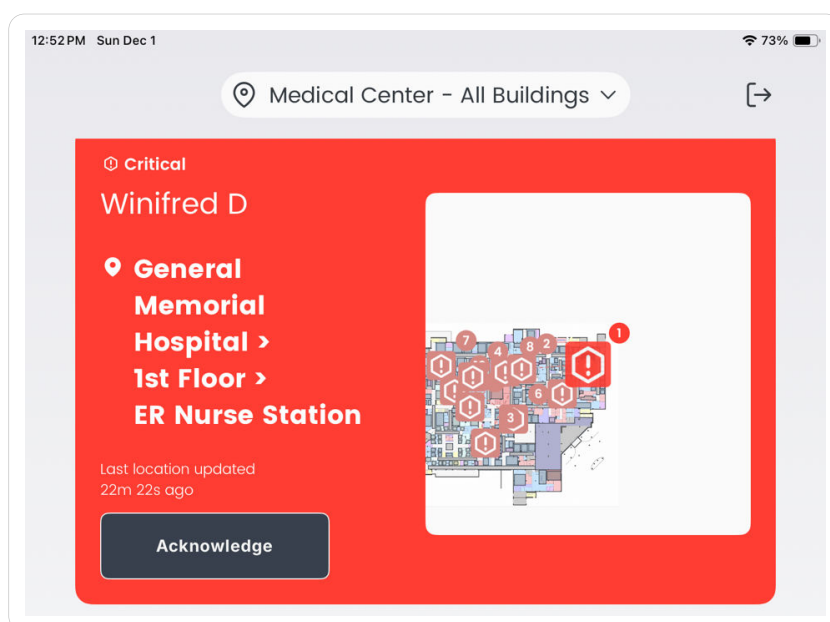


When you receive an alert, from the **Kio Staff Safe Alert iPad app** you can quickly:

- View the **staff's location**, along with details of their last location update.
- **Acknowledge the alert** to indicate that action is being taken. Acknowledging an alert provides other responders and staff with the visibility into the current status of the alerting incident.

An alert pinpoints the staff's last known location with a pulsing icon. If the staff moves to a different room after activating the alert, the location details and map view dynamically update to reflect their current location

Last location detail: Provides when the staff's last location was received. A warning icon is displayed when the last location received has exceeded the lost tag threshold time period.



Critical alert types also emit an audio notification.

Resolve an active alert

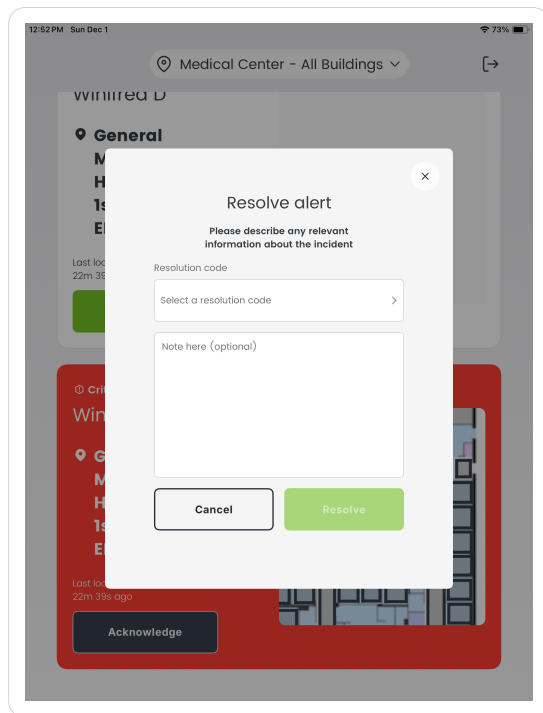
Resolving an alert indicates that the staff incident resulting in the alert has been responded to and de-escalated. Essentially, all necessary actions have been taken to ensure the safety and well-being of the staff member that activated the alert.

Things to know

- To resolve an alert, it must first be in the Acknowledged status. If applicable, you can acknowledge the alert and then proceed to resolve it.



- To resolve an alert, you will be required to select a Resolution Code. The available options are: Duplicate, Handled by security, Handled before security arrived, Accidental, Test, Other.
- When you resolve an alert, it is removed from the Simple View in both the web and iPad mobile app. This ensures immediate visibility into only active alerts.



1. From the app, locate the alert > tap **Resolve**.
2. Tap the applicable **Resolution Code** > enter **Notes** related to the alerting incident > tap **Resolve**.


Notes provided should follow your organization's policies and procedures.

The alert is removed from app.

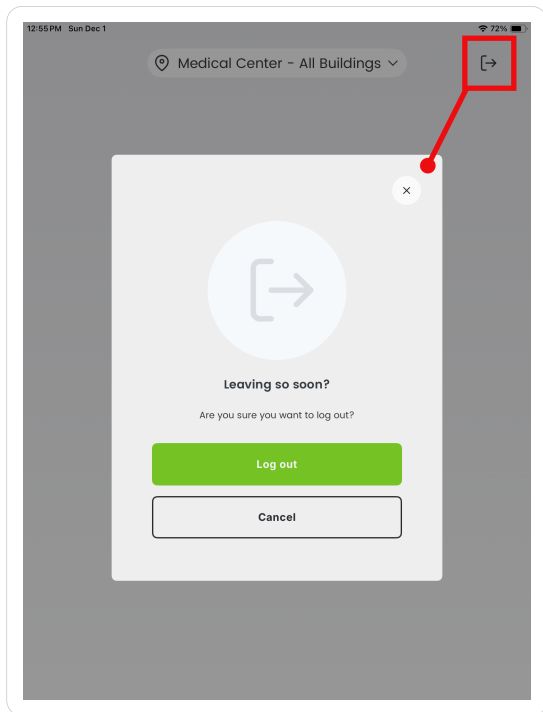
To view the details of a resolved alert, from a web browser sign in to your organization's Kio Cloud URL > select the Kio Staff Safe Emerg. Call app > from the Alerts menu, select the List view > select the Resolved tab > select the alert's Name.

Log out of the app

For security reasons, it's recommended to log out of the app when you're not actively responding to alerts. This is particularly important if multiple staff members share the iPad, as the signed-in user is identified as the one acknowledging or resolving alerts from the app.

From the upper-right corner, tap the icon  > tap **Log out**.





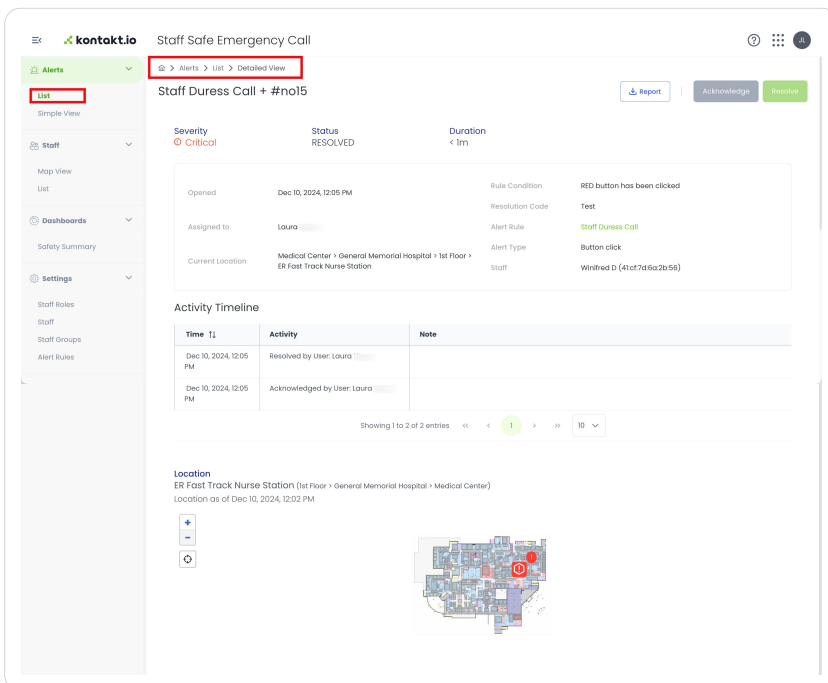
Alert details and history

Each alert maintains a detailed profile with a log of all activities. An alert's activity timeline includes the details of each status change, alert notification details, and notes entered by users. From an alert, you can also download an alert incident report that provide a complete record of all activities.

View the details of an alert

1. From your **Kontakt.io Launchpad**, select **Staff Safe Emerg. Call**.
2. From the **Alerts** menu, select **List**. This view filters the alerts by their current status - New, Acknowledged, Resolved.
3. Once you locate the alert, select its **Name**.

From the alert's profile, you can view the following details and activity.



About the alert details

Detail	Description
Severity	<p>Identifies the severity of the alert.</p> <p>The severity is configured within the Alert Rule that triggered the alert. A rule's severity can be either be Critical, High, Medium, Low, or Info.</p>



Detail	Description
Status	<p>The current state of the alert.</p> <p>Within Kio Staff Safe, the state of an alert is identified by its status — New, Acknowledged, or Resolved — providing users with an instant overview of each alert's current state and enabling data-driven metrics.</p>
Responded by	<p>Only displayed if the Include Responder is set in the Alert Rule that triggered the alert.</p> <p>Responded by is the name of the user (responder), assigned to the Incident Responder Staff Group, that first entered the room-level location of where the alert was activated.</p>
Response Time	<p>Only displayed if the Include Responder is set in the Alert Rule that triggered the alert.</p> <p>The Response Time is the duration of time from when the alert was activated to when the first responder (Responded by) entered the room-level location where the alert was activated.</p>
Duration	<p>The duration of an alert is the total time between when the alert is first triggered (activated) and when it is resolved.</p> <p>This duration measures how long the alert remained in an active state, providing a timeline from activation to resolution.</p>
Opened	Date and timestamp of when the alert was triggered (activated by staff from their Smart Badge).
Assigned to	The name of the user that created the Alert Rule that triggered the alert.
Current Location	The last received location of the staff at the time the alert was activated.
Original Location	<p>The location where the alert was initially activated.</p> <p>This is only displayed if the staff member has moved to a different room-level location from where the alert was originally activated. This feature, along with the current location, helps track both the origin and current location of the staff, which can be critical for safety and response purposes.</p>
Rule Condition	<p>The Alert Rule's button event that activated the alert.</p> <p>The button event is set within the Alert Rule, which can be set to either the blue button, red button, or any button.</p>
Resolution Code	The value selected when a user changed the alert's status to resolved.
Note	The value entered by a user when they changed the alert's status to resolved.
Alert Rule	The name of the Alert Rule that activated the alert.
Alert Type	The Alert Rule type; this value will always be Button click.
Staff	Who activated the alert from their Smart Badge, including the badge's 12 character MAC address.



Activity Timeline

The Activity Timeline includes each activity and a timestamp of all actions taken during from alert activation to resolution.

- Each alert status change - when the alert was activated, acknowledged, and resolved.
- Alert notifications details.
- Who made a status change and the notes entered during a status change.
- Staff room-level location changes that occurred during the duration of the alert.
- If the Alert Rule that triggered the alert is configured with a Webhook, includes the Webhook event and its details.

Location details

Provides the staff's last received location during the duration of the alert, along with any room-level movements recorded during the alert. This information allows you to track the staff's location movements that displays the sequence of locations from a map view.

Download alert incident report

For any alert in a resolved status, you can download the alert's incident report.

1. From your **Kontakt.io Launchpad**, select **Staff Safe Emerg. Call**.
2. From the **Alerts** menu, select **List**. This view filters the alerts by their current status - New, Acknowledged, Resolved.
3. Select the **Resolved** tab > locate the alert > select its **Name**.
4. From the alert, select **Report**. The PDF file is saved to your computer's default download folder.

Example of an incident report.





Incident Report

Powered by



Location: 210-216 Corridor (2nd Floor > General Memorial Hospital > Medical Center)

Date: May 23, 2024, 7:39:44 PM UTC

Duration: 42 minutes

Severity: Medium

Status: Resolved

Resolution code: Low

Staff: Crystal B (0a:59:8a:5b:77:a9)

INCIDENT

On May 23, 2024, 7:39:44 PM UTC, Crystal B (0a:59:8a:5b:77:a9) triggered an alert by pushing Blue button on Kontakt.io device to report an incident at 210-216 Corridor (2nd Floor > General Memorial Hospital > Medical Center).

This incident was resolved in 42 minutes.

NOTES

Example of a resolution note - follow your organizations policies.

FOR MORE INFORMATION

Please contact Julie Lininger.




Download alert incident report

For any alert in a resolved status, you can download the alert's incident report.

1. From your **Kontakt.io Launchpad**, select **Staff Safe Emerg. Call**.
2. From the **Alerts** menu, select **List**. This view filters the alerts by their current status - New, Acknowledged, Resolved.
3. Select the **Resolved** tab > locate the alert > select its **Name**.
4. From the alert, select **Report**. The PDF file is saved to your computer's default download folder.

Example of an incident report.



kontakt.io

Incident Report

Powered by



kontakt.io

Location: 210-216 Corridor (2nd Floor > General Memorial Hospital > Medical Center)

Date: May 23, 2024, 7:39:44 PM UTC

Duration: 42 minutes

Severity: Medium

Status: Resolved

Resolution code: Low

Staff: Crystal B (0a:59:8a:5b:77:a9)

INCIDENT

On May 23, 2024, 7:39:44 PM UTC, Crystal B (0a:59:8a:5b:77:a9) triggered an alert by pushing Blue button on Kontakt.io device to report an incident at 210-216 Corridor (2nd Floor > General Memorial Hospital > Medical Center).

This incident was resolved in 42 minutes.

NOTES

Example of a resolution note - follow your organizations policies.

FOR MORE INFORMATION

Please contact Julie Lininger.



Analytics and metrics

The Kio Staff Safe **Dashboards** menu **Safety Summary** provides insights and metrics for all staff duress alerts.- helping organizations monitor alert trends, response times, and alert resolutions. Users can interact with the dashboard by clicking on bars, locations, or segments in the charts to get detailed insights or filter the data further.

Safety Summary

The following details the features and metrics of the Safety Summary available from the Dashboards menu.

Filters

When a filter is set, it is applied to all metrics.

- **Resolution Codes:** view metrics by all or specific Resolution Codes.
- **Alert Rules:** view metrics by all or specific Alert Rules; identified by the name of the Alert Rules.
- **Location:** view metrics by all or specific location, from campus-wide overviews down to individual buildings and floors within buildings.
- **Date Range:** view metrics by the available time periods or set a custom date range.

Overall metrics

These metrics offer a comprehensive overview of all alert activity, accompanied by visual indicators that signal any changes in alert metrics compared to the preceding date range. For instance, when viewing the Last 30 days the visual indicators depict whether the metrics have increased or decreased in comparison to the prior 30 day time period.



Metric	Definition
Alerts	The total number of alerts. Offers a high-level view of the overall frequency of alerting incidents, useful for trend analysis.
Average Alerts Per Day	Average number of alerts activated daily. Helps gauge the average duress or assistance alerting incidents.



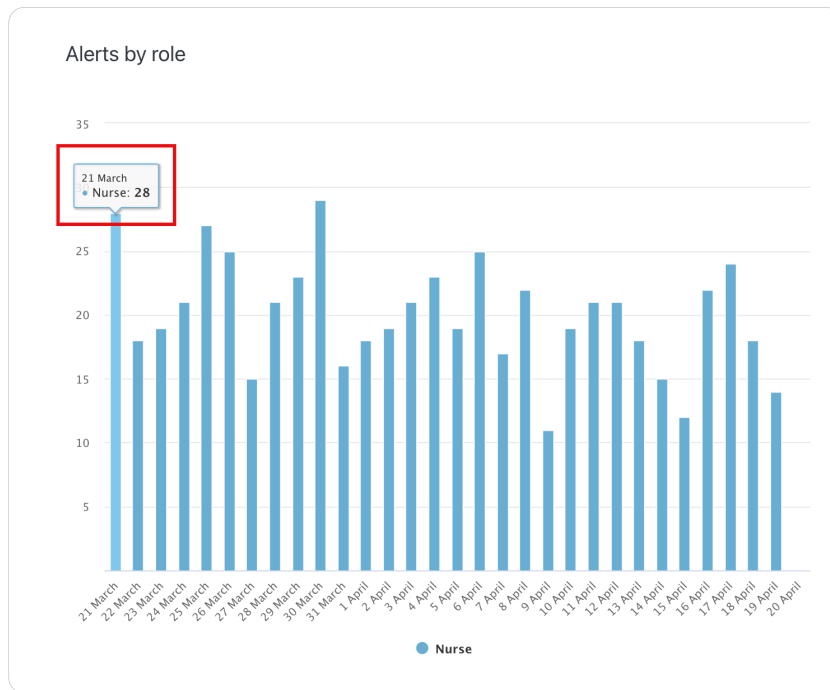
Metric	Definition
Average Time to Acknowledge	<p>Average duration of time taken to change the state of an alert to Acknowledged after its been activated.</p> <p>Specifically, this is the time between when an alert was activated by a button press event to when someone (a responder) changed the alert's status to acknowledged.</p>
Average Time to Respond	<p>The average duration of time for responders to arrive at the room-level location where alerts were activated. Only applies if Alert Rules have a Staff Group assigned to the Include Responder setting.</p> <p>Specifically, this is the time between when an alert was activated by a button press event to when the first responder, assigned to the Include Responder group, entered the room-level location where the alert was activated. Also, when a responder enters the room, the system automatically changes the alert status to acknowledged.</p> <p>Metric prerequisites: (1) Alert Rules assigned to a Include Responder Staff Group(s), (2) Staff Group(s) include staff responsible for responding to alerts (such as security staff), (3) those within the Responder Staff Group are assigned to and wearing a Kontakt.io Smart Badge.</p>
Average Alert Duration	<p>The average duration of time from alert activation to resolution.</p> <p>Indicates overall effectiveness in handling incidents; a shorter duration may signify better time to respond and resolution.</p>



Alerts by role

This metric segments alerts by Staff Roles. This metric can aid in identifying roles that are most frequently faced with duress situations in need of assistance.

You can interact with the chart by selecting a bar within the chart to view more details, and also select a role from the x-axis to filter the chart by role for more targeted insights.

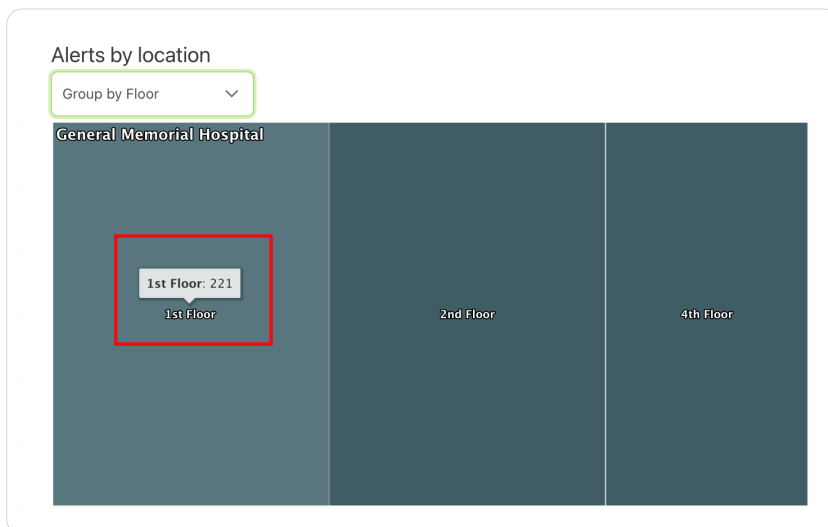
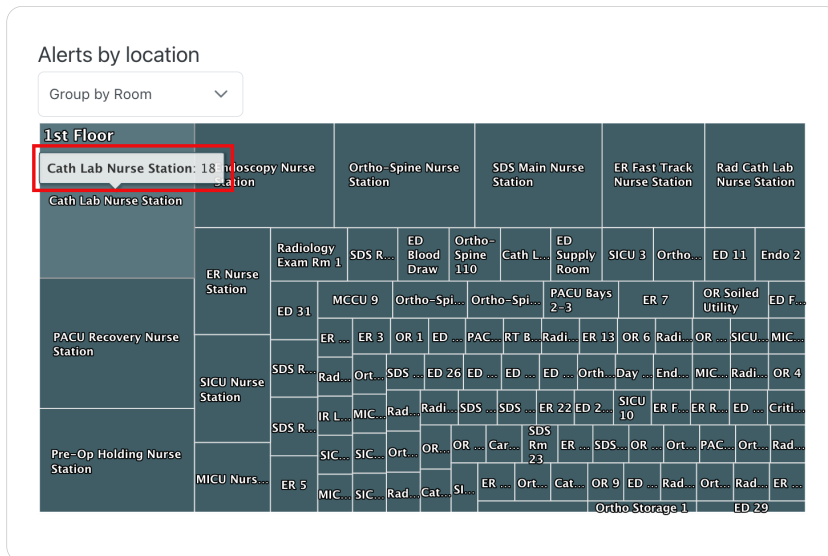


Alerts by location

Segments alerts by specific location, along with the ability to group by room, floor, or building. Can aid in pin-pointing high-risk areas or locations that may benefit from additional resources or safety measures.

You can interact with the chart by selecting a location to view the alert count detail.



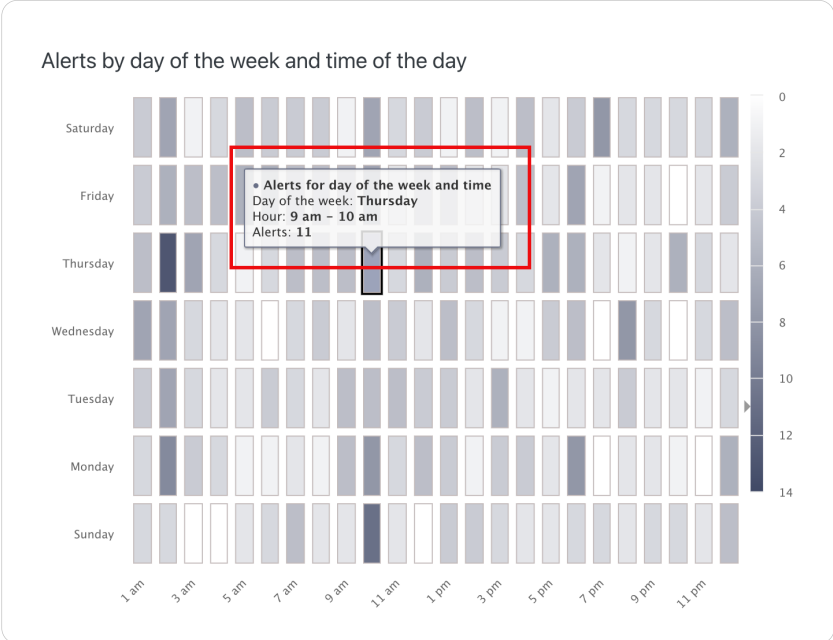


Alerts by Day/Week and Time

Segments the frequency of alerts across different days of the week and time (hour) within each day. Can aid in identifying peak times/days of alerting incidents that may benefit from additional resources or safety measures.

You can interact with the chart by selecting a specific time period to view additional details.

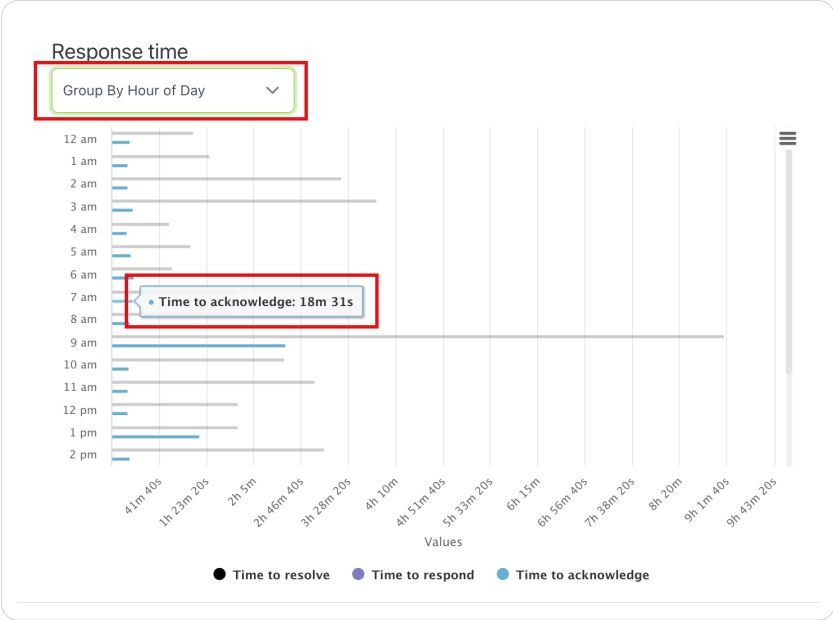




Response time

Segments the alerts by response time based on the time the alert was activated to when it was acknowledged, responded to (requires Include Responder group with an Alert Rule), and when it was resolved.

The metrics can be filter to: Group by Hour of Day, Floor, and Building.





Staff locations

Kio Staff Safe provides the capability to locate staff, equipped with Smart Badges, by campus, building, and at the floor and room-level. This granular level of visibility is especially valuable in large, multi-story buildings where pinpointing staff locations in real-time can significantly impact the outcome of emergency situations. In addition, all location history is stored within each staff's profile.

In the event of an emergency or a security threat, knowing the location of staff allows for the rapid mobilization of nearby personnel. In the case of a required evacuation, having the real-time visibility into staff locations can aid in ensuring that all personnel are safely accounted for and evacuated, enhancing safety protocols.

Search and locate staff

You can quickly determine the location of staff from the Staff List menu.

1. From your **Kontakt.io Launchpad**, select **Staff Safe Emerg. Call**.
2. From the **Staff** menu > select **List**.
3. From the list view, you can **search** by their Staff ID, Name, Attributes, or Tag ID (assigned badge) or apply column **filters** to narrow down the list.
4. From the **Location** section, their location details are displayed, along with a visual floor plan map.

View staff within a specific location

You can quickly identify the staff located within a floor from the Staff Map View.

1. From your **Kontakt.io Launchpad**, select **Staff Safe Emerg. Call**.
2. From the **Staff** menu > select **Map View**
3. Select the **Location** tab.
4. Navigate to the **campus, building** > select the **floor name**.
5. All staff located on the floor are displayed.
6. From the floor plan, each icon represents a staff member. Selecting an icon displays the staff's information.

View staff location history

Each time staff changes a room location, the location change is received and stored by Kio Staff Safe. All location changes are viewable from the profile of each staff member. The data available for each location change includes when Staff entered and exited the room, the location details, and the amount of time they were present in the room.

1. From your **Kontakt.io Launchpad**, select **Staff Safe Emerg. Call**.



2. From the **Settings** menu > select **Staff**.
3. From the list view, you can **search** by their Staff ID, Name, Attributes, or Tag ID (assigned badge) or apply column **filters** to narrow down the list.
4. To view their profile, select their **Staff ID or Name**.
5. Select the **Location History** tab.

By default, the history shows the current day and last 6 days of history. You can also choose a specific date range.



Staff management

Staff management involves creating and managing the staff that are wearing Kontakt.io Smart Badges and Staff Groups. Those wearing a badge are required to be added to Staff Safe and assigned to their badge (tag). Staff also includes responders assigned to a Staff Group within the Include Responder setting in Alert Rules. Once added and assigned to a badge, staff can activate an alert from their badge.



You can also add and manage staff from Company Settings. Kontakt.io recommends use of Company Settings during the first-time setup of Kio Staff Safe and for those that have multiple Kio solution-based apps. In Company Settings, Staff Roles are Entity Types and Staff are Entities - which are located in the Entity Management menu. The only setting that cannot be managed from Company Settings are Staff Groups.

The following staff management instructions are performed from the Kio Staff Safe app.

Things to know

- Only those assigned to the Administrator role within Kio Staff Safe can view and manage staff.
- Staff are required to be assigned to a Staff Role.

A Staff Role is a method to categorize staff by their roles within your organization. Staff Safe provides metrics by roles, and roles can also be assigned to Alert Rules. Staff Roles are Entity Types within Company Settings.

For example, in a healthcare setting roles may include Nurse, Physician, Medical Assistant, to Security. And in a workplace environment, roles could represent departments, teams, or a job type or classification.

- Staff can optionally be assigned to Staff Groups.

Staff Groups provide an additional method to segment staff. Unique to groups, staff can be assigned to one or multiple groups,

Staff Groups are required for the "response time" metric. When configuring an Alert Rule, a specific Staff Group is assigned to the Incident Responder setting. The response time is measured by the system tracking which responder - a staff member wearing a smart badge and assigned to the group - first enters the room location where an alert was activated.

- Kontakt.io Smart Badges worn by a staff are identified as a Tags in the Kio apps.

Tags are Kontakt.io's IoT BLE devices that are either worn by people (Smart Badge, Nano Tag) or attached to things (Asset Tag).



- There are a few Staff Management capabilities that can only be completed from Company Settings, which includes:

Editing the Staff Role assigned to Staff (Entity)

Editing a Staff Role's icon or color (Entity Type)

Editing the values set in a Staff Role's Status Group & Value (Entity Type)

Deleting Staff Roles (Entity Types)

Add a Staff Role

Staff Roles are a categorization of staff that commonly mirrors the types or roles or positions within your organization. All staff are required to be assigned to a Staff Role. Staff Roles are included in alert metrics and can also be assigned to Alert Rules.

1. From your **Kontakt.io Launchpad**, select **Staff Safe Emerg. Call**.
2. From the **Settings** menu, select **Staff Roles**.
3. From the upper-right corner, select **Create Staff Roles**.

4. Configure the following settings:

Name: enter a unique name to identify the role.

Profile Type and Assigned Applications are automatically set to the Kio Staff Safe values.

5. Select **Next** and update the **Status Descriptor Status values** for the role. Optional, and may or may not apply to your Kio Staff Safe deployment.

The Status Descriptor is for use in Room Type rules. These rules provide the capability to automate the status of assets or people (entities) by their real-time room location.

6. Select **Next** > you can now create **Attributes** for the role > select **Add Attribute**. This is an optional setting.

Attributes set in a Staff Role are a form of metadata (information) that's provided for the staff assigned to the role. For example, this could include their job title, department, or contact information. Attributes can be set to required or optional.

Staff assigned to this role will inherit these Attributes and their values are provided when staff are added.

7. Select **Create**. Staff can now be assigned to this new role.



The Staff Role's icon and color, which are displayed in maps, is managed from the Staff Role (Entity Type) in Company Settings.

Add Staff Groups

Staff Groups provide a method to group staff or segment staff. Staff can be assigned to one or multiple groups.



Staff Groups are required for the "response time" metric. When configuring an Alert Rule, a specific Staff Group is assigned to the Incident Responder setting. The response time is measured by the system tracking which responder - a staff member wearing a smart badge and assigned to the group - first enters the room location where an alert was activated.

1. From your **Kontakt.io Launchpad**, select **Staff Safe Emerg. Call**.
2. From the **Settings** menu, select **Staff Groups**.
3. You can create a group or add multiple groups at the same time.

To create a group, select **Create Group** > enter its **Name** and select a color > select **Save**.

To add multiple groups (bulk add), there must be one group created. To add multiple groups, select **Export CVS** > add the groups to the CSV file (do not delete or change the header row) > select **Import CVS** to add the groups.

Staff can now be assigned to the Staff Group from their profile.

Add staff

1. From your **Kontakt.io Launchpad**, select **Staff Safe Emerg. Call**.
2. From the **Settings** menu, select **Staff**.
3. From the upper-right corner, select **Create Staff**. A new staff profile is created.
4. Configure the following settings.

Staff Role: from the drop-down list, select their role.

Staff ID: must be unique value; duplicates are not allowed. This could be an the staff's ID within another system.

Staff Name: should identify the person; duplicates are allowed. Serves as an alias of their Staff ID or a secondary unique identifier.

Assigned Tag: select the Kontakt.io Smart Badge being given to the staff. The badge's unique ID and MAC address is printed on the badge. A badge can also be assigned at a later date.

Attributes: when the assigned Staff Role has required attributes, you will need to provide these values now.

5. When done, select **SAVE**.

If you need to assign a Staff Group, return to the Staff view and select the Staff's ID or Name. From their profile, you can then assign one to multiple groups.

Add multiple staff at one time (bulk add)

When you need to add a handful to hundreds of new Staff, you can leverage the export and import features. You'll first export a CSV file, add the staff to the file, and then import the file.





Before you begin, be sure there is one staff for each Staff Role being added.

During this bulk add process, you will export a CSV file to serve as a template. Staff Roles may have different attributes, included in the export CSV file, and you want to ensure to have all settings when bulk adding staff.

For example, if you have multiple Staff Roles, such as a Nurse, Security, and Provider, you'll need one staff for each role before you begin.

1. From your **Kontakt.io Launchpad**, select **Staff Safe Emerg. Call**.
2. From the **Settings** menu, select **Staff**.
3. From the **Staff Type** column, select its **filter icon** > enter the name of the **Staff Role** of the staff being added.
4. With the user(s) displayed for the Staff Role, select **Export CSV**.
5. From the Exported CSV file, add each user as a row and their column settings.
Do not delete or change the first row column names.
If there are settings that are not known, a user profile can be update once they are added to Kio Staff Safe.
6. Once the file includes all users and saved, select **Import CVS**.
7. From the **Staff** menu, verify the new users have been added.



Staff badge management

Staff badge management involves assigning staff to their Kontakt.io Smart Badge and replacing a badge if it becomes lost or damaged. When staff activate a duress alert from their badge, their assigned badge is how Kio Staff Safe knows their real-time location and provides responders with this critical information to locate staff when it matters the most.

Things to know

- Assigned role: You must be assigned to the Staff Safe Administrator role to manage badges assigned to staff.
- Power on badge: [66] By factory default, badges arrive powered OFF from Kontakt.io and are required to be powered ON prior to distributing badges to staff. If your organization has ordered badges to arrive powered ON, when distributing a badge be sure to verify its powered ON.
- When assigning staff to their badge, be sure to verify they are associated to an Alert Rule. [70]
- Badges can also be assigned from the Kio Entity Manager mobile app.

Assign badge to staff

Before a Kontakt.io badge is distributed to a staff member, they must be assigned to the badge. Each badge has a Unique ID and MAC address, which is printed on the badge's holder, non-button side.

You can assign staff to their badge from the Kio Staff Safe web app (instructions below), Kio Entity Manager mobile app, or from the staff's entity in Company Settings.

With the badge in hand, complete the following steps from **Kio Staff Safe**.

1. From your **Kontakt.io Launchpad**, select **Staff Safe Emerg. Call**.
2. From the **Settings** menu, select **Staff**.
3. From the list, locate the staff.
4. Select their **Staff ID or Name**. Their profile is displayed.
5. From the upper-right corner, select **Edit**.
6. From the **Assigned Tag** section, search for the badge's 12-character MAC address or Unique ID > select the badge.
7. Verify that the badge's MAC address or Unique ID is correct.
8. Select **Save**.



9. To verify the badge assignment and the staff is associated to an alert rule, it's recommended to activate a test alert from the badge. Once the alert is activated, you can resolve the alert and set its Resolution Code to Test and log a note indicating testing badge assignment and operation. If an alert was not activated from a button press (three times in quick succession), verify the staff is associated to an Alert Rule and the button press that triggers an alert (blue, red, or either button).

If the staff member is new to Kio Staff Safe, be sure to share the article Guide to activate a staff duress alert [27]. This article also includes a Quick Start Guide and explainer video.

Replace a staff's badge

When a Kontakt.io Smart Badge is lost, damaged, or being returned to Kontakt.io for warranty, a new badge is required to be assigned the staff member. The staff's assigned badge (tag) delivers their real-time location when they activate an alert, which is why a proper replacement and badge assignment is critical. If a damaged badge is to be disposed of, be sure to follow your organization's electronic device disposal policy.



Write down the 12-character MAC address of both badges - printed on the holder, non-button side of the badge. If the badge being replaced is lost, you can get its MAC address during Step 1.

Step 1: Assign the new badge to staff

1. From your **Kontakt.io Launchpad**, select **Staff Safe Emerg. Call**.
2. From the **Settings** menu, select **Staff**.
3. From the list, locate the staff member that requires their badge to be replaced.
4. Select their **Staff ID or Name**. Their profile is displayed.
5. From the upper-right corner, select **Edit**.
6. From the **Assigned Tag** section, select the **tag** > select **Clear Filters** > search for the new badge's 12-character MAC address and select the new badge.
7. Select **Save**.



To verify the badge assignment and the staff is associated to an alert rule, it's recommended to activate a test alert from the badge. Once the alert is activated, you can resolve the alert and set its Resolution Code to Test and log a note indicating a replacement badge test was performed. If an alert was not activated from a button press (three times in quick succession), verify the staff is associated to an Alert Rule and the button press that triggers an alert (blue, red, or either button).

Step 2: Update the Deployment Status of each badge

The Deployment Status of a badge represents its current lifecycle, indicating whether it is:



- Deployed: in use (assigned)
- To be Deployed: available inventory (can be assigned)
- End of life: no longer in use or disposed of

The Deployment Status is also used by Kio Cloud Device Health to monitor badges (tags), with only badges in the Deployed status are actively monitored.

1. From your Kontakt.io **Launchpad**, select **Device Management 2.0**.
2. From the **Inventory** menu, select **Tags**.
3. Update new badge status:

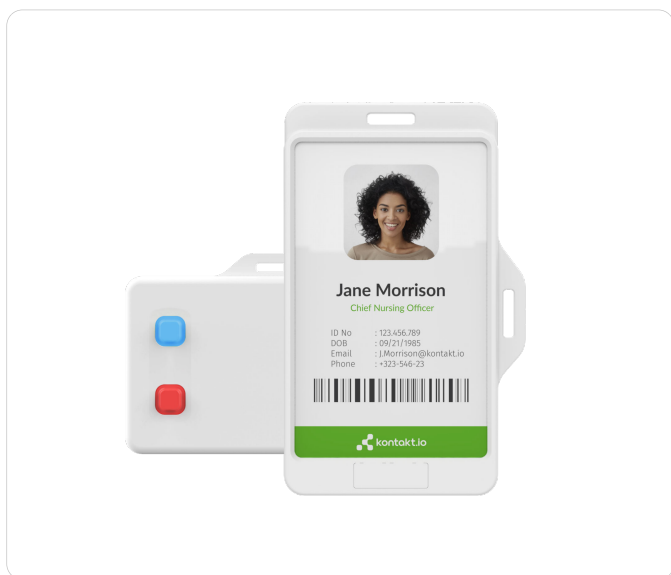
From the **Search Devices** field, enter **MAC address** of the **new badge** assigned > select is **ID** > from the **General** tab, set its **Deployment Status** to **Deployed** > select **Save**.

4. Update the badge replaced:

From the **Search Devices** field, enter the badge's **MAC address** > select is **ID** > from the **General** tab, set its **Deployment Status** to **End of life** > select **Save**.

Power on or off a Smart Badge

By default, Smart Badges are shipped from Kontakt.io with their power OFF and must be powered ON before use. However, you can request to have badges shipped powered ON when placing an order.



Topics include:

- Power on a Smart Badge [67]
- Power off a Smart Badge [67]



- Verify a Smart Badge is powered on [67]

Power on a Smart Badge

If a badge's LED does not blink after pressing and quickly releasing either the blue or red button, follow these steps to turn it on:

1. **Press and hold** either the blue or red **button for 5 seconds**.
2. When you see the button LED blink, it's your confirmation the badge is ON.

Power off a Smart Badge

To power off a badge, follow these steps:

1. **Press and hold** either the **blue or red button for 5 seconds**.
2. Once the **LED stops blinking**, it indicates that the badge has been **turned OFF**.

When OFF, the LED does not blink when pressing and quickly releasing a button.

Verify a Smart Badge is powered on

To verify a badge is ON, press and quickly release the BLUE or RED button and verify you see its LED blink for a few seconds.



Continuously pressing either button may result in activating a button press event. If you do not see an LED blink after a button press, do not press a button for 5 seconds to allow the device to clear the previous button event.

Smart Badge insert reference card

Prior to distributing badges to staff, this handy reference card can be printed and inserted into the badge.


[Download PDF for the Smart Badge model](#)



kontakt.io Smart Badge + Activate Duress Alert
response to your real-time location


How to signal for help

Press either **button**
3 times in quick
succession



Wear on site at all times
Buttons facing your body
Not covered by other items
Not in your pocket

Watch the video




Download PDF for the Smart Badge 3 model

kontakt.io Smart Badge + Activate Duress Alert
response to your real-time location


How to signal for help

Press either **button**
3 times in quick
succession



Wear on site at all times
Buttons facing your body
Not covered by other items
Not in your pocket

Watch the video



If your organization has Alert Rules configured to activate staff duress alerts from only the blue or red button or if the badges are configured to activate an alert with one press, please submit a support request. Our team can provide custom PDF inserts.

Additional resources

The following provide learning resources for staff wearing Kontakt.io Smart Badges.



- Kio Staff Safe Quick Start Guide

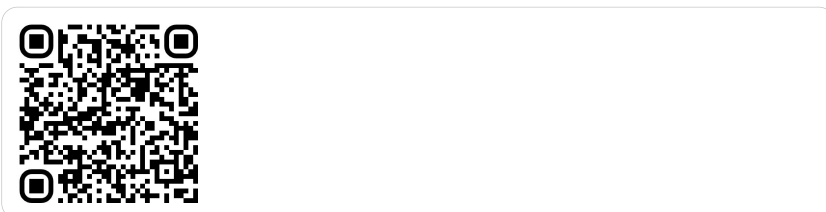
Provides instructions for activating a duress alert by **pressing any button three times in quick succession**, along with guidelines for **wearing a badge**.

The buttons that activate an alert, either the blue, red, or any button, and the number of presses may vary by your organization's deployment.

- Kio Staff Safe explainer video. Get a 2 minute overview of how it all works.

This video highlights a Portal Light infrastructure along with Smart Badges. Your deployment may vary to include third-party BLE to Wi-Fi gateways such as Cisco Access Points, and Kontakt.io Beam Minis or Portal Beams.

Scan the QR Code



Alert Rule management

Alert Rules define the monitored conditions that trigger staff duress alerts, primarily based on button events from a Kontakt.io Smart Badge that are worn by staff.

When the conditions set in an Alert Rule are met, the rule activates a new alert and notifications are sent. These conditions include the Smart Badge button event (blue, red, or any button), the staff the rule applies to, the location monitored by the rule, and actions. Actions specify who receives alert notifications and the notification method. Notifications can be sent via email, SMS text, or through a Webhook to a third-party system. Webhooks are configured in Company Settings and assigned to Alert Rules.



To view and manage Alert Rules, you must be assigned to the Administrator role within the Kio Staff Safe app. Roles are managed by those assigned to the Administrator role within the Kio Cloud Users app.

Alert Rule settings

Each rule is configured with the following settings.

Category	Settings
General	<p>Alert Name: Uniquely identifies the rule. Recommended to define a standard naming convention. For example, Campus name or building. location, type of alert, staff type (role, group) as "Main Campus Critical Nurses Only"</p> <p>Alert Description (optional): For information sharing purposes.</p> <p>Alert Severity: Options include: Critical, High, Medium, Low, and Info. A rule set to Critical, results an in-app and audio notification.</p> <p>Include Responder: To allow the system to auto-acknowledge a first responder and track response time metrics, an Alert Rule's Include Responder setting is required to be assigned to a Staff Group. A Staff Group(s) must include those Staff designated as responders for the alerts activated by the Alert Rule.</p>
Applies To	<p>Identifies the staff, those wearing and assigned to a Smart Badge, the rule will monitor. Options include: specific Staff, Staff Role, or Staff Group.</p> <p>When any of the staff assigned to the Applies To activates an alert from their badge, the Alert Rule immediately triggers a new alert and sends alert notifications that are defined within the rule's Actions.</p>
Locations	<p>Identifies the locations, managed in Kio Cloud Smart Location, the rule will monitor.</p> <p>For example, if you have multiple campuses and responders unique to each campus, assigning specific campus locations to a rule allows you to set the rule's actions (alert notification methods) to be set to the specific location responders.</p>



Category	Settings
Conditions	<p>The Smart Badge button event that will activate and trigger an alert.</p> <p>Options include: Blue Button, Red Button, or Any Button.</p>
Actions	<p>Identifies how responders or other staff are notified when an alert is activated by a staff from their Smart Badge.</p> <p>An alert is required to be set to one action and multiple methods can be set. Regardless of the method, all alert notifications include the Alert Severity, Staff Name, and the location where the alert was activated including the campus, building, floor, and room.</p> <p>Available notification methods include:</p> <ul style="list-style-type: none"> • Email: Alert notifications are sent to each email address. Be sure to include a subject and optionally add additional information to the message. • Text (SMS): Alert notifications are sent to each phone number. Phone numbers must include the country code (for example, for the US entered as 1-area code-xxx-xxxx). • Webhooks: Alert notifications are sent to a third-party system. Webhooks are managed from Company Settings and commonly created and configured by IT staff or those responsible for integration. <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>! To allow those that receive notifications to view, acknowledge, and resolve an alert, they are also required to be a Kio Cloud User assigned to a Staff Safe user role with permissions to alerts [75].</p> </div>

Create an alert rule

When creating a new alert rule, you'll be guided through the six configuration steps.

1. From your **Kontakt.io Launchpad**, select **Staff Safe Emerg. Call**.
2. From the **Settings** menu, select **Alert Rules**.
3. Select **Create Alert > Button Click**.



4. You are guided through each the following configuration steps.


- **Step 1: General:** set the name to uniquely identify the rule and its severity level.

If your organization is tracking alert response times by responders wearing badges, from the Include Responder setting, select the Staff Group the responders are assigned to.

By default, the rule is in active status (ON) and monitors the configured conditions that will trigger alerts. If you don't want alerts to be triggered, such as during the setup phase, you can deselect Activate Alert Rule after saving. When you begin a testing or go-live phase, the rule's status will be required to be changed to ON.

- **Step 2: Locations:** select the campus and or building locations the rule will monitor.
- **Step 3: Applies to:** select the staff the rule will monitor.
- **Step 4: Conditions:** select the button event that triggers an alert.
- **Step 5: Actions:** set how and who is notified when an alert is activated.
- **Step 6: Summary:** verify all settings are correct. To edit a setting, select its edit icon.

5. Once the six steps are complete, select **Save**.

 Once a new Alert Rule is active (ON), it's recommended to test activating alerts on a subset of badges following your organization's acceptance testing requirements.

Edit an alert rule

1. From your **Kontakt.io Launchpad**, select **Staff Safe Emerg. Call**.
2. From the **Settings** menu, select **Alert Rules**.
3. From the list, locate the rule > select its **Alert Name**. Its profile is displayed.
4. Select **Edit** > locate the setting being edited > select its **edit icon**.

To edit additional settings, select NEXT to advance to the next group of settings.

5. Once complete, select **Save**.



Alert Rules and Webhooks

Kontakt.io supports a one-way integration to send Kio Staff Safe alerts to third-party systems. This is achieved using Webhooks, which are created and managed within the Kio Cloud Company Settings. Once created, Webhooks are then assigned to Kio Staff Safe Alert Rules to enable the integration.

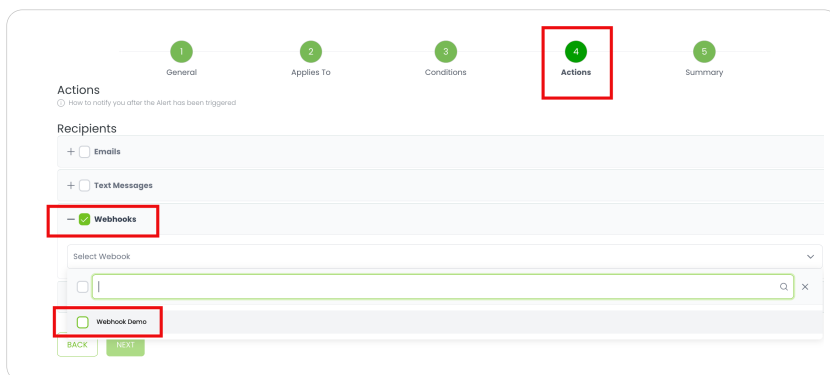
Prerequisites

- Alert Rule [70] is created.
- Webhook is created in Kio Cloud Company Settings and assigned to the Staff Safe Emergency Call app.
- You're assigned to the Kio Staff Safe Administrator [75] role.

Assign a Webhook to an alert rule

An Alert Rule can be assigned to one or multiple Webhooks. If you need to create a new Alert Rule, from the relevant Kio App, go to its Settings menu > select Alert Rules > Create Alert Rule.

1. From your **Kontakt.io Launchpad**, open the relevant Kio App.
2. From the **Settings** menu, select **Alert Rules**.
3. From list, select the **Name** of the Alert Rule > select **Edit**.
4. Navigate to the **Actions** section > select the **Webhook** option > select the **Webhook** to be assigned.



5. Select **Save**.

Test the Webhook integration

1. Activate an alert.

Staff Safe alert: activated from a Kontakt.io Smart Badge - staff assigned to the badge must be included in the Alert Rule with the assigned Webhook.

2. Confirm the third-party system received the alert.



- From your **Kontakt.io Launchpad**, select the relevant **Kio App** > navigate to the **Alerts** menu, select the **List** view > locate and select the **alert** activated in step 1 > view its **Activity Timeline** > verify the Webhook event is present and view its details.
- Go to **Kio Cloud Company Settings** > navigate to the **Webhooks** menu > select the **History Log** tab > verify the alert event details and a successful status (200).

View an alert's Webhook events

When an alert is triggered by an Alert Rule with an assigned Webhook, you can view the Webhook event from the alert's profile.

- From your **Kontakt.io Launchpad**, select the **Staff Safe Emerg. Call** app.
- Navigate to the **Alerts** menu, select the **List** view.
- Locate and select the **alert** > view its **Activity Timeline** > locate the Webhook event and view its details.
- From the **Activity Timeline** > locate the Webhook alert event(s).

Each event response/status provides option to show details for additional information.

The screenshot displays the 'Staff Safe Emergency Call' alert profile. The top section shows alert details: 'Opened' on Aug 20, 2024, 01:34 PM, 'Rule Condition' 'RED button has been clicked', 'Resolution Code', 'Alert Rule' 'Danger Zone R', and 'Alert Type' 'Button click'. The 'Current Location' is 'Kaskada > Cathall > Floor 1 > Büro'. A floor plan is visible on the right.

The 'Activity Timeline' table shows the following events:

Time	Activity	Note
Aug 20, 2024, 01:34 PM	Notification delivered via webhook. Status code: 200. Show details	
Aug 20, 2024, 01:34 PM	Error occurred. Response from the webhook was not successful. Status code: 404. Show details	
Aug 20, 2024, 01:34 PM	Notification has been scheduled to be sent via WEBHOOK channel (id: 13a88970-e771-4979-866c-54b96e0a0a83, 3f5940b-9b6c-4d8a-9b79-74d3d7bd9fa).	
Aug 20, 2024, 01:34 PM	Notification sent to [redacted] via EMAIL.	

The 'History log details' panel for the selected event shows:

- ID:** [redacted]
- Webhook:** Accept
- Log Date:** Aug 20, 2024, 01:34 PM
- URL:** [redacted]
- Status code:** 200

The 'Request' section shows an outgoing request to a remote server with headers: POST https://[redacted], accept: */*, content-length: 20, content-type: text/plain; charset=UTF-8, host: [redacted], User-Agent: Kio Cloud/1.0, X-Kio-Cloud-Request-id: 452a86ff-59f4-4e35-bdbd-1cf4a273f29a. The body contains a message: [{"message": "[redacted]"}].

The 'Response' section shows an incoming response with headers: Incoming Response: 452a86ff-59f4-4e35-bdbd-1cf4a273f29a, Duration: 8 ms, HTTP/1.1 405 Method Not Allowed, Connection: keep-alive, content-length: 150, Content-Type: text/html, Date: Tue, 20 Aug 2024 11:34:11 GMT, Server: [redacted], Set-Cookie: AWSALB=[redacted]; [redacted].



User access management

For those who require access to **Kio Staff Safe**, they need to be added as users and assigned roles from the Kio Cloud Users app. Kio Cloud utilizes role-based permissions to control user access to Kio apps and their permission levels.

Things to know

- You must be assigned to the Administrator role within User Management to view, add, and edit users.
- If a user is not assigned to a role within an app, the app is not displayed in their Kio Cloud Launchpad.
- A user's email address can only be associated with a single Kio Cloud account.
- Once a user is added, only the Kontakt.io support team can change their email address. You will need to submit a Kontakt.io support request for an email address change.
- If your organization has integrated Kio Cloud with its Single Sign-On (SSO) identity provider (IdP), user management within the Kio Cloud Users app is limited to viewing SSO users and their assigned roles. The first time a user authenticates to Kio Cloud with their SSO credentials, their user profile is automatically created within the Kio Cloud Users app.
- The apps available are those activated in your organization's Kio Cloud account. If you don't see an app or want to activate another app, submit a Kontakt.io support request

Roles associated to Kio Staff Safe administration

Optionally, you may also choose to assign the Kio Staff Safe users to roles within the related apps, which include Company Settings and Entity Manager. These users are commonly those responsible for administration type tasks.

- **Company Settings** Includes Entity and Room Management.
Entity Management is where Entity Types (staff roles) and Entities (staff) are also managed.
Room Management includes room types, room matching, and room type rules by entity type. Room management is only managed from Company Settings and is shared with each of the Kio solution-based apps.
- **Entity Manager** Commonly used by those only responsible for adding and managing staff and assigning and distributing badges. The Mobile App user role also grants a user's access to the Kio Entity Manager mobile app to assign badges to staff.

About user profiles

Each user has a unique profile that includes the following details.

- **First Name, Last Name, Email**



- **Unique Ext id:** A unique Staff ID (Entity ID in Company Settings) that allows up to a maximum of 35 characters.

Commonly, an unique identifier from an external system or can be a ID for use within the Kio solution-based apps.


Additionally, required to access the iOS Kio Nurse Assistant mobile app for Asset Tracking and Hand Hygiene.

- **Sign-in method:** identifies if the user's sign in and authentication method, either SSO or email.
- **Roles for apps:** identifies the user's assigned role within each app within the Kio Cloud platform.

Staff Safe: roles and permissions



All roles will receive in-app visual and audio notifications for critical alert types.

Role	Permissions
Administrator	<p>✔ This role has full permissions — they can view and manage everything within the app.</p> <p>What a user assigned to this role can do:</p> <ul style="list-style-type: none"> • View all data and perform actions within all menus - including Alerts, Analysis, and Settings. • Manage Staff including adding and editing Staff Types (basic settings), Staff (basic settings), and Staff Groups. • Manage (add, edit, delete) Alert Rules. <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p> Advanced Staff (Entity) management is completed from Company Settings. This includes the capabilities to manage the advanced settings for Staff Roles (Entity Types) and Staff (Entities), including the capabilities to delete Staff Roles and remove Staff.</p> <p>For those only responsible for managing Staff, consider assigning a user to the Staff Manager role in the Entity Manager app. This role has limited permission that restricts a user to only adding and editing Staff.</p> <p>For those only responsible for assigning Smart Badges to Staff, consider assigning a user to the Mobile User role in the Entity Manager app. This role has limited permissions that restricts a user to assigning badges from the Kio Entity Manager mobile app.</p> </div>



Role	Permissions
User	<p>✔ This role has restricted permissions to only the Alerts and Dashboard menus — they can view all data within these menus and perform all actions including changing the status of an alert (acknowledged, resolved) and download alert incident reports.</p> <p>✘ This role does not have permission to the Settings menu.</p> <p>Role is ideal for: those that require access to alert activity and metrics, and may also be responsible for responding to alerts and tasked with documenting incident activities.</p>
Alert User	<p>✔ This role has restricted permission to only the Alerts menu including the List and Simple View — they can view all alerts and details, change the status of an alert (acknowledge, resolve), and download alert incident reports.</p> <p>✘ This role does not have permission to the Analysis and Settings menus.</p> <p>Role is ideal for: those responsible for responding to alerts and tasked with documenting alert incident activities.</p>

Add a user and assign their roles

1. From your **Kontakt.io Launchpad**, select **Users**.
2. From the upper-right corner, select **Add User**.
3. Enter their **details** > select **Add User**. They will receive an email from hello@kontakt.io to set their password.
4. Next, you'll need assign their role for the apps they require access to. From the **list of users**, search for their name > select their **name**.
5. From the section **Roles for Apps** > select **Edit**.
6. From each app they require access to, **select a role** to assign their permissions > select **Save**.

Edit a user's assigned roles

A user's assigned role determines their access and permissions within each of the apps. If a user is not assigned to a role within an app, the app is not available from their Kontakt.io Launchpad.

1. From your **Kontakt.io Launchpad**, select **Users**.
2. From the list of users, locate the user > select their **Name**.
3. From the **Roles for Apps** section, select **Edit**.
4. From an app, update their assigned role > select **Save**.



Remove a user's access to Kio Cloud

From a user profile, the disable and delete options allow you to remove a user's access to your Kio Cloud account. Once removed, all user activity within the Kio apps is retained for historical metrics and reference. Commonly, this action is performed when a user has left your organization or no longer requires access to Kio Cloud.

- **Disable option:** Only applies to users that sign in with SSO.
- **Delete option:** Only applies to users that sign-in with email.

