

# Kio Staff Safe

## Alert Rule Administration Guide

## Table of Contents

Alert Rule management .....	3
Alert Rule settings .....	3
Create an alert rule .....	4
Edit an alert rule .....	5
Alert Rules and Webhooks .....	6
Prerequisites .....	6
Assign a Webhook to an alert rule .....	6
View an alert's Webhook events .....	7



## 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
<b>General</b>	<p><b>Alert Name:</b> 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><b>Alert Description (optional):</b> For information sharing purposes.</p> <p><b>Alert Severity:</b> Options include: Critical, High, Medium, Low, and Info. A rule set to Critical, results an in-app and audio notification.</p> <p><b>Include Responder:</b> 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>
<b>Applies To</b>	<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>
<b>Locations</b>	<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
<b>Conditions</b>	<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>
<b>Actions</b>	<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"> <li>• <b>Email:</b> Alert notifications are sent to each email address. Be sure to include a subject and optionally add additional information to the message.</li> <li>• <b>Text (SMS):</b> 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).</li> <li>• <b>Webhooks:</b> 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.</li> </ul> <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 10px; margin-top: 10px;"> <p><b>!</b> 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.</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.

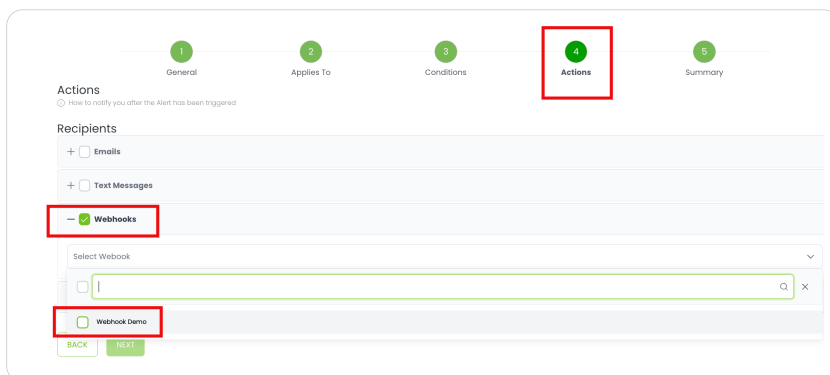
### Prerequisites

- Alert Rule [3] 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 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 alert profile for "Staff Safe Emergency Call". The alert is "Opened" on Aug 20, 2024, at 01:34 PM. The rule condition is "RED button has been clicked". The resolution code is "Danger Zone R". The alert rule is "Button click". The current location is "Kaskada > Cathall > Floor 1 > Büro".

The Activity Timeline shows four events:

Time	Activity	Note
Aug 20, 2024, 01:34 PM	Notification delivered via webhook. Status code: 200. <a href="#">Show details</a>	
Aug 20, 2024, 01:34 PM	Error occurred. Response from the webhook was not successful. Status code: 404. <a href="#">Show details</a>	
Aug 20, 2024, 01:34 PM	Notification has been scheduled to be sent via WEBHOOK channel (id: 13a88970-e771-4979-866c-54b96e0a0a83, 3f5940b-9b6c-448a-9b79-7403a7bd9fa).	
Aug 20, 2024, 01:34 PM	Notification sent to [redacted] via EMAIL.	

The History log details for the selected event (Aug 20, 2024, 01:34 PM) are as follows:

```

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

Request
Outgoing Request: 452a86ff-59f4-4e35-bdbd-1cf4a273f29a
Remote: [redacted]
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
{"message": "[redacted]"}

Response
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]; ~VjogvDgvgfjJURBTWV+

```

