# Team Leader GuideMobile Guide

Version 6.11.4.1

Legal Notice

This document is proprietary and confidential to Aurea and is available only under a valid non-disclosure agreement. No part of this document may be disclosed in any manner to a third party without the prior written consent of Aurea. The information in these materials is for informational purposes only and Aurea assumes no responsibility for any errors that may appear therein. Aurea reserves the right to revise this information and to make changes from time to time to the content hereof without obligation of Aurea to notify any person of such revisions or changes.

You are hereby placed on notice that the software, its related technology and services may be covered by one or more United States (“US”) and non-US patents. A listing that associates patented and patent-pending products included in the software, software updates, their related technology and services with one or more patent numbers is available for you and the general public’s access at https://markings.ipdynamics.ai/esw/ (the “Patent Notice”) without charge. The association of products-to-patent numbers at the Patent Notice may not be an exclusive listing of associations, and other unlisted patents or pending patents may also be associated with the products. Likewise, the patents or pending patents may also be associated with unlisted products. You agree to regularly review the products-to-patent number(s) association at the Patent Notice to check for updates.

Aurea and Aurea Software are registered trademarks of Aurea Software, Inc. in the United States and/or other countries. Additional Aurea trademarks, including registered trademarks, are available at: https://www.aurea.com/legal/trademarks/. Jive is a registered trademark of Jive Software, Inc. in the United States and/or other countries. Additional Jive trademarks, including registered trademarks, are available at: https://www.jivesoftware.com/legal/.

# Third-party Acknowledgments

The following third party trademarks may appear in one or more Aurea® user guides:

- Amazon is a registered trademark of Amazon Technologies, Inc.
- Apache and Derby are trademarks of the Apache Software Foundation.
- Chrome is a trademark of Google Inc.
- Eclipse is a registered trademark of the Eclipse Foundation, Inc.
- HP-UX is a registered trademark of Hewlett-Packard Development Company, L.P.
- IBM, AIX, DB2, and WebSphere are registered trademarks of International Business Machines Corporation.
- Intel and Pentium are trademarks of Intel Corporation in the U.S. and/or other countries.
- JBoss is a registered trademark, and CentOS is a trademark, of Red Hat, Inc. in the U.S. and other countries.
- Linux is a registered trademark of Linus Torvalds.
- Microsoft, Active Directory, Internet Explorer, SharePoint, SQL Server, Visual Studio, and Windows are registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.
- Mozilla and Firefox are registered trademarks of the Mozilla Foundation.
- Netscape is a registered trademark of AOL Inc.
- Oracle and Java are registered trademarks of Oracle and/or its affiliates.
- Progress and OpenEdge are registered trademarks of Progress Software Corporation or one of its subsidiaries or affiliates in the U.S. and other countries.
- Red Hat and Red Hat Enterprise Linux are registered trademarks of Red Hat, Inc. in the U.S. and other countries.
- SAP and SAP NetWeaver are registered trademarks of SAP SE in Germany and in several other countries.
- SUSE is a registered trademark of SUSE, LLC.
- Sybase is a registered trademark of Sybase, Inc. in the United States and/or other countries.
- Ubuntu is a registered trademark of Canonical Limited in the United States and/or other countries.
- UNIX is a registered trademark of The Open Group in the United States and other countries.

# Contents

# Chapter 1: About AlertFind

AlertFind® Enterprise Notification Service is a cloud based, multi-tenant emergency and mass notification service (EMNS) provided as a Software-as-a-Service offering on a subscription basis.

It is intended to automate and facilitate notifications to recipients by broadcasting alerts or other messages via multiple communication channels defined in each recipient's notification profile. These channels of communication include voice calls to land lines or mobile phones using TTS (text-to-speech) or recorded voice capabilities, SMS, email and fax.

AlertFind can also integrate seamlessly with enterprise systems of record. Also, valuable contact information and group definitions can be imported into the AlertFind database and data exported out of AlertFind to capture updates made by employees.

This section provides a brief overview of how to log into AlertFind and how to send and receive notifications.

AlertFind is delivered through an application service provider (ASP) at an off-site hosting center. There is nothing to install in your environment. All interaction with AlertFind is through the web-based user interface.

# Supported Browsers

To access AlertFind, use one of the following supported web browser, with cookies and JavaScript enabled. Other browsers may not work correctly with AlertFind:

- Microsoft® Internet Explorer™ version 11 or above
- Latest Mozilla® Firefox® release version
- Latest Google Chrome "Stable" version
- Apple® Safari™ version 5.0 and higher on the Macintosh™ only
- Edge Chromium

**NOTE**

AlertFind will work with earlier versions of the major browsers but the only actively tested and supported browsers are the versions listed above.

To use the web interface to listen to notifications with attached voice recordings, install a compatible media player that supports the `.wav` audio format (for example: QuickTime or Windows Media Player). Quit AlertFind, install the media player, and then restart AlertFind.

To view the online help, you must also have JavaScript enabled in your browser.

# AlertFind Mobile App

Welcome to the AlertFind Mobile Administrator & Team Leader Guide. This guide provides step-by-step instructions for administrators and team leaders on using the AlertFind Mobile web application to open incident templates, and send and track notifications from their tablet or smartphone.

## Getting Started

### Supported Operating Systems and Devices

AlertFind Mobile has been designed to work on tablets and smartphones that use the following mobile device operating systems:

- Apple iOS (4+)
- Android OS (2+)

Due to the wide variety of mobile devices that run the Android operating system, we cannot certify that the AlertFind Mobile application can run optimally on every device.

You can download the AlertFind app from App store or Google Play store.

## Logging in and Registering the device

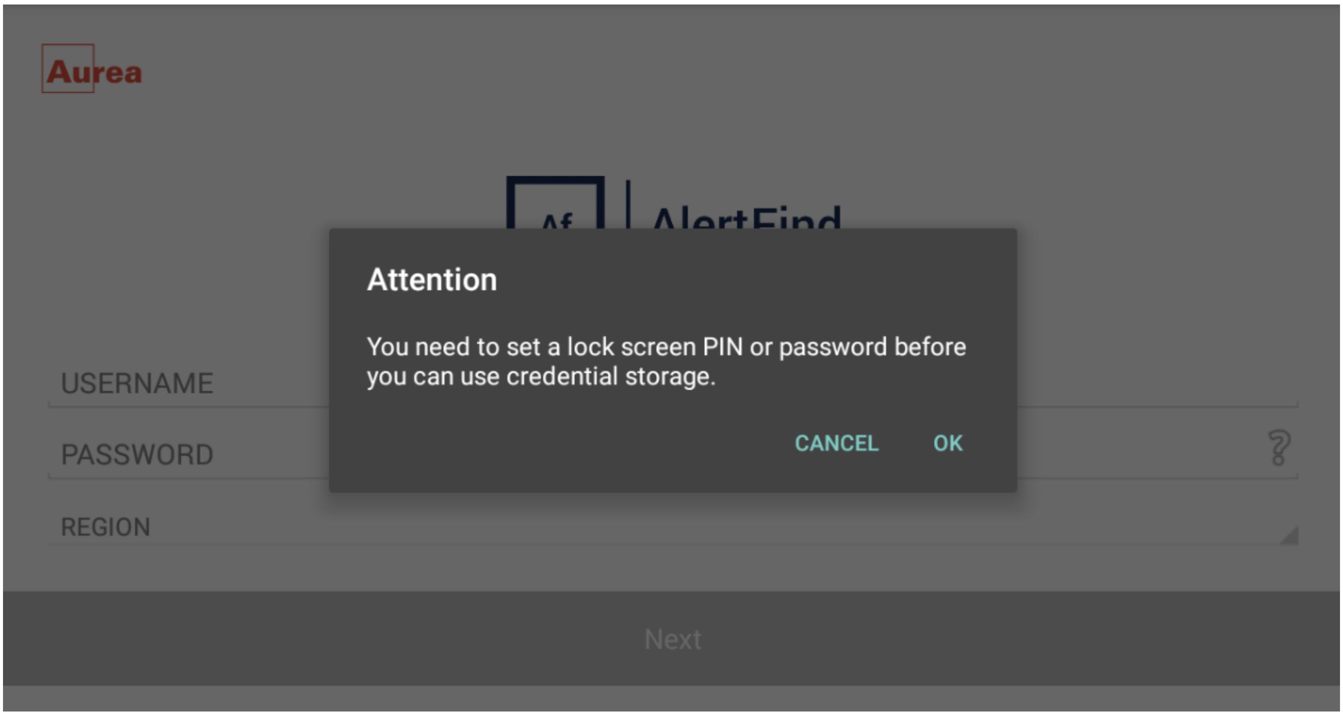
You should have the log in credentials assigned to you by your organization. Use this to login to the AlertFind mobile app, iOS or Android. The credentials are same as that for web.

Username is in the form of `user@company.com`.

**Pre-requisites to login:**

For Android users

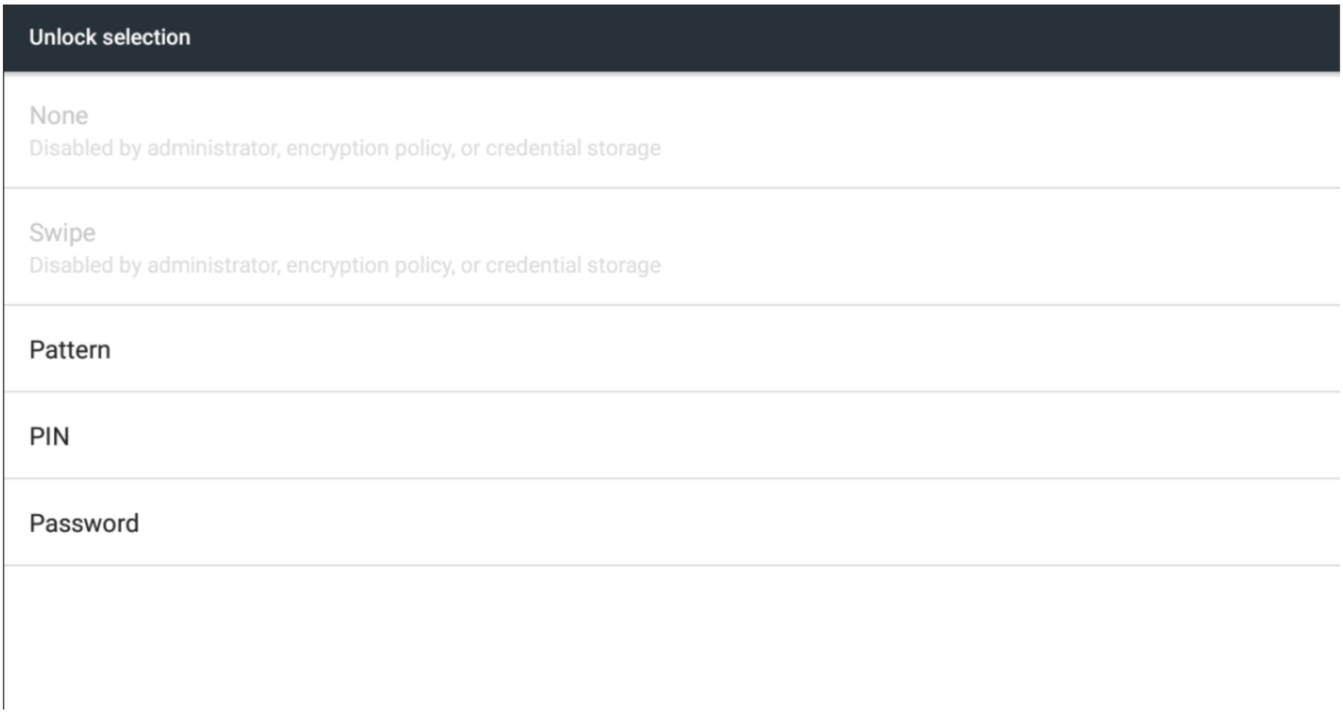
For security purposes, you have to set up a pin/password/pattern before you are taken to the log in screen, as the android OS does not make it mandatory to set these to operate the phone.



Attention

You need to set a lock screen PIN or password before you can use credential storage.

Lock Screen, PIN or Password alert


Unlock selection

None
Disabled by administrator, encryption policy, or credential storage

Swipe
Disabled by administrator, encryption policy, or credential storage

Pattern

PIN

Password

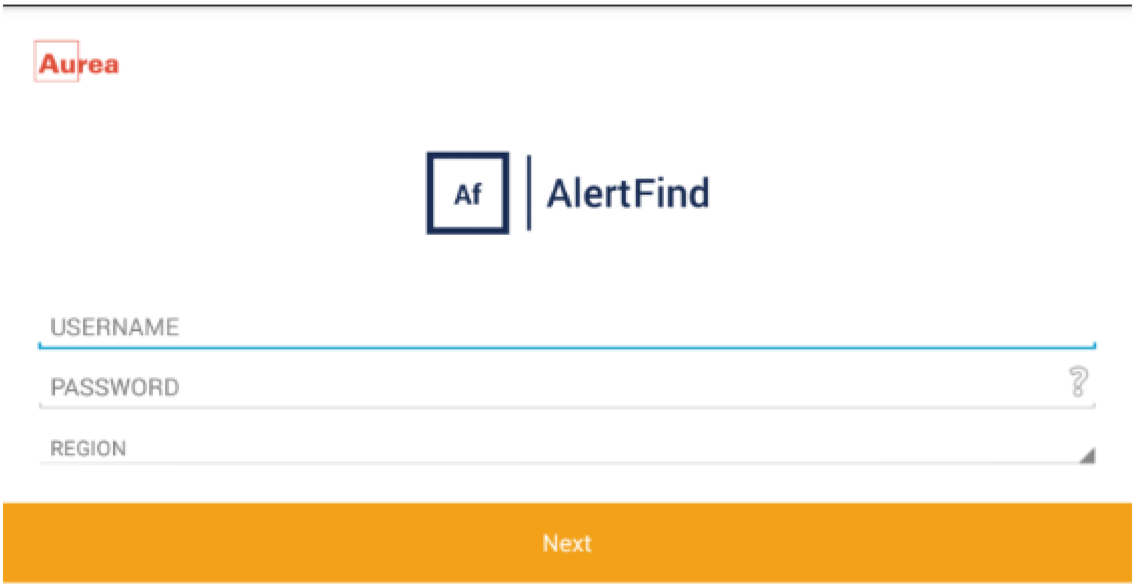
Select pattern, PIN or password

For iOS users

You are directly taken to the log in screen where you can enter your credentials, as you cannot operate your iphone without setting a pin/password/pattern.

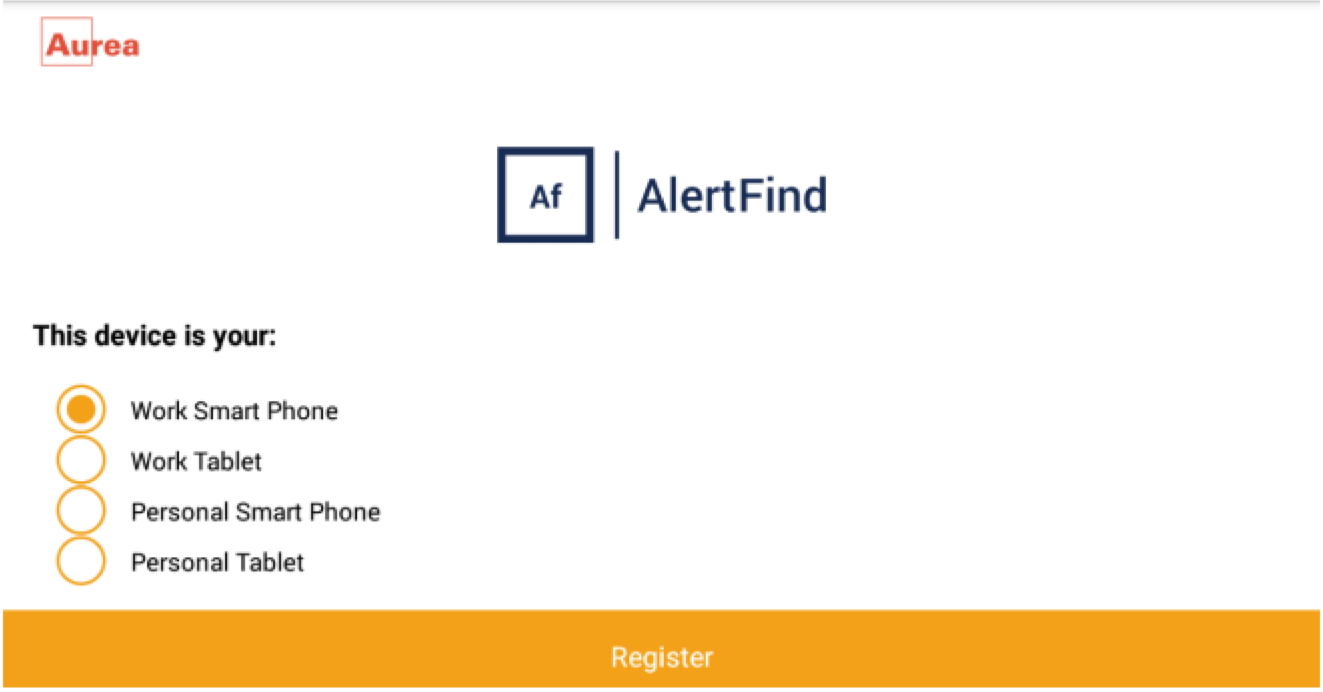
**To login and register your device:**

1. Enter **USERNAME**, **PASSWORD** and select **REGION**. Click on **NEXT**.



Enter your login credentials

2. On the device registration screen, select the device type.

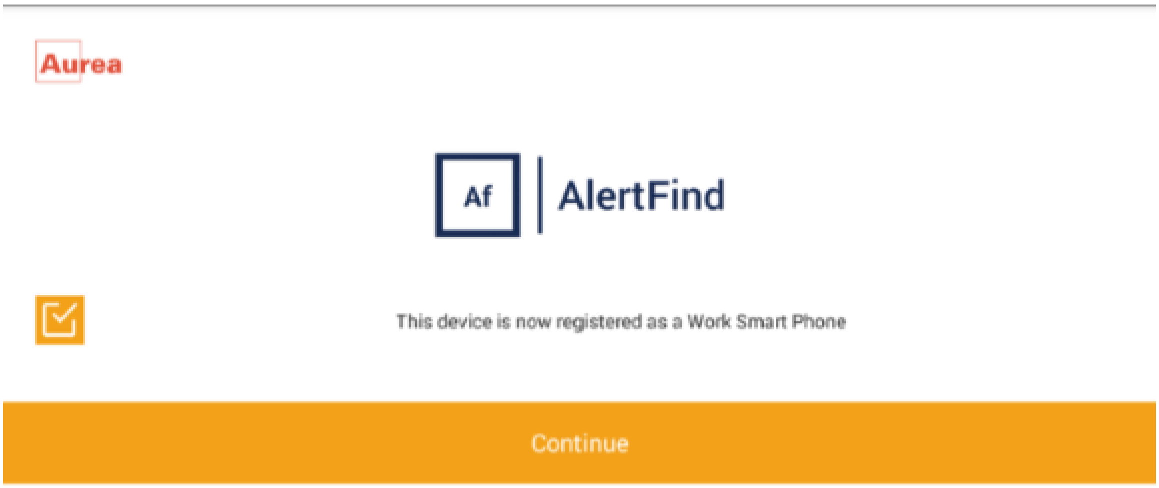


This device is your:

● Work Smart Phone
○ Work Tablet
○ Personal Smart Phone
○ Personal Tablet

Choose from the list of devices

3. Click **Register**.
4. Device registration page is displayed. Click **Continue** to start using the app.



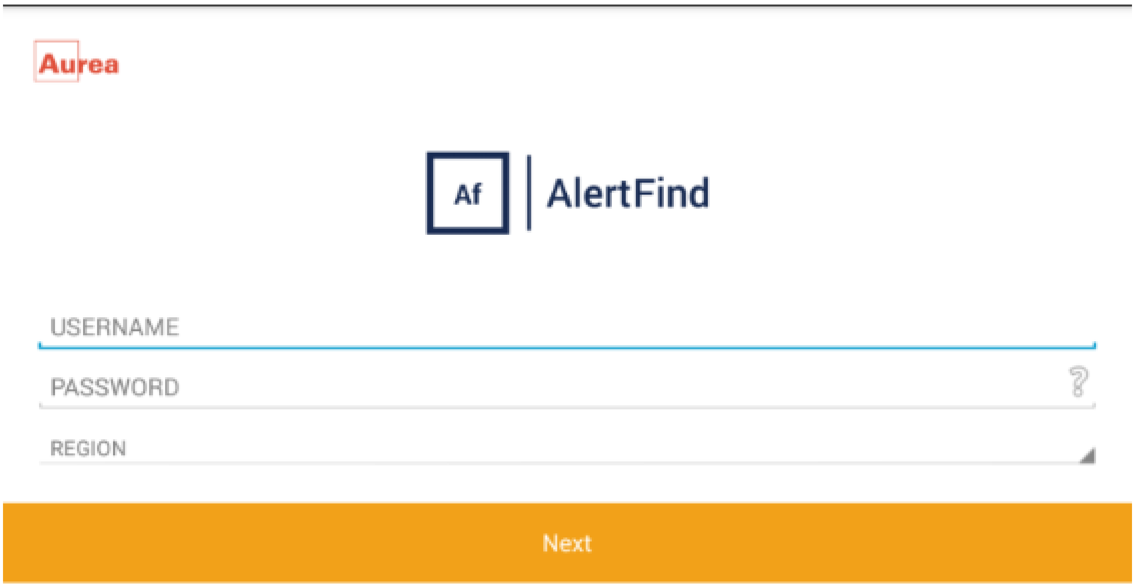
This device is now registered as a Work Smart Phone

Device registration confirmation

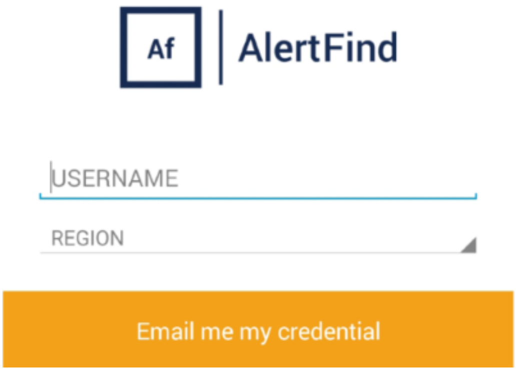
## Recover Forgotten Password

If you forget your password, do the following to recover it:

1. Click ? in the password field on log in screen. You are redirected to a page with fields **Username** and **Region**.



Login Screen



You can reset your passwor from here

2. Enter the **USERNAME** and select the region then click on **Email me my credential**. Your credentials are e-mailed to you.

## Location Check-in

You can manually provide a real-time update of your current location so that your organization's incident response or security teams can send you alerts relevant to your location.

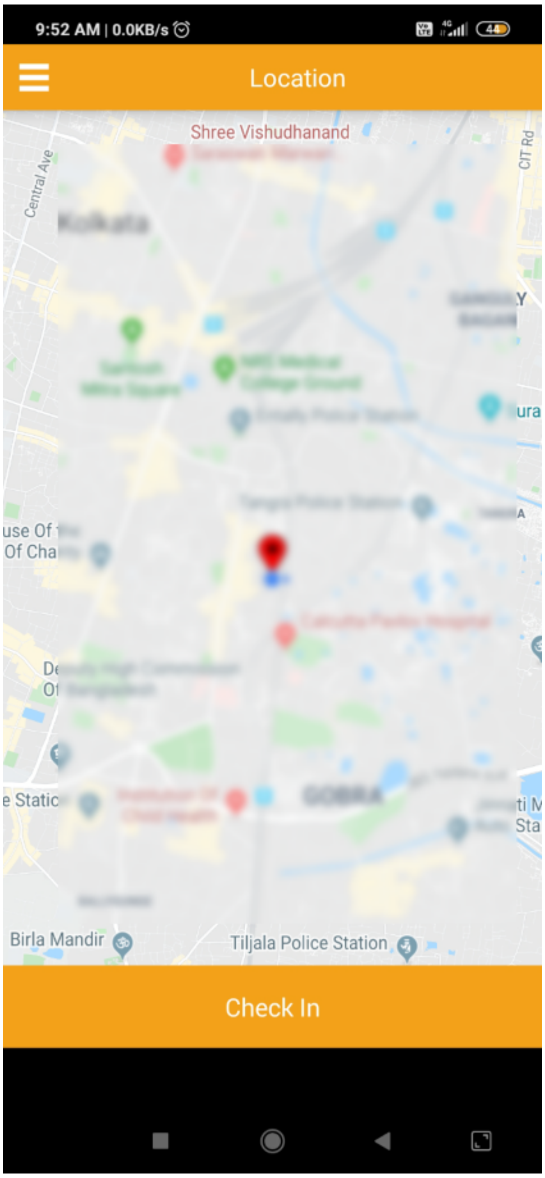
The AlertFind app does not track your location automatically. When you check in your current location in recorded. Your captured location data is only available to your account administrator.

To ensure accurate location capture, enable both Wi-Fi and GPS location service on your mobile.

If you update your location while travelling, remember to update your location once you are back home. This is to ensure that you do not receive irrelevant notifications.

For location check in, do the following:

1. Click ≡ on the top left corner and select **Location Check In**.
2. Click **Check In** on the Google map. A confirmation message is displayed with the coordinates for your current location.



Check In your location on map

3. Click **Close**.

## Using AlertFind App

Login to use the AlertFind Mobile app. The home screen of AlertFind Mobile is the Notification screen. Swipe down to refresh the screen.

You can use the top left Navigation menu ≡ to access the available features of the AlertFind Mobile app.

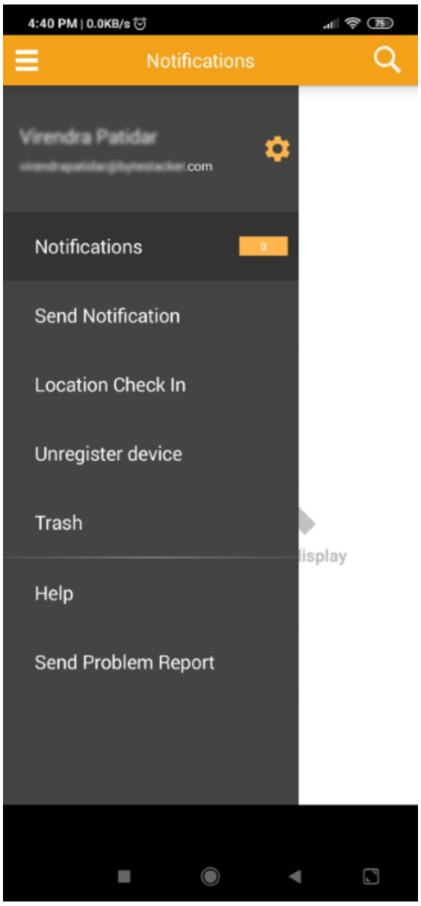
The top panel has a search icon 🔍 which can be used to find notifications.

## Unregister Device

You need to unregister your device if you want to change the device type, for example personal phone to work phone.

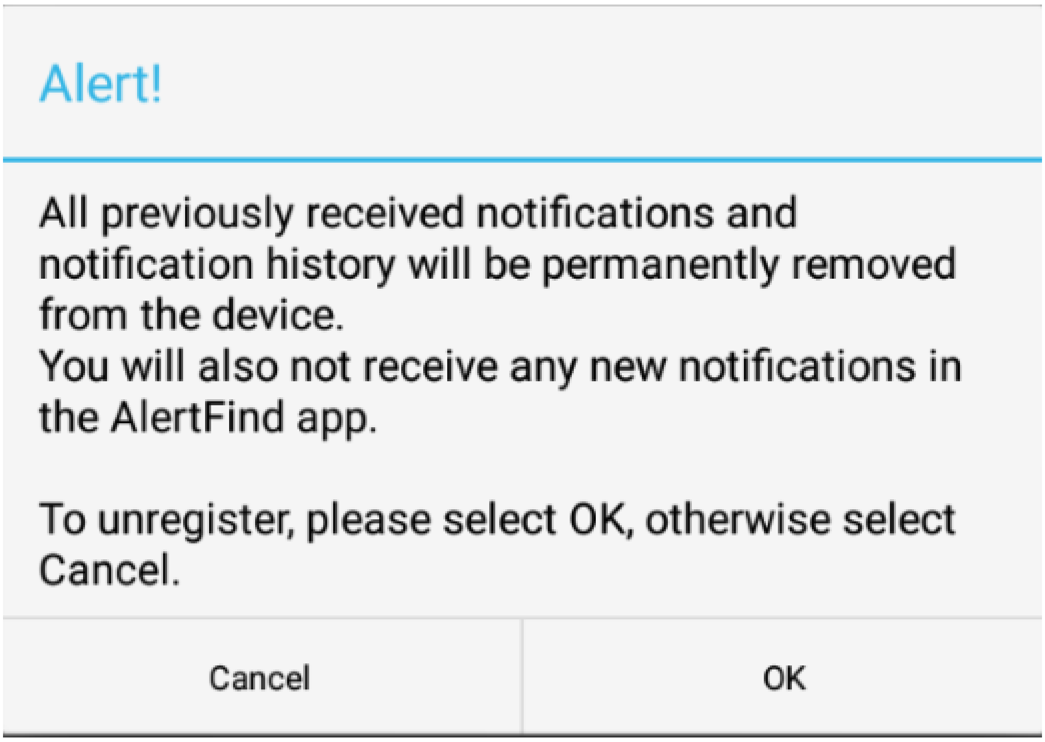
To unregister your device, do the following:

1. Click ☰ on the top left corner and select **Unregister Device**.



Select Device Unregister

2. Click **Ok** on Alert pop up.



Alert!

All previously received notifications and notification history will be permanently removed from the device.
You will also not receive any new notifications in the AlertFind app.

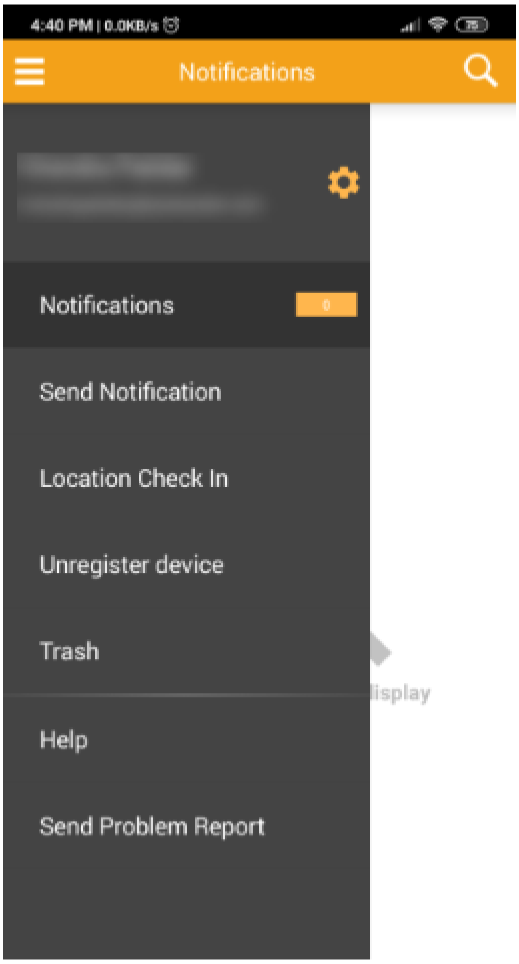
To unregister, please select OK, otherwise select Cancel.

Device Unregister alert message

## Notification

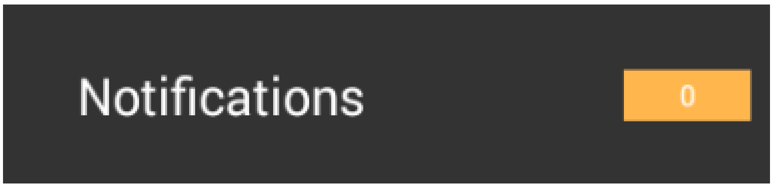
Notification page shows the list of notifications received.

To access notification page, click ☰ from the top left corner.

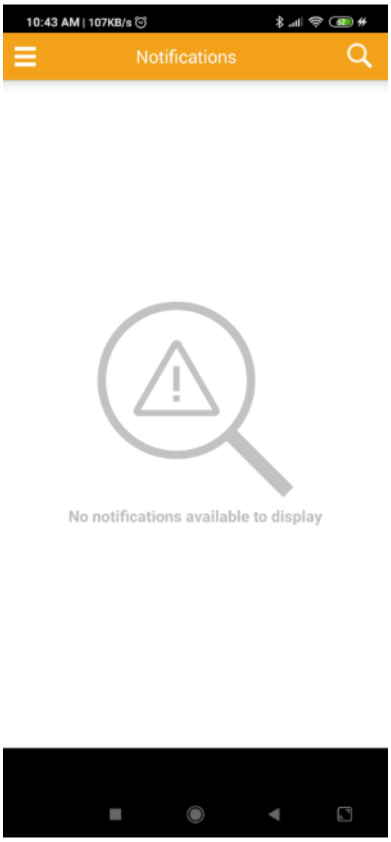


Menu items

From the menu click **Notifications**. The menu item shows the number of Notifications received in an orange box.



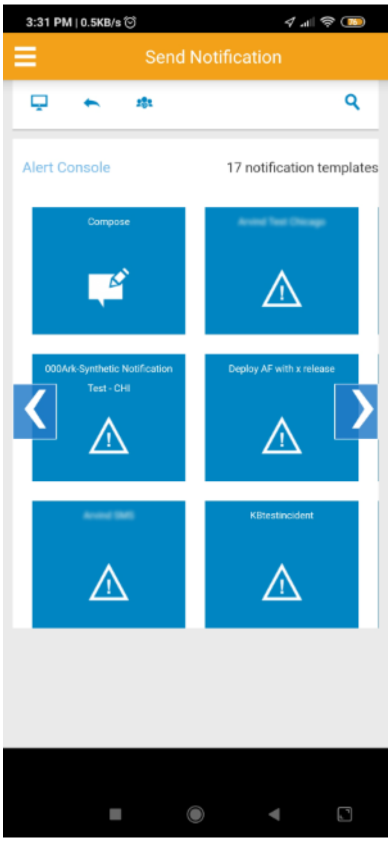
Notifications Count



Notifications Screen

## Using Alert Console

The **Alert console** is the landing page for the **Send Notification** screen. To access alert console from other section of **Send Notification** screen, click 🖥.

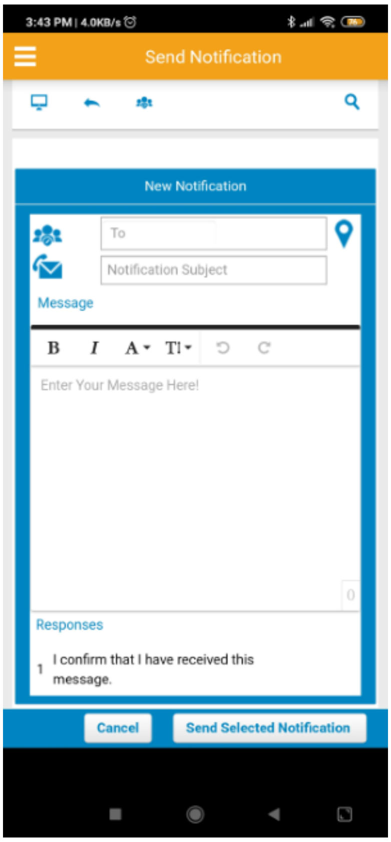


Alert Console view

There are two ways to send notification from Alert Console:

Using Compose

1. Click on **Compose** tile. **New Notification** editor is displayed.



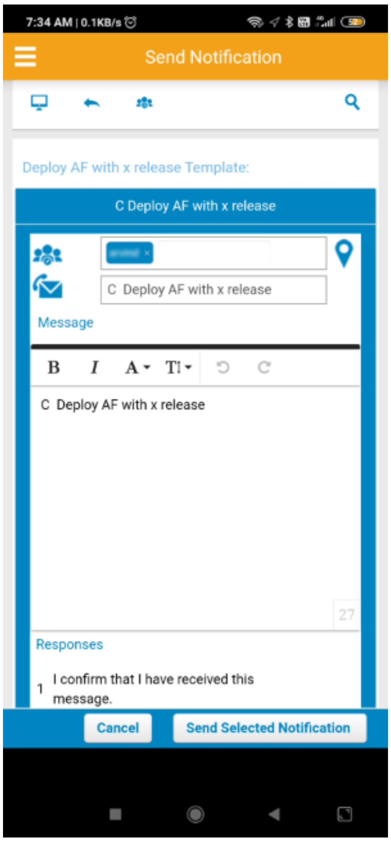
1 I confirm that I have received this message.

Compose notification

2. Enter the teams in **To** field. Alternatively, you can click 📍, then on the google map click ⬠ and draw a polygon on the map to select all the teams inside the polygon.
3. Enter the **Subject** for the notification.
4. Compose customized notification in the **Message** editor. Click **Send Selected Notification**.

### Using Template

1. Click on the required template tile. *<template name>* editor is displayed. The **Teams** are pre-defined in **To** field. The subject is pre-populated too.



Deploy AF with x release Template:

C Deploy AF with x release

C Deploy AF with x release

Message

C Deploy AF with x release

Responses

1 I confirm that I have received this message.

Template notification

2. Edit the message using the editor, if required.
3. Click **Send Selected Notification** to send or **Cancel** to abort.

## Sending a Notification

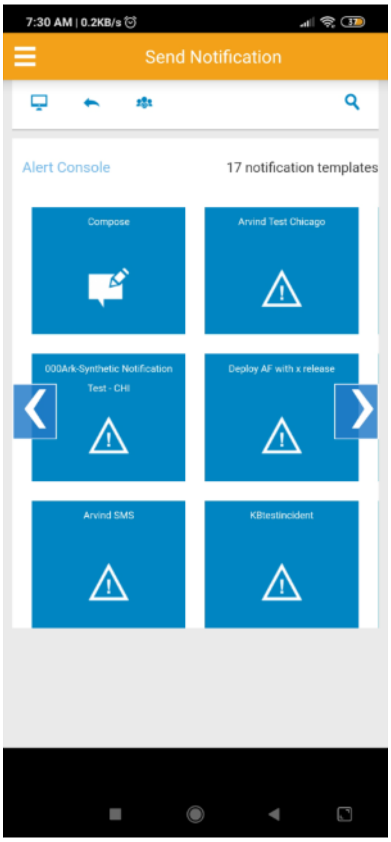
Send Notification is a screen which is used to send and track notification. It is available for administrator only. It has three sections:

- Alert Console
- Responses
- Teams

To send a notification from the AlertFind Mobile application do the following:

Click ☰ from the top left corner of any screen to view the **Send Notification** screen.

The Send Notification screen opens with **Alert Console** as default view. Here you can choose from the available notification templates to send notification. You can also choose to **Compose** your own notification message.



Send Notification - Alert Console view

A notification template must first be created in the AlertFind web application. This incident template should contain the desired notification task.

You cannot create notification templates on mobile app. It must be created on web and then used on Mobile app.

After the incident template is created, it can be opened in the AlertFind Mobile application and the incorporated notification is sent.

## Responding to notifications

When new AlertFind notifications are received your device notifications shows them (if you have not disabled notifications). You can directly click on these notifications to view them or you can see the notification by Logging into the AlertFind Mobile app and visiting the Notifications screen.

The unread notifications appear with a bold text and color icon.

To respond to a notification, do the following:

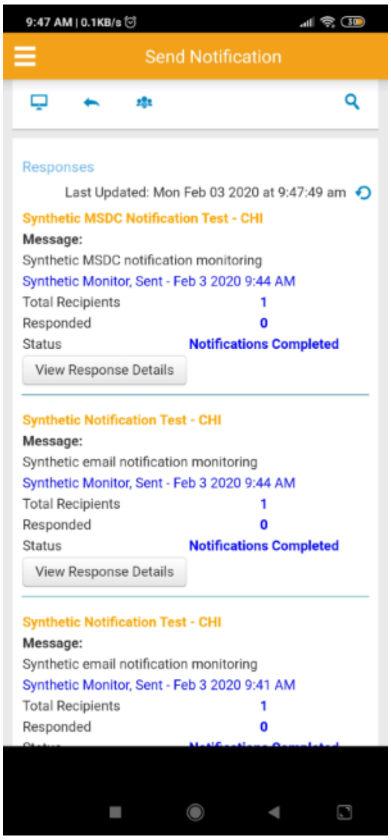
1. Select the notification. The notification detail screen is displayed.
2. Select the response option and click **Submit**. A confirmation message is displayed.

If you navigate back to the notification inbox, you can see that the text of the responded notification and notification icon appears in gray.

## Responses

From Responses you can check whether the notification sent was successful or not. You can also check the number of people who received the notification and the ones who responded to it.

To view **Responses**, go to **Send Notification** page and click ↩.



Responses

Last Updated: Mon Feb 03 2020 at 9:47:49 am

Synthetic MSDC Notification Test - CHI
**Message:**
Synthetic MSDC notification monitoring
Synthetic Monitor, Sent - Feb 3 2020 9:44 AM

| | |
|---|---|
| Total Recipients | 1 |
| Responded | 0 |
| Status | Notifications Completed |

View Response Details

Synthetic Notification Test - CHI
**Message:**
Synthetic email notification monitoring
Synthetic Monitor, Sent - Feb 3 2020 9:44 AM

| | |
|---|---|
| Total Recipients | 1 |
| Responded | 0 |
| Status | Notifications Completed |

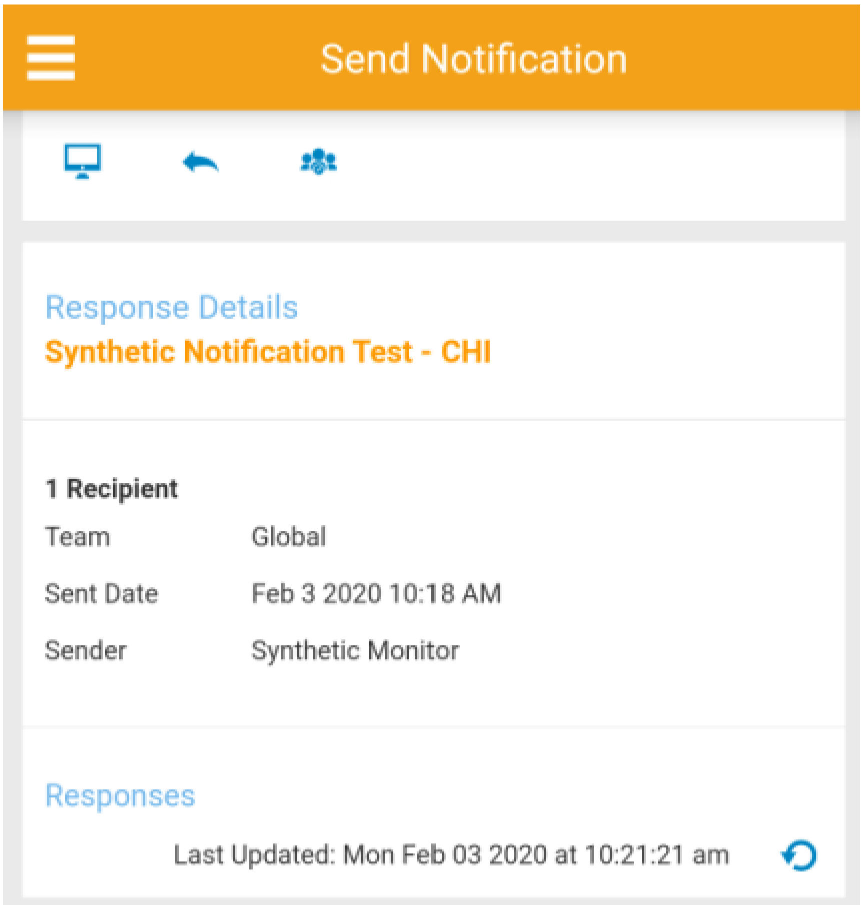
View Response Details

Synthetic Notification Test - CHI
**Message:**
Synthetic email notification monitoring
Synthetic Monitor, Sent - Feb 3 2020 9:41 AM

| | |
|---|---|
| Total Recipients | 1 |
| Responded | 0 |

Notification Responses

On the **Reponses** section, you can view the list of responses for a notification. You can click View Response Details to view the details of any response.


Send Notification

Response Details

Synthetic Notification Test - CHI

1 Recipient

| | |
|---|---|
| Team | Global |
| Sent Date | Feb 3 2020 10:18 AM |
| Sender | Synthetic Monitor |

Responses

Last Updated: Mon Feb 03 2020 at 10:21:21 am

Response Details View.

## Delete Notifications

To delete notifications, do any of the following:

- From the notification details screen, click the 🗑 to send it to **Trash**.
- In the notification inbox, swipe right on a notification from the list. This sends the notification to **Trash**.

Deleted notifications from the AlertFind mobile app goes to **Trash**.

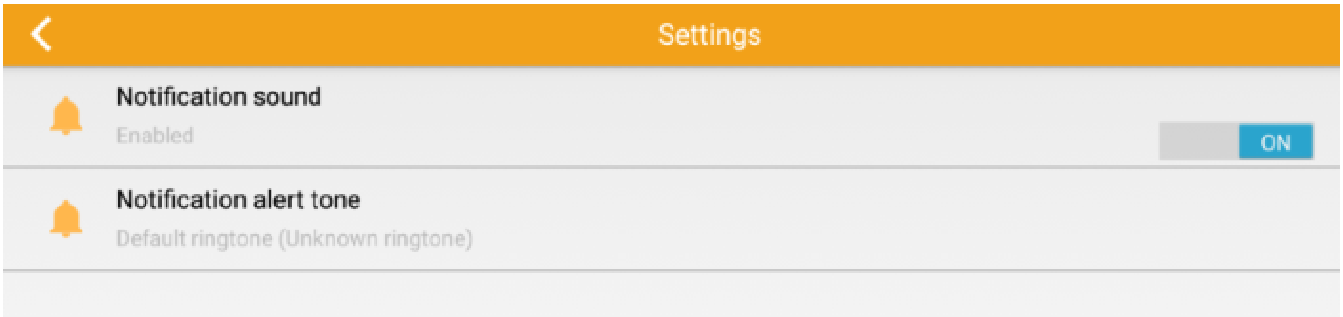
To permanently delete notifications, do the following:

1. Click ☰ and select **Trash**.
2. Select the check boxes next to the notification you want to delete permanently.
3. Click 🗑.
4. Click **Ok** on confirmation message.

## Settings

To access **Settings** screens:

1. Click ☰ from the top left corner of any screen.



Settings

Notification sound
Enabled
ON

Notification alert tone
Default ringtone (Unknown ringtone)

2. You can perform the following settings:

- Switch ON/OFF **Notification sound**
- Set your own **Notification alert tone**

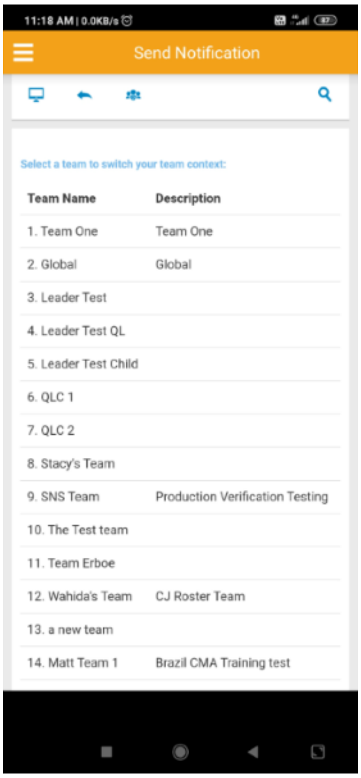
## Teams

Teams form the group of users to whom notification(s) are sent.

You can create teams on Web and use it on mobile app. Teams cannot be created directly from mobile app.

To view teams screen, do the following:

1. Click ☰ and select **Send Notification** from the menu items.
2. Click 👥 to view the teams screen. You can select the required team from the **Team Name** column.



Select a team to switch your team context:

| Team Name | Description |
|---|---|
| 1. Team One | Team One |
| 2. Global | Global |
| 3. Leader Test | |
| 4. Leader Test QL | |
| 5. Leader Test Child | |
| 6. QLC 1 | |
| 7. QLC 2 | |
| 8. Stacy's Team | |
| 9. SNS Team | Production Verification Testing |
| 10. The Test team | |
| 11. Team Erboe | |
| 12. Wahida's Team | CJ Roster Team |
| 13. a new team | |
| 14. Matt Team 1 | Brazil CMA Training test |

Select your team from the list

## Send Problem Report

If you encounter any problem while working with the AlertFind Mobile app, you can always report it to support from within the app.

To report a problem:

1. Click ☰ from the top left corner.
2. Select **Send Problem Report** from the list displayed,
3. Explain your problem and add a relevant screen shot, if required.
4. Click **Send**.

# Supported Mobile Operating Systems and Devices

## Mobile Operating Systems

AlertFind is engineered to work on tablets and smart phones and can be accessed by the standard (XHTML compliant) browsers on those devices. For a list of browsers tested with AlertFind, refer to Supported Browsers. However, versions of Chrome older than 15 are not supported on mobile devices.

AlertFind is tested and verified to function on devices that use the following operating systems:

- **Apple iOS (6+)** - Tested on iPhone 5 and above, and iPad 2 and above
- **Android OS (4+)** - Due to the wide variety of mobile devices that run the Android operating system, we cannot certify that AlertFind will run optimally on every device. Tested on Samsung Galaxy SIII, Nexus 7, Nexus 5.

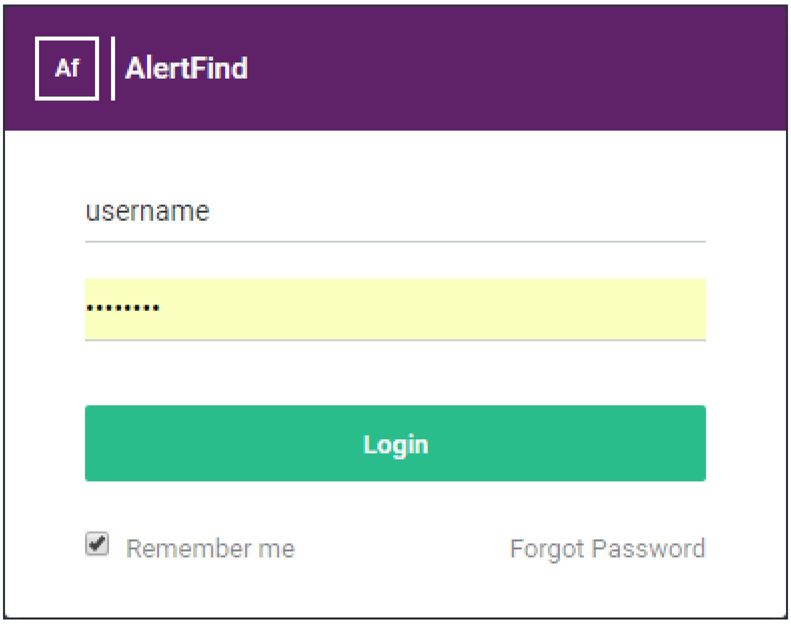
## Supported Standard Devices

AlertFind supports the following standard devices:

- Cell phone
- Fax
- Home phone
- Pager
- Personal email
- Smart phone
- Tablet
- SMS phone
- Work email
- Work phone
- Work smart phone
- Work tablet

# Logging In

We recommend to use the supported browsers to connect to AlertFind interface. Supported Browsers



AlertFind login screen

To log into AlertFind:

1. From a supported web browser, enter the web address provided by Support. The **Sign In** page appears.
2. Type the user name (usually primary work email address). If you do not know what your AlertFind user name is, contact the AlertFind administrator.
3. Type the password.

   If you have forgotten your password, click **Forgot your password?**. AlertFind sends a new password to the primary email address for the AlertFind account.
4. Click **Sign In**.

**NOTE**

AlertFind automatically logs you out after 10 minutes of inactivity.

# Adjusting the Text Size

The size of text displayed in the AlertFind desktop Web interface can be adjusted using most web browsers’ text size or zoom tools under the **View** menu.

# View the Help

To view online help, click **Help** at the top of the page. Administrators see the *Administrator Guide Help*; team leaders see the *Team Leader Guide Help*; users see the *User Guide Help*. The help launches in a new web browser tab or window.

# Using the Web Desktop Interface

To navigate through AlertFind, use the navigation button at the top of the page and the menu on the left side of the page.

**Team Security Context** is the team you are currently accessing within AlertFind. The Global Team is the root team. For more information on this feature, see Team Security Context.

The menu includes the following options and sub-choices:

| Option | Choices |
|---|---|
| **Launch Center** | • Alert Console<br>• Compose a Notification (Advanced) |
| **Notifications** | • Sent Notifications<br>• Scheduled Notifications<br>• Archived Notifications |
| **Incidents** | • Incidents<br>• Archived Incidents |
| **Notification Templates** | Manage Library |
| **Hotlines** | • Hotlines<br>• Archive Hotlines |
| **Groups** | • Broadcast Groups<br>• Escalation Groups<br>• Smart Groups |
| **Reporting** | • Devices Report |
| **Administration** | • Teams<br>• Users<br>• My Account: Settings for your personal account<br>• Application Status |

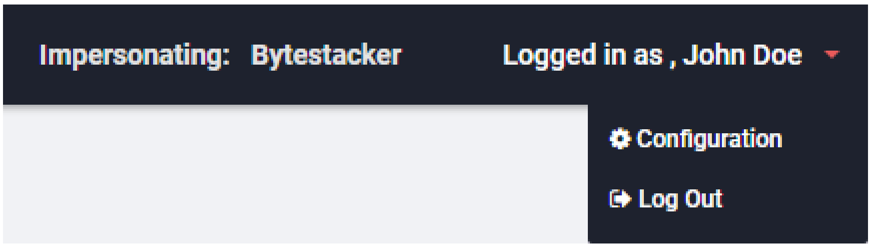
# Multiple Language Support

AlertFind’s optional language packs allows notifications to be sent in the languages purchased. Each Hotline and Hotline Pro phone number is associated with a voice, which determines the language that Hotline uses. For example, one Hotline phone number may be assigned to Serena, who speaks English for the United Kingdom, and another number assigned to Mary, who speaks English for the United States.

For more information about language packs, contact an AlertFind account representative.

# Logging Out

To log out of AlertFind, click **Logout** at the top of the page.



Logout option in the UI

# Chapter 2: Managing Users

Before you send alerts to the users of AlertFind, you must first create users, optionally teams, groups and sites.

Users can be either imported or created manually, and typically belong to a team, group or a site.

Topics in this section:

# Groups vs. Teams vs. Sites

Groups, Teams, and Sites are different, yet interrelated.

A **Group** is a collection of users, or a combination of users and groups, to whom notifications can be sent.

Groups are the lowest level gathering of users.

Groups can be created:

- Manually:
  - **Broadcast Groups** are groups of individuals or groups to which a notification is broadcast simultaneously.
  - **Escalation Groups** differ in that notifications are sent to members of the group in a specified order.
  - **Smart Groups** are dynamic groups of users, based on criteria selected when the group is defined.
- Or automatically:
  - **Ad Hoc Groups** can be automatically created when composing a notification. Its membership is composed of users who meet the selected criteria.

Example uses of Groups include:

- Regional or branch office personnel
- Information technology staff
- Executives
- Business continuity or disaster recovery unit
- Virus response group
- All employees in Building 4

Groups are interrelated with Teams and Sites in that:

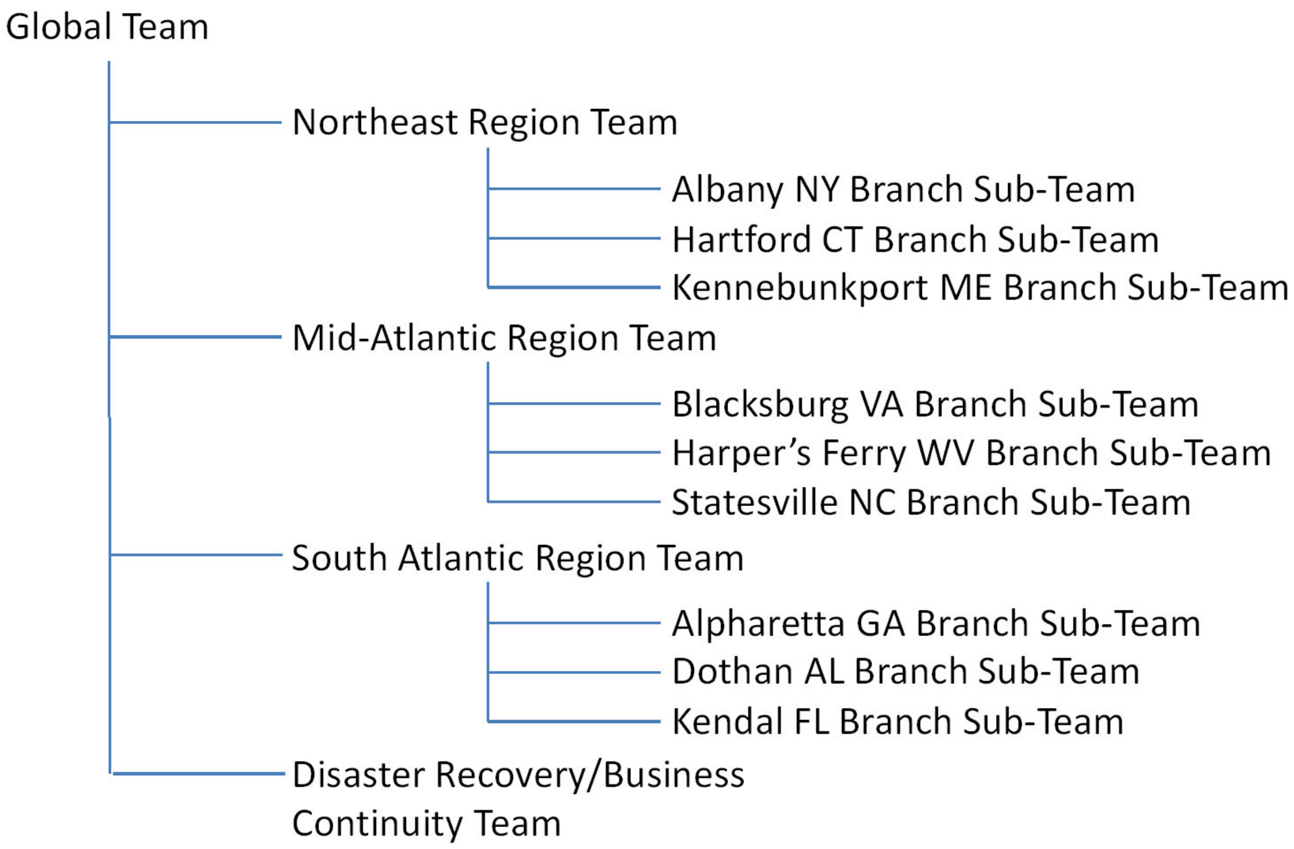
- Groups cannot contain either Teams or Sites, but Groups can be associated with both Teams and Sites.
- Groups themselves do not have an inherent geographic component. However, a Site can contain Groups of users who have been selected because they share the same geographic location.
- Groups have no inherent hierarchy. However, within a team security context, the membership of a Group is restricted by the team’s membership scope.

For more information about Groups, see Groups.

**Teams** are hierarchical structures with extensive permission settings, which allow administrators to tightly control the actions team leaders can perform and the information they can view. For example, one team leader might be granted permission to send notifications and another team leader permission to manage public data for team members.

Teams are created only manually.

Example uses of Teams include:


Global Team
Northeast Region Team
Albany NY Branch Sub-Team
Hartford CT Branch Sub-Team
Kennebunkport ME Branch Sub-Team
Mid-Atlantic Region Team
Blacksburg VA Branch Sub-Team
Harper’s Ferry WV Branch Sub-Team
Statesville NC Branch Sub-Team
South Atlantic Region Team
Alpharetta GA Branch Sub-Team
Dothan AL Branch Sub-Team
Kendal FL Branch Sub-Team
Disaster Recovery/Business Continuity Team

Teams are interrelated with Groups and Sites in that:

- A Team contains users and Groups who are within membership scope of the parent Team.
- Teams can create Groups, and those groups are available only to that Team and its sub-teams.
- Teams can create Sites, and those Sites are available only to that Team and its sub-teams, unless the Site is explicitly shared with all teams.
- Teams cannot be selected as recipients of notifications, whereas Groups and Sites can be selected. However, within a team context, if a Group or Site is selected as the recipient of a notification, only members of the Team will be included in the recipient list, all other users will be ignored.

For more information, see Teams and Permissions.

**Sites** are geographic-based assets, such as `Main Campus`, `Building 7`, or `Oil Rig 1`. Groups of users can then be associated with each of these Sites. When a geographic area is selected for a Notification in the *Map Selector* tab, all the Sites located within the geographic area selected will be included in the Notification's recipients.

Sites are only created manually.

Example uses of Sites include:

- `Building 1`, which contains the Sales and Marketing Groups.
- `Main Campus`, which contains all the Groups in the `Building 1` site, plus all the other Groups in that location.
- `Oil Rig 1`, which contains all the users of `Oil Rig 1` Group, which is a Smart Group based on the `Location` custom field.

Sites are interrelated with Groups and Teams in that:

- Sites can contain Groups, but not Teams.
- A Site can contain Groups of users who share the same geographic location, such as the Sales and Marketing Groups who both reside in the same building, but individual Groups do not have a geographic component.
- Within a team security context, the membership of a Site is restricted by the team's membership scope.
- Sites created by a Team have the option to be shared by all teams.

For more information, see Sites.

# Users

A team leader can manage information about users on teams. The information that can be managed depends on how AlertFind is provisioned, team leader permissions, and currently active team context.

This section contains the following information:

## Viewing User Lists

User lists can be viewed in several different ways, each described below.

- Viewing All Users
- Viewing All Users in the Current Team Context
- Viewing a List of Team Leaders by Team
- Viewing a List of Users by Team
- Viewing a List of Users by Group

See Filtering Lists for information on filtering tools available to all roster lists.

### Viewing All Users

Administrators, and Global team's Team Leaders, can view all AlertFind users by selecting the `Global` team context and selecting the **Users** menu.

To view a list of users:

1. Verify the team context is set for the `Global` team. For more information, see Team Security Context.
2. From the left navigation menu, **Administration** section, click **Users**. The **Users** page appears containing the list all the users on the system.

The users displayed in this list can be filtered by following the instructions under Filtering Lists.

### Viewing All Users in the Current Team Context

Administrators and Team Leaders of the current team context can view members of the current team from the **Users** menu item.

To view a list of users in the current team context:

1. Verify the correct team context. For more information, see Team Security Context.
2. From the left navigation menu **Administration** section, click **Users**. The **Users** page appears containing all the users for the current team.

The users displayed in this list can be filtered by following the instructions under Filtering Lists.

### Viewing a List of Team Leaders by Team

Team Leaders with appropriate team permissions and Administrators can view the list of each team's leaders from the **My Teams** page.

To view a list of team leaders by team:

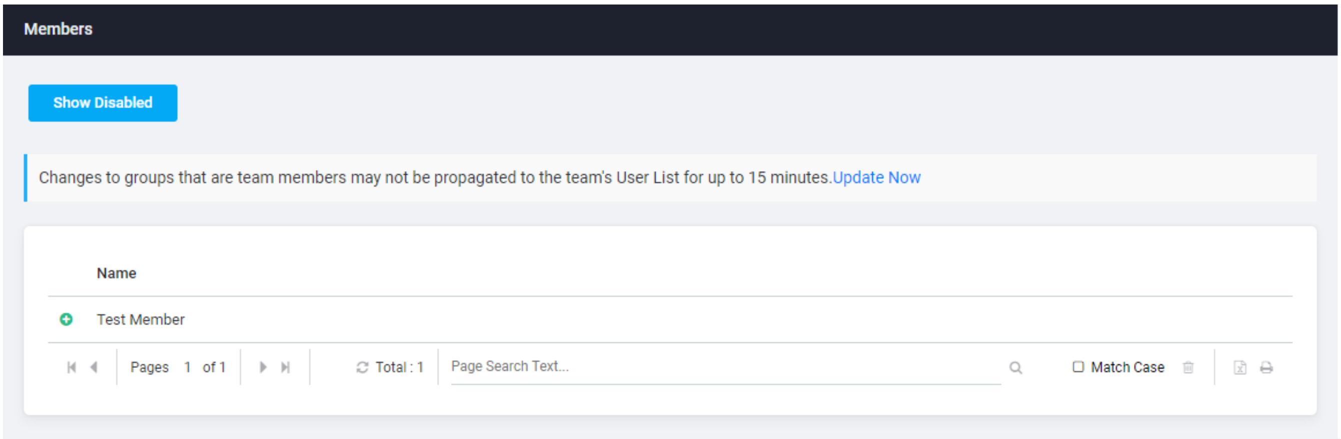
1. Verify the correct team context. For more information, see Team Security Context.
2. From the left navigation menu **Administration** section, click **Teams**. The list of teams appears.
3. Click the plus sign ⊕ next to a team to expand its team leader list with each team leader's permissions. Alternatively, click the name of a team to view the full **Team Information** page. Team leaders are listed in the **Leaders** section.
4. Click the team leader's name to view the **User Overview** page.

## Viewing a List of Users by Team

Team Leaders with appropriate team permissions and Administrators can view a list of each team's users from the **My Teams** page.

### NOTE

Since the Global team contains all members, a list of members is not available on the Global Team details page. The Members section states: **The global team contains all users and global groups.** See section Viewing All Users for a list of all users of the Global team.



Changes to groups that are team members may not be propagated to the team's User List for up to 15 minutes.Update Now

| | Name |
|---|---|
| ⊕ | Test Member |

List of Member of a team

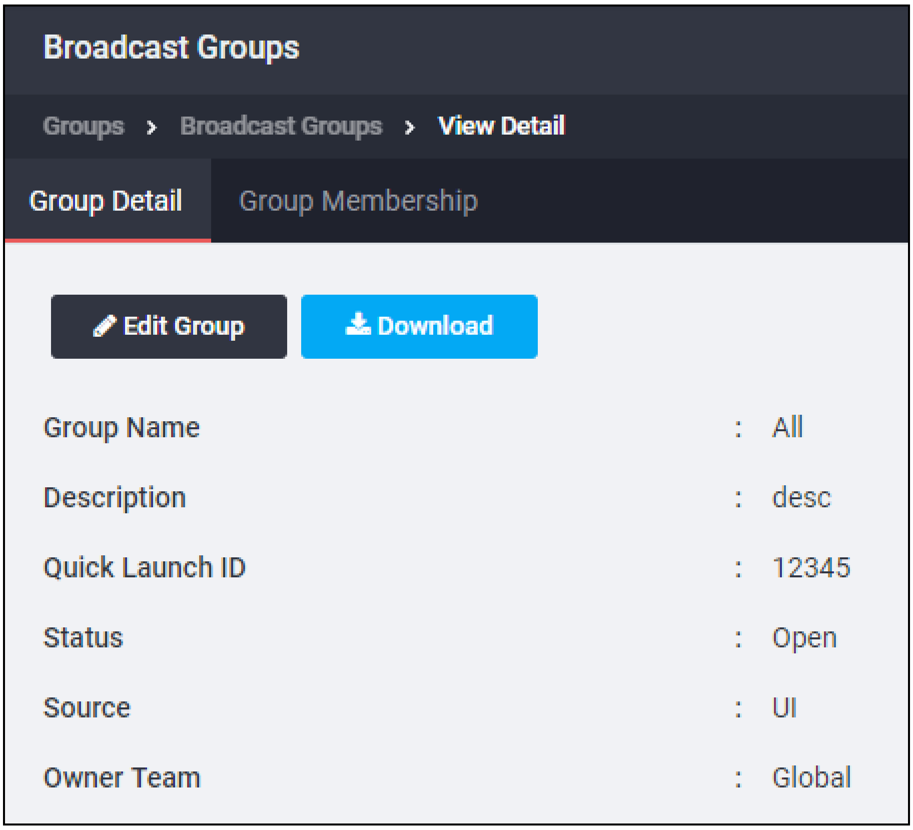
To view a list of users by team:

1. From the left navigation menu, **Administration** section, click **Teams**. The list of teams appears.
2. Click on the name of the desired team.
3. This list defaults to showing the first ten team members. To view more, select another page using the arrows besides the page number.
4. Click **View Details** to see the page overview. Alternatively, you can click the plus sign ⊕ next to a team member's name to view that member's current escalation devices. Scroll to the **Members** section to see the list of team members.

### Viewing a List of Users by Group

To view a list of users for a specific group:

1. Verify the correct team context. For more information, see Team Security Context.
2. From the **Groups** list in the left-navigation menu, click **Broadcast Groups**, **Escalation Groups**, or **Smart Groups**. A list of groups appears.
3. View the group details by either double-clicking the name of the group or selecting the group and clicking **View Details**.



| | | |
|---|---|---|
| Group Name | : | All |
| Description | : | desc |
| Quick Launch ID | : | 12345 |
| Status | : | Open |
| Source | : | UI |
| Owner Team | : | Global |

4. To view the list of group members, click the **Group Membership** tab.
5. Double-click a user or select the user and click **View Details** to view a the user’s details. This list cannot be filtered.

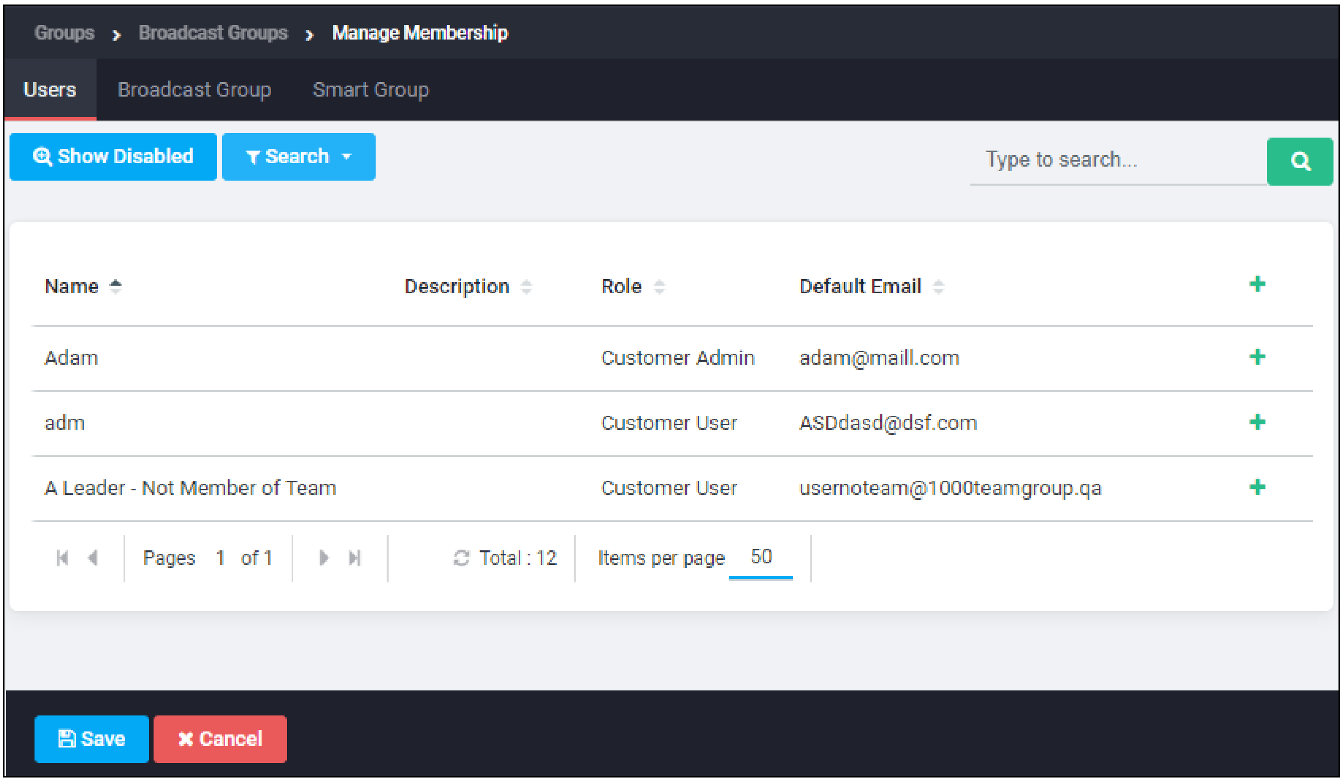
## Filtering Lists

Many user and group lists allow filtering to aid in finding a specific user or group, or sets of users or groups.

To access a filtering list navigate to **Groups > Broadcast Groups**.

Select a group and click **View Details**.

On the Group Membership tab click **Manage Membership**.



| Name | Description | Role | Default Email | + |
|---|---|---|---|---|
| Adam | | Customer Admin | adam@maill.com | + |
| adm | | Customer User | ASDdasd@dsf.com | + |
| A Leader - Not Member of Team | | Customer User | usernoteam@1000teamgroup.qa | + |

Pages 1 of 1 Total : 12 Items per page 50

To filter controls for lists

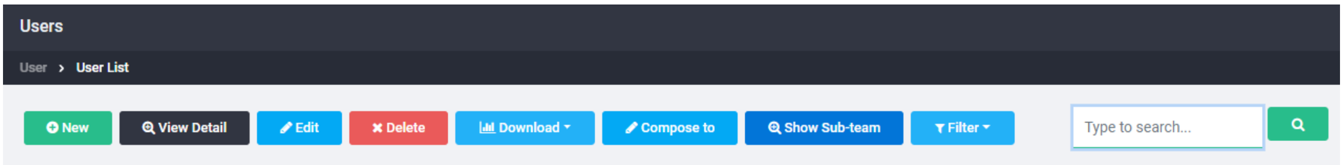
- **Alphabet Control**: Click the first letter of the user's or group's name to jump to a list of users or groups that begin with that letter.
- **Page Controls**: Use the **First** and **Previous**, **Next** and **Last** buttons as necessary to locate the page containing the user or group.
- **View Details**: Brings up the pane showing details of the user or group selected.
- **Edit**: Brings up the pane to edit the user or group selected.
- **Delete**: Deletes the currently selected user or group. A confirmation box will appear to verify the deletion.
- **Download**: Downloads a user or group report(s) based on the context.
- **Compose To**: Brings up the **Notification Editor** pane, to compose a notification to the user(s) or group(s) selected.

- **Show sub-team**: Toggle the **Show sub-team** button to show or hide sub-team like a branch or a particular region.
- **Filter**. Click **Filter** to create a new filter criteria or to delete an existing filter.

### Running a simple search

Enter the first few letters of the name into the **Search** box, and then click **Search** 🔍.

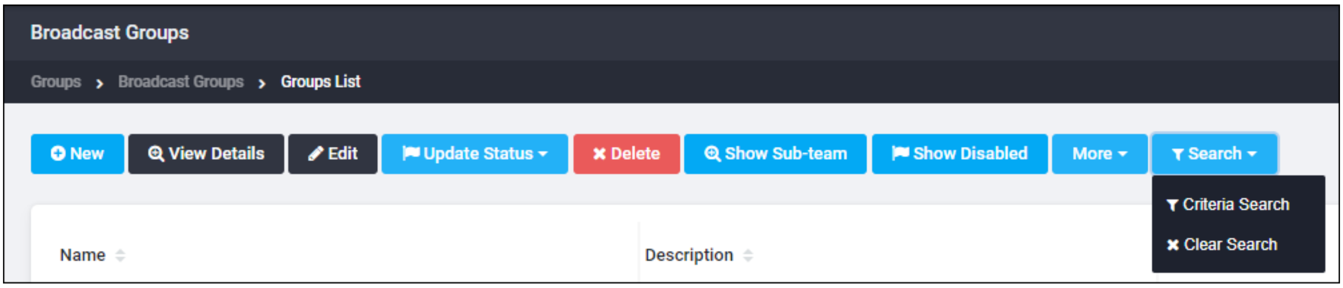
The list of items that fit the search criteria will be displayed.



### Using the Criteria Editor

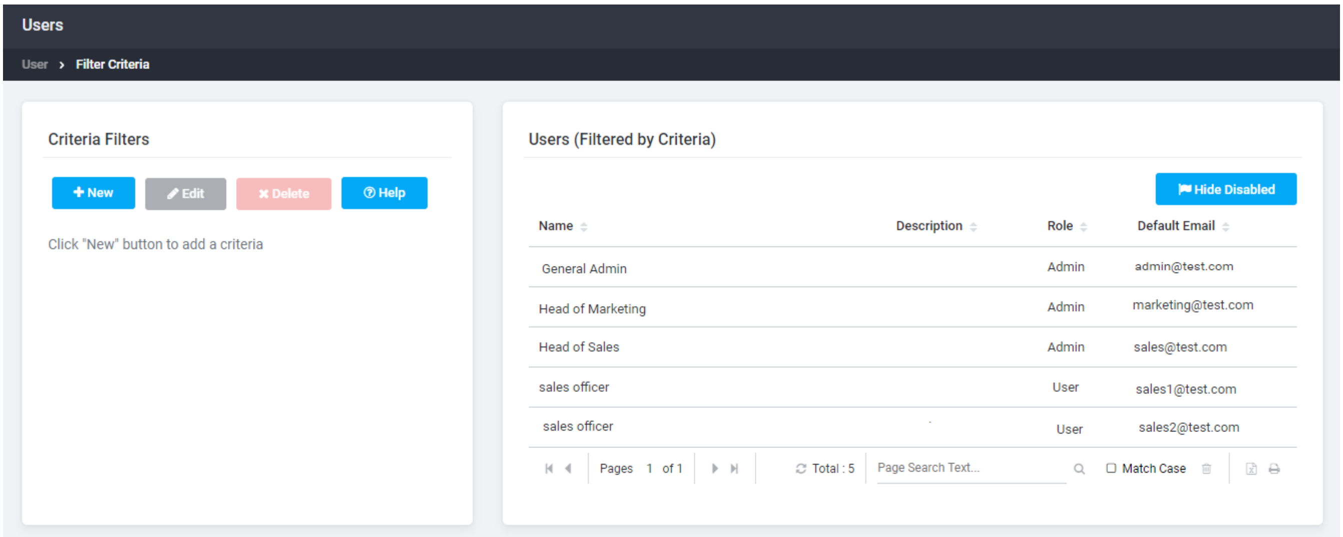
The Criteria Editor can be accessed through several mechanisms:

- From most user or group pages, click the **Search** button, then select **Criteria Search** from the list.



- On the reports pages, the button label will depend on the context, for instance: **Edit Criteria**, **Group Filter Options**, **Incident Filter Options**, or **Notification Criteria**.

The **Criteria Editor** appears. The left pane displays any filters being applied, and the matching items are displayed in the right pane. By default, no criteria filters are applied when you first view the Criteria Editor; therefore, all users, groups, incidents, etc. are displayed in the right-hand pane.



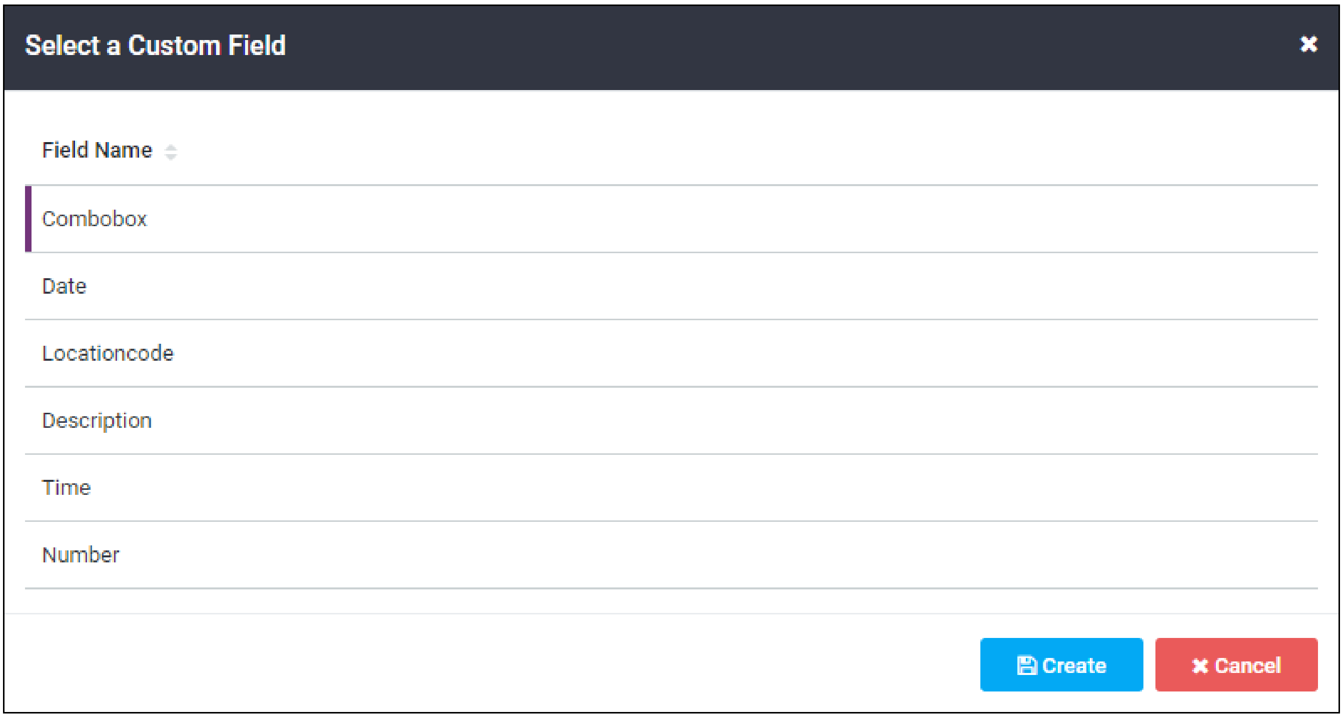
Click "New" button to add a criteria

Users (Filtered by Criteria)

| Name | Description | Role | Default Email |
|---|---|---|---|
| General Admin | | Admin | admin@test.com |
| Head of Marketing | | Admin | marketing@test.com |
| Head of Sales | | Admin | sales@test.com |
| sales officer | | User | sales1@test.com |
| sales officer | | User | sales2@test.com |

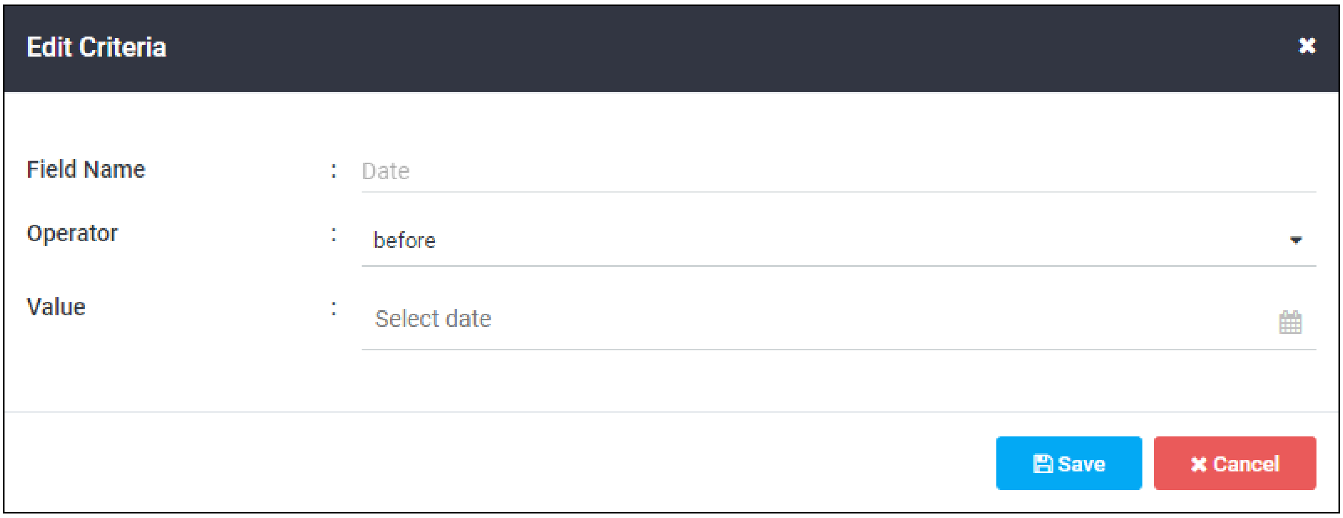
To create a new criteria filter:

1. Click **New**. The **Select a Custom Field** dialog box appears, with a list of all default fields and any custom fields defined for your organization.



| Field Name |
|---|
| Combobox |
| Date |
| Locationcode |
| Description |
| Time |
| Number |

2. Click on a field name to select it for the desired filter, and click **Create**.
3. In the **Edit Criteria** dialog box, click **Operator** drop-down to select the search criteria.



Edit Criteria

Field Name : Date

Operator : before

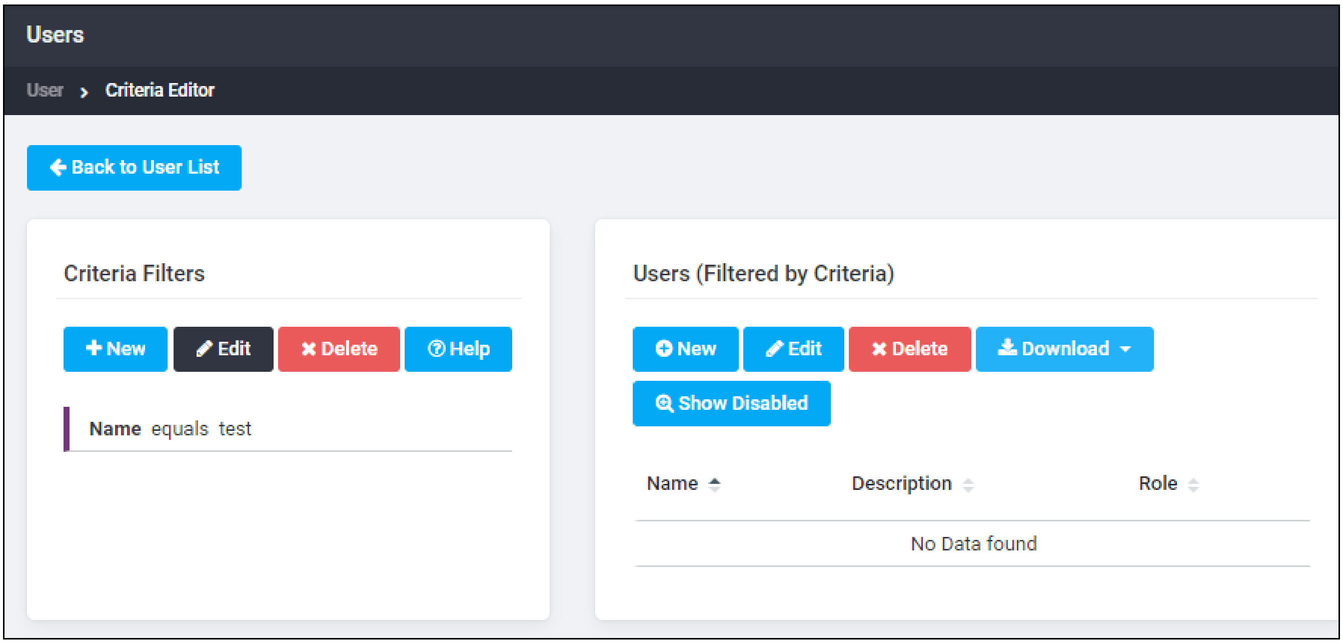
Value : Select date

The operators that can be used depend on the type of field selected. These include:

| Field type | Operator description |
|---|---|
| Text fields | `equals`, `starts with`, `contains`, `does not contain`, `ends with`, `does not equal` or `in list`<br>For most of these operators, only one text value may be entered.<br>The `equals` and `does not equal` operators are strictly matched and are case sensitive. For example, for `equals`, a criteria value of `John` will **not** match users named `john` or `John Smith`.<br>The `starts with`, `contains`, `does not contain`, and `ends with` are not case sensitive or strictly matched.<br>The `in list` operator has special considerations:<br>• `in list` items are delimited by commas. Trailing and leading spaces are ignored.<br>• There is no limit to the number of items in a list for Search Criteria.<br>• Maximum limit of 1024 characters is applicable for **Smart Groups**. The limit includes pre and post single quotes appended for each list item.<br>• All search items are strictly matched and case sensitive. For example: `Name` with an `in list` value of: `Ann Marie, Amy, Ang` will **not** match users `Ann`, `Annie`, `amy`, or `Angela Jane`. |
| Numeric fields | `equals`, `greater than`, `less than`, or `does not equal`.<br>Only the characters 0-9 are allowed to be entered into the |

| Field type | Operator description |
|---|---|
| | Value field. |
| Date fields | on, after, or before<br>For date fields, the Value entry box will change to Date and Time selection fields. |

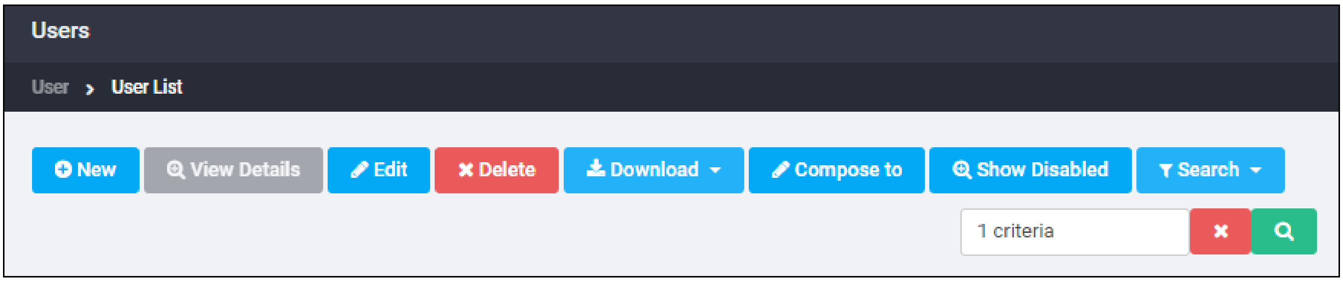
4. After the Operator is selected, enter the criteria value into the **Value** field.
5. Click the **Save** button to return to the Criteria Editor, which lists the search criteria in the left section, and everything that meets the criteria in the right section.



Name equals test

| Name | Description | Role |
|---|---|---|
| No Data found | | |

6. Click **Save** to save these criteria and return to the previous screen.
7. If the Criteria Editor was accessed from the search drop-down, the search text box contains the number of criteria applied.



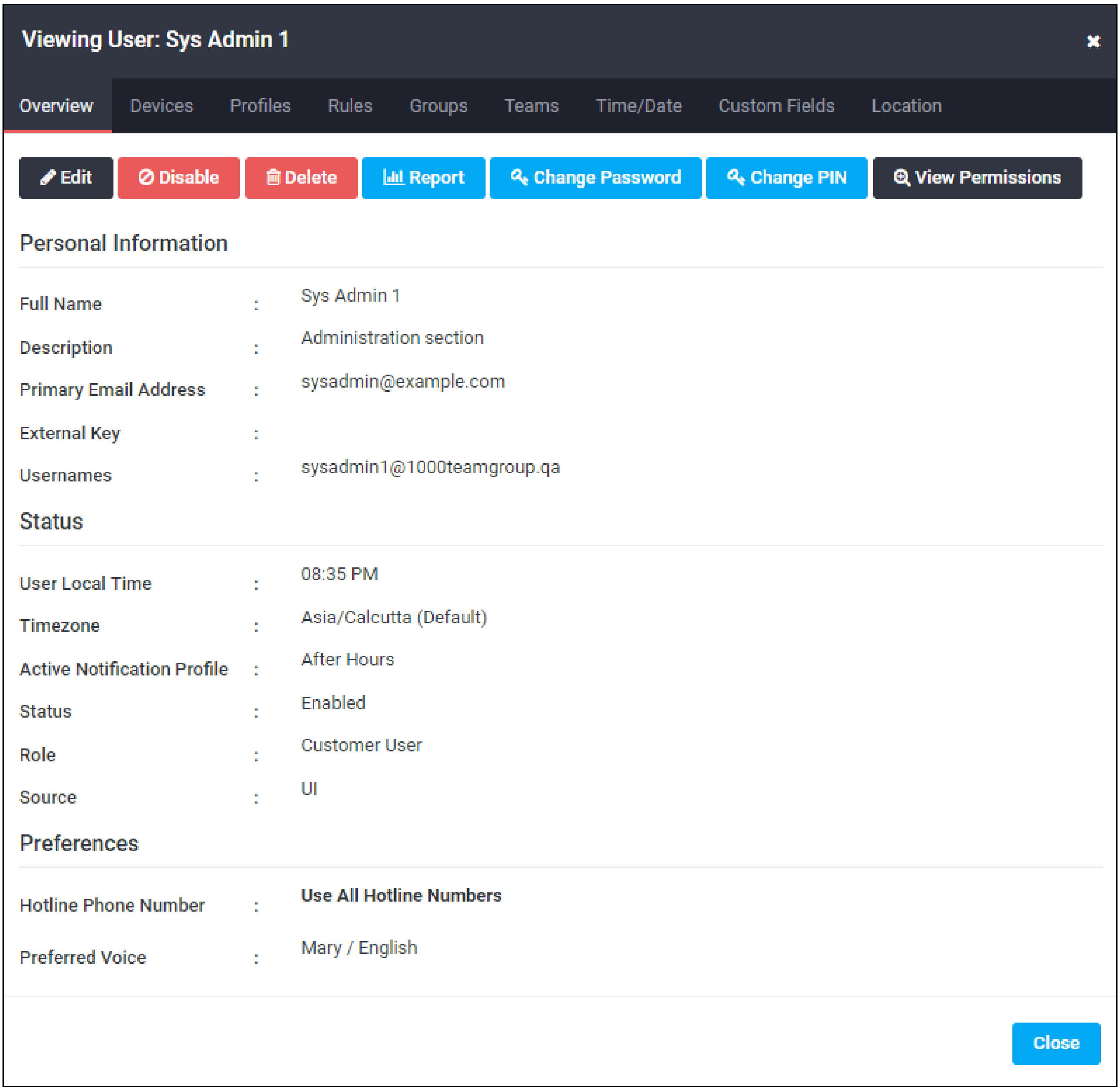
1 criteria

8. To remove the search criteria, click the red **X**.

## Viewing Individual User Details

From any list of users, double-click a user name to bring up the **User Overview** page. See Viewing User Lists for instructions on viewing user lists.

Select the user name and click **View Details**, or double-click the user's name, to display the **User Editor** window.



Viewing User: Sys Admin 1

Personal Information

Full Name : Sys Admin 1
Description : Administration section
Primary Email Address : sysadmin@example.com
External Key :
Usernames : sysadmin1@1000teamgroup.qa

Status

User Local Time : 08:35 PM
Timezone : Asia/Calcutta (Default)
Active Notification Profile : After Hours
Status : Enabled
Role : Customer User
Source : UI

Preferences

Hotline Phone Number : **Use All Hotline Numbers**
Preferred Voice : Mary / English

The **User Editor** window contains the following sections:

- **User Overview** – Lists basic user information, such as user names, email addresses, and basic personal information. Some of these information is set by default by an administrator using the **Settings** page. Other information can be set per user by an administrator or team leader by editing the user account. See Editing User Details.

- **Notification Devices** – Lists the devices available for this user. The *standard* device list is provisioned by Support, but *custom* devices can be configured, disabled, enabled, or deleted for an individual user by an administrator, team leader, or user with the necessary permissions. Users can usually edit this information for their own user accounts. See Managing User Devices.
- **Notification Profiles** – Includes definitions of what devices are used to deliver notifications to a user according to the time of the day, day of the week, or holiday period when a notification is sent. See Customizing a Notification Profile.
- **Notification Rules** – Includes definitions of special time-periods (such as Business Hours, Weekends, After Hours, or Holidays) and the notification profiles to be used when delivering notifications during those time-periods. See Customizing Notification Profiles and Rules.
- **Group Membership** – Lists groups of which the user is a member.
- **Team Membership** – Lists teams of which the user is a member.
- **Time and Date Preferences** – Lists the user’s time zone, business hours, and weekend days. See Changing a User’s Time Zone, Business Days, and Work Hours.
- **Custom Fields** – If any custom fields were imported for this user, they are listed in this section. Contact your AlertFind administrator if you want to use custom fields.
- **Location Preference** – This field is displayed only if **Allow map based notifications** has been selected in the **Default Company Settings** table. It displays a map that allows the administrator or teamleader to view, enter, or edit a user's location. See Enter or Change a User’s Location Preference.

## Managing Users

Administrators can manage users for their organization. AlertFind enables them to create and delete users, edit used details, and customize notification and rules.

Team leaders can manage users for their organization if an administrator or other team leader has granted the necessary user management permissions. Contact Support or your AlertFind administrator if you cannot access necessary user management functions.

See also:

## Editing User Details

A team leader can make changes to team members' accounts, depending on the team permissions for the current team context.

### NOTE

Depending on company settings, administrators and team leaders may not be able to change all fields discussed in this section. If you cannot access a field but need to edit it, contact Support.

#### Editing Imported Data

Even if you import user data into AlertFind, you can change it using the AlertFind web interface. However, changes may be overwritten by the next import if the source data is not also updated. Also, imported user data cannot be changed using AlertFind Web Services / API interface.

### IMPORTANT

Changes made manually in the AlertFind interface to imported fields, groups, and teams are always overwritten with the next import unless that specific field is excluded in the next import.

- If changes are made to user information through the AlertFind interface, the best practice is to ensure that these changes are propagated back to the data source.
- Passwords are the only exception to this rule. When a password is edited or reset in the AlertFind interface, the link with the imported data source is broken. To reset this password in the future, use the **Change Password** button on the **User** page.

#### Changing User Permissions

When a user is granted any specific permission, that user becomes a team leader of the team in which the permissions are granted. See Permissions for information on permissions, teams, and team leaders.

#### Changing Basic User Information

Information in basic user fields can be set in a number of ways. It can be:

- Imported into the user account.
- Propagated into the user account from the company defaults set in your organization's company settings.
- Manually created or edited by an administrator with the necessary permissions.
- Manually edited by the user.

Administrators and Team Leaders with the necessary permissions can edit a user's basic information. See Permissions for additional information. Remember that if you manually edit this information and then these fields are reimported, any manual changes you make will be lost. See Editing Imported Data.

To manually edit a user's basic information:

1. From any list of users, double-click a user name to bring up the **User Overview** page. See Viewing User Lists for instructions on viewing user lists.
2. At the top of the **User Overview** page, click **Edit**. The **Personal Information**, **Status**, and **Preferences** sections appear.
3. Depending on your permissions, you may be able to edit the following fields:
    1. **Full Name** – Enter the user's full name as it should appear in the system. This field is required.

NOTE

Enter the user's name in the same naming convention as all the other users in your system, either `FirstName LastName` or `LastName, FirstName`. If you switch conventions between imported and manually entered users, it will be difficult for you to effectively sort user lists.

The name you enter here is the name AlertFind speaks in notifications. Therefore, if you use a `LastName, FirstName` convention, AlertFind speaks the user's name as “Smith, Joe.”

2. **Description** – Enter a description of this user. This field is optional.
3. **Primary Email Address** – Enter the *primary* email address for this user. This address is used for all password resets or reminders, even if other email addresses are added to the user's profile later. This field is required.
4. **Map Default Email To** – For the **Primary Email Address** entered, choose the type of address. Usually, it is the `Work Email` address.
5. Assign a User Name to the user. One user name is required, more user names can be assigned if needed. Typically, a user's user name is the same as the primary email address.
    1. Click the **Usernames** field name to bring up the **Username Editor**. Use the **Add**, **Edit**, or **Delete** buttons to perform user name actions.
    2. To add or edit a user name, first type in the portion of the user's email address that appears before the `@` symbol, such as `johnsmith` or `john_smith`. AlertFind user names cannot include spaces, but they can include most special characters, such as underscores (_) or exclamation marks (!).
    3. Then select the domain for this email address using the drop-down list. The domain is the part of the email address that appears after the `@` symbol, such as `companyname.com`.
    4. Click **OK** to submit the user name changes.

6. **Status** – Use the **Enabled** or **Disabled** options to change the user status.
7. **Hotline Phone Number** – Choose the **user to use all hotline phone numbers** available to your organization, or assign a specific number for this user by choosing from the drop-down list.

**NOTE**
The language used when a user calls into a Hotline is determined by the language associated with that Hotline phone number. To set another voice/language for a Hotline, assign a different Hotline phone number to the user.

8. Check **Display hotlines in preferred language only** to limit the hotlines displayed in this section to those in the user's preferred language. Uncheck this box to display all available hotlines for your organization.
9. **Preferred Voice** – Accept the default voice and language for your organization, or assign another for this user by choosing one of the options available in the list. The user's preferred voice determines which language is used for spoken and text-based notifications. By default, the user's preferred language and Hotline settings are propagated from the default values set in your organization's company settings. If you have the necessary permissions, you can change users' preferred language settings.
10. Click **Save** to save the changes.

**NOTE:**

Like other user account details, these settings can be overwritten by a future import process. See Editing Imported Data for additional details.

#### Changing a User's Time Zone, Business Days, and Work Hours

Business days and work hours determine which notification profile is used for a notification. By default, a user's business days and work hours are propagated from the default values set in your organization's company settings. Administrators and Team Leaders with the necessary permissions can edit a user's settings for these fields.

Like other user account details, these settings can be overwritten by a future import process. See Editing Imported Data for additional details.

To change business days or work hours for a user:

1. From any list of users, double-click a user name to bring up the **User Overview** page. See Viewing User Lists for instructions on viewing user lists.
2. Click **Time and Date Preferences** from the list of User Editor options. The **Time and Date Preferences** page appears.
3. Click **Edit**.
4. You can accept the default time zone for your organization or choose another time zone for the user's location from the **Time Zone** drop-down list. To reset

the time zone to the organization default, click the **Use Default** button next to the **Time Zone** field.

5. You can accept the default business hours for your organization or configure custom hours for the user. To configure custom hours, use the **Business Hours Start** and **Business Hours End** drop-down lists. To reset the user’s business hours to the organization default, click the **Use Default** button next to the **Business Hours Start** and **Business Hours End** drop-down lists.
6. You can accept the default weekend days for your organization or configure custom weekend days for the user. To configure weekend days, check each day that is a weekend day for the user. Unchecked days are considered business days, and checked days are considered weekend days. To reset the user’s weekend days to the organization default, click the **Use Default** button next to the **Weekend Days** check boxes.
7. Click **Save** to save your changes and return to the **User Overview** page.

### Changing a User’s Password

Users use their passwords to log into AlertFind to access notifications, incidents, or their user accounts. If you have the necessary permissions, you can change a user’s password.

To reset a user’s password:

1. From any list of users, double-click a user name to bring up the **User Overview** page. See Viewing User Lists for instructions on viewing user lists.
2. Click **Change Password** at the top of the **User Overview** page.
3. Enter the new password into the **New Password** and **Confirm Password** fields.
4. Click **Save** to save your changes and return to the **User Overview** page.

### Changing a User’s PIN

Users use their PINs to access information in notifications or on the Hotline that requires a PIN. If you have the necessary permissions, you can change a user’s PIN.

To reset a user’s PIN:

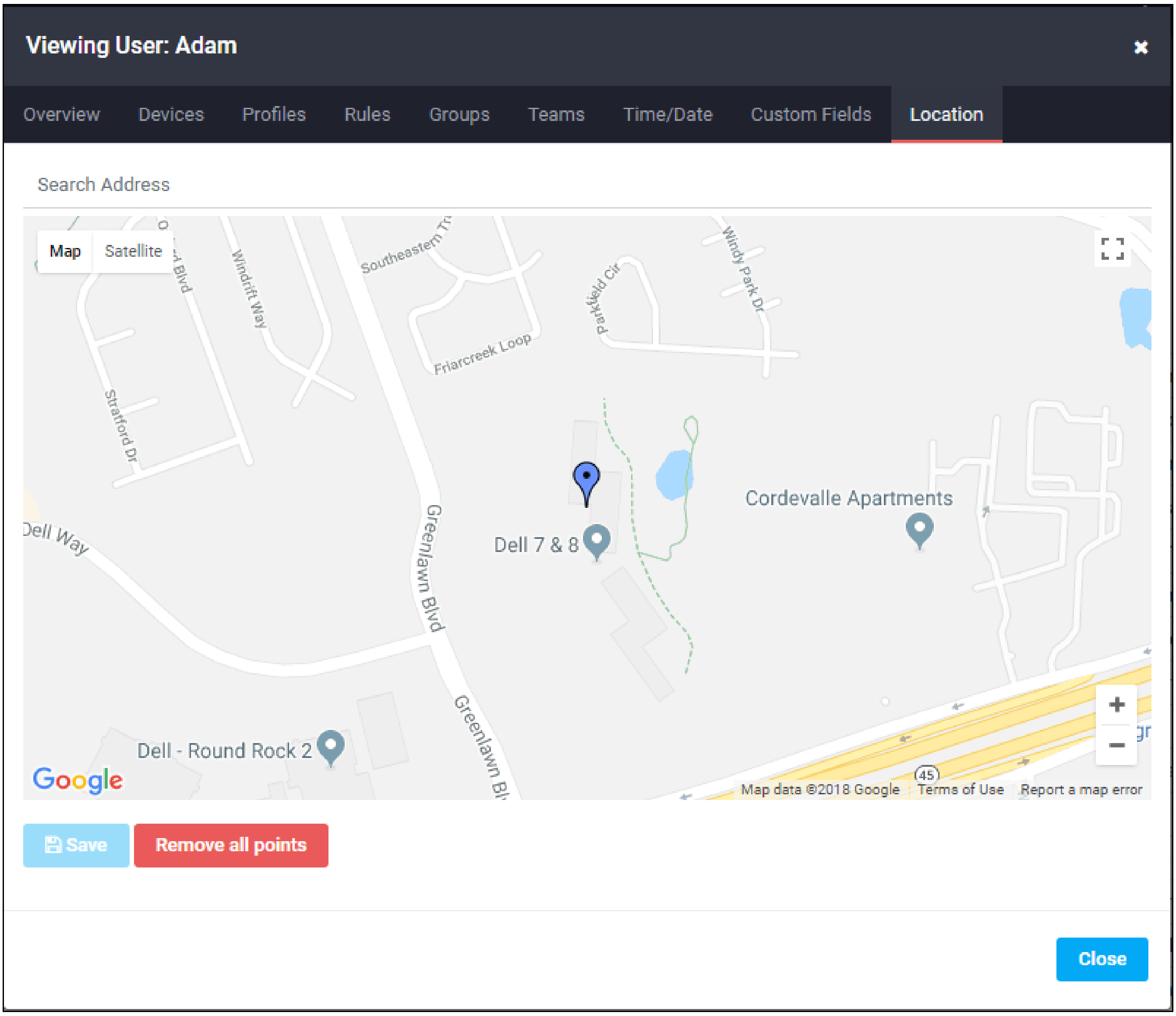
1. From any list of users, double-click a user name to bring up the **User Overview** page. See Viewing User Lists for instructions on viewing user lists.
2. Click **Change PIN** at the top of the **User Overview** page.
3. Enter the new password into the **New PIN** and **Confirm PIN** fields.
4. Click **Save** to save your changes and return to the **User Overview** page.

### Enter or Change a User’s Location Preference

If **Allow map based notifications** has been selected in the Default Company Settings table, you can map that user’s location in AlertFind.

To enter or change a user's location in AlertFind:

1. In the left-hand menu bar Administration section, select **Users**.
2. On the **Users** page, double click the user whose location you want to enter or edit.
3. In the **User Overview** window left-hand menu, select **Location Preference**. A map is displayed. If the browser requests you to share your location, answering *Yes* centers the map at your current location.
4. In the **Search Address** text box, enter the user's address. The location is indicated by an icon on the map. You can grab the location marker icon (click and hold) and move the icon to another location. For instance, if the user's location is unsearchable in Google maps, enter an address that is close to their location and then grab the icon and move it to the desired location. If you are changing locations, both the new icon and the old icon will be shown until you click Save, which will cause the old icon to disappear. Only one location can be active at a time.



5. Click **Save** to save the location or click **Remove all points** to clear all location markers.
6. Click **OK** to return to the **Users** page.

### Managing User Devices

Users can receive notifications on any device configured under the user's account. *Devices* include email accounts, telephones, fax machines, pagers, and SMS devices. Each device in a user's account must be *configured* with the necessary contact information (such as the phone number for a telephone device) before the device can receive notifications.

*Standard* devices are defined by Support when AlertFind is provisioned. Typically this standard list contains one or more email addresses and telephone numbers. Standard devices cannot be deleted from a user's account, but they can be disabled. Users with necessary permissions can create additional *custom* devices for individual users.

The types of standard devices that you may see in users' **Notification Devices** lists include:

1. **Phone Devices**–Phone devices can receive voice notifications. Configure phone devices using a telephone number, such as `555-555-1111`.
2. **Email Devices**–An email device can receive email notifications using an email address such as `user1@genericorp.com`. You can also send email notifications to some cell phone devices by configuring an email device that uses a cell phone email address, such as `5555551111@carrier.com`.
3. **SMS Devices**–SMS devices can receive short text notifications sent through an SMS gateway. Configure an SMS device using a telephone number, such as `555-555-1111`.
4. **Mobile Email Devices**–Mobile email devices can receive short email messages through an SMTP email gateway. These devices are different from regular email devices (such as BlackBerry or smart phone devices) in that they usually display a limited number of characters for each message and they cannot process graphics or attachments. In this way, messages sent to mobile email devices function similarly to those sent to SMS devices. Configure a mobile email device using a mobile email device email address, such as `5555551111@carrier.com`.
5. **Pager Devices**–Pager devices can receive short text notifications. Configure pager devices using a telephone number, such as `555-555-1111`.
6. **Fax Devices**–Fax devices can receive document-based notifications sent from one fax device to another. Configure a fax device using a telephone number, such as `555-555-1111`.

Information about each user's devices appears in the user's account in the **Notification Devices** section of the **User Overview** page. On this page, new devices can be added, enabled or disabled, and device information updated.

The status of each device in the list is indicated by the following text:

- Devices listed in all **black text** are configured and enabled, and are ready to receive notifications.

- Devices displaying **Not Configured** in red text cannot receive notifications until they are configured. See Configuring a Standard Device.
- Devices listed in **gray text** with the label **(disabled)** next to the device name are configured but disabled. These devices cannot receive notifications until they are enabled. See Enabling or Disabling Devices.

Administrators and Team Leaders with the necessary permissions can:

- Configure a standard device–See Configuring a Standard Device.
- Add a new custom device–See Adding a New Custom Device.
- Edit, enable, or disable a device–See Enabling or Disabling Devices.
- Delete a custom device–See Deleting or Unconfiguring a Device.

Like other user account details, manual device changes can be overwritten by a future import process. See Editing Imported Data for additional details.

### Configuring a Standard Device

When a standard device is defined by the default company settings but is not configured for a user, the name of the device appears in the **Notification Devices** list in red text and with a **Not Configured** label. For the device to receive notifications, the device must be configured.

To configure a standard device:

1. From any list of users, double-click a user name to bring up the **User Overview** page. See Viewing User Lists for instructions on viewing user lists.
2. Click **Notification Devices** from the list of User Editor options. The **Notification Devices** page appears.
3. Select the device to configure, then double-click it, or click the **Edit/Configure** button. Provide the necessary configuration information in the dialog box that appears.

| Option | Description |
|---|---|
| To add an **email address** or **WAP-enabled cell phone**: | 1. Type a valid **Email Address**. This field is required.<br>2. To add this device but disable it, click **Disable** at the top of the page. The device will be added but will be unable to receive notifications until it is enabled. See Enabling or Disabling Devices.<br>3. Click **Save** to return to the **Notification Devices** list. |
| To configure a new **voice phone number**: | 1. Select **US/Canada** or **Other**. The **Phone Number** entry field changes depending on your choice.<br>NOTE<br>The correct format for an **Other** phone number is: |

| Option | Description |
|---|---|
| | [COUNTRY_CODE][CITY AREA_CODE][PHONE_NUMBER].<br>Numbers that include '0' between the country code and the city/area code are invalid in AlertFind. For example, the phone number 44(0) 207 333 4444 is invalid.<br>However, a UK number such as 44 20 7333 4444 is valid. In this example, the area code for London (20) is separated by spaces from the rest of the phone number. AlertFind will eliminate spaces so that number will become 442073334444.<br>2. Enter a valid telephone number. This field is required.<br>3. To set advanced dialing options required to reach this phone device, check **Use advanced dialing options** and set any advanced options.<br>NOTE<br>When AlertFind calls an office phone, it can encounter an automated system that requires an extension number to be dialed. AlertFind dials the extension and waits for the user to pick up. If the time to connect is too long, then AlertFind assumes the caller did not pick up and attempts to leave a voicemail. The amount of delay depends on the PBX.<br>To add additional delays to the post-dial string to extend the AlertFind time-out time, in the **Use advanced dialing options** dialog box, insert additional commas (,) in the **Post-dial** field. One comma indicates a pause of one second.<br>4. To add this device but disable it, click **Disable** at the top of the page. The device is added but will be unable to receive notifications until it is enabled. See Enabling or Disabling Devices.<br>5. Click **Save** to return to the **Notification Devices** list. |
| To configure a new alpha-numeric or numeric **pager number**: | 1. Select **US/Canada** or **Other**. The **Pager Number** entry field changes depending on your choice.<br>2. Enter a valid pager number. This field is required.<br>3. Enter a **PIN**, if this pager requires one.<br>4. Select the **Carrier** from the drop-down list.<br>5. Set the **Pager Type** to either `Alphanumeric` or `Numeric`.<br>6. To add this device but disable it, click **Disable** at the top of the page. The device will be added but will be unable to receive notifications until it is enabled. See Enabling or Disabling Devices. |

| Option | Description |
|---|---|
| | 7. Click **Save** to return to the **Notification Devices** list. |
| To configure a new **SMS device**: | 1. Select **US/Canada** or **Other**. The **SMS Phone Number** entry field changes depending on your choice.<br>2. Enter a valid **SMS Phone Number**. This field is required.<br>3. Choose an option for **Max Length Handling**. Depending on the maximum message lengths imposed by the message carrier, you can choose to send all characters of a message, split messages into multiple chunks, or to truncate messages after a certain number of characters. For splitting or truncation options, you must provide the number of characters allowed before messages are chunked or truncated. Leave this field blank to use the default method for your organization.<br>4. To add this device but disable it, click **Disable** at the top of the page. The device will be added but will be unable to receive notifications until it is enabled. See Enabling or Disabling Devices.<br>5. Click **Save** to return to the **Notification Devices** list.<br>NOTE<br>• SMS messages have a 140-byte limit and are delivered in 140-byte chunks. To send messages larger than 140 bytes, devices and carriers either truncate the message or send the message in chunks of a specified length. Chunk sizes are determined by the device, by the carrier or by user settings. This means, if chunk sizes are not specified, for a languages that use single-byte character sets (such as English, Spanish, French, and German), only the first 160 characters of the message will be delivered. For languages that use double-byte character sets (such as Hindi, Korean, Chinese, and Japanese) only the first 70 characters of the message will be delivered.<br>• AlertFind sets chunking size defaults at 160 characters. If your organization sends SMS messages using double-byte character sets, you should consider changing these defaults to 70 characters to ensure that the full messages are delivered. In the **Edit Standard SMS Device** dialog box, select `Split message into smaller chunks of:` Then enter `70` in the **characters** number box and click **Save**.<br>• The system measures a single chunk's size as the number of characters in the **message header**, plus the number of |

| Option | Description |
|---|---|
| | characters to convey the portion of the **message subject** or **message body**. For example, each chunk includes the header **From {company notification system} (x of y)** plus **part of user-defined subject** or **message**. If the header length is greater than the configured chunk size, the message will not be sent. |
| To configure a new **fax number**: | 1. Select **US/Canada** or **Other**. The **Fax Number** entry field changes depending on your choice.<br>2. Enter a valid **Fax Number**. This field is required.<br>3. To add this device but disable it, click **Disable** at the top of the page. The device will be added but will be unable to receive notifications until it is enabled. See Enabling or Disabling Devices.<br>4. Click **Save** to return to the **Notification Devices** list. |
| To configure a new **mobile email device**: | 1. Enter a valid **Email Address** for the mobile email device. This field is required.<br>2. Choose an option for **Max Length Handling**.<br>3. To add this device but disable it, click **Disable** at the top of the page. The device will be added but will be unable to receive notifications until it is enabled. See Enabling or Disabling Devices.<br>4. Click **Save** to return to the **Notification Devices** list. |

4. When you return to the **Notification Devices** list, the configured device now shows up in all black text, without the **Not Configured** label. This device can be added to a notification profile by following the instructions under Customizing a Notification Profile.

You can keep this device configured but disable it to avoid receiving notifications on it. See Enabling or Disabling Devices.

#### Adding a New Custom Device

*Custom devices* are devices that can be added to an individual user account if you have the necessary permissions. Custom devices are different from the list of *standard devices* that are included for all user accounts by default. See Configuring a Standard Device for instructions on working with standard devices.

After a custom device is updated, it must added to the user’s personal escalations for it to receive notifications.

To add a new custom device:

1. From any list of users, double-click a user name to bring up the **User Overview** page. See Viewing User Lists for instructions on viewing user lists.
2. Click **Notification Devices** from the list of User Editor options. The **Notification Devices** page appears.
3. To add a new device, click **New**. A list of available devices appears.
4. Choose the device to add from the drop-down list, then follow the instructions below for each type of device:
5. Provide the necessary information for the device as mentioned in the configuration options table.
6. To add this device to this user's personal escalations, see Customizing Notification Profiles and Rules.

### Enabling or Disabling Devices

When viewing a user's **Notification Devices** list, the disabled devices are listed in ***gray*** text, with the label **(disabled)** next to the device name. These devices are configured, but cannot receive notifications until they are enabled.

Devices listed in ***black*** text are enabled and can receive notifications. Disable these devices to prevent notifications from being sent to them.

NOTE

This section assumes that you want to change a *standard* device that has already been configured or a *custom* device that has already been added. For instructions on those tasks, see Configuring a Standard Device or Adding a New Custom Device.

To enable or disable a device:

1. From any list of users, double-click a user name to bring up the **User Overview** page. See Viewing User Lists for instructions on viewing user lists.
2. Click **Notification Devices** from the list of User Editor options. The **Notification Devices** page appears.
3. Select the device to enable or disable.
4. To enable a disabled device, click the **Enable** button at the top of the **Notification Devices** list. The enabled device is listed in *black* text.
5. To disable an enabled device, click the **Disable** button at the top of the **Notification Devices** list. The disabled device is listed in *gray* text, with the label **(disabled)** next to the device name.

### Deleting or Unconfiguring a Device

This section describes instructions for deleting or unconfiguring a device in a user's account. This process removes all information about the device.

To disable a device but preserve its configuration for later use, see Enabling or Disabling Devices instead.

To delete or unconfigure a device:

1. From any list of users, double-click a user name to bring up the **User Overview** page. See Viewing User Lists for instructions on viewing user lists.
2. Click **Notification Devices** from the list of User Editor options. The **Notification Devices** page appears.
3. Select the device that you want to delete or unconfigure.
4. Click the **Delete/Reset** button at the top of the **Notification Devices** list.

When you reset a *standard* device (those that your organization requires in every user account), the configuration information for the device is removed, and the device appears as **Not Configured** in the **Notification Devices** list.

### NOTE

A standard device cannot be fully deleted. To use a disabled standard device, reconfigure it using the instructions under Configuring a Standard Device.

When a *custom* device is deleted (one that you created in addition to the standard list), it is completely *removed* from the **Notification Devices** list. To add the device back to the list, follow the instructions under Adding a New Custom Device. When you delete a device, all of its configuration information is lost, and you must recreate it completely if you need to use it again. To preserve the device information, but restrict it from use, see Enabling or Disabling Devices for instructions on disabling a device.

## Customizing Notification Profiles and Rules

Notification **profiles** define the order in which devices should be contacted for a notification and how much time should lapse between a notification being sent to the next device in the list. By default, your organization populates user accounts with a set of basic notification profiles.

Administrators and Team Leaders with permission can customize a user's notification profile. See Customizing a Notification Profile.

To remove customizations and reset the profile to the company default, follow the instructions under Resetting a Notification Profile.

Like other user account details, manual changes made to a user's notification profiles can be overwritten by a future import process. See Editing Imported Data for additional details.

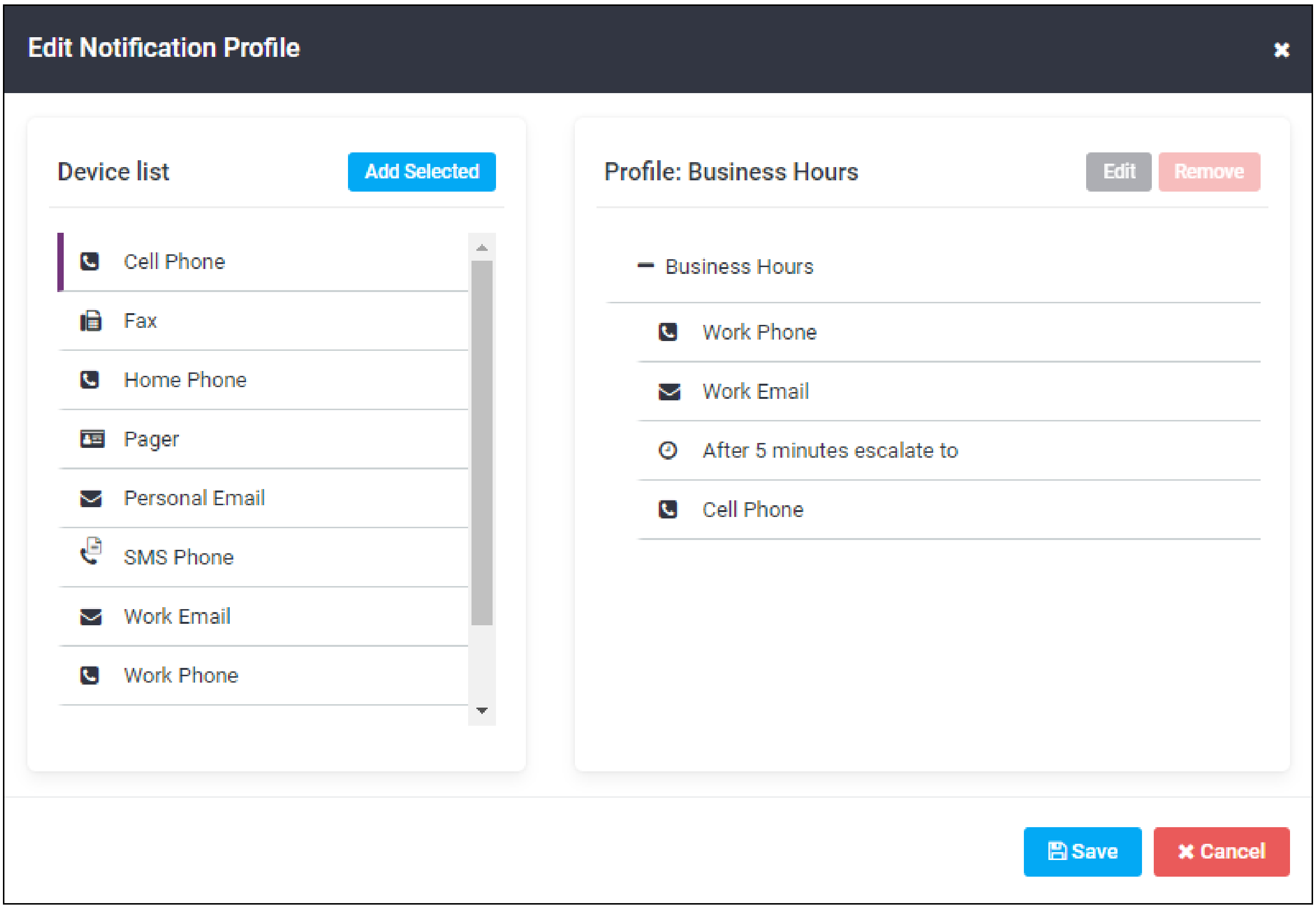
Notification **rules** define which notification profile is used to contact users during a notification sent at a specific time of day, day of the week, or holiday period. Notification rules are generally organization-wide and are set by the administrator using the Company Settings page.

### Customizing a Notification Profile

Most organizations define notification **profiles** that determine the order in which devices should be contacted for a notification. A user's default notification profile can be modified so that notifications are sent to different devices, or in a different order, or with a different amount of delay time between devices being contacted.

To customize a notification profile:

1. From any list of users, double-click a user name to bring up the **User Overview** page. See Viewing User Lists for instructions on viewing user lists.
2. Click **Notification Profiles** from the list of User Editor options. The **Notification Profile** page lists all of the notification profiles defined by your organization.
3. Select the profile to customize, then click **Configure**. The **Edit Notification Profile** page appears. On the left side is the list of all possible devices and delays that you can add to the profile. On the right side is the current list of devices and delays defined for the profile.



4. To add a device or delay to the profile, drag it from the list on the left to the list on the right, or double-click a device in the left column to add it to the list in the right column.
5. To remove a device or delay from the profile, select it in the right list and click **Remove**.
6. Click **Save** to save the customized profile. The profile now shows the label **(User Configured)** in the Notification Profile list.

### Resetting a Notification Profile

A customized notification profile can be reset to use the organization’s default settings.

To reset a notification profile to the organization default:

1. From any list of users, double-click a user name to bring up the **User Overview** page. See Viewing User Lists for instructions on viewing user lists.
2. Click **Notification Profiles** from the list of User Editor options. The **Notification Profile** page lists all of the notification profiles defined for the user account. Any profiles that are customized show the label **(User Configured)** in the Notification Profile list.
3. Select the configured profile to reset to company defaults, then click **Reset**.

4. Confirm that you want to reset the profile. The profile is returned to the company defaults, and the **(User Configured)** label disappears from the Notification Profile list.

## Enabling or Disabling Users

Administrators and team leaders with necessary permissions can *disable* users to hide them in the interface, prevent them from logging into AlertFind, and prevent them from receiving notifications, even if they are members of groups used during a notification event.

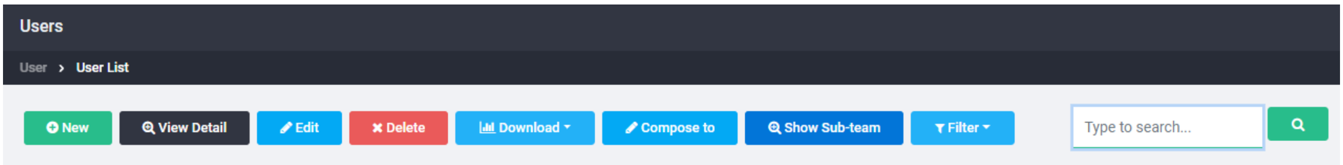
### NOTE

To delete imported users, remove them from the next roster import. Imported users cannot be permanently deleted through the web interface.

**Disable a user:**

1. From any list of users, double-click a user name to bring up the **User Overview** page. See Viewing User Lists for instructions on viewing user lists.
2. At the top of the **User Overview** page, click **Disable**. The **User Overview** page refreshes and the **Enable** button is now active.
3. Click **OK** to return to return to the **Users** page.

By default, this disabled user no longer appears in the Users list. Click the **Show Disabled** button to include disabled users in any user list.



**Enable a user:**

1. From any list of users, click the **Show Disabled** button to include disabled users in any user list.
2. Double-click a user name to bring up the **User Overview** page. See Viewing User Lists for instructions on viewing user lists.
3. At the top of the **User Overview** page, click **Enable**.

The **User Overview** page refreshes and the **Disable** button is now active. The user is now displayed in all user lists and can log into AlertFind and receive notifications.

## Adding Users to Teams or Groups

Administrators and team leaders with necessary permissions can add users to teams and groups. See Adding a User or Group to a Team or Add or remove group membership for instructions.

## Deleting Users

Administrators and team leaders with necessary permissions can delete users using the web interface.

However, if users are imported from another application, they must be removed from the source application, otherwise they are repopulated in AlertFind when data is next imported.

### NOTE

- To delete imported users, remove them from the next roster import.

  Imported users can be deleted using the AlertFind Administration web interface, but the users will be re-imported if they are not also removed from the import source data.

  Imported users cannot be deleted through Web Services / API.

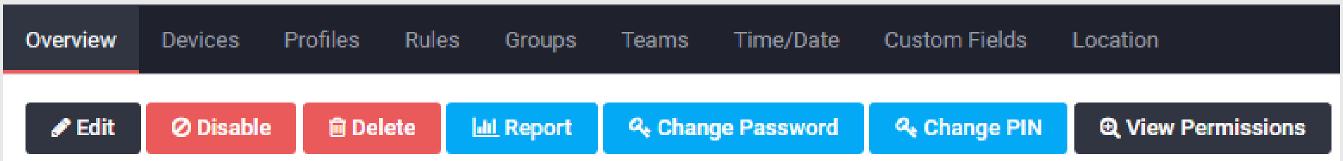
- When a user is deleted, the related configuration information is lost, and you must recreate the user completely if required.

  To preserve the user information, but restrict the use, see Enabling or Disabling Users for instructions on disabling a user.

To delete a user, perform one of the following options:

**Option 1**

1. From any list of users, double-click a user name to bring up the **User Overview** page. See Viewing User Lists" for instructions on viewing user lists.
2. At the top of the **User Overview** page, click **Delete**.

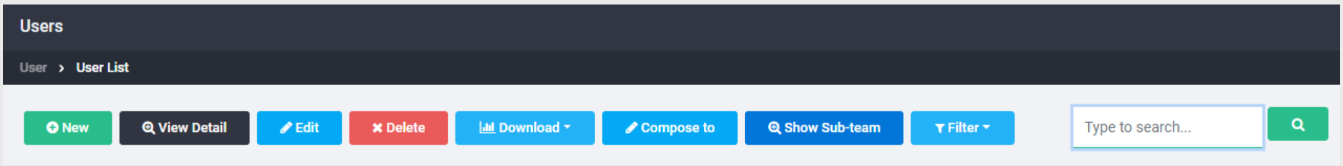


**Option 2**

1. Verify the team context is set for the desired team. For more information, see Team Security Context.
2. From the left navigation menu, **Administration** section, click **Users**.
3. Click the name of the user to be deleted to select it. Use shift-click to select a range of users,

and control-click to select multiple users.

4. Click **Delete** at the top of the **Users** page.



Click **OK** to confirm the deletion.

Be aware that **OK** is the *default* option for the confirmation dialogue box, so be careful when choosing users and using this feature, as deleted users cannot be recovered.

## User Reports

This section includes the following topics:

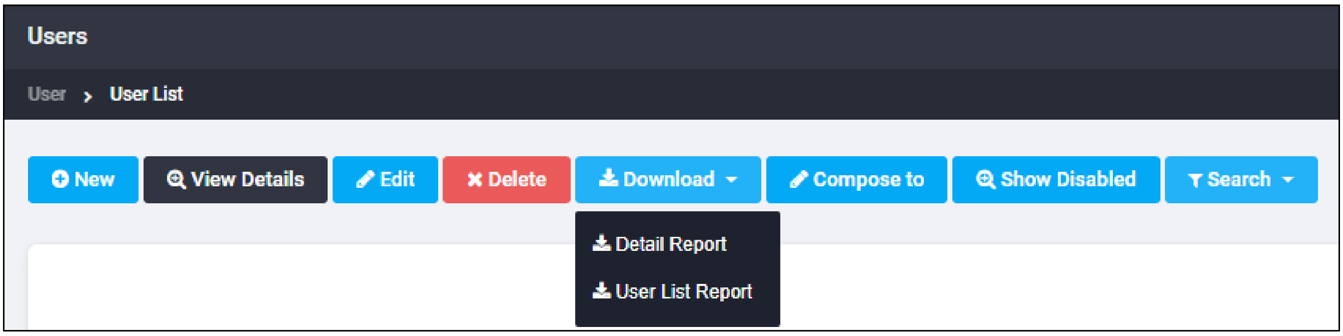
- User List Report (CSV)
- User Detail Report (CSV)
- Group Membership Report (CSV)
- Team Membership Report (CSV)

### User List Report (CSV)

Administrators and team leaders with necessary permissions can download a list of all users in the current team context.

To download a user list report:

1. Verify the correct team context. For more information, see Team Security Context.
2. On the navigation bar, click **Users**. The **Users** page appears.
3. Near the top of the **Users** page, click **Download**, then select **User List Report** from the drop-down list.



4. In the File dialog box that appears, choose to open or save the file. By default, this file is called `User List.csv`. Rename the file to indicate which user list you are downloading. Follow the dialog box instructions to save or open the file.

The user list report contains the following information for each user:

- Name
- Description
- Primary Email Address
- External key
- User name
- Data Source
- Role (Administrator or User)
- Status (enabled or disabled)
- Hotline assignment
- Time zone
- Weekend days
- Business hours
- For each standard device:

  - Device information (such as phone number or email address)
  - Device status (enabled or disabled)
  - Advanced settings (such as dialing rules)
- Custom devices for the user

### User Detail Report (CSV)

Administrators and team leaders with the necessary permissions can download a user detail report for the selected user.

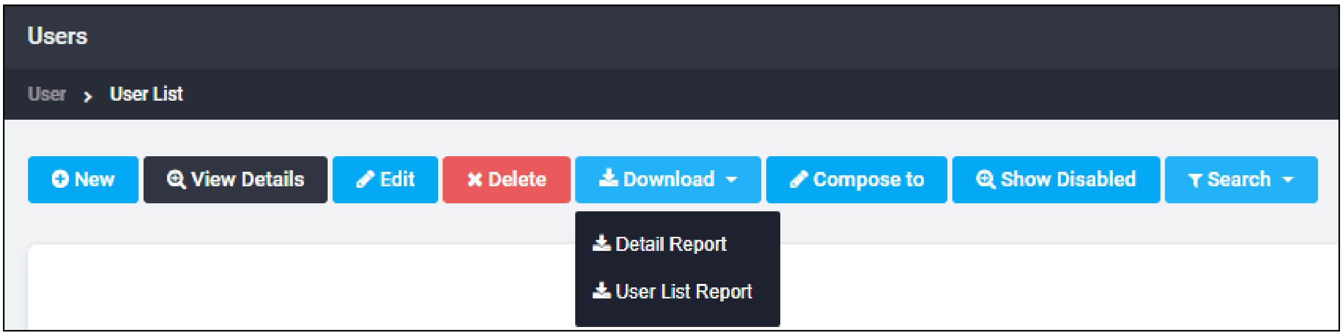
To download a user detail report:

1. Verify the correct team context. For more information, see Team Security Context.
2. On the navigation bar, click **Users**. The **Users** page appears.
3. In the user list, select the user whose details you want to download.

### NOTE

User Detail reports can also be downloaded from the **User Detail** page by clicking **Download** at the top of the **User Account** section.

4. On the **Users** page, click **Download** > **Detail Report** from the drop-down list.



5. In the File dialog box that appears, choose to open or save the file. By default, this file is called `[user name].csv`. Follow the dialog box instructions to save or open the file.

The user detail report contains the following information for the selected user:

- Name
- Description
- System access information:
  - User names
  - Hotline assignment
  - Primary email address
  - External key
  - Status (enabled or disabled)
- Personal information:
  - Time zone
  - Preferred voice/language (locale settings)

  - Weekend days
  - Business hours
- Data management information:
  - Source (imported or manually created)
  - Role (Administrator or User)
  - Permissions
- For all devices (standard or custom):
  - Device name
  - Device type
  - Device status (enabled or disabled)
  - Device address (such as phone number or email address)
- For each personal escalation:
  - Escalation name
  - Custom escalation (yes or no)
  - Escalation description
  - Escalation steps

### Group Membership Report (CSV)

Administrators and team leaders with the necessary permissions can download a group membership report for a selected user.

To download a group membership report:

1. From any list of users, double-click a user name to bring up the **User Overview** page. See Viewing User Lists for instructions on viewing user lists.
2. Click **Group Membership** from the list of User Editor options. The list of groups the user belongs to appears.
3. Click **Download**. The File dialog box appears.
4. Choose to open or save the file. By default, this file is called `Group Membership.csv` for all users. Rename the file to indicate which user's report you are downloading. Follow the dialog box instructions to save or open the file.

The group membership report contains the following information for each group the user is a member of:

- Group name
- Group type (such as Broadcast Group or Escalation Group)

### Team Membership Report (CSV)

Administrators and team leaders with the necessary permissions can download a team membership report for the selected user.

To download a team membership report:

1. From any list of users, double-click a user name to bring up the **User Overview** page. See Viewing User Lists for instructions on viewing user lists.
2. Click **Team Membership** from the list of User Editor options. The list of teams the user belongs to appears.
3. Click **Download**. The File dialog box appears.
4. Choose to open or save the file. By default, this file is called `Team Membership.csv` for all users. Rename the file to indicate which user's report you are downloading. Follow the dialog box instructions to save or open the file.

The team membership report contains the name of each team the user is a member of.

## AlertFind Recognized SMS Commands

AlertFind end-users with enabled SMS devices have the ability to send SMS commands to their AlertFind contact number. When these unsolicited text messages are received, AlertFind automatically responds. At this time, two commands are recognized: `Help` and `Unsubscribe`.

AlertFind uses the short code 55626 as the cell phone "address" when sending or replying to an AlertFind text.

### ‘Help’ SMS Command

The Help command is an SMS message containing one of the following values:

- English - `help`
- French - `info` or `aide`

Commands are *not* case sensitive.

When the AlertFind contact number receives one of the above commands, AlertFind responds to the Help message with instructions to call a phone number, which by default is set to the customer's Caller ID, but may be customized to another phone number.

### ‘Unsubscribe’ SMS Command

The Unsubscribe command is an SMS message containing one of the following values:

| Language | Command |
|---|---|
| English | • `unsubscribe`<br>• `stop`<br>• `end`<br>• `quit`<br>• `cancel` |
| French | • `arret` |

Commands are *not* case sensitive.

When the AlertFind contact number receives one of the above commands, it responds by:

- Sending a confirmation SMS to the device indicating that no further messages will be sent.
- Sending an email to the user's primary email address indicating that the device has been disabled.
- Disabling the associated device within AlertFind so no further SMS messages can be sent to the device.

To resubscribe to SMS messages, the user must contact their AlertFind administrator to have the SMS device enabled. See Enabling or Disabling Devices.

# Teams and Permissions

Teams are hierarchical and can be used to replicate an organization’s structure or manage the scope of recipients to which you can send notifications. A team can have no leader or multiple leaders. If an individual team has no leader, then only an administrator or leader of a higher level (parent) team can perform certain team actions

Permissions provide security by controlling the data that team leaders can view and actions that they can perform. Administrators have full permissions on team information; team leaders have a subset of permissions on team information; users have no permissions on team information.

If users are allowed to update their own personal contact information, they do this on the **My Account** page, which does not require team permissions.

## Team Hierarchy

Teams are based on a hierarchical structure. In the team hierarchy, a higher level team is called the *parent* team. The *Global Team* is the highest-level parent team. Sub-teams of a team are called *child* teams. Teams must contain at least one user, and can contain both broadcast and escalation groups.

Teams can be combined with *permissions* to tightly control the actions individuals can perform and the information they can view. For example, one team leader might be granted permission to send notifications and another team leader permission to manage public data for team members.

Team leaders carry their permissions in the parent team to a child team through *inheritance*. An exception to inheritance occurs when the leader is explicitly added to a sub-team. In this case you can remove permissions.

### Team Hierarchy Example

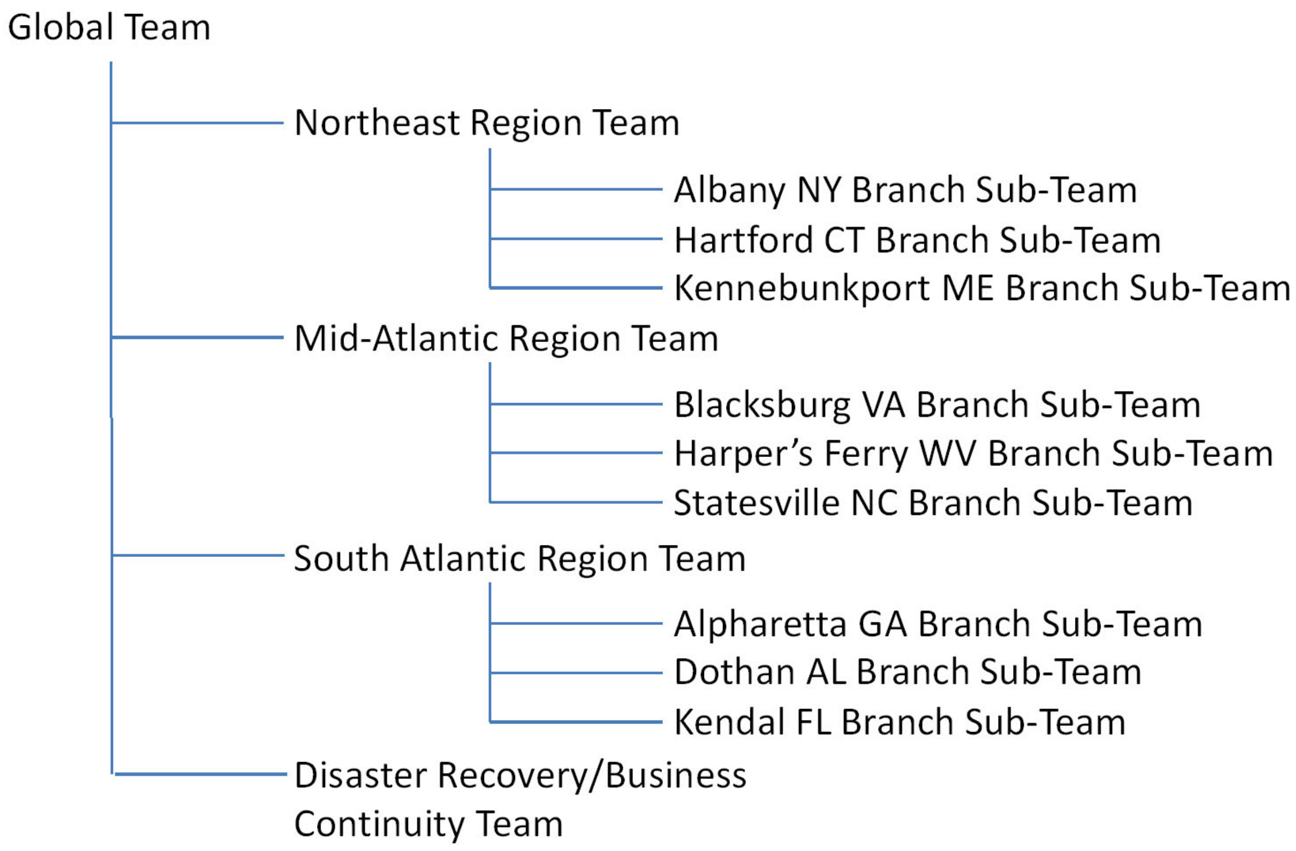
Republic Bank has three regional offices, each of which has its own manager and support staff. Each region includes three branch offices. In addition, Republic Bank uses cross-regional teams to address areas of concern to all employees such as disaster recovery and business continuity planning.

To control access to employee data, Republic Bank creates a team for each region, and then creates sub-teams for each branch. Each branch manager is made a team leader for his branch and is granted permission to send notifications to his branch. He does not have permission to send notifications to other branches in his region or in other regions.

The regional managers are leaders of regional teams, which contain the branch teams. The regional manager is a team leader for his region and can send notifications to all of the branch sub-teams in his region. He cannot send notifications to branches that are outside of his region.

In addition, Republic Bank creates a disaster recovery team. This team consists of one member from each branch. The leader of the disaster recovery team has permission to send notifications to the disaster recovery team only.

The Global Team leader can send notifications to everyone.



- Global Team
  - Northeast Region Team
    - Albany NY Branch Sub-Team
    - Hartford CT Branch Sub-Team
    - Kennebunkport ME Branch Sub-Team
  - Mid-Atlantic Region Team
    - Blacksburg VA Branch Sub-Team
    - Harper’s Ferry WV Branch Sub-Team
    - Statesville NC Branch Sub-Team
  - South Atlantic Region Team
    - Alpharetta GA Branch Sub-Team
    - Dothan AL Branch Sub-Team
    - Kendal FL Branch Sub-Team
  - Disaster Recovery/Business Continuity Team

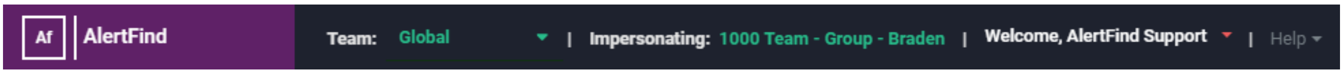
## Team Security Context

*Team security context* is the team a user is currently accessing within AlertFind. Because team leaders can have different permissions on different teams, the team security context under which they are operating determines what actions they can take in AlertFind.

Using the hierarchy example, a branch manager has `Send Notification` permission on the branch team but not on the regional team. When the branch manager is working under their regional team context, the manager is unable to send notifications. When the manager switches team security context to a branch team, the manager can send notifications to branch team members.

### Check your team security context:

Your current team security context is displayed on left-hand side of the navigation bar.


Af
AlertFind
Team: Global
Impersonating: 1000 Team - Group - Braden
Welcome, AlertFind Support
Help

### TIP

If at any point you see fewer or more groups, users, or options in the system than you expect to see, double-check your team context.

### Change your team security context:

To change team security context:

1. From the top navigation bar expand the **Teams** drop-down menu.
2. Click the desired team name to make it the active team security context.

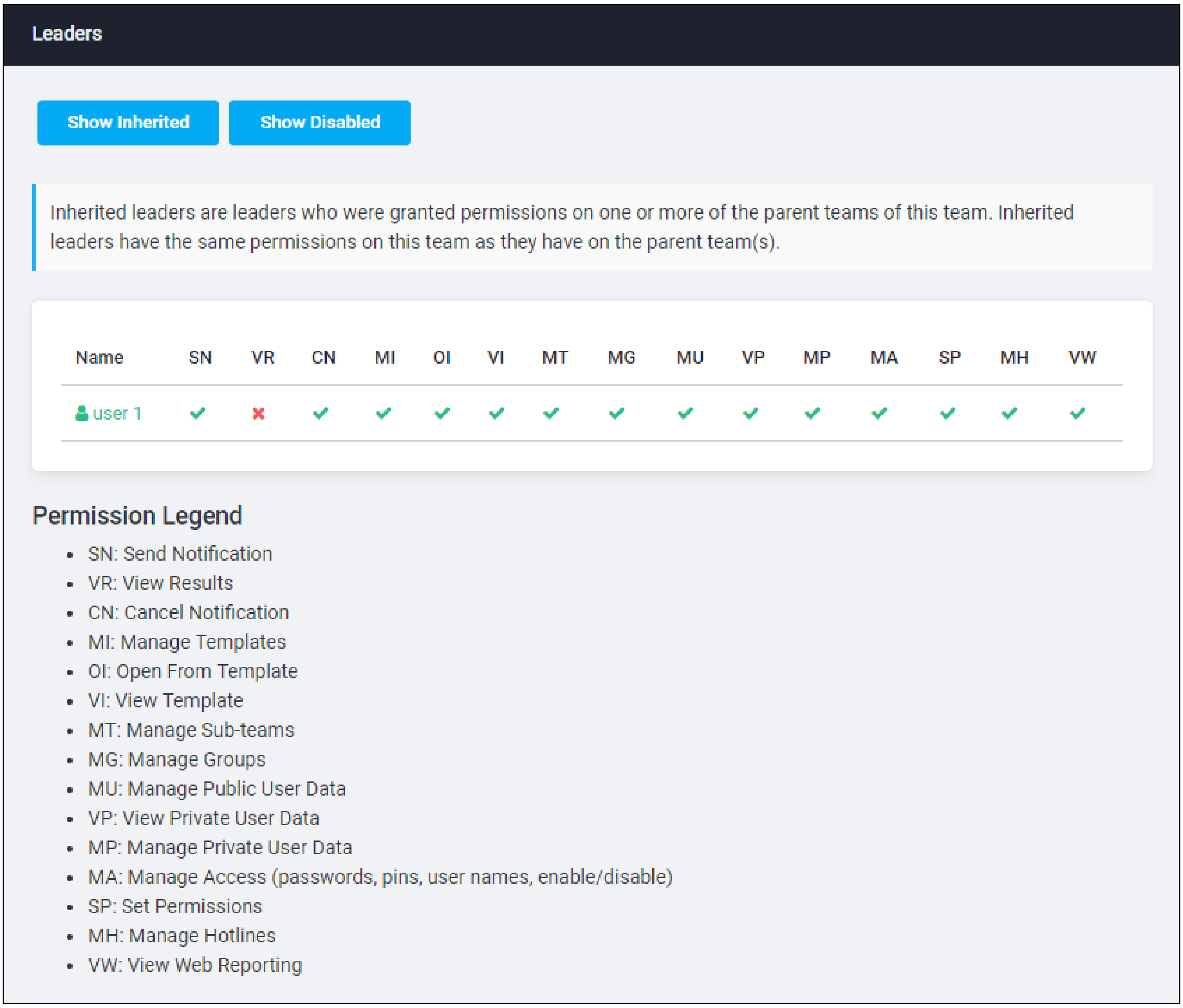
### NOTE

If a user is a leader of only one team, the user cannot change their team context.

## Permissions

*Permissions* control which information is available to a team leader, and what actions they can perform.

Permissions are assigned per team. A team leader can have different permissions on different teams. Team leaders can also inherit permissions from a higher level team. See Team Hierarchy for more information about inheritance.



Inherited leaders are leaders who were granted permissions on one or more of the parent teams of this team. Inherited leaders have the same permissions on this team as they have on the parent team(s).

| Name | SN | VR | CN | MI | OI | VI | MT | MG | MU | VP | MP | MA | SP | MH | VW |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| user 1 | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

### Permission Legend

- SN: Send Notification
- VR: View Results
- CN: Cancel Notification
- MI: Manage Templates
- OI: Open From Template
- VI: View Template
- MT: Manage Sub-teams
- MG: Manage Groups
- MU: Manage Public User Data
- VP: View Private User Data
- MP: Manage Private User Data
- MA: Manage Access (passwords, pins, user names, enable/disable)
- SP: Set Permissions
- MH: Manage Hotlines
- VW: View Web Reporting

Administrators have all permissions across all teams. Users have no team permissions by default. To make a user a team leader, the user must be granted one or more team permissions. The following icons indicate permission status:

| Icon | Indicator | Meanings |
|---|---|---|
| ✓ | green check | The permission is granted. |

| Icon | Indicator | Meanings |
|---|---|---|
| | mark | |
| ✓ | orange check mark | The permission is granted through inheritance. See Team Hierarchy for more information about inheritance. |
| ✗ | red X | The permission is not granted. |

Each team leader permission grants specific abilities.

| Label | Permission | Ability Granted | Also Requires |
|---|---|---|---|
| **Permissions and Access Permissions** | | | |
| MA | Manage Access | Edit account authentication methods (passwords, PINs), and status for any user on the team. | |
| SP | Set Permissions | Edit permissions for any user on the team with equal or lesser permissions. | |
| **Group and Team Permissions** | | | |
| MT | Manage Sub-Teams | Create sub-teams and manage users on the sub-team. Manage groups and reports for teams and sub-teams. | |
| MG | Manage Groups | Create, edit and delete groups within a team. Create Smart Groups. | |
| **User Data Permissions** | | | |
| MU | Manage Public User Data | Edit public information for any user on the team. | |
| VP | View Private User Data | View private information for any user on the team. | |
| MP | Manage Private User Data | Edit private information for any user. | VP |
| **Notification Permissions** | | | |
| SN | Send | Send notifications and create | VR |

| Label | Permission | Ability Granted | Also Requires |
|---|---|---|---|
| | Notification | incidents. | |
| VR | View Results | View notification information and Hotline Poll results. View and archive incidents. | |
| CN | Cancel Notification | Cancel in-progress notifications. | VR |
| **Incident and Notification Template Permissions** | | | |
| MI | Manage Templates | Manage templates. | VR is required to enable Save as notification template |
| OI | Open from Template | Open a template. | VI and VR |
| VI | View Templates | View templates. | |
| **Hotline Pro Permissions** | | | |
| MH | Manage Hotline | Use Hotline Pro features. | |
| **Web Reports Permissions** | | | |
| VW | View Web Reports | View web reports, if enabled for your organization. | |

## Granting Team Leader Permissions

### NOTE

Permissions are inherited. For example, if a team leader has a permission on a parent team that has child teams (sub-teams), the team leader has the permissions of the parent team on the child teams.

It is not required that a team has a leader. In this case, only an administrator or a leader of a parent team can perform actions on the team. Teams can also have multiple leaders, each with different permissions. It is not required that the leader be a member of the team of which he is a leader. For more information about permissions, see Permissions.

Users become team leaders when they are assigned any permission on a team. As such, they can be leaders of multiple teams and may have different permissions on each team.

Team leaders can be created in two ways:

- By an administrator or a parent team leader assigning permissions on the user **Account** page. See View permissions on the User Account page.
- By an administrator or a parent team leader making the user a team leader through the **Create Team** wizard. See View permissions on the Team page.

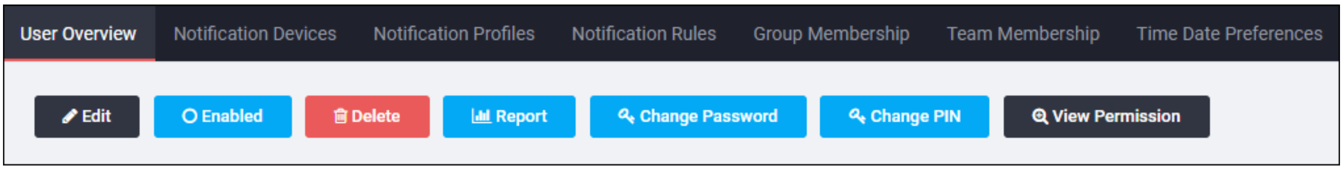
## Viewing Permissions

Permissions can be viewed in two places:

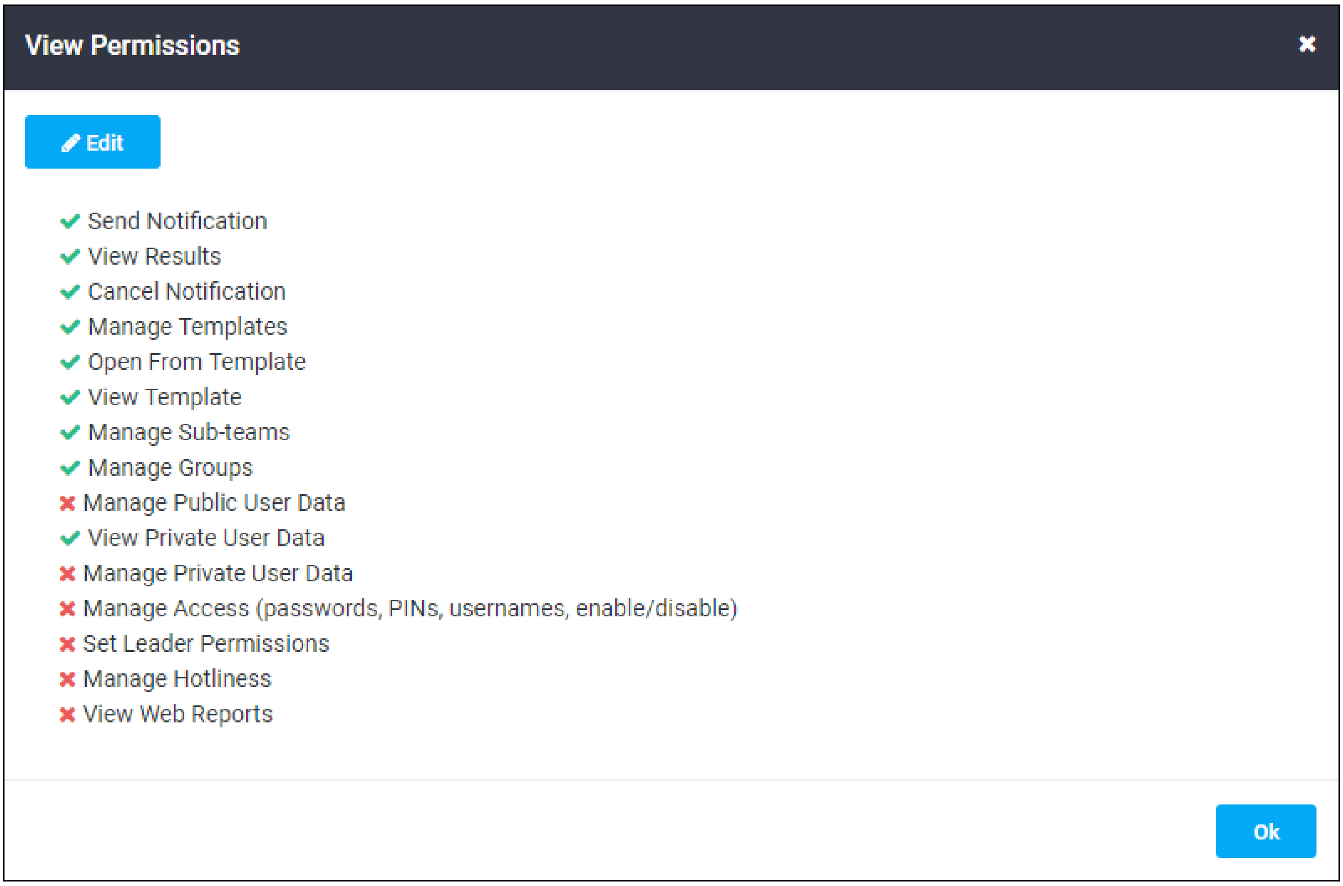
- On the **User Account** page (permissions can also be edited in this location)
- On the **Team** page (this is a view-only page)

### View permissions on the User Account page

1. Select the appropriate Team Security Context. Team permissions are based on the current Team Security Context. See Change your team security context.
2. From the left navigation menu **Administration** section, click **Users**.
3. Locate the desired user, and either double-click it or highlight it and click **View Details**.
4. Click the **View Permissions** button.



The **Permissions on Team [active team name]** window appears.



✓ Send Notification
✓ View Results
✓ Cancel Notification
✓ Manage Templates
✓ Open From Template
✓ View Template
✓ Manage Sub-teams
✓ Manage Groups
✖ Manage Public User Data
✓ View Private User Data
✖ Manage Private User Data
✖ Manage Access (passwords, PINs, usernames, enable/disable)
✖ Set Leader Permissions
✖ Manage Hotliness
✖ View Web Reports

5. If you have permission to edit a team leader’s permissions on this team, click **Edit** to add or remove permissions.

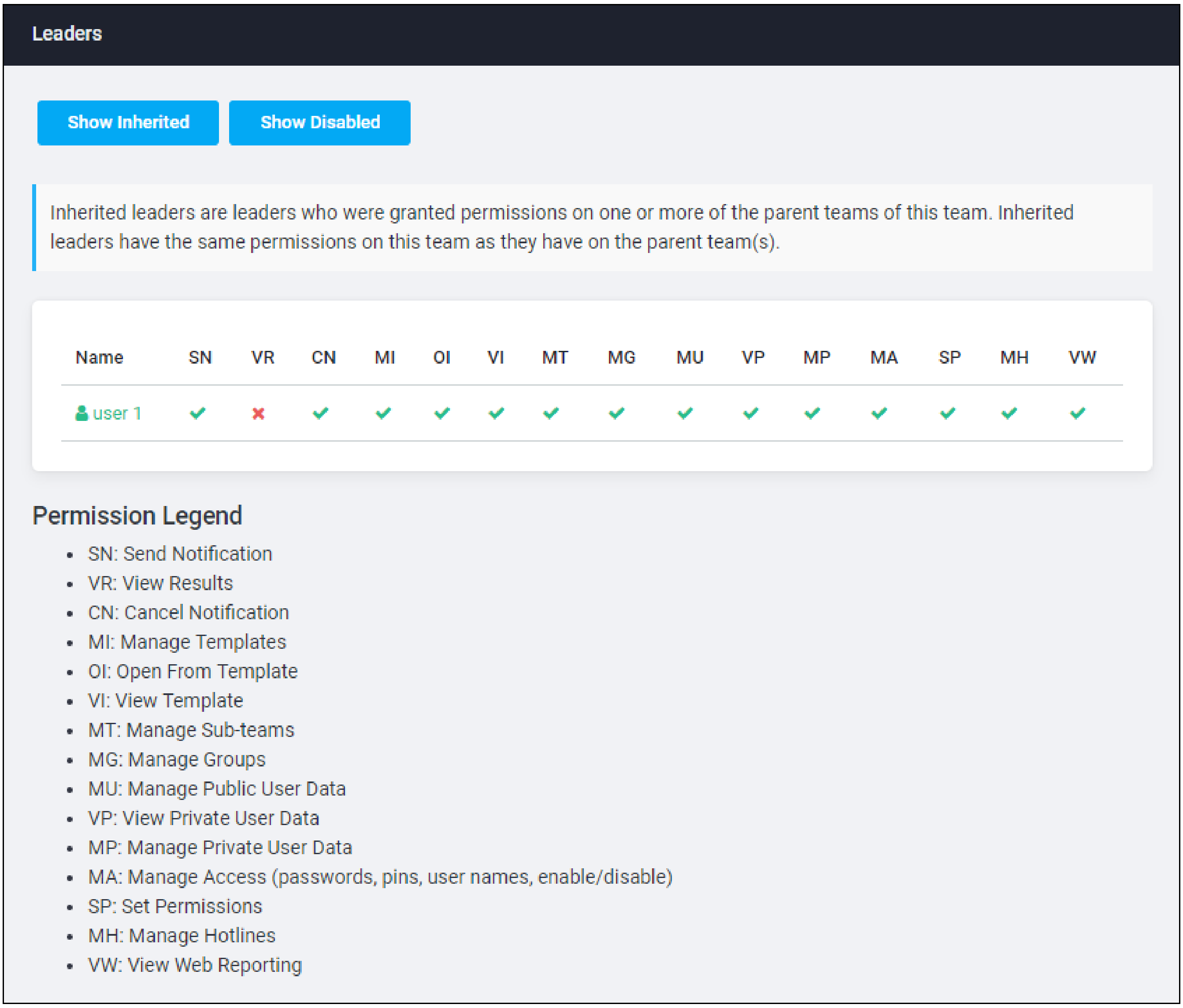
## NOTE

A team leader cannot grant a user a permission that the leader does not have.

### View permissions on the Team page

1. From the left navigation menu **Administration** section, click **Teams**.
2. On the **My Teams** page, click the name of the team to view team leader permissions. If a user is a leader of only one team, that user will see only one team.
3. Under the **Leaders** section, the leaders are listed with indicators showing the permissions they have.

See here for a list of permission status indicators. See here for more information on specific permissions. See Changing Permissions for further information.



Inherited leaders are leaders who were granted permissions on one or more of the parent teams of this team. Inherited leaders have the same permissions on this team as they have on the parent team(s).

| Name | SN | VR | CN | MI | OI | VI | MT | MG | MU | VP | MP | MA | SP | MH | VW |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| user 1 | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

Permission Legend

- SN: Send Notification
- VR: View Results
- CN: Cancel Notification
- MI: Manage Templates
- OI: Open From Template
- VI: View Template
- MT: Manage Sub-teams
- MG: Manage Groups
- MU: Manage Public User Data
- VP: View Private User Data
- MP: Manage Private User Data
- MA: Manage Access (passwords, pins, user names, enable/disable)
- SP: Set Permissions
- MH: Manage Hotlines
- VW: View Web Reporting

## Changing Permissions

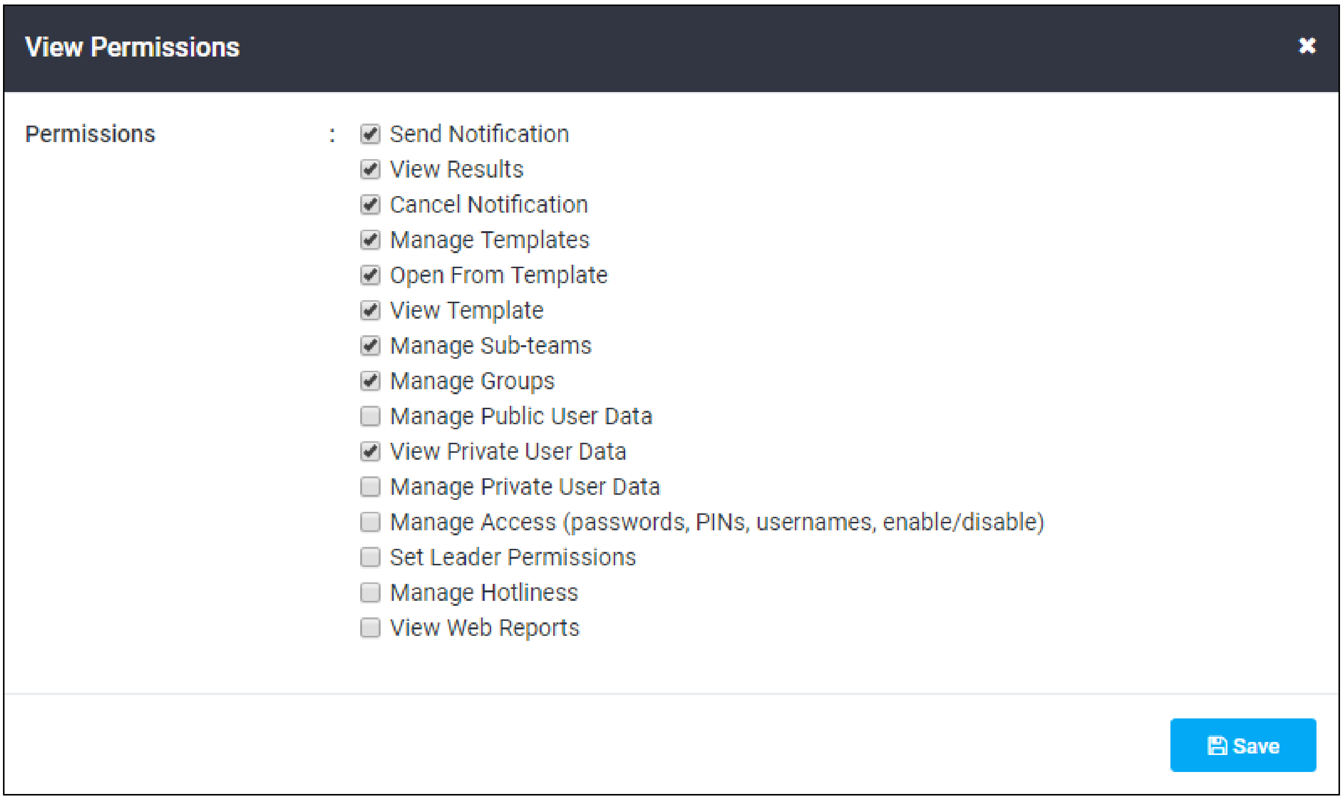
If a team leader has Set Permission (SP) permission, they can manage permissions of members of their team(s).

### NOTE

A team leader cannot grant a user a permission the team leader does not have.

To add or remove permissions for a team member:

1. From "View permissions on the User Account page", perform steps 1 through 6 to navigate to the permissions page for the desired team member.
2. Click **Edit**. By default, all permissions except Manage Permissions (MP), Manage Access (MA), and View Web Reports (VW) are preselected.



Permissions :
☑ Send Notification
☑ View Results
☑ Cancel Notification
☑ Manage Templates
☑ Open From Template
☑ View Template
☑ Manage Sub-teams
☑ Manage Groups
☐ Manage Public User Data
☑ View Private User Data
☐ Manage Private User Data
☐ Manage Access (passwords, PINs, usernames, enable/disable)
☐ Set Leader Permissions
☐ Manage Hotliness
☐ View Web Reports

3. To grant team leader permissions to a team member, add or remove the appropriate permissions by checking or unchecking each check box, leaving at least one box checked.

   To remove team leader permissions from a current team leader, uncheck all check boxes.

4. Click **Save** to save the changes.

## Managing Teams

This section describes the procedures for specific team management tasks, such as creating, editing, or deleting teams and adding or removing team members.

## The Global Team

The Global Team is the highest level team for an organization. It contains all of the users, groups, and teams in the organization. By default, all administrators are considered team leaders for the Global Team. Non-administrator users can also be made Global Team Leaders by being granted the necessary permissions on the Global Team.

## TIP

When a user is added to a group at the Global Team level, the user becomes a member of every team that contains that group.

### Granting Global Team Leader Permissions

Any team leader for the Global Team with Set Permissions (SP) permission on the Global Team can make other users Global Team leaders, granting the new team leader all or some of the permissions that the granting leader has.

### Grant or remove Global Team leader permissions for a user

1. Verify that you are in the Global Team context. (See Check your team security context for information.)
2. From the left navigation menu **Administration** section, click **Users**.
3. Locate the desired user, and either double-click it or highlight it and click **View Details**.
4. Click the **View Permissions** button. The **Permissions on Team Global** window appears.
5. Click **Edit**. The **Change Permissions for User** page appears.
6. Carefully examine the checked and unchecked permissions. Check or clear check boxes to add or remove the specific Global Team Leader permissions to assign to this user. See status indicators and Permissions for more information.
7. Click **Save** to save the selected Global Team Leader permissions to the user.

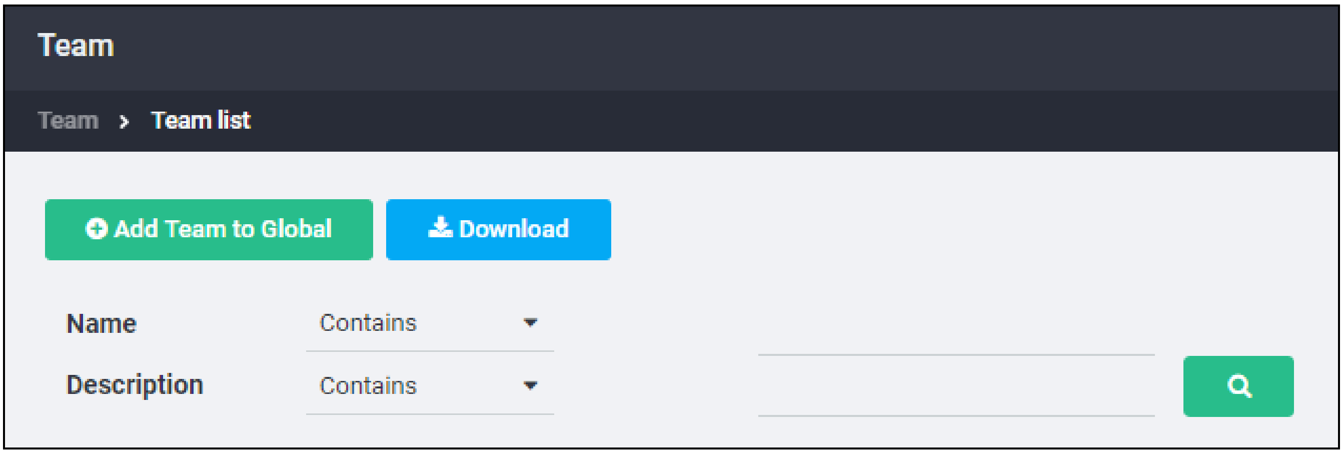
This affects team leader permissions only on the Global Team. The user does not inherit permissions for any sub-teams. The user must be explicitly granted team leader permissions for those teams separately.

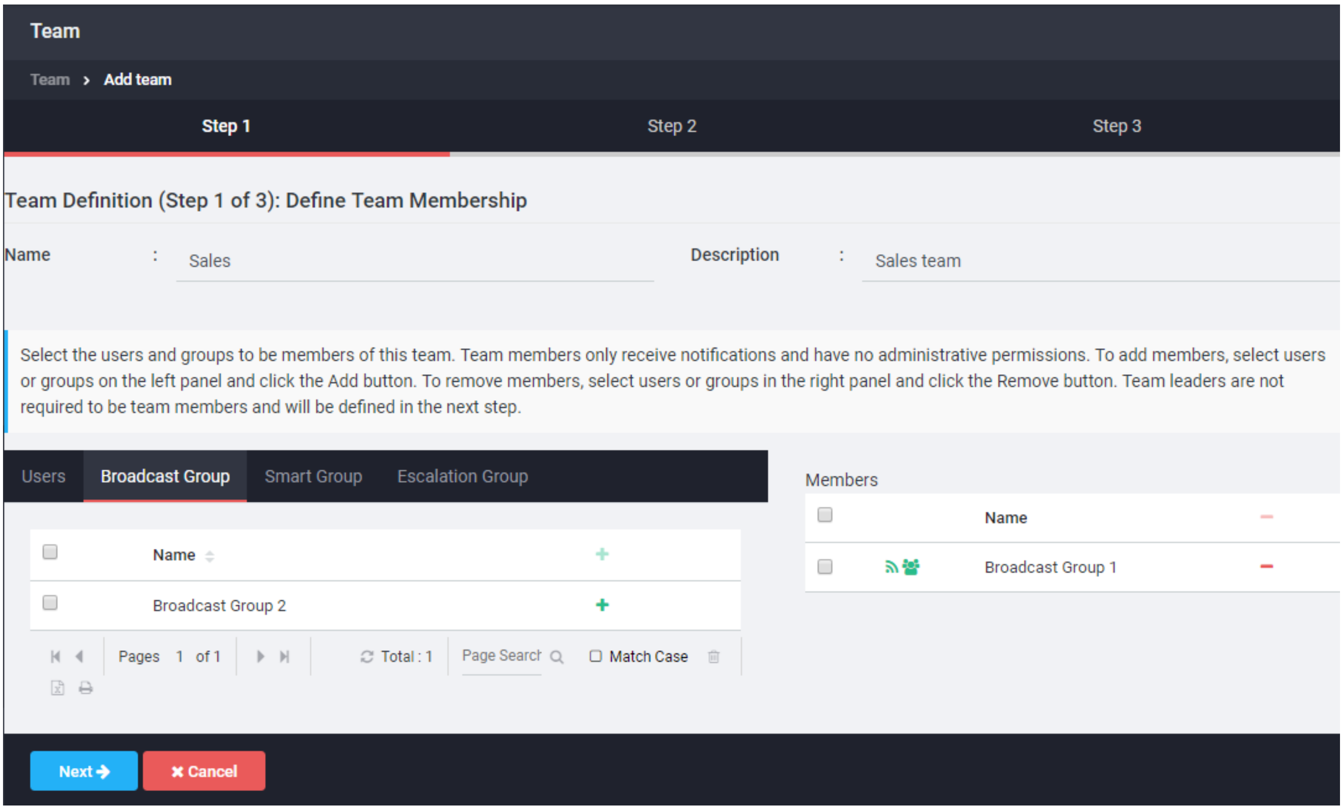
### Creating Sub-Teams of the Global Team

Any top-level teams created in the system are sub-teams of the Global Team and cannot be removed from the Global Team. Users retain all the same permissions on the sub-team as they have on the Global Team. Team leader permissions can be granted on these sub-teams to allow other members of the organization to manage these teams on your behalf.

To create a new sub-team of the Global Team:

1. From the left navigation menu **Administration** section, click **Teams**.
2. In the **My Teams** section, click **Add Team to Global**. The **Team Definition** wizard is displayed.





Team Definition (Step 1 of 3): Define Team Membership

Name : Sales

Description : Sales team

Select the users and groups to be members of this team. Team members only receive notifications and have no administrative permissions. To add members, select users or groups on the left panel and click the Add button. To remove members, select users or groups in the right panel and click the Remove button. Team leaders are not required to be team members and will be defined in the next step.

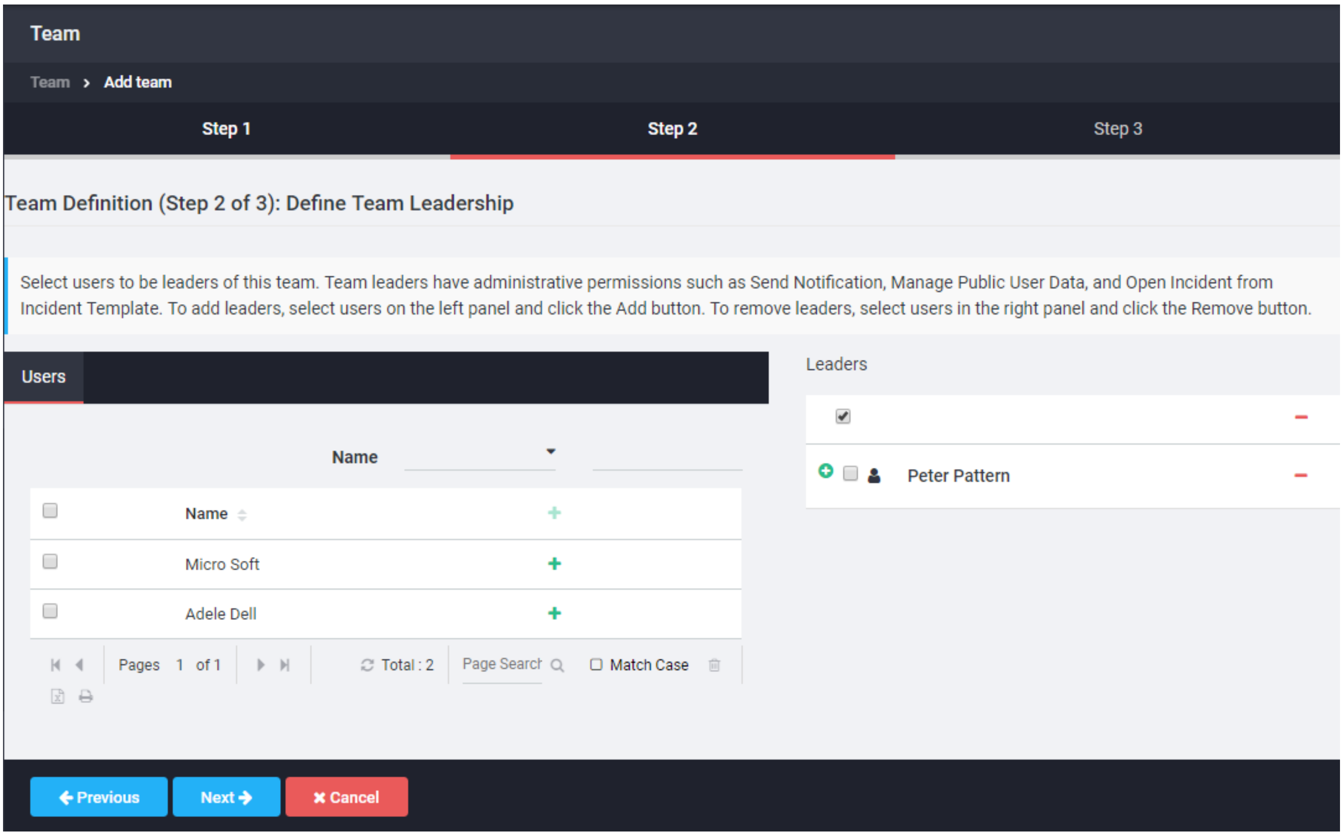
3. Type a name and description for this team. The team name is required.
4. Enter a description for this team. The description is optional.
5. Add users and groups as members of the team.

   Sel1ect users and groups from any of the tabs displayed (**Users**, **Broadcast Groups**, **Smart Groups**, or **Escalation Groups**). Use the search fields provided to search by name or filter using the Criteria Editor. See Filtering Lists for instructions on using search and Criteria Editor tools.

2. Locate the user or group to add, select it and click **Add**. The user or group is added to the **Members** list.

3. When the member list is complete, click **Next**.

6. Select the team leaders for this team.



Team Definition (Step 2 of 3): Define Team Leadership

Select users to be leaders of this team. Team leaders have administrative permissions such as Send Notification, Manage Public User Data, and Open Incident from Incident Template. To add leaders, select users on the left panel and click the Add button. To remove leaders, select users in the right panel and click the Remove button.

1. From the list of users, select a user and click **Add** to move the user into the **Leaders** list. Leaders can be selected from the users who are members of the parent team.
2. Each leader is automatically granted the default set of team leader permissions. To grant or remove permissions, click the plus sign ⊞ next to the leader whose permissions you want to change and check or clear check boxes to grant or remove specific permissions.
3. When all the team leaders are added and permissions configured, click **Next**.

7. The **Team Definition** page appears, listing the team name, members, and leaders (with their permissions). Verify the definitions and set-up are correct. If not, click **Back** to return to the previous screen and edit the team.
8. Click **Save** to save the new team.

To create additional sub-teams for this team, see "Creating Sub-Team of Existing Team". Any team leader who is granted Manage Sub-Teams (MT) permissions can also create sub-teams for this team.

### Creating Sub-Team of Existing Team

Users granted Manage Sub-Teams (MT) permissions on a team can create sub-teams (*child teams*) under the original team (*parent team*). Users inherit the same permissions on the sub-team that they have on the parent team.

To create a new sub-team of an existing team:

1. From the left navigation menu **Administration** section, click **Teams**.
2. On the **My Teams** page, click the name of the team under which you want to create a sub-team. The team information appears.
3. Scroll to the bottom of the page to the **Sub-Teams** section. Click **Add Team**. The first page of the **Team Definition** Wizard appears.
4. Type a name and description for this team. The team name is required.
5. Add users or groups as members of the team.

#### NOTE

Only users, broadcast groups, Smart Groups, and escalation groups available to the parent team can be added to this sub-team.

1. Users and groups can be selected from any of the tabs displayed (**Users**, **Broadcast Groups**, **Smart Groups**, or **Escalation Groups**). Use the search fields provided to search by name or filter using the Criteria Editor. See Filtering Lists for instructions on using search and Criteria Editor tools.
2. Locate the user or group to add, select it and click **Add**. The user or group is added to the **Members** list.
3. When the member list is complete, click **Next**.

6. Select the team leaders for this team.
    1. From the list of users, select a user and click **Add** to move the user into the **Leaders** list. Leaders can be selected from the users who are members of the parent team.
    2. Each leader is automatically granted the default set of team leader permissions. To grant or remove permissions, click the plus sign ⊕ next to the leader whose permissions you want to change and check or clear check boxes to grant or remove specific permissions.
    3. When all the team leaders have been added and permissions configured, click **Next**.
7. The **Team Definition** page appears, listing the team name, members, and leaders (with their permissions). Click **Save** to save changes, or click **Back** to return to the previous screen and edit the team before saving it.

### Editing Team Information, Members, and Leaders

If users have been granted the necessary permissions on a team, they can edit the team name, description, members list, team leaders list, and team leader permissions using this procedure.

To edit team information:

1. From the left navigation menu **Administration** section, click **Teams**.
2. On the **My Teams** page, click the team name you want to edit. The team information page appears.
3. If you have the necessary permissions to edit this team, an **Edit** button appears in the **Team Information** section at the top of the page. Click **Edit**. The **Team Definition** Wizard appears.
4. Edit the team name and description. A team name is required.
5. Add or remove users or groups.

NOTE

Only those users, broadcast groups, smart groups, and escalation groups that are available to the parent team can be added to this sub-team.

   1. To remove users and groups, select a user or group in the **Members** list and click **Remove**.
   2. To add users and groups, locate the user or group using any of the tabs displayed (**Users**, **Broadcast Groups**, **Smart Groups**, or **Escalation Groups**). Use the search field provided to search by name or filter using the Criteria Editor. See Filtering Lists for instructions on using search and Criteria Editor tools.
   3. Locate the user or group to add, select it and click **Add**. The user or group is added to the **Members** list.
   4. When the member list is complete, click **Next**.

6. Add or remove team leaders, and grant or remove additional team leader permissions.
   1. To remove a team leader, select the leader in the **Leaders** list and click **Remove**.
   2. To add a leader, select a user from the available list of users and click **Add** to move the user into the **Leaders** list.
   3. To grant or remove permissions for a leader, click the plus sign ⊕ next to the leader whose permissions you change and check or clear check boxes to grant or remove specific permissions.
   4. When the **Leaders** list and leader permissions are configured, click **Next**.

The **Team Definition** page appears, listing the team name, members, and leaders (with their permissions).

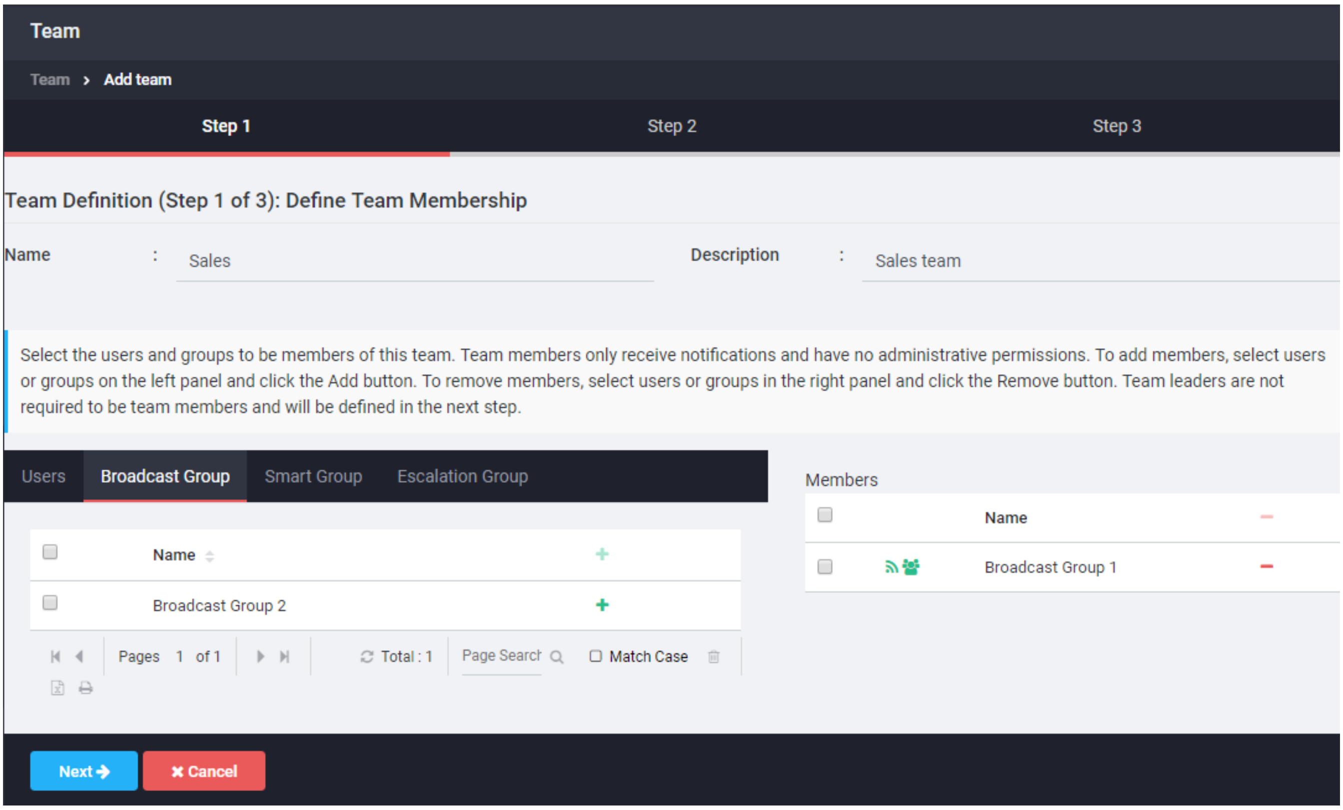
7. Click **Save** to save changes, or click **Back** to return to the previous screen and edit the team before saving it.

## Adding a User or Group to a Team

A team leader can add users, broadcast groups, escalation groups, and Smart Groups to any team created. A team leader can also assign leadership of any team they create. These actions can be performed on teams they did not create and only if the creator of the team grants these permissions.

To add a user or group to a team:

1. From the left navigation menu **Administration** section, click **Teams**.
2. Click the name of the team to which you want to add the user or group. The **Team** page appears.
3. Click **Edit**.



Team Definition (Step 1 of 3): Define Team Membership

Name : Sales

Description : Sales team

Select the users and groups to be members of this team. Team members only receive notifications and have no administrative permissions. To add members, select users or groups on the left panel and click the Add button. To remove members, select users or groups in the right panel and click the Remove button. Team leaders are not required to be team members and will be defined in the next step.

| □ | Name | + |
|---|---|---|
| □ | Broadcast Group 2 | + |

Members

| □ | | Name | − |
|---|---|---|---|
| □ | | Broadcast Group 1 | − |

### NOTE

Only users, broadcast groups, Smart Groups, and escalation groups available to the parent team can be added to a sub-team.

4. To add users and groups, locate the user or group using any of the tabs displayed (**Users**, **Broadcast Groups**, **Smart Groups**, or **Escalation Groups**). Use the search fields provided to search by name or filter using the Criteria Editor. See Filtering Lists for instructions on using search and Criteria Editor tools.
5. Locate the user or group to be added, select it and click **Add**. The user or group is added to the **Members** list.
6. When the member list is complete, click **Next**.

7. To make a user a team leader, select the name and click **Add** to move it to the leaders column. You cannot grant team leader permissions to groups.
8. When the **Leaders** list and leader permissions are configured, click **Next**. The **Team Definition** page appears, listing the team name, members, and leaders (with their permissions).
9. Click **Save** to save your changes, or click **Back** to return to the previous screen and edit the team before saving it.

### Deleting a Team

The Global Team cannot be deleted.

Company settings determine if other teams can be deleted, and if so, by whom. A user can only delete teams for which they have been granted the necessary permissions.

When a team is deleted, the following actions occur:

- All notifications and incidents are canceled, assigned to the Global Team, and then placed in the Global Team archive.
- All associated notification templates are deleted.
- All team-specific groups are deleted.
- All sub-teams are deleted.
- All leader-specific permissions for leaders of the team are revoked; however, any permissions granted to the leaders on other teams remain in effect.

NOTE

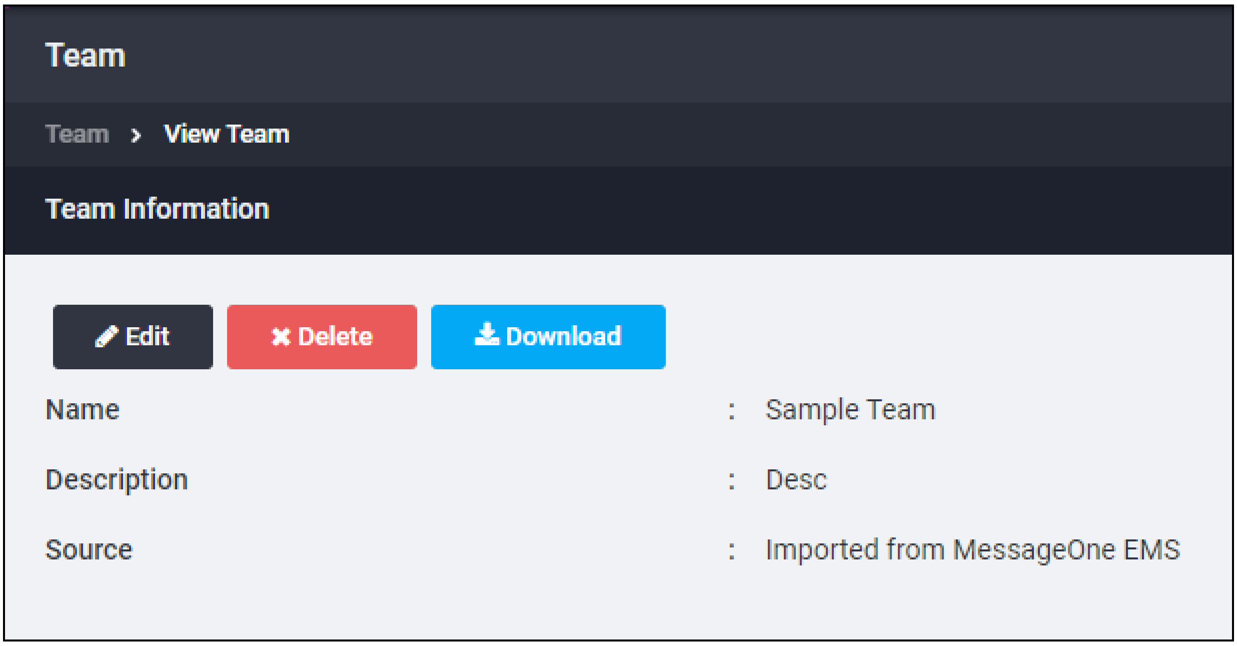
A team that has archived notifications cannot be deleted. All notifications must first be unarchived and then delete the team.

To delete a team:

CAUTION

When a team is deleted, it cannot be recovered. The team will have to be recreated, if it is needed again later.

1. From the left navigation menu **Administration** section, click **Teams**.
2. Navigate to the team to be deleted and click the team name.
3. If you have the necessary permissions to delete this team, a **Delete** button appears in the **Team Information** section at the top of the page.



Team Information

| | | |
|---|---|---|
| Name | : | Sample Team |
| Description | : | Desc |
| Source | : | Imported from MessageOne EMS |

4. Click **Delete**. A confirmation page appears.
5. Click **Yes** to delete the team or **No** to cancel the action.

If you click **Yes**, the **Teams** page is refreshed and the team is no longer listed.

## Team Reports

This section describes the following:

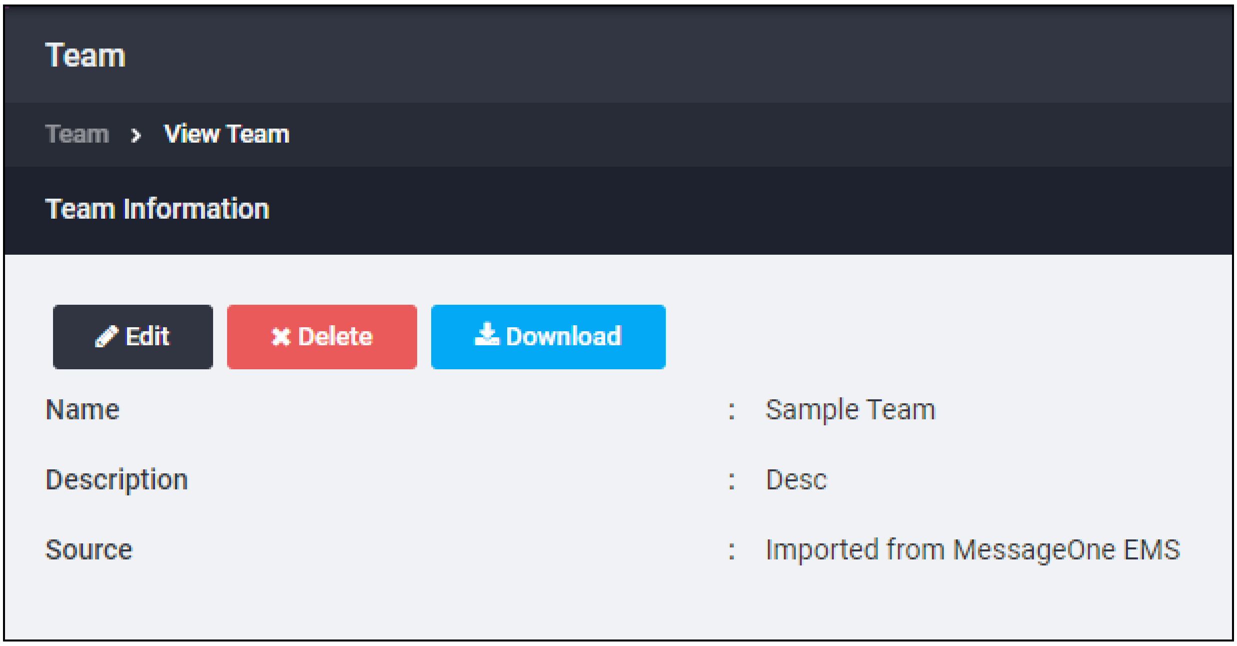
- Global Team Report (CSV)
- My Teams List (CSV)
- Specific Team Reports (CSV)

## Global Team Report (CSV)

If a user has the necessary permissions on the Global Team, they can download a CSV file containing information about the Global Team.

To download the Global Team report:

1. From the left navigation menu **Administration** section, click **Teams**.
2. From the list of teams, click **Global**.
3. On the **Team Information** page, click **Download**. A file dialog box appears.



| | | |
|---|---|---|
| Name | : | Sample Team |
| Description | : | Desc |
| Source | : | Imported from MessageOne EMS |

4. Open or save the file. By default, this file is called `Global.csv`.

Follow the dialog box instructions to save or open the file.

The Global Team report contains the following information:

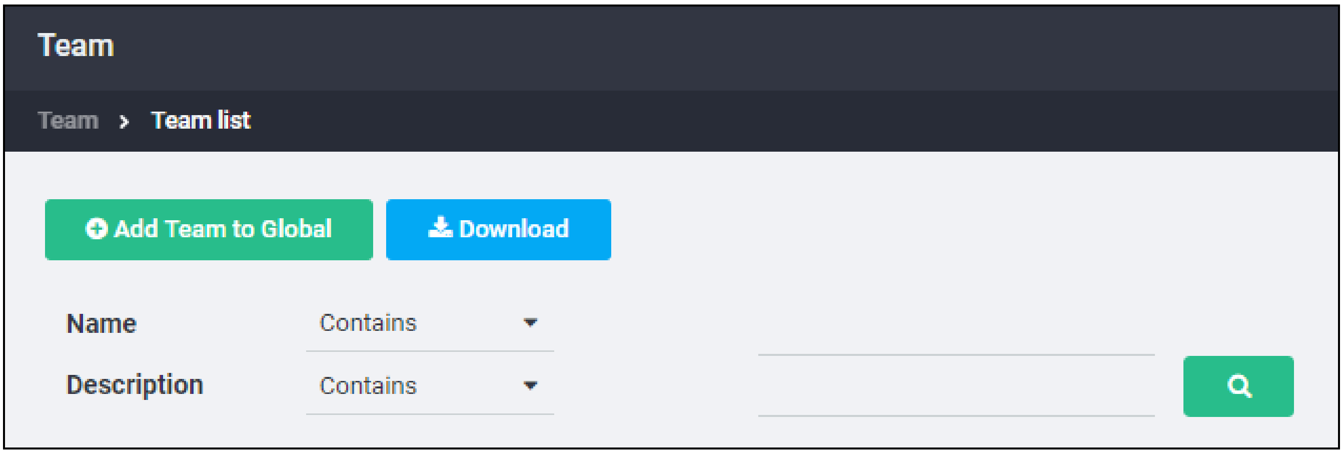
- A list of team members and whether they are enabled or disabled.
- A list of team leaders, whether they are enabled or disabled, and a list of their team permissions.
- A list of all sub-teams.

### My Teams List (CSV)

From the **My Teams** list, a CSV report that lists all your teams can be download.

To download a list of all your teams:

1. From the left navigation menu **Administration** section, click **Teams**.
2. On the **My Teams** page, click **Download**. A file dialog box appears.



3. Choose to open or save the file.

By default, this file is called `AlertFind Teams.csv`. Follow the dialog box instructions to save or open the file.

### Specific Team Reports (CSV)

If a user has the necessary permissions on a team, they can download a CSV file containing information about the team.

To download a team report:

1. From the left navigation menu **Administration** section, click **Teams**. The **My Teams** page appears.
2. Select the desired team. The **Team** page appears.
3. In the **Team Information** section of the **Teams** page, click **Download**. A file dialog box appears.
4. Choose to open or save the file. By default, this file is called `[team].csv`, where `[team]` is the name of the team. Follow the dialog box instructions to save or open the file.

The team report contains the following information:

- The name of the team.
- A list of team members and whether they are enabled or disabled.
- A list of team leaders, whether they are enabled or disabled, and a list of their team permissions.
- A list of all sub-teams.

# Groups

A group is a collection of users, or a combination of users and groups, to which notifications can be sent. Groups can be created before an incident, or while an incident is occurring.

The most common type of group is the Broadcast Group, which sends a notification simultaneously to all members of the group.

**NOTE**

- When adding a user to a group, the user becomes a member of every team that contains that group.
- If a user is a member of a team because he/she is a member of a group on that team, and he/she is later removed from the group, his/her team membership is also removed.
- If there is overlap when building groups that include a combination of users and groups, AlertFind sends the notification to each user only once.

Some examples of groups are:

- Regional or branch office personnel
- Information technology staff
- Executives
- Business continuity or disaster recovery unit
- Virus response group
- All employees

AlertFind administrators can view all groups. Team leaders can view groups specific to their team or teams, or any sub-teams of those teams.

## Group Quick Launch IDs

For companies with the Hotline or Hotline Pro feature enabled, Broadcast Groups and Escalation Groups can be assigned a Group Quick Launch ID. Administrators and team leaders with appropriate permissions can use their telephone to send Hotline announcement notifications to a group using its assigned Group Quick Launch ID.

A Group Quick Launch ID is a number that can be entered on the telephone keypad, and is assigned when the group is created. Group Quick launch IDs must consist of alphanumeric characters only. No spaces or punctuation are allowed.

### NOTE

Group Quick launch IDs and Incident Quick Launch IDs must be unique across all groups and notification templates.

To assign Quick Launch IDs, see Broadcast Groups and Escalation Groups.

To use Quick Launch IDs, see Using Quick Launch IDs and Using Quick Launch IDs with Hotline Pro

## Types of Groups

There are three types of groups: Broadcast Groups, Escalation Groups and Smart Groups. Ad Hoc Groups are a special type of Smart Group that are created when composing a notification.

- **Broadcast Groups** are groups of individuals or groups to which a notification is broadcast simultaneously.
- **Escalation Groups** differ in that notifications are sent to members of the group in a specified order. Escalation group information includes the order in which members should be contacted as well as any delay between attempts to contact members.
- **Smart Groups** are dynamic groups of users, based on criteria selected when the group is defined. As users change, they are automatically added to, or deleted from, Smart Groups based on each Smart Group’s defined criteria. Smart Groups can be used anywhere that Broadcast Groups can be used.

### Broadcast Groups

When a notification is sent to a Broadcast Group, it is simultaneously sent to every member of the group.

An unlimited number of Broadcast Groups can be created.

**NOTE**

Broadcast groups can contain other Broadcast Groups and Smart Groups. They cannot contain Escalation Groups.

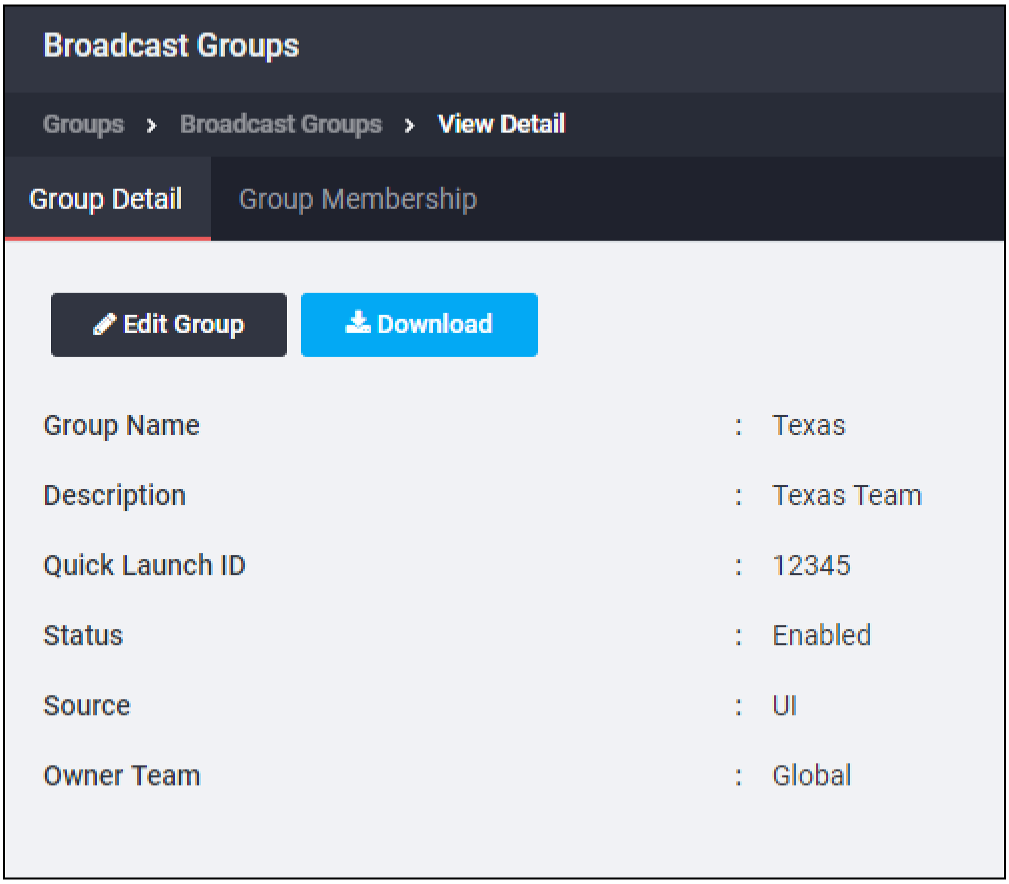
**NOTE**

If a notification does not require a response, AlertFind notifies the first device in each user’s personal escalation and considers the notification complete when it has been sent to this device.

For all notifications that require a response, AlertFind continues to notify members according to their personal escalation currently in effect, until the notification’s response is complete or is canceled.

To create a broadcast group:

1. Select the team context in which the group will be created.
2. From the left navigation menu **Groups** section, click **Broadcast Groups**.
3. Click the **New** button at the top of the page.
4. In the **Group Name** field, enter a name for this group. This is a required field. Group names must be unique within a group type.
5. In the **Description** field, enter an optional description of the group.
6. If a Group Quick Launch ID is to be used with for this group, type the code in the **Quick Launch ID** field. Group Quick Launch IDs are alphanumeric, with no spaces or punctuation allowed. If a letter is entered, AlertFind automatically converts it to a number that can be easily entered on a keypad. After the Broadcast Group is created, the number will be displayed after the Group Quick Launch ID. Alternatively click **Auto Generate Unique ID** to generate a random Quick Launch ID for this group.
7. Click **Save** to move to the **Group Membership** tab of the **Viewing Group** dialog box.



| | | |
|---|---|---|
| Group Name | : | Texas |
| Description | : | Texas Team |
| Quick Launch ID | : | 12345 |
| Status | : | Enabled |
| Source | : | UI |
| Owner Team | : | Global |

8. Click the **Manage Membership** button to bring up the **Group Membership Editor** dialog box.
9. In the **Users** tab, select the names of users to be added to this group. Use the search field provided to search by name or filter using the Criteria Editor. See Filtering Lists for instructions on using search and Criteria Editor tools.
10. Click **Add Selected** to move them to the **Members** list.
11. To add other groups to this broadcast group, click the **Broadcast Groups** or the **Smart Groups** tab. Select the groups to add and click **Add Selected** to move them to the **Members** list.
12. Click **Close** to finish adding members to the group.
13. Click **Close** to return to the **Broadcast Groups** page.

## Escalation Groups

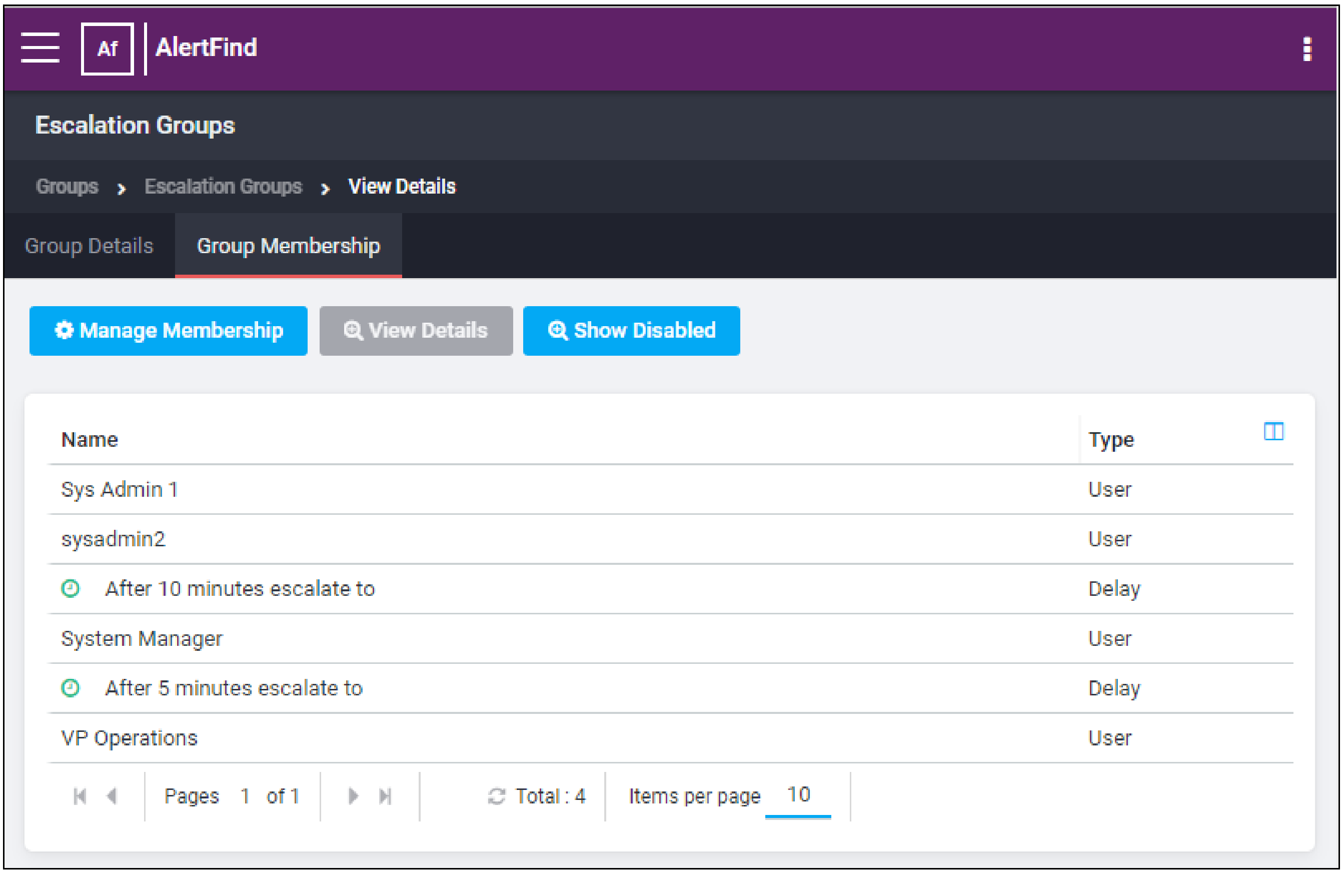
Escalation Groups are used to reach group members in a specified order. Escalation Group information includes the order in which members should be contacted as well as any delay between attempts to contact members.

Response limits control how many users can reply with a specific response. When the response limit is reached, that response is no longer available. Whether notifications continue after response limits are reached is defined by **Response Limit Handling** on the **Compose Notification Wizard**.

### Example: Notification Sent to an Escalation Group

Genericorp has a IT Response Team for which an Escalation Group exists. The team and group membership includes two system administrators, two system managers, and the Vice President of Operations. The process Genericorp has in place dictates that the system administrators be contacted immediately, the system managers be contacted 10 minutes later, and the Vice President be notified within 15 minutes of the incident. The following image shows how the escalation group set up would look.

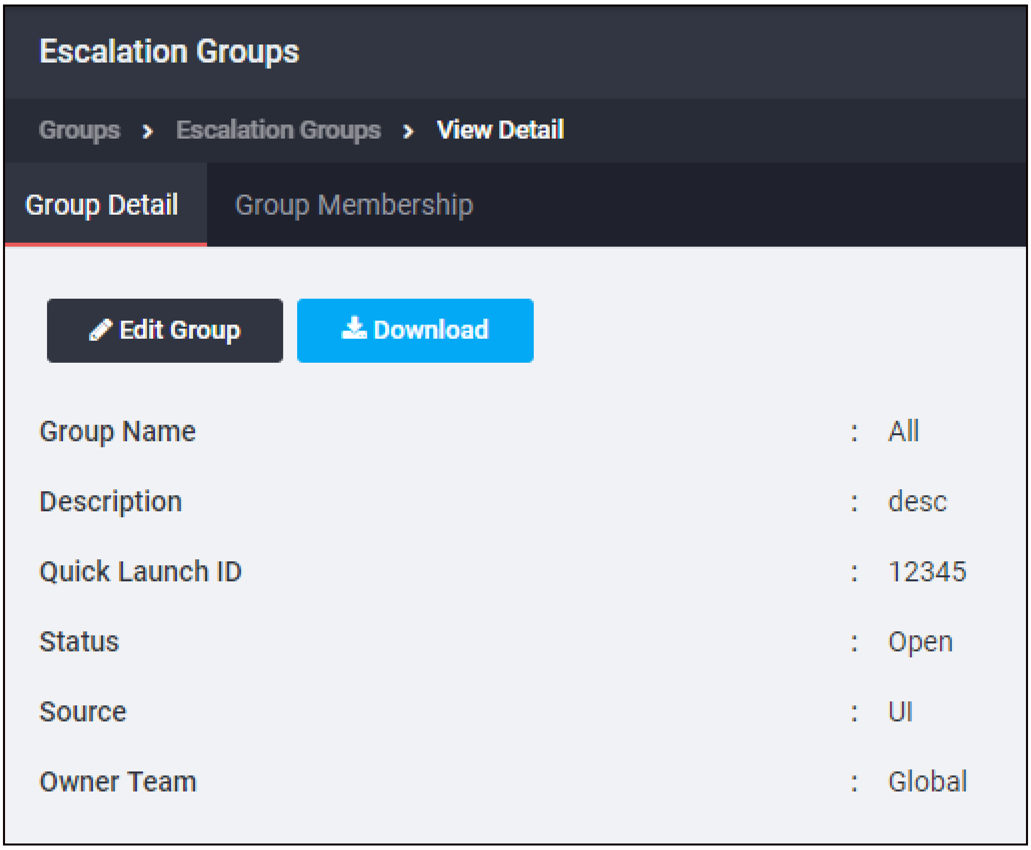
Based on this configuration, the two system administrators would be notified immediately, the system managers would be notified 10 minutes later, and the VP of Operations would be notified 5 minutes after the system managers (effectively, 15 minutes after the incident occurred).



| Name | Type |
|---|---|
| Sys Admin 1 | User |
| sysadmin2 | User |
| After 10 minutes escalate to | Delay |
| System Manager | User |
| After 5 minutes escalate to | Delay |
| VP Operations | User |

To create an escalation group:

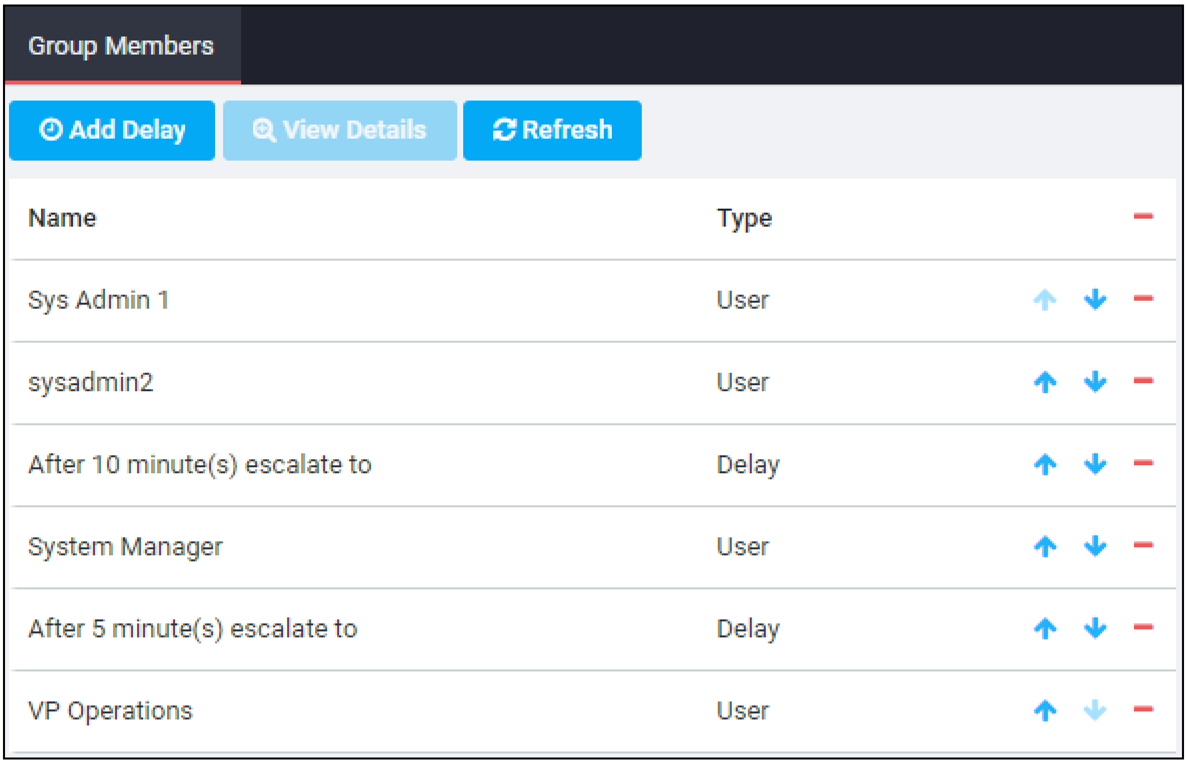
1. Select the team context in which the group will be created.
2. From the left navigation menu **Groups** section, click **Escalation Groups**.
3. Click the **New** button at the top of the page.
4. In the **Group Name** field, enter a name for this group. This is a required field. Group names must be unique within a group type.
5. In the **Description** field, enter an optional description of the group.
6. If a Group Quick Launch ID is to be used with for this group, type the code in the **Quick Launch ID** field. Group Quick Launch IDs are alphanumeric, with no spaces or punctuation allowed. If a letter is entered, AlertFind automatically converts it to a number that can be easily entered on a keypad. After the Escalation Group is created, the number will be displayed after the Group Quick Launch ID. Alternatively, click **Auto Generate Unique ID** to generate a random Quick Launch ID for this group.



|  |  |  |
|---|---|---|
| Group Name | : | All |
| Description | : | desc |
| Quick Launch ID | : | 12345 |
| Status | : | Open |
| Source | : | UI |
| Owner Team | : | Global |

7. Click **Save** to move to the **Group Membership** tab of the **Viewing Group** dialog box.
8. Click the **Manage Membership** button to bring up the **Group Membership Editor** dialog box.

9. In the **Users** tab, select the names of users to add to this group. Use the search fields provided to search by name or filter using the Criteria Editor. See Filtering Lists for instructions on using search and Criteria Editor tools.
10. Click **Add Selected** to move them to the **Members** list.
11. To add other groups to this broadcast group, click the **Broadcast Groups**, **Escalation Groups** or the **Smart Groups** tab. Select the groups to be added and click **Add Selected** to move them to the **Members** list.
12. To add a delay between notifications, select the name which the delay should be added *after*. Click **Add Delay**. Type a number in the **Delay (minutes)** box. Click **Save** to return to the **Group Membership Editor** dialog box.
13. Use the **Move Up** and **Move Down** buttons to change the escalation order, until all users, groups and delays are in the desired order.



| Name | Type | − |
|---|---|---|
| Sys Admin 1 | User | ↑ ↓ − |
| sysadmin2 | User | ↑ ↓ − |
| After 10 minute(s) escalate to | Delay | ↑ ↓ − |
| System Manager | User | ↑ ↓ − |
| After 5 minute(s) escalate to | Delay | ↑ ↓ − |
| VP Operations | User | ↑ ↓ − |

14. Click **Save** to create the group.
15. Click **Close** to return to the **Escalation Groups** page.

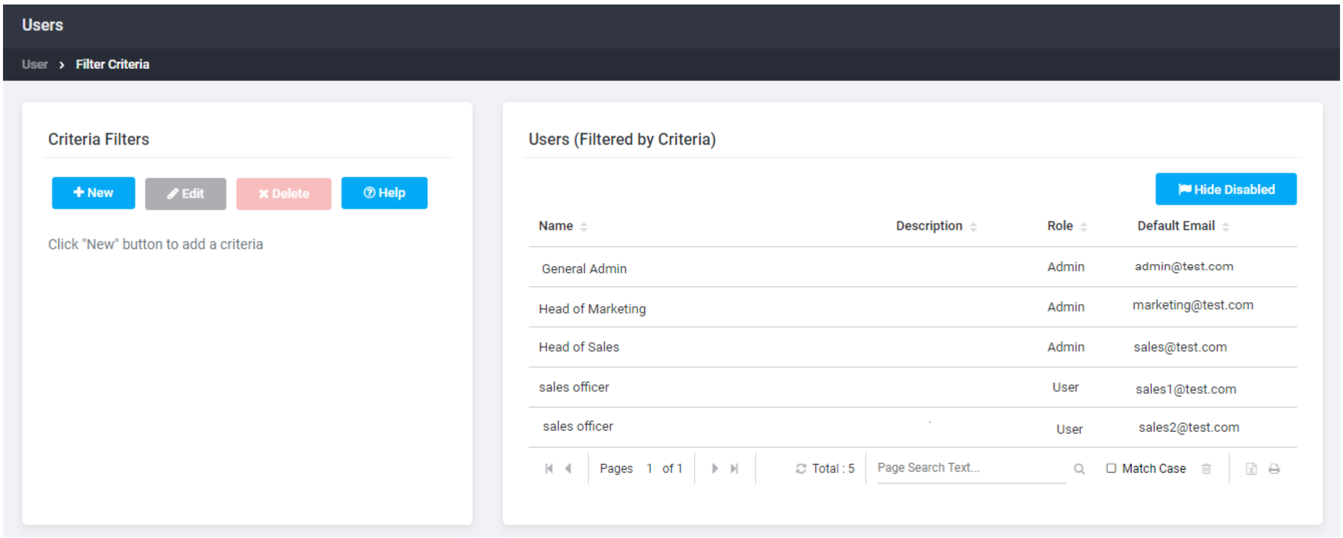
## Smart Groups

Smart Groups are dynamic groups of users based on the criteria selected when defining the group. The members of a Smart Group automatically change as users change based on the criteria selected to build the group.

For example, if a Smart Group has been created for users whose department is `IT`, any new users imported with the property `Department` and the value `IT` are automatically added to the Smart Group, users no longer in that department are deleted from the group.

To create a Smart Group:

1. Select the team context in which the group will be created.
2. From the left navigation menu **Groups** section, click **Smart Groups**.
3. Click the **New** button at the top of the page. The **Create Group Details** dialog box appears.
4. In the **Group Name** field, enter a name for this group. This is a required field. Group names must be unique within a group type.
5. In the **Description** field, enter an optional description of the group.
6. Click the **Edit Criteria** button to bring up the **Criteria Editor** dialog box.
7. Click the **New** button to create a new criteria that will be used to define the group. See Using the Criteria Editor for instructions on using search and Criteria Editor tools.



Click "New" button to add a criteria

| Name | Description | Role | Default Email |
|---|---|---|---|
| General Admin | | Admin | admin@test.com |
| Head of Marketing | | Admin | marketing@test.com |
| Head of Sales | | Admin | sales@test.com |
| sales officer | | User | sales1@test.com |
| sales officer | | User | sales2@test.com |

8. After the criteria have been created and verified, click **Save**. The **Viewing Group** dialog box appears and displays the new Smart Group.
9. Click **Close** to return to the **Smart Groups** page.

### Ad Hoc Groups

An Ad Hoc Group is automatically created when composing a notification. Its membership is composed of users who meet the selected criteria. In this way, they are similar to Smart Groups.

One advantage of Ad Hoc Groups is that they can be used to send a notification to a set of users who meet the criteria at the time the notification is sent. For example, if the notification is scheduled to be sent in three days, users who meet the criteria in three days will receive it. This means the recipient list does not have to be manually updated –the Ad Hoc Group manages the recipient list.

Another advantage of Ad Hoc Groups is that they are built using the *contains* constraint, which enables the use of a key word to build the Ad Hoc Group. For example, to send a notification to all managers regardless of the department they manage, enter a value of `manager` for the property **title**. The *contains* constraint would create a Ad Hoc Group containing everyone with the word `manager` in their title.

Administrators or team leaders who have Manage Groups (MG) permission can create Ad Hoc Groups.

**NOTE**

Ad Hoc Groups do not have names because they are created during the Compose Notification process.

If a notification template includes an Ad Hoc Group, the notification is only sent to users who meet the criteria for inclusion in the Ad Hoc Group at the time the notification is sent.

For more information about how to create Ad Hoc Groups, see Smart Groups.

## Managing Groups

This section describes how to locate, view, and manage a group. Administrators of AlertFind can also edit, enable and disable groups accordingly.

Topics in this section:

### Locate a Group

#### NOTE

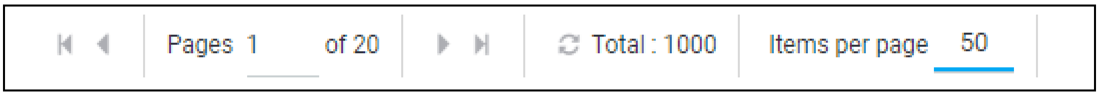
By default, only enabled groups are displayed. To view all groups, including disabled groups, click **Show Disabled** on the menu bar.

To locate a group

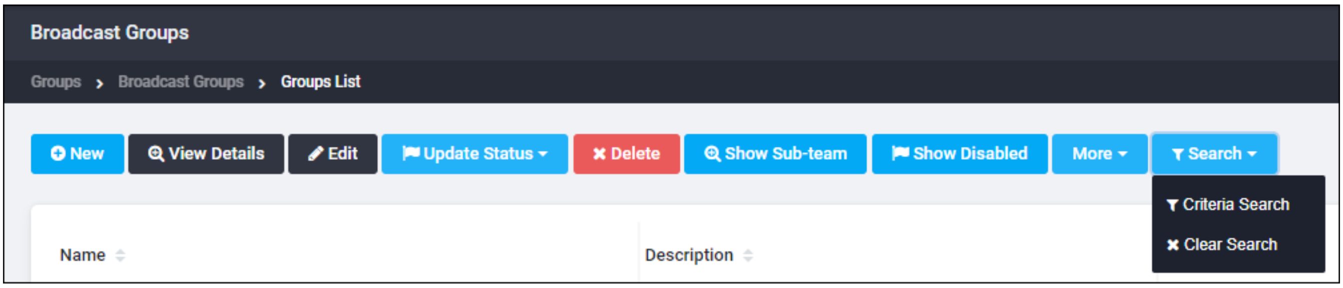
1. Select the team context.
2. From the left navigation menu **Groups** section, click the button for the type of your group you are looking for.

There are three ways to locate a group:

- Find the name by scrolling through the list of group names for that type of group and by using the **First**, **Previous**, **Next** and **Last** buttons.



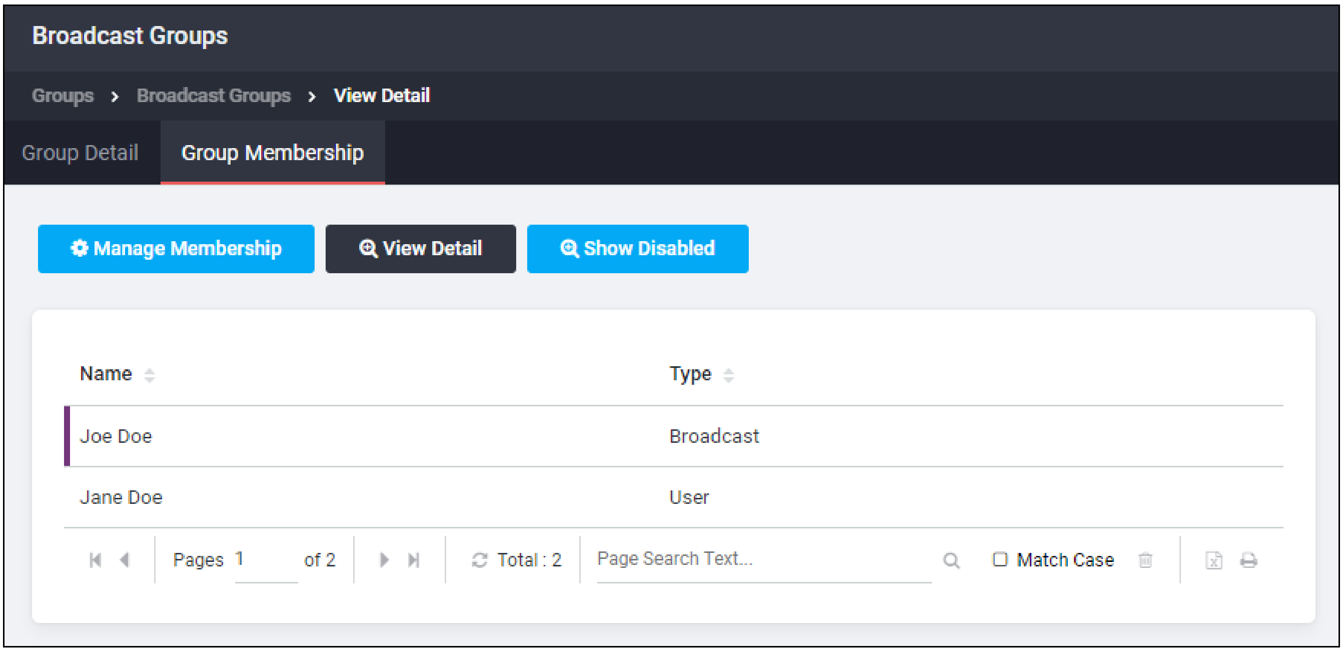
- To run a simple search, enter the first few letters of a group’s name into the Search box, then click Search 🔍.
- To create a custom search, click the **Search** drop-down and select **Criteria Search**. See Using the Criteria Editor.



## Viewing Group Members

To view group membership

1. Select the team context.
2. In the left navigation menu **Groups** section, click the button for the group type (*Broadcast Groups*, *Escalation Groups*, or *Smart Groups*).
3. In the list of groups, select the desired group and click the **View Details** button to bring up the **Viewing Group** page.
4. In the **Viewing Group** window, click the **Group Membership** tab to view a list of members for the selected group.



| Name | Type |
|---|---|
| Joe Doe | Broadcast |
| Jane Doe | User |

### Managing Group Membership

#### CAUTION

Discuss change precedence settings with Support to retain changes made to groups and ensure changes are not overwritten with the next roster import.

To add or remove group membership:

1. Select the team context.
2. In the left navigation menu **Groups** section, click the button for the group type (*Broadcast Groups*, *Escalation Groups*, or *Smart Groups*).
3. In the list of groups, select the desired group and click the **View Details** button, to bring up the **Viewing Group** page.
4. Click the **Group Membership** tab.
5. In the tool bar, click **Manage Membership**.

- **To add** a new user or group:
    1. In the **Group Membership Editor** dialog box, click the tab for the user or group to be added.
    2. Select the new user(s) or group(s) and click **Add Selected** to move the entry to the right-hand **Members** pane.
    3. Repeat as needed to add all users or groups.
    4. When all users or groups have been added, click **Close**.
- **To remove** a user or group:
    1. In the **Members** pane of the Group Membership Editor dialog box, select the user(s) or group(s) to be removed, and click the **Delete** button.
    2. In the *Delete Selected* verification dialog box, click **OK**.
    3. Repeat as needed to remove users or groups.
    4. When finished, click **Close**.

### Editing Groups

#### CAUTION

Discuss change precedence settings with Support to retain changes made to groups and ensure changes are not overwritten with the next roster import.

To edit groups:

1. Select the team context.
2. Select the desired group. The **Viewing Group** dialog box appears.

#### NOTE

By default, only enabled groups are displayed. To view all groups, including disabled groups, click **Show Disabled** on the menu bar.

3. Click the **Edit Group** button. This displays the **Edit Group Details** dialog box.
4. Change the `Group Name`, `Description` or `Quick Launch ID` as needed. The fields are described in detail in the Creating Groups sections. See Broadcast Groups, Escalation Groups and Smart Groups.
5. Click **Save**.

### Disabling a Group

To make a group unavailable for notifications, disable it. To disable a group:

1. Select the team context.
2. In the left navigation menu **Groups** section, select the group type (*Broadcast Groups*, *Escalation Groups*, or *Smart Groups*).
3. Select the group name.
4. In the tool bar, select **Update Status** > **Disable Group**. The group is no longer displayed in the list of available groups.

View disabled groups by clicking **Show Disabled** at the top of the **Broadcast Groups**, **Escalation Groups** or **Smart Groups** page. Disabled groups are shown with the word 'disabled' within parentheses beside the name.

Click **Show Disabled** a second time to hide the disabled groups.

### Enabling a Disabled Group

To enable a disabled group:

1. Select the team context.
2. In the left navigation menu **Groups** section, select the group type (*Broadcast Groups*, *Escalation Groups*, or *Smart Groups*).
3. View disabled groups by clicking **Show Disabled** button. Disabled groups are shown with the word **disabled** within parentheses beside the group name.
4. Click the desired group name to select the group.
5. Select **Update Status** > **Enable Group**.

The group name now appears without the word **disabled** in parentheses on the **Broadcast Group**, **Escalation Group**, or **Smart Group** page.

# Sites

The **Sites** feature allows the definition of geographic-based assets, such as `Main Campus`, `Building 7`, or `Oil Rig 1`. Groups of users can then be associated with each of these Sites. Once a Site is created and Group(s) associated with it, when a geographic area is selected for a Notification in the *Map Selector* tab all the Sites located within the geographic area selected will be included in the Notification's recipients.

## Administering Sites

Administrators can:

- Manage all sites on all teams.
- Within a team context, associate any group to a site.
- Designate any site as *Shared with Global*.

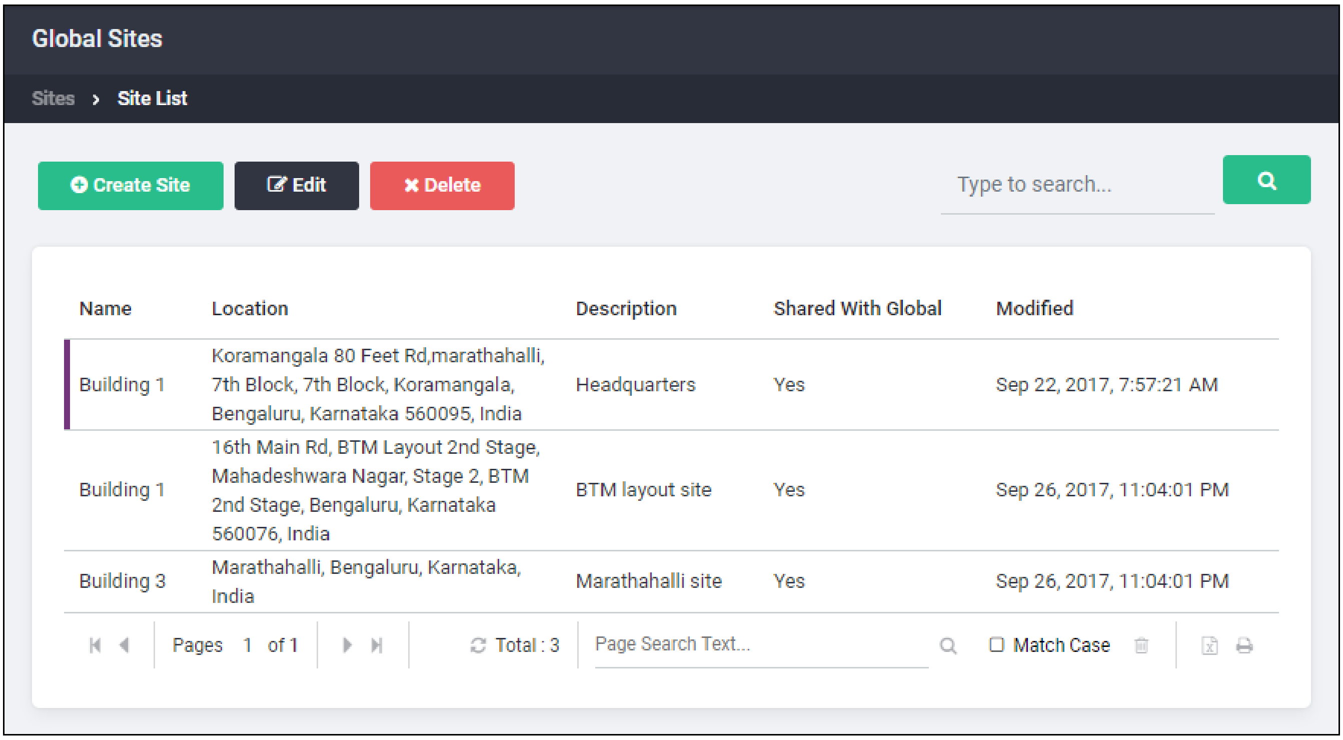
Team Leaders can:

- Manage sites only for their direct team(s).
- Associate only groups that belong to their direct team(s).

## View List of Sites

To view a list of sites:

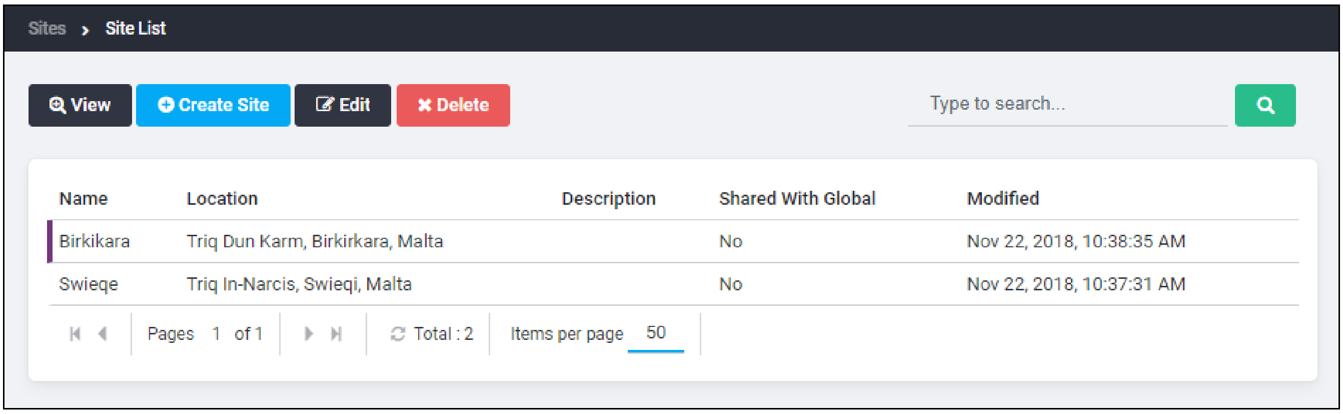
1. Select the team context to view the list of sites available to that team. See Team Security Context
2. In the left navigation menu under the **Assets** section, click **Sites**.
3. If you are in the Global team security context, the **Sites** page displays all sites that belong to the Global team, including sites that have been designated to be *Shared with Global*.



| Name | Location | Description | Shared With Global | Modified |
|---|---|---|---|---|
| Building 1 | Koramangala 80 Feet Rd,marathahalli, 7th Block, 7th Block, Koramangala, Bengaluru, Karnataka 560095, India | Headquarters | Yes | Sep 22, 2017, 7:57:21 AM |
| Building 1 | 16th Main Rd, BTM Layout 2nd Stage, Mahadeshwara Nagar, Stage 2, BTM 2nd Stage, Bengaluru, Karnataka 560076, India | BTM layout site | Yes | Sep 26, 2017, 11:04:01 PM |
| Building 3 | Marathahalli, Bengaluru, Karnataka, India | Marathahalli site | Yes | Sep 26, 2017, 11:04:01 PM |

To view sites belonging to a certain team and if those sites haven't been *Shared with Global*, switch to the appropriate team security context and click **Sites** again.

If you selected a Team security context other than Global, the **Sites** page will display all sites that belong to the current team and have **not** been designated to be *Shared with Global*.



| Name | Location | Description | Shared With Global | Modified |
|---|---|---|---|---|
| Birkikara | Triq Dun Karm, Birkirkara, Malta | | No | Nov 22, 2018, 10:38:35 AM |
| Swieqe | Triq In-Narcis, Swieqi, Malta | | No | Nov 22, 2018, 10:37:31 AM |

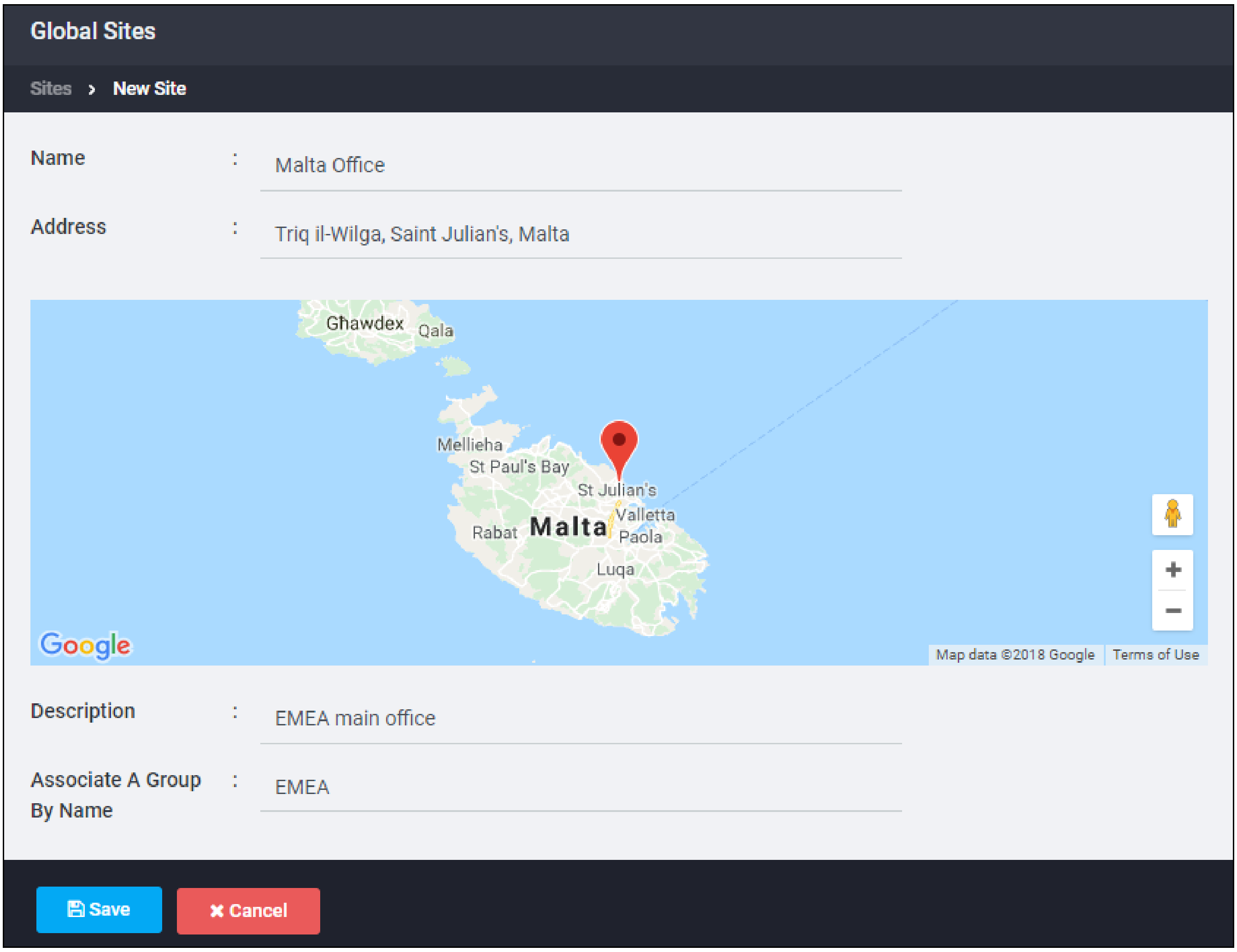
- To see all the sites that have been Shared with Global, including all of this team’s sites that have been shared, click **Global** on the team security context.
- To return to this page from the **Site List** page, select a different team in the team security context. Sites are listed in the order they were created, with the newest site appearing last.

5. Click the **Previous** and **Next** button to navigate to further pages. The **Search** function is a keyword search of the `Site Name` field.
6. To view the details of an individual Site, click on the Site name.

## Create A Site

To create a site:

1. Select the team context to which you want to add the new Site. See Team Security Context.
2. In the left navigation menu under the **Assets** section, click **Sites**.
3. Click on the **Create Site** button. This brings up the Create Site page.



Name : Malta Office

Address : Triq il-Wilga, Saint Julian's, Malta

Description : EMEA main office

Associate A Group By Name : EMEA

4. Enter the Name of the Site into the **Name** field.

Site names must be unique. If the system gives you an error message when you enter the Site name, it means that another Team is using that Site name, so you will need to choose a different Site name.

5. Type an address into the **Address** field. As you type, Google will match what you type with known addresses.

Alternately, click the **Specify location using map** link. The Google map page comes up. Locate the desired region on the map. Click on the location marker icon, 📍, and click on the map to place the location. To move the icon, click on the hand icon, ✋, then click-and-hold on the location marker and move it to the correct location. Click **Done** when completed.

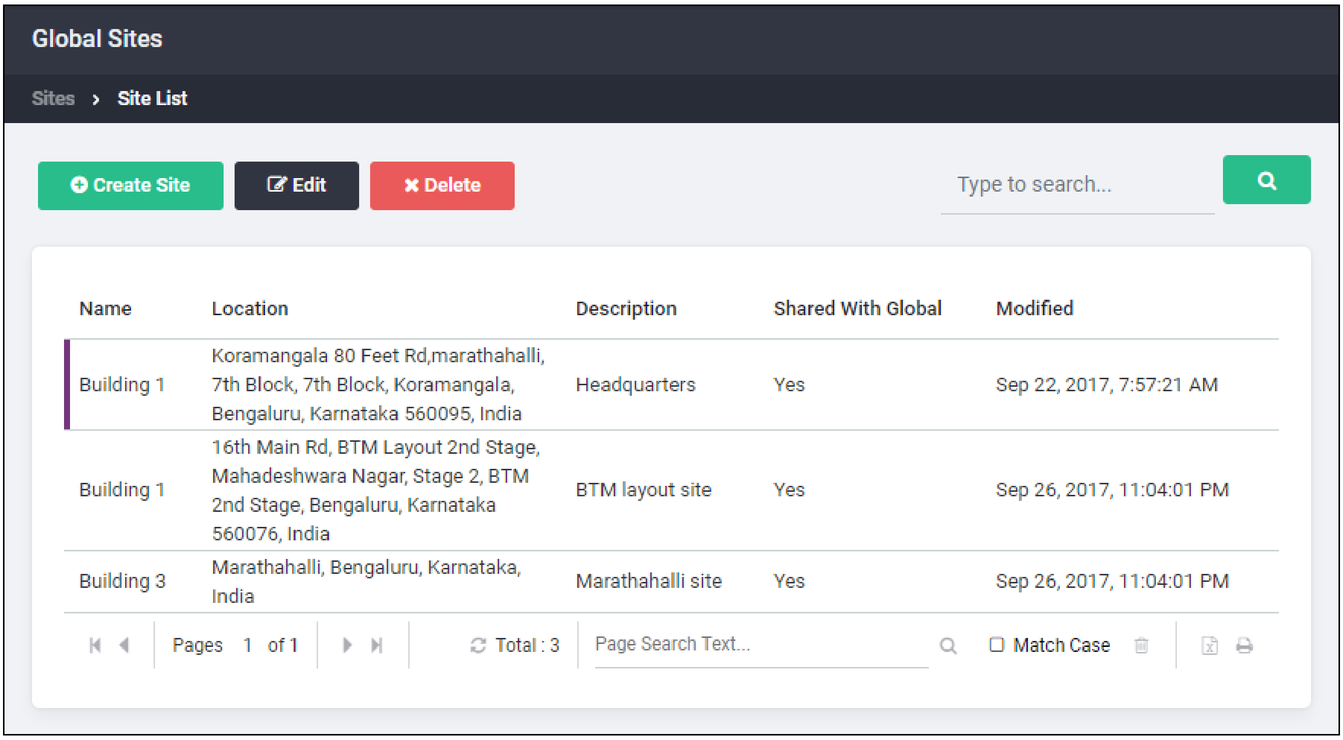
6. (Optional) Enter a Description.
7. (Optional) To associate a group with this Site, begin to type the name of the group. The system will list matches, click on the desired Group. Repeat to add more Groups. Groups can also be added later.
8. Click the **Save** button to save the Site. A success confirmation pane appears
9. Click **OK**.

## Edit A Site

Administrators may have to switch to a specific team context to administer Sites not *Shared with Global*.

To edit a site:

1. Select the team context to which you want to add the new Site. See Team Security Context.
2. In the left navigation menu under the **Assets** section, click the **Sites** link.
3. Locate the Site to be edited. Sites are listed in alphabetical order. Use **Previous** and **Next** button to navigate to further pages. The **Search** function is a keyword search of the `Site Name` field.
4. Click **Edit**.



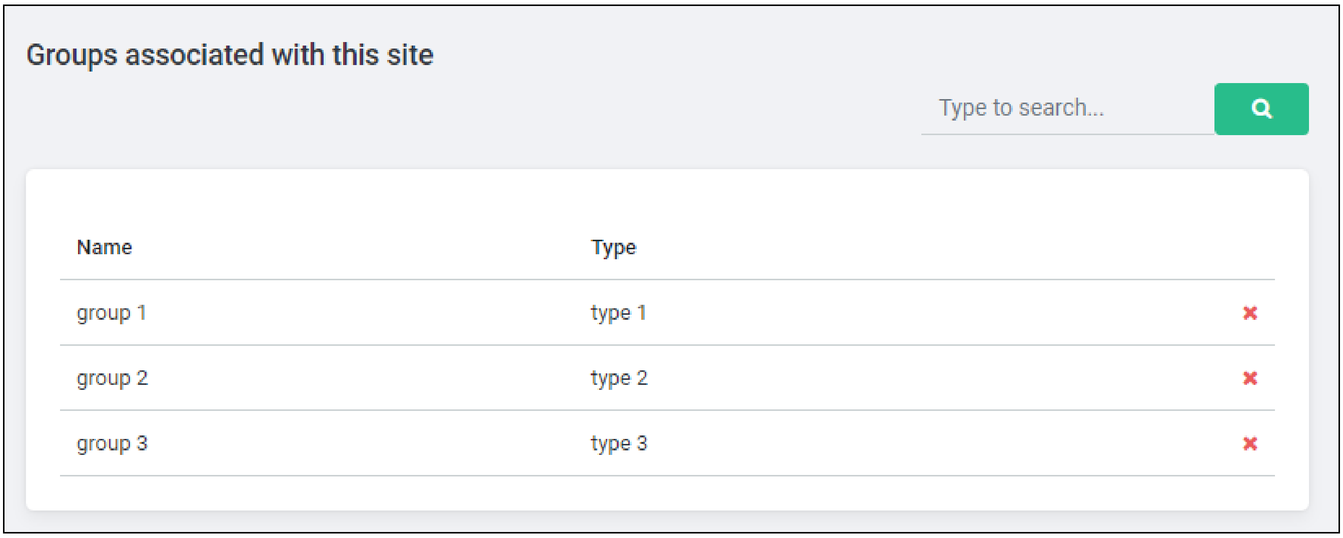
| Name | Location | Description | Shared With Global | Modified |
|---|---|---|---|---|
| Building 1 | Koramangala 80 Feet Rd,marathahalli, 7th Block, 7th Block, Koramangala, Bengaluru, Karnataka 560095, India | Headquarters | Yes | Sep 22, 2017, 7:57:21 AM |
| Building 1 | 16th Main Rd, BTM Layout 2nd Stage, Mahadeshwara Nagar, Stage 2, BTM 2nd Stage, Bengaluru, Karnataka 560076, India | BTM layout site | Yes | Sep 26, 2017, 11:04:01 PM |
| Building 3 | Marathahalli, Bengaluru, Karnataka, India | Marathahalli site | Yes | Sep 26, 2017, 11:04:01 PM |

5. Edit information as needed.
6. When done, click the **Save** button. A success confirmation pane appears.
7. Click the **OK** button.
8. To associate Groups with this site, click the **Associate more groups** button.
9. In the **Associate a group by name** text field, type in the beginning of the group name. As you type, the system will list matches. Select the desired Group.
10. Repeat typing more characters in the text box to associate more Groups.
11. Click the **Associate** button when all the desired Groups are listed.

### Delete A Site

To delete a site:

1. Select the team context to which you want to add the new Site. See Team Security Context
2. In the left navigation menu under the **Assets** section, click the **Sites** link.
3. Locate the Site to be deleted.
    - Sites are listed in alphabetical order. Click the **Previous** and **Next** button to navigate to further pages.
    - The **Search** function is a keyword search of the `Site Name` field.
4. Go to the Site details page by clicking on the Site name.
5. If there are any Groups associated with this Site, remove the groups from the list. To do this, hover your mouse over the row of the Group to be removed.

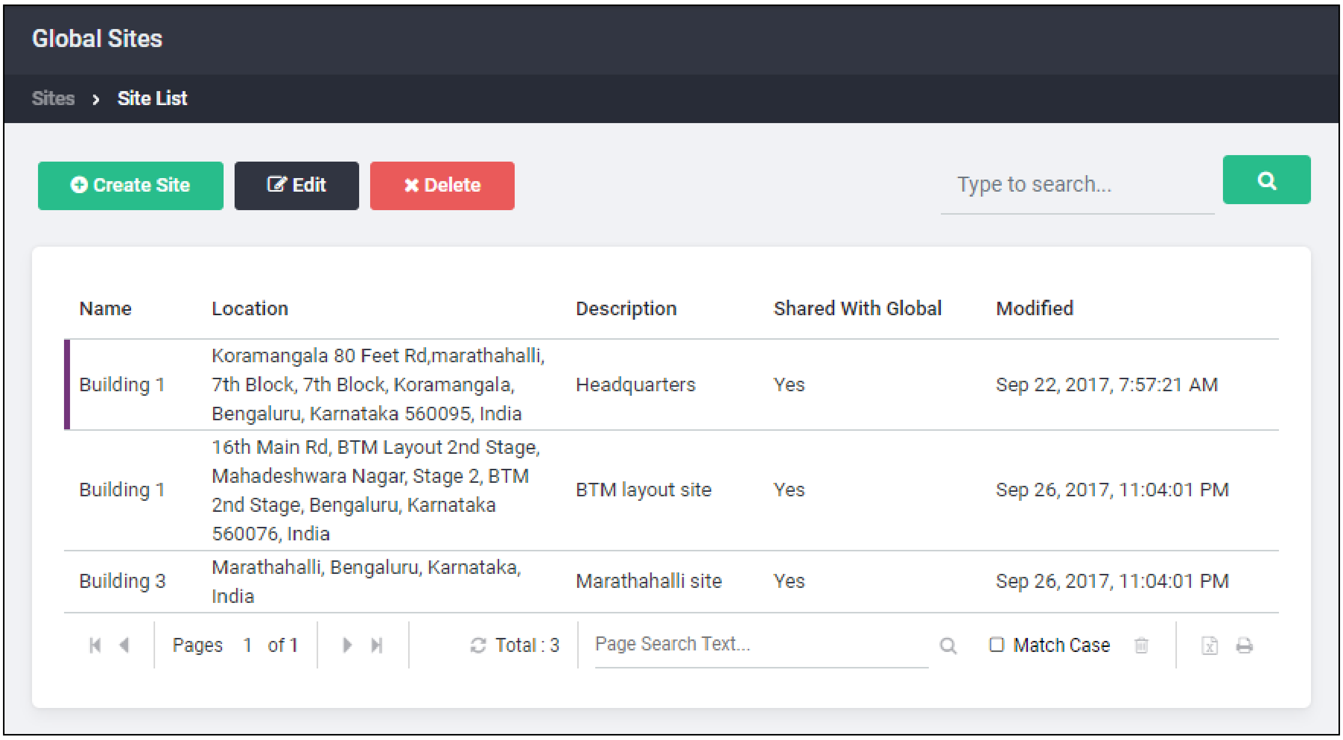


Groups associated with this site

| Name | Type | |
|---|---|---|
| group 1 | type 1 | ✖ |
| group 2 | type 2 | ✖ |
| group 3 | type 3 | ✖ |

When the **X** appears, click on it. When the confirmation pane appears, click on the **Confirm** button.

6. When all the Groups have been disassociated, return to the main Sites page.
7. Select the site and click **Delete**.



| Name | Location | Description | Shared With Global | Modified |
|---|---|---|---|---|
| Building 1 | Koramangala 80 Feet Rd,marathahalli, 7th Block, 7th Block, Koramangala, Bengaluru, Karnataka 560095, India | Headquarters | Yes | Sep 22, 2017, 7:57:21 AM |
| Building 1 | 16th Main Rd, BTM Layout 2nd Stage, Mahadeshwara Nagar, Stage 2, BTM 2nd Stage, Bengaluru, Karnataka 560076, India | BTM layout site | Yes | Sep 26, 2017, 11:04:01 PM |
| Building 3 | Marathahalli, Bengaluru, Karnataka, India | Marathahalli site | Yes | Sep 26, 2017, 11:04:01 PM |

8. Click **Yes** in the next screen to confirm the deletion.

## Using Sites

Sites are available to be used in **Quick Compose** on the Alert Console, and on the AlertFind Administration pages, **Compose (Advanced)** in the left-hand navigation menu, and the **Notification Editor**.

In the **Notification Editor**/**Composed (Advanced)** Recipient Editor pane, Sites are selected using the **Map Selector** tab. When a polygon is drawn, all users of the selected Team Context are included in the Groups associated with the Sites whose location is within the polygon, are included as recipients of the Notification. See Use the Recipient Editor for more information.

When using **Quick Compose** on the Alert Console, click the geographic location icon, 📍, and draw polygon(s) surrounding the location of the notification's recipients. All users who are part of the selected Team Context and included in the Groups associated with the Sites located within the defined polygon(s), will be included as recipients to the notification. The bottom right of the pane will display the number of sites included within the polygon(s). See Recipient Editor for more information.

# SmartContact

SmartContact is an administrative function added to AlertFind. SmartContact discovers missing contact information and automatically run a workflow to capture and update the related contact information.

SmartContact allows an organization to start the initial setup and configuration. The process consists of the following tasks:

- Selecting and adding people and/or groups
- Drafting messages
- Scheduling messages

Once configured, SmartContact runs in the background autonomously and keeps sending follow-ups to people requesting them to provide missing contact information, eventually to be updated in the AlertFind contacts.

SmartContact helps your organization by providing the following services:

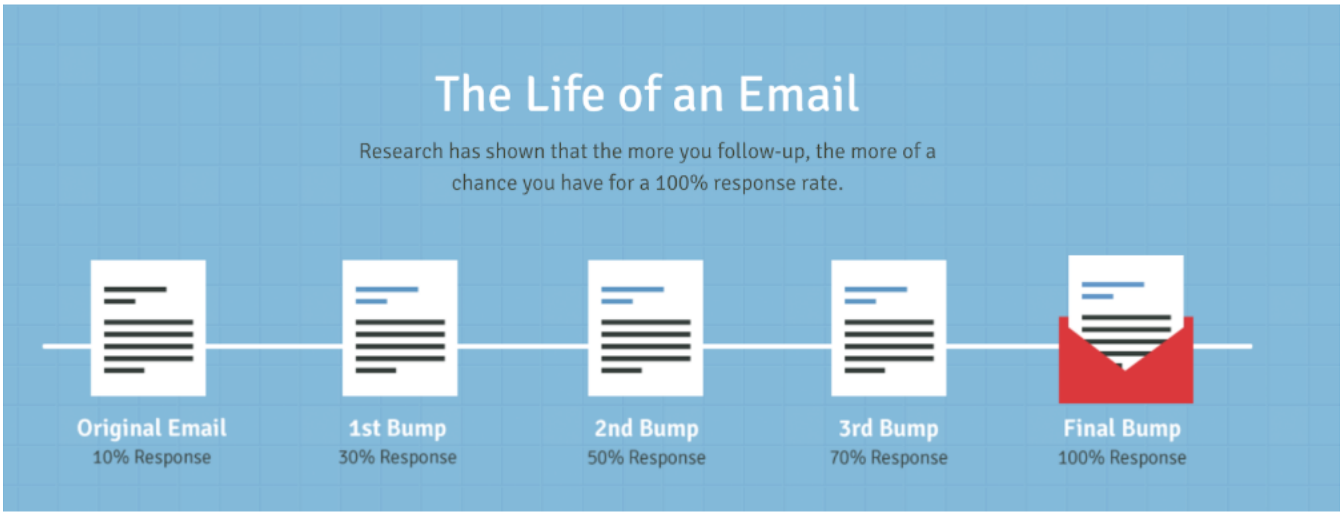
- Scanning existing AlertFind database to shortlist people with missing contact information.
- Providing manual and automated data import options to organizations for easy configuration.
- Reporting via dashboard with a health-checkup to provide a report on the percentage of data filled for selected fields.

### Follow up emails

Once configured, SmartContact sends an initial email requesting the recipient provide missing contact information. SmartContact monitors the email thread. When there is no response, it automatically sends follow up emails.

The default thread consists of the following emails:

- Original email
- First bump emails
- Second bump email
- Third bump email
- Final bump email



On the configuration page, administrators can also choose the number of days between bump emails. By default, this is set to two business days between each bump email.

Topics in this section:

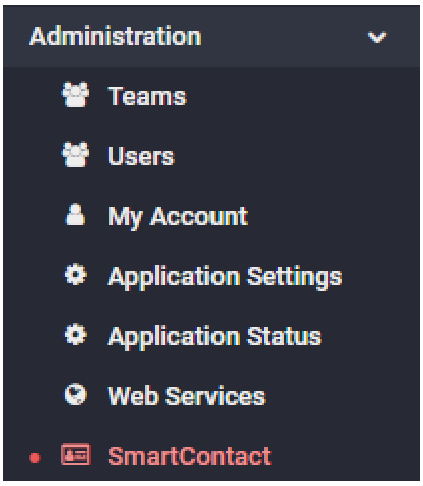
## Initial Setup

SmartContact discovers missing contact information and automatically run a workflow to capture and update the contact information.

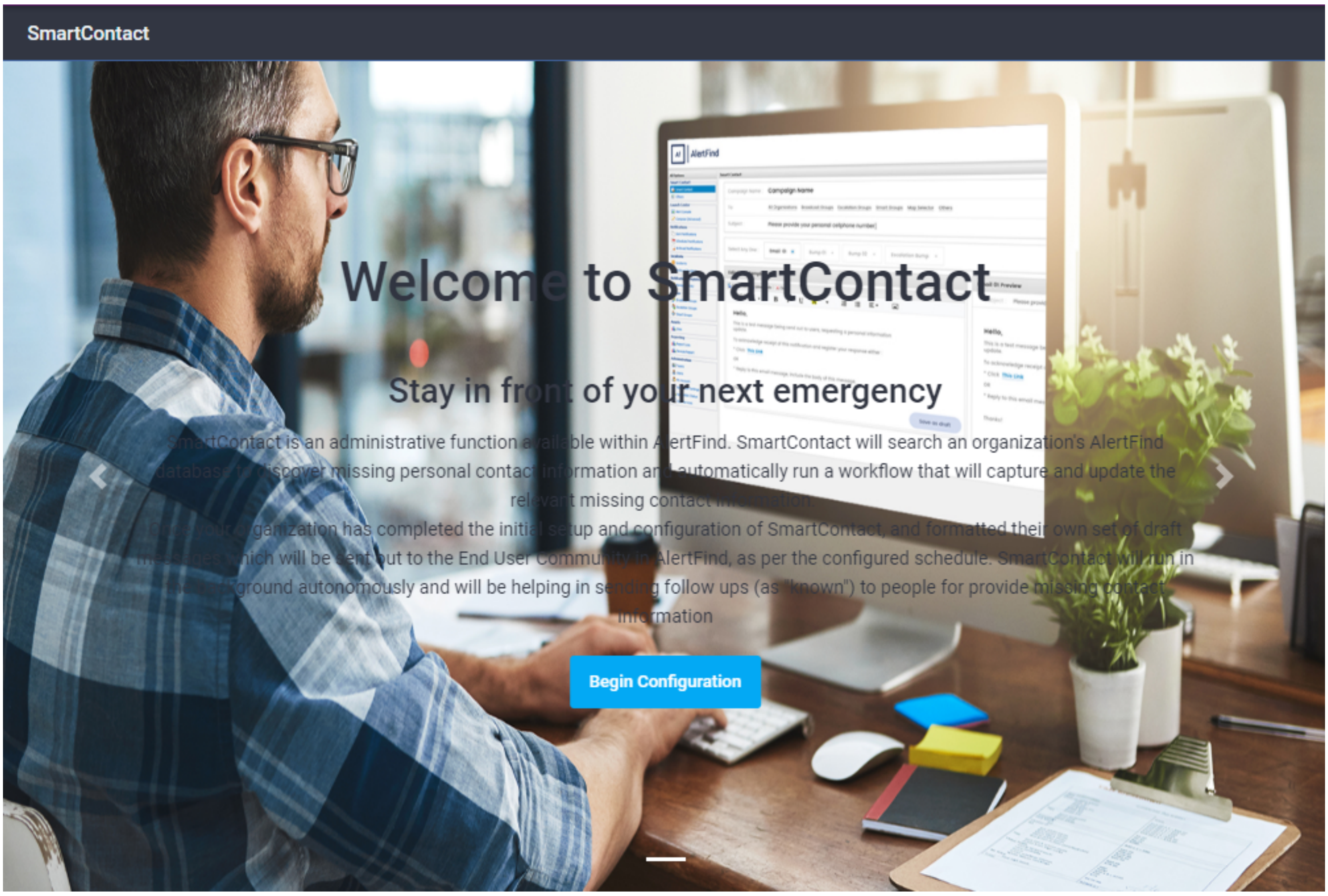
SmartContact can be configured during the initial setup of the system and will run in the background, autonomously at all times.

To start the initial setup:

1. Log in to AlertFind.
2. Go to **Administration > SmartContact**.



The SmartContact link initiates a new configuration landing page.



Welcome to SmartContact

Stay in front of your next emergency

SmartContact is an administrative function available within AlertFind. SmartContact will search an organization's AlertFind database to discover missing personal contact information and automatically run a workflow that will capture and update the relevant missing contact information.

Once your organization has completed the initial setup and configuration of SmartContact, and formatted their own set of draft messages which will be sent out to the End User Community in AlertFind, as per the configured schedule. SmartContact will run in the background autonomously and will be helping in sending follow ups (as "known") to people for provide missing contact information

This page contains two links:

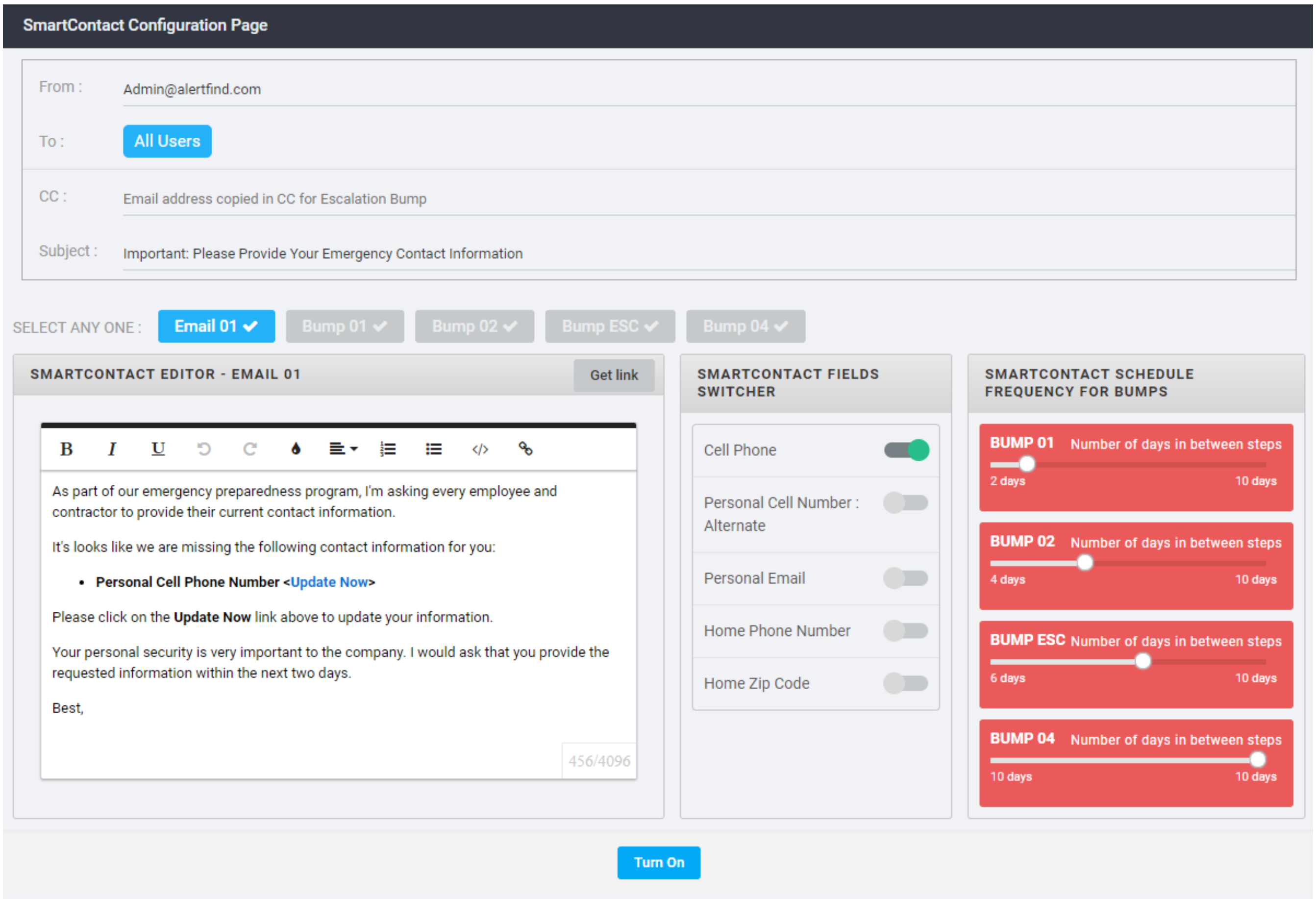
- Configuration
- Health Monitor

## Configuration

On the configuration page, administrators are able to configure the list of recipients to monitor and run against. By default, Smart Contact run against the full organization list of users. SmartContact skips all users that have complete information available.

To start the configuration:

1. Log in to AlertFind.
2. Go to **Administration > SmartContact**.
1. Click **Configuration**.



SmartContact Configuration Page

From : Admin@alertfind.com

To : All Users

CC : Email address copied in CC for Escalation Bump

Subject : Important: Please Provide Your Emergency Contact Information

SELECT ANY ONE : Email 01 ✓ Bump 01 ✓ Bump 02 ✓ Bump ESC ✓ Bump 04 ✓

SMARTCONTACT EDITOR - EMAIL 01

As part of our emergency preparedness program, I'm asking every employee and contractor to provide their current contact information.

It's looks like we are missing the following contact information for you:

- **Personal Cell Phone Number <**Update Now**>**

Please click on the **Update Now** link above to update your information.

Your personal security is very important to the company. I would ask that you provide the requested information within the next two days.

Best,

456/4096

SMARTCONTACT FIELDS SWITCHER

| | |
|---|---|
| Cell Phone | ● on |
| Personal Cell Number : Alternate | off |
| Personal Email | off |
| Home Phone Number | off |
| Home Zip Code | off |

SMARTCONTACT SCHEDULE FREQUENCY FOR BUMPS

| | | | |
|---|---|---|---|
| BUMP 01 | Number of days in between steps | 2 days | 10 days |
| BUMP 02 | Number of days in between steps | 4 days | 10 days |
| BUMP ESC | Number of days in between steps | 6 days | 10 days |
| BUMP 04 | Number of days in between steps | 10 days | 10 days |

On the configuration page, Administrators can customize the content and schedule for an email campaign designed to get 100% of recipients to provide their requested contact information. Click **Turn On** once the requested information is filled.

To complete the configuration page, four areas need to be filled:

- General Information
- SmartContact Editor

- SmartContact Select Fields
- SmartContact Schedule Frequency for Bumps

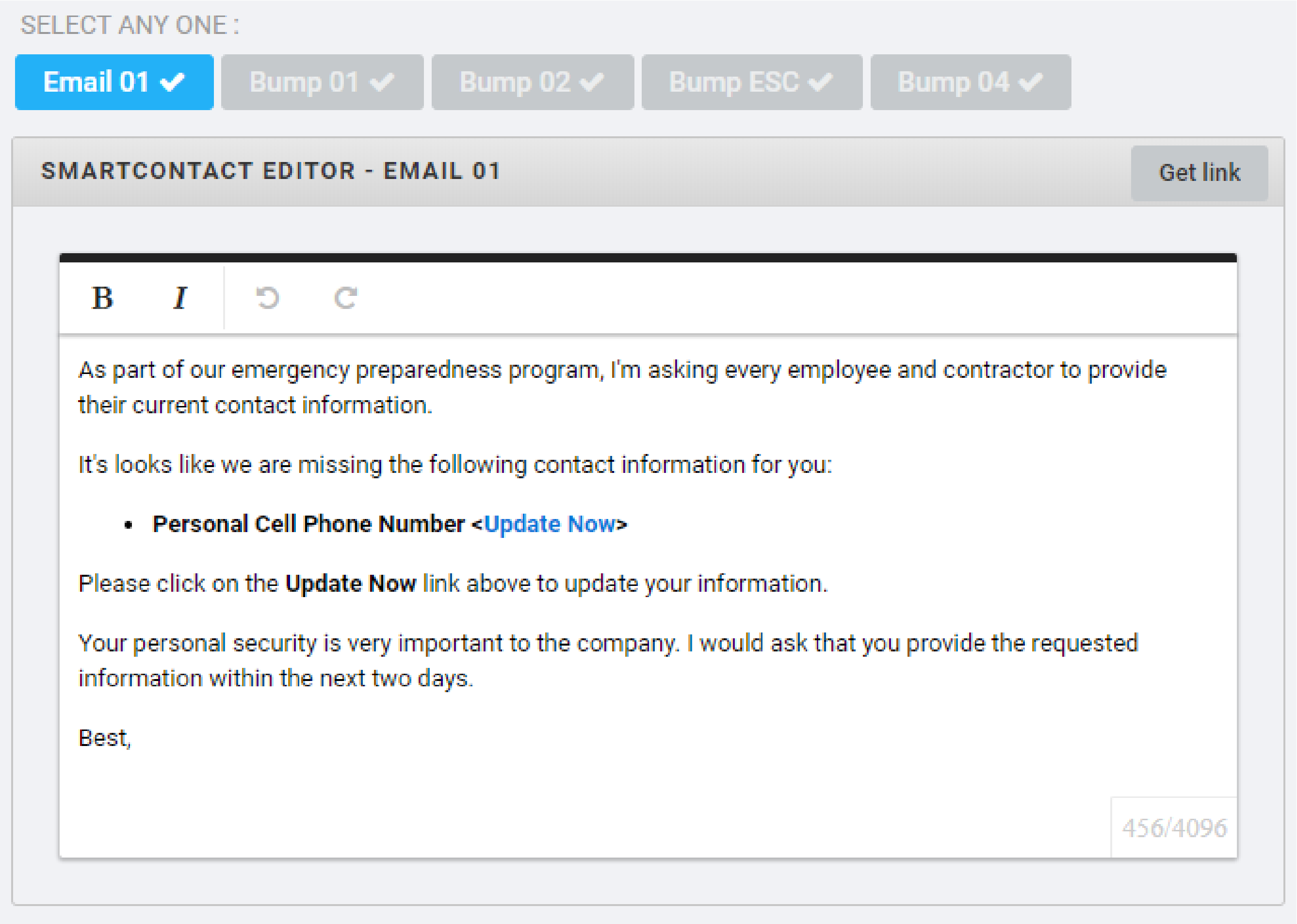
General Information

The general area contains basic information about the emails to be sent:

| Field | Description |
|---|---|
| **From** | Email of the sender. |
| **To** | List of recipients. By default, it is set to **All Users**. |
| **CC** | Other recipients to be copied. |
| **Subject** | To be edited according to the email to be sent. |

SmartContact Editor

SmartContact is pre-configured with five email templates to be sent in sequence to users that do not have complete information stored in AlertFind.



As part of our emergency preparedness program, I'm asking every employee and contractor to provide their current contact information.

It's looks like we are missing the following contact information for you:

- **Personal Cell Phone Number <Update Now>**

Please click on the **Update Now** link above to update your information.

Your personal security is very important to the company. I would ask that you provide the requested information within the next two days.

Best,

The emails will be sent in the sequence that they appear on the interface.

Edit each template accordingly to reflect the previous emails already sent and the necessary action to be taken.

Use the **Get Link** to add a link to where the user needs to update his information.

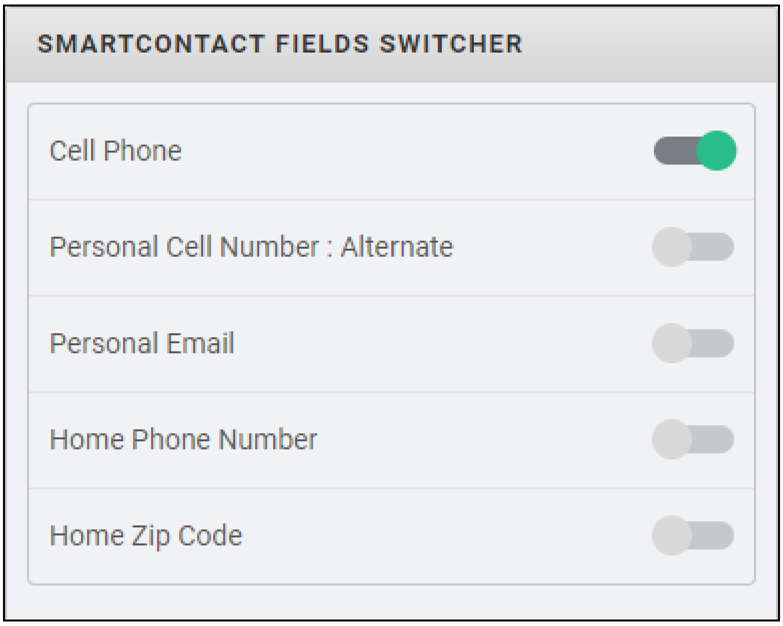
SmartContact Select Fields

Slide the selector to the right to determine which fields will be added to the check.

**NOTE**

At the moment, only the option to enable or disable the cellphone is available.

The other options will be available at a later stage.



SMARTCONTACT FIELDS SWITCHER

Cell Phone ●

Personal Cell Number : Alternate ○

Personal Email ○

Home Phone Number ○

Home Zip Code ○

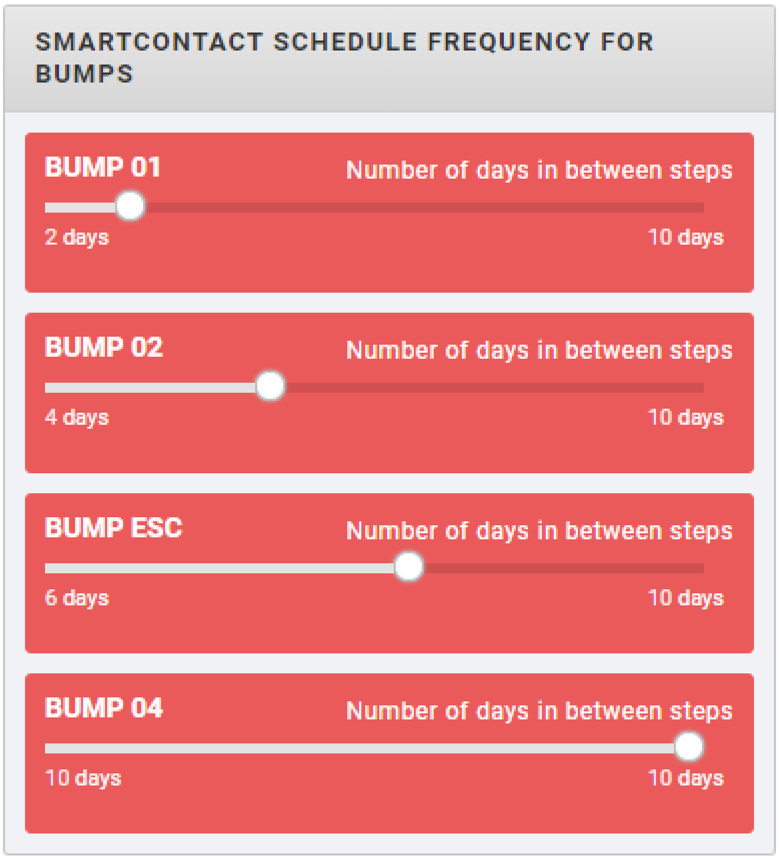
By default, the Personal Cell Phone Number will be turned on and all others would be turned off. When enabled, the additional fields would also come into the consideration for the lookup.

The available fields to be selected are:

- Cell Phone
- Personal Cell Number: Alternate
- Personal Email
- Home Phone Number
- Home Zip Code

SmartContact Schedule Frequency for Bumps

SmartContact offers administrators the possibility to schedule the intervals between emails.



SMARTCONTACT SCHEDULE FREQUENCY FOR BUMPS

BUMP 01 Number of days in between steps

2 days 10 days

BUMP 02 Number of days in between steps

4 days 10 days

BUMP ESC Number of days in between steps

6 days 10 days

BUMP 04 Number of days in between steps

10 days 10 days

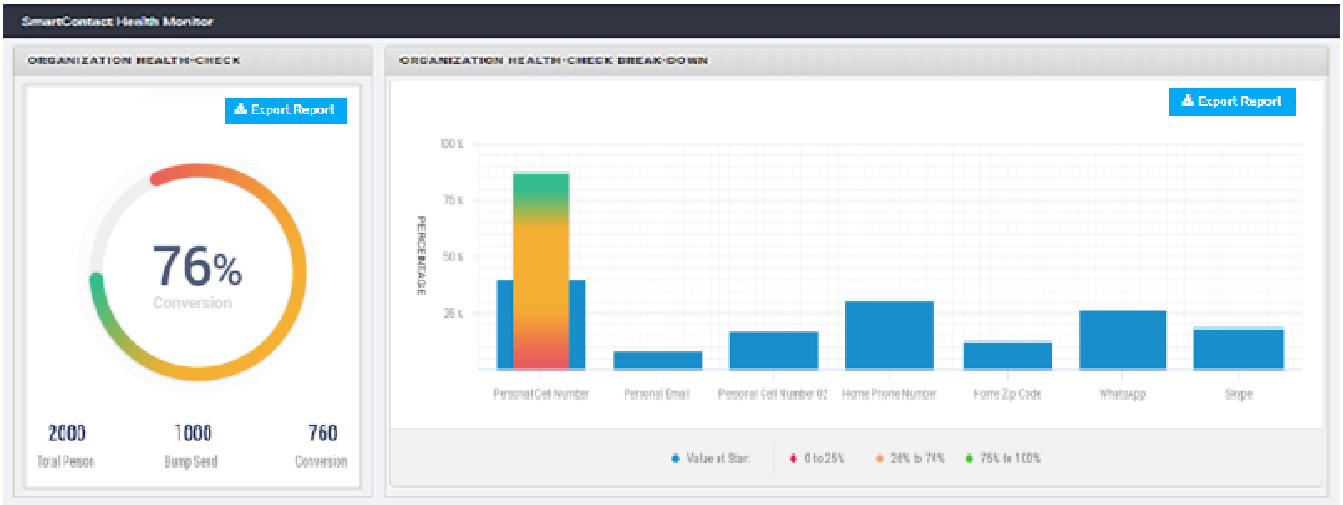
Slide the selector to the right to set the interval between emails. The options available are between 1 and 10 days for each step.

## Health Monitor

SmartContact allows AlertFind administrators' to have an overview of the contact information for each organization.

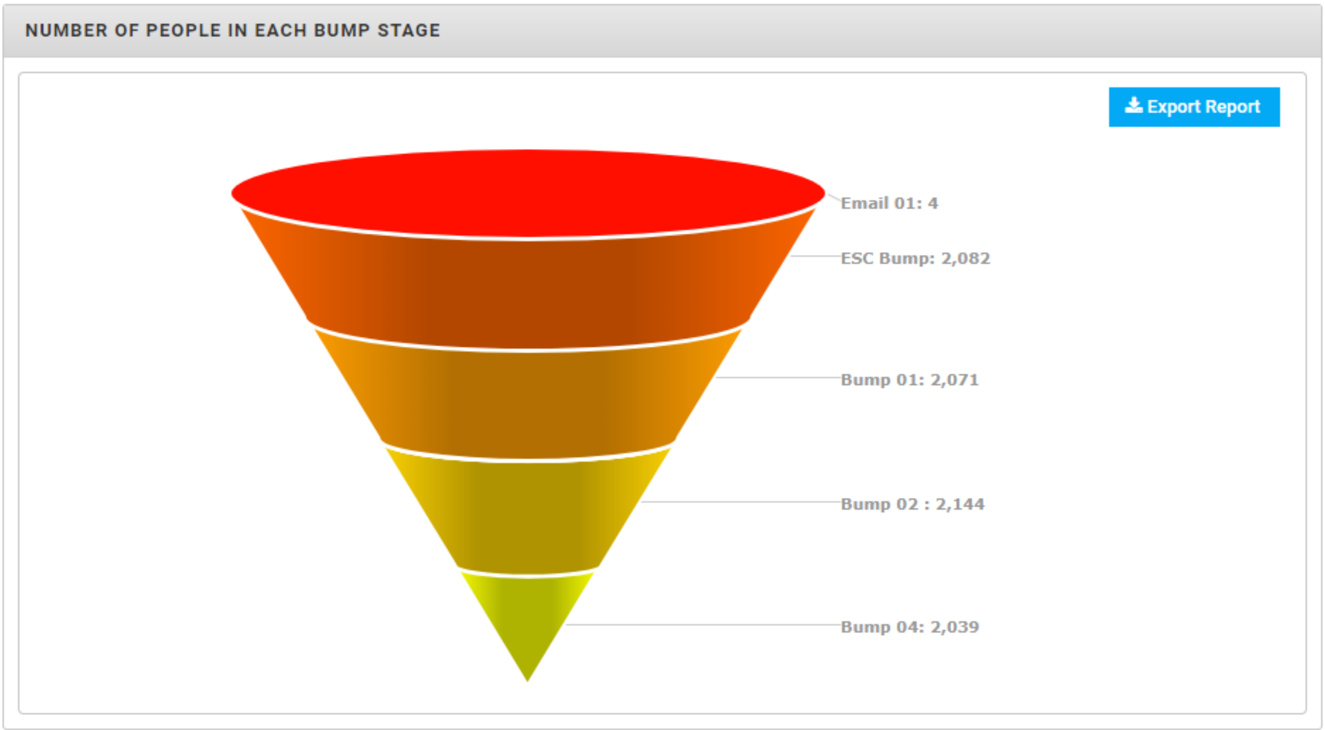
To access the Health Monitor:

1. Log in to AlertFind.
2. Go to **Administration > SmartContact**.
1. Click **Health Monitor**.



The Health Monitor contains the following information:

- Overall Organization Health-check showing how much percentage of the data is filled in the system for the selected fields.
- Smart Contact has found X amount of records which are missing personal information.
- Smart Contact has recovered Y amount of personal information.
- Funnel Chart showing Number of People in each Bump Stage.



Each chart contains an **Export Report** button that exports an XLS file with the details of each report.

# Chapter 3: Using Alerts

In this section, you learn how to compose and send a notification or an incident alert to a user. You will also learn how to create notification templates with pre-configured Notifications that can be sent simultaneously, making crisis communications consistent, quicker and more effective.

# Types of Alerts

Notifications, Incidents and Notification Templates are different, yet interrelated.

### What is a Notification?

A **Notification** is an individual notice made up of a set of recipients, a message body and an optional set of required response(s). A Notification can be sent (executed) individually, or if a Notification Template has been created that contains several Notifications, all the template's Notifications can be sent with one command.

Examples of Notifications include:

- One-time notice to employees that the office will be opening late due to weather conditions, with no required response.
- A reminder to parents that school will be let out early due to parent-teacher conferences.
- A broadcast to a group of employees with time-critical information, that all recipients need to respond to, to acknowledge receipt of the broadcast

For more information, see Notifications.

### What is an Incident?

An **Incident** is a record of the sending and acknowledgment of one or more Notifications.

Incidents can be created:

- Manually, either by manually adding existing individual Notifications, or by creating new Notifications within the Incident interface, or a combination of both.
- Or automatically, from a Notification Template, including all that template's Notifications.

An Incident can have a status of `Open` while it is still being acted upon, then be set to `Closed` when action is completed, resulting in a record of all Notifications that were included in that Incident's record.

An Incident, with its included Notifications, can be saved as a Notification Template.

Example uses of Incidents include:

- A tornado warning has been issued for a region that is covered by a sub-set of your employees. A Notification is sent, with a map-based set of recipients, which the recipients are required to acknowledge. At a later time, the tornado warning's area is expanded. The team leader or administrator then creates an Incident for this tornado, adds the first Notification into the new Incident, and from within the Incident interface is able to send new Notifications and track their responses.

- A Notification is sent out to upper-management about a troubling situation at the manufacturing plant. It is then decided that new Notifications need to be sent to various levels of management and employees containing information specific to each level. An Incident is created to track all of these Notifications in one place. Once the situation has been resolved, it is determined that this situation might happen again, and a Notification Template is created from the Incident to be used as a framework the next time this same thing happens.

For more information, see Incidents.

### What are Notification Templates?

**Notification Templates** make it easy to reuse Notifications or Incidents for situations that are expected to repeat.

For quick access, Notification Templates are displayed on the Alert Console. In contrast, neither individual Notifications nor Incidents are displayed on the Alert Console.

Notification Templates are created:

- Manually, either by copying existing individual Notifications, or by creating new Notifications within the Notification Template interface, or a combination of both.
- Or automatically, from an Incident, including all that Incident’s Notifications.

After a Notification Template is created, it can be edited as desired, including adding or deleting Notifications, and changing Notification settings.

Notification Templates can automatically create an Incident if that ability is enabled in the template.

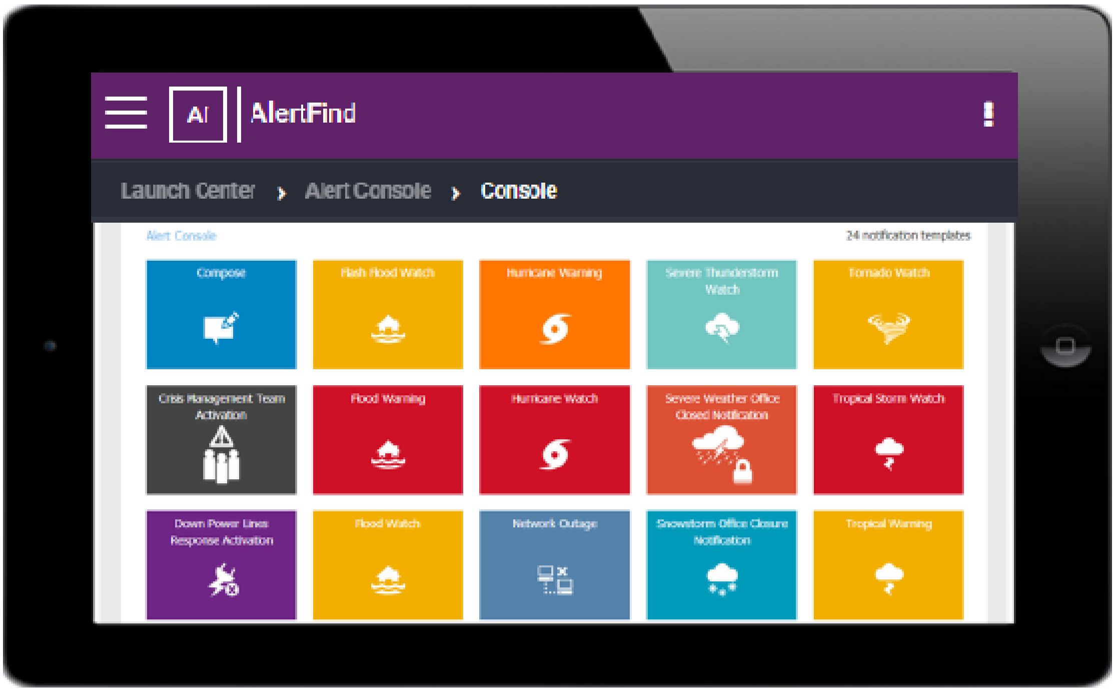
Example uses of Notification Templates include:

- A reminder to students and teachers regarding recurring event at the school, where administrators need to receive one Notification, teachers another, and parents a third Notification, with each Notification requiring differing acknowledgments. Before the Notification Template is sent, each Notification is edited to provide the name, date and time of the event.
- In an area where sever weather reoccurs, a Notification Template is created containing the basic Notifications that will need to be sent. A Notification is sent out to upper-management and other Notifications to various levels of management and employees containing information specific to each level. The template is edited before it is sent with any pertinent current information. And the feature is enabled to create an Incident to track all of these Notifications in one place.

For more information, see Notification Templates.

# Alert Console

The Alert Console is a mobile-optimized, responsive web interface that can be used by AlertFind administrators and team leaders. The combination of the Alert Console and the enhanced Notification Templates features makes it possible for anyone with minimal AlertFind training to easily send a notification, or a series of pre-defined notifications, for critical communication scenarios.



The Alert Console works on any device (desktop, smart phone, or tablet). It automatically identifies and responds to the screen size of the device that you are using. Since the Alert Console is designed to be displayed on both a desktop or on a mobile device, you can use either your fingers or a mouse to interact with the Alert Console interface.

## Use the Alert Console Interface

To use the Alert Console, you should have the following permissions: *Send Notification*, *View Results*, *Cancel Notification*, *Open From Template*, and *View Template*.

The Alert Console works on any device (desktop, smart phone, or tablet). It automatically identifies and responds to the screen size of the device that you are using. Since the Alert Console is designed to be displayed on both a desktop or on a mobile device, you can use either your fingers or a mouse to interact with the Alert Console interface.

From the Alert Console, you can do the following:

- Select your team context. See Select Your Team Context.
- Use *Quick Compose* to create and send a notification without any advanced options. See Use Quick Compose.
- Search for a notification template. See Search for a Notification Template.
- Review a template notification. See Review or Edit a Template Notification in the Alert Console
- Edit a template's launch options. See Notification Template Launch Options
- Edit the recipient list, the subject, and the message text of a template's notification(s) and send the notification(s). See Edit and Send a Notification(s) from a Notification Template. The combination of the enhanced Notification Templates features and the Alert Console makes it possible for anyone with minimal AlertFind training to easily send one or a series of pre-defined notifications for different critical communication scenarios.
- Return to the Console window from a sub-window. See Return to the Alert Console Window.
- Check the responses to a notification. See Check Notification Responses.
- Go to the desktop Web interface. See Navigate to the Administrative User Interface.

## Select Your Team Context

*Team security context* is the team a user is currently accessing within AlertFind. Because team leaders can have different permissions on different teams, the team security context under which they are operating determines what actions they can take in AlertFind. For more information, see Team Security Context.

### NOTE

Once you have selected a team context, then when you go to the console window, you will see the templates for that team. Only the templates for your selected team are displayed in the console window.

To select your team context:

1. In the Console window tool bar, click **My Teams**.
2. In the displayed selection box, select a team. You are returned to the Console window with the team you selected as your team context.

## Use Quick Compose

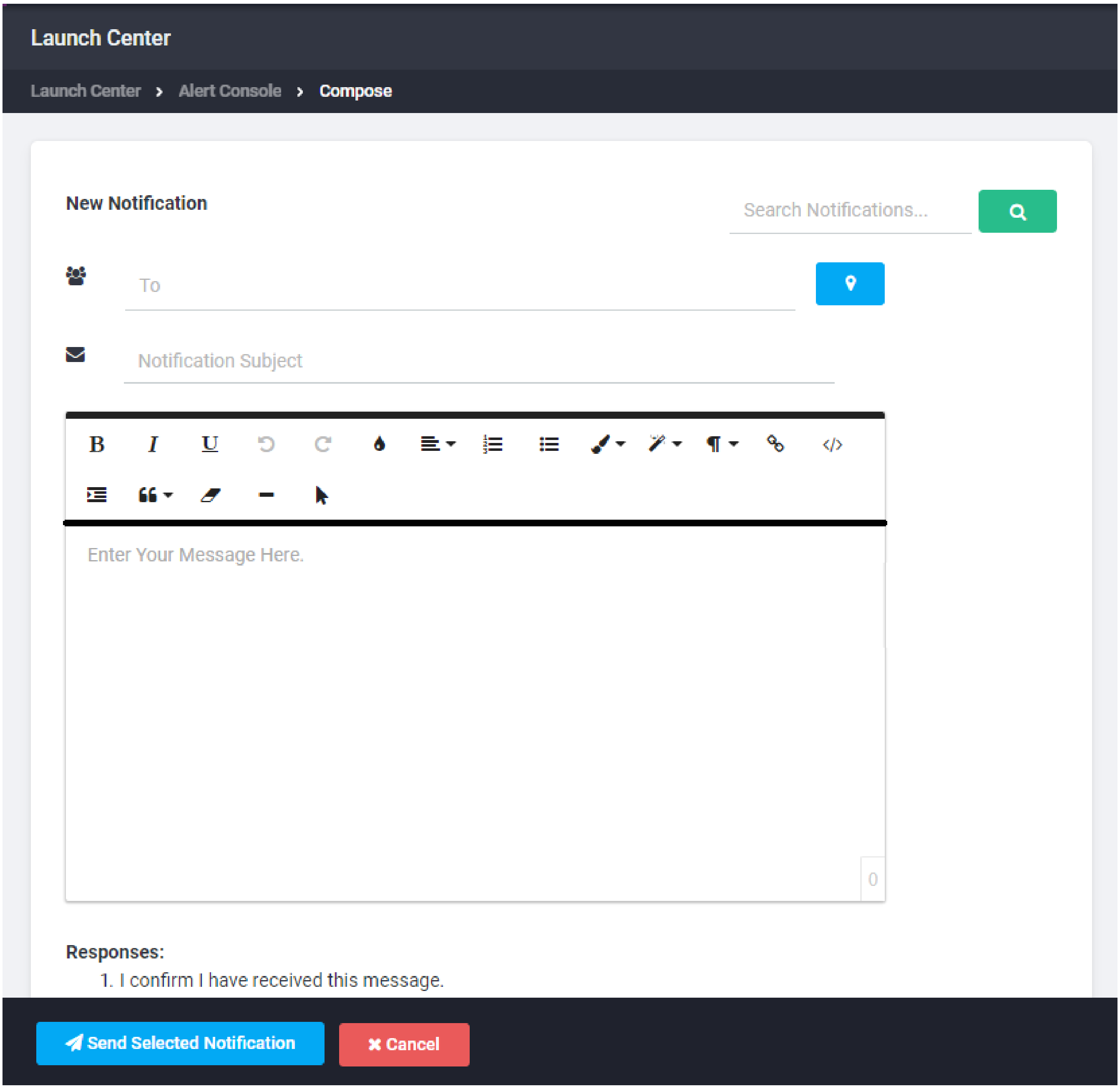
You can use *Quick Compose* from the **Alert Console** interface to quickly compose and send Notifications that do not require advanced options.

### NOTE

If you want to create a Notification with more options, go to the **AlertFind** desktop interface > **Launch Center** > **Compose (Advanced)**.

To create a notification using Quick Compose:

1. In the Alert Console, click the **Compose** icon. The **New Notification** window appears.



Responses:

1. I confirm I have received this message.

2. In the **To** text box, type the name of a user or group, or enter a geographical location where the users to whom you want to send the notification reside (see Send a notification to AlertFind users within a geographical location.
3. In the **Notification Subject** text box, type the message subject.
4. In the **Message** text box, type the message.
5. If you are satisfied with the notification, click **Send Selected Notification** or click **Cancel** to cancel the operation.

## Search for a Notification Template

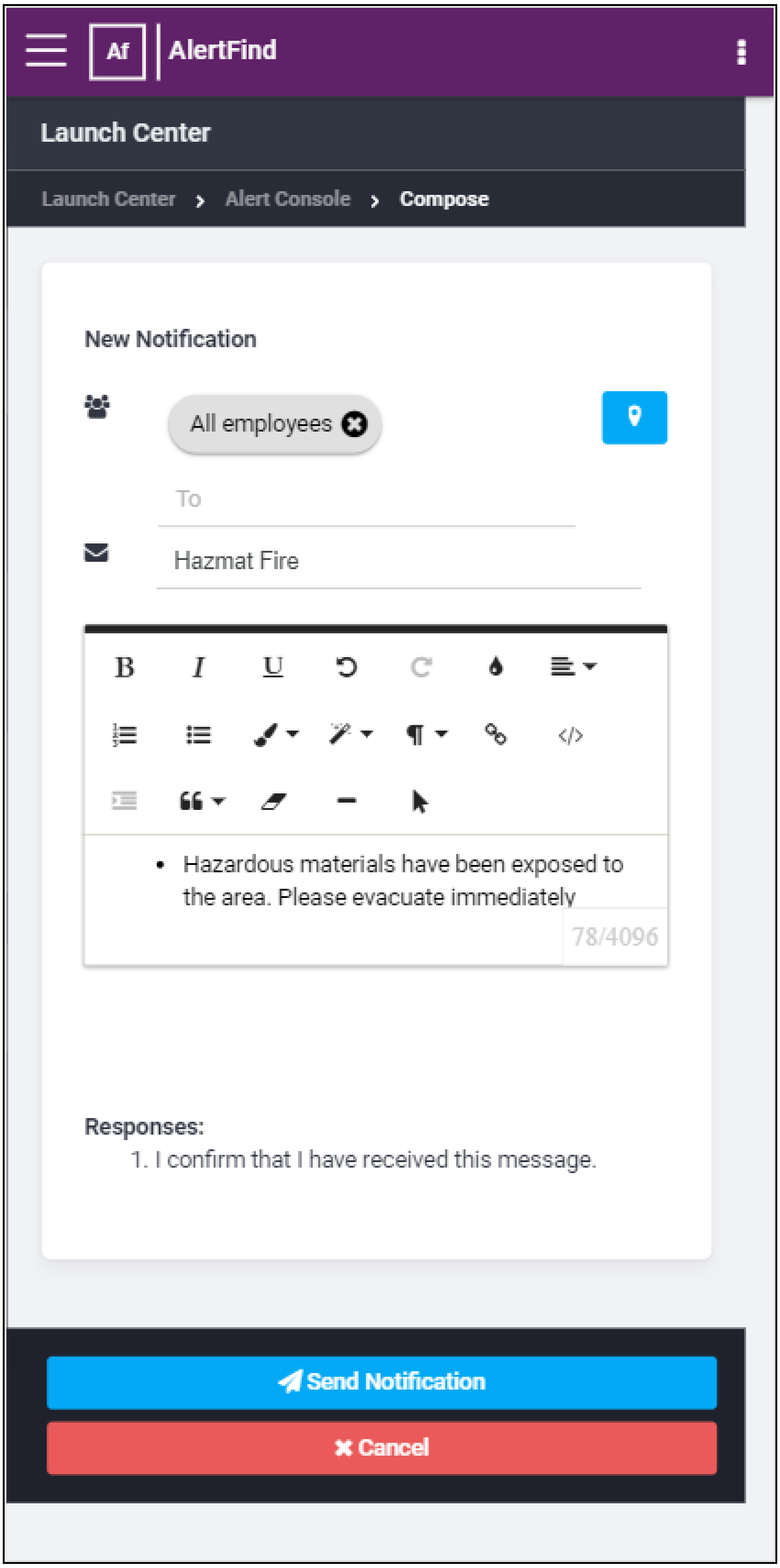
Icons for all the notification templates are displayed in the Alert Console window, though you will not see them all at once on a mobile device.

To search for a notification template, in the **Search** text box, enter part of a template title or the whole title. Templates with that text in its title is displayed.

Alternatively, click the left or right arrow to move the template icon display to the right or the left, or with your finger or the mouse, simply move the display to the right or the left.

## Review or Edit a Template Notification in the Alert Console

After you select a template in the Alert Console, a Quick Compose view of the template notification(s) opens. If enabled for editing, then you can edit the notifications for the selected template.



New Notification

All employees

To

Hazmat Fire

- Hazardous materials have been exposed to the area. Please evacuate immediately

78/4096

Responses:

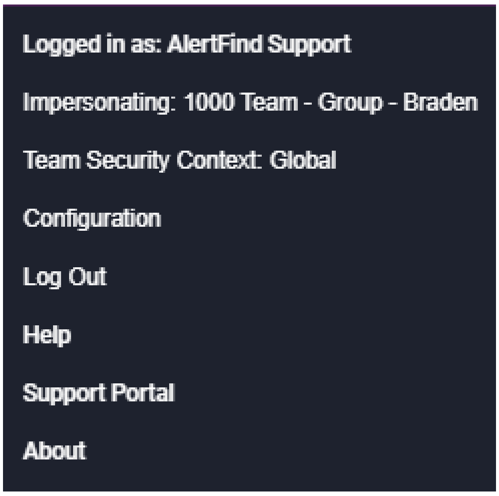
1. I confirm that I have received this message.

There are four components on the screen:

- **Mast Head**: This is the same as for all AlertFind Web pages. When enabled, there is an optional company logo on the far right of the Mast Head.

NOTE

The preceding example is of a small-sized screen, If you click on the box on the right side of the masthead, the following options display. These options are visible as part of the Mast Head on a desktop screen.



Logged in as: AlertFind Support

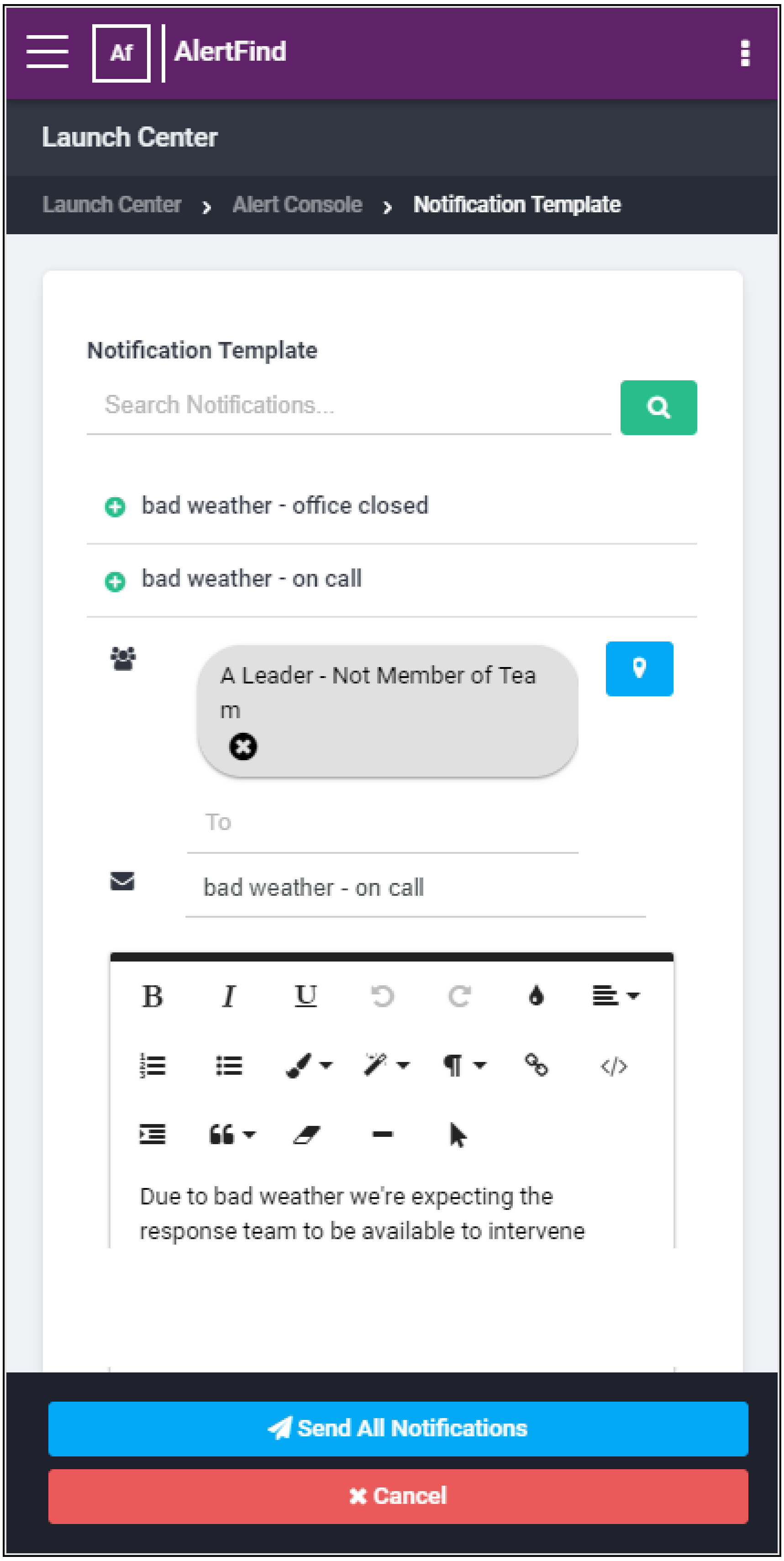
Impersonating: 1000 Team - Group - Braden

Team Security Context: Global

- **Context Tool Bar**: Allows navigation around the console and has a notification search bar. If you enter text into the *Search notifications* text box, the Compose and Edit component only displays notifications that have the searched for text somewhere in their subject lines.
- **Quick Compose View**: Where you can prepare notifications to be sent and review and edit them.
- **Send Bar**: From this bar, you can either cancel your work and go back to the template selection screen or you can send the notification(s). The **Send Notification** button text changes if the template is set to send all notifications.

### Quick Compose View

In the Quick Compose view, you can preview a notification prior to sending, though you can edit it only if it is enabled for editing.



bad weather - on call

Due to bad weather we're expecting the response team to be available to intervene

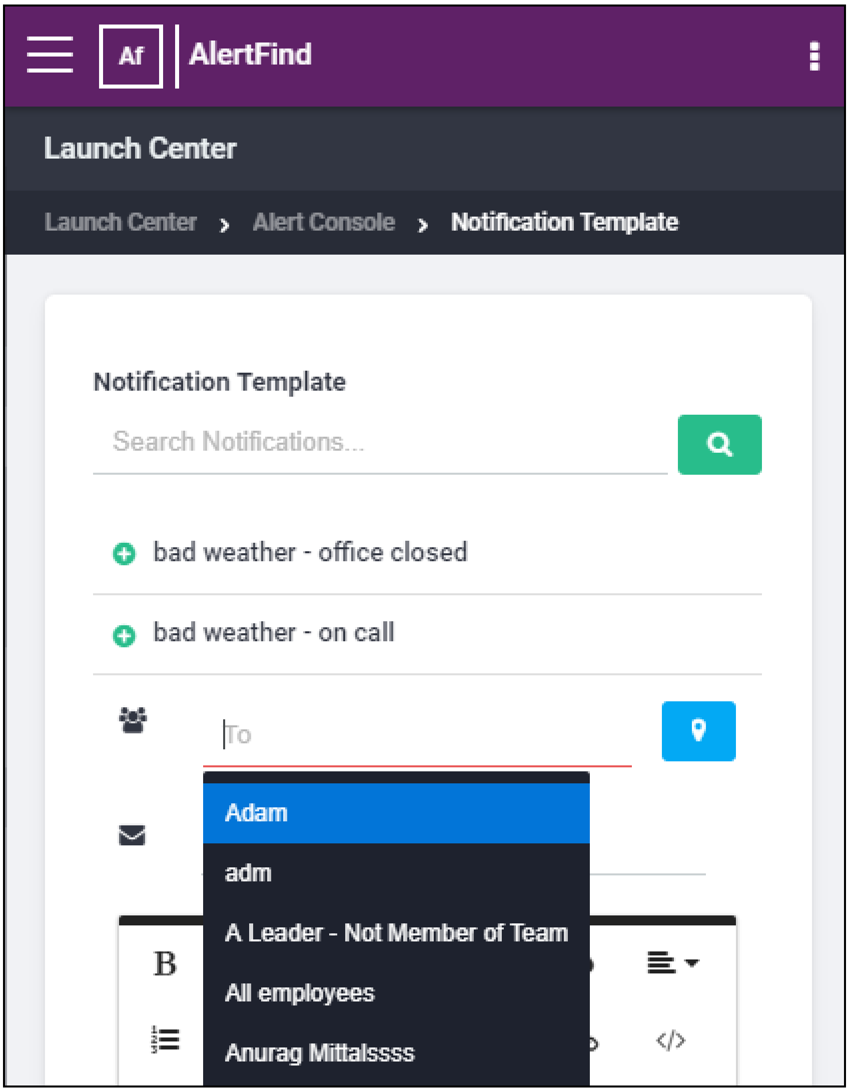
Sub-Components:

- **Template Title**: shows the title of the template.
- **Hint Text**: changes depending on how the notification template launch option *Send all notifications* is set:
    - If *Send All Notifications* has been checked in the template, then the message is *Pushing "Send All Notifications" will send all notification tasks*.
    - If *Send All Notifications* has not been checked in the template, then the message is *Select notification to review message content*.
- **Notification Toggle**: Each notification has a toggle button showing the notification subject or *New Notification* if the subject is empty. When clicked, the notification preview or editor drops down and you see the message details. The notification is then highlighted in blue. If a second notification toggle is clicked, the first notification editor is closed, the toggle is un-highlighted, and the new notification is opened and highlighted.
    - If the template is set to Send All Notifications, then all of the notifications are always highlighted, even when closed
    - If the template is set not to Send All notifications, then highlighting a notification also selects it for sending.
- **Geographical Location Icon**: Allows you to send a notification to all users within a geographical location. See Send a notification to AlertFind users within a geographical location
- **Recipient Selector**: shows the list of recipients. If the template has *Enable Editing* checked, then you can add new recipients here, using a drop-down auto complete. See Recipient Editor.
- **Subject line**: shows the notification subject. This is the same as the text in the notification toggle.
- **Message Body**: the body of the message. Placeholder text is present if there is no text.
- **Response Table**: shows the possible responses and the respective response codes.

If the template does not allow editing, the text fields are gray.

## Recipient Editor

In the recipient editor, you are able to view and edit the list of recipients. The editor displays a list of the current recipients. Next to the current list, you can begin typing the name of a recipient user or group. Once at least one letter is typed, a drop down appears that displays all users and groups, the names of which begin with the entered text. Users appear before groups. Users are denoted with an icon of one person. Groups are denoted by an icon of two people.



## Sub-Components:

- **Geographical Location Icon** 📍: The geographical location icon to the right of the **To** text box enables you to select a geographical location to which you can send the notification. All users within the selected location receive the notification when it is sent. See Send a notification to AlertFind users within a geographical location.

- **Current Recipients**: Displays a list of recipients. Recipients can be removed by clicking the "x" associated with a recipient or by pressing the backspace or delete key.
- **Recipient Input**: Next to the current recipients, you can begin typing in the name of a recipient user or group. Once at least one letter is typed, a drop-down text box appears.
- **Drop-Down List**: displays all users and groups, the names of which begin with the entered text:
  - Users are denoted with an icon of one person and Groups are denoted with an icon of two people.
  - Recipients are sorted by type (user/group/type of group) and sub-sorted alphabetically.
  - You can select a recipient from the Drop Down with either the mouse/touch or using the arrows and enter key.

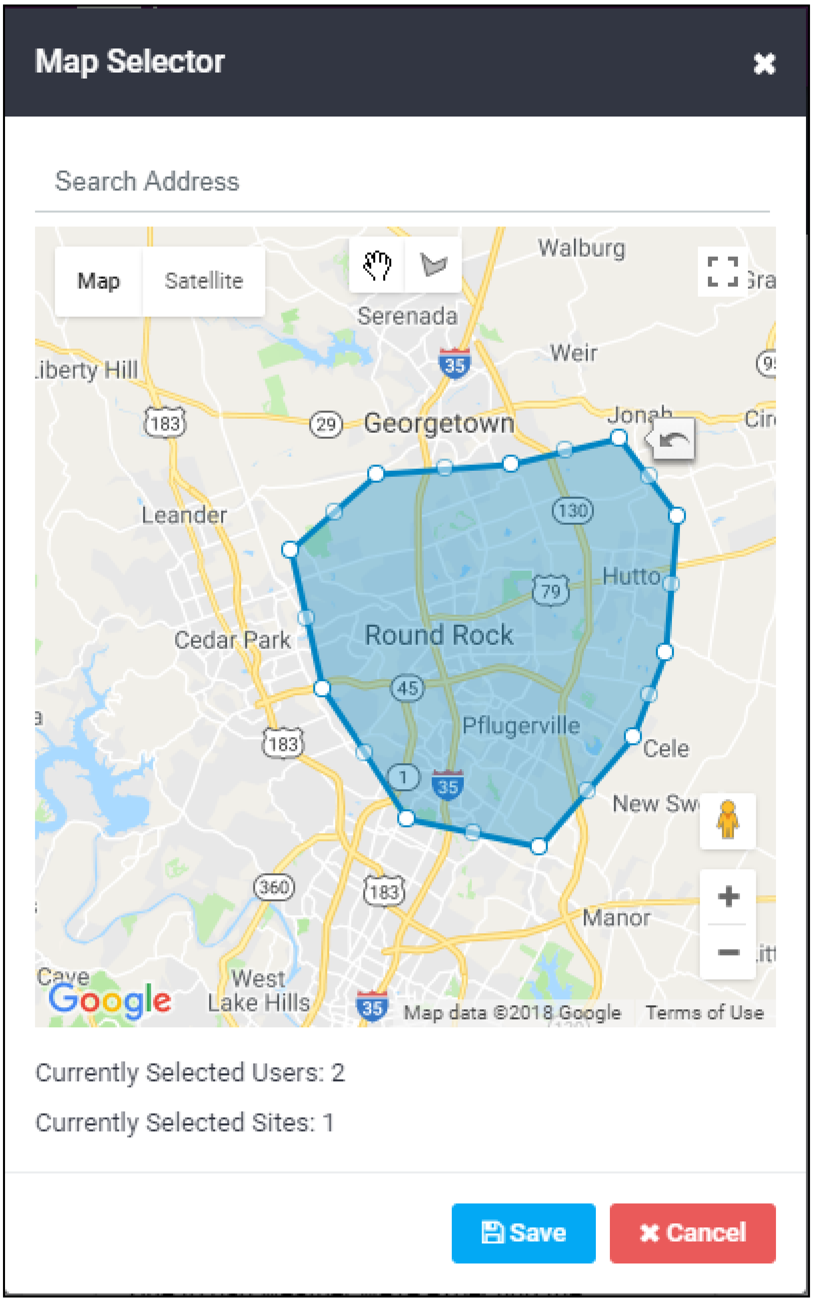
### Send notifications to AlertFind users within a geographical location

This feature has the following requirements:

- **Enabling map-based notifications**: Map based notifications must first be enabled by the administrator before you can use this feature.
- **Selecting individual users**: A user's map coordinates must be in the database. This is done through the User Editor **Location Preference** window. See Enter or change a user’s location in AlertFind.
- **Selecting one or more Sites**: Sites must be created and populated with Groups of users. See Create A Site.

To send a notification to AlertFind users within a geographical location:

1. From the **Alert Console**, click the **Compose** icon.
2. Click the **Geographical Location Icon**, 📍, which is to the right of the **To** text field.
3. With your finger or mouse, move the displayed map to select the general map area that you want.



Currently Selected Users: 2

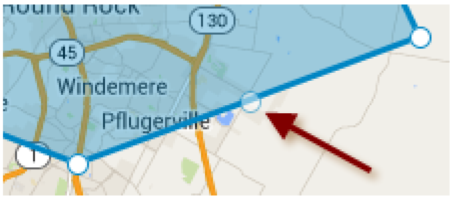
Currently Selected Sites: 1

4. Click the polygon icon . Then select a specific geographical location by clicking on the map to start drawing the polygon. Next, click at each corner of the polygon. Double-click on the last point, or click on the first point, to enclose the area.

   If you want to move the polygon, click the hand icon, , using the hand cursor, click-and-hold on the polygon and drag it to the new position.

   To edit the shape of the polygon, using the hand cursor, , click-and-hold on a corner point and move it to the desired location.

   To create new points, click-and-hold on a new-point dot between the existing corner points, and drag to the desired location.



- When using the hand cursor, you can click on the Undo icon, ↶, to undo the last action.
- Draw more polygons, if desired.
- All users and Sites located within the polygon(s), and members of the selected team context, will be recipients of the Notification.
- The **Currently Selected Users** and **Currently Selected Sites** counts update when a polygon is added, changed or moved.

NOTE

No individual polygon within a group can be deleted by itself. To delete all polygons, if the location(s) hasn't been saved, click **Cancel**. Otherwise, click **Done** and return to the composition window and delete the *Temporary Group* that corresponds to the polygons to be deleted.

5. Click **Done** to save the area and return to the notification composition screen, or **Cancel** if you choose not to save a location.

### Notification Template Launch Options

Notification Templates support several configurable behaviors for when notifications are sent from the Alert Console:

NOTE

These options are only available and configurable from the desktop Notification Templates library page. They are not configurable from the Alert Console.

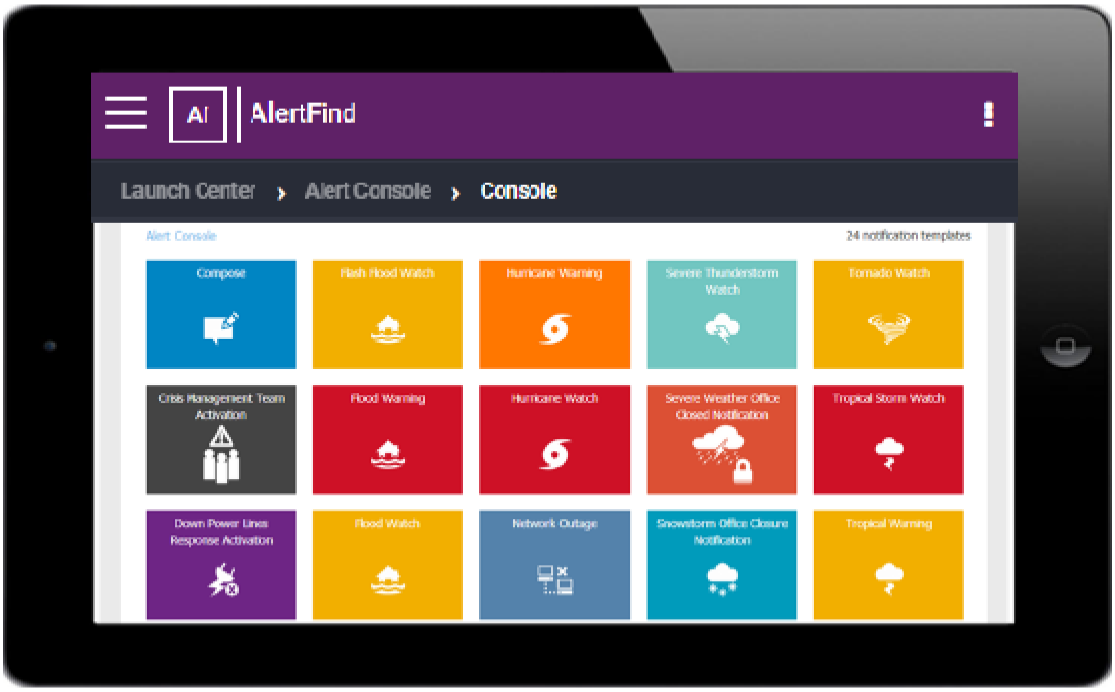
- **Enable Editing**: This allows a team leader to change the recipients, subject, and body of a notification before it is sent. This change is only valid for the instance in which it is sent (It does not change the template itself). This is turned on by default.
- **Send All Notifications**: If a template contains more than one notification, selecting this option forces all notifications of the template to go together. This is turned on for existing Incident Templates to maintain backwards compatibility, but is turned off by default for anything new. Sending All Notifications allows the editor to define a Quick Launch ID. You must select this option if you want to utilize the quick launch feature.
- **Create Incident**: If selected, the system will create an Incident when the notification(s) is sent and link those notifications to the Incident. This is turned on for existing Incident Templates to maintain backwards compatibility, but turned off by default for anything new.

## Edit and Send a Notification(s) from a Notification Template

Since notification templates can be pre-configured in your team’s template library, you should not have to do much editing when the time comes to send one or a series of notifications for various communication scenarios. However, if the notification template is enabled for editing, you can edit the notification recipients, subject, and message when sending the notification(s).

To edit and send a notification or multiple notifications using the Alert Console:

1. As an administrator or team leader with the permissions to send notifications, click the **Alert Console** link in the left navigation bar. This launches the Alert Console. Quick Compose and any other Notification Templates are displayed in the Alert Console screen.


AI
AlertFind
Launch Center › Alert Console › Console
Alert Console
24 notification templates
Compose
Flash Flood Watch
Hurricane Warning
Severe Thunderstorm Watch
Tornado Watch
Crisis Management Team Activation
Flood Warning
Hurricane Watch
Severe Weather Office Closed Notification
Tropical Storm Watch
Down Power Lines Response Activation
Flood Watch
Network Outage
Snowstorm Office Closure Notification
Tropical Warning

2. Select a notification template by clicking it in the Alert Console window.

### NOTE

The *Open Incident* button is no longer available. To use *Quick Compose* to create and send a notification, in the Alert Console, click **Compose**. See Use Quick Compose. To create and send a notification from the desktop using the notification advanced features, from the left menu bar, Launch Center section, select **Compose (Advanced)**.

3. In the template window, click the notification title bar to open it. If there is more than one notification, then click the first notification to open it.
4. If needed, edit the recipients in the **To** text box, the subject in the **Subject** text box, and message text in the **Message** text box.
5. When finished, click the notification title bar to close the notification.

6. If there is more than one notification and you need to edit other notifications, repeat steps 3 and 4 for the other notifications you would like to edit.
7. When finished, if you have one notification, click **Send Selected Notification**. If you have more than one notification, click **Send All Notifications**. Or, click **Cancel** to cancel the operation. The Alert Console window displays.

## Return to the Alert Console Window

When in a sub-console window, you can return to the Alert Console window at any time.

To return to the Console window, in the Alert Console window tool bar, click **Console** or at the top-left of the window, click the browser back arrow.

## Check Notification Responses

To check notification responses, in the Alert Console window tool bar, click **Responses**.

A **Responses** window is displayed listing notification responses. For each response, the following is listed:

- Notification Subject
- Response Rate
- Message
- Sender
- Total Recipients
- Responded
- View response details button

## Navigate to the Administrative User Interface

To go the Web desktop interface:

1. Click **Home**.
2. To return from the Web desktop interface to the Alert Console, in the desktop left menu bar Launch Center section, click **Alert Console**.

# Notifications

A *Notification* is a message sent to a user device (such as an email address, telephone, or fax machine) and can contain:

- **Message text**, which can be read in an email, fax, or text message, or read aloud by the text-to-speech (TTS) engine for a telephone Notification.
- **Audio files** that are prerecorded and uploaded to the message or recorded using call-to-record. See Supported Audio Files for details.
- **Attachments** that can be delivered along with the message, depending on the device.
- **Secure information** that requires recipients to authenticate themselves using a PIN or external key before they can receive the Notification.

Notifications can be sent in any language for which your organization purchased language packs.

When **Send** is clicked, AlertFind begins sending Notifications to the selected users. It tries to contact the first device in each person's currently active personal escalation list. Notifications are delivered according to the escalation in effect when the notification is sent.

For example, if the test was sent at 9:00 PM, AlertFind searches for the first configured device in the user's After Hours escalation list (assuming this user has the default business hours of 8:00 AM to 6:00 PM) because the notification is sent outside of regular business hours.

If AlertFind is not able to make contact with the first device in the escalation list, it moves on to the second device. It continues through the user's configured device list until it either receives confirmation from the recipient, leaves a voice mail (in which case it continues on the escalation path), or exhausts all device options.

See Configuring a Standard Device for more information about escalations and notification delivery.

### NOTE

Because AlertFind has no way of knowing if an email was successfully delivered, it considers a Notification task sent to an email address as complete. This does not mean the email is considered confirmed.

## Notification Prerequisites

Prior to sending a notification, AlertFind must be provisioned and several integral parts of the system must be set up:

- Users
- Groups
- Teams (optional)

Most company information, such as time zone, personal escalations, business hours, and the ability to customize AlertFind prompts, can be edited by an AlertFind administrator. Other company settings must be configured by Support. These settings are typically discussed and configured during provisioning, but may be updated at any time by contacting Support.

## Compose Notification

You can use *Quick Compose* on the **Alert Console** interface to quickly compose and send Notifications that do not require advanced options. See Create a notification using Quick Compose.

This section discusses the **Compose (Advanced)** desktop option for creating and sending Notifications. The **Notification Editor** enables you to compose a Notification with basic information and advanced options including scheduling, escalation override, multiple responses and device retries.

Basic options available for Notifications: (See Compose a basic Notification)

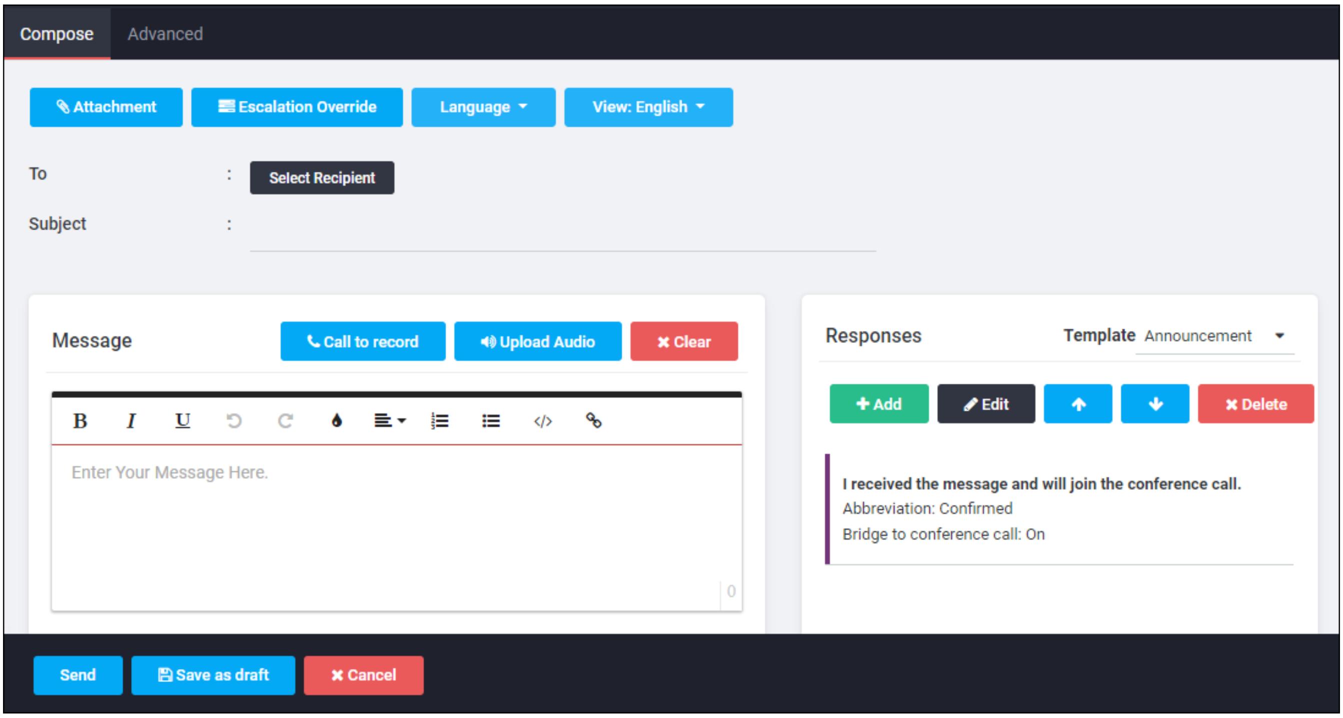
- Choose an optional notification template
- Change the available responses or response limits
- Add recipients
- Set the notification subject
- Include a text message or an audio file
- Attach files
- Set a custom escalation
- Send the notification in additional languages
- Send the notification immediately after composing

Advanced options available for Notifications: (See Add advanced options to a Notification)

- Require recipients to authenticate themselves before receiving the message
- Allow recipients to respond to the notification by calling a Hotline
- Set a priority flag
- Set a maximum number of times a phone call will be retried
- Schedule the notification for later delivery or recurring delivery
- Email results of the notification to yourself or someone else

### Compose a basic Notification:

1. Ensure the correct team context. See Team Security Context.
2. In the left menu bar under **Launch Center**, click **Compose (Advanced)**. The **Notification Editor** window appears. The Announcement response template is selected by default.



I received the message and will join the conference call.
Abbreviation: Confirmed
Bridge to conference call: On

3. **Select Recipients:** To select the users and groups to send this Notification to, click the blue **To** button. The **Recipient Editor** window appears.
   - Double-click a name to move it to the **Recipients** section.
   - Alternatively, in the **Map Selector** tab, create a polygon and click **Add Polygon(s)** button to add it to the Recipients list. All users and Sites located within the polygon(s), and members of the selected team context, will be recipients of the Notification. See Send a notification within a geographical location for more information on using the map-based recipient selection feature.
4. (Optional) **Select Language:** If language packs were purchased by your organization, to send this Notification in other supported languages, click the **Language** drop-down, click **Language Settings** and select the languages for this Notification. Click **OK** to return to the Notification Editor. The following fields will need to be customized for each language selected: `Subject`, `Message`, `Responses`. To view the Notification as it will appear in another supported language, choose a different language from the **View:** drop-down list. See Use the Language Settings Editor for additional instructions.
5. **Enter Subject:** Type a **Subject** for the Notification. A subject is required. Notifications cannot be sent without a subject. This field's value:
   - Appears as the subject in email notifications
   - Is *spoken* in phone notifications
   - Is displayed on reports and progress pages
6. **Enter Notification Body:** See "Use The Message Pane" for more information. In the **Message** pane, perform one of the following options:

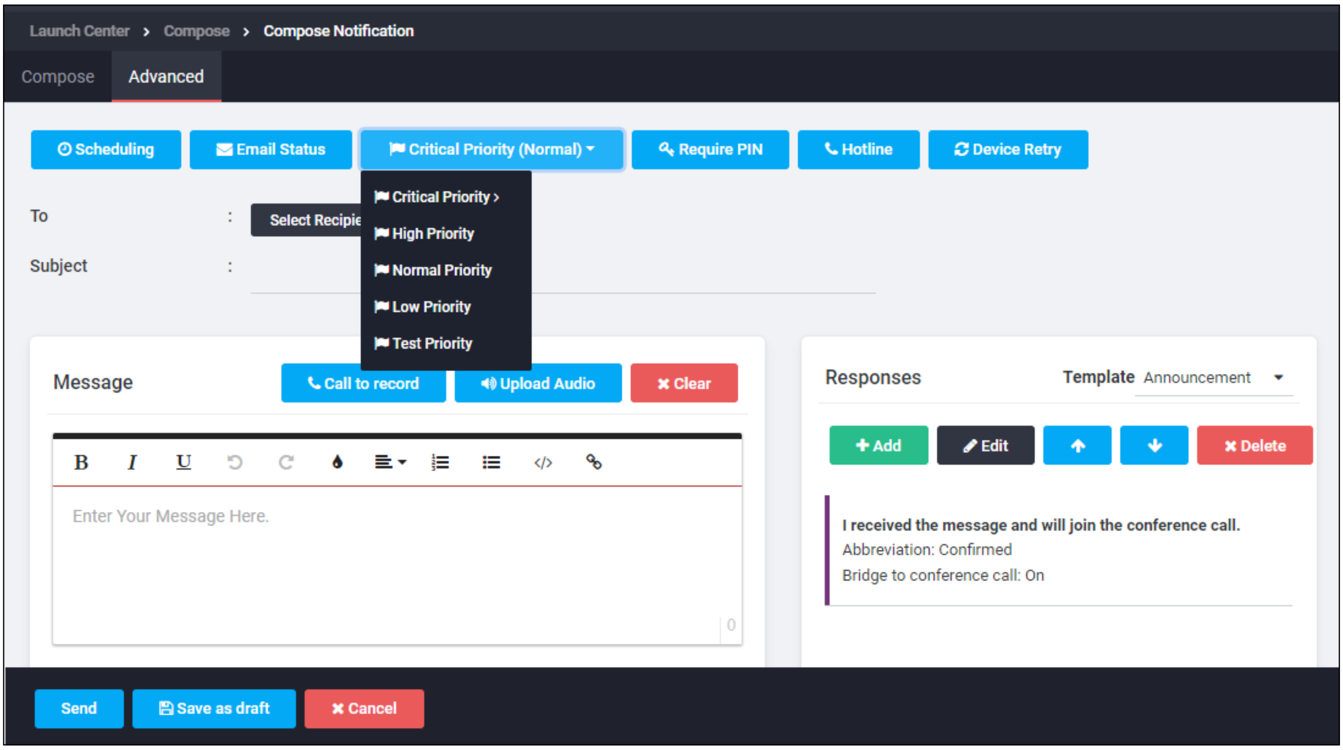
- Type the text for the Notification message body. This message body is the message that is delivered by text devices (email, fax, and SMS) or spoken by the TTS engine for phone notifications.
- Click **Call to record** to record a message on the phone
- Click **Upload Audio** to upload an audio message.

7. **Edit Response:** To use a predefined response template, click **Template** on the **Compose** tab. The list of available response templates appears. Select the template to be used. See "Use the Notification Editor" for a list of template types. If you do not want to change the default response template, continue to the next step. Otherwise:
   - To create a new response in addition to the default responses, click **New**. The **Response Editor** is displayed.
   - To edit or add responses or response limits, click the response in the **Responses** section, then click **Edit**. The **Response Editor** is displayed.
   - Any changes made to responses apply only for this Notification. See Use the Response Editor for additional details.
8. When finished editing responses, click **OK** to return to the Notification Editor.
9. **Add attachments:** If attachments need to be included with the notification, click **Attachment** button. When **Attachments Editor** appears, click **Add** and browse to the location of the file to attach. See Use the Attachments Editor for additional instructions. When finished adding attachments, click **OK** to return to the Notification Editor.
10. **Customize Escalation:** To customize the type of devices or the order in which they are contacted, click **Escalation Override** button. The **Escalation Editor** displays. See Use the Escalation Editor for additional instructions. When finished editing escalations, click **OK** to return to the Notification Editor.
11. **Advanced Options:** The Notification should now contain all required information. To add advanced options, follow the instructions under Add advanced options to a Notification.
12. **Finish Notification**: To complete the Notification, do one of the following:
    - Click **Send** to immediately begin sending the Notification.
    - Click **Save as Draft** to save the Notification. It can be edited further, scheduled for delivery at a specific time (or at a recurring time), or sent at a later time. Draft Notifications are located on the **Scheduled Notifications** page.
    - Click **Cancel** to discard this Notification.

### Add advanced options to a Notification:

After completing the basic options for a notification (see Compose a basic Notification), use the **Advanced Options** tab to add additional options to the notification.

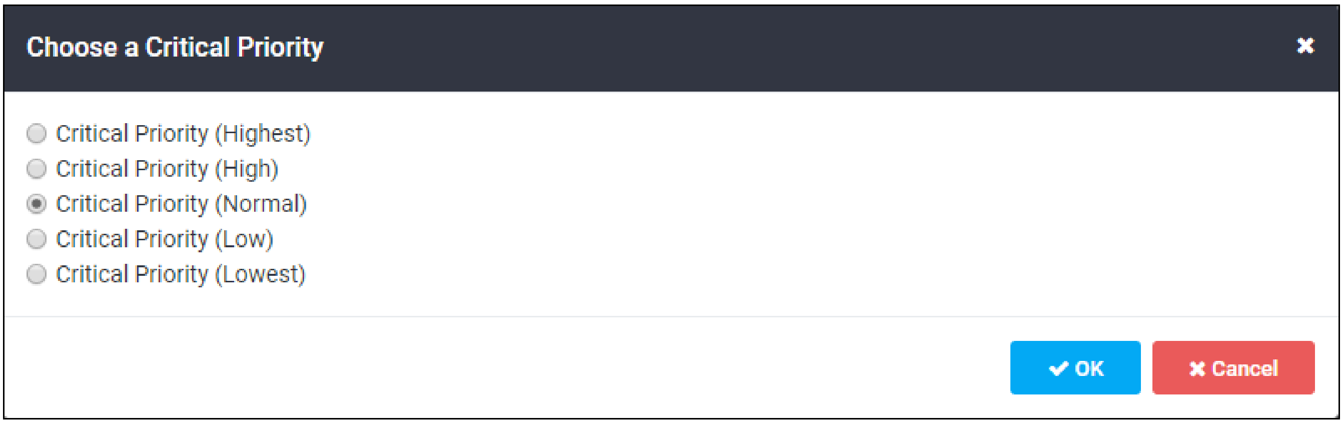
1. Click **Advanced Options** in the Notification Editor.



I received the message and will join the conference call.
Abbreviation: Confirmed
Bridge to conference call: On

1. To send email results of this notification, click **Email Status**. The **Email Results Editor** is displayed.
    1. Click **Email to:** and then type the email address(es) of the recipients in the field.
    2. Enter the number of hours after which the results will be emailed. Must be a whole number 1 or greater.
    3. Click **OK** to return to the Notification Editor.

3. To set a priority flag for the notification, click the priority drop-down next to **Normal** and select a value. Selecting a priority value that is higher than your organization's other active notifications' priorities, dynamically changes the delivery rate for *all* your organization's active notifications, giving this notification a faster delivery rate compared to lower priority notifications. The default priority is `Normal Priority`.



○ Critical Priority (Highest)
○ Critical Priority (High)
● Critical Priority (Normal)
○ Critical Priority (Low)
○ Critical Priority (Lowest)

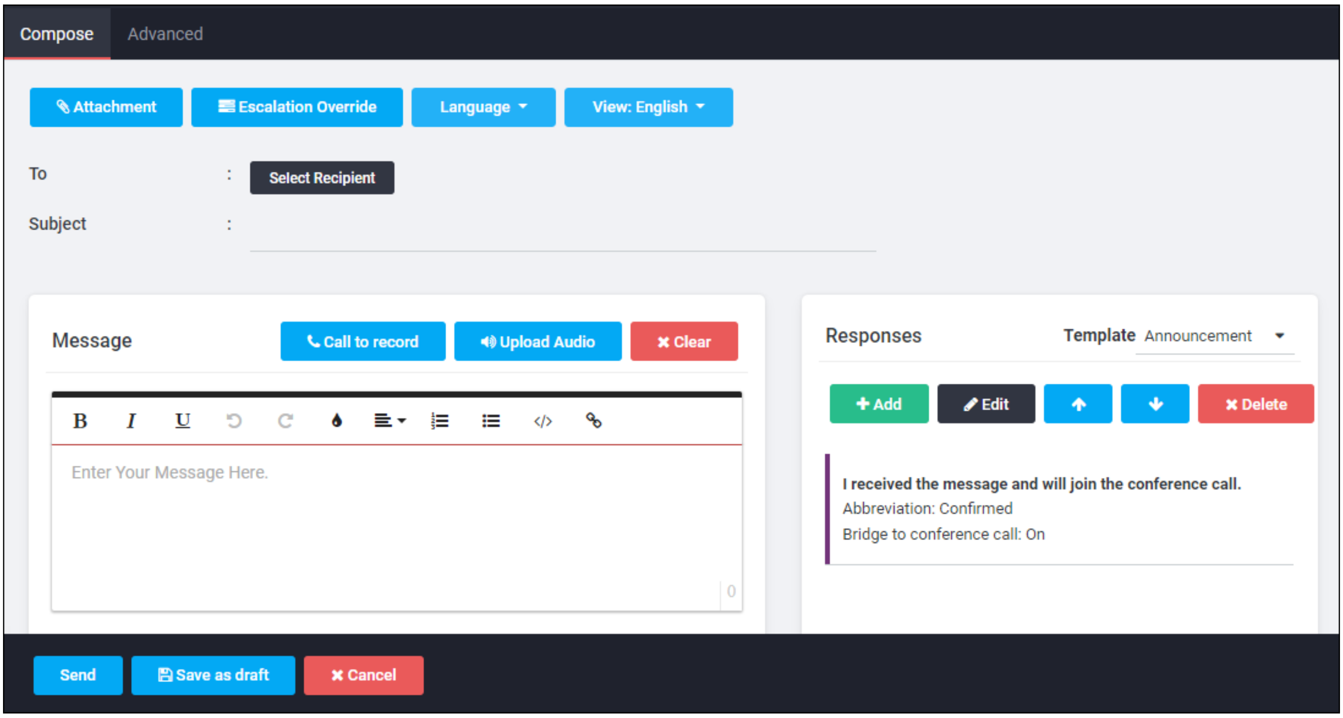
4. To make the notification recipients enter a PIN to hear or read the message, click **Require PIN**. Toggle this button on (darkened) or off (lightened) to enable a PIN for recipients to hear or read the message.
5. Choose whether to allow recipients to respond to this notification by calling a Hotline. To enable this option, click **Hotline**. The **Hotline Call Back Editor** window displays. Select the type of Hotline callback instructions the recipient receives. Options are:
    - Use user default Hotline phone number
    - Use all Hotlines
    - Do not allow responses through Hotlines
6. Click **Save** to return to the Notification Editor.
7. Set the maximum number of times a phone call will be retried for this notification. Click **Device Retry**. Choose the system default retry setting, or choose a specific number of retries. If this value is set to zero, the call is made once, but not retried. Click **OK** to return to the Notification Editor.
8. Choose to send the notification now, save it to send manually later, send it on a schedule, or create a recurrence pattern for notifications to be sent multiple times.

| Sending option | Description |
|---|---|
| To send the notification now | Click **Send**. |
| To save this notification to manually send later | Click **Save as Draft**. Send it later by following the instructions under Manually Send a Notification. |
| To schedule this notification for delivery at a future date or time, or to add a recurrence pattern, click **Scheduling**. | • To repeat this notification on a recurring schedule, set a **Recurrence pattern**: `No Recurrence`, `Daily`, `Weekly`, `Monthly`, `Annually`, or `Hourly`. Complete the additional recurrence options displayed for the recurrence pattern chosen.<br>• In the **Start Time** row, select the date and time when you want the notification scheduling to begin.<br>• in the **End Time** row, select either **No end time** or **End after**. If **End after** is selected, enter the number of hours after which to stop sending this notification.<br>• Click **Save** to save the scheduling and recurrence options. |

## Use the Notification Editor

From the left navigation menu, **Launch Center** section, click **Compose (Advanced)** to display the **Notification Editor**.

This window has two major subsections (**Message** and **Responses**) and two tabs (**Compose** and **Advanced Options**). The red outline of the **Subject** field indicates that it is required and the notification cannot be sent until one is provided.



Template Announcement

I received the message and will join the conference call.
Abbreviation: Confirmed
Bridge to conference call: On

1. Use the **Compose** tab to set basic options for the notification.

| Option | Description |
|---|---|
| **Template** | Select a notification template type. Templates automatically fill in basic responses. If language packs were purchased, templates are available in multiple languages.<br>Templates are available for the following types of notifications:<br>• **Announcement**–One default response: “I confirm I have received this message.”<br>• **Note**: Each response has an *abbreviation*, which is a shortened form of the response. For example, *Confirmed* is the abbreviation for this default response.<br>• **Conference Call**–Two default responses: “I received the message and will join the conference call” or “I received the message but cannot attend the conference call.”<br>• **Poll/Survey**–Two default responses: “Yes” or “No.”<br>• **First Responder(s)**–One default response: “I confirm that I |

| Option | Description |
|---|---|
| | will take action regarding this message.” This template also enables the setting for Response Limit Handling, which stops delivery of the notification when response limits have been reached. |
| **Attachment** | Attach files to the notification. By default, attachments are stored on the server, and recipients receive a link to the attachment in the notification. A copy of attachment can be included with the notification. See Use the Attachments Editor for more details. |
| **Escalation Override** | Override the standard escalation rule in effect at the time the notification is sent and define an escalation specifically for this notification. See Use the Escalation Editor for more details. |
| **Language** | If language packs were purchased, select a language in which to send the notification here. See Use the Language Settings Editor for more details. |
| **View** | If language packs were purchased, select the language in which to view the **Notification Editor** window. |

2. Use the **Advanced Options** tab to set advanced options for the notification.

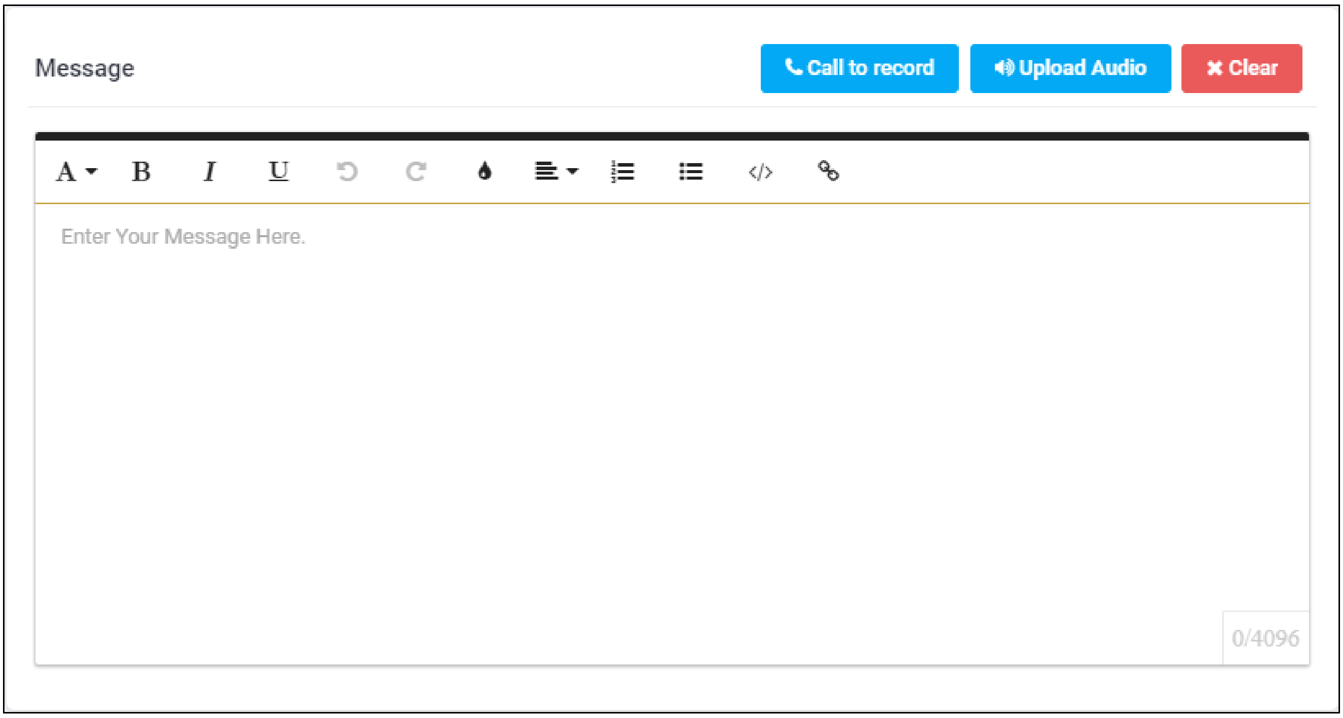
| Option | Description |
|---|---|
| **Scheduling** | Schedule the notification to be sent after a delay, or to set a recurrence rule for a recurring notification. See Add advanced options to a Notification for scheduling instructions. |
| **Email Status** | Indicate whether to send an email status report about the notification and to whom to send it. See Add advanced options to a Notification for more details. |
| **Priority flags** | Set a priority for the notification. The red exclamation mark ! is high priority, the blue down arrow ↓ is low priority, and the green check ✓ is test priority. Toggle off all flags to send the message with no given priority. |
| **Require PIN** | If this notification requires authentication to read or hear it, click **Require PIN**. Toggle this button on (darkened) or off (lightened) to require or not require a PIN. |
| **Hotline** | Use the Hotline Callback Editor to select the Hotline callback instructions the recipient receives. See Add advanced options to a Notification for more details. Options are:<br>• Use user default Hotline phone number<br>• Use all Hotlines |

| Option | Description |
|---|---|
| | • Do not allow responses through Hotlines |
| **Device Retry** | Use the Device Retry Editor to set the maximum number of times a call will be retried for this notification. If this value is set to zero, the call is made once, but not retried. |

3. Use the **Message** section to enter the text of the notification as it appears in written notifications (email, fax, SMS, pager) and as it is spoken by the TTS engine for phone notifications. A call-to-record audio file, or an uploaded audio file, can be used to complete this field. See Use The Message Pane.
4. Use the **Responses** section to create the possible responses to the notification. See Use the Response Editor for additional details.

### Use The Message Pane

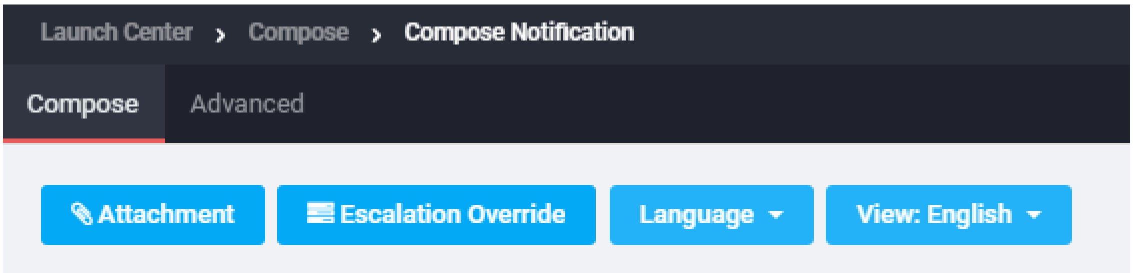
Use the Message pane to create the body of the message:



Choose one of the following methods to enter the message body:

- Type the body of the message into the **Message** pane. This text message body is the message that is delivered by text devices (email, fax, and SMS) or spoken by the TTS engine for phone notifications. The number of characters you type is displayed beside the **Message** header. This is because some SMS providers have a set maximum message length. This number helps you stay within this limit. If you exceed the limit, the message may be delivered in multiple parts. Text-based messages can be personalized using variables. See Personalize text-based messages using variables
- AlertFind can call a phone number and have that person record the message using the **Call to record** button. This option will be handled the same way as uploaded audio files. See Use Call to Record option.
- Use the **Upload Audio** button to upload a WAV audio file. This file is played for phone call recipients. Other recipient types are directed to call the Hotline or Hotline Pro number to listen to the message. See Use Upload Audio option

If language packs were purchased, message text must be provided for each language selected. Use the **View:** drop-down list to choose a language, then type the language's message into the **Message** pane, or record or upload an audio message.



### Personalize text-based messages using variables

To personalize the notification, the following variables may be used:

- `${user.name}` – The user’s full name.
- `${user.userNames[0]}` – User's user name/login ID.

NOTE

Variables must be typed in the message exactly as they appear above. All variables start with the `$` (dollar sign) and must be enclosed in `{}` (curly braces).

### Use Call to Record option:

To have AlertFind call so a message can be recorded, click **Call to record**. In the **Call to Record** window displayed, enter the phone number AlertFind should call and then, click **Call now**.

### Use Upload Audio option:

To upload a previously recorded audio file, click **Upload Audio**. The **File upload dialog** window displays. Click **Add**. A file selection window opens. Navigate to the file to upload.

The file to be uploaded must be a WAV file in a supported format. See Supported Audio Files. Click **Open**. Click **OK**.

### Use the Response Editor

Use the Response Editor to set the available responses for this notification. A default set of responses are available when a template is chosen. See Use the Notification Editor for a list of template types and default responses.

All responses provided must be options, because they will follow the words “Press *n*” for voice notifications. For example, a response for a first responder notification might read “`if you will take action on this notification`.” AlertFind prepends “Press *n*” to the response text so that the recipient hears “Press 1 if you will take action on this notification.”

#### IMPORTANT

Instructional text will be included in the SMS indicating that the user should check their email for the audio and/or the attachments. Each available response will be listed by the abbreviation for the response, not the full response text.

Example Chunked SMS Messages

```
1 of 3 (From TMobile Device Notification System) Mike
Rosenfelt has lost his car keys. Your presence is requested
immediately on a conference call to discuss
```

```
2 of 3 (From TMobile Device Notification System) this crisis.
The conference call phone number is 1 (866) 489-0573 and the
meeting ID is 7696151. Attachments
```

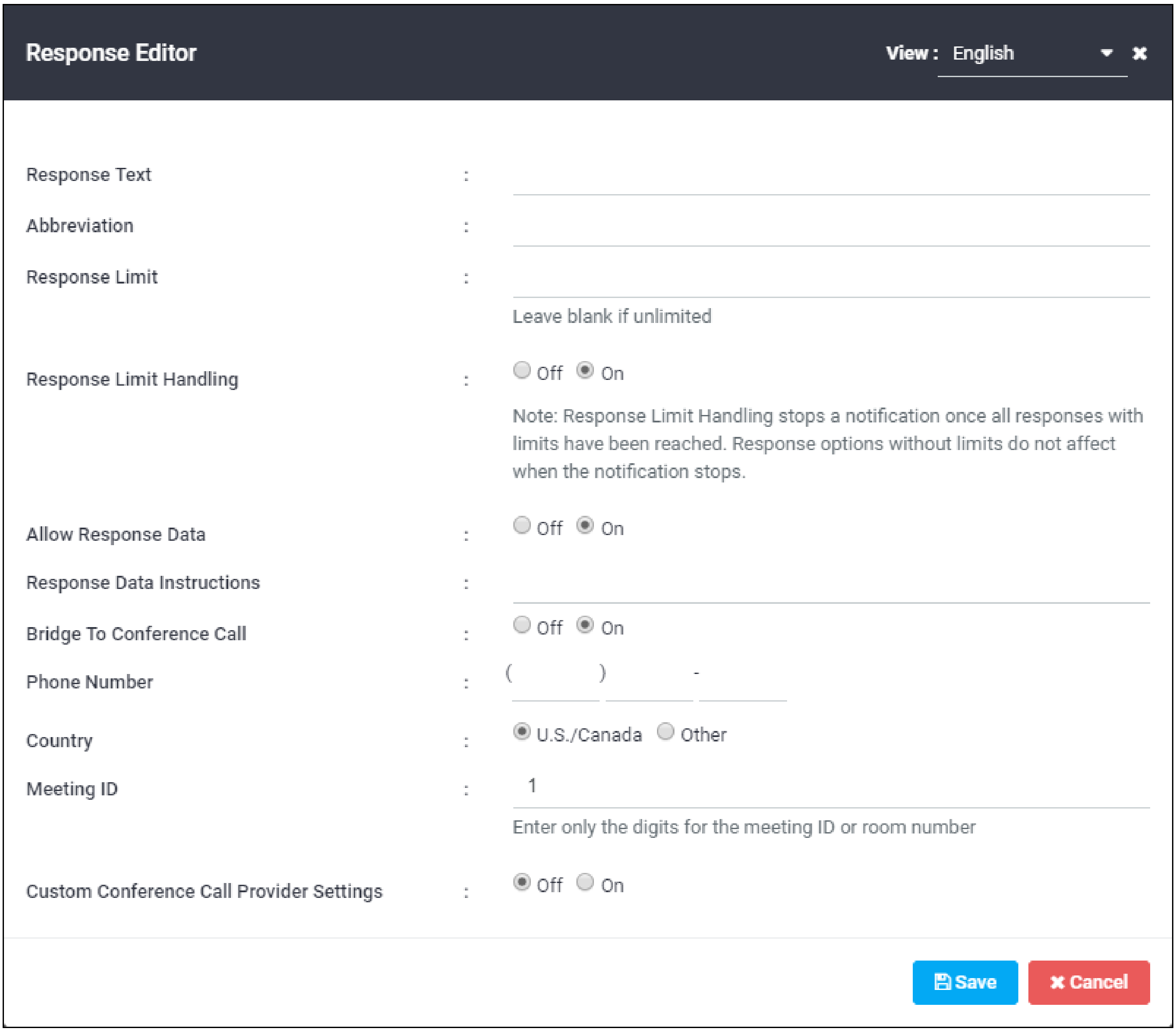
```
3 of 3 (From TMobile Device Notification System) included in
email. Reply with 9649 to respond Attend, 9071 to respond No
Attend.
```

#### NOTE

Type the responses in the language selected for this notification. To create responses in another language, choose a different language from the **View** drop-down list.

**Create additional responses from the Notification Editor:**

1. In the Notification Editor **Responses** section, click **Add**. The Response Editor window is displayed. The following is an example of the Response Editor window with all the available response options.



| | | |
|---|---|---|
| Response Text | : | |
| Abbreviation | : | |
| Response Limit | : | Leave blank if unlimited |
| Response Limit Handling | : | ○ Off ● On<br>Note: Response Limit Handling stops a notification once all responses with limits have been reached. Response options without limits do not affect when the notification stops. |
| Allow Response Data | : | ○ Off ● On |
| Response Data Instructions | : | |
| Bridge To Conference Call | : | ○ Off ● On |
| Phone Number | : | (    )    - |
| Country | : | ● U.S./Canada ○ Other |
| Meeting ID | : | 1<br>Enter only the digits for the meeting ID or room number |
| Custom Conference Call Provider Settings | : | ● Off ○ On |

2. In the **Response Text** field, type the response to be created. This is the text that is sent in text notifications and spoken in voice notifications.
3. In the **Abbreviation** field, type the response abbreviation. For example, *Confirmed* for *I confirm that I have received this message*, or *Attend* for *I will attend the meeting*.
4. In the **Response Limit** field, enter a limit number If there is a limit to the number of users who can select this response. For example, for a first responder notification, type 1 in this field. (If you are using the first responder template, this is automatically set to 1.) If you set a response limit, also set **Response Limit Handling** to **On**.
5. Set **Allow Response Data** to **On** if you want to allow recipients to enter data in response to the notification. This displays the **Response Data Instructions** field. Enter here the instructions recipients see or hear when they are prompted to enter numeric data. For example, this field might say, “Enter your current contact phone number including area code.”

6. To bridge recipients to a conference call, set **Bridge to conference call** to **On**. This displays fields for setting a US or international phone number and a meeting ID.

NOTE

The correct format for an **Other** phone number is:

`[COUNTRY_CODE][CITY AREA_CODE][PHONE_NUMBER]`.

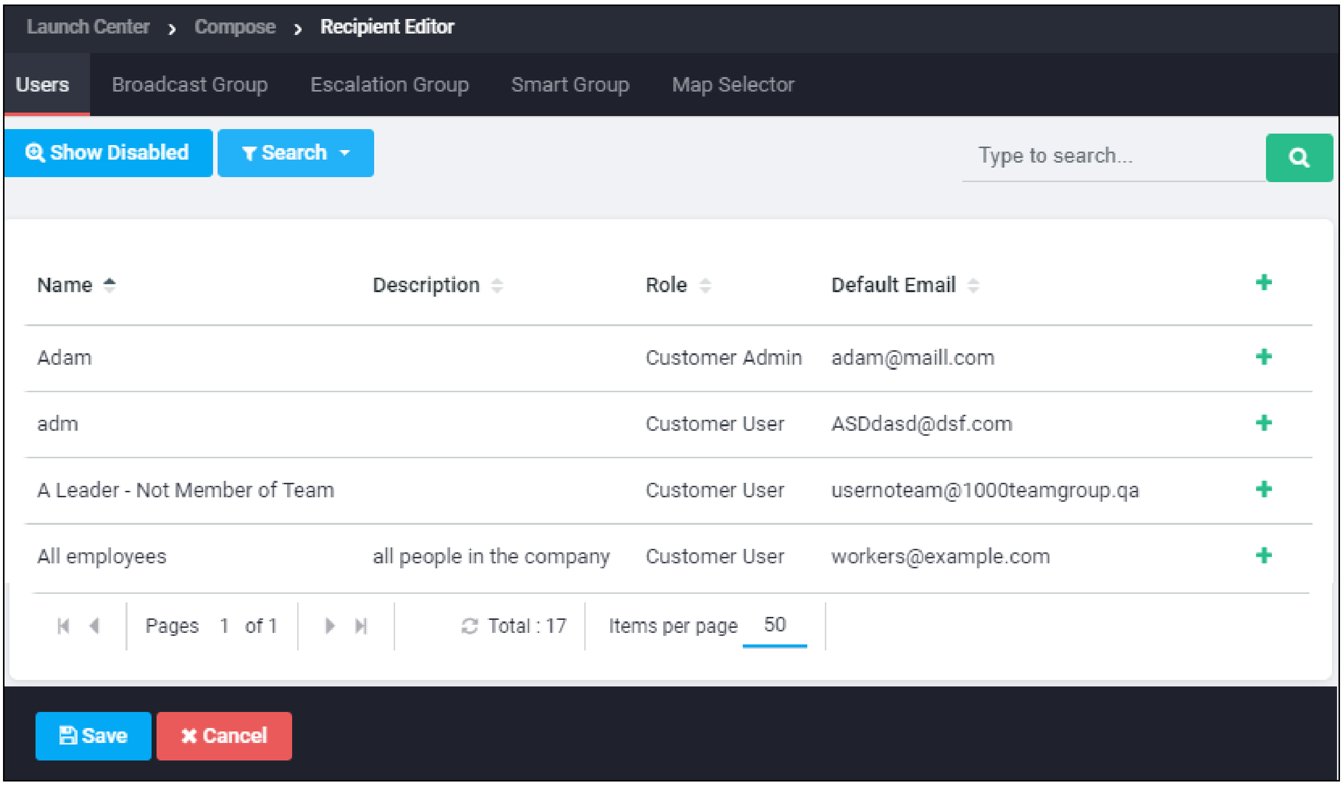
Numbers that include '0' between the country code and the city/area code are invalid in AlertFind. For example, the phone number 44(0) 207 333 4444 is invalid.

However, a UK number such as 44 20 7333 4444 is valid. In this example, the area code for London (20) is separated by spaces from the rest of the phone number. AlertFind will eliminate spaces so that number will become 442073334444.

7. To include a prefix or suffix to the meeting ID, set **Custom conference call provider settings** to **On**. Set **AnswerOnMedia** to **On** only if AlertFind cannot connect to the conferencing bridge using the bridge number, meeting ID, and any required suffices or prefixes. If you are able to connect a conference call using the standard fields, there is no need to enable **AnswerOnMedia**. This option enables AlertFind to connect the user to the conference call bridge the moment the initial **ring** is heard, rather than wait for the bridge to pick up. This means a user will hear the ringing tones once he or she selects the transfer option. Use this feature only when a conference call bridge has a habit of not connecting a call when it picks up the transfer.
8. When you are finished editing the response and response options for this notification, click **Save** to return to the Notification Editor.

## Use the Recipient Editor

Use the Recipient Editor to add recipients for the notification and set any delays or specific recipient orders. From the **Notification Editor**, click the blue **To** button to display the **Recipient Editor**.



| Name | Description | Role | Default Email | + |
|---|---|---|---|---|
| Adam | | Customer Admin | adam@maill.com | + |
| adm | | Customer User | ASDdasd@dsf.com | + |
| A Leader - Not Member of Team | | Customer User | usernoteam@1000teamgroup.qa | + |
| All employees | all people in the company | Customer User | workers@example.com | + |

- **Users**: To add individual users to the recipient list, click the **Users** tab, then either double-click user names to move them to the Recipients list, or select names and click **Add Selected**. Use the search fields provided to search by name or filter using the Criteria Editor. See Filtering Lists for instructions on using search and Criteria Editor tools. To view details about a user, select the name, then click **View Details**. This displays the user’s complete name, default email address, and any other available custom fields.
- **Groups**: To add a group to the recipient list, click a group tab (such as **Broadcast Groups**, **Escalation Groups**, **Smart Groups**). Double-click a group or select groups and click **Add Selected** to add a group to the **Recipients** list.
- **Map-Based Region**: To select users and Sites within a map region, click the **Map Selector** tab, and using the polygon icon draw the region(s) that encompass the users and Sites to be notified. Once the region is drawn, click **Add Polygon(s)** to add the region’s users to the Recipients list. See Send a notification to users within a geographical location for more information on using the map-based selection feature.
- **Delay**: To add a delay between when two users are contacted, click **Add Delay**. The **Add Delay** window displays. Type the length of time of the delay, then click **Save**.

- **Notification Order**: To arrange a specific order in which recipients will be notified, use the **Up** and **Down** arrows to arrange recipients and delay times.

When the **Recipients** list is arranged, click **Save** to return to the Notification Editor.

### Use the Compose To Feature

To quickly compose a notification to any user or group shown in the system:

1. From the left navigation menu **Administration** section, select **Users** (or from the **Groups** section, select the desired group).
2. If you are on the **Users** page, select the individual user(s) to whom you want to send the notification, select the user name and click the **Compose to** option in the menu bar.

If you are on a Groups page, select the individual group(s) to whom you want to send the notification, right click and select the **Compose to** option in the menu list.

A new notification is opened and preloaded with a recipient list containing the selected users or groups.

### Use the Attachments Editor

Use the Attachments Editor to attach files to a notification. From the Notification Editor, click **Attachment**. The **Attachments Editor** displays.

To add an attachment, click **Add**. The **File upload** dialog box is displayed. Click **Add**. A file selection window opens. Navigate to the file to be attached, select it, and click **Open**. The attachment is displayed in the list.

By default, attachments are stored on the server to keep the size of notifications small and to ensure quick delivery.

- To send a copy of an attachment with every message, choose **Include a copy of attachments in each notification**.

CAUTION

Sending large attachments or sending even small attachments to many recipients can quickly overload email servers.

- To keep attachments on the server, choose **Include a link to attachments in each notification**. This allows recipients to access attachments without potentially delaying delivery.

Click **OK** to return to the **Notification Editor**.

### Use the Escalation Editor

Use the Escalation Editor to customize the type of devices or the order in which they are contacted. From the Notification Editor, click **Escalation Override**. The **Escalation Editor** displays.

Select the type of escalation to be used for this notification.

- **Do not override personal device escalations**–Uses the device escalation defined for each individual recipient.
- **Specify a custom device escalation**–Specifies which devices, in which order, should be used for this notification. If this option is selected, the **Edit Custom Escalation** window displays. To create the custom escalation, drag devices from the left section of the window to the name of the custom escalation in the right section of the window. When the escalation is created, click **Save** to return to the Escalation Editor.
- **Skip specified devices in each personal device escalation**–Skips a specific device type, even if it appears in a recipient's personal escalation. If this option is selected, the **Escalation Editor** window displays. Click the check box next to a device type to skip this type of device in every recipient's escalation list. The selected device or devices are not contacted for this notification.

Click **OK** to return to the Notification Editor.

### Use the Language Settings Editor

If language packs have been purchased, to send a notification in another supported language, click the **Language** drop-down list on the **Compose** tab of the Notification Editor. Two options appear: **Language Settings** and **Change default notification language**.

- To change the language for this notification or to make other languages available, click **Language > Language Settings**. Click the check box for all languages to use for this notification.
- To change the default language for this notification, click **Language > Change Default Language** and choose another language from the available list. The default language is used when the notification is not available in a user’s preferred language.
- To view the notification and edit text as it will appear in another supported language, choose a different language from the **View:** drop-down list.

When finished editing the settings in the Language Editor, click **OK** to return to the Notification Editor.

### Supported Audio Files

Only WAV audio files are supported. When call-to-record is used, the recording is saved in the correct format. To create a WAV file using another method, use recording software to confirm that the file is in one of these formats:

- 8bit, 8Khz, u-law wave file (Riff format)
- 16bit, 8Khz, PCM wave file (Riff format)
- 8bit, 8Khz, u-law Sphere file
- 16bit, 8Khz, PCM Sphere file

## View Notifications

This section contains the following topics:

- View a List of Notifications and History
- View Notification Status and Details

## View a List of Notifications and History

To view a list of notifications for a specific team, along with their history, click the name of the team on the **Teams** page. Next, click **Sent Notifications** in the left navigation menu.

The **Sent Notifications** page displays. These notifications can be sorted by clicking on any of the column titles.

To view a list of sent notifications along with their history:

1. From the left navigation menu **Administration** section, click **Teams** to display the **Teams** page.
2. Click the name of the team whose notifications you want to view.
3. From the left navigation menu Notifications section, click **Sent Notifications**. The **Sent Notifications** page displays for the team you have selected. The following fields are displayed on the **Sent Notifications** page:

| Column Heading | Definition |
|---|---|
| **!** | The **!** represents the priority icon that indicates the priority of the notification. |
| **Notification Details** | The subject of the notification, its status (completed, canceled), and the team to which it was sent. |
| **Responses** | The number of notifications confirmed and the number for which no confirmation has been received. |
| **Sender** | The full name of the person who initiated the notification. |
| **Date** | The day, date, time and time zone when the notification was sent. |

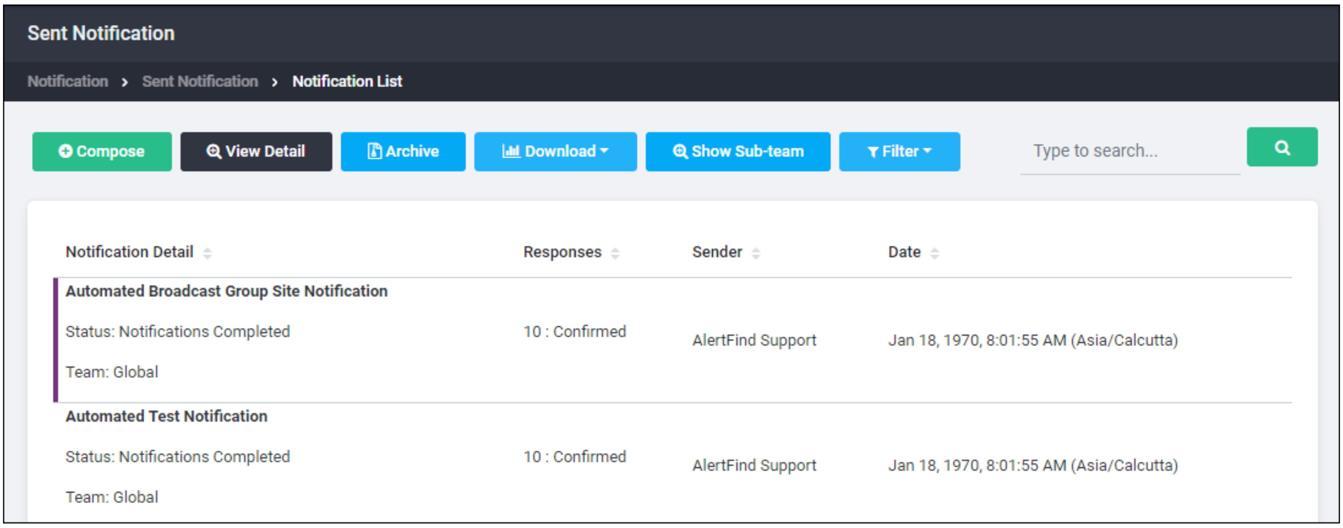
4. To view details about any notification, double-click the notification. The **Viewing Notification** page is displayed.

## View Notification Status and Details

*Notification status* means the state of the notification; that is, whether it is scheduled, completed, or canceled. *Notification details* include the notification results with the response of each recipient listed.

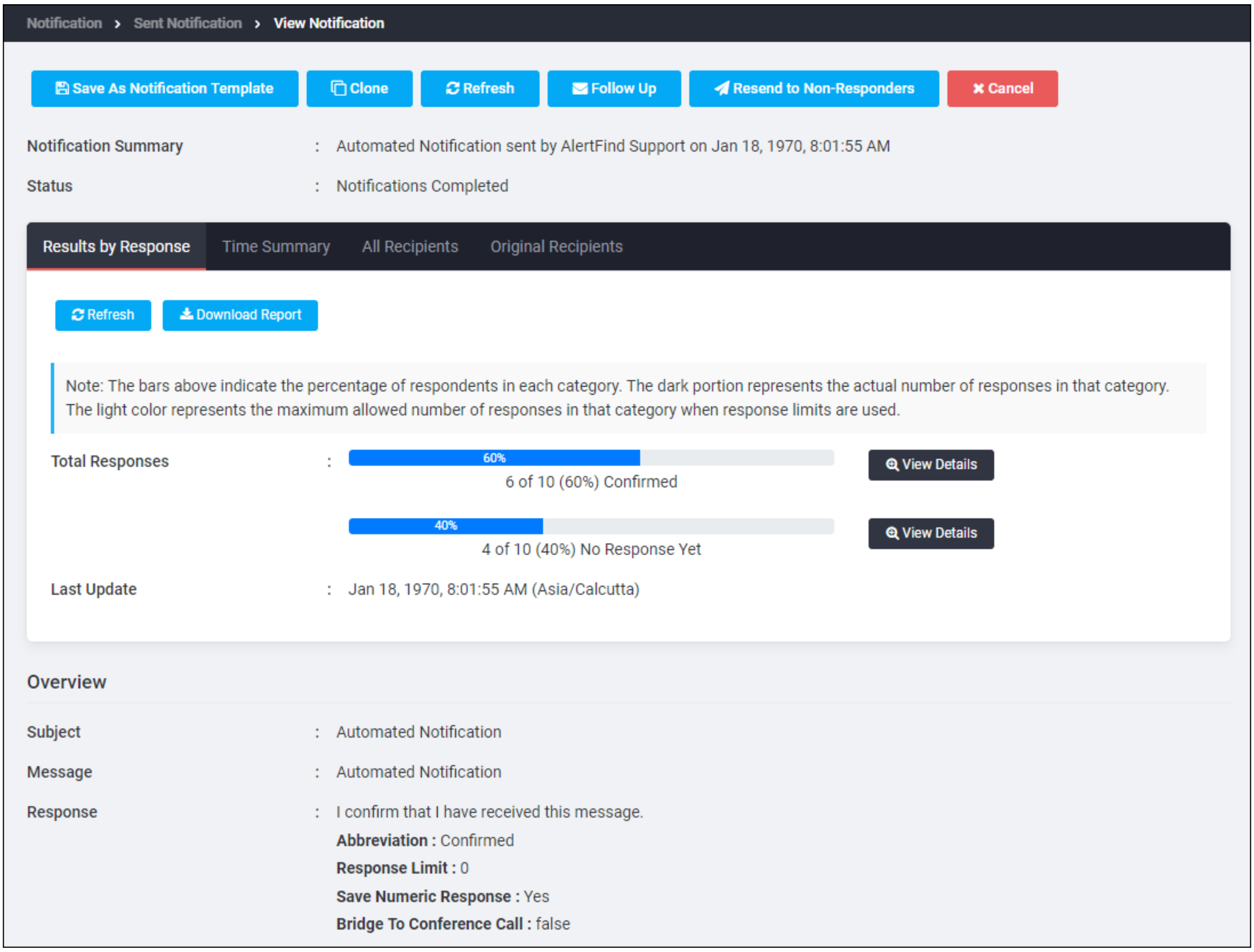
To view the notification status and details:

1. From the left navigation menu **Notifications** section, click **Sent Notifications**. The **Sent Notifications** page for the selected team is displayed. There are four columns of information for each sent notification listing notification summary information: Notification Details, Responses, sender, and date. In the Notification Details column, the subject, status, and team are listed.



| Notification Detail | Responses | Sender | Date |
|---|---|---|---|
| Automated Broadcast Group Site Notification<br>Status: Notifications Completed<br>Team: Global | 10 : Confirmed | AlertFind Support | Jan 18, 1970, 8:01:55 AM (Asia/Calcutta) |
| Automated Test Notification<br>Status: Notifications Completed<br>Team: Global | 10 : Confirmed | AlertFind Support | Jan 18, 1970, 8:01:55 AM (Asia/Calcutta) |

2. Locate the desired notification and double-click it, or click it and then click **View Details**.



Notification Summary : Automated Notification sent by AlertFind Support on Jan 18, 1970, 8:01:55 AM

Status : Notifications Completed

Note: The bars above indicate the percentage of respondents in each category. The dark portion represents the actual number of responses in that category. The light color represents the maximum allowed number of responses in that category when response limits are used.

Total Responses : 6 of 10 (60%) Confirmed

4 of 10 (40%) No Response Yet

Last Update : Jan 18, 1970, 8:01:55 AM (Asia/Calcutta)

Overview

Subject : Automated Notification

Message : Automated Notification

Response : I confirm that I have received this message.

**Abbreviation :** Confirmed

**Response Limit :** 0

**Save Numeric Response :** Yes

**Bridge To Conference Call :** false

3. For the result details, view the four tabs: **Results by Response**, **Time Summary**, **All Recipients** and **Original Recipients**.

   - The **Results by Response** tab describes notifications that have been confirmed, not confirmed, or for which there have been no responses. If the notification is a poll, the number of responses for each option is displayed.
   - Click the **View Details** button next to any response to view more information about respondents.
   - The **Time Summary** tab organizes response information according to how long it took users to respond.
   - The **All Recipients** tab displays an list of individual notification recipients with information about the last update for each recipient and the most recent status of each recipient.
   - The **Original Recipients** tab displays a list of the notification’s original recipients, such as the name of the group or groups that were selected.

6. For other notification details, view the **Notification Details** section.

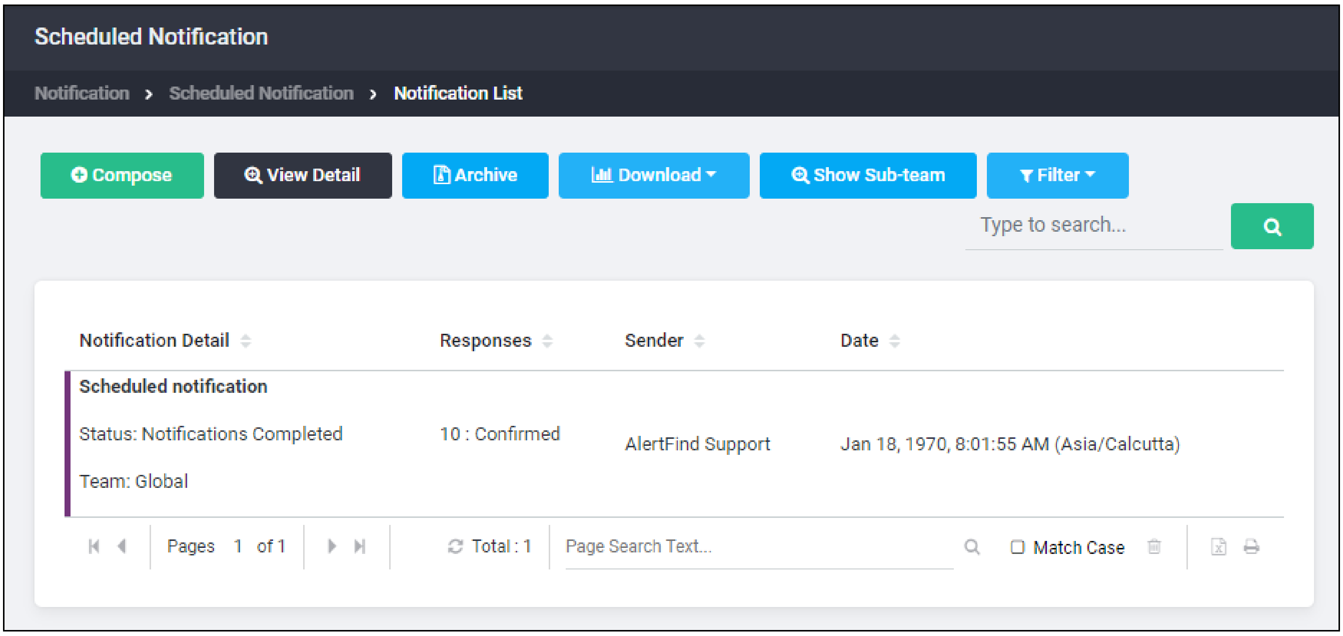
## Work With Scheduled Notifications

This section contains the following topics:

- View and Send Scheduled Notifications
- Manually Send a Notification

## View and Send Scheduled Notifications

The **Scheduled Notifications** page displays notifications scheduled to be sent at a later date or time, as well as those being held for manual execution.



Scheduled Notification

Notification › Scheduled Notification › Notification List

| Notification Detail | Responses | Sender | Date |
|---|---|---|---|
| **Scheduled notification**<br>Status: Notifications Completed<br>Team: Global | 10 : Confirmed | AlertFind Support | Jan 18, 1970, 8:01:55 AM (Asia/Calcutta) |

To view scheduled notifications:

1. From the left navigation menu **Notification** section, select **Scheduled Notifications** to display the **Scheduled Notifications** page.
2. The **Scheduled Notifications** page has the same fields as the Sent Notifications page.
3. To view details about any notification, double-click the notification in the **Notification Details** column or select the notification in the Notification Details column and click the **View Details** button. If the notification is being held for manual execution, if you are ready to send it, click the **edit** button to open the Notification Editor and then click **send**.

### Manually Send a Notification

To send a notification that has been saved as a draft, click **Scheduled Notifications** in the left navigation menu to access the notification and send it.

To manually send a notification:

1. Click **Scheduled Notifications** in the **Navigation** section of the left menu bar. The **Scheduled Notifications** page appears. This page lists the notifications on hold for manual execution or scheduled to be sent in the future.
2. Locate the notification to be sent manually. Double-click the notification in the **Notification Details** column or select the notification in the Notification Details column and click the **View Details** button.
3. Click the **edit** button to open the Notification Editor and then click **send**.

## Resend Notification to Non-Responders

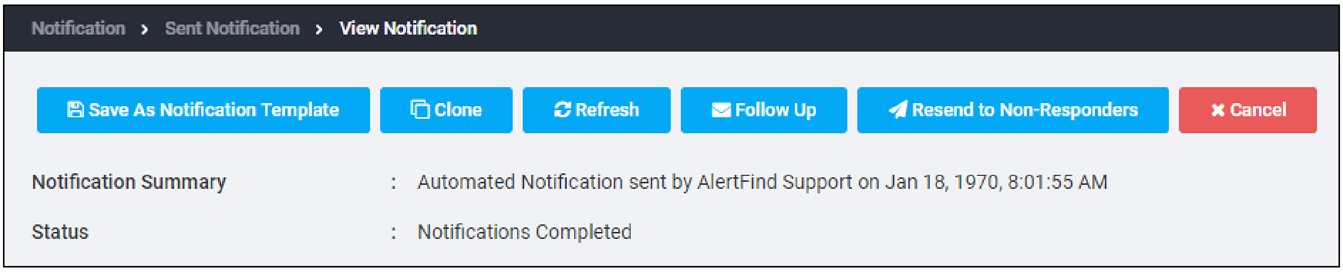
Notifications can be re-sent to users who have not yet responded to the Notification.

- Users who have responded will not receive the resent notification.
- Resent Notifications cannot be edited before they are sent again.

AlertFind considers resent notifications to be part of the original Notification, and tracks them, and their associated responses, as a continuation of the original notification.

To resend notification to non-responders:

1. From the left navigation menu **Notifications** section, click **Sent Notifications** to view the **Sent Notifications** page for the selected team's active, non-archived notifications.
2. Locate the Notification to resend in the Notification Details column, and double-click the subject of the Notification to display the **Viewing Notifications** page.
3. Click the **Resend to Non-responders** button. The re-sent Notification will be sent only to users who did not respond. These users will be listed in the **To...** field.


Notification › Sent Notification › View Notification
Save As Notification Template
Clone
Refresh
Follow Up
Resend to Non-Responders
Cancel

Notification Summary : Automated Notification sent by AlertFind Support on Jan 18, 1970, 8:01:55 AM

Status : Notifications Completed

4. Click **Send** to initiate the resending of the Notification.

The **Result Log** (in the **All Recipients** tab) for each of the non-responders will show the date and time the Notification was resent to that user.

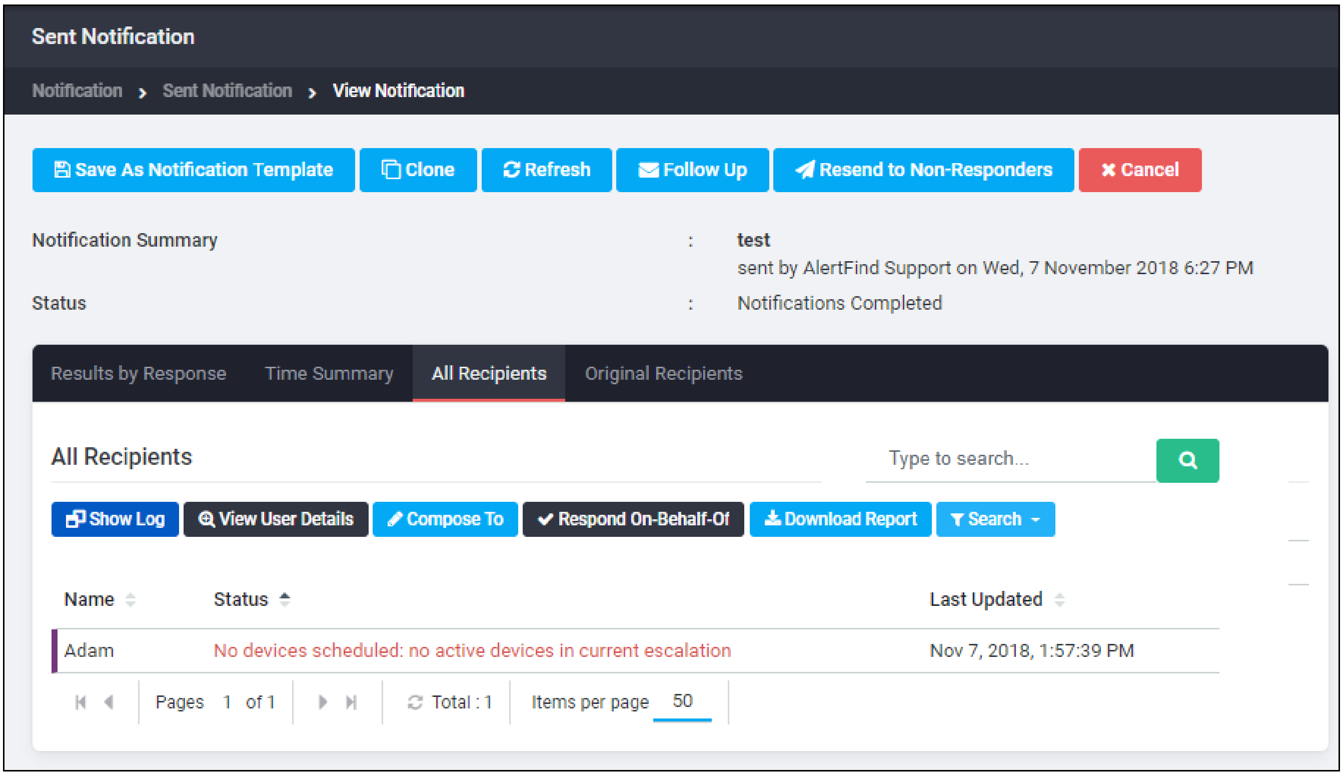
## Respond On Behalf of a User

The ability has been added to manually mark a user as having responded to a Notification. This is useful during real emergencies, when a user may not be able to respond via AlertFind but can check-in with their manager or another person.

Once the feature has been enabled, administrators and team leaders can go to the **View Notification** page, **All Recipients** tab, right-click on the user and select **Respond on-Behalf-Of** from the menu.

To respond on behalf of another recipient:

1. From the left navigation menu **Notifications** section, click **Sent Notifications** to view the **Sent Notifications** page for the selected team's active, non-archived notifications.
2. Locate the Notification that needs to be manually responded to in the Notification Details column, and double-click the subject of the Notification to display the **ViewDetails** page.
3. Click the **All Recipients** tab.
4. Select the user under the **All recipients** list. Multiple users can be selected and manually responded to at one time.



Notification Summary : test
sent by AlertFind Support on Wed, 7 November 2018 6:27 PM

Status : Notifications Completed

| Name | Status | Last Updated |
|---|---|---|
| Adam | No devices scheduled: no active devices in current escalation | Nov 7, 2018, 1:57:39 PM |

5. Click **Respond On-Behalf-Of** to respond to the Notification.
6. Select appropriate response from the drop-down.
7. Add comment if additional information is required.
8. Click **Save**.

The **Result Log** for the recipient(s) will show the date and time the Notification was responded to, and who performed the response.

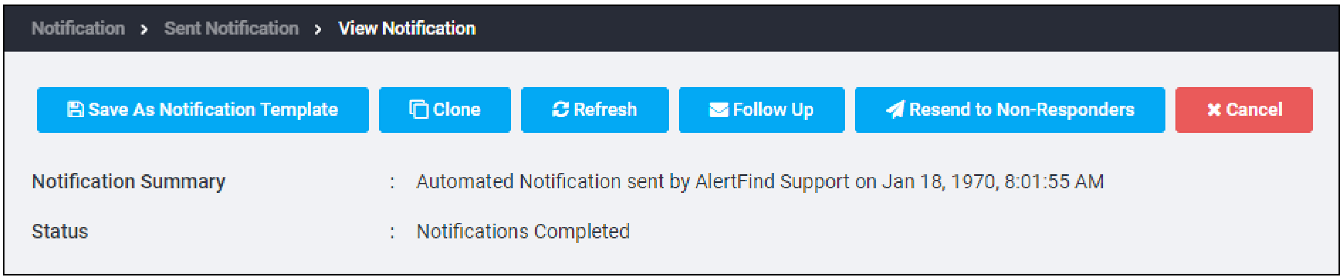
## Send Follow-Up Notifications

Use follow-up notifications to send notifications to recipients of a canceled notification, or to recipients of active or archived notifications who responded with a specific answer.

AlertFind considers follow-ups to be new notifications and tracks them, and their associated responses, separately from the original notification. Compose follow-up notifications using the same process as you would to compose an original notification. All options available to notifications are available to follow-up notifications.

To send follow-up notifications:

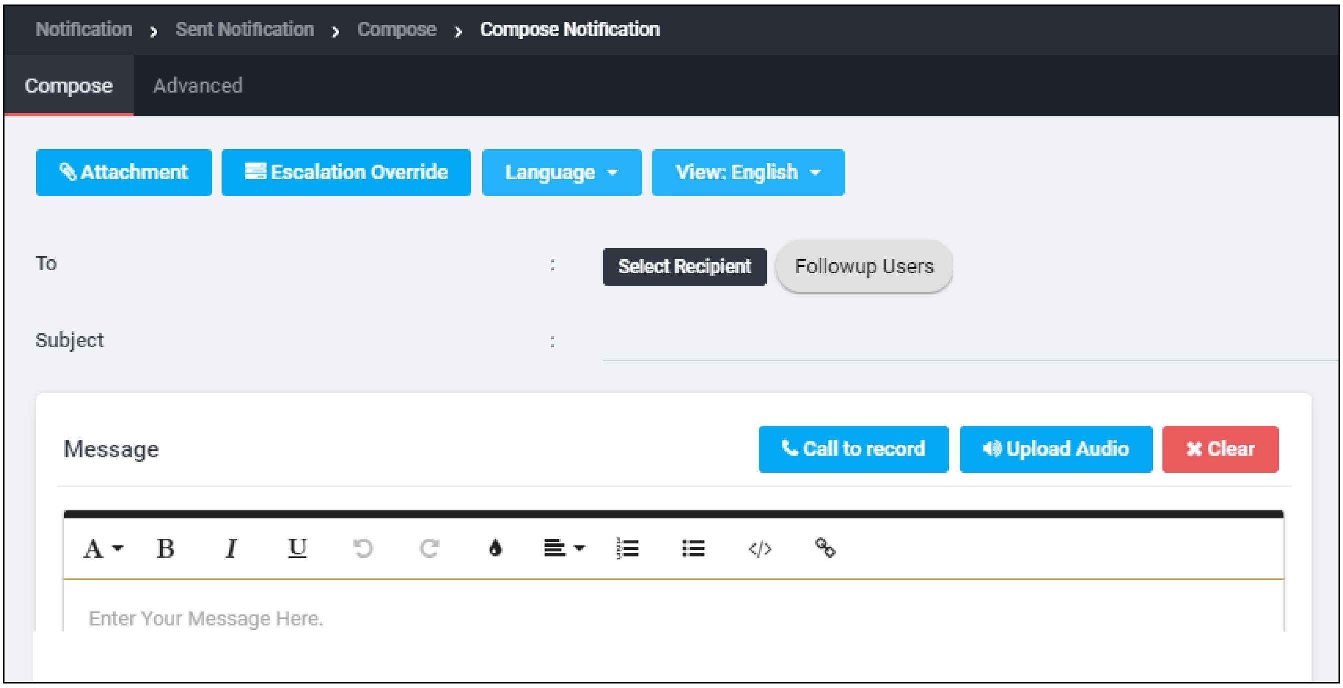
1. From the left navigation menu **Administration** section, click **Teams**, and then from the page displayed, select the desired team to view its notifications.
2. To send a follow-up for a completed or canceled Notification, from the left navigation menu, **Notifications** section, click **Sent Notifications**. To send a follow-up for an archived Notification, from the left navigation menu, **Notifications** section, click **Archived Notifications**.
3. Locate the Notification to send a follow-up notification.
4. In the Notification Details column, double-click the subject of the notification to display the **Viewing Notifications** page.
5. To send a follow-up Notification to non-responders, click the **Follow Up** button, *OR*, to send a follow-up Notification to a specific set of responders:


Notification › Sent Notification › View Notification
Save As Notification Template
Clone
Refresh
Follow Up
Resend to Non-Responders
✖ Cancel

Notification Summary : Automated Notification sent by AlertFind Support on Jan 18, 1970, 8:01:55 AM

Status : Notifications Completed

1. In the Total Responses list, click the **View Details** button next to the response for which you want to send a follow-up.
2. Click the **Follow-up** button.



To : Select Recipient Followup Users

Subject :

Message

6. The **Notification Editor** displays. By default, the follow-up notification will be sent to a dynamically created Ad Hoc Group consisting of the original recipients and called `Follow-up Users`.
7. Compose the notification as discussed in Compose Notification.
8. Click **Send** to initiate the follow-up notification.

If desired, repeat this process to send follow-up notifications to users who responded with a different response.

## Cancel a Notification

An in-progress, completed, or scheduled notification can be canceled. This might be needed if:

- The wrong notification was sent.
- The situation has changed and the notification is no longer relevant.
- A poll or survey notification was sent and received an adequate number of responses.

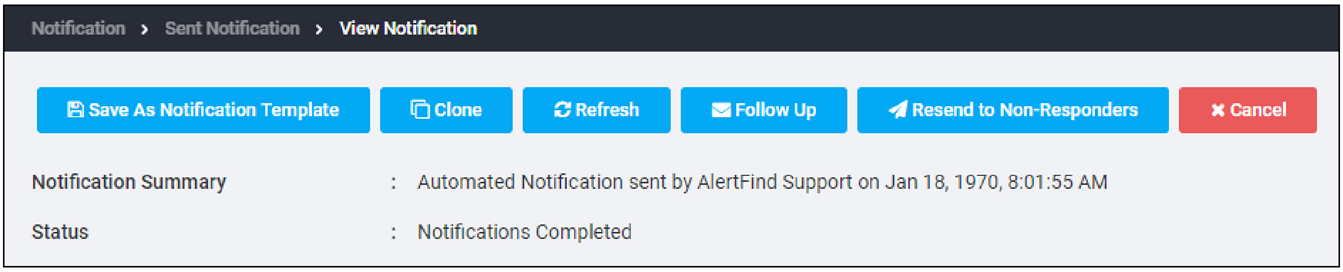
After a notification is canceled, the cancellation cannot be undone. To reach recipients who did not receive the canceled message, a new notification must be sent.

### NOTE

When a notification is canceled, AlertFind still accepts responses from email devices and from the web confirmation page for recipients who received the message before it was canceled. However, recipients cannot continue to respond to the notification through Hotline or Hotline Pro.

To cancel a notification from the Sent Notifications page:

1. From the left navigation menu **Administration** section, click **Teams**, and then from the page displayed, select the team for which you want to view notifications.
2. From the left navigation menu **Notifications** section, click **Sent Notifications** to view the **Sent Notifications** page for the selected team's active, non-archived notifications.
3. Double-click the notification you want to cancel or click the notification and click **View Details** to open the notification in the **Viewing Notification** window.
4. Click the **Cancel** button next to the **Status** field.


Notification › Sent Notification › View Notification
Save As Notification Template
Clone
Refresh
Follow Up
Resend to Non-Responders
Cancel

Notification Summary : Automated Notification sent by AlertFind Support on Jan 18, 1970, 8:01:55 AM

Status : Notifications Completed

5. A confirmation box displays. Click the **OK** button to cancel the notification.

Once the notification is canceled, the Sent Notifications page will display a status of Canceled and the name of the user who canceled it and the Notification Details page will also display the time the notification was canceled.

### NOTE

When a notification is canceled processing will stop, and no more messages are sent to any remaining recipients. To reach recipients who did not receive the canceled message, a new notification must be sent.

To cancel an active, in-progress notification by archiving it, see Archive Notifications.

## Archive Notifications

Any notification can be archived, including those that have been canceled. Archiving removes the notification from the **Sent Notifications** or **scheduled Notifications** page and cancels any notification that is in progress. Completed notifications are moved to the archive with the status of completed. You may want to archive notifications that you no longer need to view, or to shorten the list displayed on the **Sent Notifications** page.

To archive a notification:

1. From the left navigation menu Administration section, click **Teams**, and then from the page displayed, select the team for which you want to view notifications.
2. From the left navigation menu Notifications section, click **Sent Notifications** to view the **Sent Notifications** page for the selected team’s active, non-archived notifications.
3. Select the notification that you want to archive.
4. Click **Archive** on the menu bar. The **Confirm** dialog is displayed.
5. Click **OK** to archive the notification or **Cancel** to cancel the action.

If **OK** was clicked, that notification is removed from the **Sent Notifications** page and now appears on the **Archived Notifications** page.

NOTE

You can also batch archive or batch unarchive notifications by selecting more than one notification at a time and then clicking **Archive** (if you are on the Sent Notifications page) or **Un-archive** if you are on the **Archived Notifications** page.

### View Archived Notifications

A list of archived notifications can be viewed with the following information for each notification:

- Notification Details (Subject and Status)
- Responses
- Sender
- Date and Time Sent

To view the list of archived notifications:

1. From the left navigation menu **Administration** section, click **Teams**, and then from the page displayed, select the team for which you want to view notifications.
2. From the left navigation menu **Notifications** section, click **Archived Notifications**. The list of archived notifications is displayed.

You can download either a CSV summary report or a CSV detailed report of the archived notifications. Click **Download** and select either **Notification List Summary Report** or **Notification List Detailed Report** to view the respective report.

To send follow-up notifications, see Send Follow-Up Notifications.

### Unarchive a Notification

Unarchiving a notification makes it visible on the list of sent notifications, but does not activate the notification or make it available for sending. It is still considered a completed or canceled notification.

To unarchive an archived notification:

1. From the left navigation menu **Administration** section, click **Teams**, and then from the page displayed, select the team for which you want to view notifications.
2. From the left navigation menu **Notifications** section, click **Archived Notifications**. The list of archived notifications is displayed.
3. Select the archived notification to be unarchived.
4. Click **Un-archive** near the top of the page. Answer **OK** to the confirmation dialog. The notification is unarchived and is now listed on the Sent Notifications page.

## Notification Reports

This section contains the following topics:

- Email Results of Completed Notifications
- Download Notification Details

## Email Results of Completed Notifications

A notification is considered *complete* when AlertFind has successfully sent the notification to all scheduled devices or exhausted the escalation for each user.

For individual notification tasks (a notification to a specific device), the type of device contacted determines when the task is complete:

- An email notification is complete when the email is sent.
- A phone notification is complete when AlertFind reaches a person or leaves a voice mail.
- An SMS notification is complete when the device has been reached.
- A fax notification is complete when the device has been reached.
- A pager notification is complete when the device has been reached.

Three CSV-formatted results files can be emailed to a designated individual (or distribution list). These include:

- `NotificationResponses.csv`
- `NotificationTimeHistogram.csv`
- `NotificationRecipients.csv`

The CSV files emailed are identical to the download reports available on the **Sent Notifications** page.

### NotificationResponses.csv

The *Notification Responses Report* contains the following information:

- Subject of the notification
- Sent Time
- Expire, if set
- Recurrence, if set
- Sender (full name of the person who sent the message)
- Message (text of the message)
- Priority, if set
- Authenticated (whether authentication was required for this notification)
- Response Limit Handling
- Hotline, if available (use User’s Default Hotline, Use all Hotlines, or Do not allow responses through the Hotline)
- Email Results (to whom)
- Current Status of the notification
- Response Summary for the notification

        - Abbreviation
        - Count of this response
        - Limit (if one exists)
        - Bridge (to conference call)
        - Data (entered by recipient)
        - Description
- Details for each response
    - Name of recipient
    - External Key
    - Last Update
    - Response
    - Data (entered by recipient)
    - Status of notification task for this recipient
    - Last Confirmed Device Name
    - Last Confirmed Device Address
    - Last Confirmed Hotline Label
    - Last Confirmed Hotline Number Label
    - Last Confirmed Hotline Number

**NotificationTimeHistogram.csv**

The *Notification Response Time Report* contains the following information:

- Subject
- Sent Time
- Expire, if set
- Recurrence, if set
- Message (set to `recorded audio` if a recorded message was used for the notification)
- Priority
- Authenticated
- Response Limit Handling
- Hotline, if available (use User’s Default Hotline, Use all Hotlines, or Do not allow responses through the Hotline)
- Email results (to whom and at what address)
- Current Status of the notification
- Response Summary

  - Confirmed
    - Number of the response
    - Abbreviation of the response
    - Count of this response
    - Limit (if one exists)
    - Bridge (to conference call)
    - Data (entered by recipient)
    - Description (the response)
  - No response yet
  - Total
- Response Time Summary (in 5 minute increments)
- Total responses

#### NotificationRecipients.csv

The *Notification Recipients Report* includes details about each recipient's specific response information. The following information is included in the `NotificationsReceipients.csv` file:

- Subject
- Sent Time
- Expire, if set
- Recurrence, if set
- Message (set to `recorded audio` if a recorded message was used for the notification)
- Priority
- Authenticated
- Response Limit Handling
- Hotline, if available (use User's Default Hotline, Use all Hotlines, or Do not allow responses through the Hotline)
- Email results (to whom and at what address)
- Current Status of the notification
- Response Summary
  - Confirmed
    - Number of the response
    - Abbreviation of the response
    - Count of this response

        - Limit (if one exists)
        - Bridge (to conference call)
        - Data (entered by recipient)
        - Description (the response)
    - No response yet
- Information about each recipient
    - Name
    - External key
    - Description
    - Last Update (for example, Tue May 8 2017 4:23:44 PM)
    - Response
    - Data (entered by recipient)
    - Status of notification task
    - Last Confirmed Device Name
    - Last Confirmed Device Address
    - Last Confirmed Hotline Label
    - Last Confirmed Hotline Number Label
    - Last Confirmed Hotline Number

### Download Notification Details

A CSV summary report can be downloaded for all sent notifications, either in summary or individually.

To download notification details:

1. From the left navigation menu **Administration** section, click **Teams**.
2. Select the desired team.
3. From the left navigation menu **Notifications** section, click **Sent Notifications**. The **Sent Notifications** page is displayed for the selected team's active, non-archived notifications.
4. Click **Download** in the menu bar. You have the option to download either the **Notification List Summary Report** or **Notification List Detailed Report**.

A **File Download** dialog box is displayed requesting whether you want to open the CSV file, save it, or cancel the action. If you click **Save File**, the report file is automatically saved to your default Download directory. The default file name is **Notification List.csv**.

You can also download the summary of a single notification by performing the following additional steps:

1. In the **Sent Notifications** page, select your desired active, non-archived notification and view its details.
2. In the **Results by Response** tab, click the **Download Report** button.

A **File Download** dialog box is displayed requesting whether you want to open the CSV file, save it, or cancel the action. If you click **Save File**, the report file is automatically saved to your default Download directory. The default file name is **Notification List.csv**.

# Notification Templates

Notification Templates are used to create communication plans with pre-configured Notifications that can be sent simultaneously, making crisis communications consistent, quicker and more effective.

If the template has the **Enable Editing** option checked, the Notification’s subject, recipients, and message can be edited from the Alert Console at the time the Notifications are to be sent, without effecting the original template.

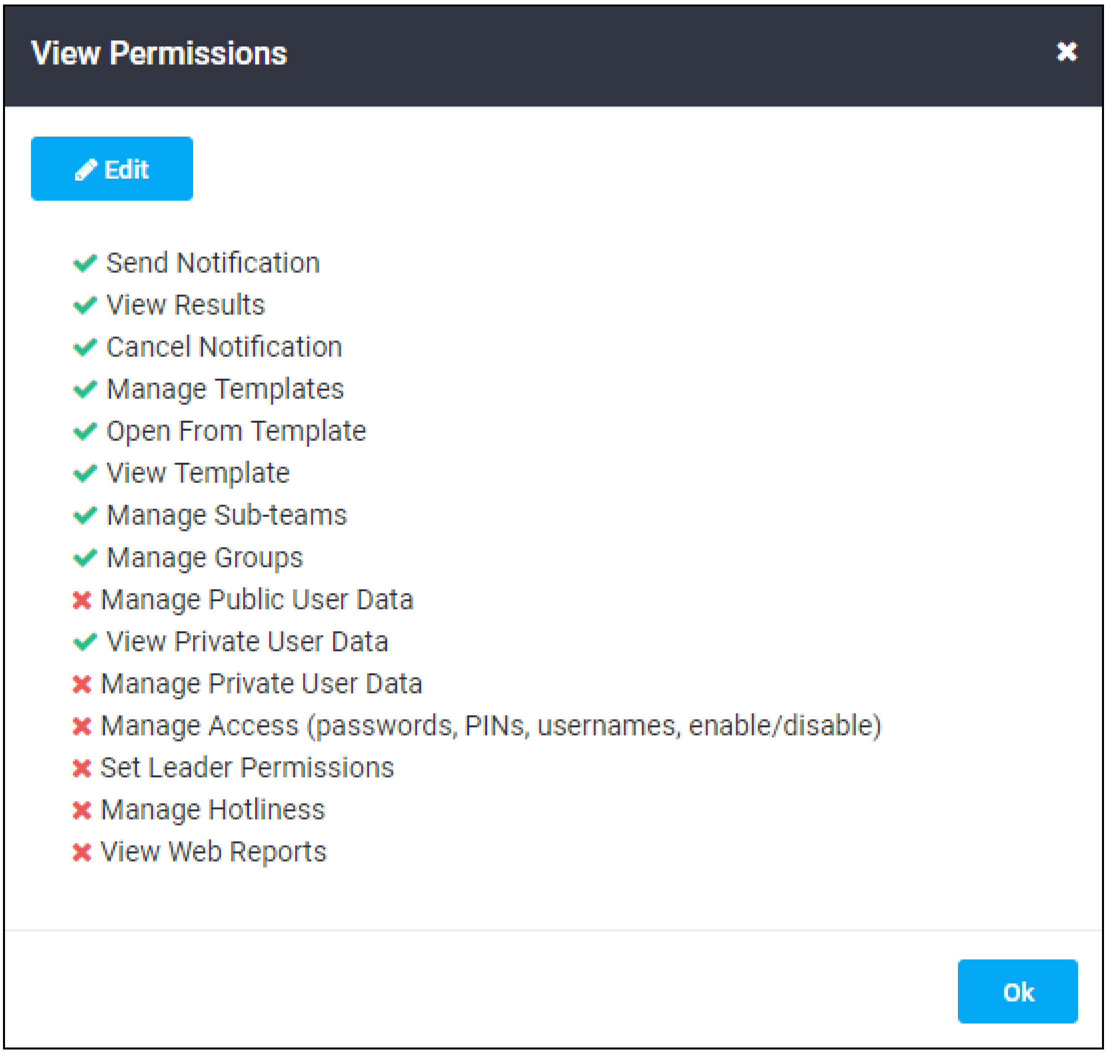
Notification Templates also make it easy to link Notifications to Incidents since they can automatically create an incident if you select that feature in the template.

## Manage Template Permissions

To use the **Notifications Template** library, you must have the **Manage Templates** permission for the team you are on. Administrators and Team Leaders can have this permission enabled.

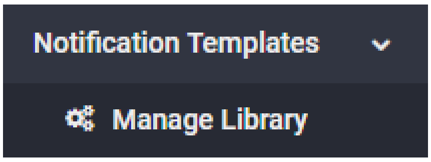
To see what permissions you have:

1. In the left menu bar in the **Administration** section, select **My Account**.
2. In the **User Overview** menu bar, click **View Permissions**. In the following example of an Administrator's permissions on Team Global, all the permissions are selected. The **Manage Templates** permission is the one singled out by the red rectangle.



- ✓ Send Notification
- ✓ View Results
- ✓ Cancel Notification
- ✓ Manage Templates
- ✓ Open From Template
- ✓ View Template
- ✓ Manage Sub-teams
- ✓ Manage Groups
- ✖ Manage Public User Data
- ✓ View Private User Data
- ✖ Manage Private User Data
- ✖ Manage Access (passwords, PINs, usernames, enable/disable)
- ✖ Set Leader Permissions
- ✖ Manage Hotliness
- ✖ View Web Reports

If you have the **Manage Templates** permission, you will get the **Manage Library** option in your left navigation menu.



With this option, you can view, edit, create, and delete the notification templates for the team that is your current team context. These templates are stored in the selected team's **Notification Templates** library page.

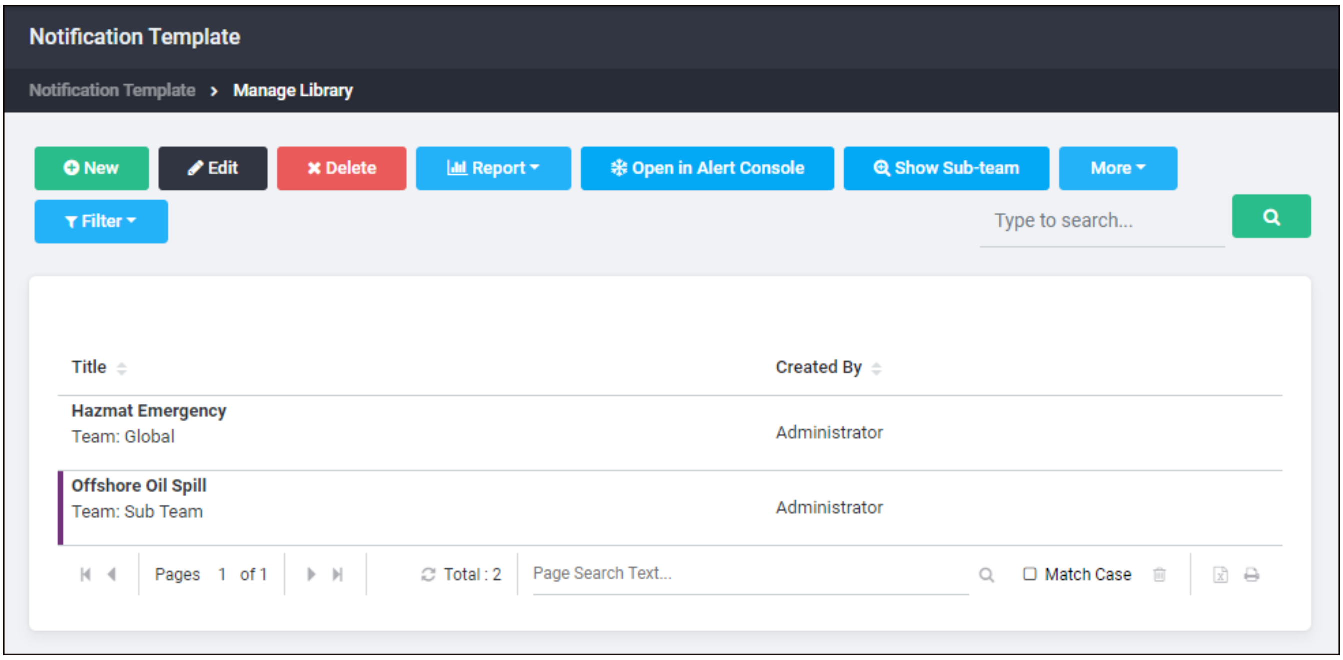
Without the **Manage Templates** permission, you will not get the **Manage Library** menu option, nor will you be able to view, edit, create, or delete notification templates.

## View a List of Notification Templates

Each team has a different notification template library. If the list of notification templates does not appear correct, check your team context.

### See the template library for your team:

1. In the left menu bar **Administration** section, select **Teams** to display **My Teams** page.
2. On the **My Teams** page, select the desired team.
3. In the left menu bar **Notifications** section, select **Manage Library**.The following is an example list of templates on the **Notification Templates** page of a team library.



| Title | Created By |
|---|---|
| **Hazmat Emergency**<br>Team: Global | Administrator |
| **Offshore Oil Spill**<br>Team: Sub Team | Administrator |

### See the sub-teams' templates:

Normally, the Notification Templates listed belong only to the explicit team context. If you also want to see all the notification templates that belong to all the sub-teams of the selected team, go to the **Notification Templates** page, and click the **Show Sub-Team** button. The list updates to include all Notification Templates that belong to the current team and all subordinate teams that you have permission to view. A subordinate team does not list templates that belong to a superior team. The Global team context can view all Notification Templates.

To hide the templates for the sub-teams, click the **Show Sub-Team** button again.

### See the template library for a different team:

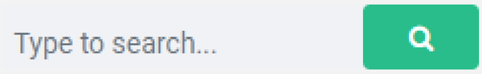
1. In the left menu bar **Administration** section, select **Teams** to display the **My Teams** page.

2. On the **My Teams** page, select the desired team.
3. In the left menu bar **Notification Templates** section, select **Manage Library**.

## The Notification Templates Tool Bar

The following table lists the **Notification Templates** page tool bar options:

| Option/Buttons | Function |
|---|---|
| ⊕ New | To create a new template, click **New**. A new template is opened ready for input. See Create a New Notification Template. |
| ✎ Edit | To edit an existing template, select it and click **Edit**. The selected template is opened ready for editing. See Edit a Notification Template. |
| ✖ Delete | To delete a template, select it and click **Delete**. The selected template is deleted from the **Notification Templates** library page where it was stored. See Delete a Notification Template. |
| 📊 Report ▾ | To download a template report, click the down arrow next to the **Report** button. You have two choices:<br>• A **Detailed Report** of a selected template.<br>• A **List Summary Report** of all the templates.<br>See Downloading Notification Template Reports. |
| ❄ Open in Alert Console | To open a template in the Alert Console, click **Open in Alert Console**.<br>See Edit and Send a Notification(s) from a Notification Template |
| 🔍 Show Sub-team | To display your sub-team's notification templates, click **Show Sub-team**. Click the button again to hide sub-teams' templates.<br>See See the sub-teams' templates: |
| More ▾ | To clone one or more Notification Templates to new team(s), select the template(s) to clone, click **More...** > **Clone to Team(s)**, select the team or teams, click **Clone**.<br>See Clone Notification Template to Team(s) |
| ▼ Filter ▾ | To Filter the templates available use the **Search Criteria** to add new filter criteria to narrow down the items displayed. |

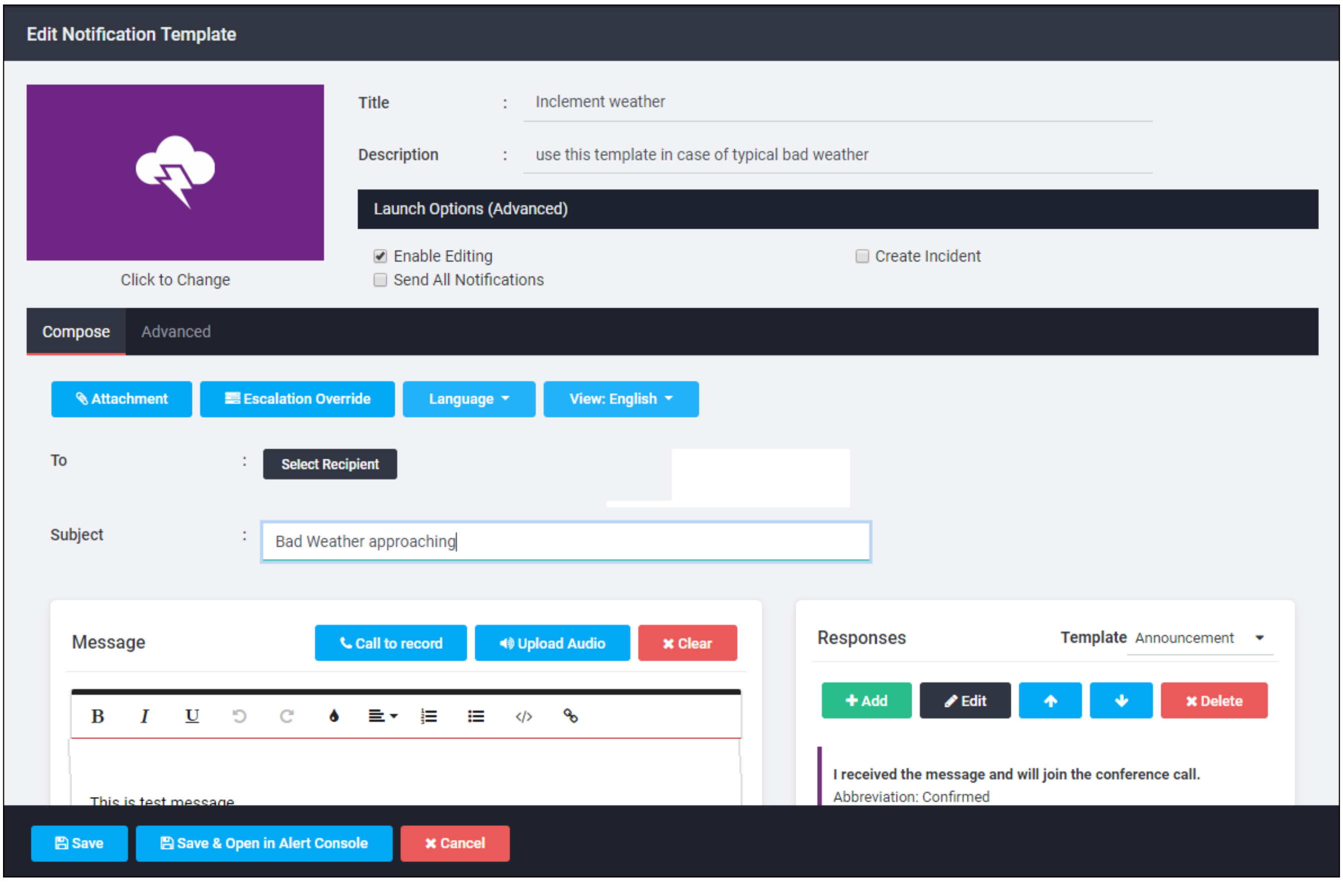
| Option/Buttons | Function |
|---|---|
|  | To find a template by template title, enter the title or part of the title in the **Search** box. To search by a custom field, click the down arrow. You then have the choice of searching by Description, Quick Launch ID, or Title. |

## View a Notification Template

To view a notification template:

1. Go to your team's **Notification Templates** page. See View a List of Notification Templates.
2. Double-click the template you want to view.

The following is an example notification template.



Title : Inclement weather

Description : use this template in case of typical bad weather

☑ Enable Editing
□ Send All Notifications
□ Create Incident

To :

Subject : Bad Weather approaching

This is test message

Template Announcement

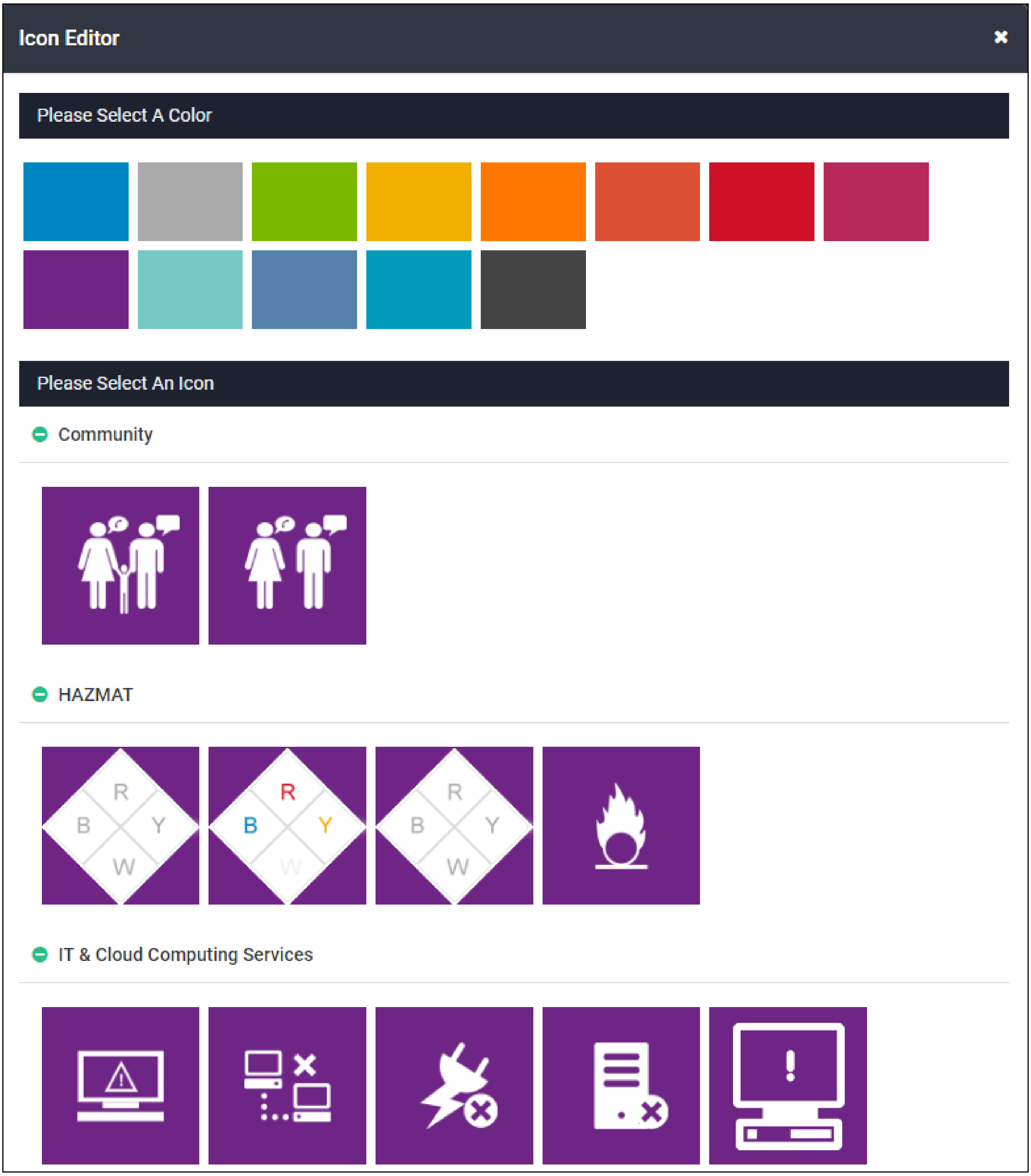
I received the message and will join the conference call.
Abbreviation: Confirmed

## Select a Template Icon

The template icon along with the template name is displayed in the **Alert Console** page to allow a person to select that template to send one or more notifications.

To select an icon and tile color for a notification template:

1. When in the **Creating Notification Template** or the **Editing Notification Template** window, click the template icon to display the Icon Editor window with a list of all available icons and colors.



2. In the **Icon Editor** window color selection box, select an icon color.
3. In the **Icon Editor** window icon selection box, click an icon to use it as the icon associated with this notification template in the Alert Console.

## Select Template Launch Options

Each notification template has the following **advanced** options called **Launch Options**. These are used when a template notification(s) is sent from the Alert Console.

To select an option, click on the check box next to it and a check mark will be displayed in it. To deselect it, click again, and the check mark will be removed:

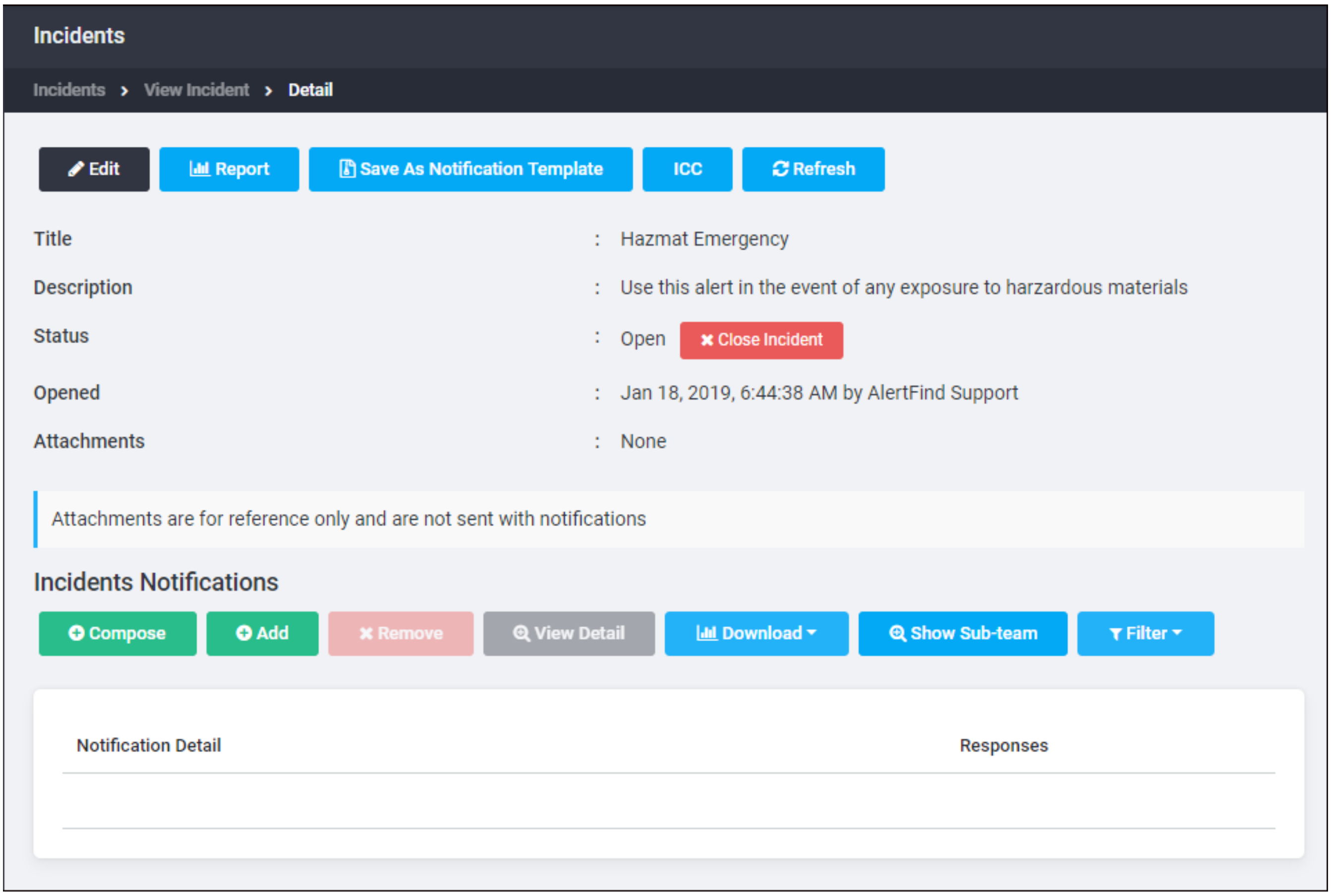
| Option | Description |
|---|---|
| **Enable Editing** | To allow the person sending this notification from the **Alert Console** to edit or change the notification subject, recipients, and message, check this option.<br>This does not change the template itself. Rather, it enables the sender of the notification to make edits to this specific notification prior to sending. The notification template will remain unchanged.<br>For example, if you created an Inclement Weather notification template and had **Enable Editing** checked in the template, then when sending the notification from the **Alert Console**, the person sending the notification could change the message body to include the specific office location that is affected. In this case, the sent notification would say Inclement Weather, but the message body would have more specific site information. |
| **Send All Notifications** | To require that all the notifications linked to this template be sent at the same time, check this option.<br>An example of when this might be appropriate is when you want to send one message to activate the crisis response team and another general message to employees. Both notifications have to go out.<br>When this is *unchecked*, AlertFind will send only the selected notification and not any others that are linked to the template. An example of when this is appropriate is the **Hurricane Alert** notification template. In this template, **Send All Notifications** is *unchecked*. This means, when people select this template from the **Alert Console**, they must pick one of the available Hurricane Notifications to send. They cannot send more than one notification at the same time. |
| **Quick Launch ID** | To have the notification sent over a Hotline and as a text message, enter a **Quick Launch ID**. You can have the system generate one or you can create one of your own. For example, 1001 or BADWEATHER. This option is not available unless you check **Send All Notifications**. |

| Option | Description |
|---|---|
| Create Incident | To automatically create an incident when this template notification(s) is sent from the **Alert Console**, check **Create Incident**.<br>In this case an open incident is automatically created, linked to the template's notification(s), and listed on the AlertFind**Incidents** page when the notification(s) is sent.<br>If you check this option, you will be prompted for adding attachment(s) to the template. You can add up to 5 attachments of up to 50 MB.<br>The following task example is of an incident automatically created by the **Hazmat Emergency** alert when it was sent. |

To see an automatically created incident:

1. From the left menu bar, in the Incidents section, select **Incidents**. This displays a page of all listed Incidents.
2. To see the created incident, double-click the new incident (or select it and click **View Details**) to view it.

The following is an example of an incident automatically created by the **Hazmat Emergency** alert when it was sent.



Title : Hazmat Emergency

Description : Use this alert in the event of any exposure to harzardous materials

Status : Open

Opened : Jan 18, 2019, 6:44:38 AM by AlertFind Support

Attachments : None

Attachments are for reference only and are not sent with notifications

The incident takes on the title of the notification template along with its description. Any attachments and all notifications linked to the incident are listed.

Incident templates created prior to AlertFind 5.0 work the same way they previously worked. However, they will also have the new advanced launch options. In this case, **Enable Editing** is turned off by default and **Send All Notifications** and **Create Incident** are turned on by default. If needed, you can edit these options.

## Save Multiple Notifications to a Template

A template can have more than one notification linked to it. This means that you can model a template:

- To send one and only one notification. In this case, the **Send All Notifications** launch option is not selected and there is only one notification linked to the template.
- To send one notification, but which can be different depending on the situation. In this case, the **Send All Notifications** launch option is not selected and only one of several notifications linked to the template is selected.
- To send different notifications at the same time to different people, each with different tasks. In this case, the **Send All Notifications** launch option is selected and several notifications are linked to the template.

### Compose a template notification:

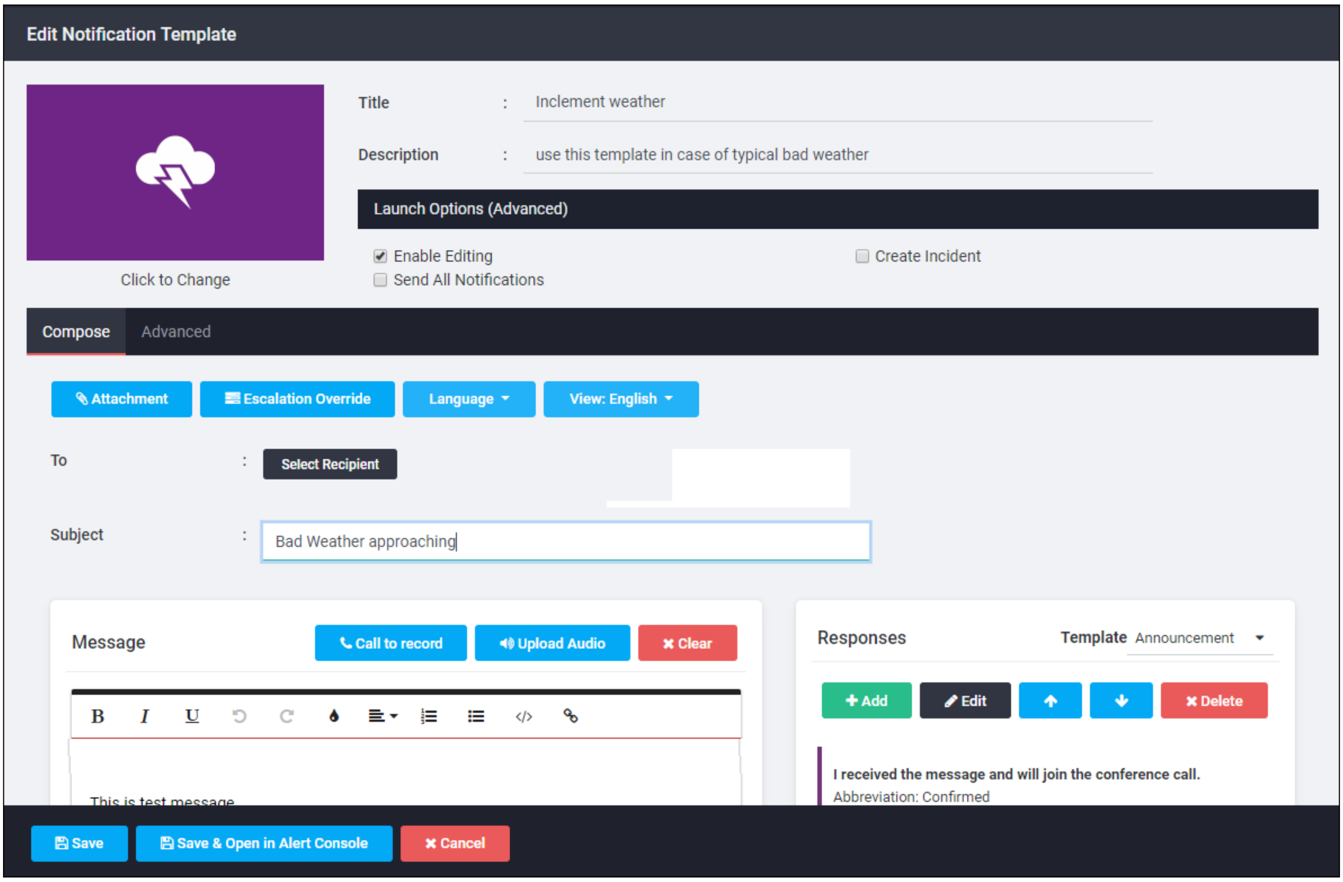
Use the features on the **Compose** and **Advanced Options** tabs. For a description of these features, see Compose Notification.

1. In the **Compose** tab, click **To...** to select the notification recipients.
2. In the **Subject** line, enter a notification subject.
3. In the **Message** text box, enter a notification message.
4. In the **Responses** text box, click **New** to enter a new response, or click **Edit** to enter the default one.
5. In the **Advanced Options** tab:
   - Click **Scheduling** to set up the notification schedule and recurrence.
   - Click **Email Status** to set up emailing the results of this notification.
   - Click **Normal** to select a priority for the notification.
   - Click **Require Pin** to require a pin for this notification.
   - Click **Hotline** to set up hotline call back instructions.
   - Click **Device Retry** to set up the maximum number of call retries.

### Add a second notification to a template:

1. Click the **More Notifications** button at the bottom of the **Notification Templates** window.
2. In the Notifications list box, click **New** to create a totally new notification, click **Clone** to create a copy of the currently open notification.
3. Create the new notification, or edit the cloned notification, as you would create or edit any notification.
4. When you have finished creating notifications, all of them are listed in the template **Notifications** list box. These notifications are linked to this

notification template. The following is an example of an **Inclement Weather** template having a list of notifications.



Edit Notification Template

Title : Inclement weather

Description : use this template in case of typical bad weather

Launch Options (Advanced)

☑ Enable Editing
☐ Send All Notifications
☐ Create Incident

To : Select Recipient

Subject : Bad Weather approaching

Message

This is test message

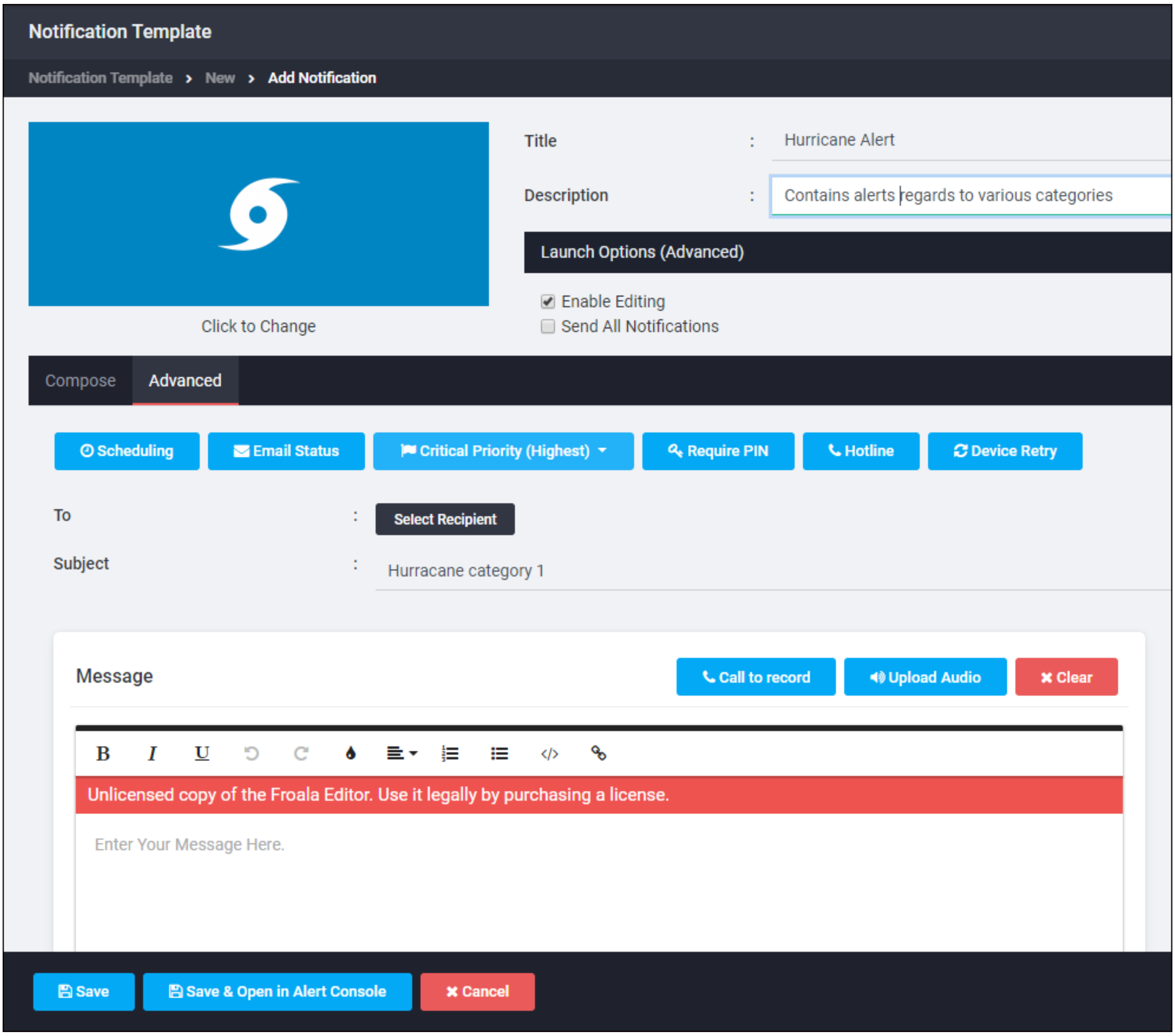
Responses Template Announcement

I received the message and will join the conference call.
Abbreviation: Confirmed

5. When you are finished with the template, click **Save & Close** to save it in the template library and close it or click **Save & Open in the Alert Console** to save it in the template library and to review it in the Alert Console.

Notification templates enable you to send out a series of different communications related to an incident all at the same time. This is the case in the following example since the **Send All Notifications** launch option is selected.

In the following example of a Hurricane Alert, the **Send All Notifications** option is not selected. In this example, only the Hurricane Alert for a Category 1 notification, the selected notification, would be sent.



Title : Hurricane Alert

Description : Contains alerts regards to various categories

☑ Enable Editing

□ Send All Notifications

To :

Subject : Hurracane category 1

Unlicensed copy of the Froala Editor. Use it legally by purchasing a license.

Enter Your Message Here.

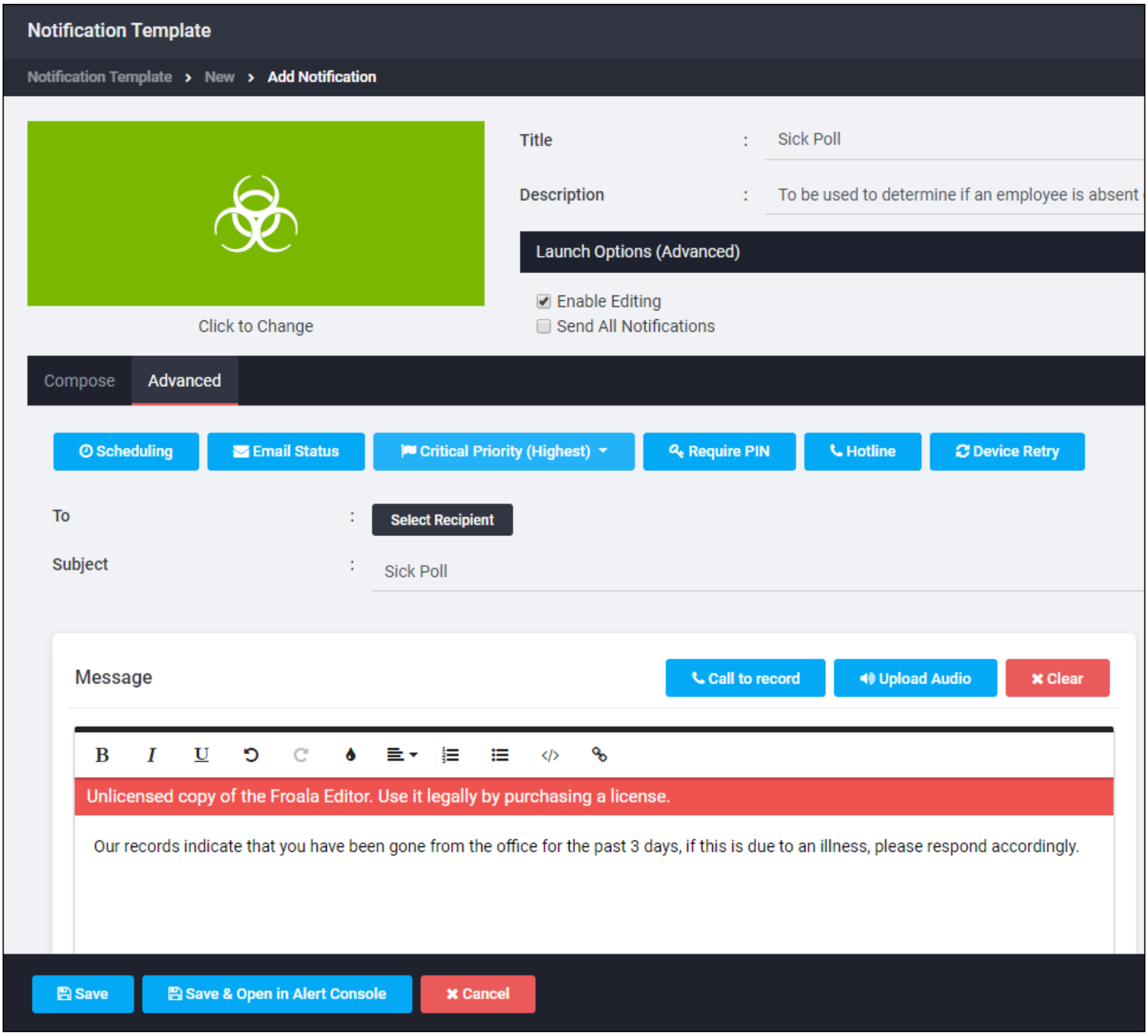
You can also delete a notification by selecting a notification in the template **Notifications** list box and clicking **Delete**.

You can choose to hide the notifications list by clicking **Hide Notifications** at the bottom left of the **Notifications** list box.

### The Notification Display When Opening a Template

Depending on the number of notifications linked to a template, the notification display for the template is different when opening the template:

- If a template has only one notification linked to it, when you open the template, the template **Notifications** list is hidden and the **More Notifications** button is displayed at the bottom left of the template window. An example of this is the **Sick Pole** template. In this example, the **More Notifications** button is singled out by the red rectangle.



Notification Template

Notification Template > New > Add Notification

Title : Sick Poll

Description : To be used to determine if an employee is absent

Launch Options (Advanced)

☑ Enable Editing
☐ Send All Notifications

To : Select Recipient

Subject : Sick Poll

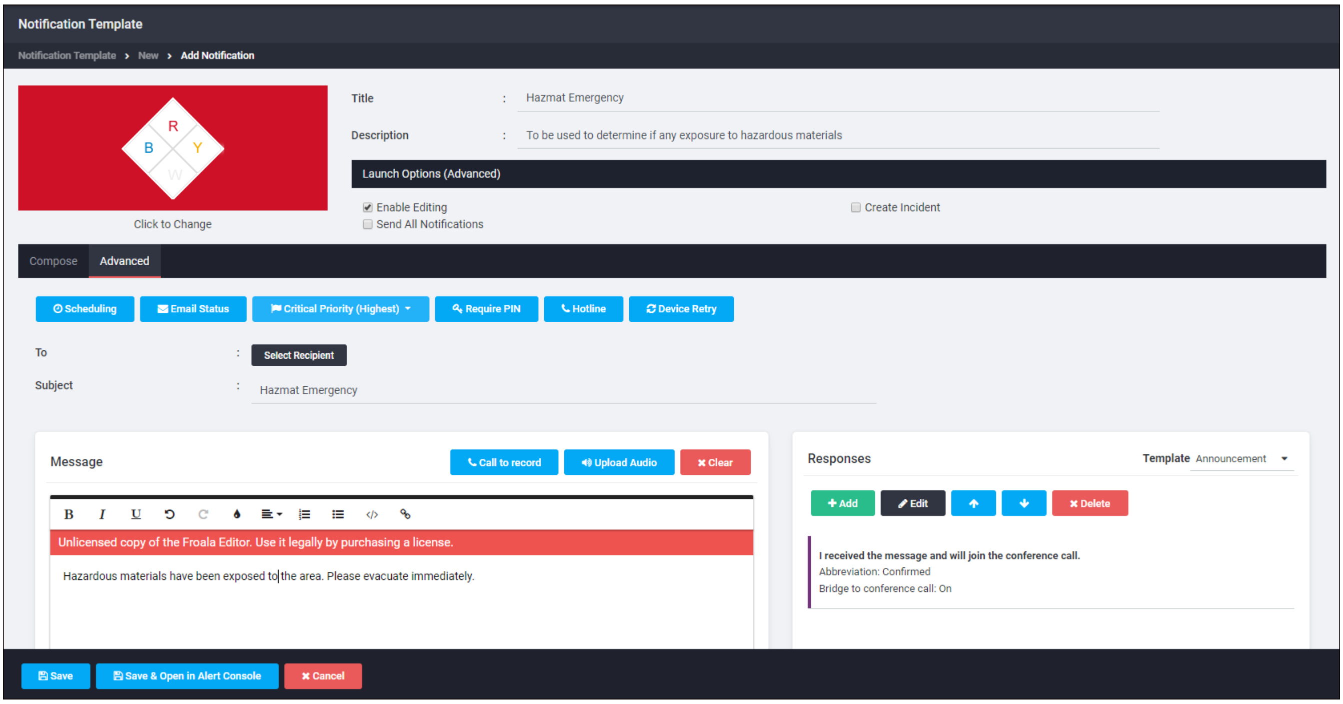
Message

Unlicensed copy of the Froala Editor. Use it legally by purchasing a license.

Our records indicate that you have been gone from the office for the past 3 days, if this is due to an illness, please respond accordingly.

- If a template has more than one notification linked to it, when you open the template, the **Notifications** list box containing the notifications linked to the template is displayed as in the **Inclement Weather** template. See View a Notification Template.
- You can choose to create a template with different notification tasks that can be carried out at the same time. For example, the **Hazmat Emergency**

template is set up to send two completely different notifications at once: one to all employees informing them there is an emergency and they should evacuate the building, and the other to the emergency response team telling them there is an emergency and they need to take care of it. You can hide all but the selected notification by clicking the **Hide Notifications** button, which is singled out in the following example by the red rectangle.



Notification Template

Notification Template > New > Add Notification

Title : Hazmat Emergency

Description : To be used to determine if any exposure to hazardous materials

Launch Options (Advanced)

☑ Enable Editing

□ Send All Notifications

□ Create Incident

To : Select Recipient

Subject : Hazmat Emergency

Message

Unlicensed copy of the Froala Editor. Use it legally by purchasing a license.

Hazardous materials have been exposed to the area. Please evacuate immediately.

Responses

Template Announcement

I received the message and will join the conference call.
Abbreviation: Confirmed
Bridge to conference call: On

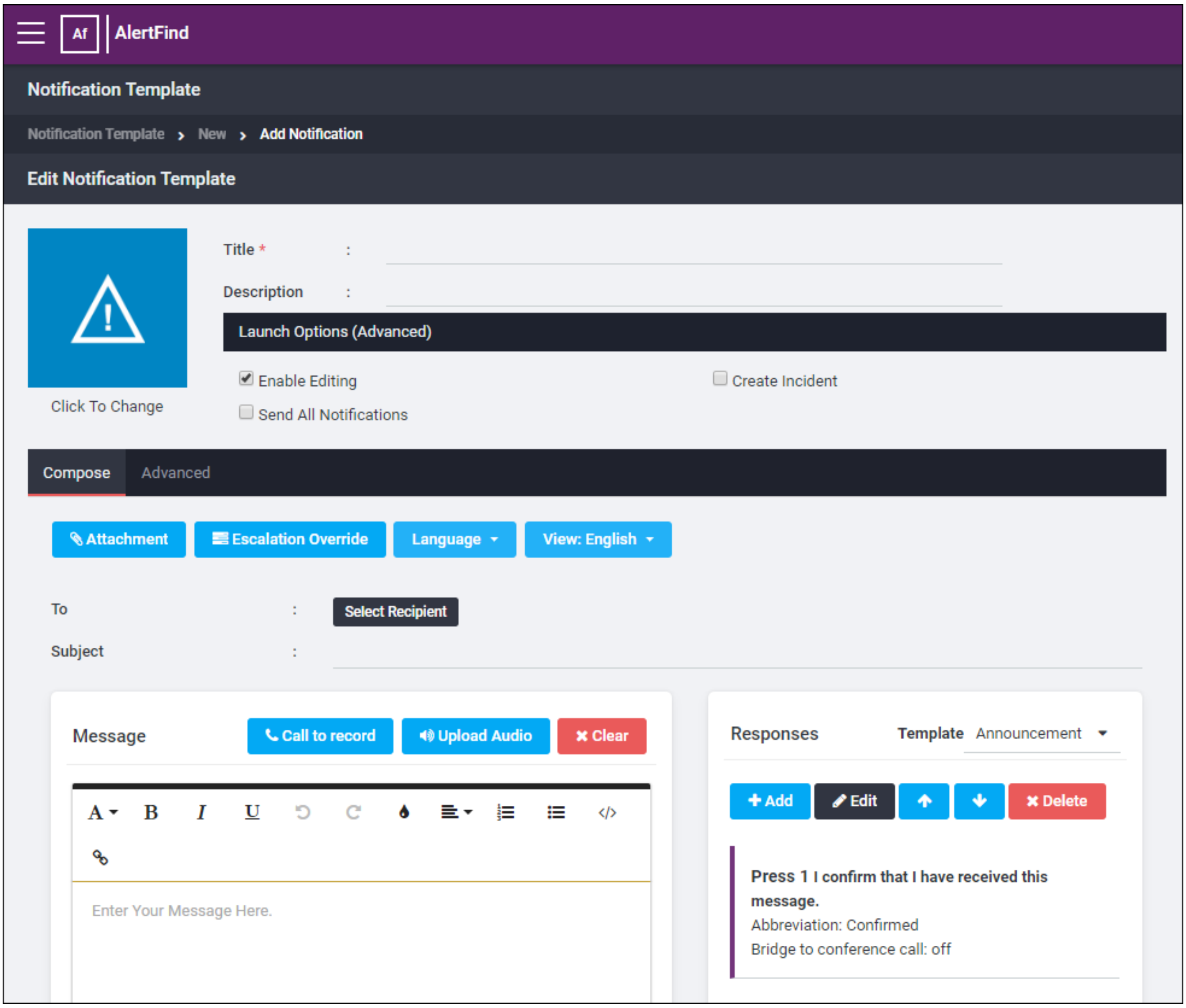
## Create a New Notification Template

### NOTE

None of your edits are saved to the server until you click **Save & Close** or **Save & Open in Alert Console**. Click **Cancel** to close the **Create Notification Template** window without saving the edited template.

To create a new notification template:

1. Go to your team's **Notification Templates** page. See View a List of Notification Templates.
2. On the **Notification Templates** page, click **New**. This displays the **Create Notification Template** window. The template items with a red horizontal line are required edits.



Title * :

Description :

☑ Enable Editing

□ Create Incident

□ Send All Notifications

To :

Subject :

Template Announcement

**Press 1 I confirm that I have received this message.**
Abbreviation: Confirmed
Bridge to conference call: off

3. Enter a title in the **Title** box and an optional description in the **Description** box.

4. Select an icon to associate with the template. See Select a Template Icon.
5. Select the launch options that you want. See Select Template Launch Options.
6. Create your notification(s). See Save Multiple Notifications to a Template.
7. Click **Save & Close**. The new template is saved in your team's **Notification Templates** library page. Alternatively, click **Save & Open in the Alert Console** to save it in the template library and review it in the Alert Console.

## Edit a Notification Template

### NOTE

None of your edits are saved to the server until you click **Save**. Click **Cancel** to close the **Editing Notification Template** window without saving the edited template.

To edit a notification template:

1. Go to your team’s **Notification Templates** page. See View a List of Notification Templates.
2. In the **Notification Templates** library page, select the template to be edited. This displays the **Editing Notification Template** window.

### NOTE

The **Editing Notification Template** window contains the same template features as the **Create Notification Template** window. The only difference is that the notification template being edited already has a title, description, selected launch options, and one or more notifications linked to it.

3. Edit the features as required. See Select a Template Icon, Select Template Launch Options, and Save Multiple Notifications to a Template for explanations of how to edit these items.
4. Click **Save and Close** or **Save and Open in Alert Console**. The edited template is saved in your team's **Notification Templates** library page and closed or opened for review in the Alert Console, depending on your choice of buttons.

## Save an Existing Incident as a Notification Template

Any existing incident can be saved as a notification template. You might want to do this if the incident information could be used for a future event.

To save an existing incident as a template:

1. In the left navigation menu **Administrator** section, click **Teams**.
2. Select a team to make that your active team context.
3. In the left navigation menu **Incidents** section, click **Incidents**. A list of incidents for your current team context appears.
4. Double-click the title of the incident that you want to save as a template. The **Viewing Incident** page appears.
5. Click **Save As notification template** at the top of the page. The **Editing Notification Template** page appears with the following information:
   - **Title**–The title of the incident, which is now the title of the notification template.
   - **Description**–The description of the notification template as typed on the **Incident** page.
6. Edit the Launch Options as desired. See Select Template Launch Options.

Associated notifications appear at the bottom of the page. For instructions on editing them, deleting them, or adding more notifications, see Save Multiple Notifications to a Template.

7. When you have finished any desired edits, click **Save and Close** or **Save and Open in Alert Console**. The edited template is saved in your team's **Notification Templates** library page and closed or opened for review in the Alert Console, depending on your choice of buttons.
8. Click **OK** to close the **Viewing Incident** window.

## Save an Existing Notification as a Notification Template

Any existing notification can be saved as a notification template. You might want to do this if the notification could be used in the future.

To save an existing notification as a notification template:

1. In the left navigation menu **Administrator** section, click **Teams**.
2. Select a team to make that your active team context.
3. In the left navigation menu **Notifications** section, click **Sent Notifications**. The **Sent Notifications** page for your current team context appears.
4. Locate the notification your want to save as a notification template. You can sort the list by type, subject, or sent time. Use the **Next** and **Prev** buttons to navigate through the list of notifications.
5. To search by **Subject**, use the `starts with`, `contains`, and `end with` options and type the subject (or part of the subject) you are searching for. Click **Search**. A list of notifications that meet your search criteria displays. You can also click the down arrow next to **Search** to search by one or more of these fields:
   - Sent by
   - Sent to
   - Type (Announcement, First Responder)
   - Priority (Test, Low, Normal, High)
   - Sent time (Sent After or Sent Before. Click the calendar icon to select a date, then enter a time.)
6. Double-click the name of the notification you want to save as a notification template. The **Viewing Notification** page appears. This page shows responses to the notification as well as basic information about the notification and delivery options for the notification.
7. Click **Save As Notification Template**. The **Editing Notification Template** page displays.
8. Edit any template features that you might want to edit. See Edit a Notification Template.
9. Click **Save and Close** to save the template, **Save and Open in Alert Console** to save it and review it in the Alert Console, or **Cancel** to cancel the operation. If saved, the new template is listed on the Notification Templates page.
10. Click **Close** to close the **Viewing Notification** page.

## Delete a Notification Template

When you delete a notification template, you delete any notifications associated with the template.

To delete a notification template:

1. Go to your team's **Notification Templates** page. See View a List of Notification Templates.
2. Locate the template you want to delete and select it.
3. In the tool bar, click **Delete**. AlertFind asks you to confirm that you want to delete the notification template.
4. Click **OK** to delete the notification template or **Cancel** to cancel the action.

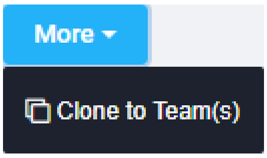
The **Notification Templates** page displays and the notification template is no longer on the list of notification templates.

## Clone Notification Template to Team(s)

Clone one or more Notification Templates to one or more teams.

To clone notification template(s) to team(s):

1. Go to your team's **Notification Templates** page. See View a List of Notification Templates.
2. Select the template(s) to be cloned. Shift-click to select several contiguous templates. Control-click to select individual templates
3. In the tool bar, click the **More...** > **Clone to Team(s)** button. This brings up the **Teams** pane, which displays all the teams you have permission to access.



4. Select the team or teams that the template(s) are to be cloned to. Shift-click to select several contiguous teams. Control-click to select individual teams
5. Click **Clone** to clone the notification template(s).

The **Notification Templates** page displays, with the new template(s), which can be edited as desired.

## Sending a Template Notification From an SMS Device

Using Hotline or Hotline Pro, you can launch an incident with a Quick Launch ID. For detailed information about how to do this, see Using Quick Launch IDs or Using Quick Launch IDs with Hotline Pro.

To send a template notification using a Quick Launch ID:

1. Select the **Quick Launch ID** in the **Launch Options** section of the template.
2. Use the ID you entered or the one you had AlertFind generate for the template.
3. Use a command line with the following parameters:

```
[notify [-u user phone number] [-h] [-p PIN] -ql code [-hv]
```

Where:

- `[-h]` returns instructions on using this command.
- `[-hv]` returns verbose instructions on using this command.
- `[-p] [PIN] PIN`
- `-ql [code]` is the Quick Launch ID code for a notification template.
- `[-u] [phone numbers]` device address, including country code.

For example: `notify -u 15125551234 -p 0000 -ql 1000`

### NOTE

To send a template notification through SMS, you need to send the text to the AlertFind short code (the AlertFind cell phone address– 55626)

## Creating a Complex Notification Template

Consider this more complex example of the use of incidents and notification templates. Assume that during an ice storm, you want the first responders from three key teams to be on a conference call as soon as possible. For this example, we will use escalation groups called disaster recovery (DR), human resources (HR), and information technology (IT). Note that you do not need specific individuals, only the first responder from each escalation group. Because your area is prone to ice storms, you want to save this notification structure for quick and easy execution. To do this, you want to create a notification template:

1. Create your DR, HR, and IT escalation groups.
2. Create a template with a linked notification to contain the conference call information for all three escalation groups.
3. Use the **Clone** feature to create three simultaneous notifications to the three key escalation groups, limiting the response from each escalation group to one person. The steps that follow explain this in greater detail.

**TIP**

The **Clone** feature enables you to create multiple notifications with identical information in the subject line, body text, and conference call information. Each notification has its own escalation list. If you do not use **Clone** and instead create one notification and send it to all three escalation groups, AlertFind only allows the first responder from all of the escalation groups to respond instead of one responder from each escalation group. By using the **Clone** feature to create three notifications, all three escalation groups are notified at the same time and the correct number of respondents is allowed.

4. Save the Notification Template.

The following sample procedure shows you how to create a notification template that bridges first responders from three escalation groups to a conference call. For instructions on creating escalation groups, see Escalation Groups.

To create an example complex notification template:

1. Create a notification template. See Create a New Notification Template.
   1. Select an icon to associate with the template.
   2. Enter the Title and Description.
   3. For the Launch Options, select **Send All Notifications** and **Create Incident**. If you have attachments, add the attachments. See Select Template Launch Options.
2. Create your first notification in the notification section of the template. See Compose Notification.

   1. In the **Compose** tab, select an escalation group for the **To** field. Then enter information in the **Subject** and **Message** fields.
   2. In the Responses section, click **New** and in the Response Editor, set the **Response Limit** to 1, select **Bridge to conference call**, and fill in the required information. Then click **OK**. This ensures that the first person to respond to the call is bridged to the conference call.

3. Using the Clone feature, make two identical copies of the notification. See Save Multiple Notifications to a Template.
4. In the **To** field of the cloned notifications, edit the escalation group so each message has a different group. If necessary edit any other information in the message for the appropriate group.
5. Click **Save & Close** to finish, or if you want to review the template in the Alert Console, click **Save & Open in Alert Console**.

## Downloading Notification Template Reports

You can download a Microsoft Office Excel CSV (Comma Separated Values) report on one template or on all the templates in your team's **Notification Templates** library.

To download a Notification Template Report:

1. In the left menu bar Administration section, select **Teams** to display the **Team** page.
2. On the **Team** page, select the team.
3. In the left menu bar Notifications section, select **Manage Library**. This displays the **Notifications Templates** page for your team.
4. Decide the type of report you want: a **Detailed Report** for one template or a **List Summary Report** for all the templates:
   - For a detailed report, select **Report** button > **Detailed Report**.
   - For a summary list report, select **Report** button > **List Summary Report**.

The report is automatically saved to your **Download** directory and, if you have Microsoft Excel, it opens in a window as an Excel file. You can either save the file or close it without saving the file.

A Detailed Report contains the template title, description, linked notification(s), and date. A List Summary Report lists all the templates in the library.

# Incidents

In AlertFind, you can create an incident and link one or more notifications and attachments to that incident.

Incidents can be saved as *notification templates* so that they can be easily reused. Best practices for incident or crisis communications recommends the creation of pre-scripted message templates to defined groups of people. For example, you might set up a notification template to send a pre-defined notification to alert your IT team when a server is down.

Notification Templates are saved to the *Notification Template library*. This library comes with a default set of templates that you can use and edit. See Notification Templates for how to use this library.

NOTE

When you use a Notification Template, AlertFind can automatically create an incident for you and automatically link your notification(s) to the incident.

*Incident Templates* that you created prior to AlertFind 5.0 are stored in the Notification Templates library and become Notification Templates. You can use them in the same way you previously used them. However, they also inherit the additional features of the **Notification Template** library.

## Working with Incidents

You can do the following with incidents:

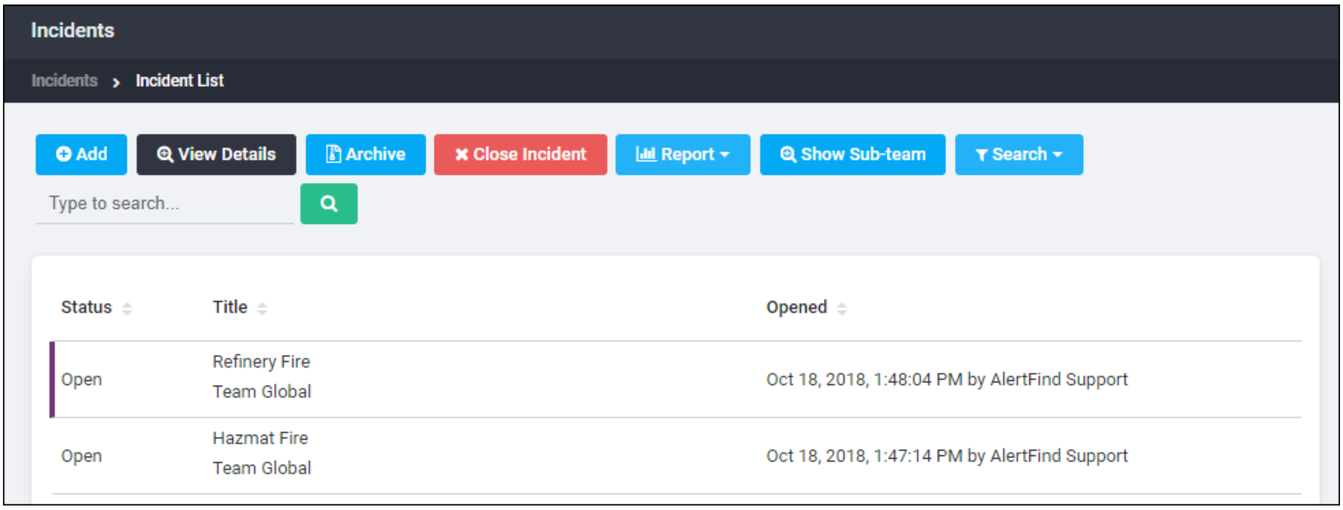
- View a list of existing incidents or an individual incident. See Viewing a List of Incidents and Viewing an individual incident.
- Search for an incident. See Searching for an Incident.
- Create a new incident. See Creating a New Incident.
- Compose, edit, or remove one or more notifications automatically linked to an incident. See Working with Incident Notifications.
- Edit an existing incident and its notifications. See Editing an Existing Incident.
- Save an incident with its linked notifications as a notification template. Save an Existing Incident as a Notification Template.
- Archive an incident or unarchive it. See Archiving Incidents and Un-archiving Incidents
- Download a CSV report on one or all your incidents. See Reporting on Incidents.

## Viewing a List of Incidents

You can view a list of incidents by team or, if in the Global Team context, you can view a list of all incidents.

To view a list of incidents:

1. In the left menu bar in the Administration section, click **Teams**.
2. On the **My Teams** page, select a team to make that your active team context.
3. In the left menu bar in the **Incidents** section, click **Incidents**. The **Incidents** page for the selected team appears. The following is an example Incidents page.



| Status | Title | Opened |
|---|---|---|
| Open | Refinery Fire<br>Team Global | Oct 18, 2018, 1:48:04 PM by AlertFind Support |
| Open | Hazmat Fire<br>Team Global | Oct 18, 2018, 1:47:14 PM by AlertFind Support |

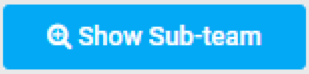
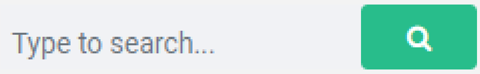
The following table describes the page columns.

| Column | Description |
|---|---|
| **Status** | Open or closed. |
| **Title** | The name of the incident and its team. This name also appears in the Incident Collaboration Center. |
| **Opened** | The day, date, and time the incident was opened, as well as the person who opened the incident. |

You can sort a list of viewed incidents by Status, Title, or Date.

## Tool Bar Options for the Incidents Page

The following table lists and describes the **Incidents** page tool bar options. These are the things you can do with incidents when viewing the **Incidents** page.

| Option/Button | Function |
|---|---|
| | Click **Add** to create a new incident. See Creating a New Incident. |
| | Double-click an incident or select it and click **View Details** to see the incident details. See Viewing an Individual Incident. |
| | Select an incident and click **Archive** to archive the incident. It is placed on your team's **Archive Incidents** page. See Archiving Incidents |
| | Select an open incident and click **Close Incident** to close the incident. |
| | Using the **Report** option, you can create two different CSV reports: A Detailed Report or a List Summary Report. See Reporting on Incidents. |
|  | To display a list of your sub-team's incidents, click **Show Sub-team**. |
|  | Using the **Search** option, you can search for an incident by title or description, or on whether it is open or closed. See Searching for an Incident. |

## Searching for an Incident

To search for an incident

1. Go to the Incidents page. See Viewing a List of Incidents.
2. Perform one of the following:

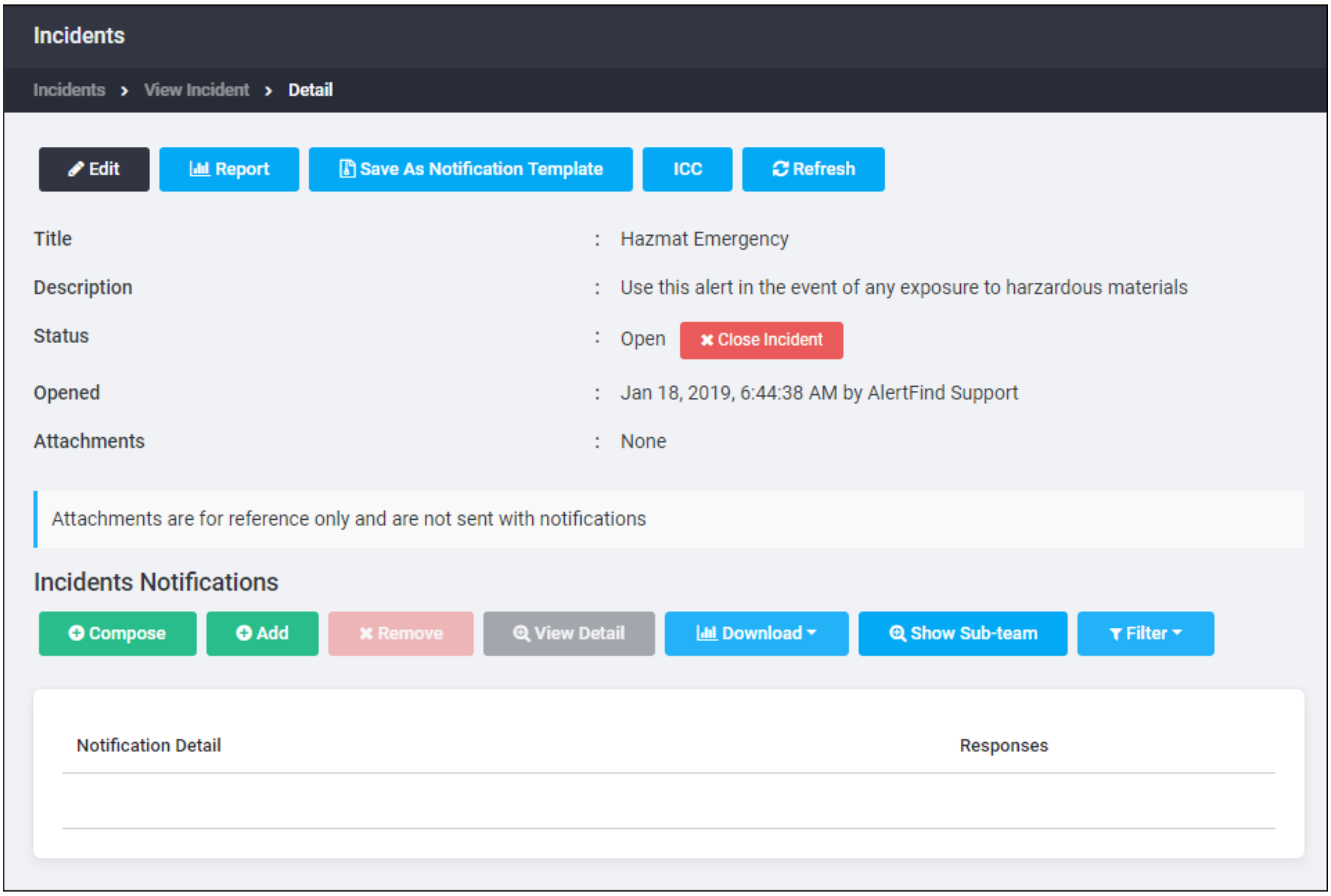
    - Enter a title or part of a title in the **Search** text box and click 🔍.
    - Click the down arrow next to the **Search** button and select one of the following additional options for creating a custom search:
        - **Opened** (the date the incident was opened)
        - **Closed** (the date the incident was closed)
        - **Description**
        - **Title**

To clear your custom search setting, click the **Search** down arrow and then select **Clear Search**.

## Viewing an Individual Incident

To view an incident:

1. Go to your team's **Incidents** page. See Viewing a List of Incidents.
2. Double-click the desired incident or select it and click **View Details**. The following is an example incident.



Incidents
Incidents > View Incident > Detail
Edit
Report
Save As Notification Template
ICC
Refresh

| | | |
|---|---|---|
| Title | : | Hazmat Emergency |
| Description | : | Use this alert in the event of any exposure to harzardous materials |
| Status | : | Open ✖ Close Incident |
| Opened | : | Jan 18, 2019, 6:44:38 AM by AlertFind Support |
| Attachments | : | None |

Attachments are for reference only and are not sent with notifications

Incidents Notifications

| Notification Detail | Responses |
|---|---|

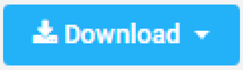
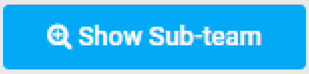
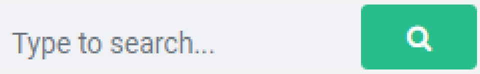
## Tool Bar Options for the Viewing Incident Page

In the **Viewing Incident** page, in addition to adding, removing, or editing notifications linked to the incident, you can also do the following tasks listed in the page tool bar.

| Option/Button | Function |
|---|---|
| Edit | Click **Edit** to edit the incident title, description, and attachments. |
| Report | Click **Report** to create a **CSV** Incident Report of the opened incident. If you have Microsoft Excel installed, the report automatically opens in Excel in a new window.<br>The report lists the incident features such as title, description, open time, and closed time. It also lists any notification linked to the incident along with the notification details for each notification. |
| Archive | Click **Archive** to remove this incident from your team's **Incidents** page and place it on your team's **Archived Incidents** page. See Archiving Incidents. |
| Save As Notification Template | Click **Save As Notification Template** to save the viewed incident as such. See Save an Existing Incident as a Notification Template. |
| Refresh | Click **Refresh** to refresh the Web page. |

## Working with Incident Notifications

The following table lists and describes the **Incident Notifications** tool bar options.

| Option/Button | Function |
|---|---|
| | Click **Compose** to compose a new notification automatically linked to the incident. See Compose Notification. |
| | Click **Add** to add an existing notification to the incident. See Adding Notifications to an Incident. |
| | Select one or more notifications and click **Remove** to remove the notification(s) from the Incident. See Removing Notifications from an Incident. |
| | Double-click a notification in the **Incident Notifications** list or select it and click **View Details** to see or edit the notification details. |
|  | The **Download** option enables you to download a **CSV** report on an individual notification linked to the incident or a CSV report on all the notifications linked to the incident. See Downloading Incident Notification Reports. |
|  | Click **Show Sub-team** to view the list of your sub-team’s notifications. |
|  | Use the **Search** option to search for a specific notification linked to the incident being viewed. See Searching for an Incident Notification. |

### Adding Notifications to an Incident

You can create a new notification to link to an incident or add one or more existing notifications to link to an incident. See Add a new notification to an incident and Add an existing notification to an incident.

**Add a new notification to an incident:**

1. View the incident. See Viewing an Individual Incident.
2. In the Incident Notifications section, click **Compose**. See Use the Compose To Feature if you have any questions.
    1. Click **Template**, and select the template type for the notification.
    2. Click **Attachment** to add an attachment.
    3. Click **Escalation Override** to override escalation rules for this notification.
    4. Click **To** to enter the recipients.
    5. Enter the subject in the **Subject** text box.
    6. Enter the message in the **Message** text box.
    7. In the **Responses** section, leave the template response as is or edit it and/or enter a new response.
3. Click **Advanced Options** to enter any of the advanced options features (For more information refer to Add advanced options to a Notification):
    - **Scheduling**: to set up notification scheduling and any recurrence.
    - **Email Status**: to send email results of this notification.
    - **Normal**: to select a priority value for this notification.
    - **Require PIN**: to require notification recipients to enter a PIN to hear or read the message.
    - **Hotline**: to allow recipients to respond to this notification by calling Hotline.
    - **Device Retry**: to set the maximum number of times a phone call will be retried for this notification.
4. When you have completed drafting the notification, click **Save as draft**. The **Viewing Notification** window is displayed with an overview of the notification.
5. Click **Edit** to edit anything. When done, again click **Save as draft**.
6. Click **Close** to close the **Viewing Notification** window.
7. Click **OK** to close the **Viewing Incident** window.

**Add an existing notification to an incident:**

1. View the incident. See Viewing an Individual Incident.
2. In the **Incident Notifications** section, click **Add** to add an existing notification to the incident.

3. On the left side of the **Manage Incident Notifications** window, select a notification to be added and click **Add Selected**. The selected notification is displayed in the **Incident Notifications** list box on the right side of the window.
4. Click **Close** to close the **Manage Incident Notifications** window.
5. Click **OK** to close the **Viewing Incident** window.

### Removing Notifications from an Incident

To remove one or more notifications from an incident:

1. View the incident. See Viewing an Individual Incident.
2. In the **Incident Notification** section, select the notification or notifications and click **Remove**.
3. At the confirmation prompt, click **OK** to continue with the operation or **Cancel** to cancel it.

The notification(s) link to the incident is removed, but the notification(s) itself remains listed on the **Scheduled Notifications** page.

### Downloading Incident Notification Reports

You can download a detailed **CSV** report of an individual notification linked to the incident or a summary list **CSV** report of all the notifications linked to the incident.

To download incident notification reports:

1. View the incident. See Viewing an Individual Incident.
2. In the Incident Notifications list, select the notification for which you want a report.
3. Click the down arrow next to the **Report** button, and select either **Notification List Detailed Report** or **Notification List Summary Report**.

If you have installed Microsoft Excel on your system, the report will be automatically opened in a separate window in Excel. It will also be automatically saved to your **Download** directory. The report contains the incident title, subject, date, and all the notification details.

### Searching for an Incident Notification

To search for a specific notification linked to an incident:

1. View the incident. See Viewing an Individual Incident.
2. Perform one of the following:
    - In the Incident Notifications section, enter a notification subject or part of a subject in the **Search** text box and click 🔍.
    - In the Incident Notifications section, click the **Search** down arrow, and select one of the following additional options for creating a custom search:
        - Priority
        - Received by
        - Response abbreviation
        - Sent by
        - Sent Time
        - Subject

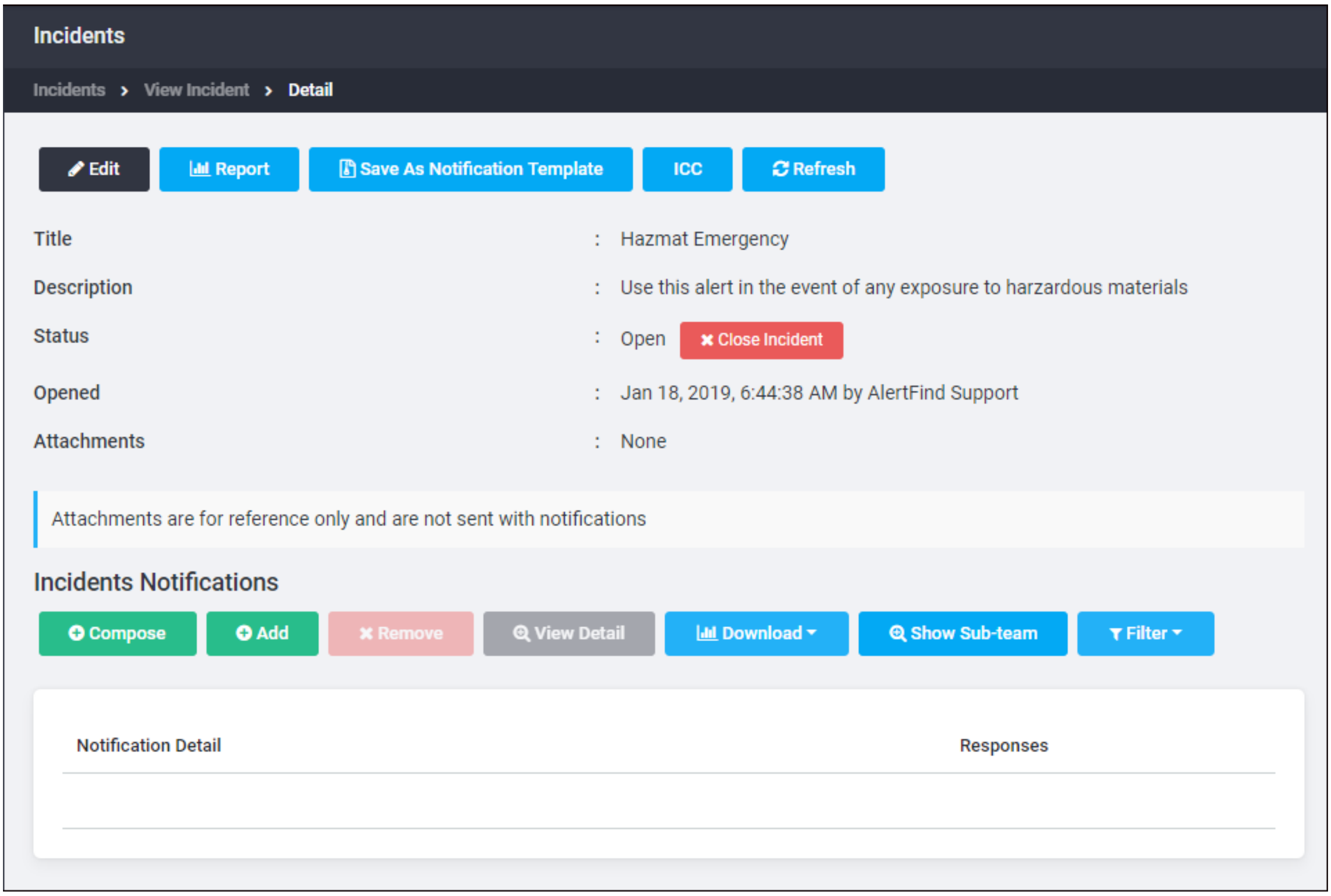
To clear your custom search setting or the text in the search box, click **Clear Search**.

## Creating a New Incident

Administrators can create incidents for any team. Team leaders can create incidents for their teams if they have been granted that permission (**Manage Templates**).

To create a new incident:

1. Go to your team's **Incidents** page. See Viewing a List of Incidents.
2. On the Incidents page for the selected team, click **Add**. The **Create Incident** window displays.
3. In the Create Incident window, type a title for the incident. This is a required field.
4. Type a description of the incident. This is an optional field.
5. Click **Attachments** if you want to add attachments to this incident. You can add up to 5 attachments of a total size of not more than 50 MB. If you choose to add an attachment, a new window appears so that you can navigate to the location of the attachment. Note that attachments are for reference only and are not sent with notifications.
6. Click **Save**. The **Viewing Incident** page is displayed. This page allows you to create one or more notifications and automatically link them to the incident. The following is of an example incident with two notifications already linked to it.


Incidents
Incidents > View Incident > Detail
Edit
Report
Save As Notification Template
ICC
Refresh

Title : Hazmat Emergency

Description : Use this alert in the event of any exposure to harzardous materials

Status : Open

Opened : Jan 18, 2019, 6:44:38 AM by AlertFind Support

Attachments : None

Attachments are for reference only and are not sent with notifications

Incidents Notifications

| Notification Detail | Responses |
|---|---|

7. In the Incident Notifications section, click **Compose** to create a notification automatically linked to the incident. See Compose Notification for instructions on how to compose notifications. You can compose as many notifications as you may need to link to the notification. You can also click **Add** to link a previously created notification to the incident. This displays the **Manage incident notifications** window. In that window, select the notification you want to add and click **Add Selected**. When you have finished adding notifications, click **Close**.
8. When you have finished creating your incident, click **Close**. The new incident is listed on you team's **Incidents** page.

## Editing an Existing Incident

To edit an existing incident:

1. View the **Incidents** page for your team. See View an incident.
2. Locate the incident you want to edit. You can sort by any column by clicking on the column heading.
3. Select the incident and click **View Details**. The **Viewing Incident** page appears.
4. To edit the title or description of the incident, or to add an attachment, click **Edit**.
5. To save the information about this incident in a CSV file, click **Report**.
6. To add notifications to the incident, click **Add** in the **Incident Notifications** section.
7. To remove a notification, select it and click **Remove** in the **Incident Notifications** section.
8. To archive the incident and remove it from the incident list, click **Archive**.
9. To save this incident as a template, click **Save as Notification Template**. The **Editing Notification Template** page displays. For instructions on editing a notification template, see Edit a notification template.
10. Click **Save** when you have finished your edits.
11. In the **Viewing Incident** page, click **OK** when you are finished your edits.

## Reporting on Incidents

To create a CSV incident report:

1. Go to the Incidents page. See Viewing a List of Incidents.
2. Click the **Report** down arrow and select either **Incident List Summary Report** or **Incident Detailed Report**.

The report is listed on the bottom left of the page and automatically saved to your **Download** directory. If you have Microsoft Excel installed on your system, the report is opened in Excel.

## Archiving Incidents

When an incident has been archived, it is closed and cannot be reopened. It can be unarchived. Archiving an incident cancels any notifications associated with the incident.

To archive an incident:

1. View your teams **Incidents**. See Viewing a List of Incidents.
2. Locate the incident and double-click it to select it. (You can sort by any column on the page by clicking the name of the column.)
3. Click **Archive** > **OK** to archive and close the incident, or **Cancel** to cancel the action.
4. View the archived incidents by selecting **Archived Incidents** in the left-hand menu.

## Unarchiving Incidents

When an incident is unarchived, it is no longer displayed on the list of archived incidents.

To unarchive an incident:

1. View your team’s archived incidents. See View archived Incidents.
2. Locate and select the incident you want to unarchive. You can sort by any column on the page by clicking the name of the column. You can also search for a specific incident:
   - By scrolling through the list of incident titles and using the **Next** and **Prev** buttons.
   - By entering a title in the search text box and clicking 🔍 or by clicking down arrow next to the **Search** button and creating a custom search. You can search by Title, Description, Open Time (before and after), and **Close Time** (before and after). Click the calendar icon to select a date.

### NOTE

When you click a date on the calendar, the time is automatically entered as 12:00 AM. Manually type the correct time for your search after selecting the date.

### TIP

When searching by description, you can modify your search by changing the operator in the description **Edit Criteria** dialog box to be one of the following: **starts with**, **contains**, **ends with**, or **equals**. Then type part of the description in the search text box.

3. Click **Un-archive**. A confirmation prompt asks if you are sure you want to un-archive the incident. Click **OK** to continue with the operation or **Cancel** to cancel the operation. If you click **OK**, the incident is unarchived and moved to the **Incidents** page as a closed incident.

# Chapter 4: Hotline and Hotline Pro

Hotline and Hotline Pro provide one or more central phone numbers that users can call for information. For example, a number can be provided for employees to call on bad weather days to determine when or if they should come into the office. To implement this, administrators and team leaders can send notifications and launch notification templates using both Hotline and Hotline Pro.

Every organization that uses AlertFind has access to the basic Hotline. The **basic Hotline** is a phone number that a user can call to hear an announcement or to check his or her inbox. Administrators and team leaders with appropriate permissions can send notifications or launch notification templates from the voice interface. The features and uses of the basic hotline are covered under Basic Hotline.

Organizations that need extended hotline functions can upgrade to **Hotline Pro**. In addition to the basis Hotline functions, Hotline Pro allows you to customize the voice interface in multiple languages, post announcements, gather information from polls, and gather information from advanced reporting features. All of the features and uses of Hotline Pro are covered under Hotline Pro.

## Basic Hotline

The basic Hotline is a phone number that users can call to hear an announcement or to check their inboxes. Administrators and team leaders with appropriate permissions can send notifications or launch notification templates from the voice interface.

The Hotline for new customers contains three elements:

- Welcome message
- Notification inbox
- Compose Notification

You must contact Support to obtain a Hotline phone number.

Basic Hotline functions:

### Basic Hotline Features

When you first call the Hotline number, you hear the welcome greeting. Users hear this greeting and can, after entering a valid PIN, access their notification inbox. Only administrators, and team leaders with appropriate permissions, can compose notifications.

The Notification Inbox and Compose Notification option make up the Hotline **Main Menu**.

NOTE

Hotline supports up to 20 levels in the tree, and up to 99 options and sub-options.

## Responding to Notifications Through the Hotline

To listen to their messages, callers must identify and authenticate themselves.

The Hotline voice prompts informs the caller everything they need to know to respond to a Hotline Notification. If they respond to the notification from an email address, the email message contains instructions. For more information about responding to notifications, see Use the Notification Editor.

## Composing a Notification Using Hotline

To compose a notification using the Hotline, call the Hotline and select **Compose Notification** from the main menu. Listen to the voice prompts to select one of the following starting points for your notification:

- Enter a Quick Launch ID
- Open an incident from a notification template
- Select a broadcast group
- Select an escalation group

A Quick Launch ID is a number assigned to a notification template, broadcast group, or escalation group. To use a Quick Launch ID, use the keypad of your phone to enter the number.

NOTE

All Quick Launch IDs must be unique. In other words, you cannot have a notification template Quick Launch ID that is the same as a broadcast group or escalation group Quick Launch ID.

To send a notification using the Hotline:

1. Select **Compose Notification** from the **Main Menu**.
2. Select one of the four methods described above to send the notification.
3. If you enter a Quick Launch ID for a notification template, AlertFind reads the name of the notification template you have selected and offers you three choices:
    1. Press 1 to open an incident from this notification template and send all notification tasks not set for manual execution. If you select this option, the incident is immediately opened and sent to all recipients.
    2. Press 3 to review notification tasks

TIP

It is possible to open an incident from a template that has no notification tasks. To avoid this, review notification tasks before initiating the incident.

   3. Press 9 to select a different notification template
   4. Press 0 to return to the Main Menu

4. If you choose to open an incident from a notification template, AlertFind reads your available notification templates to you. It then offers you the same three choices you are offered if you select a Quick Launch ID.
5. If you choose to use a broadcast or escalation group, AlertFind reads the list of groups to you.
   1. If you select a group that is on multiple teams, AlertFind requests you to select the appropriate team.
   2. AlertFind then requests you to record your message.

## Using Quick Launch IDs

If your AlertFind instance has notification templates, broadcast groups, or escalation groups with Quick Launch IDs, you can launch a notification using the Hotline or Hotline Pro voice interface.

**NOTE**

All Quick Launch IDs must be unique. In other words, you cannot have a notification template Quick Launch ID that is the same as a broadcast group or escalation group Quick Launch ID.

### Launch a notification with a broadcast group or escalation group Quick Launch ID

1. Call the Hotline or Hotline Pro phone number. If you are using Hotline Pro, the Hotline must have a **Compose Notification** option.
2. Follow the voice prompts to select **Compose Notification.**
3. Identify yourself and enter your PIN.
4. Press 1 to enter a Quick Launch ID.
5. Use the keypad of your phone to type the Quick Launch ID. AlertFind reads the name associated with the Quick Launch ID.
6. (Optional) If this Quick Launch ID is associated with multiple teams, you are requested to select the appropriate team.
7. Press 1 to compose a notification for this group.
8. Record your message.
9. Follow the voice prompts to accept or rerecord the message. AlertFind requests you to wait while it processes your request.
10. Select from one of the four options:

   1. Press 1 to send the notification.
   2. Press 2 to set the priority of the notification.
   3. Press 3 to define when or if notification results should be mailed to you.
   4. Press 4 to turn on authentication for this notification. This requires callers to authenticate themselves before hearing the notification.

AlertFind informs you that the notification has been initiated.

11. You can now review notification status by logging in to the AlertFind web interface and clicking **Sent Notifications**.

**Launch a notification using a notification template Quick Launch ID**

1. Call the Hotline or Hotline Pro number. The Hotline must have a **Compose Notification** option.
2. Follow the voice prompts to select **Compose Notification**.
3. Identify yourself and enter your PIN.
4. Press 1 to enter a Quick Launch ID.
5. Use the keypad of your phone to type the Quick Launch ID. You will hear a message as “You are about to open an incident from the notification template [template name] with description [description].” and AlertFind offers four options:
   1. Press 1 to open an incident with this notification template and send all notification tasks that are not set for manual execution.
   2. Press 3 to review the notification tasks for this notification template. If you select this option, AlertFind reads the notification tasks to you. It also offers you the ability to review the recipient list and reads the priority of the notification to you.

   **NOTE**

   It is possible to send a notification template with no associated tasks. To ensure you do not accidentally do this, press 3 to review notification tasks before sending the notification template.

   3. Press 9 to select a different notification template.
   4. Press 0 to return to the Main Menu.

7. Review notification status by logging in to the AlertFind web interface and clicking **Sent Notifications**.

# Hotline Pro

Hotline Pro enables you to have one or more customizable voice user interfaces, accessible from one or more phone numbers. Callers to Hotline Pro can hear announcements, respond to polls, and check their voice mail inbox. Administrators and team leaders can use the customization features of the web interface to compose polls and customize options available on a Hotline, and use the voice interface to compose notifications and to launch incidents from notification templates.

The Hotline Pro web interface enables you to interact with Hotlines to fine-tune them to your specific needs.

Hotline Pro provides ability to perform the following tasks:

- Create Hotline Polls
- Create and customize multiple Hotlines
- Create custom Hotline menus for your organization
- Design team-specific Hotlines (with different Hotline numbers for each team)
- Activate and deactivate Hotlines and Hotline options as necessary
- Transfer callers to multiple conference call phone numbers
- Transfer callers to a different Hotline phone number
- Capture caller-entered response information and information on nodes callers access during calls
- Request identification by phone number, user name, or other identification information. Other identification can include an employee ID number, other company identifier, or an identifier from a third-party system. To use other identification, this option must be enabled on the **Company Settings** page.
- Request authentication with a PIN number

**NOTE**

- Hotline Pro supports up to 20 levels in a tree, and up to 99 options and sub-options.
- To add Hotline Pro, contact Support.

Hotline Pro topics in this chapter:

---

## Multiple Language Support

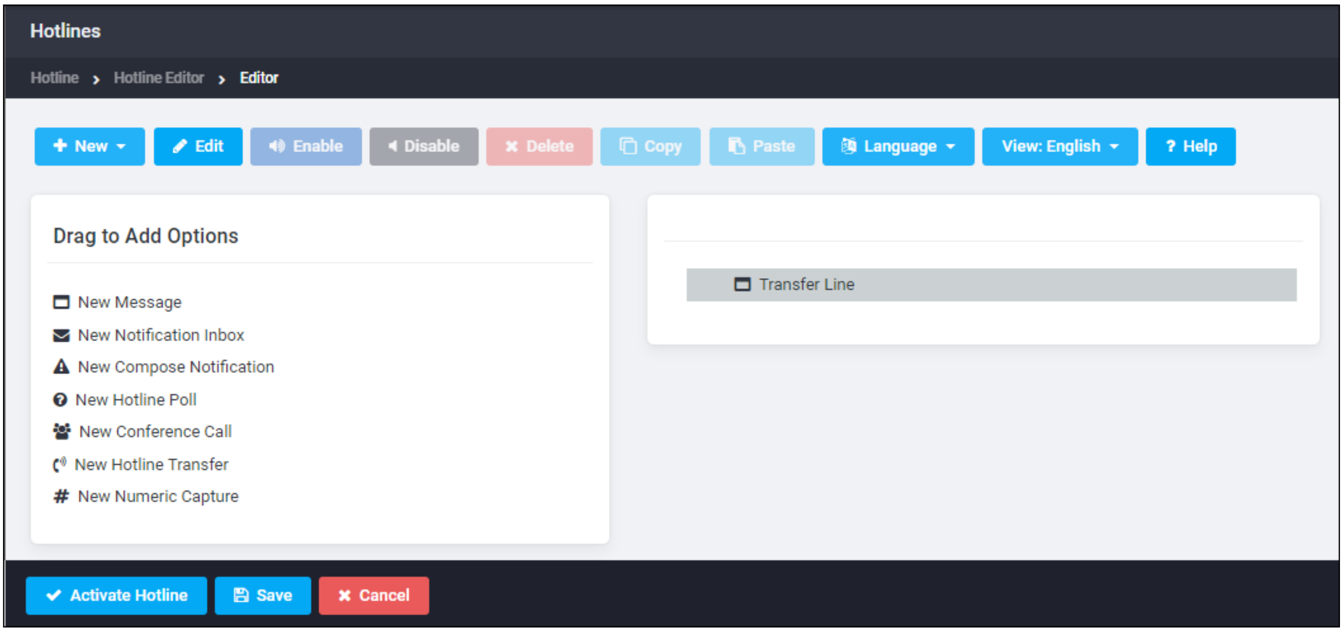
If your company purchased language packs and multiple languages are enabled, you can create Hotlines in multiple languages. One use of this might be to create a Hotline with your poll in multiple languages (create the message and responses in the desired language), and then create one master notification that enables callers to press a key to transfer to a Hotline in their preferred language.

If your company purchased additional language packs, and if these languages have been enabled, you can create Hotlines in multiple languages. Contact your AlertFind Administrator to learn more about additional languages.

Languages are attached to Hotline phone numbers. You might have one phone number for users who speak English, a second phone number for users who speak French, and a third phone number for users who speak Spanish. All users who call the same number hear the same voice and language.

## Creating a Hotline

With Hotline Pro, you can log into AlertFind and use the Hotline Editor to build a robust hotline that includes a variety of node types, including:



- **New Message**: Create a new message that callers hear when they call the Hotline Pro phone number. Use this for company announcements such as “We are closed today because of inclement weather.” This option does not, by default, require the users to identify or authenticate themselves. Anyone who calls in hears this message unless you specifically set up security for this message. For more information about security, see Security.
- **New Notification Inbox**: Create a voice mail inbox for new and historical notifications for callers to listen to them. Messages are stored in the inbox for thirty days by default.
- **New Compose Notification**: Enable administrators and team leaders with appropriate permissions to create new notifications by calling into the Hotline.
- **New Hotline Poll**: Create a new Hotline Poll to gather votes from authenticated users. You can create a poll that gathers numeric information from callers to the Hotline, or alphanumeric information from users responding by email. See "Creating a Hotline Pro Poll Node" for more details.
- **New Conference Call**: Present callers with multiple conference call numbers. For example, you could have one conference call for the IT response team, one for the disaster recovery team, and one for the management team.

- **New Hotline Transfer**:Transfer callers to a different Hotline. For example, in the event of a flu pandemic, you might want to set up one Hotline for well callers, and another number for sick callers. Using the New Transfer Call option, callers are greeted and then offered two (or more) options that transfer them to the appropriate Hotline.
- **New Numeric Capture**: Gather a variety of numeric responses from callers. Unlike a poll node that presents few options from which callers can choose, a numeric capture node allows callers to enter numbers appropriate for their situation. You might use a numeric capture node during a flu pandemic to gather information on the body temperatures of callers who are ill. A numeric capture node will allow callers to enter their exact temperatures in multiple digits, such as `99.7` or `102.3`.

**TIP**

To set up per-team Hotlines, first access the team for which you want to create the Hotline, then create the Hotline. Repeat this for every team for which you want to create a Hotline.

**TIP**

If you are creating Hotlines for multiple languages, enable all languages you want to use before you add any options to the Hotlines. Doing this allows AlertFind to display default template responses in the desired language.

To enable multiple languages,

1. click **Language** in the menu bar.
2. Select **Language Settings**.
3. Select languages you want to use.
4. If you create a multilingual Hotline, you must complete all required fields for all languages.

To create a new, customizable Hotline:

1. Click **Hotlines** in the navigation bar.
2. Click **New,** enter a name for the Hotline and click **OK**. The **Hotline Editor** appears.
3. Build the Hotline using any of the available node types. You can add a node using one of the following methods:
   - Dragging and dropping nodes from the left column into the right column. For the first option you add to the Hotline, a green plus sign indicates when you can drop the new option into the Hotline. For subsequent options, blue dotted lines appear to help you place the option exactly where you want it in the Hotline.
   - Clicking **New** from the **Hotline Editor** menu and then, selecting the node to be added from the drop-down list.

- Right-clicking the Hotline name to display the drop-down list of nodes. Select the node to be added from the drop-down list.

4. Add nodes. Refer to the following sections for more information on each type of node you can add:

   - Add a **New Message** node to add typical Hotline navigation tree options, such as “Press 1 to report an absence.” See Creating a Hotline Message Node.
   - Add a **New Notification Inbox** node to create a voice mail inbox for callers to hear new and historical notifications. See Creating a Notification Inbox Node.
   - Add a **New Compose Notification** node to enable administrators and team leaders with appropriate permissions to create new notifications by calling into the Hotline. See Creating a Compose Notification Node.
   - Add a **New Hotline Poll** node to Create a new Hotline Poll to gather votes from authenticated users. See Creating a Hotline Pro Poll Node.
   - Add a **New Conference Call** node to present callers with multiple conference call numbers to which they can connect. See Creating a Conference Call Node.
   - Add a **New Hotline Transfer** node to transfer callers to a different Hotline. See Creating a Hotline Transfer Node.
   - Add a **New Numeric Capture** node to gather numeric input from callers. See Creating a Numeric Capture Node.

5. When you are done adding and configuring each node of the Hotline, return to the **Hotline Editor** and click **Activate Hotline**.

## Creating a Hotline Message Node

Message nodes can contain text or audio announcements and other sub-options. Message nodes form the basic navigation structure for most Hotlines.

To create a Hotline message node:

1. Access the Hotline you want to add the message node to by clicking **Hotlines** in the left menu bar, then selecting the appropriate Hotline. The **Hotline Editor** appears.
2. Add a **New Message** node to Hotline by dragging **New Message** from the left column into the Hotline tree in the right column. The **Hotline Option Editor** appears. Use this editor to set the options for this node.
3. In the **Message Name** field, type the text you want the TTS engine to read when a caller accesses this node of the Hotline. Type the words that you want callers to hear immediately after the option number. For example, to build a message node that says, “Press 1 to hear weather updates for your location,” type `to hear weather updates for your location` into the **Message Name** field.

4. You can click the **Actions** field name to bring up the **Action Editor**. Set up action logging to capture information about callers accessing this node. See Capturing Node Actions for more information on gathering information on node actions.
5. By default, message nodes have no security restrictions. You can increase this to **User Identification Required** or **User Identification and PIN Authentication Required**. When you increase security for a node, a lock icon appears on the node in the Hotline Pro tree. For more information about security, see Security.

NOTE

When callers call in to Hotline Pro from a phone in their AlertFind personal escalation list, AlertFind recognizes them but still asks them to identify themselves by asking, “If you are Sam, press 1. If you are not Sam, press 2.”

TIP

You can control access to sub-options by setting security at the main message level. Sub-options (children) inherit the security of the main message (the parent). This can be used to simplify security management.

6. In the **Message** section, you can:
   - Type a message for the AlertFind TTS engine to read.
   - Click **Call to Record** and type the phone number AlertFind should call to obtain the message. Click **Call Now** to initiate the call process. The status of the call appears in the window so that you can track the progress of recording. When the message has been recorded, the WAV appears on the **Hotline Option Editor** page.
   - Click **Upload Audio** to upload an audio file. The file you upload must be a WAV file in a supported format. See Supported Audio Files.
7. Click **Save** to save this node. Continue adding other nodes or options to the hotline until it is complete. To activate your Hotline, see Activating Your Hotline.

## Creating a Notification Inbox Node

New notifications and confirmed notifications are stored in the notification inbox. A notification inbox node requires that callers identify and authenticate themselves before they can listen to messages. Messages are stored in the inbox for thirty days (to change this length of time, contact your AlertFind administrator).

To create a notification inbox node:

1. Access the Hotline you want to add the notification inbox node to by clicking **Hotlines** in the left menu bar, selecting the appropriate Hotline, and clicking **Edit**. The **Hotline Editor** appears.

2. Add a **Notification Inbox** node to Hotline by dragging **New Notification Inbox** from the left column into the Hotline tree in the right column. The **Hotline Option Editor** appears. Use this editor to set the options for this node.
3. In the **Inbox Name** field, type the text you want the TTS engine to read when a caller accesses this node of the Hotline. Type the words that you want callers to hear immediately after the option number. For example, to build a node that says, "Press 1 to access your personal inbox," type `to access your personal inbox` into the **Inbox Name** field.
4. Click the **Actions** field name to bring up the **Action Editor**.
5. Set up action logging to capture information about callers accessing this node. See Capturing Node Actions for more information on gathering information on node actions.

NOTE

Notification inbox nodes always require identification and authentication. This security setting cannot be changed.

6. Click **Save** to save this node.
7. Continue adding other nodes or options to the hotline until it is complete.

To activate your Hotline, see Activating Your Hotline.

## Creating a Compose Notification Node

Compose Notification nodes allow administrators and team leaders with appropriate permissions to create new notifications by calling into the Hotline and following the instructions under Composing a Notification Using Hotline.

To create a compose notification node:

1. Access the Hotline you want to add the message node to by clicking **Hotlines** in the left menu bar, selecting the appropriate Hotline and clicking **Edit**. The **Hotline Editor** appears.
2. Add a **New Compose Notification** node to Hotline by dragging **New Compose Notification** from the left column into the Hotline tree in the right column. The **Hotline Option Editor** appears. Use this editor to set the options for this node.
3. In the **Compose Name** field, type the text you want the TTS engine to read when a caller accesses this node of the Hotline. Type the words that you want callers to hear immediately after the option number. For example, to build a node that says, "Press 1 to compose a notification for the flu pandemic hotline," type `to compose a notification for the flu pandemic hotline` into the **Compose Name** field.
4. Click the **Actions** field name to bring up the **Action Editor**.
5. Set up action logging to capture information about callers accessing this node. See Capturing Node Actions for more information on gathering information on node actions.

NOTE

Compose Notification node always require identification and authentication. This security setting cannot be changed.

6. Click **Save** to save this node.
7. Continue adding other nodes or options to the hotline until it is complete.

To activate your Hotline, see Activating Your Hotline.

## Creating a Hotline Pro Poll Node

A Hotline Poll contains a question with a list of possible responses from which recipients can choose. These responses can bridge callers to a conference call and save numeric information entered by the recipient.

By default, Hotline Polls require identification. This is the minimum security setting. You can increase this security to identification and authentication by clicking the **Security** button on the **Hotline Option Editor** page and selecting the identification and authentication choice. For more information, see Security.

To set up a Hotline Pro Poll:

1. Access the Hotline you want to add the message node to by clicking **Hotlines** in the left menu bar, selecting the appropriate Hotline, and clicking **Edit**. The **Hotline Editor** appears.
2. Add a **New Hotline Poll** node to Hotline by dragging **New Hotline Poll** from the left column into the Hotline tree in the right column. The **Hotline Poll Option Editor** appears. Use this editor to set the options for this node.
3. In the **Poll Name** field, type the text you want the TTS engine to read when a caller accesses this node of the Hotline. Type the words that you want callers to hear immediately after the option number. For example, to build a node that says, “Press 1 to respond to the flu pandemic poll,” type `to respond to the flu pandemic poll` into the **Poll Name** field.
4. Enter a **Description** for this poll. The description is required. It is how you will find the poll results later in reports.
5. Click the **Actions** field name to bring up the **Action Editor**.
6. Set up action logging to capture information about callers accessing this node. See Capturing Node Actions for more information on gathering information on node actions.

NOTE

By default, Hotline Polls require at least the security level of **User Identification Required**. You can increase the security level by clicking the **Security** field name and selecting **User Identification and PIN Authentication Required**. For more information, see Security.

7. In the **Message** section, you can:

- Type a message for the AlertFind TTS engine to be read.
- Click **Call to Record** and type the phone number AlertFind should call to obtain the message. Click **Call Now** to initiate the call process. The status of the call appears in the window so that you can track the progress of recording. When the message has been recorded, the WAV appears on the **Hotline Option Editor** page.
- Click **Upload Audio** to upload an audio file. The file you upload must be a WAV file in a supported format. See Supported Audio Files.

7. In the **Responses** section, provide the responses that callers can choose for this poll. For instructions on options available in the Response Editor, see Use the Response Editor.

NOTE

A poll can have only one conference call number regardless of settings in individual responses. The last conference call number entered is the one used by the Hotline.

8. Add scheduling options to the poll so that it is presented to callers only during certain time-frames or days. See Setting Poll Scheduling or Recurrence Options for more information.
9. Create email notifications to send poll results to specific recipients. See Emailing Poll Result Reports.
10. Click **Save** to save the poll.
11. Continue adding other nodes or options to the hotline until it is complete.

To activate your Hotline, see Activating Your Hotline. You can view the results of the poll by following the instructions under Viewing Hotline Poll Results.

### Emailing Poll Result Reports

When you set up a poll, you can select to have the poll results mailed to specific recipients.

To protect private data, permissions are applied to emailed poll results:

- If you send poll results to one of your own email addresses, your permissions determine whether private data is visible in the report.
- If you send poll results to a different email address, AlertFind validates that email address against the list of active AlertFind user addresses. If the email address exists in AlertFind, the permissions associated with that email address determine whether private data is visible in the report. If the address cannot be validated, private data is not included in the report.

You can specify how long the poll will run before results are sent. This delay can be in hours and minutes with a minimum of ten minutes. The results are emailed based on the scheduled time of the Hotline Poll, or if the poll is not scheduled, they are sent to you based on the time the Hotline was activated.

NOTE

If you send email results to a disabled user, the email is sent but no private data is displayed, regardless of the permissions assigned to the recipient.

TIP

To send the report to a distribution list, create a user with the distribution list name. Grant that user permission to view (or not to view) private data. See here for a list of permissions.

To email poll results:

1. Double-click the poll node in the Hotline tree. The **Hotline Poll Option Editor** appears.
2. Click **Email Results**. The **Email Results Editor** appears.
3. Select **Email to** and type the email address to send results to.
4. For **Send results after**, enter a time in hours and minutes.
5. Click **OK**.

### Setting Poll Scheduling or Recurrence Options

By default, the poll is presented to callers anytime they call the Hotline. You can add scheduling options to the poll so that it is presented to callers only during certain time-frames or days. To set scheduling and recurrence for a Hotline Poll:

1. Double-click the poll node in the Hotline tree. The **Hotline Poll Option Editor** appears.
2. Click **Scheduling**. The **Scheduling** page appears.
3. To set date constraints to limit when the poll is presented, set a **Start Time** and **End Time**.
4. To add a recurrence pattern, select an option from the **Recurrence Pattern** drop-down list and provide specifics for the fields that appear.

TIP

When you set a recurring Hotline Poll to start in the past, the poll begins as soon as you activate the Hotline, and then recurs on the pattern you specify.

5. Click **Save**. The **Hotline Poll Option Editor** page appears, and the **Scheduling** field displays your entry.

### Viewing Hotline Poll Results

You can view Hotline Poll results for one specific Hotline or for all Hotlines. To view Hotline Poll Results:

1. Click **Hotlines** in the menu bar. The **Hotlines** page appears.
2. Click **View Results** on the **Hotlines** page menu and choose either:
   - **Poll Results for Selected Hotline**
   - **Poll Results for All Hotlines**

If you select **Poll Results for Selected Hotline**, the **Hotline Polls** page for the selected Hotline appears.

- You can search this list by subject or by state (**All**, **Current**, **Completed**, **Future**). The **Current** list includes expired and disabled polls. Future occurrences of recurring polls appear when you select **Future**. Past occurrences of recurring polls appear when you select **Completed**.
- To sort the list alphabetically (ascending or descending), click the **Subject** column heading.
- Click **Download** to download a summary report about this Hotline; click **Download Detailed** to download a detailed report about this Hotline.
- Click the plus sign to display the poll question and the **Details** button, which displays the **Results** page for this poll.
- The **Results** page displays the **Responses**, **Time Summary**, and **Recipients** tabs. It also displays **Basic Info**, **Delivery Options**, and **Conference Calls Info.**

If you select **Poll Results for All Hotlines**, the **Hotline Polls** page appears with a list of all Hotlines Polls on all Hotlines in this team context.

- You can search the list by subject.
- To sort the list alphabetically (ascending or descending), click the **Subject** column heading.
- To download a summary report or a detailed report for this set of Hotlines, click the appropriate download button.
- Click the plus sign to display the poll question and the **Details** button, which displays the **Results** page for this poll.
- The **Results** page displays the **Responses**, **Time Summary**, and **Recipients** tabs. It also displays **Basic Info**, **Delivery Options**, and **Conference Calls Info.**

## Creating a Conference Call Node

You can add a conference call node to allow callers to transfer to a conference call.

To add a conference call node:

1. Access the Hotline you want to add the message node to by clicking **Hotlines** in the left menu bar, selecting the appropriate Hotline, and clicking **Edit**. The **Hotline Editor** appears.
2. Add a **New Conference Call** node to Hotline by dragging **New Conference Call** from the left column into the Hotline tree in the right column. The **Hotline Option Editor** appears. Use this editor to set the options for this node.
3. In the **Conference Call Name** field, type the text you want the TTS engine to read when a caller accesses this node of the Hotline. Type the words that

you want callers to hear immediately after the option number. For example, to build a message node that says, “Press 1 to connect to the conference call,” type `to connect to the conference call` into the **Conference Call Name** field.

4. Click the **Actions** field name to bring up the **Action Editor**.
5. Set up action logging to capture information about callers accessing this node. See Capturing Node Actions for more information on gathering information on node actions.

NOTE

- By default, conference call nodes have no security restrictions. You can increase this to **User Identification Required** or **User Identification and PIN Authentication Required**. When you increase security for a node, a lock icon appears on the node in the Hotline Pro tree. For more information about security, see Security.
- When callers call in to Hotline Pro from a phone in their AlertFind personal escalation list, AlertFind recognizes them but still asks them to identify themselves by asking, “If you are Sam, press 1. If you are not Sam, press 2.”

TIP

You can control access to sub-options by setting security at the main message level. Sub-options (children) inherit the security of the main message (the parent). This can be used to simplify security management.

5. To enter the conference call phone number, select **US/Canada** or **Other** and enter a valid **Phone Number**.
6. Enter the conference call **Meeting ID**.
7. If your conference call provider requires additional dialing prefixes, suffixes, or settings, select `On` for **Custom conference call provider settings** and enter any data required.
8. Click **Save** to save this node.
9. Continue adding other nodes or options to the hotline until it is complete.

To activate your Hotline, see "Activating Your Hotline".

## Creating a Hotline Transfer Node

You can create Hotline Transfer nodes to transfer a caller from one Hotline to another. You are limited only by the number of Hotline phone numbers you have available. For example, in a flu pandemic situation, you might want to transfer well callers to one Hotline and sick callers to another Hotline. In this case, you can create two Hotline transfer options, one for well callers and one for sick callers.

If your company purchased language packs, you can use this feature to set up a main Hotline that transfers callers to a Hotline in their preferred language.

To add a new Hotline Transfer node:

1. Access the Hotline you want to add the message node to by clicking **Hotlines** in the left menu bar, selecting the appropriate Hotline, and clicking **Edit**. The **Hotline Editor** appears.
2. Add a **New Hotline Transfer** node to Hotline by dragging **New Hotline Transfer** from the left column into the Hotline tree in the right column. The **Hotline Option Editor** appears. Use this editor to set the options for this node.
3. In the **Hotline Transfer Name** field, type the text you want the TTS engine to read when a caller accesses this node of the Hotline. Type the words that you want callers to hear immediately after the option number. For example, to build a message node that says, “Press 1 to transfer to the English language hotline,” type `to transfer to the English language hotline` into the **Hotline Transfer Name** field.
4. Click the **Actions** field name to bring up the **Action Editor**.
5. Set up action logging to capture information about callers accessing this node. See Capturing Node Actions for more information on gathering information on node actions.

NOTE

- By default, hotline transfer nodes have no security restrictions. You can increase this to **User Identification Required** or **User Identification and PIN Authentication Required**. When you increase security for a node, a lock icon appears on the node in the Hotline Pro tree. For more information about security, see Security.
- When callers call in to Hotline Pro from a phone in their AlertFind personal escalation list, AlertFind recognizes them but still asks them to identify themselves by asking, “If you are Sam, press 1. If you are not Sam, press 2.”

TIP

You can control access to sub-options by setting security at the main message level. Sub-options (children) inherit the security of the main message (the parent). This can be used to simplify security management.

6. In the **Select a phone number** section, choose the hotline to transfer callers to when they choose this option.
7. Click **Save** to save this node. Continue adding other nodes or options to the hotline until it is complete.

To activate your Hotline, see "Activating Your Hotline".

## Creating a Numeric Capture Node

A numeric capture node allows you to collect specific numeric information from callers. For example, you can add a Numeric Capture node to find out how many days an employee has been sick with the flu, or how high the employee’s body temperature has been during the last 24 hours.

When a caller provides a numeric response to a numeric capture node, the **Capture Data Field Name** (that you provide when you create the node) and value (as entered by the caller) are written to the call log report.

| Hotline Name | User Name | Call ID | Call Start Time | Action Time | Call Data Name | Call Data Value |
|---|---|---|---|---|---|---|
| Flu Data Collection | Julie Smith | 1215 | 8/5/2018 13:38 | 8/5/2018 13:38 | Employee Fever | 1002 |
| Flu Data Collection | Julie Smith | 1215 | 8/5/2018 13:38 | 8/5/2018 13:39 | Days Sick | 1 |

There are a few important considerations you must plan for when you use numeric capture nodes:

- **Field names are reusable during calls.** If a caller accesses the same node more than once and enters data each time, your call log report will show each successive field name and value pair captured during the call.
- AlertFind does not process, filter, or manipulate these reports in any way. For example, if a caller responds to a node and then goes back to respond again, your report might look like the following. See Best Practices for Hotline Data Collection for important planning considerations and methods for using numeric capture along with node Action reporting.

| Hotline Name | User Name | Call ID | Call Start Time | Action Time | Call Data Name | Call Data Value |
|---|---|---|---|---|---|---|
| Flu Data Collection | Julie Smith | 1215 | 8/5/2018 13:38 | 8/5/2018 13:38 | Employee Fever | 1002 |
| Flu Data Collection | Julie Smith | 1215 | 8/5/2018 13:38 | 8/5/2018 13:39 | Days Sick | 1 |
| Flu Data Collection | Julie Smith | 1215 | 8/5/2018 13:38 | 8/5/2018 13:40 | Days Sick | 2 |

To create a numeric capture node:

1. Access the Hotline you want to add the message node to by clicking **Hotlines** in the left menu bar, selecting the appropriate Hotline, and click **Edit**. The **Hotline Editor** appears.
2. Add a **New Numeric Capture** node to Hotline by dragging **New Numeric Capture** from the left column into the Hotline tree in the right column. The **Hotline Option Editor** appears. Use this editor to set the options for this node.
3. In the **Numeric Capture Name** field, type the text you want the TTS engine to read when a caller accesses this node of the Hotline. Type the words that you want callers to hear immediately after the option number. For example, to build a message node that says, “Press 1 to enter the number of days you

have had flu symptoms," type `to enter the number of days you have had flu symptoms` into the **Numeric Capture Name** field.

4. Provide a descriptive **Field Name** for the data you are requesting the caller to enter, such as `Number of Days Ill` or `Highest temperature in last 24 hours.`

NOTE

Because this feature is so highly customizable, numeric capture labels are written to the report exactly as you enter them in the **Capture Data Field Name** field. AlertFind does not process, filter, or manipulate numeric capture data in any way.

5. Click the **Actions** field name to bring up the **Action Editor**.
6. Set up action logging to capture information about callers accessing this node. See "Capturing Node Actions" for more information on gathering information on node actions.

NOTE

- By default, hotline transfer nodes have no security restrictions. You can increase this to **User Identification Required** or **User Identification and PIN Authentication Required**. When you increase security for a node, a lock icon appears on the node in the Hotline Pro tree. For more information about security, see "Security".
- When callers call in to Hotline Pro from a phone in their AlertFind personal escalation list, AlertFind recognizes them but still requests them to identify themselves by asking, "If you are Sam, press 1. If you are not Sam, press 2."

TIP

You can control access to sub-options by setting security at the main message level. Sub-options (children) inherit the security of the main message (the parent). This can be used to simplify security management.

6. In the **Message** section, you can:
   - Type a message for the AlertFind TTS engine to read.
   - Click **Call to Record** and type the phone number AlertFind should call to obtain the message. Click **Call Now** to initiate the call process. The status of the call appears in the window so that you can track the progress of recording. When the message has been recorded, the WAV appears on the **Hotline Option Editor** page.
   - Click **Upload Audio** to upload an audio file. The file you upload must be a WAV file in a supported format. See Supported Audio Files.
7. Click **Save** to save this node.
8. Continue adding other nodes or options to the hotline until it is complete.

To activate your Hotline, see Activating Your Hotline.

## Security

**Compose Notification** and **Notification Inbox** nodes require that users identify themselves with a phone number or name (or external key, if that option is used by your company), and authenticate with a PIN. **Hotline Poll** nodes require at least identification (but not authentication).

Other node types do not require security settings. You can choose:

- **No restrictions**–Anyone can hear the message.
- **User Identification Required**–Callers must identify themselves to AlertFind before hearing the announcement or continuing to further sub-options.
- **User Identification and PIN Authentication Required**–Callers must identify themselves to AlertFind and enter their PIN before hearing the announcement or continuing to further sub-options.

You can also set security on the welcome message after you have authenticated yourself to AlertFind. Adding security at this level prevents callers from accessing any of your Hotline Pro options until they identify or authenticate themselves (depending on the security setting you select).

NOTE

When callers call in to Hotline Pro from a phone in their AlertFind personal escalation list, AlertFind recognizes them but still requests them to identify themselves by asking, “If you are Sam, press 1. If you are not Sam, press 2.”

The lock icon indicates a node that has security explicitly set to be higher than its parent option or its default security level. Any options inside this node will inherit its security settings.

## Activating Your Hotline

When you have added all of your options to the Hotline, click **Activate Hotline.** The **Hotline Activation Editor** page appears. The **Hotline Activation Editor** page displays all of the available Hotline numbers. Select the phone numbers you want to assign to this Hotline and click **Save**.

You can also activate your Hotline by selecting it, clicking **Edit**, and then clicking **Activate**.

NOTE

Your Hotline is not available to callers until you activate it. You must reactivate after any changes to hear those changes.

## Using Hotline Pro Phone Numbers

When Hotline Pro is provisioned, you are given one Hotline phone number. To request additional numbers, contact your AlertFind administrator.

If you assign a Hotline Pro phone number, which is already assigned to another Hotline, to a new Hotline, the phone number is removed from the first Hotline and reassigned to the new Hotline.

TIP

You may assign useful labels such as `Toll Free` to Hotline Pro numbers so that users can select the appropriate Hotline Pro phone number.

NOTE

Each Hotline phone number is associated with one language. If you want to have Hotlines available in different languages, you must purchase additional language packs and Hotline phone numbers, and have the languages enabled by Support.

## Editing a Hotline

To make changes to a Hotline, select the Hotline and then select **Edit > Edit Hotline Details** or right-click on the Hotline and select **Edit Hotline Details**. Doing so creates a draft Hotline that can be edited without changing the original Hotline. You can edit active and inactive Hotlines.

To view the Hotline without creating a draft, double-click on the Hotline or select the Hotline and select **View** on the toolbar.

When you edit a Hotline, you edit a draft copy of the selected Hotline. Your changes are not made active (available to be heard in the Hotline) and will not affect the active Hotline until you re-activate the Hotline.

Users with `Manage Hotline` permissions may edit Hotlines by calling the Hotline's phone number. Once the Hotline has been connected, press the pound key on your phone (#), enter your pin number, and follow the prompts.

Changes made over the phone will become active immediately. If there is an inactive draft of the Hotline made through the website, changes made over the phone will not affect the draft copy, changes will only affect the active version of the Hotline.

You cannot activate an archived Hotline. You must restore it first, then reactivate it.

## Changing the Order of Hotline Options

To change the order of options in your Hotline, drag them into place. The blue dotted lines show you where the option will be placed.

To make an option a sub-option, select the option you want to move and drag it onto the option that is the parent option. The parent option is grayed when it is selected.

## Using Quick Launch IDs with Hotline Pro

If your AlertFind instance has notification templates, broadcast groups, or escalation groups, or Smart Groups with Quick Launch IDs, you can launch a notification using the Hotline Pro voice interface.

### NOTE

All Quick Launch IDs must be unique. In other words, you cannot have a notification template Quick Launch ID that is the same as a broadcast group, escalation group, or Smart Group Quick Launch ID.

**Launch a notification with a broadcast group, escalation group, or Smart Group Quick Launch ID:**

1. Call the Hotline Pro number. The Hotline must have a **Compose Notification** option.
2. Follow the voice prompts to select **Compose Notification.**
3. Identify yourself and enter your PIN.
4. Press 1 to enter a Quick Launch ID.
5. Use the keypad of your phone to type the Quick Launch ID.
6. AlertFind reads the name associated with the Quick Launch ID.
7. If this Quick Launch ID is associated with multiple teams, you are asked to select the appropriate team.
8. Follow the voice prompts to compose a notification for this group.
9. Record your message.
10. Follow the voice prompts to accept or rerecord the message.
11. AlertFind requests you to wait while it processes your request.
12. Select from one of the four options:
    1. Press 1 to send the notification.
    2. Press 2 to set the priority of the notification.
    3. Press 3 to define when or if notification results should be mailed to you.
    4. Press 4 to turn on authentication for this notification. This requires callers to authenticate themselves before hearing the notification.
13. After setting the priority, defining email results behavior, and setting authentication (if required), press 1 to send the notification. AlertFind informs you that the notification has been initiated.
14. You can now review notification status by logging in to the AlertFind web interface and clicking **Sent Notifications**.

### Launch a notification using a notification template Quick Launch ID:

1. Call the Hotline Pro number. The Hotline must have a **Compose Notification** option.
2. Follow the voice prompts to select **Compose Notification**.
3. Identify yourself and enter your PIN.
4. Press 1 to enter a Quick Launch ID.
5. Use the keypad of your phone to type the Quick Launch ID.
6. AlertFind informs, “You are about to open an incident from the notification template [template name] with description [description].” You are offered four options:

    1. Press 1 to open an incident with this notification template and send all notification tasks that are not set for manual execution.
    2. Press 3 to review the notification tasks for this notification template. If you select this option, AlertFind reads the notification tasks to you. It also offers you the ability to review the recipient list and reads the priority of the notification to you.

NOTE

It is possible to send a notification template with no associated tasks. To ensure you do not accidentally do this, press 3 to review notification tasks before sending the notification template.

    3. Press 9 to select a different notification template.
    4. Press 0 to return to the Main Menu.

7. You can now review notification status by logging in to the AlertFind web interface and clicking **Sent Notifications**.

## Gathering Data From Hotline Pro Calls

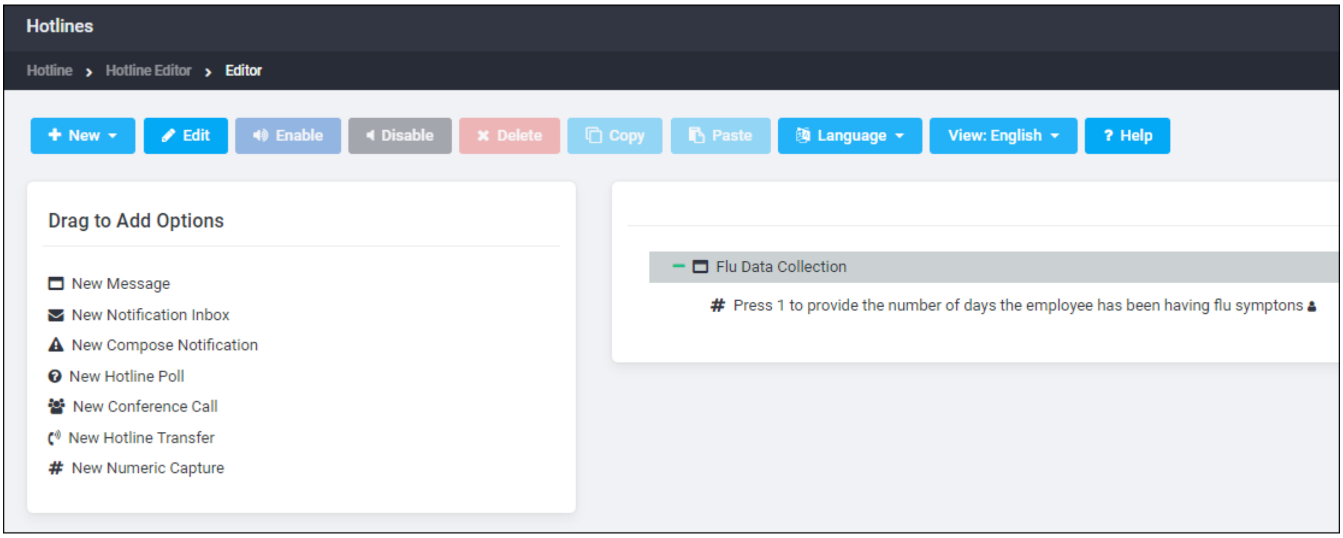
Using Hotline Pro, you can report on information gathered during calls. You can gather information by adding **Numeric Capture** nodes to a Hotline, or by adding **Action** options to any node. See the following sections for instructions:

- Creating a Numeric Capture Node
- Capturing Node Actions
- Best Practices for Hotline Data Collection

### Capturing Node Actions

For any type of node that you add to a hotline, you can collect and report on when callers access (or traverse) each node during calls. To capture and report on callers accessing a selected node, define an **Action** that is written to the call log report whenever callers access the node.

For example, the sample Hotline in this figure contains several message nodes that collect information about whether employees or their family members are showing any signs of the flu. These two message nodes indicate either that the employee *is* showing flu symptoms or that the employee is *not* showing any symptoms.



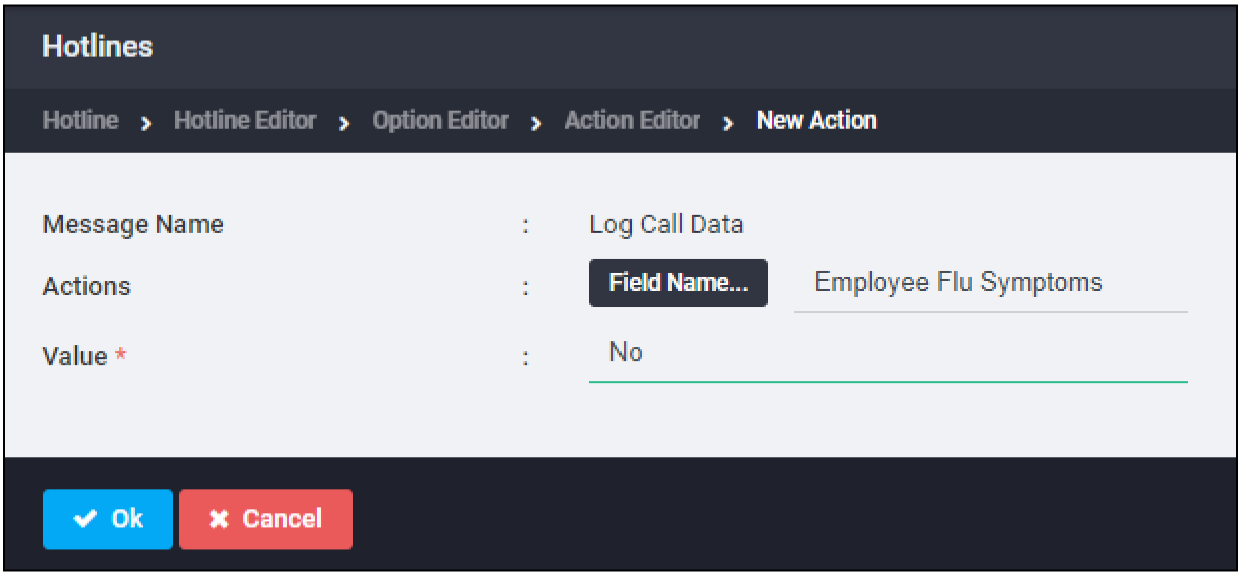
Flu Data Collection

Press 1 to provide the number of days the employee has been having flu symptoms

## Collect information on nodes during a call:

For each node you want to report on, click the **Actions** button to define a **Field Name** and corresponding **Value** to be reported in the call log.

For example, to gather responses from node 1 (`Press 1 if the employee is not showing any signs of the flu`), add an **Action** to that message node using the following **Field Name** and **Value**.


Hotlines
Hotline › Hotline Editor › Option Editor › Action Editor › New Action
Ok
Cancel

| | | |
|---|---|---|
| Message Name | : | Log Call Data |
| Actions | : | Field Name... Employee Flu Symptoms |
| Value * | : | No |

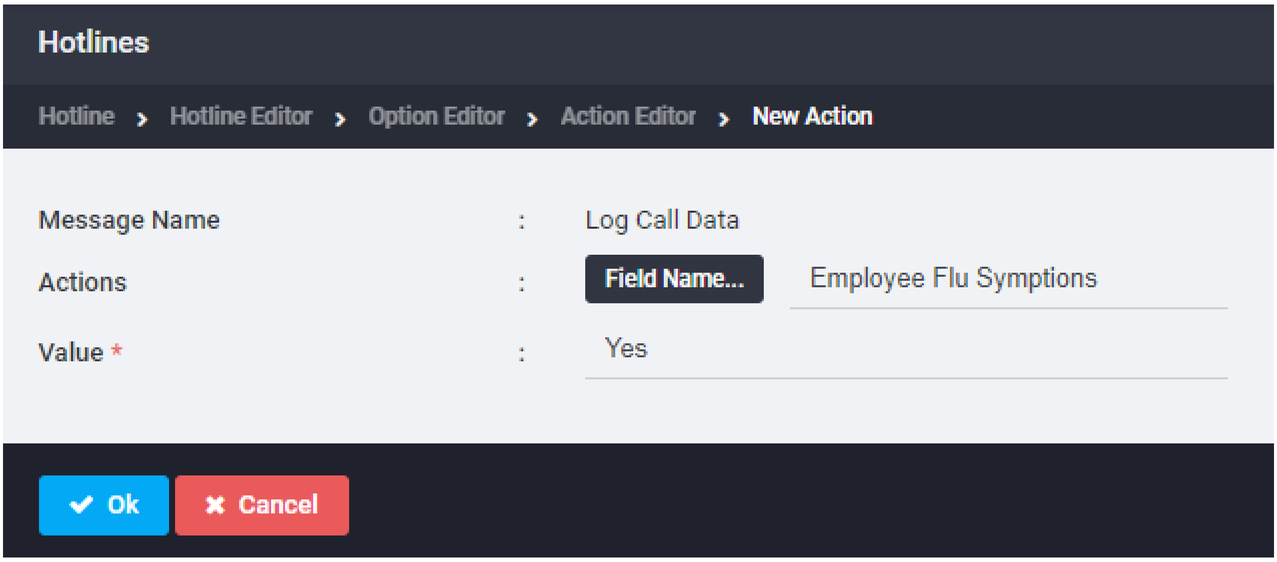
NOTE

Because this feature is so highly customizable, the fields and values captured are written to the report exactly as you enter them in the **Action** dialog boxes. AlertFind does not process, filter, or manipulate the field or value data in any way.

When a caller presses `1` in response to this message, this field name and value are written to the call log report.

| Hotline Name | User Name | Call ID | Call Start Time | Action Time | Call Data Name | Call Data Value |
|---|---|---|---|---|---|---|
| Flu Data Collection | John Smith | 1201 | 8/5/2018 13:38 | 8/5/2018 13:38 | Employee Flu Symptoms | NO |

To gather responses from node 2 (`Press 2 if the employee is showing symptoms of the flu`), add an **Action** to the message node using the following **Field Name** and **Value**.



Hotlines

Hotline › Hotline Editor › Option Editor › Action Editor › New Action

Message Name : Log Call Data

Actions : Field Name... Employee Flu Symptions

Value * : Yes

When a caller presses `2` in response to this message, this field name and value are written to the call log report.

| Hotline Name | User Name | Call ID | Call Start Time | Action Time | Call Data Name | Call Data Value |
|---|---|---|---|---|---|---|
| Flu Data Collection | John Doe | 1205 | 8/5/2018 13:52 | 8/5/2018 13:53 | Employee Flu Symptoms | YES |

You can choose to collect information on only one of these nodes. For example, to collect and report only on confirmed cases of employee illness, set the **Action** only on node 2 (`Press 2 if the employee is showing symptoms of the flu`). Your report would contain entries only for actions on node 2.

CAUTION

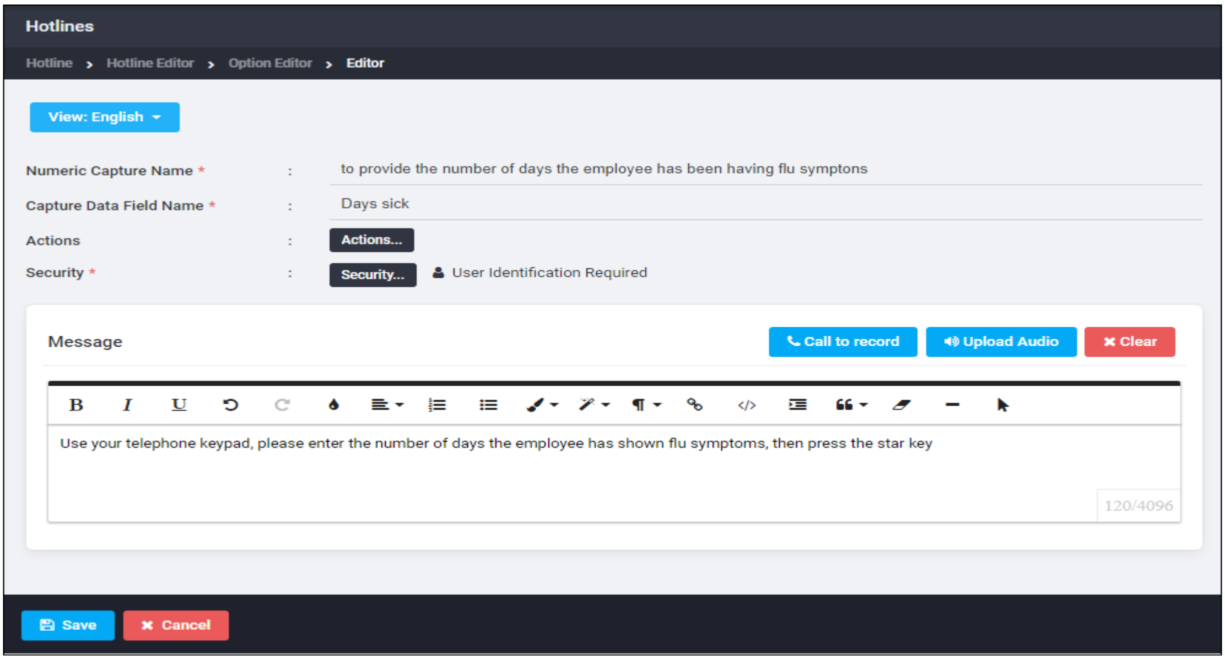
If you *manually deactivate and edit* a Hotline with Action reporting after it has been activated, you *will lose* any node action reporting that had been collected prior to the changes being made to the Hotline. If you need to edit a Hotline with Action reporting after it has been activated, use one of these workarounds to preserve your reporting data:

- **Do not manually deactivate the Hotline before you edit it.** Instead, edit the Hotline while it is in the Active state. This will cause the system to automatically archive the original Hotline (and its reporting results) before activating the new Hotline with your changes. You can find the results of the original Hotline in the archive.
- **Archive the Hotline before you edit and reactivate it.** This will archive the data collected up to the time of the archive, edit, or reactivation.
- **Run and save a Hotline Pro Call Details report** for the Hotline before editing it. This will give you a report of the data collected up to the time of the edit.

### Best Practices for Hotline Data Collection

Because neither Node **Action** nor **Numeric Capture** field names have to be unique and can be reused as many times as they are accessed during a call, you must plan and set up your data collection Hotline to use field names and values to produce usable reports.

For example, you could use a **Numeric Capture** node to collect information on how many days an employee or any members of the employee's household have been sick with the flu. You could create a Numeric Capture node with a **Capture Data Field Name** of `Days Sick`.



Numeric Capture Name * : to provide the number of days the employee has been having flu symptons

Capture Data Field Name * : Days sick

Actions : Actions...

Security * : Security... User Identification Required

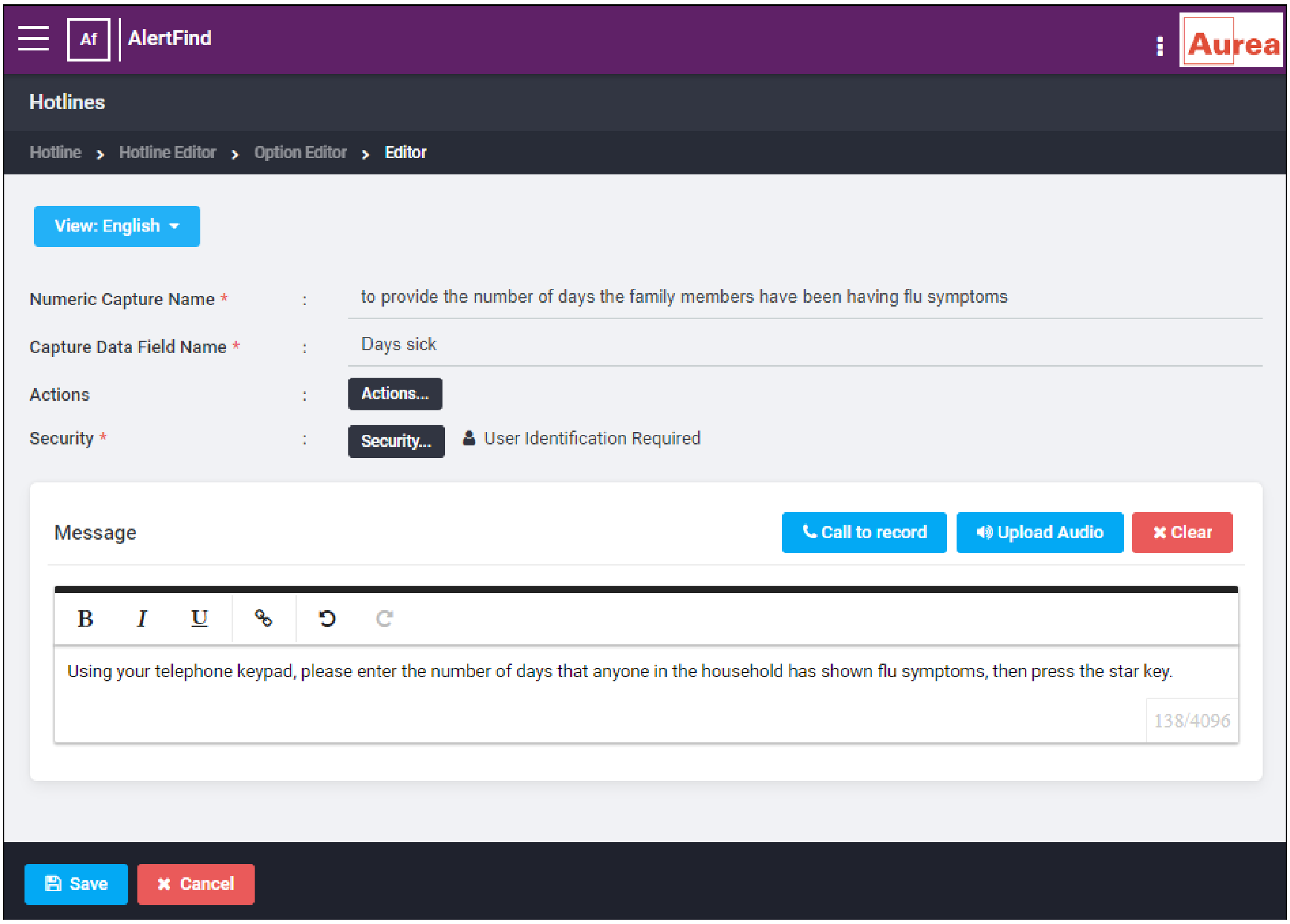
Use your telephone keypad, please enter the number of days the employee has shown flu symptoms, then press the star key

120/4096

When a caller uses this node to report than an employee has been ill for three days, an entry appears in the call log reading as in the example below.

| Hotline Name | User Name | Call ID | Call Start Time | Action Time | Call Data Name | Call Data Value |
|---|---|---|---|---|---|---|
| Flu Data Collection | Julie Smith | 1215 | 8/5/2018 13:38 | 8/5/2018 13:40 | Days Sick | 3 |

If you also wanted to gather information on how many days that other members of the employee's household have been sick, you could copy the **Numeric Capture** node you created and modify it to ask for the number of days other household members have been sick. This copied node would also have a **Capture Data Field Name** of `Days Sick`.



Numeric Capture Name * : to provide the number of days the family members have been having flu symptoms

Capture Data Field Name * : Days sick

Actions :

Security * : User Identification Required

Message

Using your telephone keypad, please enter the number of days that anyone in the household has shown flu symptoms, then press the star key.

138/4096

When a caller uses this node to report that another member of the employee's household has been ill for two days, a second entry will appear in the call log as in the example below. Without any additional identifying information, this report would tell you the number of days people have been sick, but would give you no way to classify that data by days of employee illness versus days of household member illness.

| Hotline Name | User Name | Call ID | Call Start Time | Action Time | Call Data Name | Call Data Value |
|---|---|---|---|---|---|---|
| Flu Data | Julie | 1215 | 8/5/2018 | 8/5/2018 | Days Sick | 3 |

| Hotline Name | User Name | Call ID | Call Start Time | Action Time | Call Data Name | Call Data Value |
|---|---|---|---|---|---|---|
| Collection | Smith | | 13:38 | 13:40 | | |
| Flu Data Collection | Julie Smith | 1215 | 8/5/2018 13:38 | 8/5/2018 13:41 | Days Sick | 1 |

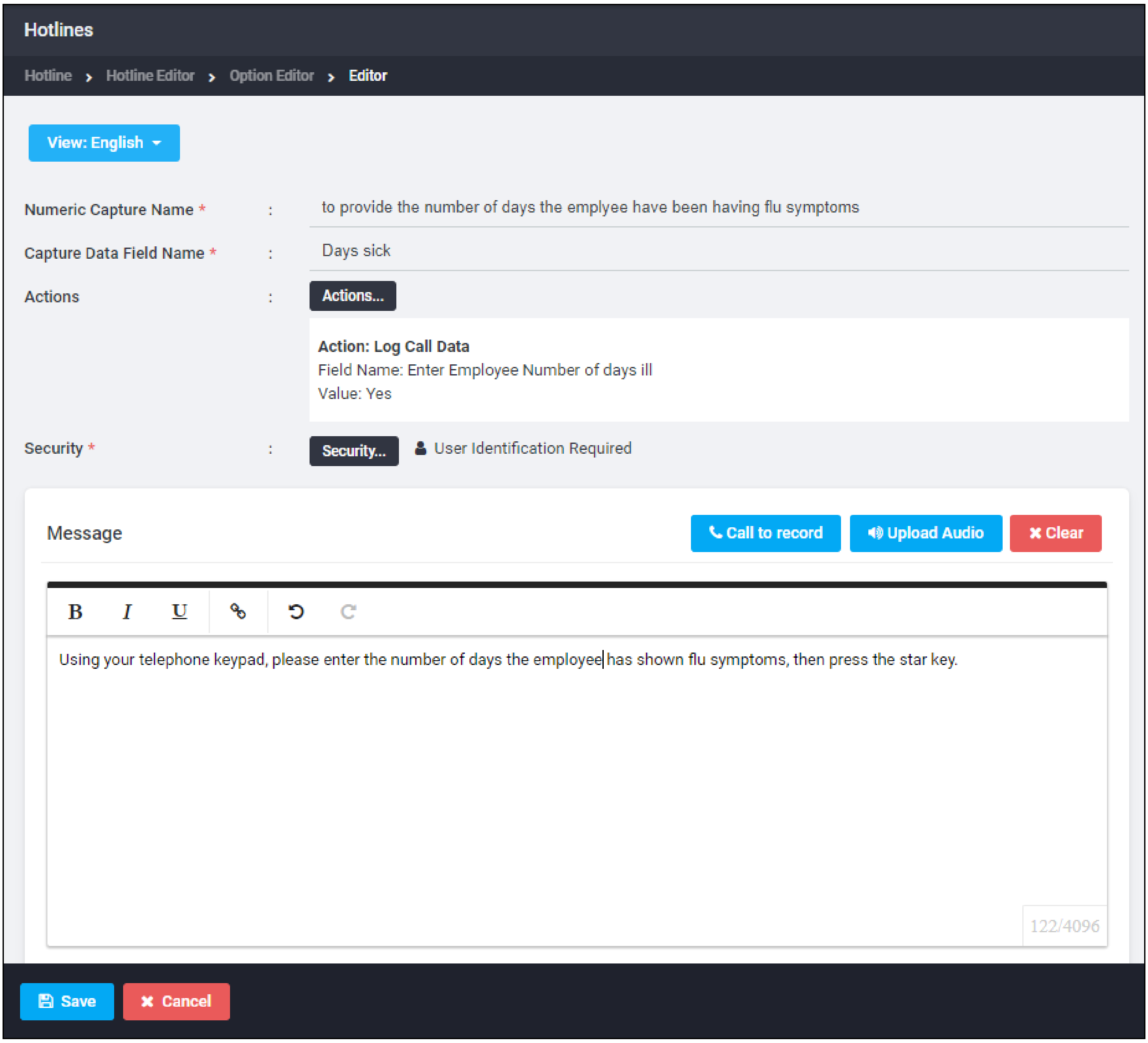
If you were only interested in compiling a general report of the number of days employees or their family members have been sick, then reusing this same field name could be acceptable. However, if you were interested in classifying the number of days *employees* have been sick separately from the number of days *household members* have been sick, reusing this field name will not allow you to extract such details from the call log report.

There are two ways to differentiate these two different data points to create a more robust, usable report.

- **Define unique Capture Data Field Names for each Numeric Capture node.** One method to capture clearly identifiable data is to use a different **Capture Data Field Name** for each Numeric Capture node. In this case, you could copy the Numeric Capture node you created for the employee and modify it to ask for the number of days other household members have been sick. You would also have to change the **Capture Data Field Name** to a more descriptive value, such as `Household Members Days Sick`. You might also provide a descriptive value for the employee days sick field name, such as `Employee Days Sick`. Using these unique Capture Data Field Names, entries in your call log report would look like this:

| Hotline Name | User Name | Call ID | Call Start Time | Action Time | Call Data Name | Call Data Value |
|---|---|---|---|---|---|---|
| Flu Data Collection | Julie Smith | 1215 | 8/5/2018 13:38 | 8/5/2018 13:40 | Employee Days Sick | 3 |
| Flu Data Collection | Julie Smith | 1215 | 8/5/2018 13:38 | 8/5/2018 13:41 | Family Member Days Sick | 1 |

- **Combine generic, reusable Capture Data Field Names with unique Action Node Field Names.** A second method allows you to reuse generic Capture Data Field Names in conjunction with Action Node field names. Using this method, you could keep both **Capture Data Field Names** set to `Days Sick`, but you would add an Action to each Numeric Capture node to identify which node the caller is responding to. For example, the Numeric Capture node asking how many days the employee has been sick would include an **Action** like this:



Numeric Capture Name * : to provide the number of days the emplyee have been having flu symptoms

Capture Data Field Name * : Days sick

Actions :

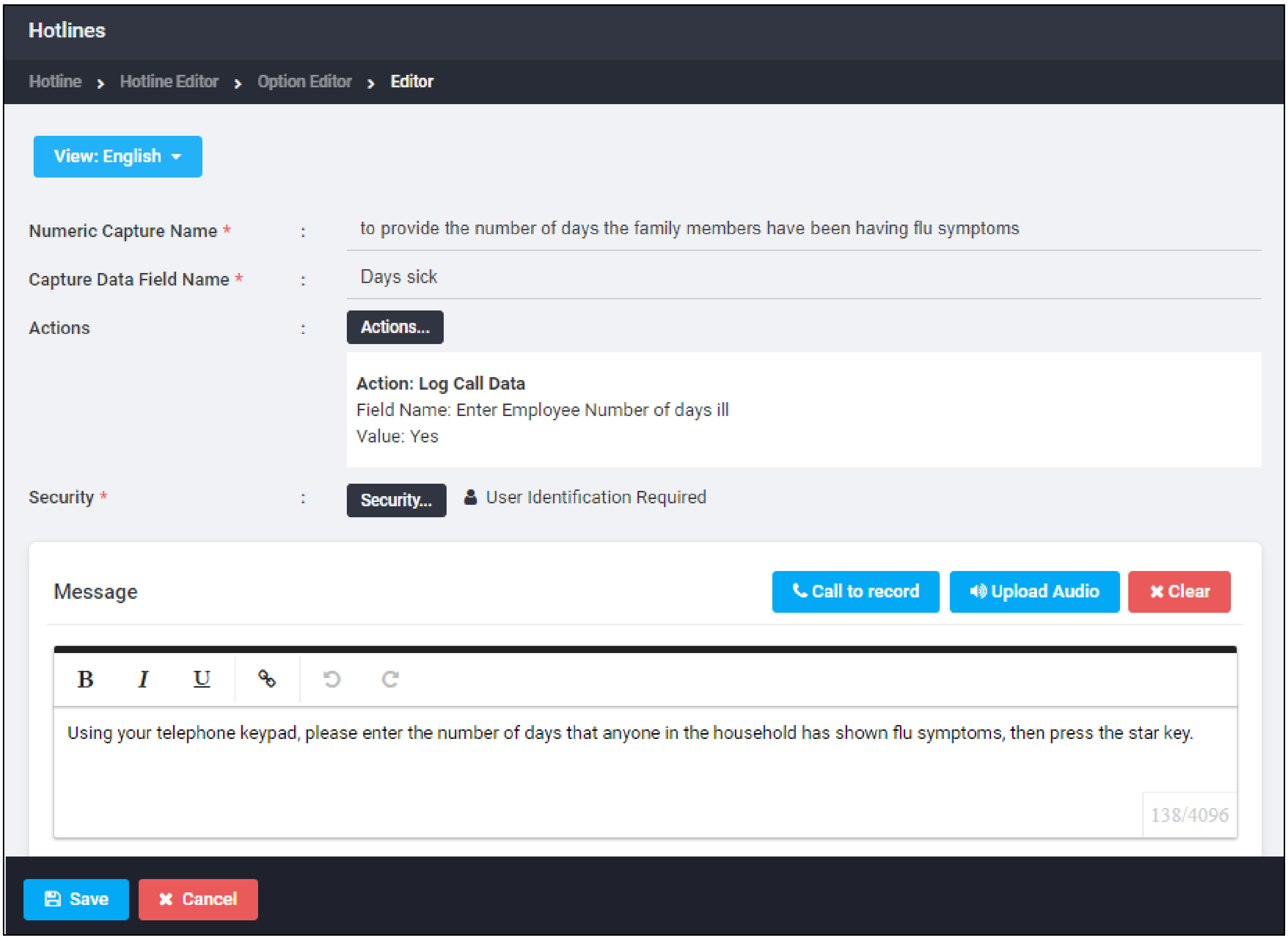
**Action: Log Call Data**
Field Name: Enter Employee Number of days ill
Value: Yes

Security * : User Identification Required

Using your telephone keypad, please enter the number of days the employee has shown flu symptoms, then press the star key.

122/4096

And Numeric Capture node asking how many days other members of the household have been sick would include an **Action** like this:



Numeric Capture Name * : to provide the number of days the family members have been having flu symptoms

Capture Data Field Name * : Days sick

Actions :

Action: Log Call Data
Field Name: Enter Employee Number of days ill
Value: Yes

Security * : User Identification Required

Message

Using your telephone keypad, please enter the number of days that anyone in the household has shown flu symptoms, then press the star key.

138/4096

The combination of capturing the Action on the node plus the Numeric Capture information provides a report like the following one.

| Hotline Name | User Name | Call ID | Call Start Time | Action Time | Call Data Name | Call Data Value |
|---|---|---|---|---|---|---|
| Flu Data Collection | Julie Smith | 1215 | 8/5/2018 13:38 | 8/5/2018 13:40 | Entered Employee Number of Days Ill | YES |
| Flu Data Collection | Julie Smith | 1215 | 8/5/2018 13:38 | 8/5/2018 13:40 | Days Sick | 3 |
| Flu Data Collection | Julie Smith | 1215 | 8/5/2018 13:38 | 8/5/2018 13:41 | Entered Family Member Number of Days Ill | YES |
| Flu Data Collection | Julie Smith | 1215 | 8/5/2018 13:38 | 8/5/2018 13:41 | Days Sick | 1 |

## CAUTION

If you *manually deactivate and edit* a Hotline with Action reporting after it has been activated, you *will lose* any node action reporting that had been collected prior to the changes being made to the Hotline. If you need to edit a Hotline with Action reporting after it has been activated, use one of these workarounds to preserve your reporting data:

- **Do not manually deactivate the Hotline before you edit it.** Instead, edit the Hotline while it is in the Active state. This will cause the system to automatically archive the original Hotline (and its reporting results) before activating the new Hotline with your changes. You can find the results of the original Hotline in the archive.
- **Archive the Hotline before you edit and reactivate it.** This will archive the data collected up to the time of the archive, edit, or reactivation.
- **Run and save a Hotline Pro Call Details report** for the Hotline before editing it. This will give you a report of the data collected up to the time of the edit.

## Archived Hotlines

To view archived Hotlines, click **Archive** under **Hotlines** drop-down list located at the top of the **Hotlines** page. The list of archived Hotlines appears.

To reactivate an archived Hotline:

1. Select the Hotline you want to reactivate.
2. Click **Edit** in the menu. The drop-down list appears.
3. Select **Restore selected archive**. This Hotline now appears in your list of Hotlines (visible when you click **Hotlines** in the left menu bar.

NOTE

You can hide information about archived Hotlines by right-clicking on the column heading to display the drop-down list. From this list, select **Columns**. Uncheck the columns you do not want to display.

# Chapter 5: Reporting

Several types of reports are available to administrators and team leaders. On any page that has a **Download** button, a CSV report of the information on that page can be downloaded.

In addition, the following reports are available:

1. *Reports Lists* provides many reports that can be customized to provide only the information needed, then viewed interactively, exported in CSV or PDF, or saved to recreate new reports with the same parameters. See Report Lists - Report Templates and Report Lists - My Reports .
2. *Device Reports* provide information about users and devices, such as users with no configured devices, or with specific devices configured. Reminders can be sent to users based on the results of Device Reports. See Devices Report.

## Report Lists - Report Templates

The **Report Lists** menu option allows administrators, and other users with permission, to create and customize many AlertFind reports.

Most reports are generated exactly the same way. See the following sections for general instructions:

- Create Reports - General Instructions
- Configure and Save Custom Reports

For report-specific information, refer to the following report sections:

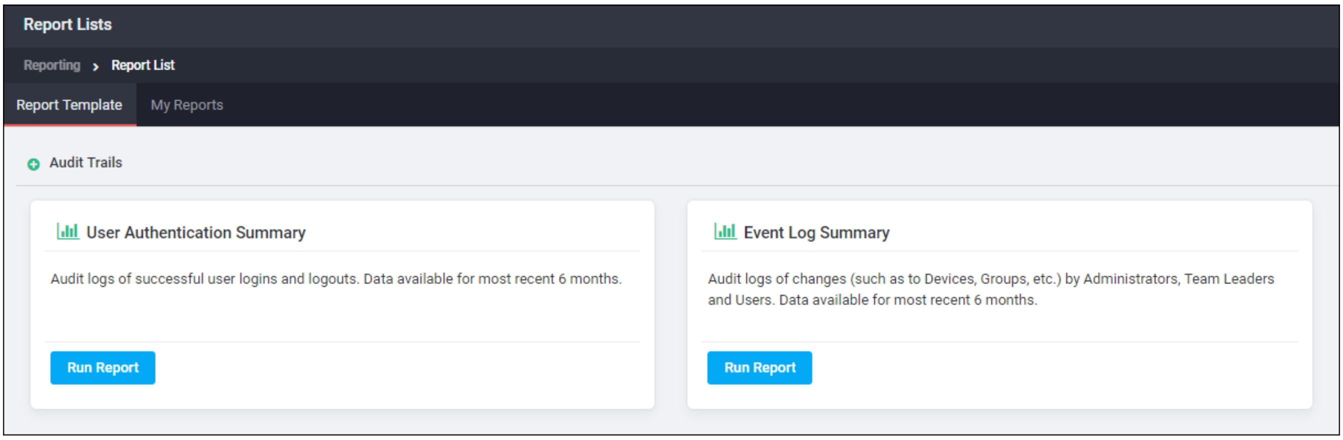
- Audit Trail Reports (see Audit Trails Reports )
- Group Reports (see Group Reports )
- Hotline Reports (see Hotline Reports )
- Incident Reports (see Incident Reports )
- Notification Reports (see Notification Reports )
- Team Reports (see Team Reports )
- Usage Reports (see Usage Reports )
- User Reports (see User Reports )

You can run the reports in real time from the **Report Templates** tab, or you can configure and save customized settings for reports that you run frequently or that you want to schedule to generate on a recurring basis. These customized report settings are then saved for you in the report you have named on the **My Reports** tab. See Report Lists - My Reports.

## Create Reports - General Instructions

### Create a report:

1. Verify the correct team context. For more information, see Team Security Context.
2. From the left navigation menu, Reporting section click **Report Lists**. The available reports appear on the **Report Templates** tab. Scroll down for more reports.



Report Lists

Reporting > Report List

Report Template | My Reports

Audit Trails

User Authentication Summary

Audit logs of successful user logins and logouts. Data available for most recent 6 months.

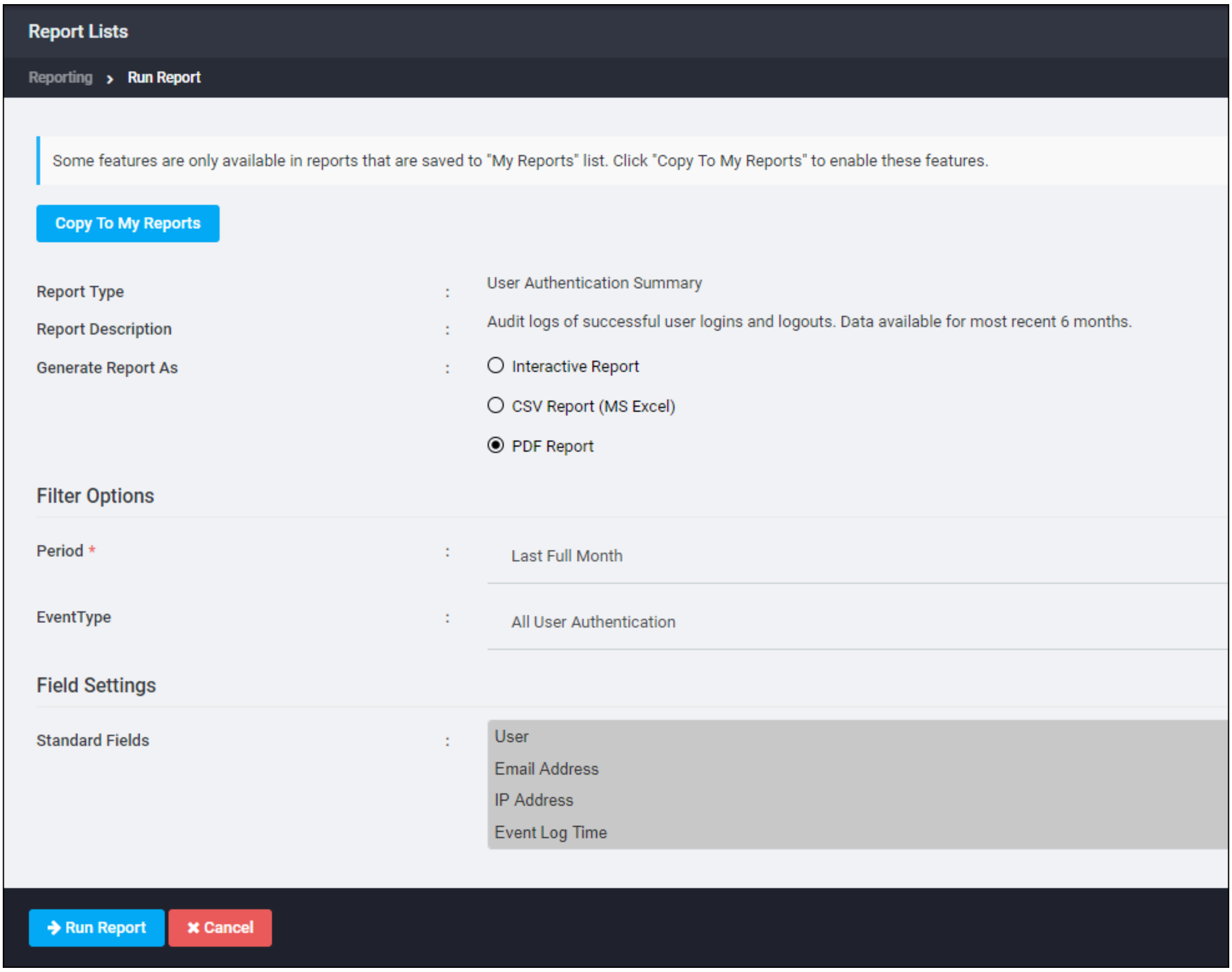
Run Report

Event Log Summary

Audit logs of changes (such as to Devices, Groups, etc.) by Administrators, Team Leaders and Users. Data available for most recent 6 months.

Run Report

3. Double-click the report to bring up the **Define Report Parameters** page.


Report Lists

Reporting > Run Report

Some features are only available in reports that are saved to "My Reports" list. Click "Copy To My Reports" to enable these features.

Report Type : User Authentication Summary

Report Description : Audit logs of successful user logins and logouts. Data available for most recent 6 months.

Generate Report As : ○ Interactive Report ○ CSV Report (MS Excel) ● PDF Report

Filter Options

Period * : Last Full Month

EventType : All User Authentication

Field Settings

Standard Fields : User<br>Email Address<br>IP Address<br>Event Log Time

4. Choose the report output format from the **Generate Report As** choices. Not all options are available for all reports.
   - **Interactive Report**: creates a web-based report displayed in the web browser. You can choose to save the report as a PDF or CSV file after you view it in interactive mode. If you cannot see all the fields in the Interactive Report window, you can resize each column of data or the entire window by dragging and resizing with the mouse.
   - **CSV Report**: creates a CSV (comma separated values) version of the file. You have the option of saving the CSV report template on the **My Reports** tab. You can download the CSV report and open it with any spreadsheet program that handles CSV files. You can also use the Report Notification Editor to send a generated CSV report to recipients. See Set Notification Options.
   - **PDF Report**: creates a PDF version of the file. You have the option of saving the PDF report template as a report on the **My Reports** tab. You can download the PDF report and open it with Adobe Acrobat Reader. You can also use the **Report Notification Editor** to send a generated PDF report to recipients. See Set Notification Options.

- **Preview Report**: displays a subset of data in the web browser. It does not display the full data set. For full reports, you must save as PDF or CSV and view the saved report.

NOTE:

- When you generate a report as PDF or CSV, or when you save an interactive report, the report appears in the **Pending and Completed Reports** section at the bottom of the **Report Lists** page. See Pending and Completed Reports .
- The **Advanced Options** section is grayed out until after you have copied a report configuration to **My Reports**. See Report Lists - My Reports for information on saved reports.
- If you are planning to save a customized report to run on a recurring schedule, set the **Filter Options** and **Field Settings** options first, copy the report to **My Reports**, and then set the **Advanced Options**. See Configure and Save Custom Reports for instructions.

5. Under the **Filter Options** section, the report results can be narrowed by setting options that are unique for each report. See the specific report detail section for information on available fields and search criteria.
   - If you provide no specific search criteria, the search returns all information available for your current team context.
   - Many reports allow defining the report time **Period**. See Define a Report Time Period for definitions of the data returned.
   - Many reports allow access to the **Criteria Editor**. See Using the Criteria Editor.
6. Under **Field Settings** is a list of all the `Custom Fields` and `Standard Fields` available for this report. The listed fields vary for each report. See the specific report detail section for information on fields available. Select which fields are to be included in the report. All fields are preselected, which is shown as the field names being displayed with a blue background. To unselect a field, click it and the backgrounds turns white. To reselect it, click it a second time.
7. To run this report with the options selected, click **Run Report**. AlertFind generates the report.
   - If *Interactive* or *Preview* report are selected, the report is displayed in a new window.
   - On the **View Report** page, click **Edit** to change the report parameters and run it again. You can also click **Save as PDF** or **Save as CSV** to save the report.
   - If *PDF* or *CSV* output is selected, the report will be run in the background. See Pending and Completed Reports.
8. To save this report configuration as a custom report under the **My Reports** tab, click **Copy to My Reports**. This will make the additional fields available

such as a *Report Title* to label the saved report. See Configure and Save Custom Reports for instructions.

### Define a Report Time Period

#### NOTE

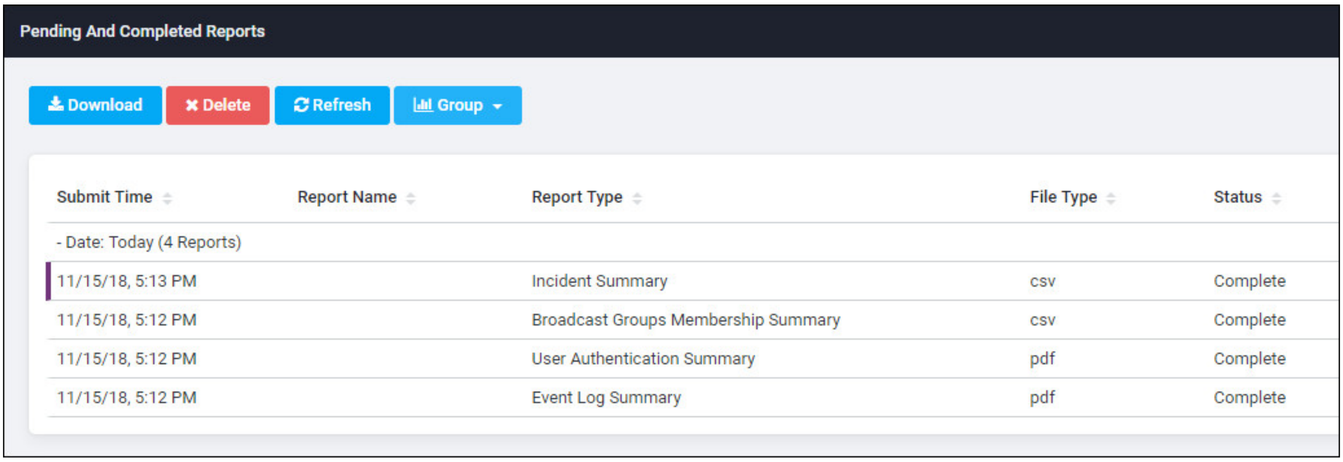
All reports have a Time Zone automatically included in the time Period.

Under the **Filter Options** section, many reports allow the report results set to be narrowed by defining the report time **Period**.

1. **Today**–Returns entries from midnight today up to time the report is run. This is always a partial day report. If the report is run at 2:37PM (14:37), it will cover the hours from 0:00 to 14:37.
2. **Yesterday**–Returns the full 24-hour report for yesterday, starting at midnight yesterday and ending at midnight today. If the report is run on November 29, the report will contain all of the information from YYYY-11-28 0:00 to YYYY-11-29 0:00.
3. **Last Full Hour**–Returns the report for the last completed full hour. If the report is run at 2:37PM (14:37), it contains data from 1:00-2:00PM (13:00 to 14:00).
4. **Last Full Week**–Returns the report for the last completed full week, from midnight on Sunday of the previous week up to midnight last Sunday. If the report is run on Wednesday, November-29, it will contain information from midnight on Sunday, November-19 (YYYY-11-19 0:00) up to midnight on Saturday, November 25 (YYYY-11-25 0:00).
5. **Last Full Month**–Returns the report for the last completed full month, from the first day of the previous month to the first day of the current month. If the report is run on November 29, it will contain information from midnight on October 1 (YYYY-10-01 0:00) up to midnight on November 1 (YYYY-11-01 0:00).
6. **Last Full Year**–Returns the report for the last completed full year, from the first day of the previous year to the first day of the current year. If the report is run on November 29, 2010, it will contain information from midnight on January 1, 2009 (2009-01-01 0:00) up to midnight on January 1, 2010 (2010-01-01 0:00).
7. **Last 12 Full Months**–Returns the last twelve complete months of data. If the report is run on November 29, 2010, it will contain information from midnight on November 1, 2009 (2009-11-01 0:00) up to midnight on November 1, 2010 (2010-11-01 00:00).
8. **Specific Dates**–Returns the report from the `Start Date` date and time up to the `End Date` date and time. Use the calendar icons to set the start and end dates, and the drop-down menu to select the times.

### Pending and Completed Reports

All PDF and CSV reports are run in the background so you can continue to perform AlertFind functions while the reports are processing. After a PDF or CSV report has been initiated, it is added to the **Pending and Completed Reports** pane. Also, all PDF or CSV reports initiated from the **My Reports** tab are listed in this pane.



| Submit Time | Report Name | Report Type | File Type | Status |
|---|---|---|---|---|
| - Date: Today (4 Reports) | | | | |
| 11/15/18, 5:13 PM | | Incident Summary | csv | Complete |
| 11/15/18, 5:12 PM | | Broadcast Groups Membership Summary | csv | Complete |
| 11/15/18, 5:12 PM | | User Authentication Summary | pdf | Complete |
| 11/15/18, 5:12 PM | | Event Log Summary | pdf | Complete |

When the report has finished processing, the *Status* changes from `Pending` to `Completed`. The Status refreshes automatically, but if you want to check the report's status before the page refreshes, click the **Refresh** button.

To open or download a report, either click once on the report's table row to select the report and then click the **Download** button, or just double-click the report's row. If multiple reports are selected, only the first report is downloaded.

All PDF and CSV reports are retained in case you want to view them at a later date. When you view a report listed in the Pending and Completed reports table, you are viewing a saved report, *not* regenerating the report. Each report contains the date it was generated.

To remove a report from the list, select the report and then click the **Delete** button. You can select a range of reports to delete using the SHIFT key or several reports using the CTRL key.

## Audit Trails Reports

The Audit Trails section contains the following two reports:

### Event Log Summary Report

The *Event Log Summary* report provides a detailed view of the audit logs of changes (such as to Devices, Groups, etc.) by Administrators, Team Leaders and Users.

The following **Generate Report As** options are available:

- Interactive Report
- PDF Report

- CSV Report (MS Excel)

The following **Filter Options** are available:

- **Period**: This filter sets the time period for the report. The default value is `Last Full Month`. For descriptions of the time period options, see Define a Report Time Period.
- **Event Type**: This field sets the specific Event Type to be reported. The default value is `All Events`, any other choice in the drop-down list reports only that one specific Event Type. The following Event Types are available:
  - Broadcast Group: Created, Removed, Members Added, or Members Removed
  - Escalation Group: Created, Removed, Members Added, or Members Removed
  - Smart Group: Created, Removed, or Criteria Changed
  - User Role Updated
  - Notification Template: Created, Removed, or Changed
  - User: Created, Removed, Enabled, or Disabled
  - User Device: Created, Deleted, Enabled, or Disabled
  - Password Policy Update
- In the **Field Settings** section, the following standard report fields are available:
  - User: User who performed the event.
  - Email Address: Email address of the user who preformed the event.
  - IP Address: IP address of the user who performed the event.
  - Event Log Time: Time the event was performed.
  - Event Type: A description of the event type.
  - Description: A description of the event performed, such as the email address of the user disabled, the name of the group to which members were added, or the name of a disabled device and owner’s email address.

### User Authentication Summary Report

The *User Authentication Summary* report provides a detailed view of the audit logs of user sign-in and sign-out behavior.

The following **Generate Report As** options are available:

- Interactive Report
- PDF Report
- CSV Report (MS Excel)

The following **Filter Options** are available:

- Period: This filter sets the time period for the report. The default value is `Last Full Month`. For descriptions of the time period options, see Define a Report Time Period.
- Event Type: This field sets the specific Event Type to be reported. The default value is `All User Authentication`, any other choice in the drop-down list reports only that one specific Event Type of user `Sign in` or `Sign out` events.

In the **Field Settings** section, the following standard report fields are available:

- User: User who signed in or out.
- Email Address: Email address of the user.
- IP Address: IP address of the user.
- Event Log Time: Time the user signed in or out.
- Event Type: A description of the event type.
- Description: The name of the user who signed in or out.

## Group Reports

You can create the following types of group reports:

### Broadcast Groups Membership Summary Report

The *Broadcast Groups Membership Summary* report provides a summary of a membership of selected or all broadcast groups, including broadcast group, name and type information.

The following **Generate Report As** options are available:

- Interactive Report
- CSV Report (MS Excel)

The following **Filter Options** are available:

- Group Filter Option: This filter displays the criteria editor to limit the list of groups to those who meet the selected criteria. To include all groups, leave the field blank. For information on how to use the criteria editor, see Using the Criteria Editor.

In the **Field Settings** section, the following standard report fields are available:

- Broadcast Group: The name of the broadcast group.
- Name: The name of the group.
- Type: The type of the membership.

### Broadcast Group Summary Report

The *Broadcast Group Summary* report provides a summary of all broadcast groups, including group description, team, and quick launch ID information.

The following **Generate Report As** options are available:

- Interactive Report
- CSV Report (MS Excel)

The following **Filter Options** are available:

- Group Filter Option: This filter displays the criteria editor to limit the list of groups to those who meet the selected criteria. To include all groups, leave the field blank. For information on how to use the criteria editor, see Using the Criteria Editor.

In the **Field Settings** section, the following standard report fields are available:

- Name: The name of the group.
- Description: The group’s description field.
- Team: The team context the group belongs to.
- Quick Launch ID: The group’s quick launch ID number.
- Status: Whether the group is enabled or disabled.

### Smart Group Summary Report

The *Smart Group Summary* report provides a summary of all smart groups, including group description, team, criteria, and quick launch ID information.

The following **Generate Report As** options are available:

- Interactive Report
- CSV Report (MS Excel)

The following **Filter Options** are available:

- Group Filter Option: This filter displays the criteria editor to limit the list of groups to those who meet the selected criteria. To include all groups, leave the field blank. For information on how to use the criteria editor, see Using the Criteria Editor.

In the **Field Settings** section, the following standard report fields are available:

- Name: The name of the group.
- Description: The group’s description field.
- Team: The team context the group belongs to.
- Criteria: The criteria selected.
- Quick Launch ID: The group’s quick launch ID number.

### Escalation Group Membership Summary Report

The *Escalation Group Membership Summary* report provides a summary of membership of selected or all escalation groups, including user name, type and delay information.

The following **Generate Report As** options are available:

- Interactive Report
- CSV Report (MS Excel)

The following **Filter Options** are available:

- Group Filter Option: This filter displays the criteria editor to limit the list of groups to those who meet the selected criteria. To include all groups, leave the field blank. For information on how to use the criteria editor, see Using the Criteria Editor.

In the **Field Settings** section, the following standard report fields are available:

- Escalation Group: The Escalation group name.
- Name: The name of the group.
- Team: The team context the group belongs to.
- Type: The membership type.

### Escalation Group Summary Report

The *Escalation Group Summary* report provides a summary of all escalation groups, including group description, team, and quick launch ID information.

The following **Generate Report As** options are available:

- Interactive Report
- CSV Report (MS Excel)

The following **Filter Options** are available:

- Group Filter Option: This filter displays the criteria editor to limit the list of groups to those who meet the selected criteria. To include all groups, leave the field blank. For information on how to use the criteria editor, see Using the Criteria Editor.

In the **Field Settings** section, the following standard report fields are available:

- Name: The name of the group.
- Description: The group’s description field.
- Team: The team context the group belongs to.
- Quick Launch ID: The group’s quick launch ID number.
- Status: Whether the group is enabled or disabled.

## Hotline Reports

The available Hotline reports will depend on the features that have been enabled for your organization. The following four reports are available if all Hotline features are enabled:

### Hotline Pro Call Details Report

The *Hotline Pro Call Details* report provides a detailed view of the data collected from callers during Hotline calls.

The following **Generate Report As** options are available:

- Interactive Report
- PDF Report
- CSV Report (MS Excel)

The following **Filter Options** are available:

- Hotline Name: Limits the report results to a subset of Hotlines. Enter all or part of a Hotline name. Only Hotlines whose names match the criteria you enter in this field will appear in the report. To show results for all Hotlines, leave this field blank.
- Period: This filter sets the time period for the report. The default value is `Last Full Month`. For descriptions of the time period options, see Define a Report Time Period.
- Edit Criteria: Limits the report results by the User information, such as user name or description. See Using the Criteria Editor for more information on using the Criteria Editor.

In the **Field Settings** section, all custom fields are listed along with the following standard report fields:

- Hotline Name
- User Name, if captured during the call
- Call ID
- Call Start Time
- Action Time: The time when the data was captured during the call
- Call Data Name: The field name captured during the call, as defined by the person who created the Hotline.
- Call Data Value: The field value captured during the call, as defined by the person who created the Hotline.

#### NOTE

For more information on how to gather information from Hotline calls using **Call Data Name** and **Call Data Value** fields, see Gathering Data From Hotline Pro Calls.

### Hotline Poll Details Report

The *Hotline Poll Details* report provides response details for Hotline polls during a specified period.

The following **Generate Report As** options are available:

- Interactive Report
- PDF Report
- CSV Report (MS Excel)

The following **Filter Options** are available:

- Period: This filter sets the time period for the report. The default value is `Last Full Month`. For descriptions of the time period options, see Define a Report Time Period.
- Poll Name: Limits the report results to a subset of polls. Enter all or part of a poll name. Only polls whose names match the criteria you enter in this field will appear in the report.
- Edit Criteria: Limits the report results by the User information, such as user name or description. See Using the Criteria Editor for more information on using the Criteria Editor.

In the **Field Settings** section, all custom fields are listed along with the following standard report fields:

- Hotline Name
- Poll Name
- User Name
- Time
- Response
- Extra Data

### Hotline Poll Non-Responders Report

The *Hotline Poll Non-Responders* report information for users who did not respond to Hotline polls during the specified period.

The following **Generate Report As** options are available:

- Interactive Report
- PDF Report
- CSV Report (MS Excel)

The following **Filter Options** are available:

- **Period**: This filter sets the time period for the report. The default value is `Last Full Month`. For descriptions of the time period options, see Define a Report Time Period.
- **Poll Name**: Limits the report results to a subset of polls. Enter all or part of a poll name. Only polls whose names match the criteria you enter in this field will appear in the report.

- **Edit Criteria**: Limits the report results by the User information, such as user name or description. See Using the Criteria Editor for more information on using the Criteria Editor.

In the **Field Settings** section, all custom fields are listed along with the following standard report fields:

- Name: the name of the users who have not responded to the poll.

### Hotline Summary Report

The *Hotline Summary* report shows a summary of all your active Hotlines.

The following **Generate Report As** options are available:

- Interactive Report
- PDF Report
- CSV Report (MS Excel)

There are no **Filter Options** available for this report

In the **Field Settings** section, the following standard report fields are listed:

- Number: The hotline number.
- Hotline: The name of the hotline.
- Team: The team the hotline belongs to.
- Last Edited: The time the hotline was last edited.
- Last Edited By: The user who last edited the hotline.

## Incident Reports

Only one Incident summary report can be created.

### Incident Summary Report

The *Incident Summary Report* is a summary view of all incidents, including incident description, opening and closing information.

The following **Generate Report As** options are available:

- Interactive Report
- CSV Report (MS Excel)

The following **Filter Options** are available:

- Incident Filter Options: Limits the report results by the following fields:
  - Closed Date
  - Incident Description
  - Opened Date
  - Incident Title

See Using the Criteria Editor for more information on using the Criteria Editor.

In the **Field Settings** section, all custom fields are listed along with the following standard report fields:

- Title: the title of the Incident.
- Description: the Incident's description.
- Opener: the user who opened the Incident.
- Opened Date
- Closer: the user who closed the Incident.
- Closed Date

## Notification Reports

You can create the following types of Notification reports:

### Notification Response Details Report

The *Notification Response Details* displays the possible responses for a set of notifications, including the recipients and their selected response.

The following **Generate Report As** options are available:

- Interactive Report
- PDF Report
- CSV Report (MS Excel)

The following **Filter Options** are available:

- Period: This filter sets the time period for the report. The default value is `Last Full Month`. For descriptions of the time period options, see Define a Report Time Period.
- Notification Criteria: opens the Criteria Editor to narrow the report by selecting one of the following notification fields:
  - Priority
  - Received by
  - Response abbreviation
  - Sent by
  - Sent time
  - Subject
- Edit Criteria: Limits the report results by the User information, such as user name or description.

  See Using the Criteria Editor for more information on using the Criteria Editor.

In the **Field Settings** section, the following standard report fields are available:

- Sent Time: Date and time Notification was sent.
- Subject: Subject of the Notification.
- Team: The team originating the notification.
- Incident Name: Incident name, if applicable.
- Sender: The name of the user who sent the Notification.
- Recipient Name: The name of the user who received the Notification.
- Possible Response: This column combined with the next column state whether or not the user responded to the Notification.
- Device Name: The name of the device.
- Device Address: The address of the device.
- First Confirmed Time: The time at which the first confirmation is received.
- Last Confirmed Time: The time at which the last confirmation is received.
- First Confirmed Elapsed Time: The elapsed time since the first confirmation was received.

### Scheduled Notification Detail Report

The *Scheduled Notification Detail* displays a detailed view of scheduled notifications with a record for each recipient (user or group).

The following **Generate Report As** options are available:

- CSV Report (MS Excel)

The following **Filter Options** are available:

- Notification Criteria: opens the Criteria Editor to narrow the report by selecting one of the following notification fields:
  - Priority
  - Received by
  - Response abbreviation
  - Sent by
  - Sent time
  - Subject

See Using the Criteria Editor for more information on using the Criteria Editor.

In the **Field Settings** section, the following standard report fields are available:

- Team: The team originating the notification.
- Incident Name: The name of the incident.
- Sender: The name of the user who sent the Notification.
- Subject: Subject of the Notification.

- Message: The message included in the Notification.
- Recurrence: The pattern of the recurrence of the Notification.
- Expiration: The expiry date of the Notification.
- Priority: The priority of the Notification.
- Authenticated: Identifies whether the notification is authenticated or not.
- Hotline: Specifies the hotline number to be used.
- Attachments: Files to be attached to the Notification.
- Email Results: Specifies the email status.
- Current Status: Status of the Notification.
- Recipient Name: The name of the recipient.
- Recipient Type: The type of the recipient (user, team or group).
- Description: Description of the Notification.

### Sent Notification Detail + Recipient Custom Fields Report

The *Sent Notification Detail + Recipient Custom Fields* displays a list of all recipients of all sent notifications along with their responses, including recipient custom fields.

The following **Generate Report As** options are available:

- CSV Report (MS Excel)

The following **Filter Options** are available:

- Notification Criteria: Opens the Criteria Editor to narrow the report by selecting one of the following notification fields. It already has two Sent Time criteria set by default that cannot be deleted:
  - Priority
  - Received by
  - Response abbreviation
  - Sent by
  - Sent time
  - Subject

See Using the Criteria Editor for more information on using the Criteria Editor.

In the **Field Settings** section, the following standard report fields are available:

- Sent Time: The time at which the Notification was sent.
- Sender: The name of the user who sent the Notification.
- Subject: Subject of the Notification.
- Team: The team originating the notification.

- Incident Name: The name of the incident.
- Current Status: Status of the Notification.
- Recipient Name: The name of the recipient.
- Response: Specifies whether the response was received or not.
- Last Notification Result Log Event: A log of events.
- Last Confirmed Device Name: The device name from where the last confirmation is received.
- Last Confirmed Device Address: The device address from where the last confirmation is received.

### Sent Notification Summary Report

The *Sent Notification Summary* report shows all notifications sent during a specified time frame for your current team context. From this summary report, you can select a specific notification to see the *Notification Response Details* report for that Notification, which provides an overview so that you can evaluate its effectiveness.

The following **Generate Report As** options are available:

- Interactive Report
- PDF Report
- CSV Report (MS Excel)

The following **Filter Options** are available:

- Period: This filter sets the time period for the report. The default value is `Last Full Month`. For descriptions of the time period options, see Define a Report Time Period.
- Notification Criteria: opens the Criteria Editor to narrow the report by selecting one of the following notification fields:
    - Priority
    - Received by
    - Response abbreviation
    - Sent by
    - Sent time
    - Subject

See Using the Criteria Editor for more information on using the Criteria Editor.

Under **Field Settings**, the following standard report fields are listed:

- Sent Time
- Subject
- Team

- Incident Name
- Canceled
- Sender
- Total Recipients
- Recipients Responded

From the Sent Notification Summary report, click the **Subject** of the notification for which you want to view details. The Notification Response Details report appears for the notification selected.

## Team Reports

You can create the following team reports:

### Team Leadership Report

The *Team Leadership* report provides a list of team leaders and their permissions on the specified team.

The following **Generate Report As** option is available:

- CSV Report (MS Excel)

In **Filter Options**, you just have the option to provide a team name.

In the **Field Settings** section, the following standard report fields are available:

- Team Leader Name: The name of the team leader.
- Team Name: The name of the team.
- The status (enabled or disabled) of the all the team permissions (SN, VR, CN, MI, OI, VI, MT, MG, MU, VP, MP, MA, SP, MH, and VW) are listed

### Team Membership Report

The *Team Membership* report provides a list of sub-teams and members of a specified team.

The following **Generate Report As** option is available:

- CSV Report (MS Excel)

In **Filter Options**, you just have the option to provide a team name.

In the **Field Settings** section, the following standard report fields are available:

- Team Name: The name of the team.
- Parent Team: The name of the parent team.
- Member Name: The name of the team member.
- Member Type: The type of member (user or group)
- Data Source: The source of the data (created in the UI or imported).

### Team Summary Report

The *Team Summary* report shows a summary of all the teams for your organization and their hierarchy.

The following **Generate Report As** options are available:

- Preview Report: This interactive preview report displays Team information for the Global team and the first *two* levels of sub-teams beneath the Global team. To see a report listing all teams generate a PDF or CSV report.
- PDF Report
- CSV Report (MS Excel)

This report does not have any **Filter Options** or **Field Settings**.

The Team Summary report contains the following fields:

- Name: The name of the Team.
- Description: The Team’s description.
- Source: The column displays whether the Team was imported or manually created.
- User Members: Number of users that are members of the Team.

## Usage Reports

You can create the following three types of Usage reports:

### Usage Summary Report

The *Usage Summary* report gives an estimate of system usage. All call durations are rounded up to the nearest minute.

The following **Generate Report As** options are available:

- Interactive Report
- CSV Report (MS Excel)
- PDF Report

The following **Filter Options** are available:

- Period: This filter sets the time period for the report. The default value is `Last Full Month`. For descriptions of the time period options, see Define a Report Time Period.

In the **Field Settings** section, the following standard report fields are available:

- User Count: The number of users.
- Outbound Minutes: The total duration of voice phone calls sent from AlertFind Notifications to users. All call durations are rounded up to the nearest minute.

- Outbound Calls: The count of voice phone calls sent from AlertFind Notifications to users.
- Inbound Minutes: The total duration of voice phone calls from users to Hotlines. All call durations are rounded up to the nearest minute.
- Inbound Calls: The count of voice phone calls from users to Hotlines.
- Total Minutes Used: The accumulated duration of Inbound and Outbound minutes.
- Total Call Count: The accumulated count of Inbound and Outbound calls.
- Conference Minutes: The total duration of phone calls transferred to conference calls. All call durations are rounded up to the nearest minute.
- Conference Calls: The count of phone calls transferred to conference calls.
- Emails: The count of emails sent by AlertFind Notifications, includes messages sent to devices defined as SMTP handsets.
- Pages: The count of pager messages sent by AlertFind Notifications.
- SMS Messages: The count of SMS (text) messages sent by AlertFind Notifications.
- Faxes: The count of faxes sent by AlertFind Notifications.
- Total Activations: The count of Notifications sent. If a Notification is sent to more than one user, that will be counted as one activation.

### Team Usage Summary Report

The *Team Usage Details* report gives an estimate of AlertFind system usage broken down per team.

The following **Generate Report As** options are available:

- Interactive Report
- CSV Report (MS Excel)
- PDF Report

The following **Filter Options** are available:

- Period: This filter sets the time period for the report. The default value is `Last Full Month`. For descriptions of the time period options, see Define a Report Time Period.

In the **Field Settings** section, the following standard report fields are available:

- Team Name: The name of the team.
- All User Count: Number of users (enabled and disabled) in the team.
- Enabled User Count: Number of enabled users in the team.
- Outbound Minutes: Total duration for all outbound phone notifications sent by AlertFind to the users of the team, in minutes.

- Outbound Calls: Total number of outbound phone calls sent from AlertFind to users of the team.
- Inbound Minutes: Total duration of all IVR phone calls sent by the users of the team to AlertFind.
- Inbound Calls: Total number of IVR phone calls sent by the team members to AlertFind system.
- Total Minutes Used: Total duration of outbound and IVR phone calls of the team, in minutes.
- Total Call Count: Total number of outbound and inbound phone calls of the team.
- Conference Minutes: Total time, in minutes, of all conference calls ran by the team.
- Conference Calls: Total number of conference calls started by the team.
- Emails: Total number of emails sent by the team.
- Pages: Total number of pages sent by the team.
- Faxes: Total number of faxes sent by the team.
- SMS Messages: Total number of text messages sent by the team.
- Total Activations: Number of messages (a message may be sent to one or more recipients, but it's only counted once) sent by the team.

## Usage Details Reports

You can create the following types of Usage Details reports:

### Usage Conference Calls Details

The *Usage Conference Calls Details* report provides a summary of your conference calls use.

The following **Generate Report As** options are available:

- Interactive Report
- CSV Report (MS Excel)
- PDF Report

The following **Filter Options** are available:

- Period: This filter sets the time period for the report. The default value is `Last Full Month`. For descriptions of the time period options, see Define a Report Time Period.

In the **Field Settings** section, the following standard report fields are available:

- Call Start: The time at which the conference call was initiated.
- Call End: The time at which the conference call ended.

- Minutes: Duration of the conference call in minutes
- Sender: The sender's name who initiated the call.
- Recipient: The recipient's name to whom the call is made.
- Subject: The subject of the call.
- Phone Number: The phone number that is used to make the call.
- Conference Start Date: The start date of the conference.
- Conference End Date: The end date of the conference.
- Conference Minutes: Duration of the conference.
- Conference Phone Number: The phone number to which the conference is associated with.
- Notification ID: The notification ID.

### Usage Outbound Calls Details

The *Usage Outbound Calls Details* report provides a summary of your outbound calls use.

The following **Generate Report As** options are available:

- Interactive Report
- CSV Report (MS Excel)
- PDF Report

The following **Filter Options** are available:

- Period: This filter sets the time period for the report. The default value is `Last Full Month`. For descriptions of the time period options, see Define a Report Time Period.

In the **Field Settings** section, the following standard report fields are available:

- Call Start: The time at which the conference call was initiated.
- Call End: The time at which the conference call ended.
- Minutes: Duration of the conference call in minutes
- Sender: The sender's name who initiated the call.
- Recipient: The recipient's name to whom the call is made.
- Subject: The subject of the call.
- Phone Number: The phone number that is used to make the call.
- Notification ID: The notification ID.

### Usage Email Notifications Details

The *Usage Email Notifications Details* report provides a summary of your email notifications use.

The following **Generate Report As** options are available:

- Interactive Report
- CSV Report (MS Excel)
- PDF Report

The following **Filter Options** are available:

- Period: This filter sets the time period for the report. The default value is `Last Full Month`. For descriptions of the time period options, see Define a Report Time Period.

In the **Field Settings** section, the following standard report fields are available:

- Sent Time: The time at which the email notification is sent.
- Sender: The sender's name who sent the email notification.
- Recipient: The recipient's name to whom the notification is sent.
- Email: The email ID used for sending the notification.
- Subject: The subject of the notification.
- Notification ID: The notification ID.

### Usage Fax Notifications Details

The *Usage Fax Notifications Details* report provides a summary of your fax notifications use.

The following **Generate Report As** options are available:

- Interactive Report
- CSV Report (MS Excel)
- PDF Report

The following **Filter Options** are available:

- Period: This filter sets the time period for the report. The default value is `Last Full Month`. For descriptions of the time period options, see Define a Report Time Period.

In the **Field Settings** section, the following standard report fields are available:

- Sent Time: The time at which the fax notification is sent.
- Sender: The sender's name who sent the fax.
- Recipient: The recipient's name to whom the fax is sent.
- Fax Number: The fax number used for sending the notification.
- Subject: The subject of the fax notification.
- Notification ID: The notification ID.

### Usage Pager Notifications Details

The *Usage Pager Notifications Details* report provides a summary of your pager notifications use.

The following **Generate Report As** options are available:

- Interactive Report
- CSV Report (MS Excel)
- PDF Report

The following **Filter Options** are available:

- Period: This filter sets the time period for the report. The default value is `Last Full Month`. For descriptions of the time period options, see Define a Report Time Period.

In the **Field Settings** section, the following standard report fields are available:

- Sent Time: The time at which the pager notification is sent.
- Sender: The sender's name who sent the pager notification.
- Recipient: The recipient's name to whom the pager notification is sent.
- Pager Number: The pager number used for sending the notification.
- Subject: The subject of the pager notification.
- Notification ID: The notification ID.

### Usage SMS Notifications Details

The *Usage SMS Notifications Details* report provides a summary of your SMS notifications use.

The following **Generate Report As** options are available:

- Interactive Report
- CSV Report (MS Excel)
- PDF Report

The following **Filter Options** are available:

- Period: This filter sets the time period for the report. The default value is `Last Full Month`. For descriptions of the time period options, see Define a Report Time Period.

In the **Field Settings** section, the following standard report fields are available:

- Delivered Time: The time at which the SMS is delivered.
- Sender: The sender's name who sent the SMS.
- Recipient: The recipient's name to whom the SMS notification is sent.
- SMS Number: The phone number used for sending the SMS notification.
- Subject: The subject of the SMS notification.
- Notification ID: The notification ID.

## User Reports

One report is available in the Users section of the Report Lists page.

### User List Report

The *User List Report* report provides data about the users under your current team context. You can narrow the report to include users only for specific roles or custom fields.

The following **Generate Report As** options are available:

- Interactive Report
- CSV Report (MS Excel)

The following **Filter Options** are available:

- User Name: To narrow the report by user name, enter all or part of a user name. Do not use a wild-card character in this field. The report returns all users whose user names contain the search string in any part of their user names (first names or last names). For example, if you enter `lau`, your search will return `Laura` and `Klaus`. If you enter `ab`, your search will return `Abbi` and `Sabrina`.
- Role: To narrow the results by role, enter `User` or `Administrator`.
- Site Name: To narrow the results by Site Name, enter the name of the Site. As the letters are entered, the drop-downs entries change to help auto-complete the Site Name.
- Group Selector: To narrow the results by Group, first select the type of group from the Group Selector drop-down, and then select the Group from the Group Name field.
- Group Name: Once the type of Group as been selected, enter the group name. As the letters are entered, the drop-downs entries change to help auto-complete the Group Name. Group Names are case sensitive.
- Edit Criteria: Limits the report results by the User information, such as user name or description.

See Using the Criteria Editor for more information on using the Criteria Editor.

In the **Field Settings** section, all custom fields are listed along with the following standard report fields:

| | | |
|---|---|---|
| Name | Timezone | Work Email |
| Description | Weekend Days | Work Phone |
| Primary Email Address | Business Hours | Custom Email |
| External Key | Cell Phone | Custom Phone |
| User Name | Fax | Custom Pager |

Data Source
Role
Status
Hotline
Home Phone
Pager
Personal Email
SMS Phone
Custom Fax
Custom SMS Phone

# Report Lists - My Reports

You can run the reports in real time from the **Report Templates** tab, or you can configure and save customized settings for reports that you run frequently, or that you want to schedule to generate on a recurring basis. These customized report settings are then saved for you in the report you have named on the **My Reports** tab. See Configure and Save Custom Reports .

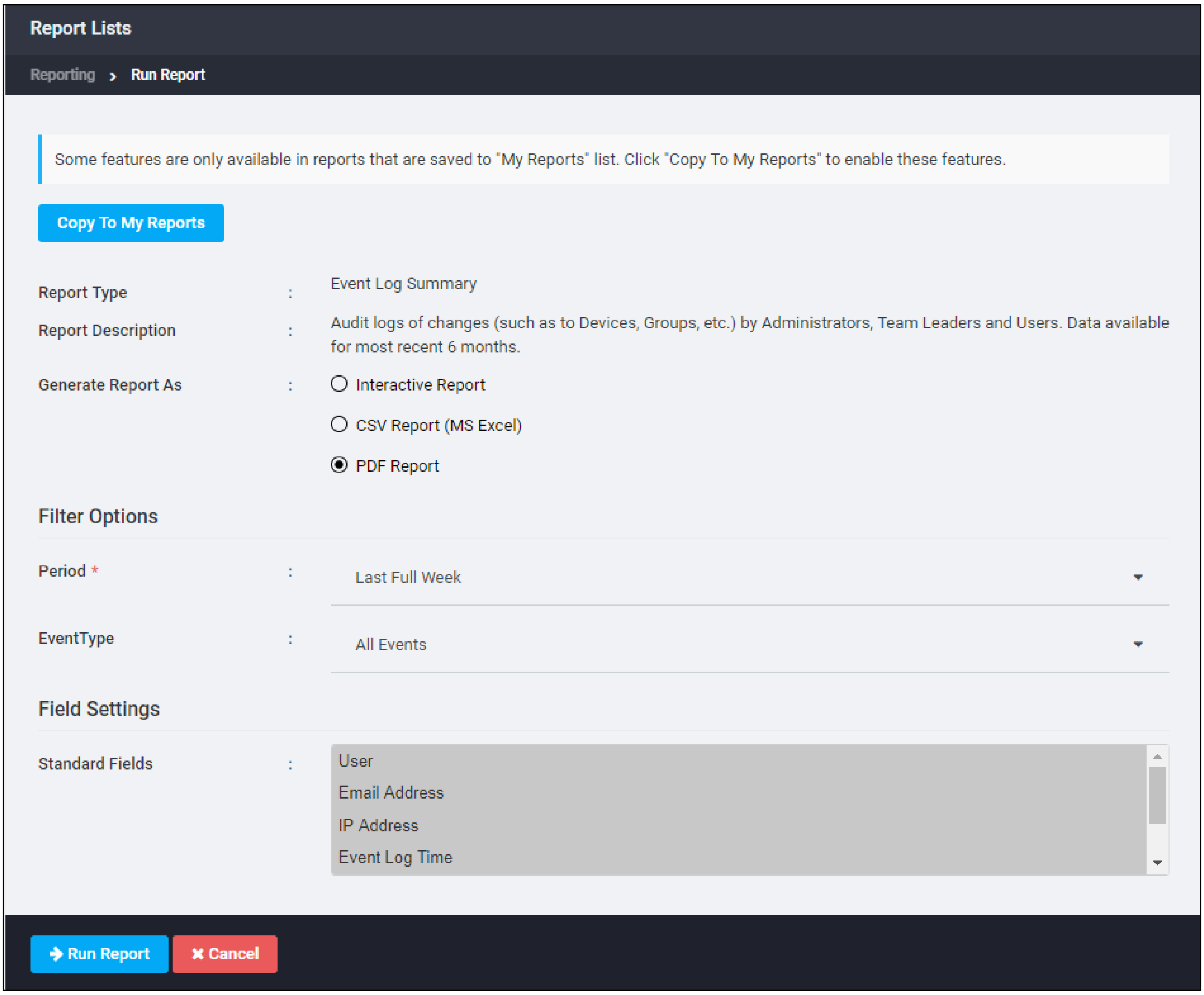
You can also send reports that you run from the **My Reports** tab to recipients by adding notification options to the customized report template. See Set Notification Options.

## Configure and Save Custom Reports

You can configure and save customized settings and options for reports that you run frequently or that you want to schedule to generate on a recurring basis.

To configure a report template and save it to My Reports:

1. From the left navigation menu Reporting section, click **Report Lists**. The available reports appear on the **Report Templates** tab.
2. On the **Report Templates** tab, double-click the report you want to configure and save or click the report and then click the pop-up **Run Report**. button. The **Run Report - Define Report Parameters** window opens.



Some features are only available in reports that are saved to "My Reports" list. Click "Copy To My Reports" to enable these features.

Report Type : Event Log Summary

Report Description : Audit logs of changes (such as to Devices, Groups, etc.) by Administrators, Team Leaders and Users. Data available for most recent 6 months.

Generate Report As : ○ Interactive Report ○ CSV Report (MS Excel) ● PDF Report

Filter Options

Period * : Last Full Week

EventType : All Events

Field Settings

Standard Fields : User, Email Address, IP Address, Event Log Time

3. Use the **Generate Report As** field to set the type of report you want to run (Interactive, PDF, or CSV). If PDF or CSV are chosen, after these report parameters are saved to **My Reports**, the **Advanced Options** pane becomes editable to allow you to set notification or scheduling options.
4. Configure the **Filter options** and the **Field Settings** that available for the type of report you selected. The standard fields in the report are listed under **Field Settings**, All fields are preselected. To delete a field, click it. To undelete it, click it a second time. The standard Field Settings and available Filter Options are unique to each report. See the following sections for descriptions of the report options:
   - Audit Trails (see Audit Trails Reports )
   - Group Reports (see Group Reports )
   - Hotline Reports (see Hotline Reports )
   - Incident Reports (see Incident Reports )
   - Notification Reports (see Notification Reports )
   - Team Reports (see Team Reports )

- Usage Reports (see Usage Report )
- User Reports (see User Reports )

5. When you have configured the basic report parameters, click the **Copy to My Reports** button. Clicking **Copy to My Reports** inserts a **Report Name** field and, depending on settings, may enable editing in the **Advanced Options** pane.
6. Provide a descriptive **Report Name**. The **Report Type** and **Report Description** fields are not editable.
7. *For PDF and CSV reports*, you can set scheduling and notifications parameters under the **Advanced Options** section. Note that scheduling and notification options are not available for interactive reports.

| | |
|---|---|
| Click**Scheduling** | 1. In the **Scheduling** pane, check the **Start Time** check box and use the Calendar menu and time drop-down list to set the date and time when the report should run.<br>2. To schedule a report to run on a recurring basis, select the pattern from the **Recurrence Pattern** list: `Daily`, `Weekly`, `Monthly`, `Annually`, or `Hourly`. Set the desired recurrence pattern.<br>3. When the schedule is set, click the **Save** button. |
| To set notification and escalation options for the saved report | 1. Click **Notification**. See Set Notification Options for instructions.<br>2. Use the **Notification Settings** field to choose whether to always send reports, even if they contain no data, or to never send empty reports. |

8. Verify the **Filter options** and **Field Settings** sections have been to set correctly for the report you want to generate.
9. When all the report options are configured, to save the configuration in **My Reports**, click **Save Report**. The report will run at its next scheduled date. Alternatively, click **Save and Run Report** to save the configuration and run the report immediately.

PDF and CSV reports appear in the **Pending and Completed Reports** pane. See Pending and Completed Reports.

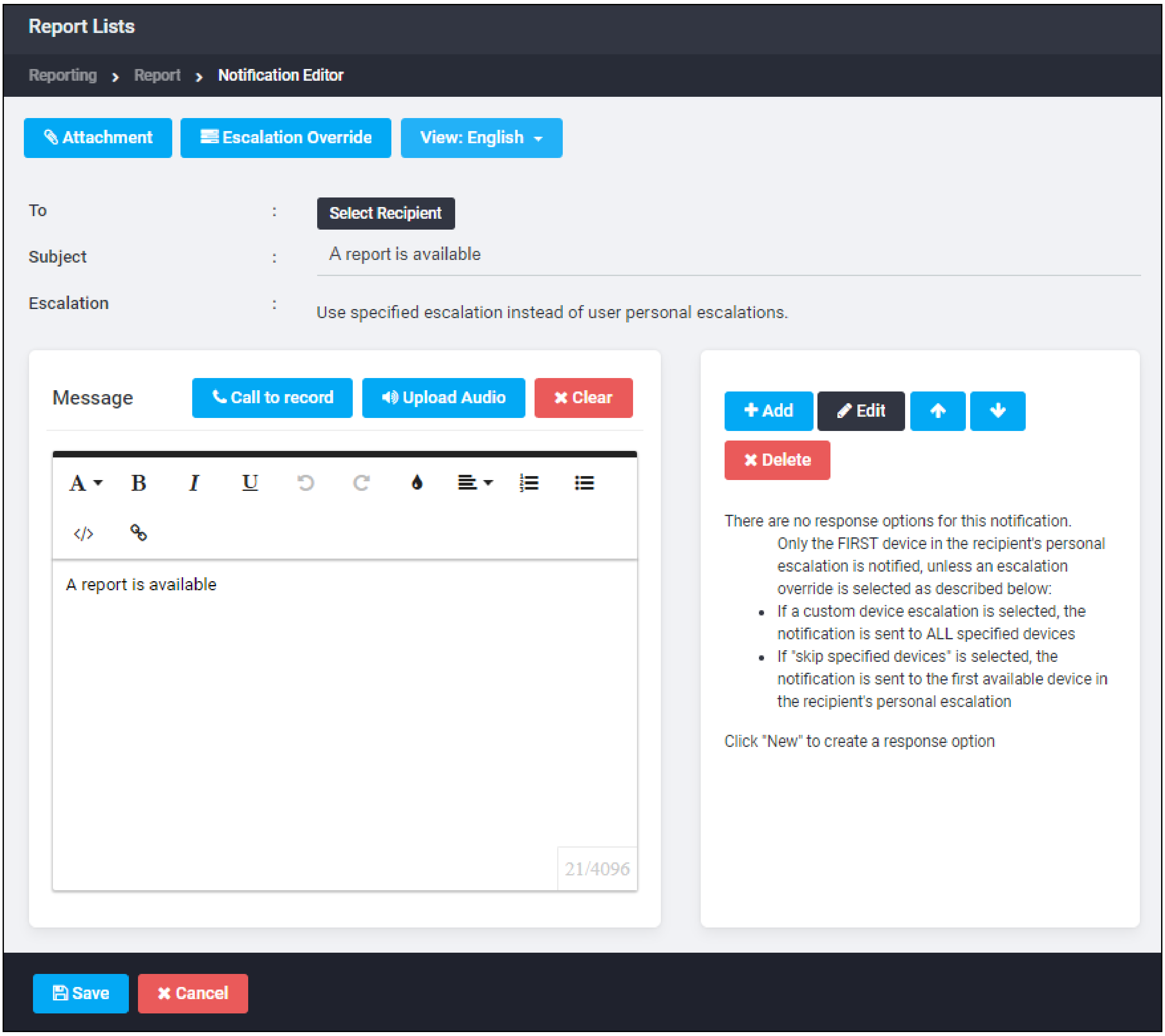
## Set Notification Options

For PDF and CSV reports that you have configured and copied to **My Reports** using the instructions under Configure and Save Custom Reports, you can add notification options using the instructions in this section.

When you add notification options for a saved report, the report can be sent as an email attachment to the recipients you specify after the report runs on its schedule. Notifications are not available for Interactive Reports.

To add notification options to a saved report:

1. From the **Define Report Parameters** page of a report you have already copied to **My Reports**, in the **Advanced Options** section, click **Notification**.



Report Lists

Reporting > Report > Notification Editor

To :

Subject : A report is available

Escalation : Use specified escalation instead of user personal escalations.

Message

A report is available

There are no response options for this notification.

Only the FIRST device in the recipient's personal escalation is notified, unless an escalation override is selected as described below:

- If a custom device escalation is selected, the notification is sent to ALL specified devices
- If "skip specified devices" is selected, the notification is sent to the first available device in the recipient's personal escalation

Click "New" to create a response option

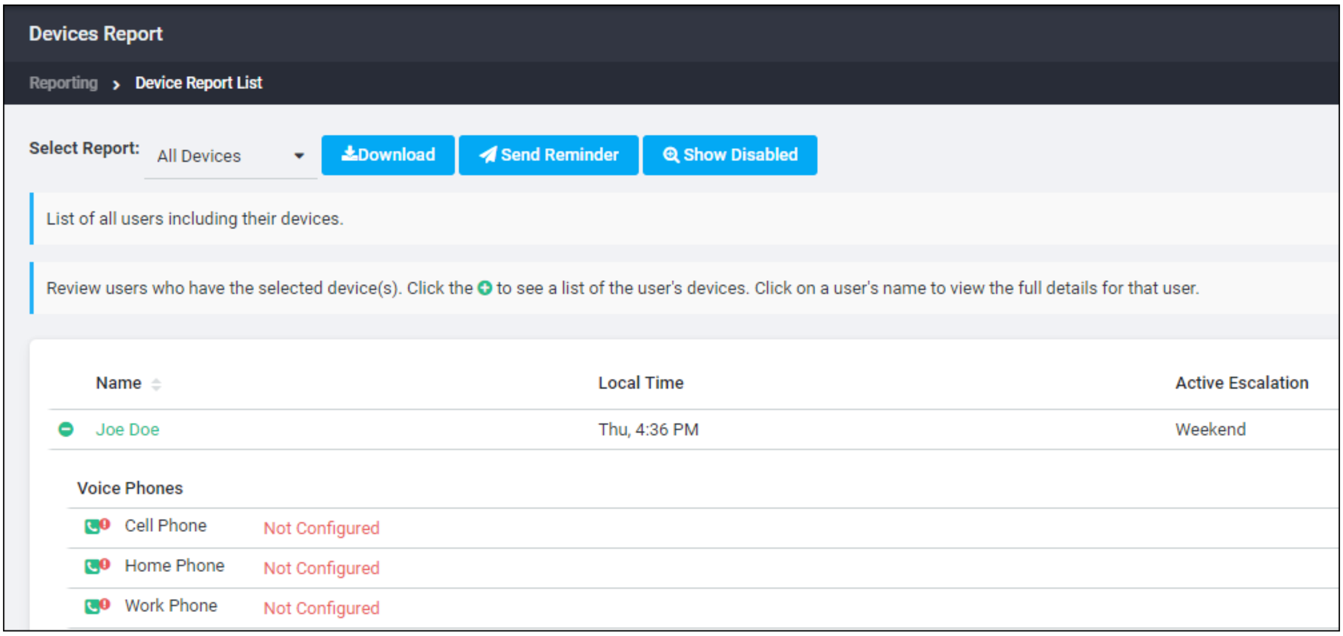
2. To specify recipients who should receive the report every time it is scheduled to run, click **To**. Use the **Recipient Editor** to choose the list of recipients, then click **Save**. See Use the Recipient Editor for more detailed instructions.
3. Provide a descriptive **Subject**. This text will appear as the subject line of the email sent to recipients with the report attached.
4. To set a custom escalation for the notifications that are sent to recipients of this report, click **Escalation Overrider**. See Use the Escalation Editor for more detailed instructions.

5. Use the **Message** section to customize the text of this notification as it will appear in written notifications (email, fax, SMS, pager) and as it is spoken by the TTS engine for phone notifications. You can also use **Call to record** or **Upload Audio** to complete this field.
6. Use the **Responses** section to create the possible responses for the notification. See Use the Response Editor for additional details.
7. When you have configured the notification options for this report, click **Save**. You are returned to the **Define Report Parameters** page.

# Devices Report

To create a device report:

1. In the left navigation menu, under **Reporting**, click **Devices Report**. The list of available reports appears.



Select Report: All Devices

List of all users including their devices.

Review users who have the selected device(s). Click the ⊕ to see a list of the user's devices. Click on a user's name to view the full details for that user.

| Name | Local Time | Active Escalation |
|---|---|---|
| ⊖ Joe Doe | Thu, 4:36 PM | Weekend |

Voice Phones

| | |
|---|---|
| Cell Phone | Not Configured |
| Home Phone | Not Configured |
| Work Phone | Not Configured |

2. The four types of device reports that you can display are:
   - **All Devices Report**–A list of all users and all of their devices.
   - **No Devices Configured Report**–A list of users who have no devices configured in their personal escalation list.
   - **Any Device Configured Report**–A list of users who have at least one device configured in their personal escalation list.
   - **Specific Devices Report**–A list of users who have a specified device configured or not configured, depending on your selection when you run the report. For a **Specific Devices** report, select a type of device from the drop-down list, then select either **configured** or **not configured** from the second drop-down list.

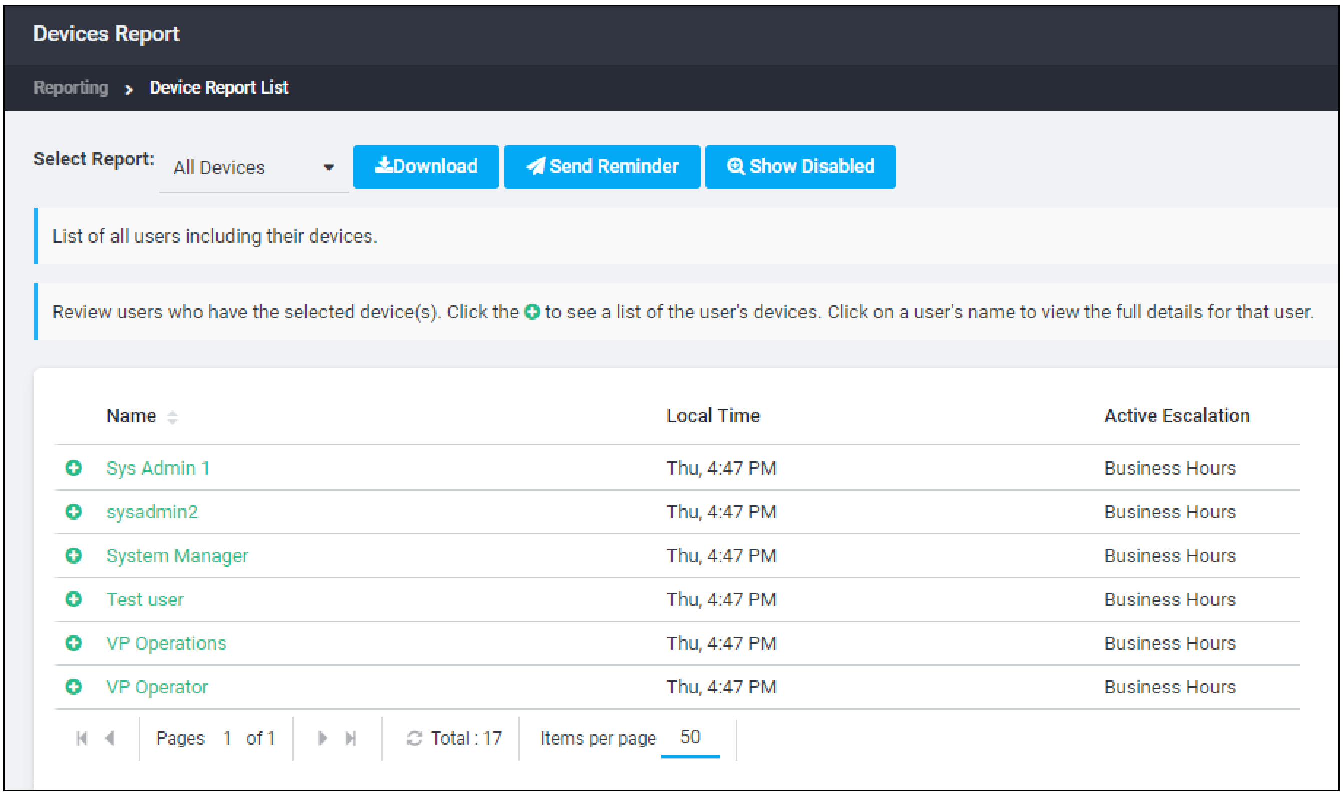
3. Click **Display** next to the type of report you want to generate the report. Report results are displayed in the **Report Results** section of the page. Use the paging commands just above the report table to customize how the report is displayed. Click the plus button, ⊞, to show a list of the user's devices.
4. To download a CSV copy of the report, click **Download**. The standard **File Download** dialog box appears. Choose to **Save** or **Open** the report.
5. To send a reminder, click the **Send Reminder** button. See Send Reminders.
6. To show disabled devices, click the **Show Disabled** button. To hide disabled devices, click the button again, which is now labeled **Hide Disabled**.

## Send Reminders

You can send reminders to users who still need to configure devices.

To send a reminder:

1. Generate the appropriate report. See Devices Report.
2. In the **Report Results** section, click the **Send Reminder** button.



Devices Report

Reporting > Device Report List

Select Report: All Devices

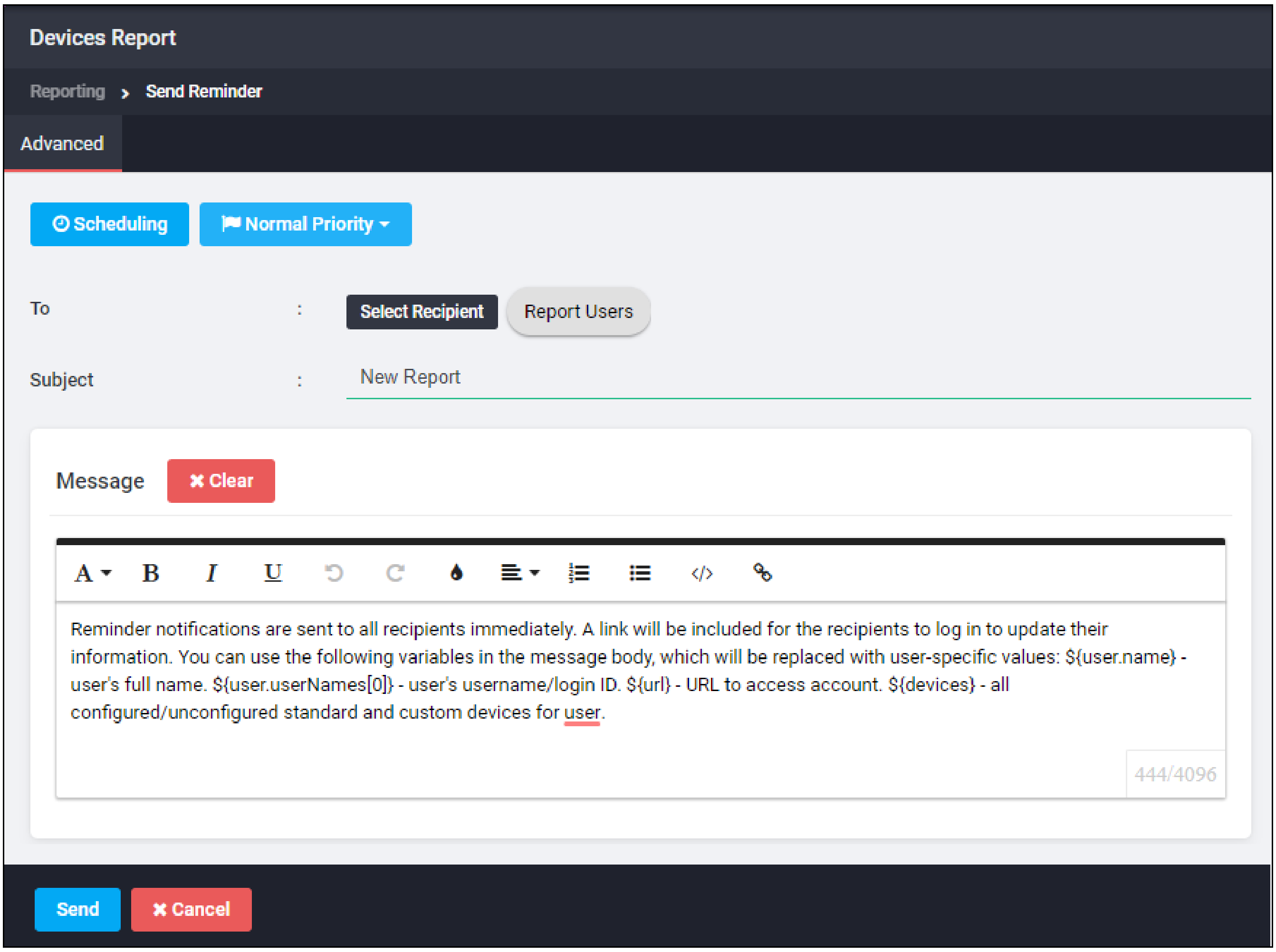
List of all users including their devices.

Review users who have the selected device(s). Click the ⊕ to see a list of the user's devices. Click on a user's name to view the full details for that user.

| | Name | Local Time | Active Escalation |
|---|---|---|---|
| ⊕ | Sys Admin 1 | Thu, 4:47 PM | Business Hours |
| ⊕ | sysadmin2 | Thu, 4:47 PM | Business Hours |
| ⊕ | System Manager | Thu, 4:47 PM | Business Hours |
| ⊕ | Test user | Thu, 4:47 PM | Business Hours |
| ⊕ | VP Operations | Thu, 4:47 PM | Business Hours |
| ⊕ | VP Operator | Thu, 4:47 PM | Business Hours |

Pages 1 of 1 Total : 17 Items per page 50

3. The **Notification Editor** window appears.



To : Report Users

Subject : New Report

Reminder notifications are sent to all recipients immediately. A link will be included for the recipients to log in to update their information. You can use the following variables in the message body, which will be replaced with user-specific values: ${user.name} - user's full name. ${user.userNames[0]} - user's username/login ID. ${url} - URL to access account. ${devices} - all configured/unconfigured standard and custom devices for user.

444/4096

4. By default, the reminder is sent to a dynamically created Ad Hoc Group called `Report Users`. To see or edit the list of users in this ad hoc group, click the **To** button to bring up the Recipient Editor. Double-click the **Report Users** entry in the In the Recipients section of the Recipient Editor to display the users for this report. From this list, you can restrict or add to the list of recipients for the reminder.

## NOTE

Reminders are sent to the user’s email address. Reminders cannot be sent to phone devices.

5. Enter a **Subject** for the reminder. A subject is required. You cannot send a reminder without a subject.
6. Compose the notification as discussed in Compose Notification. You can use the following variables in your message:
   - `${user.name}` – The user’s full name.
   - `${user.userNames[0]}` – User's user name or login ID.
   - `${url}` – Address to access AlertFind.
   - `${devices}` – All configured and unconfigured devices, both standard and custom, for the user.

NOTE

The variable must be typed in the message exactly as they appear above. All variables start with `$` (dollar sign) and be enclosed in`{}` (curly braces).

7. Click **Send** to send the reminder.

### Example of a Message Sent to Users With No Cell Phone Configured

To send a reminder to users who have no cell phone configured, generate a Specific Devices report and select **Cell Phone** is **not configured** using the drop-down fields.

A sample message requesting that users configure their cell phones might look like this:

```
Good morning ${user.name},

You currently have no cell phone defined in AlertFind.
Please follow the link in this email message to log in to
AlertFind and update this information.

${url}
```

# Chapter 6: Glossary

## A

### ad hoc group

A special type of Smart Group created during the composition of a notification. Ad hoc groups are most often used to send follow-up notifications.

### administrator

The AlertFind user role that grants the user the ability to manage company settings, add users, and administer the application for team leader and user accounts.

### Alert Console

The Alert Console is an AlertFind interface that works on any device (desktop, smartphone, or tablet). Use the Alert Console to quickly compose notifications without advanced options, to review and send notifications from notification templates, and to check notification responses, You can go back and forth between the Alert Console interface and the AlertFind desktop interface.

### AnswerOnMedia

A custom conference call provider setting in the Response Editor that enables AlertFind to connect the user to the conference call bridge the moment the initial ring is heard, rather than wait for the bridge to pick up. This means a user will hear the ringing tones once he or she selects the transfer option. Use this feature only when a conference call bridge has a habit of not connecting a call when it picks up the transfer. For more information, see "Create additional responses from the Notification Editor:" on page 108.

### authenticated notification

A notification that requires recipients to identify themselves with a PIN or external key to listen to it or to view it.

## B

### broadcast group

A group composed of users to whom you want to broadcast a message. Broadcast groups can contain other broadcast groups, but cannot contain escalation groups.

## C

### clone

An AlertFind feature that enables you to create multiple notifications with identical information, typically used to create a notification for multiple escalation groups from which you need the first responder for each. Available for notifications within a notification template.

### custom device

A customized device configuration that can be added for an individual user account. After a customized device is added to the user account, it must be included in a personal escalation before it can receive notifications.

### custom escalation

A specific escalation defined by the sender of a notification. If a custom escalation is defined for a notification, it overrides any personal escalations for individual users and the default escalation in effect for the organization.

### custom fields

Organization-specific properties that can be used be used to describe users, such as department, title, or other identifying properties. The custom fields available to your organization are defined by Support during provisioning and are based on fields imported from your system of record.

## D

### default escalation

A standard escalation available to all user accounts. A default escalation is used to deliver a notification when there is no custom escalation defined for a notification and when there is no personal escalation defined for a user.

### device

A phone number, email address, fax number, SMS device, pager, or any other communication method through which AlertFind can contact you. Support provisions your instance of AlertFind with a set of standard devices. Users with necessary permissions can add custom devices for individual user accounts.

### Dictionary

An XML file that contains the phonetic pronunciation of a word that enables AlertFind to pronounce it correctly. You can customize a dictionary file for each language pack your organization has purchased.

## E

### escalation

A set of rules and conditions that determine how a notification is delivered, including which devices are contacted, in what order, and how many minutes can pass before the notification is sent to the next device in the list.

### escalation group

A group that includes escalation information, such as the order in which users should be contacted as well as any delay between attempts to contact them. Escalation groups can contain broadcast groups and other escalation groups.

### external key

A secret number, similar to a PIN, that notification recipients use to authenticate themselves for an authenticated notification. Employee ID numbers or badge numbers can be used as external keys.

## G

### Global Team

The highest level team in AlertFind. All other teams are considered subteams of the Global Team. Only administrators and others given explicit permissions can perform certain team functions in the Global team context.

### group

A collection of users, or a combination of users and groups, to which notifications can be sent. In AlertFind, there are broadcast groups, escalation groups, Smart Groups, and ad hoc groups.

## H

### hierarchy

An ordered structure with higher and lower levels. In AlertFind, teams and groups are hierarchical. At the top level is the Global Team; all other groups and teams are children of the Global Team.

### Hotline

A phone number that notification recipients can call to hear announcements or listen to messages. Administrators and team leaders with necessary permissions can also send notifications from the Hotline.

### Hotline Pro

An optional, customizable version of Hotline through which administrators and team leaders can create polls, send announcements, and collect information from users. Administrators and team leaders with necessary permissions can also send notifications from Hotline Pro.

## I

### import

A process by which Support propagates user information from your enterprise system of record into AlertFind.

### incident

An event for which there may be notifications and attachments that you want to log and share among users. Documents related to an incident can be shared using the Document Library. Information about incidents can be tracked in the Incident Collaboration Log (ICL).

## N

### notification

A message that is sent using AlertFind. Notifications can be sent to individual recipients or to groups of recipients and can be delivered by phone, emails, fax, pager, or SMS.

### notification email address

An email address used for receiving email notifications. This address may be the same as the primary email address. A user account can contain multiple notification email addresses.

### notification profile

A standard escalation, defined by default at the organization level, and available to all users, that defines which of a user’s devices are contacted, and in which order, during a notification.

### notification rule

A rule that determines which notification profile should be used at the time a notification is sent (such as during business hours or a holiday).

### notification template

A preconfigured incident that you can reuse to launch incidents that you may need frequently.

## P

### permissions

Permissions control what information and actions are available to team leaders. Administrators and team leaders (with appropriate permissions) can manage permissions for other team leaders.

### personal escalation

A customized escalation for an individual user.

### PIN

A secret number of 4-12 numeric digits used to access authenticated notifications.

### primary email address

The email address used for all password resets or reminders for a user account. The primary email address is required for all user accounts.

### private data

Information that is available only to AlertFind users with necessary permissions. The types of data that are considered are private are defined when Support provisions AlertFind for your company.

### properties files

Plain text files that contain field labels, values, and variables used in the AlertFind user interface. By editing properties files, administrators can customize constants, date and time formats, and prompts.

### public data

Information that is available to any AlertFind user with View Public Data permission. Users can always view their own personal account information. Additional permissions are required to change public data. Public information is defined when Support provisions AlertFind for your organization.

## Q

### Quick Launch ID

A numeric identifier that can be assigned to broadcast groups, escalation groups, and incidents. Users can then use the Quick Launch ID to access the group or incident through the voice/telephone interface.

## R

### roster

A list of users and user information imported from a third-party system of record.

## S

### Smart Group

A group created based on user properties (custom fields) imported from the system of record.

### SMS

Acronym for Short Message System, the service that supports text messaging to cell phones and other devices.

### standard devices

The standard list of devices available to all user accounts. The standard devices list is defined by Support when AlertFind is provisioned and typically contains one or more email addresses and telephone numbers. The standard devices list cannot be changed, but administrators or team leaders with necessary permissions can add custom devices for individual users.

### sub-team

Any team created as a child of another team.

## T

### team

A group of users that can also contain other groups or sub-teams. Usually, the members of a team have something in common, such as location, job function, or role.

### team context

The currently active team for an AlertFind team leader or administrator. The functions a team leader can perform depends on the permissions granted to the leader for the currently active team.

### team leader

An AlertFind user account that has been granted team permissions that enable the user to perform additional functions within a specific team context A user account given specific team leader permissions still maintains the role user.

### Text-to-Speech (TTS)

The technology that enables AlertFind to speak text typed for notifications or customizable prompts.

## U

### user

An AlertFind user role that grants the user the ability to use the system to send or respond to notifications. A user account given specific team leader permissions still maintains the role user.

## W

### web interface

The AlertFind user interface that can be accessed through a web address. If your organization uses imported data, the Allow Web Administration company setting must be enabled for you to use the web interface. If you cannot use the web interface, contact Support.

# Chapter 7: Index