Symphia NowForce

Administrator Guide

For versions 5.6 and higher

Preface

Symphia NowForce's advanced dispatch and response technology provides comprehensive situational awareness. Symphia NowForce allows dispatchers, responders and third-party resources to share insights in real-time, creating faster response times to potential threats and active incidents. Symphia NowForce leverages an integrated system of live and historical event data, state-of-the-art mapping, and tailored mobile applications for responders' and reporters' input to ensure that the closest, best equipped and most appropriate personnel is dispatched.

This Guide provides:

- The administrator with the recommended sequence of tasks to prepare your NowForce installation.
- The dispatcher operator and responder user with the key flows to use to Dispatcher and NowForce Mobile App.

Documentation

- Download documentation from: Partners Portal
- Send your questions or comments on the current document, or any other Symphia user documentation, to our documentation feedback team at documentationfeedback@intellicene.com

Contacting Intellicene Sales and Marketing

About Intellicene

Intellicene's Situational Intelligence Solutions helps enterprises and governments manage complex security operations, fuse information from various sources, analyze vast amounts of data, and gain insight for better incident management, response and investigations. With our solutions, organizations can see what's happening across their operations, make quick and confident decisions for decisive actions. Powered by our Symphia portfolio of solutions, we help our customers orchestrate better outcomes to protect what matters most.

To schedule an online demo today, contact us on:

- https://www.intellicene.com/contact/
- insidesales@intellicene.com
- +1 303 305 4534

Contacting Intellicene Service and Support

For immediate assistance, contact the support team:

Contact Support	
Americas	**Symphia** Phone: +1 888 747 6246 Email: support@intellicene.com **NowForce** Phone: +1 888 924 7247 Email: nowforcesupport@intellicene.com Canada/USA - Open 9:00am to 5:00pm (Local Time) Monday to Friday CALA - Open 9:00am to 5:00pm (EST) Monday to Friday
Europe, Middle East and Africa	**UK** Symphia and NowForce: +44 208 194 3368 **Israel** Symphia and NowForce:+972 3 375 2005 Symphia Support Email: support@intellicene.com NowForce Support Email: nowforcesupport@intellicene.com Open 9:00am to 5:00pm (GMT) Monday to Friday
Asia/Pacific	**India** Symphia and NowForce: +91 225 032 3020 **Singapore** Symphia and NowForce: +65 310 51276 Symphia Support Email: support@intellicene.com NowForce Support Email: nowforcesupport@intellicene.com Open 9:00am to 5:00pm (Local Time) Monday to Friday

Contents

Preface 2

Documentation 2
Contacting Intellicene Sales and Marketing 2
About Intellicene 2
Contacting Intellicene Service and Support 3

Contents 4

Overview 8

NowForce System Components 8
Admin Settings 8
Dispatcher 8
Mobile App 9

Getting Started 12

Locating Your Organization's ID (Org ID) Number 13
Logging In and Out of Dispatcher 14
Logging In to Dispatcher 14
Logging Out of Dispatcher 15
Changing Your Password 16
Self-Registering 18
Changing the Language in Dispatcher 18

Adding Licenses to Profiles 20

Confirming Licenses 20
Adding a License to an Existing Profile 20
Creating Additional Profiles and Adding Licenses 21

User Infrastructure Settings 24

Assigning Licenses to Users 25
Adding and Managing Virtual Users 26
Adding Virtual Users 26
Dispatching a Virtual User 27

SMS on Virtual User Dispatch 29
Creating Equipment Items 30
Defining User Roles 31
Managing Groups 32
Creating New Groups 33
Editing and Deleting Groups 37
Configuring Units 39
Enable the Support Units Feature in the Organization 39
Defining Units 40
Adding New Units 41
Adding and Managing Users 45
Organization Tab 47
Mobile Device Tab 52
Adding Geofences 53
Contacts 53
Exporting User Details 55
Configuring and Applying User Update Settings for Policies 56
Viewing the User Updates Settings 56
Applying User Updates in Policies 61

Geography Infrastructure Settings 63

Creating and Editing Geofences/ Areas of Interest (AOIs) 64
Adding and Managing Points of Interest (POIs) 70
Editing and Deleting POIs 72
Importing Batch POIs 73
Setting Default Map Center and Zoom Level Preference 74

Organization Infrastructure Settings 77

Understanding the System Configurations 78
Description of System Configurations 79
Incident Location 79
SOS 80
Security 80
Incident Management 81
Mapping and Location 82
Advanced Mapping 83
Regional 83
Mobile Devices 84
Changing Org Configurations 86
Organization Configurations 86
Using the Control Center Table 86

Control Center Table Descriptions ... 87
Editing a Control Center ... 93
Archiving a Control Center ... 93
Main Control Center Overview ... 94
Main Control Center Settings ... 95
Accessing the Control Center Settings Table ... 95
Understanding Control Center Jurisdiction ... 97
Dispatcher / Supervisor Access ... 98
Control Center Jurisdictions ... 100
Incident Filtering ... 100
Other implications of the Control Center jurisdiction settings ... 106
Viewing Users on the Map ... 106
Creating New Incidents ... 106
Dispatching Responders to Incidents ... 106
Control Center Access vs. Permission Profile ... 106
Dashboard Business Intelligence (BI) Tool ... 107
Available Dashboards ... 107
Incidents Dashboard ... 107
Users Dashboard ... 108
Geofence and Map Data Dashboards ... 109
Additional Dashboard Configurations ... 110
Setting up a background image URL for Mobile SOS ... 110
How to Add and Manage Icons ... 111
Adding Icons ... 112
Configuring Two Factor Authentication Permissions ... 114
Configuring Location Settings for Mobile App Users ... 117
Android Location Settings ... 118
Frequency ... 118
Accuracy ... 118
IOS Location Settings ... 118
Distance ... 118
Accuracy ... 119
User States ... 119
Changing Logos in NowForce ... 121
Changing Your Organization's Time Zone ... 122

Incident Infrastructure Settings ... 125

Receiving and Configuring Alerts ... 126
Receiving Alerts in NowForce Dispatcher ... 126
Configuring Alerts ... 127
Putting SOS Alerts on Repeat ... 128
Incident Log Icons ... 128

Defining Asset Types 129
- Creating a New Asset Type 130
- Editing an Asset Type 131

Creating and Editing Form Templates 132
- Creating Form Templates 133
- Creating a New Form Template 134
- Form Fields 135

Attaching Form Templates to an Incident Type 138

Customizing Form Templates Assets 140
- Searchable Fields 141
- Assigning a Form to Asset Types 141

Configuring Multi Forms Permissions 142
- Adding Multi Form Permissions 143

Understanding Multi Forms 145
- Viewing, Editing and Duplicating Form Templates 146
- Form Template Name 146
- Form Template Creator 148
- Mandatory Fields 148

Adding and Modifying Incident Dispatch Rules 150
- Adding New Dispatch Rule 153
- Editing or Deleting Dispatch Rules 155

Managing Incident Types 156
- Creating a New Incident Type 156
- Editing or Deleting Incident Types 164

Limiting Address Search Results in Incident Screen 165

Adding Situation Reports to Incident Types 166

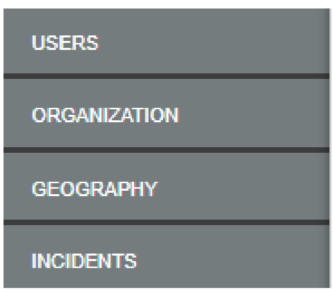
Overview

This chapter provides an overview of the Symphia NowForce components. It explains what the components of a typical Symphia NowForce installation include and the key workflows for each of the user groups, administrator, dispatcher and responder.

NowForce System Components

Admin Settings

The SymphiaNowForce system's settings are located in the Settings page, and grouped into four tab: USERS, ORGANIZATION, GEOGRAPHY AND INCIDENTS.



Each tab contains all of the associated configurations available to your organization.

This guide provides the main administrative task flows within each setting tab required to customize your installation to your organizations needs.

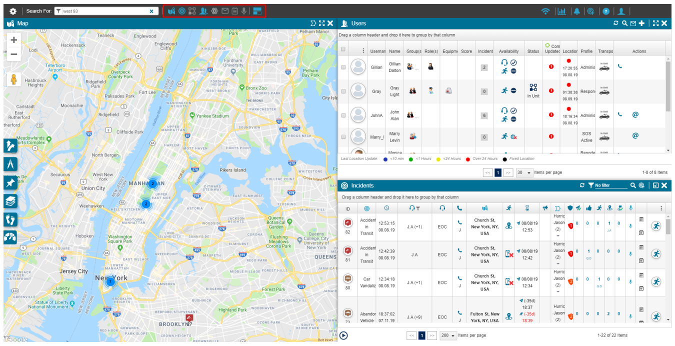
Dispatcher

The Dispatcher panel can be customized according to your requirements. You can choose the panels to display and also arrange where you want them to appear on your screen.

The following panels are available:

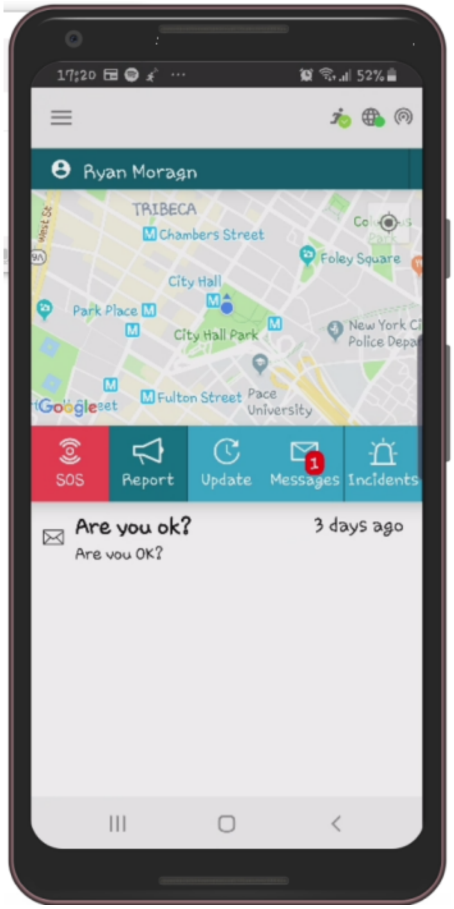
- **Maps**: Shows a map view of the area in which you are located.
- **Incidents**: Lists the open incidents.
- **Users**: Lists the user registered in your control center.

- **Units**: Lists the units you have created.
- **Assets**: Lists the assets at your disposal.
- **Messages**: Lists a history of the messages that have not yet expired.
- **Resources**: Lists the resources available in your area or in a specified geofence.
- **PTT Channels**: Lists the channels that have been created and also shows a history of the conversations in each PTT channel.



Mobile App

The NowForce Mobile App is an entirely customizable application. A typical home screen is shown below.



The application contains the following in its Main menu.

- **Home**: Returns you to the mobile app Home screen.
- **SOS**: Enables you to activate the SOS feature by tapping the **SOS** on the **Home** screen.
- **Map**: Enables you to view all active incidents and also see the location of other users in your organization.
- **Report**: Enables you to report an incident. This function is the same as tapping **Report** on the **Home** screen.
- **Incidents**: Opens the Incidents screen in which you can view all incidents assigned to you. This function is the same as tapping **Incidents** on the **Home** screen.
- **Messages**: Opens the Messages screen in which you can view all sent and received messages. This function is the same as tapping **Messages** on the **Home** screen.
- **Asset Lookup**: Opens the Asset Lookup screen in which you can search for assets.

- **Channels**: Opens the Channels screen in which you can view all the PTT channels to which you have access. The screen includes details of all messages received or sent on the PTT channels, which you can also replay.
- **Escort me**: Monitors your activity in a defined time frame of your choosing. If you feel unsafe or in a hostile environment, use this feature to set a time frame according to your activity. When the time frame expires, an SOS alert is activated, your dispatch center is immediately updated with your current location and an automated call to your emergency number is made.
- **Logout**: Logs you out of the mobile app. After logging out, you no longer receive alerts, messages, or any other type of communication from the dispatch operator.
- **Settings**: The Settings icon is located at the bottom left of the menu screen, and enables you to view and make configuration settings.

Getting Started

The following topics are covered in this section:

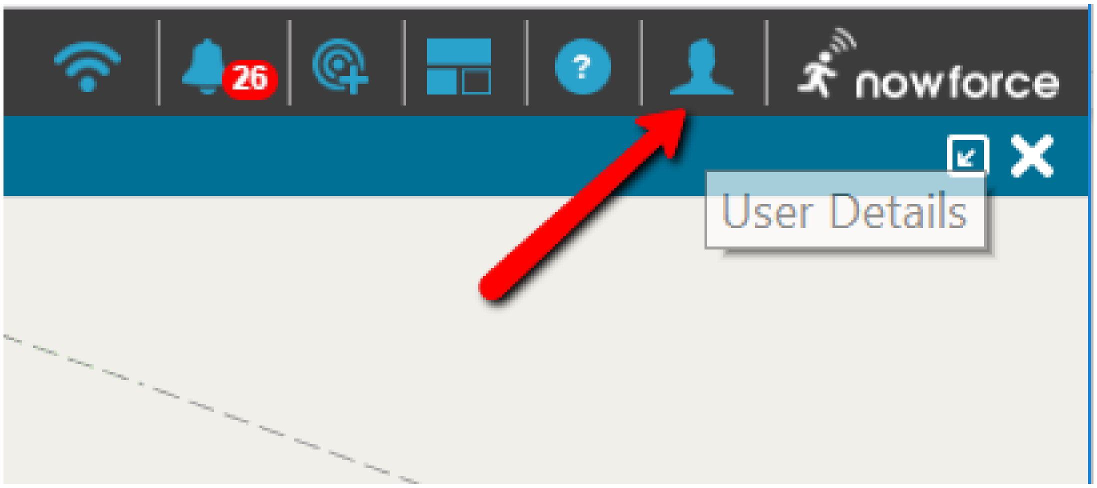
Locating Your Organization's ID (Org ID) Number 13
Logging In and Out of Dispatcher 14
Changing Your Password 16
Self-Registering 18
Changing the Language in Dispatcher 18

Locating Your Organization's ID (Org ID) Number

When you sign up to NowForce you are assigned a unique Organization ID. You will be asked for your Org ID if you request support from Intellicene Support.

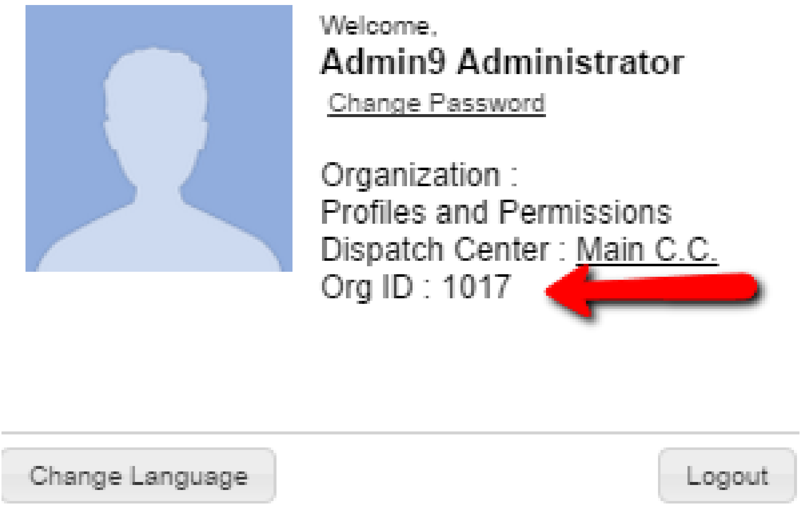
▼ To locate your Org ID

1. Log in to NowForce Control Center.



2. Click User Details.

   Your user details display.



Logging In and Out of Dispatcher

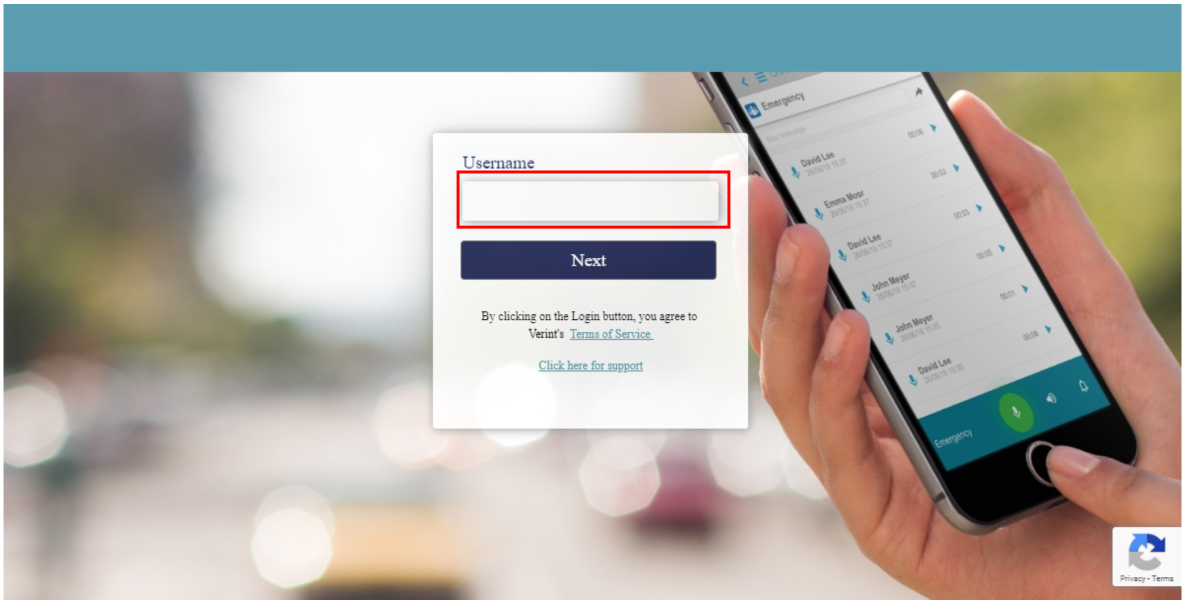
This topic describes how to log in and out of Dispatcher.

Logging In to Dispatcher

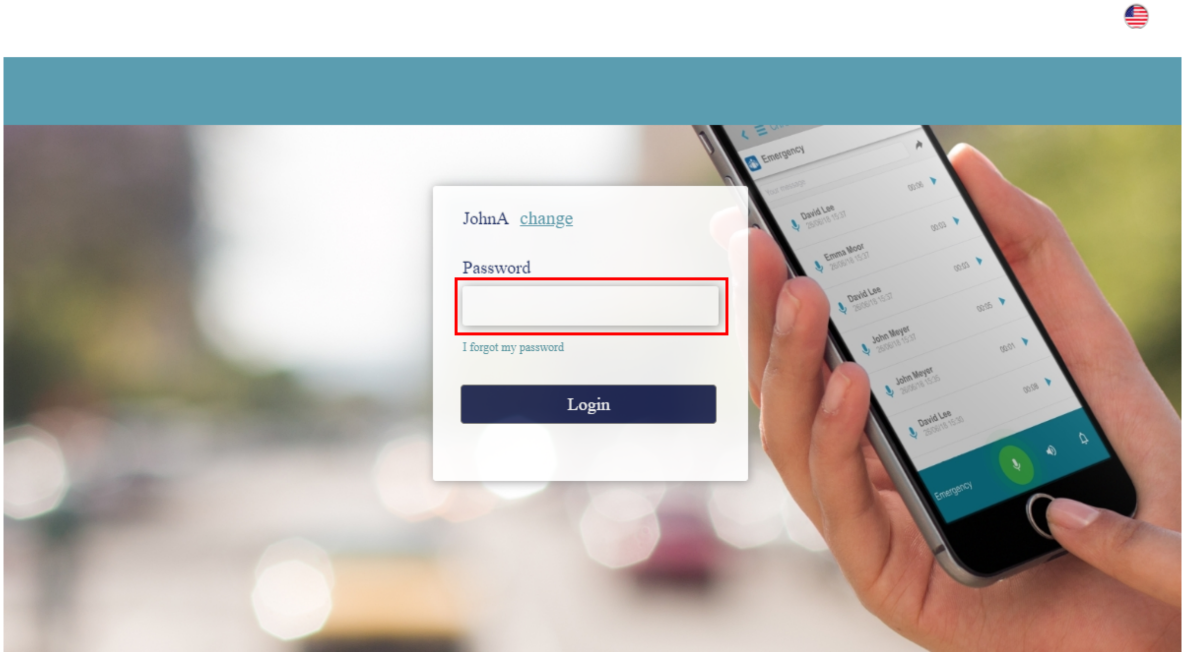
▼ To log in to Dispatcher

1. Obtain the Dispatcher URL from your system administrator.
2. Using your Chrome browser go to the Dispatcher URL.

   The **Dispatcher** login page opens.

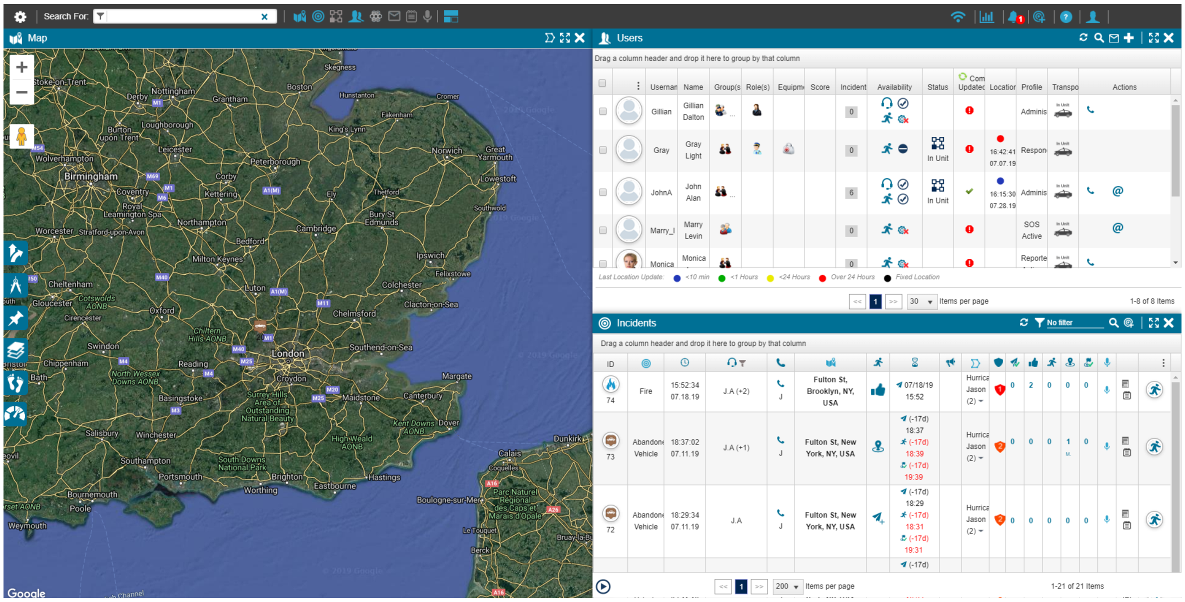


3. In the Username field, enter your user name.
4. Click **Next**.



5. In the **Password Field**, enter your password.

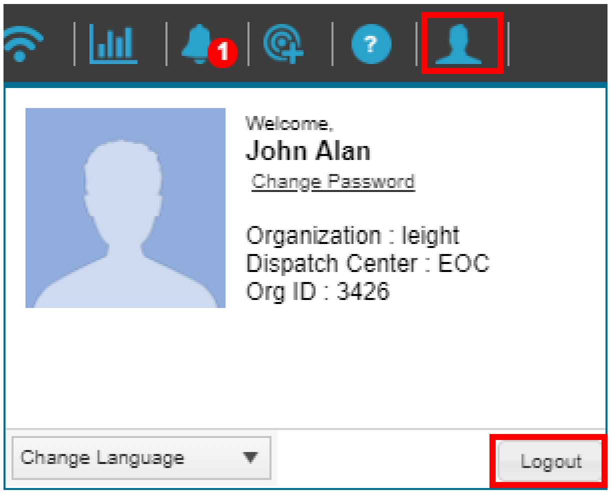
   The **Dispatcher** application opens.



Logging Out of Dispatcher

▼ To log out of Dispatcher

1. From the Dispatcher toolbar, click **User Details**.



2. Click **Logout**.

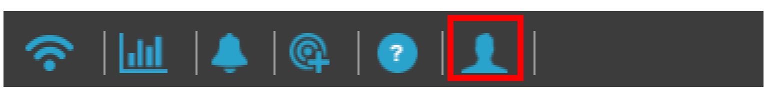
The **Dispatcher** application closes, and the **Log in** page opens.

Changing Your Password

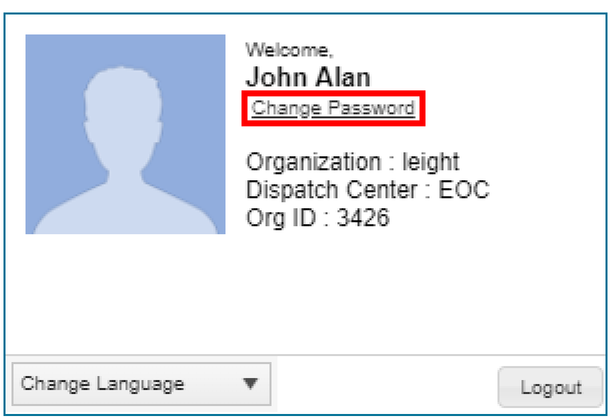
You can change your user password in Dispatcher.

▼ To change your user password

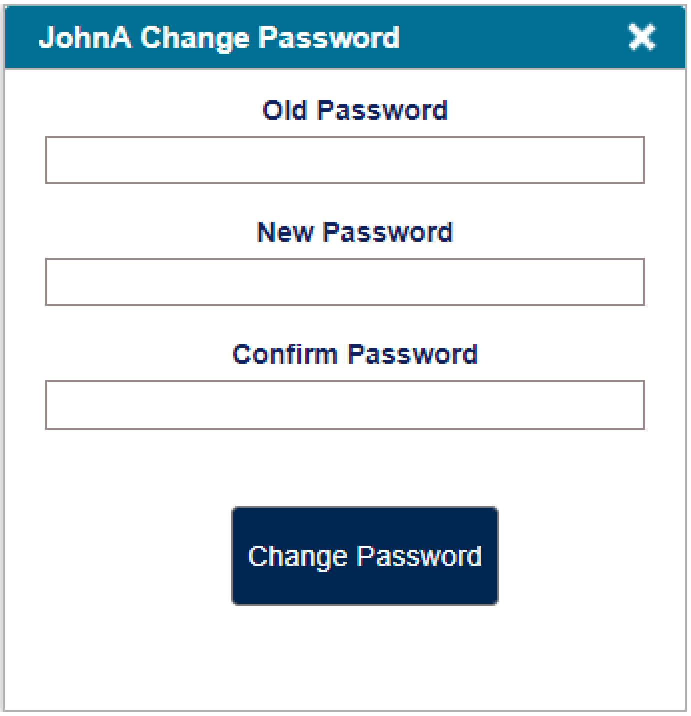
1. From the Dispatcher toolbar, click **User Details**.



The User Details pop-up opens.

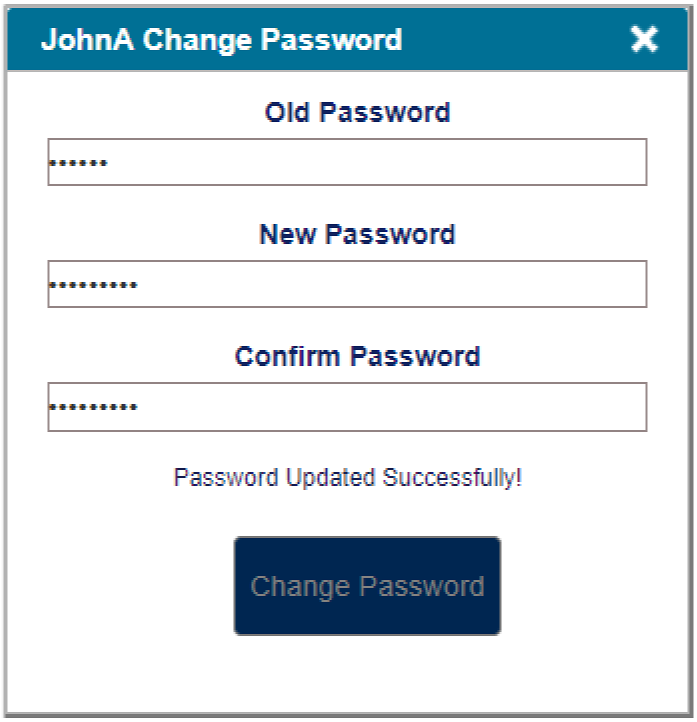


2. Click **Change Password**. The Change Password pop-up opens.



3. Enter the old password, new password, and confirm the new password in the respective fields.

4. Click **Change Password** to effect the changes.



A message appears confirming that the password updated successfully.

Self-Registering

If you want to self register to an Organization, you are given a URL (for example, https://sos.nowforce.com).

When you sign up to this URL, you will receive an email with a link that approves your login to the system.

> Note
> Organizations can choose if they want to allow self registration, or only allow administrators to register new users. If your organization does not allow self-registration, you are only sent a notification to login to the system after registration by the administrator.

Changing the Language in Dispatcher

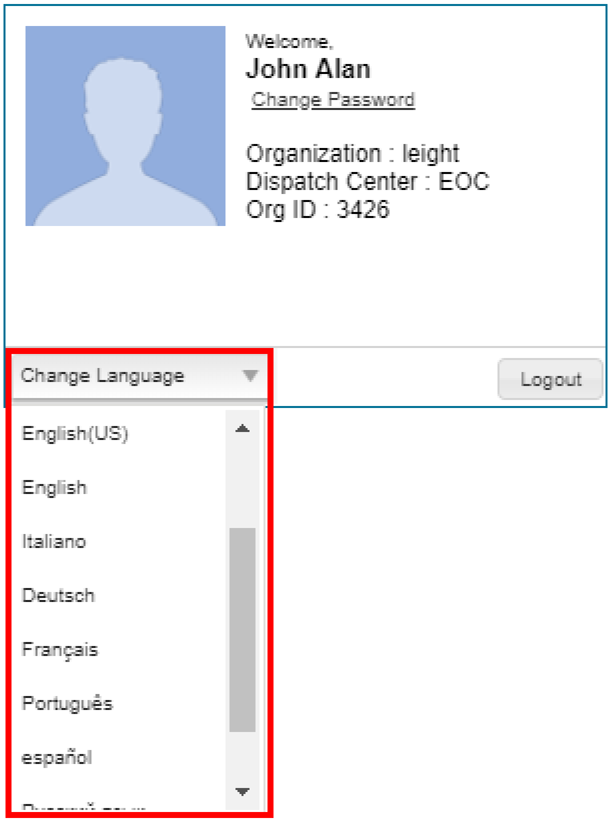
You can change the language in Dispatcher.

▼ To change the language

1. From the Dispatcher toolbar, click **User Details**.

The **User Details** pop-up opens.

2. Click **Change Language**. The **Change Language** dropdown list opens.



3. Select the required language.

Adding Licenses to Profiles

Permission profiles determine the access that each user has to specific functions in the Dispatcher and on their mobile devices. You assign each user to a permissions profile and they are allocated to the available licenses that have been allocated to that profile. This section explains how to allocate licenses to an existing profile and how to create and allocate licenses to a new profile.

Confirming Licenses

Before allocating licenses to a profiles review the Entitlement Letter you received from Symphia NowForce and confirm that the supplied licenses are correctly loaded and displaying in your License settings.

▼ To review your provisioned licenses

1. Click **Settings** (gear) in the upper left corner of the **Dispatcher** screen.

2. Click **Licenses** tab, the **Licenses** settings page opens.
3. Review the available licenses.

For further details see *Symphia NowForce Licensing Guide.*

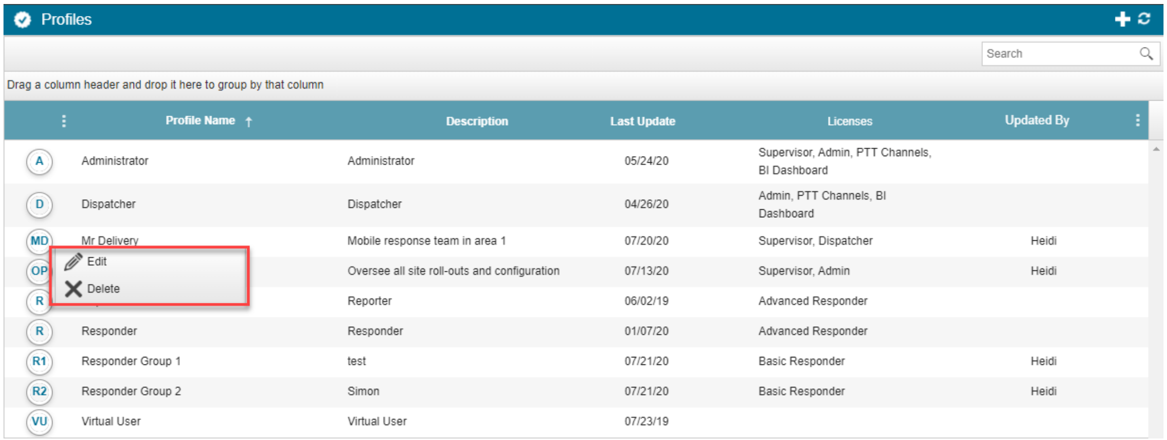
Adding a License to an Existing Profile

The Administrator, Dispatcher and Responder profiles are provided by default with NowForce Dispatcher. This section describes how to add a license to an existing profile.

▼ To allocate a license to an existing profile

1. Click **Settings** (gear) in the upper left corner of the **Dispatcher** screen.

2. Click **Profiles** tab, the **Profiles** settings page opens.



3. In the Profiles settings table, hover over the Profile name you need to edit. Select **Edit**. The **Edit Profile** page opens.
4. Select the either **Mobile** of **Desktop** tab to select the required license.
5. Select the **License** required.
6. Select **Add-Ons** tab and select relevant licenses.
7. Select **Permissions**.
8. Click **Available Only** to display on **Available Permissions**.
9. Select the **Permissions** tab and select all relevant permissions for the profile.

> Note
> Only the permissions available to the user with the selected licenses are available for selection.

10. Click **SAVE**.

> Note
> Changes to a profile takes effect on close of the profile settings page and are applied to the user the next time they log in.

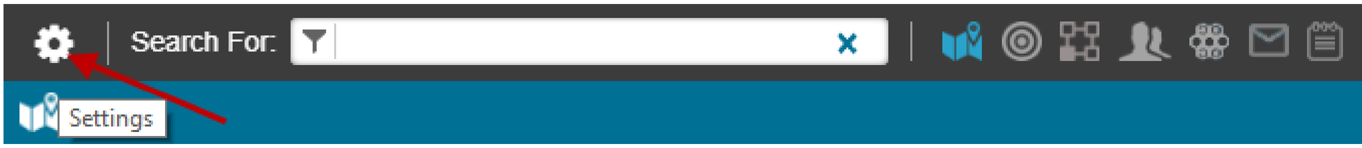
You can also create additional profiles and add licenses to new profiles.

Creating Additional Profiles and Adding Licenses

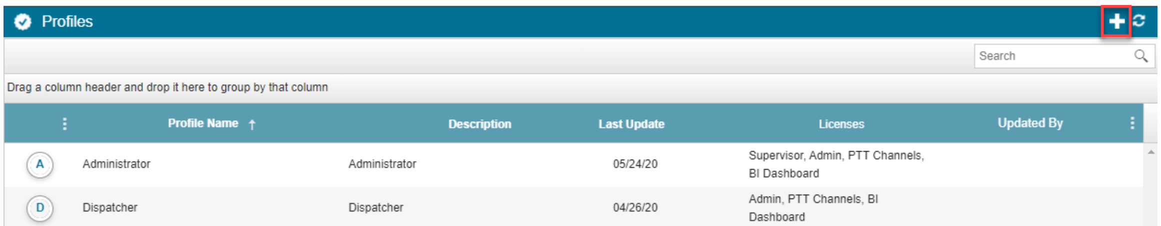
This section describes how to create additional profiles and then allocate licenses to the new profile.

▼ To create a new profile and add a license

1. Click **Settings** (gear) in the upper left corner of the **Dispatcher** screen.

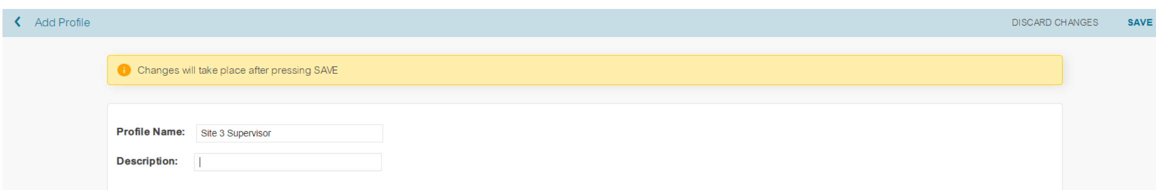


2. Click **Profiles** tab, the **Profiles Settings** page opens.



3. Click the **+** to add a profile.
4. Provide a name in **Profile Name** text box.

   A pop-up warning indicates that changes become active after pressing SAVE.



> **Note**
> Clicking **SAVE** saves all your changes and closes the **Add Profile** window, returning you to the **Profile Settings** table. To complete the setup of your new profile, select your recently added profile and click **Edit** to open, and continue the steps below.

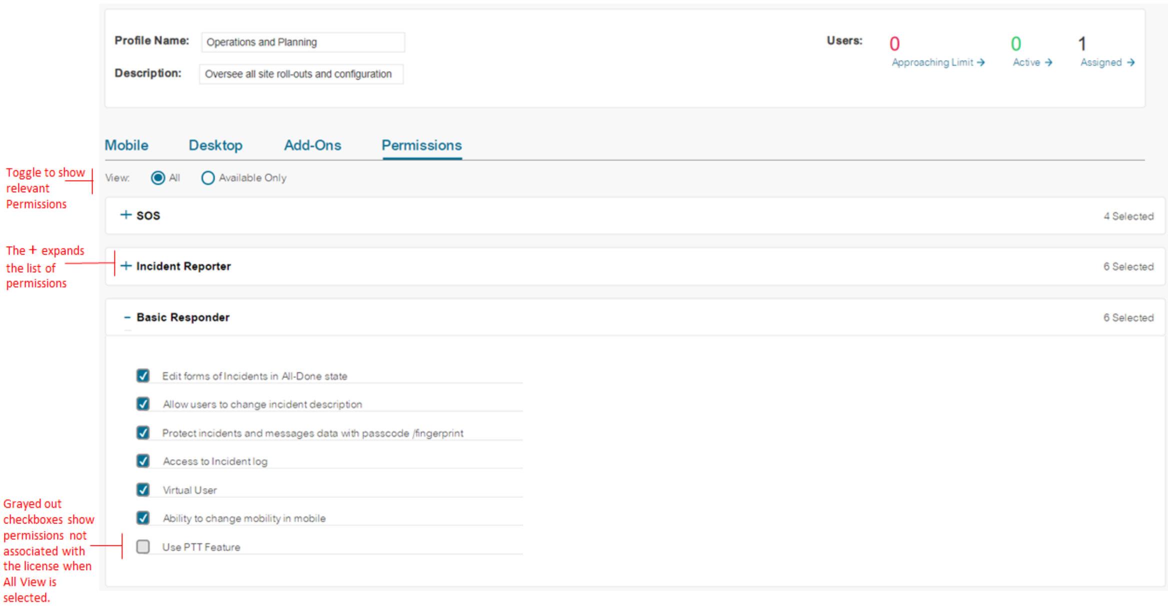
> **Caution**
> Selecting **DISCARD CHANGES** removes all changes and you must start over.

5. Add a **Description** in the text box.

> **Tip**
> Ensure your description explains the new profile's function in your organization.

6. Select the either **Mobile** of **Desktop** tab to select the required license.
7. Select the checkbox of the **License** required.
8. Select **Add-Ons** tab and select relevant checkboxes of add-on licenses.

9. Select **Permissions**.



10. Click **Available Only** to display on **Available Permissions**.

11. Select **Permissions** tab and select all relevant permissions for the profile.

> **Note**
> Only the permissions available to the user with the selected licenses are available for selection.

12. Click **Save**.

> **Note**
> Changes to a profile take effect on close of the profile settings page and are applied to the user the next time they log in.

User Infrastructure Settings

This section sets out to describe the administrative processes for defining, organizing and managing user settings in NowForce.

Permission Profiles determine the user access and authorization class. An administrator must first create Permission Profiles and then assign users to these permission profiles. The permission enable user access different areas of the Dispatcher and the NowForce Mobile App.

User Roles and Equipment are configurations that must created prior to adding users as either a role or equipment must be added to a new user.

Group settings determine user management throughout the system. In the Dispatcher, groups provide access to user details, have set dispatch rules, messaging , mapping and more. Groups also affect the management of the Control Center.

Units allow organizations to link multiple users (unit members) together and manage them under one unified entity. Each individual unit inherits its attributes and behavior from the Unit Type settings and from the settings of the specific unit.

Adding Users is undertaken in the Dispatcher screen, by either a administrator or dispatcher. Adding Users requires that all of the settings noted above are configured in the system.

The following topics are covered in this section:

Assigning Licenses to Users 25
Adding and Managing Virtual Users 26
Creating Equipment Items 30
Defining User Roles 31
Managing Groups 32
Creating New Groups 33
Editing and Deleting Groups 37
Configuring Units 39
Adding and Managing Users 45
Exporting User Details 55
Configuring and Applying User Update Settings for Policies 56

Assigning Licenses to Users

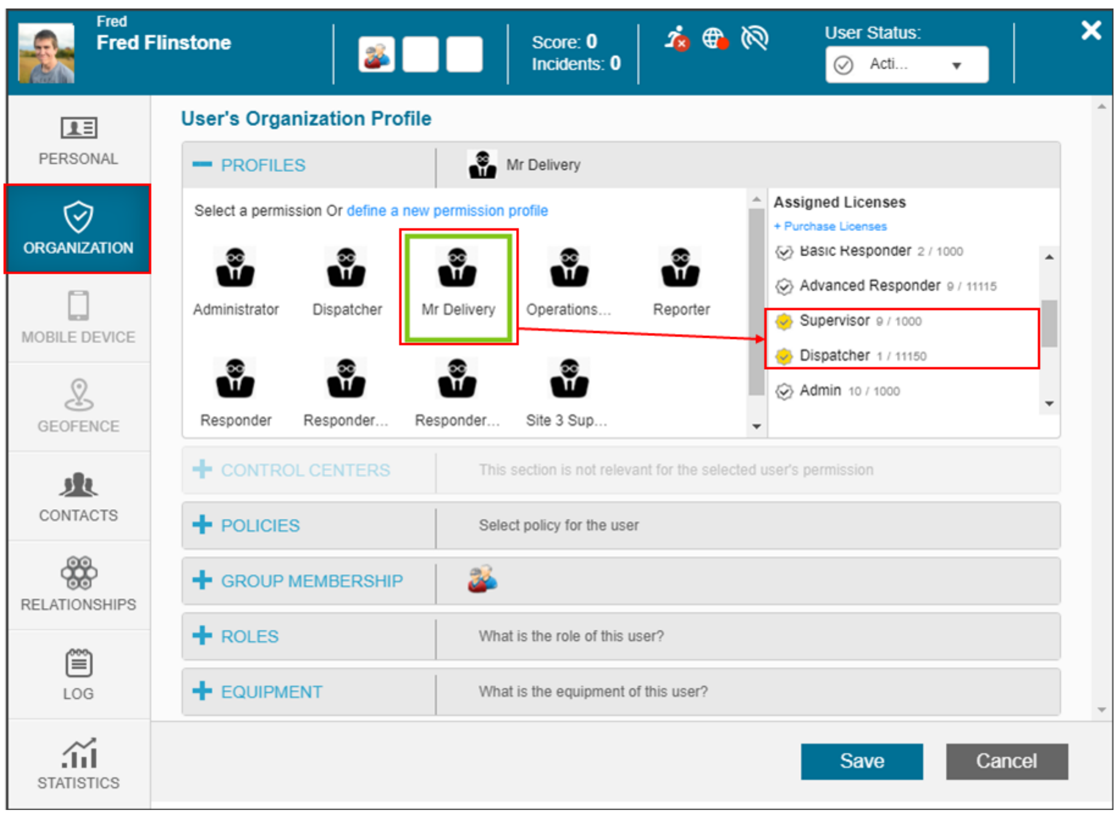
This section describes how to apply a license to a user.

> Tip
> Review your organization's Profile settings and ensure that the licenses are applied to the profiles as required.

▼ To apply a license to a user in the User Management window

1. In the Dispatcher screen, select **Users icon** from the taskbar.
2. In the User Panel, stand on the user's image displayed in the **Actions** column and select **Edit** from the popup menu. The User Management window opens.
3. In the User Management window, select **ORGANIZATION** tab and then select the Profiles to select a profile for the user.

   Each profile has its associated user license/s displayed as below:



4. Select the **Profile** required for your user.

> Tip
> Shown on the right side of the panel in **Assigned Licenses** is the number of licenses your organization has assigned out of the total number available in that profile is shown.

5. Click **Save**.

Adding and Managing Virtual Users

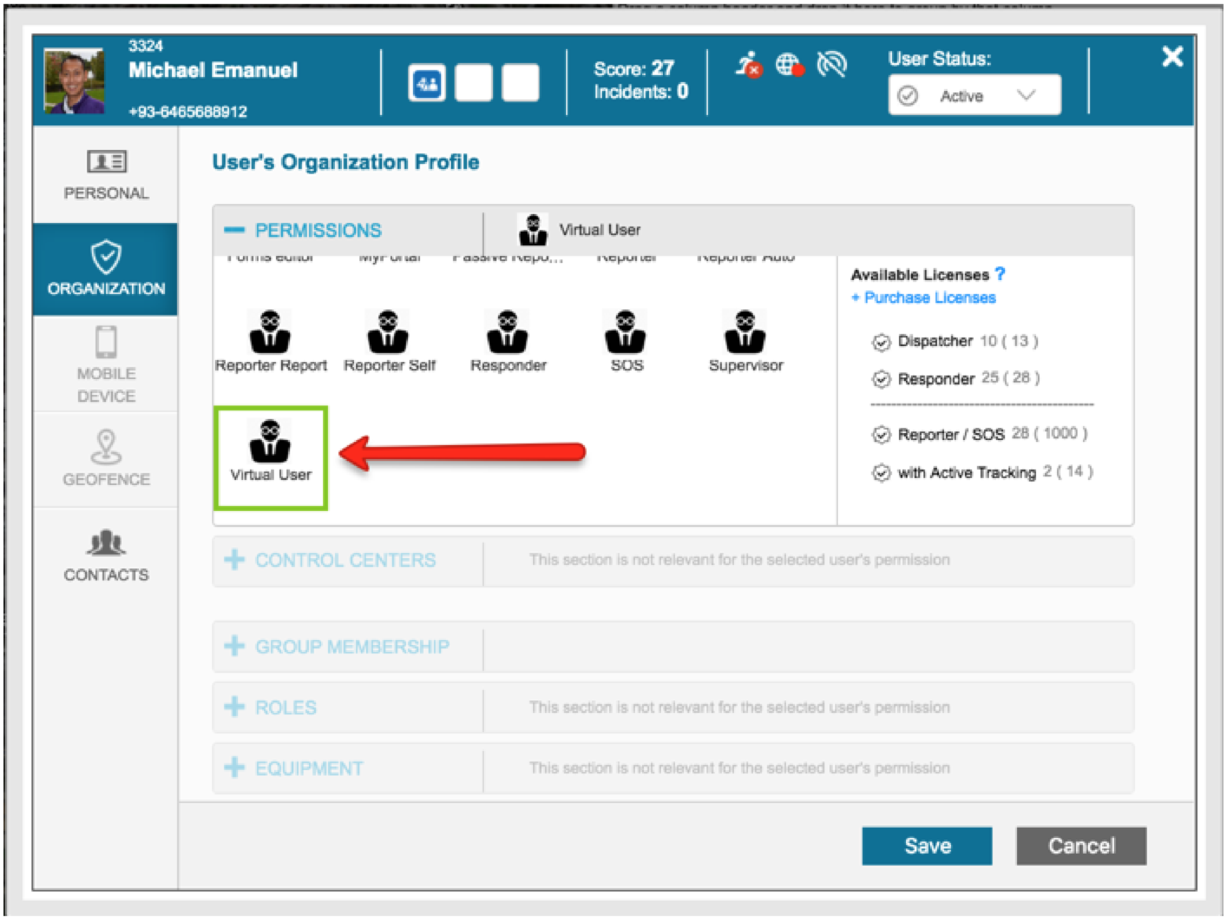
A Virtual User is User who does not use the Responder app and has to be manually dispatched and managed by the Dispatcher. The Dispatcher logs a Virtual User's timeline and actions manually.

A classic example of a Virtual User is a Responder using a radio device and can't use the Responder application, or a 'station' that needs to be called to the incident.

Adding Virtual Users

You create a Virtual User like any other user, see Adding and Managing Users.

> Note
> You need to select only the Virtual User permission profile in the Organization tab.



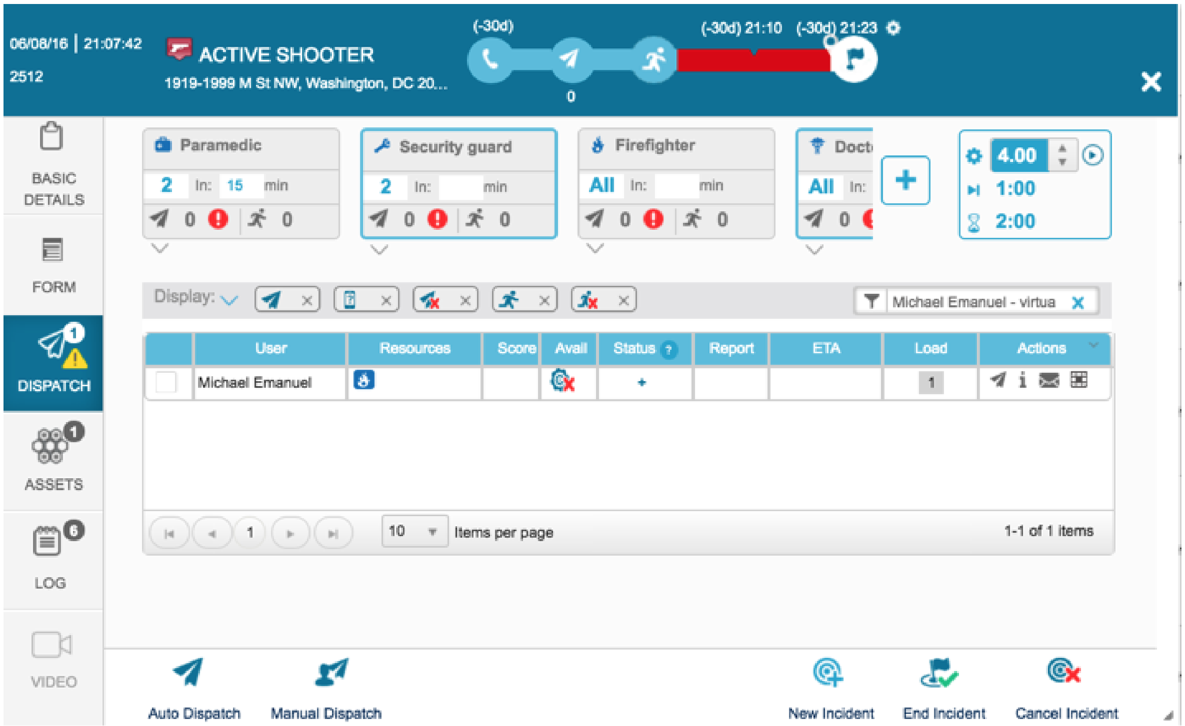
Dispatching a Virtual User

The virtual user has to be manually searched for in order to become visible in the Dispatcher tab.

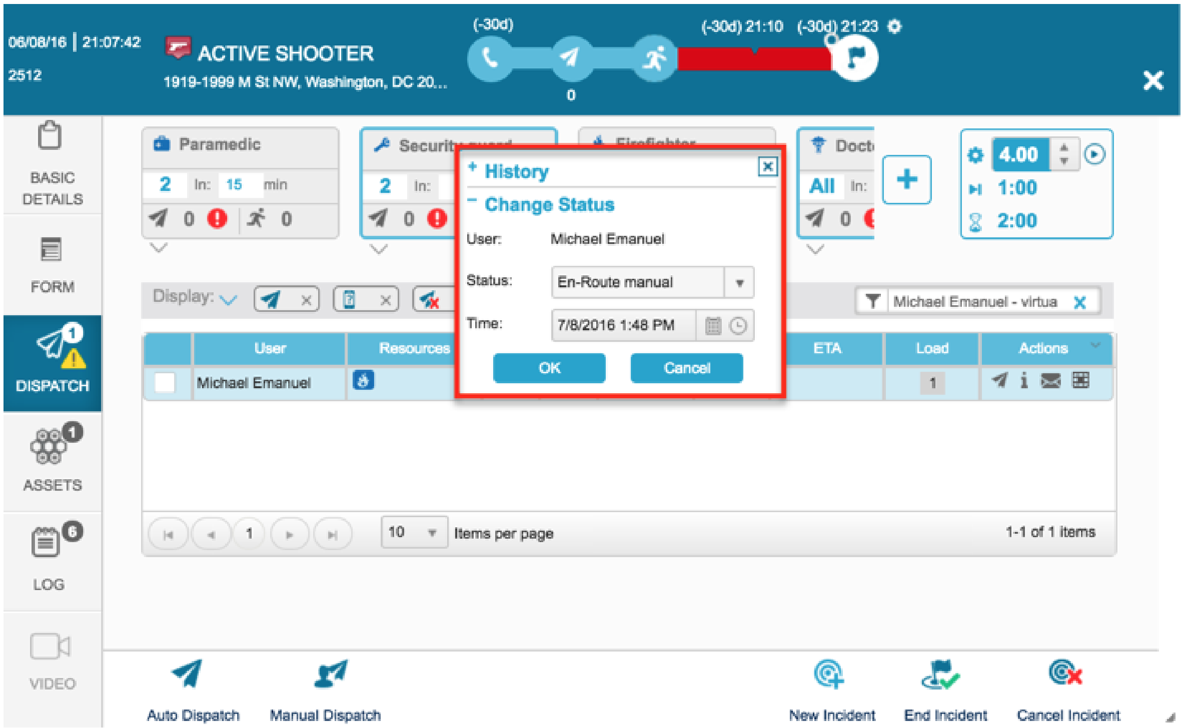
▼ To dispatch a virtual user

1. Click on the Manual Search bar to search for the Virtual User.

2. Select the **Virtual User** from the dropdown list.
3. Click the **+** icon in the Status column.

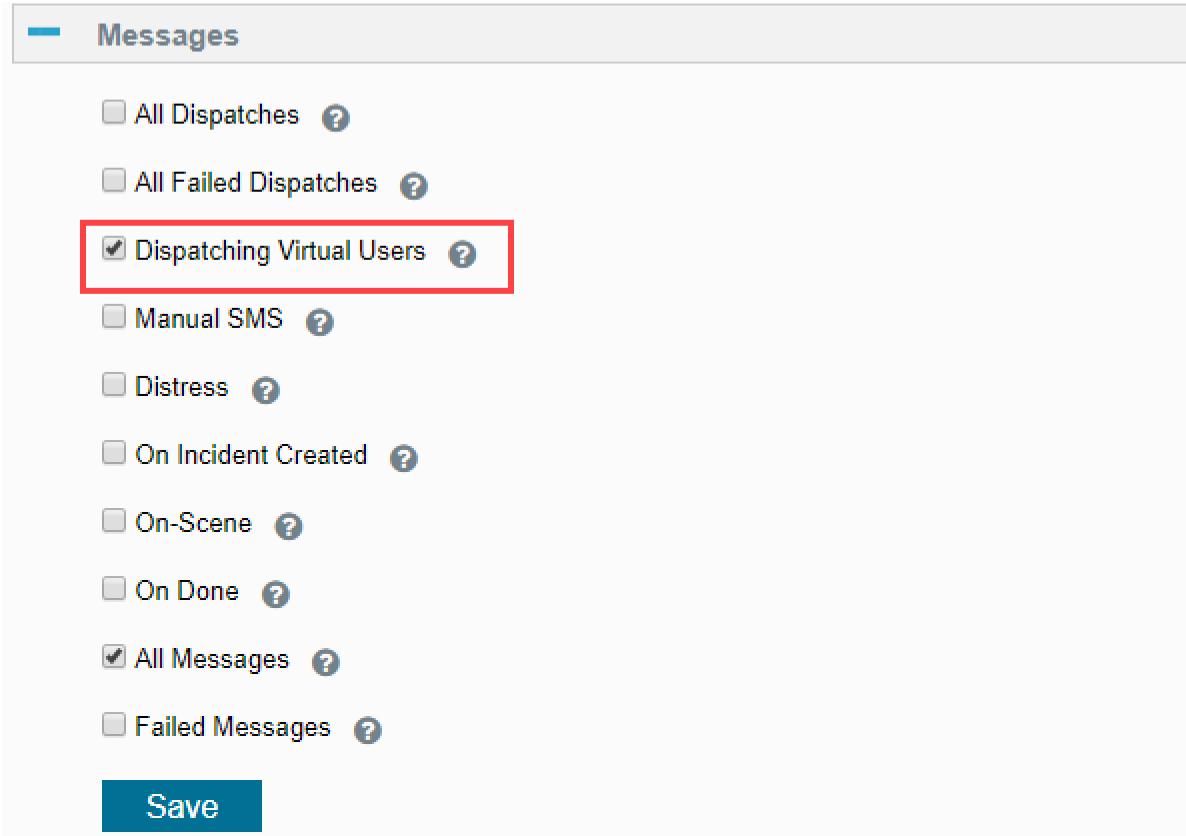


4. Manually enter the dispatch status and time.



SMS on Virtual User Dispatch

Virtual Users can be configured to receive a SMS upon manual dispatch.



Creating Equipment Items

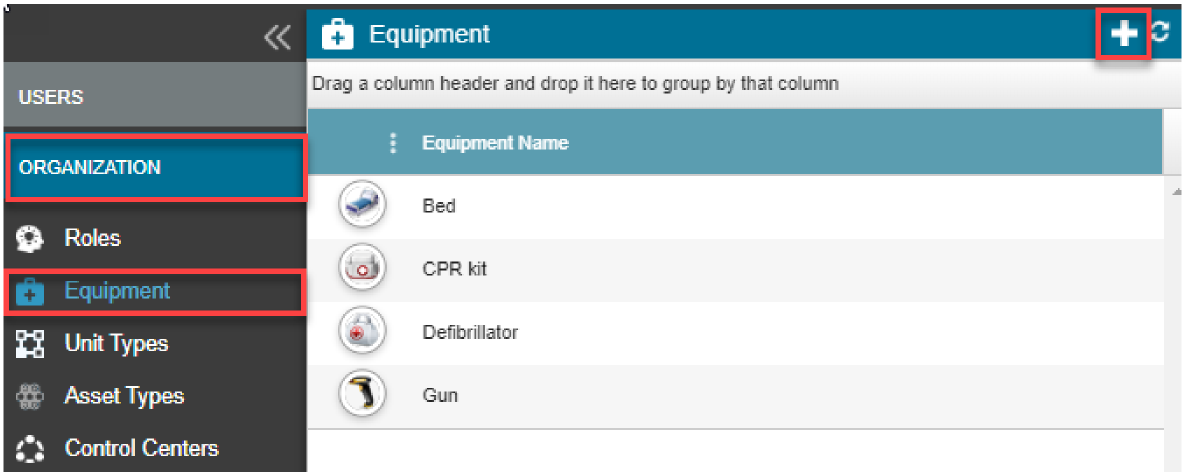
Users must be assigned either a Role or Equipment when you add a new user. See "Adding and Managing Users" (page 45).

You can configure all the Equipment available to the Dispatcher and Responder users in the ORGANIZATION settings.

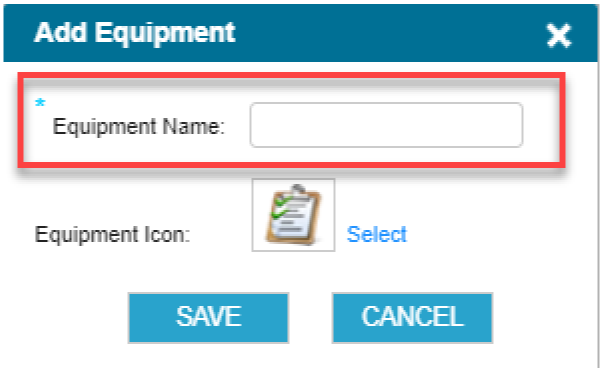
▼ To create an equipment item

1. From the **Main** screen, select **Settings** > **ORGANIZATION**, and then select **Equipment**.

   The **Equipment Names** table opens, with equipment listed in alphabetical order.



2. Click the **+Add** icon. The Add Equipment pop up opens.



3. Add your new role in the **Equipment Name** field.
4. Use **Select** to change the **Equipment Icon**.
5. Click **Save**.

Defining User Roles

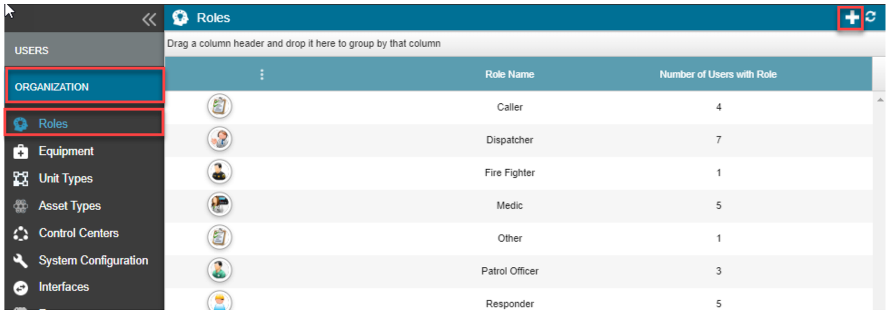
Users must be assigned either a Role or Equipment when you add a new user. See "Adding and Managing Users" (page 45).

You can configure all the User Roles available to the Dispatcher and Responder users in the ORGANIZATION settings.

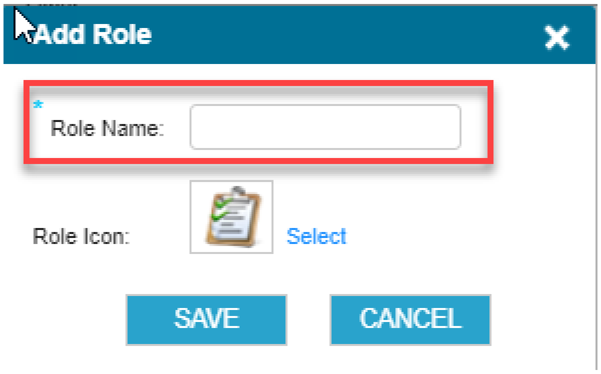
▼ To create a user role

1. From the **Main** screen, select **Settings** > **ORGANIZATION**, and then select **Roles**.

   The **Roles** table opens, with roles listed in alphabetical order.



2. Click the **+Add** icon. The Add Role pop-up opens.



3. Add your new role in the **Role Name** field.
4. Use **Select** to change the **Role Icon**.
5. Click **Save**.

Managing Groups

Groups are one of the most important features in the system as it effects user management throughout the system. Group functionality is used in the Dispatcher, Messaging, and PTT Channels. In the Dispatcher, groups provide access to user details, enable you to create dispatch rules and show users on the map according to group. Groups also affect the management of the Control Center, see Secondary Control Centers.

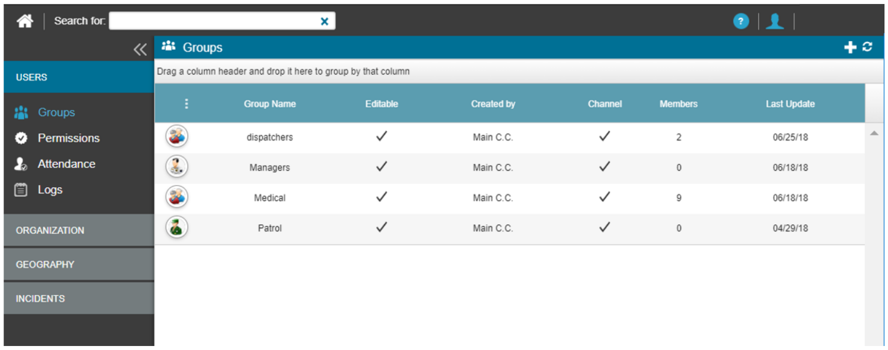
When defining groups it is recommended to keep the group organization neat and simple, meaning you should keep the group structure as close as possible to the actual structure in the organization, and then, only create the groups you really need. Having unnecessary groups, requires more effort to manage and maintain groups when you add new users to the system.

Manage groups from the Groups Settings page where you can create, edit or delete groups in the organization.

▼ To manage groups

1. From the **Main** screen, select **Settings** (gear).

The **Groups** page opens in a new tab. **Groups** lists all the groups in the organization and their related information.



> **Note**
> Users only see the groups to which they have access to view, based on the Control Center Groups jurisdiction.

Creating New Groups

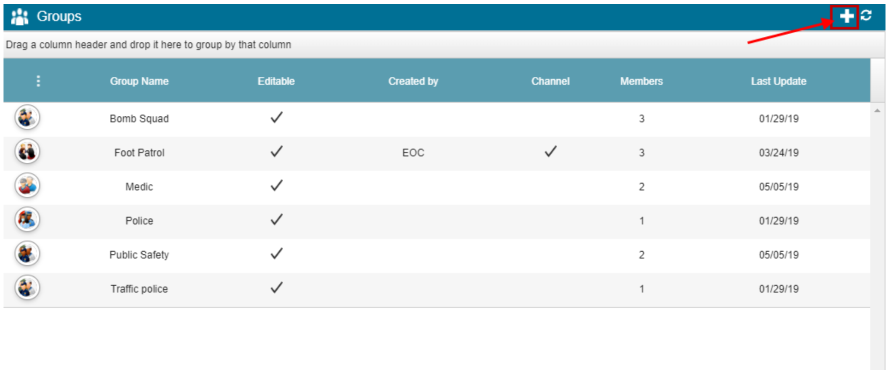
Group functionality enables you to manage and control users in the system. As part of the process of creating groups, you add users (members) to the group.

For information on how groups should be structured, see Managing Groups.

▼ To create a new group

1. From the **Main** screen, select **Settings**>**Groups**.

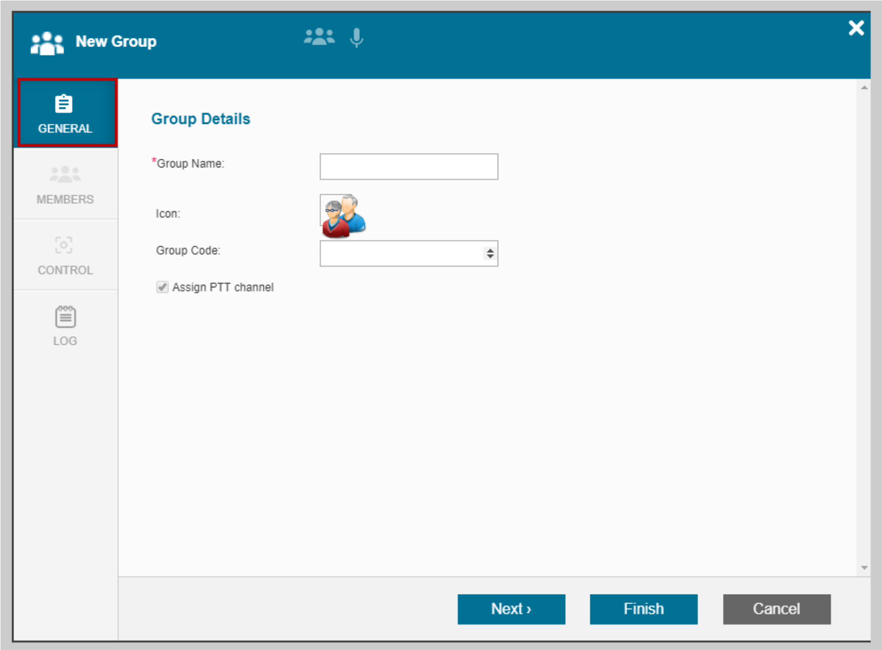
   The **Groups** page opens.



2. Click the **+** sign in the upper right corner of the Groups page.

   The **New Group** wizard opens.

3. Define the **Group Details** in the **General** tab.



- **Group Name**: The name of the new group.
- **Icon**: Click the icon button, and select an icon that best matches the group you have created. If you do not find a suitable icon you can upload new icons to the Icon Bank (For more information on how to use the icon Bank, see How to Add and Manage icons.)
- **Group Code**: (Optional) For organizations that use codes for their groups/departments.
- **Assign PTT Channel**: Select the check box if you want this group to have its own dedicated PTT channel. This check-box is grayed out and selected by default. In the future you will be able to decide whether you want to associate a PTT channel for the group or not.

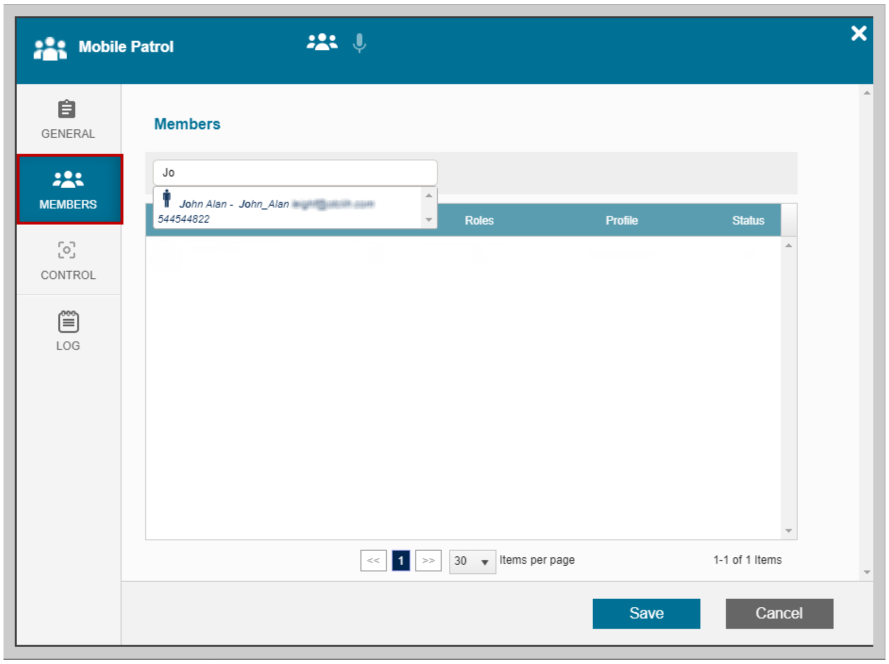
4. Click **Next**.

   The **Members** tab opens.

   This tab enables you to add users as members in the group. The Add User text box acts as a filter for all the users in the system. Start typing the name of the user whom you want to add to the group. As you type, names are added to the dropdown list.

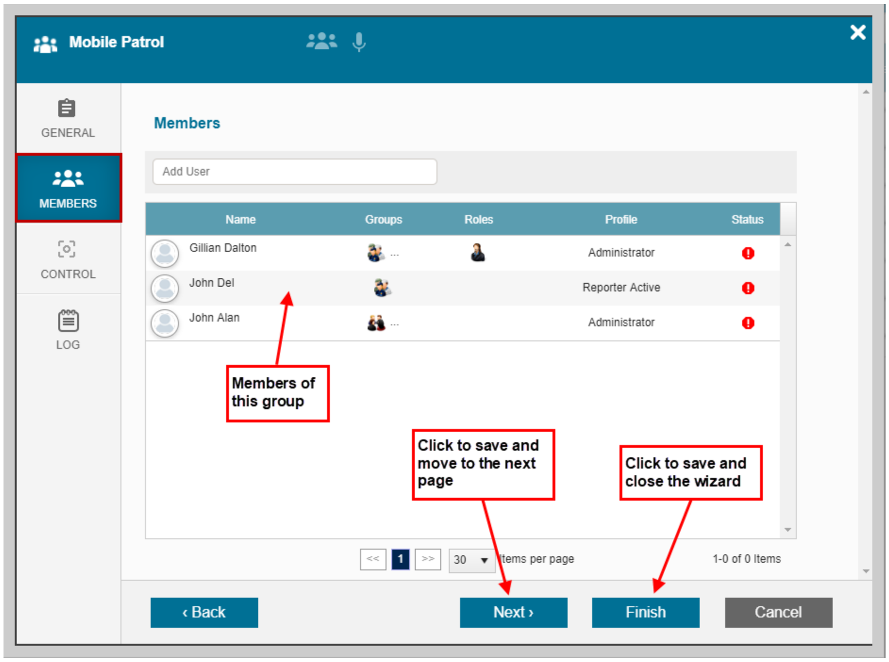
5. In the **Members** text box, start typing the name of the member you want to add to the group.

The list searches as you type.

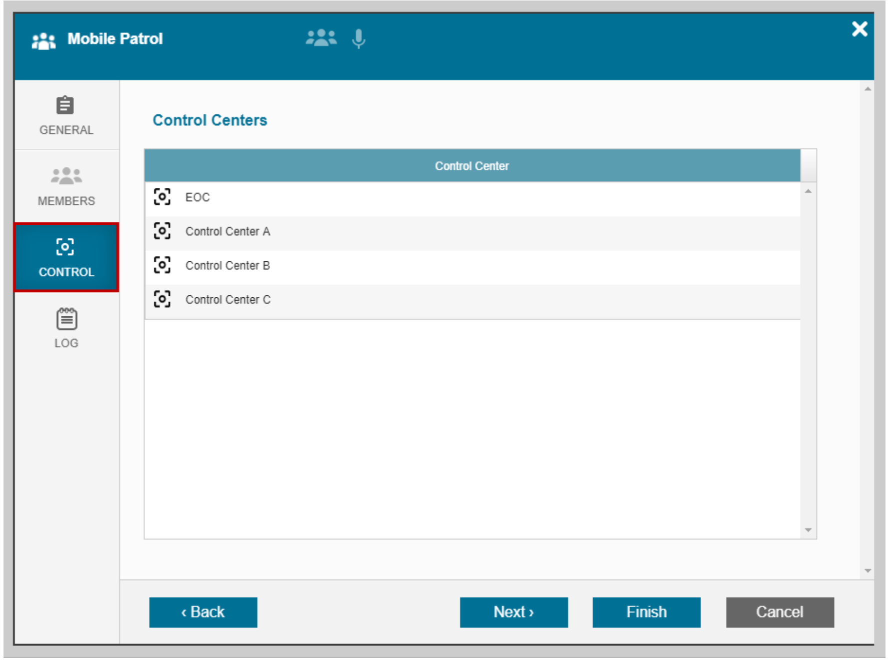


6. Select the desired name.

   The name is added to the list of members in the group. Repeat this procedure for all the users you want to add to the group. As you select each name, it is added to the list of members in the group.

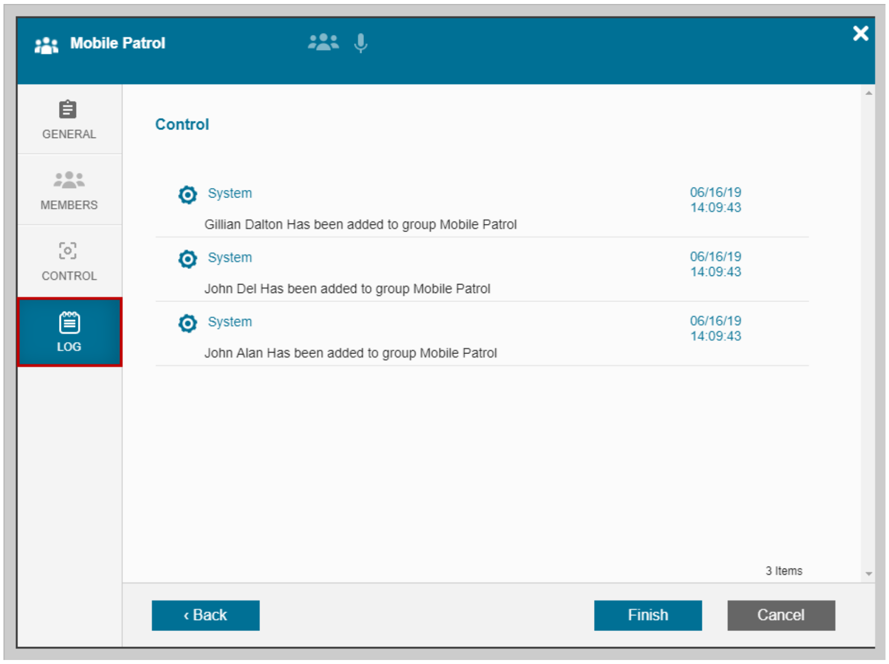


7. Click **Next**.



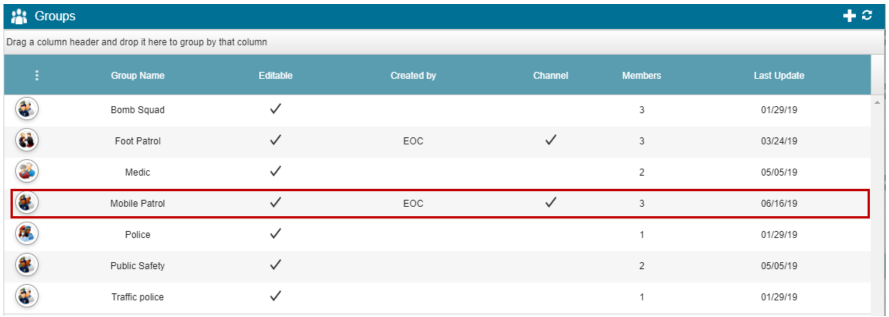
8. Click **Next**.

   The Log page opens showing a log with all the history and modifications of the group.



9. Click **Finish**.

   The new group is added to the list of groups.



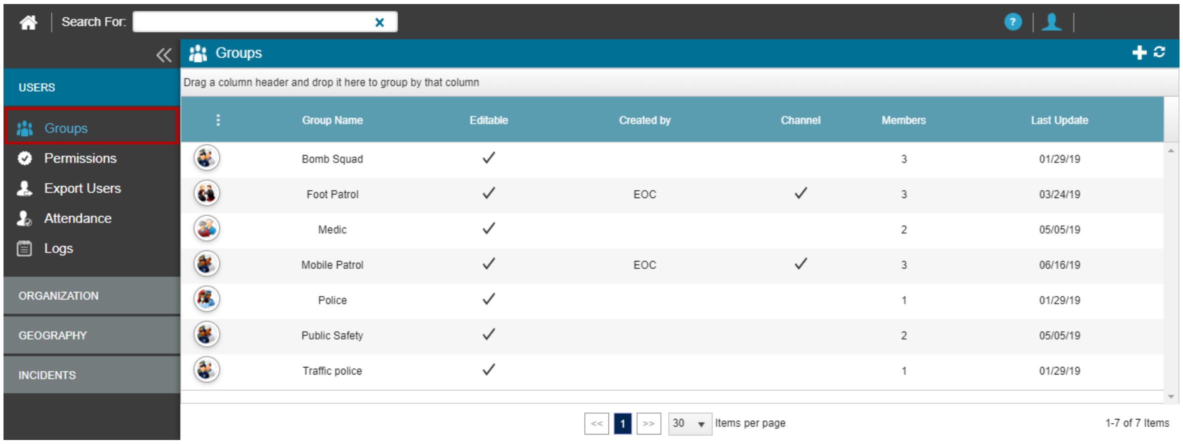
Editing and Deleting Groups

You can edit and delete groups in the **Groups** settings page.

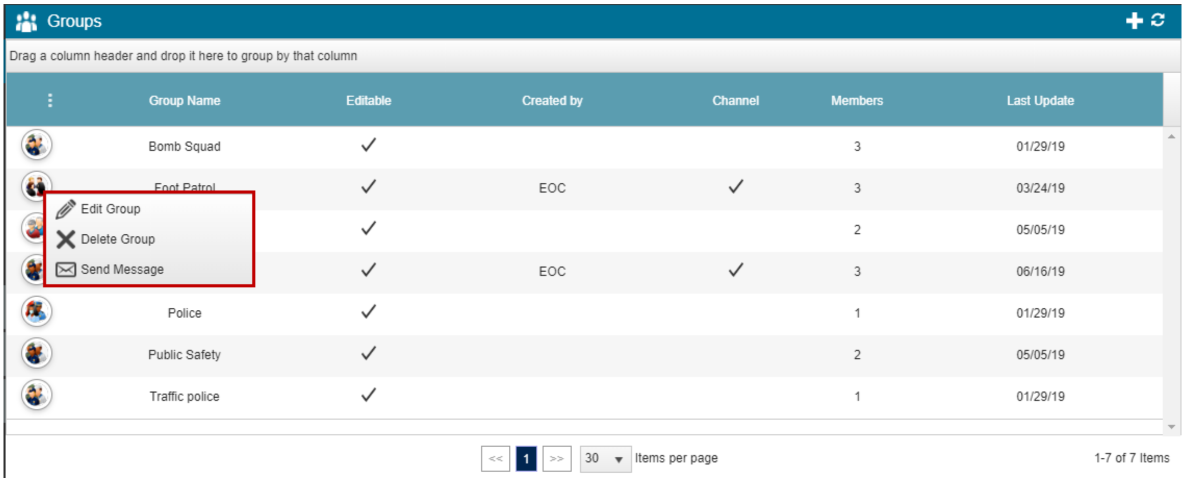
▼ To edit a group

1. On the **Main** screen, click **Settings** (gear)> **Groups** to open the **Groups** page.

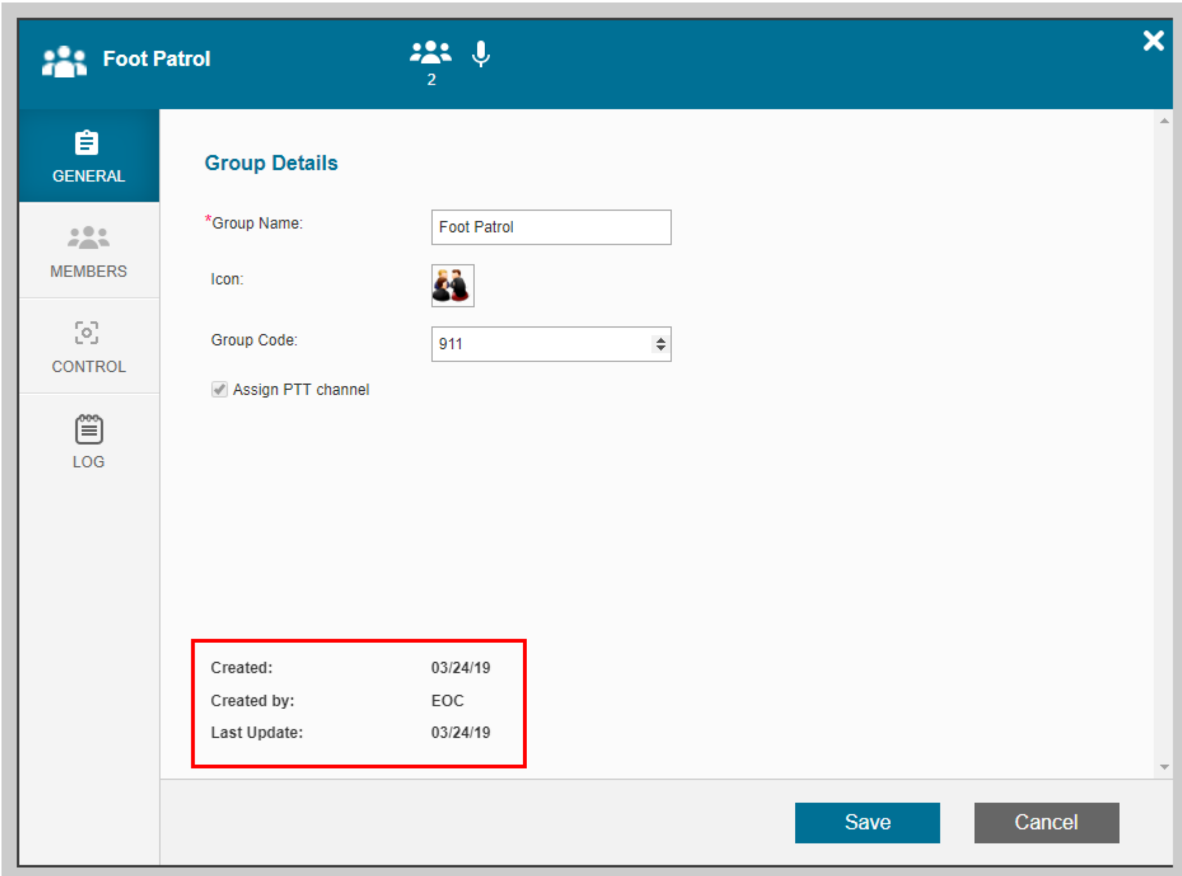
The **Groups** page opens.



2. Hover over the group you want to edit to show the **Action** menu for that group.



3. Click **Edit Group** to open the Group Management wizard.



4. Edit the information on the **General** or **Members** tab, as described in Creating New Groups.

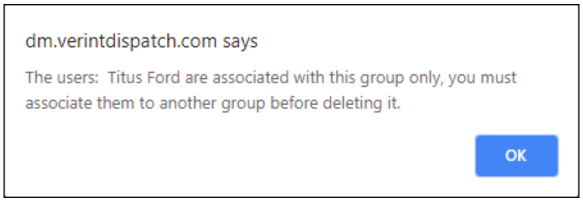
> Note
> Note: You can see technical information about the creation of the group at the bottom left of the General tab.

▼ To delete a group

1. Open the **Groups** page and locate the group you want to delete, as described above.
2. Click **Delete Group** to delete the selected group.

> Note
> You can only delete a group if all the members of the group are also members in at least one other group, since each user must be a member of a group.

If you try to delete a group that includes users who have no other group association, a message similar to the following message appears.



> Note
> Creating, editing or deleting groups can only be performed when you, the Administrator, is logged in to the main Control Center. Group Settings are not accessible in secondary Control Centers.

Configuring Units

The Units module enables organizations to link multiple users (unit members) together and manage them under one unified entity. Each individual unit inherits its attributes and behavior from the Unit Type settings (defined by the administrator) and from the settings of the specific unit.

For example, you can create a unit that would include users, vehicles, equipment specifically needed in mountain rescue. Therefore if there is an incident that involves mountain rescue, the dispatcher assigns this unit to the incident according to the Incident Dispatch Rules.

Currently the Incident is only dispatched to the Team Leader.

Enable the Support Units Feature in the Organization

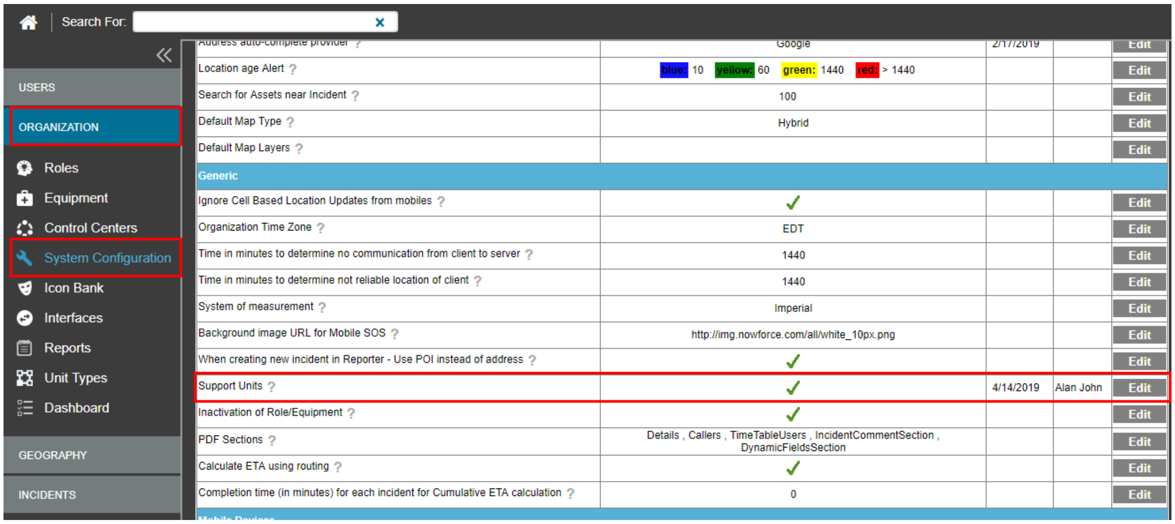
You must enable the Support Unit feature before you can define units.

▼ To enable the Support Units feature

1. From the **Main** screen, select **Settings** > **ORGANIZATION**, and then select **System Configuration**.

2. Scroll to the Generic section in the list of configurations.

   Confirm that Support Units is enabled.



3. If Support Units is not enabled, click **Edit**.
4. Select the **Support Units** check box.
5. Click **Save**.

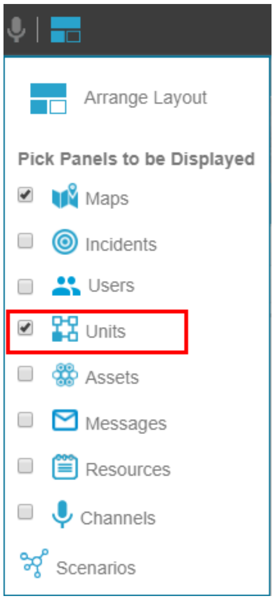
Defining Units

You define units in the Units panel.

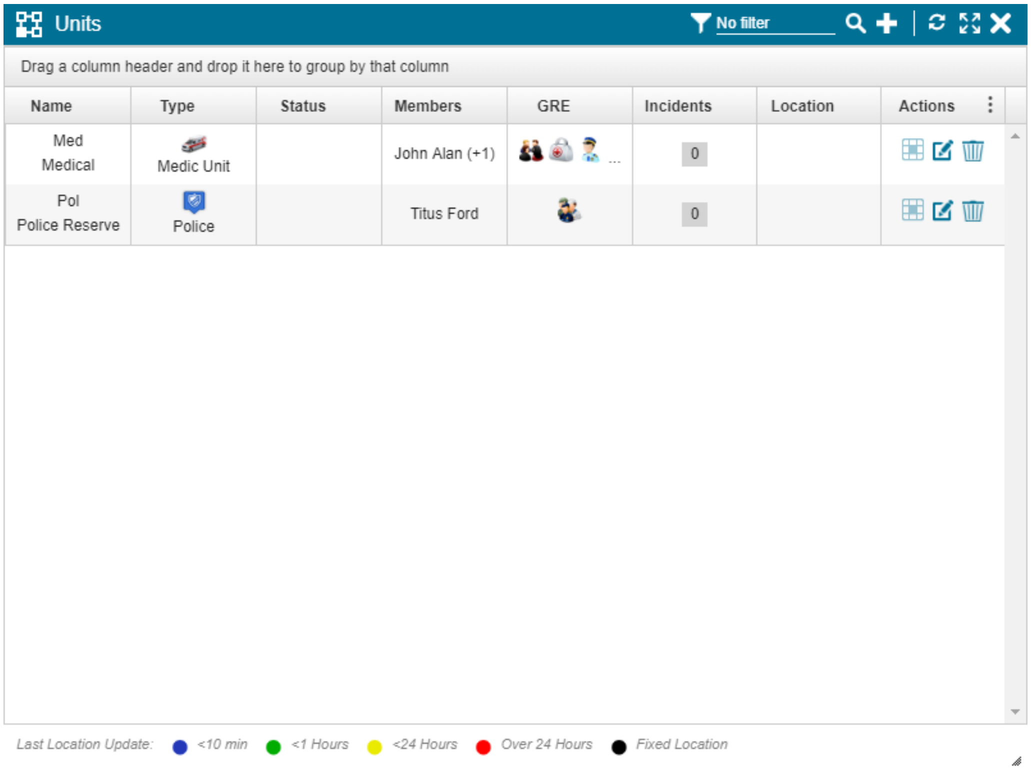
▼ To define units

1. On the Dispatcher toolbar, click the **Open Units** icon or the **Open Panels** icon to open the **Units** panel.

2. If you clicked the **Open Panels** icon, you must now select Units from the dropdown list.



The **Units** panel opens.

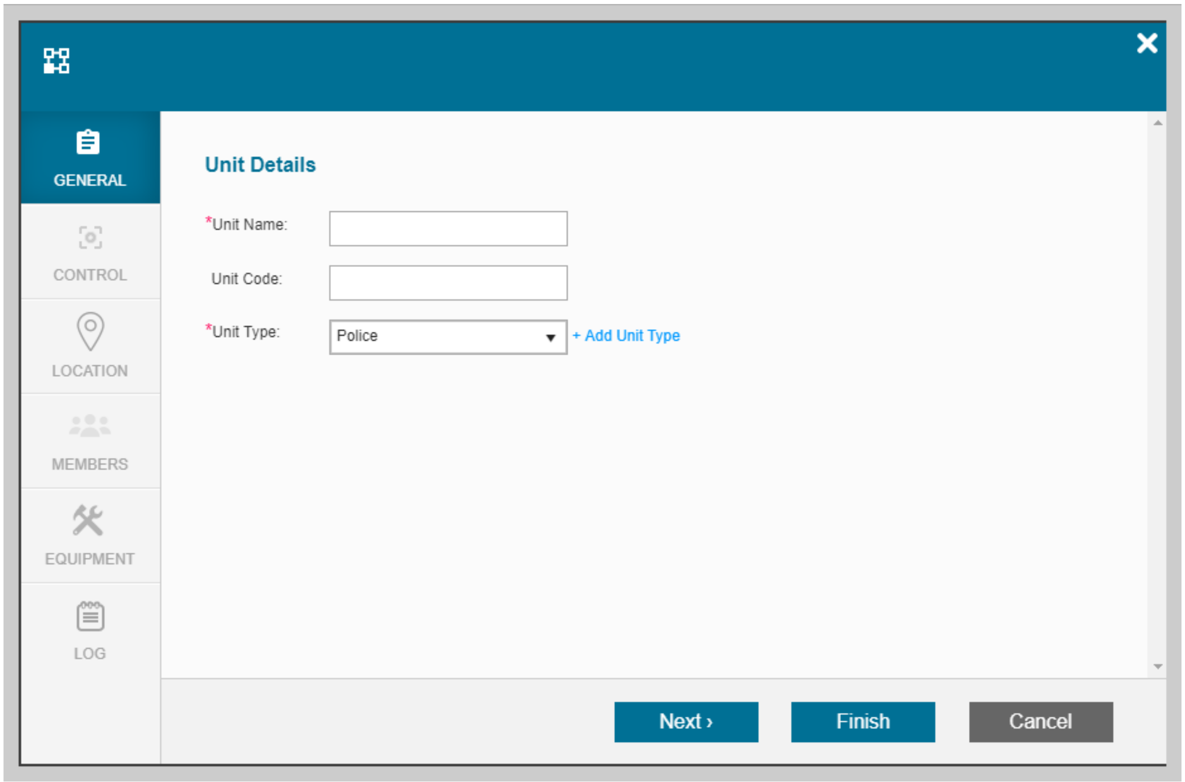


Adding New Units

▼ To add a new Unit

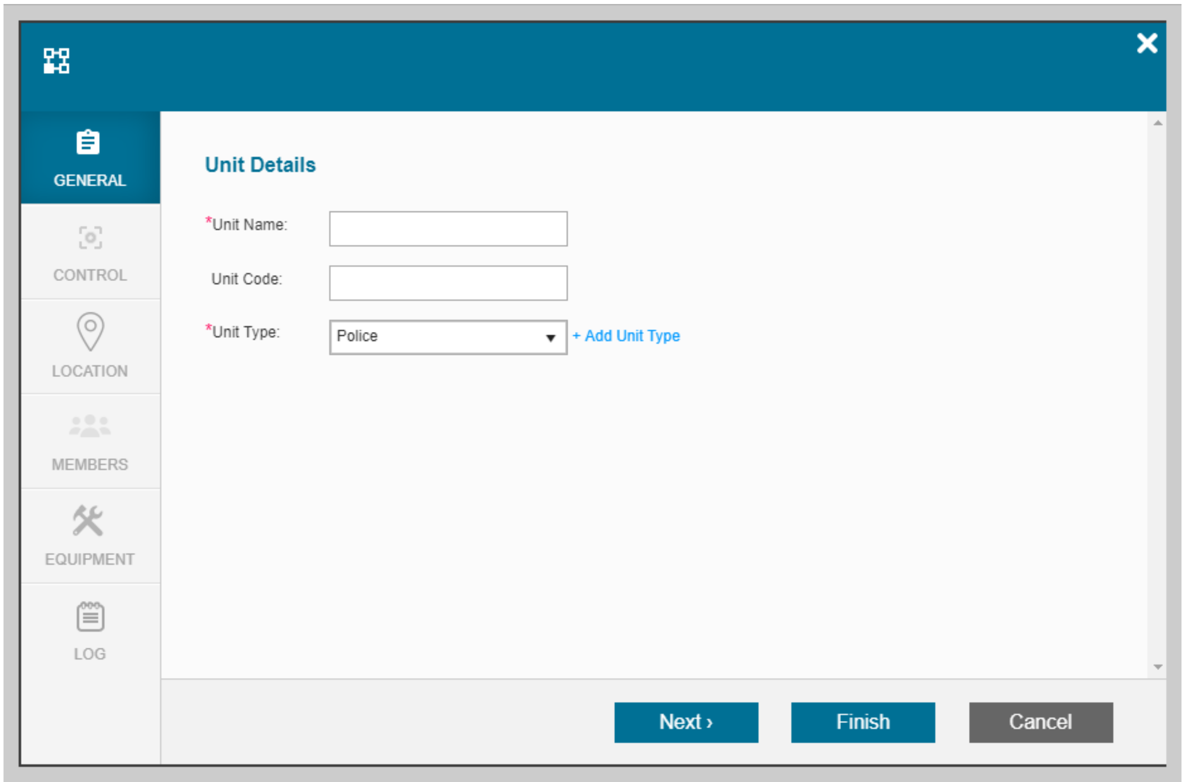
1. Click Add new unit from the toolbar.

The **Add New Unit** window opens.

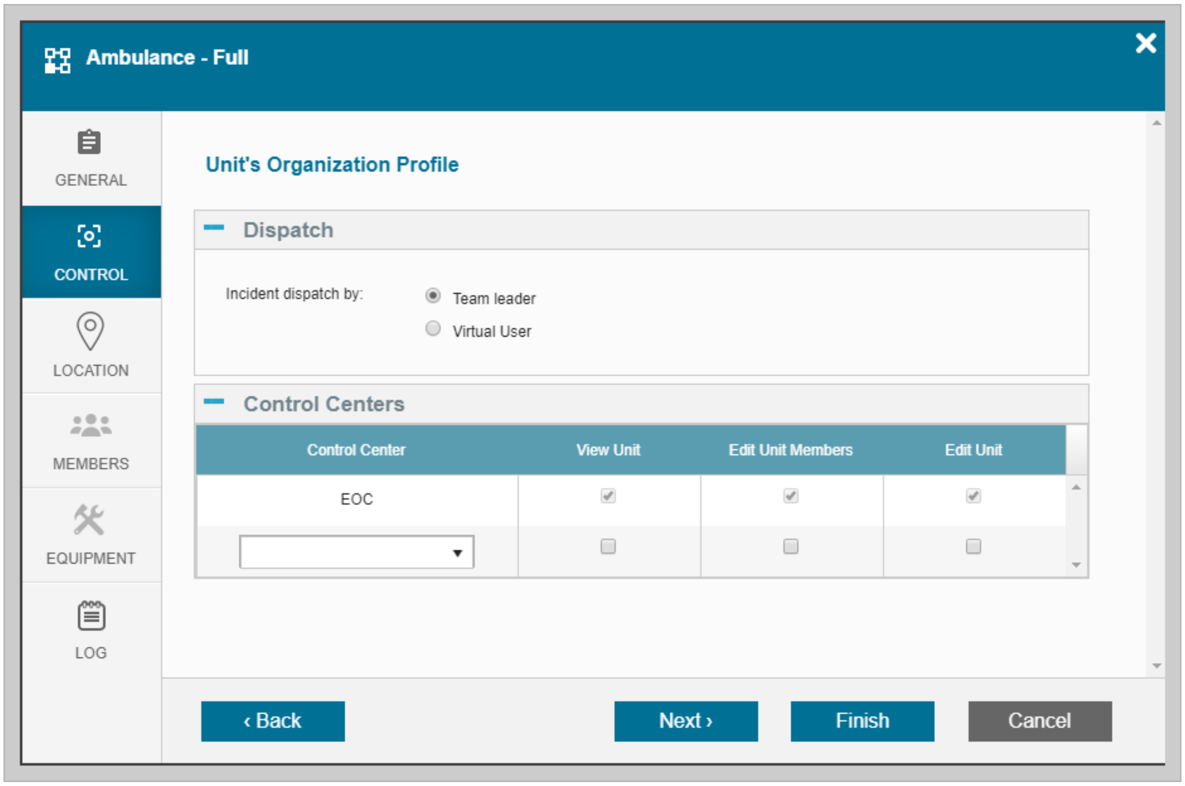


2. Enter the Unit Details as follows:
   - **Unit Name**
   - **Unit Code** (optional)
   - **Unit Type**: Select from the dropdown list.
3. Click Add new unit from the toolbar.

The **Add New Unit** window opens.


GENERAL
CONTROL
LOCATION
MEMBERS
EQUIPMENT
LOG
Unit Details
*Unit Name:
Unit Code:
*Unit Type:
Police
+ Add Unit Type
Next ›
Finish
Cancel

4. Click **Next**.



5. In the **Dispatch** area select if you want the unit to be dispatched by a **Team leader** or by a **Virtual user**.
6. In the Control Centers area, select the Control Centers in which the unit appears as well as the actions that the Control Center can perform (**View Unit, Edit Unit Members**, and **Edit Unit**).
7. Define how the system determines the location of the Unit by selecting **Location Identifer** either Team Leader of AVL from the dropdown.

> Note
> Contact NowForce Support for assistance for AVL installation.

8. Set the expected **Movement Pattern** by selecting one of the folllowing:
   - **Static Post** - for a static unit, such as guard or guarding tower at one fixed post.
   - **Route** - for a unit expected to follow a route of two or more locations (way-points).
   - **Free Movement within Geofence** - for a unit or team expected to move freely as long as it doesn't exit a geofence.

> **Note**
> For each movement pattern the system allows to define thresholds (in time of distance) that will trigger alerts for units not adhering the the planned movement pattern.

9. Add users as members to the unit by entering the username in the **Unit Member Name** open field.
10. Click **Save**.

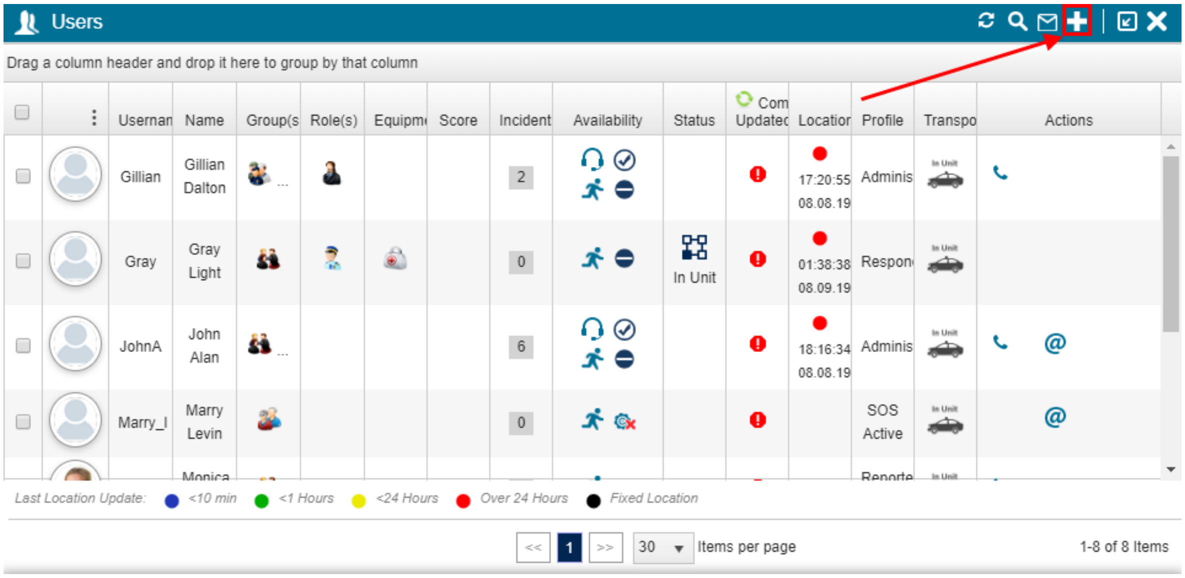
> **Note**
> - The Unit will be associated with the roles and equipment of it's user members or directly with equipment that the unit is configured with.
> - The Dispatcher Incident Rules will use these unit associations for dispatching the Unit to Incidents.

Adding and Managing Users

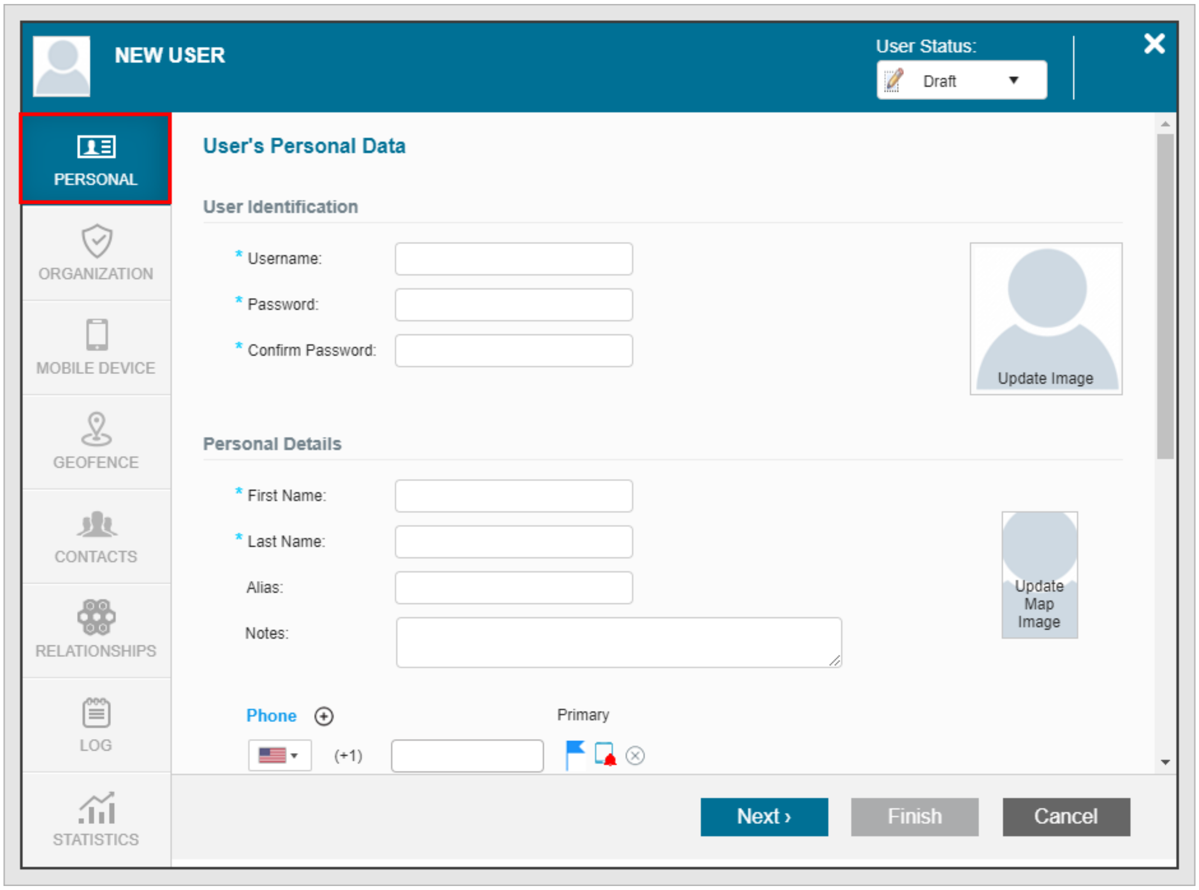
You add and manage users in the Users panel on the Dispatcher home screen. Use the search bar to help you manage your user list.

▼ To add a new user

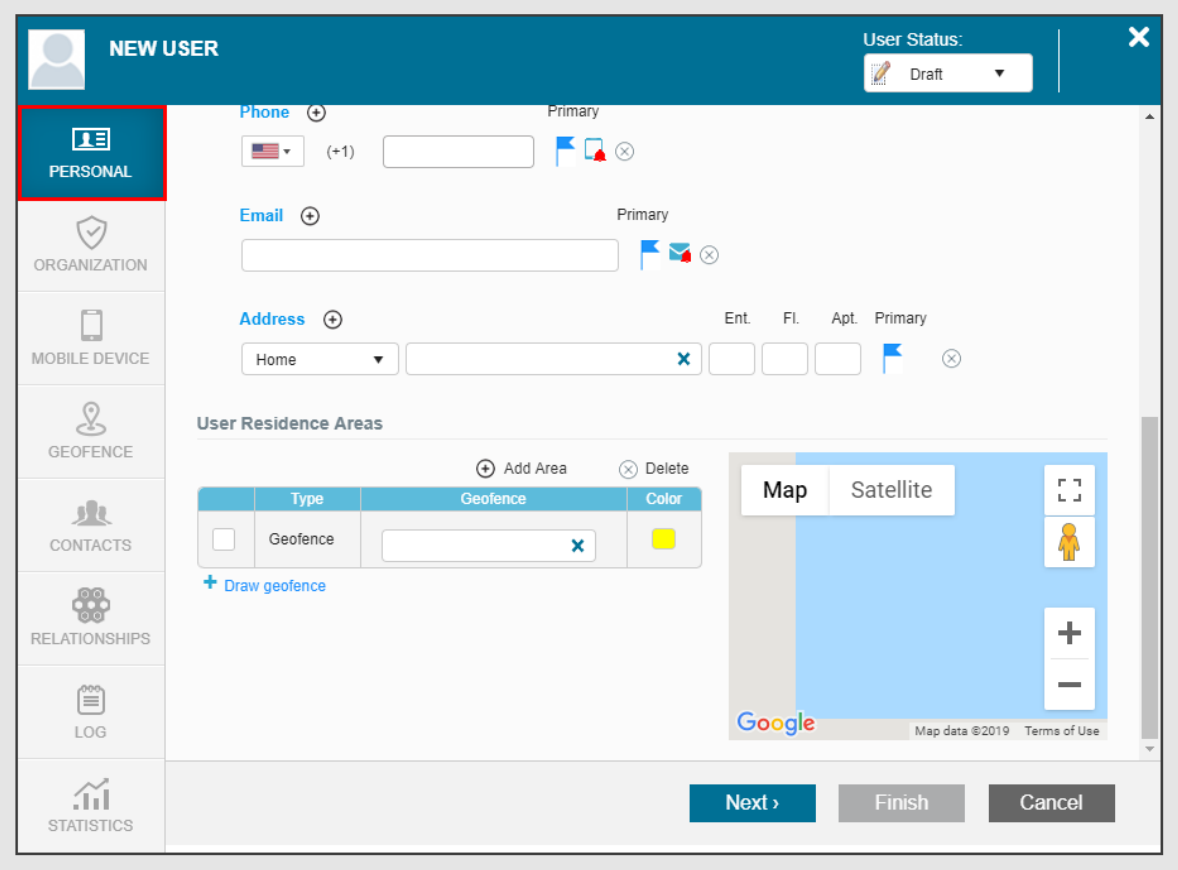
1. From the **Users** panel, click 



The **New User** window opens.



2. Scroll down to view the lower part of the **New User** window.



3. Enter the user details in the respective fields, and click **Next**.

   The **Organization** tab appears.

> Note
> The fields marked with an asterisk are mandatory. You cannot proceed to the Organization tab if these mandatory details are not entered.

A description and instructions on how to complete each tab in the New User window is provided in a separate sections below.

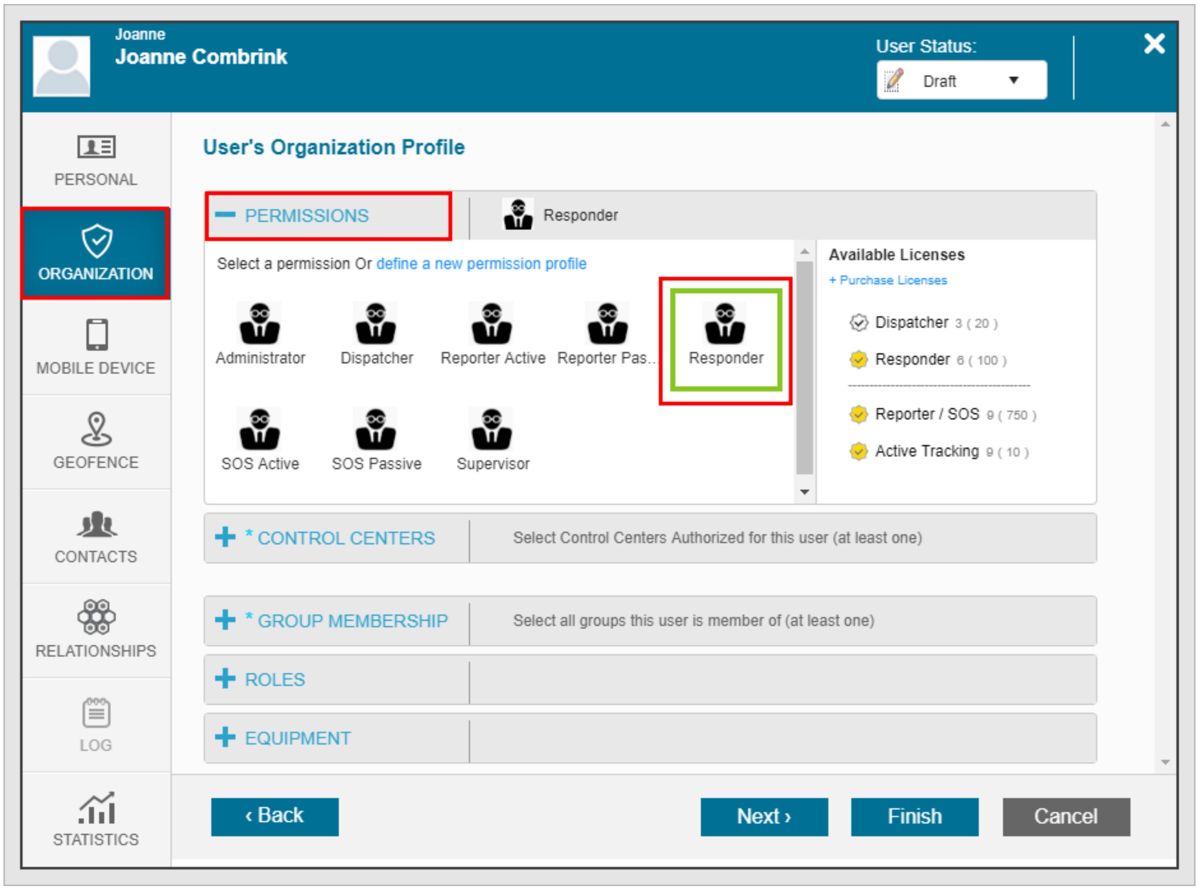
Organization Tab

Permission profiles determine the access that each user has to specific functions in the Dispatcher and on their mobile devices. You assign each user to a permissions profile and based on that profile. The user can see different aspects of the Dispatcher or mobile application and enable them to perform the different functions according to their assigned permissions. There are three default permission profiles: Administrator, Dispatcher and Responder.

Each of these can be modified according to the specific requirements of the organization, and you can also add new profiles.

▼ To complete the organization tab

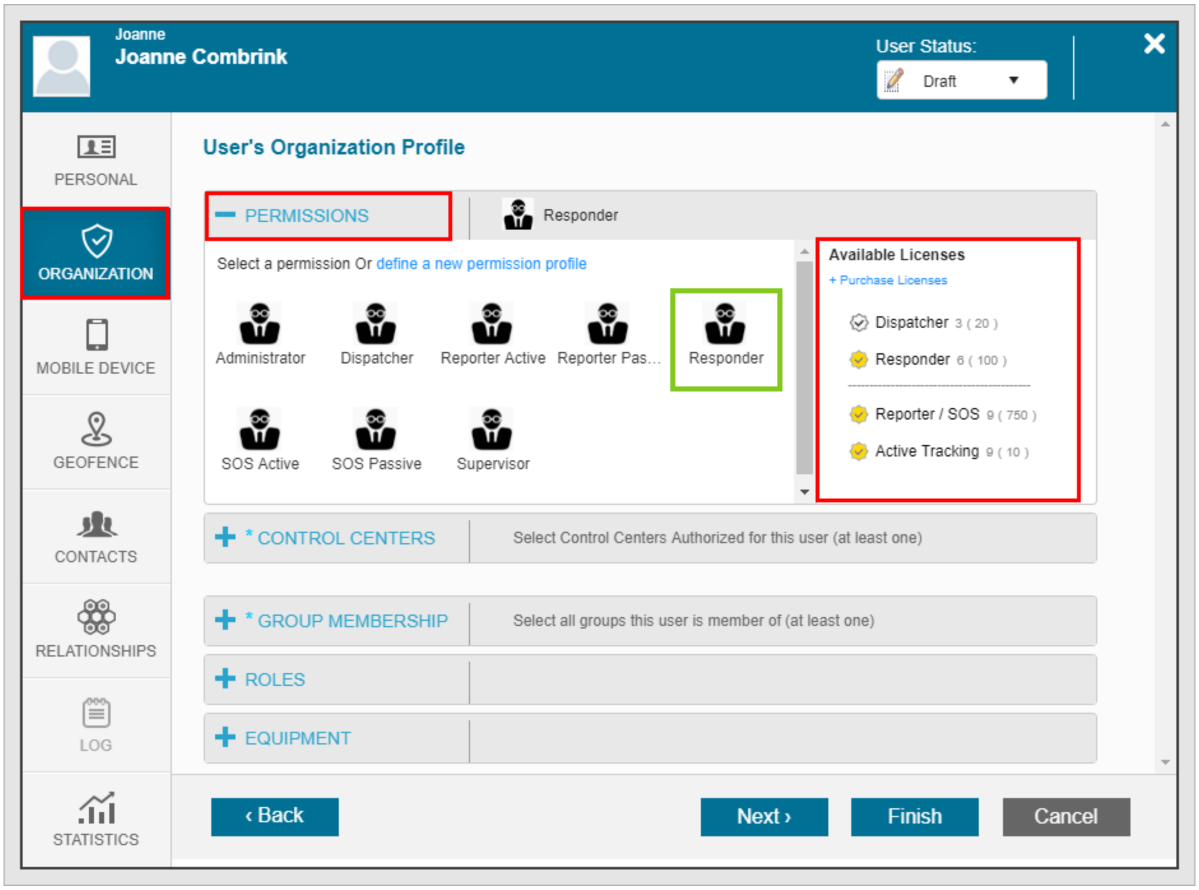
1. Select the permission profile for the new user in the **PERMISSIONS** sub-tab.



In this example, we are adding a Responder user, if you want to add a new Dispatcher you will need to assign them to a Control Center in the **Control Center** sub-tab.

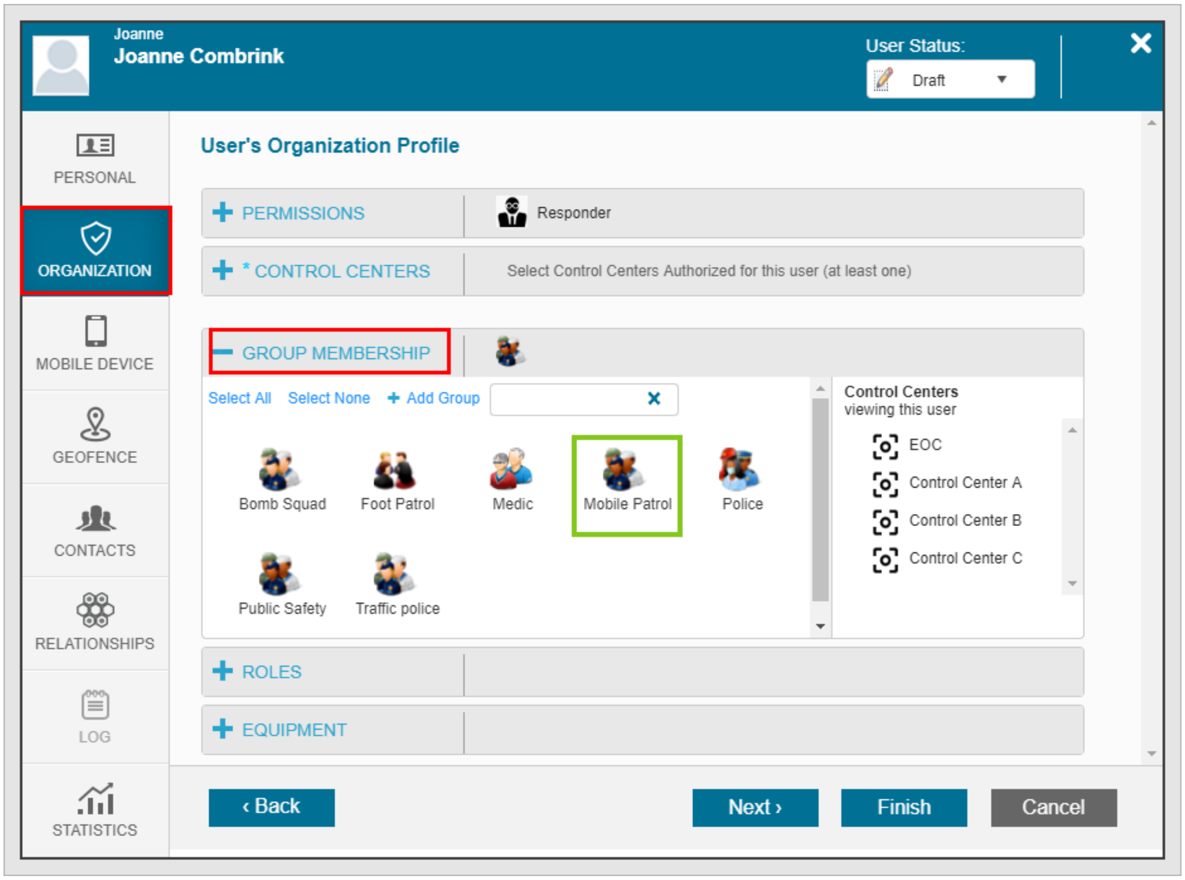
Read about how to assign dispatchers toControl Centers.

> Tip
> On the right side of the panel in **Available Licenses** you can see the number of licenses your organization uses for each permission.



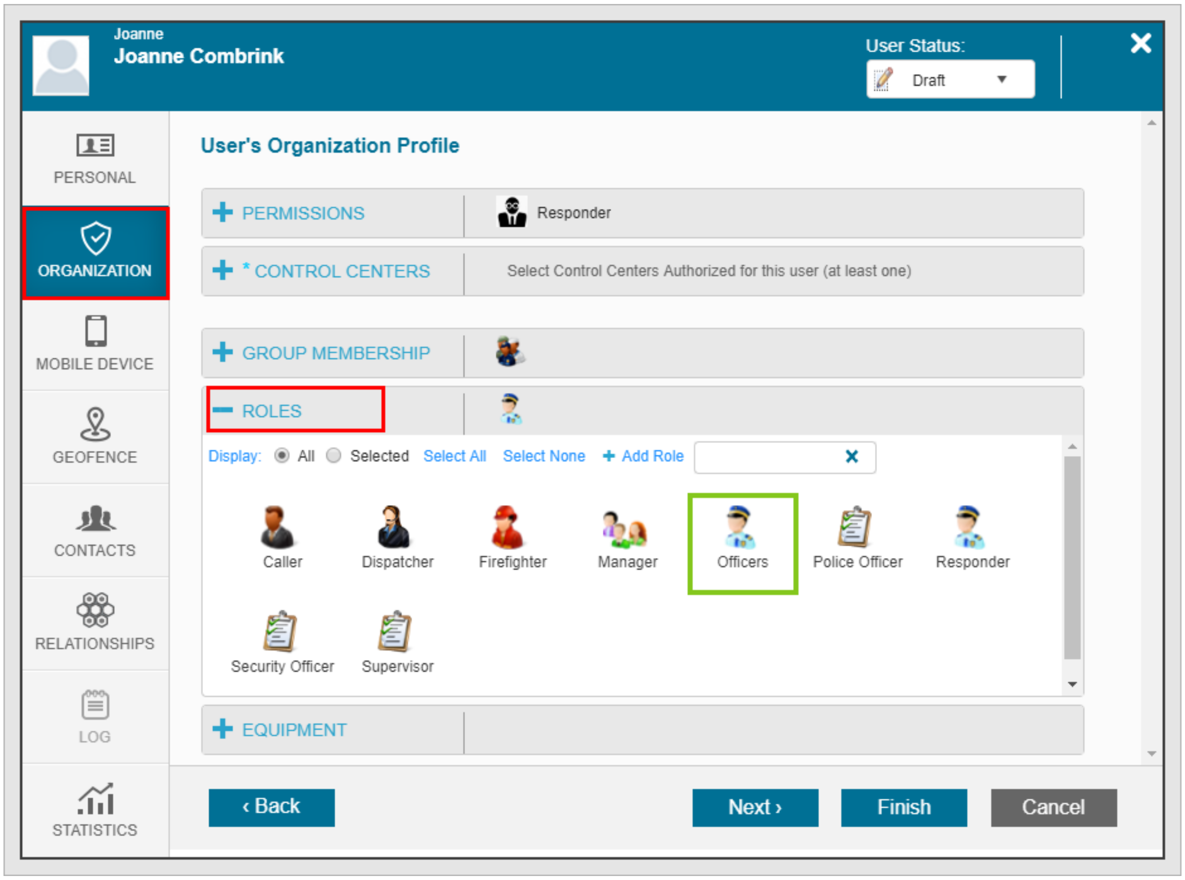
2. Click the **Group Membership** tab and choose the group you want to use.

   If required you can create a new group using the **+ Add Group** button.



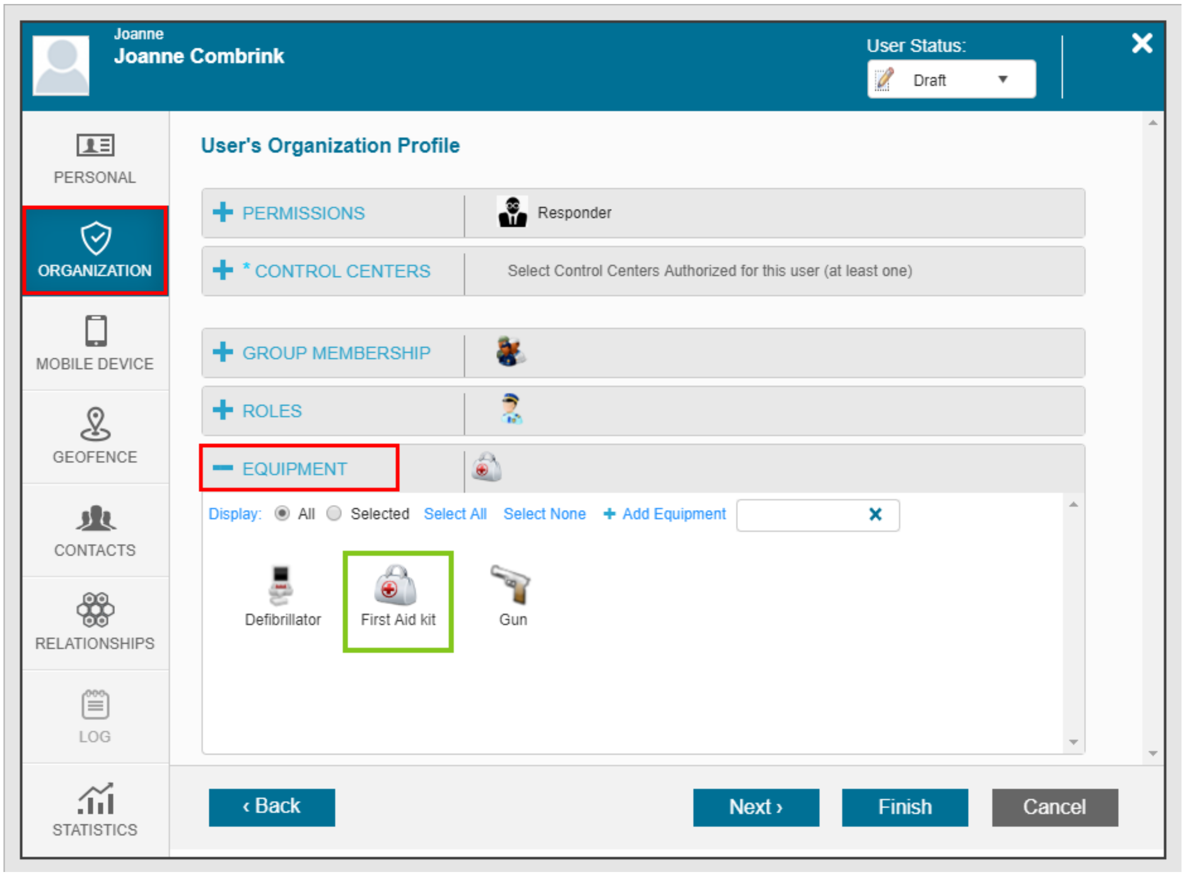
3. Click the **Roles** tab, and choose the roles you want to use.

   If required you can create a new role using the **+ Add Role** button.



4. Click the **Equipment** tab, and choose the kind of equipment the user has.

   If required you can add new equipment using the **+ Add Equipment** button.

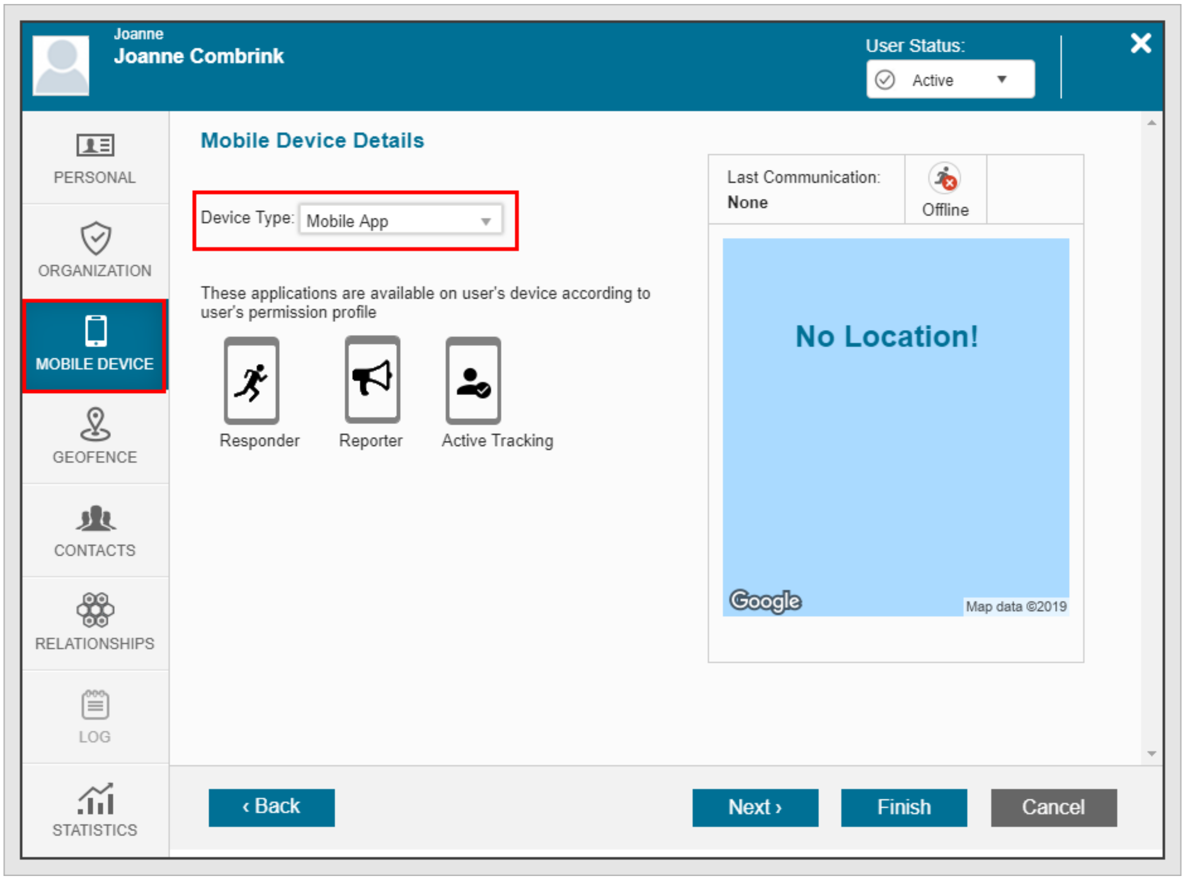


5. Click **Next** to open the **Mobile Device** tab.

Mobile Device Tab

1. Click the dropdown and select **Mobile App**.

   The Mobile Device tab enables you to see the App type based on the users permission profile. On the right side of the panel you can see the last communication status with the user. As this is a new user, no location is shown as the user has not connected yet.



2. Click **Next** to open the **Geofence** tab.

Adding Geofences

You can configure geofencing by creating personal polygons for the user that define areas on the map that are associated with that user.

You can connect personal polygons to certain incident types, to be triggered when a user enters or exits a personal polygon.

▼ To configure geofencing

1. Click the **+** to add a geofence.
2. Use the dropdown menus to add alerts for when the user enters/exits a polygon.

> Note
> An alert on a Geofence sends an SOS call for the dispatch operator whenever triggered.

Contacts

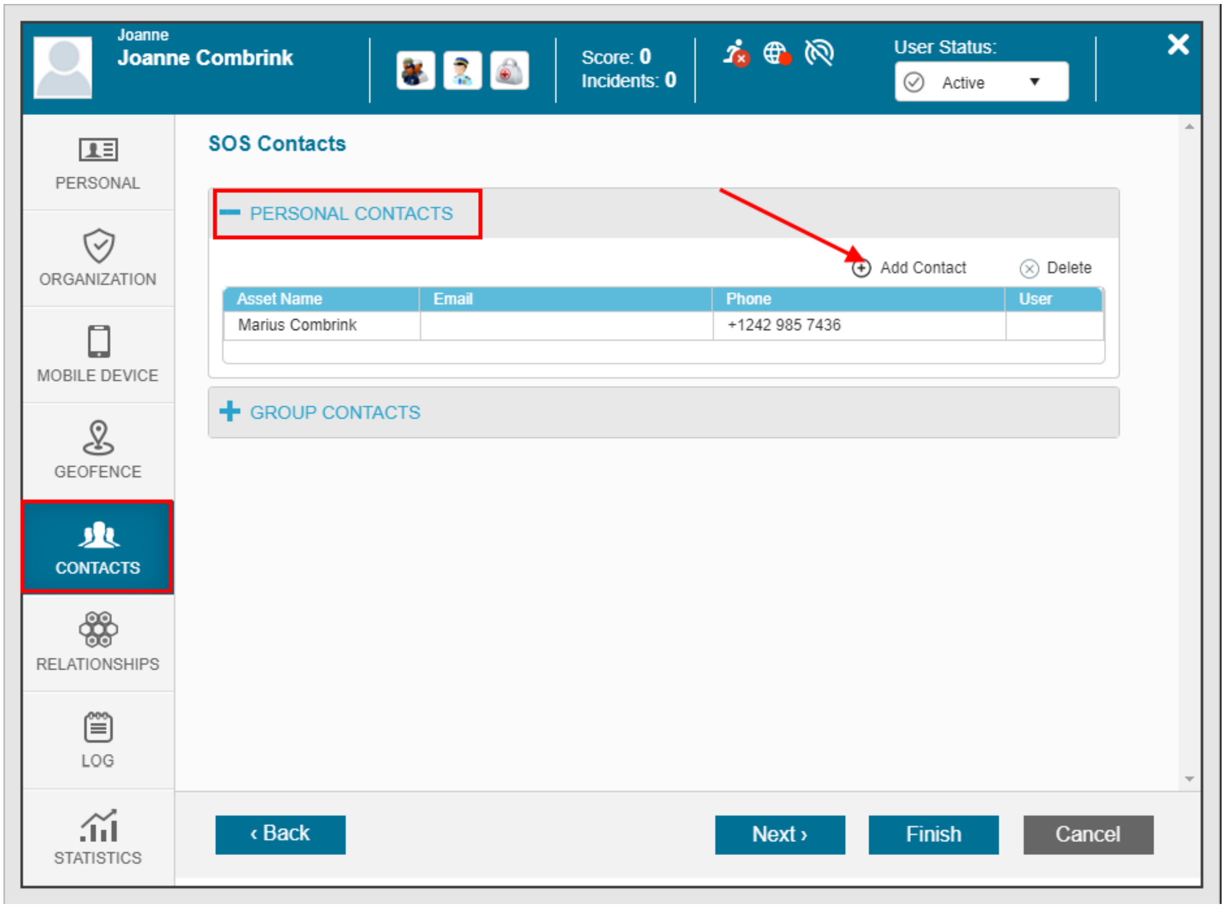
Adding Emergency (SOS) Contacts to a User

When a user activates an SOS call from the mobile application, it creates a new incident in the Dispatcher, and activates the organization's emergency response protocols.

> **Note**
> - If the user has emergency contacts listed, these contacts will be notified via SMS or email.
> - You can configure emergency contacts for each user in Dispatcher.

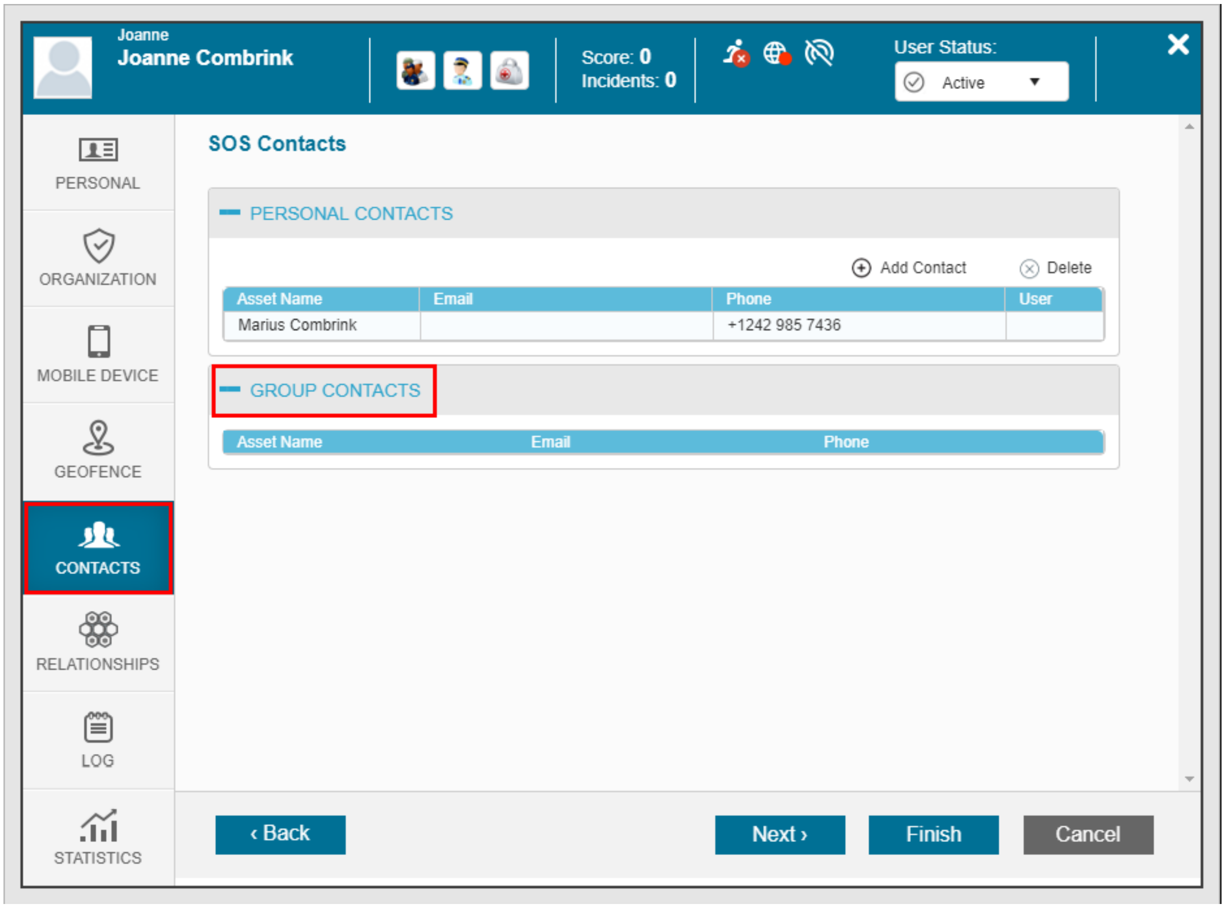
▼ To add personal contact

1. In the **PERSONAL CONTACTS** sub-tab click **Add Contacts** to add new personal contacts for the user.



Adding Group Contacts

To manage this contact list you must open the groups settings, read more about [managing groups](#).



2. Click **Finish** to save the new user details.

Read more about disabling and reactivating users.

Exporting User Details

You can export user details into an Excel file using the export feature in the User Panel.

▼ How to download User details to Excel

1. Open the User Panel.
2. Select the Excel icon on the task bar to export the displayed contents of the User Panel.

> **Note**
> The export function works on the currently displayed page in User Panel page. To download other pages in the User Panel toggle using the arrow keys to the required page and click Export.

Configuring and Applying User Update Settings for Policies

User Updates (UUs) are a simple and versatile tool for user-system interactions and for triggering user-related processes. The intuitive User Update interface combined with its ability to connect with multiple system functions make it a powerful tool.

User Updates can be accessed in the mobile app with a tap on a button, they may include a simple 2 word title, a text update or a responsive form. The update can be set to include the users' location and an update alert. All UUs are registered to the User's log as time tagged log entries. Historical User Updates can be searched for investigation in the User Panel.

User Updates can be sent the individual user via the mobile app or by the operator (via Dispatcher) or by a third party system (via API). User Updates can also be set to impact other operational processes (such as Policies) or even trigger events in external systems (like access control). User Updates are a simple and at the same time a powerful tool in your NowForce system.

The following are covered in this section:

- Describing the User Updates settings and how the administrator can define and modify behavior of User Updates.
- The role User Updates play in the Policies framework.

> **Note**
> User Updates are available for all mobile licenses from Monitored Reporter and above.

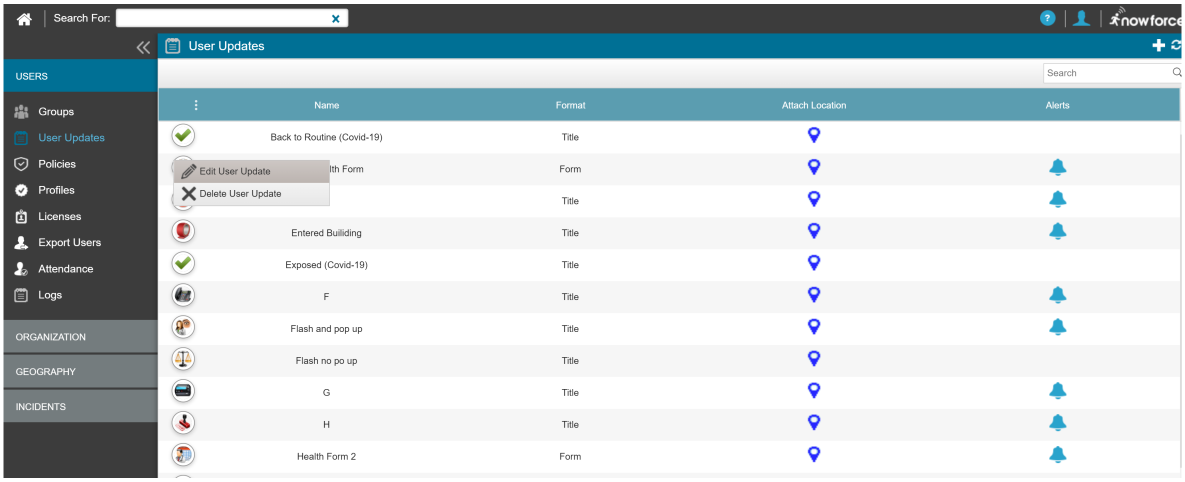
The monitoring user-system interactions are detailed in the *Symphia NowForce User Guide*.

Viewing the User Updates Settings

The administrator can view and edit User Updates in the Settings.

▼ To view the User Update settings

1. Click **Settings** (gear) in the upper left corner of the **Dispatcher** screen.



2. Click **USERS**>**User Updates**.
3. Hover over an Update's icon, select **Edit User Updates** to edit that Update.

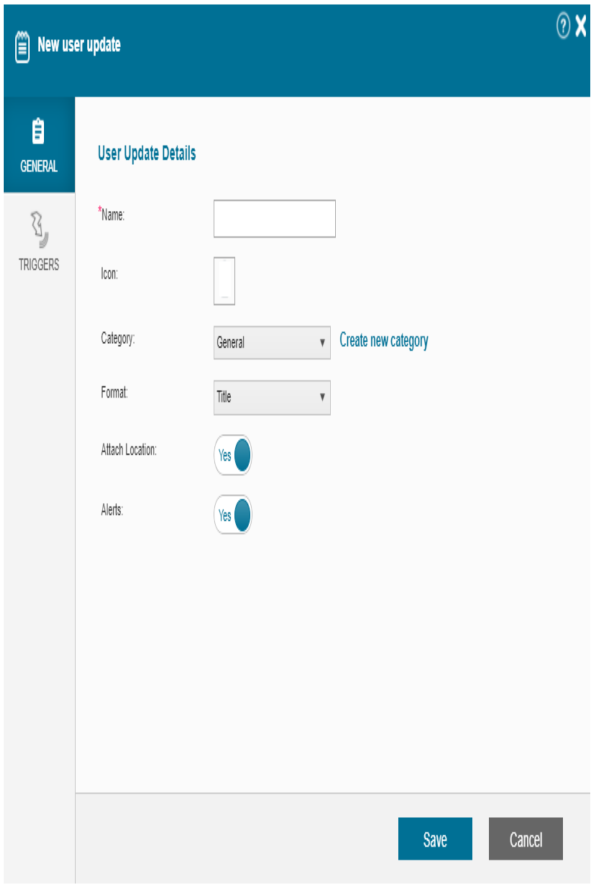
Administrators can create new User Updates.

▼ To add a new User Update

1. Click **Settings** (gear) in the upper left corner of the **Dispatcher** screen.

2. Click **USERS**>**User Updates**.

3. Select the **+** to add a new update.

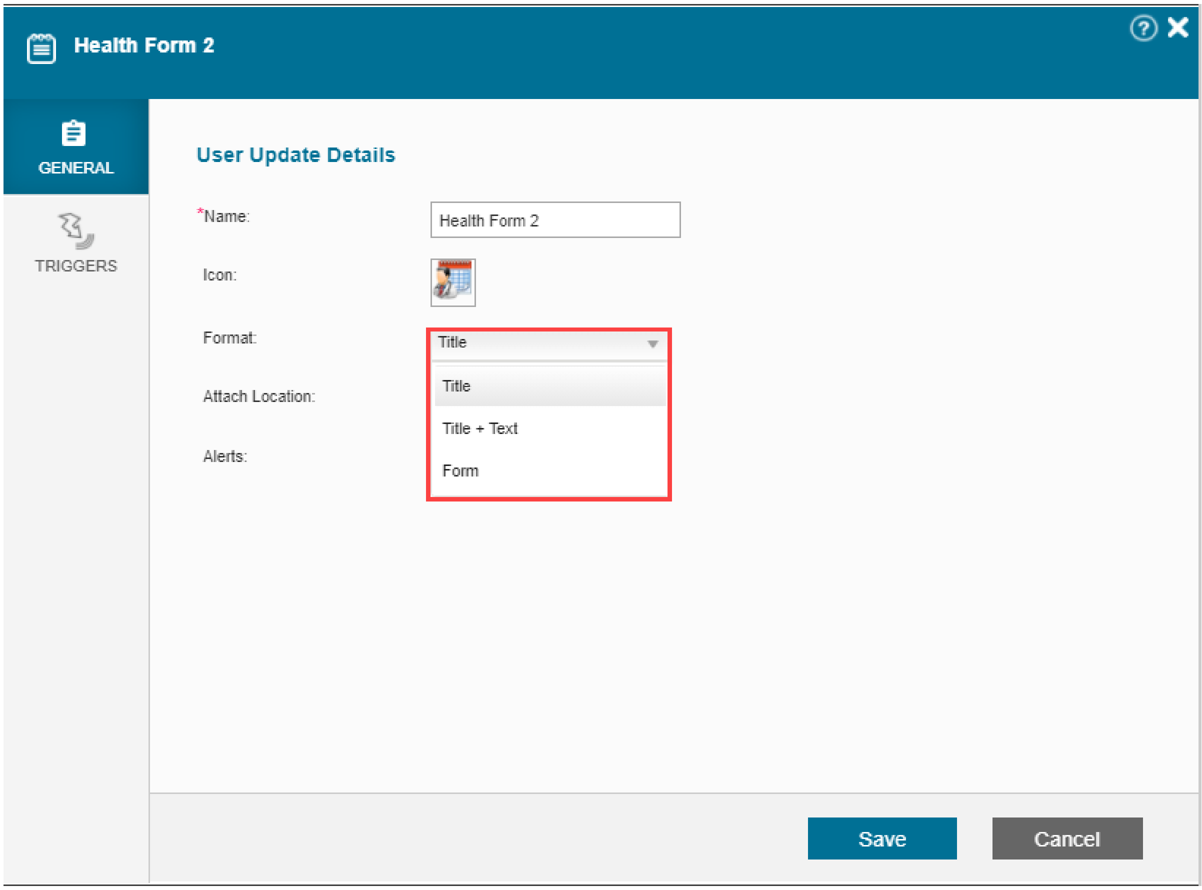


4. In the General tab, enter a **Name** in the field.
5. Select an **Icon** from the list.

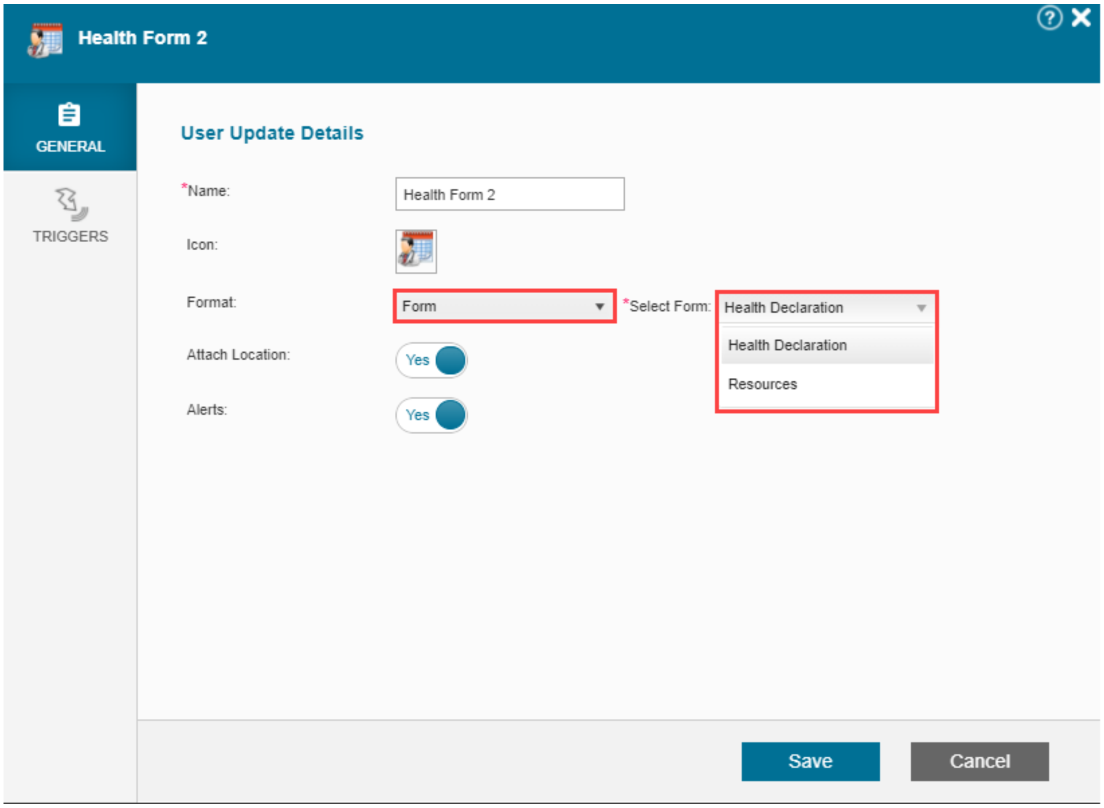
> Note
> You define icons in the Icon settings page.

6. Select a **Category** from the dropdown.

> Note
> Click **Create new category** to create new categories.



7. Select the **Format** of the user update from the list:
   - **Title only** - This is the simplest format. The mobile user will only have to click the title button to send a User Update.
   - **Title + Text** - This format allows the user to attach text to the update.



- **Form** - This is a format permits the administrator to design a form that will be attached to the user update. If **Form** is the option selected, then also select a **form type** from the **Select Form** dropdown. See "Creating and Editing Form Templates" (page 132).

8. Attach **Location** by toggling the switch to **Yes**. This option will attach the user's location to the UU. This means the app location will be saved to the user's location history.

> Note
> This option will upload a single user's location also for Monitored Reporter licenses that do not upload app locations routinely.

9. Attach **Alerts** by toggling the switch to **Yes**. This option will trigger an alert on the operator screen every time a user sends the user update.

> Tip
> It is recommended to activate the alert only for unique important updates to ensure routine alerts do not flood the system.

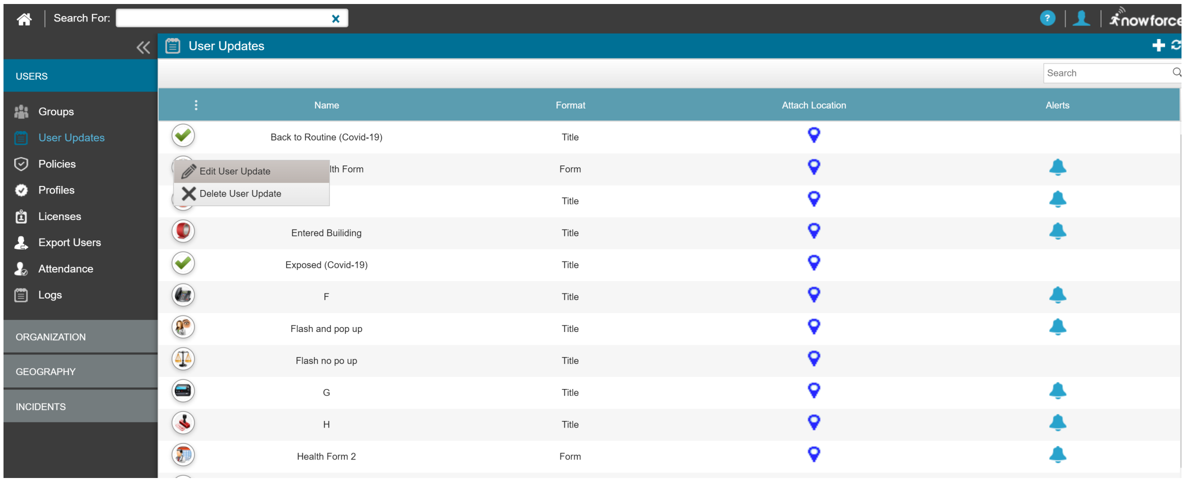
10. Click **Save**.

Applying User Updates in Policies

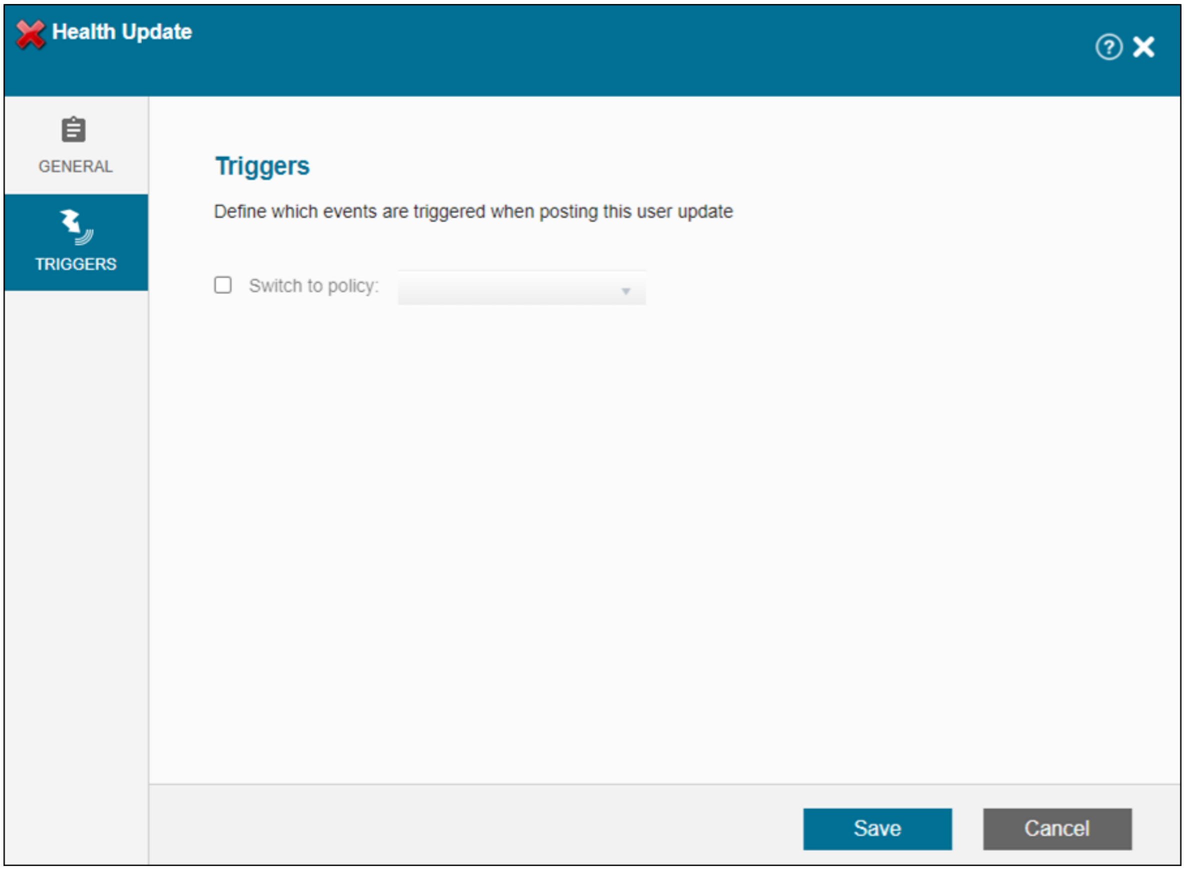
User Updates are one of the logical triggers that define a user's transition from one policy to another, for more information about transitioning in Policies see the NowForce Policies Guide.

▼ To apply a User Update as a transition trigger in a Policy

1. Click **Settings** (gear) in the upper left corner of the **Dispatcher** screen.



2. Click **USERS**>**User Updates**.
3. Hover over an Update's icon select **Edit User Updates** to edit that Update.
4. Select the **Triggers** tab.



5. Click the checkbox and select the required policy from the **Switch to policy** list.
6. Click **Save**.

Read more about "Creating and Editing Form Templates" (page 132)

Read more about Policies.

Geography Infrastructure Settings

Geography settings set the parameters for your organization's geofences, Control Center jurisdiction, points of interest, user and incident management and the visual display in the map module. In addition, these configurations support several specialized add-on features.

Creating and Editing Geofences/ Areas of Interest (AOIs) 64
Adding and Managing Points of Interest (POIs) 70
Importing Batch POIs 73
Setting Default Map Center and Zoom Level Preference 74

Creating and Editing Geofences/ Areas of Interest (AOIs)

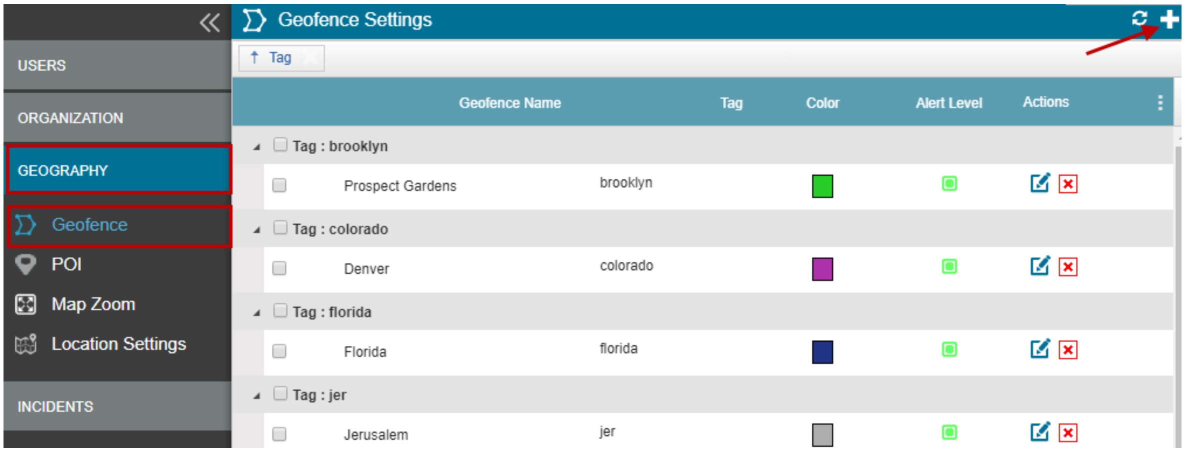
Geofences are polygons (closed shapes) drawn on a map, identifying an area of interest (AOI). Specific jurisdiction related data like resources, incidents, log of activities and alerts can all be attributed to an AOI.

To create and edit a geofence, your Permission Profile settings under Advanced Settings must be selected for Add/Edit Areas of Interest. For more information on editing and adding User Permission Profile Settings click here.

▼ To create a geofence

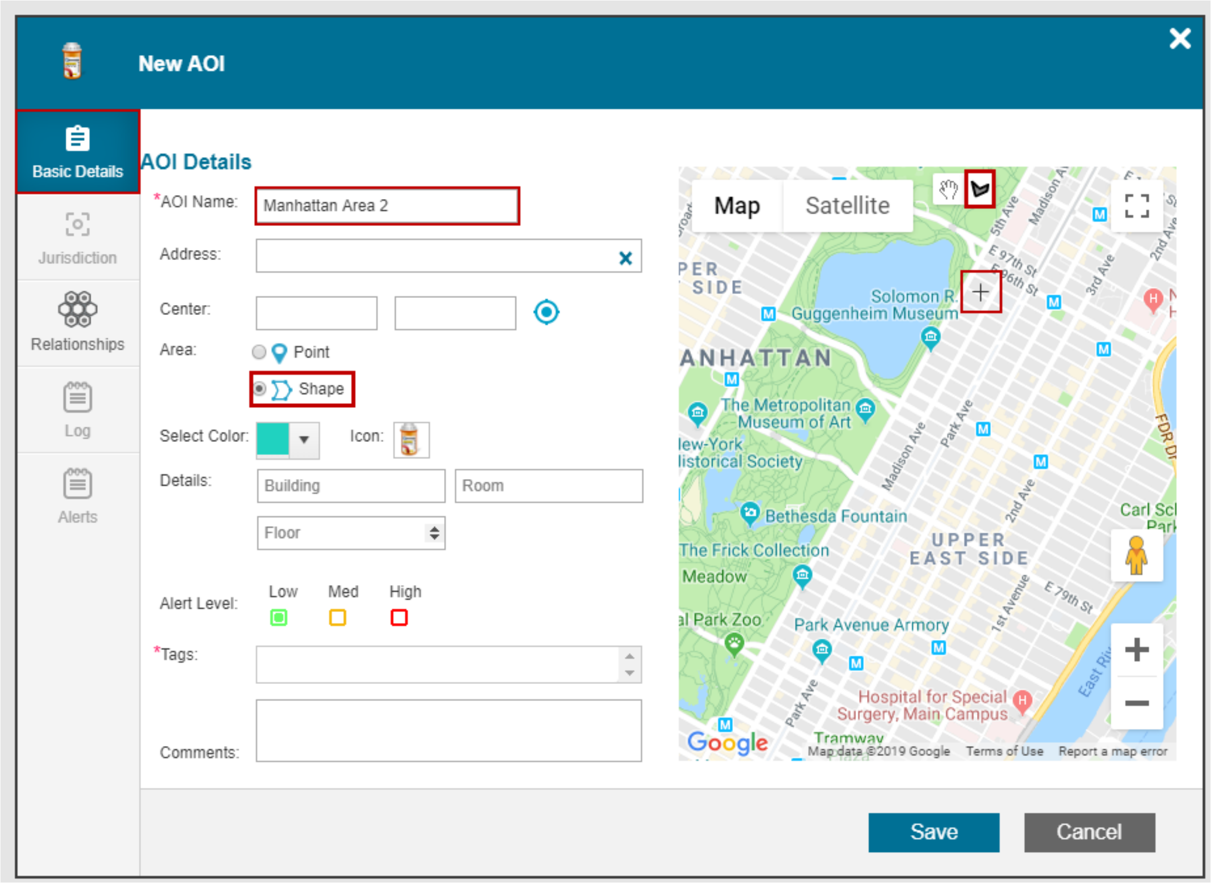
1. From the **Main** screen, select **Settings** > **GEOGRAPHY**, and then select **Geofence**.

The Geofence Settings table opens.

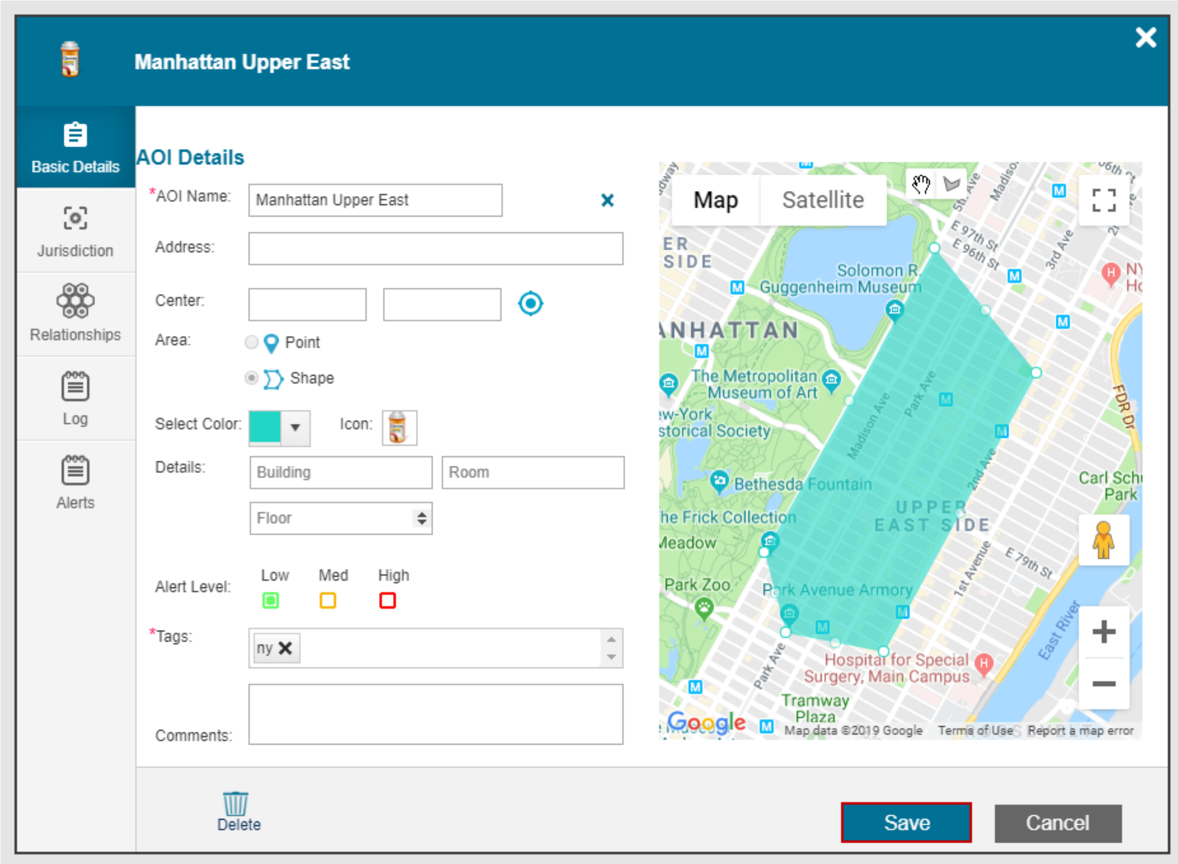


2. Select the **+ Add New Geofence** icon.

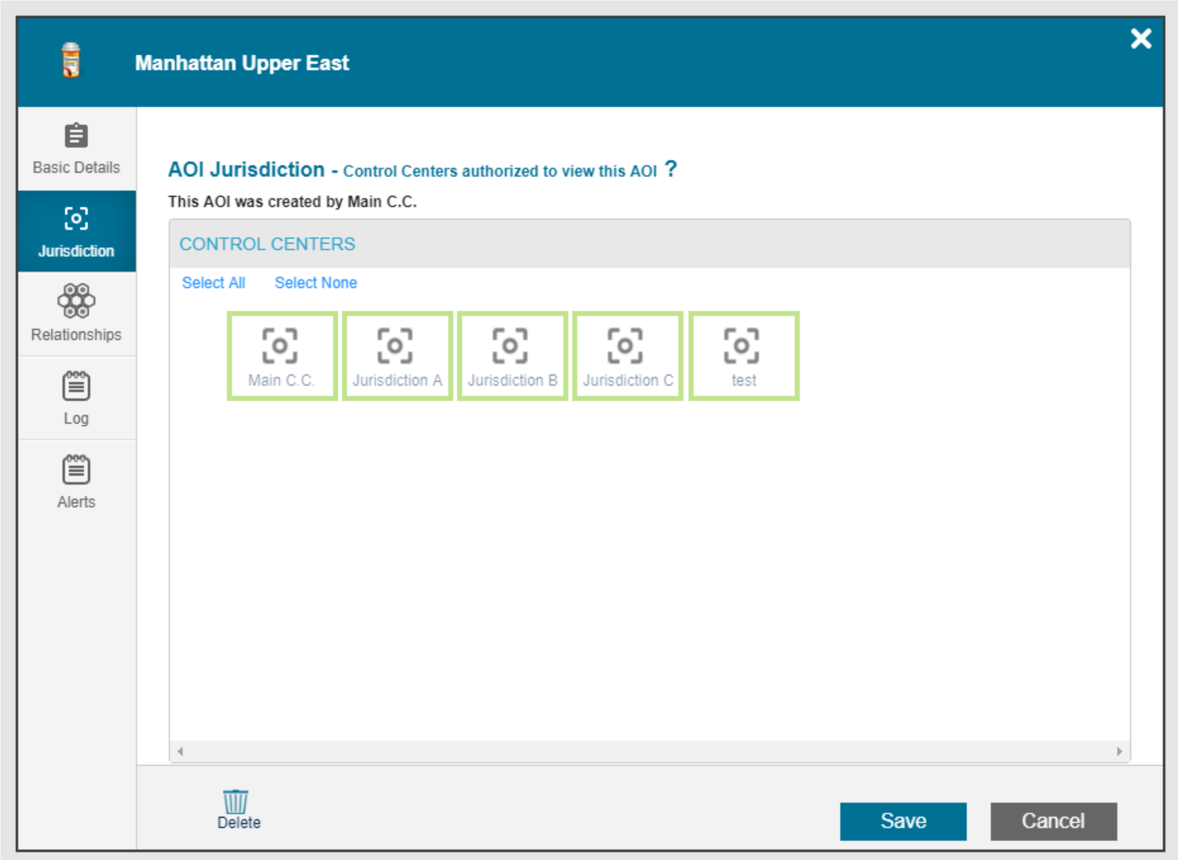
   A New **AOI** window opens. Default view is the **Basic Details** tab.



3. Insert the name of the new geofence in the **AOI Name** field.
4. Ensure that the Area option **Shape** is selected.
5. Select the **Draw a Shape** icon on the map. A **+** appears on the map.
6. Click the **+** at each point in the map to draw the outline of your polygon.
7. Select **Save**.

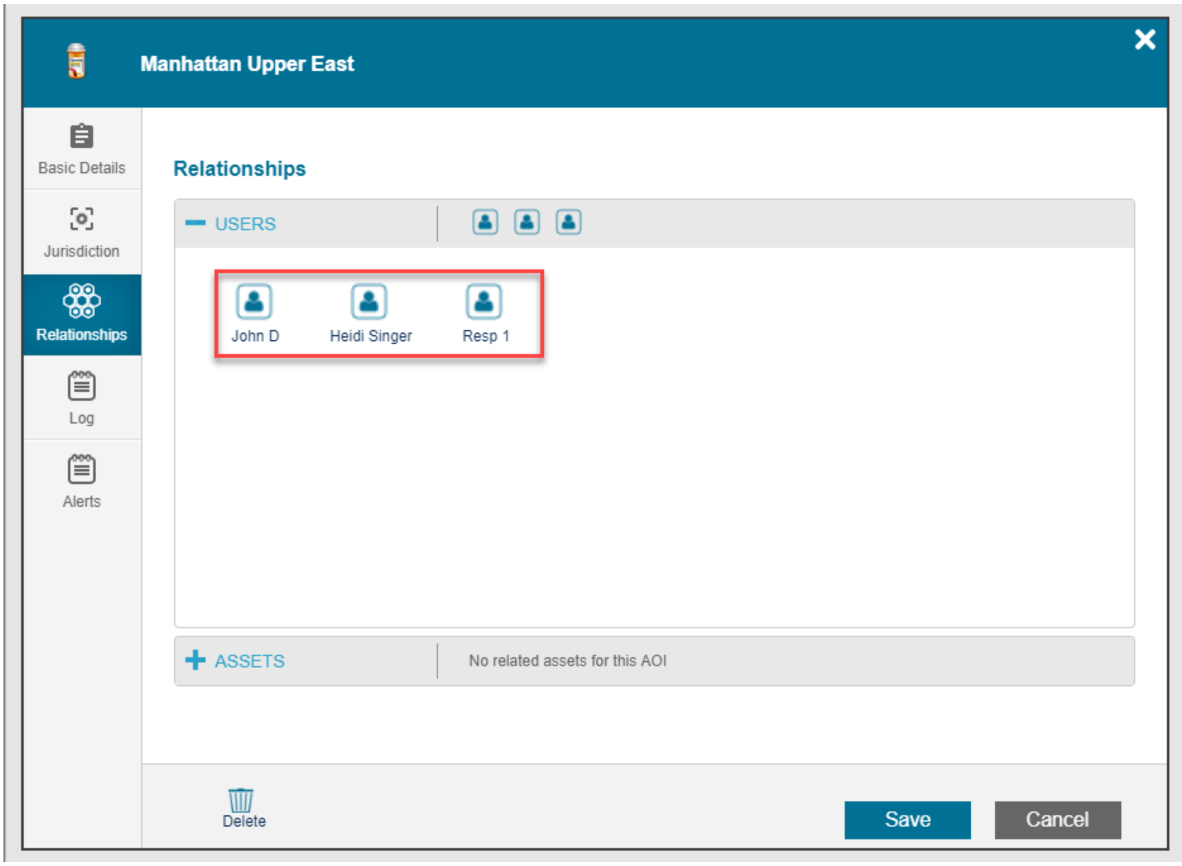


The next tab, Jurisdiction opens.

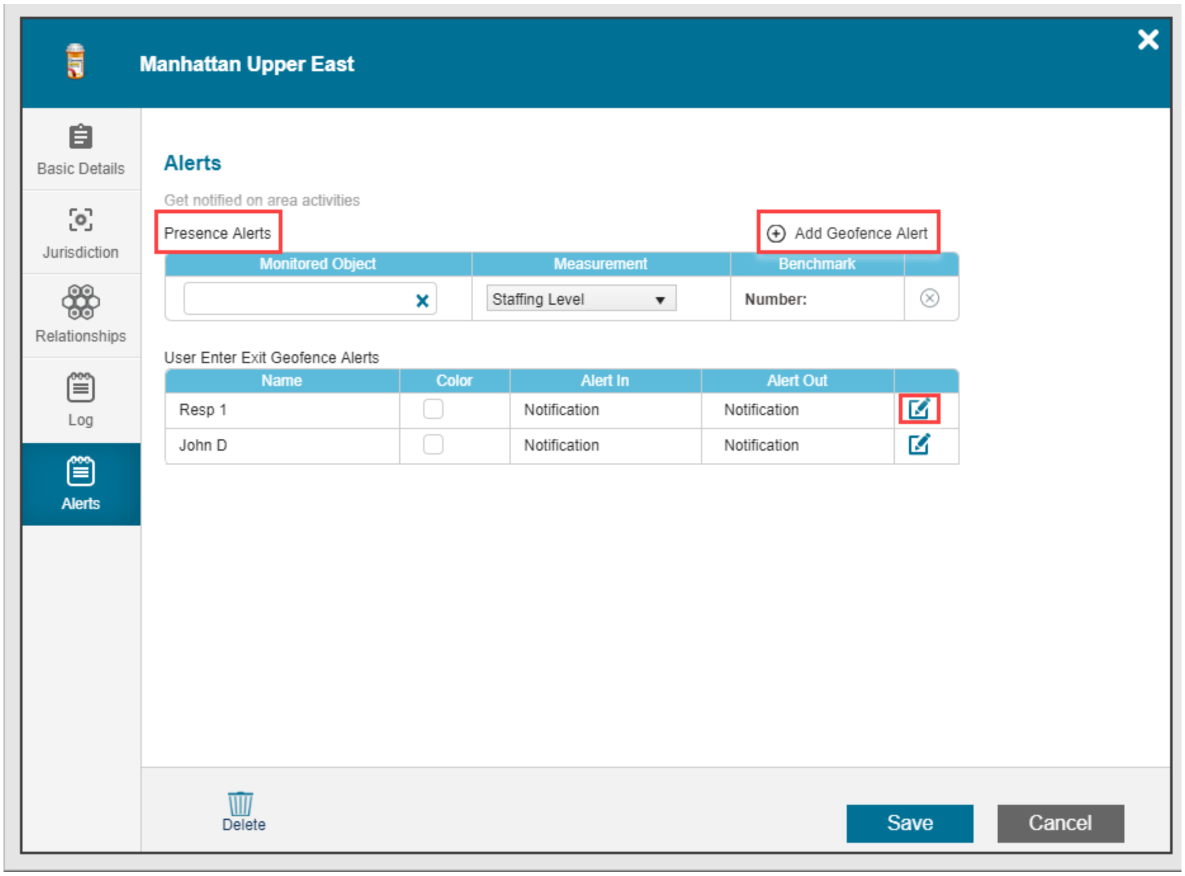


8. Select the **Control Centers** allowed to view the new Geofence.
9. Select **Save**.

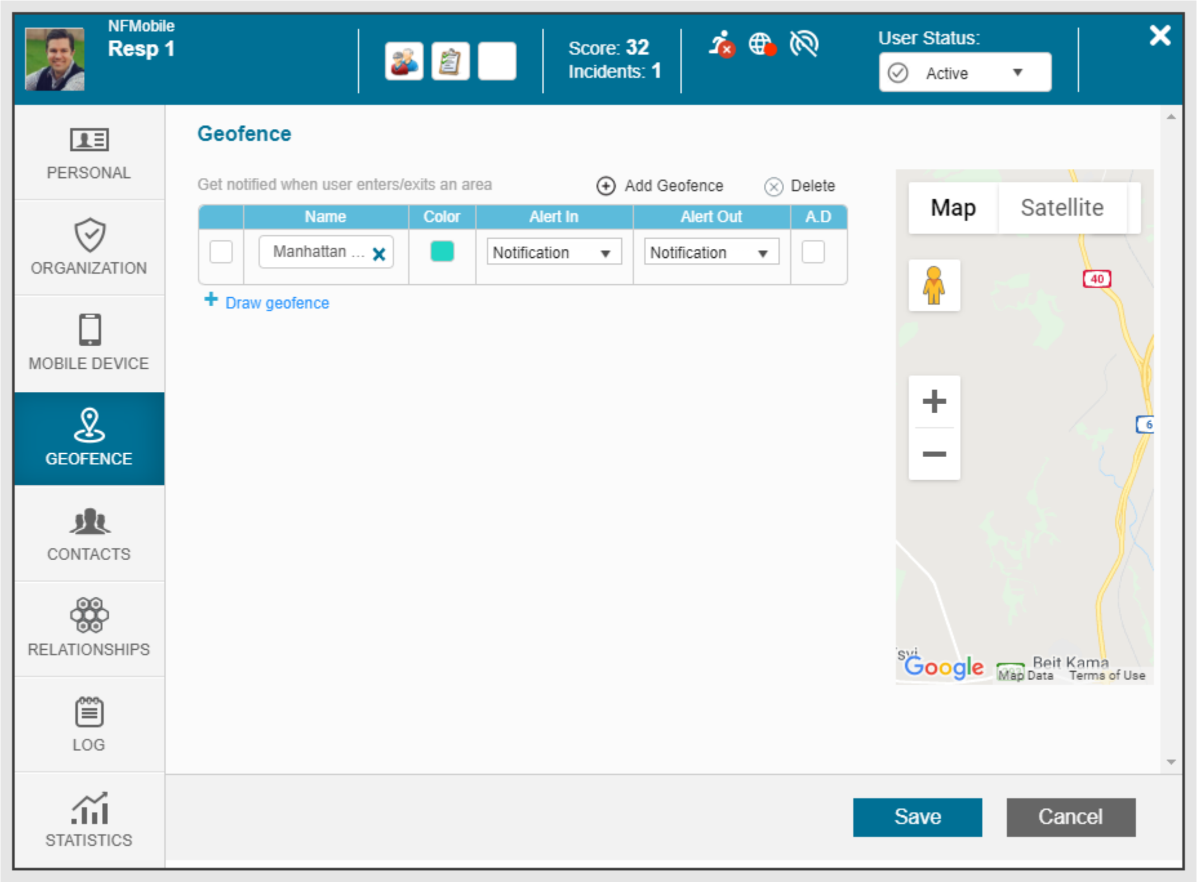
10. The next tab, **Relationships** opens.



11. The tab is view only. For editing or adding users and assets to an AOI see Adding and Managing Users and Adding and Editing Assets.
12. Click on the **Log** tab to view all activities related to the Geofence.
13. Click on the **Alerts** tab. Select **Add Geofence Alert** to add a new Presence Alert by completing the fields and selecting the measurement from the drop down menu.



14. Select the **Edit** icon to amend the **User Enter and Exit Geofence Alerts**, the User's Permission Settings opens and is editable.



15. Amend the User's **Geofence** settings as required and click **Save** in the User's Permissions Settings Geofence tab.
16. Click **Save** on the **New AOI** screen.

Adding and Managing Points of Interest (POIs)

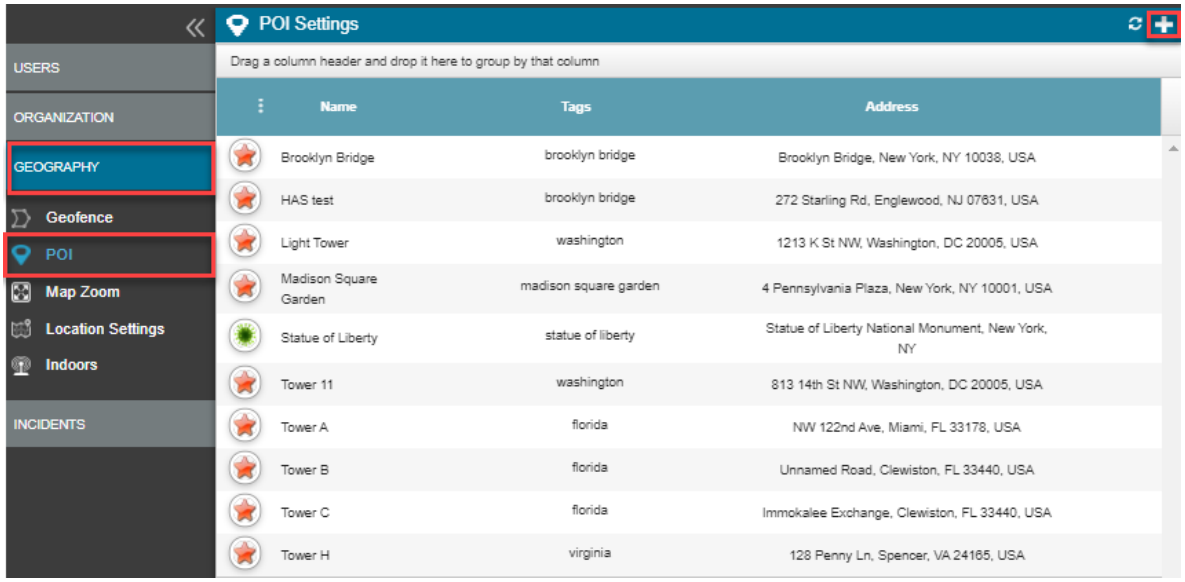
A POI (Point of Interest), is a location that is of interest to your organization. It can be anything on the map, for example, an intersection, a fire hydrant, a police station, any point on the map that you choose to save. POIs are useful for many reasons. They can be used as points of reference. You can see them on the map when you show the POI layer from the info tab. You can add a location to an incident using a POI, and create new POIs from the address of new incidents.

▼ To add a POI

1. From the **Main** screen, select **Settings** > **GEOGRAPHY**, and then select **POI**.

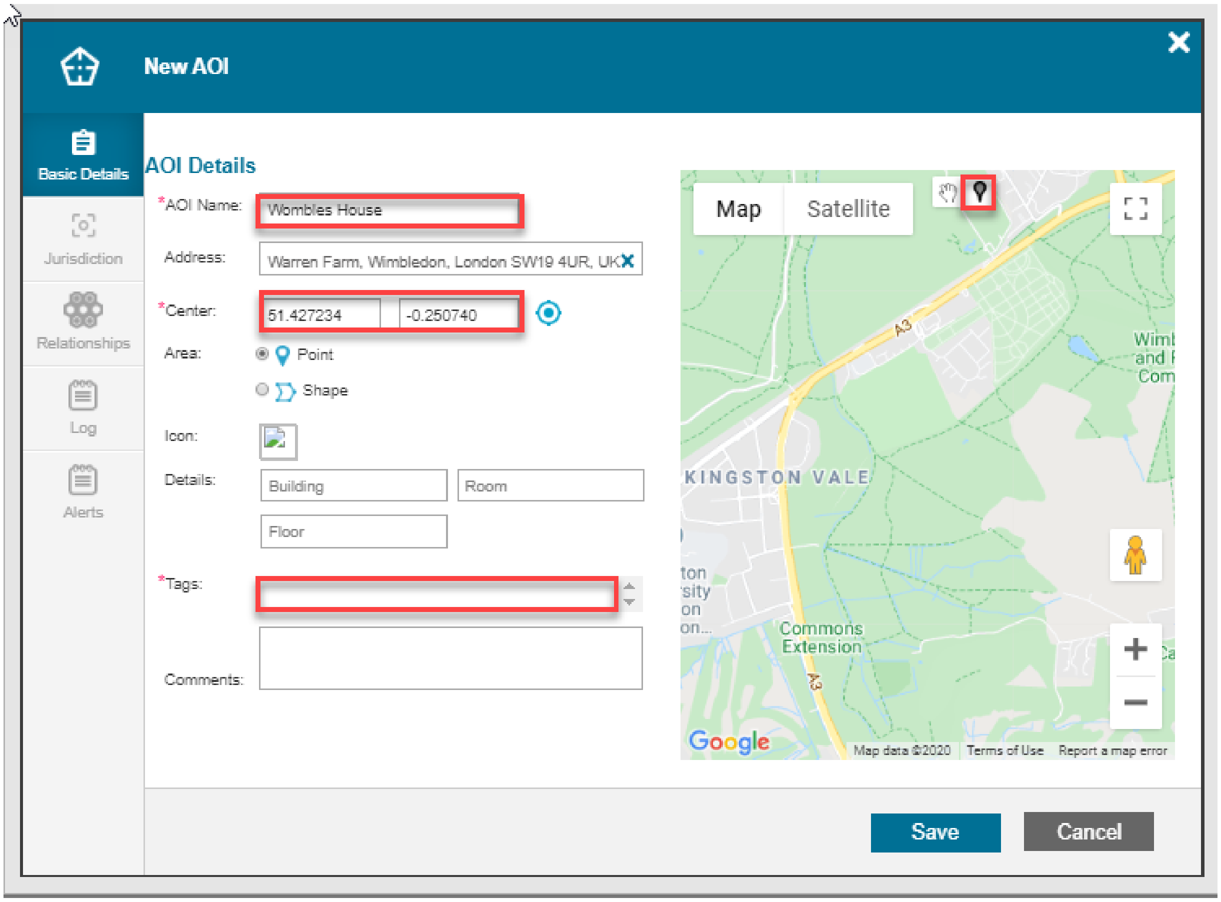
   

   The POI Settings table opens.

2. Click the **+** icon to **Add a New POI**.

   The **New AOI** module opens.



3. Complete **AOI Name** field.
4. Click on the **Pin icon** above the map, then click the map to set the coordinates. The **Address** and **Center** fields will populate.
5. Select the relevant **AOI tag** from the dropdown. For more about AOIs read here.
6. Click **Save**.

Editing and Deleting POIs

▼ To edit a POI

1. Click the **down arrow** in the Actions column of the POI you want to make changes to.
2. Click **Edit** to edit the POI.
3. Type the changes into the relevant fields.
4. Click **Save**.

▼ To delete a POI

1. Click the **down arrow** in the Actions column of the POI you want to make changes to.
2. Click **Delete** to delete the POI
3. A confirmation pop-up appears.
4. Click **OK**.

Importing Batch POIs

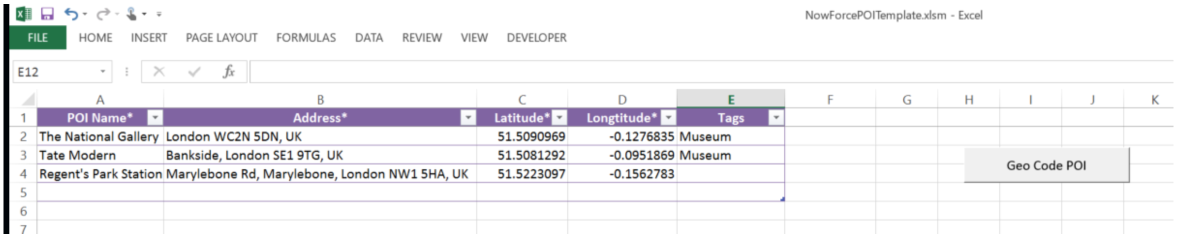
A POI (Point of Interest), is a location that is of interest to your organization. It can be anything on the map, for example, an intersection, a fire hydrant, a police station, basically any point on the map that you choose to save. POIs are useful for many reasons: they can be used as points of reference and you can see them on the map when you show the POI layer from the info tab.

You can add a location to an incident using a POI, and create new POIs from the address of new incidents. Adding multiple POIs to your maps can be undertaken easily by populating an Excel template.

▼ To batch import POIs

1. Request the **Excel** template file (**POI Template**) from Intellicene Support or download from this [link](#)).
2. Populate each field: **Name**, **Address**, **Latitude**, **Longitude**, **Tags**.

> **Note**
> All fields are mandatory.



POI Name*	Address*	Latitude*	Longtitude*	Tags
The National Gallery	London WC2N 5DN, UK	51.5090969	-0.1276835	Museum
Tate Modern	Bankside, London SE1 9TG, UK	51.5081292	-0.0951869	Museum
Regent's Park Station	Marylebone Rd, Marylebone, London NW1 5HA, UK	51.5223097	-0.1562783	

> **Tip**
> If you do not have the geo-coordinates for your POI, you can automatically generate geo-coordinates by entering the Address field and clicking the Geo Code POI button. The Latitude and Longitude fields will be populated.

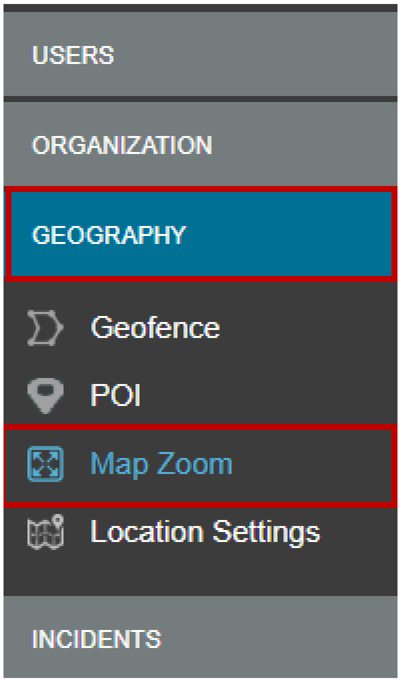
3. Save the file and email to Intellicene Support.

Setting Default Map Center and Zoom Level Preference

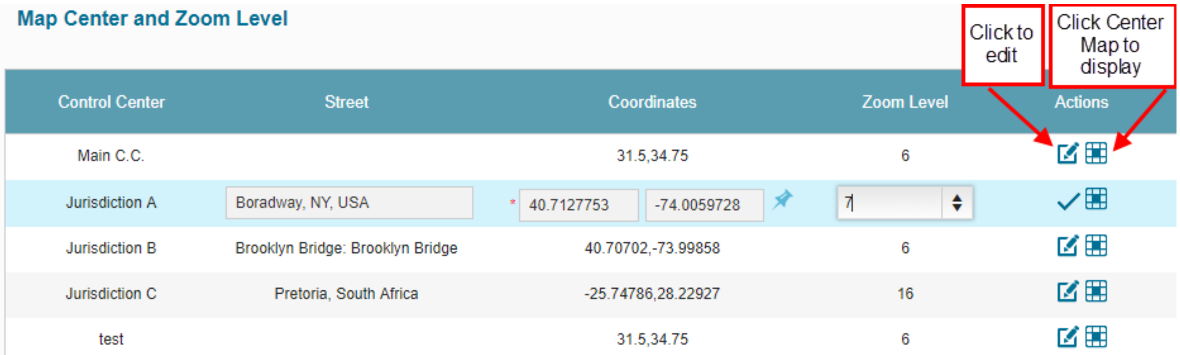
The default map view is displayed when the operator logs into a Control Center or selects the Open Map panel. You can customize the default map center and zoom level for each Control Center.

▼ To set the default map center and zoom level preference

1. From the **Main** screen, select **Settings** > **Geography**, and then select **Map Zoom**.



The Map Center and Zoom Level table opens.

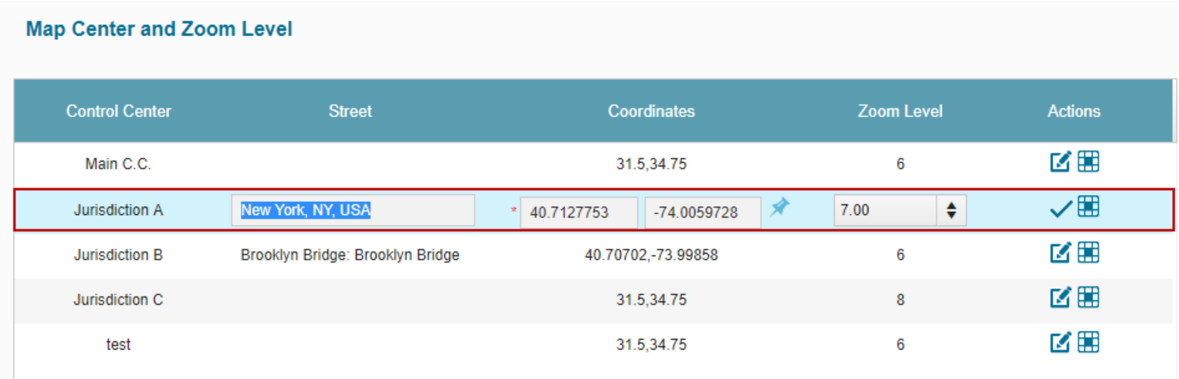


Map Center and Zoom Level

Control Center	Street	Coordinates	Zoom Level	Actions
Main C.C.		31.5,34.75	6	
Jurisdiction A	Boradway, NY, USA	* 40.7127753 -74.0059728	7	
Jurisdiction B	Brooklyn Bridge: Brooklyn Bridge	40.70702,-73.99858	6	
Jurisdiction C	Pretoria, South Africa	-25.74786,28.22927	16	
test		31.5,34.75	6	

2. In the **Actions** column, click of the Control Center whose map you need to edit.

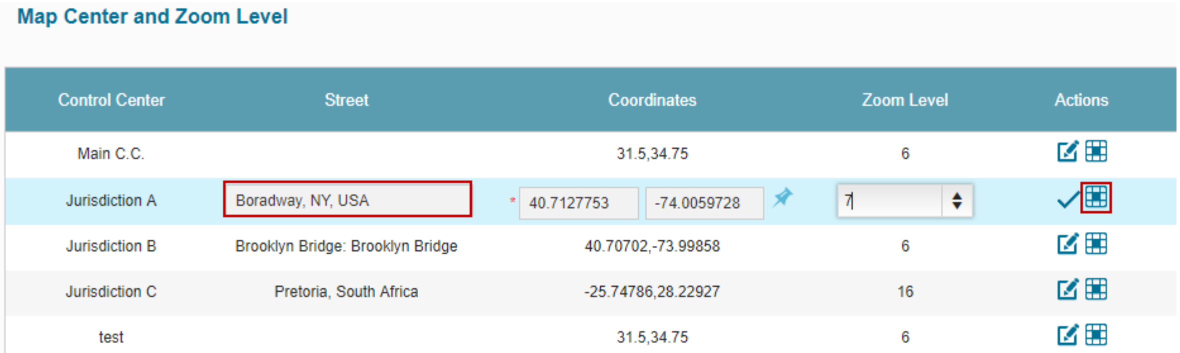
   The **Street**, **Coordinates** and **Zoom Level** fields become editable.



Map Center and Zoom Level

Control Center	Street	Coordinates	Zoom Level	Actions
Main C.C.		31.5,34.75	6	
Jurisdiction A	New York, NY, USA	* 40.7127753 -74.0059728	7.00	
Jurisdiction B	Brooklyn Bridge: Brooklyn Bridge	40.70702,-73.99858	6	
Jurisdiction C		31.5,34.75	8	
test		31.5,34.75	6	

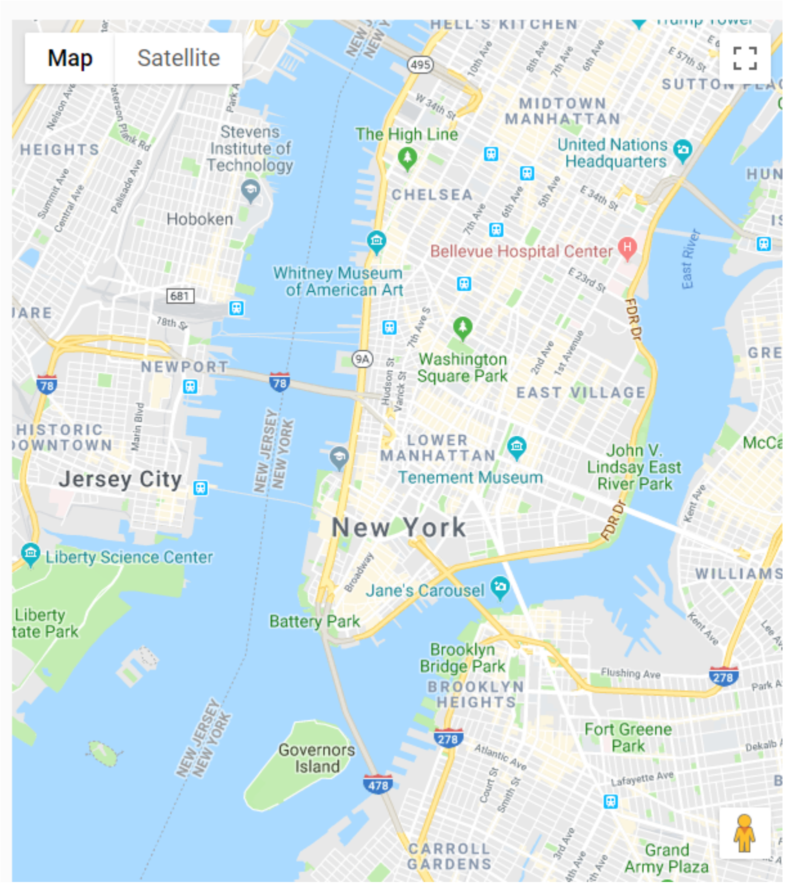
3. Type a new address into the **Street** field. Corresponding Coordinates are automatically added.



Map Center and Zoom Level

Control Center	Street	Coordinates	Zoom Level	Actions
Main C.C.		31.5,34.75	6	
Jurisdiction A	Boradway, NY, USA	* 40.7127753 -74.0059728	7	
Jurisdiction B	Brooklyn Bridge: Brooklyn Bridge	40.70702,-73.99858	6	
Jurisdiction C	Pretoria, South Africa	-25.74786,28.22927	16	
test		31.5,34.75	6	

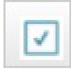
4. Click the **Center Map** icon to display the new map in the preview panel.



5. Select the **Increase or Decrease Value** arrow to adjust the **Zoom Level** to your preference. The map adjacent to the table previews the changes to the zoom level.

Map Center and Zoom Level

Control Center	Street	Coordinates	Zoom Level	Actions
Main C.C.		31.5,34.75	6	
Jurisdiction A	New York, NY, USA	* 40.7127753 -74.0059728	7.00	
Jurisdiction B	Brooklyn Bridge: Brooklyn Bridge	40.70702,-73.99858	6	
Jurisdiction C		31.5,34.75	8	
test		31.5,34.75	6	

6. Click the  to save.

Organization Infrastructure Settings

The Organization configurations allow you to customize the NowForce installation to suit your organization's requirements.

Located within Organization settings are the over-arching system configuration settings which relate across the platform to incident location and management, mapping, mobile services and system security among others.

The specific control centers, icons, integrations, reporting and business intelligence tools settings are also located in the Organization settings.

Understanding the System Configurations 78
Changing Org Configurations 86
Using the Control Center Table 86
Main Control Center Overview 94
Understanding Control Center Jurisdiction 97
Dashboard Business Intelligence (BI) Tool 107
Setting up a background image URL for Mobile SOS 110
How to Add and Manage Icons 111
Configuring Two Factor Authentication Permissions 114
Configuring Location Settings for Mobile App Users 117
Changing Logos in NowForce 121
Changing Your Organization's Time Zone 122

Understanding the System Configurations

The System Configuration tab lists the settings for the Dispatcher and Mobile applications. Configurations should not be confused with permissions. Configurations define the settings for the entire organization and its users, while permissions affect individual users or user groups.

The Configuration table is divided into categories, based on configurations relevant to different sections of the Dispatcher and Mobile applications. Some examples of settings that can be configured here are default map layers, default tab for dispatch and settings used to determine whether an incident is a duplicate incident or not.

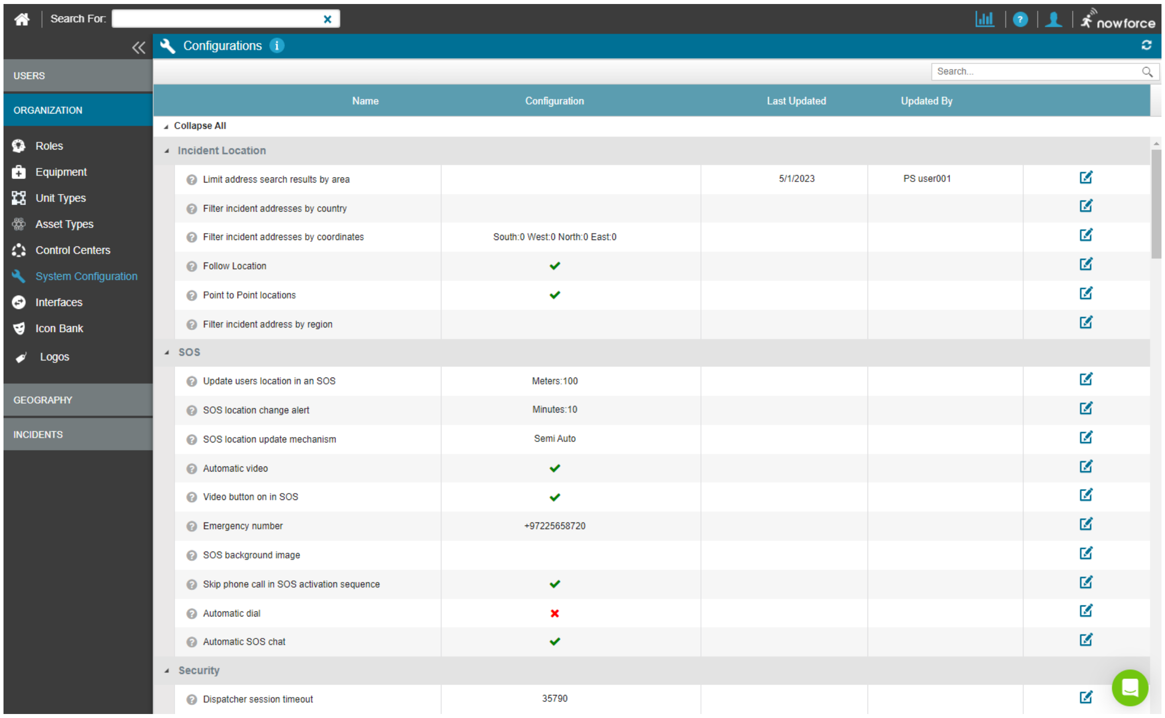
> Note
> The changes you make to the configuration settings affect all users, so be careful when changing configuration settings as the changes you make affect all users who log into the Dispatcher.

▼ To access organization system configuration settings

1. From the **Main** screen, select **Settings** > **Organizations**, and then select **System Configuration**.

   The **Configurations** table opens.



2. Scroll to the required setting and click **Edit**.
3. Modify the settings as required. A description of the various settings is listed below.
4. Click **Save**.

Description of System Configurations

The following list displays the organization configuration available in the system. Additional options may or may not appear, depending on your organization's settings.

Incident Location

- **Limit address search results by area:** Specify the area the address search should focus on when opening an incident.
- **Filter incident addresses by country:** Specify the country the address search should focus on when opening an incident. Enter the two-letter country code, e.g. US into the field.
- **Filter incident address by coordinates:** Specify the longitude and latitude coordinates the address search should focus on when opening an incident.
- **Follow Location:**: When enabled the incidents location updates automatically by following the changing physical location of the selected entity (caller, user, unit).

- **Filter incident address by region:** Specify the region (country or city) that the address search should focus on when opening an incident. Enter the two-letter country code, e.g. US into the field.

SOS

- **Update Users location in an SOS**: Set how far the SOS user moves (in meters) before the system recommends updating the incident location.
- **SOS location change alert:** Set the frequency for the SOS Location change alert pop up in Dispatcher in minutes.
- **SOS location update:** Select the mechanism for location updates in Dispatcher. Options are: Auto – Updates location automatically in the background, no dispatcher action required. Manual – Updates the location and sends a pop-up message to the dispatcher requesting for approval, or Semi Auto– Updates location automatically in the background and displays pop-up notification message.
- **Automatic video**: Starts video automatically on SOS
- **Video button on in SOS:** Displays video button in SOS
- **Emergency Number:** Set the SOS emergency contact number.
- **SOS background image:** Add the SOS background image (URL) in the mobile app.
- **Skip phone call in SOS activation sequence:** SOS is activated without requiring the user to activate the call.
- **Automatically dial:** Starts dialing automatically on SOS.
- **Activate automatic chat messages:** Enables you to define if chat messages are allowed when there is an SOS activation.

Security

- **Dispatcher session timeout:** Maximum length of time (in minutes) per user session, default value is 1440 minutes.
- **Dispatcher password renewal interval:** The number of days between required password renewals for dispatch operators.
- **Number of failed log in attempts permitted:** Maximum number of permitted failed log in attempts before a user is locked out of their account for a defined period of time.
- **Mobile app password renewal interval:** The number of days between required password renewals for mobile app users.

Incident Management

- **Push notification retry intervals:** The interval time between retry attempts for sending push notifications to mobile app users. The default is 30 minutes.
- **Open manual status view:** Automatically opens manual status view when a manual search is initiated.
- **Potential responders in incident dispatch grid:** Set the maximum number of available responders (10 to 90) to display in incident dispatch grid. The available responders appear in addition to the active responders in the incident. A higher number of responders might impact incident window display performance. The default value is 30.
- **Duplicate incident alert period:** An alert is generated to the dispatcher when a potential duplicate incident being created within the specified timeframe. Default timeframe is 15 minutes.
- **Duplicate incident radius alert:** Set the radius for duplicate incidents in meters. An alert is generated to the dispatcher when a potential duplicate incident is created within the specified radius of an already existing incident. Default range is 2000m.
- **PDF export of closed incidents:** Enables the export of a closed incidents details from the incident search results panel.
- **On-Scene alert threshold:** A location update that is greater the default time set, cancels a Not On-Scene alert.
- **Closing or cancelling incident message:** A confirmation window opens when closing or cancelling an incident.
- **Display virtual users in incident dispatch grid:** Display Virtual users in the Dispatch grid.
- **Incident summary pdf sections:** Define which sections appear in the pdf download.
- **Incident creator:** The Incident creator (Dispatcher, Reporter, SOS) will effect which Control Center has jurisdiction over the Incident.
- **Cumulative ETA calculation:** When defining responder ETA, take into account when and where the responder will be located at the completion of all current assigned incidents. Time of incident is calculated based on the completion time of each incident type.
- **Export PDF of a live incident:** Export PDF for live incidents.
- **Expanded Source column:** Display a wider Source column in the Incident Panel with the full name and phone number.
- **Expanded Control column:** Display a wider Control column in the Incident Panel with the full name of the incident dispatcher
- **Incident cancellation reason:** A cancellation reason must be provided.

- **External ID numbers:** A new incident is automatically assigned an External ID (this comprises the Control Center ID and a unique sequentially generated number, e.g. 21). The external ID is in addition to the Incident ID which runs in sequential order for the entire organization.
- **Eddystone beacon prefixes:** Eddystone beacon prefixes.
- **Enable assets notification on incident creation:** Enable assets notification on incident creation. Default value is unchecked.
- **Enable assets notification when responder on scene:** Enable assets notification when responder on scene. Default value is unchecked.
- **Enable assets notification when incident is done:** Enable assets notification when incident is done. Default value is unchecked.
- **Advanced Mapping:** Advanced mapping. Default value is unchecked.
- **Require reason for closing incidents:** Require reason for closing incidents (Disposition codes). Default value is unchecked.
- **Reasons for cancelling incident:** Manage the list of reasons (disposition codes) for cancelling an incident. You can add reasons.
- **Reasons for closing incident:** Manage the list of reasons (disposition codes) for closing an incident. You can add reasons.

Mapping and Location

- **MXD layer:** Provide a name for the MXD layer.
- **Map Type:** The map type that appears in the Dispatcher map. The options are: Street, Hybrid, Satellite.
- **Map Layers:** The default active map layer in the Dispatcher map. The options are: Geofences, Clouds, Traffic Conditions, Overlay, Forecast, Available Users.
- **Location alert:** Defines location alert information.
- **Location alert popup:** Set if location alert has a popup.
- **Location age alert:** Set the duration of the color-coded location age alerts. These alerts indicate the number of minutes elapsing since user's last interaction between their mobile app and the server. Blue indicates the shortest time lapse (default is 10 minutes), and red the longest (default is 24 hours). The color alerts appear in the Location column of the User Panel.
- **Search Radius (in meters) of Assets/POIs:** Define radius limit (in meters) for Assets and POIs that are displayed to mobile user in the following modules: Reporter (when reporting

Incident on POI), Responder (in Info tab) and Asset Lookup (when searching for nearby Assets

Advanced Mapping

- **URL for autocomplete address service provider:** Enter the URL of your auto-complete provider.
- **Google Maps sign key:** Google Maps API key for SaaS NowForce installations.
- **Google Maps client ID:** Google Maps Client ID for SaaS NowForce installations.
- **API geocoding provider:** Select your API GeoCoding provider. The options are: Google, Here, Esri.
- **Map Provider:** The map that appears in Dispatcher. The options are: Google or Esri.

Regional

- **Measurement system:** Set the measurement system from the available options. Selecting Imperial or Metric defines these as the default for all users and all devices. Selecting User dependent allows the users preference to be used.
- **Organization timezone:** Set the timezone for your organization
- **Activate Units module in the system:** Selecting Activate Units Module will turn on Units Types, Units Panel and Units for Responder. Units is supported only in Advanced Responder or higher.
- **Dispatcher log in message:** Set the Dispatcher login screen welcome message.
- **Enable CLI:** Support Command Line Interface in Dispatcher.
- **Enable PBX integration on dispatcher login:** Enable dispatcher to log into their phone extension as part of their NowForce log in process.
- **Enable Glossary:** Enables access to the Glossary in Dispatcher.
- **Indoor positioning:** This enables or disables Indoor Positioning. For more information see Symphia NowForce Policies Guide.
- **Enable Dashboard:** Select your organizations BI service provider.
- **Beacon protocol:** Select beacon protocol.
- **iBeacon prefixes:** iBeacon beacons prefixes.
- **Enable Policies:** Selecting Enable Polices will turn on the Policies module in Dispatcher and Mobile App. Policies is supported from Monitored Reporter license holders and higher.

- **Notify Assets by push notification:** Push notifications are enabled and can be defined in the Communication settings.
- **Dispatcher Date format:** Select your organizations date display format
- **Show interface related fields from the Forms editor:** Turning this config will display the interface fields, pdf fields and the video controller in the form editor. Default value is unchecked.

Mobile Devices

- **Show Logout Button:** Set the Logout button to in the mobile application and enable the user to log out of the application. Turn off this configuration if you dont want to allow users to log out of the application.
- **Default screen for Android:** Selecting this sets the incident screen as the default home screen for Android mobile app users.
- **Limit address search results:** Limit the auto-address search results to a city/area.
- **Communication:** Defines the period of time in minutes to determine no communication from client to server.
- **Siren repeat interval:** Set the sirens repeat time interval (in seconds).
- **Limit active status to single incident at a time:** Setting this limits responders to be active in a single incident at a time.
- **Edit form permission:** Responders can edit an Incident form. Default value: Only when On-scene.
- **Enable video streaming:** Enables video streaming.
- **Radius that triggers "Not On-Scene" alerts:** Set the maximum permitted location (in meters) for a responder reporting On-Scene in an incident.
- **Notification of first responder On-scene:** Send a push notification to all other dispatched responders when the first responder reports On-Scene.
- **On scene report sensitivity display:** Set the distance threshold (in meters) from the incident which defines the user to be On-Scene.
- **Display non-emergency number in Mobile App:** Set the number that will display as Call Center in the mobile app.
- **New incident location uses POI:** When opening a new incident in Reporter the POI is used as the default location. This sets the location of a new incident at the defined POI. Selecting this also blocks the opening of an SOS when the user is farther than the defined meters from the defined POI.

- **Display assets:** Defines which Asset Types are visible to the mobile user in the Asset Lookup module.
- **Navigate incident location:** When enabled, mobile app users can open and use their preferred installed navigation app to navigate to a new incidents location. Users can tap on the Navigation icon in the Details tab to open their navigation app.
- **Group icon display:** Display the users group icon in their mobile apps Dashboard.
- **Application pattern protection time-out:** Set the time limit on your passcode.
- **Keep Alive interval:** Set the timeframe that allows the mobile to remain engaged with the NowForce system.
- **Allow unavailable status when active in incident**: Allows responders to set their status as unavailable when they are responding to an incident.
- **Role/Equipment deactivation:** Deactivate role or equipment.
- **On-scene default tab:** Set On-scene tab as the default tab Responder when a responder is on scene.
- **CMS URL display:** Embed your own content management in the mobile app by adding the URL. Default is the NowForce mobile tutorial videos.
- **Display incident caller in incident journal:** Displays the name of the caller in the incident on the Incident journal page.
- **Incident journal default sort view:** Select the default sort option for the Incident journal
- **Location setting Requirement:** Define whether mobile users must provide access to device location All the time or only While using the app.
- **Auto return on Done:** Returns users to the main page after selecting Done.
- **Incident tab default (mobile):** Set the default screen to Incident Tab
- **Icon URL Display:** CMS icon URL
- **Title Display:** CMS title.
- **Image upload resolution**: Define the image upload resolution - High 1MB, Mid 300Kb, Low 100K. If responders operates in a low bandwidth environment, its advised to use a low resolution. Default value is medium.
- **Offline Incident Reporting:** Allow Reporters to create incident reports when mobile device is not connected to the network. Reports will be sent to the server when network connection is re-established. Default value is unchecked.
- **Require all app permissions:** Enables you to enforce that all mobile users accept all app permissions, including granting the app access to camera, microphone, making calls, media , Bluetooth, and location.

Read more about updating configurations in the Changing Your Organization Configurations.

Changing Org Configurations

You can change your system configurations in the **Config Table**.

Organization Configurations

The System Configuration tab contains the Config table with all settings for the dispatcher and mobile applications. Any changes you make to any Config table settings affects all users within the organization.

The Config table is divided into categories, based on configurations relevant to different sections of the dispatcher and the mobile application. Some examples of settings that can be configured here are default map layers, default tab for dispatch and settings used to determine whether an incident is a duplicate incident or not.

▼ To change organization configuration

1. From the **Main** screen, select **Settings** > **Organizations**, and then select **System Configuration**.

   The **Config** table opens.

2. In the **Config** table, go to the configuration you want to change and click **Edit**. The **Config** column becomes editable.
3. Change the setting and click **Save** to save changes, or **Cancel** to discard changes.

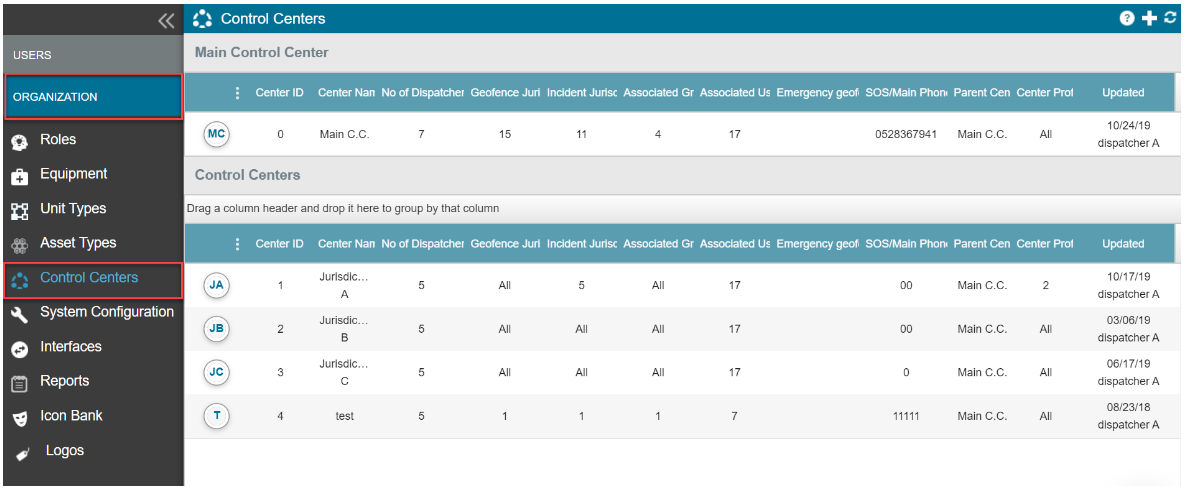
Using the Control Center Table

The Control Center table displays all the dispatch centers associated with your organization. The table is divided into two sections: The Main Control Center and Control Centers. The Main Control Center section displays information for your primary center, and the Control Centers section shows the information of any secondary Control Centers you have created.

▼ To navigate to the Control Center table

1. From the **Main** screen, select **Settings** > **ORGANIZATION**, and then select **Control Centers**.

The **Control Center** tables opens.



The Main Control Center has by definition, unlimited jurisdiction over all entities (users, groups, geofences/polygons, incident types etc.) in your organization. The Main CC's jurisdiction cannot be restricted. Therefore, editing actions within this section are limited to: changing the name of the center and SOS/Main Phone Number, and adding dispatchers.

The Control Centers have several Actions associated with editing, deleting, selecting dispatchers and the editing the center's map.

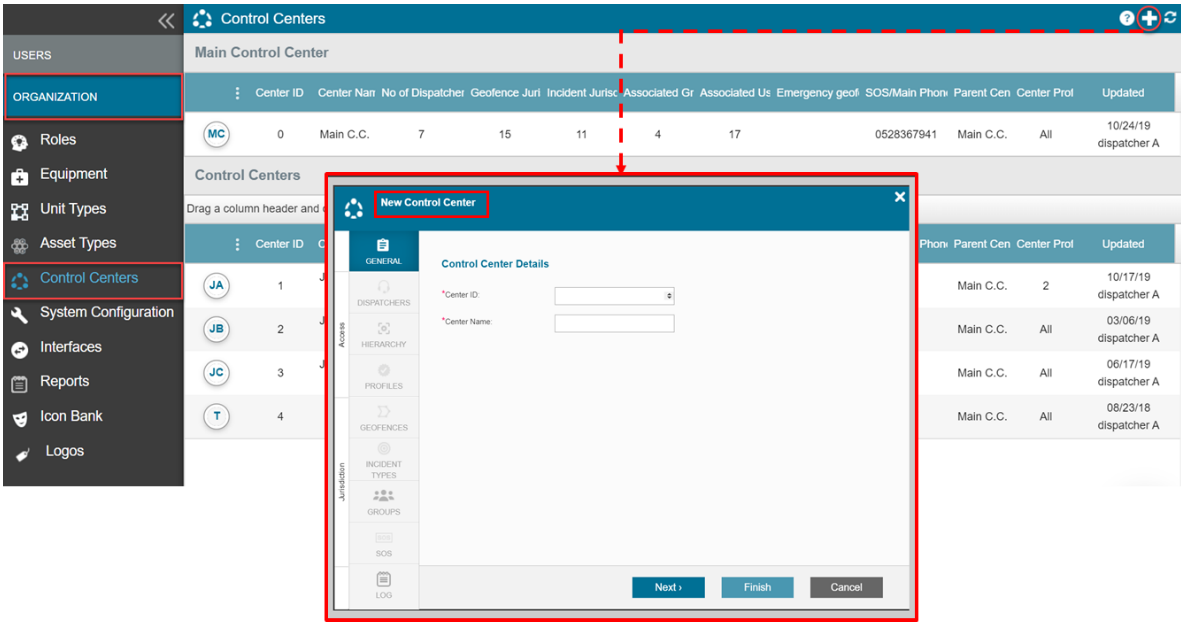
Control Center Table Descriptions

The table below sets out the descriptions of each element of the Control Center Table.

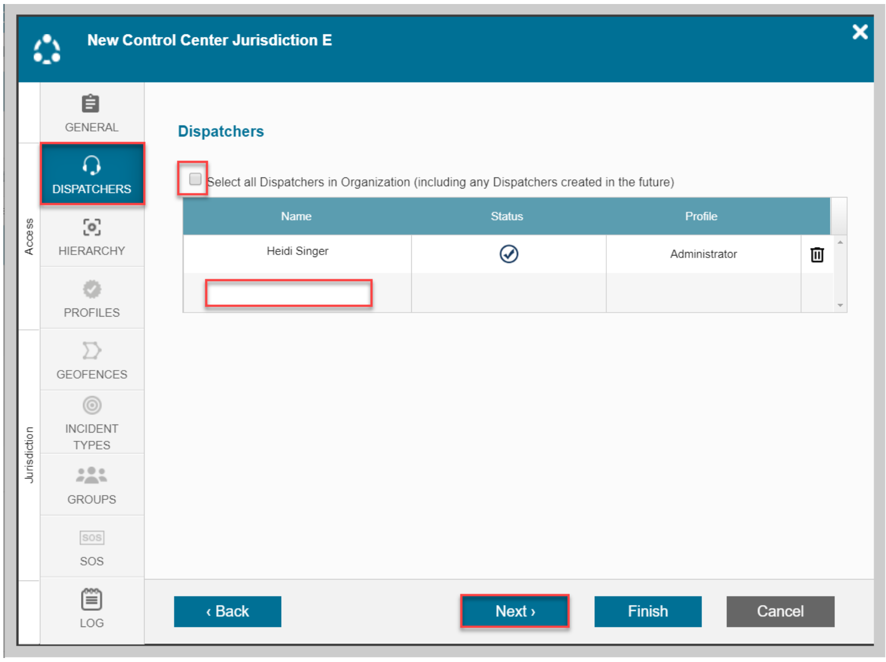
Title	Description
Center ID	A unique ID to the Control Center
Center Name	The Name of the Center that will appear in the logging window
No of Dispatchers	Shows the number of dispatchers who are associated with the center. Roll your mouse over the number to see the names of the dispatchers.
Associated SOS Users	Shows the number of users who are associated with the center as SOS users. When these users activate an SOS incident from their mobile devices, the mobile device will dial this center's SOS/Main Phone #.
Geofence Jurisdiction	Shows the number of polygons that are associated with the center. Roll your mouse over the number to see the names of the associated polygons.
Incident Jurisdiction	Shows the number of incident types associated with the center. Roll your mouse over the number to see the names of the incident types.
Associated Groups	Shows the number of groups associated with the center. Roll your mouse over the number to see the names of the groups.
Associated Users	Shows the number of users associated with the center.
Emergency geofences	Each emergency incident triggers a phone call to a control center. This option allows for decoupling between the ability to view incidents in different geofences ('Geofence Jurisdiction') and the association of one emergency number ('SOS/Main Phone #') to respond to a SOS call. * If no number is defined the application will call the number under the config setting of the organization -> EmergencyNumber
SOS/Main Phone #	This is the phone number that is associated with the center. When users who are associated with this center activate an SOS incident from their mobile devices, the mobile device will dial this phone number.

▼ To add a new Control Center

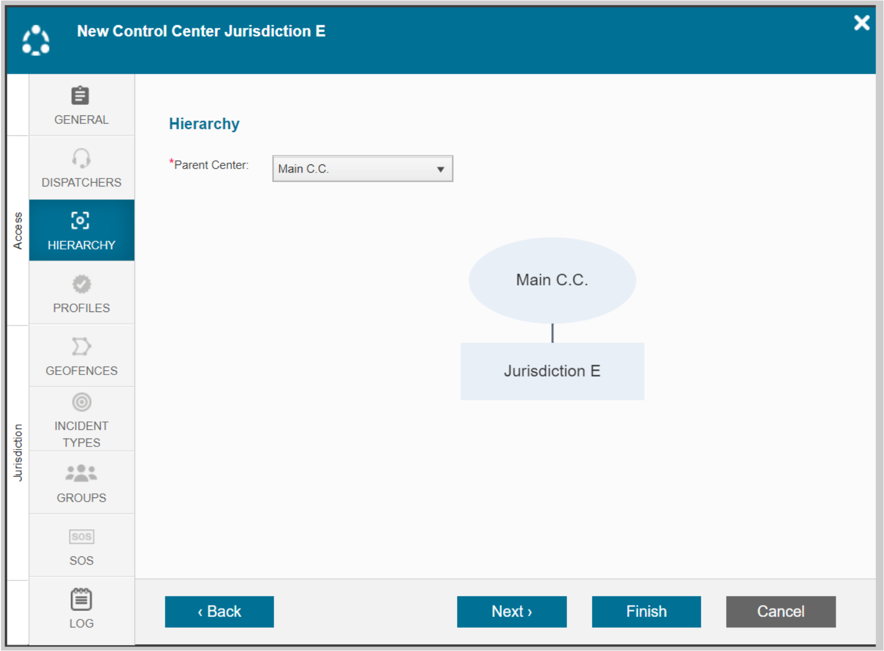
1. Select the **+** to open **Control Center** module.



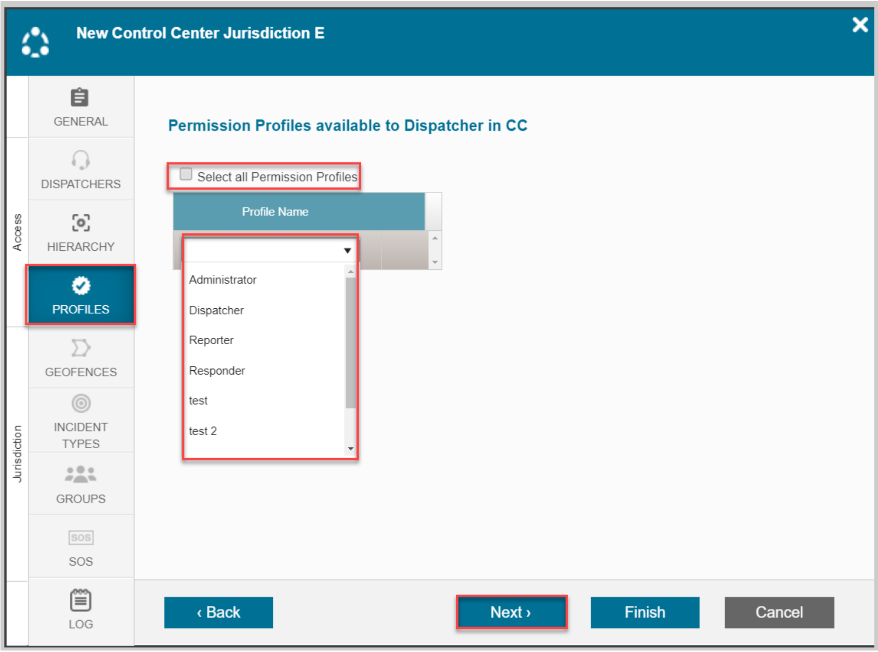
2. In the **General** tab use the arrows to select a **Center ID** and provide a name in the **Center Name** field.
3. Select **Next**.



4. In **Dispatchers** tab either select **All Dispatchers in Organization (including any Dispatchers created in the future)** or enter the specific dispatcher into **Name** field.
5. Select **Next**



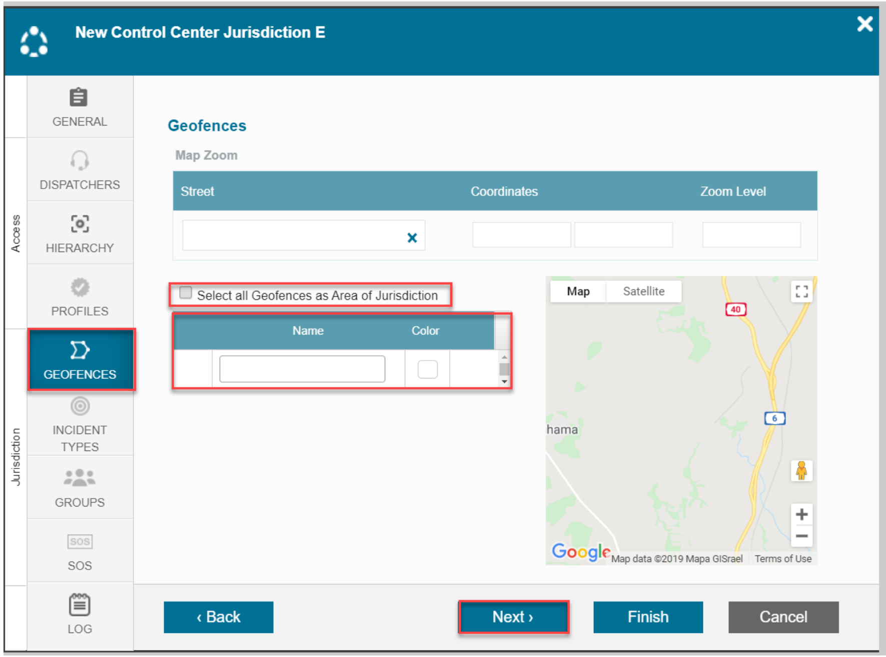
6. Select the **Parent Center** using the dropdown on the **Hierarchy** tab
7. Select **Next**.



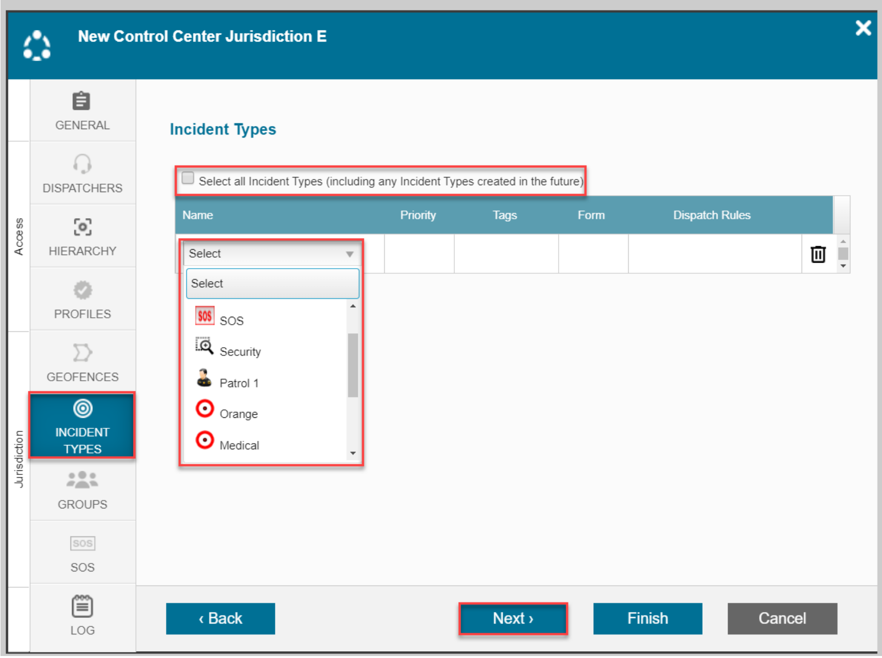
8. In **Profiles** tab either select **All Permission Profiles** or specific **Profiles** from the dropdown list. This list will define which profiles will be available to the CC operator/dispatcher when creating/editing user profiles

> Note
> Note: selecting the "All" option means that also profiles that do not exist but are created in the future will also be associated with this CC.

9. Select **Next**.

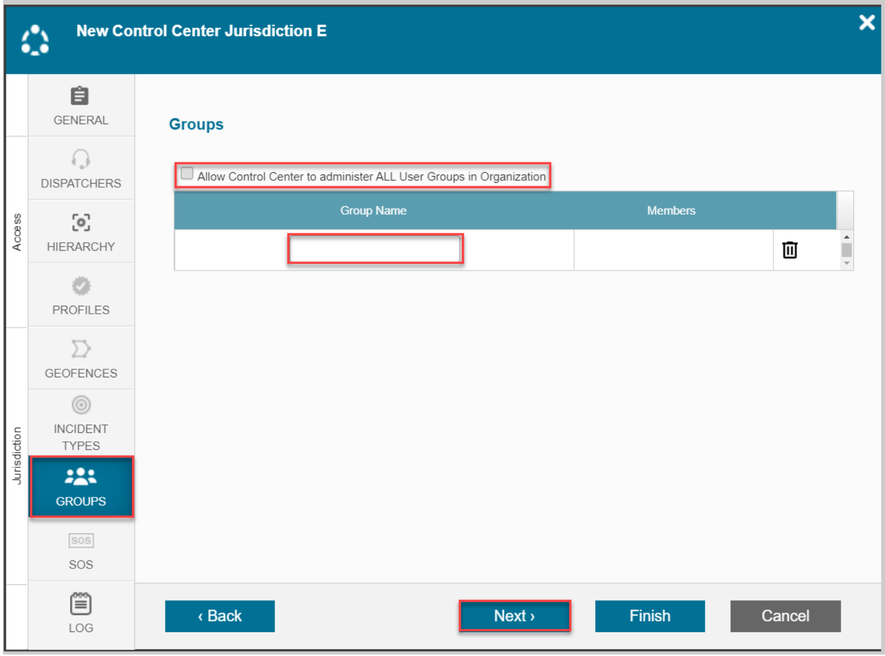


10. In the **Geofence** tab either select **Select all Geofences as Area of Jurisdiction** or using the dropdown, select the relevant geofences.
11. Select **Next**.



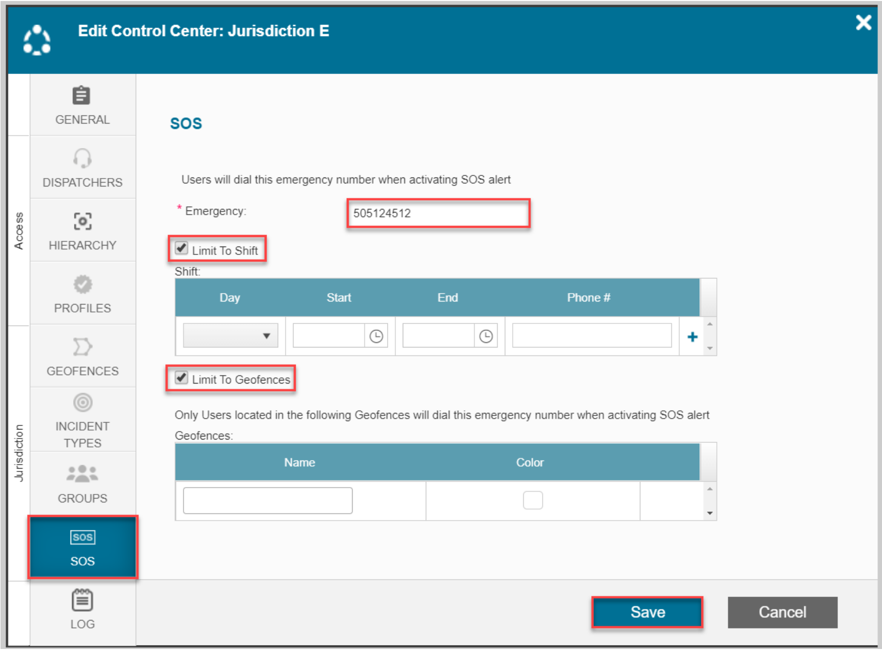
12. In the **Incident Types** tab either select **Select all Incident Types** (this will include also **Incident Types** created in the future) or using the dropdown, select the relevant Incident types.

13. Select Next.



14. In the **Groups** tab, either select **Allow Control Center to administer ALL User Groups in Organization** (including any Group created in the future) or enter the relevant **Group Names** in the text box.

15. Select **Next**

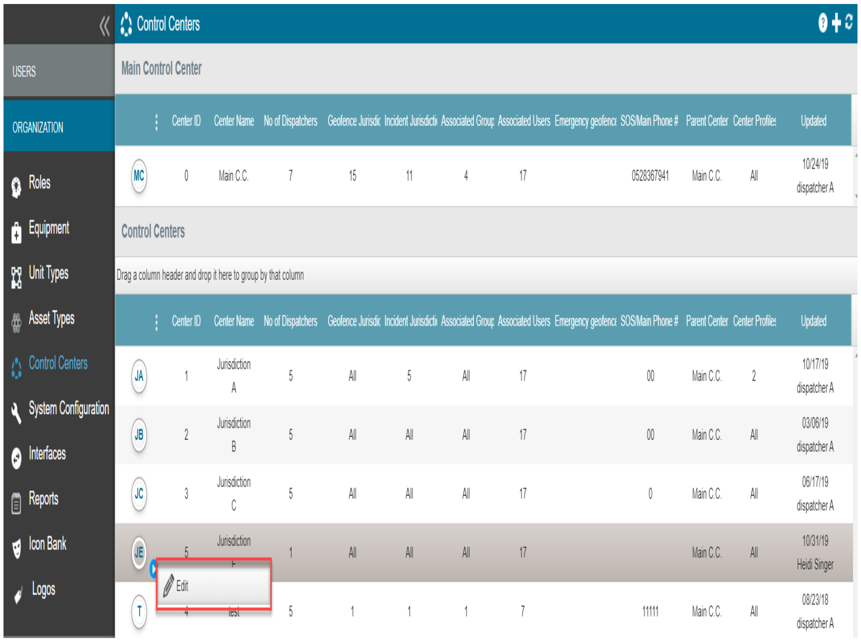


16. In the **SOS** tab type in the emergency number in the field. This is the phone number that will be dialed by the app when activating an SOS alert. You may also select Limit to Shift or Limit to Geofence for that emergency number. Additional dropdown fields appear for you to provide preferred Shift settings and Geofence settings.
17. Select **Save**
18. Close the Control Center module by selecting the **X**.

Editing a Control Center

▼ To edit a Control Center

1. In the Control Center table, **stand** on the icon of the v you wish to edit.
2. Select **Edit** and the Control Center module opens.

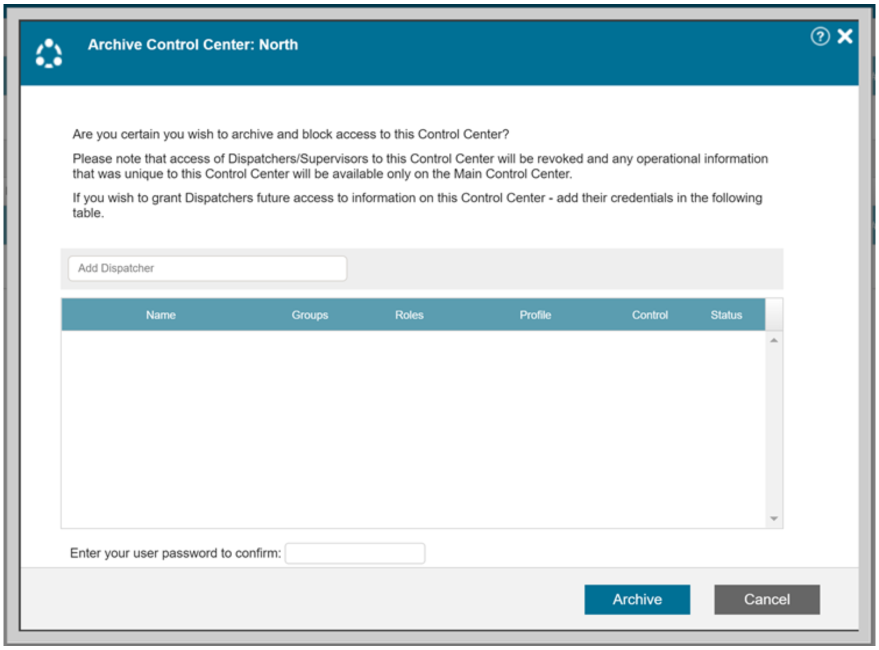


Archiving a Control Center

With the new Archive Control Center feature you can archive and lock a Control Center. All associated data is retained and remains accessible to the Dispatchers you specify for future access.

▼ To archive a Control Center

1. In the Control Center table, **stand** on the icon of the Control Center you wish to archive.
2. Select **Archive** and the **Archive Control Center** module opens.



3. In the text box enter your **user password**.
4. Select **Archive**.

Main Control Center Overview

The Control Center's settings page is where you manage all the Control Centers that have been created for the organization. You can use this page to add and manage new Control Center's. When you open the page for the first time, you will see information for one center. This is the default Main Control Center that has complete unlimited control over all resources of the organization.

> **Note**
> If your organization has no need to compartmentalize information and if you are fine with all dispatchers having access to all users, incidents and assets then it is recommended to maintain the default main control center. However, if you need to manage separate views or if you wish to limit access to information - then you will need to create and manage multiple Control Center.

Managing centers is done from the Setup Menu, in the Organization option, read more here.

Main Control Center Settings

As mentioned above, the Main Control Center is your organization's default control center. The Main CC has unlimited jurisdiction; all users, groups, geographical areas, and incident types that you create are always available in the Main CC and cannot be hidden or limited.

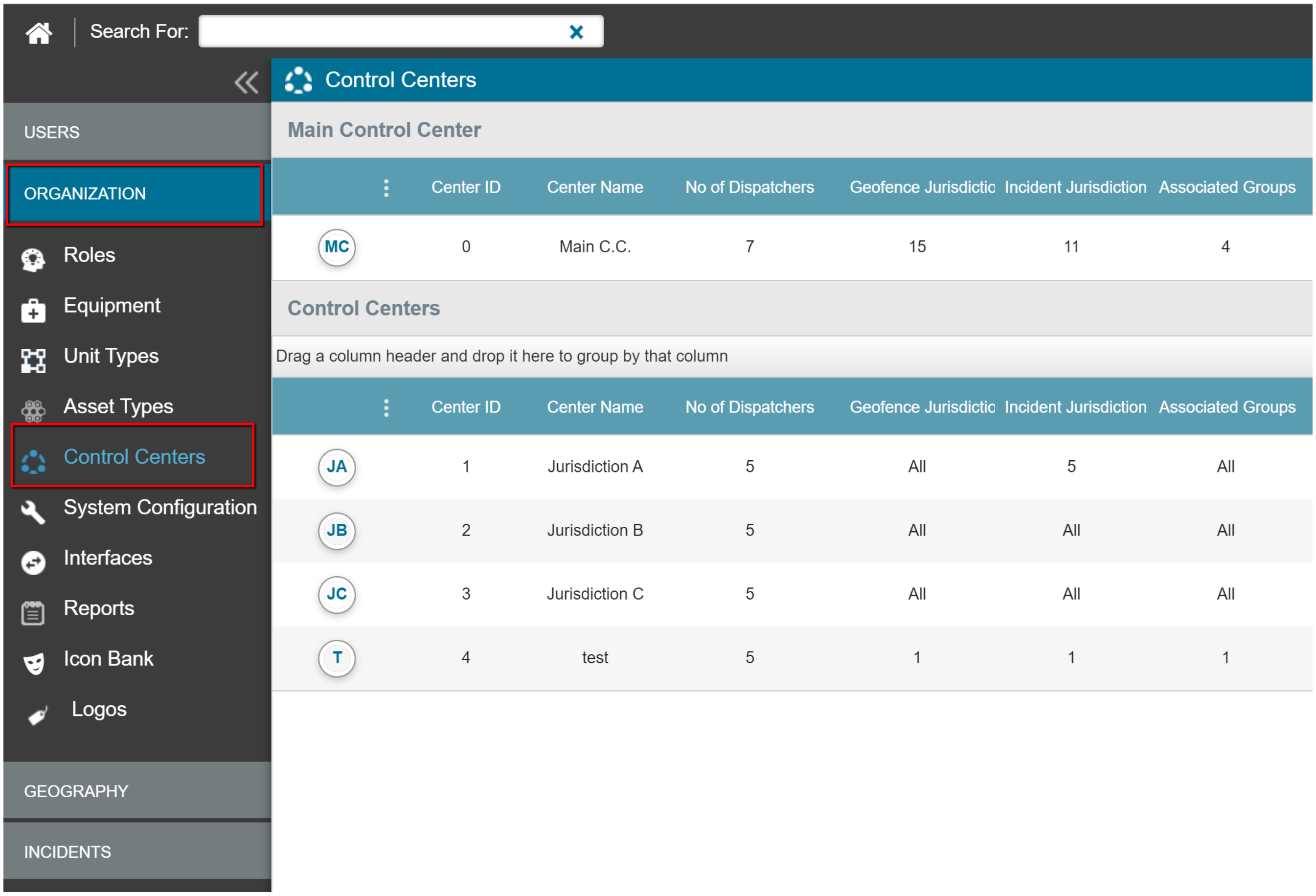
The only modifications you can make to the Main Control Center's parameters are the following:

- ID
- Name
- SOS/Main Phone Number
- Define Dispatcher/Supervisors that have access to the Main CC.

Accessing the Control Center Settings Table

From the **Main** screen, select **Settings** > **ORGANIZATION**, and then select **Control Center**.

The **Control Centers** settings table opens.



The Control Centers table is divided into two sections: The Main Control Center and any other Control Center you create. The table columns display the following information:

Title	Description
Center ID	A unique ID to the Control Center
Center Name	The Name of the Center that will appear in the logging window
No of Dispatchers	Shows the number of dispatchers who are associated with the center. Roll your mouse over the number to see the names of the dispatchers.
Associated SOS Users	Shows the number of users who are associated with the center as SOS users. When these users activate an SOS incident from their mobile devices, the mobile device will dial this center's SOS/Main Phone #.
Geofence Jurisdiction	Shows the number of polygons that are associated with the center. Roll your mouse over the number to see the names of the associated polygons.
Incident Jurisdiction	Shows the number of incident types associated with the center. Roll your mouse over the number to see the names of the incident types.
Associated Groups	Shows the number of groups associated with the center. Roll your mouse over the number to see the names of the groups.
Associated Users	Shows the number of users associated with the center.
Emergency geofences	Each emergency incident triggers a phone call to a control center. This option allows for decoupling between the ability to view incidents in different geofences ('Geofence Jurisdiction') and the association of one emergency number ('SOS/Main Phone #') to respond to a SOS call. * If no number is defined the application will call the number under the config setting of the organization -> EmergencyNumber
SOS/Main Phone #	This is the phone number that is associated with the center. When users who are associated with this center activate an SOS incident from their mobile devices, the mobile device will dial this phone number.

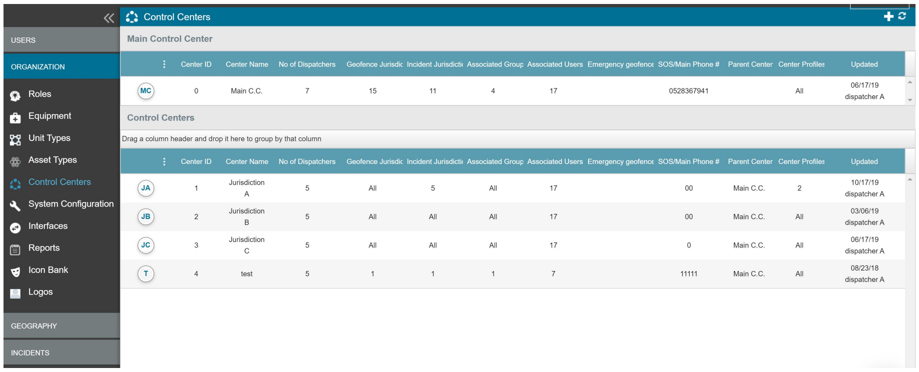
Learn more about the Control Center settings table here.

Understanding Control Center Jurisdiction

If you wish to compartmentalize and manage different sections of your organization in separate Control Centers, you can do so by creating separate Control Centers.

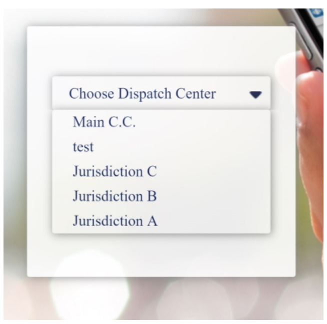
Control Centers are designed to have limited jurisdiction to specific geographies (geofences), areas of expertise (Incident Types) or specific controlled users (Groups). Notwithstanding, no matter how many Control Centers you create - there will always be a Main Control Centers that has unlimited access to all the organization jurisdiction. The Main Control Centers operates as the trunk and the Secondary Centers are its branches.

For a short overview of the Main Control Centers functions see article click here.

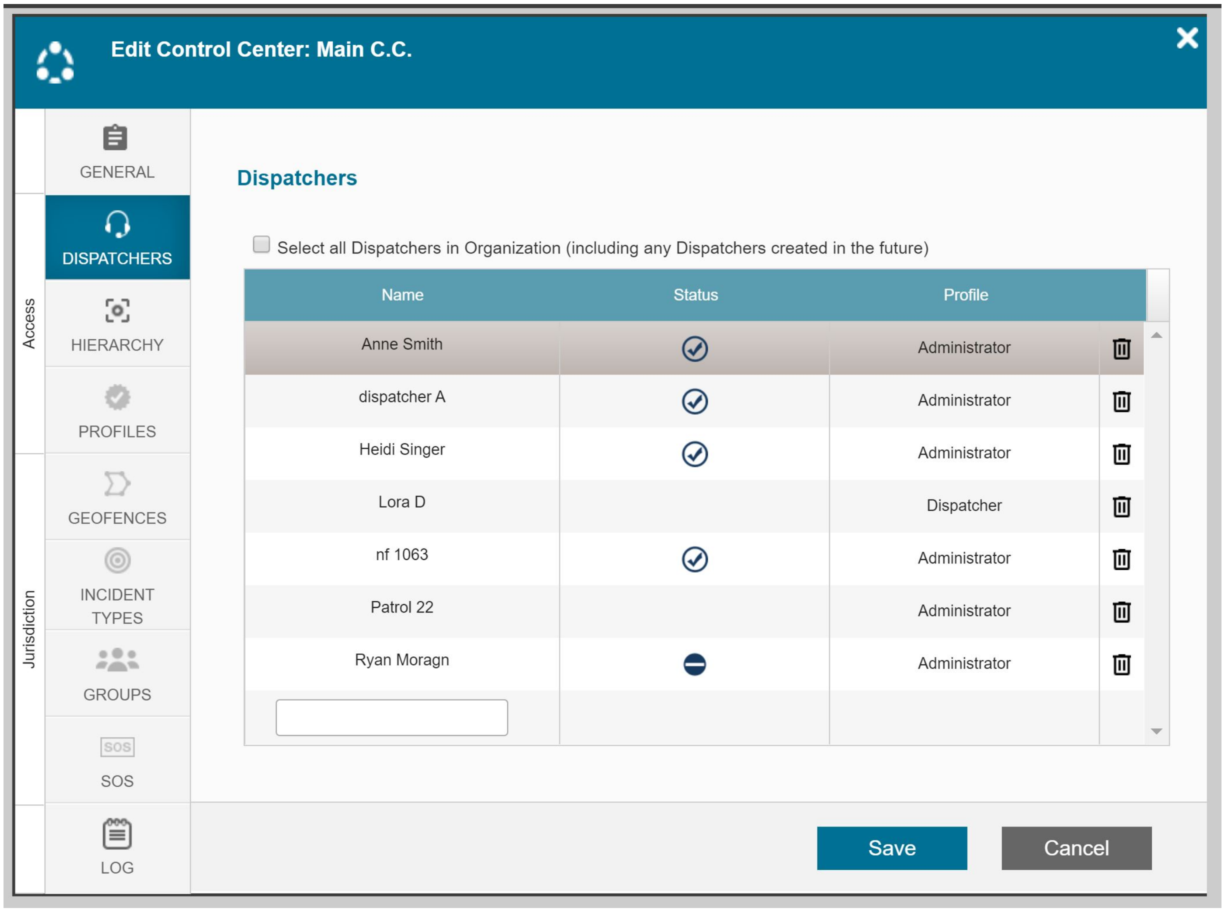


Dispatcher / Supervisor Access

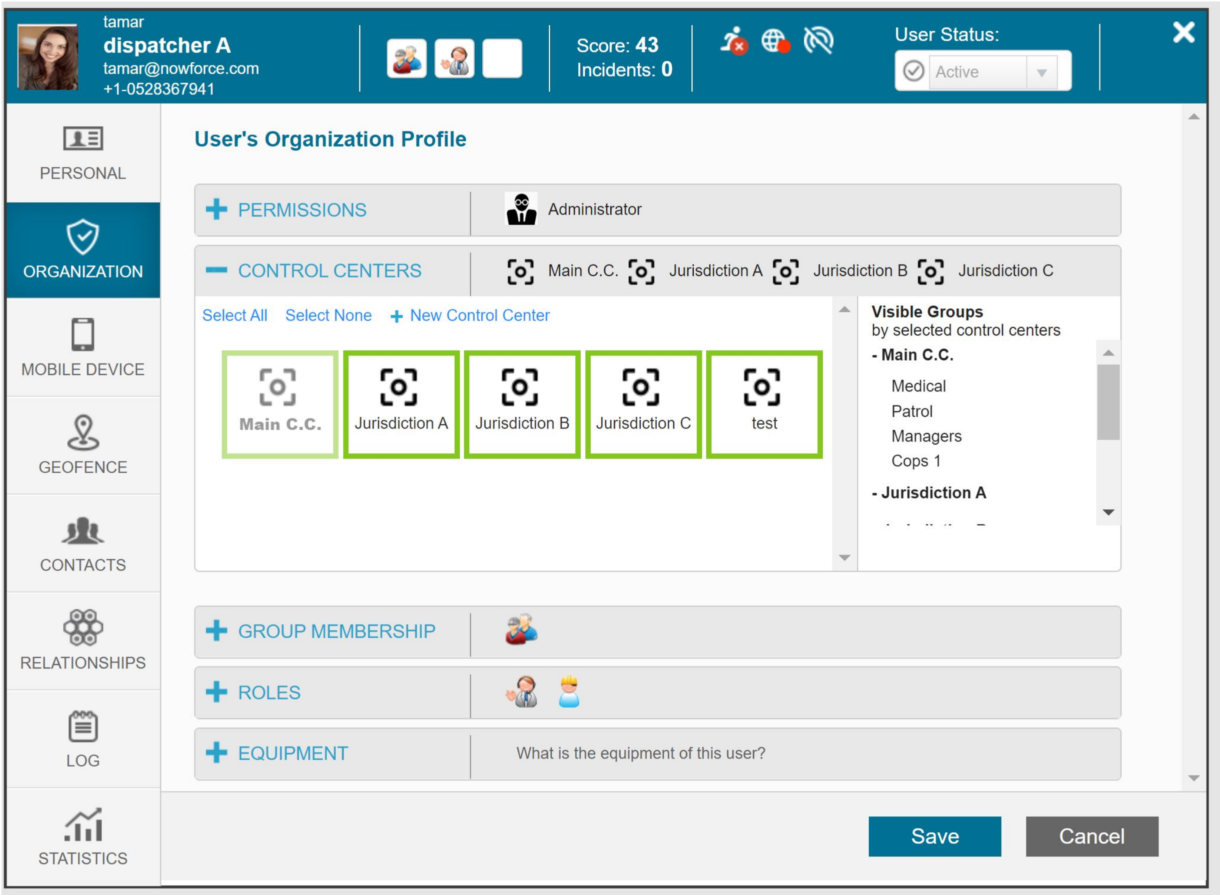
You can choose which Dispatcher/Operator has access to any of the Control Centers. Granting a Dispatcher access to the Main CC will allow that Dispatcher to view ALL Incidents in ALL areas and control ALL Users. Dispatchers with access to more than one CC will be prompted on login to choose which CC they want to login to.



Granting access of Dispatchers and Supervisors to Control Centers can be done either in the Dispatcher tab on the CC module:



or in the User Management module under the Control Centers tab:



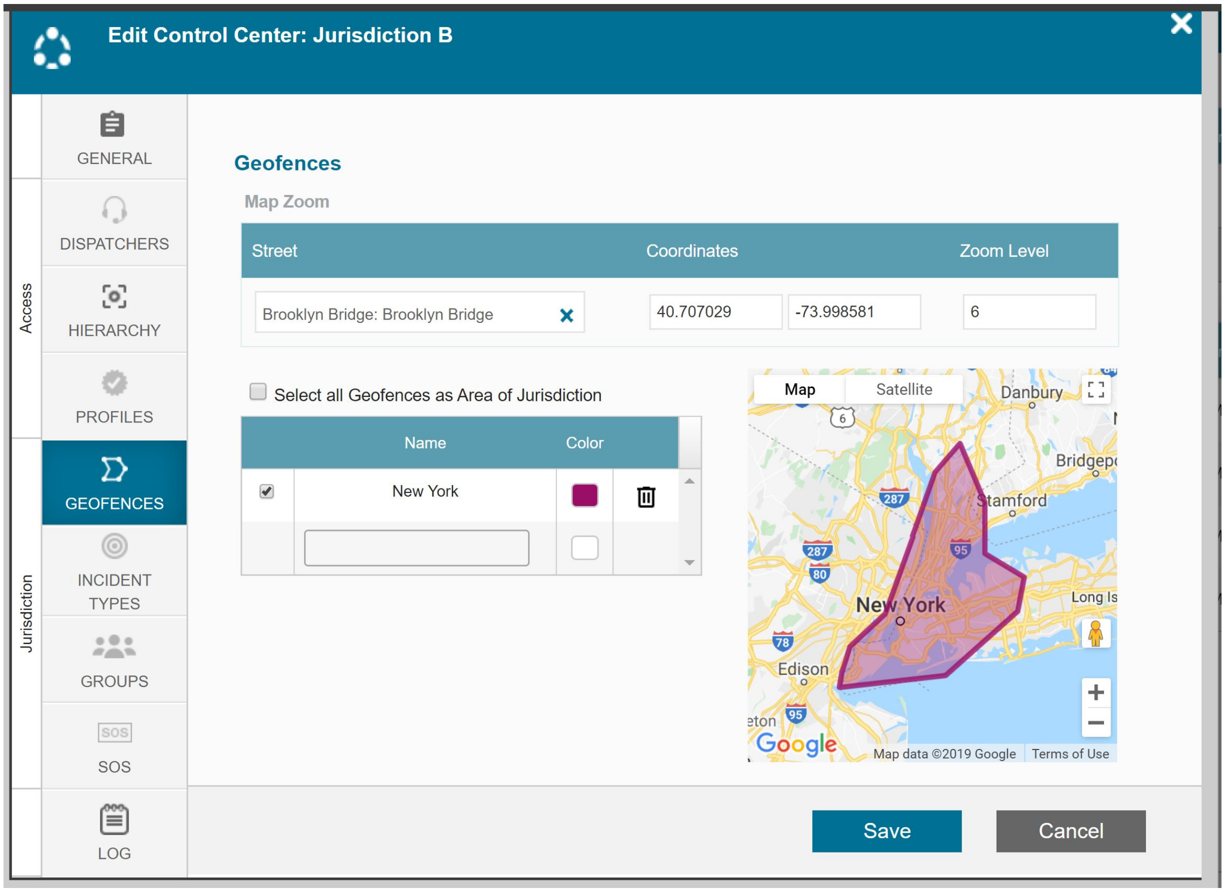
Control Center Jurisdictions

When creating a new Control Center, you are asked to define which polygons, incident types and user groups are associated to the center. This article explains the significance of these configuration with regards to:

- Incident filtering
- User filtering
- Viewing responders on the map
- Creating new incidents
- Dispatching responders to incidents

Incident Filtering

You can define which incidents are accessible in a CC based on the COMBINATION of geographic areas (geofences) and professional domain (incident types).

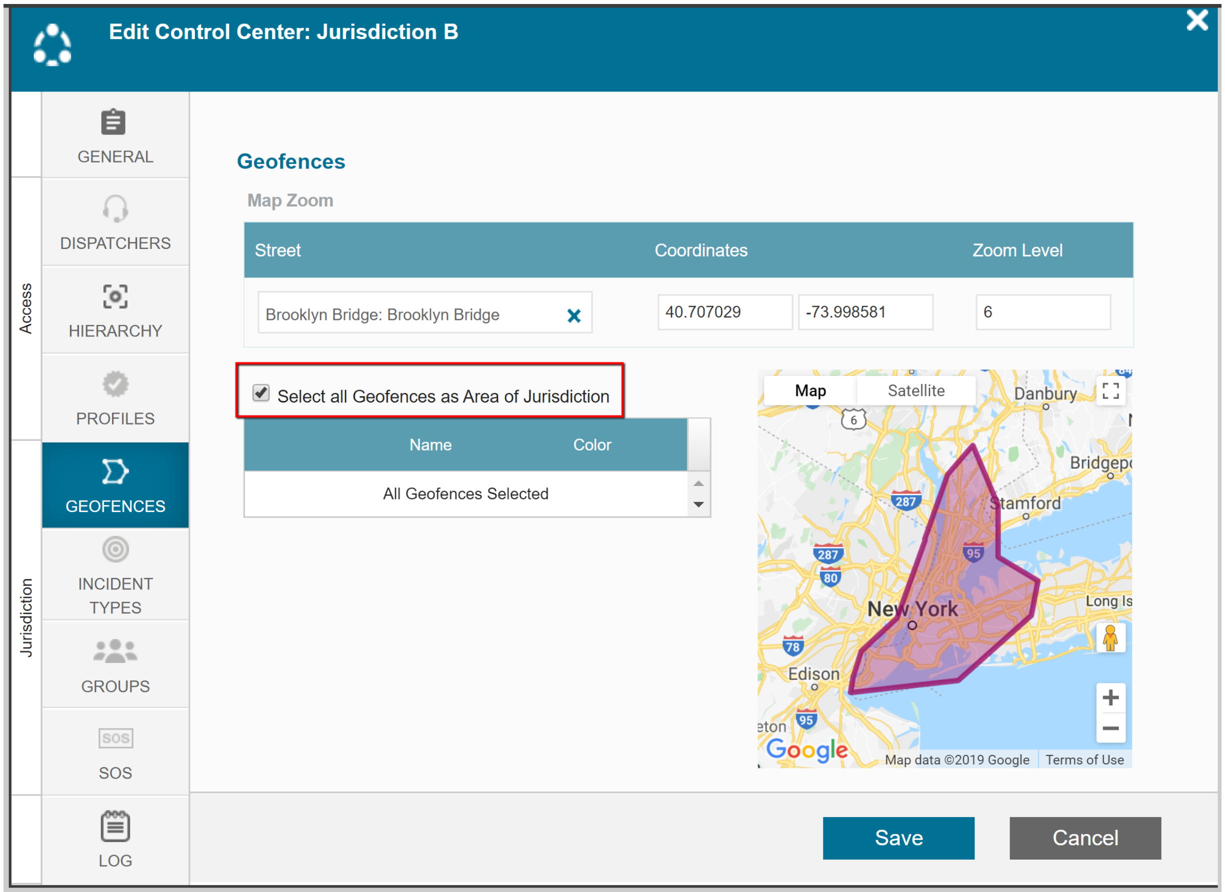


When you select specific geofences and incident types, the only incidents that will appear in the CC are incidents that match both criteria.

For example:

CC Center A is configured to have jurisdiction over the "East London" polygon and over incident type "House Fire". Therefore, the dispatcher John, who is logged into CC A, will be able to view only "House Fire" incidents that are located in the "East London" predefined geofence.

> **Note**
> If you wish the CC to view ALL areas and incident types then check the ALL checkbox. This will mean that also geofences and incident types created later will be added to this CC jurisdiction.



Additional Incidents that May Appear in the CC due to Associated Groups

Additional incidents that do not correspond to the area or incident type filtering may also appear in the CC due to a user/asset associated with both with the incident and the CC. If a user is a member of Group associated with the CC (see group association below) AND also appears as a contact (source, responder, etc) of the incident, then the SPECIFIC incident will also appear in the center.

> **Note**
> This feature is configurable via system configurations, see below for the setting:

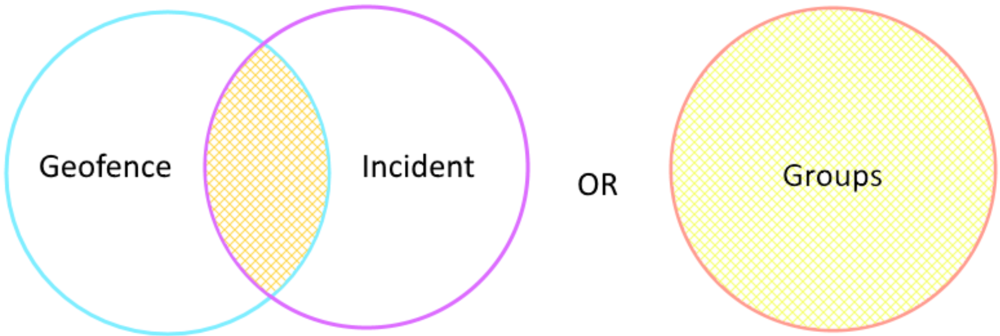
Incident Management
Default display in new dispatcher for dispatch tab view ?
Reserve Responders ?
OnScene Alert Age Seconds Threshold ?
Incident Creator effect on Incident Jurisdiction ?
Display expanded Source columns ?
Display expanded Control column ?

For example:

Jessica initiated an SOS call, which was created in the CC as incident no. 300. Jessica is a member of Group 10 which is associated with CC A. Although the incident was not located within one of the associated geofences, and incident type SOS isn't one of the authorized incident types, nevertheless, the incident will still be visible on CC A only because Jessica is a both the creator of incident no. 300 and is also a member of Group 10 which is associated to CC A.

To summarize:

The CC will display incidents where the incident type AND location match the CC jurisdiction OR any incident that was created by a user that is a member of one of the groups connected to the center.



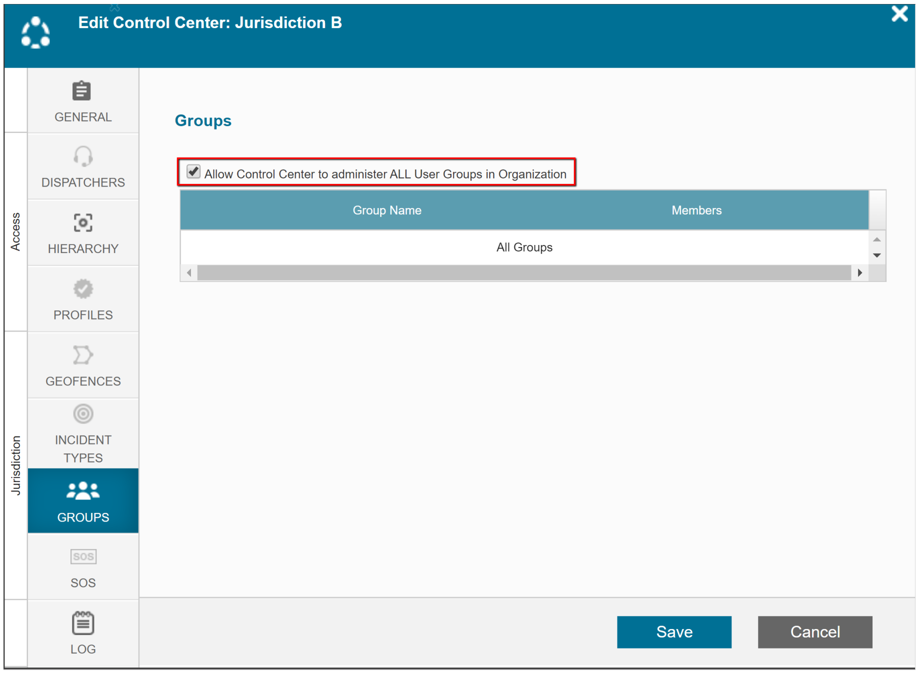
User Group Filtering

Each CC has jurisdiction over Users that are members of Groups associated with the CC. Any Group can associated with multiple Control Centers and ALL Groups are visible to the Main CC.

For example:

Control Center A is configured to have jurisdiction over Groups 10, 20 and 30. The Dispatcher John, is authorized to login in to CC A. Therefore, when John logs into CC A – he will be able to view, dispatch and communicate with all Users in Groups 10, 20 and 30.

> Note
> If you wish the Dispatcher to always have access to view any newly created Groups in the future - check "Allow CC to administer ALL User Groups".



Additional Users that May Appear in the CC due to Associated Incidents

Additional users that aren't usually associated with the CC may be visible if they happen to be users (Responders) in an incident is active that matches the criteria for incident filtering (as defined above).

For example:

Following the example above, (CC A can view Groups 10, 20, 30 and Dispatcher John has access to CC A) – Abe is not a member of any of these groups, yet he is a responder in an incident that matches the criteria for incident filtering (House Fire in East London). As long as the incident "House Fire" in "East London" is open, Abe will be visible to dispatchers logged into CC A.

Other Examples

John is a Dispatcher logged in to CC A – the CC has jurisdiction only over the "House Fire" incident type and "East London" polygon

- A new incident "Forest Fire" is created in the "East London" polygon. John didn't create the incident and none of the creators of the incident are in a group that fits the jurisdiction of CC A – In this case, John won't see the incident
- The incident is a "House Fire " outside the "East London" CC. John didn't create the incident and none of the contact persons in the incident are in a group that fits the joint jurisdiction of CC A – John won't see the incident

- The incident is a "House Fire" that happened outside the "East London" polygon, but John was the dispatcher who created that specific incident – John will see the incident AND any CC that has jurisdiction over John (via his group membership) will also be able to view this incident.
- The incident is a "Forest Fire" that is located outside the "East London" polygon. John did not open the Incident, but one of the creators of the incident (Caller/ Reporter etc.) is a member of a group that is under jurisdiction of CC A – John will see the incident

Other implications of the Control Center jurisdiction settings

Viewing Users on the Map

Only responders who belong to the groups under the jurisdiction of the Control Center will be seen on the map.

Additional responders that aren't associated with the secondary center may be visible if an incident is opened that fits the criteria for incident filtering (as defined above). These responders will only be seen while the incident is active.

Creating New Incidents

When creating new incidents in the Dispatcher, only incident types that are associated with the CC will be available for selection.

Dispatching Responders to Incidents

When dispatching responders to incidents, the only users that will be available for selection are users that are members of Groups associated with the center.

Control Center Access vs. Permission Profile

In order to allow more autonomy and flexibility in managing Control Centers while maintaining the privacy and security of each Center, you may grant access to Control Center while expanding or limiting specific functionalities of Dispatchers. In other words a Dispatcher with access to CC A may have more or less authority depending on the Dispatcher's permission profile in the system.

For example: Dispatcher John has access to CC A but has no permission to create Users or Assets.

Dashboard Business Intelligence (BI) Tool

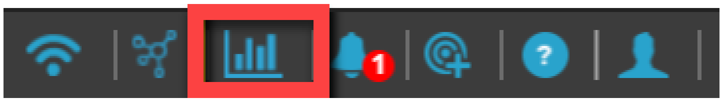
Dashboard is Symphia NowForce's Business Intelligence tool developed for quality of service analysis, event evaluation and enhanced performance reporting.

The Dashboards tool provides customers with a detailed analysis of the data collected in the system. The data is provided with clear visuals and also available in formatted reports, allowing for effective analysis to assist future decision making.

This tool is an add-on license to an existing Admin named user license in a SaaS environment.

▼ To access the Dashboard

Select the dashboard icon from the Dispatcher main task bar.



> **Note**
> If you do not see the Dashboard icon it may be either because you do not have the BI license added to your profile or because the dashboard has not been configured for your organization. To resolve this, contact NowForce Support.

Available Dashboards

There are a set of default dashboards pre-configured to your organization. These dashboards cover multiple domains of your operations on NowForce system: Users, Incidents, Geofences etc. Each dashboard can be filtered and modified based on time filters.

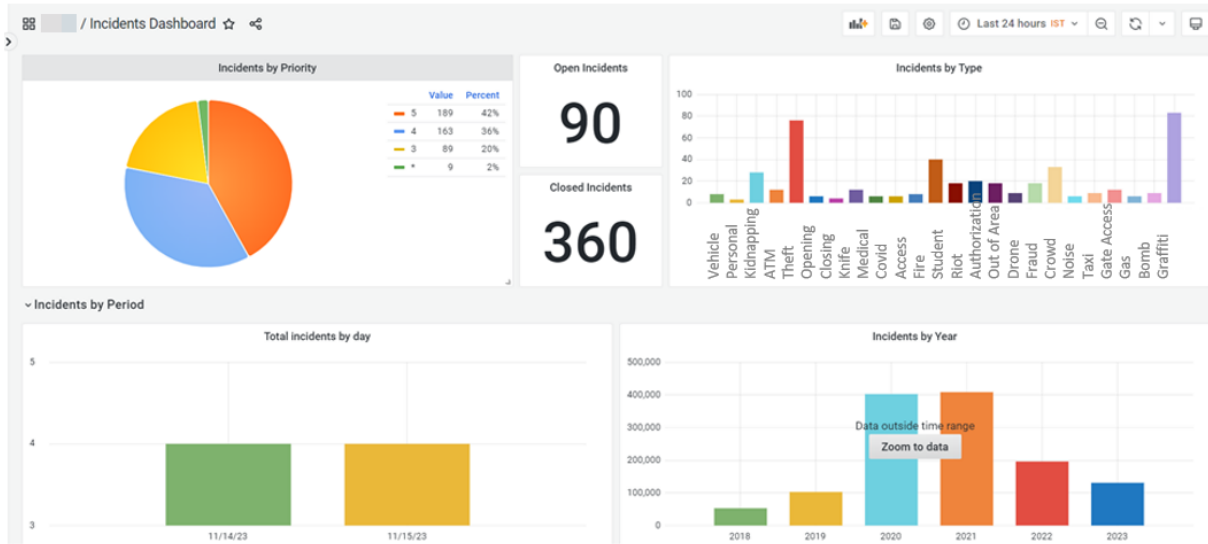
Incidents Dashboard

This dashboard provides an overview on incident statistics and allows you to drill down into the incident types and the status of incidents both current and closed in the organization.

The data is organized systematically into daily, monthly and annual occurance according to Incident type. Shown below is the following

- Incidents by priority
- Incidents by type

- Frequency of incidents (total) by day and year
- Incidents by month with an data table



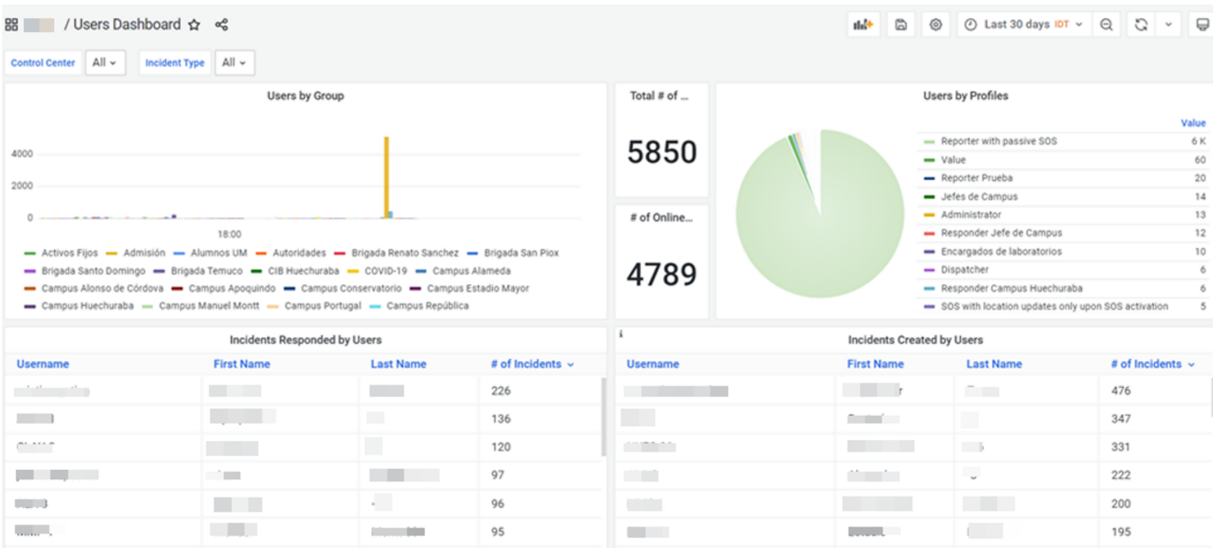
MissionID	MissionTime	Incident Type	Street	Comment
778658	2023-11-15 16:01	Unknown Vehicle	Smith Street	Reported to Metro
778657	2023-11-12 15:45	Site Opening	Grey Street	Confirmed
778656	2023-11-11 20:25	Closing	West Street	Confirmed
778655	2023-11-11 19:07	Suspicious Person	Umhlanga Boulevard	Reported to Metro
778654	2023-11-11 16:32	Medical	Stanger Street	SOP Medical
778653	2023-11-10 15:47	ATM theft	King Street	Under investigation
778652	2023-11-09 12:21	Crowd	10 Jubilee Gardens	Dispatched responders
778651	2023-11-10 08:32	Bomb Threat	West Street	SOP Bomb

Users Dashboard

The Users dashboard provides data per user group in your organization. Data is displayed by:

- Number of Users per Group
- Users allocated in each Profile

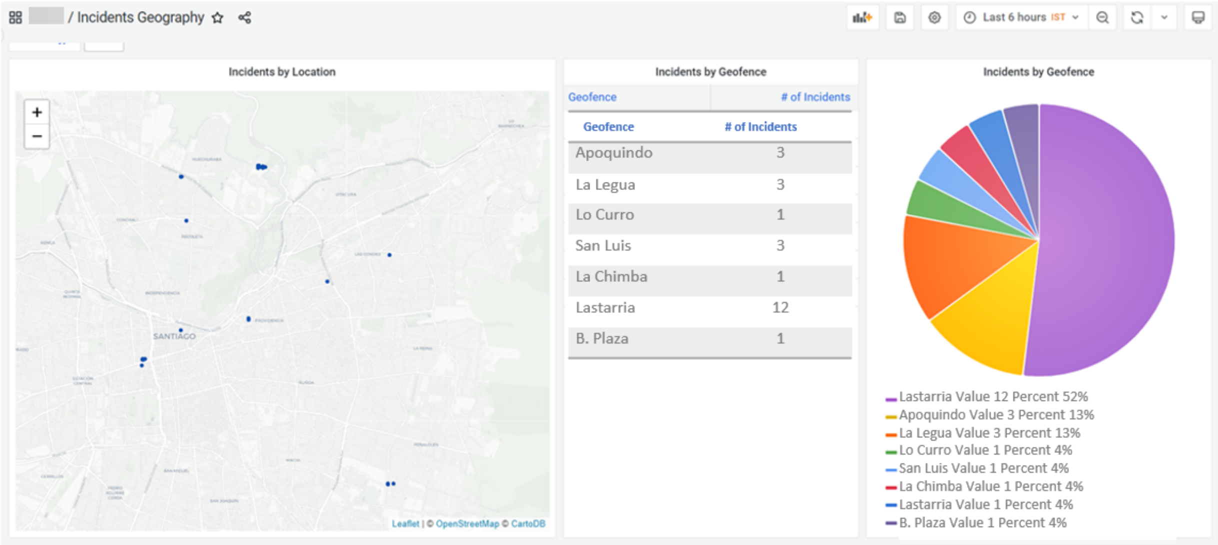
- Number of incidents created by Users (Reporters)
- The number of incidents responded to by Users (Responders)



Geofence and Map Data Dashboards

In addition to providing dashboards about Incidents and Users,your organizational data can be displayed according to your geofence boundaries. Dashboards providing mapped and geo-referenced data included the following as shown:

- Incidents by Location
- Incidents by Geofence (listed)
- Distribution of Incidents in Geofences (graphic)



Additional Dashboard Configurations

Additional bespoke Dashboards for your organization can be ordered from the NowForce Professional Services team. Contact NowForce Support for more information.

Setting up a background image URL for Mobile SOS

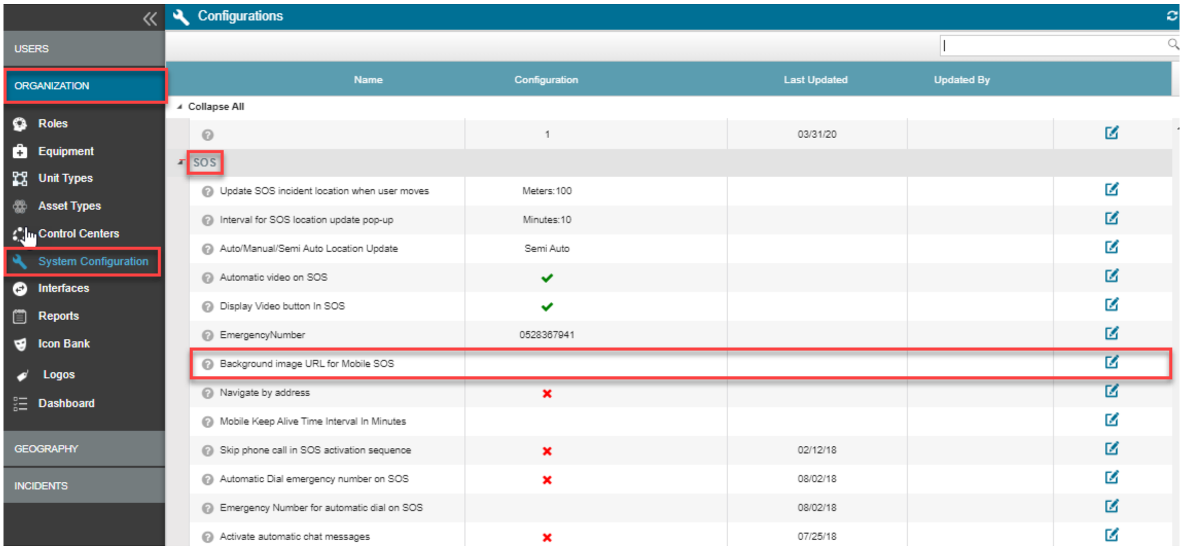
Each organization can be set up a custom entrance screen to the mobile application. This background image can be an image or a HTML page that can include a logo and a few sentences.

▼ To configure the background image

1. From the **Main** screen, select **Settings** > **ORGANIZATION**, and then select **System Configuration**.

The **Configurations** table opens.

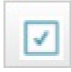
2. Scroll down to the **SOS** settings in the table.



3. Click on the  to edit the **Background image URL for Mobile SOS** setting.

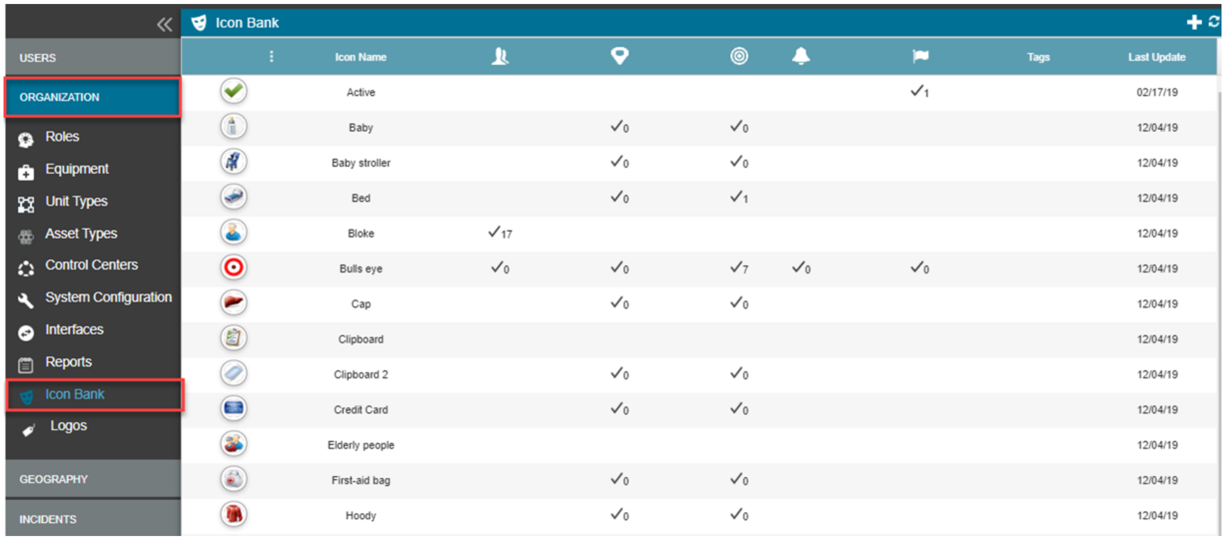
   The **Configuration** field becomes editable.

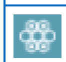
4. Make your changes.

5. Click  to save your changes.

How to Add and Manage Icons

You can upload the following file types: ICO, GIF, JPG or PNG. It is recommended that you upload small icons, no larger than 30x30 pixels to optimize display. All icons that are larger than 30x30 pixels will be resized automatically when uploaded.



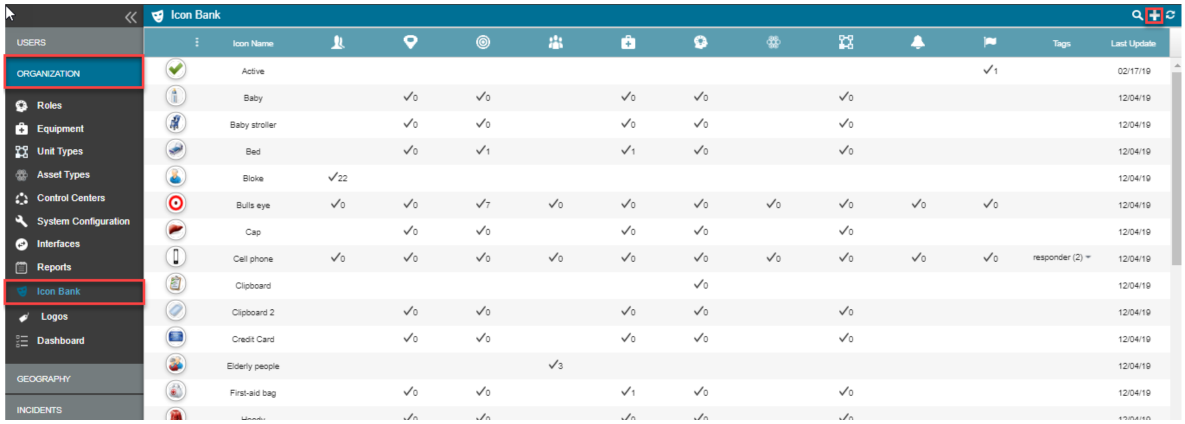
NowForce Icon	Description
	Incidents
	Point of Interest
	Users
	Groups
	Equipment
	Roles
	Assets
	Unit
	Alarms
	Dynamic Status

Adding Icons

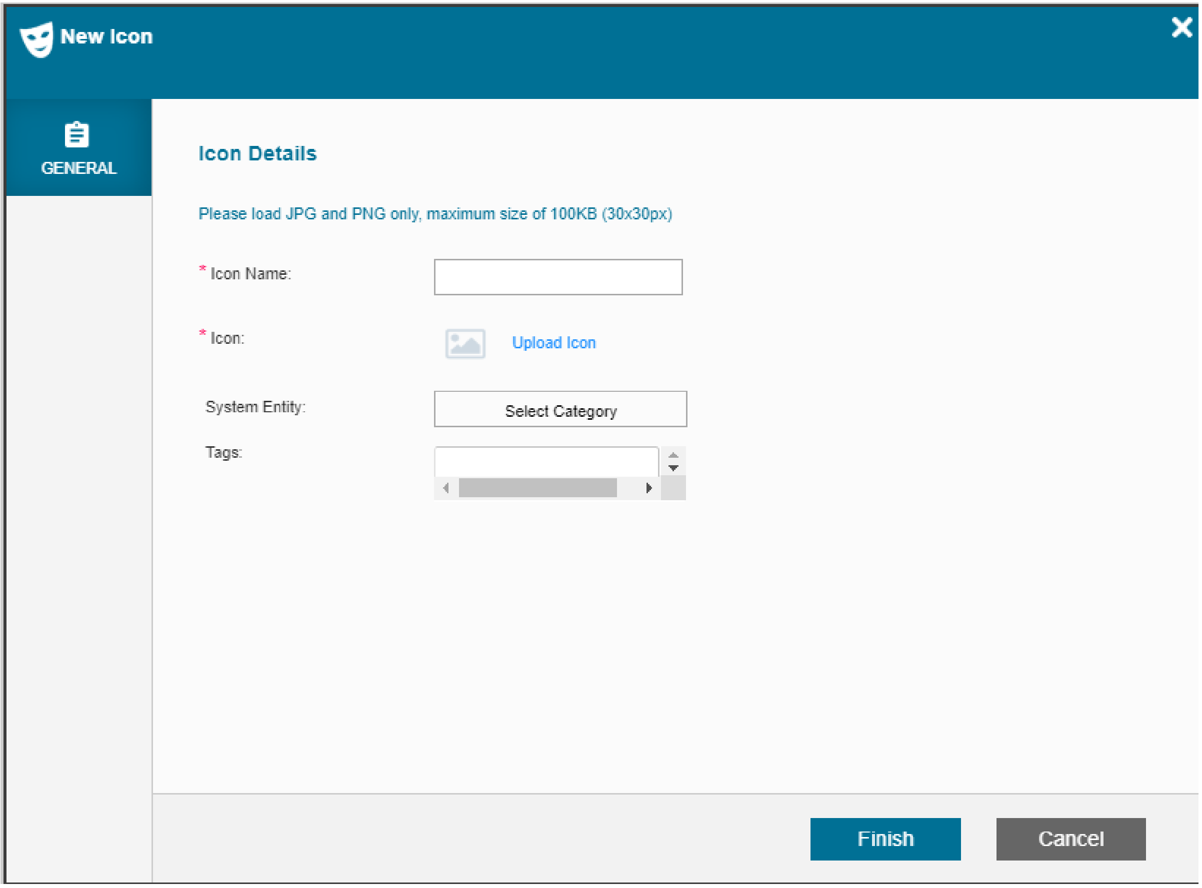
▼ To upload icons

1. From the **Main** screen, select **Settings** > **ORGANIZATION**, and then select **Icon Bank**.

2. Click the **+** to add a new icon.



3. New Icon window opens.



4. Complete the **Icon Name** field.
5. Click **Upload Icon t**o select the image file for upload.

   Your uploaded icon image displays.
6. Select all relevant System Categories in the **System Entity** field.
7. Click **Load Icons**. A dialog box opens, showing the file explorer.
8. Choose the file/files you want to upload and click **Open**.

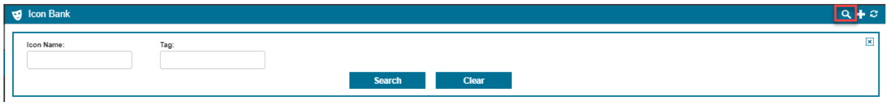
   The files will be uploaded into the Icon Bank.
9. Click **Finish**.
10. The **Icon Bank** table opens, with icons listed in alphabetical order.

    The Search By Name option is located on the top right of the Icon Bank. You can use this to search for individual icons by name

▼ To search by name

1. **Click** the magnifying glass.

   The **Icon Search** box opens.



2. In the text box, type the name or part of the name of the icon.
3. Click **Search**.

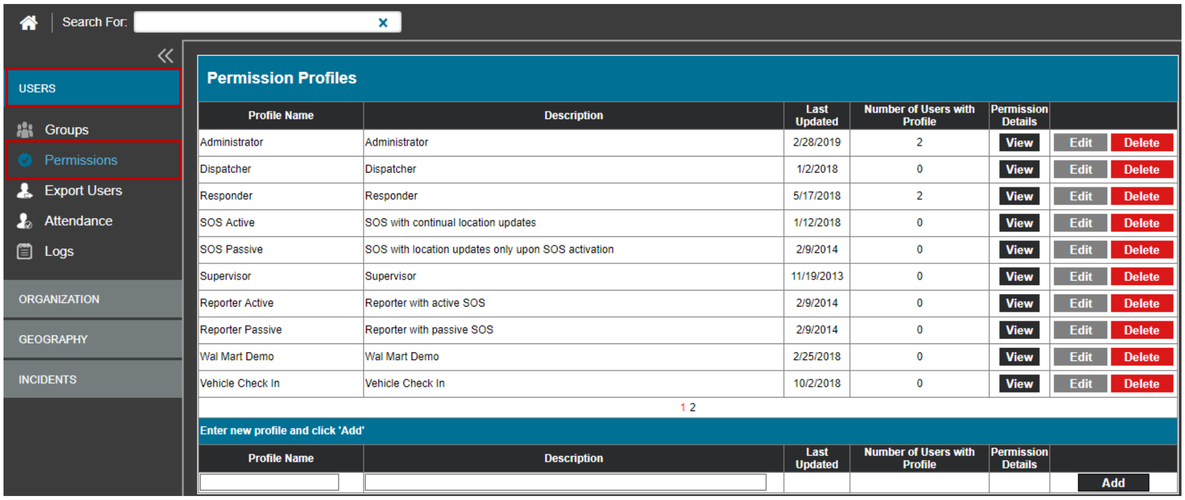
Configuring Two Factor Authentication Permissions

Two Factor Authentication provides an extra layer of security that enables you to verify the identity of a user when they log in to the Dispatcher or the mobile app. These permissions are not configured by default, and must be added, as required, to the respective user profiles.

▼ To add the permission to a user profile

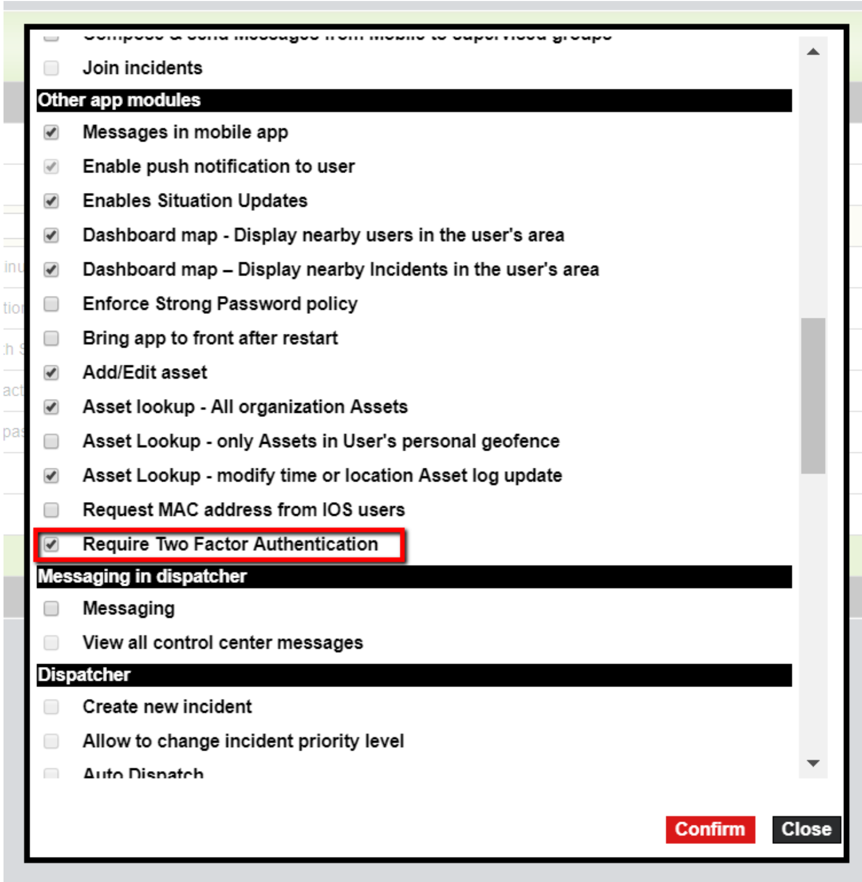
1. In the **Dispatcher** screen, click **Settings>Permissions**.

The **Permission Profiles** table opens.

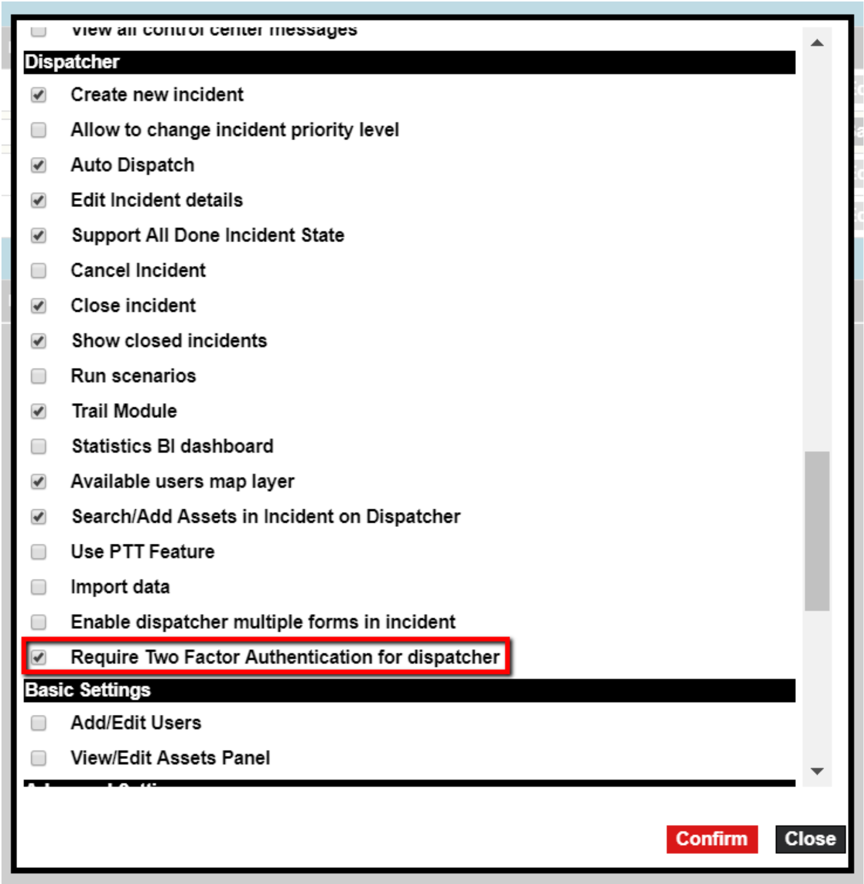


2. Select the profile you want to change, and click **Edit**, and then click **Edit** again to edit it's permissions.
3. Scroll to the **Other app modules** section to add the **Two Factor Authentication** to an app user profile.

4. Select **Require Two Factor Authentication**.



5. If you want to add the **Two Factor Authentication** to a dispatcher user profile, scroll to the **Dispatcher** section.
6. Select **Require Two factor Authentication for dispatcher**.



7. Click **Confirm**.
8. In the Settings page, click **Save**.

Configuring Location Settings for Mobile App Users

You can configure the rate and accuracy settings for Mobile app users within the Location Settings. This allows you to set parameters for your organization's sampling requirements while giving consideration to app users' mobile battery usage. The settings differ for Android and IOS devices. Set parameters for both operating systems.

To define exceptions to the general location sampling settings, use the **Exceptions for Routine State** area. You can also define the length of time to save the history of user locations on the mobile device.

Android Location Settings

The Android location settings define when an Android device sends its location to the server. This applies both while the app is running in the foreground and in the background. The Android Location settings apply to an IOS device while the app is running in the foreground only.

The location settings include **Frequency** and **Accuracy.**

Frequency

- These are the intervals between location sampling.
- Minimal sample rate (interval) is 0.17 minutes.
- Maximum interval is set by the number entered by the Admin. The application will try to sample a location at 85% of that interval time defined taking in to account several factors that tries to optimize the battery consumption and device performance

Accuracy

- None - no location sampling
- Low - ~10Km accuracy
- Balanced - ~100m accuracy
- High - best accuracy (usually the device location based on GPS).

IOS Location Settings

The IOS location settings define when an IOS device sends its location to the server while the app is running in the background.

The location settings include **Distance** and **Accuracy**.

Distance

- The minimum change in distance that triggers sending the app's new location to the server.

Accuracy

- Best for navigation
- Nearest 3 feet
- 328 feet
- 0.6 miles
- 1.86 miles

User States

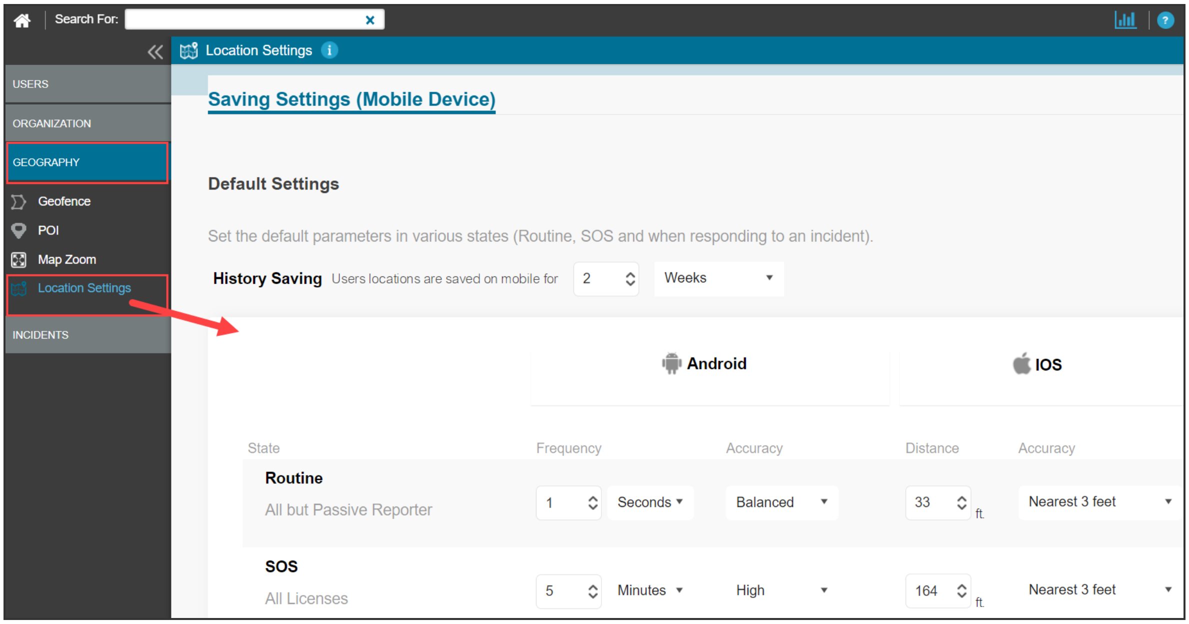
Location parameters are defined for each of the following user states.

- **Routine -** will sample a Responder App user at this rate and accuracy when the user is not in the midst of responding to an incident.
- **In SOS Mode -** will sample a Responder/Report/SOS App user at this rate and accuracy once the user has activated the emergency SOS notification on their phone.
- **En Route -** will sample a Responder/Reporter App user at this rate and accuracy once the user has reported to dispatch that they are "En Route" to the scene of an incident.
- **On Scene -** will sample a Responder/Reporter App user at this rate and accuracy once the user has reported to dispatch that they have arrived "On Scene" to an incident.

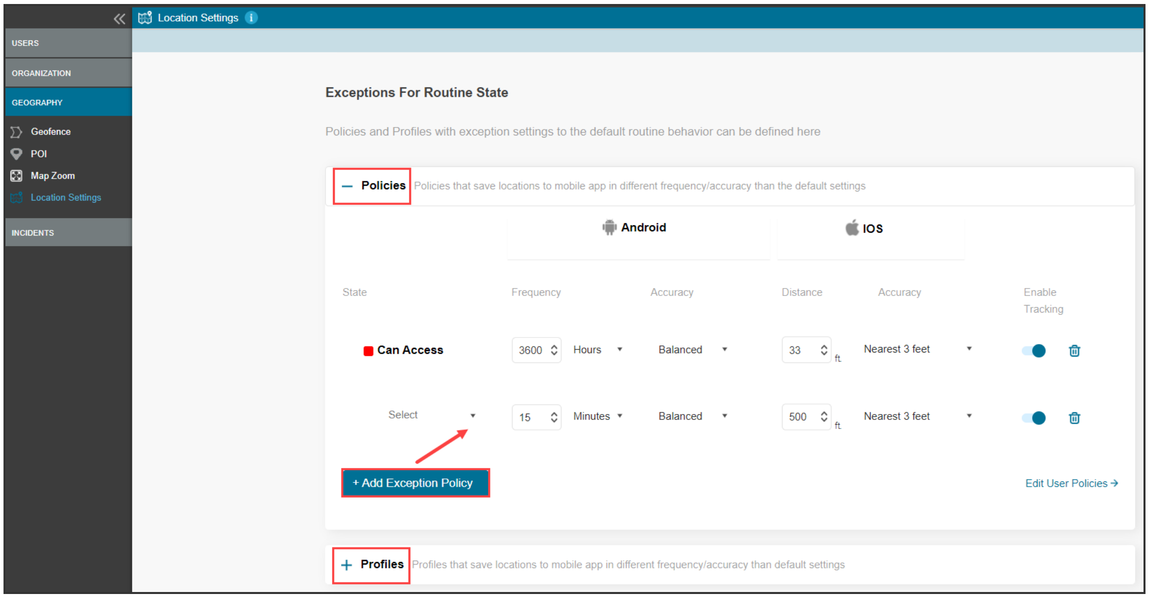
▼ To configure the Location settings

1. From the **Main** screen, select **Settings** > **GEOGRAPHY** and then select **Location Setting**.

The **Location Settings** table opens.



2. Use the dropdown menus to select the required new settings.
3. (Optional) To add exceptions to the location settings, in the **Exceptions For Routine State area**, do as follows:
   a. Expand either **Policies** or **Profiles**.
   b. Click **Add Exception Policy/Profile**.



   c. Use the dropdown menus to select the required settings.

> **Note**
> If a policy or profile does not exist, you must add a policy or profile before creating an exception.

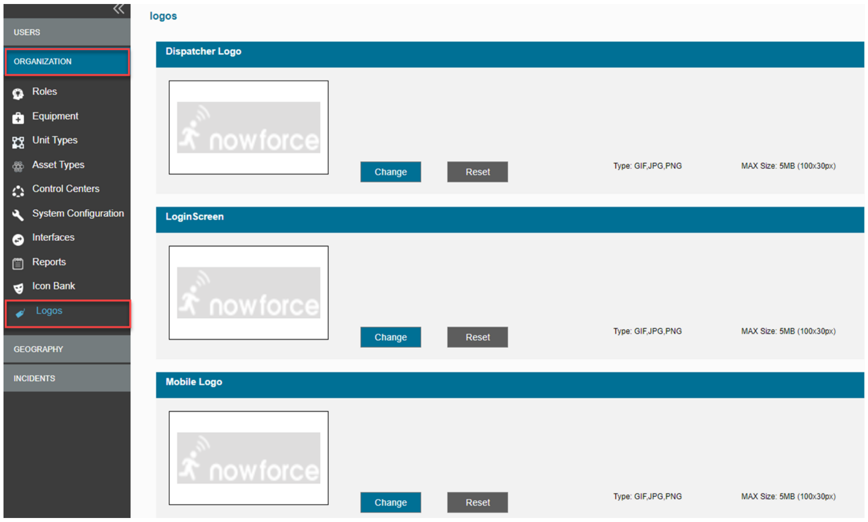
4. Click **SAVE** to save your changes.

Changing Logos in NowForce

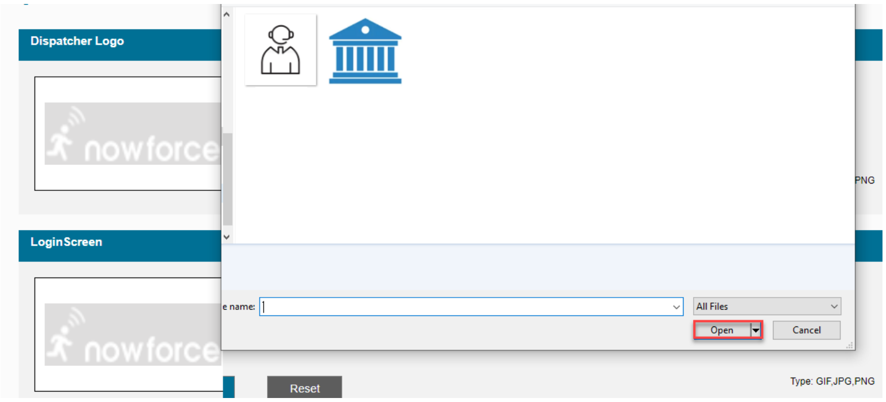
You can personalize the displayed logo on the **Dispatcher** main screen, **Login** screen and your **Responder** mobile app by replacing the default NowForce logos with customized images.

▼ To update a logo

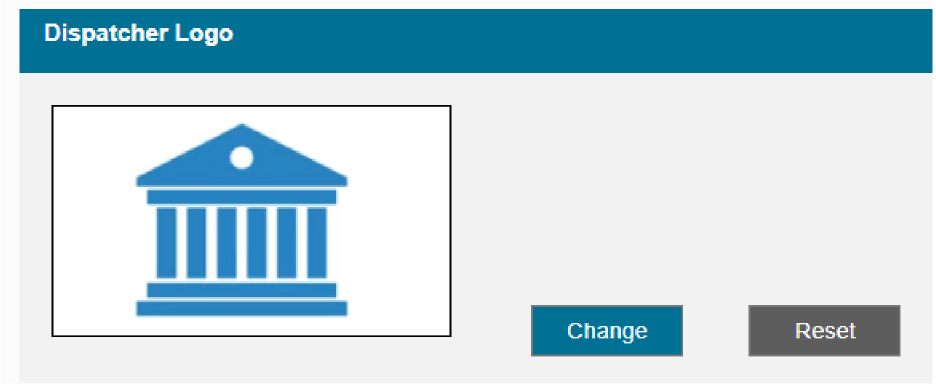
1. From the **Main** screen, select **Settings** > **ORGANIZATION** > **Logos**.



2. Next to the logo image you want to change, select **Change**.
3. Locate and select the new logo image, and click **Open**.



The image appears in review in the logo box.



4. Select the to close the logos settings page

> **Note**
> - The size of the new logo image can impact the speed of the image upload.
> - Image files must be in GIF, JPG or PNG format with a maximum size of 5MB (resolution 100 x 30px).
> - Updates to a mobile logo occur when the mobile device next synchronizes to the server. The mobile application synchronizes automatically when a user logs in. You can manually sync by going to the Info menu on the mobile device and selecting Sync.

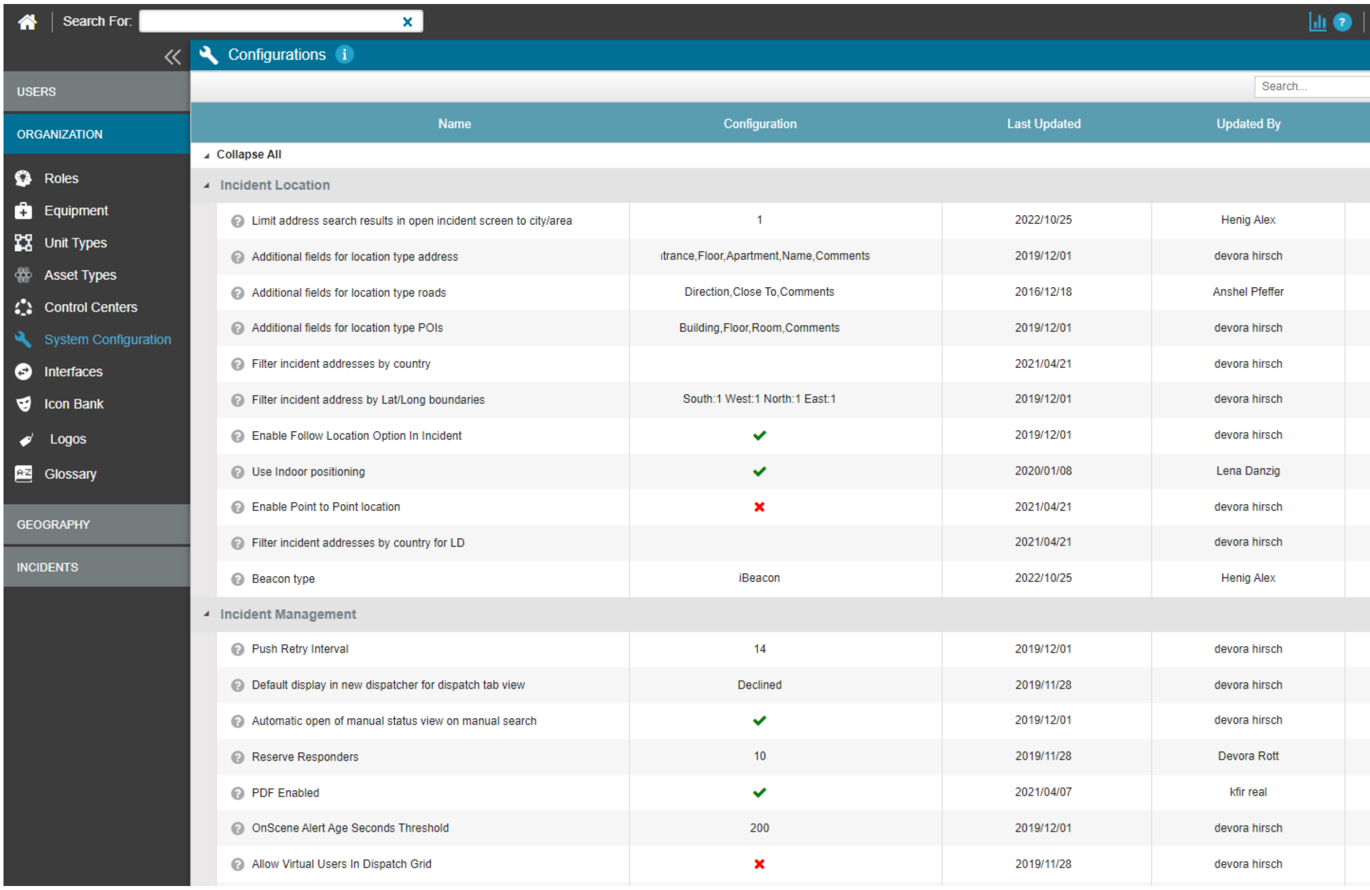
Changing Your Organization's Time Zone

You can change the time zone setting in the System Configuration settings.

▼ To change an organization's time zone setting

1. From the **Main** screen, select **Settings** > **Organizations**, and then select **System Configuration**.

The Config table opens.



2. In the **Config** table, go to **Generic** > **Organization Time Zone**.
3. Click **Edit** and select a time zone from the list.

Generic				
Enable Follow Location Option In Incident ?	✓	2/28/2019	A dispatcher	Edit
Organization's MXD layer ?				Edit
Ignore Cell Based Location Updates from mobiles ?	✗			Edit
Time in minutes to determine no communication from client to server ?	2880	8/29/2018	A dispatcher	Edit
Organization Time Zone ?	IST			Edit
Support Units ?	✓			Edit
Inactivation of Role/Equipment ?	✓	10/19/2017		Edit
Enable CLI ?	✓	6/5/2019	A dispatcher	Edit
PDF Sections ?	Details , Callers , TimeTableUsers , IncidentCommentSection , DynamicFieldsSection			Edit
Calculate ETA using routing ?	✓	7/4/2018	A dispatcher	Edit
Completion time (in minutes) for each incident for Cumulative ETA calculation ?	30	7/4/2018	A dispatcher	Edit

4. Click **Save**.

Incident Infrastructure Settings

The Incident module in Dispatcher and NowForce Mobile App is the core of the NowForce system, and brings together all the sub-systems users, maps, equipment, roles, groups, assets, messaging etc.

Before you begin

All the User, Geography and Organization settings of the related sub-systems, supporting the Incident module, must be configured prior to configuring any of the Incidents settings.

> **Tip**
> The administrator should configure settings for Forms, Dispatch Requirements, SLA, Statuses, Alerts prior to undertaking the Incident Types settings.

Receiving and Configuring Alerts 126
Incident Log Icons 128
Defining Asset Types 129
Creating and Editing Form Templates 132
Attaching Form Templates to an Incident Type 138
Customizing Form Templates Assets 140
Configuring Multi Forms Permissions 142
Understanding Multi Forms 145
Adding and Modifying Incident Dispatch Rules 150
Managing Incident Types 156
Limiting Address Search Results in Incident Screen 165
Adding Situation Reports to Incident Types 166

Receiving and Configuring Alerts

Receiving Alerts in NowForce Dispatcher

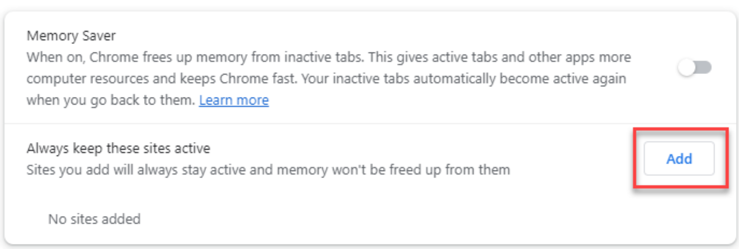
The NowForce Dispatcher web application is supported by Google Chrome browser.

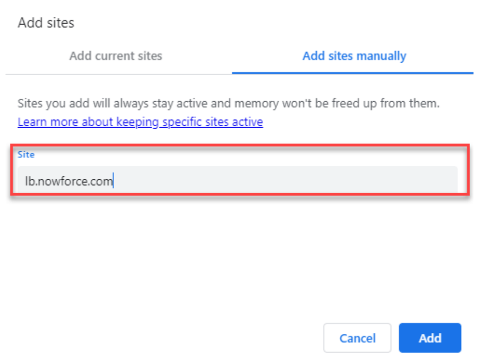
NowForce Dispatcher only receives audible alerts when NowForce is the open and active Chrome tab.

> Tip
> If the Dispatcher tab in your browser is not your main active working tab, we recommend you follow the steps below to configure your Chrome web browser to ensure that you always receive audible alerts for NowForce Dispatcher.

▼ To ensure that you always receive alerts set your NowForce site to active and create a shortcut to the site.

1. In your Chrome browser, click the ⋮ (Customize and control Google Chrome) from the context menu select **Settings**> **Performance**>**Memory Saver** .
2. Click **Add** and provide the site name.





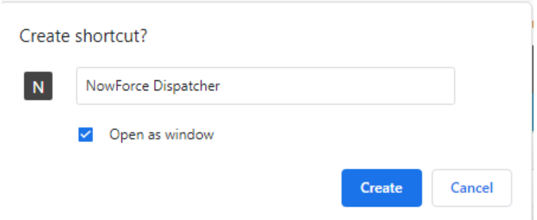
3. Click **Add**.

Your NowForce Dispatcher tab will always be kept active in Chrome.

> Tip
> In addition, set your NowForce Dispatcher site as a pinned shortcut on desktop taskbar. This ensures that your NowForce Dispatcher is saved as a web application and is always available to the operator.

4. In your Chrome browser, click the ⋮ (Customize and control Google Chrome) from the context menu select **More tools**> **Create Shortcut...**.

5. On the popup message, select the checkbox **Open as a window** and click **Create**.

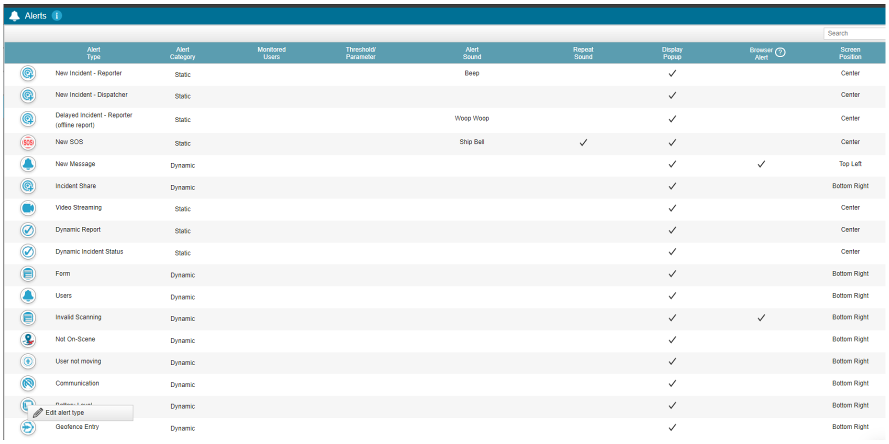


Your NowForce Dispatcher web application shortcut is created and pinned to your taskbar.

Configuring Alerts

Alerts are used raise awareness of a task or activity that requires the users attention in the system. Incidents have many different kinds of alerts and these can be managed from within the Alerts settings.

1. From the **Main** screen, select **Settings** > **INCIDENTS**, and then select **Alerts**.

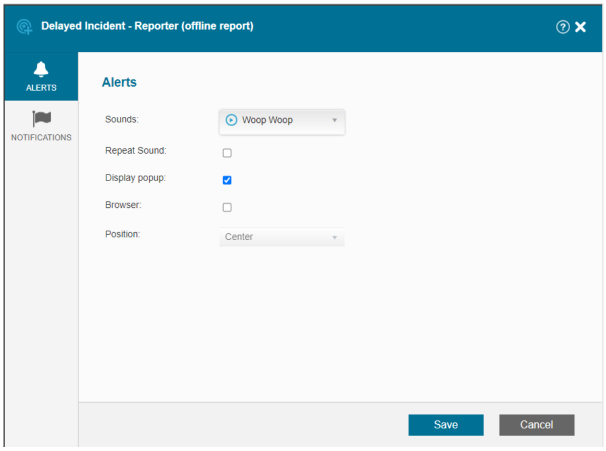


Alerts

Alert Type	Alert Category	Monitored Users	Threshold/ Parameter	Alert Sound	Repeat Sound	Display Popup	Browser Alert	Screen Position
New Incident - Reporter	Static			Beep		✓		Center
New Incident - Dispatcher	Static					✓		Center
Delayed Incident - Reporter (offline report)	Static			Woop Woop		✓		Center
New SOS	Static			Ship Bell	✓	✓		Center
New Message	Dynamic					✓	✓	Top Left
Incident Share	Dynamic					✓		Bottom Right
Video Streaming	Static					✓		Center
Dynamic Report	Static					✓		Center
Dynamic Incident Status	Static					✓		Center
Form	Dynamic					✓		Bottom Right
Users	Dynamic					✓		Bottom Right
Invalid Scanning	Dynamic					✓	✓	Bottom Right
Not On-Scene	Dynamic					✓		Bottom Right
User not moving	Dynamic					✓		Bottom Right
Communication	Dynamic					✓		Bottom Right
[illegible]	Dynamic					✓		Bottom Right
Geofence Entry	Dynamic					✓		Bottom Right

2. To edit an Alert types, stand on the Alert type and choose **Edit alert type**.

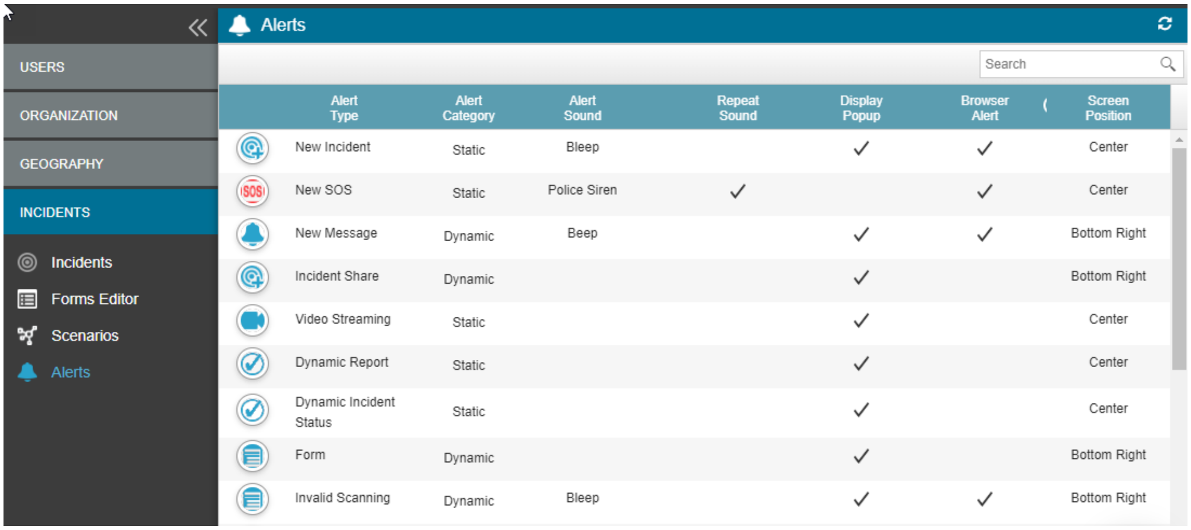
3. The Alert Type window opens, and you can configure the alert.



4. When you are done, click **Save**,

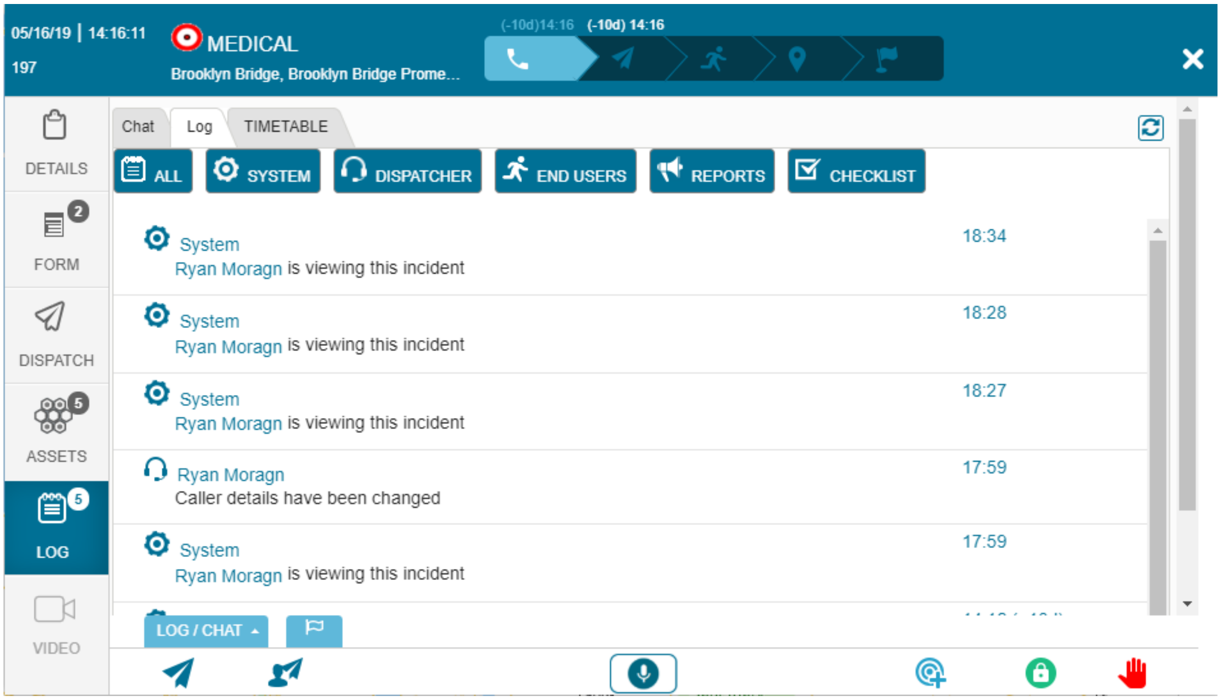
Putting SOS Alerts on Repeat

You can select if you want an SOS incident alert to play only once or in a repeat loop by check/unchecking the **Repeat Sound** option for the **New SOS** alert type.



Incident Log Icons

Incident log icons enable you to quickly identify the source of the log entry.



Icon	Log Source
	Dispatcher log
	Mobile user log
	Item logged automatically by the system

Defining Asset Types

Administrators define specific asset types according to the asset category.

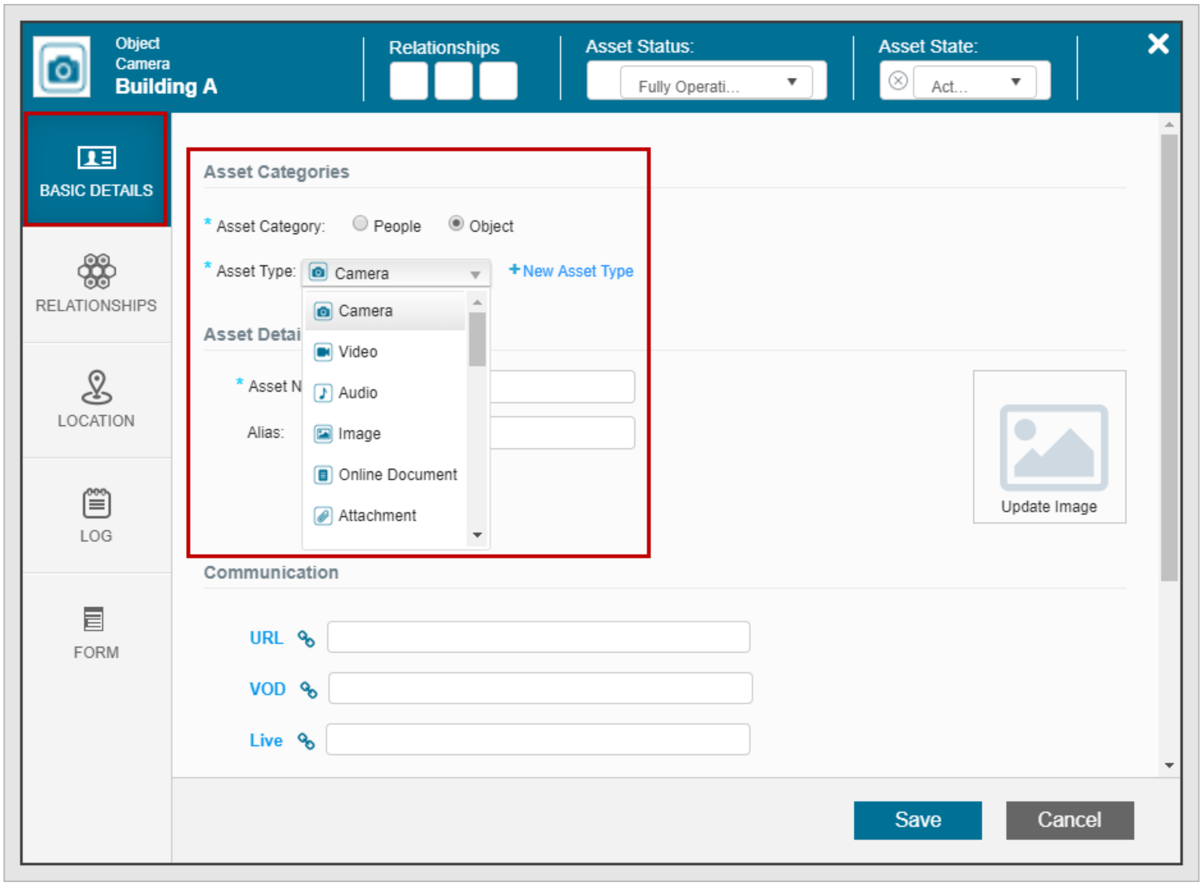
Example

- In the Objects asset category, you can have assets types such as cameras, exit doors, fire hydrants, and so on.
- In the People asset category, you can have asset types such as contacts, black or white lists, and so on.

For more information on assets, see Assets Overview.

You can only select one asset type per asset category. The asset type also includes an asset icon, the asset layer on the map and the asset form.

Define the asset type in the **Basic Details** tab.



NowForce is installed with default assets types, and you can chose whether to use a default asset type or whether you want to create a new asset type.

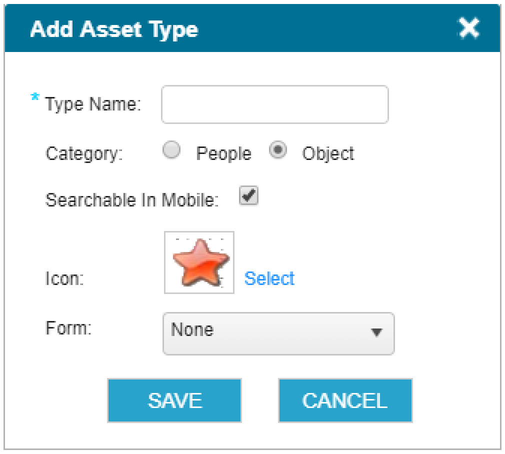
> Note
> You cannot edit a default asset type nor do they have a form associated.

Creating a New Asset Type

Create new asset types in the Basic Details tab of the Assets panel.

▼ To create a new asset type

1. Open the **Assets** panel, as described in Assets Overview.
2. In the **Basic Details** tab, click **+New Asset Type**.



3. Enter the following details:

   - In the **Type Name** field, enter the name of the asset type.
   - Select if the asset **Category** is **People** or **Object**.
   - Select the **Searchable in Mobile** check box if you want the asset type searchable on mobile devices.
   - Select the **Icon** you want associated with this asset type.
   - From the **Form** dropdown list, select the form for this asset type. If there is no form created for this type of asset you can create a new form as described in Customising Form Templates for Assets.

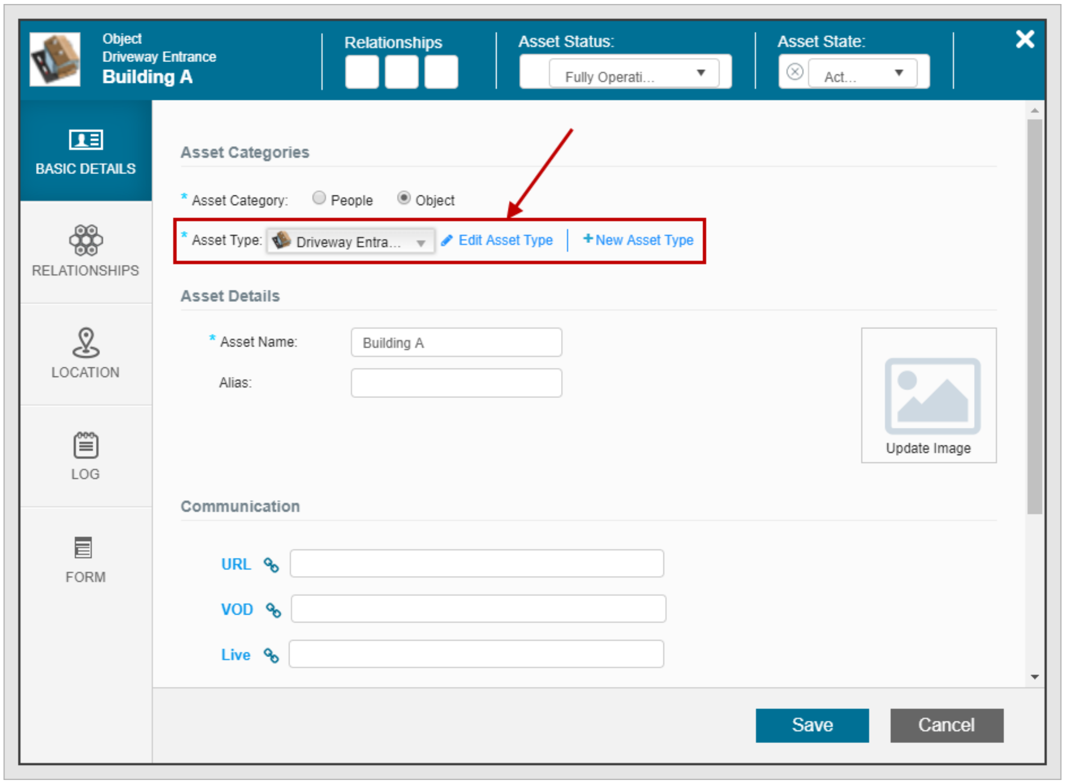
4. Click **Save**. The new asset type appears in the **Asset Type** dropdown list.

Editing an Asset Type

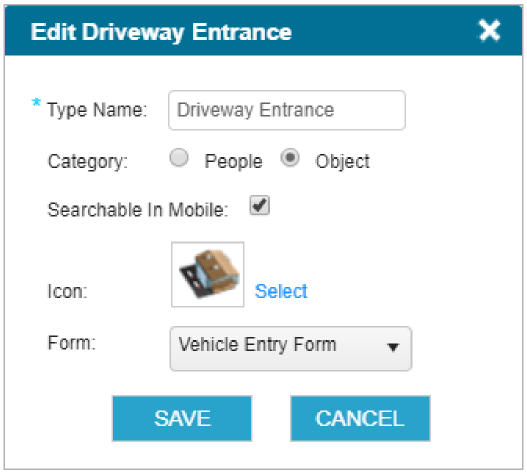
You can only edit asset types that you have created and only if the asset type is not associated with an asset. This means that you cannot edit any of the default asset types.

▼ To edit an asset type

1. Open the **Assets** panel, as described in Assets Overview.
2. In the **Basic Details** tab, click **Edit Asset Type**.



The Edit Asset Type window opens.



3. Edit the fields as required.
4. Click **Save**.

Creating and Editing Form Templates

Form Templates are pre-configured digital documents that are associated with an:

- **Incident**: Form templates enable responders to report relevant information from the field to the dispatcher and vice versa. You can attach one or more form templates to each incident type. These forms appear in the Dispatcher and in the mobile application when an incident is launched.
- **Asset**: Form templates provide the Dispatcher and the mobile application additional information about an asset. Each asset can have only one form attached to it. The asset form is accessible and can be edited by any user with the correct permissions (Dispatcher or mobile application user).
- **User Update**: Form templates enable users to share updates relevant to their status or resource requirement. You can attach one ore more form template as an in-incident user update or as part of a policy to determine transition of a user from one policy to another.

This topic describes how to create a form template. After you complete the creation of the basic form template, continue with the specific procedure to customize the form template for incidents or assets.

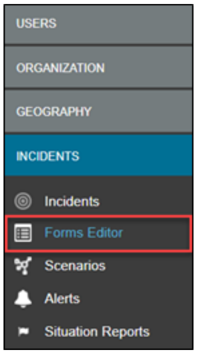
Creating Form Templates

To create a new form in the system, you must have the correct permissions to access the system's settings.

▼ To create a new form template

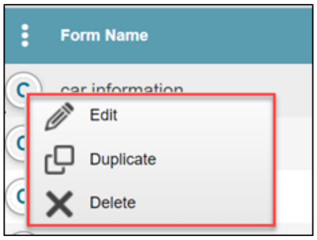
1. Click **Settings** (gear) in the upper left corner of the **Dispatcher** screen.

2. Click the **Incidents** tab, and then select **Forms Editor**.



3. In the Forms Table, you can:

- Create an entirely new form from scratch, by clicking on the **+** or,
- Duplicate an existing form and edit its contents by selecting the form, right-clicking, then selecting the **Duplicate** option.

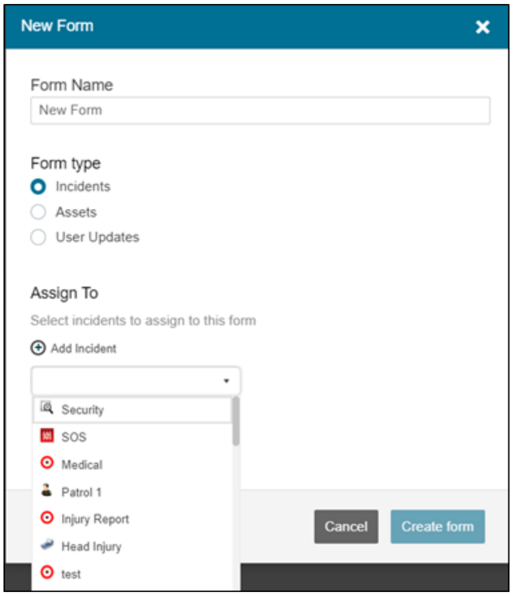


Creating a New Form Template

You can create a new template from scratch.

▼ To create a new form

1. In the **Forms** table, select **+**. The New Form window opens.



2. Add a name in the **Form Name** field.
3. Assign it a **Form type**.
4. If you selected Form Type ***Incidents***, then in the **Assign to** dropdown appears and you can select all of the Incident Types that this form will be assigned to.
5. Click **Create form**.

Form Fields

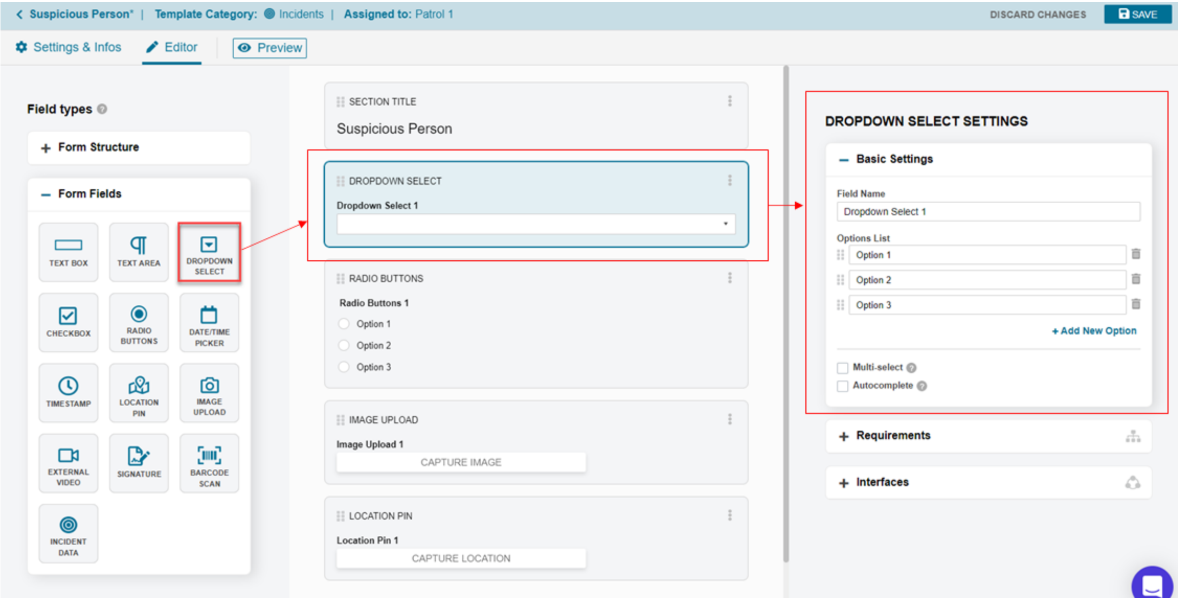
After creating a new template, you must populate it with the required fields. The following fields are available to build your form template.

- **Text Box**: Free text area limited to a defined length.
- **Text Area**: Free text area in which you can enter a description of the incident/assets (limited in size according to your defined settings)
- **Section Title**: Form/section header
- **Radio Buttons** (**+Panel**): Create a list of options, from which the user can select one or more options.
- **Checkbox**: Enables the user to an option.
- **Image Upload**: Enables the user to capture and send an image.
- **Date Time Picker**: Enables the user to enter a date and time.
- **Location Pin**: The latitude and longitude of the user/incident.
- **Time Stamp**: The time the form was completed.
- **Signature**: Enables the user to insert a signature into the form.
- **External Video**: Enables the user to capture and send a video.
- **Panel**: The panel to which the radio buttons are added.
- **Dropdown Select**: Enables the user to choose from a dropdown list.
- **Barcode Scan**: Enables the user to scan a QR code and compare that scanned code against a predefined list.

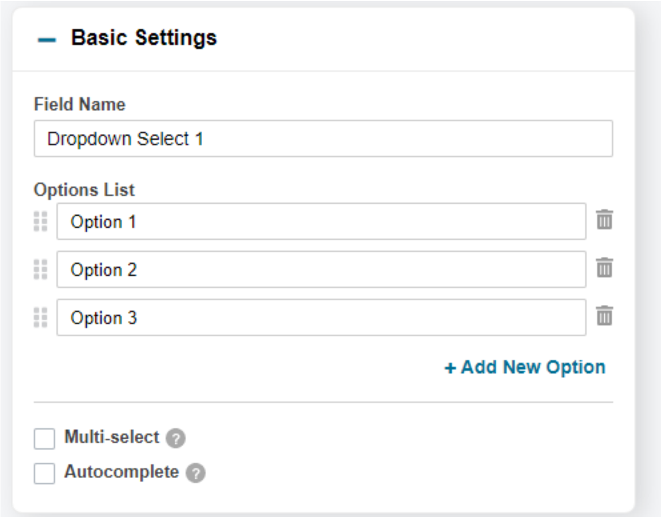
In the context of the above definitions, the user refers to the person completing the form template.

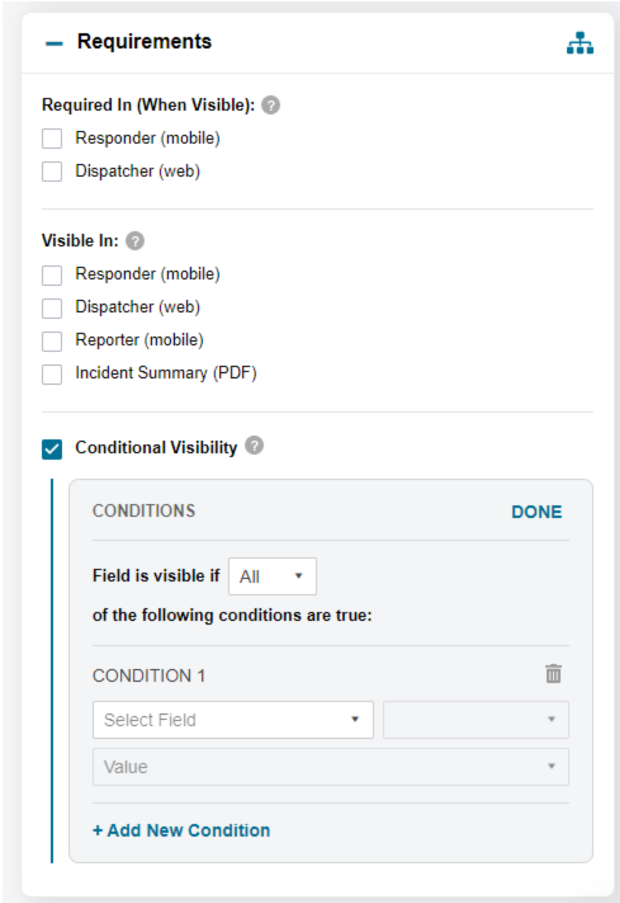
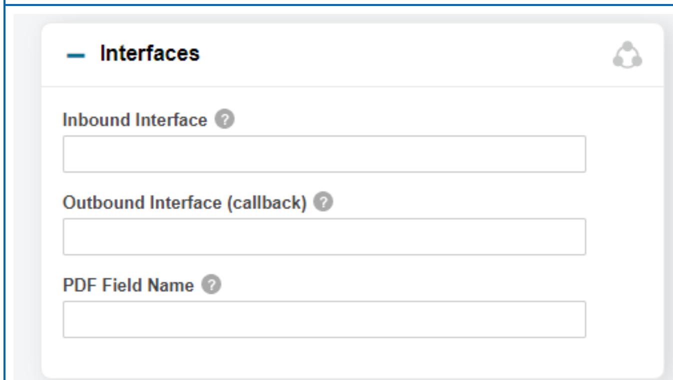
▼ To populate a form template

1. Drag and drop the required fields from the left panel into the form workspace.



2. To edit a field, click on the field to open the list of **Settings** that relate to that form. These include **Basic Settings**, **Requirements** and **Interfaces**.

	The **Basic Settings** lets you configure the field with a name, number of selectable options. Where available, multi-select and autocomplete can be added to the field.

	**Requirements** settings allow you to set the field visible to different types of users in Dispatcher and Mobile, as well as set the terms of Conditional Visibility for the field.
	**Interfaces** configurations allow you to specify field names for the API integrations your organization may have, as well as set the PDF field name for the form.

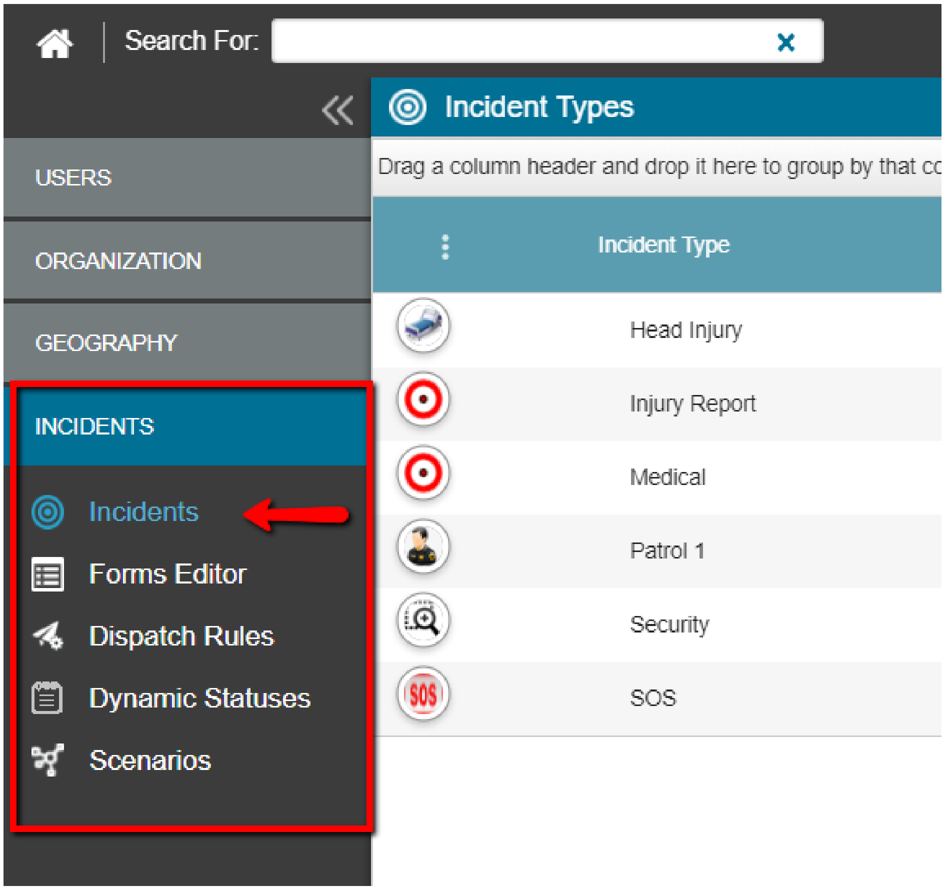
3. Repeat the process until you have all the fields inside of your form.
4. Click **Save**.

Attaching Form Templates to an Incident Type

Forms enable responders to report relevant information from the field to the dispatcher and vice versa. You can attach one or more form to each incident type when creating a new incident type or by editing current incident types, see Managing Incident Types and Creating and Editing Incident Form Templates.

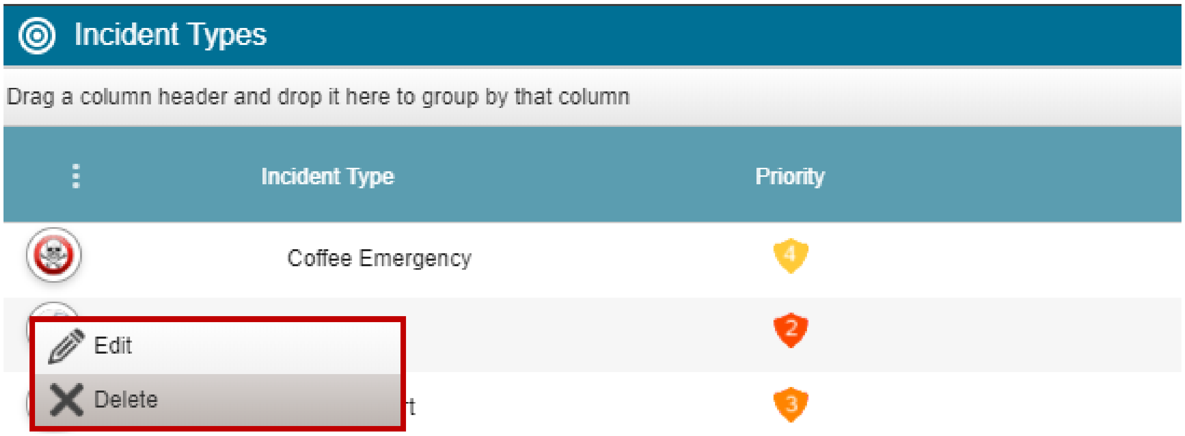
▼ To attach forms to an incident type

1. From **the** Main Screen select **Settings** > **INCIDENTS**, and then select **Incidents**.



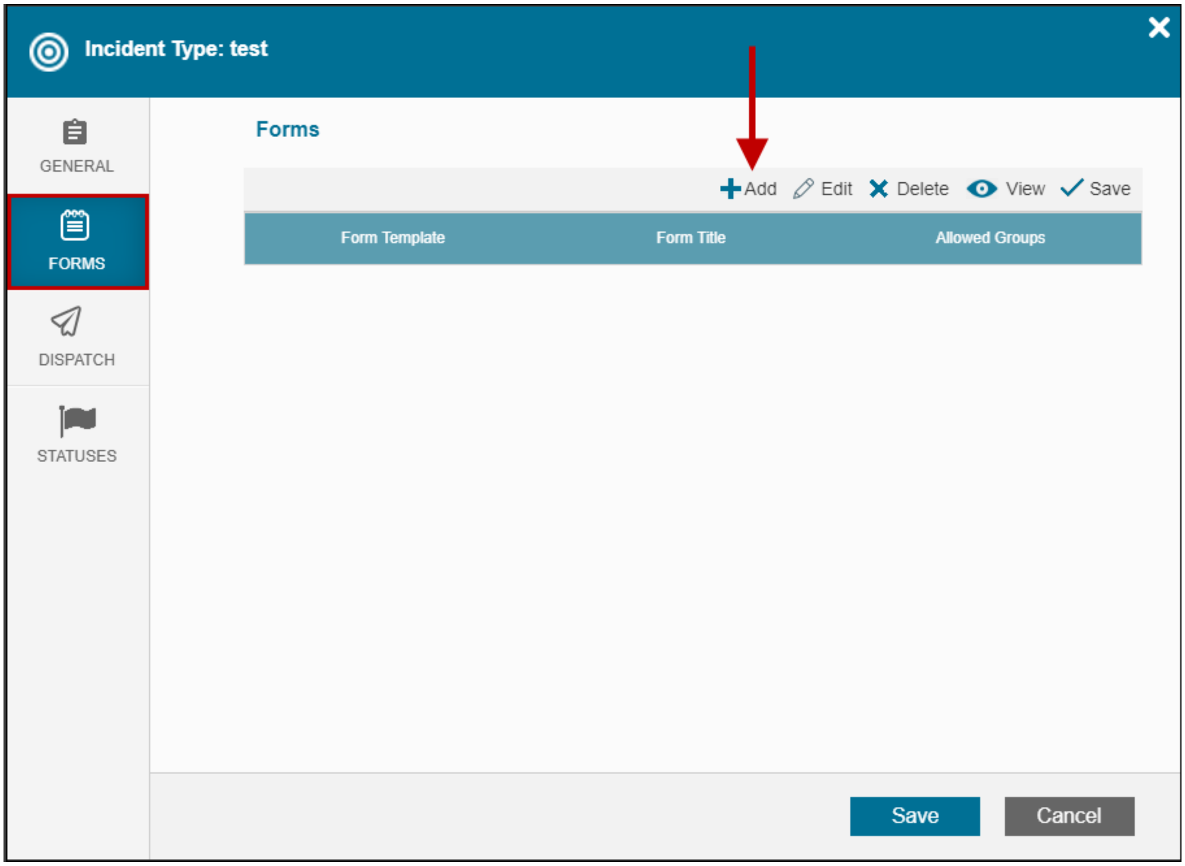
The Incident Types table opens.

2. Stand on the **Incident Type** you want to add a **Form** to, and click **Edit**.

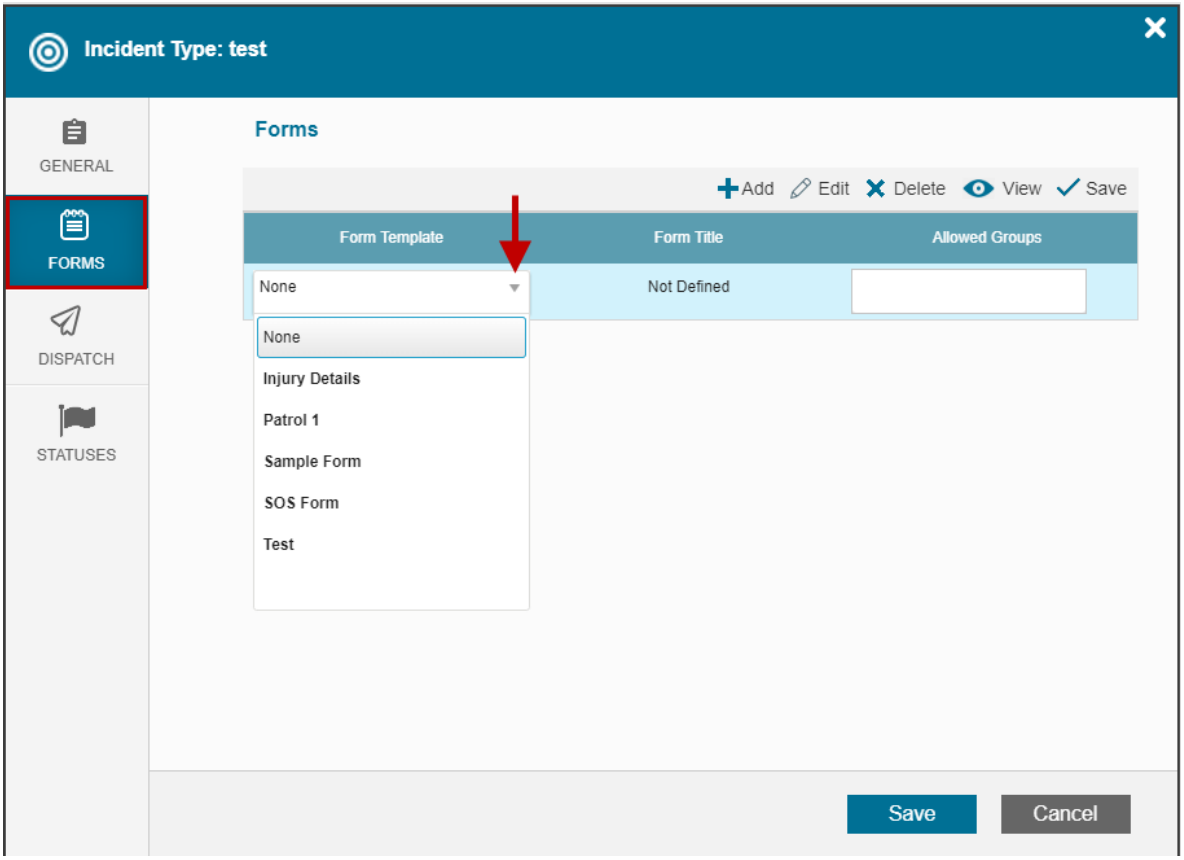


The incident type window opens.

3. Select the **Forms** tab.



4. Click **+ Add** to add a form.



5. From the dropdown select the **Form Template** you want to you wish to add to the **Incident Type**, and the **Allowed Groups**.
6. Click **Save**.

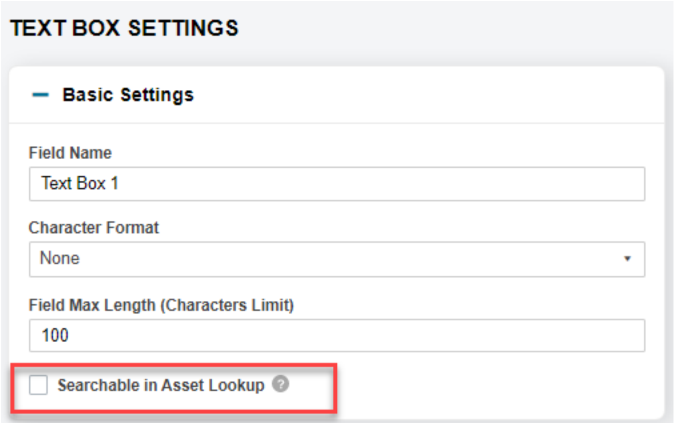
Customizing Form Templates Assets

Forms are pre-configured digital documents that are associated with an asset type to give the users (dispatchers and mobile app users) specific information about the asset. Each asset type has one form attached to that sis appears in the **Asset Form** tab. The asset form and its information is accessible and can be edited by any user with the correct permissions (dispatchers and mobile app users).

The procedures described in this article are a continuation of the procedures described in [Creating and Editing Form Templates.]

Searchable Fields

To facilitate the Asset Lookup mobile module you can define fields that are searchable. When you insert a new text box, select the **Searchable in Assets Lookup** checkbox.

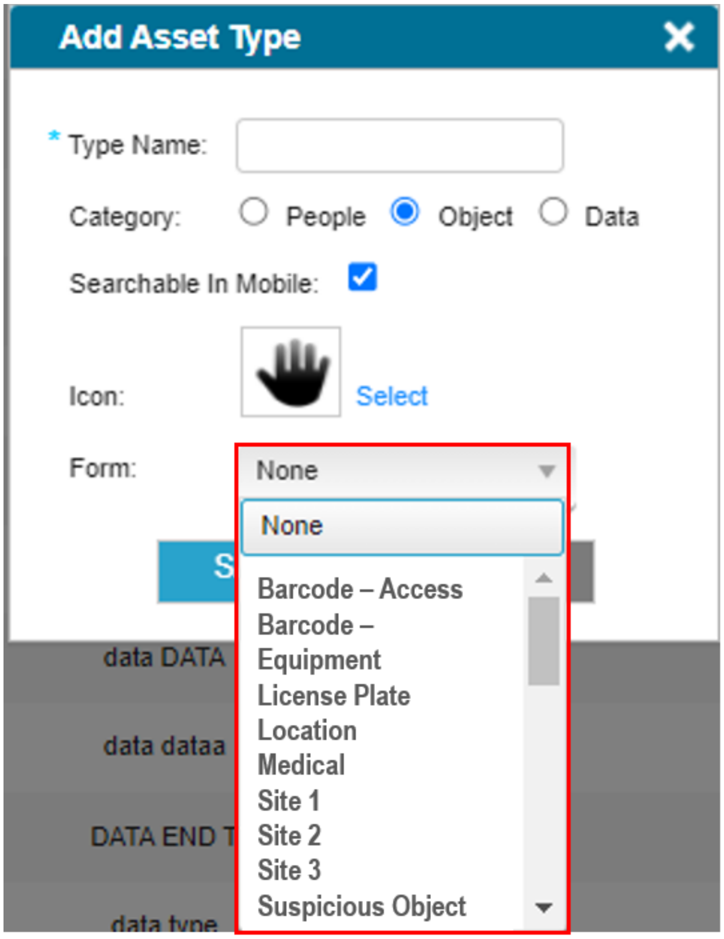


> Note
> You can only make Text Box or Text Area fields searchable.

After making you changes, click **Save** to save the form template.

Assigning a Form to Asset Types

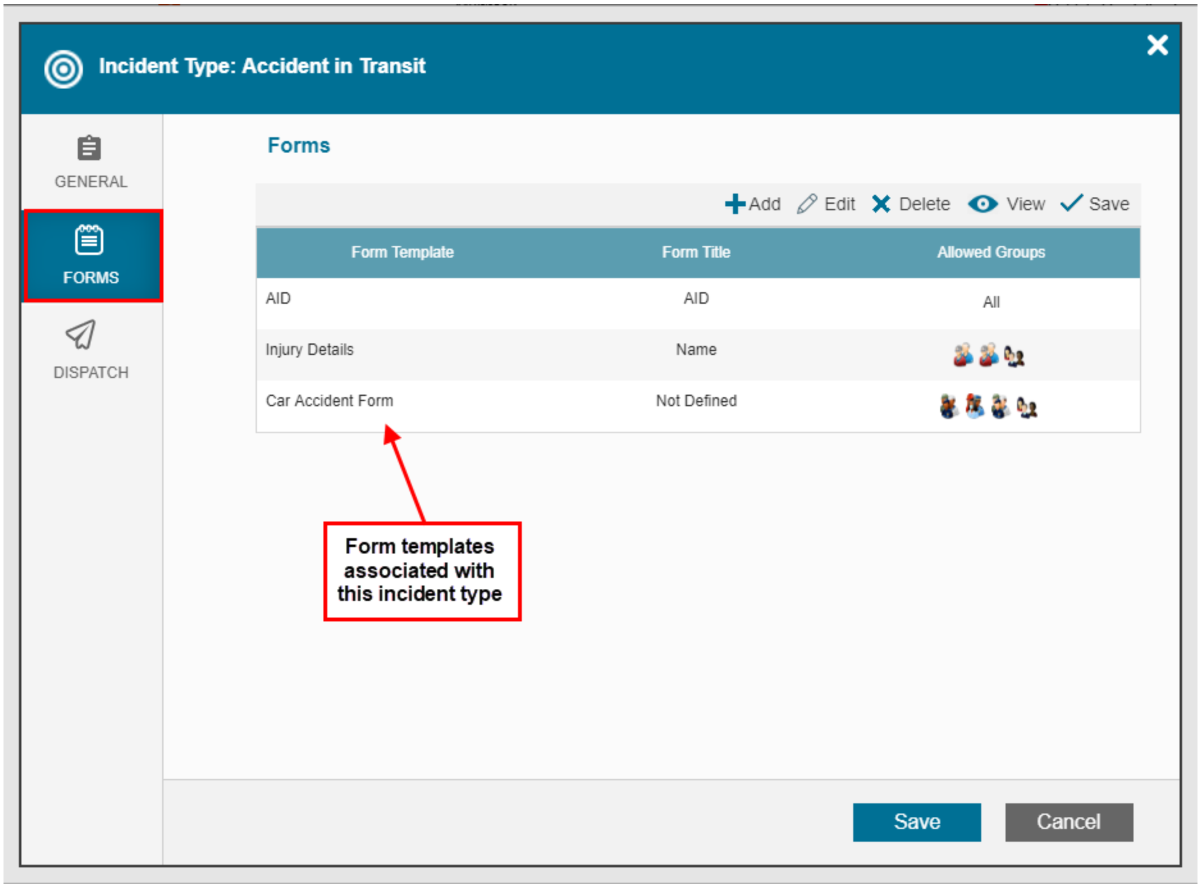
Once the form has been created it can now be assigned to an **Asset Type**, select the required form from the dropdown.



Read more about Assets.

Configuring Multi Forms Permissions

System administrators can associate more than one form template to each incident type, and define groups of dispatchers and responders who can view and edit each form.



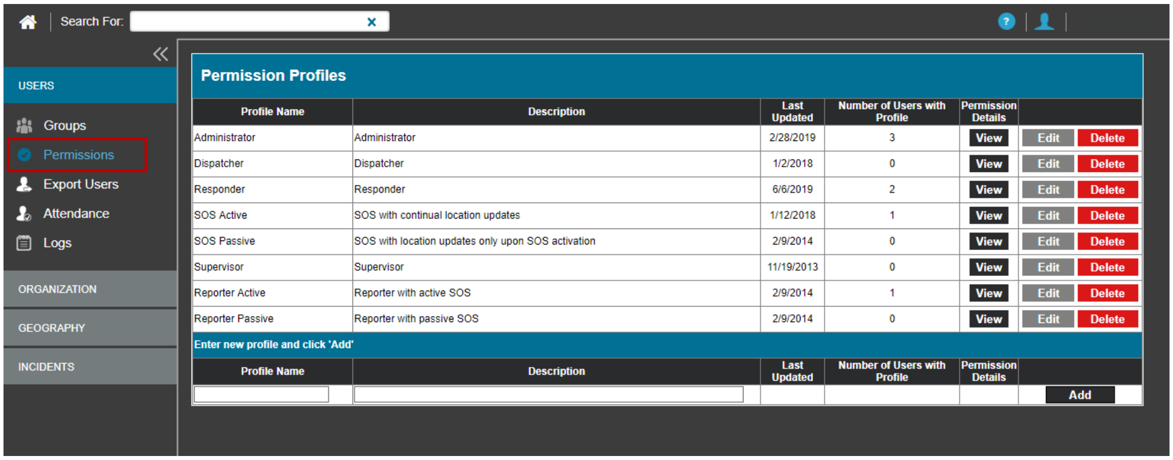
Adding Multi Form Permissions

As an Administrator you can add multi form permissions to dispatchers and responders. Once these permissions are granted, dispatcher and responders can view, edit and duplicate multiple forms for incidents.

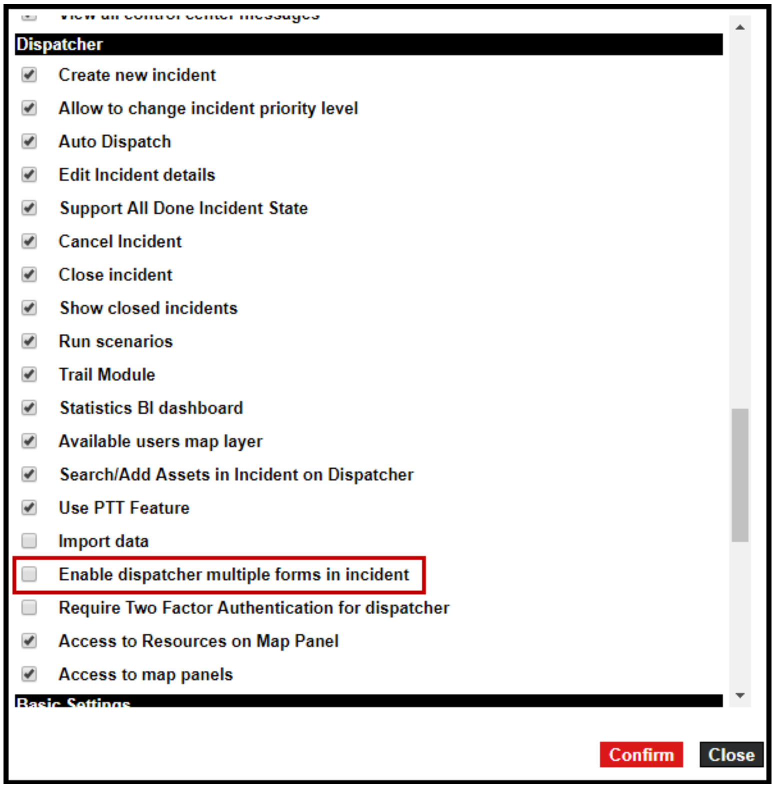
▼ To add multi form permissions

1. From the **Main** screen, select **Settings** > **USERS**, and then select **Permissions**.

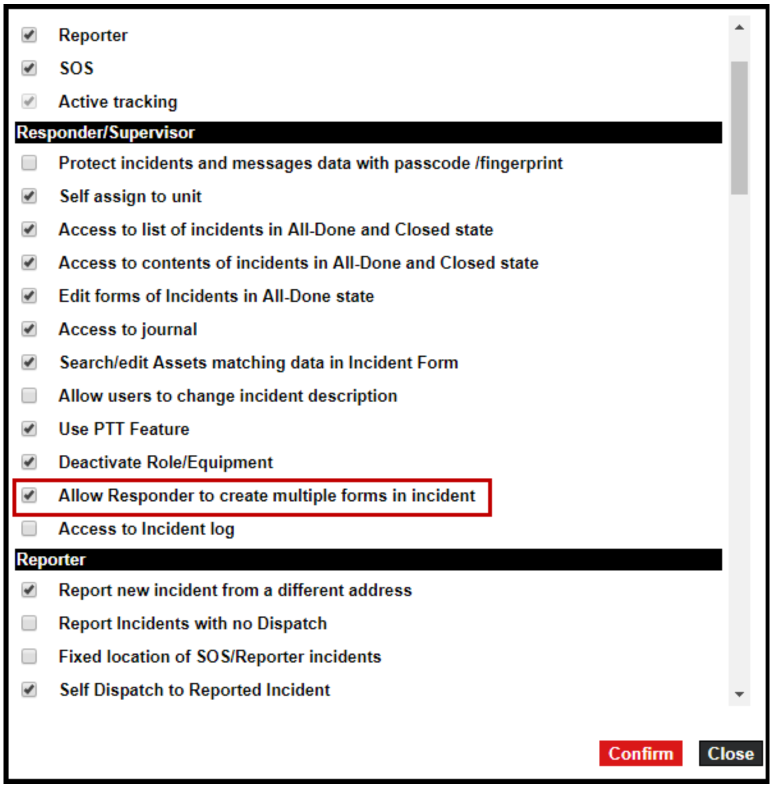
The Permissions settings table opens.



2. Select the profile you want to change, and click **Edit**, and then click **Edit** again to edit its permissions.
3. If you want to add the permission to a dispatcher user profile, scroll to the **Dispatcher** section, and select **Enable dispatcher multiple forms in incident**.



4. If you want to add the permission to an app user profile, scroll to **Responder** and select the **Allow Responder to create multiple forms in incident** check box.



5. Click **Confirm**.
6. Click **Save**.

Read more about Multi Forms.

Read more about Multi Forms in Dispatcher.

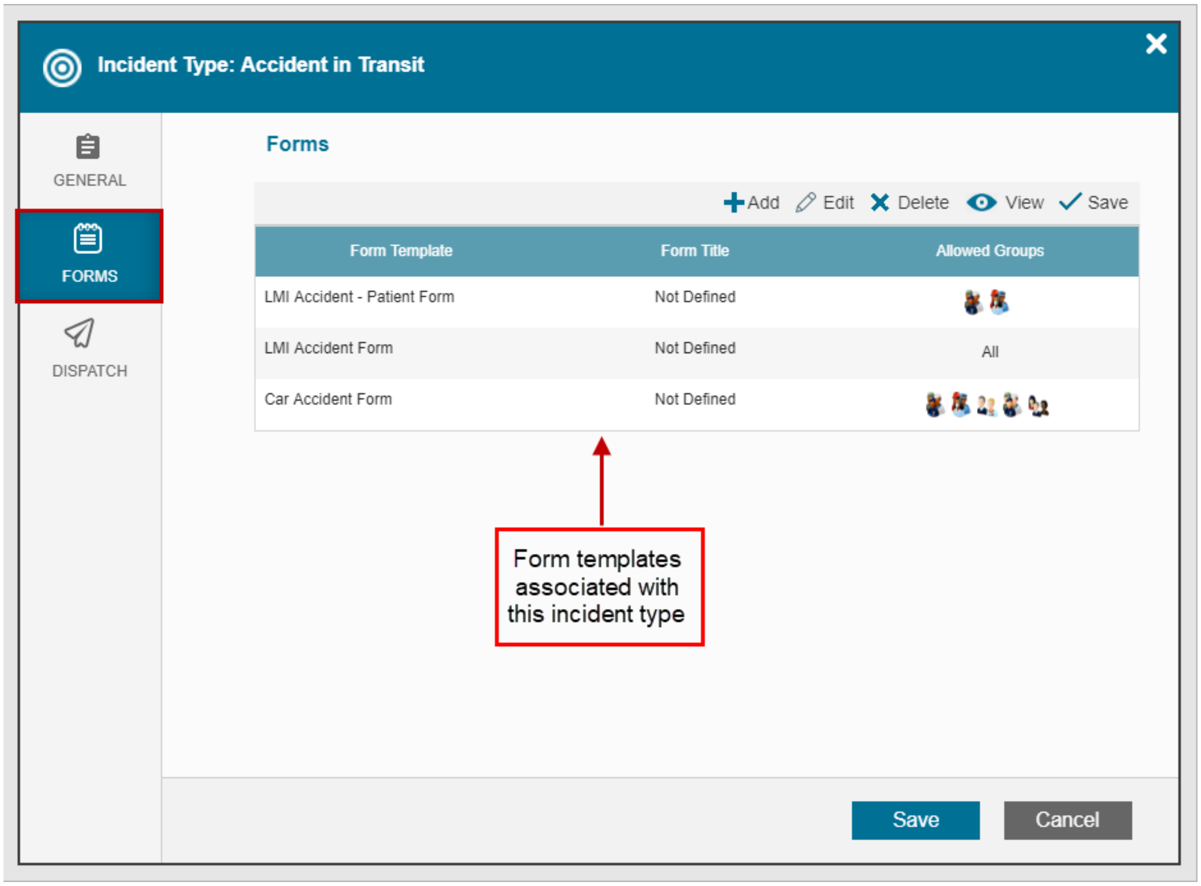
Read more about Multi Forms in the mobile app.

Read more about Managing Incident Types.

Understanding Multi Forms

As a system administrator you can associate more than one form template with each incident type, and decide which groups of users can view and edit each form. This feature enables dispatchers and responders to select the most relevant form from the **Forms** dropdown list in the **Incidents** window. Dispatchers or responders to the incident can either use an existing form or duplicate a form, for example:

- Multiple responders in the same incident can each complete a separate form
- Multiple participants in the same incident (i.e. separate forms for each person involved in the same accident) can each complete a separate form



Viewing, Editing and Duplicating Form Templates

As an administrator, you can create incident types. When you create a new incident type, you also assign form templates to the incident type as well as the groups that can view, duplicate or edit the form template.

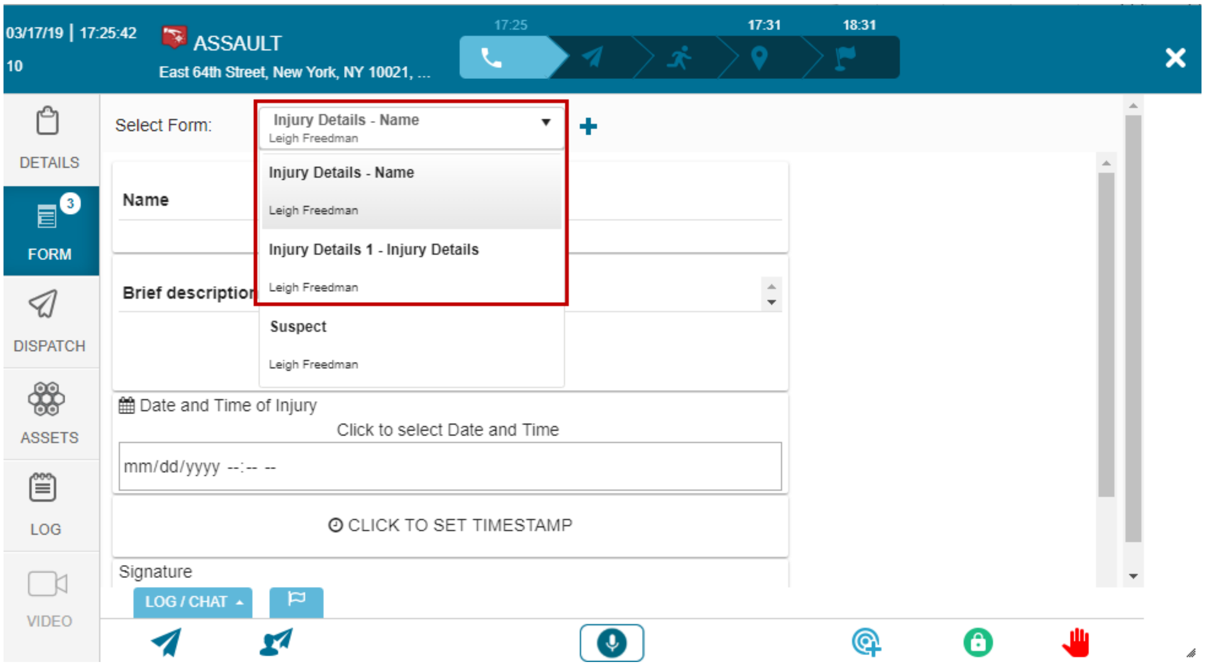
Form Template Name

Each new form is tagged with the name of the form template. Depending on how the system administrator defined the form, the form name can also include the text entered in the form tile field.

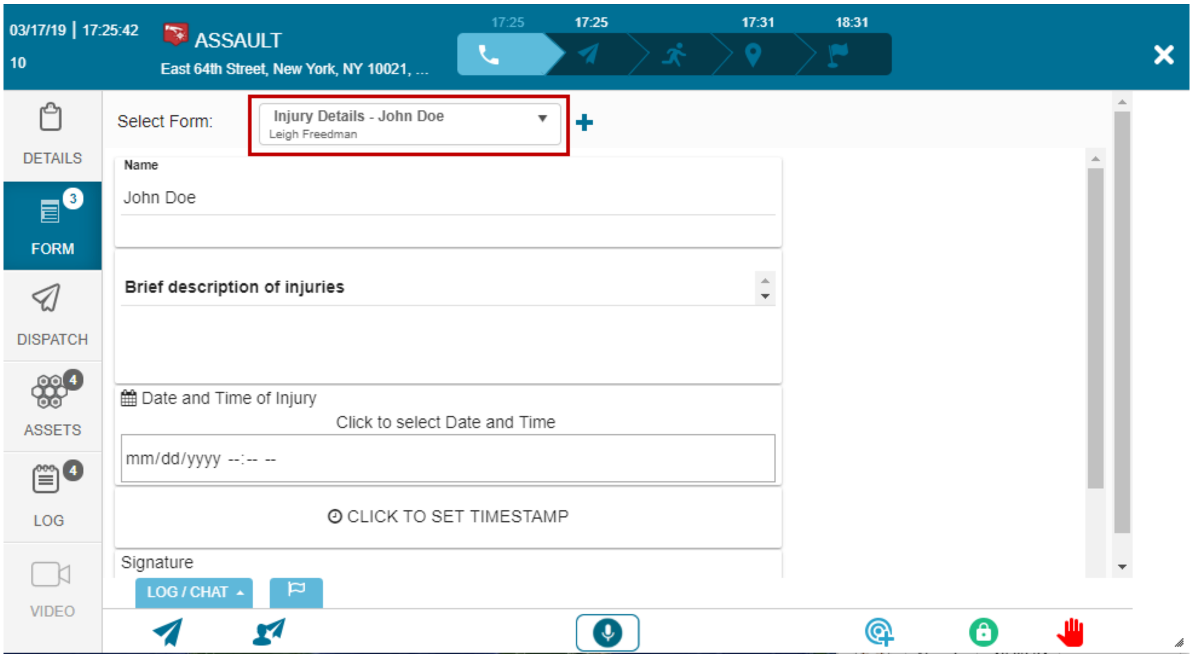
In this case, when you create a new form template, the title of the form includes both the form name and after the form’s title field is populated, the form name inherits its title from the text entered to this field.

For example, the following screenshot shows an incident that has three form templates:

- **Injury Details** that includes a field called **Name**.
- **Injury Details 1** that does not include any fields
- **Suspect** that also does not include any fields.



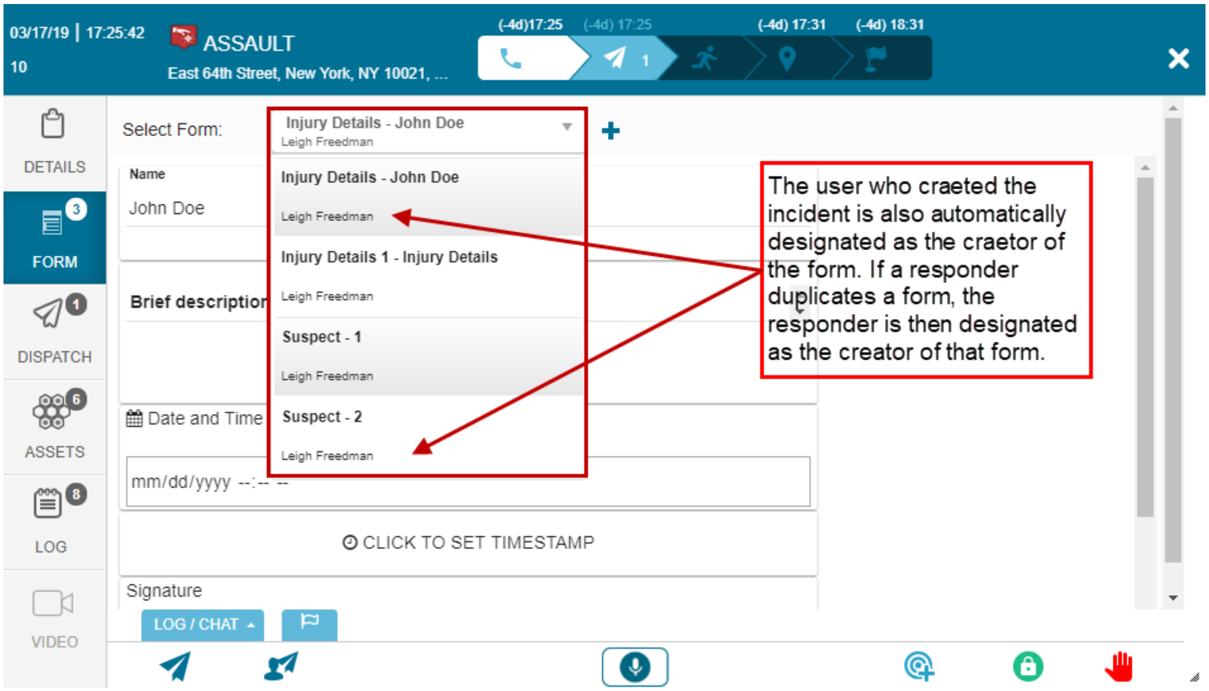
If you choose the form that includes the **Name** field, and enter the required details, the form name is changed (after you save it), to include the name entered in the field, as shown in the following example.



Form Template Creator

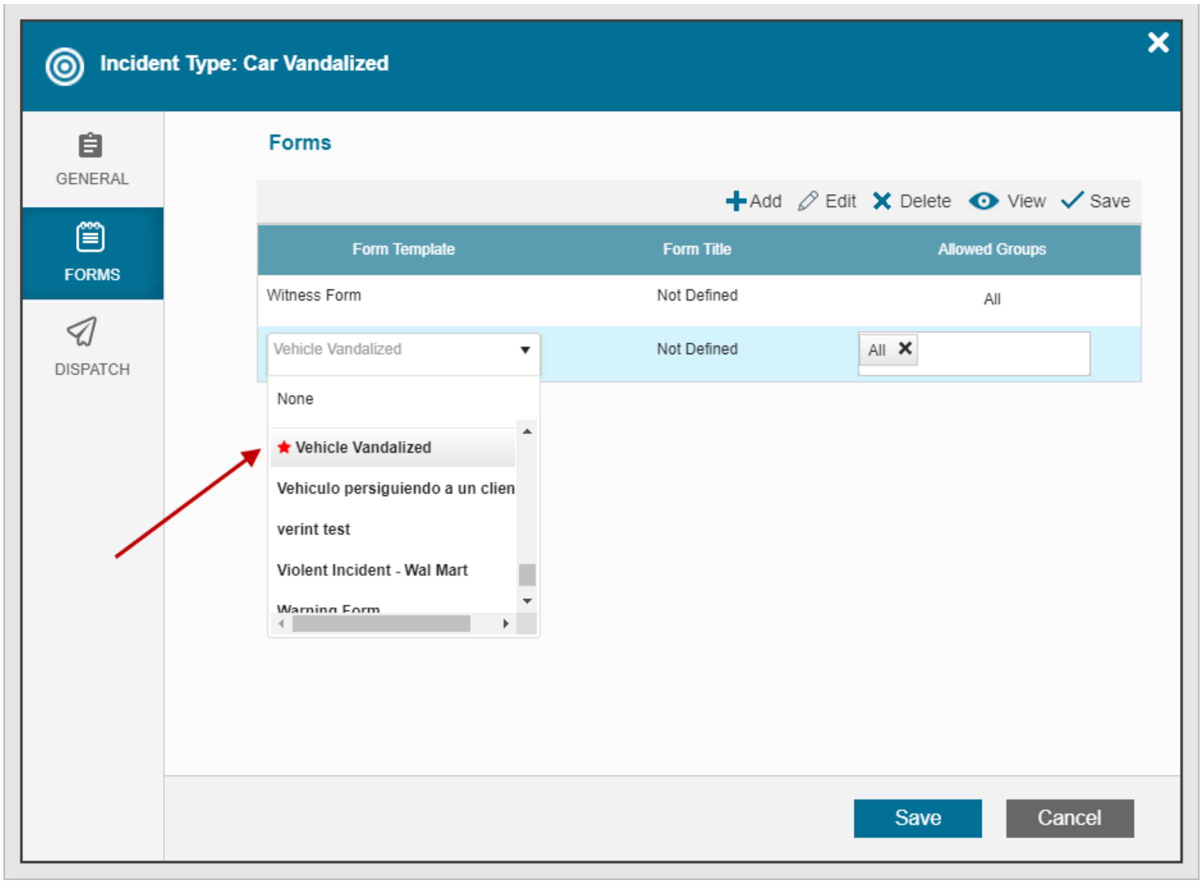
The name of the creator of each form in an Incident appears below the form name in the **Forms** tab.

When an Incident is opened, all forms already created for that Incident type are designated as being created by the user who opened the Incident. If a form template is duplicated, the creator is the user who duplicated the form template.

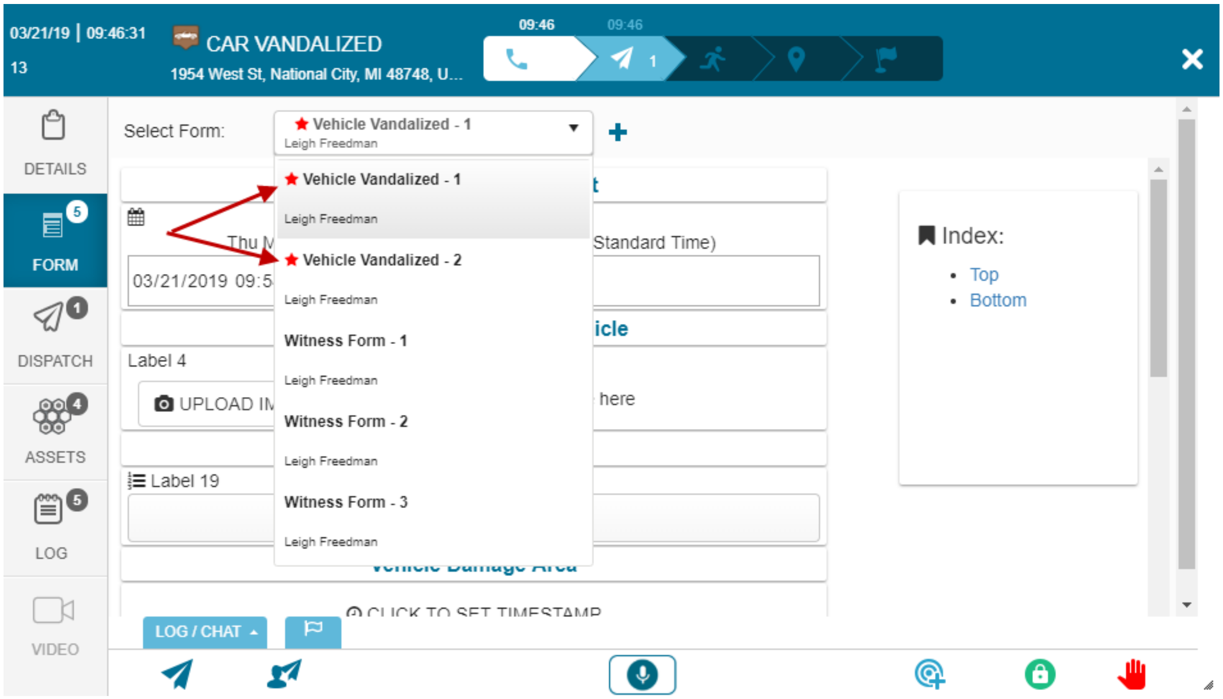


Mandatory Fields

Form templates can be defined (by the administrator) with mandatory fields. A red star icon appears next to the name of a form that has mandatory fields. The red star icon also appears next to the mandatory fields in the form.



In addition, the red star icon appears next to the form name in the Incidents window.



The dispatcher can only close an incident when all the mandatory fields of all the form templates are completed.

A responder user can only report an incident as **Done** if all mandatory fields in the original form templates, and any form templates created or duplicated by them are completed.

- Read more about Multi Forms in the Dispatcher.
- Read more about Multi Forms in the mobile app.
- Read more about configuring Multi Forms permissions.
- Read more about Managing Incident Types.

Adding and Modifying Incident Dispatch Rules

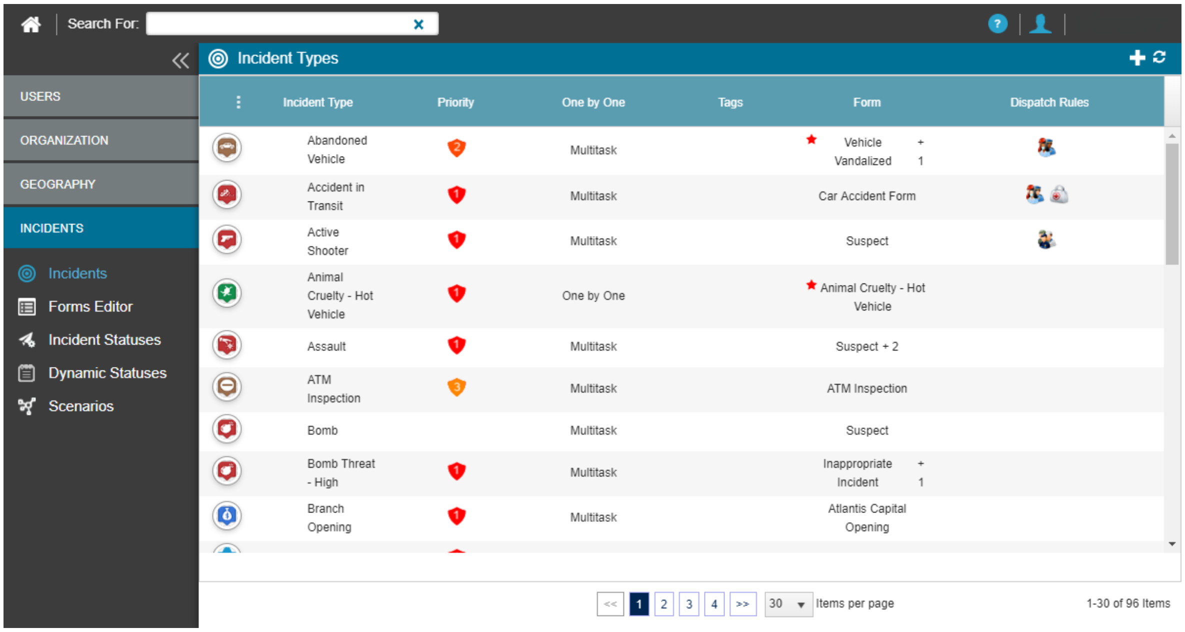
Incident types are defined and managed according to predefined rules set by the organization's administrators and other permitted users. Read more about creating incident types.

When you create a new incident type, and to ensure the proper progress of that incident in the system, you must define the Incident rules in the Dispatch tab of the relevant incident type.

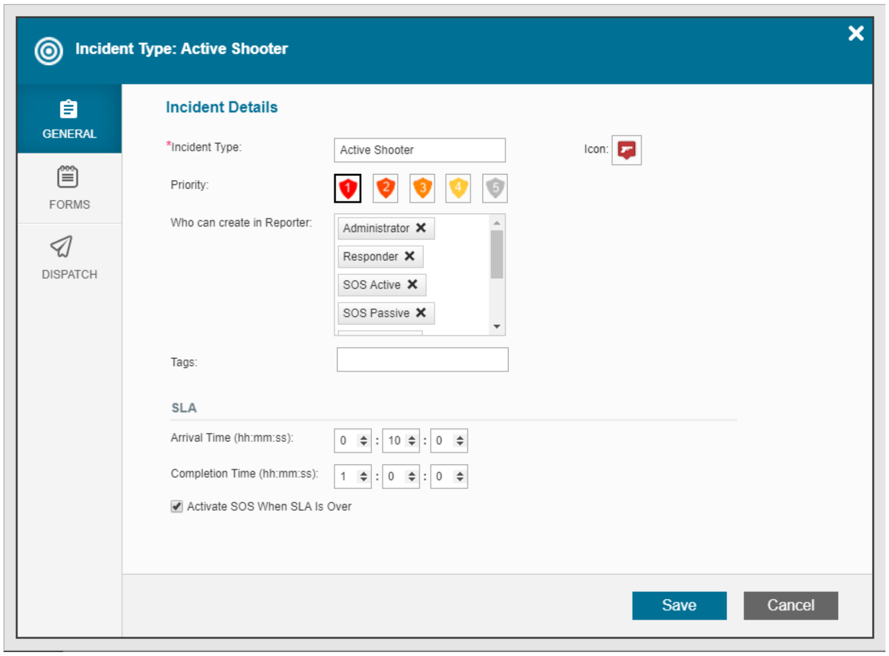
▼ To define dispatch rules

1. From the **Main** screen, select **Settings** > **INCIDENTS**, and then select Incidents.

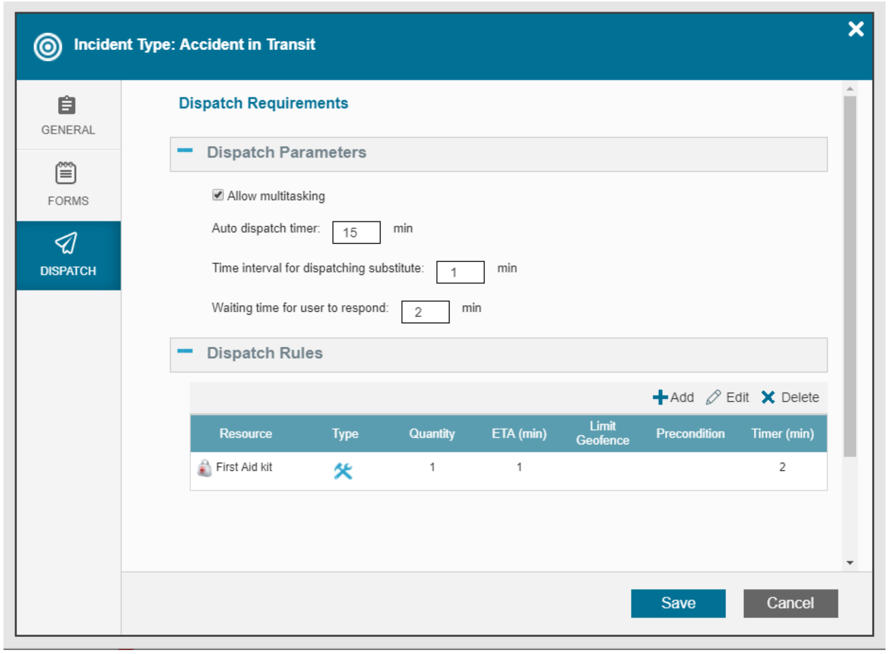
The **Incident Types** panel opens.



2. Hover your cursor over the incident whose dispatch rules you want to modify, and click **Edit**.
3. Modify the **Incident Type** details, as required.



4. Click **Save**.
5. Click **Dispatch** to add or modify dispatch rules.



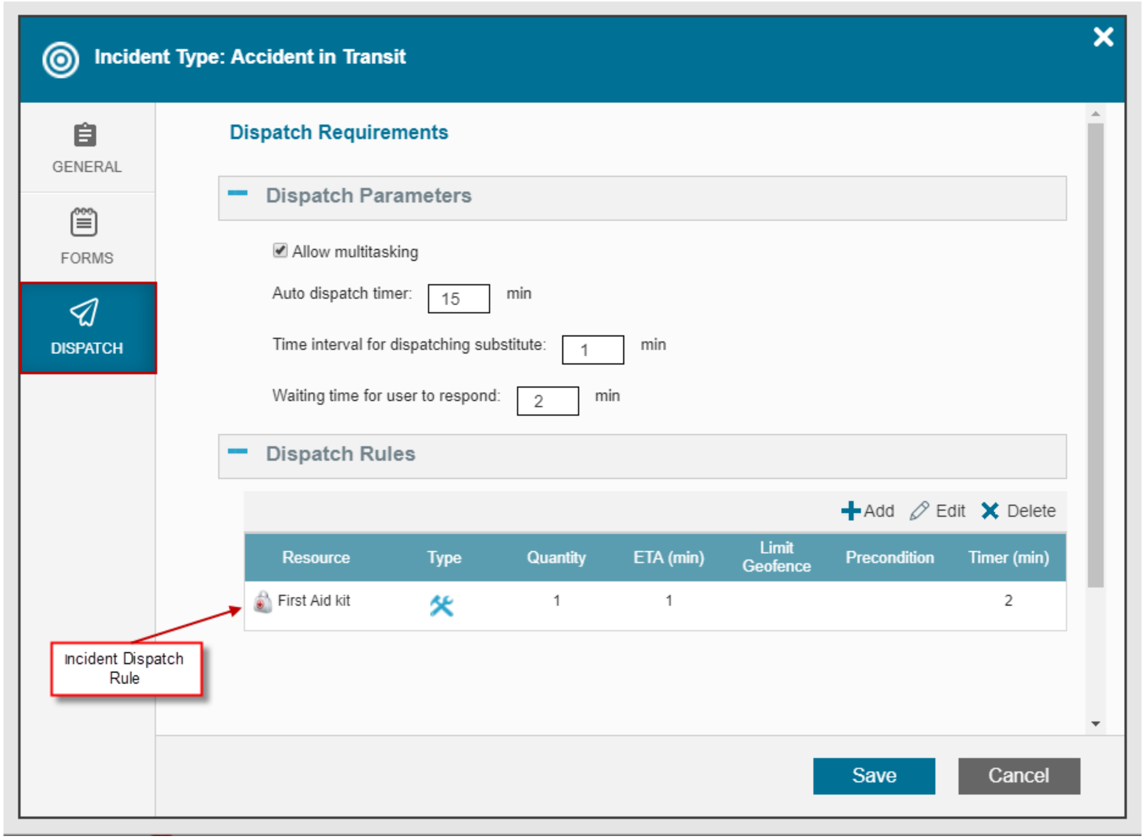
The **Dispatch** tab has the following areas:

Dispatch Parameters:

- **Allow multitasking**: If selected, this option enables dispatchers to dispatch responders to other incidents whilst they are responding to the current incident. The current incident is thus considered a multitask incident. If this option is not selected, a responder who accepts the incident does not receive other incidents until they have completed their role in the current incident.
- **Auto dispatch timer**: Defines the length of time that the incident is considered to be "live" within the system and is the amount of time that the dispatcher has to find available responders to dispatch to the incident.
- **Time interval for dispatching substitute**: Determines the length of time that must elapse before the system automatically dispatches the next closest available responder. To avoid time lags, this setting must be less than the Waiting time for user to respond.
- **Waiting time for user to respond**: Determines the length of time that the incident remains in a responders main screen (Active Incidents table), before it moves to the Incidents table.

Dispatch Rules:

- Lists the existing incident dispatch rules that you can edit. You can also add new rules or delete existing rules.

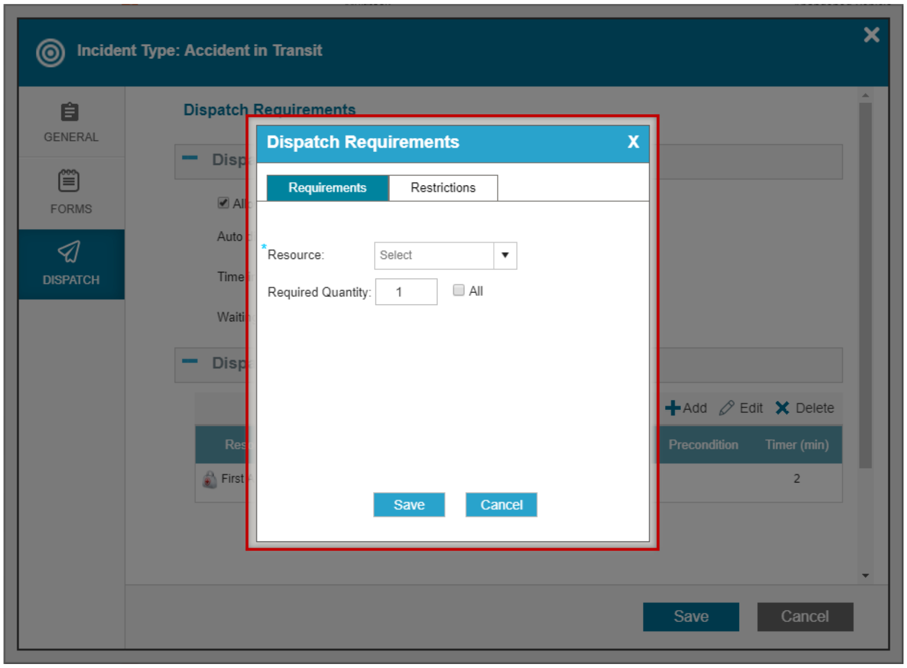


Adding New Dispatch Rule

▼ To add a new dispatch rule

1. Click **+Add** in the **Dispatch Rules** area.

   The Dispatch Requirements window opens.

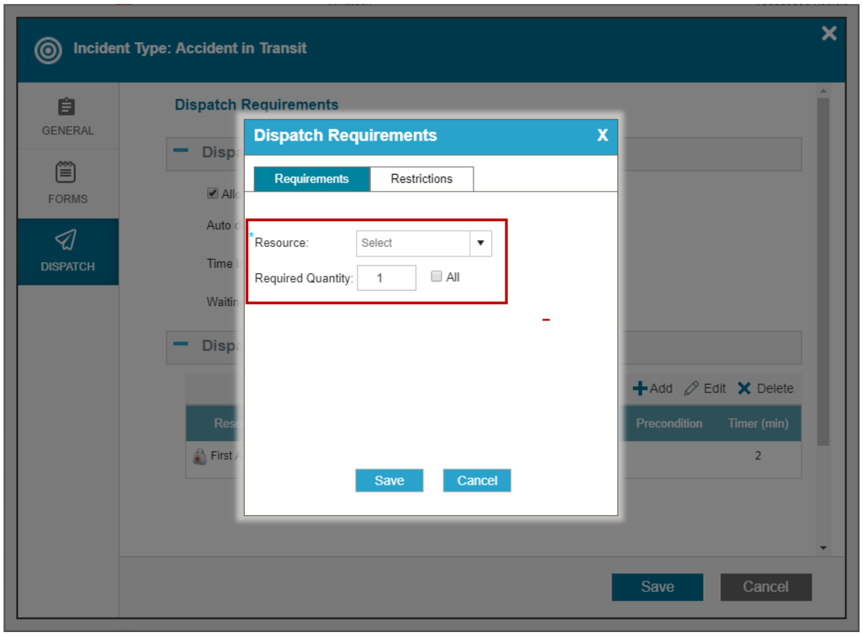


2. In the **Requirements** tab, set the resource category you want to dispatch and the number of resources required:

   - **Resource**: From the **Resource** dropdown list, select the type of resources you want dispatched to the incident. The resources are based on the groups, roles and equipment you have in your account. It is most important to choose the correct category to ensure that responders who match these rules are associated with the chosen category (member of the group/fulfill a certain role/carry certain equipment), are dispatched to the incident.

     > Note
     > A **Group**/**Role**/**Equipment** icon is displayed next to each resource name, to indicate the resource type.

   - **Required Quantity**: Number of resources necessary. You can select from:
     - **All**: Click **All** to dispatch all the available resources in the selected category.
     - **Required Quantity**: Enter the number of available resources you want dispatched in the selected category.



3. In the **Restrictions** tab, add the time and a geofence limitations to the dispatch rule:
   - In the **Timing** area, specify if you want the dispatch to start only after a specific time, or after a decision in the incident dynamic status update.
   - In the **Limitations** area, set the ETA and Geofence limitations as follows:
     - **Limit ETA**: Select this option if you want to limit the dispatched responders to include only those who have an Estimated Time of Arrival (ETA) less than or equal to the ETA defined in the dispatch settings for each specific incident. Click **Limit ETA** and enter the number of minutes a responder's ETA must be in order to be dispatched this specific incident type.
     - **Limit Geofence**: Select this option if you want to limit the dispatched responders to include only those whose User Residence Area (as defined in the User Management window) falls in the geofence in which the incident is located.
4. In the **Dispatch Requirements** window, click **Save** to save your new rule.
5. Click **Save** in the **Incident Type** window and add the category to the incident type dispatch rules.

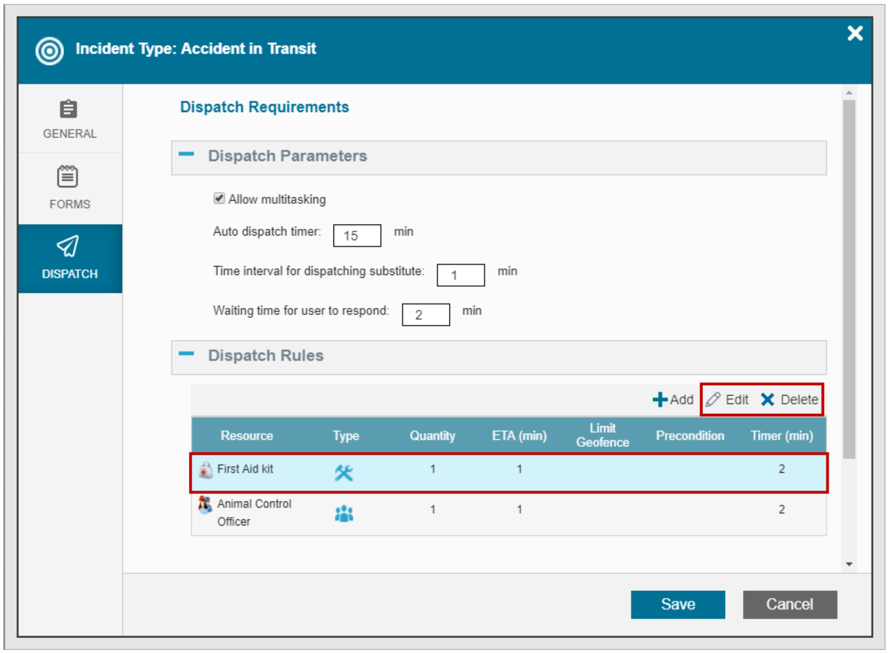
Read more about two-step dispatch.

Editing or Deleting Dispatch Rules

You can also edit or delete the dispatch rules from the Incident type Dispatch tab.

▼ To edit a dispatch rule

1. In the **DISPATCH** tab of the **Incident Type** module select the rule and click **Edit**.



2. The rule become editable. Make your changes.
3. Click **Save**.

▼ To delete a dispatch rule

1. In the **DISPATCH** tab of the **Incident Type** module select the rule and click **Delete**.
2. Click **Save**.

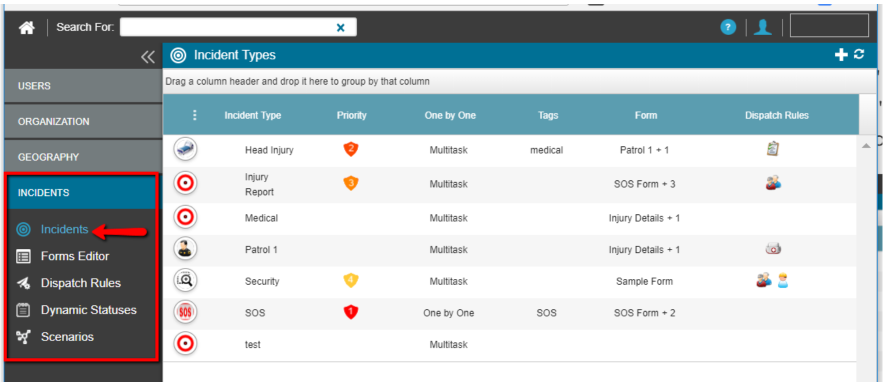
Managing Incident Types

You can configure all the Incident types available to the Dispatcher and Responder users in the Incidents Setting table.

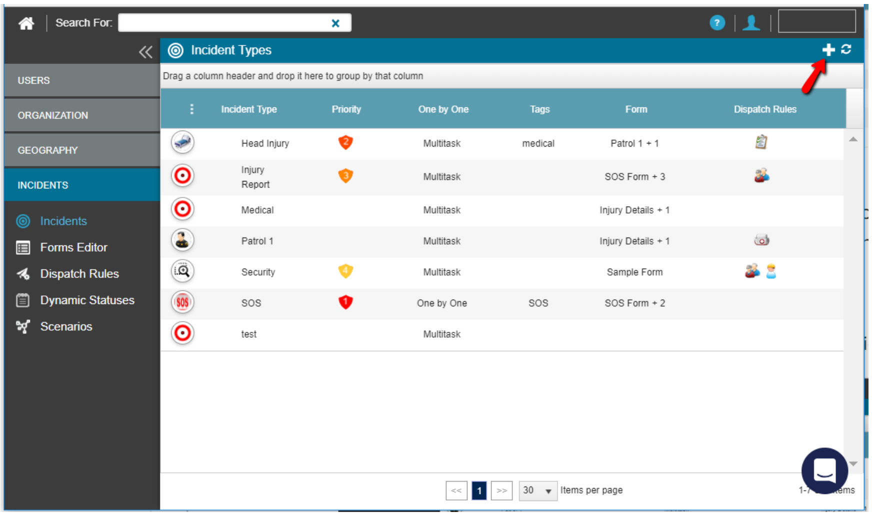
Creating a New Incident Type

1. From the **Main** screen, select **Settings** > **INCIDENTS**, and then select **Incidents**.

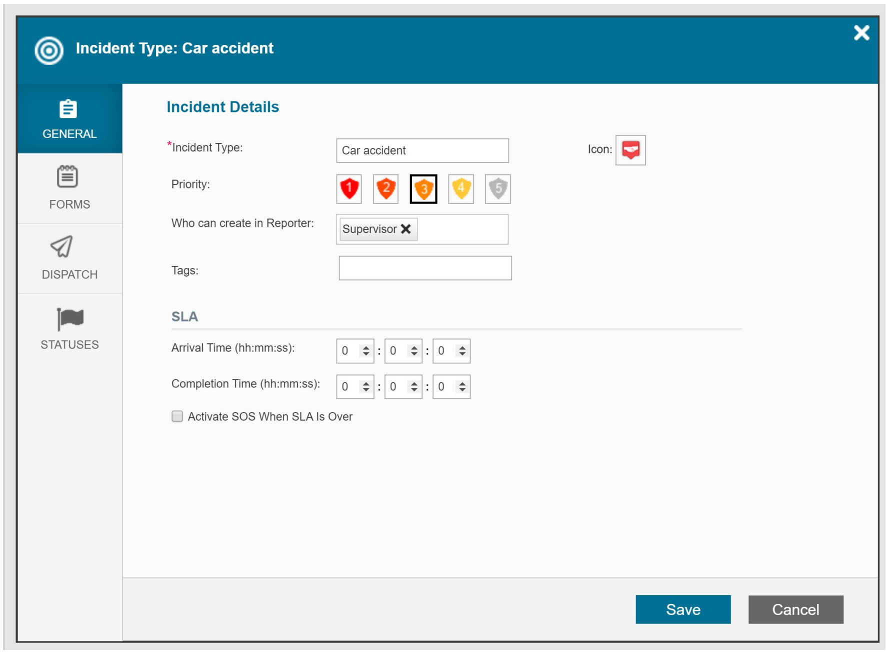
   The **Incidents Types** table opens, with incidents listed in alphabetical order.



2. Click **+**sign at the upper right corner to add a new **Incident Type**.



The **New Incident Type** window opens, in the **General** tab view.

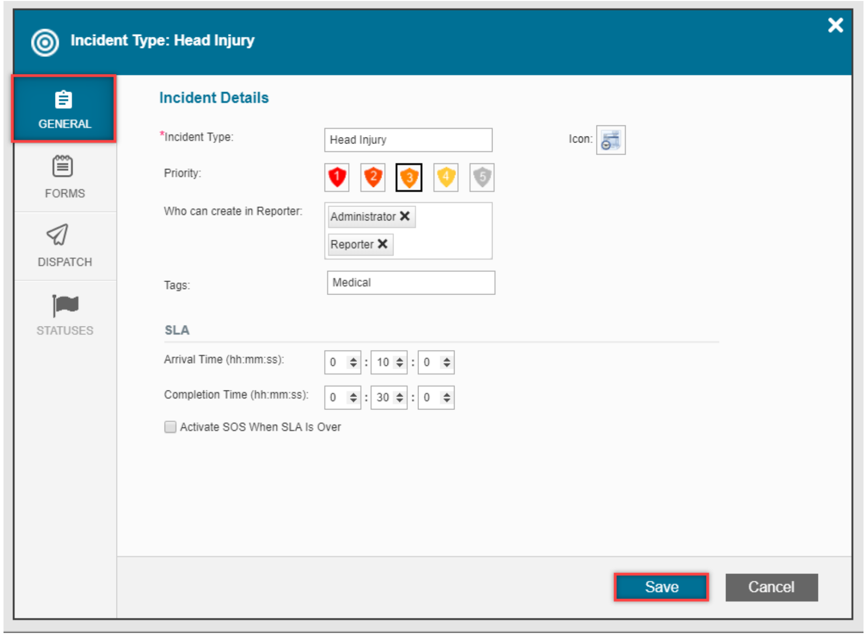


3. Enter the name of the new incident in the **Incident Type** field.
4. Click the **Icon** to open the Search Icon window.

> Note
> When an incident of this type is active, this icon will appear on the map at the incident location. It will also appear in the incident panel in the Dispatcher Screen and on the Incident window. The icon appears on the mobile responder when the responder is dispatched to an incident.

5. Click on a **Priority** to associate the incident's priority level from 1-5, where **1 is the highest**.
6. Select the permission profiles of **Who can create in Reporter** to define which mobile users can open a new incident of this type from their mobile application. Read about creating incidents from the mobile reporter.
7. Enter key words into the **Tags** field.

> Note
> Tags assist the dispatcher when searching for incident types and are used as filters for incidents layers on the map.



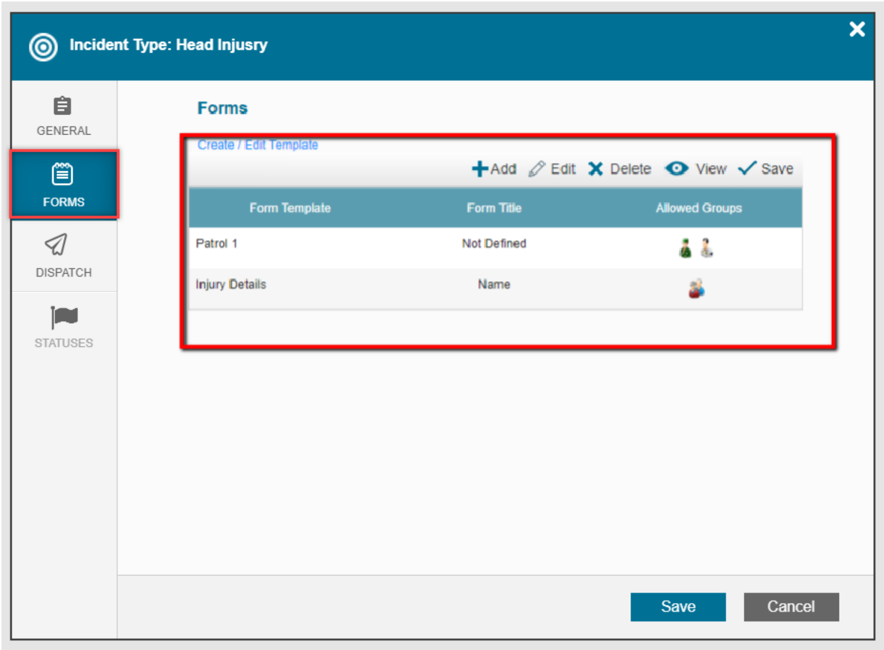
8. **SLA** (Service Level Agreement): The SLA allows you to add to any incident two counters with alerts.

   - *Arrival time* is how much time you set as a guideline for the **first** Responder to arrive (on scene). Arrival time can be defined here (in the incident type settings) as a fixed timer for all incidents of this type but it can also be set in real-time by the dispatcher for a specific incident (i.e. a time set in accordance with a customer).
   - *Completion time* is how much time you set as a guideline for the **first** Responder to complete a task ("Done"). The Completion time is defined as a countdown timer and it is measured from the moment the first Responder reports on-scene (arrival time). This means the period of time is fixed but the trigger for the timer alters according to the actual on-scene report.
   - *Activate SOS When SLA is Over* activates an SOS alert when the SLA completion time is up. Read more about SOS alerts.

9. Click **Save** and switch to the **Forms** tab.

10. In the **Forms** tab you can define what form templates are associated with this incident type. You may designate a name for each template and define which Responder Groups will have access to each form as they fill the form after responding to the incident.

> **Note**
> You can associate more than one form template to each incident type.



11. Click the **+** sign to add a new Form template. Forms can be:

- Added to by clicking: 

- Edited by clicking: 

- Deleted by clicking: 

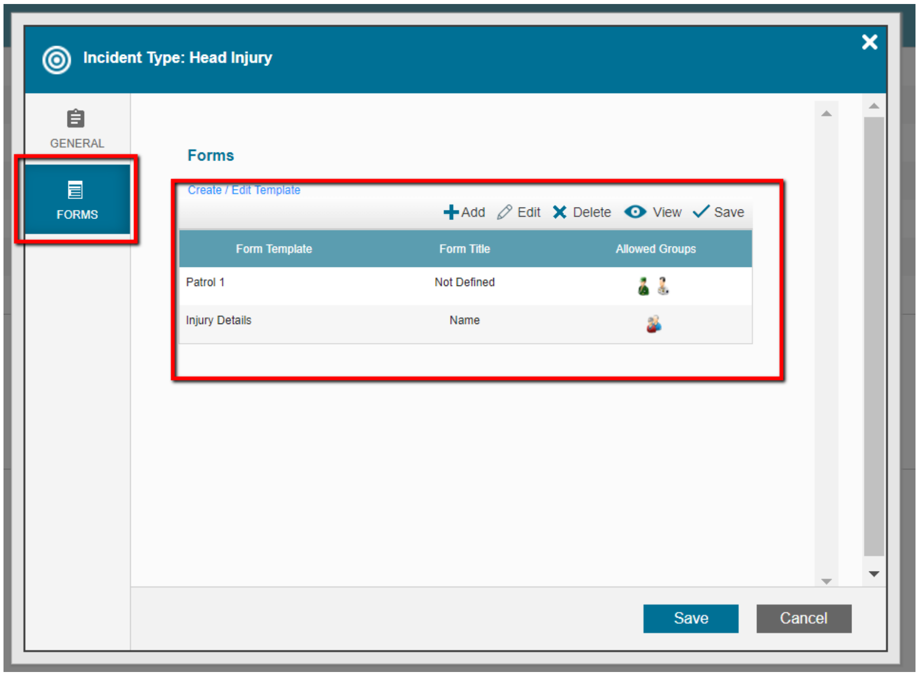
- Viewed by clicking: 

- Saved by clicking: 

The Forms tab includes the following columns:

- **Form Template**: Chose the Form template you want to add to the incident type from the list of the available forms.
- **Form Title**: The title of this form template when a user (dispatcher or mobile user) will open a new incident from this incident type. The **Form Title** will be based on the field you set as **Dynamic Form Title** in the chosen form template, or just the form template name in case you didn't set a field as a **Dynamic Form Title**.For more information on how to set a from field as **Dynamic Form Title**, see Creating and Editing Form Templates .
- **Allowed Groups**: What groups can view, edit and duplicate this form template.

Lets look at the incident type to clarify:



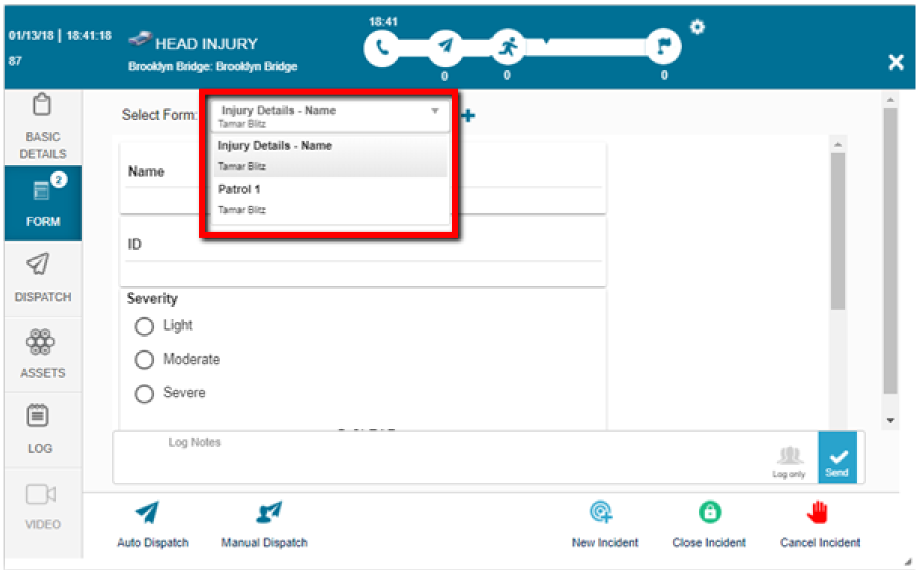
We have an incident type named **Head Injury**.

Two **Form Templates** are associated to this incident type:

- **Form Template** named **Patrol 1**. Since we didn't set any field in the **Form Template** as **Dynamic Form Title** we don't have a title for this form (hence Not Defined). Only users who are members in the groups **Managers** and **Patrol** can view, edit and duplicate this **Form Template**.
- **Form Template** named **Injury Details** which the field **Name** in this **Form Template** was set as **Dynamic Form Title**. Only users who are members in the group '**Medical** can view, edit and duplicate this '**Form Template**'.

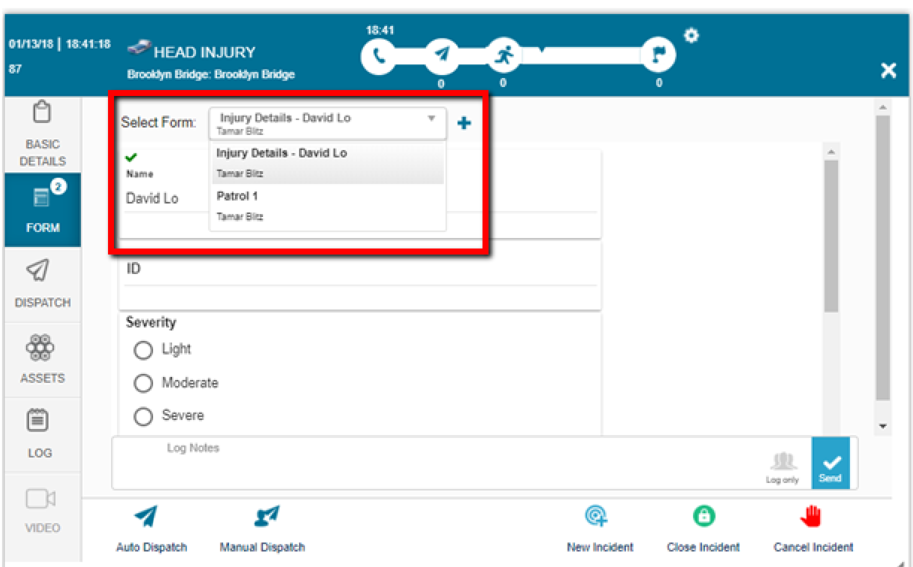
When a user who is a member of the groups **Manager**, **Patrol** and **Medical** opens a new **Head Injury** incident, the user sees both forms, and their names will be based on the 'Form Title' as defined above.

The form title in the new incident is composed of the name of the **Form Template** (for example **Injury Details**) + name of the **Dynamic Form Title** field (for example **Name**), if it was defined:



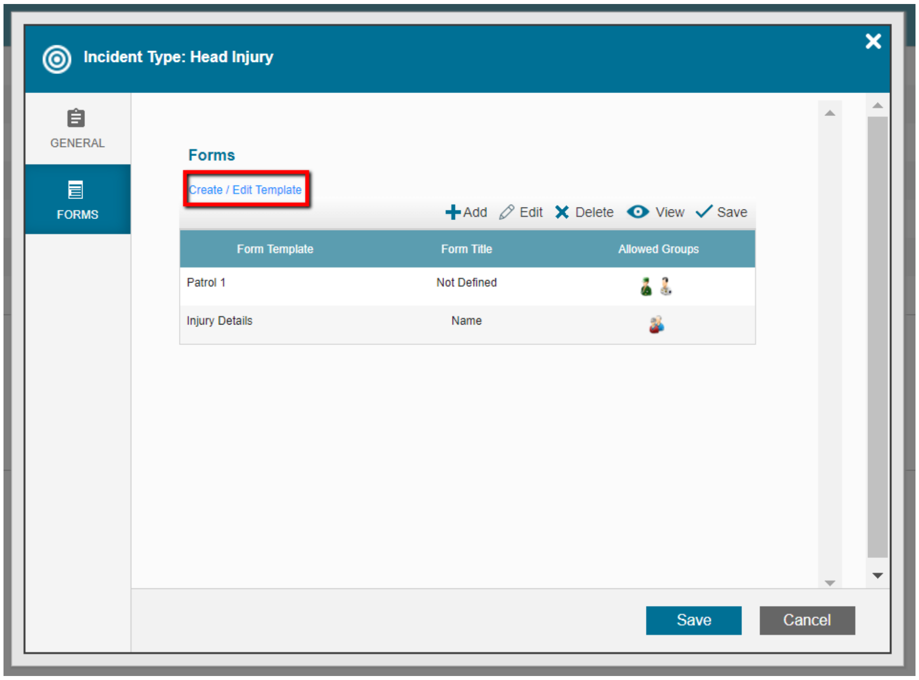
> **Note**
> A user who is a member of the groups **Managers** and **Patrol** only sees the **Patrol 1** form template. A user who is a member of the **Medical** group only, sees only the **Injury Details** form template.

After a user fills in the **Name** field in the **Injury Details** template form, the form title changes to the value of this field, which in our example is David Lo:



The **Patrol 1** form title will remain **Patrol 1** since no filed in this form template was defined as **Dynamic Form Title**.

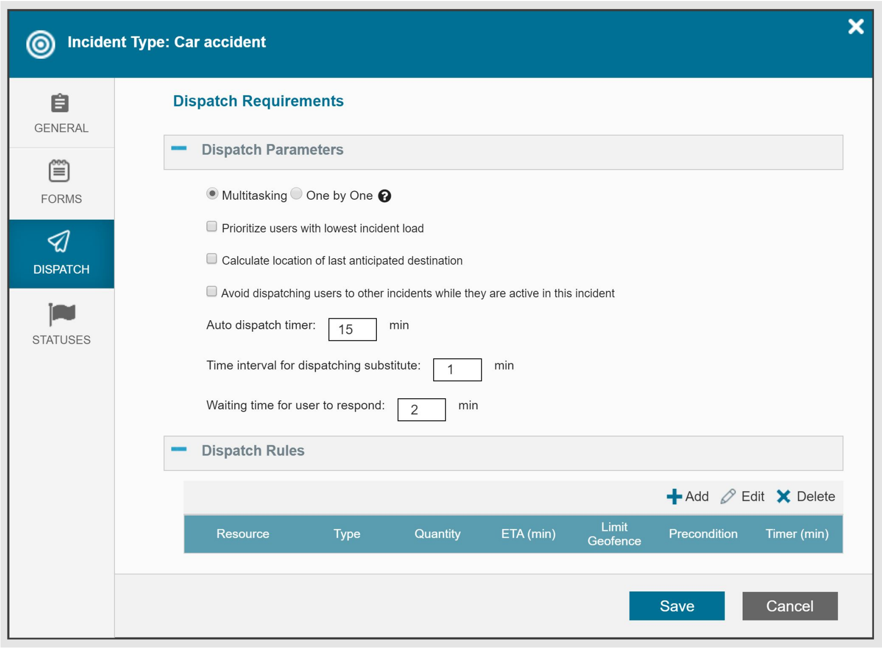
If we have duplicated **Template** Form, a running number will be added to the **Form Title** in the new incident:



Note

There is an option to create a new form templates or edit one by clicking on **Create/Edit Template**. Read about how to [Create and edit an Incident Form Template.]()

12. Click **Save** and the **Dispatch** tab becomes accessible.



13. **Dispatch parameters**

    - **One by One -** If an incident type is defined as one by one **-** then the auto dispatch engine will not dispatch to this incident any responders already active in another one-by-one incident.

      > Note
      >
      > If you do not check the **One by One** checkbox, this incident type is defaulted as a **Multitask** incident, which means that a responder will be able to receive this Incident whilst responding to prior Incidents.

    - **Prioritize users with lowest incident load -** auto-dispatch engine will prioritize incident load over ETA. This dispatch policy is relevant for organizations that prefer sharing the incident load evenly rather than always dispatching the closest person.
    - **Calculate location of last anticipated destination -** auto-dispatch engine will Calculate ETA of candidate responders not based on their current location but rather their expected location/destination after concluding all assigned incidents.
    - **Avoid dispatching users to other incidents while they are active in this incident -** when auto-dispatch engine will search for relevant responders for OTHER incidents, it will ignore responders already active in this incident type.
    - Complete the **Dispatch Requirements** preferred for this incident, click **Save**.

Editing or Deleting Incident Types

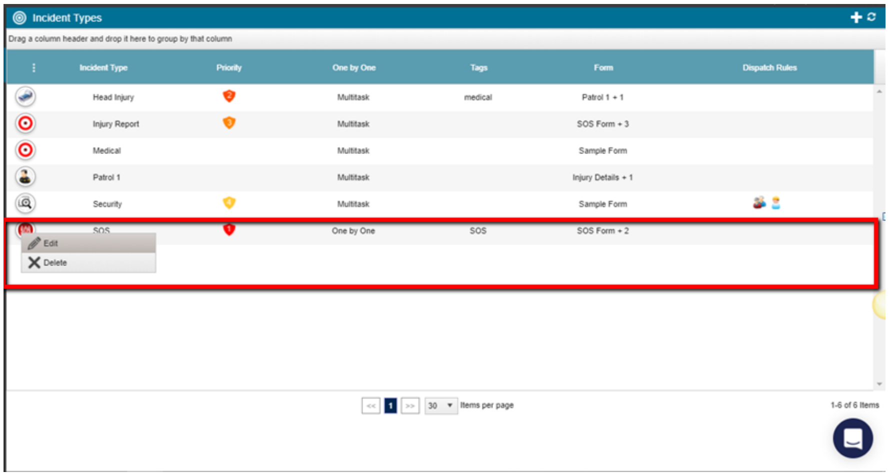
1. To edit incident types, stand on the incident type and choose **Edit**.

   The Incident Type window opens, and is editable.

2. To delete an incident type, stand on the incident and choose **Delete**.

   A Warning window opens.

3. Click **Delete** again to remove the incident from the list.



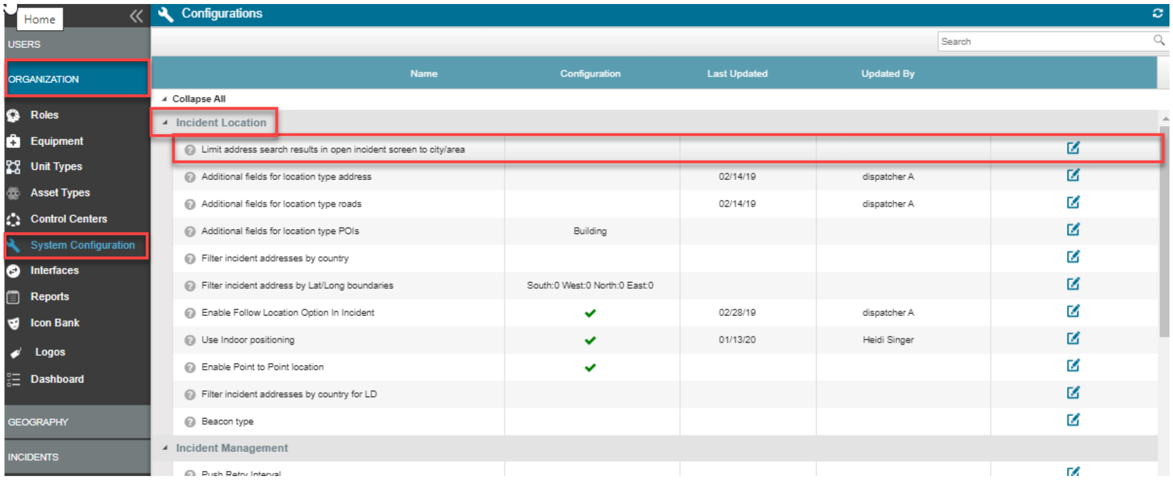
Limiting Address Search Results in Incident Screen

You can set limits on the address search results that appear under the map in the Incident Module when creating a new incident. This setting allows you to limit the search results to a specified region or city aligned to your control center jurisdiction.

▼ To limit the address search results

1. From the **Main** screen, select **Settings** > **ORGANIZATION**, and then select **System Configuration**.

2. The **Configuration** table opens.



3. In the **Incident Location** section find the setting **Limit address search results in open incident screen to city/area** and click  icon.

   The setting becomes editable.

4. Make your changes.

5. Click the  icon to save.

Adding Situation Reports to Incident Types

You can add Situation Reports to an Incident Type to enable responders to be more specific with their reports when they arrive at an incident. There are 2 types of User Updates that can be used as statuses for incidents:

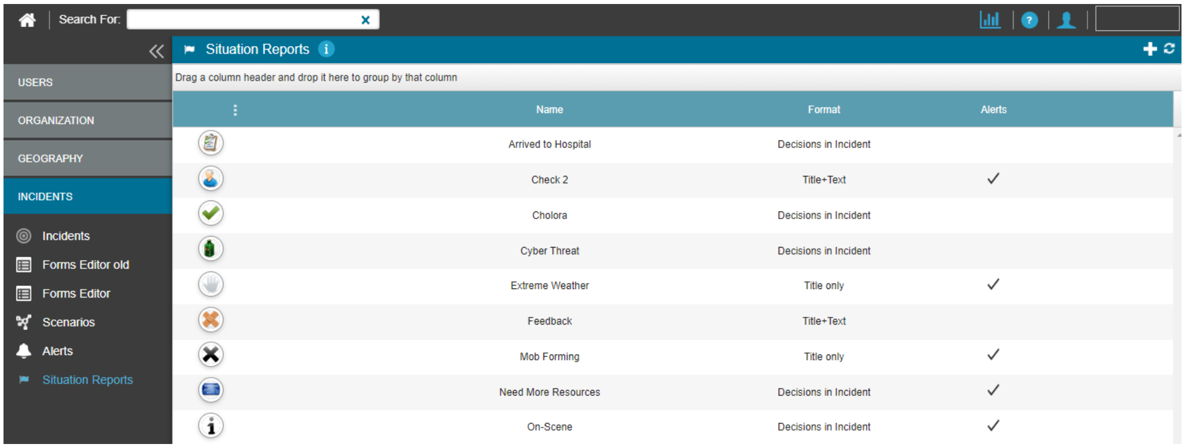
- **Progress Statuses**: These are the statuses reported by responders as part of their progress in the incident life cycle and include the statuses of: Acknowledge, En-Route, On-Scene and Done.
- **Situation Reports**: These are the alerts responders can report in order to describe a situation that requires the attention of other participants in the incident. These reports are addable and customizable.

You can select from the already configured Situation Reports or create and add a new one from inside of the Incident Type's Status tab.

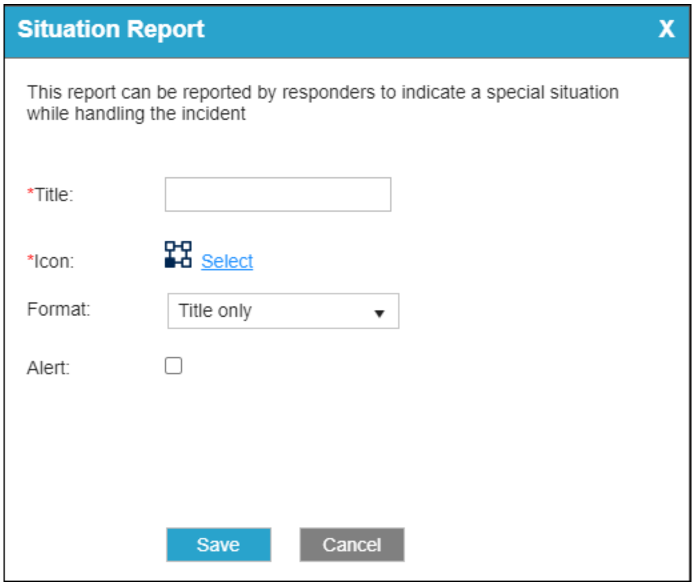
▼ To create a new Situation Report status

1. From the Main screen, select **Settings**> **INCIDENTS**, and then select **Situation Reports**.

The **Situation Reports** table opens.



2. Click the **+** to add a new **Situation Report**. The **Situation Report** pop up opens.

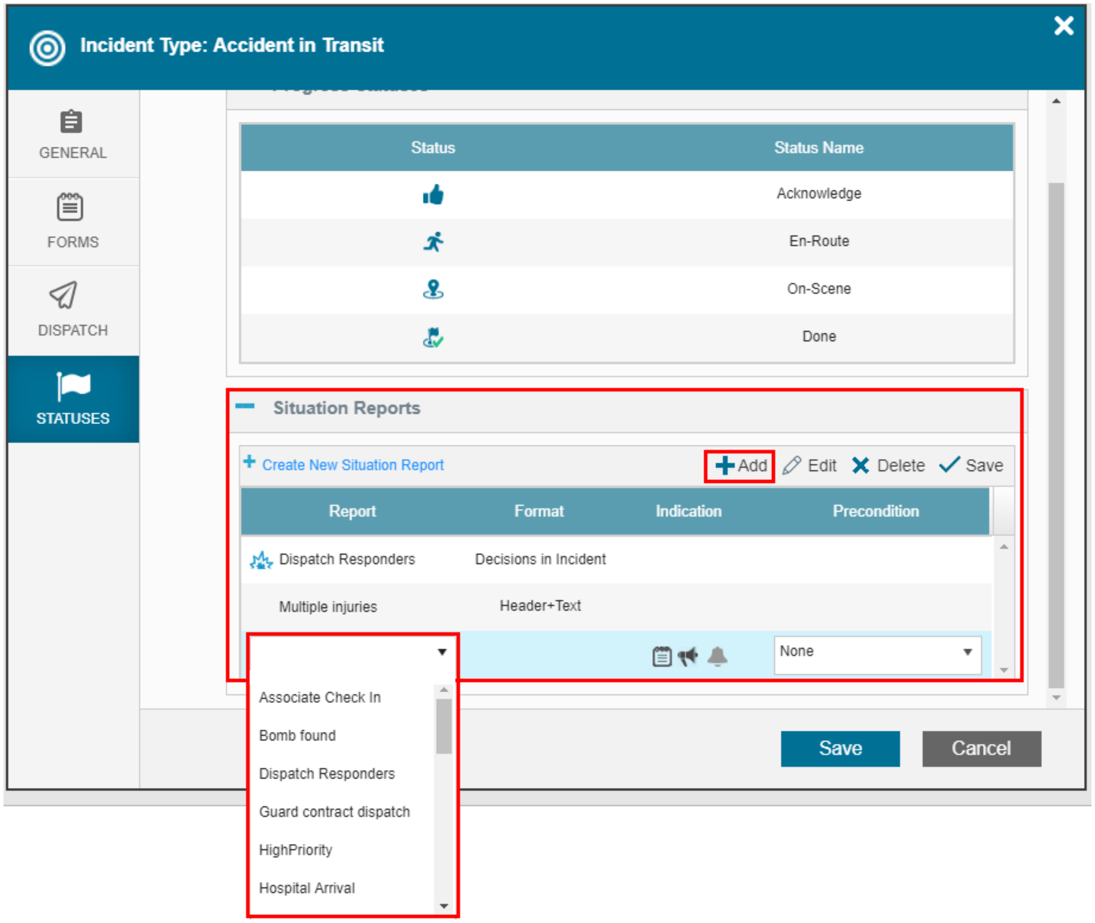


3. Complete the fields, and click **Save**.

   The new Situation Report becomes available in the Situation Reports dropdown inside of the Incident Types module, and is now addable to an Incident Type.

▼ To add a Situation Report to an Incident Type

1. From the Main screen, select **Settings**> **INCIDENTS**, and then select **Incidents**.
2. Locate the incident to which you want to add the new Incident Situation Report too and after hovering your cursor over the incidents icon, select **Edit**.
3. Click on the **STATUSES** tab In the Incident Type moduleTo add a Situation Report that already exists to the incident, go to the Situation Reports area, click +Add and select the required dynamic status from the Report dropdown list.
4. To add a **Situation Report** that already exists to the incident:
   a. Go to the **Situation Reports** area, click **+Add** and select the required dynamic status from the Report dropdown list.



   b. Click **Save**,
5. To create a ***new*** Incident Situation Report, go to the Situation Reports area, click **+Create New Situation Report**.
   a. In the **Situation Report** pop up opens. Complete the fields and click **Save**.

   The The new Situation Report becomes available in the Report dropdown list.

   b. Return to step 4 above and add the new Situation Report to the Incident Type.

6. Click **Save**.