Everbridge Mobile App Guide

Everbridge Suite

December 2023

Everbridge Suite
2023
Printed in the USA

Everbridge, Inc.
155 N. Lake Avenue, 9th Floor
Pasadena, California 91101 USA
Toll-Free (USA/Canada) +1.888.366.4911

Visit us at www.everbridge.com

Overview

The **Everbridge Mobile** application gives you the ability for two-way communications with your organization. It runs on smartphones and tablets, like Apple iPhone, Apple iPad, and Android devices.

You can receive Notifications, send a confirmation, and send replies. With two-way communication, you will become the eyes and ears of your organization during an incident. Your replies are available to the organization to help with the proper response to an incident. The location of your device allows your organization to pinpoint the area involved (shown on the map from the **Universe** tab). You can attach photos (not to exceed 1 MB) to your messages for additional information. Your organization can also allow you to send unsolicited messages to notify of conditions you have discovered. Your organization can allow you to share messages with your own contacts to help extend the reach of important notifications — via email, SMS, or Twitter.

> **NOTE:** The Everbridge Mobile app is developed for your native device type. The examples in this guide show using it on an Apple iPhone. Your screens might not look identical to the examples, but the features are the same.

Getting Started With Everbridge Mobile App

There are two ways to use the Everbridge Mobile App: as an **Anonymous User** or as a **Registered User**.

To get started with the Everbridge Mobile App:

1. Download and install the app from either the **Apple App Store** or the **Google Play Store**.
2. Do one of the following from the Welcome screen:
    a. Find an **Organization** or **Subscription** - A page is displayed where you enter your Organization search term(s) and search. Organizations that match your search terms display in the app, and you tap the desired term.
    b. Explore the **Map** and follow the on-screen instructions.
3. Configure the settings for your account in the app.

Refer to the following sections for more information.

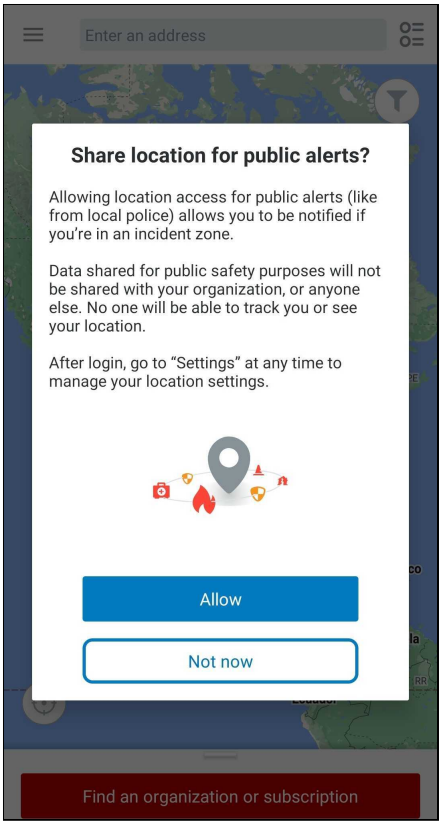
Using Everbridge Mobile App as an Anonymous User

Anyone can use the **Everbridge Map** without being a registered user of an Organization or a Member Portal user. Any users that are not registered to an Organization are considered **Anonymous Users**.

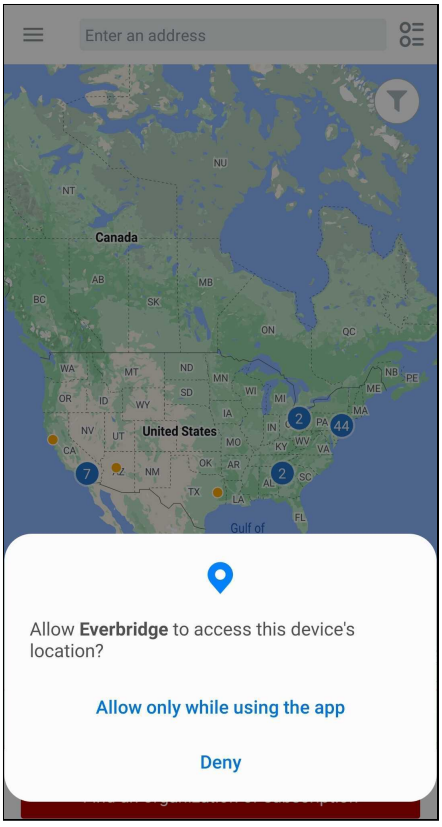
To use Everbridge as an Anonymous User:

1. Depending on your device, go to either the **Apple App Store** or **Google Play** and search for the **Everbridge Mobile App**.
2. Download and install the app on your device.
3. Open the Everbridge Mobile App on your device. The Everbridge login screen is displayed.

4. Tap **Explore the Map**. The soft request to share your location is displayed and provides an explanation of how Everbridge will use your location.

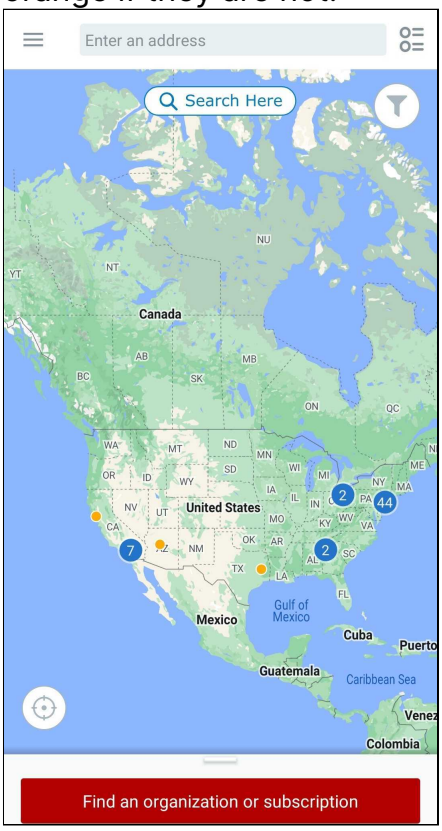


5. Tap **Allow Location Access** to zoom the Map to your current location and display active events around you. Or, tap **Not Now** to navigate the Map without sharing your location.



6. If you have allowed your location to be shared, Everbridge will zoom to your current location and display any active events around you. If you are zoomed out, polygons will become dots. They will be **red** if they are **Priority** and

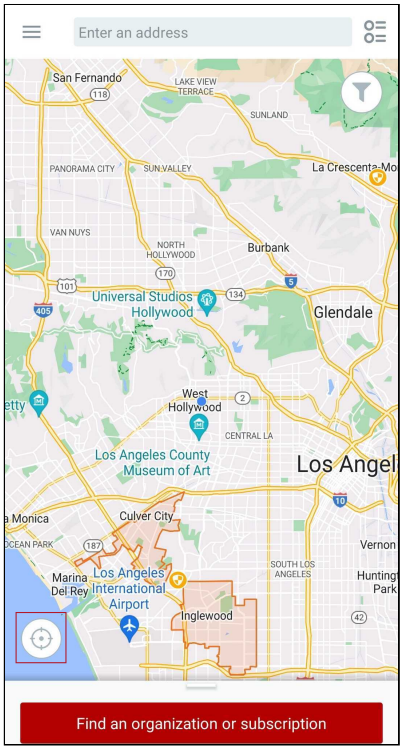
orange if they are not.



- If you are zoomed in far enough, the full polygon will display and will be **red for Priority** and **orange for non-Priority**.
- If you have not shared your location, the Map will default to a country-level view of the United States.

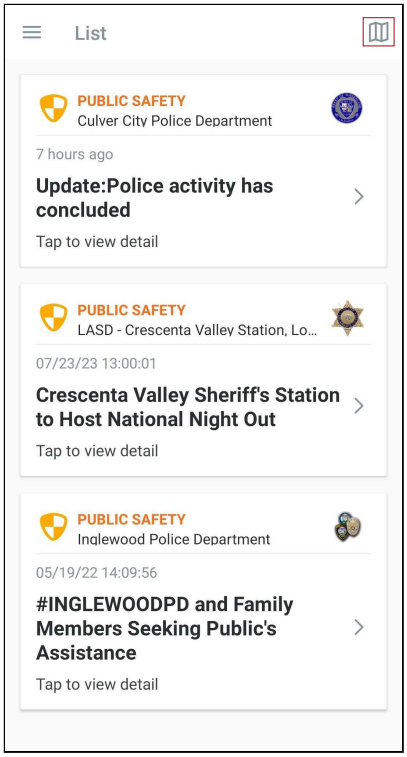
7. Review the following about using the Map:

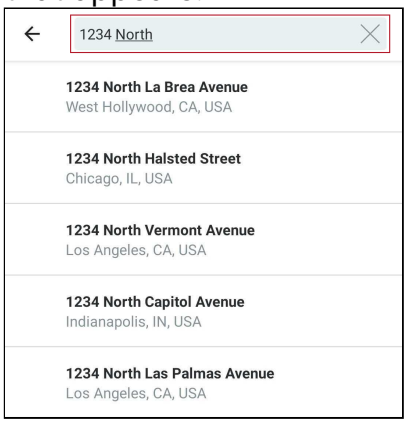
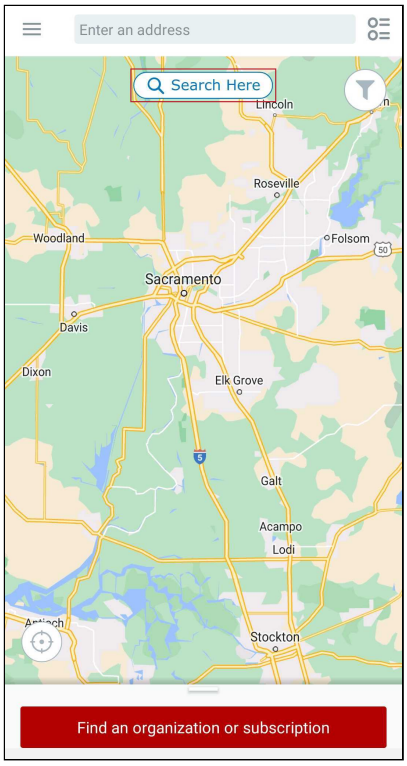
Action	Description
Zoom In	Pinch your fingers together on the Map to zoom in.
Zoom Out	Spread your fingers apart on the Map to zoom out.
Tap	Tap the **Compass** icon, located at the bottom left of the screen, to see your location.

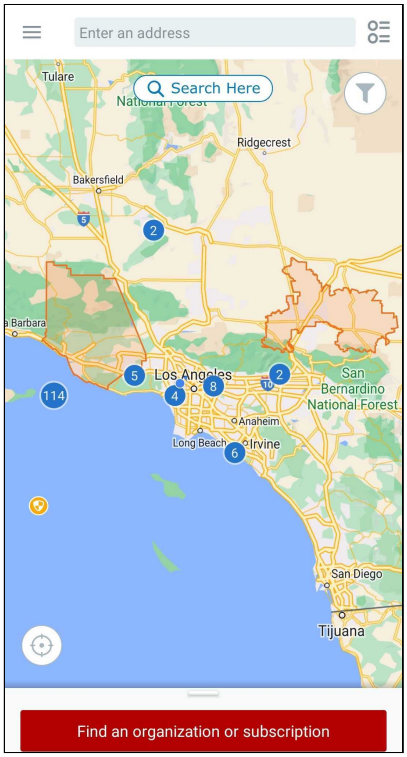


You can also drag the screen left, right, up, and down to pan around the Map.

Tap the **List** icon, located at the upper-right of the screen, to display a list of all the Incidents.



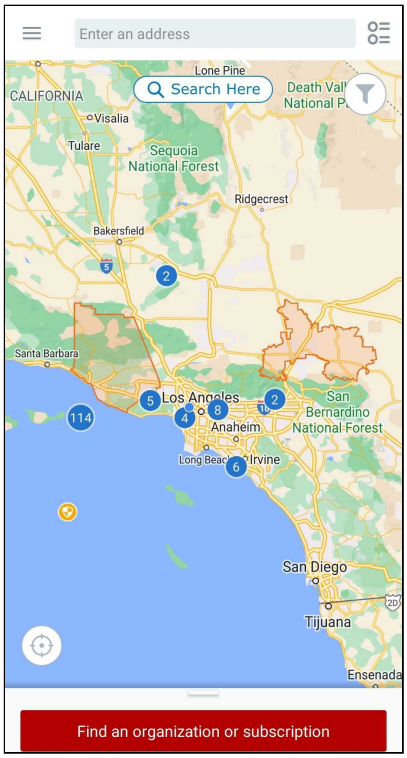
	Tap the **List** icon again to return to the Map.
Search	Enter an address and tap the address you want from the list that appears. 
Pan the Map	Tap **Search Here** after you have moved the Map location from one area to another. This way, any Incidents for the area are updated. 
Cluster	Tap a dot containing a number to expand the cluster to see the number of Incidents in the same area. Refer to the procedure To expand a cluster, below for more details.



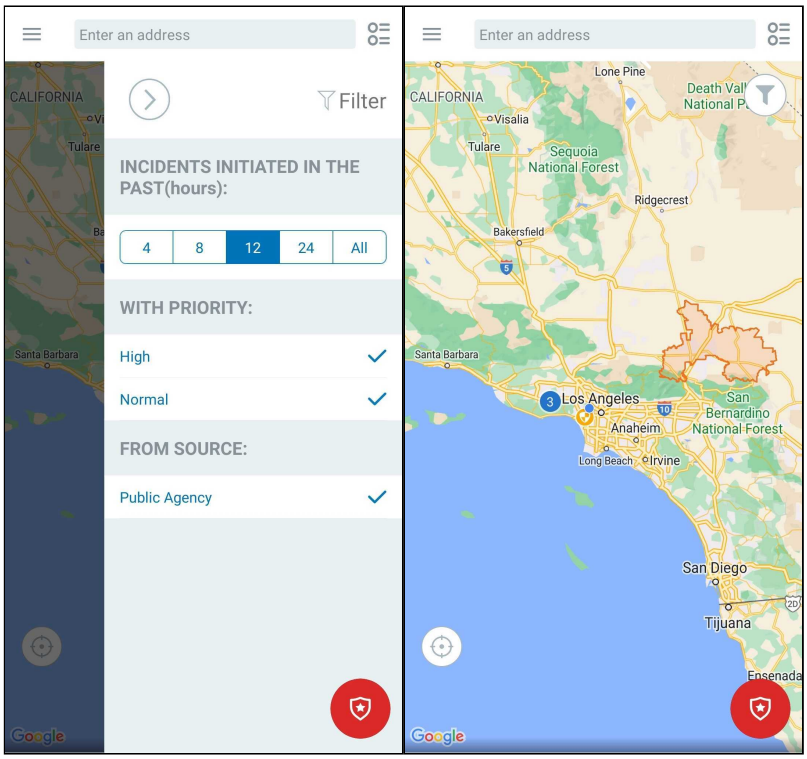
Filter

Tap the **Filter** icon (looks like a funnel) to see Incidents in the past 4, 8, 12, 24, or All hours. Then select High and/or Normal priority.

The following example shows no filters.

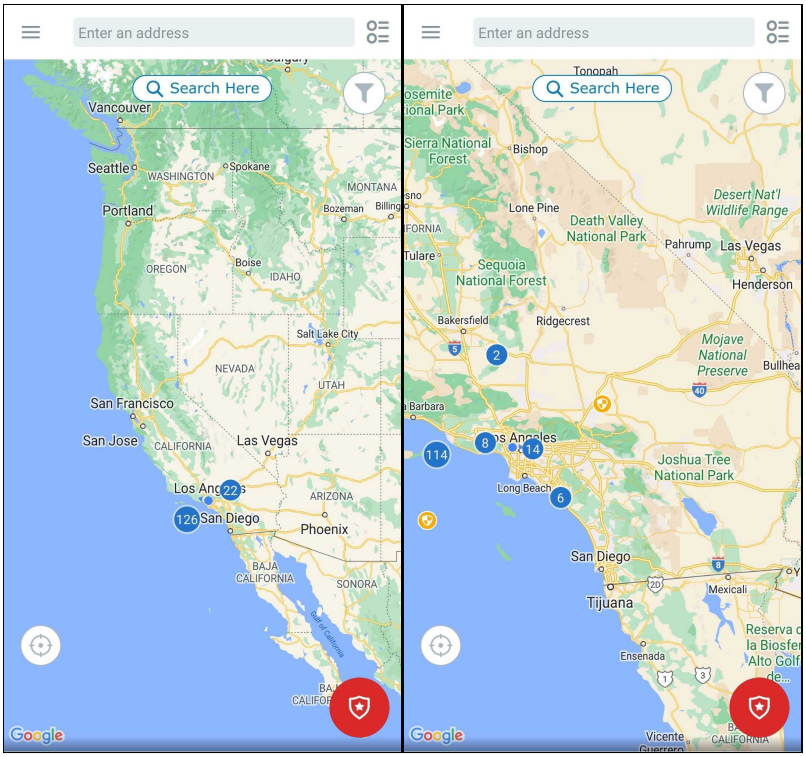


In addition, if your Organization uses Incident Zones, you can select From Source: **Public** or **Private**. In the following examples, **Public** (Public agencies) was selected.



To expand a cluster:

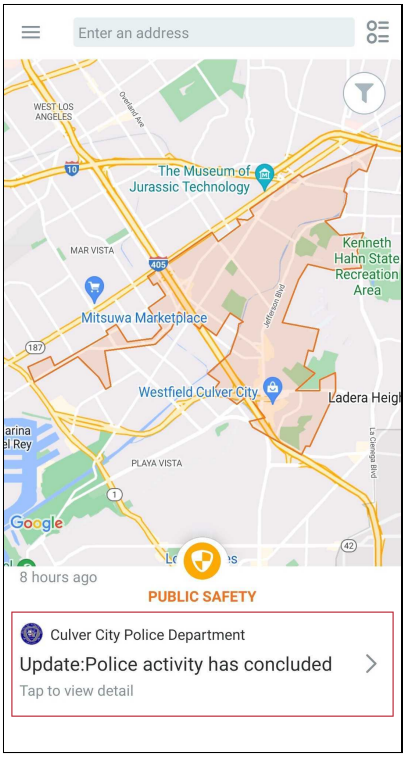
1. Tap a blue dot containing a number to expand the cluster. The Map zooms in to display the active events in the area of the cluster. The cluster separates and displays the actual polygons that were previously clustered together.



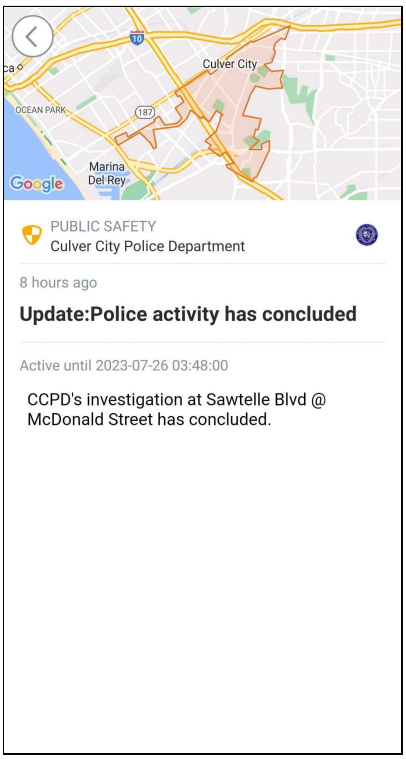
When viewing your Everbridge Map, you might see a few different polygons:

- **Purple Polygon** - Indicates that there is more than one Incident in that area.
- **Orange Polygon** - Indicates non-priority Incidents with orange icons.
- **Red Polygon** - Indicates priority Incidents with red icons.

2. Tap a **polygon**. A preview of the events that are in the shape appears at the bottom of the screen. The Map zooms to center the polygon on the upper portion of the interface.



3. Swipe left to cycle through all the events that are in the polygon.
4. To see the details of an Incident, tap on its preview.



5. Tap the **Back** button at the top to return to the Incident.

There are two ways to get data on the Everbridge Map:

1. Everything published to Nixle is uploaded to the Map.
2. Incident Zones.

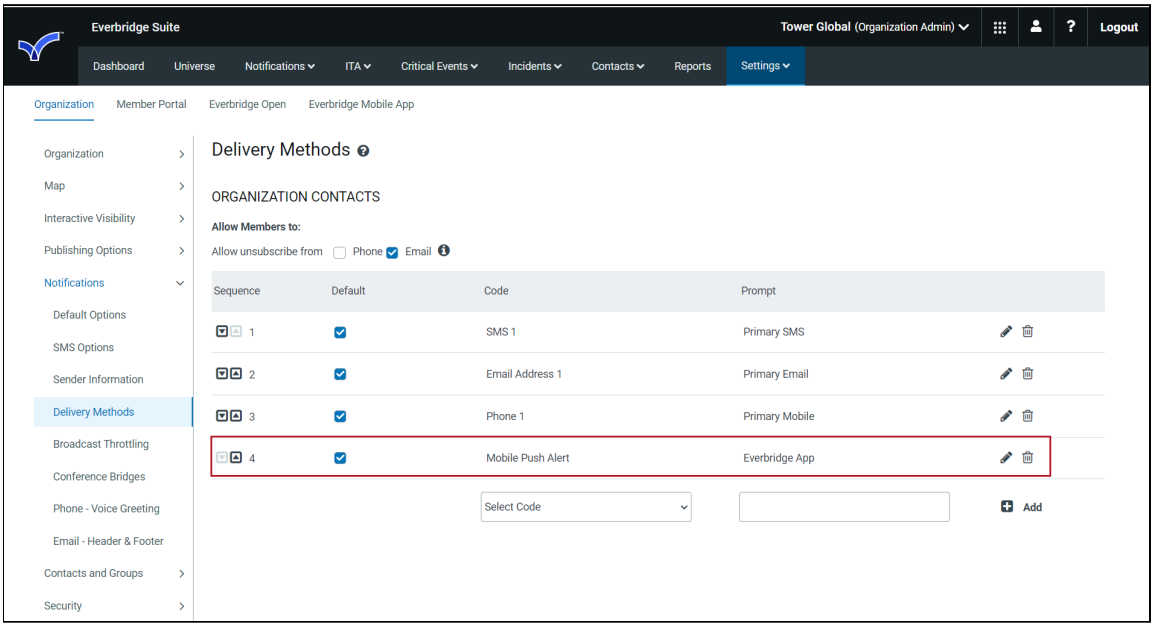
Enabling the Everbridge Mobile App

The **Notifications Settings** in your Organization allow you to directly configure many default options within the Everbridge Suite system. It provides immediate access to the Organization Settings so that you can adjust them specifically to your Organization's preferences.

As an Administrator, access the **Settings** tab, then click **Notifications** on the left-hand pane.

Delivery Methods

Click **Delivery Methods** to configure the available options in Everbridge Suite. You can view the various Delivery Methods by selecting them from the drop-down list. Selecting the Delivery Method reduces the number of options to select to launch a message and can help reduce the risk of human error. In this case, you must select **Mobile Push Alert**.



All Delivery Methods are explained below. You can:

- Add new Delivery Methods to the list and set the prompt. When you add a prompt to a selected method, the prompt is displayed to the contact. There are a number of path codes from which you can choose. The different path

codes will prompt you for different types of input when you add a contact. For example, choosing:

- **E-Mail Address** provides a text box to type an SMTP address (username@domain.com). An example prompt might be a Business Email or a Personal Email address. The contact confirms by clicking the link: "Please click here to acknowledge receipt of this message."
- **Phone** allows you to type a phone number. An example prompt might be Business Phone or Home Phone. Type the digits with or without the hyphens and/or brackets. (For international phone numbers, provide the Country Code + City Code + number.)
  - **Phone** - The contact confirms a phone Delivery Method by pressing a key requested at the end of the message.
  - **Fax** - The contacts confirm a fax Delivery Method by calling the phone number provided on the fax, entering their contact ID and password, then typing the PIN provided on the fax.

    NOTE: When you edit a Phone Delivery Method, you can change the prompt.

- **Extension Phone** has a text box for a phone number and one for an extension number.
- **SMS Device** has a text box for a phone number. An example prompt might be Text Message. Type the digits with or without the hyphens and/or brackets. The contacts confirm an SMS device Delivery Method by using the device's **Reply-to** option.
- **Numeric Pager Device** allows you to type a pager number. Type the digits with or without the hyphens and/or brackets.
- **TTY Device** has a text box for a phone number.
- Mobile Push Alert

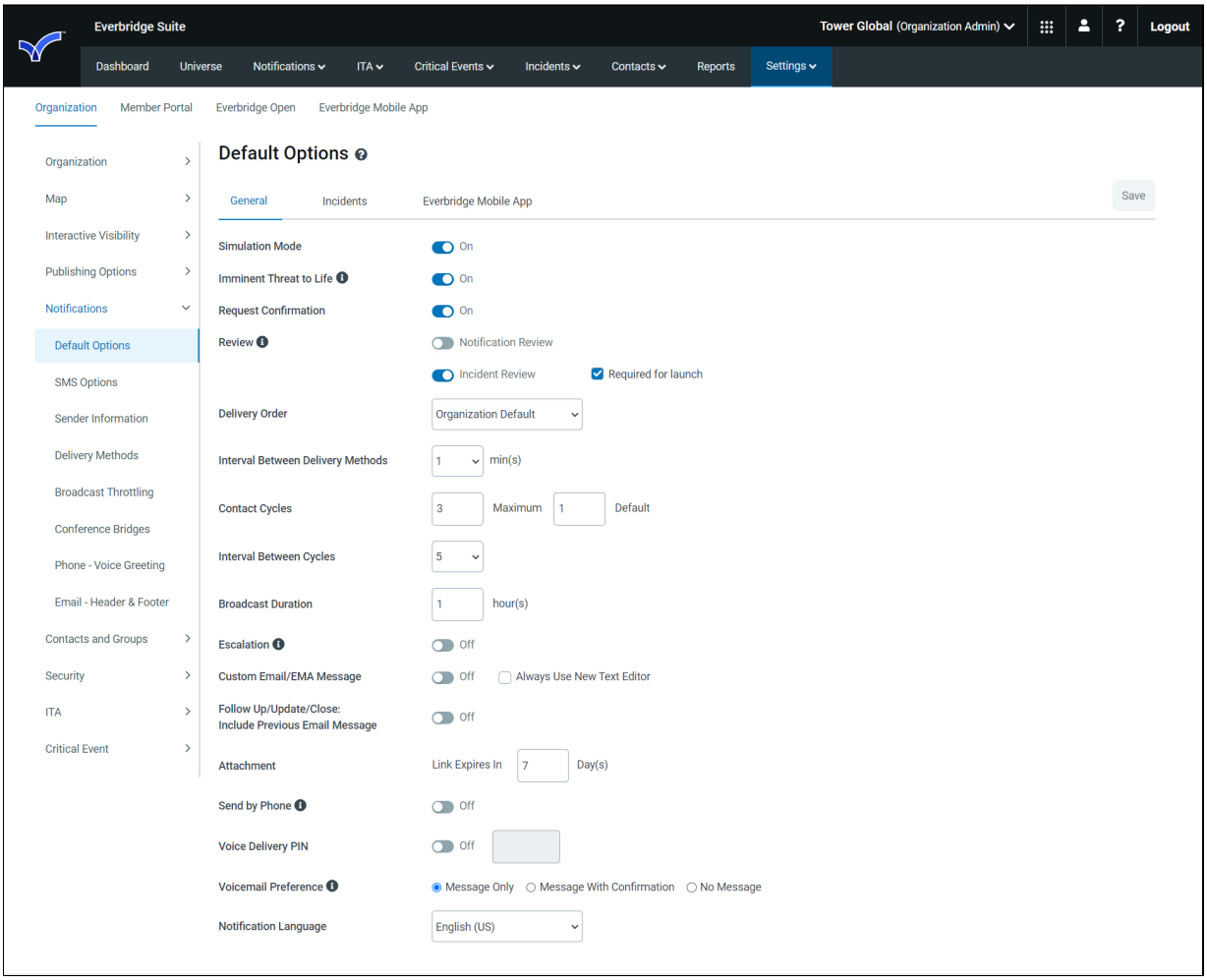
  NOTE: The Everbridge Mobile App runs on iPhones, iPads, and Android Smart Phones and tablets. It is fully integrated with the Everbridge Suite and turns Notifications into two-way communication. This enables end recipients to become the "eyes and ears" of the Organization during a crisis by responding to surveys, supplying additional information, and sharing their locations and real-time images from the scene.

- Move Delivery Methods in the list using the **Up and Down arrows** located on the left-hand side of each path code. When you send a Notification, the default methods are already selected for you as Delivery Methods for that Notification. The Notification sender can change the methods for the

Notification, but setting the defaults for the most common Delivery Methods helps to eliminate mistakes. You can edit a method by clicking the Pencil icon in the desired row. After making changes, click the **Save** icon to keep your changes or the **Cancel** icon if you do not want to keep your changes. You can delete a method by clicking the **Trash Bin** in the desired row. Confirm the deletion. (Be careful that this Delivery Method has not been used in a template or recurring Notification.)

Default Options

Next, click **Default Options**. Enter your Default Options and click **Save** when you are done. When you are sending a Notification, you can change these settings if needed. Configuring the most commonly used settings as the Default Options reduces the chances of human error while sending the Notification.



You can enter all your Default Options (discussed next) or only the Everbridge option.

NOTE: Selecting the **Message Sharing** checkbox under **Notifications** > **Default Options** > **Everbridge Mobile App** allows your contacts to share solicited messages with their extended network and default Notification sharing.

- **Simulation Mode** - Toggle on to enable users to practice sending Notifications and Incidents without notifying any Organization contacts. To send a Notification or Incident in Simulation Mode, users must turn off the "Go Live" toggle in the upper-right of the screen when drafting a new Notification.
    - Account Administrators (or Organization Admins) can set a user's permission to "**Restrict to simulation mode only**" for Notifications and Incidents separately. This will allow that user to only send simulated Notifications or Incidents. These settings can be configured in under **Access** > **Roles**.
- **Imminent Threat to Life** -Toggle on if your Organization uses Life Safety Notifications.
- **Notification Language** - Use this option to include the language-appropriate text or voice prompts in each message. The Language setting is also used to convert your message text into an audio message for Notifications sent to the voice path. Your users can select another language when preparing a new Notification. (Note: The language setting does not translate the text. You must enter the text in the correct language.)
- **Voice Delivery PIN** - Use this option to ensure your Notifications sent to a phone path are only heard by an authorized recipient. Select the checkbox and enter a PIN (4-10 digits). Distribute the PIN to your contacts before sending a voice Notification. When your recipients receive a voice call, they will first be prompted to enter the PIN before the Everbridge application will play the message. Your message senders can disable this option when preparing a Notification if they do not want message recipients prompted for a PIN code.
- **Confirmation Requested** - Use this option to request a confirmation of receipt from your message recipients. For example, in a Notification sent to an email address, Everbridge will include a hyperlink for the users to confirm receipt of the message. In a voice message, users are prompted to press a key. The Notification Report reflects who confirmed receipt of your Notification.
- **Review** - Enable or disable the Review step for Incidents or Notifications, and specify if it's required for launch.
- **Enforce Privacy** - Enforces privacy limits for your Delivery Methods to only the Everbridge Mobile App and will display “New private Notification” on the device home and lock screen instead of the Notification subject.

- **Voice Mail Preference** - Use this option to instruct the Everbridge application how to behave if it encounters voice mail when attempting to deliver a voice Notification. You can select whether to end the call (No Message), leave the message (Message Only), or leave the message along with call-back information for confirming receipt (Message with Confirmation).
- **Broadcast Cycles** - Use this option to set the number of times the Everbridge application should attempt to notify your contacts. In **Maximum**, enter the highest number of cycles your users can use; they will not be able to change this value when preparing a Notification. In **Default**, enter a default value for all new Notifications; your users will be able to change this value before they send the Notification. For example, if you send a Notification to contacts who have four devices in their Contact Record and the Broadcast Cycles is set to "2," then the Everbridge application attempts to send the Notification twice to all devices, assuming the contact has not already confirmed receipt.
- **Broadcast Duration** - Use this option to control for how long the Everbridge application should attempt to notify your contacts and for how long your contacts have for confirming receipt of your Notification. Ensure the duration is long enough to send all of the messages. If you have a high number of contacts to whom to send messages and the duration is too short, the Notification might not go to all contacts.
- **Interval Between Cycles** - Use this option to control how long the system waits before trying the next cycle. If you use "0" (zero), the next cycle begins immediately after the previous cycle.
- **Interval Between Delivery Methods** - Use this option to control how long the system waits before moving on to the next Delivery Method for a contact. For example, if the contact has four Delivery Methods, then this is the length of time (in minutes) the system waits before sending the Notification to the next Delivery Method. If the contact confirms one path, then system will not attempt a Notification to the subsequent paths. If you use "0" (zero), then the system tries to send the Notification to all devices as quickly as possible.
- **Delivery Order** - Use this option to select the order of the Delivery Methods used for the Notification.
    - **Organization Default** - The order specified in **Settings** > **Organization** > **Notifications** > **Delivery Methods** at the Organization level. This option will override the Delivery Method order specified in the Contact Record.
    - **Account Default** - The order specified in **Settings** > **Organization** > **Notifications** > **Delivery Methods** at the Account level. This setting overrides the Delivery Method order specified in the Contact Record.
    - **Contact Preferred** -The order specified in each Contact Record.
    - **One-Time Custom** - Define the Delivery Method order for this single Notification; this option overrides all other Delivery Method orders.
- **Notification Escalations** - Use this option to allow users to define an escalation policy within a Notification under Notifications or Incidents.

- **Allow Separate Email Content** - Use this feature to allow your users to include a separate message for email Notifications using a rich text formatting tool. Users will be able to also use a separate plain text message for SMS text, fax, pagers, and text-to-speech.
- **Invite these contacts to the Incident chat** - Use this feature to create and use a chat in your Incident Notifications.
- **Launch Notifications by Phone** - Use this feature to allow your users to launch Notifications by phone for Incident Management and/or Mass Notification.
- **Scenario Manager** - Use this option for Incident Management.
- **Exercise Mode** - Use this feature to show the Exercise Mode in Incident Management. If you are using Crisis Management, the checkbox is automatically enabled and you cannot disable it. If you are using Incident Communications, you can select or clear the checkbox.
- **Incident Notification Review Step** - Enables the operator to use a review step before sending or scheduling. When you select **Yes**, a review step will be required for launch.
- **Contact Batching** - When the **Incident Management** checkbox is selected, it enables messages to be sent to contacts in batches until the number of responses is met or the broadcast duration ends.
- Everbridge Mobile App
  - **Message Sharing** - Use this feature to allow your contacts to share Notifications you send with their extended network. Optionally, toggle default Notification sharing OFF.
  - **Send Secure Push Messages** - To contacts: Select this checkbox to send Notifications to other devices like highway signs and reader boards. This is listed in the Everbridge Mobile Safety App settings because Everbridge uses the push alert Delivery Method to send the data. To Secure Messaging apps: Select this checkbox to send secure push messages to Secure Messaging Apps.
- **Event Subscription** - Select the checkbox to allow subscribers to be anonymous.

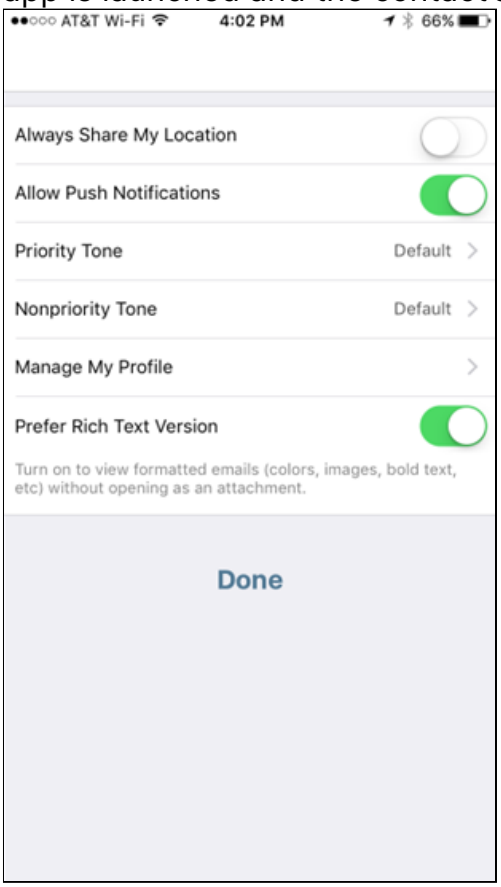
Performing Device-Only Registration

Contacts can register their devices so their administrators can send them Notifications without having to be registered in the Member Portal. This type of registration is by means of the contacts' mobile devices.

Workflow

To perform a device-only registration:

1. The Administrator logs in to the Everbridge Suite system and accesses the **Contacts** tab of your Organization.
2. The Administrator selects the desired contacts.
3. The Administrator selects **Mobile Device Registration** from the **Send Invitation Email** drop-down list or the **Device** icon for those contacts.
4. Each selected contact receives an invitation email, which is limited to one per device. If the contact wants to install it on an iPhone and an iPad, the Administrator must send two invitations. Using the mobile device, each contact clicks the URL link from the email. (A unique link is associated with a single Contact Record.) A Confirm dialog is displayed.
5. Click **OK** to launch the Everbridge Mobile App. The Everbridge Mobile App is retrieved from the device's app store.
6. Download and install the Everbridge Mobile App.
7. Open the email invitation and click the URL link again. The Confirm dialog is displayed again.Tap OK to launch the Everbridge Mobile App. This time, the app is launched and the contact's account is displayed at the Settings page.



8. Tap Done to go to the Messages page.
9. From the Contacts tab of Everbridge Suite, edit the contact to review his/or Delivery Methods. It now displays **Enabled** next to the Mobile Member App.

From the **Contacts** page, both the **Member Portal Envelope** icon and the **Device** icon are still displayed next to a contact's name. This avoids:

- using the Member Portal to sign up
- creating a username and password

The Administrator will need to resend the Device invitation if the contact deletes his/her account, deletes the Everbridge Mobile Member app, or gets a new device.

> **NOTE:** If an Organization decides to use the Member Portal after Device-Only registration, the Administrator sends the Member Portal invitation. The contact creates a username and password, and continues with the usual registration (as explained in Registering as a Member and Logging In to Everbridge with Member Portal Credentials, next). The Device-Only information is replaced with the Member Portal information. When Member Portal registration occurs, both icons are removed from the Contacts page.

Registering as a Member and Logging In to Everbridge with Member Portal Credentials

There are two ways to register as a Member of an Organization:

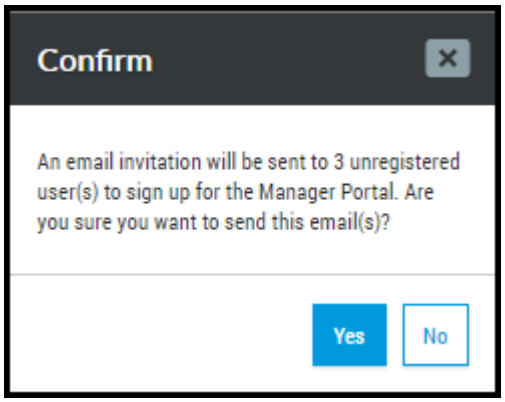
- By means of your mobile device
- Via the Member Portal

Both ways are offered in this document, but registering through your mobile device is faster.

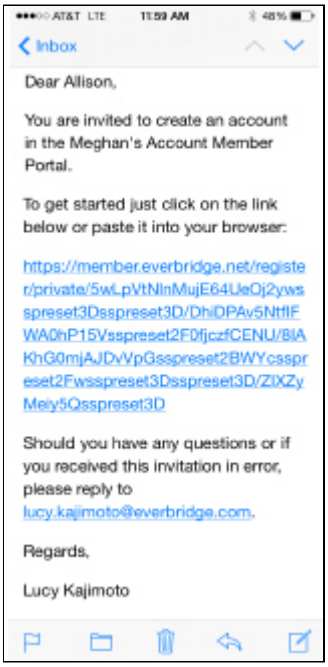
Workflow

To register a Member via the Everbridge Mobile App:

1. The Administrator logs in to the Everbridge Suite system and accesses the **Contacts** tab of the Organization.
2. The Administrator selects the desired contacts.
3. The Administrator selects **Member Registration** from the **Send Invitation Email** drop-down list or the **Envelope** icon for those contacts.
4. The Everbridge Suite system asks the Administrator to confirm the action.



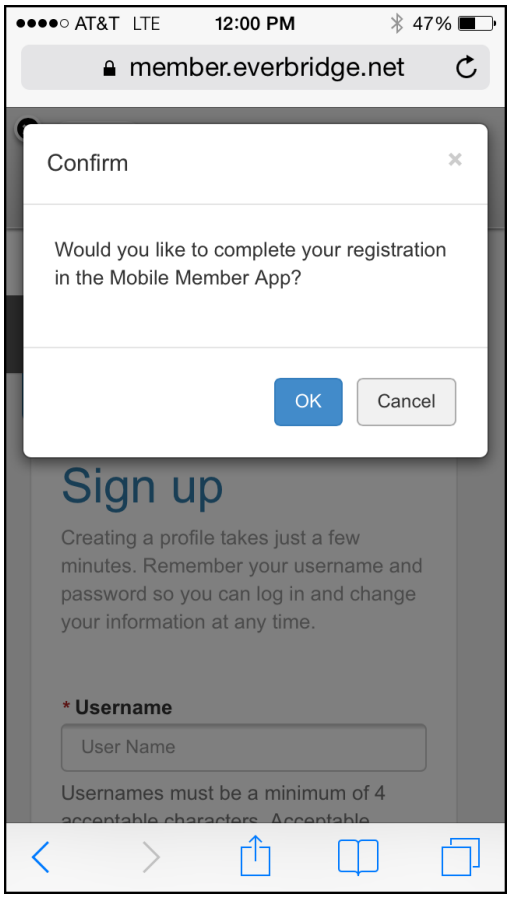
5. When the Administrator confirms the action, the selected contacts receive an email similar to the following:



6. Each contact clicks the URL link from their email.

   They can choose to complete their registration in the Everbridge Mobile App or in the Member Portal.

   - **Everbridge Mobile App** - If using an iOS or Android device, they can register via their mobile device.
   - **Member Portal** - If the contacts are not using an iOS or Android device, they can register via the Organization's Member Portal.
     - If using a **Private** portal type, the contacts are invited to access the site via email.
     - If using a **Public** portal type, the contacts access the portal via the public website.



7. The contact chooses how he or she wants to register:
    - Tap **OK**, then proceed to Registering via Your Mobile Device.
    - Tap **Cancel**, then proceed to Registering via the Member Portal.
        - If using a **Private** portal type, the contacts are invited to access the site via email. Private portal registration invitations expire after 30 days.
        - If using a **Public** portal type, the contacts access the portal via the public website.

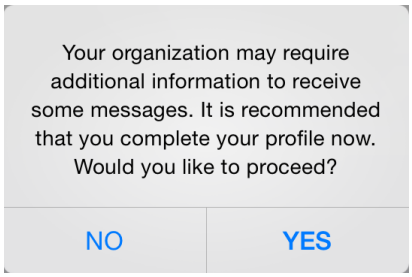
Registering via Your Mobile Device

If this is the first time you have entered the Member Portal, create a new account to add your user profile.

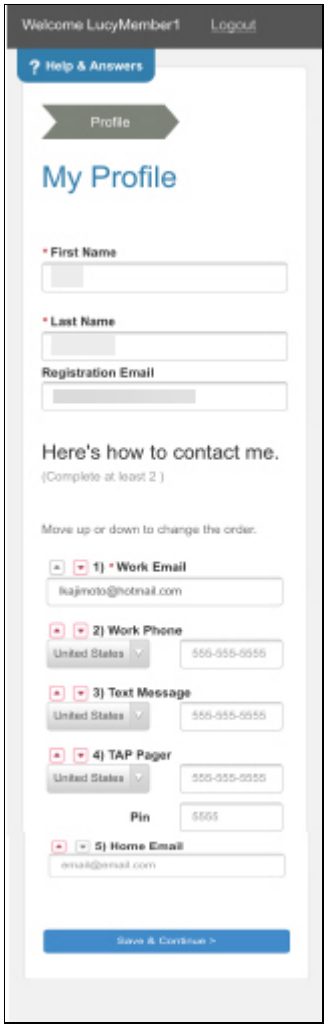
To register via your mobile device:

1. Tap **OK** to the question: **Would you like to complete your registration in the Everbridge Mobile App**? The Signup screen is displayed (scroll to see the entire page).

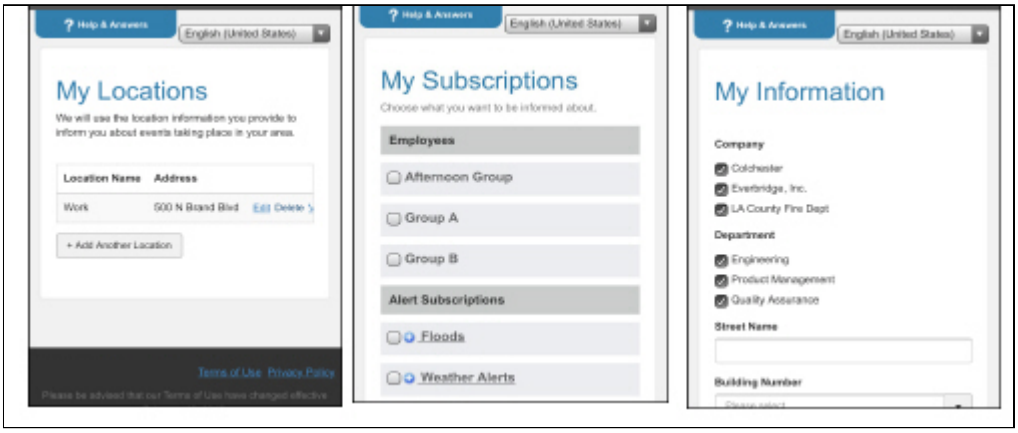
2. Fill in the fields.
3. Tap the checkbox accepting the **Terms of Use**. (You can read the Terms of Use by tapping the arrow to the right of the checkbox.)



4. Read the message and decide:
   - **NO** - You do not want to complete your profile now. Skip to the procedure To install the Everbridge Mobile App. You can complete your profile later. (See the procedure To manage your profile.)
   - **YES** - You want to complete your profile now. The first page, My Profile, is displayed.

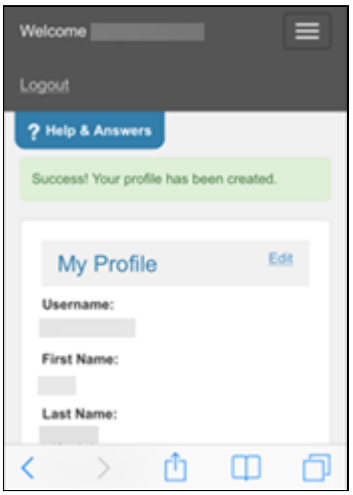


5. Fill in the fields (scroll to see the entire page), and tap **Save & Continue**.
6. From each screen, continue filling in the fields, as needed, and tap **Save & Continue**. The following examples show other pages of My Profile:



7. Scroll through the **Review** page and ensure your information is correct. As needed, tap **Edit** to modify the information.

8. Tap **Finish** to finalize your new profile. You see a message on-screen that your profile has been created.



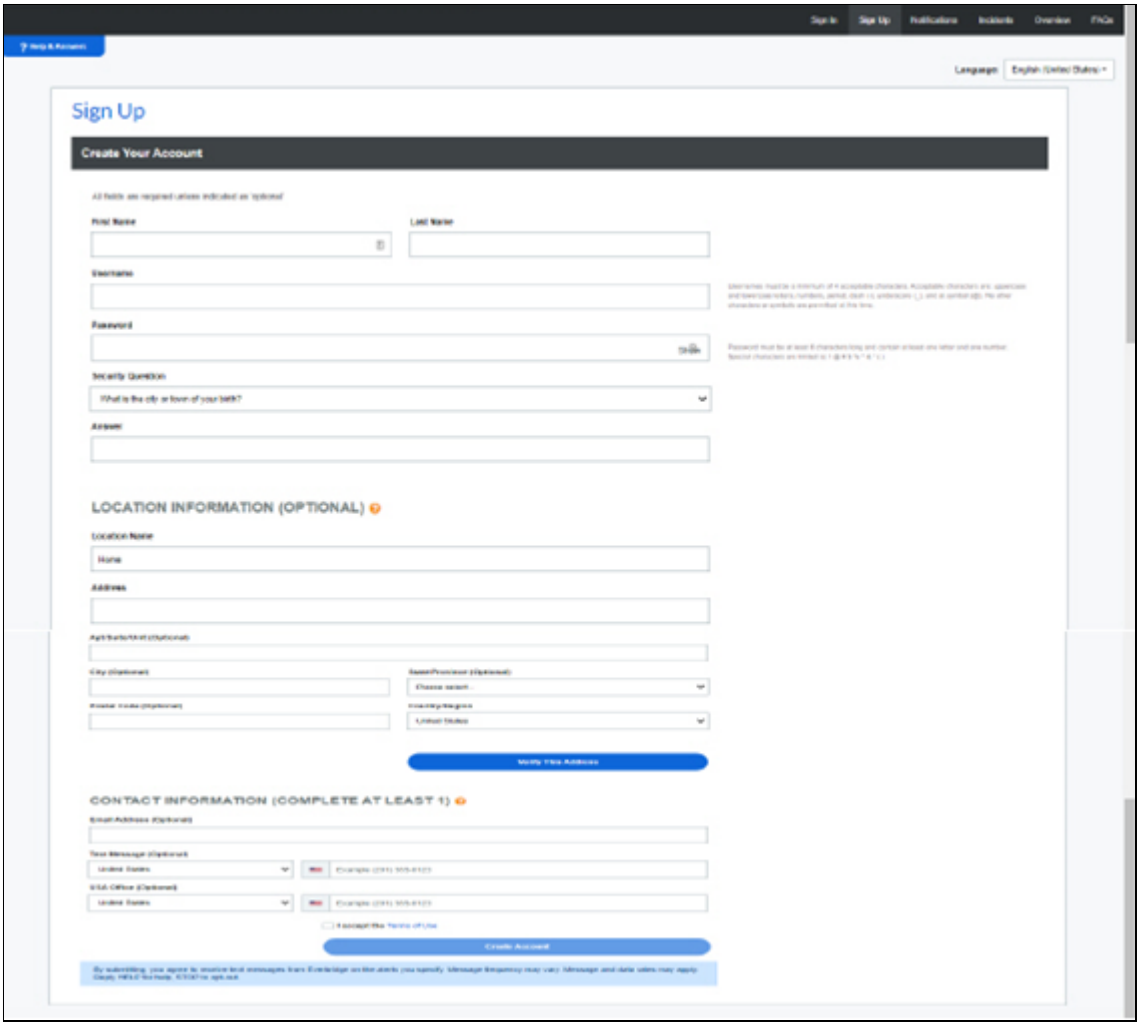
9. Tap **Done**.
    - If you already installed the Everbridge Mobile App, your account name is displayed.
    - If you need to install the Everbridge Mobile App, the Everbridge app is displayed. Proceed to To install the Everbridge Mobile App.

Registering via the Member Portal

In order to log in to Everbridge, you must first create a username and password from your Organization's Member Portal. Your Organization will give you instructions to navigate to your Member Portal where you can create or edit your account.

To create a username and password from your Member Portal:

1. If your Organization has enabled it, you will see a drop-down list of **Languages** from which to choose to view the Member Portal in that language. Alternatively, if enabled, you can view **Google Translate** as well.
2. Fill in the following fields on the **Sign Up** page.



Descriptions of the fields are explained below.

- **Username -** Create a Username for yourself. You will use this to log into the Mobile Member app. Usernames are case-sensitive and must be a minimum of four acceptable characters. Acceptable characters are: uppercase and lowercase letters, numbers, dash (-), and underscore (_). No other characters or symbols are permitted at this time.)
- **Firstname** and **Lastname** - Depending on your Organization, your Firstname and Lastname might already be filled in when you arrive at the Sign Up page. If not, fill them in now.
- **Password** - Create a Password. Passwords must be 8-64 characters long and contain at least three of the following four items: uppercase letter, lowercase letter, number, or special character. Special characters include: ! @ # $ % ^ & * (and). In the **Confirm Password** field, type the password again to confirm it. Your password does not expire. However, if you have both a Mobile Member account and a Manager Portal account, then your password expires in 90 days. If you change your

password during the 90-day period, the counter resets to zero (0) and starts a new 90-day cycle.
- **Email** - Enter your email address.
- **Security Question** and **Security Answer** - Select a security question from the drop-down list, and enter an answer that only you will know. If the system needs further confirmation of who you are, it will ask you this question.
- **Terms of Use** - Select the checkbox: **I accept the Terms of Use**. You must agree to the Terms of Use to use this site. You can review the terms by clicking on Terms of Use.
- **Click Create Your Account**. This displays your account profile for your review. The profile area of the Member Portal can be customized by your Organization, so it might not look identical to the examples shown here. You might be able to review the information or you might be able to make changes. Review or edit your information and click **Save & Continue** to move to the next screen. You have now completed your registration and can log out. Click **Logout** (top left).

3. Click **Create Your Account**.
4. Continue to Installing the Everbridge Mobile App.

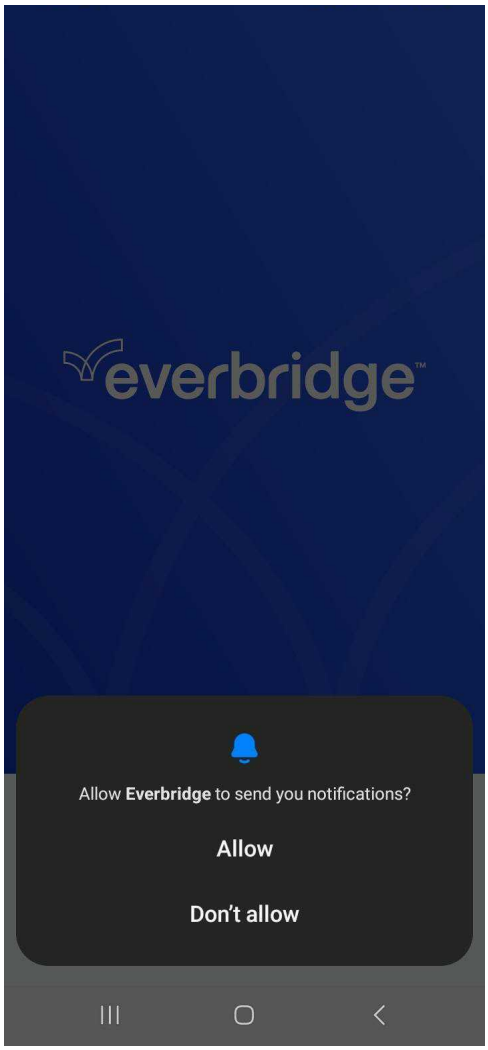
Installing the Everbridge Mobile App

After completing your Member Portal registration, the next step is to install the app for your device.

To install the Everbridge Mobile App:

1. Go to the app store for your device (Apple App Store or Google Play) and search for the Everbridge Mobile App.
2. Install the app to your device.
3. Once installed, tap **Open**. The Everbridge Welcome screen is displayed.

4. If prompted, tap **Allow** to receive Notifications.



5. Continue to the next procedure to configure the app settings.

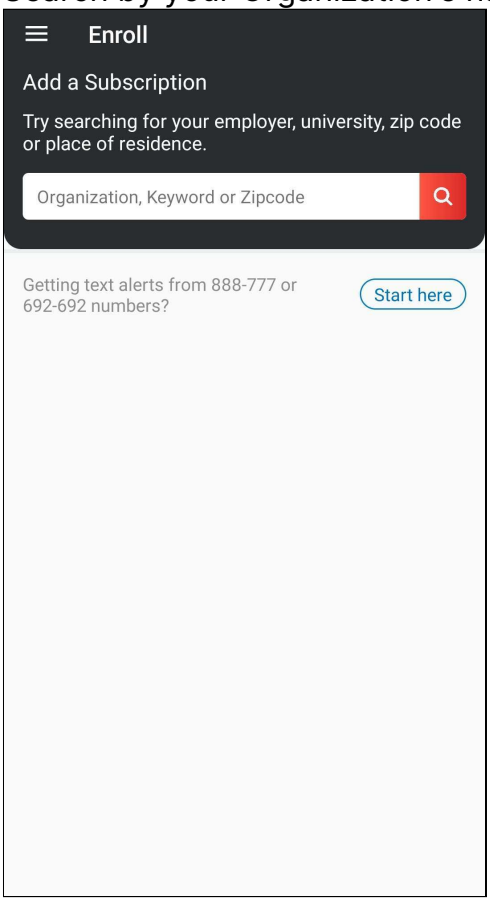
Configuring Settings

The final step is to add your account to the app and configure the Default Settings.

To configure settings:

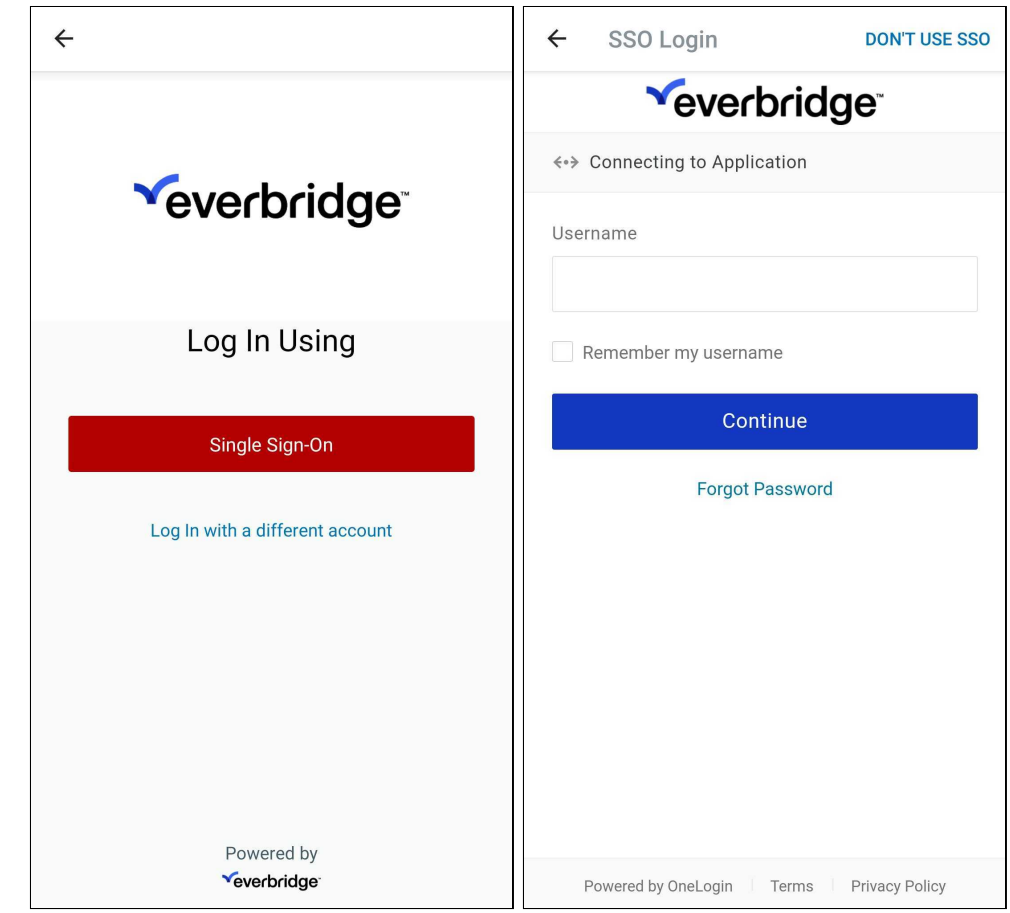
1. Assuming you already have an account, tap **Find an Organization or Subscription**.

2. Search by your Organization's name, keyword, or ZIP code.



3. Select your Organization, then enter the Username and Password you created during registration on the Member Portal.
4. Tap **Login** and skip to Step 4 for Single Sign On or Step 5. The Everbridge Mobile App settings are displayed.
5. Depending on an Organization's needs, Single Sign-on may or may not be available. In order to use Single Sign-On (SSO), your Account Administrator must enable SSO in **Account Settings** > **Security** > **Single Sign-On for Member Portal** and select the **Everbridge** checkbox for the desired Organizations.

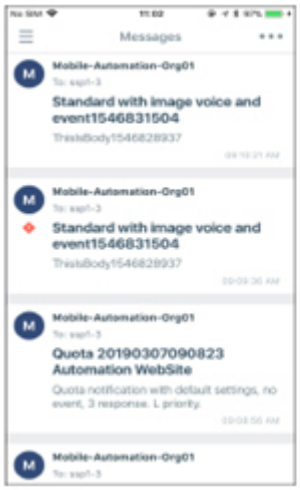
   If your Organization is using **Single Sign-On (SSO)**, enter your search term, and select your Organization. You are taken directly to your IDP URL.

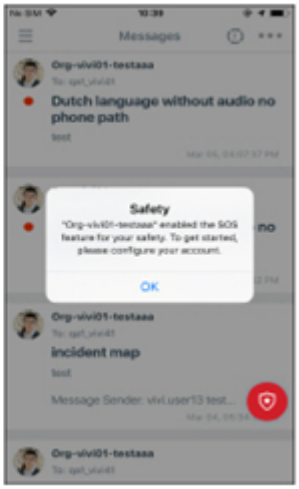


a. Search for and select the desired Organization in-app.
b. Select **Single Sign-On**.
c. Enter your username and password.

6. Optionally, tap the ON/OFF switch to change the settings.
   - Allow Push Notifications = ON - Allowing **push Notifications** will allow your Organization to reach you quickly. A push Notification is a way of communicating with a mobile device that goes directly to the application, not through email or some other path. You do not have to request the message. It simply arrives on your device, even if you are not in the Mobile Member App.
   - Priority Tone = Default - Tap **Default** to change the tone.
   - Nonpriority Tone = Default - Tap **Default** to change the tone.
   - Manage My Profile - Tap to change your Member Portal profile settings. Refer to the procedure To manage your profile.
   - Prefer Rich Text Version = ON - Keep this setting on to view formatted emails (colors, images, bold text, etc.) without opening an attachment.
7. Tap **DONE** to save your initial settings. The Everbridge Mobile App is ready to use. The first time you access the Everbridge Mobile App, you will see one of the following screens. If you have not already configured your Safety

Settings, tap **OK**, then refer to Safety Settings below.



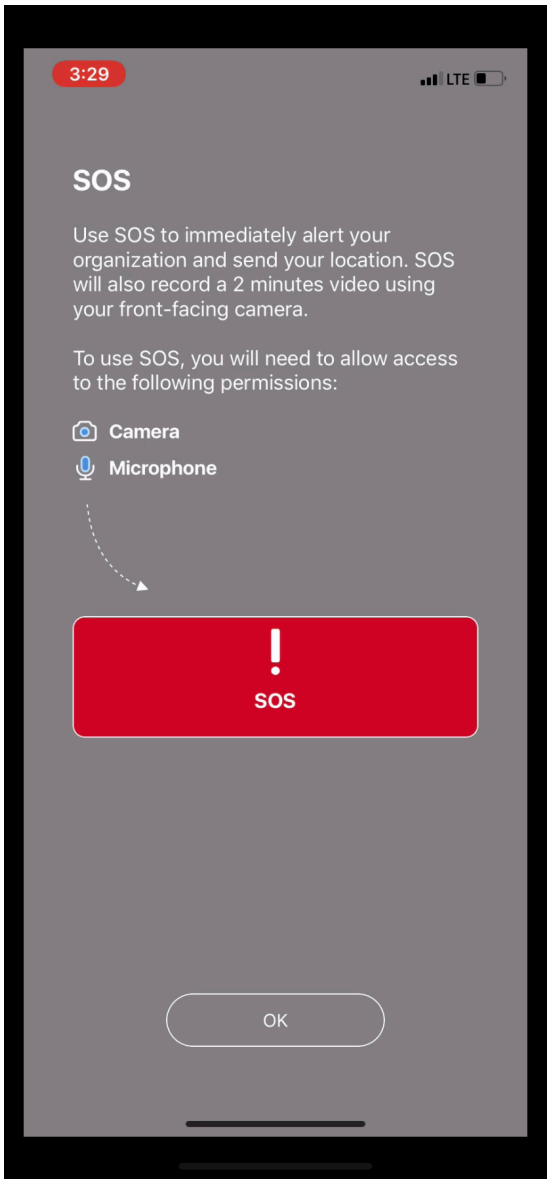


> **NOTE:** You only see the **Safety** icons at the bottom of the screen if your Organization has purchased these options.

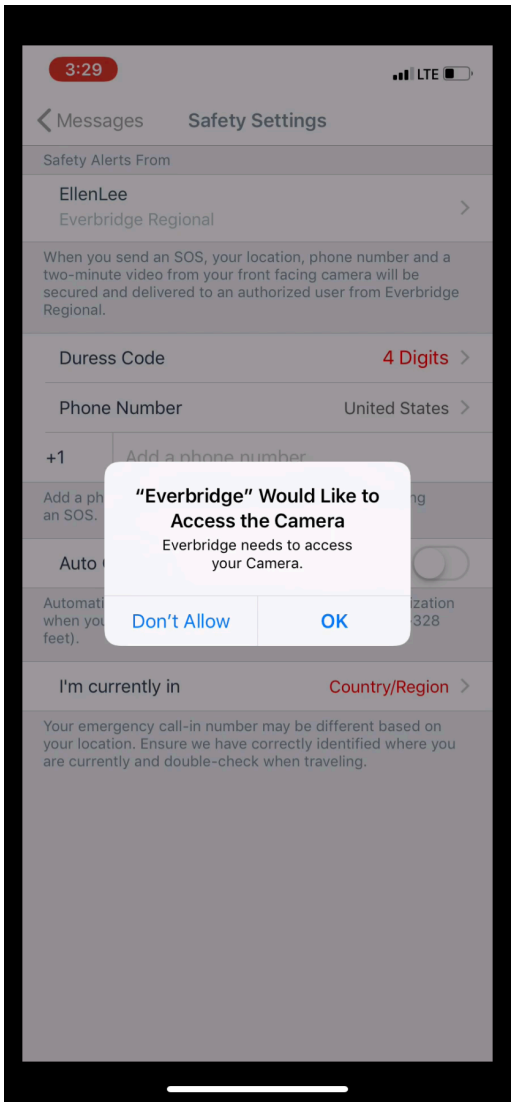
Onboarding Workflow

To log in when you have Safety Connection enabled:

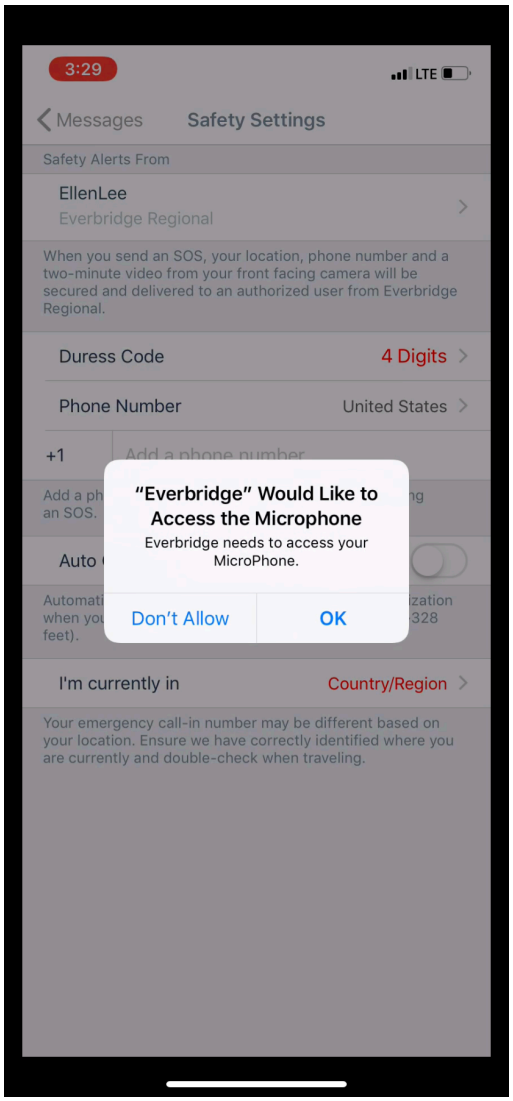
1. Login to Everbridge Mobile App. The **SOS** screen is displayed.



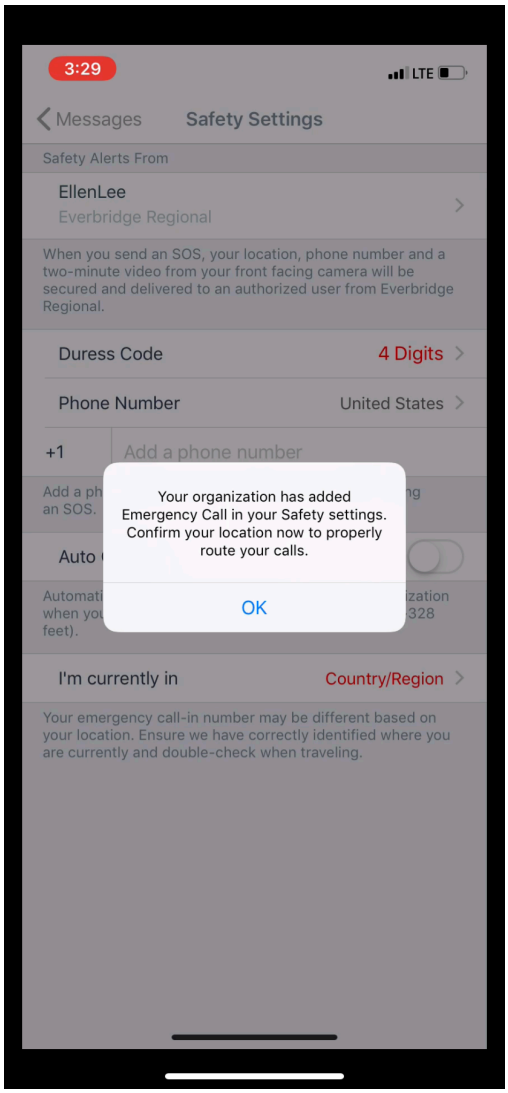
2. Tap **OK**. The **Safety Setting** screen is displayed.



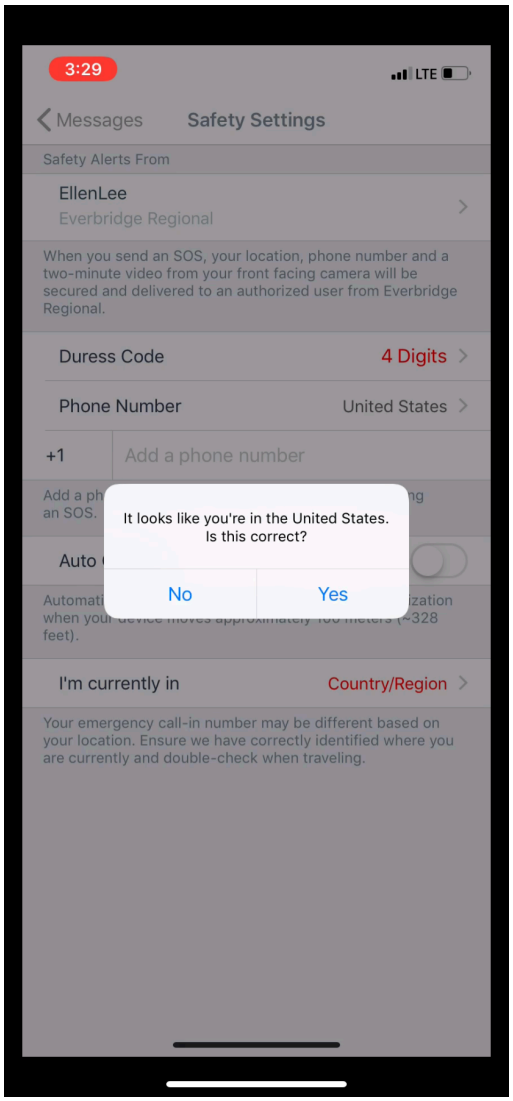
3. Tap **OK** to allow Everbridge to access the camera. The **Safety Settings** screen is displayed.



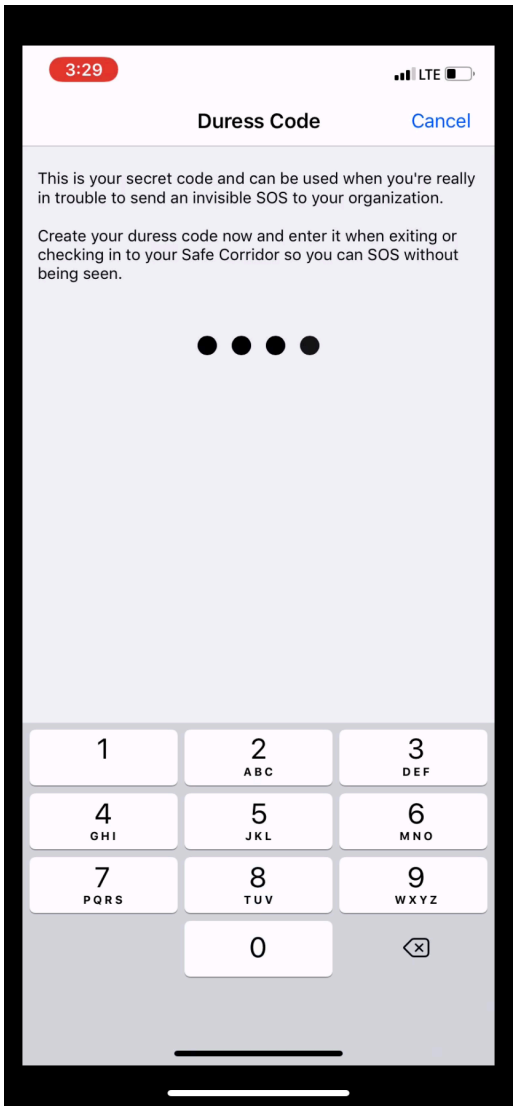
4. Tap **OK** to allow Everbridge to access the microphone. The **Safety Settings** screen is displayed.



5. Tap **OK** to confirm your location to properly route your calls.



6. Tap **Yes** if you are in the United States. (Otherwise, tap **No**.) The **Duress Code** screen is displayed.



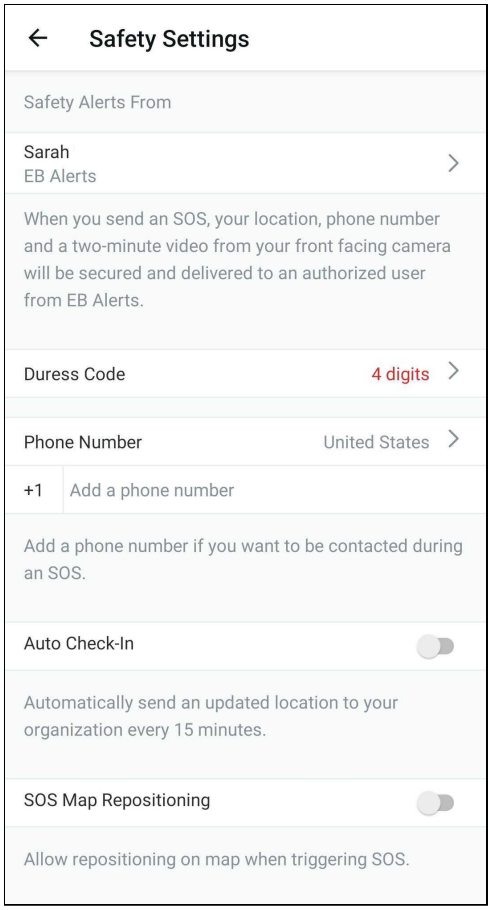
7. Enter a 4-digit code. This way, you can use the code when exiting or checking in to your **Safe Corridor** so you can send an SOS without being seen.

To change your settings in the future:

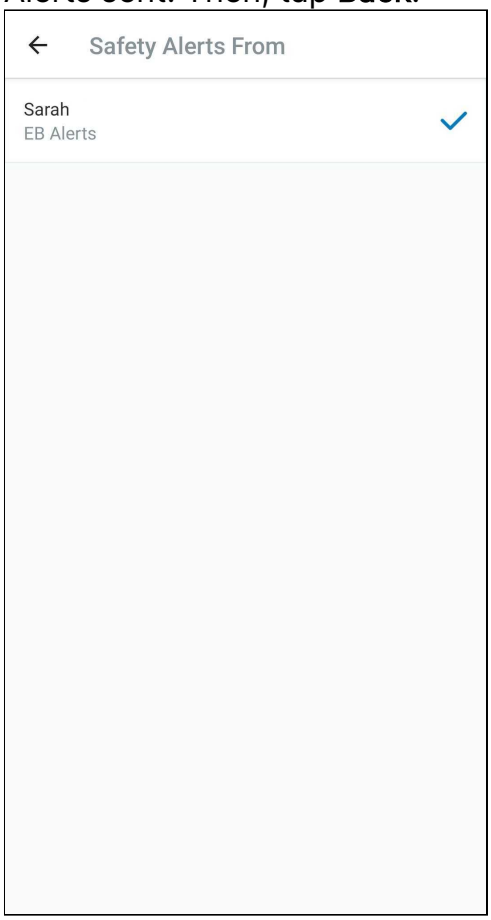
1. Open the menu, and tap **Profile**. A list of all Organizations to which you are logged in and/or subscriptions to which you are subscribed is displayed.
2. Make the desired changes, then tap **Back** until you see the **Unread Messages** screen.

> **NOTE:** To change the settings of your user profile, see the procedure To manage your profile, next.

- **Safety Settings** - Open the menu, and tap **Settings**. Then tap **Safety Settings**.

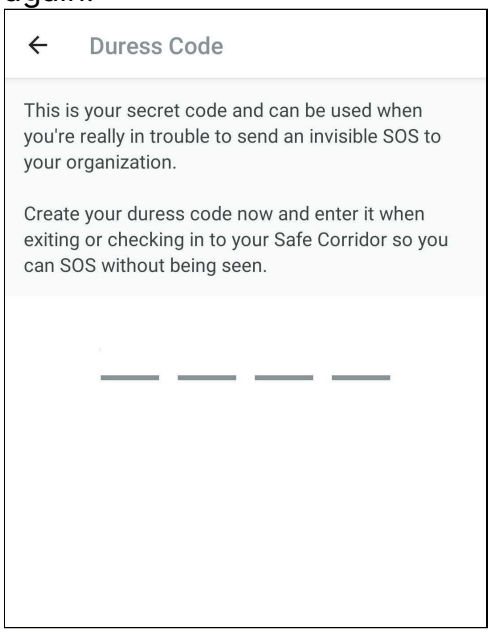

Safety Settings
Safety Alerts From
Sarah
EB Alerts
When you send an SOS, your location, phone number and a two-minute video from your front facing camera will be secured and delivered to an authorized user from EB Alerts.
Duress Code
4 digits
Phone Number
United States
+1
Add a phone number
Add a phone number if you want to be contacted during an SOS.
Auto Check-In
Automatically send an updated location to your organization every 15 minutes.
SOS Map Repositioning
Allow repositioning on map when triggering SOS.

- **Safety Alerts from** - Tap the account from which you want Safety Alerts sent. Then, tap **Back**.

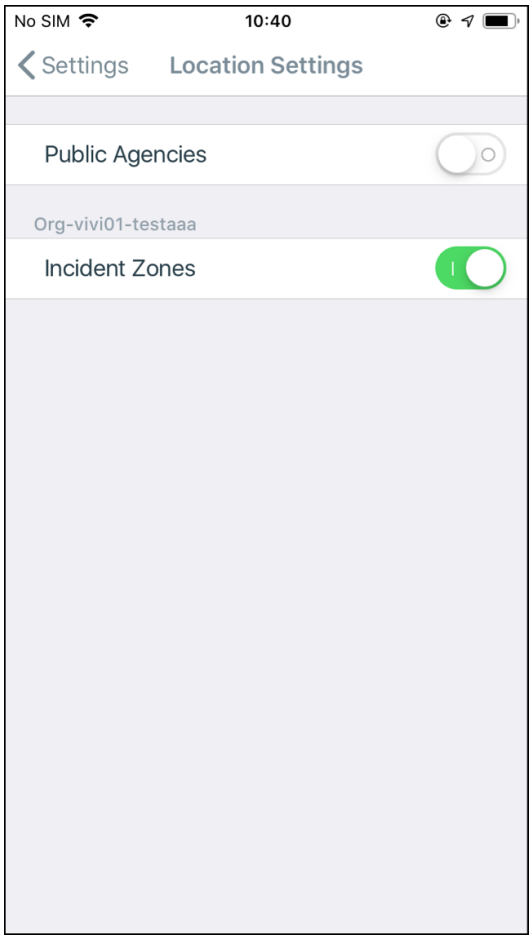


- **Duress Code** - Enter a 4-digit Duress code, which is used to trigger an **SOS** in **Safe Corridor**. Confirm the code by entering it

again.



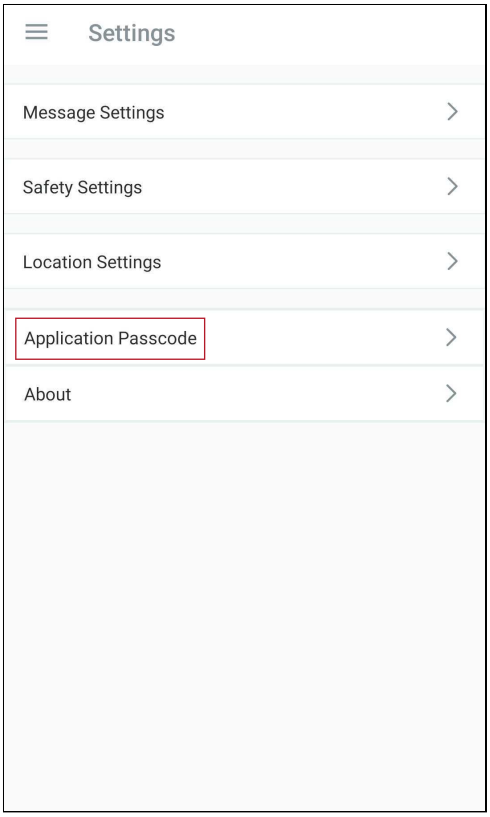
  - Add a phone number if you want to be contacted during an SOS. Select the Country/Region, then enter the phone number.
  - **Auto Check-In**—Tap to toggle ON auto check-in. With Auto Check-In enabled, your geolocation will be updated every time there has been a significant change in the device's location, such as 100 meters (109 yards) or more.
- **I'm Currently In** - If enabled, your Organization will have configured a phone number for you to contact an actual person by tapping the Emergency Call button, depending on the country where you are located. Tap **YES** to allow the GPS to determine the country. Or, tap **NO** to manually select the country from the Country drop-down list.
- Location Settings - If enabled for your Organization, you can toggle public Incident Zones and/or private Incident Zones.



- **Application Passcode** - Allows the user to configure a 4-digit passcode for their app.
- **About** - Displays the Version, Terms of Use, and Privacy Policy.

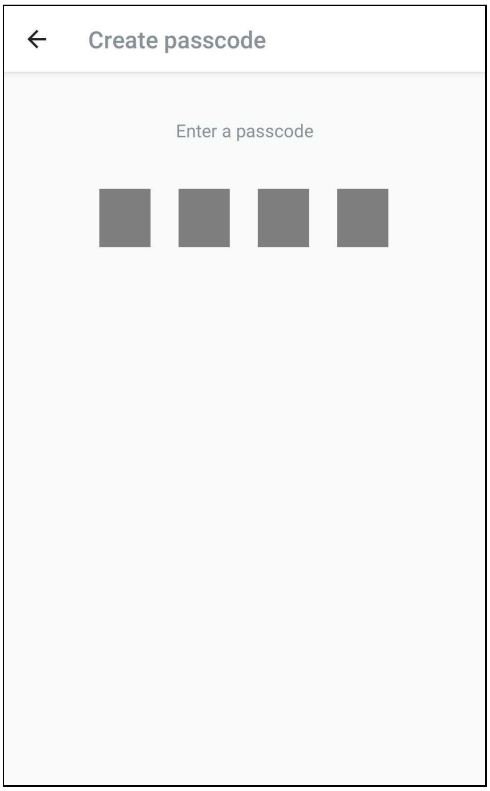
To enable an account passcode in **Settings**:

1. Tap **Application Passcode**.

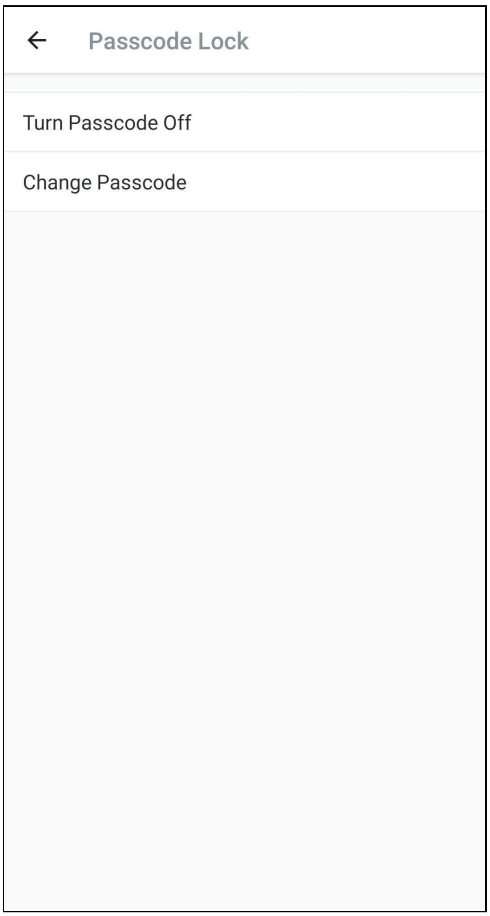


2. Tap **Turn Passcode On**.

3. Enter your 4-digit passcode and re-enter it to confirm.



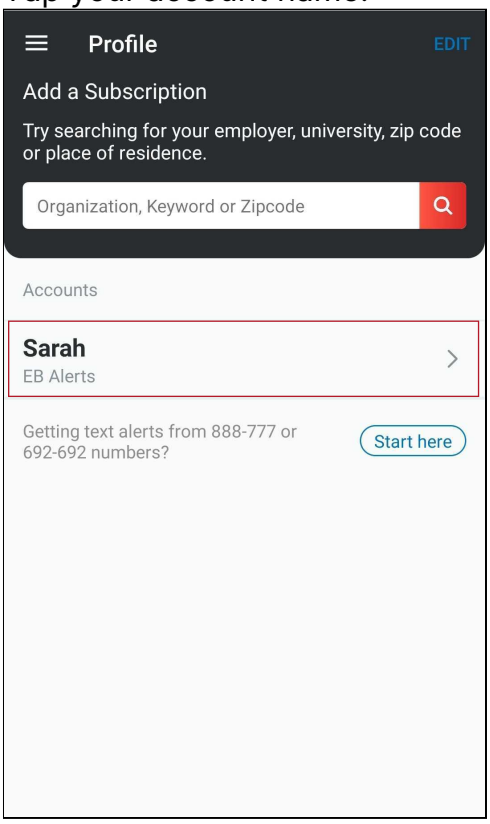
The **Passcode Lock Screen** indicates if the Passcode is on or off. You can also change your passcode from this screen.



To manage your profile:

1. Tap the hamburger menu in the top-left corner, and then select **Profile**.

2. Tap your account name.

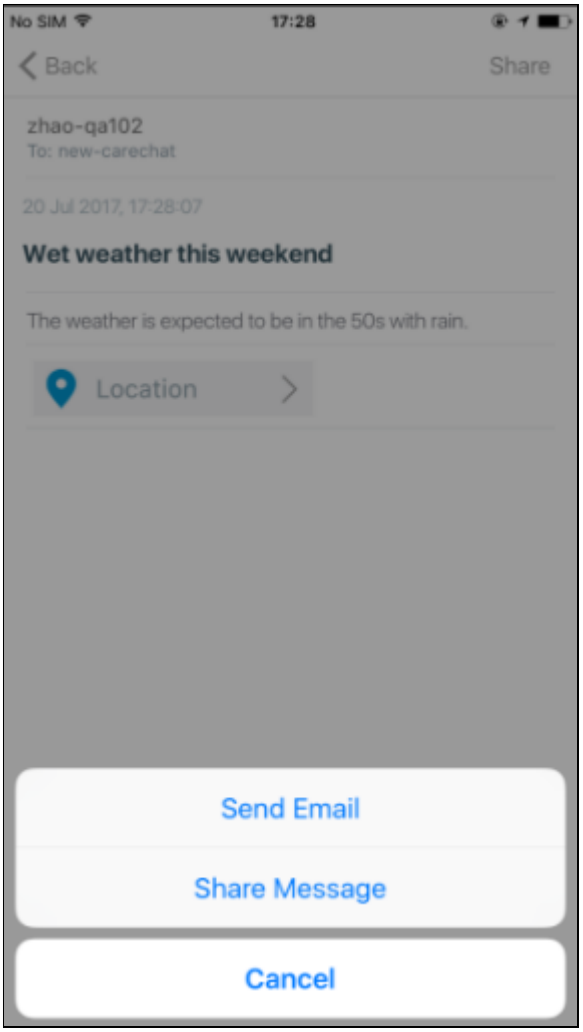


3. Tap **Manage My Profile**. The screens of your profile are displayed.
4. As needed, tap **Edit** for the section you want to modify.

5. Click **Save**.
6. Repeat Steps 4 and 5 as needed.
7. Click **Back** at the upper left-hand corner of the screen when you are finished.

Configuring Other Settings

Depending on the features you will use and the type of device you are using, you might need to configure some settings outside of the Mobile Member app. To share Notifications with your own network, you will need to make sure you have configured the accounts and the device to make them available (by means of email, SMS, and/or Twitter).



Add an Additional Account

Many users will only have one account for receiving and sending messages. Others may have more than one. For example, your employer may use Everbridge to communicate with you. While at home, your city or town may use Everbridge for public Notifications. You can use Everbridge to manage all of your accounts.

1. Open the menu and tap **Enroll** or **Profile**.
2. Follow the on-screen instructions.
3. Search for your Organization, then tap your Organization name.
4. Tap **Add Accounts**. There are three scenarios for the Organization type:
    - Search a **Public Organization**, tap your Organization name, and the Registration page is displayed. You can either register as a new user, or click **Already signed up? Login** and proceed to Step 5.
    - Search a **Private Organization that has SSO** (Single Sign-On), tap your Organization name, and the SSO Login page is displayed. You can log in as an SSO user, or click “Don’t have SSO” and proceed to Step 5.

- Search a **Private Organization that does not have SSO** (Single Sign-On), tap your Organization, and the Login page is displayed. Proceed to Step 5.

5. Enter the Username and Password for the additional account, and tap **Login**.
6. Configure your settings for this account.
7. Tap **Done**. The new account is added to the Accounts list and you are returned to your messages.

Using Everbridge Mobile App

The Everbridge Mobile App is broken into three tabs, depending on an Organization's purchased packages:

- **Notifications**
- **Incidents** - for more details, refer to the *Incident Administrator Guide*.
- **Events** - for more details, refer to the *Crisis Management User Guide*.

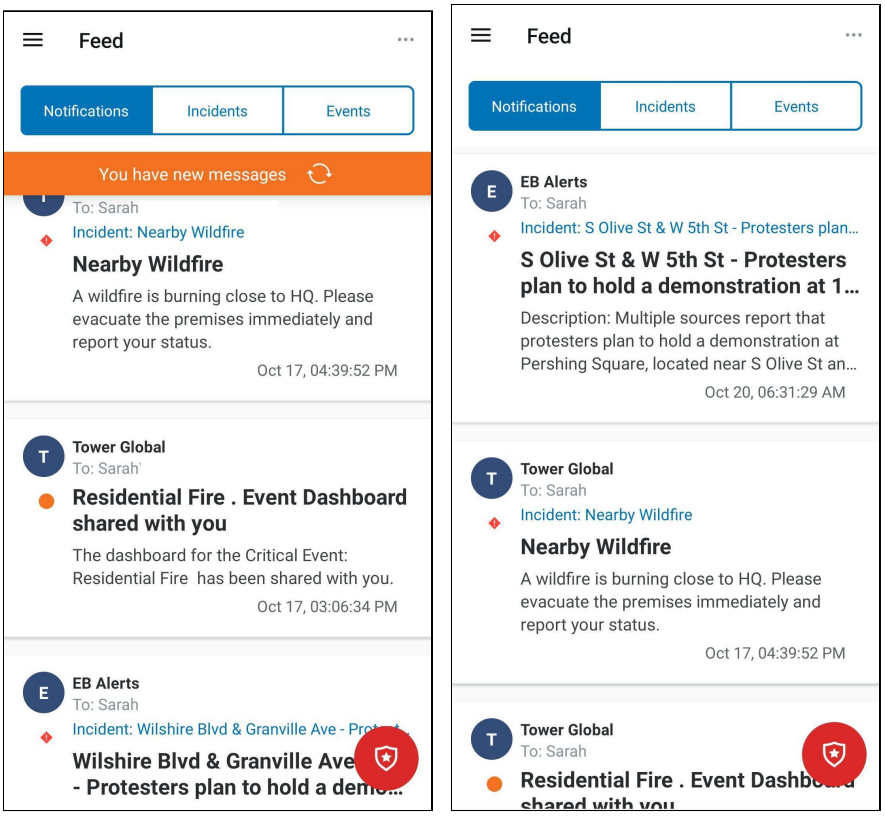
> **NOTE:** Only Organizations that have purchased **Incident Communications** and **Crisis Management** will have access to the **Incidents** and **Events** tab, respectively.

Notifications

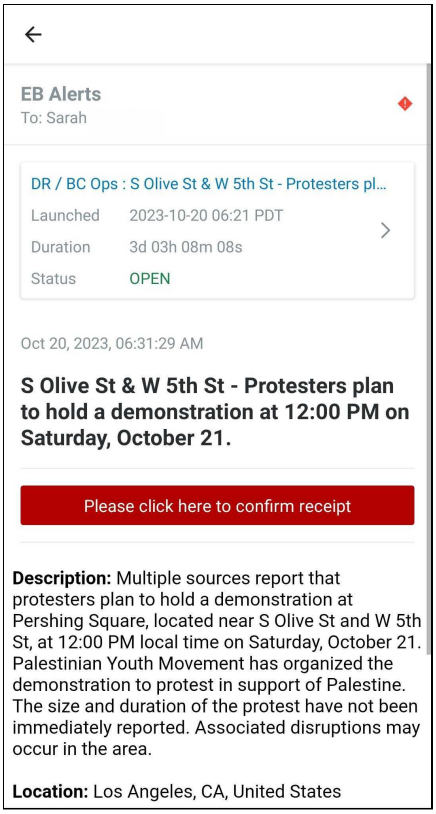
The **Notifications** tab is where users can view any Notifications received from their Organization. Assuming you have already installed and configured the Everbridge Mobile App on your device, a Notification sent to Everbridge can arrive even while it's not running. If you tap on the message, it opens it directly in the **Feed** without having to locate it in the message list.

If you are not using your device when the message arrives, you might not see the Notification. When you are viewing apps, you will see a number on the Everbridge Mobile App icon that displays how many unread messages you have. When you open Everbridge, the list of messages is displayed.

If you are already in the Everbridge Mobile App when a new message arrives, you may need to refresh the screen to see it by tapping the orange banner. Tap the message to open it and read the message from your Organization, or tap **All Messages** (see the following example) from the drop-down arrow to see all the messages.



Very often, your Organization will want to know that you received the message. Tap **Please click here to confirm receipt**. Then, click **OK** to confirm and let your Organization know that the message arrived.

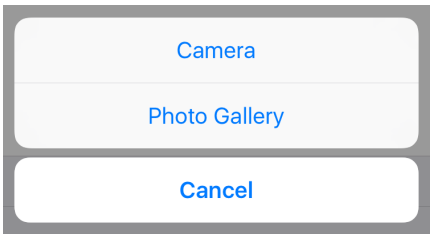


A message might contain a survey or a poll. A polling message offers you a list of responses from which to choose. Tap a response from the list. Confirm your selection. Your response is sent back to your Organization.

When your Organization sends you a message, it might allow you to send a reply, offering more information about the situation.

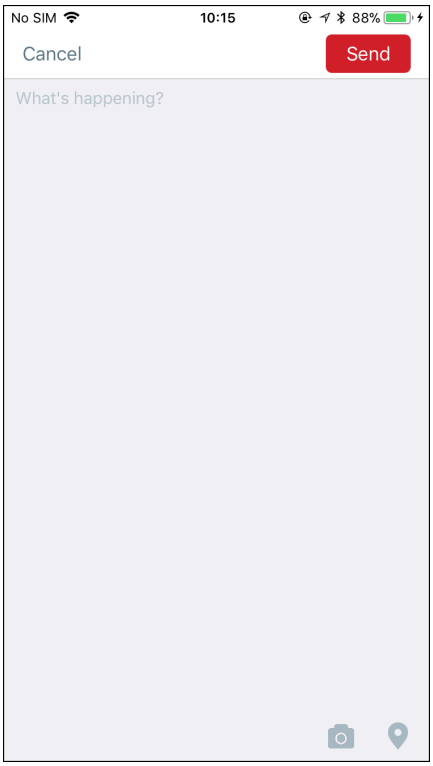
To enter a reply, tap **Send a Response** at the bottom of the screen, type your reply by overwriting “What’s happening?”, then tap **Send**. You can see the replies you have sent on the Message screen.

You can add to the intelligence of your Organization by sending photos from your location. You can send just the photo or you can send it along with the text of a reply. If photos are enabled, you see the Camera icon at the bottom of the Message screen. Tap the icon to send a photo. Depending on your device, you might be able to choose to take a new picture with the camera or select one from saved photos. You can send one attachment at a time; the size of the attachment should not exceed 1 MB.



If sending just the photo, tap **Send**. If you are sending a photo with a reply, also type the reply, then tap **Send**. Your reply shows a thumbnail of the photo.

If a message requests your location, when you send a photo or reply to a message, your location is sent back to the Organization. You will see the Map Location icon in your reply, showing you that your location has been sent.

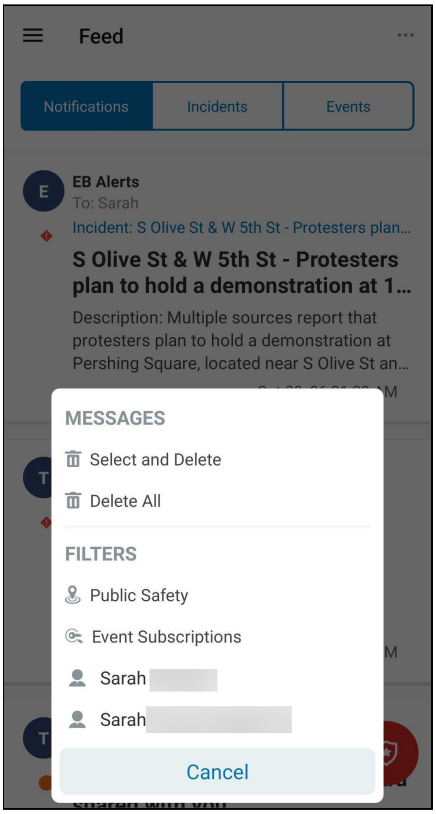


Notifications Feed Menu

Tapping the **Notifications Feed** menu in the top-right corner will reveal the following options:

- **Messages**
  - Select and Delete
  - Delete All
- **Filters**
  - Public Safety
  - Event Subscriptions

- By User Profile



Sharing a Notification

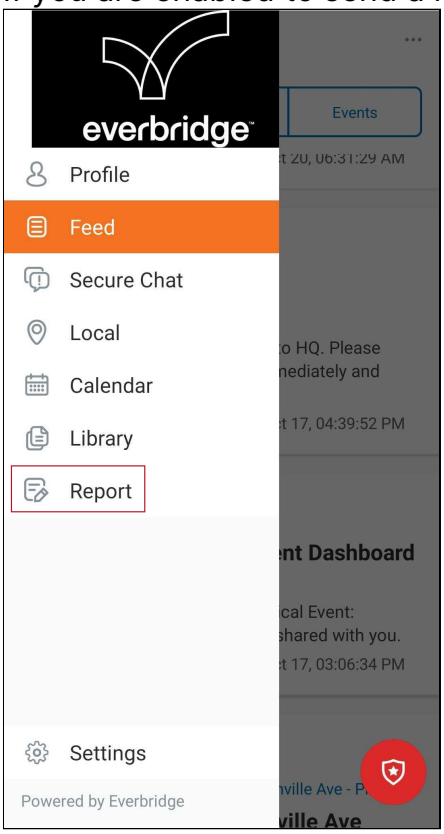
To help notify as many people as possible about an important message, your Organization may allow you to share it with people in your own network. When you send the message, tap **Share**, then choose the method to share the message. You can send it to your contacts by email, SMS, or your Twitter account. Fill in the necessary information, depending on how you are sending the message.

Send a Report

You do not have to wait for a message to arrive to reply with information about an Incident. If your Organization permits it, you can send a report whenever you encounter something the Organization should know about. These messages will appear in the Organization's Unsolicited Messages feed in Universe.

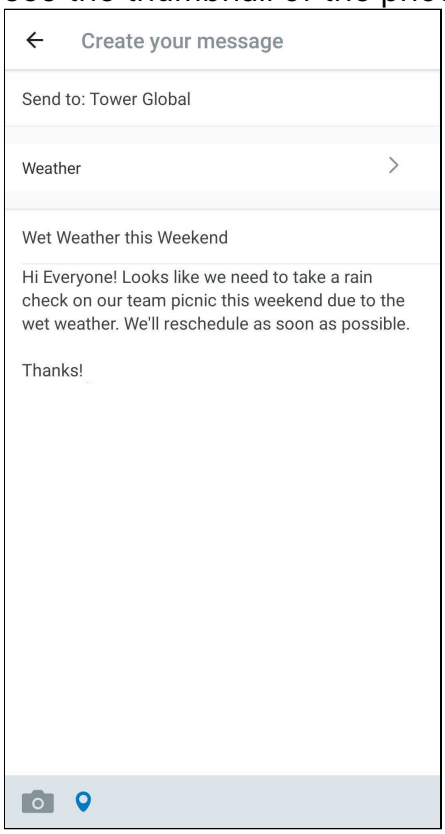
To send a report:

1. If you are enabled to send a message, tap **Report** in the Menu.

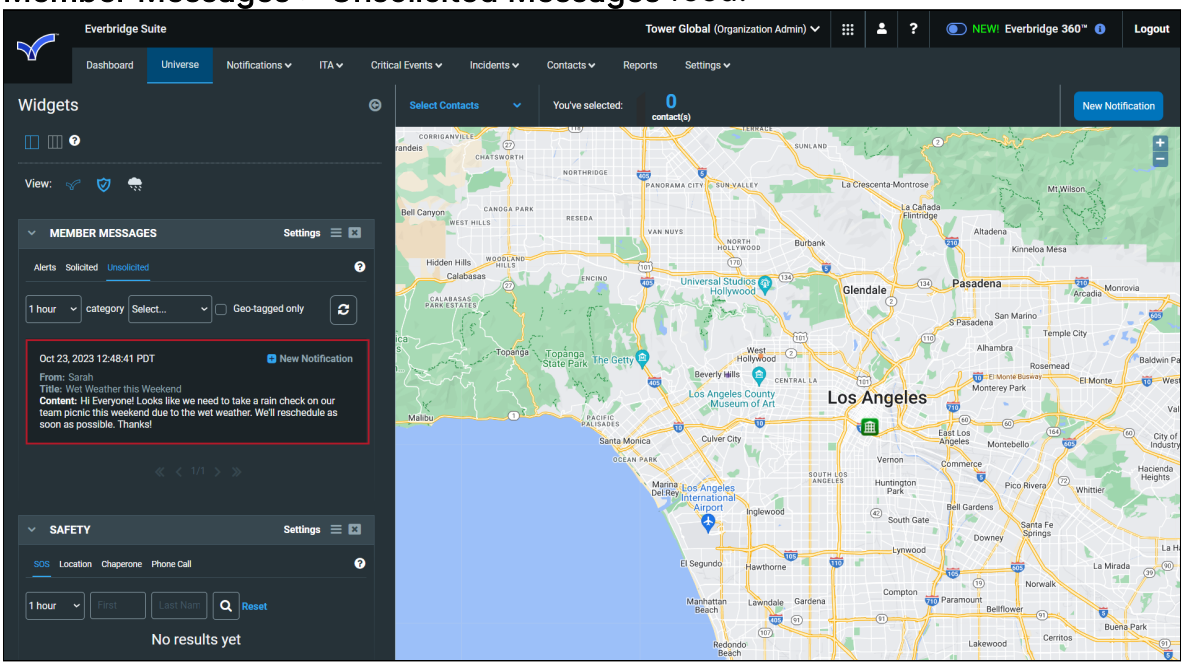


2. Your Organization name will appear at the top next to **Send to**.
3. Complete the following fields:
    - **Category** - Tap the **Category** field to select from the list of categories that have been customized by your Organization.
    - **Title** - Type a title for your message.
    - **Content** - Type the body of the message.
    - **Share Location** - If the icon is blue, then location sharing is enabled. You can tap the icon to disable your location.
        - When your message is sent, you see it on the Message screen. The thumbnail of the photo and the **Share Location** icon (if enabled) are included with the message.
    - **Image** - To send an image with your message, tap the **Camera** icon. Use the device camera or select a photo you have already stored. You will

see the thumbnail of the photo you are sending.



4. Tap **Send**.
5. The message will now appear in the Organization's Universe tab in the **Member Messages** > **Unsolicited Messages** feed.



Solicited Messages

Sending and Confirming Solicited Messages - Basics

When you are sending Notifications to contacts who are using Everbridge, it is basically the same as sending a Notification by any other delivery method. The message is sent and the member confirms the receipt of the message.

Sending and Confirming Solicited Messages - Advanced

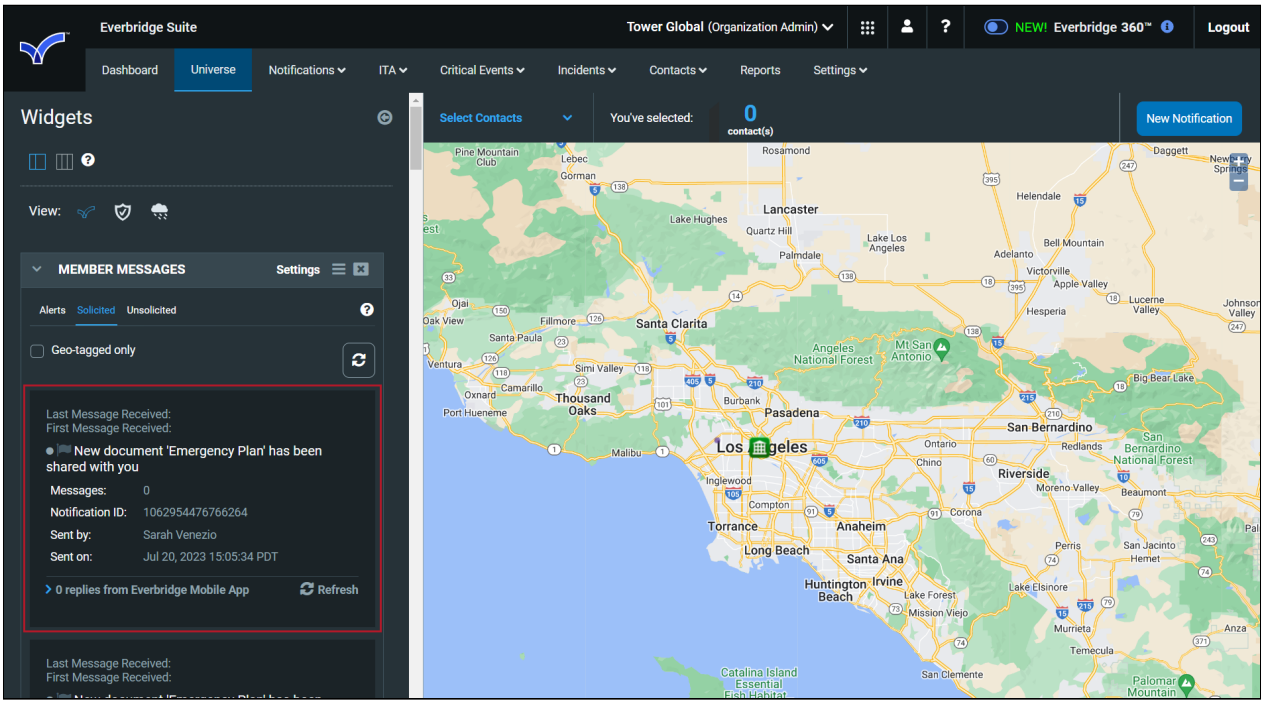
Since Everbridge allows two-way communication with the Organization, there are some additional features. When you are sending the Notification, if you have permission, you can edit the Everbridge Mobile App settings. In Everbridge Mobile App settings, you configure how the contacts can handle this Notification if they receive it in the Everbridge Mobile App. This does not affect how they handle the Notification if they receive it on some other delivery method, like email.

- **Request location** - If selected, and if the contacts allow it, their locations will be sent by the device when they respond to the Notification. You can see a marker of each contact on the map from the Universe tab.
- **Request additional information** - If selected, the contact can send a reply to the Notification. You can view the reply from the Universe tab.
- **Request image** - If selected, the contact can send a photo. You can view the photo from the Universe tab.
- **Enable Sharing Options** - If selected, the contacts can forward this message to their extended network. You will need to consider the message to decide whether to allow it to be forwarded or not. A weather or traffic alert would be a service to the network of your contacts, but you would not want to allow proprietary information about your Organization to be shared. The contact can send via email, SMS, or Twitter. If your Organization does not want to share any messages, you cannot enable sharing on the Notification.

When contacts receive a Notification in Everbridge, they can reply if you have enabled a request for additional information. They can provide more details about the incident. The replies arrive on the Universe tab. Open the Member Messages widget. The Member Messages panel appears.

Since the member replied to a Notification sent by the Organization, the reply is in the Solicited tab. You can change the time frame of received replies to display in increments of hours and day: 1 hour, 3 hours, 6 hours, 12 hours, or 1 through 7 days.

Click **Refresh** (next to the **Viewing** field) to see new replies while you are looking at this panel. If the contacts are allowing their locations to be shared, click the **Show/Hide on Map** icon to show from where they are replying. This icon shows all contacts who have replied. The Show/Hide on Map icon in a reply shows only the contact for that reply. The marker on the map shows the location of the contacts when they replied. Hover the mouse over the marker to display the reply sent by that contact.

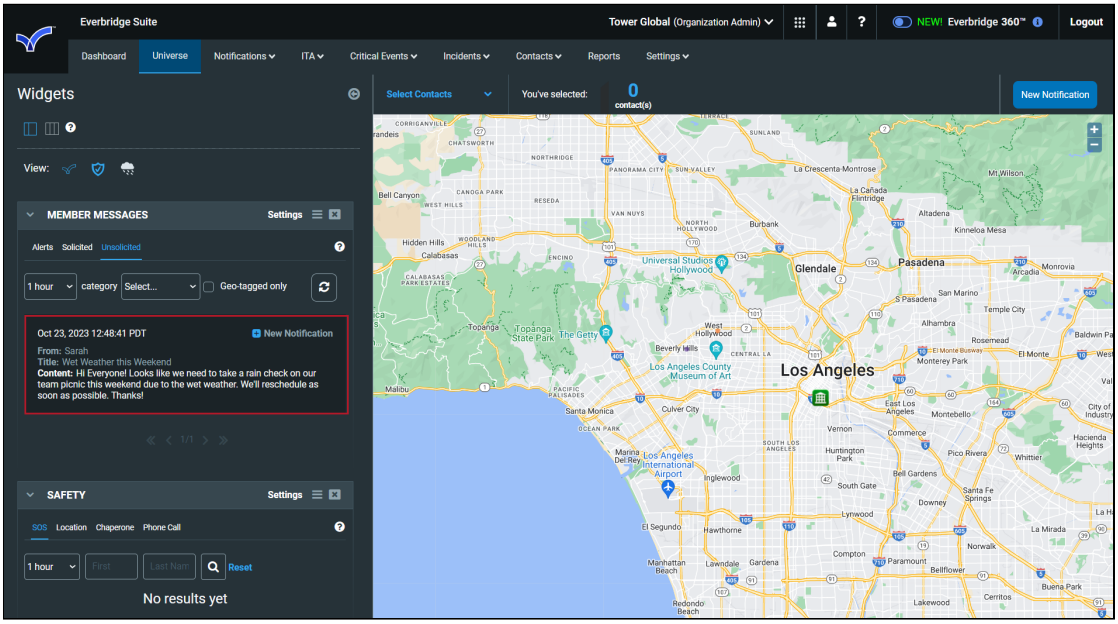


If there is an image in the reply, click the thumbnail to expand the image.

After you see the reply, you might want to send another message to that contact. Click the **Notification** icon (left of the **Show/Hide on Map** icon) in the reply. A new Notification panel appears. (There is one individual selected to receive this Notification - the person who sent the reply.) You can add more recipients if you want them to see the message. Give the message a title and type your body text. Click **Send** to start the Notification. The return message is active and is sent.

Unsolicited Messages

Contacts may be permitted to send unsolicited messages using Everbridge if they need to contact the Organization. Unsolicited messages are different than replies because no Notification has been sent. For example, an employee on his way home might want to let others know about the heat warning. The Organization could then notify other employees to avoid traveling during the hottest time of the day.



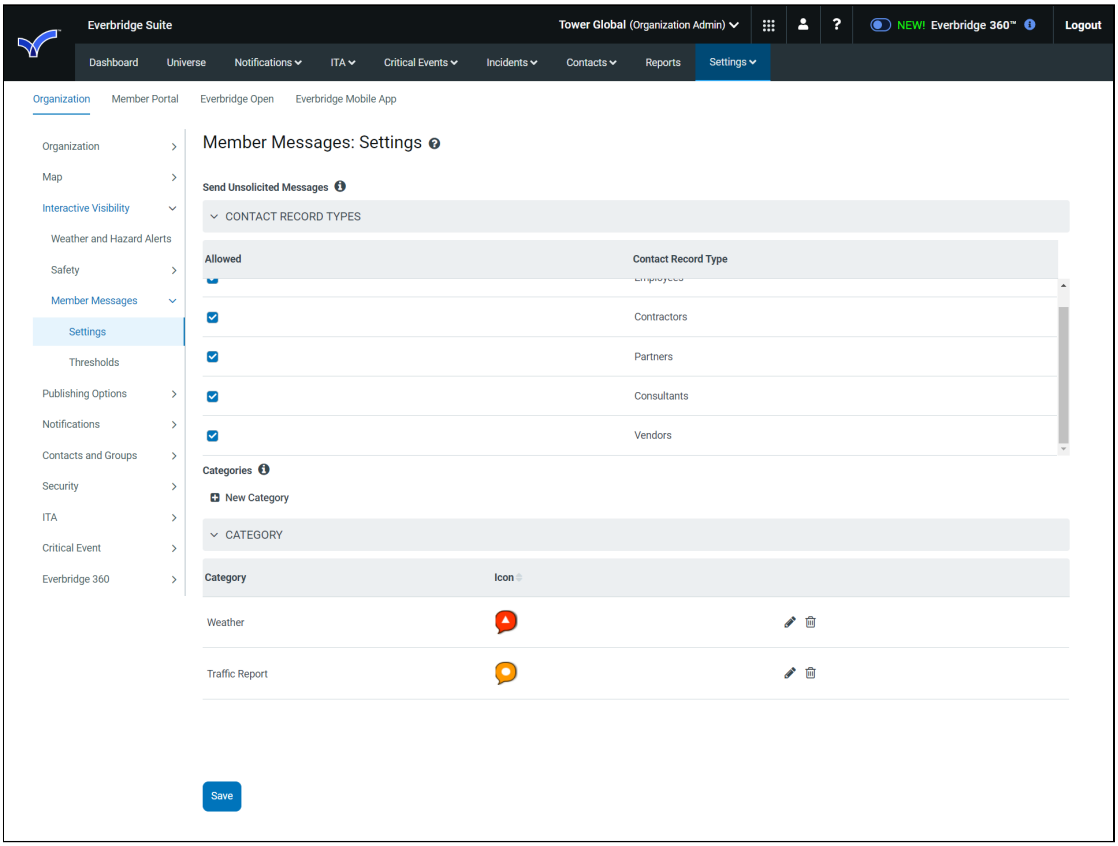
View unsolicited messages from the **Unsolicited** tab of the **Member Messages** widget from the Universe tab. The controls for viewing unsolicited messages are the same as those for viewing replies. There is an additional **Category** drop-down list that allows you to filter the messages by category. By default, you will see all unsolicited messages sent during the selected time frame.

When the contact created the message, they selected a category from the list configured for your Organization. (Example categories: Security Concern, Emergency, General Inquiry, Request.)

Choose a category from the drop-down list and you will only see messages tagged with that category.

Configuring Member Messages Settings

You can define the Member Messages settings and configure custom categories on which the application users can report using the application. The main approach is to reach individuals.



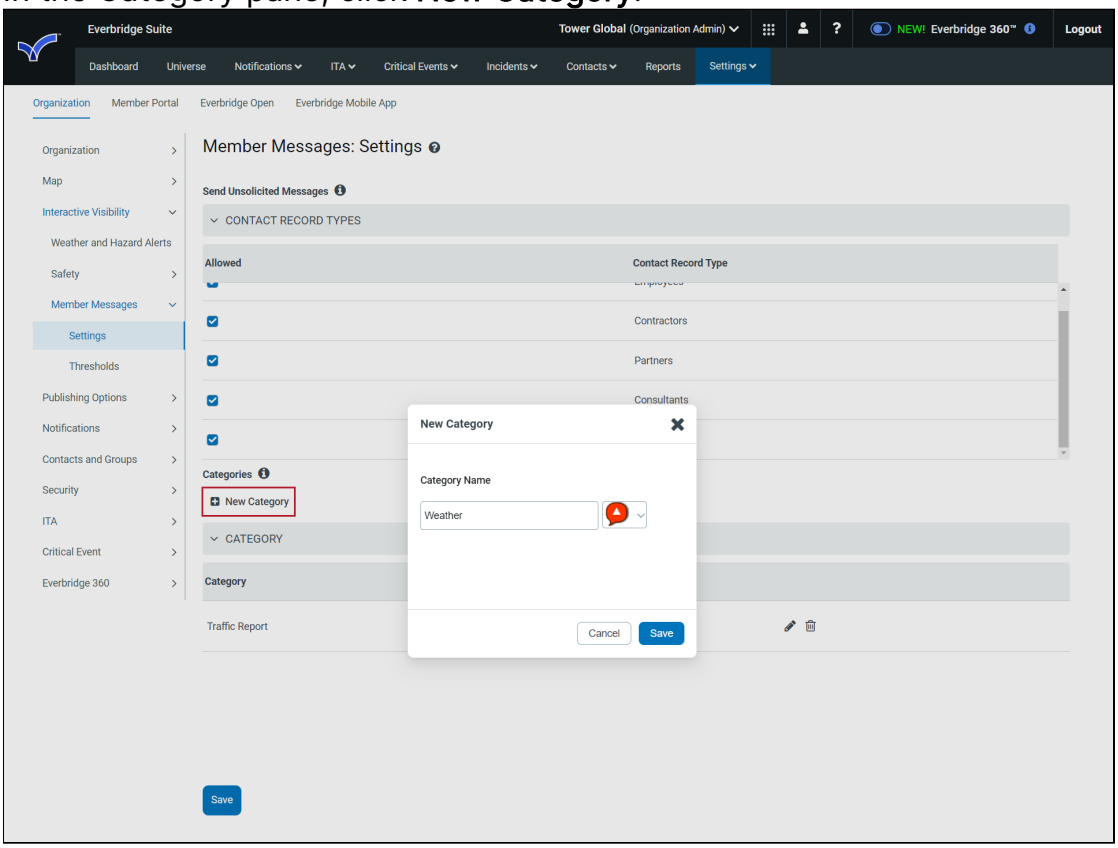
The Everbridge Mobile application must be installed, but does not have to be running. A push Notification is sent to the application. The contact (member) confirms receipt by means of Polling or Conference bridge. Contacts can respond with their locations and images they capture on-site.

To configure Member messages:

1. Select the **Allowed** checkboxes in the **Contact Record Types** pane as desired. Contacts in the selected record types will be able to send a message to you at any time.

   When selected, the end-user can send unsolicited messages back to the Everbridge system. This allows users to report information to the client based on the defined Categories.

2. In the Category pane, click **New Category**.



3. In the **Category Name** field, type a name, select the icon to display on the map, then click **Save** in the New Category dialog. Example category names: "Violence Report," "Civil Unrest Report," "Traffic Incident Report," etc.
4. Click **Save**.

To edit an existing Custom Category:

1. From the Member Messages page, click the **Pencil** icon in the row of the category to be changed.
2. Follow the steps in the procedure To configure Member messages.
3. Optionally, rename the category.
4. Click **Save**.

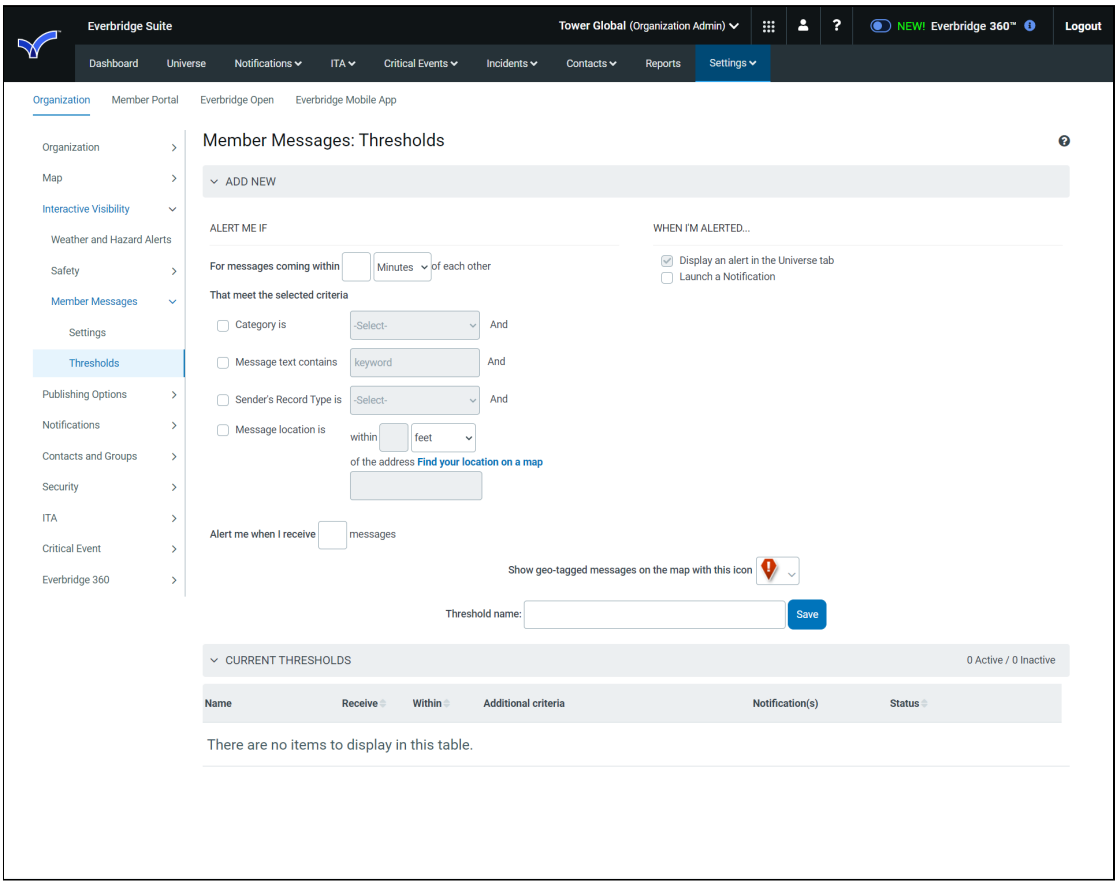
To delete a Custom Category:

1. Click the **Trash Bin** in the row of the category to be deleted.
2. Click **Yes** to confirm that you want to delete the category.

Member Messages: Thresholds

To automatically receive alerts from unsolicited messages, configure your Member Messages: Thresholds. When you select Settings > Interactive Visibility > Member Messages > Thresholds, the Member Messages: Thresholds page appears. It

displays any Current Thresholds and their on/off status. You can have up to five thresholds. You can also add a new threshold.



For each threshold, you can see the name and criteria that will trigger an alert. If the alert will launch a Notification, the name of the template is shown. The Status shows whether the threshold is currently active (ON). If it is inactive (OFF), it is still configured but is not currently monitoring information. The number of Active and Inactive thresholds is displayed at the right-hand corner of the Current Thresholds pane. You can activate/inactivate a threshold by clicking the ON/OFF toggle.

Collapse the Current Thresholds list by clicking the **Down** arrow at the top left-hand corner of the Current Thresholds pane. Expand the Current Thresholds list by clicking the **Right** arrow at the top left-hand corner of the pane. You can hide the entire panel by clicking the down arrow next to the Current Thresholds header. Click it again to open the panel.

Configuring Member Messages: Thresholds

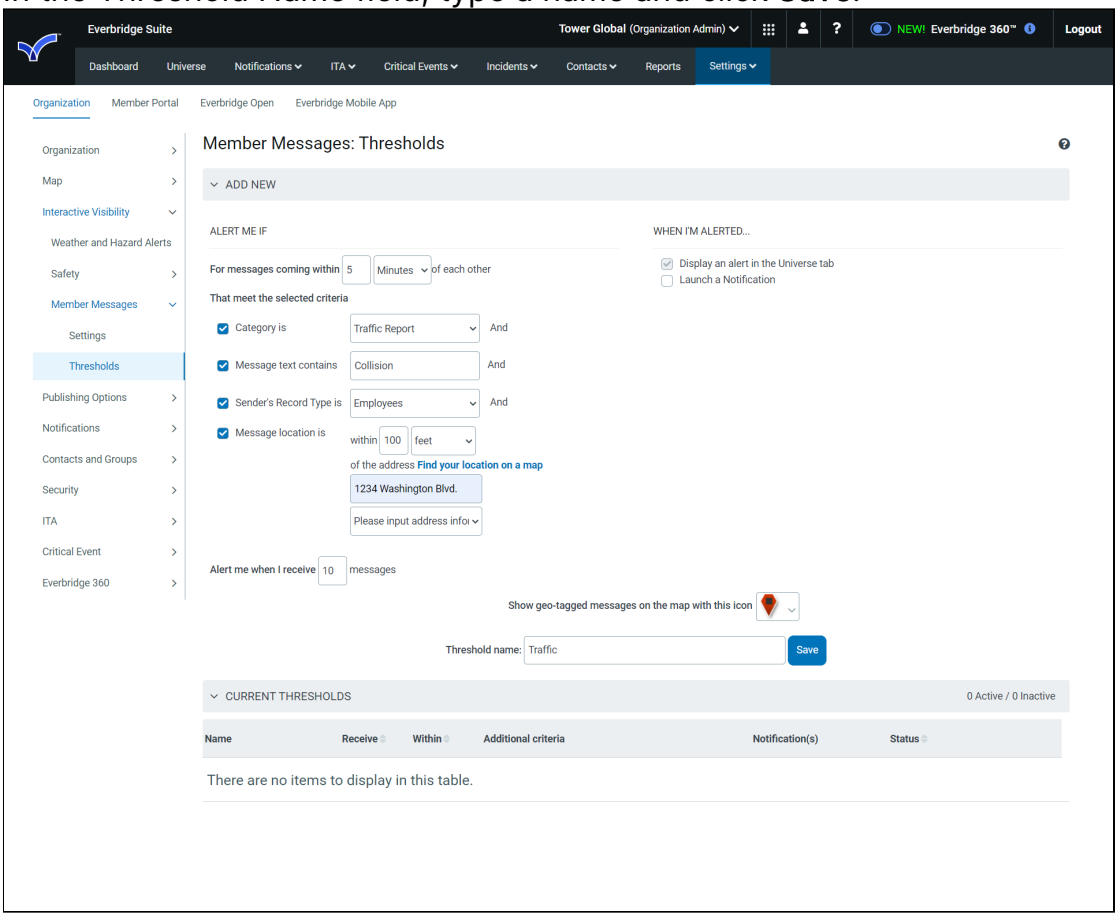
1. Type a number and select Minutes or Hours for the field: For messages coming within NN minutes/hours of each other.
2. Optionally, select the desired check box or check boxes and select from the corresponding drop-down lists:

- **Category is** - Select from the list of categories.
- **Message text contains** - Type the keyword.
- **Sender's Record Type is** - Select from the list of record types.
- **Message location is** - Type a number, select Feet, Meters, Kilometers, or Miles from the drop-down list, and type the address.

3. On the right-hand pane, select whether or not to trigger a Notification.
   - By default, the check box: Display an alert in the Universe tab is selected.
   - Optionally, select the check box to Launch a Notification.

     If you select this check box, you can select a Notification Template to add to the Threshold.

     - Search for the desired Notification Template.
     - Click the blue **+** sign. (To remove a Notification Template from the Threshold, click the Trash Bin to the left of the desired Notification Template name.)
4. Type the number of alerts that must occur, related to your criteria, prior to displaying an alert regarding your Member Messages threshold.
5. In the Threshold Name field, type a name and click **Save**.



Technical Settings

The Everbridge Mobile App uses the standard push notification services based on the operating system of the device. That is, iOS devices use **APNS** (Apple Push Notification Service) and Android-powered devices use **Android Firebase**.

iOS Ports

The APNS servers use load balancing. Your devices will not always connect to the same Public IP (Internet Protocol) address for notifications. The entire 17.0.0.0/8 address block is assigned to Apple, so it is best to allow this range in your firewall settings.

- TCP Port 5223 is used by devices to communicate to the APNS servers.
- TCP Pot 2195 is used to send notifications to the APNS.
- TCP Port 2196 is used by the APNS feedback service.
- TCP Port 443 is used as a fallback on Wi-Fi only, when devices are unable to communicate to APNS on Port 5223.

Android Ports

The device accesses the GCM servers on Ports 5228-5230. GCM does not provide specific IP addresses. It changes IP addresses frequently.

Mobile Device Management for Everbridge Mobile App

Mobile Device Management (MDM) allows mobile devices to be configured and controlled from a central location. Typically, it is used by enterprise-level Organizations to impose minimum security standards, provide Organization-recommended apps, assist users in configuration, and protect company data on both Organization-provided and BYOD devices.

The Everbridge Mobile App (hereafter, "EMA") includes support for configuration via MDM systems that support the **AppConfig** standard. This includes some custom configuration ability for EMA itself as well as the functionality provided natively by the MDM systems.

Each MDM system works differently, and details can be found in the documentation of your MDM system. But this document provides some examples of MDM capabilities, as implemented by a sample MDM system (**MobileIron Cloud**), and lists the configuration settings currently available for EMA.

> **NOTE:** MDM support is an ongoing effort, and additional configuration settings will likely become available over time.

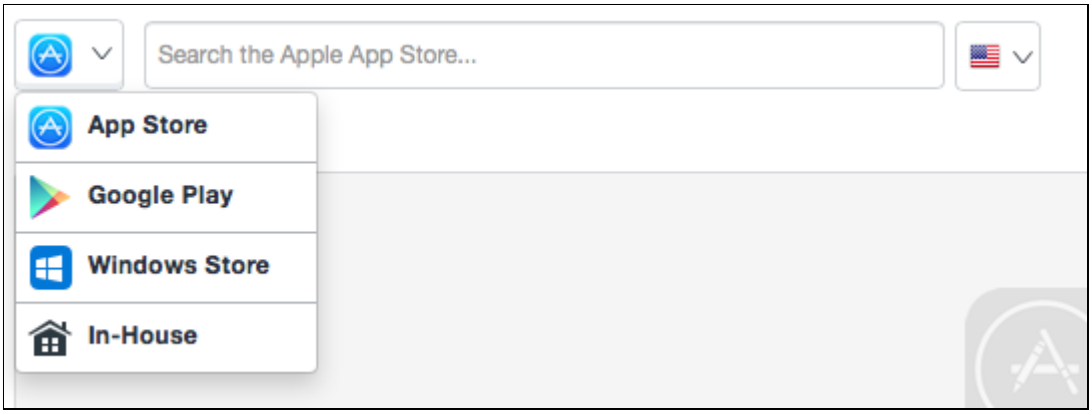
Internal App Store Distribution

MDM providers offer an Internal App Store mechanism which offers a selection of Organization-curated apps that are either automatically or optionally installed on the users's device. How this is done varies between MDM providers.

On MobileIron Cloud, you access these configurations by:

1. Select the **Apps** tab along the **MobileIron Cloud** top navigation bar.
2. If necessary, select the **App Catalog** tab in the sub-navigation bar.
3. Click the **+ Add** button

At this point, you can choose from a variety of methods to load your application, using the pull-down next to the **Search** box.



For EMA, select the **App Store** (for the iOS version) or **Google Play** (for the Android version), and type "Everbridge" into the search box. Once it's located, select it, and several screens of options will appear. On the final page (**Configure** on the left, **App Configurations** on the top), you can specify things like:

- Whether or not to force the app onto the user's device or let them choose it.
- Whether to convert unmanaged versions of the app to managed ones.
- Whether or not data from the app can be backed up to iTunes or iCloud.
- Application-specific configurations (see **Set Custom EMA configuration Settings** below)
- Per-App VPN (protected networking).

AppConnect is a proprietary MobileIron system, which extends certain apps with additional MobileIron-specific functionality. EMA is not an AppConnect-managed app, so the following two AppConnect features will not function:

- AppConnect custom configurations will not apply. Use the **iOS Managed App Configuration** option instead.
- AppTunnel. Use the **Per-App VPN** instead.

Once you have completed the steps, click **Done**, and the app will be made available to the devices of the users you specified.

> **NOTE:** This can take some time; it will not happen at all until networking is available on the device, and application downloads can take considerable time.

Remotely Wipe or Un-manage a Device

Removing a Single App

To remove a single app (such as EMA) from a device, set its distribution to **No One**, or remove the device(s) from the current distribution group.

Return a Device to an Un-managed State/Remove all Managed Apps

You can also eliminate all management from a device, which will remove all managed applications and data. As usual, the method for this varies between MDM providers, as does the name. Some providers will call this "Unmanage," others will call it "Retire."

On MobileIron Cloud, to access these configurations:

1. Select the **Devices** tab on the **MobileIron Cloud** top navigation bar.
2. If necessary, select the **Devices** tab in the sub-navigation bar as well.
3. Check the devices you want to unmanage.
4. From the **Actions** dropdown, select **Retire**.

You will be asked to confirm your actions. After retirement, the device will operate as an unmanaged device and will no longer have access to the Organization's settings, security, or policies. Retiring a device can take a few minutes, and the device may or may not reboot to complete the retirement.

Wipe a Device Completely

Finally, you can "wipe" a device, deleting all applications and data on the device (including the user's own, unmanaged apps and data), and returning the device to its factory state.

> **NOTE:** This is typically only done to protect data on a lost or stolen device, for Organization-owned devices that will be re-purposed to a new employee, or when a device gets into an "unusable" state for whatever reasons.

To access these configurations On MobileIron Cloud:

1. Select the **Devices** tab along the **MobileIron Cloud** top navigation bar.
2. If necessary, select the **Devices** tab in the sub-navigation bar as well.
3. Check the devices you wish to wipe.
4. From the **Actions** dropdown, select **Wipe**.

You will be asked to confirm your actions since this is completely destructive to the data and apps on the device. Once confirmed, the device will be erased, usually within a minute if it has network coverage. The device does not need to be unlocked for this to happen.

After wiping, the device will be restored to its out-of-the-box state. For devices that are still functional (that is, they have not been marked as stolen with their network), they may then be reconfigured as with any new device.

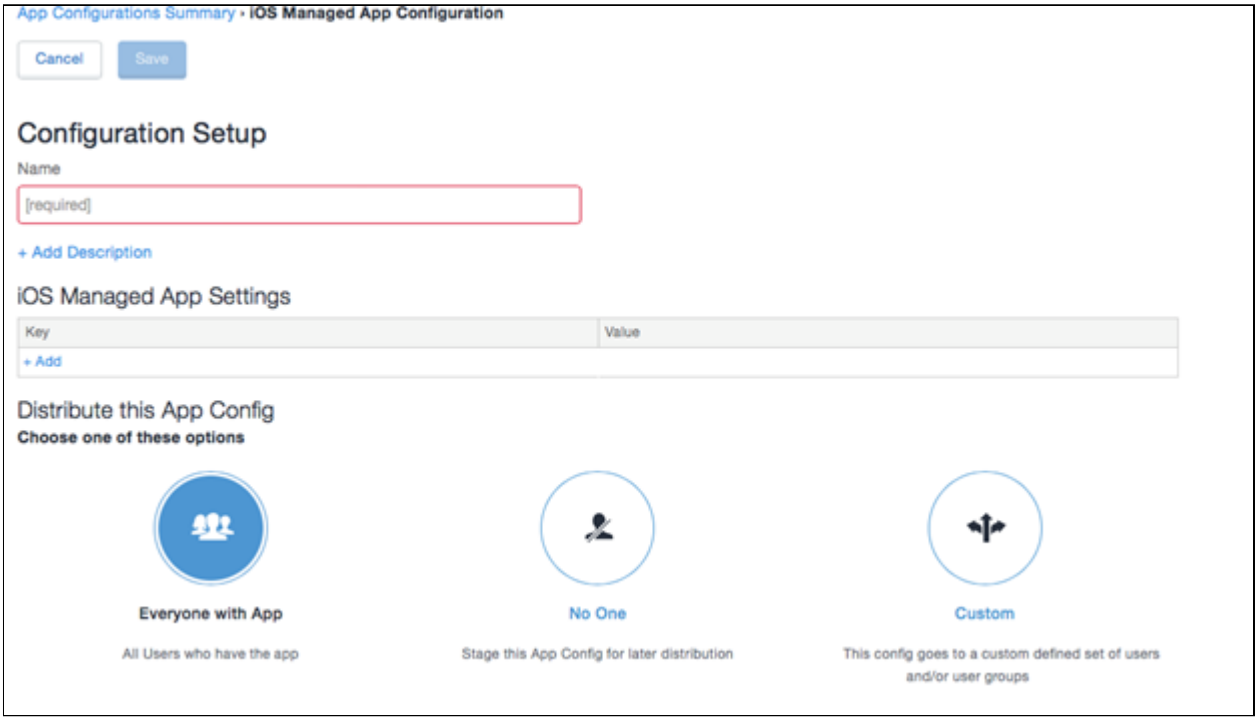
Set Custom EMA Configuration Settings

EMA supports sending application-specific configuration settings via the **AppConfig** standard. How this is done varies between MDM providers; it will typically be located in a "Configurations" tab or button associated with the specific app.

To access these configurations on MobileIron Cloud:

1. Select the **Apps** tab along the MobileIron Cloud top navigation bar.
2. If necessary, select the **App Catalog** tab in the sub-navigation bar.
3. Click the "Everbridge" name (it will list as a hyperlink) in the **App Catalog** list.
4. From the Everbridge application summary page, select the **App Configurations** tab.
5. Select **iOS Managed App Configuration** (*not* AppConnect Custom Configuration)

From this summary page, you can create, modify, delete, and activate as many sets of configurations as you like. To create a new one, click the **Add+** button.



Name the configuration whatever you like. On the bottom, you can choose which of your users will have the configuration applied; you can select **No One** if you

want to try out configuration building without affecting your users (then apply it later if you desire).

The core of this screen is the configurations themselves. These are combinations of "keys" (the name for a specific setting) and "values" (what you want to set that setting to). You can specify as many of these as you like, but only settings whose "key" and "value" are supported by the application will take effect. Keys, in particular, must exactly match a setting name, including punctuation and case. That is, "EMA_allowcopy" is not the same as "EMA_AllowCopy". The specific key/value pairs supported by an application will be documented by the application provider; the supported pairs for EMA are listed below.

Everbridge Mobile App (EMA) Configuration Settings

The configuration settings currently provided for EMA are listed below. Note that this list will increase over time, so check for newer versions of this text.

All EMA settings begin with EMA_ ("EMA" and an underscore), and must be specified exactly, including upper/lowercase. Any setting not included in a configuration will have a specified default (unless provided by another configuration sent to the same device).

The available configurations are listed starting on the next page. Once a configuration set is chosen and sent from your MDM provider, the configuration should appear on devices in a very short period of time (no more than a few minutes), assuming the devices have network connectivity. Devices in areas without wireless access--or with that access disabled--will be configured when they next return to a wireless network.

Most configurations will take effect immediately upon the device receiving them; the application does not need to be killed or relaunched.

Allow Copy

If set to **false**, the copy (and cut) command will be disabled in several locations in the application. Currently, this disallows the copying of Notification message content; it will be expanded to disable copying in more locations over the next few versions of EMA. If you have a specific request for a control that should honor this setting (i.e., that you want to prevent copying), contact your Everbridge support or sales representative.

Name	Values	Default

EMA_AllowCopy	"true" or "false"	True

Setting this value to **True** will not enable additional copy/paste operations. For privacy reasons, many parts of EMA do not allow copy and/or paste, regardless of the value of this configuration.

Allow Paste

This setting is used only on iOS. On Android, use your MDM provider's built-in policies to disable copy and paste globally.

Name	Values	Default
EMA_AllowPaste	"true" or "false"	True

If set to **false**, the paste command will be disabled in many locations in the application; it will be expanded to disable copying in more locations over the next few versions of EMA. If you have a specific request for a control that should honor this setting, contact your Everbridge support or sales representative.

> **NOTE:** Note that setting this value to true will not enable additional copy/paste operations. For privacy reasons, many parts of EMA do not allow copy and/or paste, regardless of the value of this configuration.

Allow Notification Attachments

This setting is used only on iOS. On Android, use your MDM provider's built-in policies to disable copy and paste globally.

Name	Values	Default
EMA_AllowNotification Attachments	"true" or "false"	True

If set to false, Notification attachments will not be available to the user in the messages list.

Allow Org Search String

If provided, the Org search term will be pre-populated with the specified value.

Name	Values	Default
EMA_Org_Search_String	Any string	-none-

About Geo-Tagging

There are many factors that may affect the accuracy of the retrieved locations, including:

1. A location (latitude/longitude) displays on different maps where the result may not be the same. This happens even between Google Web Maps and Google Mobile apps.
2. iOS Location Service.

Global navigation systems, like GPS (http://www.gps.gov/systems/gps/performance/accuracy/), provide the ability to pinpoint a device by using known coordinates of satellites as opposed to cell towers. *Trilateration* is used to find the intersecting point of spheres to determine the location of a GPS-enabled mobile device. GPS hardware is energy-demanding, and can quickly drain the battery of a mobile device. Apple uses the more efficient Assisted Global Positioning (AGPS) process for locating and linking to satellites. With AGPS, satellite positioning is retrieved from a cellular or Wi-Fi connection, reducing the amount of time it takes to discover a satellite.

Trilateration

Triangulation and *trilateration* are two mathematical processes for determining the location of a point. *Triangulation* uses a process of measuring angles from known locations, such as cell towers, to calculate the current position.

Trilateration determines the position of a device by calculating the intersection of circles or spheres representing the distance of a device from known locations. The accuracy of these approaches is improved as more fixed locations are used in the calculations.

Signal strength is used to predict the distance of a device from various cell towers. With the cell tower's fixed location known, a distance radius is established. Without the intersection of circles from a second or third cell tower position, we can only determine that the device is located somewhere on the circumference of the distance circle. An omnidirectional antenna on the cell tower can narrow down the position of a mobile device, but not close enough to satisfy the requirements of today's iOS apps.

Crowd-Sourcing

Apple leverages crowd-sourced information to:

1. Fine-tune the accuracy of location-based services on cellular and GPS-enabled devices.
2. Enable location-based services on non-cellular or Wi-Fi-only devices.

Crowd-sourced Wi-Fi is by far the most innovative approach for determining the location of a mobile device. Apple uses a database of Wi-Fi hot spots and cell tower locations (submitted anonymously by any number of iOS mobile devices) to help determine the coordinates of a single mobile device. Cellular, AGPS, and crowd-sourced Wi-Fi information are used to feed accurate data to iOS location-based services.

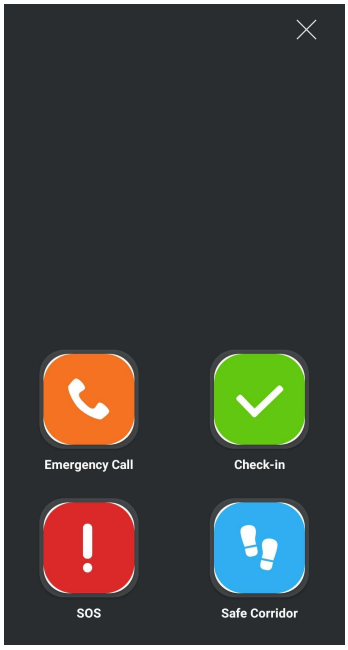
Using Safety Connection in Everbridge Mobile App

When your Organization has enabled the **SOS** feature for your safety, you are prompted to configure your account. After your **Safety Settings** are configured, you can use Safety Connection in Everbridge.

For more on Safety Connection functionality and configuration requirements, see the *Safety Connection User Guide*.

To use Safety Connection features within the Everbridge Mobile App:

1. Open the app.
2. Tap the **Safety** icon at the bottom of the page. The following menu will appear:



3. Tap the desired feature and refer to its corresponding sections for more details:
   - **Emergency Call**
   - **Check-In**
   - **SOS**
   - **Safe Corridor**

Emergency Call

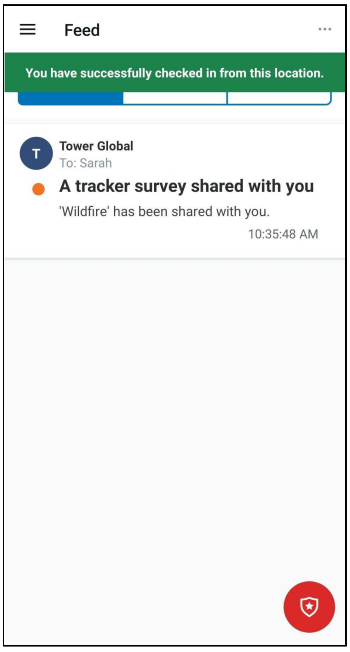
To place an Emergency Call:

1. Tap the **Emergency Call** button.
2. If prompted by your device, confirm that you'd like to complete the action via **Phone**.
3. The call is placed to the phone number configured as the **Safety Number** for your current country in **Organization Settings**.

Check-In

Tap **Check-In** to let your team know your location. If you are traveling, leave a building without badging out, and do not have Auto Check-In enabled, you are still listed as in the building and will receive any building Notifications.

A green banner will flash across the top of the page to confirm that the check-in was successful.

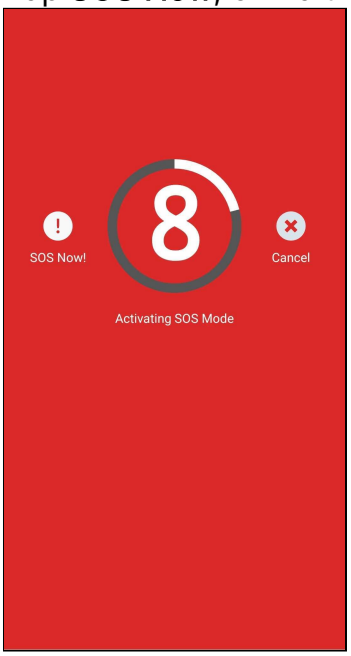


SOS

When an SOS is triggered, Everbridge obtains the location of the device and starts a 2-minute video stream. However, if the app is closed or stopped, video will not be recorded.

To issue an SOS from your device:

1. Tap the **SOS** button. If selected by mistake, tap **Cancel** to end the SOS
2. Tap **SOS Now**, or wait 10 seconds and SOS mode is triggered. activation.



When triggered, the SOS Notification is sent, which is a pre-configured message with your name and location to inform your team that you are in danger.

> **NOTE:** When SOS mode is triggered, you cannot clear the SOS code in Safety Settings.

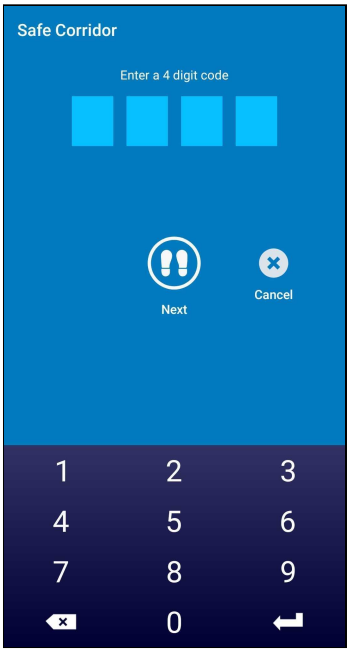
- For the SOS to be sent from a device to the EB server, there is no minimum bandwidth requirement; this is a small request and will go through as long as the user is able to connect to the internet.
- The app should also be able to capture and send the location of the device during an SOS with a minimum of 2G network.
- However, video streaming and capturing during an SOS will require a high-bandwidth network connection such as 4G or LTE.

Safe Corridor

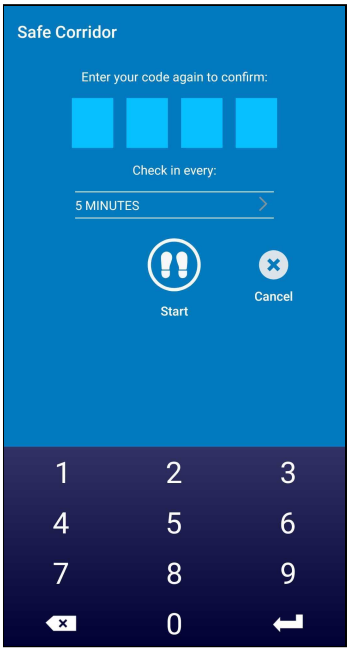
To start a Safe Corridor:

1. Tap **the Safe Corridor** button.
2. If not already enabled, you'll be prompted to enable "Always Allow" location access. Tap **Continue**.

3. Once the correct location access has been permitted, the **Safe Corridor** page appears. Enter your **4-digit Safe Corridor check-in code** so your team knows you are safe. The Safe Corridor check-in code cannot be the same as the Duress code. When you enter three consecutive incorrect Safe Corridor entries, the SOS is audibly and visibly triggered. A Duress code triggers a non-visible SOS.

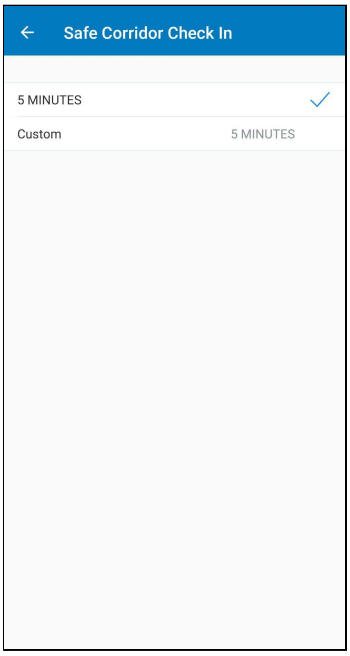


4. Tap **Next**. You'll be prompted to confirm your code again.



5. The default time between check-ins is 5 minutes. If desired, you can customize the time between check-ins by tapping the **Check in every...** field. Then, tap **Custom** to set the desired interval. The minimum length is 1 minute,

while the maximum is 60.



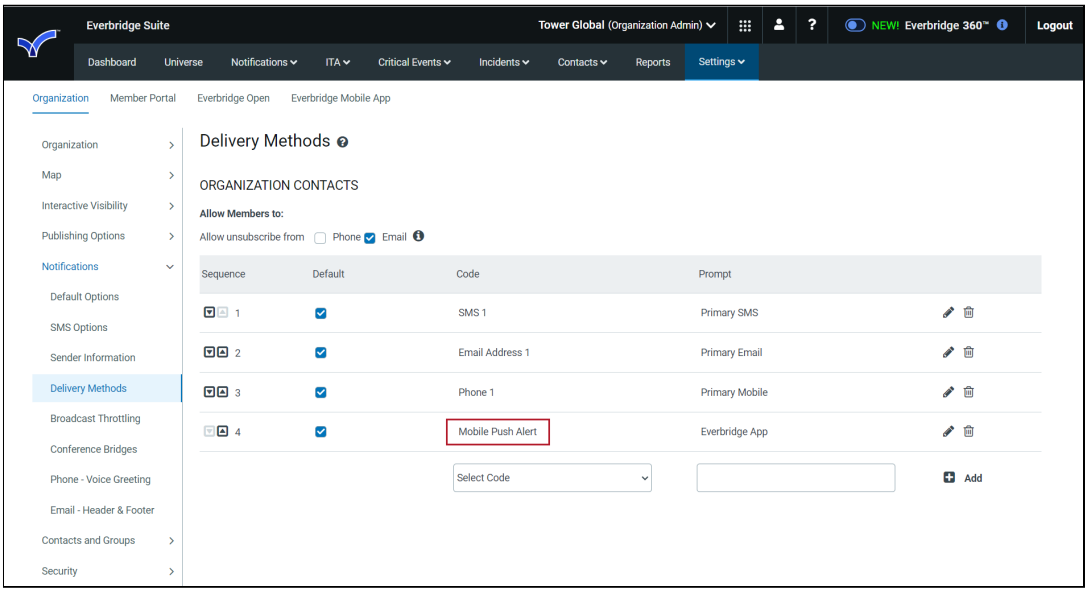
6. Once the code has been confirmed and the check-in intervals specified, tap **Start** to trigger the Safe Corridor.

> **NOTE:** The app makes an audible chime 45 seconds before the interval is met, whether the Safe Corridor interval is 1 minute or more. The chime notifies the users that they have 45 seconds to enter their code before the interval expires and an SOS is triggered.

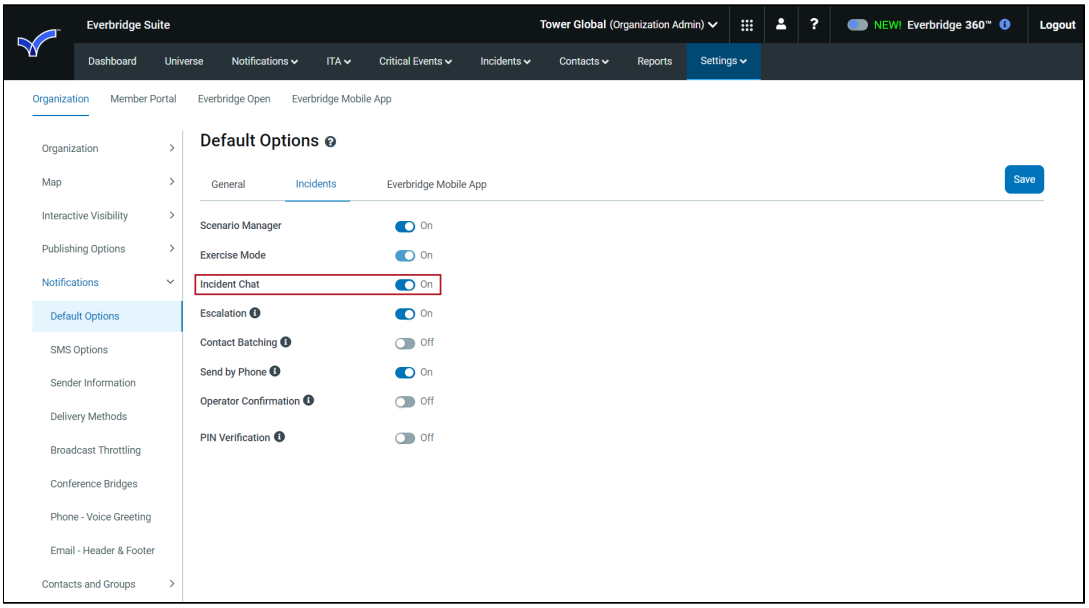
Setting Up and Using Incident Chat

Set up your Organization by performing the following steps:

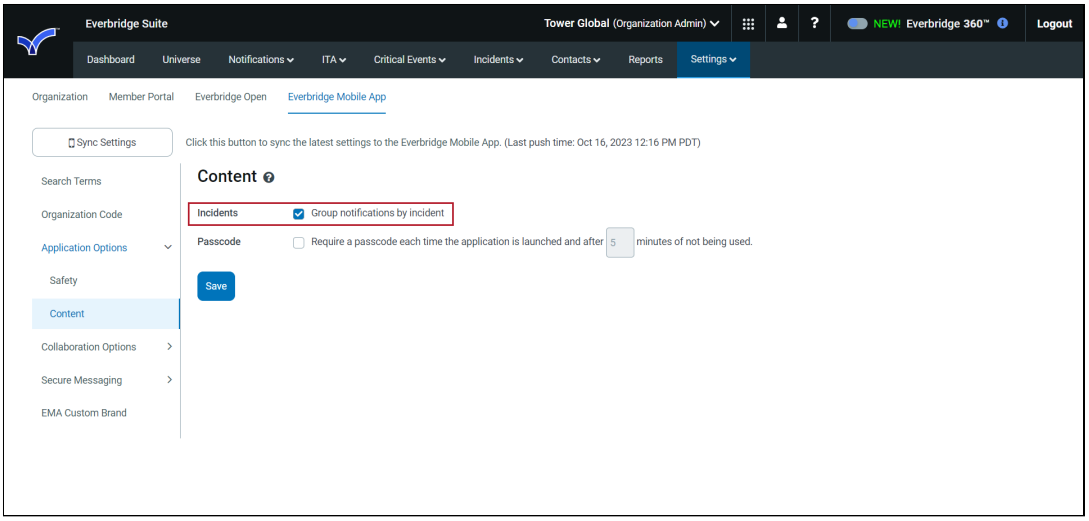
1. From the **Organization Settings** > **Notifications** > **Delivery Methods**, add **Mobile Push Alert** as a delivery method.



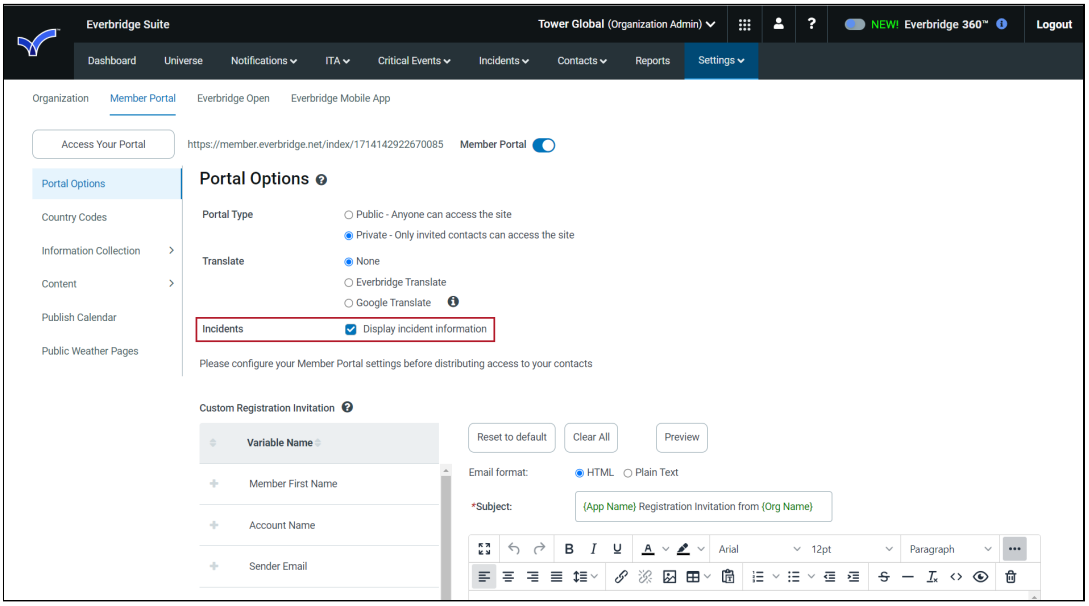
2. From **Settings** > **Organization** > **Notifications** > **Default Options** > **Incidents** sub-tab, enable **Incident Chat.**



3. From **Settings** > **Everbridge Mobile App** > **Application Options** > **Content**, select **Group Notifications by Incident.**



4. From **Settings** > **Member Portal** > **Portal Options**, select **Display Incident Information**.

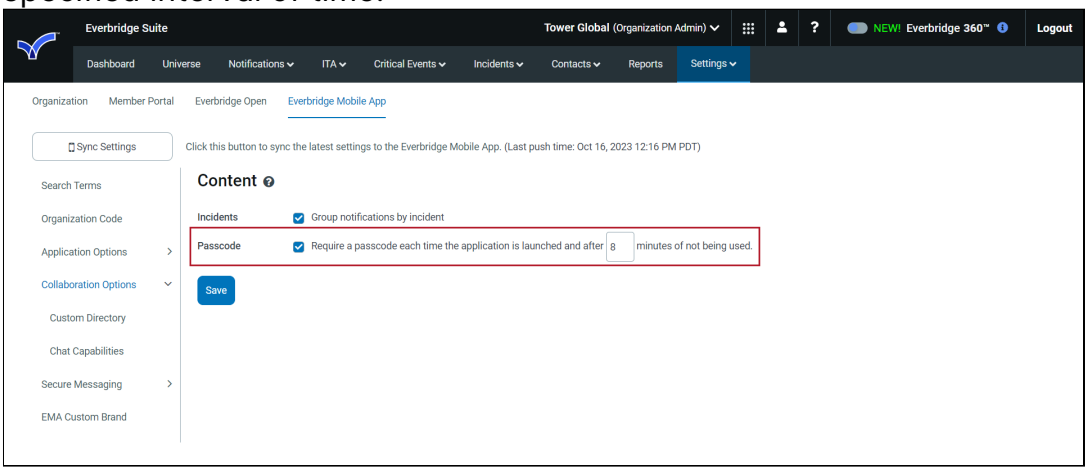


5. From the **Organization Settings** > **Peer-to-Peer Messaging** > **Settings**, select **Allow Secure Messaging users to view and securely communicate with my contact database.**

   This flag provides access to the contact database for the Organization, allowing the contact names to be available in the incident chat reports.

6. If desired, you can make the passcode required at **Settings** > **Everbridge Mobile App** > **Content**. If configured, the user will need to enter the passcode each time the app is launched, and after the app hasn't been in use for a

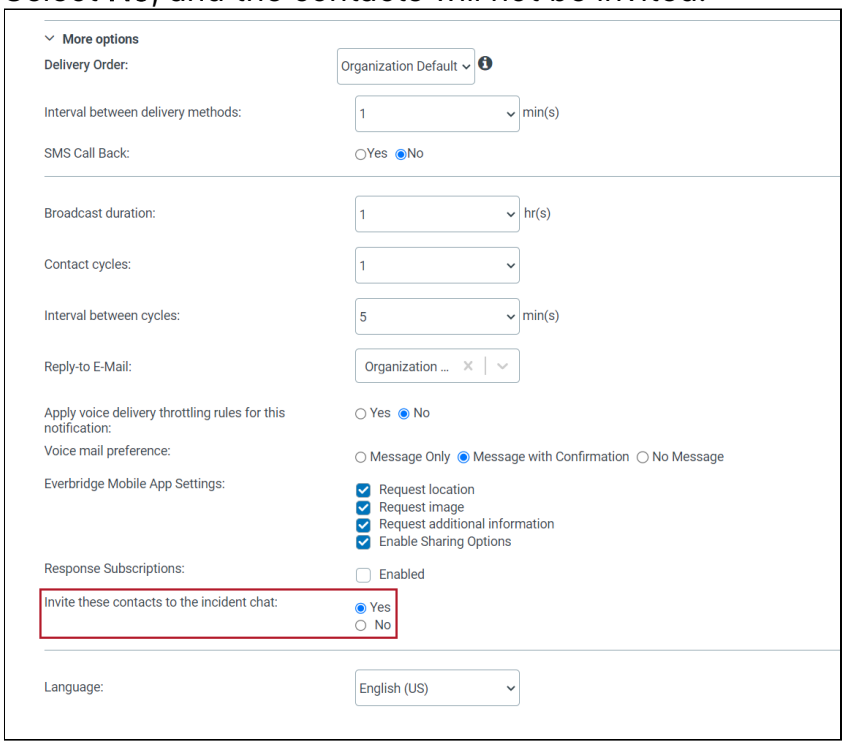
specified interval of time.



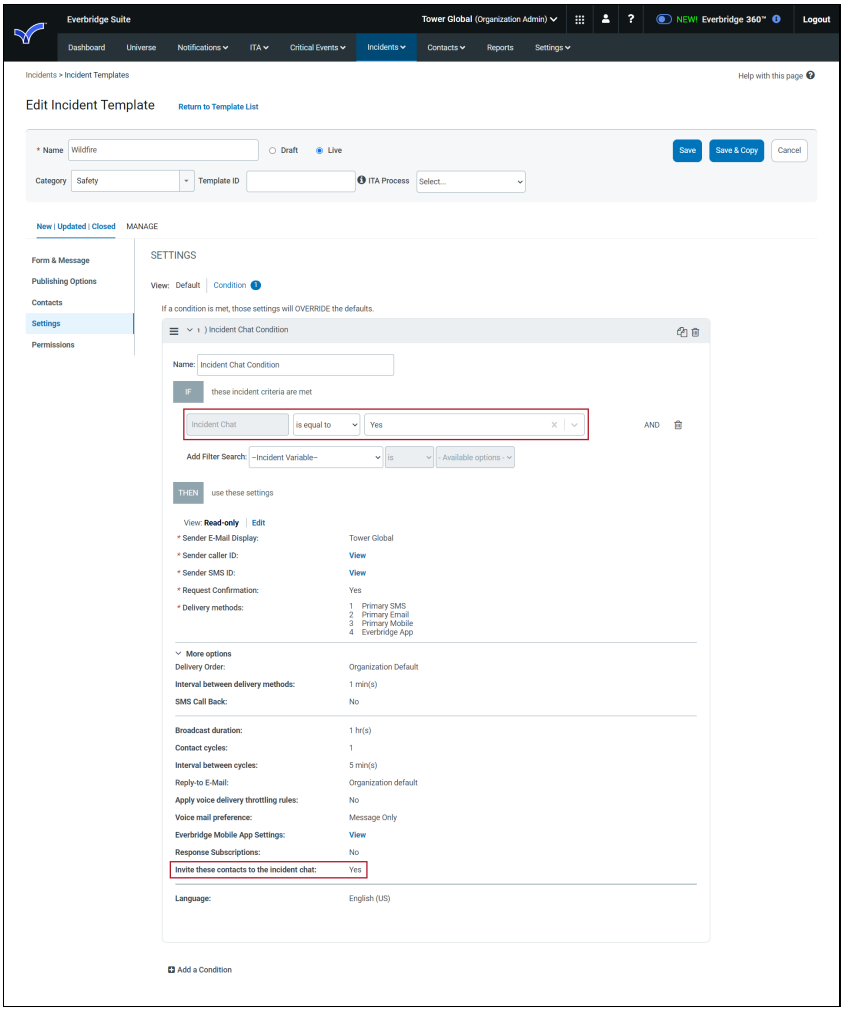
Configuring a Template for Incident Chat

Configure an Incident Template by performing the following steps:

1. From the **Incident Template Settings** > **More Options** > **Invite these contacts to the Incident chat.** The default value will pull from the Organization Settings. Choose one:
   - Select **Yes** to invite the contacts in the Notification to join the Incident chat.
   - Select **No**, and the contacts will not be invited.



2. Optionally, use conditions to let the variable values determine whether the contacts in that Incident Notification should be invited to the chat.

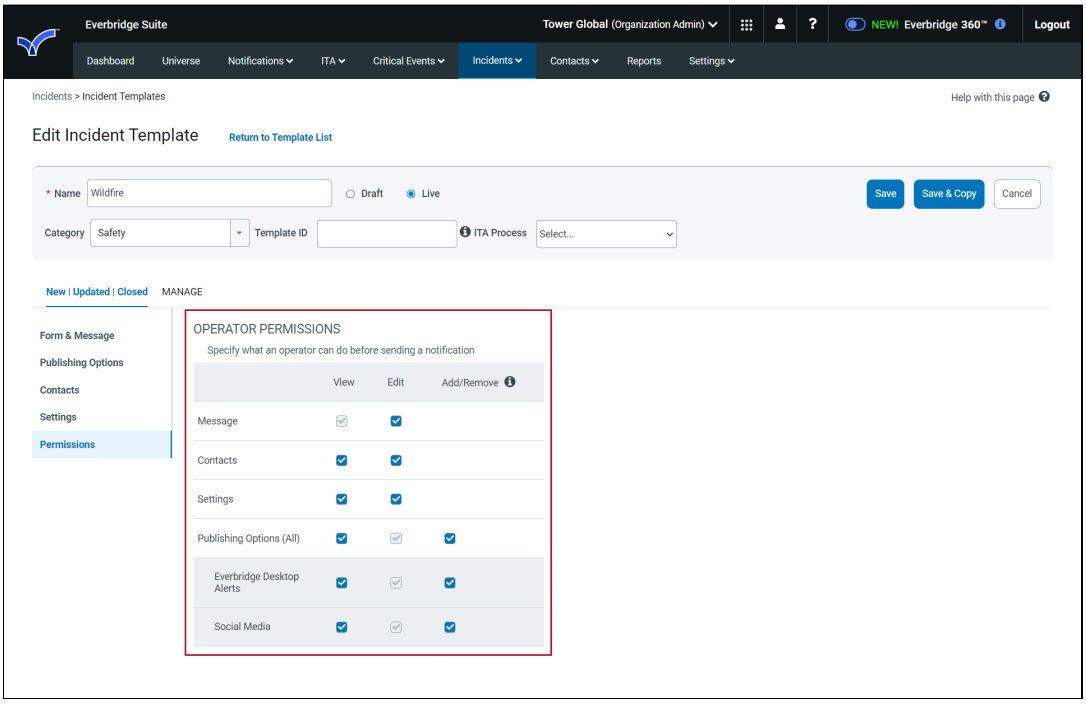


In this example, the template uses a single-selection variable called "Incident Chat," where the values are **Yes** or **No**. This gives the user launching the Incident Notification the ability to invite or not invite the contacts to join the Incident chat.

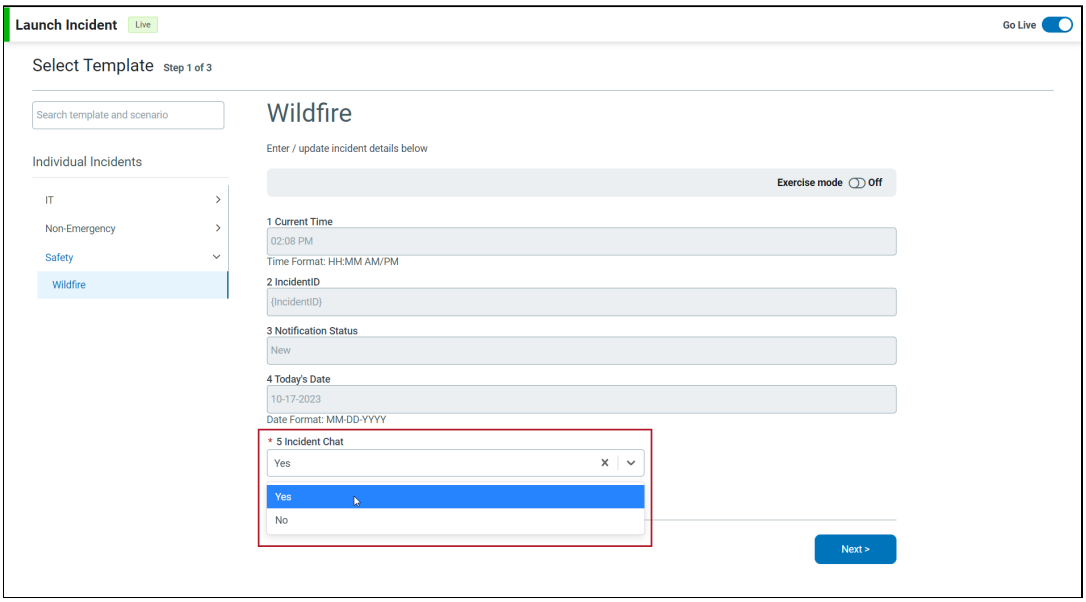
Of course, any other available conditional values can be used to determine whether the contacts selected, or that particular Incident Notification, are invited to the chat.

Launching a Chat-Enabled Incident

Since the Incident chat field is part of the Incident settings, it is available to the user launching the Incident notification based on the template's operator permissions.

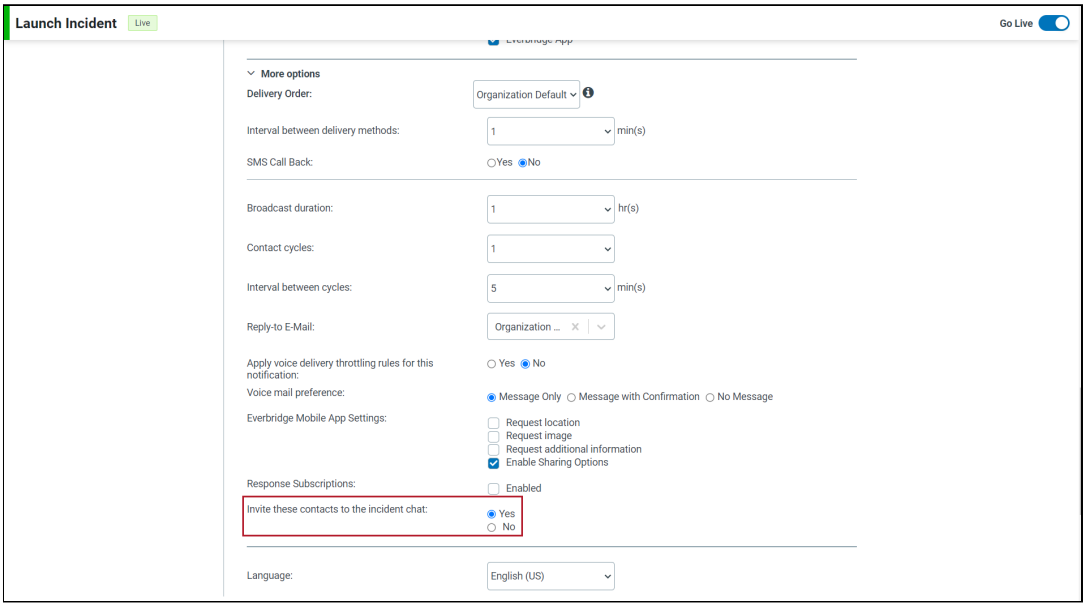


If conditional settings are applied to the template, the values selected for the variables will determine whether the selected contacts are invited to the Incident chat.



Launch an Incident by performing the following steps:

1. If the operator permissions allow the user to modify the settings at the time they are launching the notification, the user can determine whether to invite the selected contacts at the time of launch.

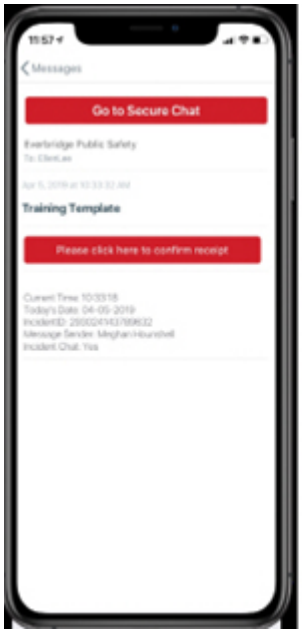


2. Make sure the **Mobile Push Alert** delivery method is selected for the Incident Template. This will ensure the notification is delivered to the contacts via the Everbridge Mobile App.

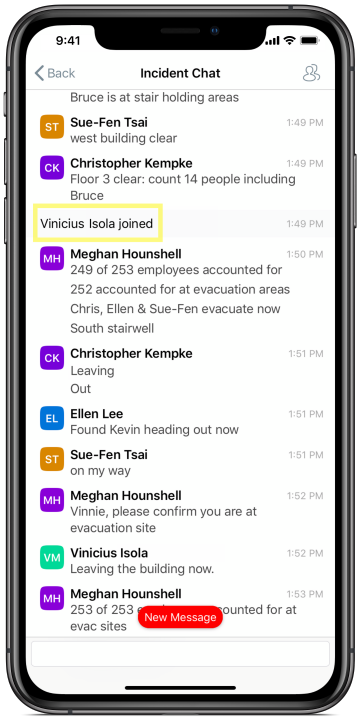
Using Incident Chat with the Everbridge Mobile App

Joining from Notification Details

1. The contacts selected for that Notification will receive an alert on their mobile device from the Everbridge Mobile App, just like any other Notification that is sent to the Mobile Push Alert delivery method.

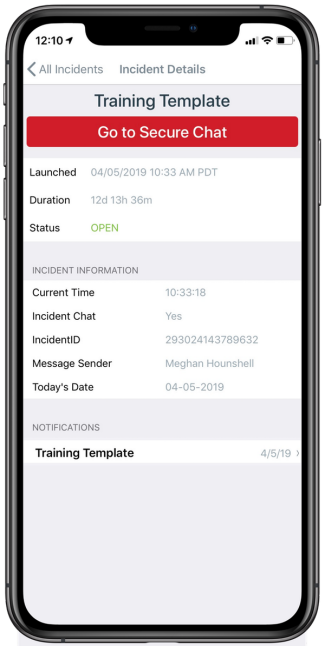


2. When the contacts view the Details page for that Notification, they will see an option on the page to **Go to Secure Chat**.
3. The Mobile user taps this button to navigate to the Incident chat.
4. If the Mobile user is tapping the **Go to Secure Chat** button for the first time for a given Incident, a “joined” message will be displayed for that user.



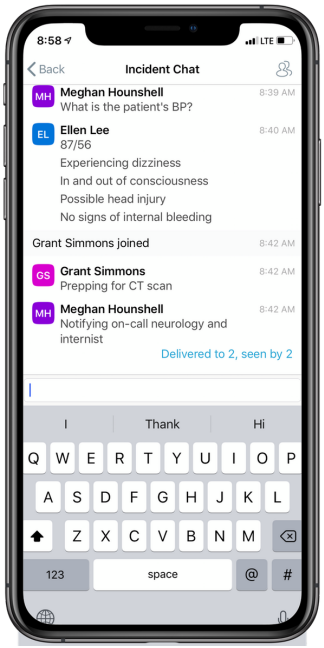
Joining from Incident Details

1. If **Group Notifications by Incident** is selected in the Organization Settings, Everbridge Mobile App users will have an **Incidents** button in the upper right of the Messages page.
2. When the user taps the Incidents button, the app displays a list of all Incidents for which that contact has received at least one Notification.
3. When the user selects an Incident from the list, the app displays the Incident details for that Incident.
4. If the contact has been invited to the Incident chat for at least one Notification for that Incident, he or she will see a button to Go to the Secure Chat.

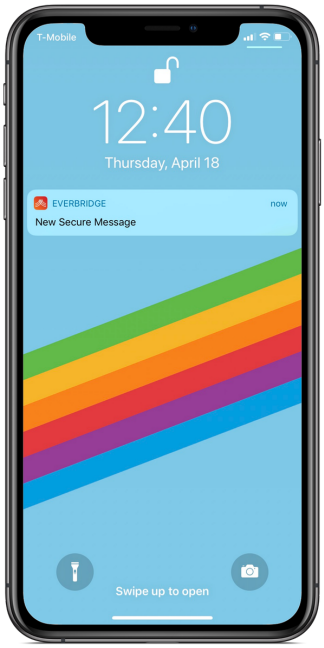


Participating in the Chat

1. The user can tap in the text field to create and send a text-based message to the chat.
2. When the user sends a message, his/her name will display as the sender, along with the time stamp of when that message was sent from the device.
3. For the most recently sent or received message in the chat, the user can see the number of participants who received and have seen that message.
4. If the user taps on the delivery / seen information, they can see a list of the participants that have received and seen the message.



5. As new users "Go to Secure Chat", a joined message will be displayed.
6. Tap the Participants icon to see who else is in the chat.
7. Each participant will be represented by the First Name and Last Name from their contact record in the Organization's contact list.
8. The avatar contains the First Name initial and the Last Name initial, and the background color is determined by an algorithm that uses the characters in the First Name and Last Name fields of the contact record in order to maintain a consistent color across all chats for that contact.
9. If the users are not actively viewing the chat, they will receive a push alert on their device that will play a unique alert tone when the device volume is on and will vibrate the device when muted.

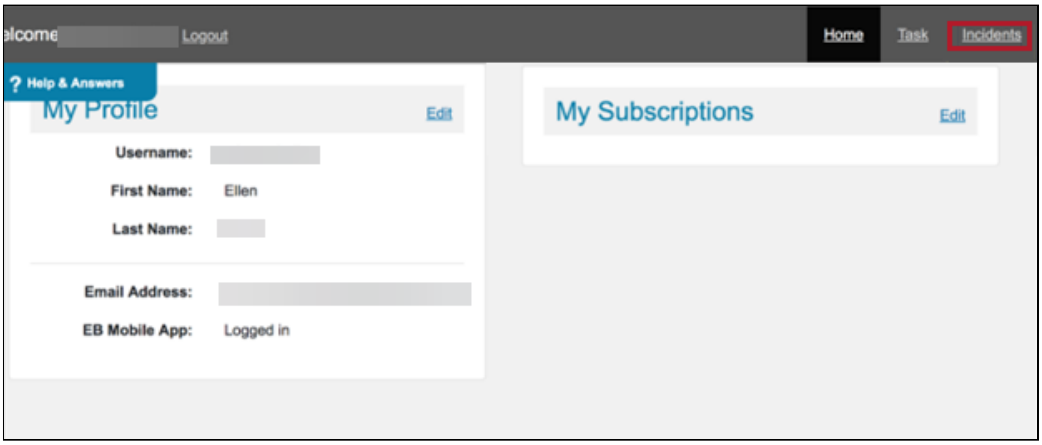


10. If the Incident Notification is sent to delivery methods other than the Everbridge Mobile App, there will not be an indication automatically added to the message, and the Notification initiator or template creator should account for this when creating the message content for that Notification.

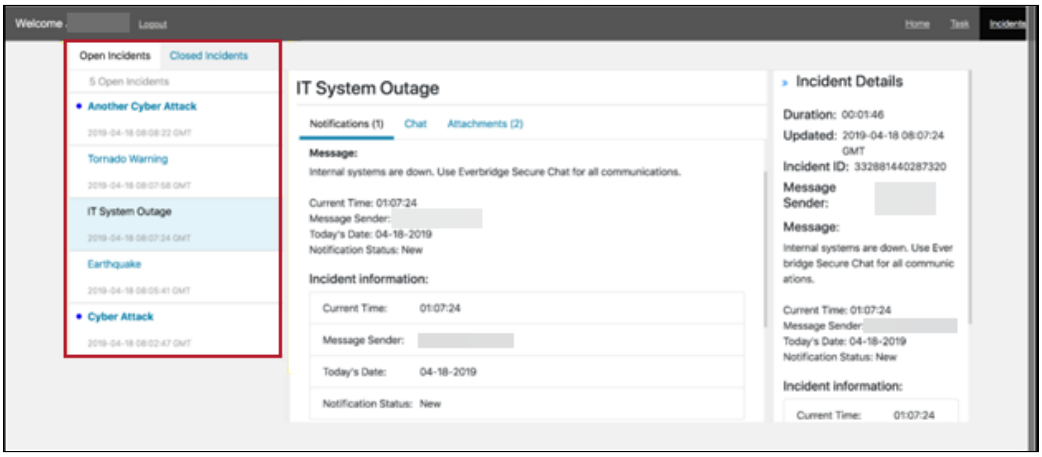
    Recommended text: "*You have been invited to join a Secure Chat for this Incident. View this message in the Everbridge Mobile App to join.*"

Using Incident Chat in the Member Portal

1. If **Display Incident information** has been selected under **Member Portal** > **Portal Options settings**, contacts logging into the Member Portal will see an Incidents link.

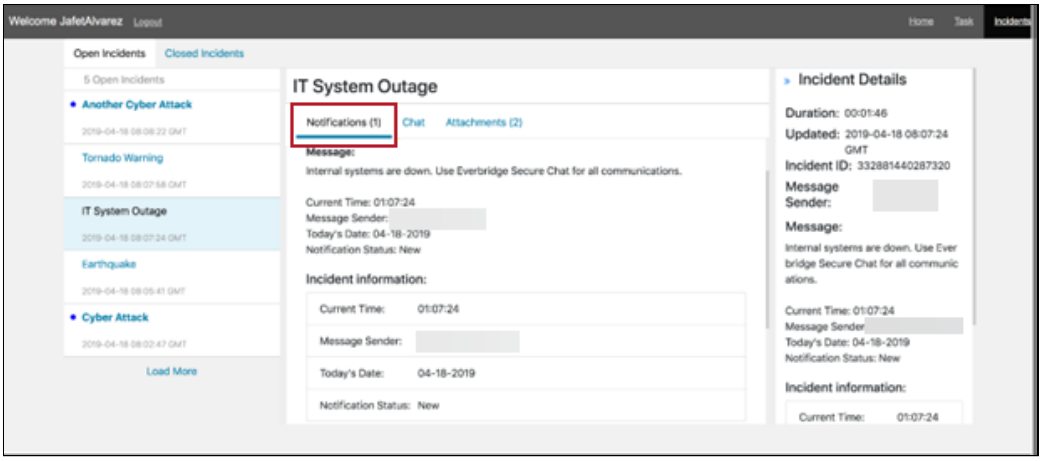


2. When the **Incidents** option is selected, the Member Portal displays a list of Incidents for which the logged-in Member Portal user has been a contact in at least one Notification for that Incident.

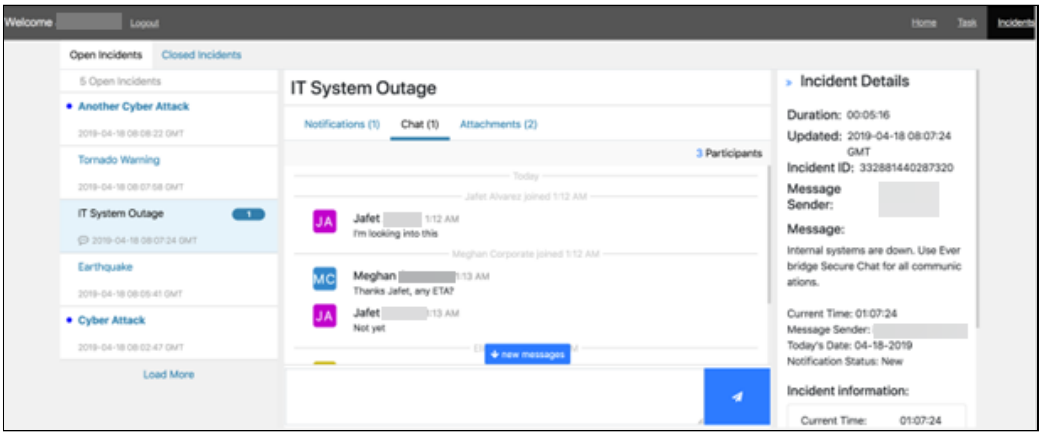


3. When the Member Portal user selects an Incident, they can see the Notifications received for that Incident.

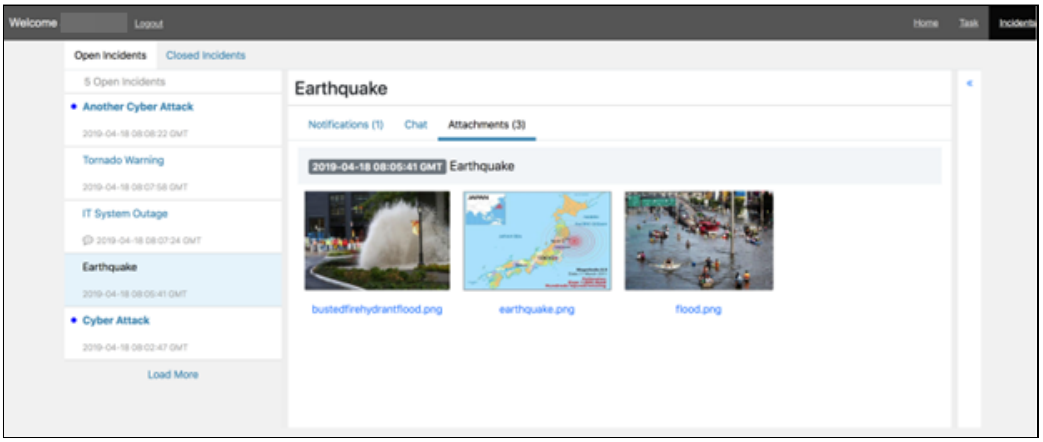
   The user will not be able to confirm Notifications from the Member Portal.



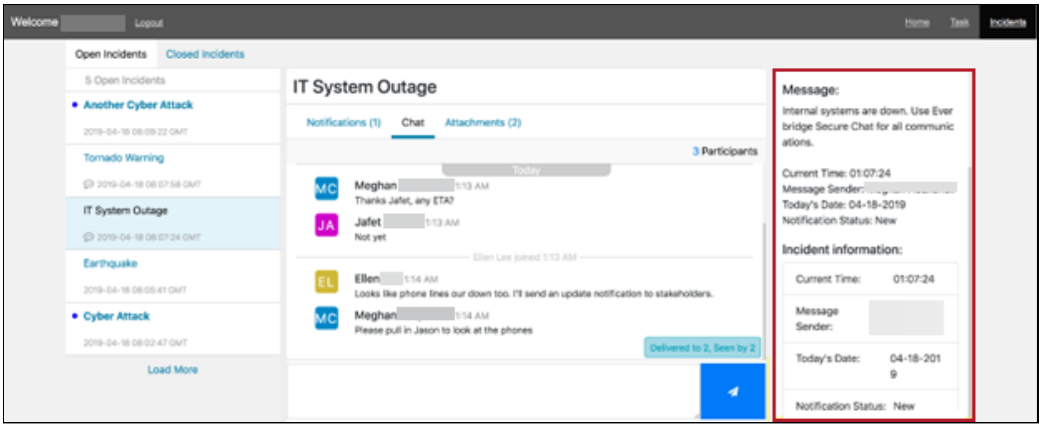
4. The user can also participate in the Secure Chat for that Incident from the Member Portal.



5. If any of the Notifications received for that Incident contain an attachment, those attachments will be available in the Attachments section for that Incident.



6. The metadata for the Incident, including the most recent variable values received for any Incident Notification, is available on the right-hand side of the page.


Welcome
Logout
Home
Task
Incidents
Open Incidents
Closed Incidents
5 Open Incidents
Another Cyber Attack
Tornado Warning
IT System Outage
Earthquake
Cyber Attack
Load More
IT System Outage
Notifications (1)
Chat
Attachments (2)
3 Participants
Today
Meghan
Thanks Jafet, any ETA?
Jafet
Not yet
Ellen Lee joined 1:13 AM
Ellen
Looks like phone lines our down too. I'll send an update notification to stakeholders.
Meghan
Please pull in Jason to look at the phones
Delivered to 2, Seen by 2
Message:
Internal systems are down. Use Ever bridge Secure Chat for all communic ations.
Current Time: 01:07:24
Today's Date: 04-18-2019
Notification Status: New
Incident information:
Current Time: 01:07:24
Message Sender:
Today's Date: 04-18-201 9
Notification Status: New

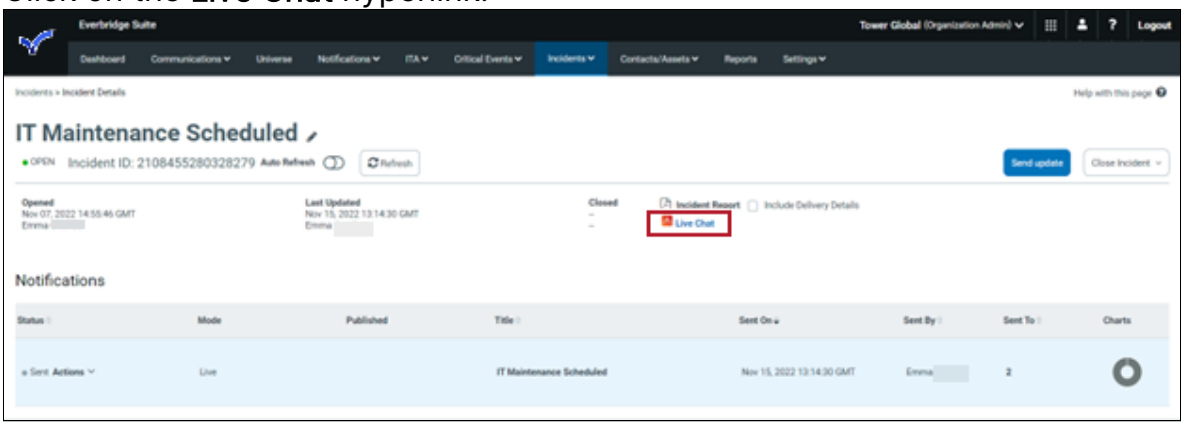
Using Incident Chat in the Manager Portal

Everbridge Users can join a live Incident Chat from the Everbridge Manager Portal if their user profile has been linked to a contact in the Organization where the Incident was sent from.

> **NOTE:** Users who attempt to access an Incident Chat when they have not been linked to a contact in the Organization will receive an error. For troubleshooting, refer to the Support Center.

To access the Incident Chat via the Manager Portal User Interface:

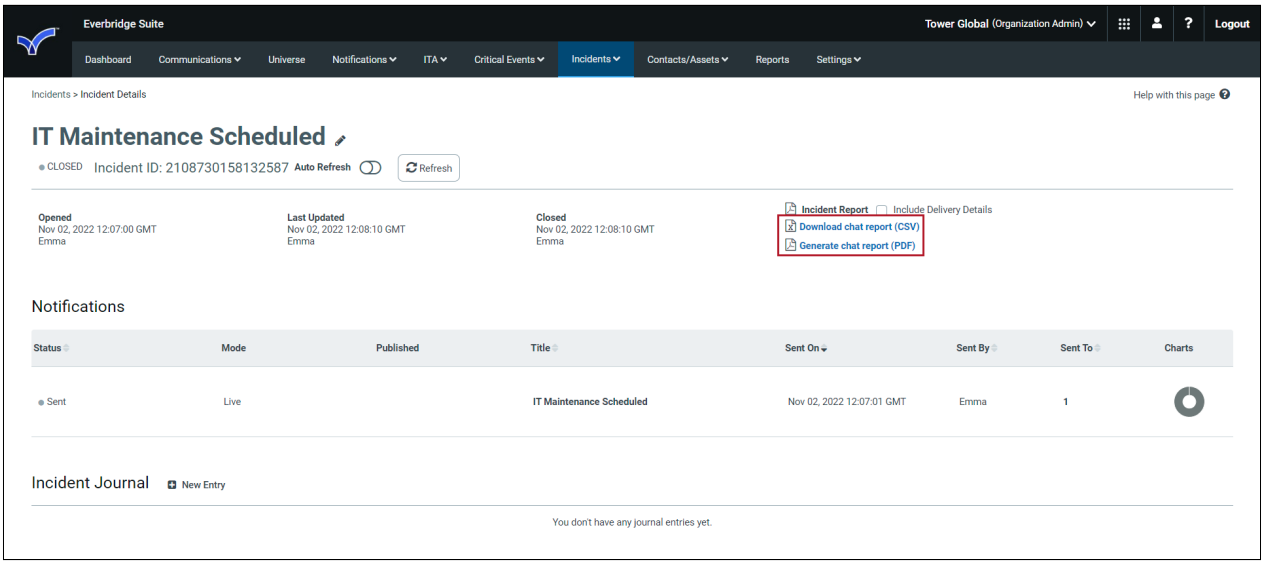
1. Log into the Manager Portal.
2. Select the appropriate organization from the upper right-hand corner.
3. Hover over the **Incidents** tab from the top menu bar and navigate to the **Open / History** from the drop-down menu.
4. Select the **Open** option next to Viewing: and click the **name** of the Incident.
5. Click on the **Live Chat** hyperlink.



Running Chat Reports

Incidents that have Live Chat enabled will show reporting once the Incident has been closed. There are two different types of reports that can be generated: PDF and CSV. Both of these reports are available to generate in the **Incident Details** screen.

Click the PDF report to download a transcript of the chat and/or click the CSV report to download detailed metadata for the chat.

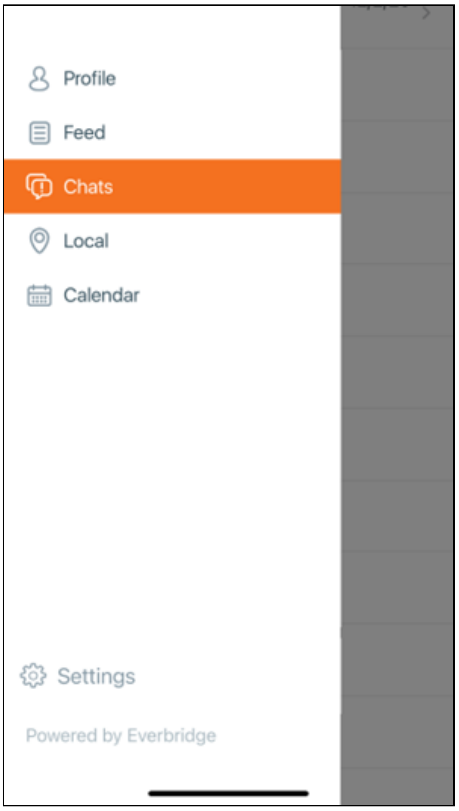


To generate and download the reports:

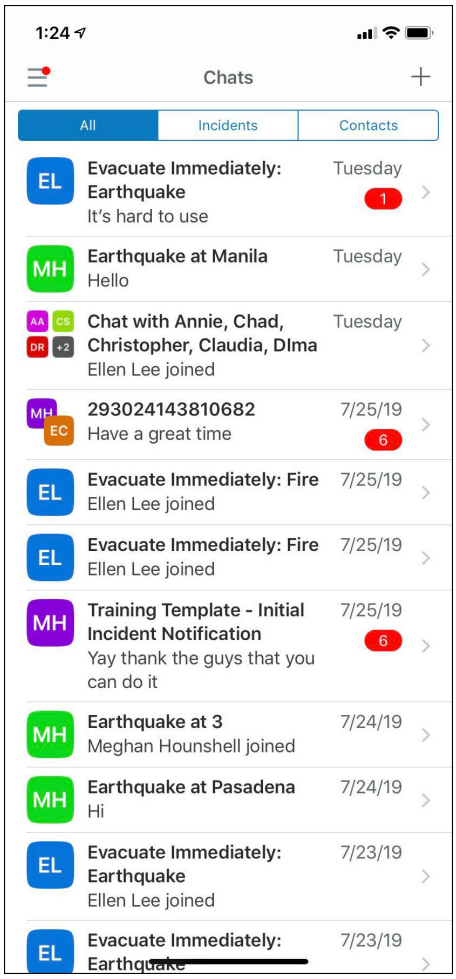
1. Log in to the Manager Portal and select the appropriate organization from the upper right-hand corner
2. Hover over the **Incidents** tab from the top menu bar and navigate to the **Open / History** from the drop-down menu
3. Select the **Closed** option next to Viewing: and click the name of the Incident
4. Whilst in the **Incident Details** screen, two hyperlinks will appear for the Incident Chat reports:
    - **Generate chat report (CSV)**
    - **Generate chat report (PDF)**
5. Click each report type to start generating the reports in the background. This may take a while, depending on how much chatting has taken place in that incident's chat.
6. The links to the reports will change to say **Download** once the files are ready for download.

Using Secure Chat

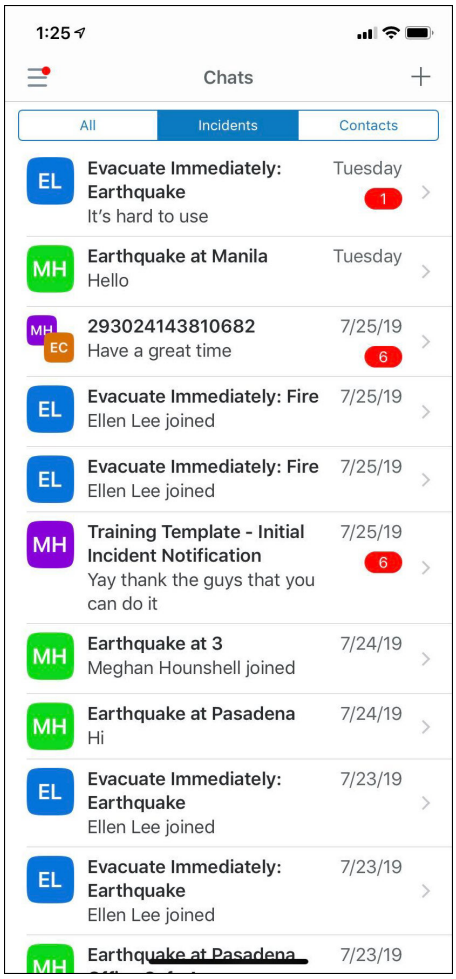
If the Mobile users have permission to Chat, they will have the **Chats** item in their menu.



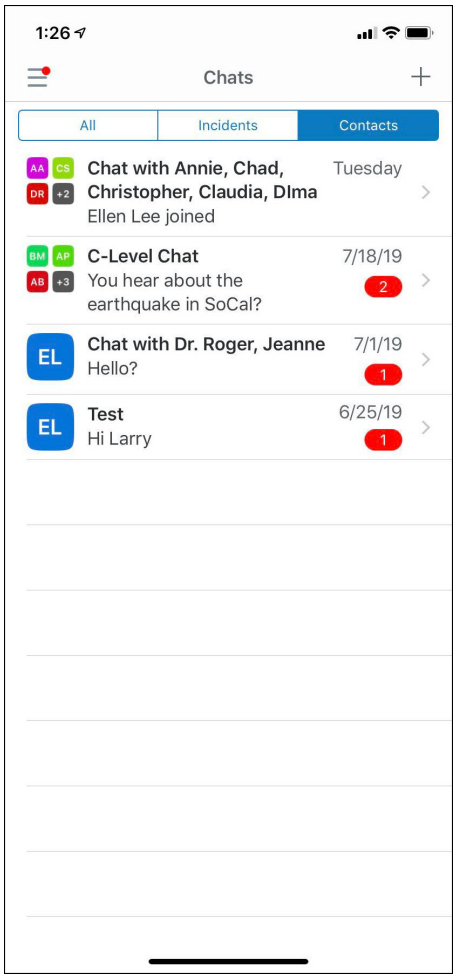
The Chats page displays a list of Chats for the mobile user. This includes Directory Chats and Incident Chats.



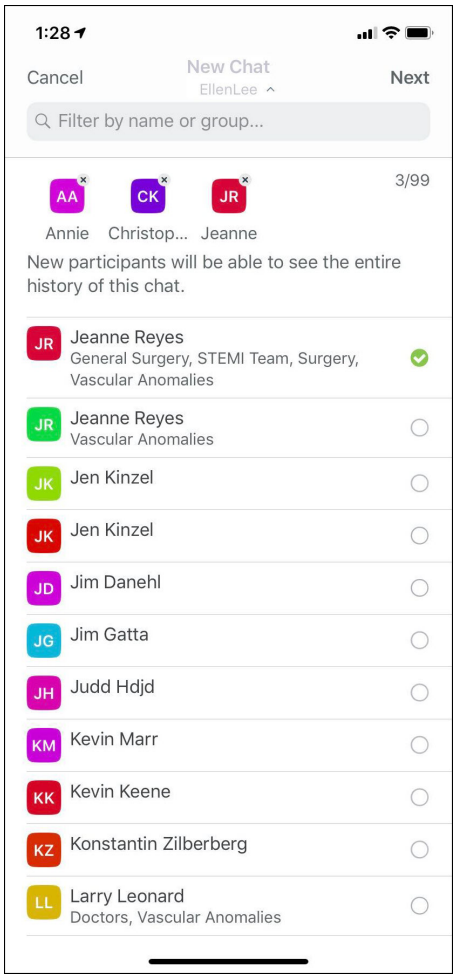
The page defaults to **All Chats**, but you can also filter by Incident Chats.



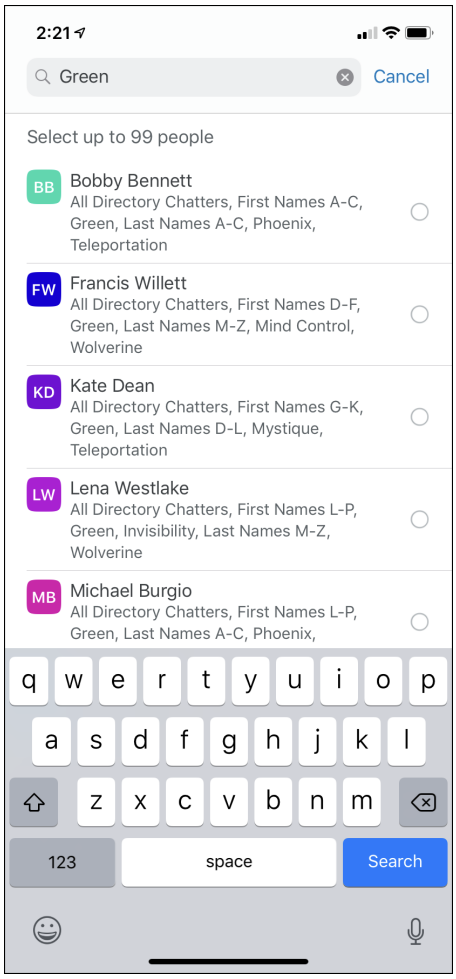
Or, you can filter by **Directory Chats**.



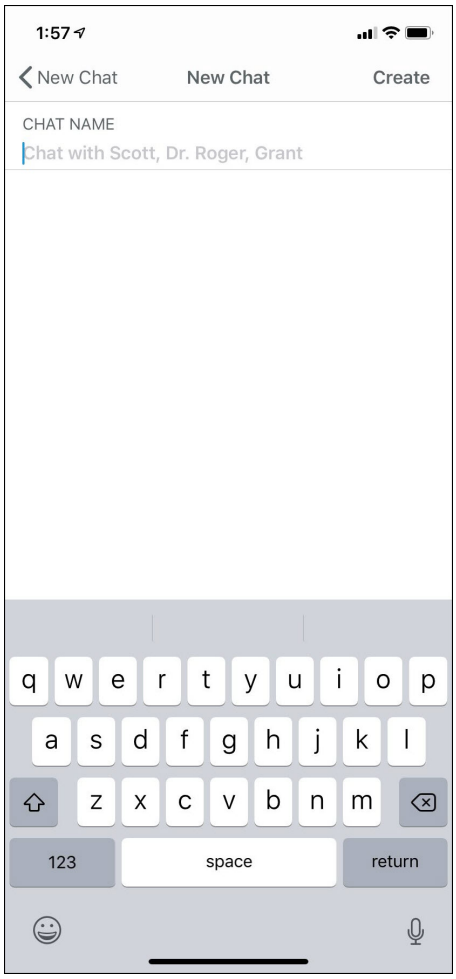
Tap the **+ symbol** in the upper right-hand corner of the screen to create a new **Directory Chat**. Here is where all the contacts in the directory appear. Users can scroll through the list and select with whom they want to Chat.



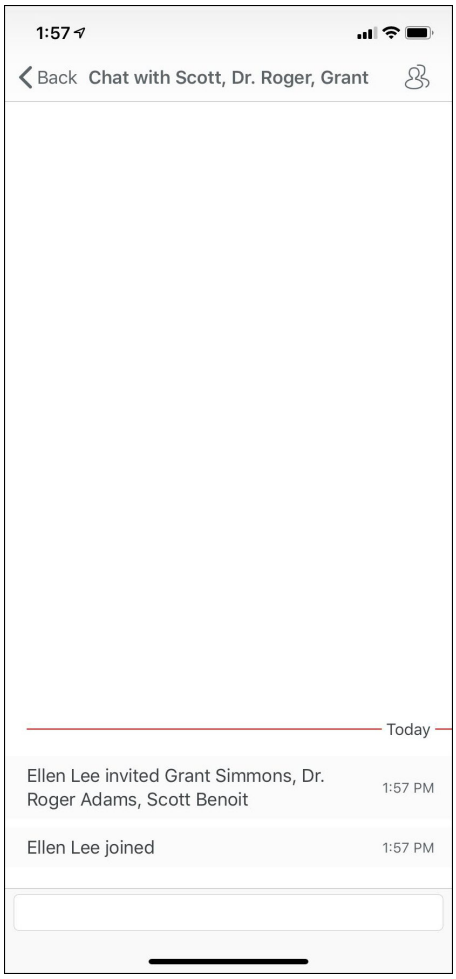
Users can also search by contact name or group name.



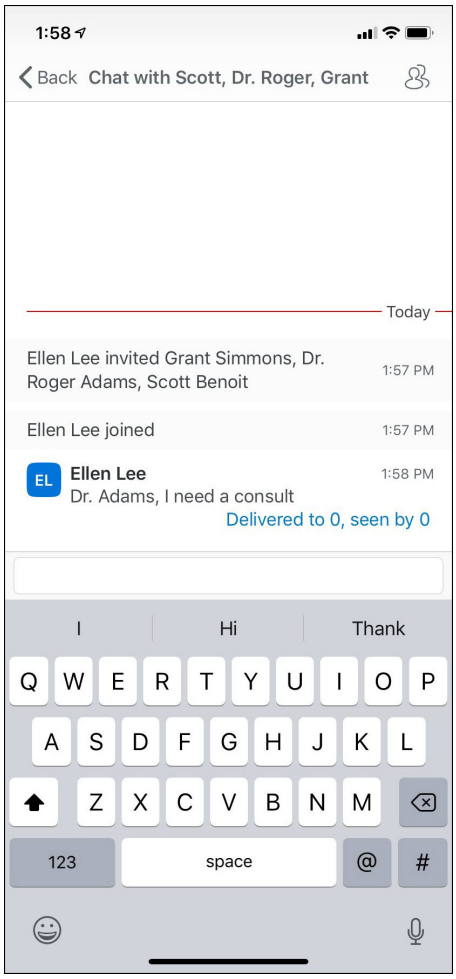
From the directory, select with whom you want to Chat, then tap **Next**, and create a name for the Chat.



You are dropped into the Chat when you tap **Create**.



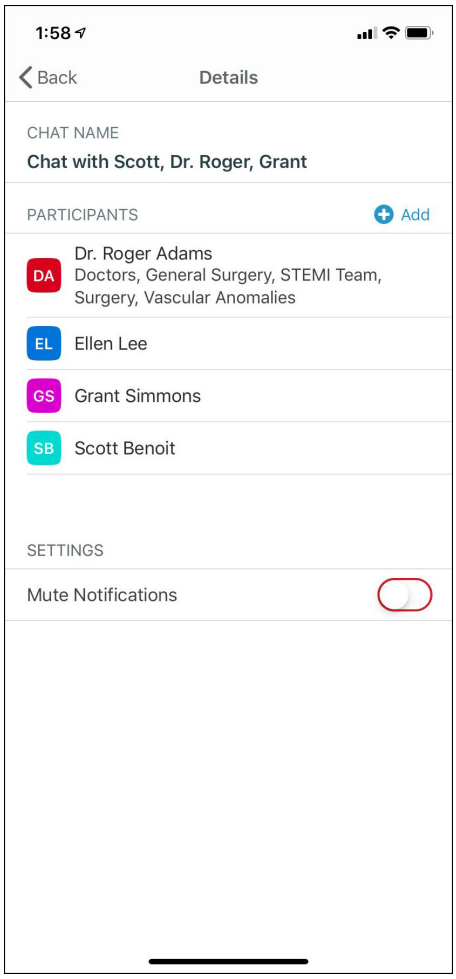
Chat works identically to Incident Chat.



Tap the **People** icon on the upper right-hand corner of the screen to see a list of participants.

- You can mute notifications, but know that you will not get alerts for new messages in a muted Chat.
- You can add more participants to the Chat from your directory.

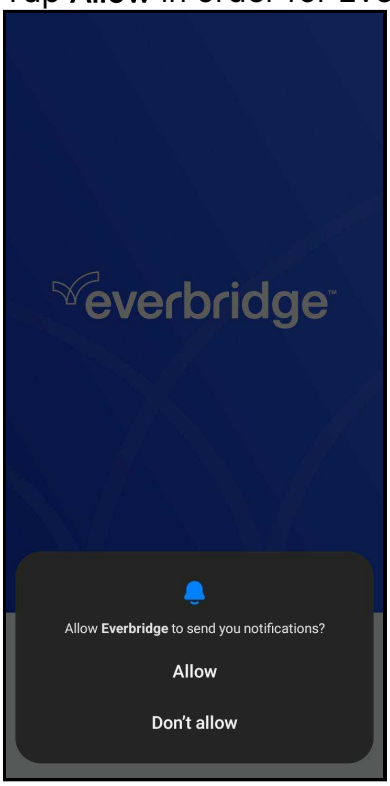
Both **Mute** and **Add** are available for existing Chats for both Directory Chat and Incident Chat.


1:58
Back
Details
CHAT NAME
Chat with Scott, Dr. Roger, Grant
PARTICIPANTS
Add
DA
Dr. Roger Adams
Doctors, General Surgery, STEMI Team, Surgery, Vascular Anomalies
EL
Ellen Lee
GS
Grant Simmons
SB
Scott Benoit
SETTINGS
Mute Notifications

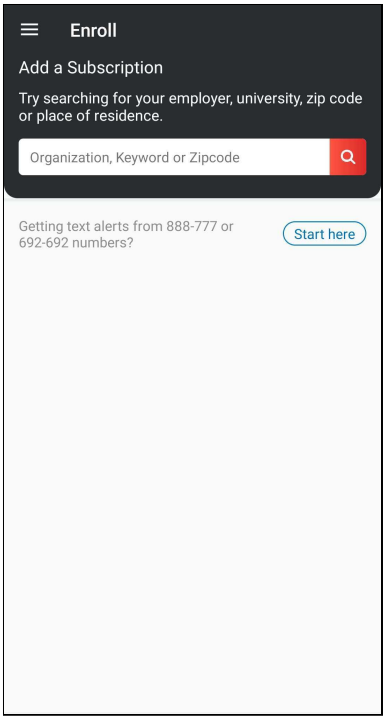
Using Video Chat

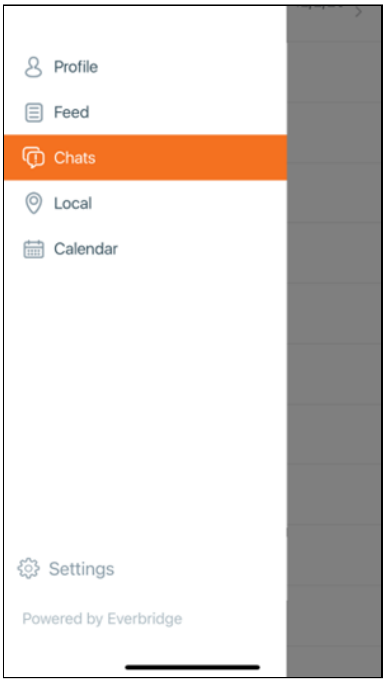
Follow the steps below to use Video Chat on your mobile device:

1. Tap **Allow** in order for Everbridge to send you notifications.

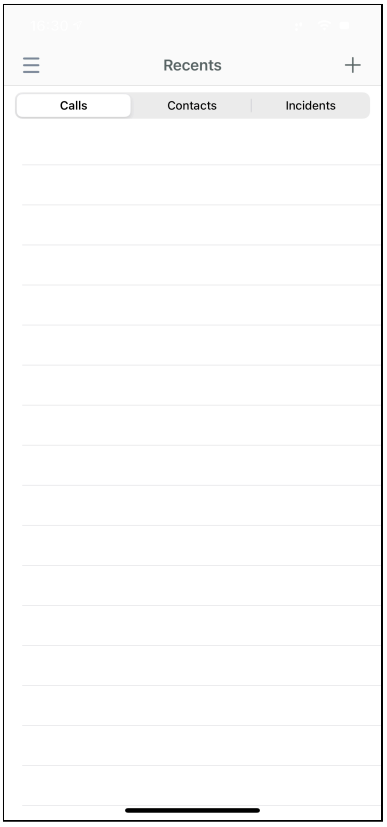


2. Enter your Organization name in the search field and tap the **Search** icon.

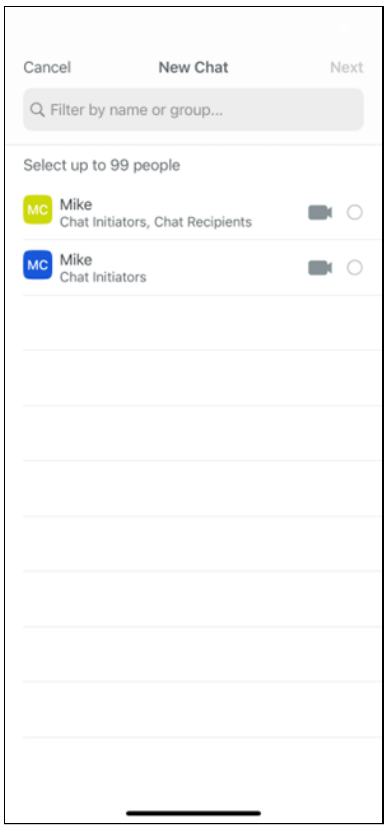


3. Sign up or log in with your existing Username and Password. Alternatively, if your organization is using Single Sign-On, from the SSO Login page, enter your Username and Password to log in.
4. From the Account Management screen, tap **Done**.
5. Tap the **Menu** icon, then select **Chats**.
6. 

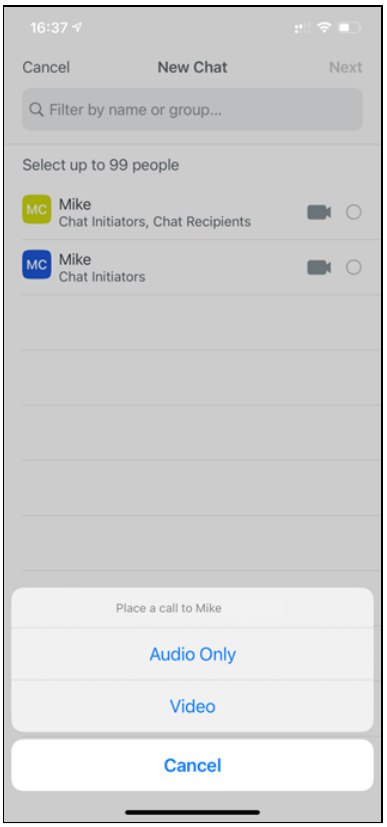
7. Tap the **+ icon** to start a new chat.



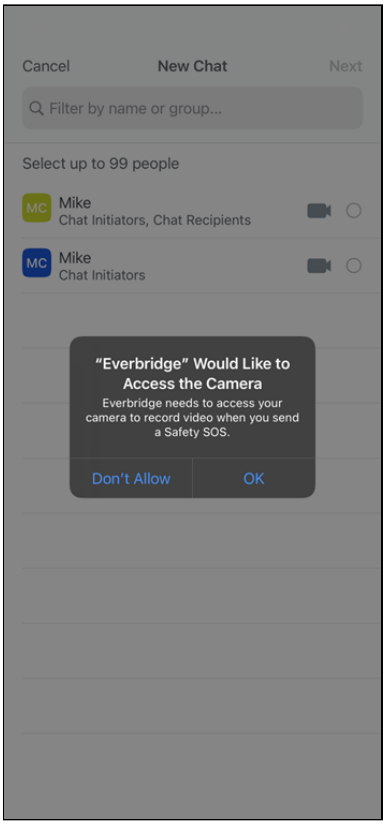
8. Search for contacts.
    - **For a Video Call** - Tap the **camera** icon.
    - **For a Text Chat** - Select the contact(s), then tap **Next**.


Cancel
New Chat
Next
Filter by name or group...
Select up to 99 people
MC
Mike
Chat Initiators, Chat Recipients
MC
Mike
Chat Initiators

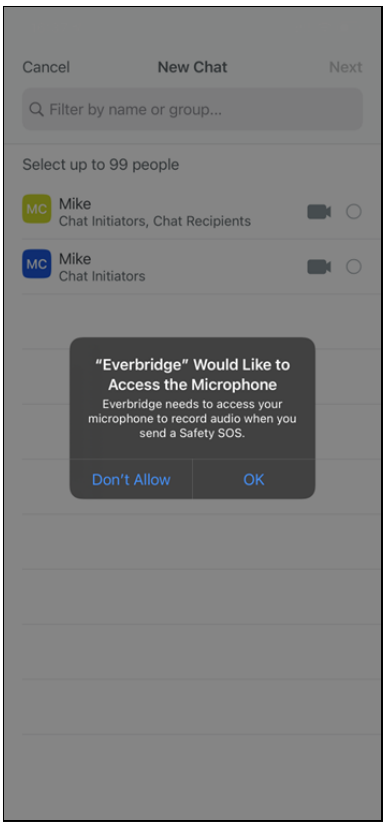
9. Tap **Video**.


16:37
Cancel
New Chat
Next
Filter by name or group...
Select up to 99 people
MC
Mike
Chat Initiators, Chat Recipients
MC
Mike
Chat Initiators
Place a call to Mike
Audio Only
Video
Cancel

10. Tap **OK** to allow access to the camera.



11. Tap **OK** to allow access to the microphone.



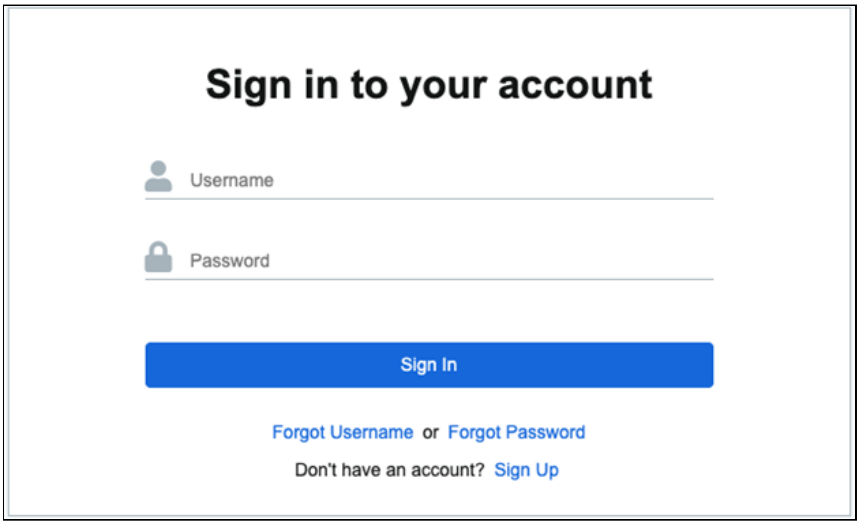
12. Tap the corresponding button to:
    - **Stop video -** Pause the video Tap it again to resume.
    - **Mute** - Mute the audio. Tap it again to unmute.
    - **Flip** - Change the active camera. Tap it again to change back.

- **End** - End the call.

Using Secure Chat in the Member Portal

Follow the steps below to use Secure Chat in your Member Portal.

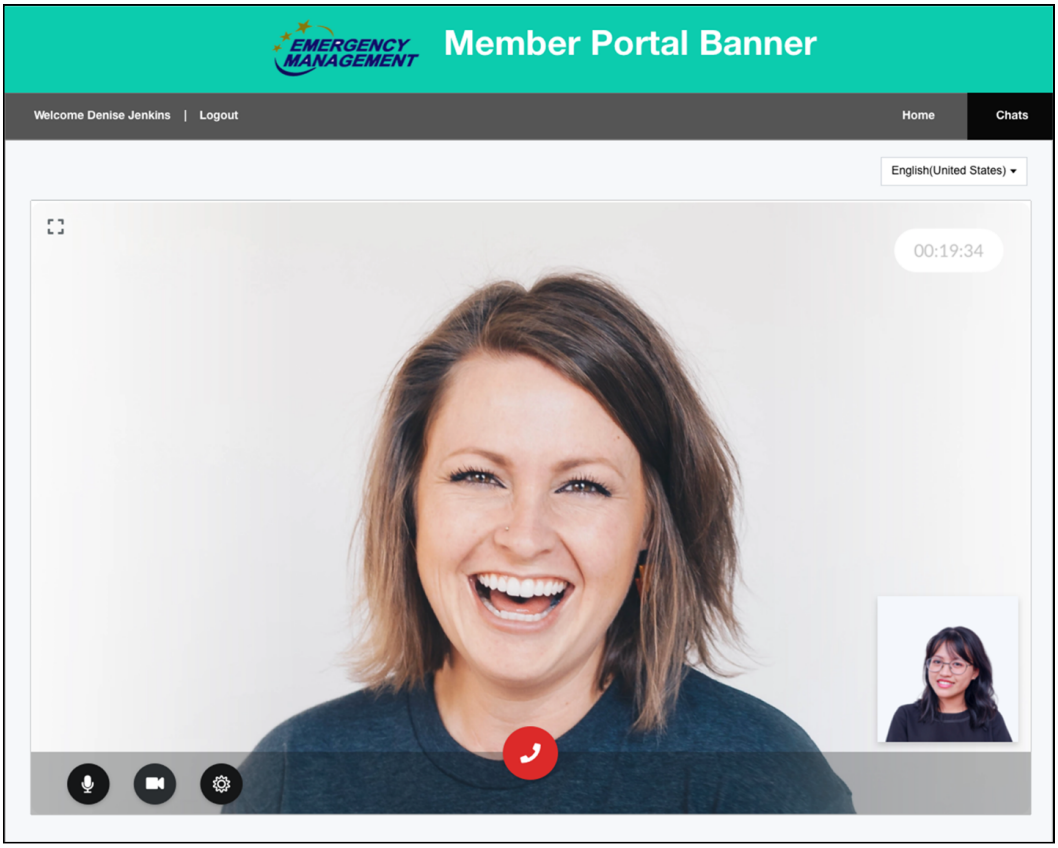
1. Open the link to your Organization's Member Portal and sign in.



2. Click the **Secure Chat** tab.
3. Click the **+ icon** to start a new chat.

4. Search for contacts with whom to chat, then click **Save**.
5. To send an attachment, click **the paper clip** icon in the Chat window.
6. To start a video call, click the **camera** icon next to the name of the contact to call.

> **NOTE:** Your browser might ask you to allow permission to use your camera and microphone for the call.



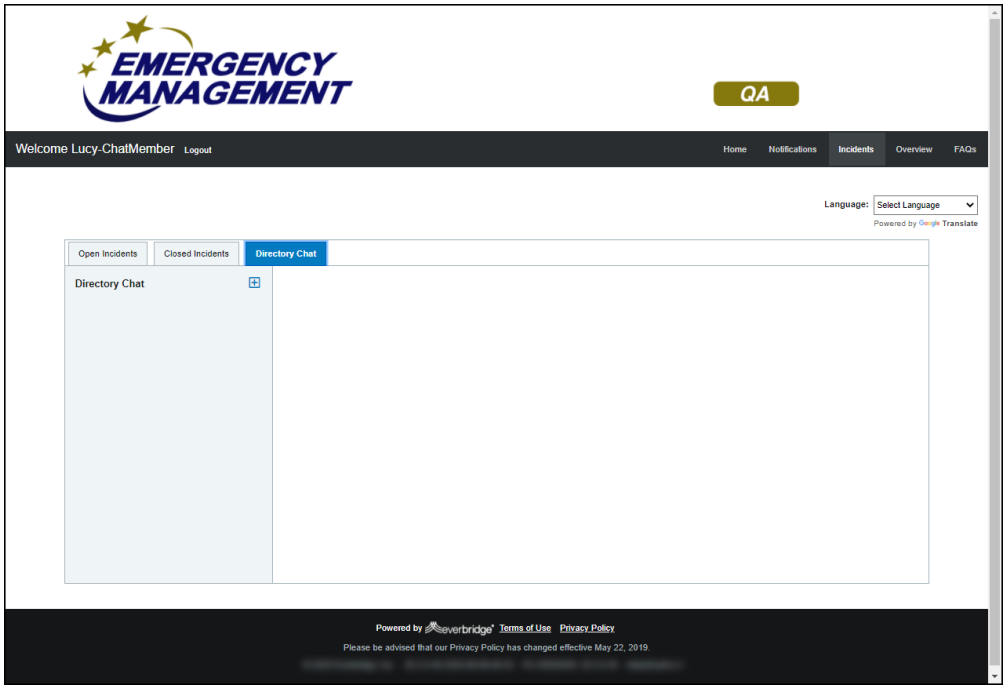
7. Use the corresponding button to:
    - Pause the video - Click the **camera** icon.
    - Mute - Click the **microphone** icon.
    - Change the audio and video source settings - Click the **cog** icon.
    - End the call - Click the **red phone** icon.

Using Directory Chat in the Member Portal

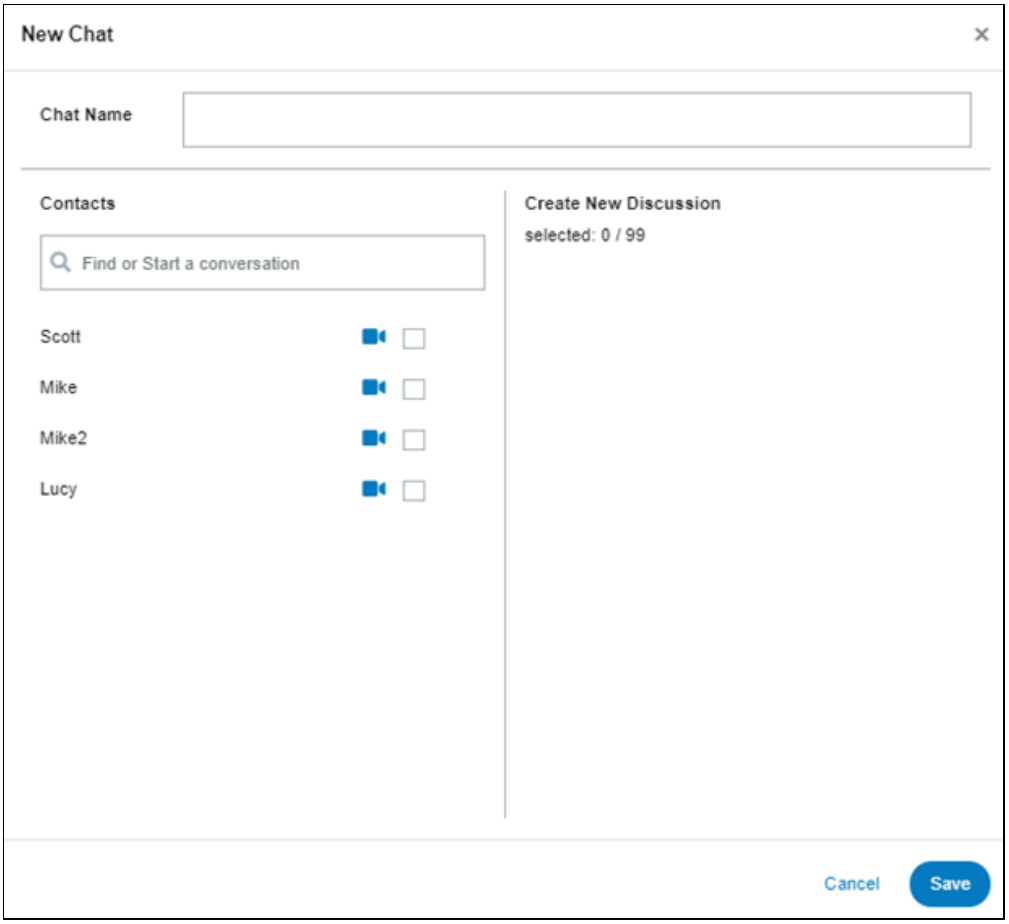
If your Organization has enabled **Secure Collaboration** > **Directory Chat** > **Enable Video Chat**, select the **Display Incident information** checkbox to enable Directory Chat in the Member Portal.

To use Directory Chat in the Member Portal:

1. Log in to the Member Portal.
2. Select the **Incidents** tab.
3. Select the **Directory Chat** subtab.



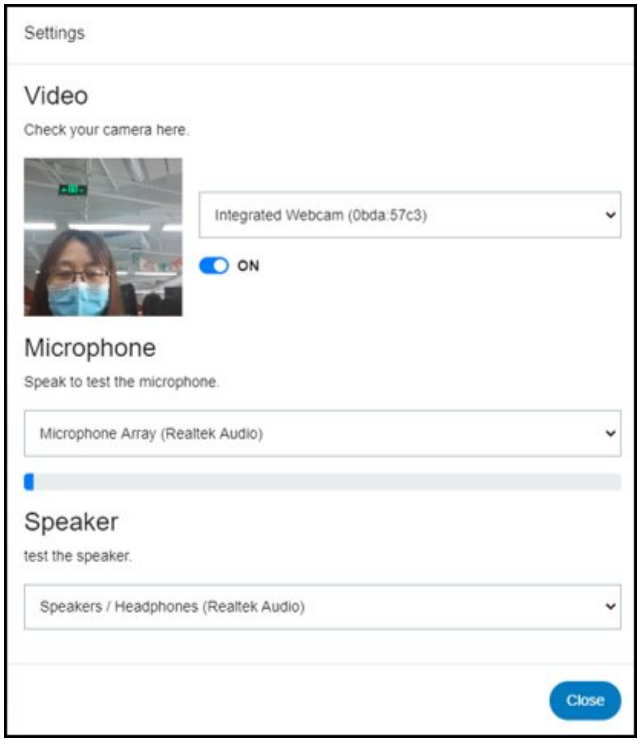
4. Click the **Plus sign (+)** to start a new directory chat. The New Chat window is displayed.



5. Enter a **Chat Name**.
6. If needed, search for the contact by name.
7. Click the check box next to a contact name to start a Text chat. The names are added to the **Create New Discussion** pane.
8. Click **Save**. The Chat Name is displayed along with the number of participants.
9. To Text chat, enter your text and/or click the **Paper Clip** icon to attach a file, then click **Send**.
10. To Video chat:
    - Click the **Video** icon in the upper right-hand corner of the panel to display the participant's list.
    - From the Participant's List, click the **Video** icon next to a contact's name. The **Calling** pop-up window is displayed.
    - Optionally, mute the audio and/or pause the video before the connection is established.
    - The contact receiving the call is shown a web browser notification and a pop-up window from which the contact can mute the audio and/or pause the video before the connection is established. To start the chat, the receiving contact clicks the green phone handle.

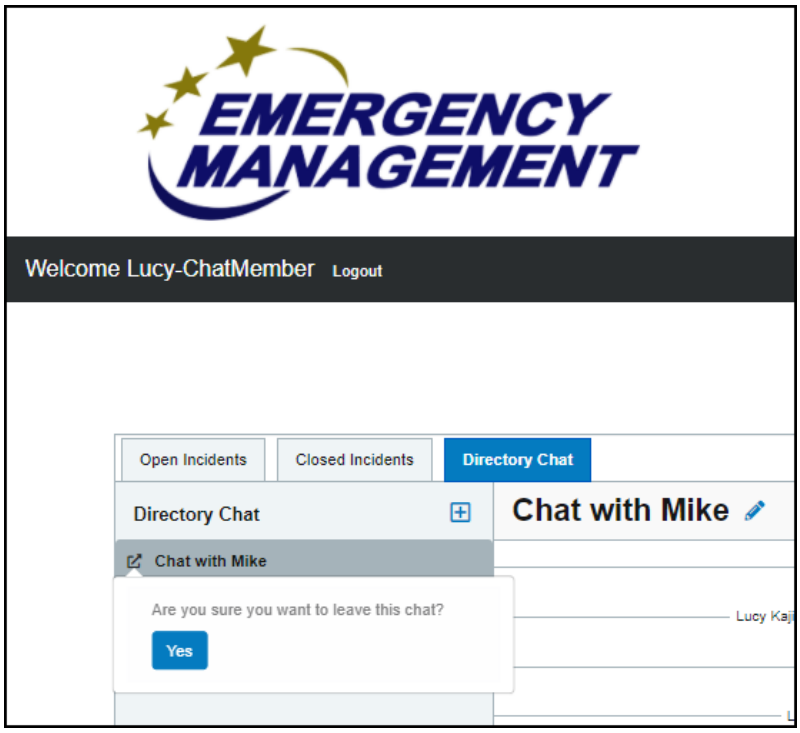
- A self-preview video is shown on the right-hand side of the screen. The caller can mute the audio and/or pause the video during the call. (If the receiving contact pauses their video, their name is displayed in the background to the other party. If the calling initiator pauses his or her own video, that person's video preview is not shown in the self-preview.)

- There is also a **Cog** icon to change the settings.



- After ending the video chat, click **Add More** to add more participants. Note that in the **Edit Chat** dialog, you can add more contacts, but you cannot remove the existing participants.

- Current participants can leave the chat by clicking the **Leave** icon (next to the Chat Name) and clicking **Yes** to confirm.



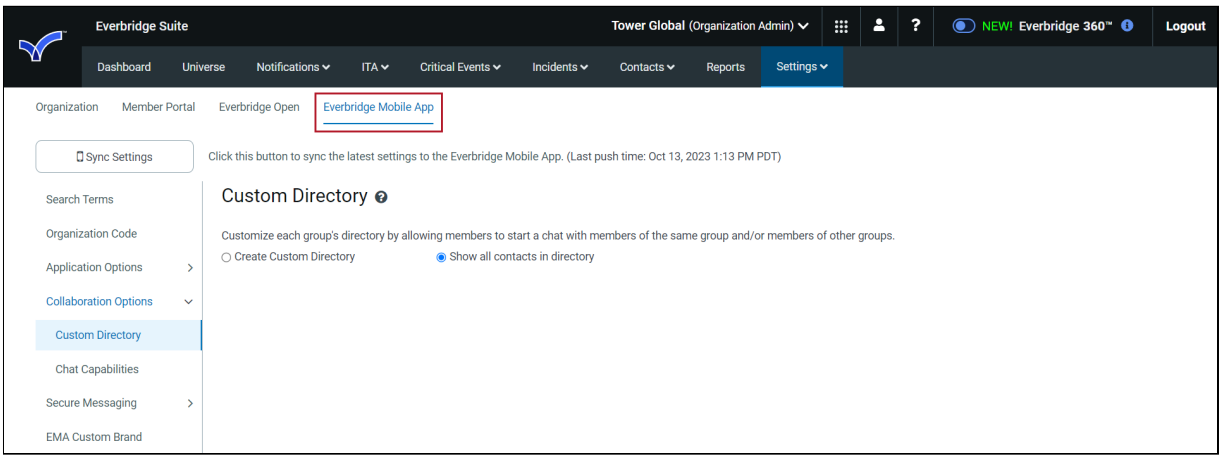
Reports

See the ***Reports*** section of the *Account Administrator Guide* or *Organization Administrator Guide* to learn about the following chat reports:

- Chat Summary
- Chat Transcript

Configuring Everbridge Mobile App Settings

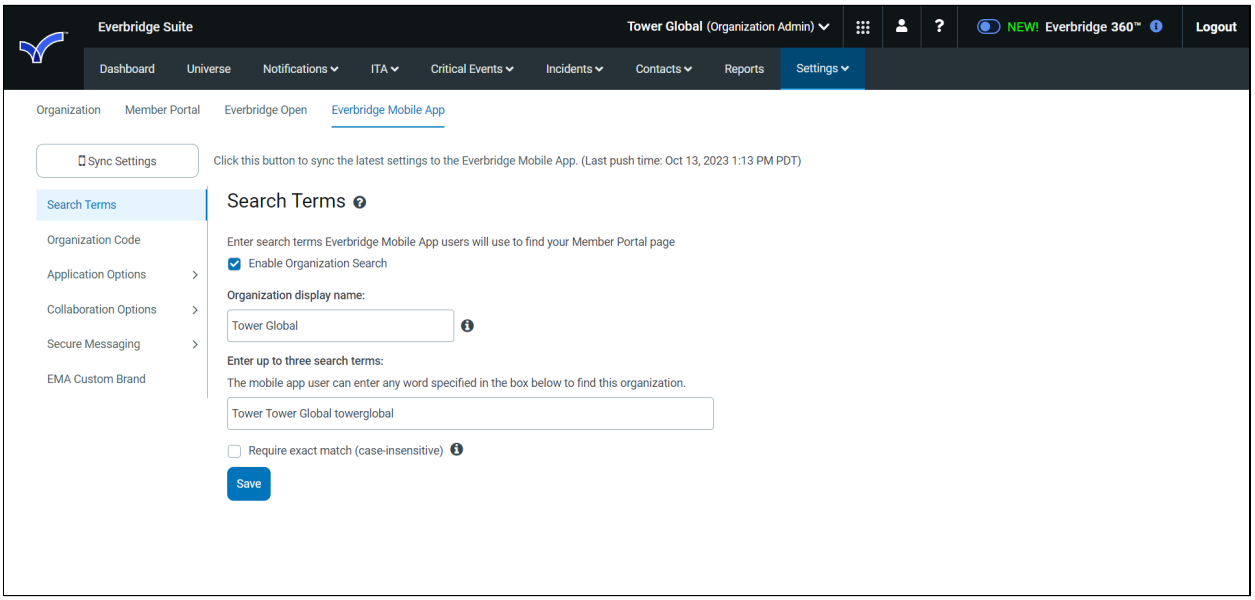
From the **Settings** tab at the Organization level, select the **Everbridge Mobile App** subtab, where you can configure your Everbridge Mobile App options.



Search Terms

The Everbridge Mobile App feature allows you to search for up to three search terms, one of which must be your organization name, from your mobile device. This can be configured from **Settings** > **Everbridge Mobile App** > **Search Terms**. If desired, you can also require an exact match by selecting the checkbox.

Click the **Sync Settings** button to synchronize the latest settings to the Everbridge Mobile App.

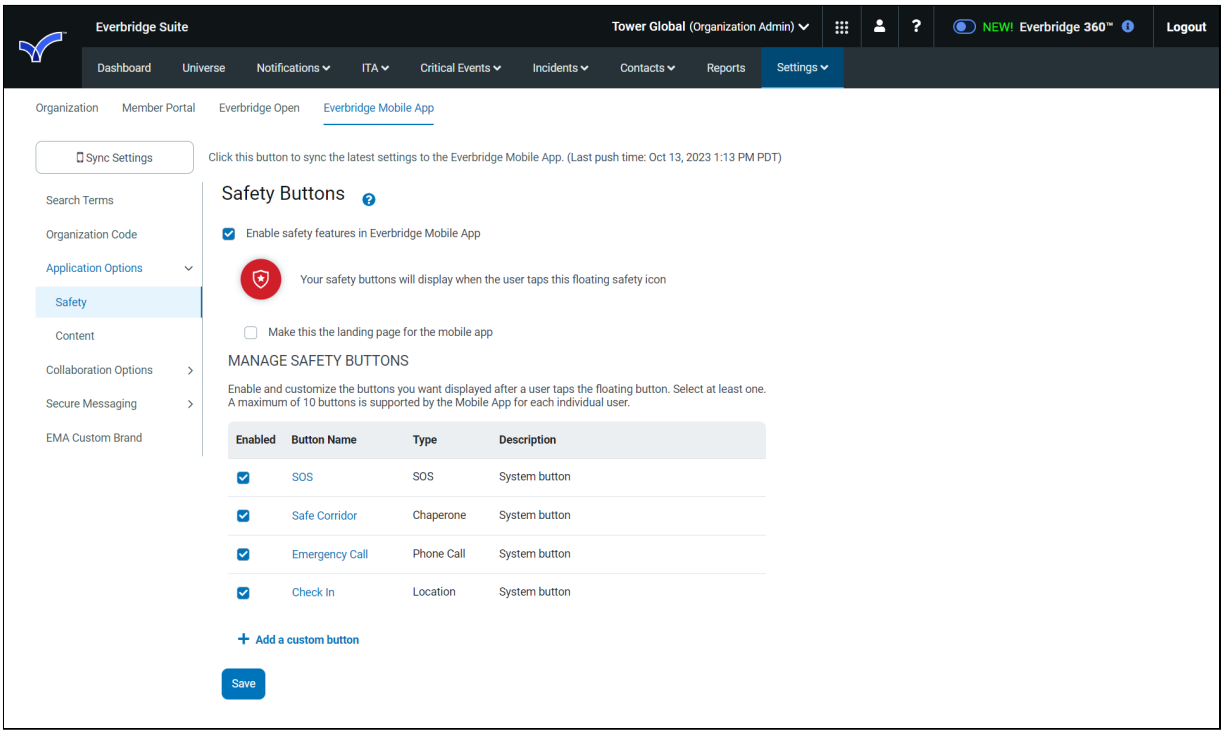


Application Options

Safety

Use this option to enable the **Safety Connection** features that will be available in the Everbridge Mobile App. For more details about Safety Connection, see the *Safety Connection User Guide*.

> **NOTE:** The maximum number of Safety buttons is 60 (including system buttons and custom buttons). The minimum number of Custom buttons is 4, the maximum number of Custom buttons is 60, where the default value is 25 (including System buttons and Custom buttons). A maximum of 10 buttons can be shown on the Everbridge Mobile App (including System buttons and Custom buttons).



Four default Safety buttons are available in Everbridge Mobile App:

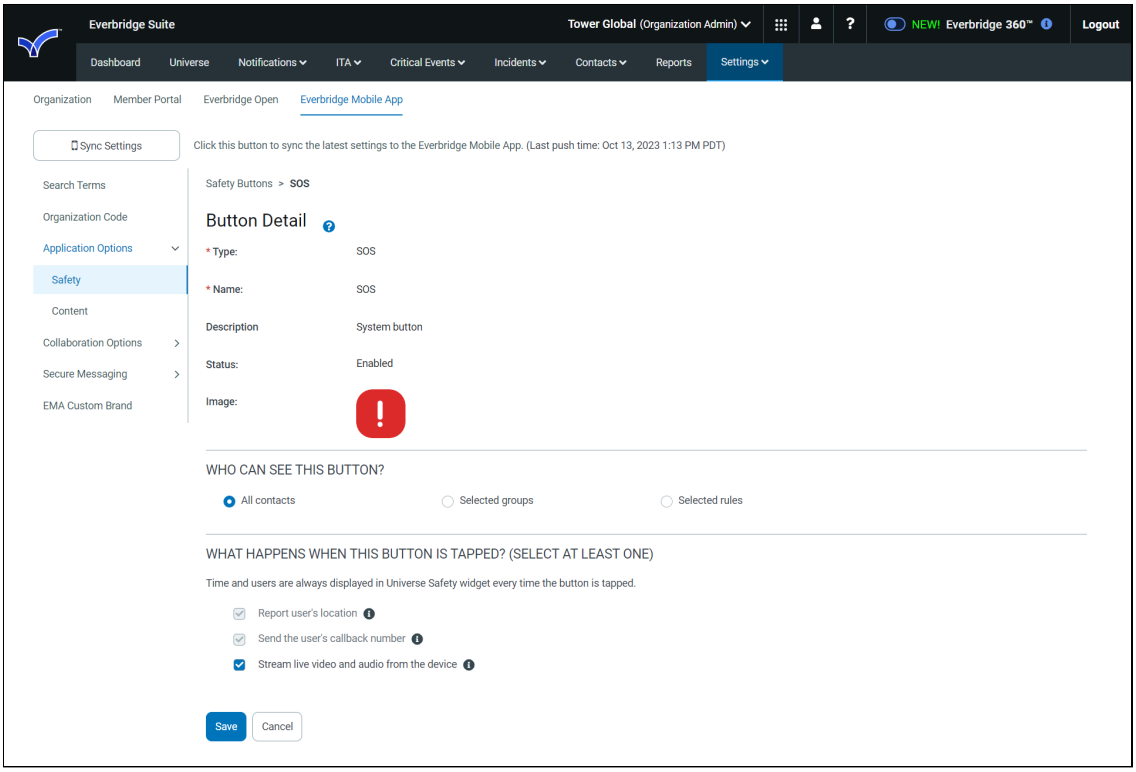
- **Check In** - Everbridge Mobile App users can voluntarily check in and report their location when, for instance, they feel they are in a potentially dangerous situation.

- **Safe Corridor** - Everbridge Mobile App users are asked to enter a preset code at regular time intervals. A missed report triggers an alert.
- **SOS** - This button triggers an SOS Alert. The recording of video and audio from the mobile device can be automatically started when this button is tapped.
- **Emergency Call** - This bridges the Everbridge Mobile App to a preset phone number.

Enable Safety Buttons

1. Navigate to **Settings** > **Everbridge Mobile App** > **Application Options** > **Safety** and make sure the checkbox: **Enable safety feature in Everbridge Mobile App.**
2. In the Everbridge Mobile App, the **Safety buttons** page is available when tapping the floating Safety icon. Optionally, select the checkbox: Make this the landing page for the mobile app. If this checkbox is selected:
   - The Mobile App will use the Safety Buttons page as the default page when the application starts.
   - After a period of inactivity of 15 minutes in the background, the Mobile App will automatically display that page when the app is in the foreground.

   If this checkbox is clear, Mobile App users will need to click to tap the floating Safety icon to access the Safety buttons page.
3. Enable any of the four default Safety buttons: SOS, Safe Corridor, Emergency Call, and Check-In by selecting the corresponding checkbox in the Enabled column.
4. Access the detailed configuration page of the button by clicking the button name. For example, see the SOS Button Detail page.



5. For any button that has been enabled, the contacts that can view or use the button the Everbridge Mobile App can be set in the *Who can see this button?* section. There are three mutually exclusive possibilities:
    - **All Contacts** - Any contact who has access to the Everbridge Mobile App will be able to use the button.
    - **Selected Groups** - One or more groups of contacts can be selected. At least one group must be selected. Only contacts who belong in the selected group(s) will be able to use the button.
    - **Selected Rules** - One or more rules can be selected. At least one rule must be selected. Only contacts who match the rule(s) definitions will be able to use the button.
6. Adjust the properties on each button. See Button Properties available for each button in the table below.
7. Click **Save** when done.

Configure Custom Safety Buttons

In addition to these four default Safety buttons, custom Safety buttons can be created. To do this:

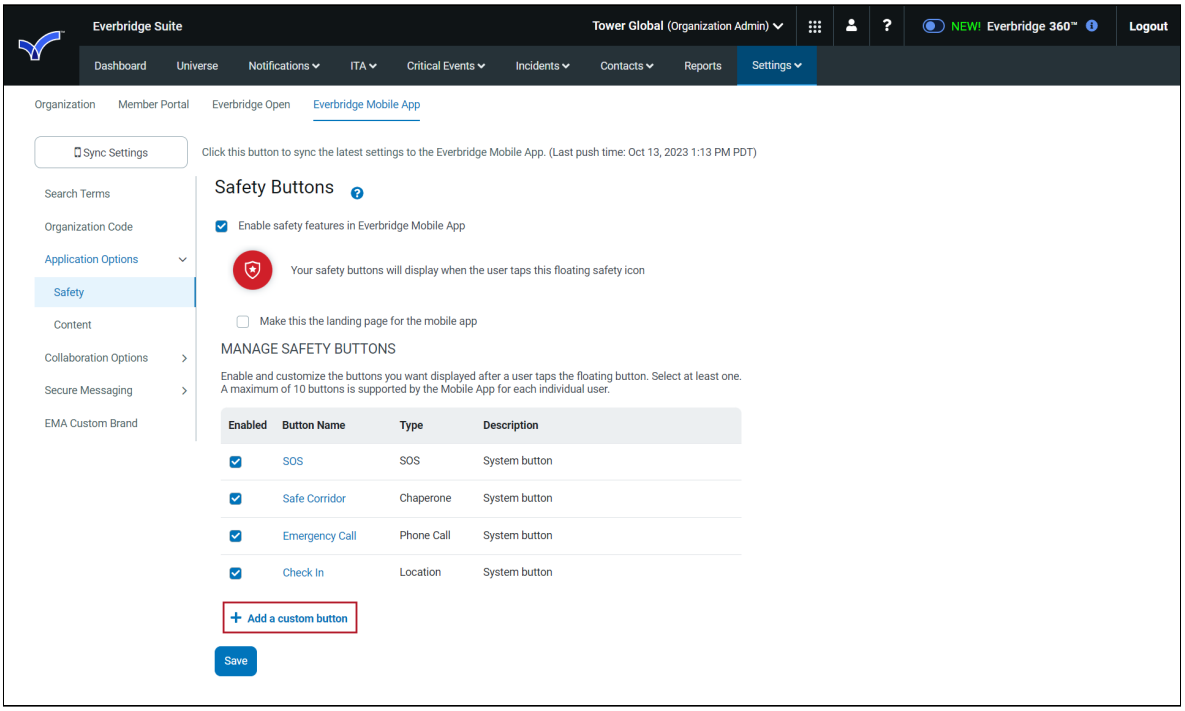
1. Navigate to **Settings** > **Everbridge Mobile App** > **Application Options** > **Safety** and make sure the **Enable safety feature in Everbridge Mobile App** checkbox is selected.

2. In the Everbridge Mobile App, the Safety Buttons page is available when tapping the floating Safety icon. Optionally, select the Make this the landing page for the mobile app checkbox.

   If this checkbox is clear, Mobile App users will need to click to tap the floating Safety icon to access the Safety buttons page.

   - The mobile app will use the Safety buttons page as the default page when the application starts.
   - After a period of inactivity of 15 minutes in the background, the Mobile App will automatically display that page when the app is in the foreground.

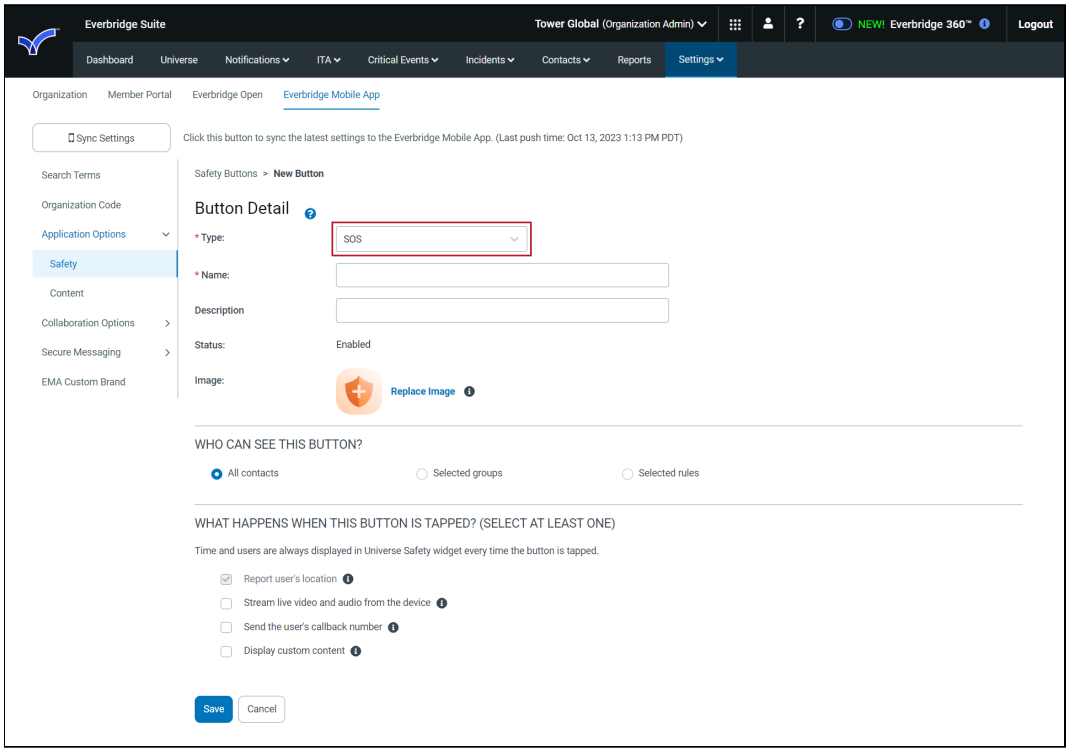
3. Click **Add a custom button**.



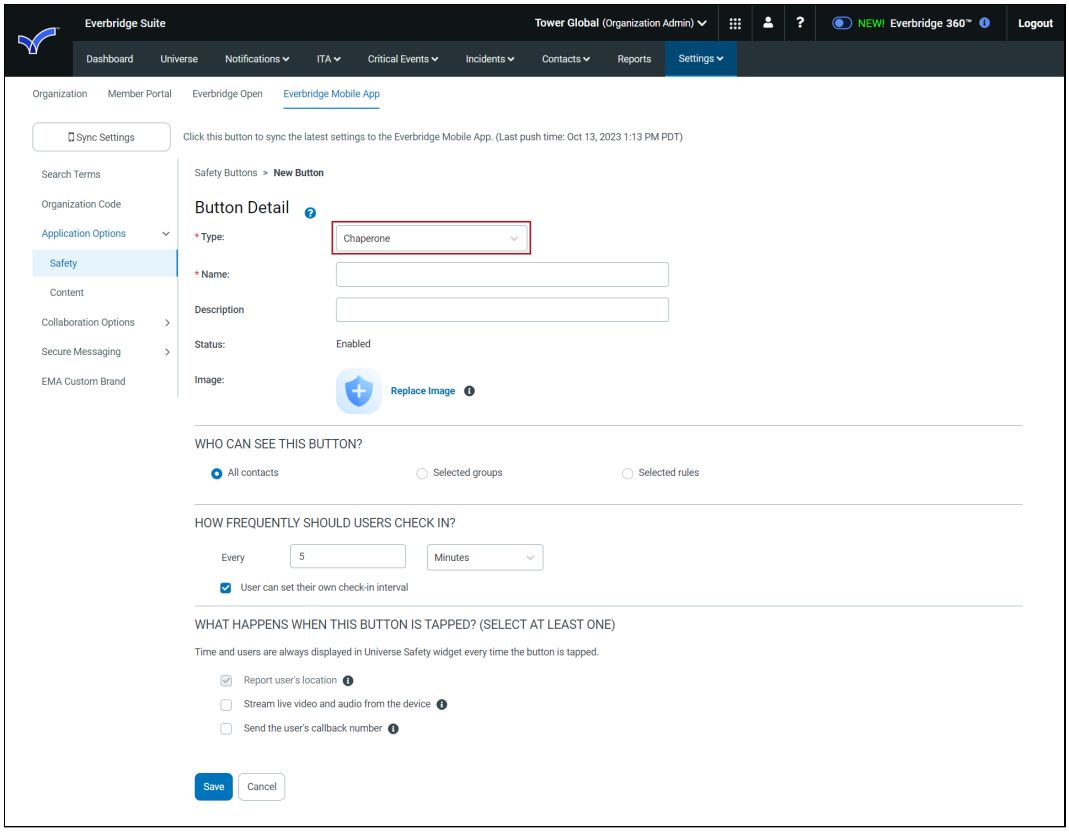
4. The **Button Detail** page appears. Select the button type from the drop-down list.
   - **SOS** - Trigger a SOS action.
   - **Chaperone** - Trigger a Chaperone/Safe Corridor action.
   - **Phone Call** - Trigger a phone call. There are about 240 countries from which to configure, including support phone numbers belonging to those countries.
   - **Location** - Trigger a check-in action.
   - **Content** - When the button is tapped, a Content page is displayed on the mobile device. This action is not visible on the Universe page and cannot trigger a threshold.
   - **Custom Form** - When the button is tapped, a questionnaire is displayed. When submitted, an Incident report is triggered.

- **Hyperlink** - When the button is tapped, the default web browser opens using the hyperlink value.

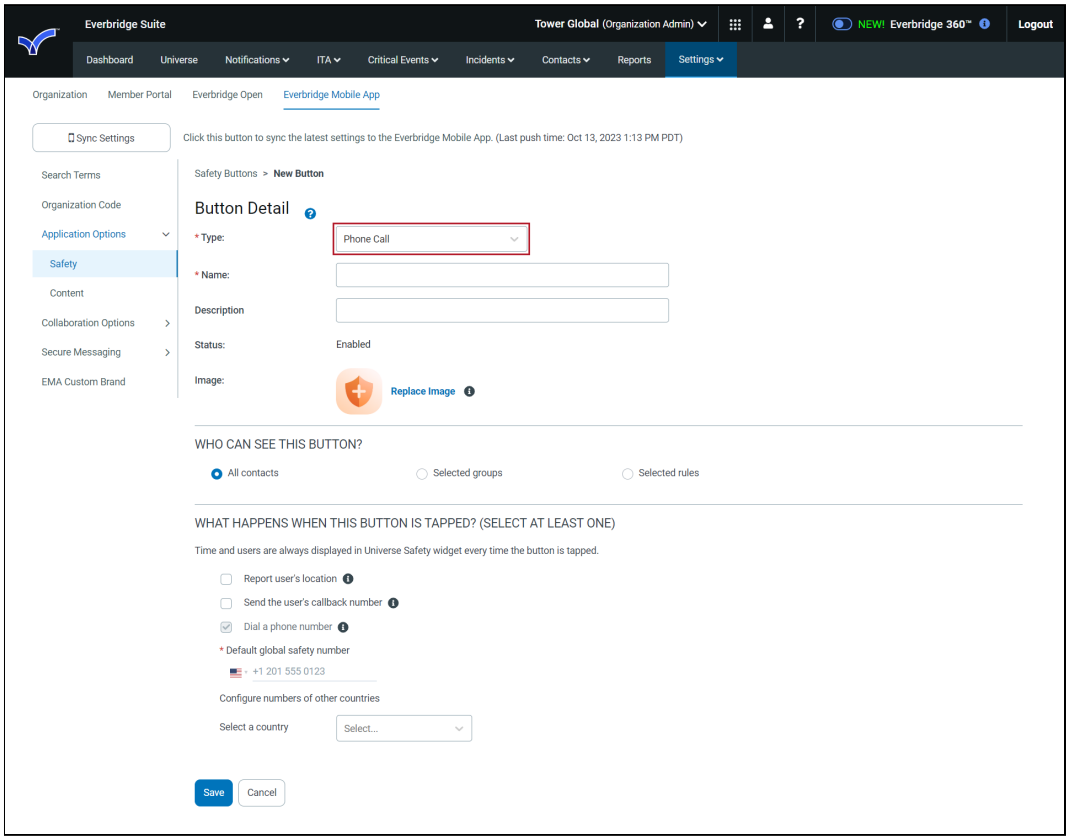
5. See the following example Button Detail pages for each button type.
   - SOS



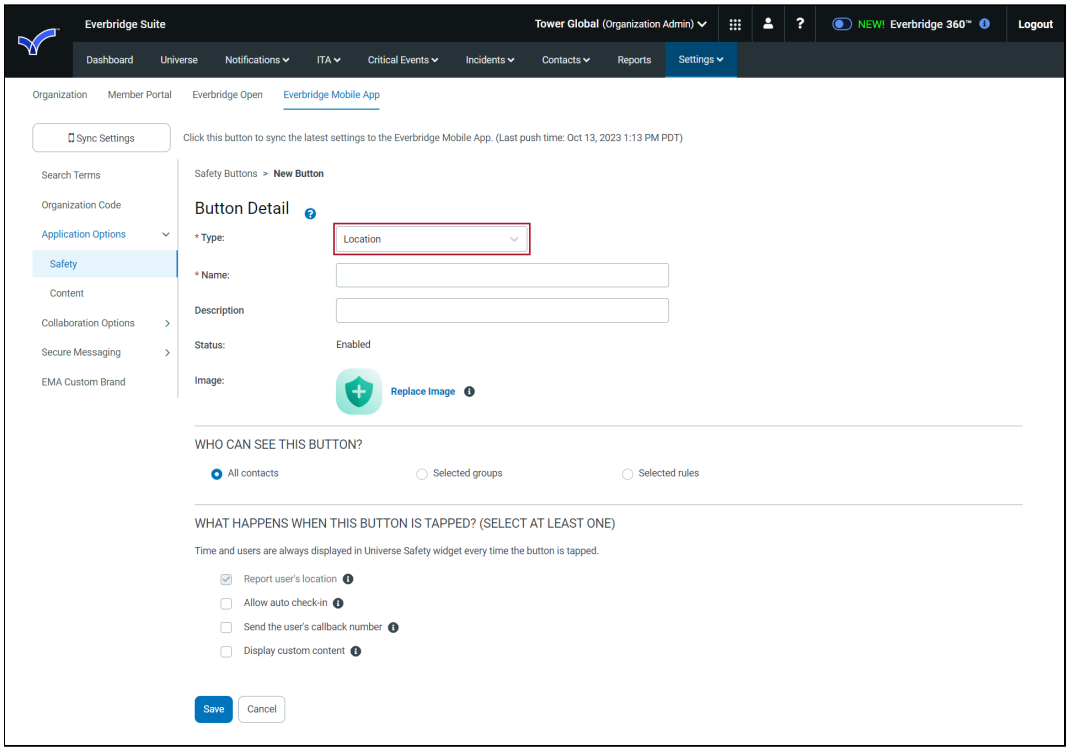
   - Chaperone


Everbridge Suite
Tower Global (Organization Admin)
NEW! Everbridge 360™
Logout
Dashboard
Universe
Notifications
ITA
Critical Events
Incidents
Contacts
Reports
Settings
Organization
Member Portal
Everbridge Open
Everbridge Mobile App
Sync Settings
Click this button to sync the latest settings to the Everbridge Mobile App. (Last push time: Oct 13, 2023 1:13 PM PDT)
Search Terms
Organization Code
Application Options
Safety
Content
Collaboration Options
Secure Messaging
EMA Custom Brand
Safety Buttons > New Button
Button Detail
* Type:
Chaperone
* Name:
Description
Status:
Enabled
Image:
Replace Image
WHO CAN SEE THIS BUTTON?
All contacts
Selected groups
Selected rules
HOW FREQUENTLY SHOULD USERS CHECK IN?
Every
5
Minutes
User can set their own check-in interval
WHAT HAPPENS WHEN THIS BUTTON IS TAPPED? (SELECT AT LEAST ONE)
Time and users are always displayed in Universe Safety widget every time the button is tapped.
Report user's location
Stream live video and audio from the device
Send the user's callback number
Save
Cancel

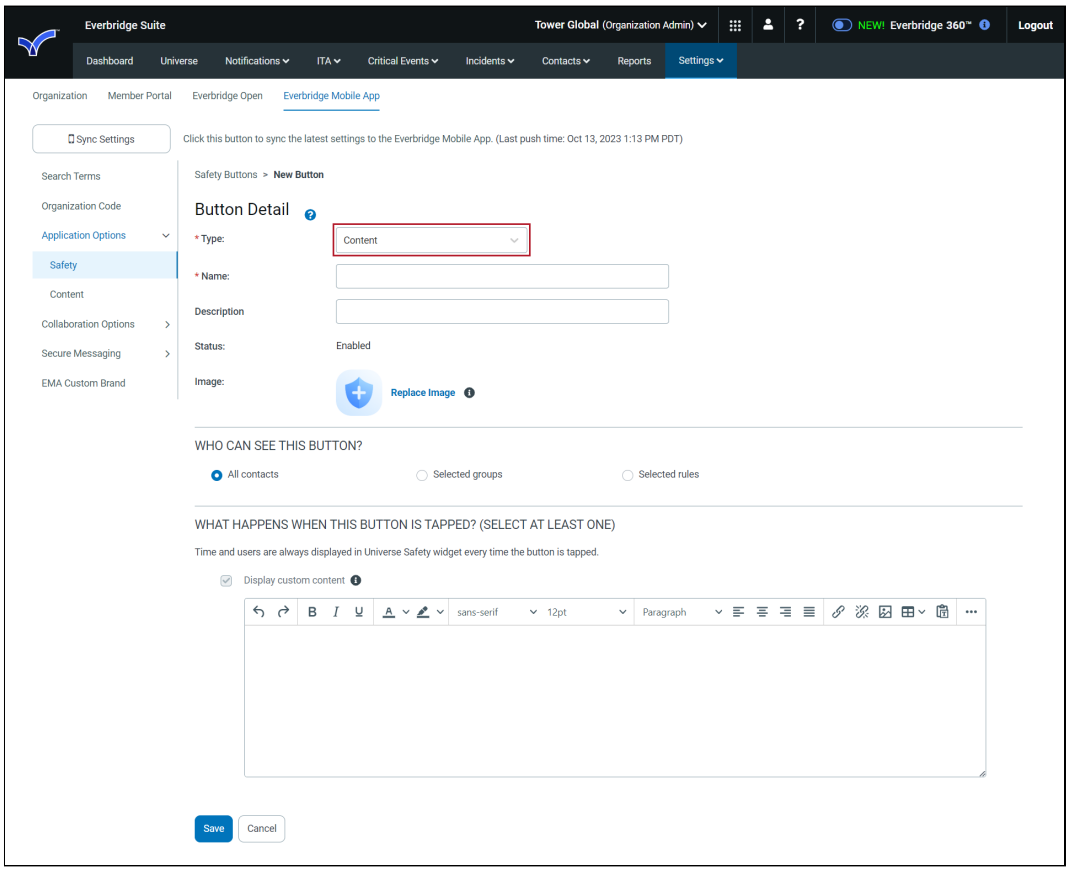
- Phone Call


Everbridge Suite
Tower Global (Organization Admin)
NEW! Everbridge 360™
Logout
Dashboard
Universe
Notifications
ITA
Critical Events
Incidents
Contacts
Reports
Settings
Organization
Member Portal
Everbridge Open
Everbridge Mobile App
Sync Settings
Click this button to sync the latest settings to the Everbridge Mobile App. (Last push time: Oct 13, 2023 1:13 PM PDT)
Search Terms
Organization Code
Application Options
Safety
Content
Collaboration Options
Secure Messaging
EMA Custom Brand
Safety Buttons > New Button
Button Detail
* Type:
Phone Call
* Name:
Description
Status:
Enabled
Image:
Replace Image
WHO CAN SEE THIS BUTTON?
All contacts
Selected groups
Selected rules
WHAT HAPPENS WHEN THIS BUTTON IS TAPPED? (SELECT AT LEAST ONE)
Time and users are always displayed in Universe Safety widget every time the button is tapped.
Report user's location
Send the user's callback number
Dial a phone number
* Default global safety number
+1 201 555 0123
Configure numbers of other countries
Select a country
Select...
Save
Cancel

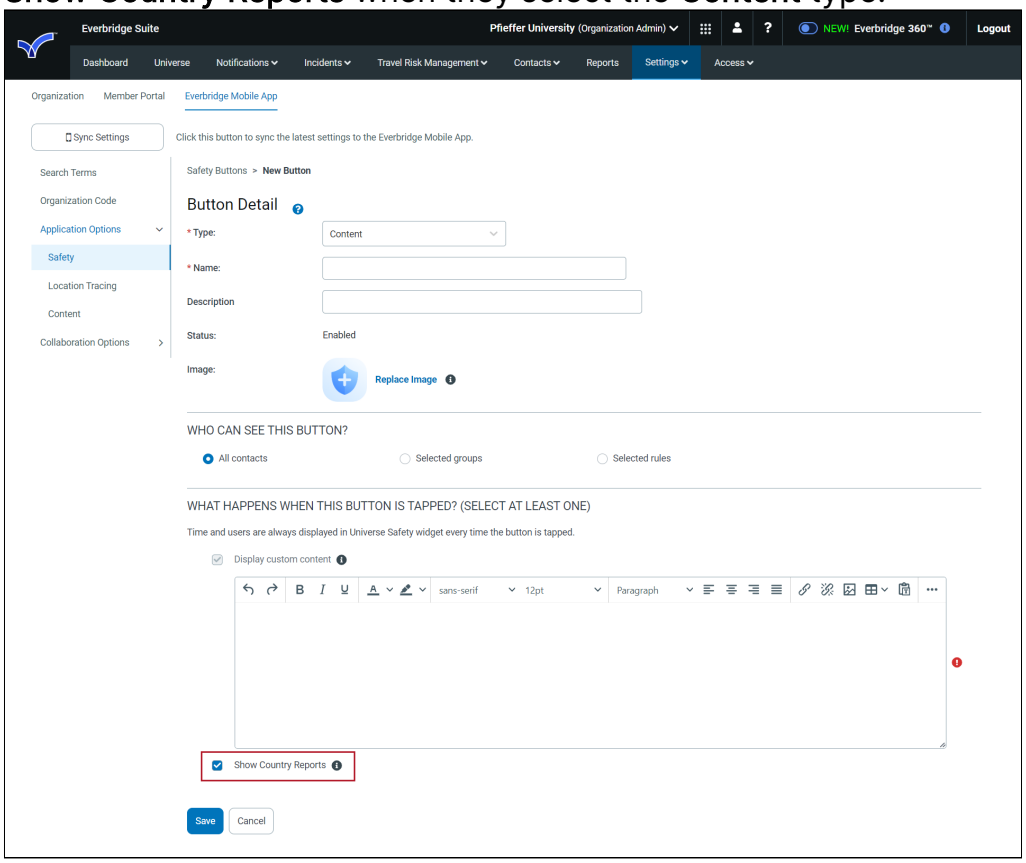
- Location



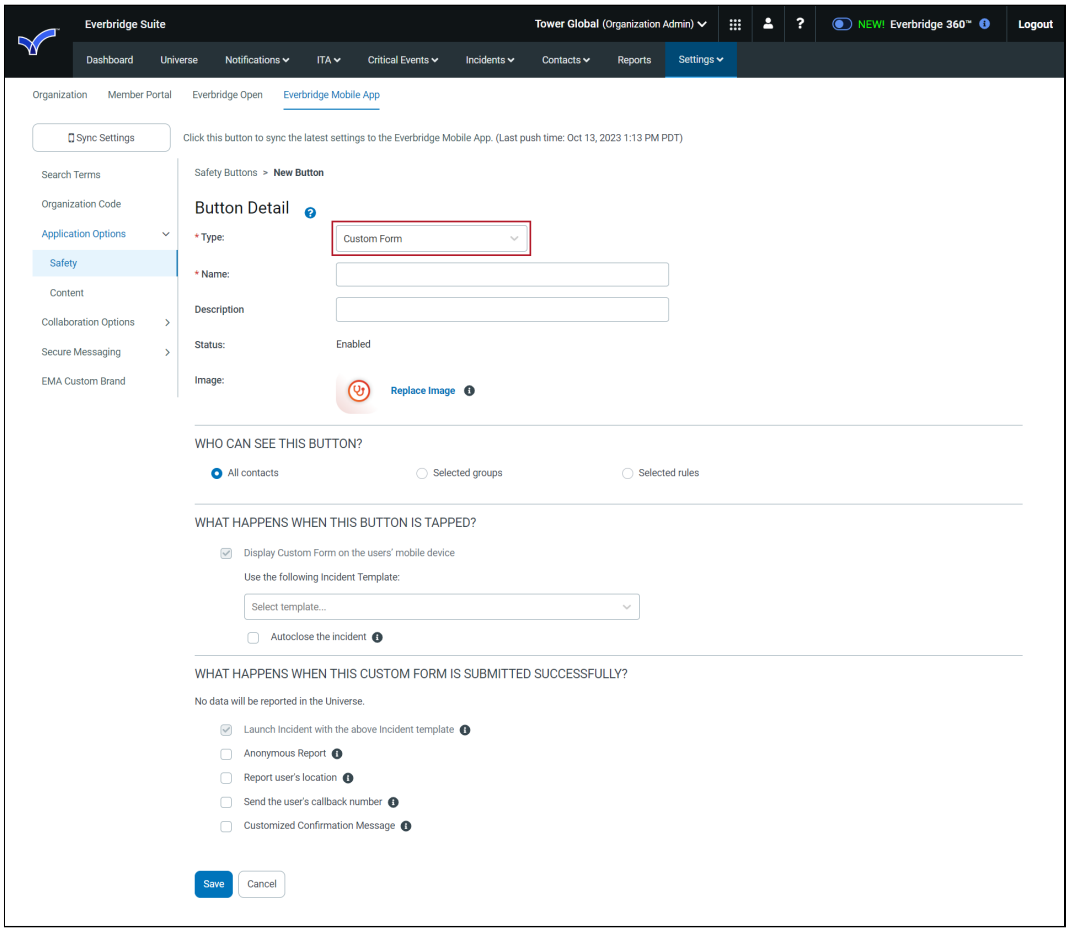
- Content



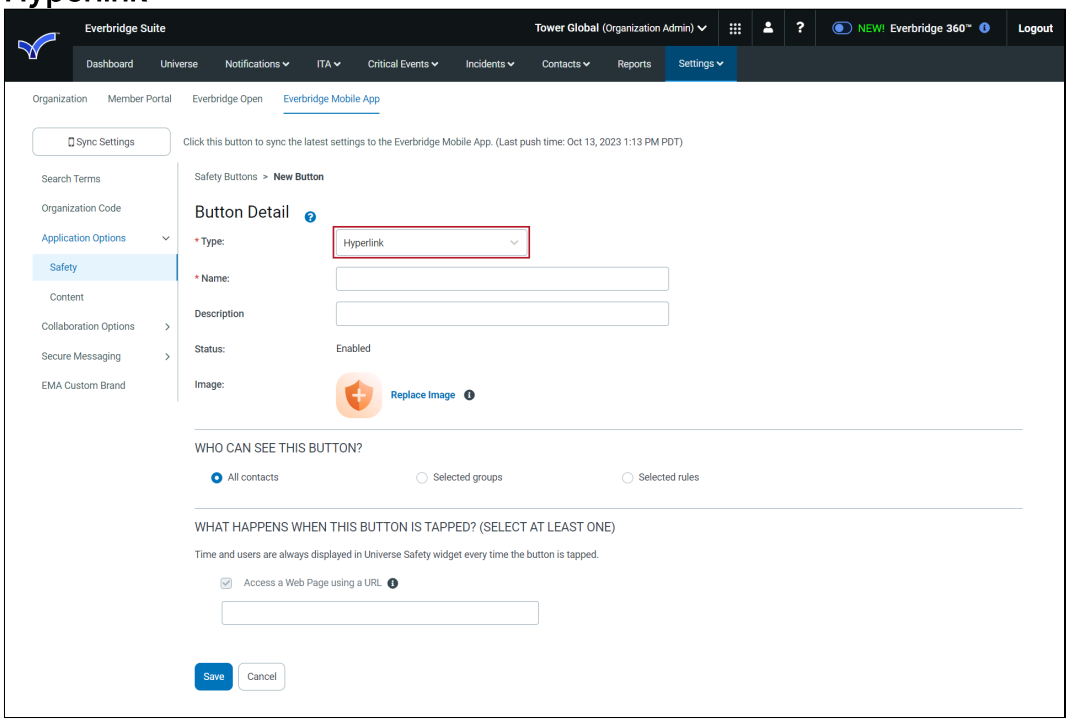
- Travel Protector customers will also see an additional option titled **Show Country Reports** when they select the **Content** type.



- Custom Form


Everbridge Suite
Tower Global (Organization Admin)
NEW! Everbridge 360™
Logout
Dashboard
Universe
Notifications
ITA
Critical Events
Incidents
Contacts
Reports
Settings
Organization
Member Portal
Everbridge Open
Everbridge Mobile App
Sync Settings
Click this button to sync the latest settings to the Everbridge Mobile App. (Last push time: Oct 13, 2023 1:13 PM PDT)
Search Terms
Organization Code
Application Options
Safety
Content
Collaboration Options
Secure Messaging
EMA Custom Brand
Safety Buttons > New Button
Button Detail
* Type:
Custom Form
* Name:
Description
Status:
Enabled
Image:
Replace Image
WHO CAN SEE THIS BUTTON?
All contacts
Selected groups
Selected rules
WHAT HAPPENS WHEN THIS BUTTON IS TAPPED?
Display Custom Form on the users' mobile device
Use the following Incident Template:
Select template...
Autoclose the incident
WHAT HAPPENS WHEN THIS CUSTOM FORM IS SUBMITTED SUCCESSFULLY?
No data will be reported in the Universe.
Launch Incident with the above Incident template
Anonymous Report
Report user's location
Send the user's callback number
Customized Confirmation Message
Save
Cancel

- **Hyperlink**



6. Once the type has been selected, enter a name and an optional description.
7. Optionally, click **Replace image** to upload a different image used on the Everbridge Mobile App. The recommended size for images is 256x256 pixels.
8. For any button that has been enabled, the contacts that can view or use the button in the Everbridge Mobile App can be set in the **Who can see this button?** section. There are three mutually exclusive possibilities:
    - **All Contacts** - Any contact who has access to the Everbridge Mobile App will be able to use the button.
    - **Selected groups** - One or more groups of contacts can be selected. At least one group must be selected. Only contacts who belong to the selected group(s) will be able to use the button.
    - **Selected Rules** - One or more rules can be selected. At least one rule must be selected. Only contacts who match the rule(s) definitions will be able to use the button.
9. Adjust the properties on each button. See Button Properties available for each button.
10. Click **Save** when done.

Button Properties

Property	System Buttons	Custom Buttons
Allow auto check-in. When selected, it is enabled and cannot be cleared. Auto check-in	Check-In	Location

will always put into the Safety Settings when using the default Check-In button.		
Report User's location. The user's location is reported to the server and used: • In the Universe to locate the position of the event (SOS, Safe Corridor) • In the Safety threshold as a criteria **NOTE:** For default buttons, custom Location, custom Chaperone, and custom SOS buttons, this option cannot be cleared.	SOS Safe Corridor Emergency Call Check-In	SOS Chaperone Phone Call Location Self-Report Custom Form
Send the user's callback number. The callback number is a setting of the Everbridge Mobile App that can be manually set by the Mobile App user. If set, this information is brought back to the server when the button is tapped and displayed on the Universe page. NOTE: For default buttons, this option cannot be cleared.	SOS Safe Corridor Emergency Call	SOS Chaperone Phone Call Location Custom Form
Stream live video and audio from the device. If selected, video and audio recording will start when the button is tapped on the mobile device and streamed to the server. The video with audio will be available from the Universe page.	SOS	SOS Chaperone
Dial a phone number. When the button is tapped, a call will be made. A global safety number must be entered. Up to 20 additional numbers can be set on a country-by-country basis. If the device is in a country for which a number has been set, that number will be dialed. If the device is in a country for which no specific number has been set, the global safety number will be used.	Emergency Call	Phone Call
Use the following Incident Template. An Incident template is attached to the custom button. Once tapped, a questionnaire made of the Incident template variables will be		Self-Report Custom Form

displayed to the Everbridge Mobile App users. Once submitted, the Incident will be triggered with the variables filled with the answers to the questionnaire.		
Autoclose the Incident. Automatically close the Incident after the notification goes out. This option is the equivalent of the "CLOSE Incident after successful send" option available on Incidents.		Self-Report Custom Form
Anonymous Report. This option will hide all the information related to the Everbridge Mobile App users using the button. Their information will not be available in the Manager Portal.		Custom Form
How frequently should users check in? The safe corridor Check-in interval can be set in minutes or seconds. This interval is the maximum time allowed for Everbridge Mobile App users to enter the preset code once they have tapped the Safe Corridor button and started the feature on their device. The default value is 5 minutes. Past this time, an alert will be generated.	Safe Corridor	Chaperone
Display custom content. This option enables the display of content in the Everbridge Mobile App when the button is tapped.	Content	SOS Location Content Self-Report Custom Form
Show Country Reports. When selected, this option enables the display of a search page under the custom content in the Everbridge Mobile App when the button is tapped.		Content

Contact Tracing

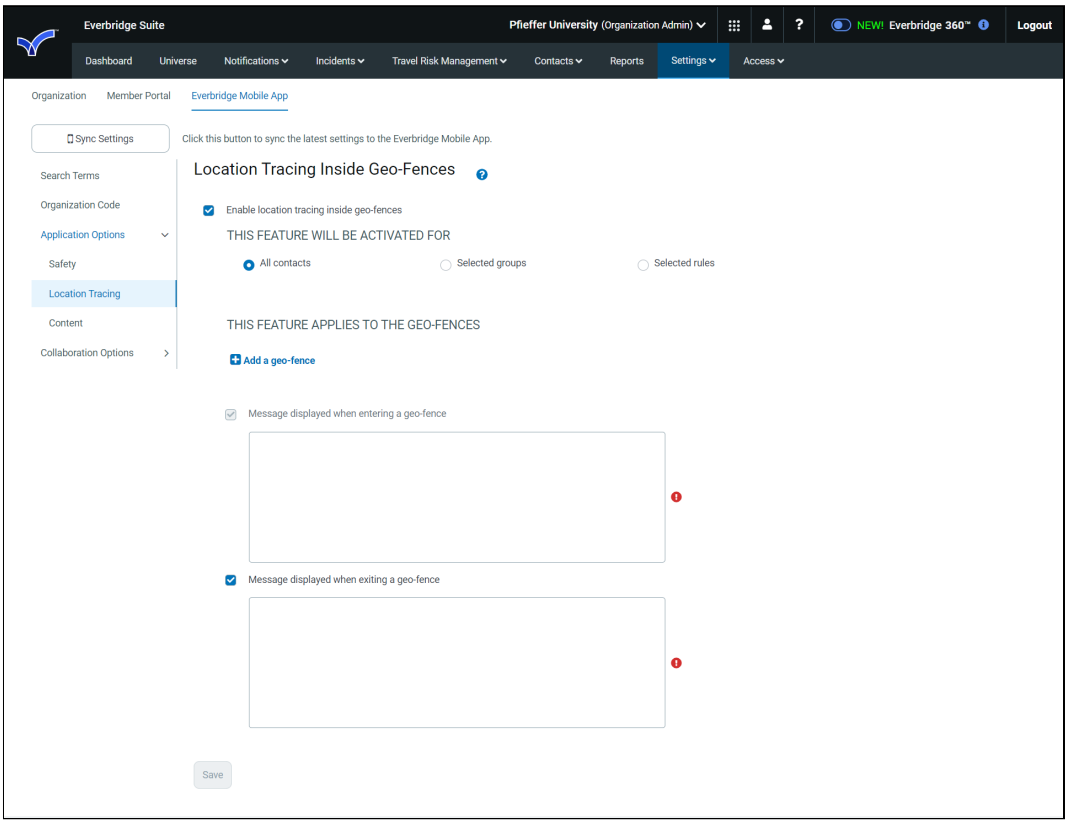
This page enables the activation of proximity-based contact tracing. Select the checkbox of the items you want or enter the required values.

- **Enable Mobile App Bluetooth Proximity Tracing** - This will activate the feature on all devices installed with the Everbridge Mobile App.
- **This feature will be activated for** - Select the radio button corresponding to the contacts you want activated for contact tracing.

- **Enable app to notify mobile users after Exposure Events** - Once a contact has self-reported positive, contacts that are at risk, identified through the proximity tracing feature will be notified. The text of the notification can be entered below the checkbox.
- **Trigger Incident after Exposure Events** - For each contact that is at risk, identified through the proximity tracing feature, an Incident will be triggered using the selected template. Optionally, the Incident can be automatically closed as soon as the notification goes out.

Location Tracing

Create geo-fences and automatically get detailed location information when contacts are within these geo-fences. The privacy of the contacts is preserved as their location data is not exposed outside the predefined geo-fence. A push notification is always sent to contacts when they enter such geo-fences.

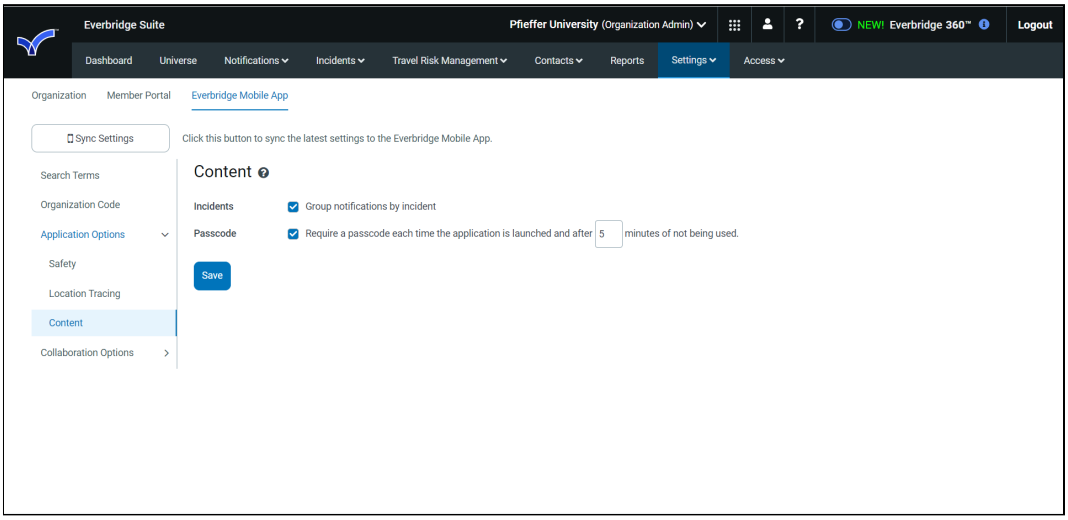


Content

Select the checkbox of the items you want.

- **Incidents** - Group notifications by Incident
- **Subscriptions** - Allow subscribers to be anonymous

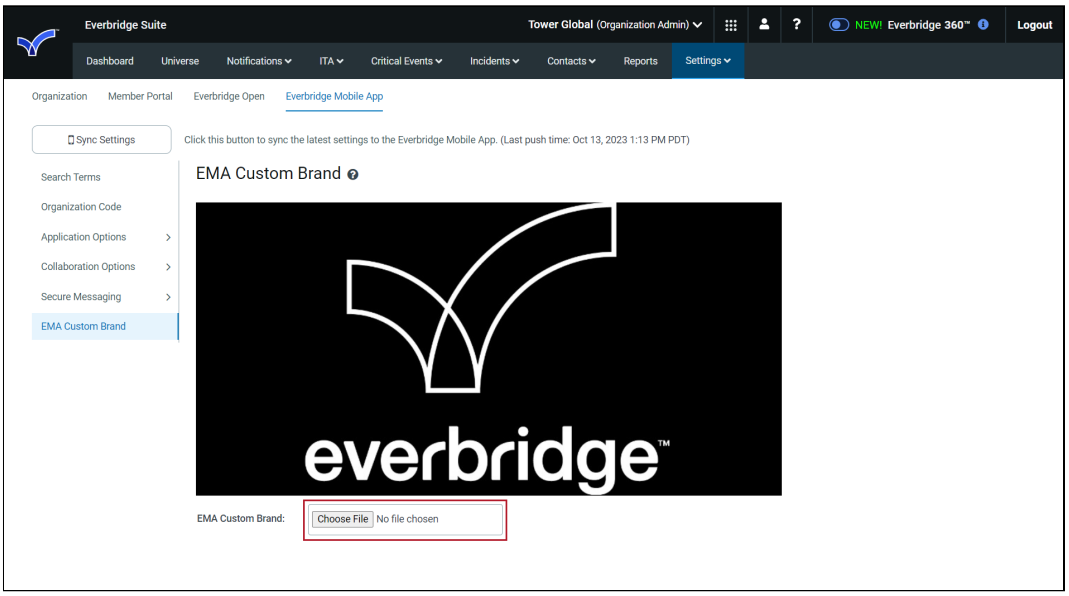
- **Passcode** - Require a passcode each time the application is launched and after a time (in minutes) of not being used. You can change the time from 5 minutes.



EMA Custom Brand

If enabled for your Organization by Support, you can choose a custom Everbridge Mobile App (EMA) banner. The image must be **840 x 420** with a ratio of width to height 2:1.

If you want to change your custom brand, click **Choose File** and select the new image. Click **Save** when you are done.



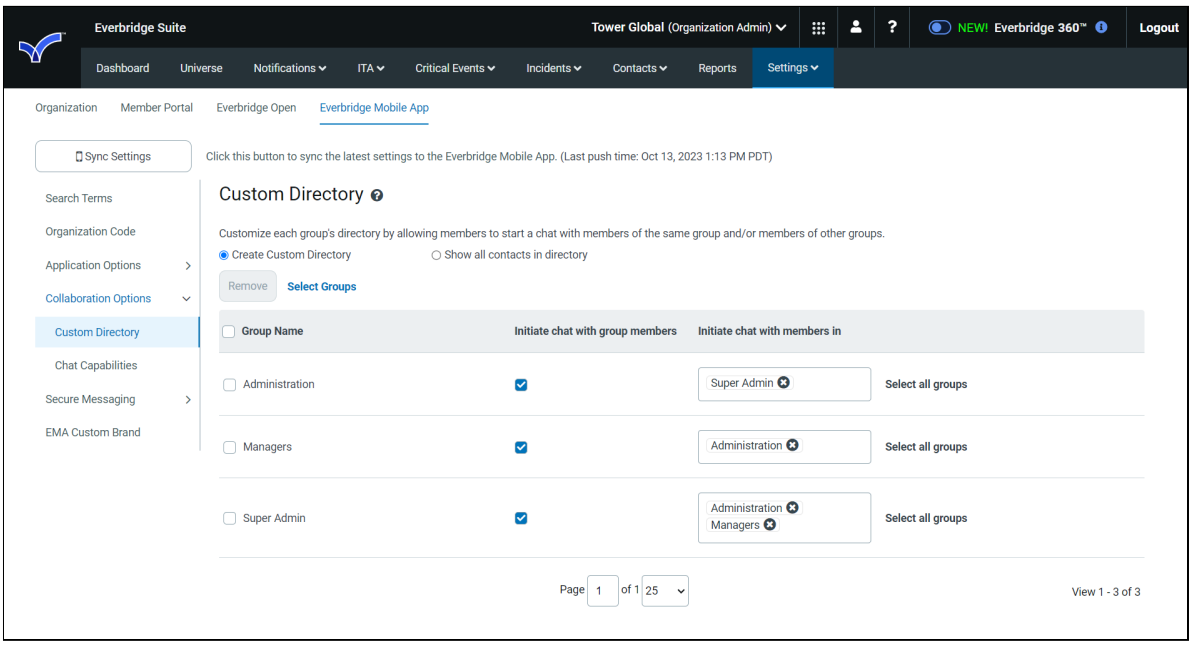
Collaboration Options

Custom Directory

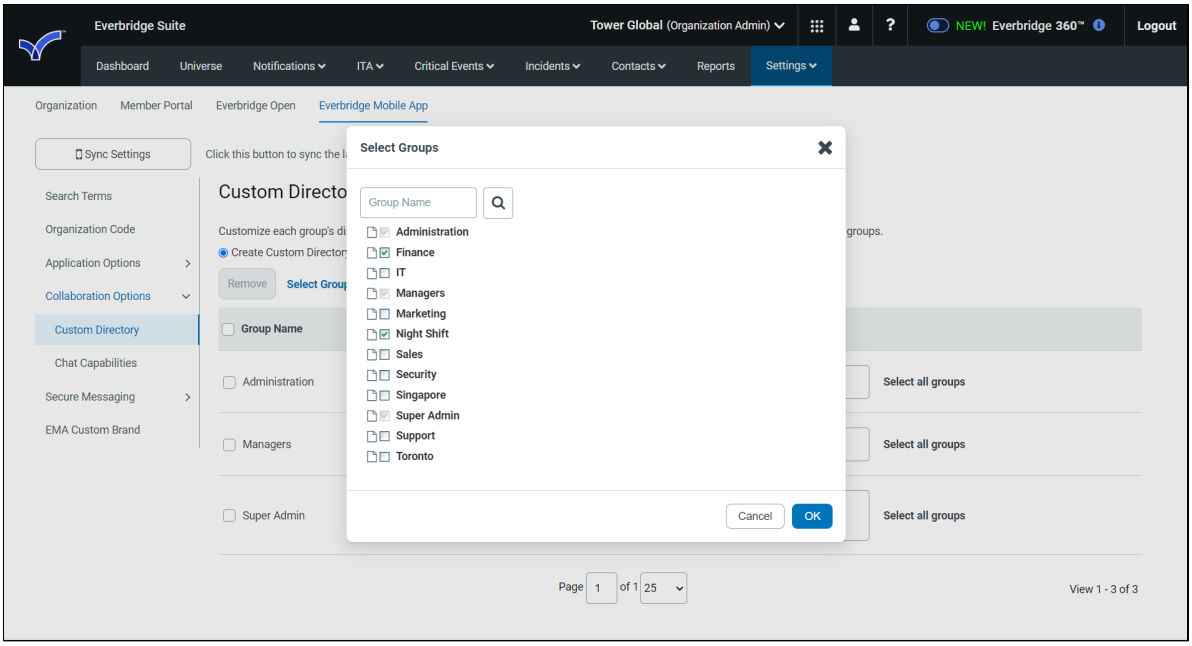
As an Administrator, you can decide if your contacts can view all other contacts in their directory, or you can create custom directories to limit your contacts by group.

Start by choosing which groups should have or be in a directory, then decide if they see other members of the same group in their directory and/or members of other groups in their directory.

A contact can start a chat with anyone in their directory and can choose up to 100 contacts for a single group chat.



When creating a Custom Directory, first, select the groups whose members should have and/or be in a directory.



Then, decide what contacts should be in each group directory, and specify which groups can initiate chats with one another.

- **Initiate chat with group members** - All members of the group can start a chat with each other of the same group.
- **Initiate chat with members in** - Members of the group can start a chat with members in selected groups.

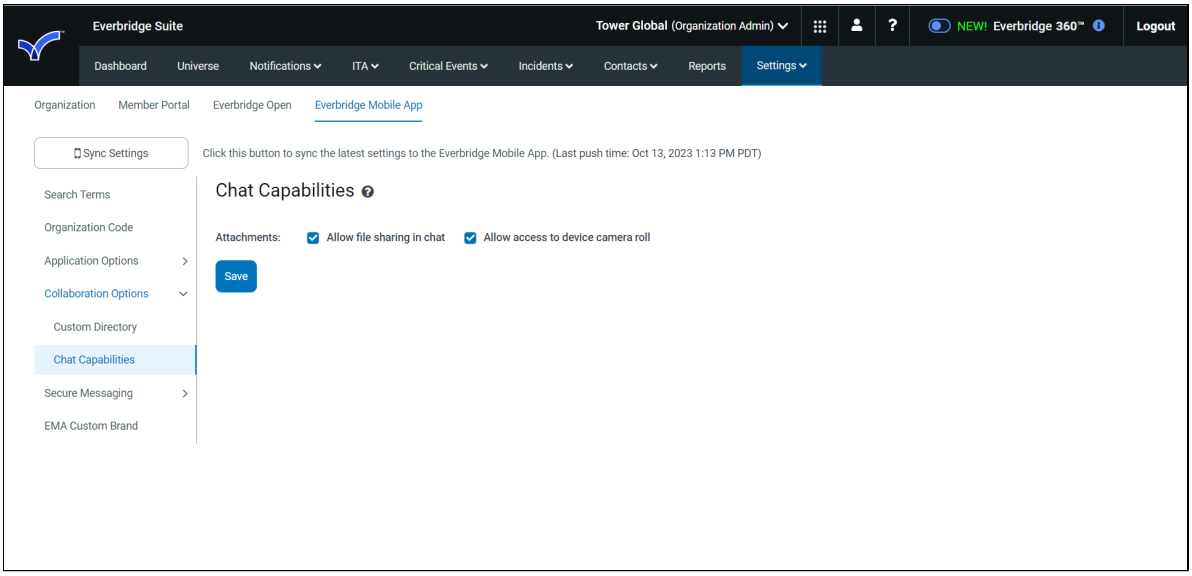
To remove a Custom Directory, select the checkbox next to the group in the **Group Name** field, and click **Remove**. Once removed, members of that group will be unable to chat using the Everbridge Mobile App because they will not have a directory or be in other contacts' directories.

NOTE: When you delete contacts or add/remove directories, it might take up to 10 minutes to sync changes on the Everbridge Mobile App. The sync can be forced within those 10 minutes by logging out and back into the Everbridge Mobile App.

Chat Capabilities

Select the attachments you want in your chat capabilities:

- Allow file sharing in chat
- Allow access to the device camera roll. From the Video Chat field, select the Enable Video Chat checkbox if applicable.


Everbridge Suite
Tower Global (Organization Admin)
NEW! Everbridge 360™
Logout
Dashboard
Universe
Notifications
ITA
Critical Events
Incidents
Contacts
Reports
Settings
Organization
Member Portal
Everbridge Open
Everbridge Mobile App
Sync Settings
Click this button to sync the latest settings to the Everbridge Mobile App. (Last push time: Oct 13, 2023 1:13 PM PDT)
Search Terms
Organization Code
Application Options
Collaboration Options
Custom Directory
Chat Capabilities
Secure Messaging
EMA Custom Brand
Chat Capabilities
Attachments:
Allow file sharing in chat
Allow access to device camera roll
Save

Secure Messaging

Secure Messaging is visible only if it is enabled for your organization. It provides compliance with industry regulations such as HIPAA (Health Insurance Portability and Accountability Act). This means hospitals and other healthcare clients can use the Everbridge Mobile application for their Secure Messaging needs, for example.

Enabling Secure Messaging

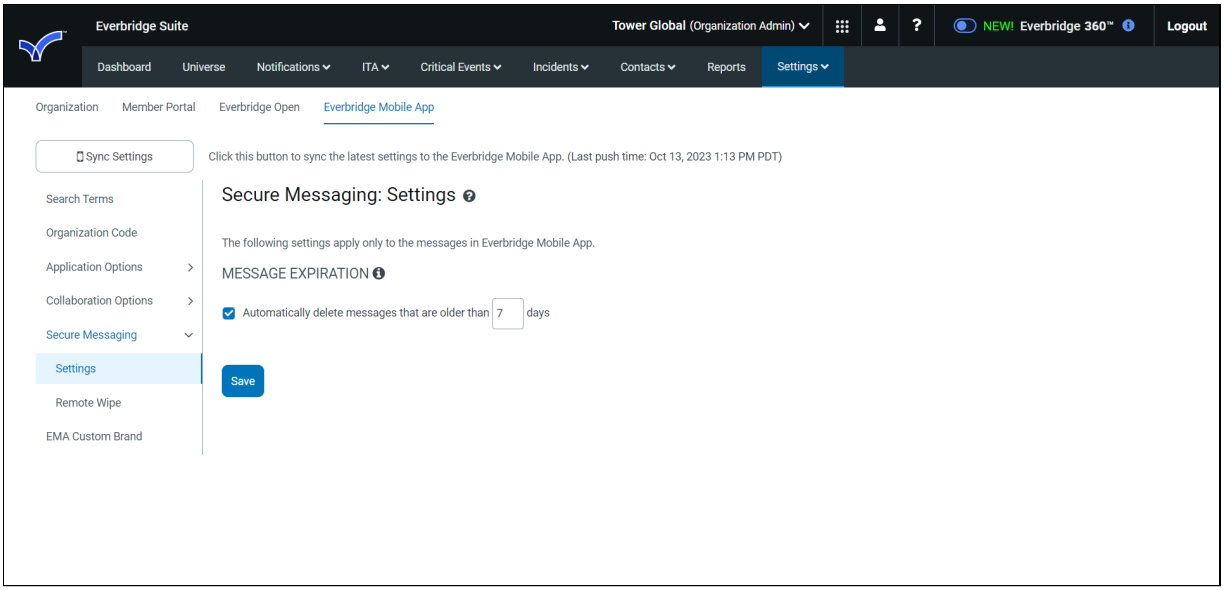
To enable a Secure Messaging user to receive Notifications:

1. Add the user to the organization as a Contact. Secure Messaging Users are not Contacts until you add them.
2. Send the contact a Member Portal Registration Invitation. The contact joins the Member Portal with a unique username/password and then uses it to log in.

> **NOTE:** To receive Notifications, the users must be logged in with their Member credentials for the organization. Alternatively, the users may sign in with their Single Sign-On (SSO) credentials. Or, the users can be sent a Quick Registration invitation where they tap on the link in the email from their mobile device, which launches the app and walks them through the registration process in the app itself.

Settings

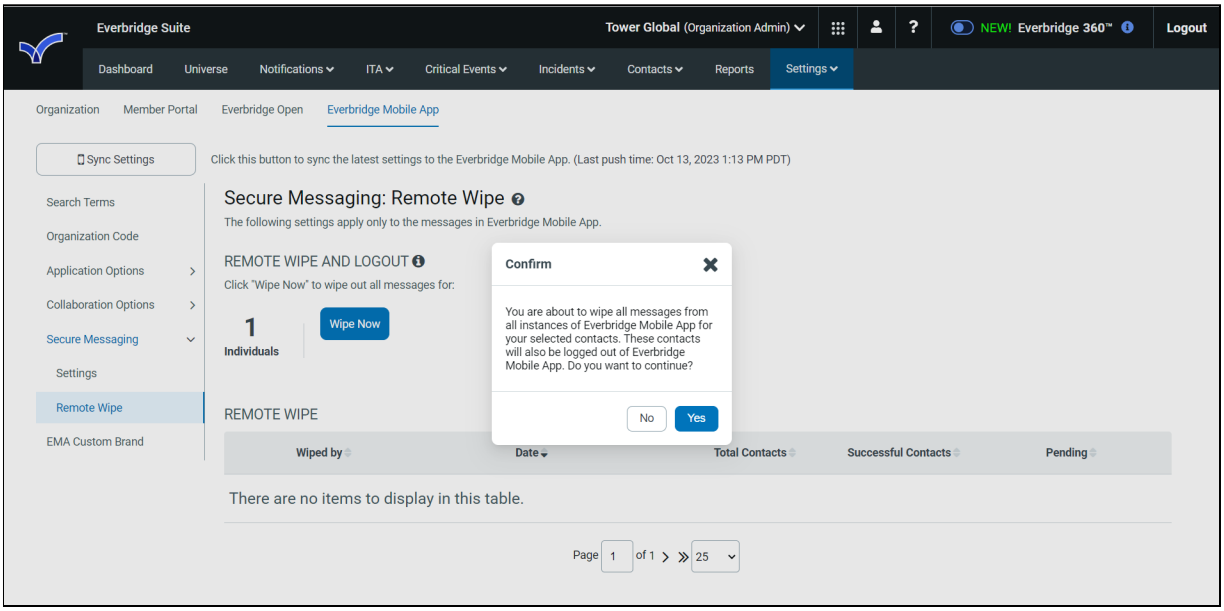
The Secure Messaging settings apply only to the messages in the Everbridge Mobile application. The **Message Expiration** feature removes all messages sent to and from the Everbridge Mobile application after the message has been stored on all Everbridge Mobile applications for the specified period of time. (Select the checkbox and enter a value of 1-180 days.)



Remote Wipe

The **Remote Wipe and Logout** feature wipes out all messages sent to and from the Everbridge Mobile app for the contacts you select. These contacts will also be logged out of the Everbridge Mobile App and will need to enter their user names and passwords again in order to receive new messages.

Select your contacts and click **OK**. Then, select the **Wipe Now** button, and click **OK** to confirm that the messages will be wiped out, and that the contacts will also be logged out of the Everbridge Mobile app. Then, click **Sync Settings** at the top of the left-hand menu.



The **Successful Contacts** column shows the number of messages that were wiped. The **Pending** column shows the number of messages that are yet to be wiped. That is, the mobile device might be off or the Everbridge Mobile app might not be launched.