



OnSolve Platform

Administrator Guide

For Accounts with the New Groups Flow

Version 8.3 | December 2023



OnSolve Platform

Administrator Guide

For Accounts with the New Groups Flow

Version 8.3

December 2023

© 2023 OnSolve, LLC. All rights reserved.

6240 Avalon Blvd.
Alpharetta, GA 30009

onsolve.com

– Proprietary & Confidential –

OnSolve, CodeRED, MIR3, One Call Now, Send Word Now, and SmartNotice are registered trademarks of OnSolve, LLC or its affiliates.

All other trademarks used herein are the property of their respective owners.

Contents

Introduction.....	14
Purpose of this Guide.....	14
Scope of this Guide	14
Support and Training	15
Customer Support Contacts	15
Support in the OnSolve Platform.....	15
Connect with Us Online.....	16
Documentation Feedback	16
Section 1: User Interface Navigation	
Sign-In Credentials.....	18
Single Sign-On	20
Multi-Factor Authentication	21
Forgot Username or Password	22
Forgot Username.....	22
Forgot Password.....	23
Control Center.....	25
Left Navigation Menu	27
Create Alert Shortcut.....	28
Map.....	29
Search	31
People.....	32
Locations	33
Account Overview	34
Static User Interface Elements	35
See What's New.....	35
Global Search.....	35
Languages.....	36
Notifications Bell and Announcements	37
Profile	38
Check In.....	38

Account Name	39
External Links	39
OnSolve URL	40
Data Subject Rights Request	40
Privacy Statement	43
Copyright Notice	43
Contact Us	43
User Feedback	43
Control Center Configuration	44
Map	44
Widgets	46
Account Widget Drawer	46
Other Control Center Widgets	49
Quick Links Bar	51
Section 2: Contact Management	
Populate and Manage Contacts	53
Manage Contacts	53
Export Contacts	54
View as User	55
Affiliations	55
Modify a Contact	56
Delete a Contact	56
Create a New Contact	57
Overview	57
Devices	59
Custom Fields	61
Locations	62
Subscriptions	64
User Privileges	67
Create and Manage Groups	70
Group Types	70
Manage Groups	70
Export Groups	71

Edit Groups	72
Delete Groups.....	72
Create a Group.....	72
Add People	75
Add Map Shapes	76
Add Groups.....	78
Add People Record Attributes	79
Add Device Attributes	82
Add Custom Fields	82
Add Advanced Filters	83
On-Call Scheduling	85
Create a New Schedule	85
Define the Schedule	86
Create Shifts	87
Add Assignments (Optional).....	91
Holidays.....	95
Create a New Holiday Calendar.....	95
Modify a Holiday Calendar	96
Delete a Holiday Calendar.....	97
Manage Schedules.....	98
Schedule Settings.....	98
Search and Filter a Schedule and Its Elements.....	98
Modify a Schedule	103
Delete a Schedule	109
Duplicate a Schedule.....	109
View Coverage	110
Export Coverage	114
Section 3: Alert Management	
Create a Quick Alert.....	118
Create an Advanced Alert.....	123
Add Alert Details.....	124
Scenario Library.....	126
Email Editor	128

Preview Alert.....	128
Add Recipients	129
Broadcast Alert	129
Quota Alert.....	133
Bulletin Board	136
Add Response Options	138
Ask a Follow-Up Question	141
Send a Cascade Alert.....	144
Select Delivery Methods.....	147
Add Delivery Methods to Contacts On the Fly	148
Enable Advanced Settings.....	151
Sender	151
Language	151
Voice	151
Email	152
Response Options	152
Text-Based	152
Delivery Attempts.....	152
Reports	153
Additional Options	154
Alert Languages.....	154
File-Based Alerting	156
Integrations	158
Voice Recording	160
Alert Variables and Sender Instructions.....	168
External Conference Bridge	171
Send Test, Save Alert, or Send Alert.....	172
Send Test	172
Send Now	173
Schedule to Send	174
Save.....	175
Create a Linked Alert	176
Manage Alerts	178

Cancel an Alert	179
Manage Saved Alerts	180
Alerts Table Details	181
Search.....	181
Sort	181
Filter	181
Favorite.....	182
Edit.....	182
Duplicate.....	182
Delete.....	182
Send.....	182
Manage Scheduled Alerts	187
Alerts Table Details	187
Search.....	188
Sort	188
Filter	188
Edit.....	188
Delete (Cancel Scheduled Alert).....	188
Manage Sent Alerts	189
Alert Table Details	189
Search.....	190
Sort	190
Filter	190
Delete.....	190
View Analytics.....	190
Resend	191
Manage Linked Alerts.....	191
Alert Table Details	191
Edit.....	191
Delete.....	191
Send.....	192
View Analytics.....	192
Alternate Alert Management Methods	193



Send by Phone	193
Receive an Alert.....	194
Reply to an Alert.....	194
Reply to an Email Alert.....	194
Reply to an SMS Alert.....	194
Reply to a Voice Alert.....	195
Reply to a Desktop Alert.....	195
Change Response.....	195
Reply to a Follow-Up Question.....	196
Connect to a Conference Bridge.....	197
Retrieve an Alert.....	198
The Alert Inbox	198
Bulletin Boards.....	201
Section 4: Reports	
Overview	203
Analytics	203
Analytics Details	204
Alert Details	205
Response Rate	206
Delivery Methods	207
Recipients Table	208
Resend an Alert.....	216
Resend Based on Response.....	216
Custom Resend	218
Ad Hoc Reports	219
Create a New Report.....	219
Example 1	222
Example 2	223
Manage Ad Hoc Reports	223
Search.....	223
Sort	223
Filter	224
Edit.....	224



Delete.....	225
Run	225
Audit Trail	226
Operations	226
Performed By.....	227
Date Range	227
Target	227
Search the Audit Trail.....	228
Export Audit Logs	228
Usage Report	229
Call List Report.....	230
Custom Reports	231
People Over Time	231
Risk Insights.....	232
Section 5: Incident Management	
LookOut.....	240
Configure LookOut Settings	240
Assign Role Permissions.....	240
Assign an Alert to a Division.....	240
LookOut Incidents	246
LookOut in OnSolve Mobile	247
SOS	248
Configure SOS Settings	248
Location Permissions	248
Assign Role Permissions.....	248
Assign an Alert to a Division.....	249
SOS Incidents.....	255
SOS in OnSolve Mobile.....	255
Lockbox.....	256
Upload Files to the Lockbox.....	256
Manage Lockbox Files	258
Search, Sort, and Filter.....	259

History.....	259
Download.....	259
Delete.....	259
View and Edit Details.....	260
Retrieve Lockbox Files	260
Shared Lockbox.....	261
Secure Lockbox via OnSolve Mobile.....	262
Section 6: Subscriptions	
Overview	265
Weather & Events	265
Create a Profile	265
Alert Types.....	268
Create a Location.....	269
Create a Subscription.....	272
Modify a Profile.....	279
View Profile History	280
Modify a Location	280
Modify a Subscription.....	281
View Subscription History	282
Delete a Profile/Location	282
Topics.....	283
Create a New Topic.....	283
Categories	283
Priorities	284
Severities	285
Manage Topics	286
Modify a Topic	286
Reorder Topics	286
Delete a Topic.....	287
View References.....	287
Text-to-Keyword.....	289
Create Keywords.....	291

Preview the Return Message for a Keyword.....	297
Keyword and Contact Management.....	299
Delete a Keyword	299
Contact Management	299
Section 7: Configure	
Integrations.....	301
Social Media and Chat	301
Slack	301
Microsoft Teams	301
Twitter	301
Systems Integrations	302
Entra ID (Azure AD).....	302
BambooHR	302
Envoy	302
Kisi	302
ServiceNow.....	303
UKG	303
Alertus.....	303
TDS.....	303
Integrations Management	304
View	304
Enable/Disable.....	304
Disconnect	304
Account Portals	306
Create a Portal	306
Overview.....	306
Branding	307
Custom Policies	307
Help Link.....	308
Access	308
Configuration	310
Portal Management	316
Modify a Portal.....	316

Delete a Portal	318
Permissions	318
Predefined Roles	318
Administrator	318
Initiator	319
Recipient (Contact)	320
Role and Role Template Management	321
Add a Role	321
Add a Role Template	333
View and Manage Roles and Role Templates	334
Divisions	335
Create a New Division	336
Edit a Division	337
Delete a Division	337
Move Records Between Divisions	337
Manage Division S/MIME Keys	338
Branding	339
Custom Verbiage	339
Security	343
Multi-Factor Authentication	343
Setup	343
Save SMS Device	343
Enable MFA	343
Reset MFA for a User	344
Default Modality Configuration	345
Section 8: Settings	
Alert Module	347
Labels	347
Overview Labels	347
Device Labels	348
Location Labels	351
Custom Fields	353
Alert Options	356



Notification Options	356
General Options.....	356
Notification Timing	357
Phone Device Types Only	358
Stop Contacting If	359
Device Priority.....	359
Division ANI.....	360
Call Throttling	360
Suppressed Alerts	361
Allowed SMS	361
Assign SMS Profiles.....	362
Edit TTS Voices.....	362
Edit Pronunciations	362
Duplicate Filters.....	363
Alert Retrieval.....	365
Section 9: OnSolve Mobile	
Overview	367
Geofenced-Enabled Alerts.....	367
Section 10: Risk Intelligence	
Overview	370
Section 11: Appendices	
Appendix A: Glossary.....	372
Appendix B: Ad Hoc Reporting Resources.....	376
Appendix C: Weather & Events Event Types	379
Appendix D: Phone Number Formatting.....	410
International Phone Numbers	410
Universal Telephony Syntax	410



Introduction

With billions of alerts sent annually and decades of proven support to the public and private sectors, OnSolve® delivers critical event management capabilities backed by unmatched industry expertise, keeping our customers safe, informed, assured, and productive during a crisis. As a leading critical event management provider, OnSolve helps our customers mitigate risk and strengthen their organizational resilience.

The OnSolve Platform is a great way to explore the new upgraded alerting system, practice workflows, test out new and updated functionalities, and provide feedback to the OnSolve development team about the experience.

The OnSolve Platform is a constantly evolving and organic product. New features will be added, and existing features will be updated regularly. Designs, experience, and functionalities are continuously being revisited based on feedback and usability testing.

Purpose of this Guide

The purpose of this *Administrator Guide* is to serve as a comprehensive reference guide for administrator-level activities and tasks within the OnSolve Platform.

Remember that the recommended best practices presented in this *Administrator Guide* are OnSolve guidelines and should always be aligned with the organization's internal policies and procedures.

Also, screenshots, with any accompanying alternative text for accessibility, and other examples found in this guide are for illustration purposes only and do not necessarily reflect actual system values.

Scope of this Guide

The scope of this *Administrator Guide* includes administrator-level activities, including:

- Populating and Managing Contacts and Groups
- Creating and Managing Schedules
- Creating and Managing Labels
- Creating and Managing Topics
- Sending and Managing Alerts
- Generating Reports
- Setting up Weather & Events Subscriptions

- Creating and Managing Roles and Role Templates
- Creating and Managing Divisions
- Configuring Settings
- Retrieving Alerts

A glossary of frequently used terms, which describe important aspects of the OnSolve Platform and organization activities, found throughout this *Administrator Guide* and often used in communications with Customer Support personnel, is provided in Appendix A.

Support and Training

OnSolve is committed to customer satisfaction. Our goal is to deliver critical time-sensitive alerts quickly, with the best customer support—to make the OnSolve Platform simple, fast, reliable, and effective. OnSolve offers several options for customers to get support. Customers can contact our Customer Support representatives at the phone numbers and email below or choose from several support and training options accessible from within the OnSolve Platform user interface.

Customer Support Contacts

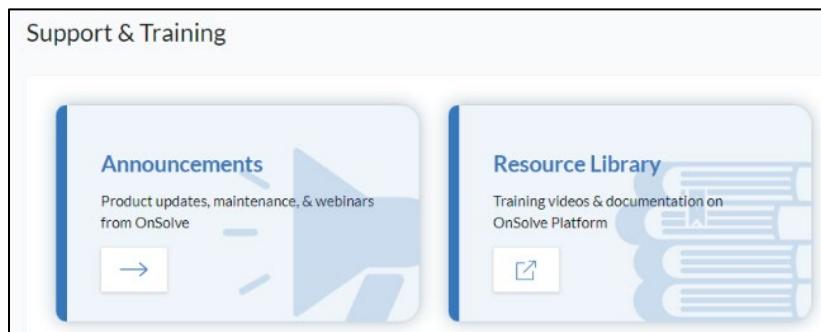
Phone: US Toll-free: +1 866-939-0911
UK: +44 20 3318 3862

Email: support@onsolve.com

Web: www.onsolve.com/resources/support/

Support in the OnSolve Platform

Select **Support & Training** on the left navigation menu to access support options.



Announcements

The **Announcements** option allows OnSolve to contact users with important and useful information regarding the OnSolve Platform.

Resource Library

The OnSolve **Resource Library** contains videos, opportunities to register for live trainings, and links to this *Administrator Guide*. It also includes our *What's New in the OnSolve Platform* document (regularly updated to include the release notes for the most current releases) and other documents.

Connect with Us Online

www.onsolve.com

X (formerly Twitter): @OnSolve

Blog: www.onsolve.com/blog

Documentation Feedback

Did you find everything you were looking for in this guide? We appreciate your feedback! Please feel free to reach out to us at documentation@onsolve.com with any comments, and note the document title and version number.



Section 1: User Interface Navigation

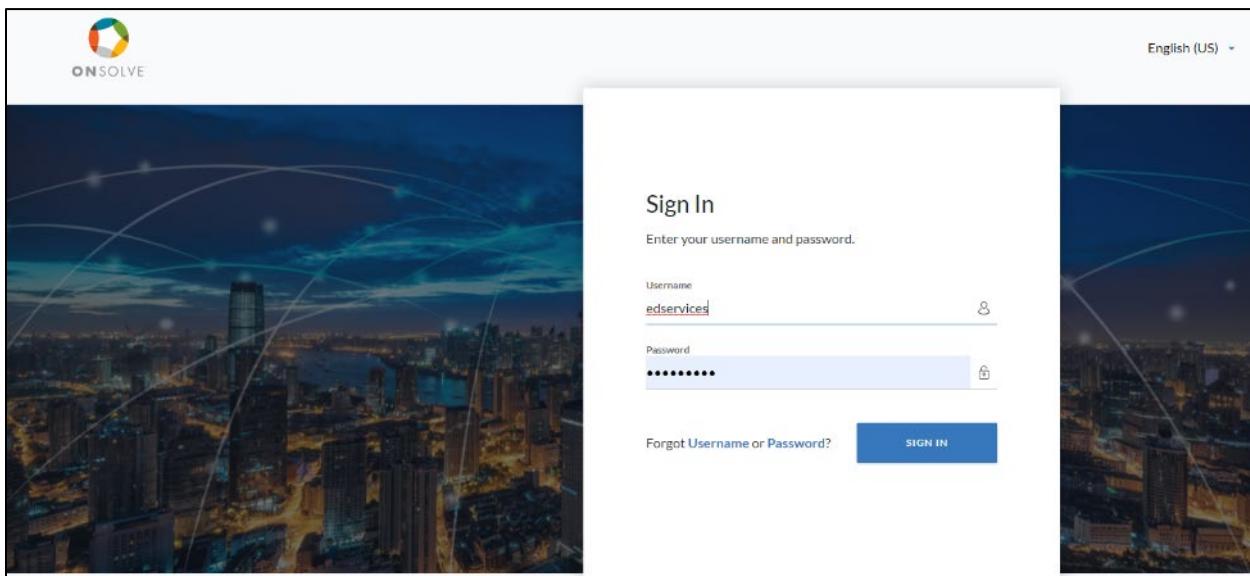
Sign-In Credentials

An OnSolve Customer Support representative initially creates main account administrator credentials. Additionally, each organization is given a dedicated sign-in URL reflecting the organization's name.

The OnSolve Platform supports the most recent versions of the following browsers:

- Firefox
- Google Chrome™
- Microsoft Edge
- Safari

Note: The OnSolve Platform does not support Internet Protocol Version 6 (IPv6).



The optimal screen resolution for viewing the OnSolve Platform in the web UI is 1920 x 1080 pixels.

To access the OnSolve Platform

1. Go to onsolve.net, enter your organization's workspace name, and select **Get Started**.

OR

Go directly to your organization's dedicated login URL.

The **Sign In** page loads in the language associated with the browser's language settings. If that language is not one of the 30 supported languages, the page defaults to English (US). If desired, choose a different language to view the **Sign In** page by selecting the drop-down list next to the current language. The selected language is also applied to all other pages of the user interface.

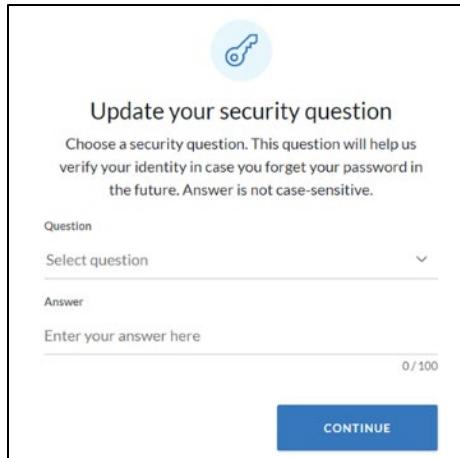
Languages		
(AE)  الْجَمِيعَةُ	Français (FR)	Português (BR)
中文 (CN)	Deutsch (DE)	Português (PT)
中文 (TW)	Ελληνικά (GR)	Română (RO)
Czech (CZ)	हिन्दी (IN)	Русский (RU)
Dansk (DK)	Magyar (HU)	Español (ES)
Dutch (NL)	Italiano (IT)	Español (MX)
English (GB)	日本語 (JP)	Svenska (SE)
English (US) 	한국어 (KR)	ไทย (TH)
Suomi (FI)	Norsk (NO)	Türk (TR)
Français (CA)	Polski (PL)	català (ES)

Note: It is important to remember that the languages available for viewing in the OnSolve Platform user interface are not necessarily the same as those provided for composing an alert when the Multi-Language Alerts (MLA) feature is enabled.

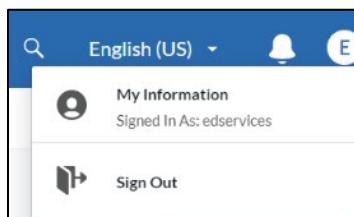
2. Enter your username and password in the fields provided. Note that while the **Username** field is not case-sensitive, the **Password** field is case-sensitive and is masked for security. If there is any trouble signing in, check to see if CAPS LOCK is enabled and turn CAPS LOCK off. Remember that your account will be locked out after an excessive number of invalid sign-in attempts.
3. Select **Sign In**.

Note: See [Multi-Factor Authentication](#) if your organization requires that you reauthenticate.

4. If this is your first time signing in, and your organization has security questions enabled, select a **Question** from the drop-down list, enter an **Answer**, and select **Continue**. Select **Continue** again to navigate to the control center view.



5. To exit the account, select **Sign Out** from the **Profile** drop-down menu in the upper right-hand corner of the control center view.



Single Sign-On

OnSolve offers SP- and IDP-initiated SSO (Single Sign-On) for any provider that is SAML2-compliant. SSO is available for the OnSolve Platform, Account Portals, and OnSolve Mobile. If you are interested in having SSO for your organization, contact your OnSolve representative.

Multi-Factor Authentication

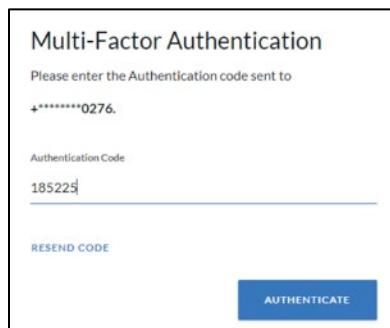
If your account administrator has enabled multi-factor authentication, confirm your identity.

1. If you have only one SMS device saved to your people record, select **Next**. If you have more than one SMS device saved to your people record, select the one to which you want to receive an authentication code, then select **Next**.



The screenshot shows the 'Multi-Factor Authentication' page. At the top, it says 'Multi Factor Authentication is required for system access. Select authentication method and complete registration.' Below this, under 'Authentication Method', 'SMS' is selected. Under 'SMS number', there is a dropdown menu labeled 'Select SMS number' containing two options: '+*****0276' and '1*****1111'. The option '+*****0276' is highlighted.

2. Enter the six-digit **Authentication Code** you received via SMS and select **Authenticate**.



The screenshot shows the 'Multi-Factor Authentication' page. It asks for the authentication code sent to '+*****0276'. Below this, there is a field labeled 'Authentication Code' containing the value '185229'. At the bottom right is a blue 'AUTHENTICATE' button.

3. On the **Success!** page, select **Continue**.

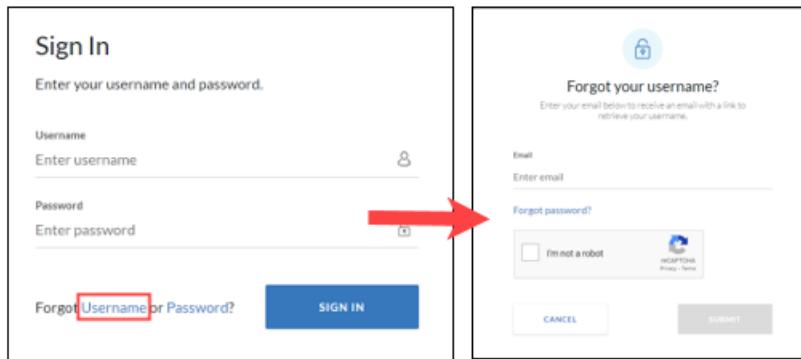
Forgot Username or Password

Users can recover their usernames and passwords from the **Sign In** page.

Forgot Username

To recover a username

1. From the **Sign In** page, select **Forgot Username**. The **Forgot your username?** window opens.



The image contains two side-by-side screenshots. The left screenshot shows the 'Sign In' page with fields for 'Username' and 'Password', and a 'Forgot Username or Password?' link highlighted with a red box. The right screenshot shows the 'Forgot your username?' window with a 'Forgot password?' link, an 'Email' input field, a 'CAPTCHA' checkbox labeled 'I'm not a robot', and 'CANCEL' and 'SUBMIT' buttons.

2. Enter the email associated with the account.

Note: The email entered must be saved as a device type in the user's profile.

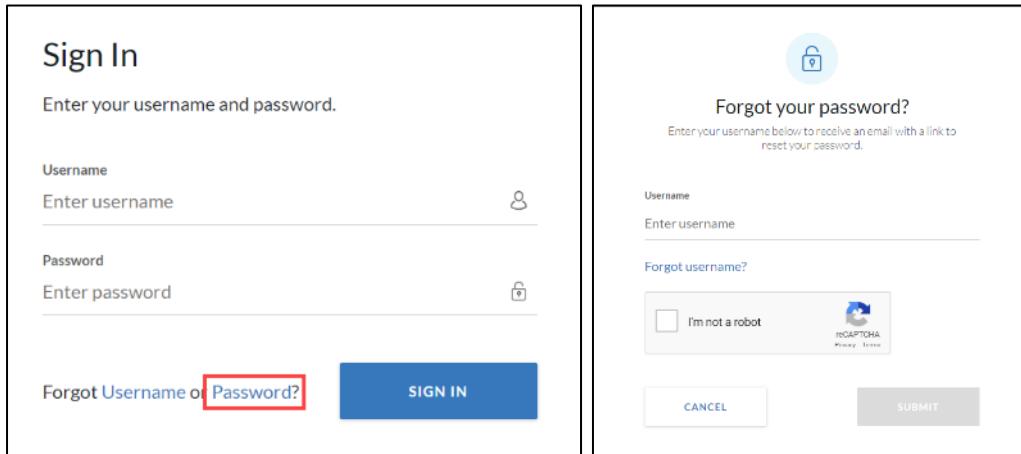
3. Select **I'm not a robot** and then **Submit**. Check your email account for the username sent from OnSolve.

Forgot Password

If you forget your password, you will need to reset it.

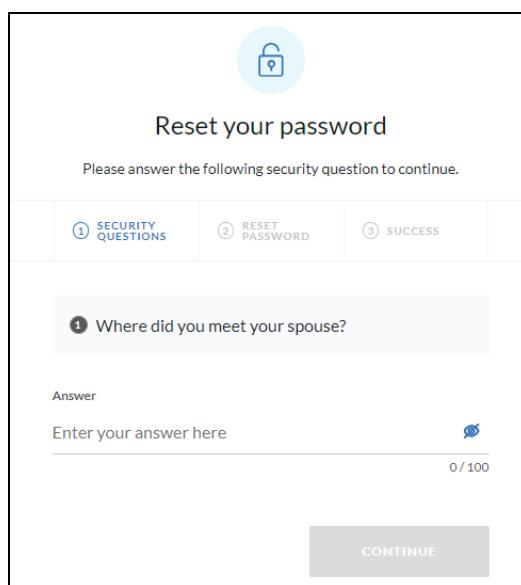
To reset a password

- From the **Sign In** page, select **Forgot Password**. The **Forgot your password?** window opens.



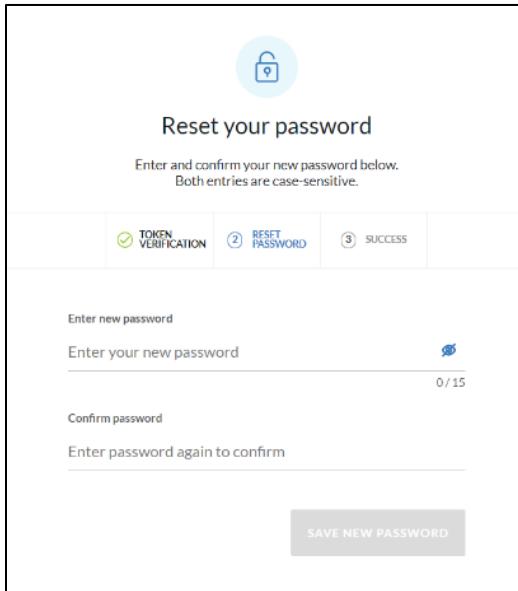
The image shows two side-by-side screenshots of a web application's sign-in interface. On the left, the 'Sign In' screen displays fields for 'Username' and 'Password'. Below these fields are links for 'Forgot Username' and 'Forgot Password?'. The 'Forgot Password?' link is highlighted with a red rectangle. A large blue 'SIGN IN' button is positioned to the right of the password field. On the right, the 'Forgot your password?' screen is shown. It features a lock icon at the top. The text 'Forgot your password?' is followed by a sub-instruction: 'Enter your username below to receive an email with a link to reset your password.' Below this are 'Username' and 'Forgot username?' input fields. A reCAPTCHA checkbox labeled 'I'm not a robot' is present, with the reCAPTCHA logo and terms 'reCAPTCHA Privacy - Terms'. At the bottom are 'CANCEL' and 'SUBMIT' buttons.

- Enter the **Username** associated with the account.
- Select **I'm not a robot** and then **Submit**. An email will be sent with password reset instructions.
- Follow the link in the email (or copy and paste the URL into a browser). The **Reset your password** page opens. If your organization has opted to use security questions, enter the answer to the security question and select **Continue**.



The image shows the 'Reset your password' page. At the top is a lock icon. The title 'Reset your password' is centered. Below it is a sub-instruction: 'Please answer the following security question to continue.' A horizontal navigation bar at the top indicates the steps: ① SECURITY QUESTIONS, ② RESET PASSWORD, and ③ SUCCESS. Step ① is active. The main content area shows a question: '① Where did you meet your spouse?' Below it is an 'Answer' field with the placeholder 'Enter your answer here' and a character limit of '0 / 100'. A 'CONTINUE' button is located at the bottom right of the form.

5. Enter and Confirm a new password. Passwords are case-sensitive.



The image shows a screenshot of a password reset interface. At the top center is a blue circular icon containing a white padlock symbol. Below it, the text "Reset your password" is centered. Underneath that, a sub-instruction reads "Enter and confirm your new password below. Both entries are case-sensitive." A horizontal navigation bar follows, featuring three items: "TOKEN VERIFICATION" (with a green checkmark icon), "RESET PASSWORD" (with a blue circular icon containing a question mark), and "SUCCESS" (with a blue circular icon containing a checkmark). The main content area contains two input fields: "Enter new password" and "Enter your new password". The second field includes a character counter "0 / 15" and a small blue info icon. Below these is another input field labeled "Confirm password" with the placeholder "Enter password again to confirm". At the bottom right of the form is a grey rectangular button labeled "SAVE NEW PASSWORD".

6. Select **Save New Password**.
7. Select **Go To Sign In** and sign in using your new password.

Control Center

After signing in, you see the control center view. The OnSolve Platform Control Center provides a centralized operating hub that allows you to visualize, automate, and orchestrate management of critical events.

Access the control center view anytime by selecting the **Control Center** option at the top of the left navigation menu.

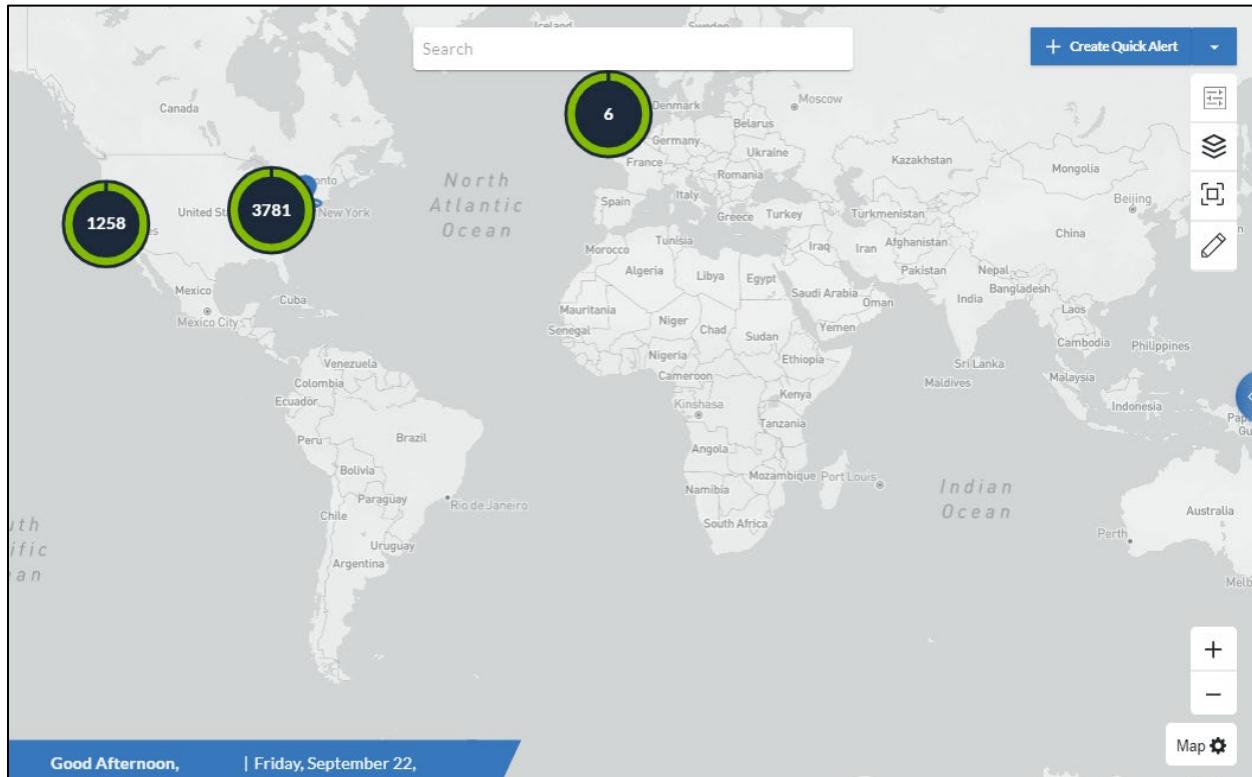


In this release, the control center view includes the following:

- A map that shows all contacts in the account who have saved locations.
- A search field to find people and locations.
- The ability to create and send a Quick Alert.
- The ability to go directly to the advanced alert workflow.
- Widgets that provide convenient and configurable views into non-geographical data from your account so you can monitor the data that is most important.
- A Custom Links Bar that you configure to open important user-defined links quickly.
- The account widget drawer, which can contain two configurable widgets.

See [Control Center Configuration](#) to learn how to customize the control center view for your account.

Note: All areas of the control center view respect the permissions set in your account. So, if, for instance, the user has permission to see information in only one division, the widgets show only that data.



Account Overview

Last 24 Hours	
2 Reached	11 Alerts Sent
1 Contacts Added	50% Responded
100% Delivered	

Widgets

Sent Alerts	Reports
ALERT NAME Quick Alert 1 (Broadcast, Active) SMS testing (Broadcast, Active)	test 32 Last used Feb 10, 2021 4:25 PM (7 Filters Applied) initiatororrolename Last used Sep 26, 2022 2:48 PM (3 Filters Applied)

Announcements
 Product updates, maintenance, and webinars from OnSolve

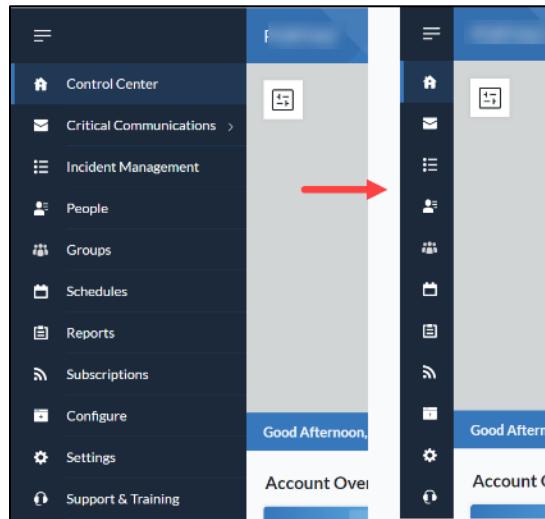
Resource Library
 Training videos and documentation on the OnSolve Platform

Reports
 Create and run Custom Reports

Quick links bar

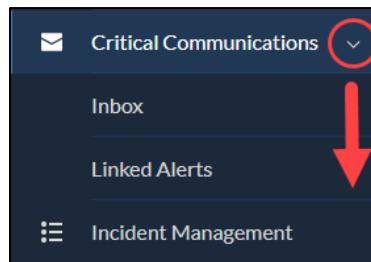
Left Navigation Menu

The left navigation menu contains twelve parent or primary menu options. This menu is collapsible to show only the icons by selecting the hamburger menu above the **Control Center** option.



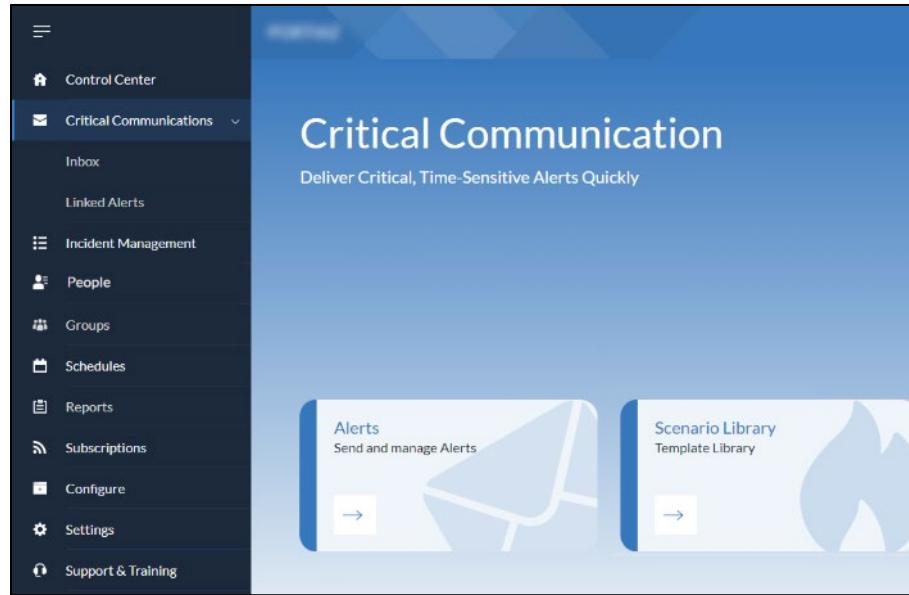
The primary menu option includes an arrow icon. This type of expandable menu option behaves in two ways depending on where you click.

If you click on the arrow, the menu expands to display secondary menu options. Menu expansion happens as such:

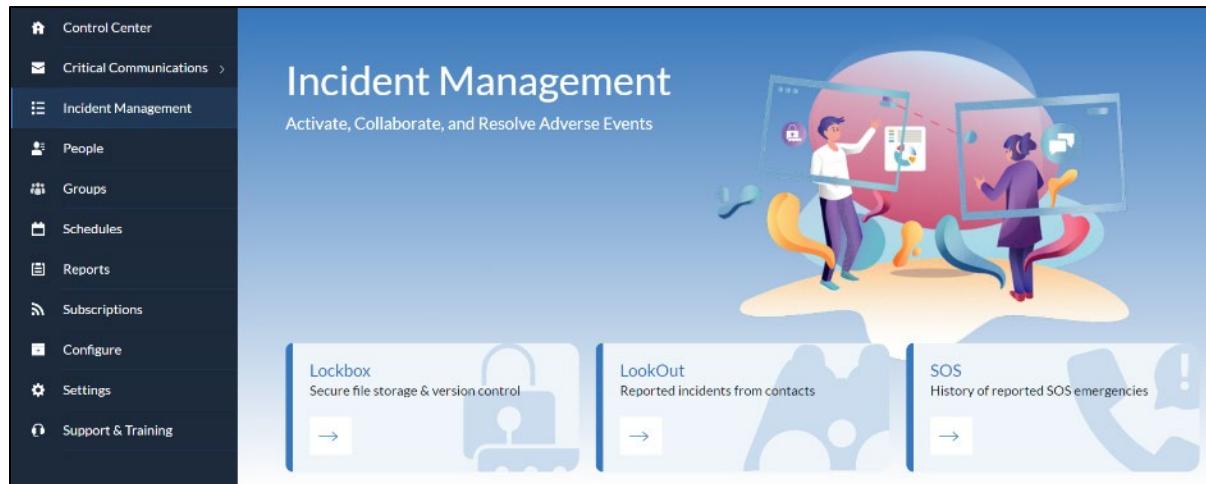


In the above example, the user selects the arrow on the **Critical Communications** menu option. That menu expands to display its secondary menus: **Inbox** and **Linked Alerts**.

If you select the menu *name*, that option's page opens.

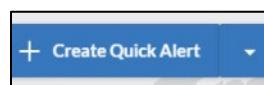


Menu options that do not expand vertically will either open that feature's page or a landing page with navigation tiles. For instance, the **Schedules** menu option leads to the **Schedules** page, while the **Incident Management** menu option leads to a choice of three navigation tiles:



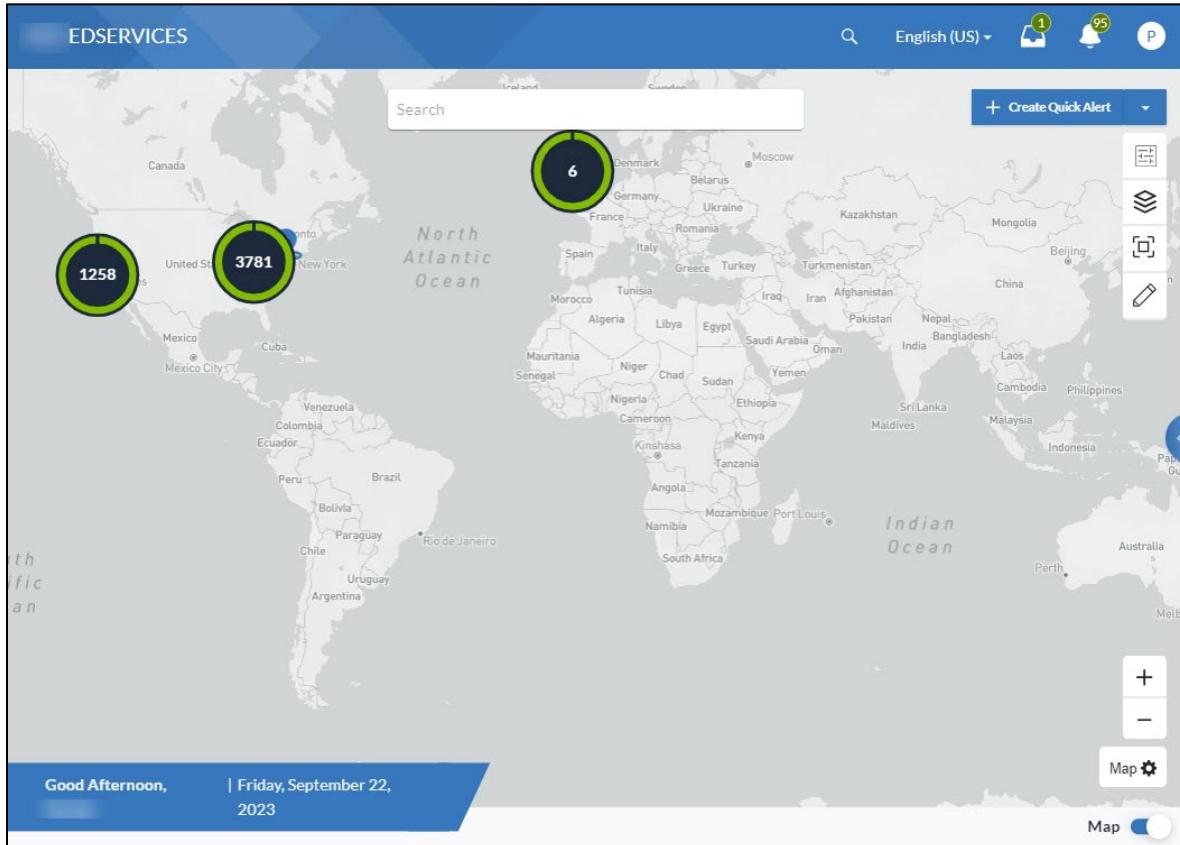
Create Alert Shortcut

At the top right of the control center view is the **+ Create Quick Alert** button. Select it to [Create a Quick Alert](#) or the down arrow to [Create an Advanced Alert](#).

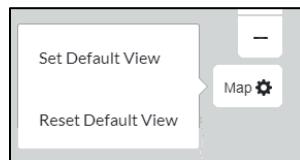


Map

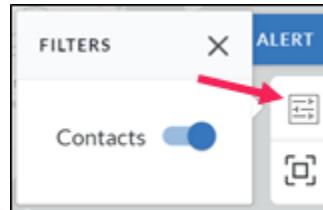
At the top of the control center view is a map showing contacts (and other entities in future releases) with saved locations represented by green circles. The number inside the circle—a map cluster—indicates a cluster of contacts with the same saved location or nearby locations. See [Locations](#) in Section 2 of this guide for more information.



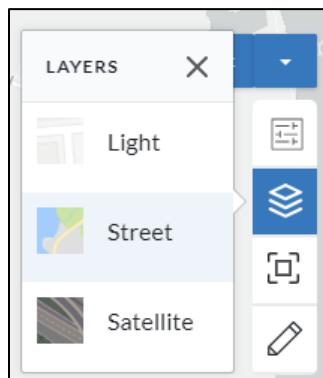
- Zoom in and out on the map by using the plus and minus buttons or by holding the control key (command key for Mac users) while using your mouse's scroll wheel.
- Note:** Use your mouse's scroll wheel to scroll up and down within the control center view.
- Use the **Search** field to find people saved in your account and locations. Learn more in [Search](#).
 - Set a default map view that your map always opens to by finding the view you want, selecting the Map cog wheel, and selecting **Set Default View**. If you explore the map, you can return to your default view by selecting the Map cog wheel and selecting **Reset Default View**.



- Select the **Filter Map** tool to choose what is displayed on the map. In this release, contacts are the only option.



- Select the **Layers** tool to choose how the map is displayed: **Light**, **Street**, or **Satellite**.



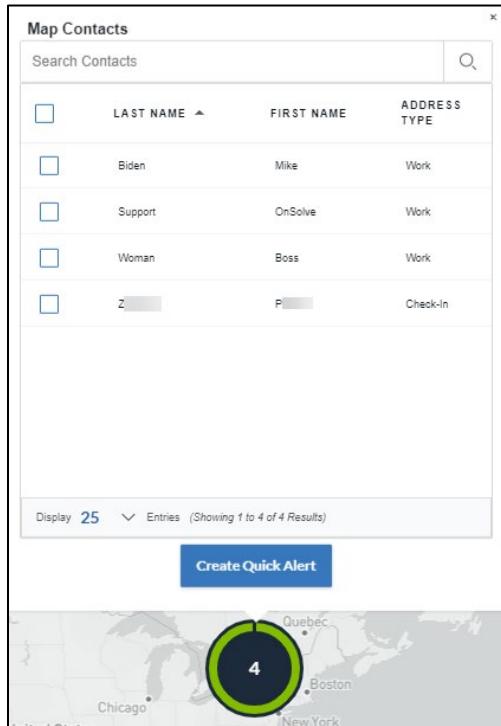
- Select the **Fullscreen Map** tool to expand the map to fit your screen. When the map is expanded, you can zoom in and out using your mouse's scroll wheel without holding the control key.



- Select the **Draw** tool to create or upload a shape to [send a quick alert to a map group](#).



- [Send a quick alert to a map cluster.](#)



The screenshot shows the 'Map Contacts' interface. At the top, there is a search bar labeled 'Search Contacts' with a magnifying glass icon. Below it is a table with columns: 'LAST NAME' (sorted by last name), 'FIRST NAME', and 'ADDRESS TYPE'. The table contains four rows of data:

LAST NAME	FIRST NAME	ADDRESS TYPE
Biden	Mike	Work
Support	OnSolve	Work
Woman	Boss	Work

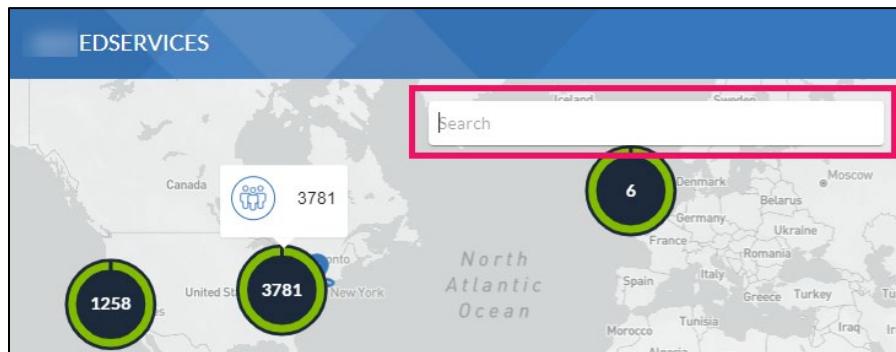
At the bottom of the table, there is a 'Display 25' dropdown and a message '(Showing 1 to 4 of 4 Results)'. Below the table is a blue button labeled 'Create Quick Alert'. The bottom half of the interface is a map showing North America and Europe. A green circular cluster marker is centered over the United States, indicating 4 alerts. Other markers are visible in Canada, the UK, and Germany.

- Select the **Map** toggle to hide or display the map in the control center view.



Search

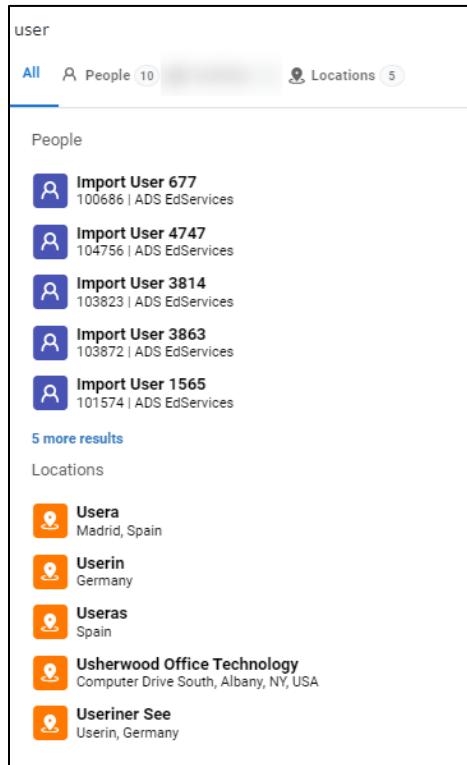
You can use the **Search** field to find people saved in your account and locations.



The screenshot shows the 'EDSERVICES' interface. At the top, there is a search bar labeled 'Search' with a magnifying glass icon. Below the search bar is a world map. Three green circular clusters are overlaid on the map, representing alert counts: one in North America (1258), one in the United States (3781), and one in Europe (6). The map also shows labels for countries like Canada, United States, Mexico, Brazil, Argentina, Australia, New Zealand, China, India, Japan, South Korea, Russia, Turkey, Spain, France, Italy, Germany, UK, Ireland, Poland, Czech Republic, Hungary, Romania, Bulgaria, Greece, Turkey, Israel, Jordan, Lebanon, Syria, Iraq, Iran, Saudi Arabia, Yemen, Oman, UAE, Qatar, Bahrain, Kuwait, Libya, Algeria, Morocco, Mauritania, Mali, Niger, Burkina Faso, Ghana, Côte d'Ivoire, Liberia, Sierra Leone, Nigeria, Cameroon, Gabon, Equatorial Guinea, São Tomé and Príncipe, Angola, Congo, Democratic Republic of the Congo, Uganda, Kenya, Tanzania, Malawi, Zambia, Zimbabwe, Namibia, Botswana, Lesotho, South Africa, Swaziland, Lesotho, and Eswatini.

People

You can search for people with saved people records in your account by entering the first few letters of their first or last names. As you type, matching people and locations are listed below.



The screenshot shows a search interface with the query "user" entered. The results are categorized into "People" and "Locations".

People:

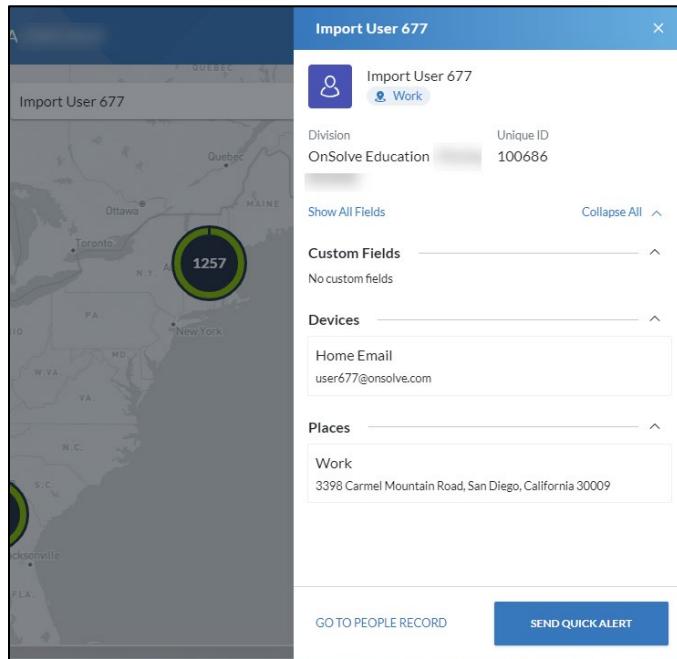
- Import User 677 (100686 | ADS EdServices)
- Import User 4747 (104756 | ADS EdServices)
- Import User 3814 (103823 | ADS EdServices)
- Import User 3863 (103872 | ADS EdServices)
- Import User 1565 (101574 | ADS EdServices)

[5 more results](#)

Locations:

- Usera (Madrid, Spain)
- Userin (Germany)
- Usersas (Spain)
- Usherwood Office Technology (Computer Drive South, Albany, NY, USA)
- Useriner See (Userin, Germany)

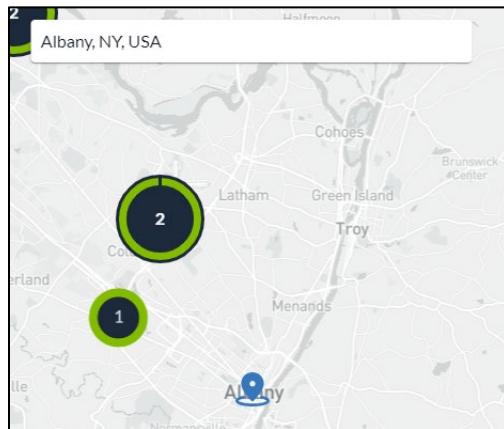
Select any person to view their people details drawer.



From the people details drawer, you can go to that person's people record by selecting **Go To People Record**, or you can select **Send Quick Alert**. The **Create a Quick Alert** window opens with this person already selected as a recipient.

Locations

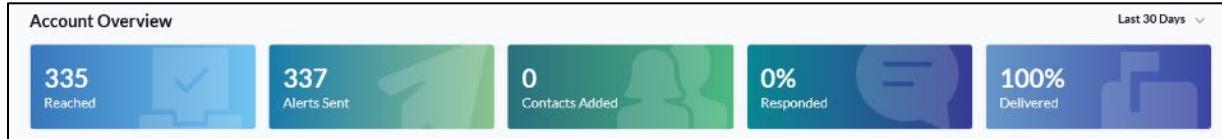
Enter the first few letters of a location, such as a city or business. As you type, matching people and locations are listed below. Select a location, and the map zooms in to that place.



Note: Locations saved in the **Locations** tab of people records are not searchable. Searchable locations are sourced from the OnSolve Platform's map provider.

Account Overview

Under the map is the **Account Overview**. The data displayed here is based on the division to which you, the logged-in user, are assigned. The Account Overview consists of five data cards: **Reached**, **Alerts Sent**, **Contacts Added**, **Responded**, and **Delivered**.



The above example shows that in the last 30 days:

- 335 contacts were reached. “Reached” means a successful delivery to at least one device type.
- 337 alerts were sent.
- 0 contacts were added to the account.
- 0% of contacts responded.
- 100% of contacts were delivered to. This is calculated by the number in the **Reached** tile divided by the number of total devices the alert was sent to.

Use the drop-down list above the **Delivered** card to change the data time frame. Options are the last **24 hours**, **7 days**, **2 weeks**, or **30 days**.

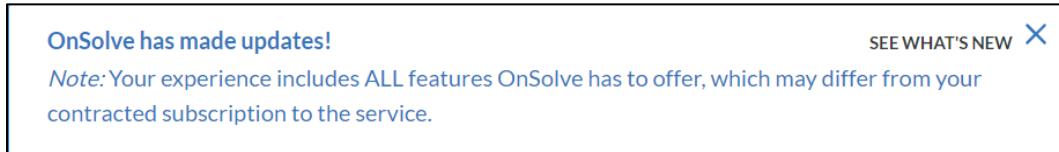


Static User Interface Elements

There are elements in the OnSolve Platform user interface that are static, staying with you as you navigate to any page. These elements are described below.

See What's New

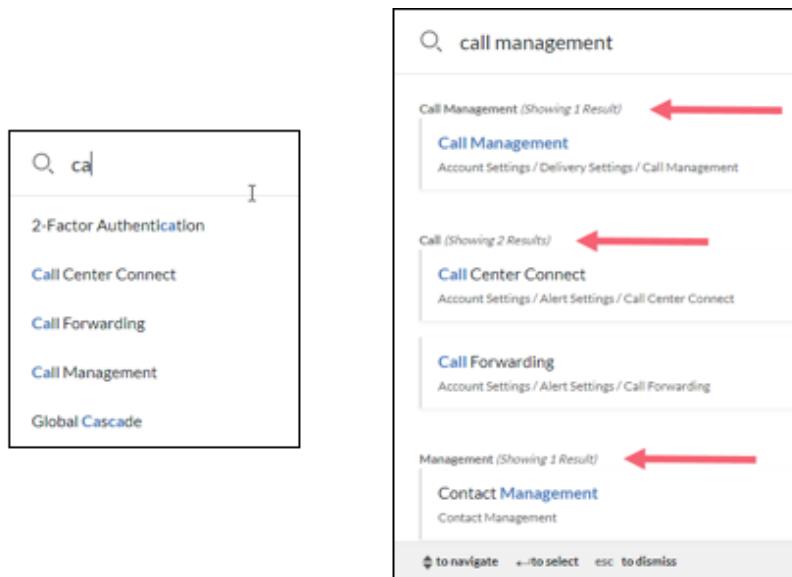
If your organization is using our sandbox (beta) environment, every time you sign in, a window opens in the upper right-hand corner with a link to get more information about recent updates.



Select **See What's New** to download the latest documentation on what has been released in the sandbox environment of the OnSolve Platform. To view the *What's New* guide at any time, navigate to **Support & Training > What's New** on the left navigation menu. Select the **X** to close the window.

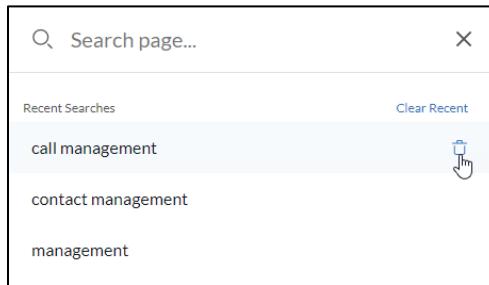
Global Search

The Global Search function is indicated by a magnifying glass icon at the top right of every page, next to the language designation. This feature allows you to search for OnSolve Platform functionalities. Search for an OnSolve Platform feature option by entering the name in the field. Select a search result to see a choice of associated pages you can navigate to. The search field incorporates predictive text, so as you type into the field, suggested terms are listed:



The screenshot illustrates the global search process. On the left, a search bar contains the partial text "ca". Below it, a list of suggestions is shown: "2-Factor Authentication", "Call Center Connect", "Call Forwarding", "Call Management", and "Global Cascade". On the right, a detailed search results panel is displayed for "call management". It shows a header "Call Management (Showing 1 Result)" with a red arrow pointing to it. Below this is a card for "Call Management" under "Account Settings / Delivery Settings / Call Management". Further down, another section for "Call" is shown with a red arrow, listing "Call Center Connect" and "Call Forwarding" under "Account Settings / Alert Settings / Call Center Connect" and "Account Settings / Alert Settings / Call Forwarding" respectively. At the bottom of the results panel, a footer provides navigation instructions: "↑ to navigate", "→ to select", and "esc to dismiss".

Once you either press the return key or select one of the suggested results, the second menu of results is listed, showing all menu options containing any searched words. In the example below, "Call Management" was searched. The top result reflects the two words together, while subsequent results are based on each word alone. Each result also provides the path for that menu option. You can select any result to be taken directly to that page.



Recent searches are saved for each unique user, but only within the current session and browser. Select **Clear Recent** to clear all recent searches, or select the trash can to remove any single result from the list of recent searches.

Languages

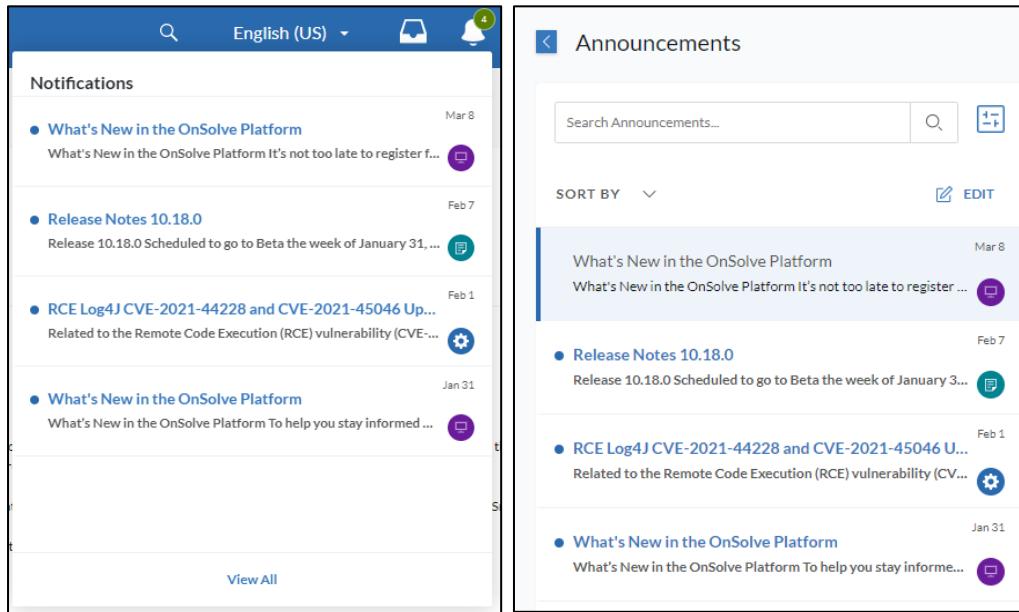
The user interface loads in the language that your browser is set to or the language you selected on the **Sign In** page, if different. You can change the UI language at any time by selecting the language drop-down list to the left of the **Profile** drop-down menu and choosing any of the 30 available languages.



Arabic	French (France)	Portuguese
Catalan	German	Portuguese (Brazil)
Chinese (Mandarin)	Greek	Romanian
Czech	Hindi	Russian
Danish	Hungarian	Spanish (Mexico)
Dutch	Italian	Spanish (Spain)
English (UK)	Japanese	Swedish
English (US)	Korean	Taiwanese (Mandarin)
Finnish	Norwegian	Thai
French (Canada)	Polish	Turkish

Notifications Bell and Announcements

The Notifications Bell displays a count of the number of unread announcements, and when selected, The Notifications menu displays the ten most recent announcements. Announcements are communications from OnSolve to you, the customer. Select any announcement or **View All** to navigate to the **Announcements** page.



Notifications Page (Left)	Announcements Page (Right)
Notifications	Announcements
What's New in the OnSolve Platform (Mar 8)	What's New in the OnSolve Platform (Mar 8)
Release Notes 10.18.0 (Feb 7)	Release Notes 10.18.0 (Feb 7)
RCE Log4J CVE-2021-44228 and CVE-2021-45046 Up... (Feb 1)	RCE Log4J CVE-2021-44228 and CVE-2021-45046 U... (Feb 1)
What's New in the OnSolve Platform (Jan 31)	What's New in the OnSolve Platform (Jan 31)
View All	Edit

The **Announcements** page can also be accessed by navigating to **Support & Training > Announcements**. Announcements can be sorted by Date or Subject and deleted as needed. Each announcement includes an icon that denotes whether the announcement is related to a webinar, product update, or maintenance.

Announcements can also be sent directly to one or more emails or distribution lists. Select the notification bell and then the settings icon to open **Notification Settings**.

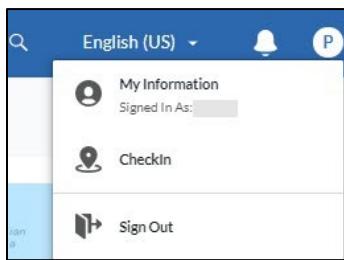


In **Notification Settings**, select **+ Add Email Address** and enter the desired email address. Enter up to ten email addresses.

Profile

The **Profile** drop-down menu is at the top right of any page. It is displayed as the first initial of the first name of the user who is currently signed in. Select the drop-down menu to:

- Select **My Information**, which leads to the people record of the signed-in user.
- **Check In**. Select **Check In** to mark your current location on the map. See [Check In](#) for more information.
- Exit the account at any time by selecting **Sign Out**. To adjust your account's timeout settings, contact Customer Support.



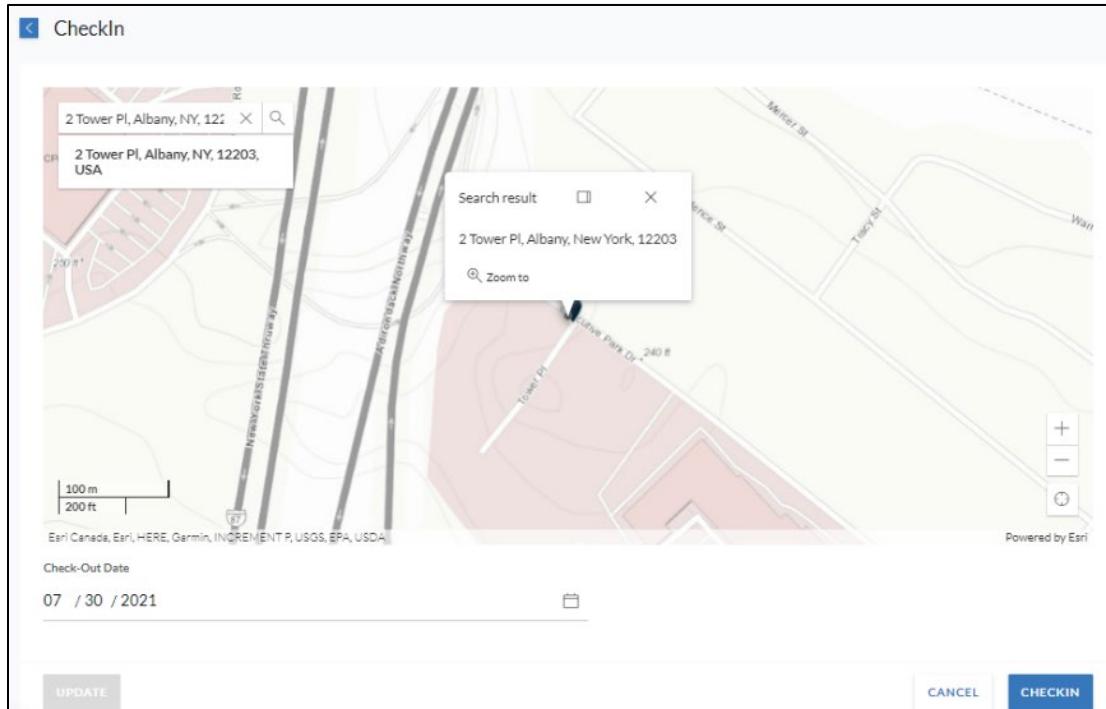
Check In

With the Check In feature, you can check yourself in from the control center view, providing a temporary location so that you get included in geofence alerts that include your location. With the applicable permissions, you can check others in via the people record **Locations** tab. See [Locations](#) in Section 2 of this guide for more information.

To check in

1. Select the **Profile** drop-down menu and then **Check In**.
2. Navigate to your location on the map and click to drop a pin. To pinpoint your location, you can:
 - Use the click and drag and zoom in/out features.
 - Use the **Find My Location** button.
 - Enter your address in the field at the top left of the map.
3. Enter the date you plan to leave that location in the **Check-Out Date** field.

4. Select Check In.



If at any time you need to update your location, repeat step 1, make the appropriate changes to location or **Check-Out Date**, and select **Update**.

Account Name

In this release, Customer Support will name the account. However, in a future release, the main account administrator will be able to define the name of the OnSolve Platform account in the **Account Name** field on the **General Information** tab of the **My Information** option of the **Profile** drop-down menu.

EDSERVICES

External Links

The following hyperlinks show at the bottom of every OnSolve Platform page:

www.onsolve.com | [Data Subject Rights Request](#) | [Privacy Statement](#) | [Copyright Notice](#) | [Contact Us](#)

OnSolve URL

Visit www.onsolve.com to see OnSolve's corporate website.

Data Subject Rights Request

The OnSolve Platform provides a mechanism to facilitate the Right to Be Forgotten. The Right to Be Forgotten allows you to request that any records held on you by a company be permanently deleted.

To make this request

1. Select **Data Subject Rights Request** at the bottom of any page. The form opens in a new browser tab.

 **ONSOLVE**
 English

Recipient Data Subject Rights

OnSolve may hold data about you and because of this, you have the right to request certain actions to be performed. Please complete the form below to request any of these actions. Data Subject Rights are based upon privacy laws including General Data Protection Regulation (GDPR) for European Union Citizens or California Consumer Protection Act (CCPA) for U.S. California Consumers, and other Laws as applicable.

OnSolve will review our systems for your data and provide a response as required by privacy laws.

Product Name:
OnSolve 10

Contact Info

* First Name: _____

* Email Address: _____

* Company Name: _____

* Required field(s)

* Last Name: _____

* Contact Phone: _____

Attach a copy of a notification that you have received:

DATA SUBJECT RIGHT
Please select from the following Data Subject Rights:

Right to be informed
I would like to be informed about the collection and use of my personal data.

Right of access
I would like the right of access to my personal data.

Right to rectification
I would like for data controllers to erase or rectify inaccurate or incomplete data.

Right to erasure
I would like for my personal data to be forgotten, deleted, and no longer processed.

Right to restrict processing
I would like to restrict the organization from processing my personal data.

Right to data portability
I would like to receive my personal data in a structured, commonly used, and machine readable format.

Right to object
I would like to object to the processing of my personal data.

Rights in relation to automated decision making and profiling
I would like for my personal data not to be subject based solely on automated processing, including profiling.

Sworn Statements / Legal notices
Please read the following statements and check the boxes to confirm that you agree.

I consent to the processing of the personal information that I am submitting in this form, as outlined below:
OnSolve, LLC (on behalf of itself and its affiliated entity) will use the personal information that you supply on this form (including your email address and any contact information) and any personal information you may submit in related correspondence for the purposes of processing your request and meeting our legal obligations. We may share details of your request with the controller associated with your information and data protection authorities.

I represent that the information in this request is accurate and that I am authorized to submit this request.
 I understand that OnSolve, LLC will not be able to process my request if the form is not properly completed.

Electronic Signature: _____ Today's Date: _____
06/17/2021

By typing your full name above, you are providing us with your digital signature, which is as legally binding as your physical signature. Please note that your signature must exactly match the first and last names that you entered at the top of this web form in order for your submission to be successful.

I'm not a robot



reCAPTCHA
Powered by Google

SUBMIT

2. In the request form, complete the required fields in the **Contact Info** section. This should be the contact information of the person to whom this request applies. Optionally, attach a copy of an alert that person has received (a screenshot, for example).
3. Select all actions you would like performed as part of this request:
 - **Right to be informed.** You would like to be informed about the collection and use of your personal data.
 - **Right of access.** You would like the right of access to your personal data.
 - **Right to rectification.** You would like for data controllers to erase or rectify inaccurate or incomplete data.
 - **Right to erasure.** You would like for your personal data to be forgotten, deleted, and no longer processed.
 - **Right to restrict processing.** You would like to restrict the organization from processing your personal data.
 - **Right to data portability.** You would like to receive your personal data in a structured, commonly used, and machine-readable format.
 - **Right to object.** You would like to object to the processing of your personal data.
 - **Rights in relation to automated decision making and profiling.** You would like for your personal data not to be subject based solely on automated processing, including profiling.
4. Check the three statement checkboxes to confirm that you agree with them.
5. Electronically sign the form by typing your name into the **Electronic Signature** field.
6. Select the **I'm not a robot** checkbox.
7. Select **Submit**. A confirmation screen will be displayed:

Recipient Data Subject Rights

OnSolve may hold data about you and because of this, you have the right to request certain actions to be performed. Data Subject Rights are based upon privacy laws including General Data Protection Regulation (GDPR) for European Union Citizens or California Consumer Protection Act (CCPA) for U.S. California Consumers, and other Laws as applicable.

OnSolve will review our systems for your data and provide a response as required by privacy laws.

Success!

Thank you, your data subject request has been submitted to the data controller.

[RETURN TO HOMEPAGE](#)

8. Select **Return to Homepage** if desired.

Privacy Statement

Follow this link to view OnSolve's Privacy Notice.

Copyright Notice

Follow this link to view OnSolve's Terms of Use.

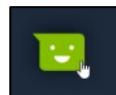
Contact Us

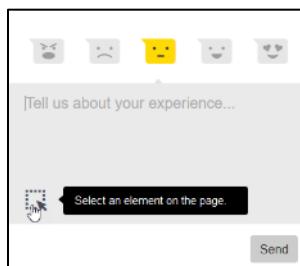
Follow this link to see several ways you can contact OnSolve for support.

User Feedback

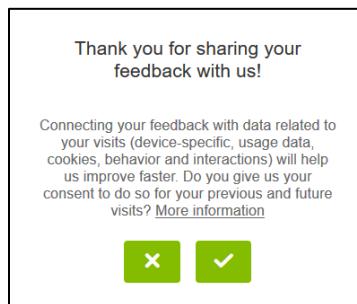
Within any page in the OnSolve Platform, users may provide feedback on their experience.



1. Select the  at the bottom left of the screen.
2. Select the icon that best represents the experience.



3. Use the text field to enter any details.
4. If desired, use the element selector to associate the UI element you described in your text.
5. Select **Send**.
6. If willing to be contacted by OnSolve about this experience, enter an email address.
7. Indicate consent to share data with OnSolve.

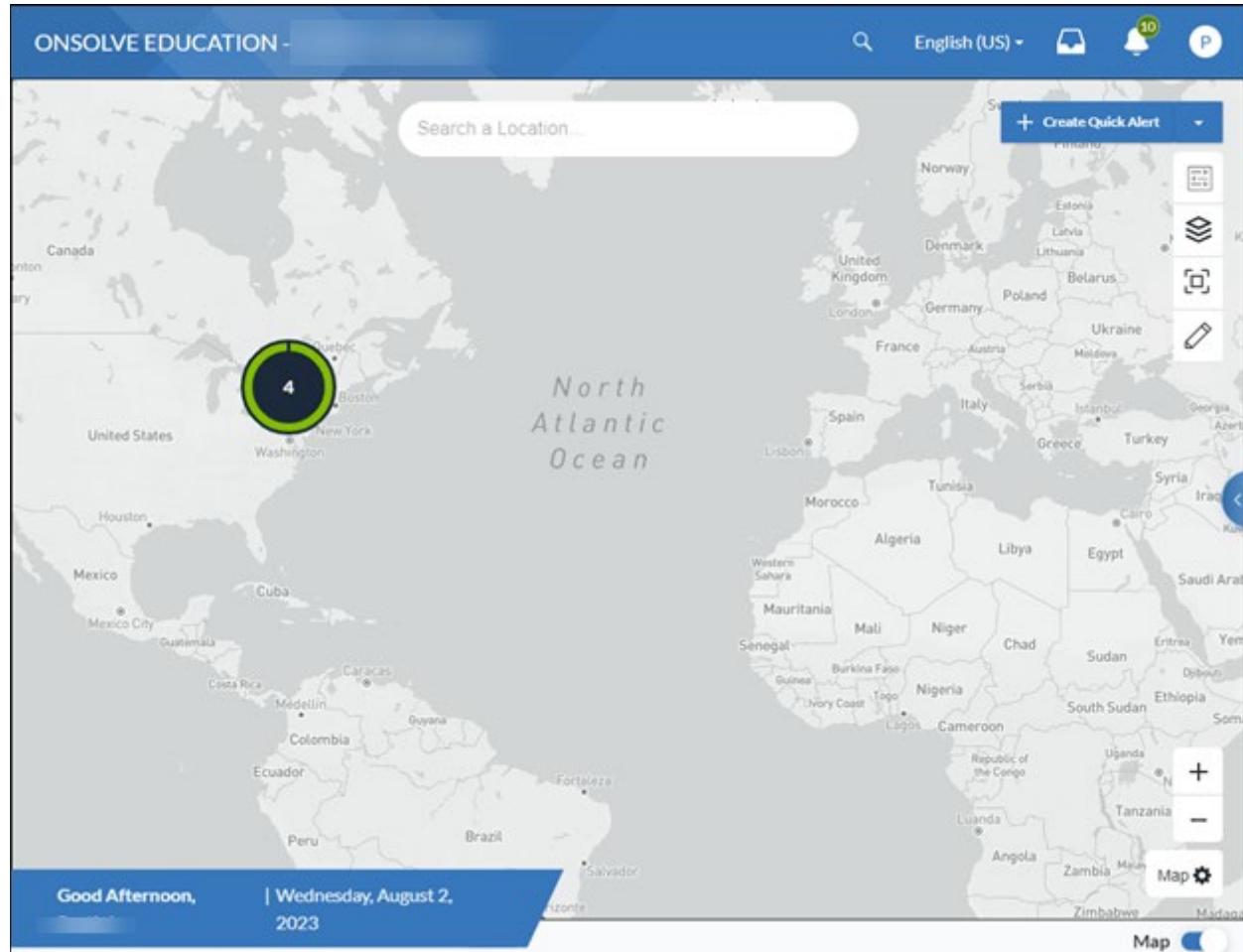


Control Center Configuration

The Control Center allows you to configure the map, widgets, and links in the Quick Links Bar to match how you work. Each user's customization is unique to their account.

Map

The first time you sign in to the OnSolve Platform, the control center view opens with a map and blank widgets. In this release, the map shows your account contacts only. In a future release, you will also be able to view events and facilities on the map.



Note: Settings for the widgets and map are persistent, meaning that when you make changes to the configurations and then log out, those changes are still set when you next sign in.

To filter what shows on the map on the Control Center view

1. On the map, select the  Filter button.
2. Toggle on the information that you want to show. In this release, **Contacts** is the only option.



3. Select **X** in the corner of the dialog box to close it after choosing what to show on the map.

To hide the map on the control center view

On the bottom right-hand corner of the map, select the **Map** toggle to turn the map off. Select the **Map** toggle again to turn it back on.

Note: The map toggle has persistence, meaning that if you turn the map off and then log out, the map does not show again until you turn it back on.

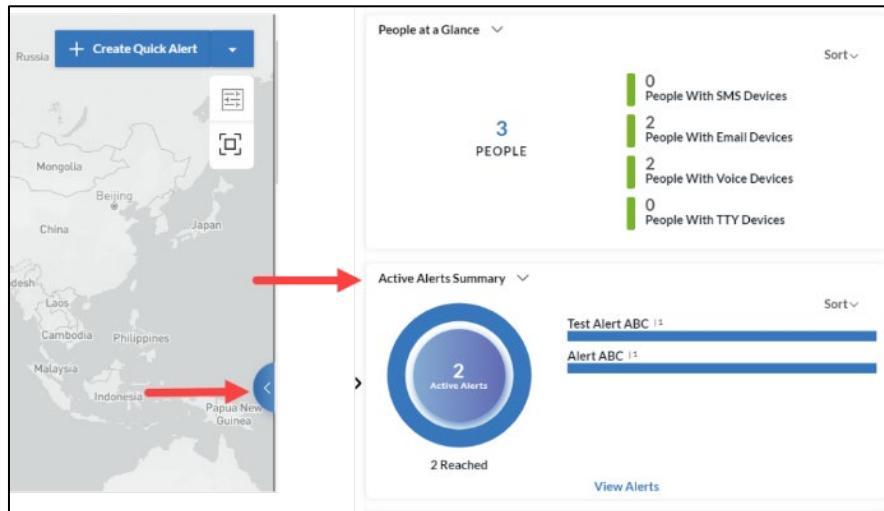


Widgets

The Control Center has widgets in two places: in the account widget drawer and below the Account Overview.

Account Widget Drawer

Select the blue tab at the right edge of the map to open the account widget drawer. In this release, the account widget drawer can be configured to contain the **People at a Glance** and **Active Alerts Summary** widgets. Select the arrow to the left of the account widget drawer to close it.



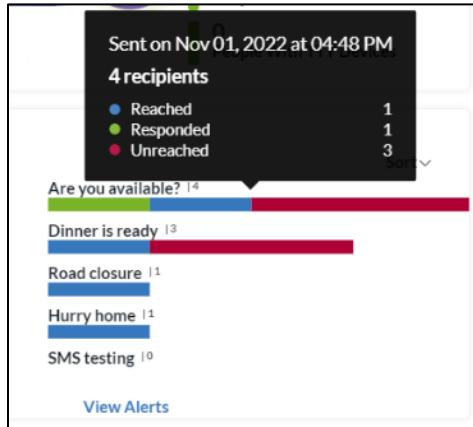
The **People at a Glance** widget provides a summary of the following:

- How many people have been added to, updated within, and removed from the account during the selected time frame.
- How many people in the account have active SMS, email, voice, and TTY devices.

Change the data time frame by selecting the **Sort** drop-down list and choosing from the options.



The **Active Alerts Summary** summarizes the data about your account's five most recent active alerts. While the widget automatically refreshes every 60 seconds, you can refresh the data at any time by closing and reopening the drawer. Each listed alert includes the alert name, how many people were sent the alert, and a bar depicting how many of those people were reached, unreached, and have responded. Hover over a bar to get details.

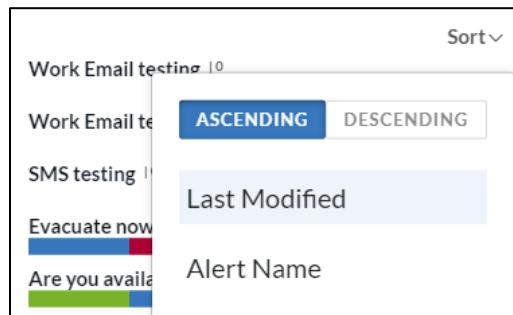


Select any alert name to see that alert's analytics, and select **View Alerts** to go to the **Alerts** page.

Hover over the **Active Alerts** circle to see how many people have been reached, unreached, and have responded from all active alerts.

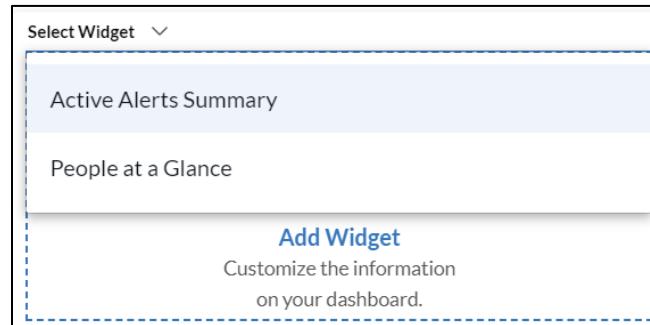


Sort your active alerts by **Last Modified** or **Alert Name** in **Ascending** or **Descending** order.

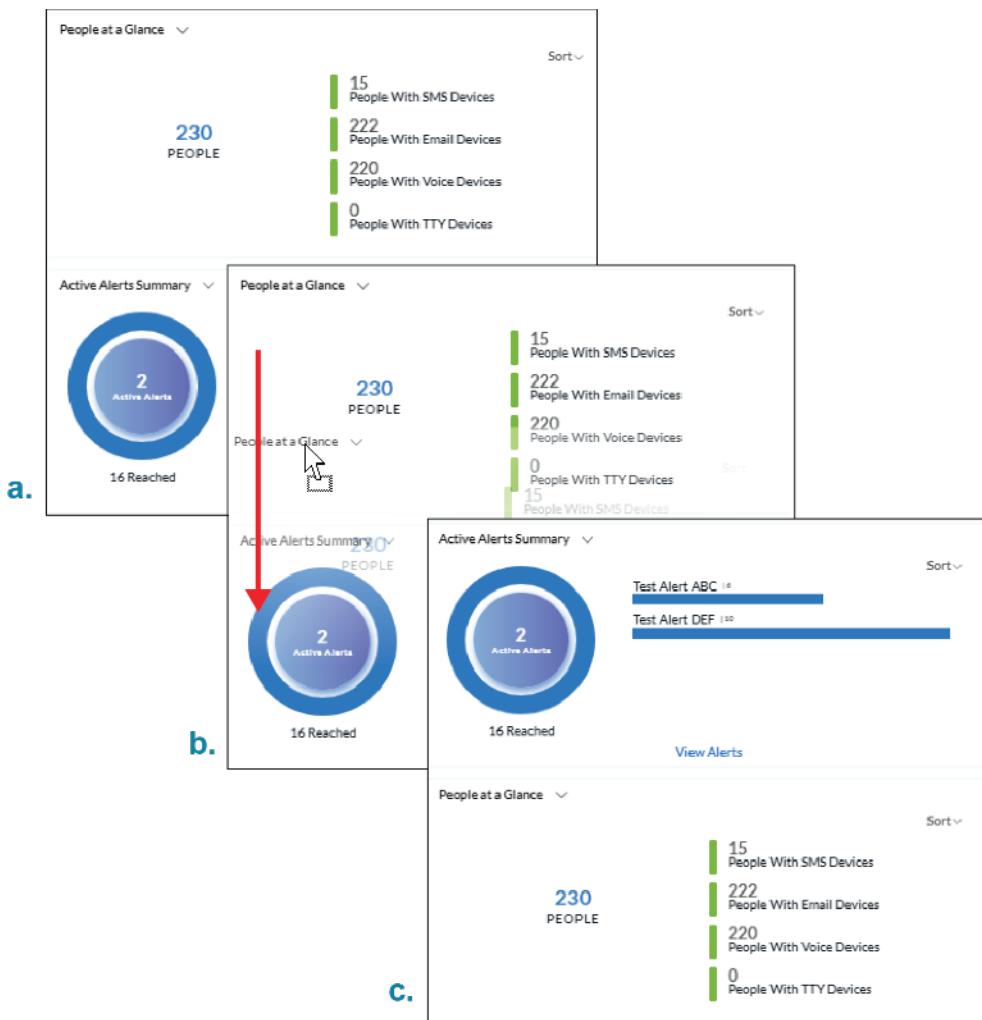


To configure a widget

- From the drop-down list, select one of the two options: **People at a Glance** or **Active Alerts Summary**.



- Drag and drop the widgets to any location in the account widget drawer.



To remove a widget

From the drop-down list, select the last option, **Remove Widget**.

Other Control Center Widgets

To show information from your account in any of the eight available widgets, you must configure them. If at any time fewer than eight widgets are displayed in your control center, select **+Add More Widgets** at the bottom of the page to configure additional ones.

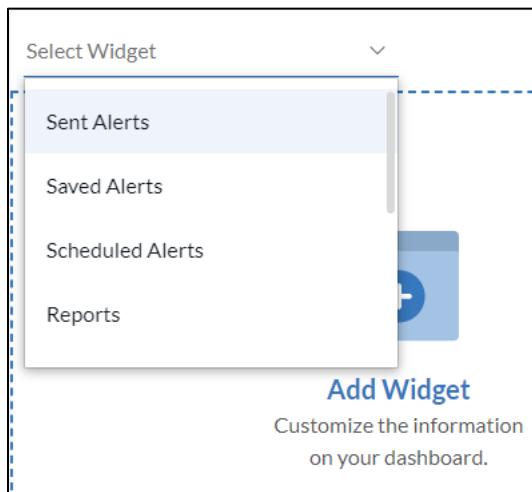


After configuring the widgets, they can be moved and arranged in the most convenient and helpful order to suit your purposes. Widgets self-arrange according to the size of your browser window or screen size, meaning that if you have a large monitor, four widgets appear side by side on a row, but for smaller screens, only one or two widgets fill a row. You can expand any widget to fit the width of your screen—and view additional columns—by selecting the widget expander (). Any adjacent widgets will shift down accordingly.

You can either view widget data directly from the control center view or load that data's page on a separate browser tab with the widget's pop-out button ().

To configure a widget

1. From the **Select Widget** drop-down list, select any of the possible options: **Sent Alerts**, **Saved Alerts**, **Scheduled Alerts**, **Reports**, **Schedules**, **Groups**, **Contacts**, or **Response Analytics**.

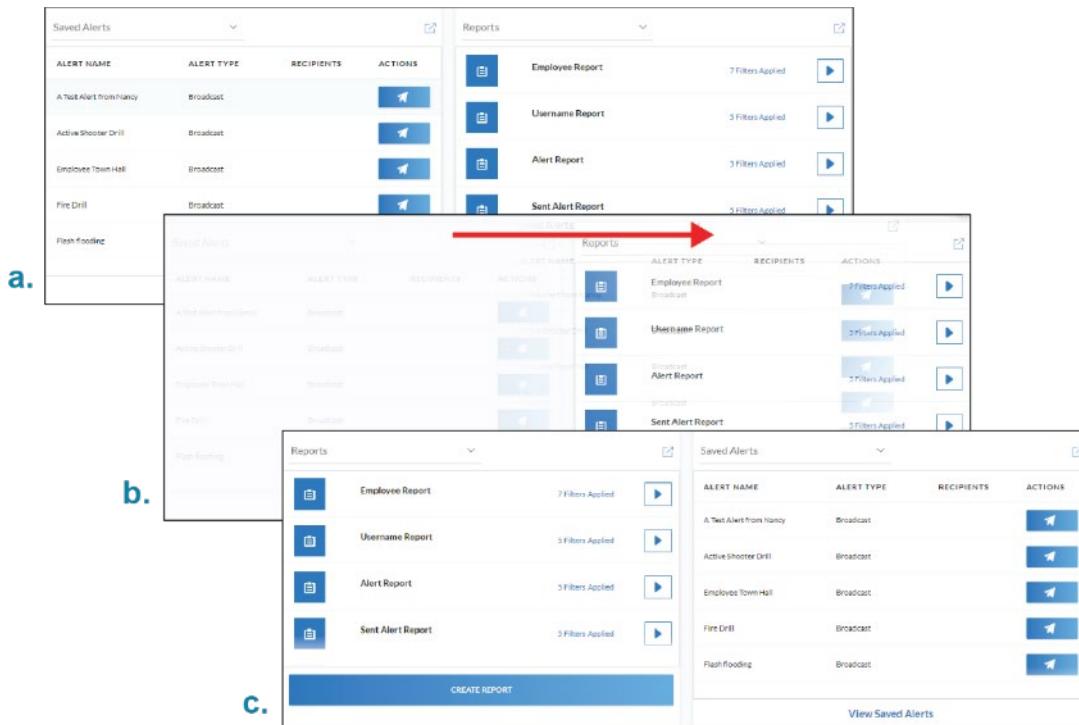


The widget shows the information that you chose, for example:

Saved Alerts			
ALERT NAME	ALERT TYPE	RECIPIENTS	ACTIONS
A Test Alert	Broadcast		
Active Shooter Drill	Broadcast		
Employee Town Hall	Broadcast		
Fire Drill	Broadcast		
Flash flooding	Broadcast		

[View Saved Alerts](#)

2. Drag and drop the widget to any location in the Control Center.



To remove a widget

From the **Select Widget** drop-down list, select the last option, **Remove Widget**.

Quick Links Bar

The Quick Links bar allows you to access commonly used areas within the OnSolve Platform quickly. You can create up to three links. Choose from **Announcements**, **Resource Library**, **Reports**, **What's New**, **Alert Module**, **Self-Registration**, **Permissions**, **Branding**, **Security**, **Weather & Events**, **Topics**, **Audit Trail**, **Usage**, **Call List**, and **Custom Reports**.



To assign a link to a Quick Link tile

1. Select  **Edit** on an available tile.
2. Select a feature from the drop-down list.



Section 2: Contact Management

Populate and Manage Contacts

A *contact* is a data record that contains the alert recipient's data, such as personal information; contact points; cascade order or profiles for voice devices; user privileges; address information for up to eight different locations; custom fields or attributes; and when OnSolve Mobile is enabled, lockbox items. The term *contact* is often used interchangeably to refer to an *alert recipient*; however, *contact* is the preferred term when referring to a record, while *alert recipient* is the preferred term when referring to an individual rather than a contact record. Every user must always have a contact record since their user credentials (access privileges) are housed within the contact record.

You can add contacts to an account either manually or via the Import Contacts tool. Follow the instructions below to [Create a New Contact](#) manually. To import many contacts at one time, see the *OnSolve Platform Import Contacts* User Guide.

Manage Contacts

The **People** page displays each contact's **Last Name**, **First Name**, **Role**, **Division**, and **Unique ID**.

Use the **Search** bar to quickly and easily locate contacts by **Last Name**, **First Name**, or **Unique ID**.

People					
	LAST NAME	FIRST NAME	ROLE	DIVISION	UNIQUE ID
<input type="checkbox"/>	Biden	Mike	Albany Sender	p	
<input type="checkbox"/>	Cat	Pumpkin	Initiator	p	
<input type="checkbox"/>	Copper	Team	Administrator	p	
<input type="checkbox"/>	Gauthier	Melissa	Administrator	p	
<input type="checkbox"/>	Granger	Hermione	Initiator	A	Hgranger
<input type="checkbox"/>	Harrison	George	Contact	p	
<input type="checkbox"/>	Lennon	John	Contact	p	

Display 25 Entries (Showing 1 to 18 of 18 Results)

Other features for managing contacts include:

- A **Filter** to refine results by **City, Company Name, Country, Device Type, Division, First Name, Job Title, Last Name, Location Types, Preferred Language, Province, Role, State, Subscription Category/Priority/Severity, Unique ID, or Zip Code**. Up to three filters may be applied.
- Ascending/descending sort (arrows in the table headers): By default, OnSolve Platform lists contacts in alphabetical order by **Last Name**. Select the arrow in the header to reverse the order or select any other column name to sort by.
- Pagination rows: Select to choose how many rows to display per page.
- Search field: Enter a Unique ID, Last Name, or First Name value (partial or complete) to find all contacts that fit the given criterion.
- Bulk **Delete**: Select the **Delete** button to delete more than one contact at a time after selecting the corresponding checkboxes to the left of each contact.
- **+ Create Contact**: Select this button to navigate to the **Create Contact** page.
- The **Import Contacts** feature. See the *OnSolve Platform Import Contacts* user guide for more information.
- **Export to CSV**. See [Export Contacts](#) for more information.

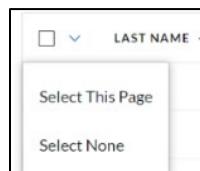
Export Contacts

You can export a maximum of 620,000 of your account contacts to a CSV file. For each contact included, the file lists their Primary Key, people record information, associated devices, group membership subscriptions, and custom fields. It does not list passwords for those contacts who have logins.

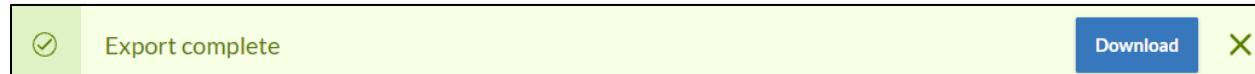
Note: If you have more than 620,000 contacts in your account, you can apply a filter(s) before step 1 below to pare your contacts down to fewer than 620,000. Export, then repeat, applying complementary filters until all contacts have been exported.

To export contacts

1. Select which contacts you want to export.
 - To export all contacts, select *no* checkboxes.
 - To export select contacts, check the checkboxes next to the desired contacts or use the **Select This Page** option.



2. Select **Export to CSV**. When the export is complete, a **Download** button appears.



3. Select **Download**. The CSV file downloads to your computer. The **Download** button is available for 24 hours from the completion of the export.

View as User

The View as User feature allows users with this permission to view and act as another user in the same organization, in turn allowing those users to verify what others have access to within the OnSolve Platform. To view as another user, the target user must have a username and password saved in their people record.

To view as user

1. Select the desired contact from the **People** page. That contact's record opens.
2. Select **View as User** from the top right of the page. The control center view opens so you can view the OnSolve Platform and act as the selected contact.

Any time you are viewing as another user, the OnSolve Platform displays a banner with the name of the contact you are viewing as.



To stop viewing as that user, select **Exit View**.



Affiliations

The **Affiliations** section of a people record is a list of all instances where that contact:

- Is a member of a group (including a map group)
- Is a member of a schedule
- Has been listed as an alternate contact
- Has been included as a recipient in an alert

Each affiliation includes the date when that affiliation started.

View a contact's affiliations by navigating to **People**, selecting the desired contact, and selecting the **Affiliations** section. This section is not editable.

REFERENCE	TYPE
Chi-Group3	Member of Contact Group
dan.multiple4	Alert Contact

Modify a Contact

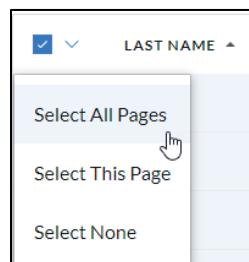
To modify a contact

1. Select **People** from the left navigation menu.
2. Select the desired contact. That contact's record opens to the **Overview**.
3. Select any of the tabs (**Devices**, **Custom Fields**, etc.) to make edits in those tabs. Select **Save** after making changes on any tab.

Delete a Contact

To delete a contact

1. On the **People** page, select the checkbox next to the desired contact(s). To delete a full page of contacts, select the drop-down arrow next to the checkbox in the header row, and choose **Select This Page**. To delete all contacts in the account, select the same drop-down arrow and **Select All Pages**.



2. Select **Delete**.
3. Select **Delete** again to confirm.

Create a New Contact

Overview

1. From the **People** page, select **+ Create Contact**. The **Create Contact** page opens to the **Overview** (see the next page).
2. Enter the contact's **First** and **Last Names**. Optionally, enter a **Middle Name**.
3. Optionally, add the contact's **Unique ID**, **Job Title**, **Company Name**, **Telephony ID**, and **PIN**.
 - **Unique ID:** an optional identifier unique to the contact, such as an employee ID, badge number, etc.

Note: Although optional, it is highly recommended to utilize this data field. The **Unique ID** is used as the index to identify existing records during data maintenance.

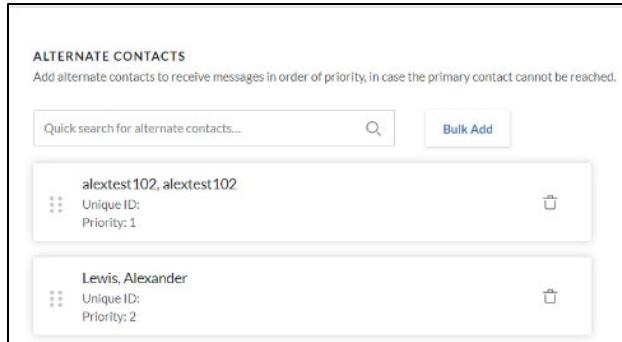
 - **Telephony ID:** This unique ID identifies the recipient and matches the caller during the retrieval of pending messages. This is an auto-generated number unless customized here. The Telephony ID is not required if calling from a number saved in the recipient's people record.
 - **PIN:** This Personal Identification Number can be set to be required in conjunction with the Telephony ID when retrieving messages and sending alerts.
4. Select the **Division** the contact should be a part of.
5. Select the contact's **Time Zone**.

6. Select the contact's Preferred Language.

Create Contact

OVERVIEW	DEVICES	CUSTOM FIELDS	LOCATIONS
<p>FirstName Enter first name 0/120</p> <p>Middle Name (Optional) Enter middle name 0/120</p> <p>Last Name Enter last name 0/120</p> <p>Unique ID (Optional) Enter unique ID 0/100</p> <p>Job Title (Optional) Enter job title 0/100</p>			
<p>Company Name (Optional) Enter company name 0/100</p> <p>Telephony ID (Optional) Enter telephony ID 0/15</p> <p>PIN (Optional) Enter PIN 0/8</p> <p>Division Maple Demo</p> <p>Time Zone UTC</p> <p>Preferred Language English (GB)</p>			
<p>ALTERNATE CONTACTS Add alternate contacts to receive messages in order of priority, in case the primary contact cannot be reached</p> <p>Quick search for alternate contacts... <input type="text"/> <input type="button" value="Advanced Search"/></p>			

7. Optionally, assign up to 20 **Alternate Contacts**. These contacts receive alerts when the primary contact cannot be reached. Use the search field to search by name or select **Bulk Add** to sort by names and roles and select multiple contacts at once. Once added, alternate contacts can be dragged into a different contact order or deleted.



The screenshot shows a list of alternate contacts. At the top, there is a header 'ALTERNATE CONTACTS' and a note: 'Add alternate contacts to receive messages in order of priority, in case the primary contact cannot be reached.' Below this is a search bar labeled 'Quick search for alternate contacts...' with a magnifying glass icon and a 'Bulk Add' button. Two contacts are listed in a table format:

alextest102, alextest102	Unique ID:	<input type="button" value="Delete"/>
	Priority:	1
Lewis, Alexander	Unique ID:	<input type="button" value="Delete"/>
	Priority:	2

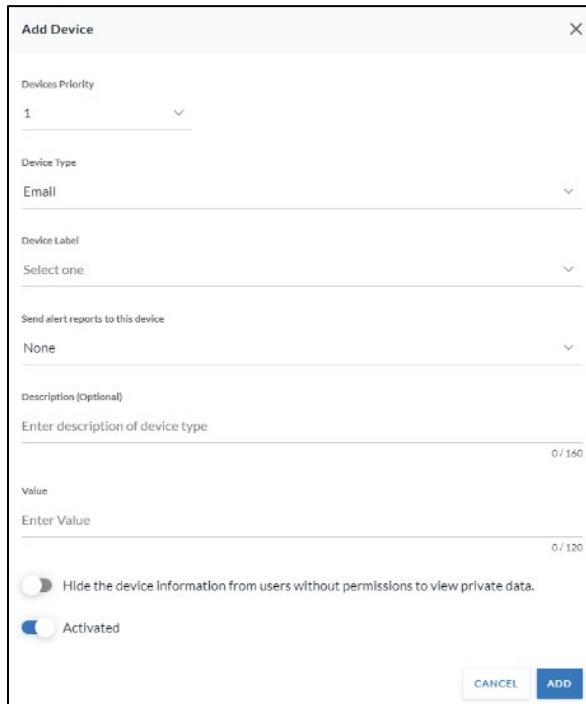
8. Select **Next** to move on to **Devices**.

Devices

Device labels are created ahead of time by navigating to **Settings > Alert Module > Labels**. See [Device Labels](#) in Section 8 of this guide for more information.

Adding a device is optional. To skip this step, select **Next**.

1. Select **Add Device**. The **Add Device** window opens.



The 'Add Device' window contains the following fields:

- Device Priority:** A dropdown menu set to '1'.
- Device Type:** A dropdown menu set to 'Email'.
- Device Label:** A dropdown menu set to 'Select one'.
- Send alert reports to this device:** A dropdown menu set to 'None'.
- Description (Optional):** A text area with placeholder 'Enter description of device type' and character count '0 / 160'.
- Value:** A text area with placeholder 'Enter Value' and character count '0 / 120'.
- Hide the device information from users without permissions to view private data.**: A toggle switch.
- Activated**: A toggle switch.

At the bottom right are 'CANCEL' and 'ADD' buttons.

2. Choose a **Devices Priority**. This determines the order in which this device will be contacted in the case that an alert sender selects multiple modalities and chooses not to have the system overrule this order.
3. Choose a **Device Type**. Options are:
 - Voice
 - TTY Phone
 - Email
 - Pager One Way
 - Pager Two Way
 - Pager Numeric
 - SMS
 - Fax
 - Any custom labels

Notes

When you select **Email** as the device type, you can then **Send alert reports to this device** in conjunction with the **Send periodic reports** advanced setting, coming in a future release. Choose **None**, **PDF**, or **Text** as the output type. This field is required; if you do not want this contact to receive alert reports, choose **None**.

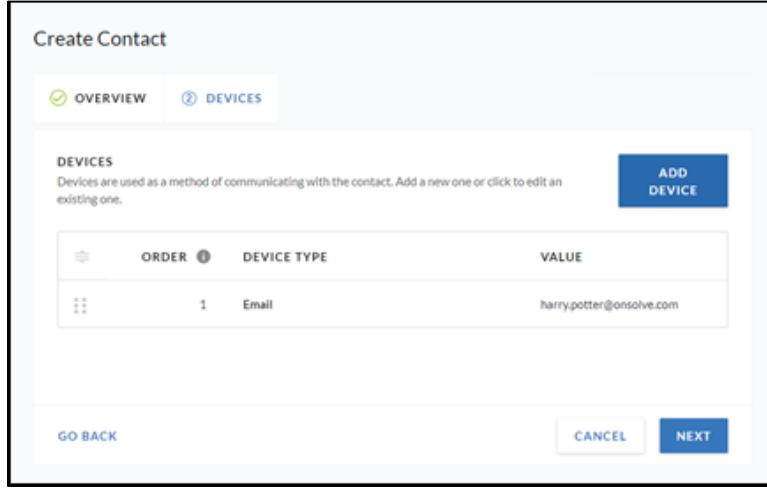
When you select any pager options as the device type, two additional fields are displayed: **Pager Carrier**, a drop-down list from which you must select their pager carrier, and optional **PIN**.

OnSolve Mobile is listed as a device in a people record when that contact is signed in to the app. When they sign out, the device is removed from their people record.

The alphanumerical string in the **Value** column of the **Devices** tab of a people record is the mobile app ID and is unique to each device with OnSolve Mobile.

4. Choose a **Device Label**.
5. Optionally, enter a **Description** for the device.
6. Enter the **Value** for the device. For instance, enter a phone number if the device type is Voice. See [Appendix D](#) in this guide for information on phone number formatting.
7. Choose whether to hide the device address from users who do not have permission to view private data.
8. Choose whether this device should be active (default) or inactive. The device is never contacted when inactive but remains saved to the people record.

- Select **Add**. The device is added to that contact.



Create Contact

OVERVIEW **DEVICES**

DEVICES
Devices are used as a method of communicating with the contact. Add a new one or click to edit an existing one.

ORDER	DEVICE TYPE	VALUE
1	Email	harry.potter@onsolve.com

ADD DEVICE

GO BACK **CANCEL** **NEXT**

- Add another device or select **Next** to move on to **Custom Fields**.

Custom Fields

Custom fields are created ahead of time by navigating to **Settings > Alert Module > Labels** and selecting the **Custom Fields** tab. See [Custom Fields](#) in Section 8 of this guide for more information. Adding custom fields is optional.

To add a custom field

- Select **Add Custom Field**. The **Add Custom Field** window opens.



Add Custom Field

Select a custom field to add.

Custom Field

Select one

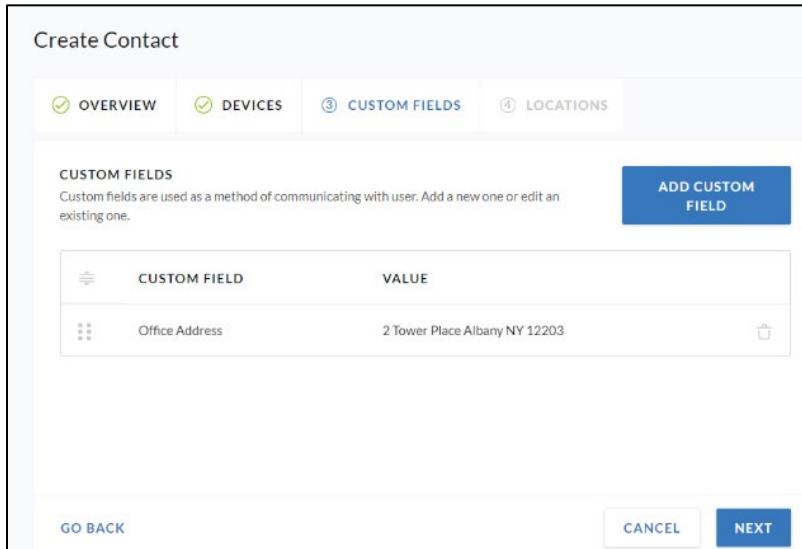
Value

Please enter a value

CANCEL **ADD**

- Choose a **Custom Field**.

3. Enter a **Value** for that custom field. For example, if the custom field is “Department,” the value could be “Sales.”
4. Select **Add**. The custom field is added to that contact.



The screenshot shows the 'Create Contact' screen with the 'CUSTOM FIELDS' tab selected. A table lists a single custom field: 'Office Address' with the value '2 Tower Place Albany NY 12203'. There is a blue 'ADD CUSTOM FIELD' button at the top right of the table area.

CUSTOM FIELD	VALUE
Office Address	2 Tower Place Albany NY 12203

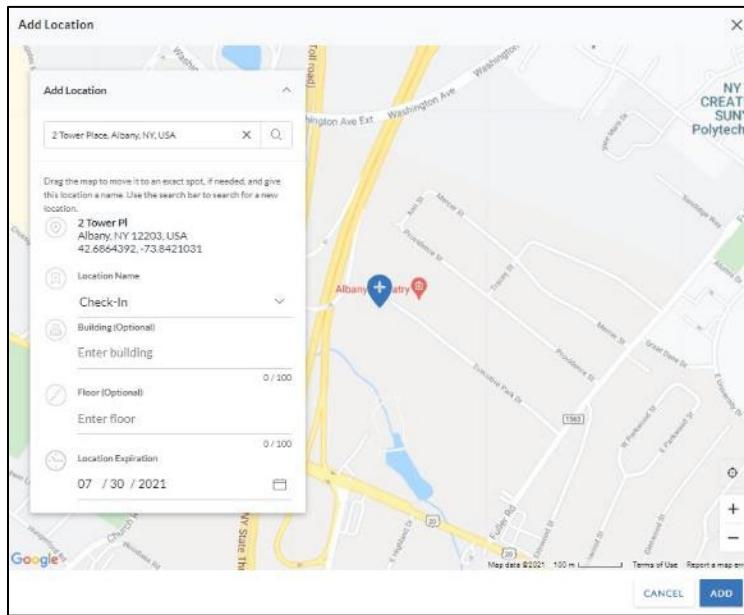
5. Add more custom fields or select **Next** to move on to **Locations**.

Locations

Locations are used when alert senders want to target a specific geographic area. Add locations to a people record so that when these geo-enabled alerts are sent, contacts with saved locations in that area are alerted. Additionally, using **Check In** as a location allows you to set an expiration date for the contact being at that location. Adding locations is optional.

To add a location

- From the **Locations** tab, select **Add Location**. The **Add Location** window opens.



- Enter an address into the search field and press the enter key or select the search icon.
- Choose a **Location Name** or **Check-In**. The location name options in this drop-down list are sourced from the [Location Labels](#) page.
- Optionally, add a **Building**.
- Optionally, add a **Floor**.
- If you chose **Check-In** in step 3, enter a **Location Expiration**. Once the expiration date is passed, this location is automatically deleted from the people record.
- Select **Add**. The location is added to the **User Locations** list.
- Select **Save**, then **Next** to continue to **Subscriptions**.

Subscriptions

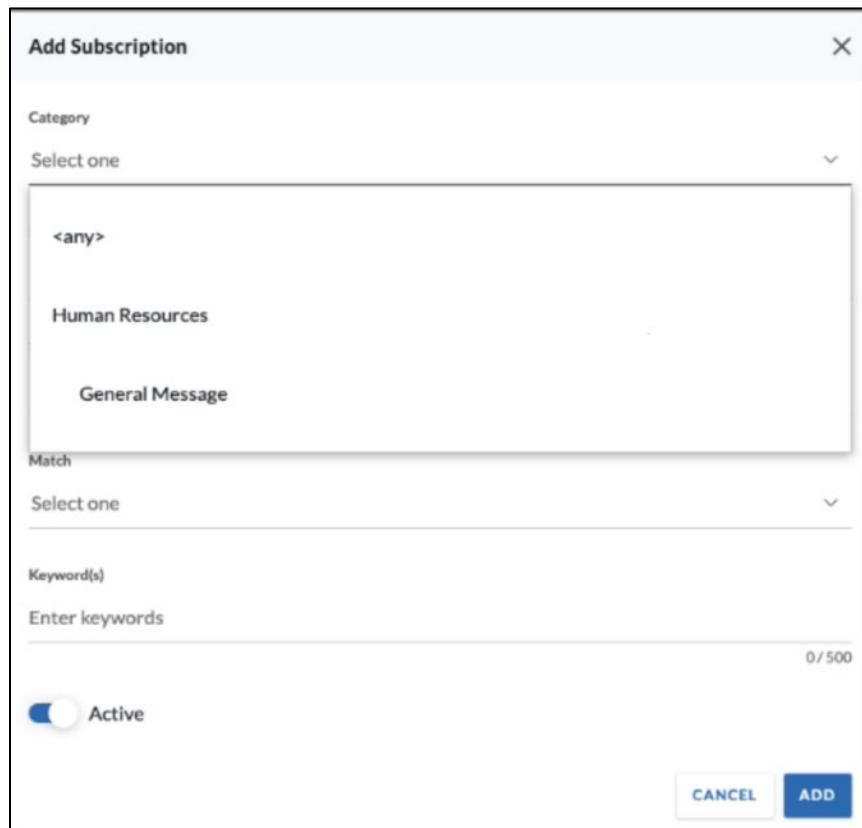
Subscriptions allow contacts to receive alerts according to the topics that alert senders choose upon creating an alert. When a contact subscribes to a topic, they receive any alerts tagged with that topic that meet the contact's subscription match criteria.

Topics are comprised of categories, priority levels, and severity levels. These topics must be created and saved in the account before contacts can subscribe to them. See [Topics](#) in Section 6 of this guide to learn how to create them.

You can also suppress subscriptions. That is, you can define a time frame during which contacts will not receive alerts containing topics to which they are subscribed.

To add a subscription

1. Select **Add Subscription**. The **Add Subscription** window opens.
2. Select one option from any of the **Category**, **Priority**, and **Severity** drop-down lists. Each drop-down list has the option of <**any**> so that you are not limited to only one choice in each list.



The screenshot shows the 'Add Subscription' dialog box. It has sections for 'Category' (with a dropdown 'Select one' and an option '<any>'), 'Match' (with a dropdown 'Select one'), and 'Keyword(s)' (with a text input field 'Enter keywords' and a character count '0 / 500'). At the bottom is a toggle switch labeled 'Active' and two buttons: 'CANCEL' and 'ADD'.

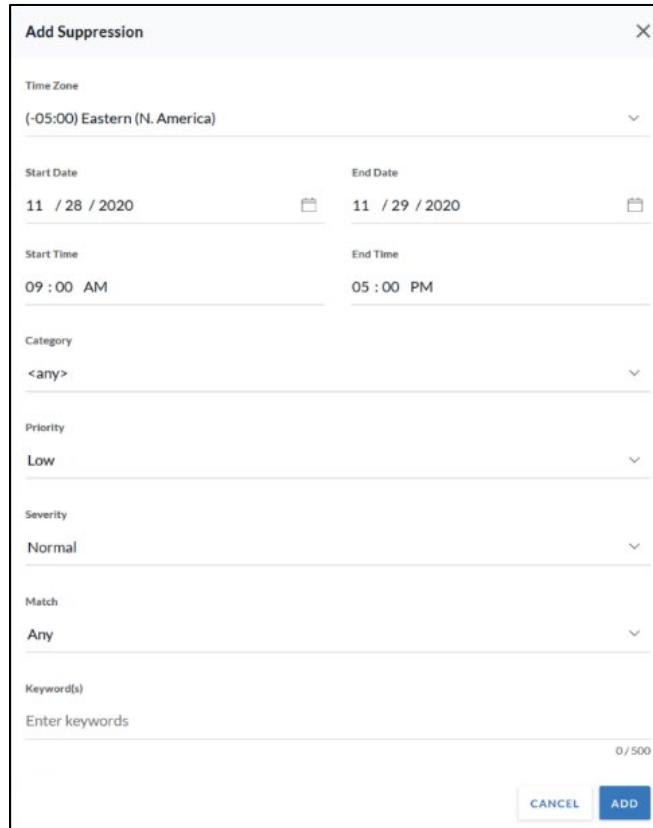
3. In the **Match** drop-down list, select:
 - **All**. This contact receives an alert only if the alert matches the category, priority, and severity selected in step 2 and contains all the keywords entered in step 4.
 - **Any**. This contact receives an alert only if the alert matches the category, priority, and severity selected in step 2 and contains any of the keywords entered in step 4.
 - **Advanced**. This contact receives an alert only if the alert matches the category, priority, and severity selected in step 2 and contains keywords according to the Boolean expression you can enter in step 4.
4. If desired, enter keywords that must be present in an alert for the contact to receive it. Use spaces or commas to separate multiple keywords if you select **All** or **Any** as the match in step 3. Enter a Boolean expression if you select **Advanced** in step 3.
5. By default, this subscription is **Inactive**. Optionally, toggle the subscription to be active.
6. Select **Add**. The contact receives alerts that include all four components of the subscription: category, priority, severity, and keyword(s).
7. Add more subscriptions and suppressions, or select **Next** to continue to **User Privileges**.

To add a suppression

1. From the **Subscriptions** tab, select **Suppressions**.



2. Select **Add Suppression**. The **Add Suppression** window opens.



The screenshot shows the 'Add Suppression' dialog box. It includes fields for Time Zone (-05:00) Eastern (N. America), Start Date (11 / 28 / 2020) and End Date (11 / 29 / 2020), Start Time (09 : 00 AM) and End Time (05 : 00 PM). There are dropdowns for Category (<any>), Priority (Low), Severity (Normal), and Match (Any). A text input field for Keyword(s) with placeholder 'Enter keywords' and character count '0 / 500'. At the bottom are 'CANCEL' and 'ADD' buttons.

3. Select the **Time Zone** to which the suppression times will apply.
4. Select a **Start Date** and **End Date**.
5. Select a **Start Time** and **End Time**.
6. Select a **Category**, **Priority**, and **Severity** for which this suppression applies. Each drop-down list has the option of <any> so that you are not limited to just one choice in each list.
7. In the **Match** drop-down list, select either:
 - **All**. Alerts will only be suppressed if the alert contains all the topics included in this suppression.
 - **Any**. Alerts will be suppressed if the alert contains any of the topics included in this suppression.
 - **Advanced**. Add keywords that must be included in the alert name or message body to suppress the alert.
8. Select **Add**.
9. Add more subscriptions and suppressions, or select **Next** to continue to **User Privileges**.

User Privileges

The **User Privileges** tab is where an authorized user can assign a role to a contact, enable them as a user of the OnSolve Platform, and unlock their account if they are locked out.

Configure User Privileges

If desired, assign users the ability to sign in to the OnSolve Platform and assign them the roles of an administrator, initiator, a custom role, or one or more custom role templates.

CONFIGURE USER PRIVILEGES
Enable user login and select a role to configure privileges for this contact.

Administrator
Administrators have full access to the account, including default configurations, feature settings, user role creation, and access to all divisions.

Initiator
Initiators have access to send alerts, view reports, as well as manage contacts and groups.

Contact
When user privileges are disabled, the contact role is assigned by default.

Albany Sender

Atlanta Sender

Custom Role Template
Create a custom role for a contact by assigning role templates and associating them with specific divisions.

ASSIGNED ROLE TEMPLATE
The list of the Role Templates that have been added to the contact's profile.

ADD ROLE TEMPLATE

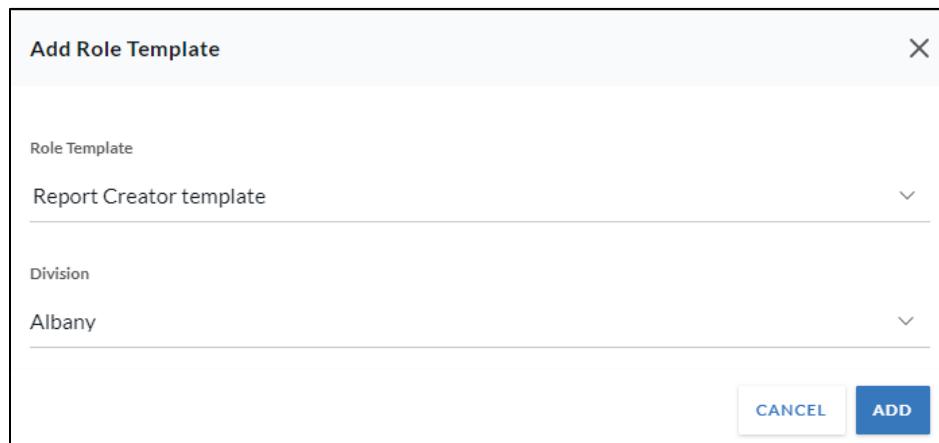
To assign user privileges

1. Select a role for this user. Options include:

- **Administrator:** Full access to the account, including default configurations, feature settings, user role creation, and access to subaccounts.
- **Initiator:** Access to send alerts and manage contacts and groups.
- **Contact (Recipient):** No access to the account. Synonymous with having user privileges disabled. This is the default role.

Note: The name for this role is “Recipient” when managing roles from the **Configure > Permissions > Roles** or **Add Role** pages. The name for this role is “Contact” in all other places in the user interface.

- **Custom Role:** When custom roles are saved to the account, they are listed here. See [Add a Role](#) in Section 7 of this guide to create a custom role.
 - **Custom Role Template:** The **Add Role Template** button is active when custom role templates are saved to the account. See [Add a Role Template](#) in Section 7 of this guide to create a custom role template.
2. If you select **Custom Role Template**, follow these steps to add up to 150 role templates per user:
- a. Select **Add Role Template**. The **Add Role Template** window opens.



The screenshot shows a modal window titled "Add Role Template". It has two dropdown menus: "Role Template" set to "Report Creator template" and "Division" set to "Albany". At the bottom are "CANCEL" and "ADD" buttons.

- b. Select a **Role Template** from the drop-down menu.
 - c. Select the **Division** where the permissions in the template will apply.
 - d. Select **Add**.
 - e. Repeat steps a–d to add up to 150 role templates per user.
3. Optionally, select **Enable User Login**.



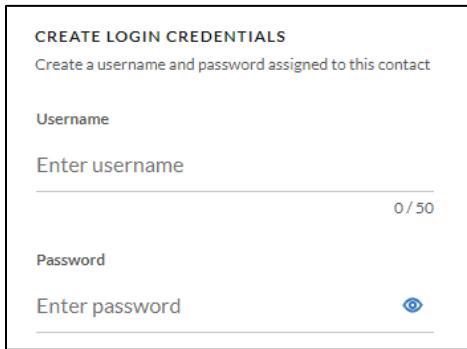
Create Login Credentials

1. Assign a **Username** and **Password** for this user.

CREATE LOGIN CREDENTIALS
Create a username and password assigned to this contact

Username
Enter username _____ 0 / 50

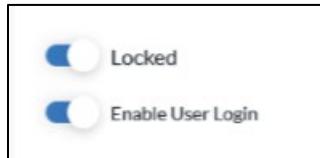
Password
Enter password 



2. Select **Save**

Unlock User Account

Users are locked out of their accounts when they attempt to sign in too many times without success. In this case, a **Locked** toggle is displayed on the **User Privileges** tab, but only for those users with the [Unlock User Account](#) permission. Those authorized users may unlock these accounts by toggling off the **Locked** option.



Reset Security Questions

If you have security questions enabled for the account, you can reset a contact's security questions by selecting **Reset Security Questions** and then **Confirm**. The next time that contact attempts to sign in, they must first select a new security question and provide the answer.

Custom Role Template
Create a custom role for a contact by assigning role templates and associating them with specific divisions.

Enable User Login

SECURITY QUESTIONS
Security questions allow for account recovery.

RESET SECURITY QUESTIONS

CANCEL **SAVE**



Create and Manage Groups

Creating groups within the OnSolve Platform allows users to group alert recipients to reflect organizational structure, divisions, and business units. You can then send targeted alerts to these groups and avoid over-alerting the entire organization. Targeted alerting also facilitates delegating alerting privileges to specific individuals based on job responsibilities.

All groups are displayed via the **Groups** option on the left navigation menu.

Group Types

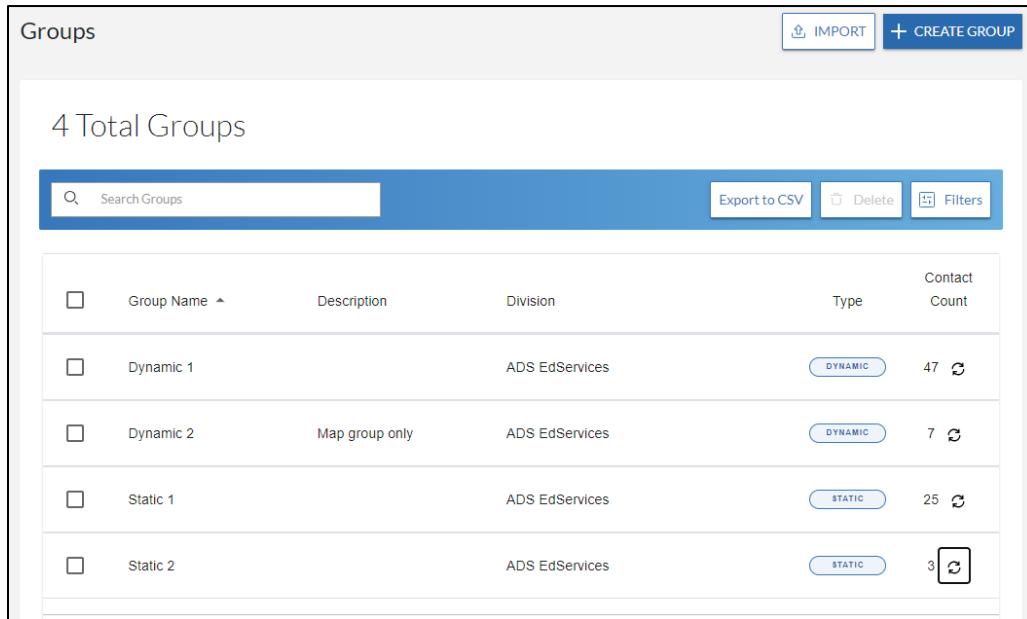
There are two main group types:

- **Static Groups:** Static groups are created by selecting specific people to be group members.
- **Dynamic Groups:** Dynamic groups are groups whose membership is defined by criteria. As data in the account changes and updates, so do dynamic groups. A group containing map shapes, filters, or other groups, is considered a dynamic group.

Manage Groups

The **Groups** page displays each group's **Group Name**, **Description**, **Division**, **Type**, and **Contact Count** (number of alert recipients in a group).

A **Search** bar is provided to locate groups quickly and easily by the **Group Name**, **Group Description**, or **Division**.



The screenshot shows the 'Groups' page with the following details:

	Group Name	Description	Division	Type	Contact Count
<input type="checkbox"/>	Dynamic 1		ADS EdServices	DYNAMIC	47
<input type="checkbox"/>	Dynamic 2	Map group only	ADS EdServices	DYNAMIC	7
<input type="checkbox"/>	Static 1		ADS EdServices	STATIC	25
<input type="checkbox"/>	Static 2		ADS EdServices	STATIC	3

Other features for managing groups include:

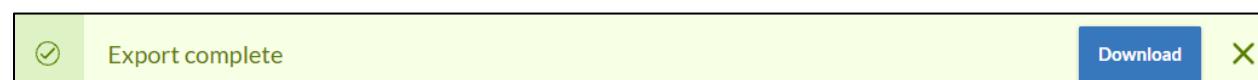
- A **Filter** to refine results by **Group Description**, **Group Division**, **Group Name**, or **Group Type**.
- Ascending/descending sort (arrows in the **Group Name** table header): By default, groups are listed alphabetically. Select the arrow in the header to reverse the order.
- The refresh icon  to refresh the contact count for any group.
- **Delete**. Select the checkbox next to any group and select **Delete** to delete that group.
- **Load More**. If your account has more saved groups than displayed, select **Load More** at the bottom of the page to load more groups.
- **Bulk Delete**. Select **Delete** after selecting the corresponding checkboxes to the left of each group.
- **+ Create Group**. Select this button to navigate to the **Create Group** page.

Export Groups

You can export any and all groups in your account to a CSV file. For each group included, the file will list the Group Primary Key, Group Name, Group Division, and for every group member, their people record information, associated devices, and custom fields. It does not list passwords for those contacts who have logins.

To export groups

1. Select which groups you want to export.
 - To export all groups, select *no* checkboxes.
 - To export select groups, select the checkboxes next to the desired groups.
 - Use the **Search Group** field to find desired groups by **Group Name**, **Description**, or **Division**.
 - Filter groups by **Group Description**, **Group Division**, **Group Name**, or **Group Type**.
2. Select **Export to CSV**. When the export is complete, a **Download** button is displayed.



3. Select **Download**. The CSV file downloads to your computer. The **Download** button is available for 24 hours from the completion of the export. Additionally, the file is emailed to you if you have an email address saved in your people record.

Edit Groups

Any group can be edited by selecting it on the **Groups** page. Select the edit  icon in any criterion, make any desired changes, select the checkmark  , then select **Save**.

Delete Groups

To delete groups

From the **Groups** page, select the checkbox next to each desired group and select **Delete**.

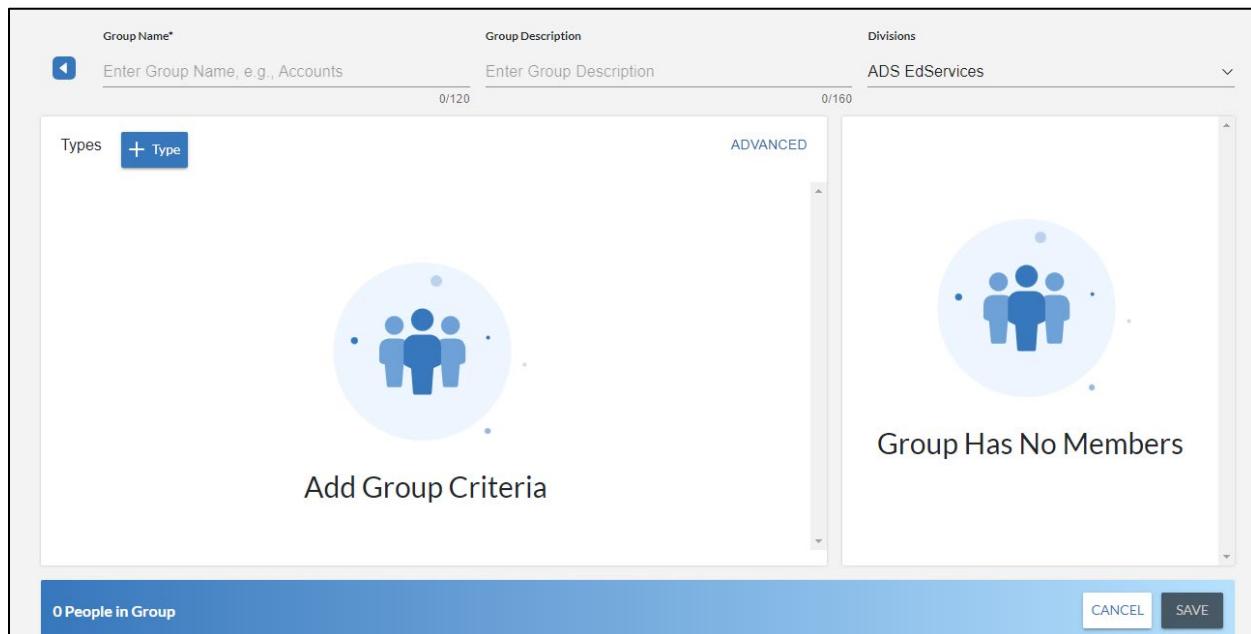
Create a Group

Membership in a group is determined by the criteria you set. Criteria can be defined by the inclusion or exclusion of:

- Specific, manually selected people.
- People who have saved addresses in a map shape-defined area.
- People with other people record attributes, such as a particular job title or user role.
- Other groups.

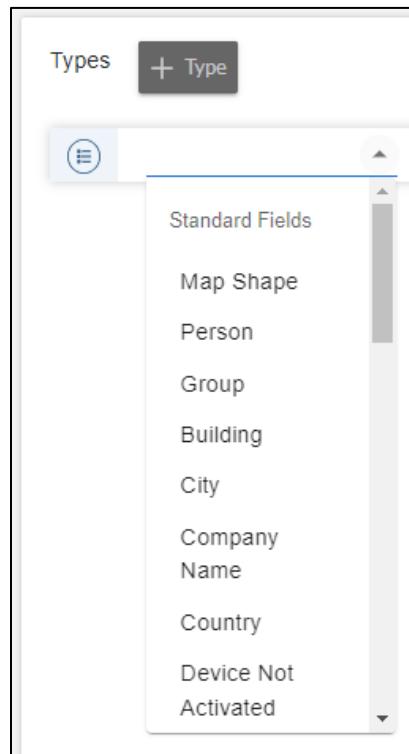
To create a group

1. From the **Groups** page, select **+Create Group**. The Create Group page opens.



The screenshot shows the 'Create Group' page. At the top, there are fields for 'Group Name*' (with placeholder 'Enter Group Name, e.g., Accounts'), 'Group Description' (with placeholder 'Enter Group Description'), and 'Divisions' (set to 'ADS EdServices'). Below these are sections for 'Types' (with a '+ Type' button) and 'Add Group Criteria' (with a circular icon showing three blue figures). A message 'Group Has No Members' is displayed. At the bottom, a blue bar shows '0 People in Group' and contains 'CANCEL' and 'SAVE' buttons.

2. Enter a **Group Name**.
3. Optionally, enter a group **Description**. This field can describe the intent of the group, who it contains, or when to send alerts to this group.
4. Select the **Division** in which this group should reside.
5. Select **+Type** to add a criterion.
6. In the first drop-down menu, select a parameter. Options are:
 - [Person](#)
 - [Map Shape](#)
 - [Group](#)
 - [Contact record attributes](#), such as **Building**, **First Name**, or a saved device type.
 - [Device attributes](#)
 - [Custom fields](#)



7. Complete the criterion by following the instructions specific to the items listed above, and selecting the checkmark  to save. At any point, select the edit icon to edit the criterion or the delete icon to delete it.

8. Optionally, repeat steps 5–7 to add up to 125 criteria. As you add criteria, the section on the right updates the list of people in your group.

Name	Division	Role
	ADS EdServices	Administrator
Melody Aguon	ADS EdServices	Recipient
Tony Almond	ADS EdServices	Recipient
Doyle Baker	ADS EdServices	Recipient
Madeline Barker	ADS EdServices	Recipient
	ADS EdServices	Administrator
Karen Bozeman	ADS EdServices	Recipient

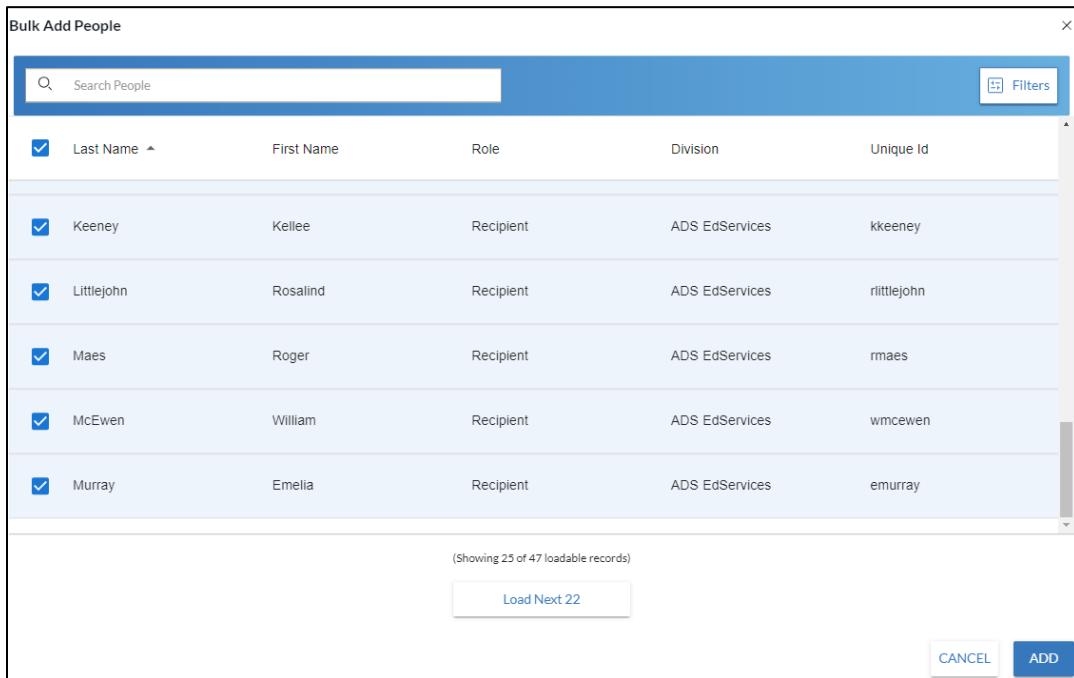
[View all \(47\) People](#)

9. Select **Save** to save the group or **Cancel** to return to the **Groups** page.

Add People

To add people to your group

1. In the parameter drop-down list, select **Person**. The **Bulk Add People** modal opens.



The screenshot shows the 'Bulk Add People' modal. At the top is a search bar labeled 'Search People' and a 'Filters' button. Below is a table with columns: Last Name, First Name, Role, Division, and Unique Id. The 'Last Name' column has a checked checkbox at the top. Five rows of data are listed:

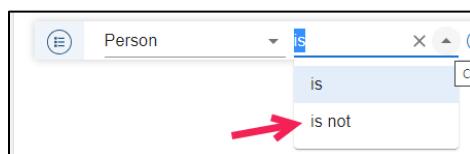
Last Name	First Name	Role	Division	Unique Id
Keeney	Kellee	Recipient	ADS EdServices	kkeeney
Littlejohn	Rosalind	Recipient	ADS EdServices	rlittlejohn
Maes	Roger	Recipient	ADS EdServices	rmaes
McEwen	William	Recipient	ADS EdServices	wmcewen
Murray	Emelia	Recipient	ADS EdServices	emurray

(Showing 25 of 47 loadable records)

Load Next 22

CANCEL **ADD**

2. Choose individual people by selecting the corresponding checkboxes.
 - Use the **Search Contacts** field to search for specific contacts.
 - Use the **Filters** option to narrow down your search.
 - Use the top checkbox to select all in the modal.
 - Select **Load Next** to load more people.
3. Select **Add**.
4. Optionally, change the parameter in the second drop-down list from **is** to **is not** to exclude the selected people rather than include them.



5. Select the checkmark  to save the criterion.

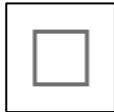
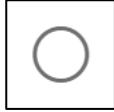
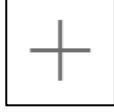
Note: A group that consists of only people is a static group. If any other type of parameter is added, the group becomes dynamic.

Add Map Shapes

When a map shape is added as a group criterion, any people with saved locations in that shape are added to the group. This includes people with locations in the shape that are saved after the group is created, including check-in locations.

To add a map shape

1. In the parameter drop-down list, select **Map Shape**. The **Add Map Shape** modal opens.
2. Use any of the available tools to define a shape:

Tool	Description
	<p>Rectangle: Use the rectangle tool to define a rectangular-shaped area on the map to identify recipients located within those boundaries. Once drawn, the rectangle can be rotated by moving the rotation handle and moved, rotated, or resized.</p>
	<p>Polygon: Use the polygon tool to define a free-formed shaped area on the map to identify people located within those boundaries. Click once to select a starting point, click again to select an edge of the boundary, and continue to click and define boundary edges. Click on the originating point to complete the shape.</p> <p>Note: The final edge must connect to the originating point for the shape to be considered finished.</p>
	<p>Circle: Use the circle tool to define a circular-shaped area on the map to identify recipients located within those boundaries. Once drawn, the circle can be rotated by moving the rotation handle and moved, rotated, or resized. The circle can be changed to an oval by selecting one of the four point and dragging it.</p> <p>After initially drawing a circle, you can change its radius and select the units of distance.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <div style="display: flex; justify-content: space-between;"> Radius <input type="radio"/> km <input checked="" type="radio"/> mi </div> <div style="margin-top: 5px;"> <input type="text" value="1200"/> </div> </div>
	<p>Zoom-In: Position the map in the desired location and zoom in to see more map detail.</p>

Tool	Description
	Zoom-Out: Position the map in the desired location and zoom out to focus on a larger map area.
	Find My Location: Use to zoom into the user's location on the map. Note: The browser location setting must be enabled for Find My Location to work.

3. Draw your shape on the map, capturing the people you want to include or exclude in the group. Optionally, add more shapes. You can add unlimited shapes, mix shape types, and overlap shapes.
- To exclude the people with saved locations in the shape from the group, select the **Exclude** toggle in the shape summary bar that opens at the bottom of the map.

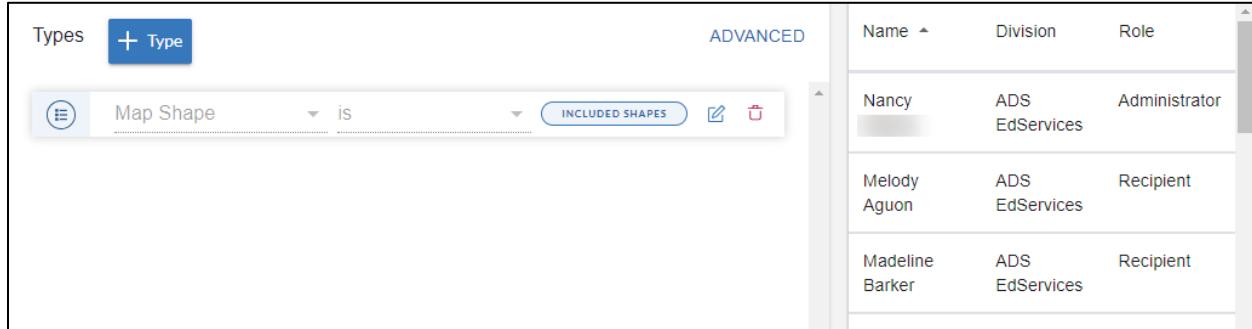


- Delete a shape by selecting it and then selecting the trash can icon.
4. Once your shape is complete, click outside the shape to finalize it. At the bottom of the map, the shape summary bar confirms the number of shapes drawn and the number of people in the shape(s).



5. Optionally, turn **Geofence OFF** to exclude people receiving alerts via the OnSolve Mobile app based on their geolocation.
6. Select **ADD**.
7. Optionally, change the parameter in the second drop-down list from **is** to **is not** to exclude the selected people rather than include them (or the opposite if you selected to exclude in step 3).

8. Select the checkmark  to save the criterion. Any people with locations inside (or outside, if excluding) the shape(s) are added to the list in the section to the right.

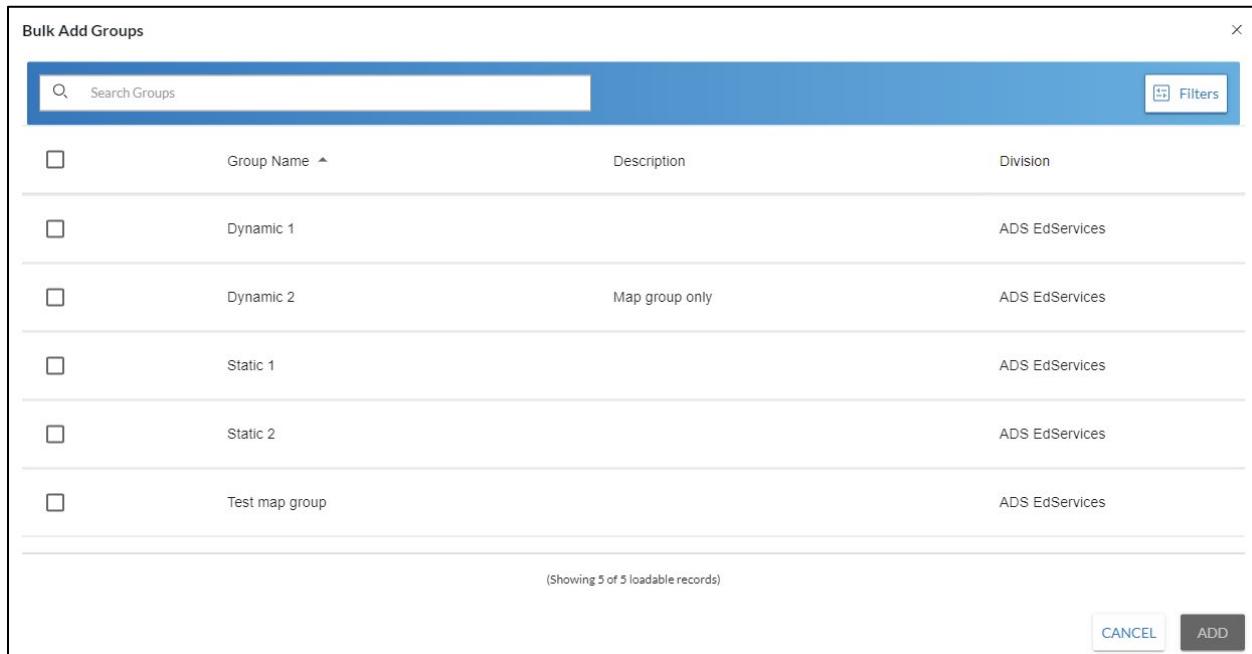


The screenshot shows a user interface for creating a criterion. On the left, there's a search/filter bar with dropdowns for 'Map Shape' and 'is', and buttons for '+ Type' and 'ADVANCED'. On the right, a table lists users with columns for Name, Division, and Role. The users listed are Nancy (ADS EdServices, Administrator), Melody Aguon (ADS EdServices, Recipient), and Madeline Barker (ADS EdServices, Recipient).

Name	Division	Role
Nancy	ADS EdServices	Administrator
Melody Aguon	ADS EdServices	Recipient
Madeline Barker	ADS EdServices	Recipient

Add Groups

1. In the first parameter drop-down list, select **Group**. The **Bulk Add Groups** modal opens.



The screenshot shows the 'Bulk Add Groups' modal. It includes a search bar labeled 'Search Groups' and a 'Filters' button. A list of groups is displayed with checkboxes next to each group name. The groups listed are Dynamic 1, Dynamic 2, Static 1, Static 2, and Test map group. All groups belong to the ADS EdServices division. At the bottom, it says '(Showing 5 of 5 loadable records)' and has 'CANCEL' and 'ADD' buttons.

<input type="checkbox"/>	Group Name	Description	Division
<input type="checkbox"/>	Dynamic 1		ADS EdServices
<input type="checkbox"/>	Dynamic 2	Map group only	ADS EdServices
<input type="checkbox"/>	Static 1		ADS EdServices
<input type="checkbox"/>	Static 2		ADS EdServices
<input type="checkbox"/>	Test map group		ADS EdServices

2. Choose individual groups by selecting the corresponding checkboxes.

- Use the **Search Groups** field to search for specific groups.
- Use the **Filters** option to narrow down your search.
- Use the top checkbox to select all in the modal.
- Select **Load Next** to load more groups.

3. Select **Add**.
4. Optionally, change the parameter in the second drop-down list from **is** to **is not** to exclude the selected groups rather than include them.
5. Select the checkmark to save the criterion. All members of the added group(s) are added to the list in the section to the right.

Add People Record Attributes

People can be added to the group based on attributes saved in their people records.

Overview Tab

To add people record overview attributes

1. In the drop-down list, select an attribute. The options from the people record **Overview** tab are:
 - **Building**
 - **City**
 - **Company Name**
 - **Country**
 - **Division**
 - **First Name**
 - **Floor**
 - **Job Title**
 - **Last Name**
 - **Middle Name**
 - **Preferred Language**
 - **State**
 - **Street Address 1**
 - **Street Address 2**
 - **Timezone**
 - **Unique ID**
 - **Username**
 - **Zip Code**

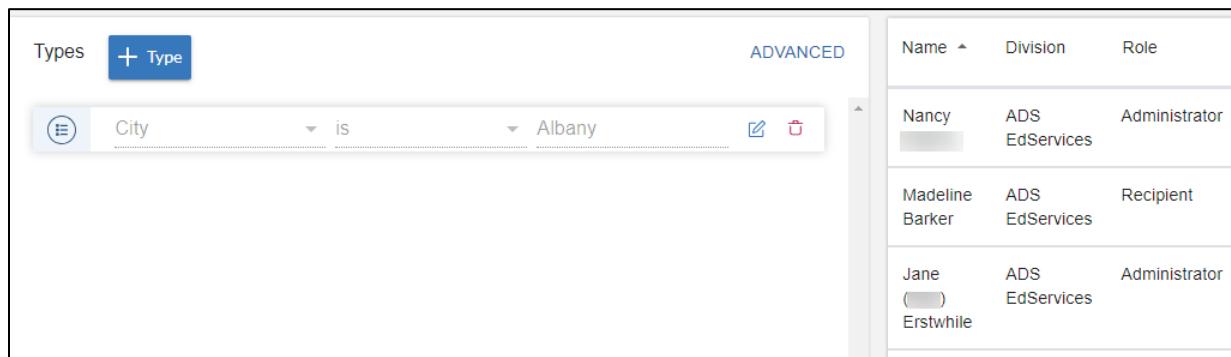
2. Select a parameter from the second drop-down list. The options are:

- **is**
- **is not**
- **contains**
- **does not contain**
- **starts with**
- **ends with**
- **is blank**
- **is not blank**

3. In the field for the third parameter, enter a keyword or partial keyword.

Note: If you chose **is blank** or **is not blank** in step 2, skip step 3.

4. Select the checkmark to save the criterion. Any people who match that criterion are added to the list in the section to the right.



The screenshot shows a search interface on the left and a results table on the right. The search interface includes fields for 'Types' (set to '+ Type'), 'City' (set to 'Albany'), and a dropdown menu for 'is'. The results table lists three people: Nancy, Madeline Barker, and Jane Erstwhile, along with their Division (ADS/EdServices) and Role (Administrator/Recipient).

Name	Division	Role
Nancy	ADS EdServices	Administrator
Madeline Barker	ADS EdServices	Recipient
Jane Erstwhile	ADS EdServices	Administrator

Devices Tab

The options from the people record **Devices** tab are:

- **Email**
- **Fax**
- **SMS**
- **Pager**
- **Phone Number**

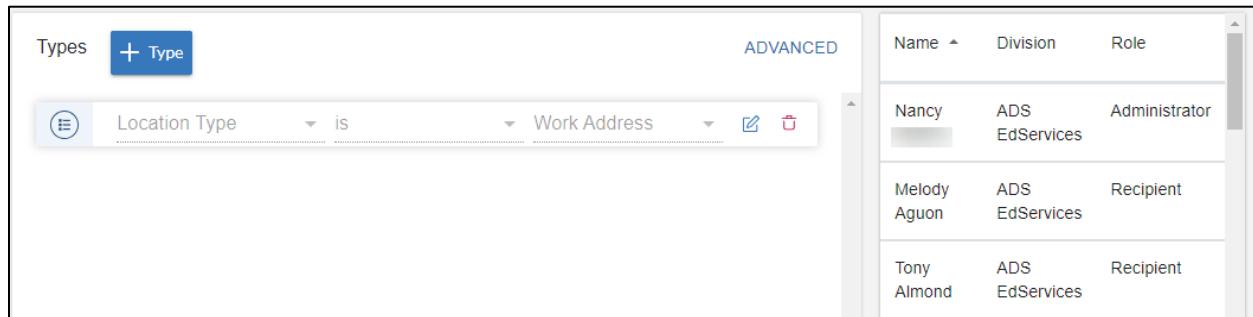
To add people record devices attributes

Follow steps 1–4 above, entering an email address or digits in the keyword field.

Locations Tab

To add locations

1. In the parameter drop-down list, select **Location Type**.
2. In the second parameter drop-down list, select **is** or **is not**.
3. In the third parameter drop-down list, select from the location labels saved in the account.
4. Select the checkmark to save the criterion. Any people who match that criterion are added to the list in the section to the right.



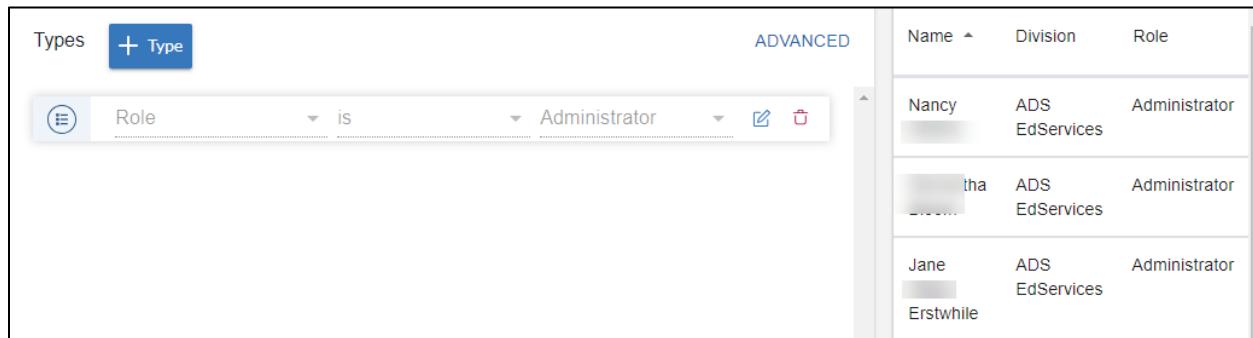
The screenshot shows a user interface for managing locations. On the left, there is a search bar with three dropdown menus: 'Location Type' (set to 'Work Address'), 'is' (selected), and 'Work Address'. To the right of the search bar is an 'ADVANCED' button. On the far right is a table titled 'Name' with columns for 'Division' and 'Role'. The table contains three rows of data:

Name	Division	Role
Nancy	ADS EdServices	Administrator
Melody Aguon	ADS EdServices	Recipient
Tony Almond	ADS EdServices	Recipient

User Privileges Tab

To add a people record user privileges attribute

1. In the parameter drop-down list, select **Role**.
2. In the second parameter drop-down list, select **is** or **is not**.
3. In the third parameter drop-down list, select from the roles saved in the account.
4. Select the checkmark to save the criterion. Any people who match that criterion are added to the list in the section to the right.



The screenshot shows a user interface for managing user privileges. On the left, there is a search bar with three dropdown menus: 'Role' (set to 'Administrator'), 'is' (selected), and 'Administrator'. To the right of the search bar is an 'ADVANCED' button. On the far right is a table titled 'Name' with columns for 'Division' and 'Role'. The table contains three rows of data:

Name	Division	Role
Nancy	ADS EdServices	Administrator
tha...lton	ADS EdServices	Administrator
Jane Erstwhile	ADS EdServices	Administrator

Add Device Attributes

You can add people to the group based on whether they have a saved device marked as private or not activated.

To add a device attribute

1. In the parameter drop-down list, select **Device Private** or **Device not Activated**.
2. Leave the second parameter drop-down list set to **is**.
3. In the third parameter drop-down list, select **Yes** or **No**.
4. Select the checkmark  to save the criterion. Any people who match that criterion are added to the list in the section to the right.

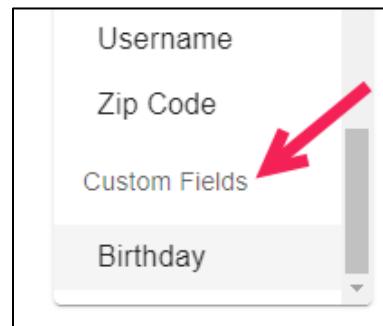


The screenshot shows a user interface for filtering contacts. On the left, there's a 'Types' section with a '+ Type' button. Below it are two dropdown filters: 'Device Not Activ...' (set to 'is Yes') and 'Device Private' (set to 'is No'). To the right is a table titled 'Name' showing three users: Nancy, Melody Aguon, and Tony Almond, all assigned to 'ADS EdServices' and 'Recipient' roles.

Name	Division	Role
Nancy	ADS EdServices	Administrator
Melody Aguon	ADS EdServices	Recipient
Tony Almond	ADS EdServices	Recipient

Add Custom Fields

You can add people to a group based on their custom fields. Custom fields saved in the account are available to select at the bottom of the first parameter drop-down list under **Custom Fields**.



To add custom fields

1. In the drop-down list, select a custom field.
2. In the second drop-down list, select **is**, **is not**, **contains**, etc.
3. In the field for the third parameter, enter a keyword or partial keyword.

Note: If you chose **is blank** or **is not blank** in step 2, skip step 3.

4. Select the checkmark  to save the criterion. Any people who match that criterion are added to the list in the section to the right.



Name	Division	Role
Melody Aguon	ADS EdServices	Recipient

Add Advanced Filters

Advanced filters allow you to combine criteria and sets of criteria with AND and OR operators to create logic that determines the group's membership.

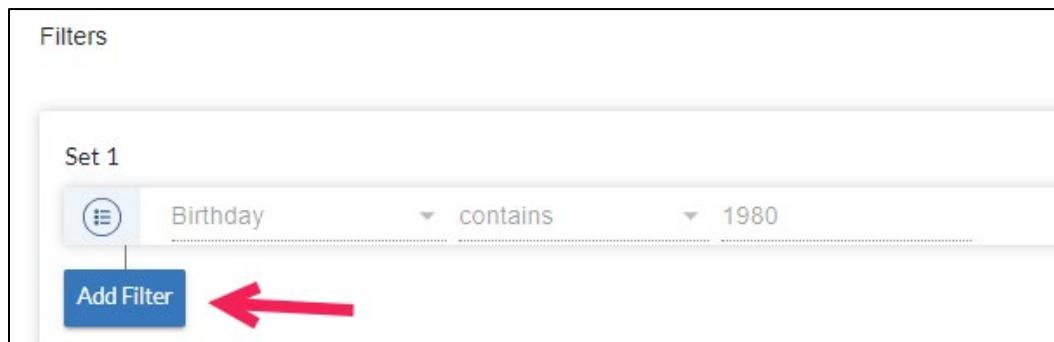
- Use the AND operator if you want people to satisfy all criteria in the set (or between sets) to be brought into the group.
- Use the OR operator if you want people to satisfy any criterion in the set (or between sets) to be brought into the group.

To create sets of criteria using advanced filters

1. Select **Advanced**.

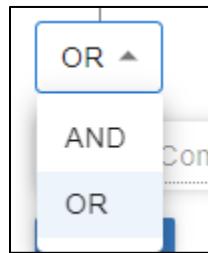


2. Select **Add Filter**.
3. Add your first filter (criterion) and select the checkmark to save it.
4. Optionally, create a set of criteria by selecting **Add Filter** under your first filter.



- a. Add a second criterion and select the checkmark to save it.

- b. Select **OR** or **AND** as the operator.



- c. Repeat steps a–b until you have the desired filters in this set.

5. Optionally, add more sets by selecting **Add Set** under the previous set and choosing **AND** or **OR** as the operator between sets.
6. Repeat steps 2–5 until you have all your desired filters. There is no limit to the number of sets you can create.
7. When all desired people have been added, select **Save**. Any people who match the logic created by the filter(s) are added to the list in the section to the right.

Example

The below example creates a group that includes contacts [whose company is OnSolve and whose city is Albany] OR [whose company is OnSolve and whose job title is Manager]. In other words, this group contains every OnSolve employee who works in Albany or is a manager.

Filters

Set 1

Company Name is OnSolve

AND

City is Albany

Add Filter

OR

Set 2

Company Name is OnSolve

AND

Job Title is Manager

Name	Division	Role
Nancy Adams	ADS EdServices	Administrator
Samantha Bloom	ADS EdServices	Administrator

[View all \(2\) People](#)

On-Call Scheduling

On-Call Scheduling allows administrators and authorized users to set up an organized work plan. Each schedule contains one or more shifts consisting of a time period with an associated list of recipients or groups to whom alerts may be sent.

When an alert is sent to a schedule, the OnSolve Platform determines which shifts are active at that time and sends the alert to the users associated with those shifts. If no users are available, no alert will be sent.

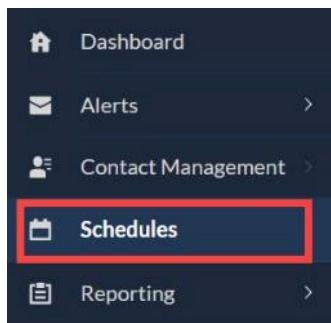
Create a New Schedule

Creating a new schedule involves:

1. Defining the schedule
2. Creating shifts
3. Adding assignments
4. Assigning permissions
5. Adding exceptions

To start the process

1. Navigate to **Schedules**.



2. Select **+ Create Schedule**.



Define the Schedule

1. Enter a **Schedule Name**.
2. Enter a schedule **Description**.
3. Select the **Division** in which this schedule should reside.
4. Select the **Time Zone**.

Note: Schedules always appear and operate in the time zone of the user viewing or using it.

Create New Schedule

① OVERVIEW ② SHIFTS ③ ASSIGNMENTS

DEFINE NEW SCHEDULE
Fill out the information below to start defining a schedule.

Schedule Name
Test 4 / 120

Description
Test Schedule 13 / 160

Division ⓘ
Education Services

Time Zone
(-05:00) Eastern (N. America)

5. Select **Next**.

Create Shifts

Shifts can be created either from scratch or by duplicating an existing shift.

Create a New Shift

Add Shift

SHIFT DETAILS
Enter name and recommended number of contacts to cover a shift:

Shift Name
Morning shift

13 / 120

Coverage ?

3

TIERS ?
Tiers represent the escalation order in which contacts are alerted. Add up to 10 tiers.

- TIER 1** □
Wait Time Duration (1 min - 17 hours)
00 : 05
- TIER 2** □
Wait Time Duration (1 min - 17 hours)
00 : 05
- TIER 3** □

DATE(S) AND REPEAT CYCLES
Select the date and time and when you would like it to repeat.

Start Date
08 / 21 / 2020 □

Start Time
09 : 00 AM

Work on holiday(s)

Duration (HHH:MM)
003 : 00

Holiday Calendar
Select a Calendar ▼

Recurrence
 Once Repeating

Repeat Cycle
Weekly ▼

Repeats On
SUN MON TUE WED THU FRI SAT

End Date

Every (1-26 weeks)
1 week(s)

Repeat Until
12 / 31 / 2020 □

CANCEL
ADD

1. Select **Add Shift**. The **Add Shift** window opens.
2. Enter a **Shift Name**.
3. Optionally, enter a **Coverage** number. This is the number of people desired to cover the shift.
4. Add one or more **Tiers**. A tier acts as an escalation level where tier 1 assignees are contacted first, tier 2 second, etc. For each tier except the last, set the **Wait Time Duration**, which is how many hours/minutes pass before the next tier is contacted. Add up to 10 tiers per shift.

Note: By default, a shift always has at least one tier. Subsequent tiers are contacted only in quota alerts.

5. Set the **Start Date**, **Start Time**, and **Duration** for the shift.
6. Optionally, set the shift so assignees do not **Work on holiday(s)**. If assignees should not work on holidays, select which holiday calendar applies to the shift. See [Holidays](#) for more information.
7. In **Recurrence**, choose whether this shift occurs only **Once** or is a **Repeating** shift. If repeating, select a **Repeat Cycle** of **Daily**, **Weekday**, **Weekly**, **Monthly**, **Quarterly**, **Yearly**, **Custom Pattern**, or **Holidays Only**.
 - If **Daily**, set the repetition frequency of the shift in days.
 - If **Weekday**, set the repetition frequency of the shift in days. Weekday repetition operates similarly to Daily repetition, except that it skips weekends.
 - If **Weekly**, set the repetition frequency in weeks, and in **Repeats On**, which days of the week the shift repeats on.
 - If **Monthly**, set the repetition frequency in months, and in **Repeats On**, whether the shift should repeat on the day of the month or a particular day of the week.
 - If **Quarterly**, choose from the two **Repeats On** drop-down lists to set exactly when during the quarter the shift repeats.
 - If **Yearly**, choose from the two **Repeats On** drop-down lists to set exactly when during the year the shift repeats.
 - If **Custom Pattern**, set the repetition pattern in days and in **Repeats On**. Optionally, choose on which days the shift repeats.
 - If **Holidays Only**, nothing else is required, and the shift only applies to the dates in the selected holiday calendar.

Enter a repeat interval in the **Every** field. This number further determines how frequently the shift repeats. For example, if **Repeat Cycle** is set to **Weekly** and **Every** is set to 3, the shift is active on week 1, inactive on weeks 2 and 3, and active again on week 4.

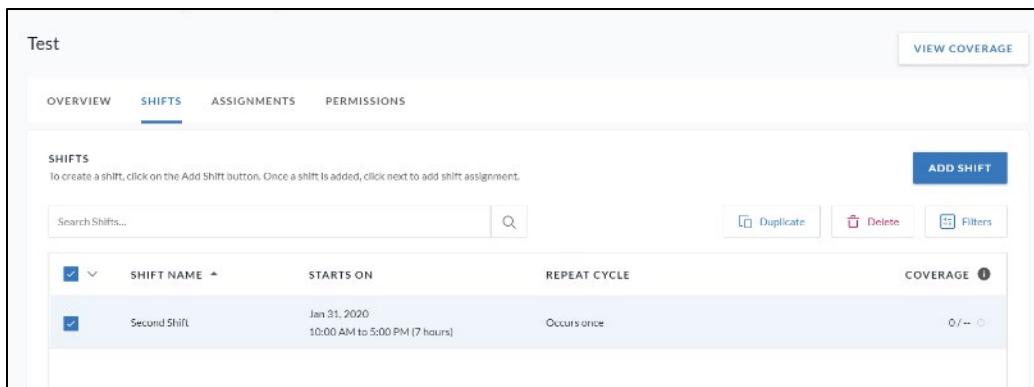
Note: The unit of time in the **Every** field will match what was set in the **Repeat Cycle** field, and the unit is days if **Repeat Cycle** is set to **Custom Pattern**.

8. Optionally, set an **End Date**.
9. Select **Add**.
10. Repeat steps 1-9 to add an unlimited number of shifts.
11. Select **Done** to complete the process and create the schedule, or Select **Next** to continue with adding assignments.

Duplicate a Shift

To duplicate a shift within a schedule

1. Navigate to **Schedules**.
2. Select the desired schedule.
3. Select the **Shifts** tab.
4. Check the checkbox next to the desired shift to duplicate and select **Duplicate**.

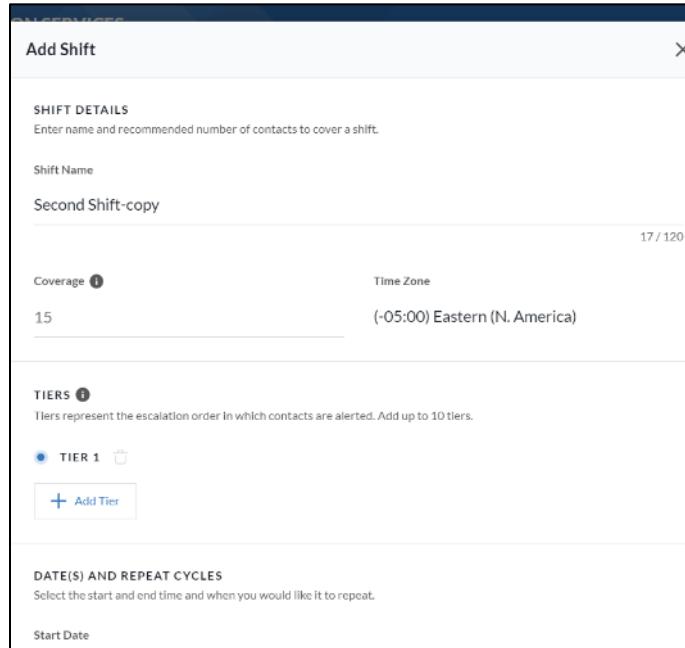


The screenshot shows the 'Shifts' tab selected within a 'Test' schedule. A single shift, 'Second Shift', is listed with the following details:

SHIFT NAME	STARTS ON	REPEAT CYCLE	COVERAGE
Second Shift	Jan 31, 2020 10:00 AM to 5:00 PM (7 hours)	Occurs once	0 / --

At the top right of the table, there are three buttons: 'Duplicate' (highlighted), 'Delete', and 'Filters'. At the bottom right of the table, there is a small circular icon with a question mark.

The selected shift opens as if the user is creating a new shift but with the original shift's data. The shift name defaults to “<name of copied Shift >-copy.” The same assignments are also listed, but all these elements can be edited before saving the new shift.



SHIFT DETAILS
Enter name and recommended number of contacts to cover a shift.

Shift Name
Second Shift-copy

Coverage 15 Time Zone (-05:00) Eastern (N. America)

TIERS
Tiers represent the escalation order in which contacts are alerted. Add up to 10 tiers.

TIER 1

[+ Add Tier](#)

DATE(S) AND REPEAT CYCLES
Select the start and end time and when you would like it to repeat.

Start Date

5. Select Done.

Add Assignments (Optional)

1. Select Add Assignment.
2. Select which **Contacts**, **Groups**, and/or nested **Schedules** should be assigned to that shift by selecting the appropriate tab and finding the desired recipients.

Add Assignment

CONTACTS **GROUPS** **SCHEDULES**

To add assignments, select from the list of contacts below.

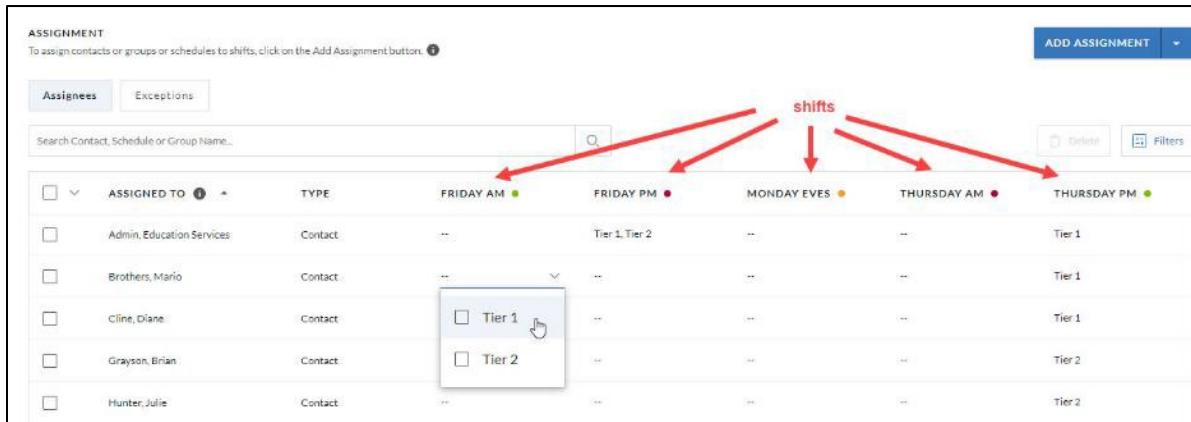
Search Something...

<input type="checkbox"/> ▾	CONTACT NAME ▾	UNIQUE ID
<input type="checkbox"/>	Ahab, Captain	UniqueID-26
<input type="checkbox"/>	Angstrom, Rabbit	UniqueID-36
<input type="checkbox"/>	approvee, approvee	approvee
<input type="checkbox"/>	Banks, John	UniqueID_88
<input type="checkbox"/>	Barnes, Jake	UniqueID-55
<input type="checkbox"/>	Bart, Lily	UniqueID-49

Display 25 ▾ Entries (Showing 1 to 25 of 88 Results) 1 2 3 4 >

3. Select Add.

4. In the **Assignment** table, assign each contact to any number of tiers in any of the shifts. Contacts assigned to tier 1 are alerted first, tier 2 second, etc. When shifts are fully covered, they are indicated by a green dot; when partially covered, by an orange dot; and when there is zero coverage, a red dot.



ASSIGNMENT
To assign contacts or groups or schedules to shifts, click on the Add Assignment button. [?](#)

Assignees **Exceptions**

Search Contact, Schedule or Group Name...

	ASSIGNED TO ?	TYPE	FRIDAY AM	FRIDAY PM	MONDAY EVES	THURSDAY AM	THURSDAY PM
<input type="checkbox"/>	Admin, Education Services	Contact	--	Tier 1, Tier 2	--	--	Tier 1
<input type="checkbox"/>	Brothers, Mario	Contact	--	--	--	--	Tier 1
<input type="checkbox"/>	Cline, Diane	Contact	--	<input type="checkbox"/> Tier 1	--	--	Tier 1
<input type="checkbox"/>	Grayson, Brian	Contact	--	--	--	--	Tier 2
<input type="checkbox"/>	Hunter, Julie	Contact	--	--	--	--	Tier 2

ADD ASSIGNMENT [?](#)

Filters

5. When all tiers in all shifts have at least one assigned contact, select **Done**.
6. Select **Back to Schedules**.

Add Assignment Exceptions (Optional)

If any assignees expect to be unavailable during any of their shifts, exceptions can be created to account for that. Additionally, replacement contacts can be assigned for those shifts.

Note: To create an exception for an individual contact, that contact must be added to the shift as a contact and not as part of a group or schedule.

In the **Assignees** tab, assignments that include exceptions are denoted with a flag.



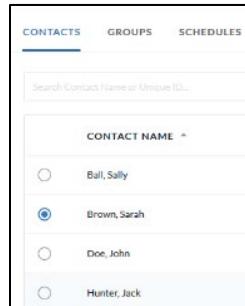
	ASSIGNED TO ?
<input type="checkbox"/>	102
<input type="checkbox"/>	103
<input type="checkbox"/>	A.Tier 1
<input type="checkbox"/>	A.Tier 2
<input type="checkbox"/>	A.Tier 3

To add an assignment exception

1. On the **Assignments** tab, select **Add Exception**.



- Choose the contact, group, or schedule that needs an exception.



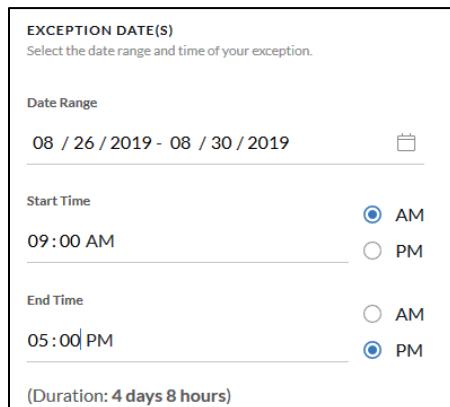
CONTACTS GROUPS SCHEDULES

Search Contact Name or Unique ID...

CONTACT NAME ▾

- Ball, Sally
- Brown, Sarah
- Doe, John
- Hunter, Jack

- Select **Next**.
- Enter the **Date Range** and **Start** and **End Times** for the exception. The dates and times entered define a *continuous* block of time. In the example below, the exception lasts from 9:00 AM on August 26 to 5:00 PM on August 30, as opposed to 9:00 AM to 5:00 PM on each of those days.



EXCEPTION DATE(S)
Select the date range and time of your exception.

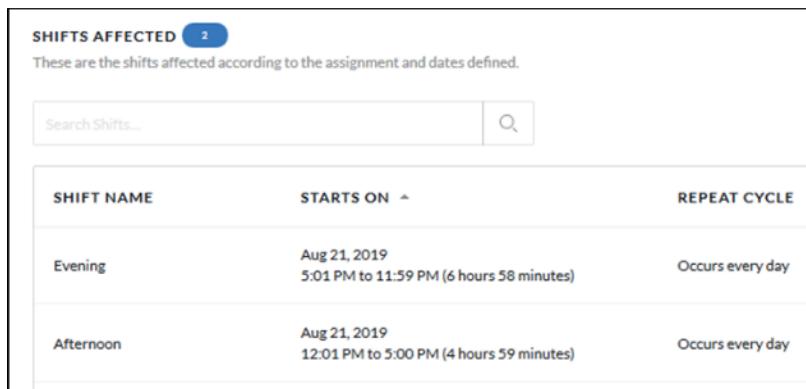
Date Range
08 / 26 / 2019 - 08 / 30 / 2019

Start Time
09:00 AM AM PM

End Time
05:00 PM AM PM

(Duration: 4 days 8 hours)

- Select **Next**. The assignee's shifts that are affected by this exception are displayed.

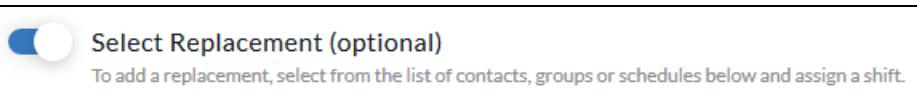


SHIFTS Affected 2

These are the shifts affected according to the assignment and dates defined.

SHIFT NAME	STARTS ON ▾	REPEAT CYCLE
Evening	Aug 21, 2019 5:01 PM to 11:59 PM (6 hours 58 minutes)	Occurs every day
Afternoon	Aug 21, 2019 12:01 PM to 5:00 PM (4 hours 59 minutes)	Occurs every day

6. Select **Done**, or, if a replacement should be assigned to cover this shift, select the **Select Replacement** toggle, and continue to step 9.



Once **Select Replacement** is toggled on, a list of available contacts is displayed, with the option to display groups and schedules.

	LAST NAME	FIRST NAME	ROLE	UNIQUE ID	SHIFT
<input type="checkbox"/>	Admin	Education Services	Administrator		--
<input type="checkbox"/>	Brothers	Mario	Recipient	0123456	--
<input type="checkbox"/>	Rogers	Raina	Recipient	re503	--

Display 25 Entries (Showing 1 to 3 of 3 Results)

GO BACK CANCEL DONE

7. Select which contact(s) should be the replacement, and in the **Shift** column, select which of the affected shifts the replacement is for.

	LAST NAME	FIRST NAME	ROLE	UNIQUE ID	SHIFT
<input type="checkbox"/>	Admin	Education Services	Administrator		--
<input type="checkbox"/>	Brothers	Mario	Recipient	0123456	--
<input checked="" type="checkbox"/>	Rogers	Raina	Recipient	re503	All

Display 25 Entries Selected 1 of 3 Results

GO BACK CANCEL DONE

8. Select **Done**.

Holidays

Holidays are days that shifts can be repeated on, as well as days that shifts can skip over. See [Create Shifts](#) to learn how to create shifts that take holidays into regard. But before shifts can consider holidays, administrators must define what those holidays are by creating holiday calendars.

Only administrators can create, modify, and delete holiday calendars. However, all holiday calendars are available for use by anyone creating schedules.

Create a New Holiday Calendar

To create a new holiday calendar

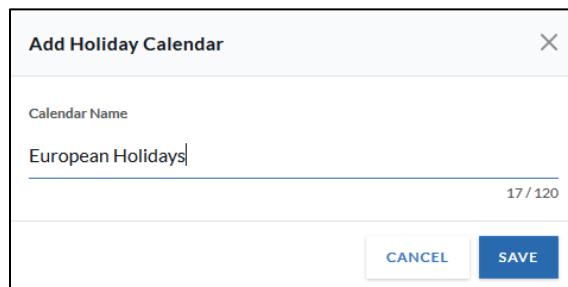
1. From the **Schedules** page, select **View Holidays**.

Note: On-Call Scheduling requires that there always be at least one saved holiday calendar. One is provided upon the first use of On-Call Scheduling.

2. Select **Add Holiday Calendar**.

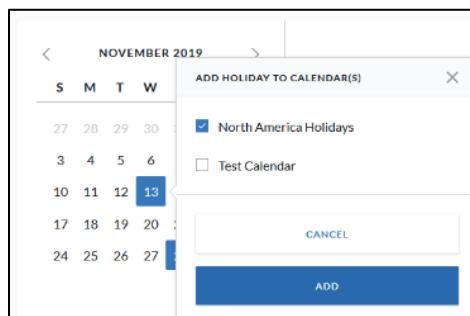


3. Enter a name for the holiday calendar and select **Save**.



The dialog box has a title bar "Add Holiday Calendar" and a close button "X". It contains a "Calendar Name" field with the value "European Holidays" and a character count indicator "17 / 120". At the bottom are "CANCEL" and "SAVE" buttons.

4. Select a date from the calendar, select the holiday calendar to which it should be added, and select **Add**.



5. Repeat step 4 until the holiday calendar is complete.

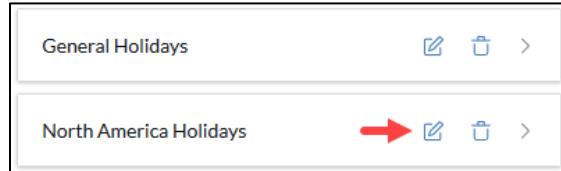
Modify a Holiday Calendar

Users can modify calendars by renaming them and adding/deleting dates.

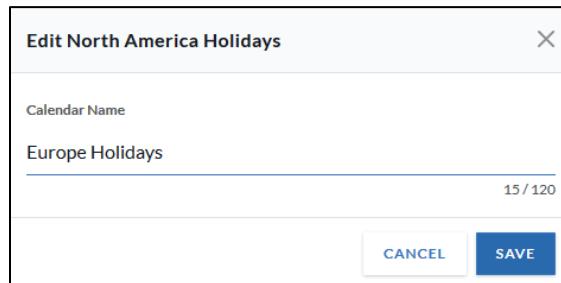
Rename an Existing Calendar

To rename an existing holiday calendar

1. From the **Holidays** page, select the **modify** icon next to the desired holiday calendar.



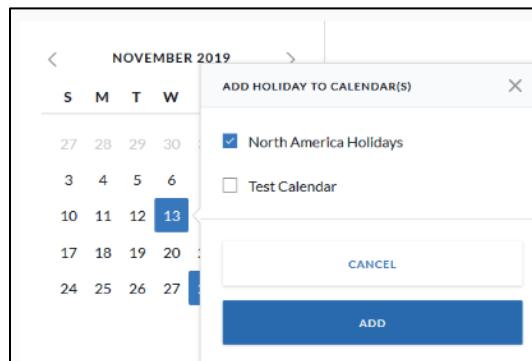
2. Type a new name and select **Save**.



Add/Delete Dates

To add new dates to an existing holiday calendar

1. Select the desired date from the calendar.
2. Select to which holiday calendar the date should be added and select **Add**. Dates can be added to any saved calendars.



To delete dates from an existing holiday calendar

1. Click on the holiday calendar name or the arrow to expand the field.



North America Holidays

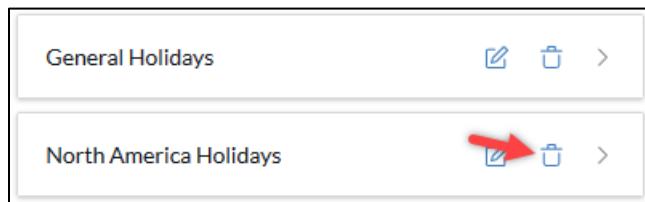
09/02/2019 10/14/2019 11/13/2019

11/28/2019

2. Select the delete icon next to the desired date.
3. Select **Delete** to confirm, or, if selecting an alternate calendar, **Delete & Reassign**.

Delete a Holiday Calendar

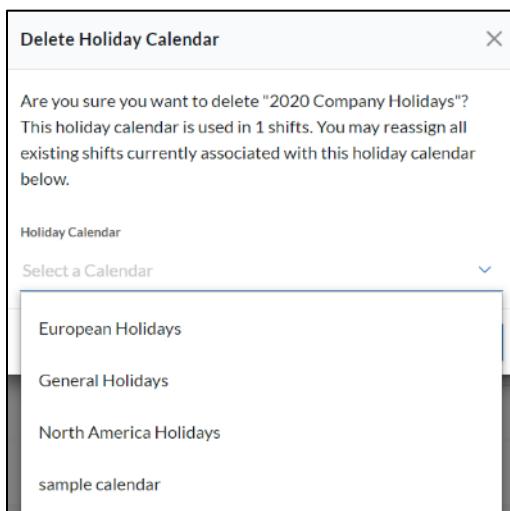
From the **Holidays** page, select the **delete** icon next to the desired calendar.



General Holidays

North America Holidays

If the calendar is being used in any shifts, an alternate calendar will need to be assigned to those shifts. Use the drop-down list to select an alternate calendar and select **Delete & Reassign**.



Are you sure you want to delete "2020 Company Holidays"?
This holiday calendar is used in 1 shifts. You may reassign all
existing shifts currently associated with this holiday calendar
below.

Holiday Calendar

Select a Calendar

European Holidays

General Holidays

North America Holidays

sample calendar

Manage Schedules

Schedule Settings

In Schedule Settings, you can set a default Wait Time Duration – the time the OnSolve Platform waits between contacting one tier and attempting to reach the next - that applies to all schedules. When creating a shift, the wait time duration between tiers will default to the time entered in Schedule Settings.

To set a default wait time duration

1. From the **Schedules** page, select **Settings**. The **Schedule Settings** page opens.
2. Set a **Wait Time Duration** of between 1 minute and 17 hours.
3. Select **Save**.

Search and Filter a Schedule and Its Elements

Saved schedules and their shifts and assignments can be searched and filtered.

Search

For schedules, shifts, and assignments, use the search field to search by name:

MANAGE SCHEDULES
Select from the list of schedules below or create a new schedule.

test

<input type="checkbox"/>	SCHEDULE NAME	DESCRIPTION	LAST MODIFIED
<input type="checkbox"/>	O_TestTimeZoneSchedule	test	Jul 17, 2019 09:11 AM US/Pacific
<input type="checkbox"/>	000aaa-NEWForCopyTestSCHED-400	asd	Jun 28, 2019 10:49 AM US/Eastern

SHIFTS
To create a shift, click on the Add Shift button. Once a shift is added, click next to add shift assignment.

morning

<input type="checkbox"/>	SHIFT NAME	STARTS ON	REPEAT CYCLE
<input type="checkbox"/>	Morning	Jul 12, 2019 9:00 AM to 12:00 PM (3 hours)	Occurs every day

ASSIGNMENT

To assign contacts or groups or schedules to shifts, click on the Add Assignment button. [?](#)

Assignees **Exceptions**

Search Contact, Schedule or Group Name...

<input type="checkbox"/> ASSIGNED TO ?	TYPE	FRIDAY AM ●	FRIDAY PM ●
<input type="checkbox"/> Admin, Education Services	Contact	Tier 1	Tier 2
<input type="checkbox"/> Brothers, Mario	Contact	--	--

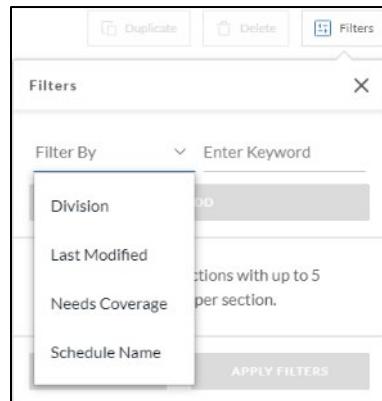
Filter

Schedules, shifts, and assignments (both assignees and exceptions) can be filtered. The application of filters is described below for schedules, but the steps are the same for shifts and assignments.

Note: A maximum of three filters can be applied, and for filters involving keywords, up to five keywords can be applied per filter.

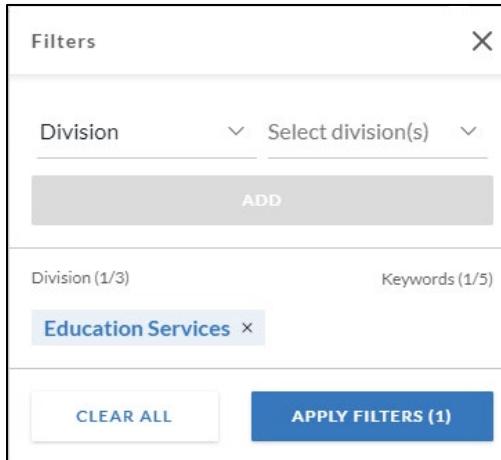
Schedules can be filtered by **Division**, **Last Modified**, **Needs Coverage**, or **Schedule Name**.

1. From the **Manage Schedules** page, select **Filters**.
2. Select your filter of choice:



- For **Division**, select the division.
- For **Last Modified**, enter a date range.
- For **Needs Coverage**, select **Yes** or **No**.
- For **Schedule Name**, enter the name as a keyword.

3. Select **Add**. That filter will be displayed toward the bottom of the **Filters** window.

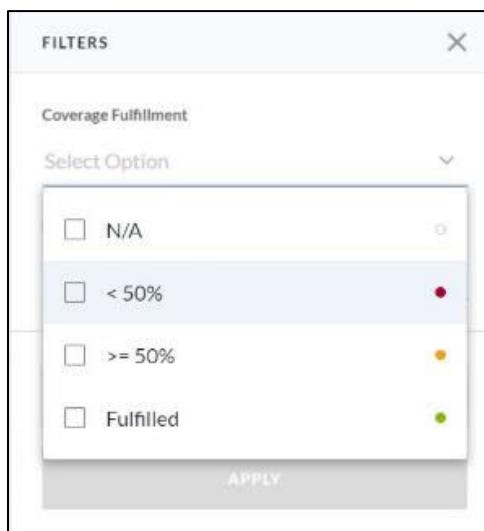


4. Optionally, add up to two more filters.
 5. When finished adding filters, select **Apply Filters**.

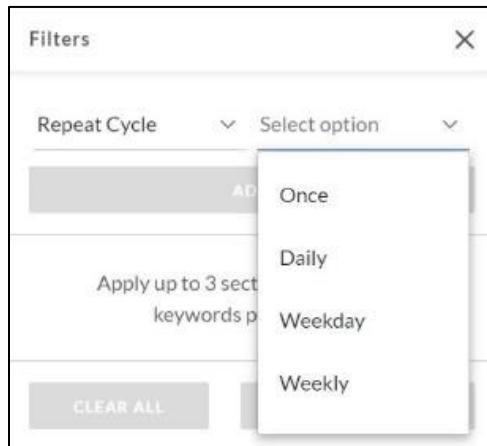
Note: Select **Clear All** to clear any filters.

Shifts can be filtered by **Coverage Fulfillment**, **Shift Name**, amount or **Repeat Cycle** type.

- For **Coverage Fulfillment**, choose between three coverage amounts as well as Not Applicable:
 - N/A
 - < 50%
 - >/= 50%
 - Fulfilled



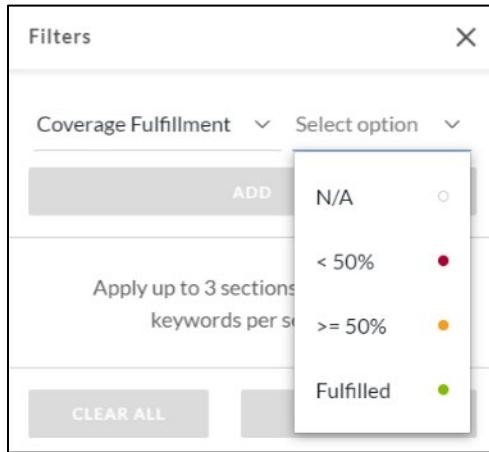
- For **Repeat Cycle**, choose between cycle types of:
 - Once
 - Daily
 - Weekday
 - Weekly
 - Monthly
 - Quarterly
 - Yearly
 - Custom Pattern
 - Holidays Only



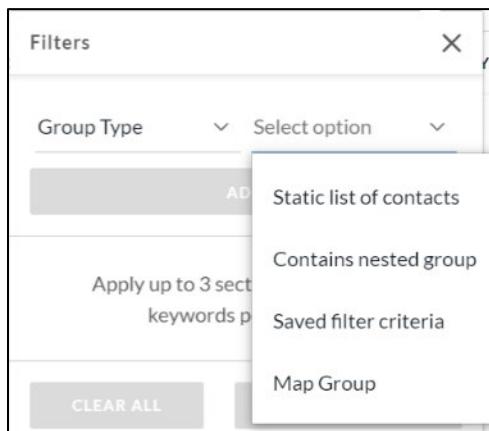
- For **Shift Name**, enter up to five keywords.

Assignees can be filtered by **Contact First Name**, **Contact Last Name**, **Contact Role**, **Coverage Fulfillment**, **Division**, **Group Name**, **Group Type**, **Has Exception**, **Schedule Name**, **Tier Number**, or **Recipient Type**.

- For **Contact First Name**, enter up to five keywords.
- For **Contact Last Name**, enter up to five keywords.
- For **Contact Role**, choose between the available roles.
- For **Coverage Fulfillment**, choose the coverage level:
 - <50%
 - >/= 50%
 - Fulfilled

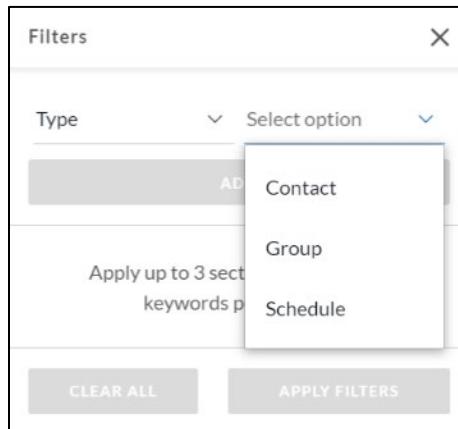


- For **Division**, choose between the available divisions.
- For **Group Name**, enter up to five keywords.
- For **Group Type**, choose between:
 - Static list of contacts
 - Contains nested group
 - Saved filter criteria
 - Map Group



- For **Has Exception**, select Yes or No.
- For **Schedule Name**, enter up to five keywords.
- For **Tier Number**, choose between unassigned and all the available tiers.

- For recipient **Type**, choose between the three types of recipients:
 - Contact
 - Group
 - Schedule



Exceptions can be filtered by **Assignee Name**, **Date Range**, or **Has Replacement**.

- For **Assignee Name**, enter up to five names as keywords.
- For **Date Range**, select start and end dates.
- For **Has Replacement**, select **Yes** or **No**.

Modify a Schedule

Schedules can be modified by adding, deleting, or modifying shifts or assignments.

Add a Shift to an Existing Schedule

To add a new shift to an existing schedule

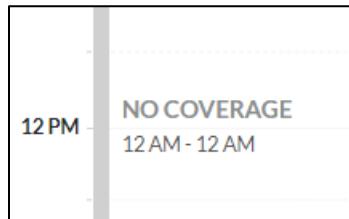
- From the **Schedules** page, select the desired schedule.
- Select the **Shifts** tab.
- Select **Add Shift**.
- Add Shift details as described in *Create Shifts*.
- Select **Save**.

Add a Shift to a Shift Gap

Shifts can be added specifically to cover gaps created by other shifts.

1. While viewing the daily coverage of a schedule, select any time labeled **No Coverage**.

Note: For more information on viewing coverage, see [View Coverage](#).



2. In the **Add Shift** window that opens, enter shift details as described in *Create Shifts*.
3. Select **Save & Add Assignee**.
4. Assign coverage by selecting contacts, groups, and/or schedules and assigning tiers to each.
5. Select **Assign**.

Modify an Existing Shift

To modify an existing shift

1. From the **Schedules** page, select the desired schedule.
2. Select the **Shifts** tab.
3. Select the desired shift.
4. Modify details as needed.
5. Select **Save**.

Delete a Shift from an Existing Schedule

To delete a shift from an existing schedule

1. From the **Schedules** page, select the desired schedule.
2. Select the **Shifts** tab.

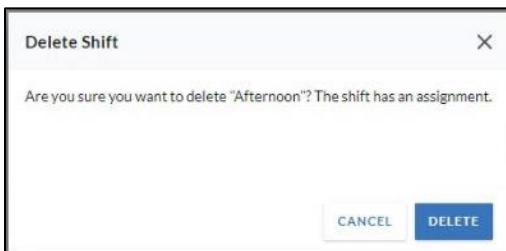
3. Select the checkbox next to the desired shift(s).

	SHIFT NAME	STARTS ON
<input checked="" type="checkbox"/>	Afternoon	Jul 12, 2019 12:30 PM to 5:00 PM (4 hours 30 minutes)
<input type="checkbox"/>	Morning	Jul 12, 2019 9:00 AM to 12:00 PM (3 hours)

4. Select **Delete**.



If the shift has assignments, a warning is displayed:



5. Select **Delete** or **Cancel**.

Note: Since a shift must contain at least one assignment, deleting all a shift's assignments is impossible.

Add an Assignment to an Existing Shift

To add an assignment to a shift

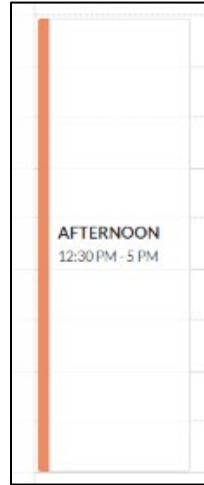
- From the **Schedules** page, select the desired schedule.
- Select the **Assignments** tab.
- Select **Add Assignment**, then **Add New**.
- Add Assignments as described in [Add Assignments \(Optional\)](#).
- Select **Save**.

Note: When the **Add Assignment** window opens, all current assignments are listed with a checkmark. Users can uncheck these to delete assignments at the same time they are adding any new ones.

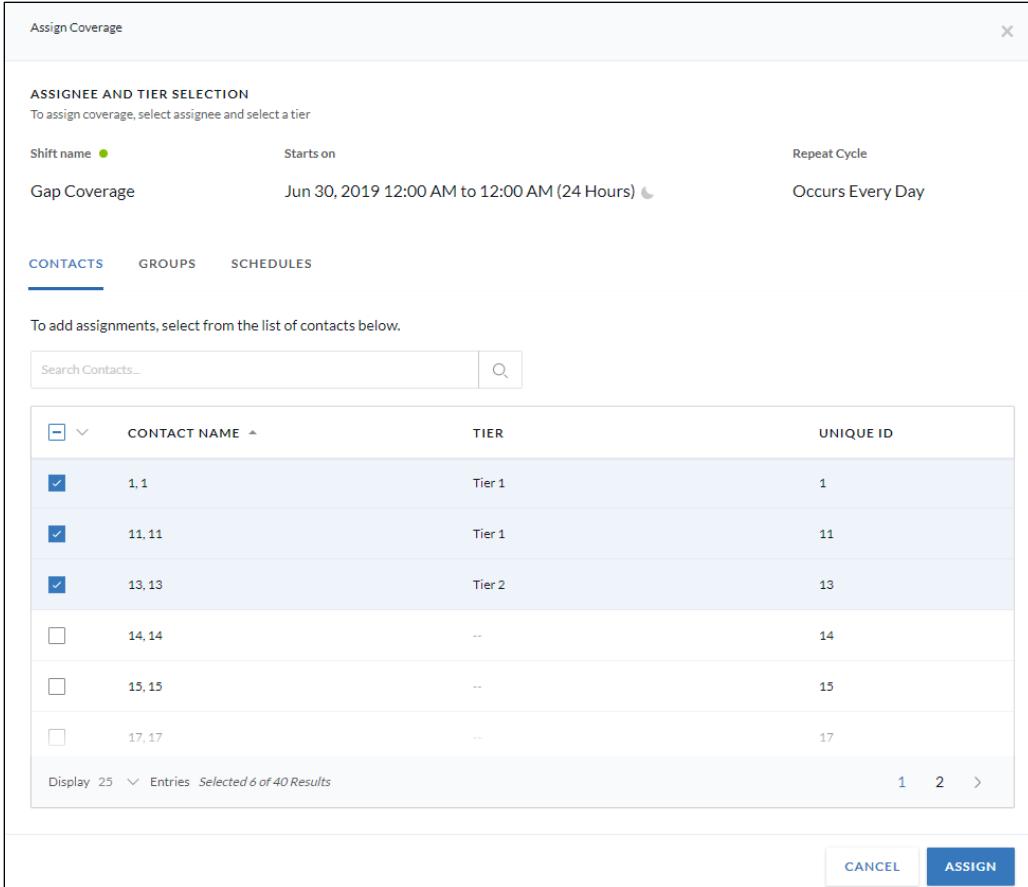
Add an Assignment to a Shift Needing Coverage

Assignments can be made specifically to cover a gap in shift coverage.

1. While viewing the daily coverage of a schedule, select any shift in orange, indicating a coverage gap.



2. In the **Assignee and Tier Selection** window that opens, assign coverage by selecting contacts, groups, and/or schedules and assigning tiers to each.



The screenshot shows the 'Assign Coverage' window with the following details:

- Shift name:** Gap Coverage
- Starts on:** Jun 30, 2019 12:00 AM to 12:00 AM (24 Hours)
- Repeat Cycle:** Occurs Every Day
- CONTACTS tab selected:** Shows a list of contacts with checkboxes and tier assignments.
- Search Contacts...:** Search bar with a magnifying glass icon.
- Table Headers:** CONTACT NAME, TIER, UNIQUE ID
- Table Data:**

	CONTACT NAME	TIER	UNIQUE ID
<input checked="" type="checkbox"/>	1, 1	Tier 1	1
<input checked="" type="checkbox"/>	11, 11	Tier 1	11
<input checked="" type="checkbox"/>	13, 13	Tier 2	13
<input type="checkbox"/>	14, 14	--	14
<input type="checkbox"/>	15, 15	--	15
<input type="checkbox"/>	17, 17	--	17
- Display:** 25 Entries Selected 6 of 40 Results
- Buttons:** CANCEL (light blue), ASSIGN (blue)

3. Select **Assign**.

Delete an Assignment from an Existing Shift

To unassign a contact/group/schedule from a shift

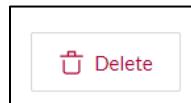
1. From the **Schedules** page, select the desired schedule.
2. Select the **Assignments** tab.
3. On the desired assignee, select the **Tier** drop-down list in the **Shift** column.



4. Assign the "--" tier to that assignee.

To remove an entire contact/group/schedule from being a possible assignee to a shift

1. On the tab, select the checkbox next to the desired assignee(s).
2. Select **Delete**.

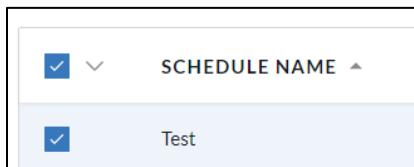


3. A warning is displayed if that assignee is currently assigned to a shift. Select **Delete** to confirm.

Delete a Schedule

To delete a Schedule

1. Navigate to the **Schedules** page.
2. Select the checkbox next to the schedule(s) to be deleted.



3. Select **Delete**.
4. Select **Delete** again to confirm.

Duplicate a Schedule

Schedules can be duplicated to aid in making separate yet similar schedules. The user must have **Create** and **Modify** permissions to duplicate a schedule.

To duplicate a schedule

1. Navigate to the **Schedules** page.
2. Check the checkbox next to the schedule to duplicate.
3. Select **Duplicate**.



The selected schedule opens as if the user is creating a new schedule but with the original schedule's data. The Schedule Name defaults to "<name of copied Schedule>-copy." The same shifts are listed as well as the same assignments, but all these elements can be edited before saving the new schedule.

4. Select **Done**.

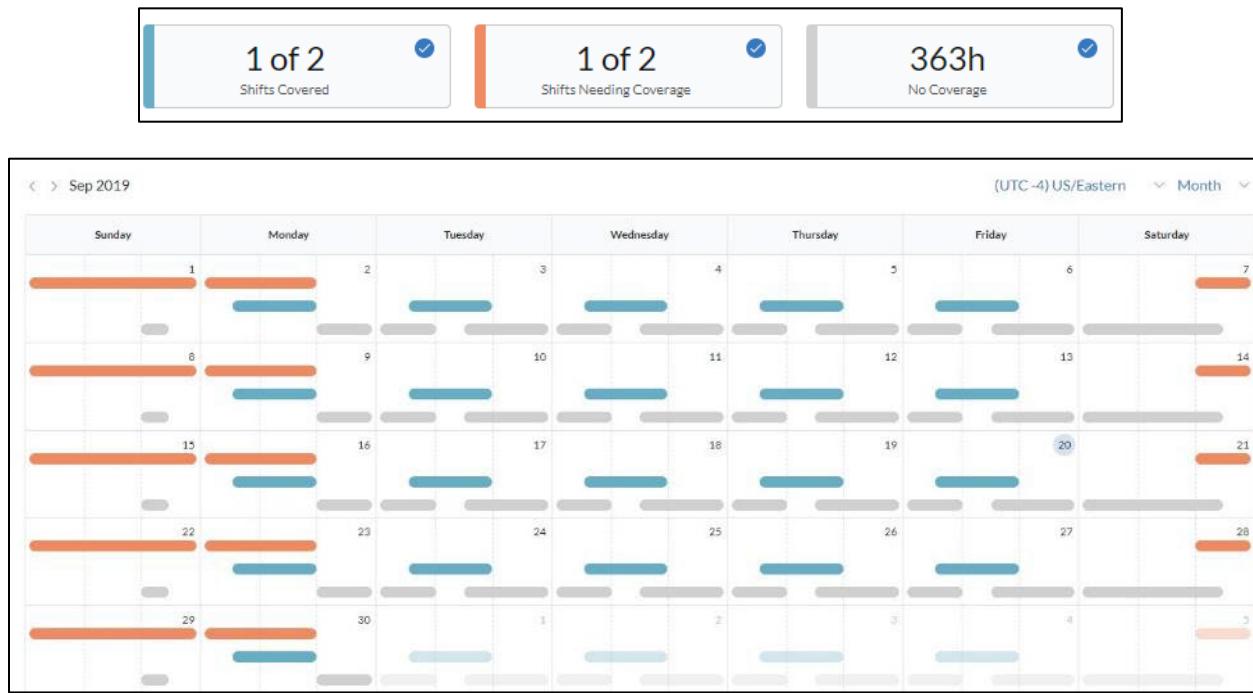
Note: Any contacts, groups, and nested schedules the user doesn't have access to are removed in the duplication process.

View Coverage

To view a schedule and the provided coverage, navigate to **Schedules** in the left navigation menu, and select the **Coverage** icon next to the desired schedule. Or, select the desired schedule and then **View Coverage**.

<input type="checkbox"/>	SCHEDULE NAME	DESCRIPTION	LAST MODIFIED	COVERAGE
<input type="checkbox"/>	Test	Test Schedule	Jan 29, 2020 02:41 PM	
<input type="checkbox"/>	test sched	test	Feb 10, 2020 08:57 AM	

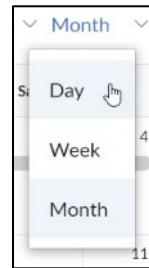
By default, the monthly view is displayed:



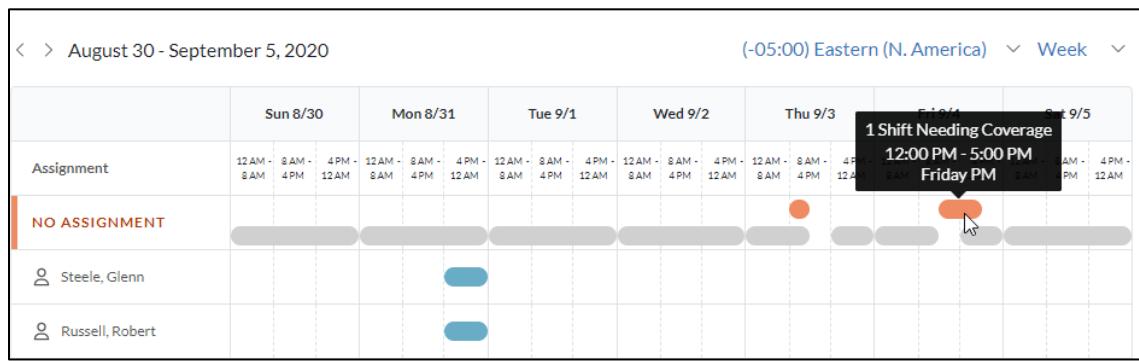
The legend above the calendar explains the three colors that may be displayed on the calendar:

- **Shifts Covered – Blue:** Blue indicates the shifts that have at least one contact assigned to them.
- **Shifts Needing Coverage – Orange:** Orange indicates shifts that have no contacts assigned to them. Select any orange bar to assign coverage.
- **No Coverage – Grey:** Grey indicates times of the day not covered by a shift. The legend at the top displays the total number of hours not covered by a shift.

The calendar view can also be set to **Month** or **Day** by selecting from the drop-down list.



In any view, hover over a shift to see more details. Select any orange bar to assign coverage.



The screenshot shows a weekly calendar view from August 30 to September 5, 2020. The time axis is labeled from 12 AM to 4 PM for each day. A tooltip at the top right of the screen says "1 Shift Needing Coverage" for the "Friday PM" shift. A cursor is hovering over an orange bar representing a shift gap for "Steele, Glenn". Other users listed are "Russell, Robert" and "NO ASSIGNMENT".

Note: For more information on how to add coverage to shift gaps, see [Add a Shift to a Shift Gap](#).

View Exceptions

Use the weekly or daily calendar views to see shifts with exceptions. They are colored blue but with a gradient to denote that the shift is covered but contains exceptions.



WEEKLY VIEW



DAILY VIEW

View Coverage Overview Details

Use the daily view to select any shift and see coverage details. For a shift that contains exceptions, select **View Exception** to see those details.

Coverage Overview

Assignee
Poppins, Mary
Type
Contact

SHIFT DETAILS
Listed below is the shift(s) details of the assigned contact, group or schedule.

Day: 6:00 PM - 2:00 PM (20 hours)

Starts on
Jul 1, 2019
Repeat Cycle
Occurs every day
Tier
Tier 1

SHIFT DETAILS
Listed below is the shift(s) details of the assigned contact, group or schedule.

Day: 6:00 PM - 2:00 PM (20 hours) EXCEPTION

Starts on
Jul 1, 2019
Repeat Cycle
Occurs every day
Tier
Tier 1
Exceptions

Sep 26, 2019 - Oct 2, 2019
12:00 AM - 12:00 PM VIEW EXCEPTION

Poppins, Mary Exception

Temporarily remove a contact, group, or schedule from one or more shifts and optionally add a replacement.

DATES **REPLACEMENTS**

EXCEPTION DATE(S)
Select the date range and time of your exception.

Date Range
09 / 26 / 2019 - 10 / 02 / 2019

Start Time
12:00 AM AM
 PM

End Time
12:00 PM AM
 PM

(Duration: 6 days 12 hours)

Poppins, Mary Exception

Temporarily remove a contact, group, or schedule from one or more shifts and optionally add a replacement.

DATES **REPLACEMENTS**

SHIFTS AFFECTED ?
These are the shifts affected according to the assignment and dates defined.

Search Shifts...

SHIFT NAME	STARTS ON	REPEAT CYCLE
Day	Jul 01, 2019 6:00 PM to 2:00 PM (20 hours) <input type="button" value=""/>	Occurs every day

Export Coverage

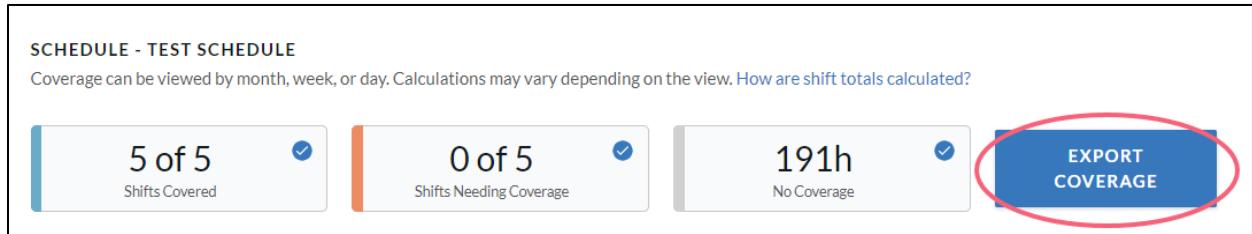
Users can export a schedule's coverage to an ICS file and use that file to import the coverage into their calendar application.

Note: As the OnSolve Platform only exports schedule coverage into ICS files, only calendar applications that work with ICS files can import the coverage.

- From the **Schedules** page, select the **View Coverage** icon next to the desired schedule.

<input type="checkbox"/> <input type="button" value="▼"/>	SCHEDULE NAME	DESCRIPTION	LAST MODIFIED	COVERAGE
<input type="checkbox"/>	Test Schedule	Test for Export Coverage	Mar 19, 2020 08:36 AM	<input type="button" value=""/>

2. Select **Export Coverage**.

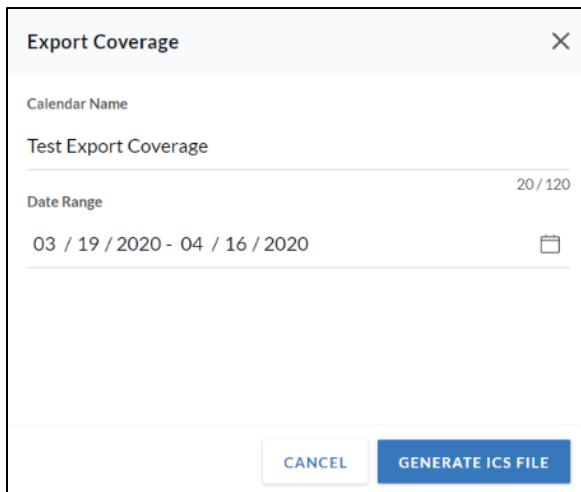


SCHEDULE - TEST SCHEDULE
Coverage can be viewed by month, week, or day. Calculations may vary depending on the view. [How are shift totals calculated?](#)

5 of 5 Shifts Covered 0 of 5 Shifts Needing Coverage 191h No Coverage EXPORT COVERAGE

3. Enter a **Calendar Name**.

4. Enter a **Date Range** to export. The default is the next 30 days.



Export Coverage X

Calendar Name
Test Export Coverage

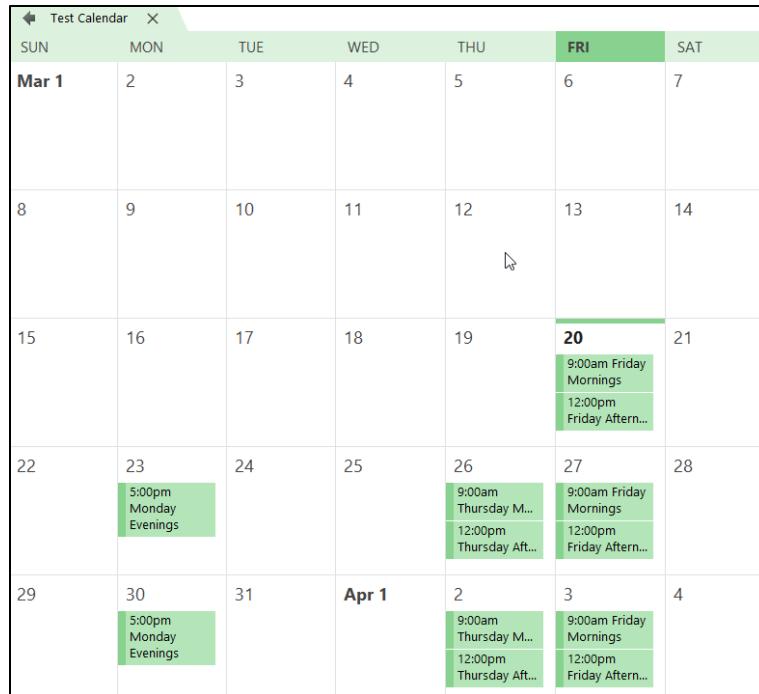
Date Range
03 / 19 / 2020 - 04 / 16 / 2020 20 / 120

CANCEL GENERATE ICS FILE

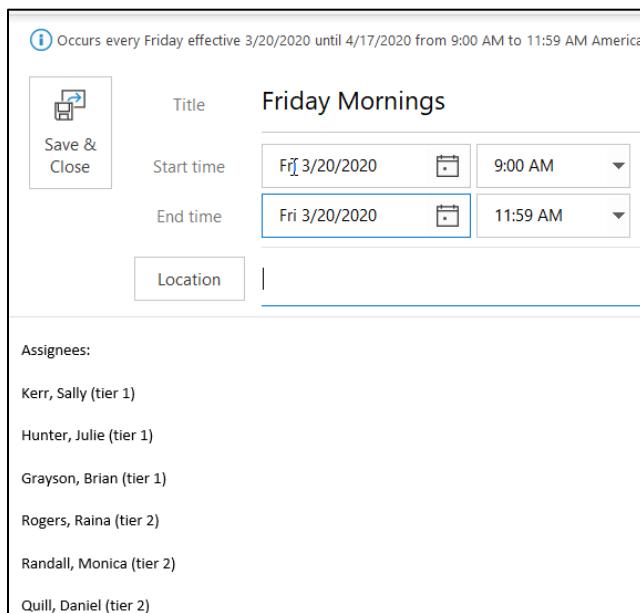
5. Select **Generate ICS File**.

6. Select **Download ICS File**.

7. Navigate to the ICS file on your computer and open it. The file will open in the user's default calendar application.



8. Open any shift to see assignees and their shifts.



Note: The above images are from Microsoft Outlook. To open an ICS file in an application other than the user's default, right-click on the file, select **Open with**, and choose the desired application.



Section 3: Alert Management

Create a Quick Alert

Quick Alert allows you to conveniently create and send an alert directly from your control center view. This streamlined feature set lets you send critical alerts to contacts instantly.

While quick alerts can be sent to contacts, groups, schedules, and topics, you can also send a quick alert to every contact in the same map cluster, or to a map group you create on the fly using the Control Center map and people's saved locations. To do so, see [Send a Quick Alert to a Map Cluster](#) and [Send a Quick Alert to a Map Group](#), respectively.

Notes

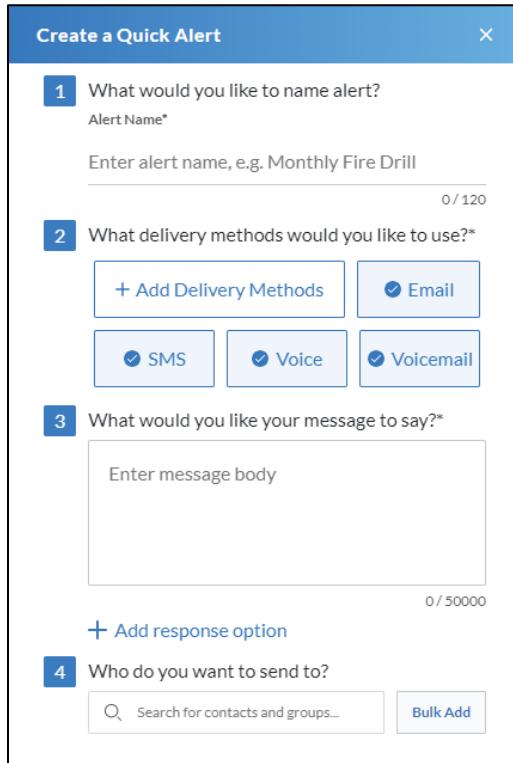
You can only send quick alerts on the fly; they cannot be saved or scheduled.

In this release, quick alerts are sent according to the OnSolve Platform's default delivery settings:

- One contact attempt cycle.
- A text device delay of 10 minutes.
- Device priority is based on the recipients' individual priority settings from their people records.
- Strict device delay is set to OFF.
- Only Contact Once is set to OFF.

To create a quick alert

1. Select **+ Create Quick Alert** from the control center view. The **Create a Quick Alert** window opens from the right.



The screenshot shows the 'Create a Quick Alert' window with the following steps:

- 1** What would you like to name alert?

Enter alert name, e.g. Monthly Fire Drill
0 / 120
- 2** What delivery methods would you like to use?*
 -
 - Email
 - SMS
 - Voice
 - Voicemail
- 3** What would you like your message to say?*

0 / 50000
 -
- 4** Who do you want to send to?
 -
 -

2. Enter an **Alert Name**.
 3. Select delivery methods. Email, SMS, Voice, and Voicemail are pre-selected; click on any to deselect them. Select **+Add Delivery Methods** to choose other delivery methods.
- Note:** You can configure default modalities for quick alerts by navigating to **Configure > Default Modality Configuration** and following the instructions in [Default Modality Configuration](#).
4. Compose the message body.
 5. Optionally, add response options and actions.
 6. Choose recipients by searching for names or by using the **Bulk Add** option.

Note: A warning is displayed if you add more than 5000 recipients.

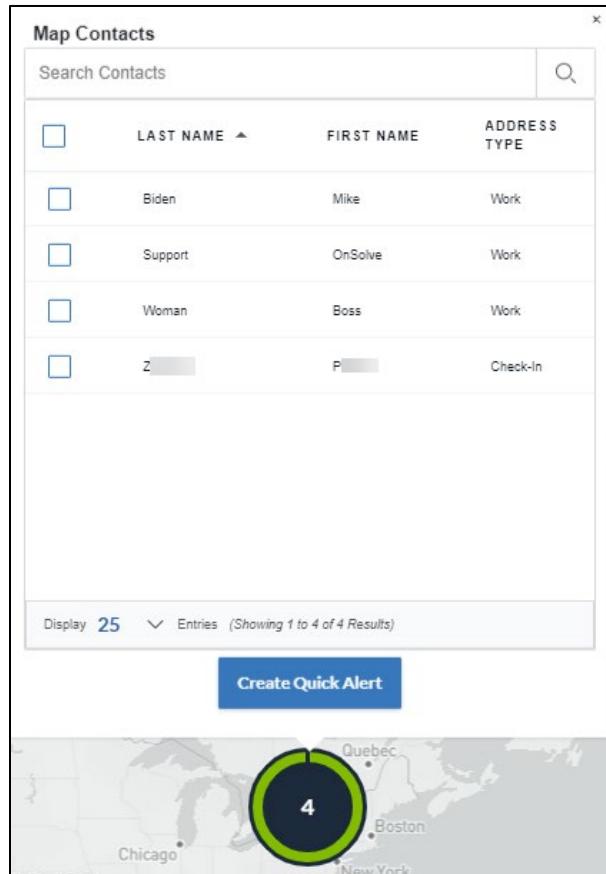
7. Select **Send Now**.

Note: If you change your mind before sending and instead want to create an advanced alert, select **Continue to advanced alert**. The alert overview opens prepopulated with all the information you already entered.

To send a quick alert to a map cluster

1. Select the map cluster. A table of contacts in that cluster opens.

Note: The contacts in a map cluster can change depending on how zoomed in or out on the map you are. Zoom in to view clustered contacts within a smaller area and zoom out to view clustered contacts within a larger area.



The screenshot shows a 'Map Contacts' interface. At the top, there's a search bar labeled 'Search Contacts' with a magnifying glass icon. Below the search bar is a table with four rows of contact information. The columns are labeled 'LAST NAME ▲', 'FIRST NAME', and 'ADDRESS TYPE'. The contacts listed are Biden (Mike, Work), Support (OnSolve, Work), Woman (Boss, Work), and Z (P, Check-in). At the bottom of the table, there's a 'Display 25' dropdown and a note '(Showing 1 to 4 of 4 Results)'. Below the table is a blue button labeled 'Create Quick Alert'. At the very bottom of the interface is a map showing locations like Chicago, Boston, and New York. Overlaid on the map is a green circle containing the number '4', indicating the count of contacts in the cluster.

	LAST NAME ▲	FIRST NAME	ADDRESS TYPE
<input type="checkbox"/>	Biden	Mike	Work
<input type="checkbox"/>	Support	OnSolve	Work
<input type="checkbox"/>	Woman	Boss	Work
<input type="checkbox"/>	Z	P	Check-in

Display 25 Entries (Showing 1 to 4 of 4 Results)

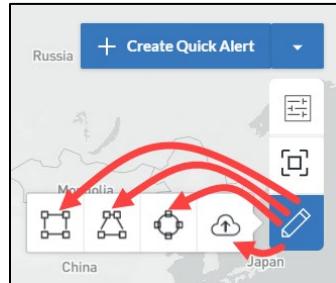
Create Quick Alert

4

2. Select the contacts to include in the quick alert.
 - Use the **Search Contacts** field to search by First Name or Last Name.
 - Select all contacts on that page of the table by selecting the top-most checkbox.
3. Select **Create Quick Alert**.
4. Continue with step 2 [to create a quick alert](#). The contacts you selected are already saved as recipients. You may add more recipients if desired.

To send a quick alert to a map group

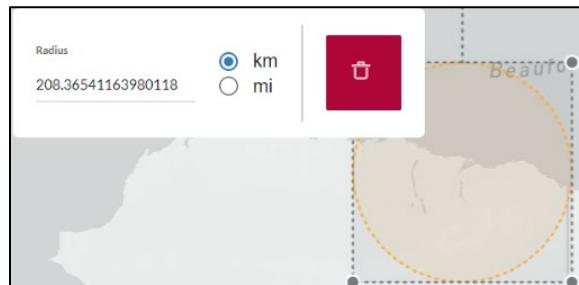
1. Select the drawing tool and choose the square, polygon, or circle drawing option, or import a shape.



- To use the square drawing tool, click and hold as you move your mouse to create the square. Once the square is created, you can drag it to any place on the map or click and drag a corner point to resize it. You can also rotate it by using the rotation handle.



- To use the polygon drawing tool, click on the map to choose a starting point, and continue clicking on different points on the map to create the shape's corner points. Complete the shape by clicking again on the starting point. Once the shape is complete, you can drag it to any place on the map or click and drag a corner point to reshape it. Click outside the polygon to finalize it.
- To use the circle drawing tool, click and hold as you move your mouse to create the circle. Once the circle is defined, optionally adjust the radius length or unit of distance. Drag it to any place on the map or resize it. You can also reshape it to an oval and rotate it using the rotation handle. Click outside the circle to finalize it.



- To upload a shape file, drag and drop a file, or browse your computer to upload a file. Accepted file types are .shp and .kml. The shape appears on the map. Drag it to any place on the map or click and drag a corner point to reshape it.



- Draw or import your shape onto the map, capturing the contacts you want to include or exclude in your alert. Optionally, add more shapes. You can add unlimited shapes, mix shape types, and overlap shapes.
 - To include the people with saved locations in the shape in your alert, continue to step 3.
 - To exclude the people with saved locations in the shape from your alert, select the **Exclude** toggle in the shape summary bar that opens at the bottom of the map.



- Delete a shape by selecting it and then selecting the trash can icon.
- Once your shape is complete, click outside the shape to finalize it. At the bottom of the map, the shape summary bar confirms the number of shapes drawn and the number of people in the shape(s).



- Optionally, turn **Geofence ON** to include people who can receive alerts via the OnSolve Mobile app.
- Select **Create Quick Alert** in the Quick Alert Mapping Bar. The **Create Quick Alert** window opens. To complete and send the quick alert, follow the instructions in [To Create a Quick Alert](#). The people with saved locations in your shape(s) are saved to a map group that is listed as a recipient of the quick alert. If desired, you can add contacts, more groups, schedules, and topics as recipients. This map group also saves to your **Groups** page.



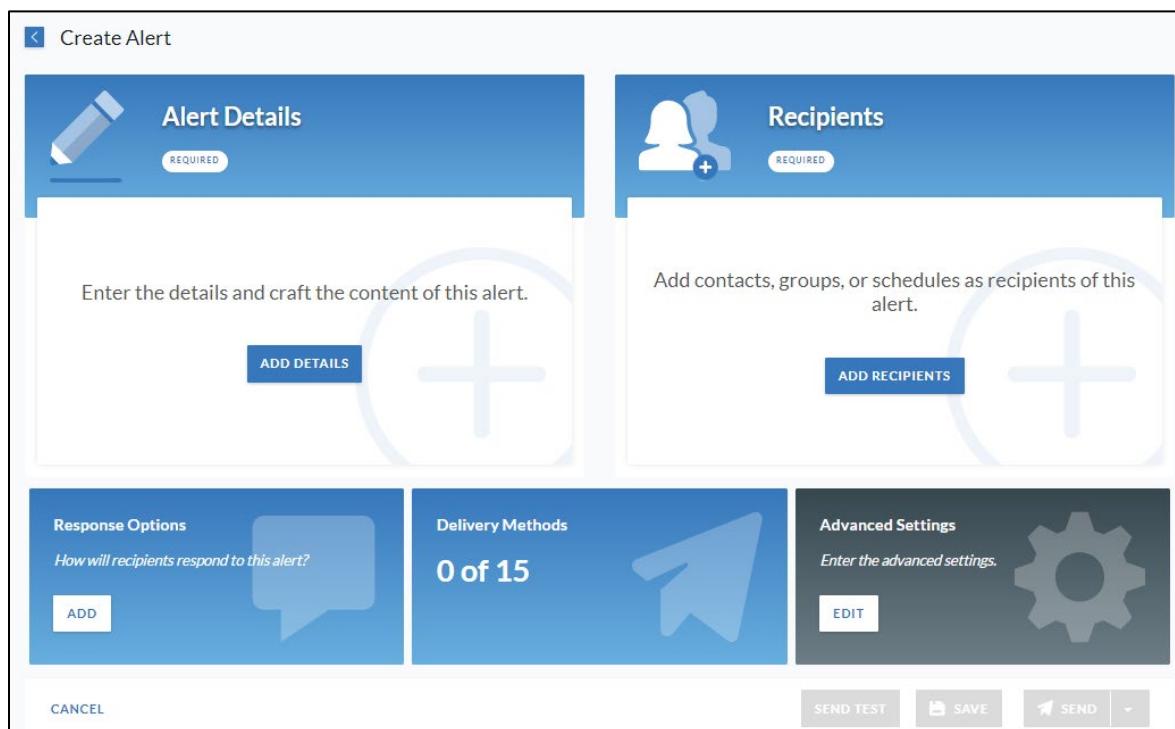
Create an Advanced Alert

An alert is a voice or text communication composed by an administrator or authorized user to one or more designated recipients in the organization's account and delivered via the OnSolve Platform. OnSolve verifies alert delivery and status in real time, recording and presenting voice and text responses as they are generated.

An advanced alert is the traditional multi-component alert sent from the OnSolve Platform. Traditional alerts include a flexible variety of sending options, with alert delivery to multiple groups at one time, recipient selection and device label specification, and optional features such as Response Options, Conference Bridge, Customizable Alert Introduction, and Cascade.

Create an advanced alert by selecting the arrow next to **+ Create Quick Alert** from the control center view. Starting with a scenario from the **Scenario Library** is also an option.

The advanced alert-creation process is comprised of up to five sections: **Alert Details**, **Recipients**, **Response Options** (optional with a Broadcast alert, required with a Quota alert), **Delivery Methods** (optional), and **Advanced Settings** (optional). While you can start with any of these sections and complete them in any order, the type of alert—Broadcast, Quota, or Bulletin Board—can determine which sections are relevant or accessible. As you complete each required section, it is marked **Complete**.



Note: The Response Options section can be configured to be required. Contact an OnSolve representative to have this option enabled.

Add Alert Details

You have the choice of starting a new alert from scratch or selecting a scenario from the Scenario Library. See [Scenario Library](#) for more information.

To start a new alert from scratch

- From the alert overview, select **Add Details**. The **Alert Details** page opens.

The screenshot shows the 'Alert Details' page. At the top, there's a header with a back arrow and the title 'Alert Details'. Below it is a section for 'Alert Name*' with a text input field containing 'Enter alert name, e.g. Monthly Fire Drill' and a character count of '0 / 120'. To the right is a blue button labeled '+ Insert Variables'. The next section is 'Alert Description' with a text input field containing 'Enter alert description' and a character count of '0 / 160'. Below that is a 'Division' dropdown menu set to 'Albany'. The 'Message Body *' section includes a language selector ('English (US)') and a link to '+ Add Language'. A 'Customize Message' button is also present. A modal window titled 'Customize Message' is open, showing tabs for 'All', 'Email', 'SMS', 'Voice', and 'Voicemail'. The 'All' tab is selected, showing a message body placeholder: 'Name'.

- Enter an **Alert Name**.
- Enter an **Alert Description**.
- Select the **Division** to which this alert will be accessible. The divisions displayed in this drop-down list are dependent upon your user privileges.
- Compose the **Message Body**.
 - Optionally, customize by device type by selecting **+ Customize Message** and choosing the desired device type. A new tab opens to compose the alert to send to that device type. Text entered in the **All** tab copies to the new tabs and can be edited. You can customize the message body in the alert for the following device types:
 - Email
 - SMS
 - TTY Phone
 - Fax

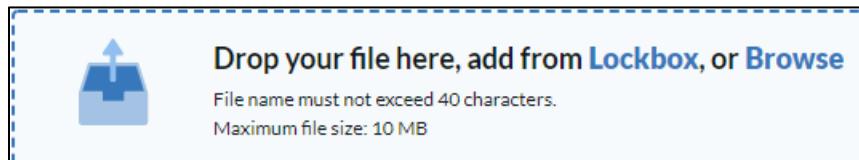
- Voice
- Voicemail
- Pager One-Way
- Pager Two-Way
- Recording

Notes

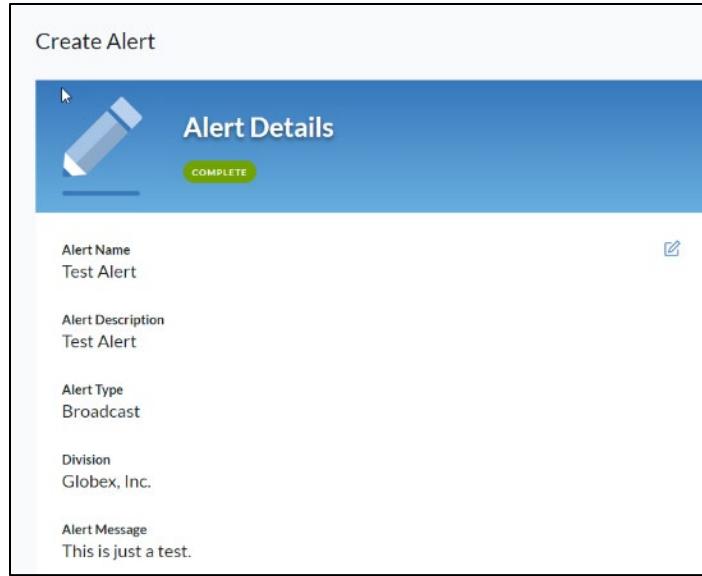
Messages can be customized based on whether recipients answer their voice devices or if the alerts go to voicemail. Customize by **Voice** and **Voicemail**, respectively.

When customizing for SMS, you can preview how the text message is segmented every 160 characters.

- b. To record an alert, see voice recording for [Message Body](#).
 - c. Optionally, select your [Languages](#) options.
 - d. Optionally, add **Alert Variables**. See [Alert Variables](#) for more information.
6. Optionally, add attachments or add files from the lockbox. Attachments are visible to email recipients, and lockbox files are visible to recipients with any text-based device. See [Lockbox](#) in Section 5 of this guide to learn more about adding files to the lockbox. Drag and drop the files into the attachment section, select **Browse** to upload the file, or select **Lockbox** to select a lockbox file.
- Attachments, but not lockbox files, are scanned with antivirus software, and if a virus is detected, a warning is displayed, and the file is not attached.
 - Only one lockbox file can be included in each alert.
 - An unlimited number of non-lockbox files can be added as long as file names do not exceed 40 characters and file sizes do not exceed 10 MB.



7. Select **Save**. The **Alert Details** section on the alert overview displays a summary of those details.



Scenario Library

The Scenario Library contains commonly used alerts defined by industry and event type. These predefined scenarios can be selected via the **Critical Communications > Scenario Library** option on the left navigation menu.

Scenario Library			
SCENARIO NAME	INDUSTRY	DESCRIPTION	MESSAGE PREVIEW
Alternate Side Parking	Event - Public Notifications	Alternate Side Parking	Please be advised that alternate side parking rules will be in effect for all roads within city limits until further notice... Any vehicles parked illegally will be towed by municipal agencies.
Boil Water Notice	Event - Public Notifications	Boil Water Notice	The area water supply to the municipalities of <area names> has been compromised... Officials are testing the water quality and will provide updated information as it becomes available... At this time, officials have ls...
Bomb Threat	Energy & Utilities	Bomb Threat Summary and Next Steps	On <Date>, a bomb threat was received on the <Number# floor, building>... The authorities have been contacted to investigate the threat... So far, we are unable to validate it. Until the authorities recommend further action, the b...
Bomb Threat	Health Care	Actions and Next Steps	On <Date>, a bomb threat was received on the <Number# floor, building>... The authorities have been contacted to investigate the threat... So far, we are unable to validate it. Until the authorities recommend further action, the b...

Display 25 ▾ Entries (Showing 1 to 25 of 146 Results)

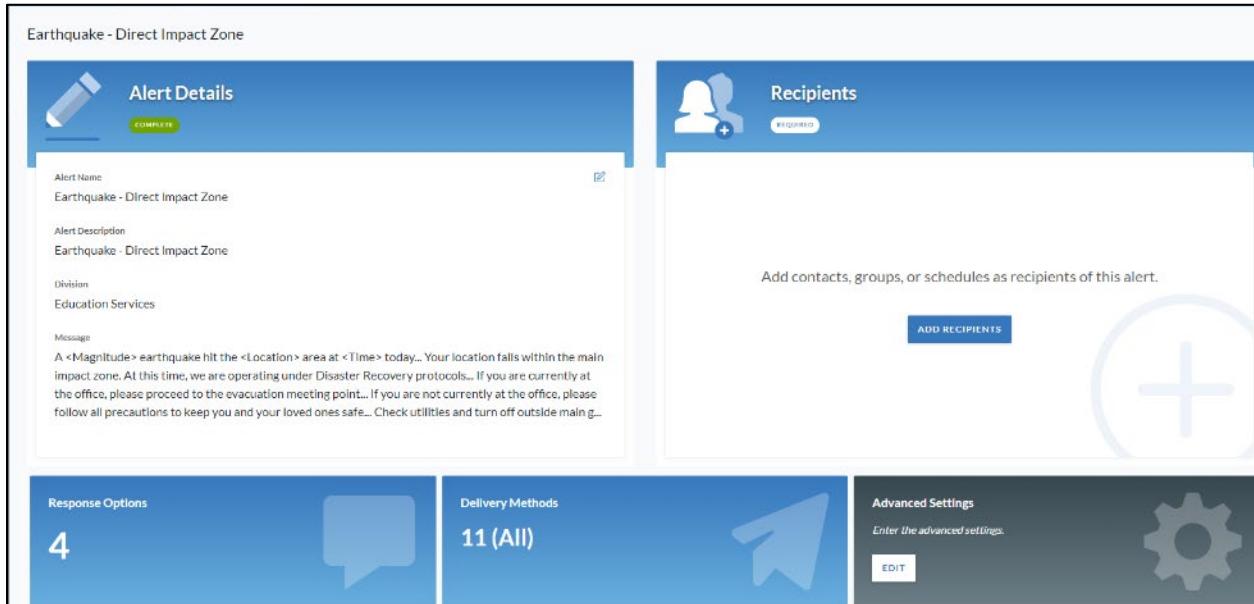
1 2 3 4 5 >

A list of available scenarios is displayed. You can locate scenarios by:

- Using the search bar to find scenarios by **Scenario Name, Description, or Message Preview**.
- Sorting alphabetically by **Scenario Name**.
- Filtering by **Has Response Option or Industry**.
 - For **Has Response Options**, choose **Yes** or **No**.
 - For **Industry**, choose one of the options in the drop-down list.

To use a scenario in an alert

1. After locating your desired scenario, select it. The alert overview opens, and that scenario's details are populated into the **Alert Details** section. If that scenario has saved response options or delivery methods, those are carried over.



The screenshot shows the 'Earthquake - Direct Impact Zone' alert overview. The left panel, titled 'Alert Details', contains fields for Alert Name ('Earthquake - Direct Impact Zone'), Alert Description ('Earthquake - Direct Impact Zone'), Division ('Education Services'), and a Message block. The right panel, titled 'Recipients', includes a 'Required' field, a 'Add contacts, groups, or schedules as recipients of this alert.' text area, and a 'ADD RECIPIENTS' button. Below these are sections for 'Response Options' (4), 'Delivery Methods' (11 (All)), and 'Advanced Settings' (with an 'Edit' button).

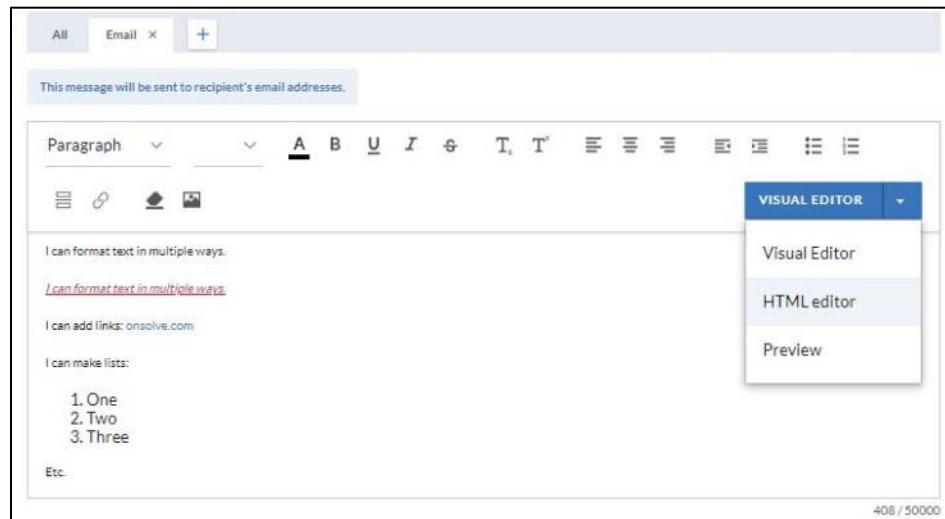
2. Continue with adding **Recipients** and, if desired, configuring **Advanced Settings**.

Note: After choosing a scenario, any part of it may be edited. From the alert overview, select the section you want to edit (**Alert Details, Response Options**, etc.), and make the desired edits.

Email Editor

If you choose Email as a device type when composing an alert, a WYSIWYG (What You See Is What You Get) editor is available to format the text of the alert. Most common editing tools are available, including font size, font color, font style, adding links, numbered and bulleted lists, and inserting a photo. Hover over any formatting component to read a tooltip.

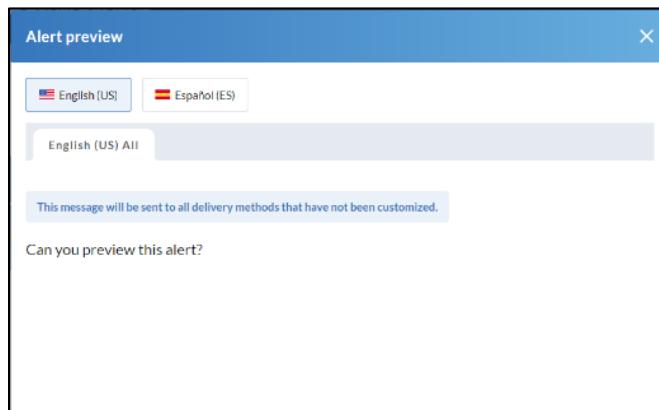
Any recipient with HTML email will see the alert as you formatted it.



To aid in editing, use the drop-down list to toggle between the **Visual Editor** (WYSIWYG), the **HTML editor**, and the **Preview**.

Preview Alert

Once the **Alert Details** are saved, you can preview the content of the alert by double-clicking within the **Alert Details** section. The **Alert Preview** window opens, and you can select any language or customization tab to see that content.

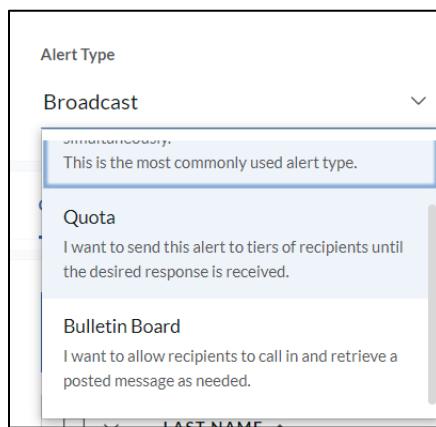


Add Recipients

The method of adding recipients depends on the chosen alert type—Broadcast, Quota, or Bulletin Board.

Note: You can save an alert without adding recipients to it. However, the alert type must be selected to save.

1. From the alert overview, select **Add Recipients**.
2. The **Alert Type** defaults to **Broadcast**. If desired, select **Quota** or **Bulletin Board** instead.



Note: You can change the alert type at any point before sending but will then need to re-select your recipients.

Broadcast Alert

The Broadcast method is the most versatile alert delivery method. Broadcast alerts are designed to disseminate information quickly for contacting many people simultaneously on single or multiple devices.

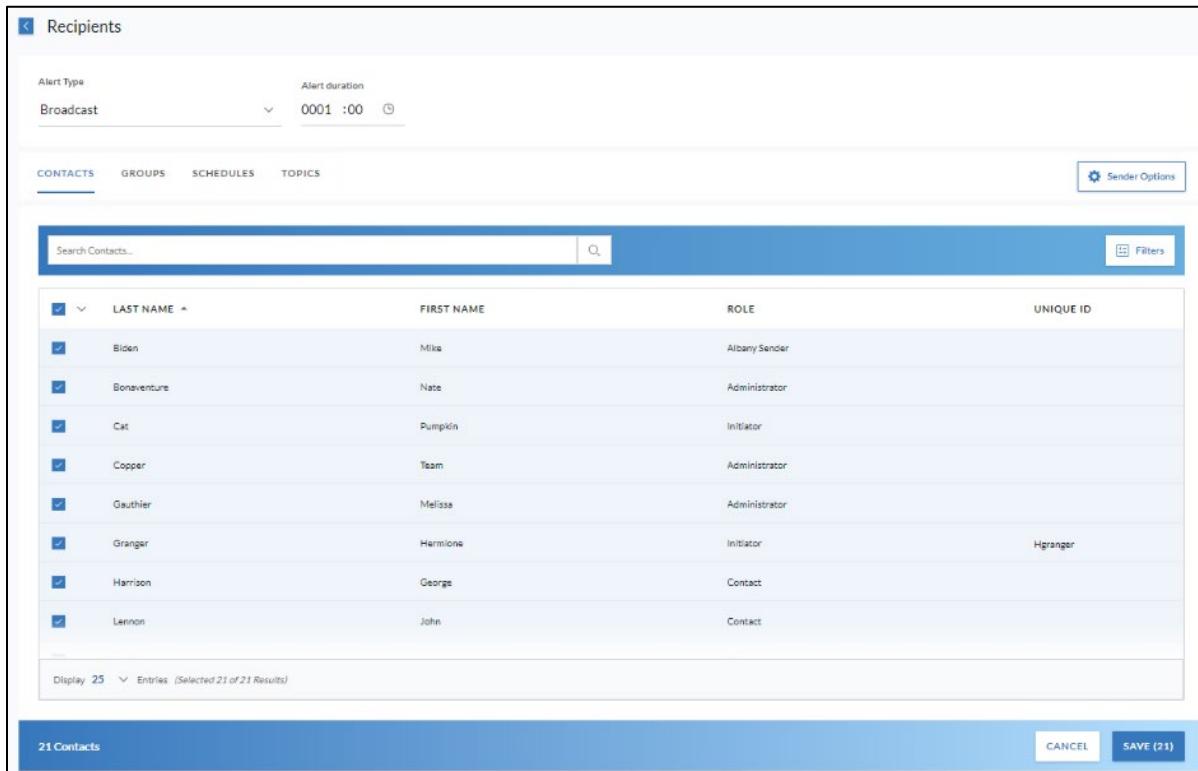
The alert stops attempting to contact the recipient when one of the following actions occurs:

- The recipient listens to and responds to the alert using one of the available response options.
- All contact attempt cycles have been completed.
- The alert duration expires.

To create a broadcast alert

1. From the **Recipients** page, set the **Alert Duration**. Alert duration determines how long the alert is active and can be set anywhere between 1 minute and 2016 hours. Once the alert duration expires, the system stops sending it out, whether or not all contact attempt cycles were completed and despite any other setting that would otherwise cause the alert to continue.

2. Choose the desired contacts, groups, schedules, and topics to add as recipients. Or, add contacts with [File-Based Alerting](#). To aid in finding, including, or excluding the desired contacts, groups, and schedules, consider using the following:
 - The search field
 - Filters
 - The **Select This Page** and **Select All Pages** options



LAST NAME	FIRST NAME	ROLE	UNIQUE ID
Biden	Mike	Albany Sender	
Bonaventure	Nate	Administrator	
Cat	Pumpkin	Initiator	
Copper	Team	Administrator	
Gauthier	Melissa	Administrator	
Granger	Hermione	Initiator	Hgranger
Harison	George	Contact	
Lennon	John	Contact	

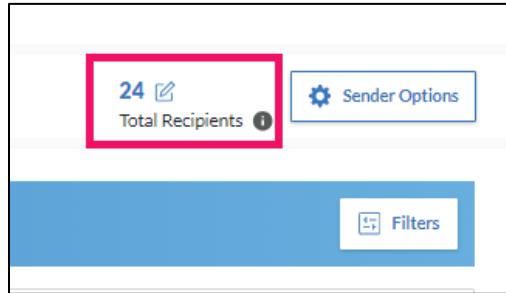
Display 25 ✓ Entries (Selected 21 of 21 Results)

21 Contacts CANCEL SAVE (21)

- When adding topics, select the **Category**, **Priority**, and **Severity** that will determine which contacts will receive the alert. In this release, you can choose only one option per topic.

Note: The **Send to Subscribers** advanced setting must be enabled to send an alert to topics.

- Exclude individual people from selected groups by selecting **Total Recipients** from the **Contacts** tab.



The **Current Recipient** window opens. Select next to those people you want to remove and select **Save**.

A screenshot of the 'Current Recipient' window. The title bar says 'Current Recipient' with a close button 'X'. At the top, there is a search bar 'Search Recipients...', a magnifying glass icon, and a 'Filters' button. To the right, it shows '2 Excluded' and '24 Total Recipients'. The main area is a table with columns: EXCLUDE, LAST NAME, FIRST NAME, ROLE, and UNIQUE ID. Each row contains a checkbox in the 'EXCLUDE' column. The data in the table is:

EXCLUDE	LAST NAME	FIRST NAME	ROLE	UNIQUE ID
<input checked="" type="checkbox"/>	Aguon	Melody	Recipient	maguon
<input checked="" type="checkbox"/>	Almond	Tony	Recipient	talmond
<input checked="" type="checkbox"/>	Baker	Doyle	Recipient	dbaker
<input checked="" type="checkbox"/>	Barker	Madeline	Recipient	mbarker
<input checked="" type="checkbox"/>	Bloom	Samantha	Administrator	sbloom

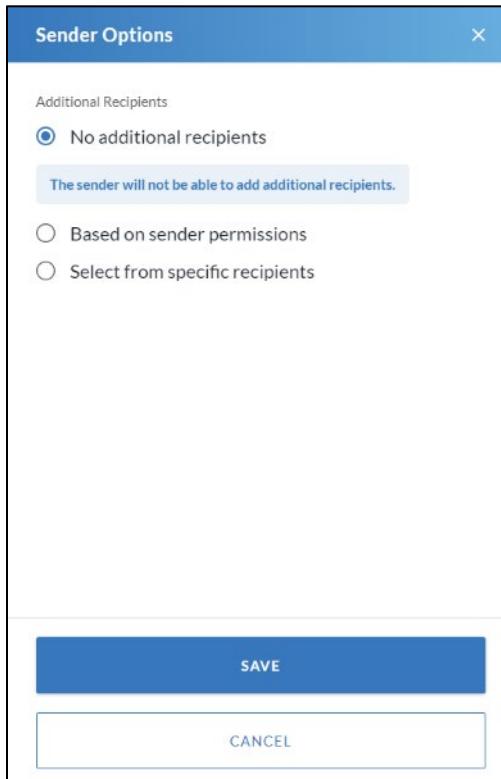
(Showing 1 to 25 of 26 loadable records)

Load Next 25

CANCEL SAVE

3. Optionally, allow alert senders access to additional recipients upon sending the alert.

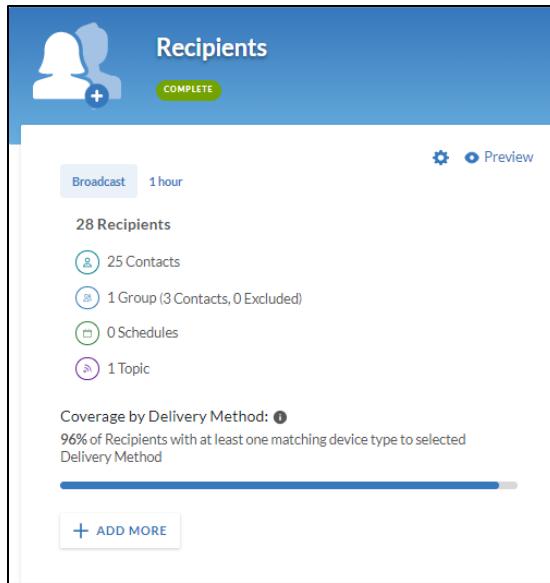
a. Select **Sender Options**.



- Choose **No additional recipients** to limit the alert sender to the recipients you selected in step 2.
- Choose **Based on sender permissions** to allow the alert sender to add more recipients to the alert based on their user role's permissions. This option automatically saves the alert as an alert template.
- Choose **Select from specific recipients** to add specific contacts from which the sender can choose. This option automatically saves the alert as an alert template.

b. Select **Save**.

4. Select **Save**. The **Recipients** section on the alert overview displays a summary of the number of contacts, groups, schedules, and topics to receive the alert and the alert type.



At any point before sending the alert, you can:

- Select **+ Add More** to add or remove recipients.
- Select **Preview** to see which contacts, groups, schedules, and topics you've added.
- Select the **Sender Options** cog wheel icon to edit sender options.
- Check **Coverage by Delivery Method**, which lists the percentage of recipients with at least one device type that matches your selected delivery methods. This data is provided once delivery methods have been selected, either manually or by default.

Quota Alert

The Quota Alert differs from the Broadcast alert type in that it uses escalation tiers to allow the sender to control who gets contacted and in what order. A Quota Alert is ideal when looking for a particular number of responders, or volunteers, from a group of people.

A Quota Alert requires at least one response option designated as the "desired" response. Once the required number of recipients choose the desired response, the alert ends and no longer attempts to contact users on the recipient list. See [Add Response Options](#) and [Response Options](#) for more information.

Tier Advancement

The system advances to the next tier when either:

- All recipients in a tier have been contacted, but the quota has not been met or
- The tier duration expires.

Recipient Contact Order

- If only one contact is in a tier, the OnSolve Platform contacts all selected devices for the set number of contact attempt cycles for that contact. The alert is advanced to the next tier if the quota is not met by the time the tier duration expires or after all contact attempts have been exhausted.
- If multiple contacts or groups are in a tier and **Contacted at Once** is set to **One**, the order in which contacts are alerted is based on the time since those contacts last received an OnSolve alert. The contact who least recently received an OnSolve alert is contacted first, and the contact who most recently received an OnSolve alert is contacted last.
- When schedules are assigned to a tier, the recipient contact order depends on the day and time the alert is sent. At the time of sending an alert, the OnSolve Platform sends the alert to those recipients who are on call at that time.

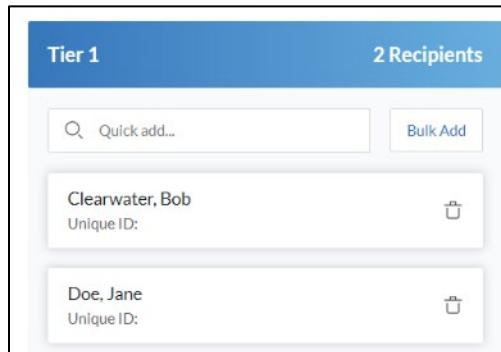
To create a quota alert

1. After selecting **Quota** as the alert type, enter the **Number of People Needed** to respond with the desired response.
2. Enter the number of recipients who should be **Contacted at Once**, or if they all should be contacted at once, select the **All** checkbox.

Number of People Needed	Contacted at Once	<input type="checkbox"/> All
3	5	

3. Add contacts, groups, schedules, and topics to Tier 1. Use the **Quick add** option to search for individual contacts/groups/schedules and the **Bulk Add** option to add multiple contacts/groups/schedules/topics at once.

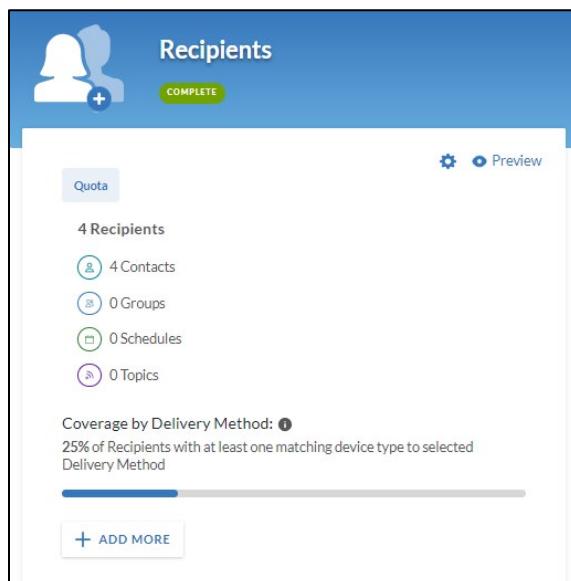
Note: Topics can only be added as recipients through the **Bulk Add** option.



4. Enter, in hours and minutes, how long the OnSolve Platform should wait to stop contacting this tier and move on to the next tier. If there is only one tier, the entered time is the total alert duration.



5. If desired, add up to 50 total tiers by selecting **+ Add Tier** and repeating steps 3–4. Delete tiers by selecting the trash icon.
6. Select **Save**. The **Recipients** section on the alert overview displays a summary of the number of contacts, groups, and schedules to receive the alert and the alert type.



At any point before sending the alert, you can:

- Select **+ Add More** to add or remove recipients.
- Select **Preview** to see which contacts, groups, schedules, and topics you've added.
- Select the **Sender Options** cog wheel icon to edit sender options.
- Check **Coverage by Delivery Method**, which lists the percentage of recipients with at least one device type that matches your selected delivery methods. This data is provided once delivery methods have been selected, either manually or by default.

Bulletin Board

A bulletin board is a passive alert in that the OnSolve Platform does not actively attempt to contact anyone. Instead, your contacts call in and retrieve a posted message, as needed and at their convenience. For instructions on retrieving a bulletin board alert and the number(s) to use, see [Bulletin Boards](#) in Section 9 of this guide. Administrators who use bulletin board alerts should distribute the call-in phone number to their contacts.

When creating a bulletin board alert, the **Delivery Methods** section is inaccessible, and the **Advanced Settings** section is limited to those settings that apply to this type of alert. Response options do work in conjunction with bulletin board alerts.

To create a Bulletin Board alert

1. After selecting **Bulletin Board** as the alert type, set the **Alert Duration**. Alert duration determines how long the alert is active and can be set anywhere between 1 minute and 2016 hours. Once the alert duration expires, contacts who call in cannot listen to this alert.
2. Choose the desired contacts, groups, and topics to add as recipients. These are the contacts who, after the system verifies them via their telephony IDs or phone numbers, will be authorized to listen to the alert. To aid in finding or selecting the desired contacts, groups, and topics, consider using the following:
 - The search field
 - Filters
 - The **Select This Page** and **Select All Pages** options

When adding topics, select the **Category**, **Priority**, and **Severity** that will determine which contacts can call in to listen to the alert. In this release, you can choose only one option per category.

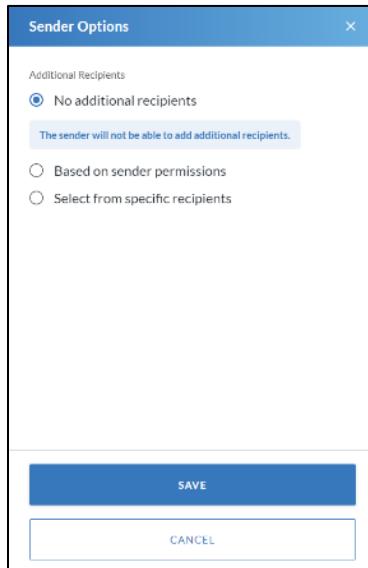
Notes

Bulletin board alerts cannot have schedules as recipients.

The **Send to Subscribers** advanced setting must be enabled to send alerts to topics.

3. Optionally, allow alert senders access to additional recipients upon sending the alert.

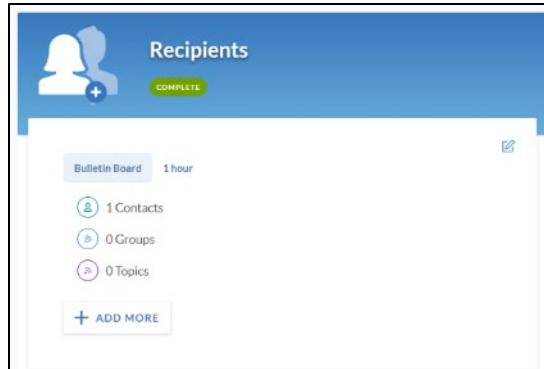
- a. Select **Sender Options**.



- Choose **No additional recipients** to limit the alert sender to the recipients you selected in step 2.
- Choose **Based on sender permissions** to allow the alert sender to add more recipients to the alert based on their user role's permissions. This option automatically saves the alert as an alert template.
- Choose **Select from specific recipients** to add specific contacts from which the sender can choose. This option automatically saves the alert as an alert template.

- b. Select **Save**.

- Select **Save**. The **Recipients** section on the alert overview displays a summary of the number of contacts, groups, and topics eligible to call in to listen to the alert and the alert type.



At any point before sending the alert, select **+ Add More** to add more recipients to the alert or select the edit icon to remove recipients.

- In the **Alert Details** section, the **Message Body** content you provide is the content of the alert that people hear when they call in. Customize the message by **Recording** so callers hear a recorded voice when they call in. Or compose the message body in the **All** tab, and callers will hear the message via a text-to-speech engine.

Note: Content in the **Recording** tab will override any content in the **All** tab.

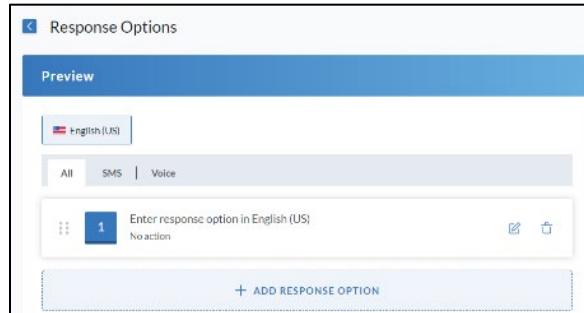
- Select **Send**. While the alert isn't sent to the recipients you selected, this alert is now posted to the bulletin board, and those recipients are eligible to call in and listen to the alert.

Add Response Options

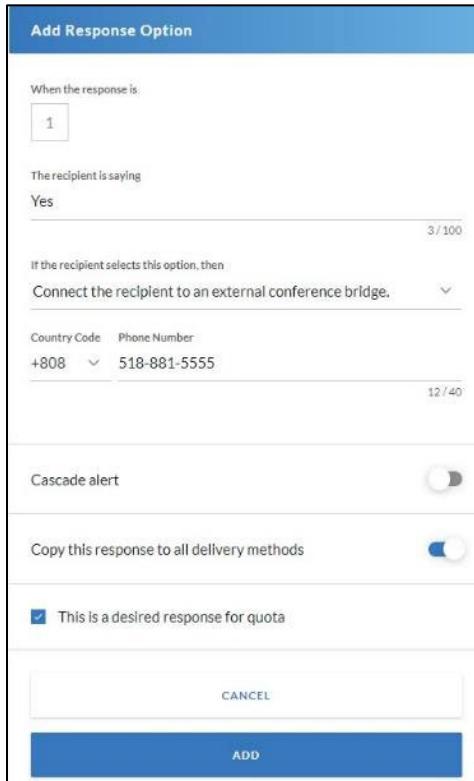
Optionally, include structured responses to gain reportable feedback from your recipients.

Note: When a contact receives an email alert with response options, they have the option of responding in three ways: Selecting the link that represents their response, replying to the email with the number that corresponds to their response, or calling in to a provided phone number.

- From the alert overview, in the **Response Options** section, select **Add**.



2. Select **+ Add Response Option**. The **Add Response Option** section opens on the right.
3. For each response option, determine the text of the response, as well as the resulting action. The response number is auto-generated and not editable.



The screenshot shows the 'Add Response Option' dialog box. At the top, it says 'When the response is:' followed by a box containing the number '1'. Below this, it asks 'The recipient is saying' and has a field with 'Yes' and a character count of '3 / 100'. Underneath, it says 'If the recipient selects this option, then' and has a dropdown menu set to 'Connect the recipient to an external conference bridge.' A country code and phone number field shows '+808 518-881-5555'. There's a note '12/40' below it. Further down are checkboxes for 'Cascade alert' (unchecked), 'Copy this response to all delivery methods' (checked), and 'This is a desired response for quota' (checked). At the bottom are 'CANCEL' and 'ADD' buttons.

- a. Enter the text of the response option in the **The recipient is saying** field.
- b. If the message body of the alert was recorded, Optionally, **Record response options**. These response options are sent to recipients with voice devices. Follow the instructions in voice recording for [Response Options](#).
- c. Select the resulting action from the **If the recipient selects this option, then** drop-down list. The options are **No action**, **Connect the recipient to an internal conference bridge**, **Connect the recipient to an external conference bridge**, **Mark the recipient as not available**, and **Ask a follow-up question**.
 - If connecting the recipient to an internal conference bridge and using the sandbox (beta) environment, select the **571** number from the **Conference Bridge Number** drop-down list. If using the production environment, select the **858** number. These are the only options in this release of the OnSolve Platform.
 - If connecting the recipient to an external conference bridge, see [External Conference Bridge](#).
 - If asking a follow-up question, see [Ask a Follow-Up Question](#) below.

Notes on Internal Conference Bridge

Participants are unmuted upon joining an internal conference bridge and cannot be muted.

The maximum duration of an internal conference bridge is 48 hours.

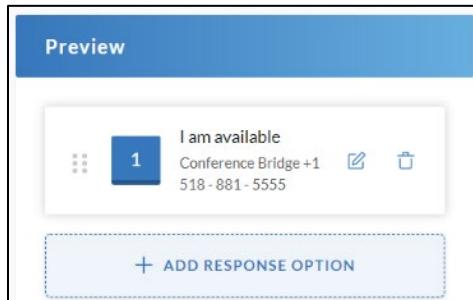
The internal conference bridge closes if no one joins within 15 minutes and 15 minutes after the last person has left.

OnSolve recommends no more than 25 participants in a single internal conference bridge, although the system can handle more.

OnSolve recommends no more than 20 concurrent internal conference bridges, although the system can handle more.

There is no dashboard from which a user can see who is on the internal conference bridge, drop callers, mute callers, etc.

4. Select whether to send a **Cascade alert**. See [Send a Cascade Alert](#) for detailed information.
5. Select **Copy this response to all delivery methods** if you are sending the alert to multiple delivery methods and want recipients of all methods to have the same response options.
6. If creating a quota alert, select whether **This is the desired response for quota**. By default, this is selected but may be deselected. More than one response may be designated as a desired response. See [Quota Alert](#) for more information.
7. Select **Add**. The saved response option appears in the preview to the left.

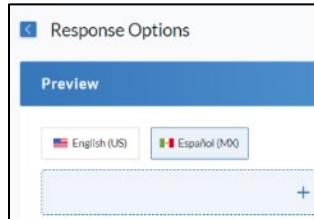


8. Repeat steps 2–7 until all desired response options have been added. There is no limit to the number of responses you may add. At any point, modify a response option by selecting the edit icon or delete it by selecting the trash can.
9. If the message body is customized by device type, select the next device type tab and repeat steps 2–7 for each device type.

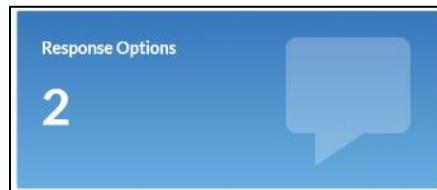


Note: If the message body is customized for **Recording**, see voice recording for [Response Options](#).

10. If the message body is composed in more than one language, select the next listed language and repeat steps 2–8 above.



11. Select **Save**. The **Response Options** section on the alert overview displays the number of response options in the alert as well as other details about those response options.



If any recipients respond to an alert with anything other than the provided response options, these other responses are recorded in that alert's analytics.

Ask a Follow-Up Question

When adding response options to an alert, one available action for the system is to ask a follow-up question, allowing the sender to collect additional information from recipients. For instance, in an alert asking recipients if they are safe, for those who answer “yes,” the sender could then ask if those recipients are available to help others.

Notes

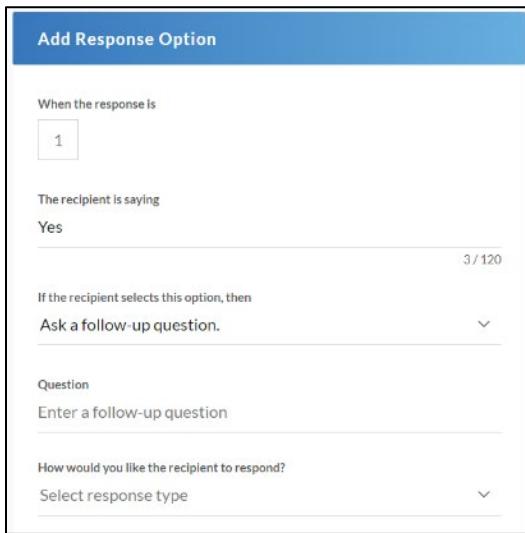
In this release, the OnSolve Platform does not include the content of recipients' follow-up answers on that alert's **Analytics** page. This will be available in a future release.

Follow-up questions are available to recipients only via email, voice, and SMS delivery methods.

For recipients to view follow-up questions when receiving alerts via SMS, your account must have enabled the Always Use SMS Response Links setting. Contact OnSolve Customer Support to have this setting enabled or disabled.

To ask a follow-up question

1. After following steps 1–3 above, select **Ask a follow-up question** from the **If the recipient selects this option, then** drop-down list.



The screenshot shows the 'Add Response Option' dialog box. It includes fields for 'When the response is' (containing '1'), 'The recipient is saying' (containing 'Yes'), 'If the recipient selects this option, then' (containing 'Ask a follow-up question.'), 'Question' (containing 'Enter a follow-up question'), and 'How would you like the recipient to respond?' (containing 'Select response type'). There are also dropdown menus for 'Ask a follow-up question.' and 'Select response type'.

2. Enter the follow-up **Question**. If the response options for your alert have audio components (recorded voice or uploaded audio file), you must also provide audio components for your follow-up questions. See voice recording for [Follow-Up Questions](#).
3. Choose the response type to be made available to recipients:
 - Multiple choice
 - Free-form Response
4. Continue based on the response types below.

Multiple Choice

The Multiple Choice response type allows users to add an unlimited number of response options from which recipients may choose one.

After selecting **Multiple choice** in step 3 above, type in a response option in the **Option** field and select **+**. Repeat to add an unlimited number of response options.

- Reorder response options by dragging and dropping.
- Delete response options by selecting the trash can.
- Add a cascade alert by selecting . See [Send a Cascade Alert](#) for detailed information.

Optionally, add another follow-up question(s). When done, select **Add**.

How would you like the recipient to respond?

Multiple Choice

↳ Option +

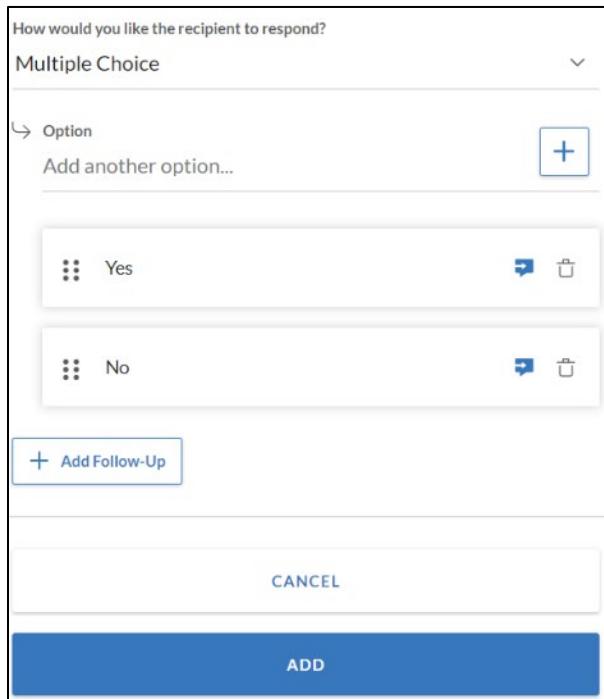
Add another option...

::: Yes	✖
::: No	✖

+ Add Follow-Up

CANCEL

ADD



Free-form Response

The Free-form response type allows recipients to respond by typing whatever they would like.

Note: The Free-form response type is not compatible with voice alerts.

After selecting **Free-form Response** in step 3 above, optionally add another follow-up question(s). When done, select **Add**.

Send a Cascade Alert

The cascade feature automatically launches subsequent alerts based on the response to an initial alert. Each alert included in the cascade has a separate recipient list (contacts, groups, or schedules), message, response options, device priority, and advanced settings. A cascaded alert can be sent based on the response from an initial message or a multiple-choice follow-up question.

Cascade can be used by disaster recovery teams and business continuity planners to make communications with multiple groups of people more efficient and easier to manage. For example, this two-tiered quota alert uses cascading to react to an emergency: A company's Facilities Manager needs to determine whether the building should be evacuated due to an emergency and sends an alert to the Building Manager (Tier 1). If the response from the query is "Yes, start evacuation procedures now," a cascading alert is automatically launched to all employees in that building (Tier 2) with instructions to evacuate.

A broadcast alert that uses cascading could include a questionnaire with branched responses based on an initial set of questions. For example, a broadcast cascade alert can be used at a restaurant with a long line of waiting customers to manage seating shortages. A broadcast alert can be sent to the waiting customers in case of a longer wait time than anticipated and allow them to opt out of their reservation or continue to wait, allowing the restaurant to juggle the seating shortages and keep customers from feeling forgotten while waiting.

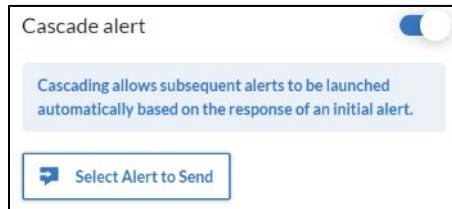
The cascade feature is a powerful communication tool, but an alert can spiral out of control quickly if not properly planned. Map out the entire cascade so there is no mistake as to who gets each alert, who can respond, and what happens when the response is registered. Preplanning can be especially useful if one cascading alert continues to cascade to subsequent alerts.

For instance, this example results in an unexpectedly large number of alerts being sent: A broadcast alert is delivered to 200 recipients. Response 1 includes the cascade option to trigger a subsequent alert to Group B. 150 of the 200 recipients respond with Response 1, and each response triggers the cascading alert to Group B. Recipients in Group B are sent the same cascading alert 150 times.

Note that if the intent is that only one responder is expected to send the cascade of further responses, then the cascade is best served using the Quota alert method. This method ensures that only one individual can respond and launch the cascade. In a Broadcast alert, all recipients can respond simultaneously, with each user possibly launching the cascade, resulting in many undesired duplicate alerts.

To set up a cascade alert

1. Enable a cascaded alert in the **Add Response Option** section by selecting the **Cascade alert** toggle. Once **Cascade alert** is toggled on, the user can select an alert to send.



2. Choose **Select Alert to Send**. The **Select Alert to Cascade** window opens.

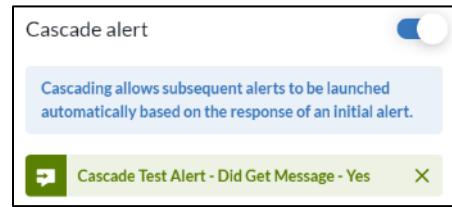
ALERT NAME	LAST MODIFIED	ALERT TYPE	STATUS	RECIPIENTS
Cascade Test Alert - Base Message for Broadcast	Created Jun 23, 2020 at 7:32 AM by Samantha	Broadcast	Saved	
Cascade Test Alert - Did Get Message - Yes	Created Jun 23, 2020 at 7:12 AM by Samantha	Broadcast	Saved	
Cascade Test Alert - Overtime Hours	Created Jun 23, 2020 at 7:02 AM by Samantha	Broadcast	Saved	
Test	Created Mar 12, 2020 at 1:20 PM by Samantha	Broadcast	Saved	
Test Alert	Created Mar 12, 2020 at 1:40 AM by Samantha	Broadcast	Saved	

Display 25 Entries Selected 1 of 12 Results

CANCEL **ADD**

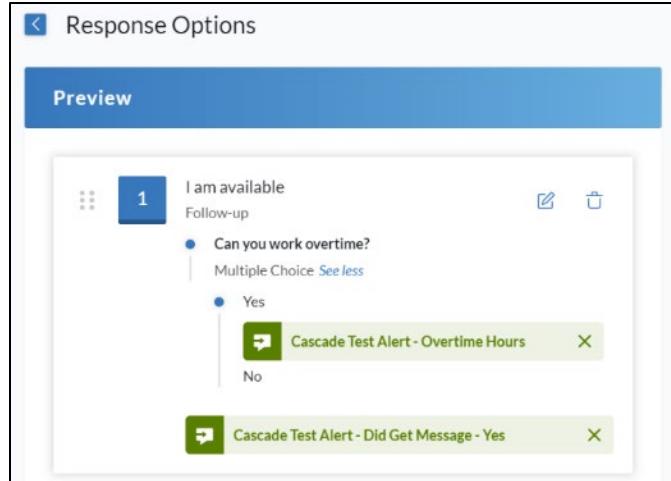
Note: Cascade alerts must be previously created to show in the list. See [Create an Alert](#) for details.

3. Select an existing alert and select **Add**. The selected alert shows in the **Add Response Option** section.



Note: Users can delete the cascade alert and start over by selecting the X to the right of the named alert and selecting another message from the **Select Alert to Cascade** window.

4. When finished adding all settings for a particular response option in **the Add Response Option** section, select **Add** again. All cascade alerts for the response option show in the **Preview** section.



The screenshot shows the 'Response Options' interface with a 'Preview' tab selected. It displays a list of response options under the heading 'I am available'. The first option is 'Can you work overtime?' (Multiple Choice) with the 'Yes' radio button selected. This selection triggers a cascade alert titled 'Cascade Test Alert - Overtime Hours'. The second option is 'No', which triggers a cascade alert titled 'Cascade Test Alert - Did Get Message - Yes'. Both cascade alerts are shown in green boxes with an 'X' icon to close them.

Select Delivery Methods

The Delivery Methods section allows you to determine which device types will be contacted and, if desired, in what order.

1. From the alert overview, select **Delivery Methods**. The **Delivery Methods** page opens with devices set to your account's default. To edit your account's default delivery methods settings, see [Device Priority](#) in Section 8 of this guide.

The screenshot shows the 'Delivery Methods' page. At the top, there are buttons for 'Turn Off All' and 'Reset to Default'. Below this, there are four columns: 'Off', 'Recipient Settings', '1', and '2'. The 'Off' column contains icons for Alertus Outbound, Microsoft Teams, Slack, Twitter, and Fax. The 'Recipient Settings' column contains icons for 2-Way Pager, Mobile Phone, Numeric Pager, TTY Phone, Work Phone, Home Email, Home Phone, and 1-Way Pager. The '1' column contains one item: 'Work Email' at 96%. The '2' column contains one item: 'SMS' at 4%. To the right, there is a large empty box with a dashed border and a plus sign that says '+ ADD ANOTHER PRIORITY LEVEL'. At the bottom right are 'CANCEL' and 'SAVE' buttons.

- Devices in the **Off** column are not contacted.
- Devices in the **Recipient Settings** column are contacted in the order each recipient has set in their people record. When there are devices in this column *and* in a priority column, the system looks to column 1 first, and if a recipient has any other devices listed as priority 1, the system will contact those next. See [Devices](#) in Section 2 of this guide for more information.
- The numbered columns represent priority levels, and the devices in those columns are contacted in that order. Devices in column **1** are contacted first, column **2** second, and so on.
- The percentage listed in each delivery method indicates the percentage of added recipients with that particular device saved in their people record.



- The percentage bar indicates the percentage of added recipients who have at least one selected delivery method and can expect to receive the alert.
 - Select **View Contacts With No Match** to see which selected recipients don't have any of the selected delivery methods, and if desired, [Add Delivery Methods to Contacts On the Fly](#).
2. Drag and drop delivery methods into the appropriate columns. Note that there can be more than one delivery method in each column.
- Add more priority levels by selecting **+ Add Another Priority Level**.
 - Delete columns by selecting the trash can.
 - To turn all devices **Off**, select **Turn Off All**.
 - To reset to your account's default, select **Reset to Default**.
3. Select **Save**. The **Delivery Methods** section on the alert overview displays the number of device types to be contacted.



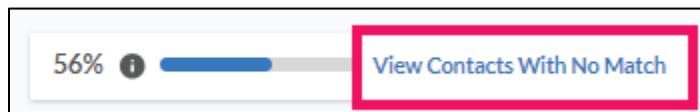
At any point before sending the alert, select the **Delivery Methods** section to edit that section.

Add Delivery Methods to Contacts On the Fly

You can add delivery methods to those recipients who don't have any of the selected delivery methods directly from the **Delivery Methods** page.

To add delivery methods to contacts

1. From the **Delivery Methods** page, select **View Contacts With No Match**.



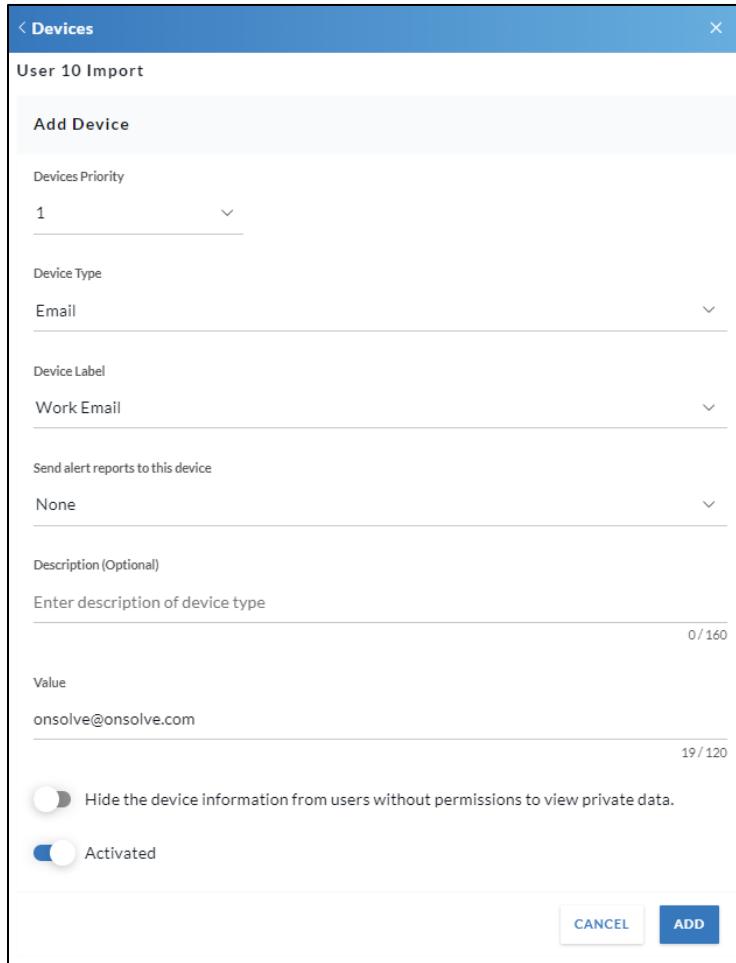
The **Contacts With No Match** window opens.

Contacts With No Match				
Search Recipients...				Export
NAME	UNIQUE ID	DIVISION	ROLE	ACTION
[REDACTED], Sam		ADS EdServices	Administrator	
User 10, Import		ADS EdServices	Contact	
User 100, Import		ADS EdServices	Contact	
User 1000, Import		ADS EdServices	Contact	
User 1001, Import		ADS EdServices	Contact	
User 1002, Import		ADS EdServices	Contact	
User 1003, Import		ADS EdServices	Contact	
User 1004, Import		ADS EdServices	Contact	
User 1005, Import		ADS EdServices	Contact	
(Showing 1 to 25 of 33 loadable records)				
Load Next 25				
CANCEL		DONE		

2. Select the **Action** icon next to a contact. The **Devices** window opens.



3. Select **+ Add Device**. The **Add Device** window opens.



The screenshot shows the 'Add Device' window with the following fields:

- Devices Priority:** Set to 1.
- Device Type:** Set to Email.
- Device Label:** Set to Work Email.
- Description (Optional):** A text input field with placeholder "Enter description of device type" and character count "0/160".
- Value:** An input field containing "onsolve@onsolve.com" with character count "19 / 120".
- Hide the device information from users without permissions to view private data.**: An unchecked checkbox.
- Activated**: A checked checkbox.

At the bottom are two buttons: **CANCEL** and **ADD**.

- a. Select the **Devices Priority**, **Device Type**, and **Device Label**.
- b. Optionally, enter a **Description**.
- c. Depending on the device type, enter additional required information such as **Phone Number** or **Value**.
- d. Select whether the device information should be hidden from users without permission to view private data.
- e. Keep the device **Activated** to ensure this contact receives the alert.
4. Select **Add**.
5. Repeat step 3 to add another device to this contact, or select the back arrow or **X** to return to the **Contacts With No Match** window.
6. Repeat steps 2–5 for any additional contacts.
7. Select **Done**.

Enable Advanced Settings

The **Advanced Settings** section allows you to choose various options to add to the alert. Enable any setting by selecting the toggle. Currently available advanced settings are listed below, and more will be available in future releases. Advanced settings are categorized into **Sender**, **Language**, **Voice**, **Email**, **Response Options**, **Text-Based**, and **Delivery Attempts** sections. When finished configuring these settings, select **Save** at the bottom of the page.

Note: Advanced Settings are displayed according to the settings configured in **Settings > Alert Module**. See [Alert Module](#) in Section 8 of this guide for more information.

Sender

Sender Alias. Designate an alias to use in place of the sender's first and last name. Select the toggle to enable, then enter the desired alias.

Language

Allow Recipients to Select Language. For voice alerts with more than one language saved, allow recipients to choose which language they will hear the alert.

Voice

Play Greetings. The OnSolve Platform plays an introductory message when the phone is answered that identifies the sender and recipient of the alert.

Allow Message Replay. Add a voice prompt to the alert that allows recipients to press a button to replay the message.

Validate Identity by Name. Recipients must validate their identity by confirming their name before the alert will be delivered.

Validate Identity by PIN. Recipients must validate their identity by entering their PIN before the alert will be delivered.

Leave a Voicemail Message. The OnSolve Platform will leave a voicemail on voice devices with voicemail boxes. Use the **Message contains** drop-down list to select if the system should leave the **Message Only**, the **Callback Info Only**, or both the **Message and Callback Info**.

Identical Device Suppression. If two or more recipients share the same phone number and are included in the same alert, the OnSolve Platform will attempt to contact that number only once for all recipients sharing that phone. Reporting will show Identical Device Suppressed.

Stop Contacting If. For voice alerts, set rules for when the system will stop contacting a recipient. The system will stop contacting a recipient when any one of the enabled conditions is met. Options

are **Recipient Listened to Entire Message**, **Recipient Listened to Partial Message**, **Entire Message Left on Voicemail**, **Partial Message Left on Voicemail**.

Expedited Delivery. Enable the OnSolve Platform to allocate additional telephony ports to expedite voice alert delivery.

Email

Digitally Sign Emails. Attach a digital signature to email alerts to confirm to the recipient that the email is coming from a trusted source. An S/MIME key must be uploaded and active to use this setting. See [Manage Division S/MIME Keys](#) in Section 8 of this guide for more information.

Set Email Priority. Set the priority level of alerts sent via email. Options are **Low**, **Normal**, **High**, and **Highest**.

Response Options

Allow Recipients to Change Response. Allow recipients to change their response after their initial response has been submitted.

Require Recipients to Confirm Response. For voice alerts, require recipients to confirm their response by pressing a keypad number on their phone.

Invalid SMS Response. Activate an autoreply when an unrecognized response is received from an SMS device. The autoreply includes instructions to enter a recognizable response.

Text-Based

Only Contact Once. The OnSolve Platform sends the alert to text-based devices only once, ignoring further contact attempt cycles.

Delivery Attempts

Send to Subscribers. Enable the OnSolve Platform to check each recipient's people record for subscribed topics. The alert is delivered to the subscribed recipient if a matching Category, Severity, and Priority are found.

Contact Alternates. The OnSolve Platform will send the alert to a recipient's assigned alternate contacts if the original recipient is unavailable.

Calling Order. For quota alerts, set the default calling order of your recipients to use a vertical or horizontal matrix.

- When set to **Vertical**, the OnSolve Platform attempts to reach the first contact in the first tier via all their selected devices, one device priority at a time, until reached. If the contact is not reached

once all devices have been cycled through, or the contact has been reached but the quota has not been met, the system moves to the next contact in that tier.

- When set to **Horizontal**, the OnSolve Platform will attempt to reach all contacts in that tier, one at a time, starting with their priority 1 devices. If no contacts in that tier are reached on their priority 1 devices, or if any have but the quota has not been met, the system cycles back to the first person in that tier and again alerts contacts one at a time, now via their priority 2 devices.

Note: The order in which the system alerts contacts in a tier is based on when contacts were last sent an alert. The contact who was least recently alerted will be alerted first, and the most recently alerted will be alerted last.

Contact Attempt Cycles. Specify the number of times the alert will cycle through recipient devices in the event of a non-response to the alert. Enter a digit in the text field.

Strict Device Delay. Implement a fixed delay between each device in a recipient's contact cycle (for both text and voice devices). If **Strict Device Delay** is enabled, then the time set for the **Text Device Delay** becomes the delay used between every device.

Text Device Delay. Specify the amount of time the system should wait between consecutive contact attempt cycles for text-based devices in the event of a non-response to the alert. Enter the delay length in hours and minutes.

Contact Cycle Delay. Specify the amount of time (in hours and minutes) the OnSolve Platform should wait between consecutive contact attempt cycles in the event of a non-response to the alert. The delay begins when the first device in a recipient's device list is contacted. Contact Cycle Delay applies when Contact Attempt Cycles is set to 2 or higher.

Reports

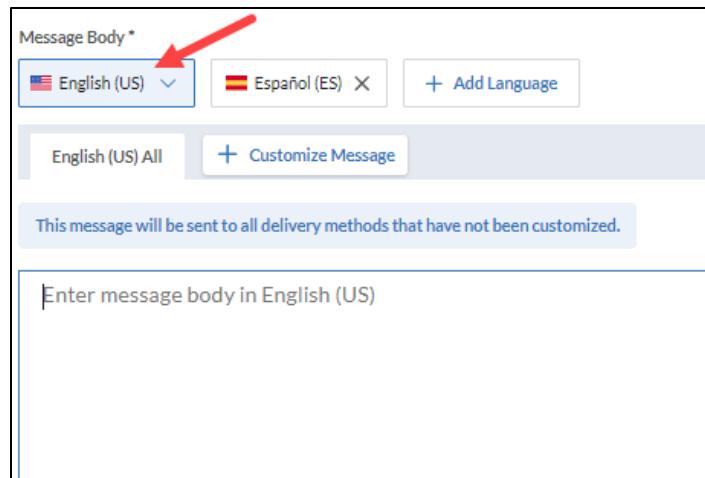
Add Report Recipients. Send alert reports at a specified interval to the recipients you choose.

Additional Options

Alert Languages

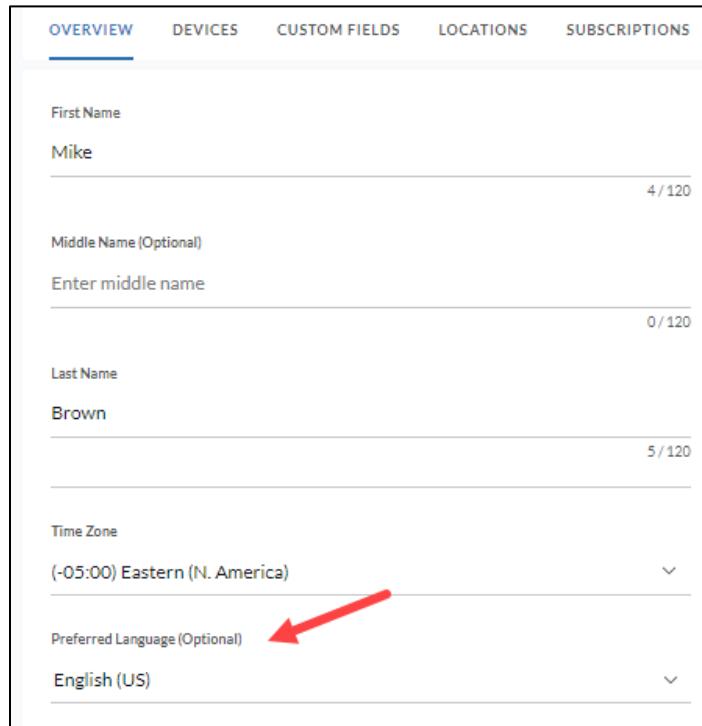
Three language setting options come into play when the OnSolve Platform determines what languages should be used for which recipients.

Account Default Language: Set by OnSolve Customer Support, this language is displayed in the first **Message Body** tab when you create an alert. If no other languages are added to the alert, all contacts receive the alert in this language. If other languages are added, but none are the preferred languages for any contacts, those contacts receive the alert in the Account Default Language.



The screenshot shows the 'Message Body' section of the alert creation interface. At the top, there is a dropdown menu labeled 'English (US)' with a red arrow pointing to it. To its right is a button for 'Español (ES)' with an 'X' icon, and a 'Add Language' button. Below this, there are two tabs: 'English (US) All' and '+ Customize Message'. A note below the tabs states: 'This message will be sent to all delivery methods that have not been customized.' At the bottom, there is a large text input field with the placeholder 'Enter message body in English (US)'.

Preferred Language: Set on each contact's people record, this is the language in which those contacts receive alerts provided that language was also added to the alert, as in the case of Español (ES) in the above example. If a contact's preferred language is not added to the alert, they receive the alert in the Account Default Language or the Alert Default Language if set (see description below).

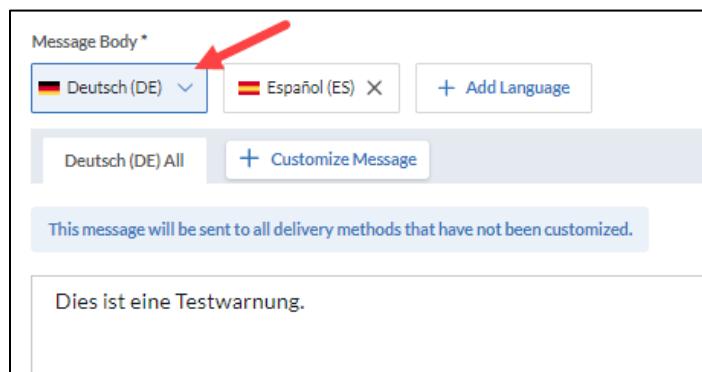


The screenshot shows the 'OVERVIEW' tab selected in the top navigation bar. The form fields include:

- First Name: Mike (4/120 characters)
- Middle Name (Optional): Enter middle name (0/120 characters)
- Last Name: Brown (5/120 characters)
- Time Zone: (-05:00) Eastern (N. America)
- Preferred Language (Optional): English (US)

A red arrow points to the 'Preferred Language (Optional)' dropdown menu.

Alert Default Language: Set for each alert, this language overrides the Account Default Language but not contacts' preferred languages. This setting helps accounts that don't manage the preferred language field in the account's people records but have recipients in areas that don't speak the account's default language. When this feature is enabled, the Account Default Language is in the first language tab, and changing it to anything else makes that new language the Alert Default Language.



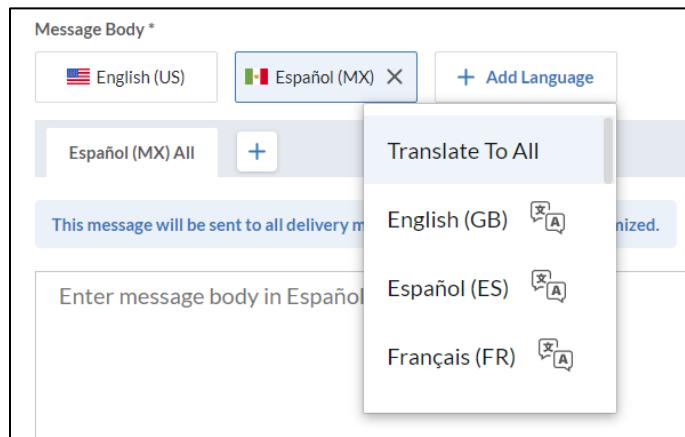
The screenshot shows the 'Message Body *' section of an alert message configuration. It includes:

- Language selection dropdown: Deutsch (DE) (highlighted with a red arrow)
- Other language options: Español (ES) (with a delete icon), + Add Language
- Delivery method: Deutsch (DE) All
- Customization button: + Customize Message
- Note: This message will be sent to all delivery methods that have not been customized.
- Message content: Dies ist eine Testwarnung.

As the Alert Default Language applies to only the current alert, the next time you create an alert, the Account Default Language is back in place.

To choose alert languages

Optionally, compose the message body in additional languages by selecting **+Add language** and choosing the language from the drop-down list, taking the settings described above into account. If enabled, the Automated Language Translation feature translates the content from your default language tab into the additional language tabs. To translate the message into all available languages at once, select **Translate To All**. Remove any language by selecting the **X** next to it.



File-Based Alerting

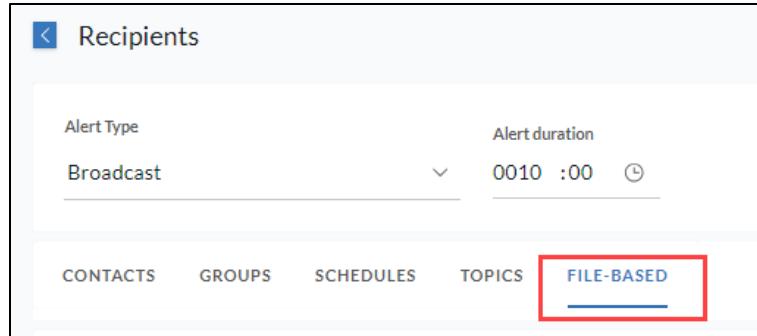
The File-Based Alerting feature allows you to send a broadcast alert using a file of unique IDs. This method of adding recipients can be helpful if you do not want to create a group or manually select each contact individually. Contact customer support to enable this feature for your account.

To send to a file of contacts

1. Create a file of contacts listing only their unique IDs in the first column and with a header in the first row. These contacts must already exist in your account.

Note: File-based alerting supports TXT, CSV, XLS, and XLSX file types. The maximum accepted file size is 10MB or 130,000 rows.

2. In the **Recipients** section of creating an alert, set the **Alert duration** and then choose the **File-Based** tab.

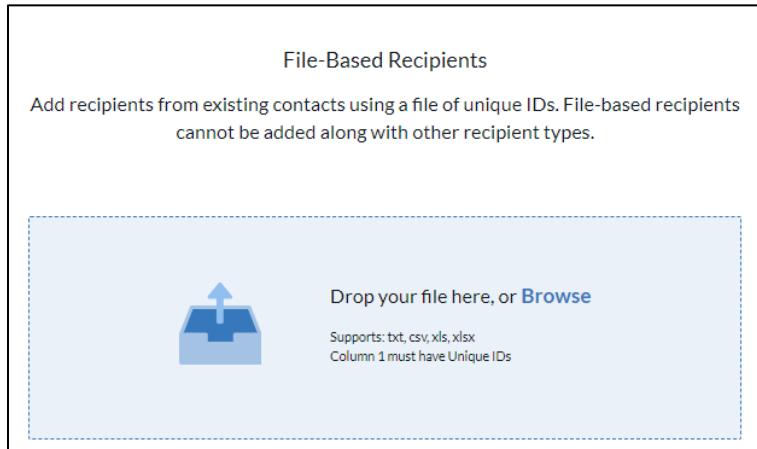


Notes

When using file-based alerting, you cannot also choose recipients from the **Contacts**, **Groups**, **Schedules**, or **Topics** tabs.

Sender Options are not available when using file-based alerting.

3. Drag and drop your file of unique IDs into the center of the page or select **Browse** to find your file on your device.



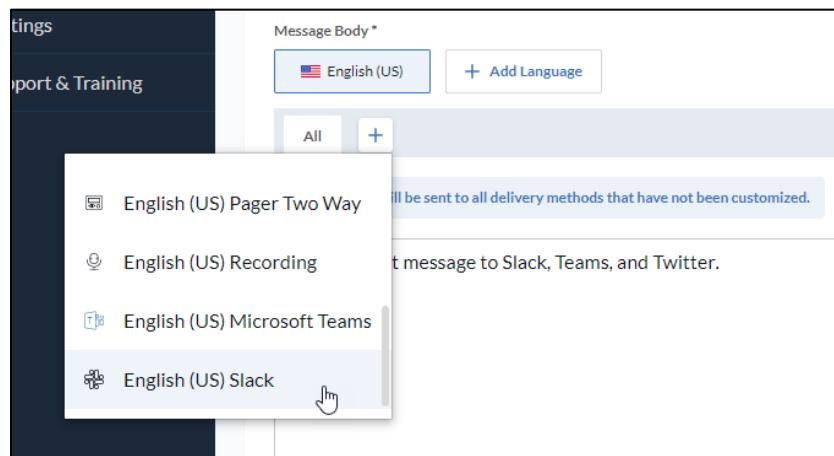
4. Once the file has been uploaded, select **Save**. Continue creating your alert.

Integrations

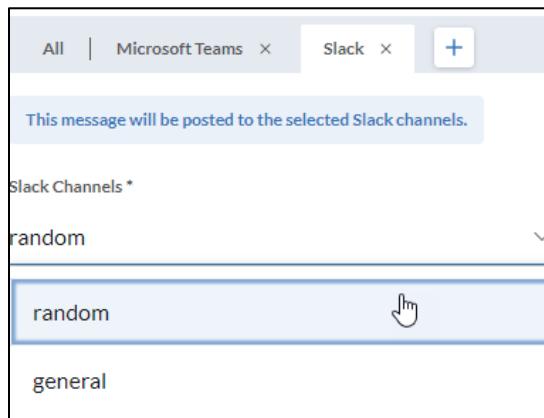
The integrations feature allows you to send alerts to third-party applications. The OnSolve Platform can integrate with Slack, Microsoft Teams, and Twitter. See [Integrations](#) in Section 7 of this guide for instructions on how to set up these accounts. Continue below for instructions on how to send alerts to these applications.

To send an alert to Slack, Teams, or Twitter

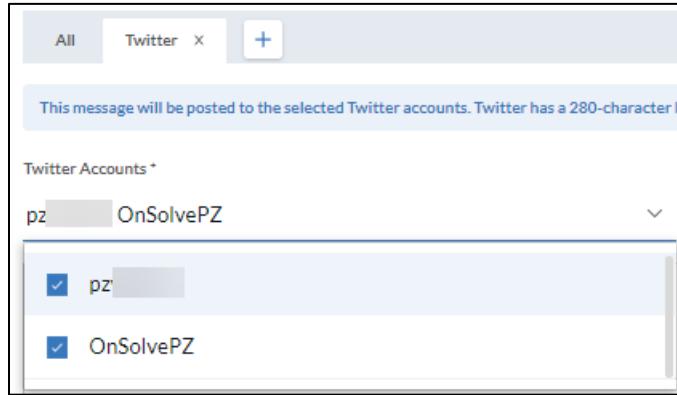
1. When composing the message body, select the **+** next to the **All** tab and choose the desired integrated third-party application. A new tab opens to compose the alert to be sent to that application.



- For Slack and Teams, choose the desired channel from the drop-down list. Only one channel can be selected to receive the alert.



- For Twitter, select as many integrated accounts as you'd like from the **Twitter Accounts** drop-down list.



- Compose the message body for Slack or Teams, as the message body in the **All** tab is not copied over for those third-party applications as they are for other device types. The message body **will** copy over for Twitter.
- Select **Save** and continue with the alert creation process.

Notes

Alert variables are unavailable in the message body of alerts customized for Slack, Teams, and Twitter.

Once you customize an alert for one of these third-party applications, those device types default to device priority 1 in the Delivery Methods section.

To send an alert to one of these integrated third-party accounts only and no other recipients, save the alert first, then send it from the **Saved** alerts tab of the **Alerts** page.

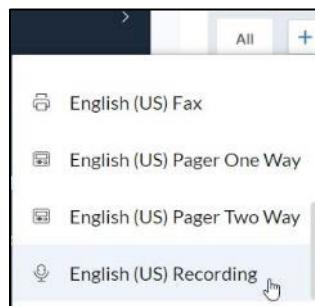
Voice Recording

Voice Recording allows you to either upload a prerecorded audio file or use the OnSolve Platform to record an alert, response options, and follow-up questions in someone's voice instead of using Text-to-Speech (TTS) conversion.

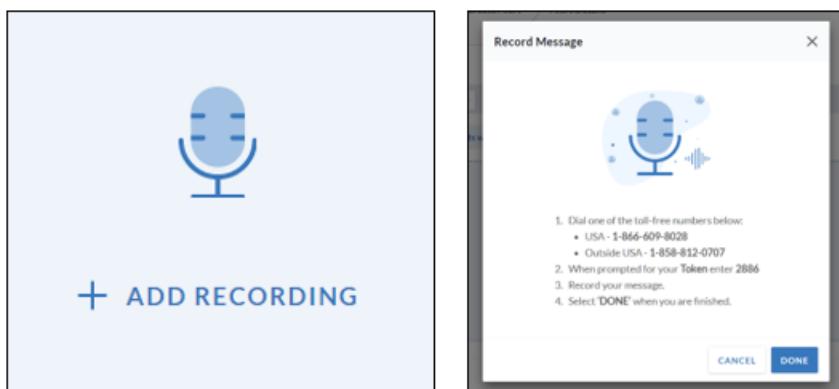
Message Body

To voice record the message body

1. Above the **Message Body** field of the **Alert Details** page, select **+** next to the **All** tab, and choose **Recording**.



2. Select **Add Recording**. An instructional message opens.



Notes

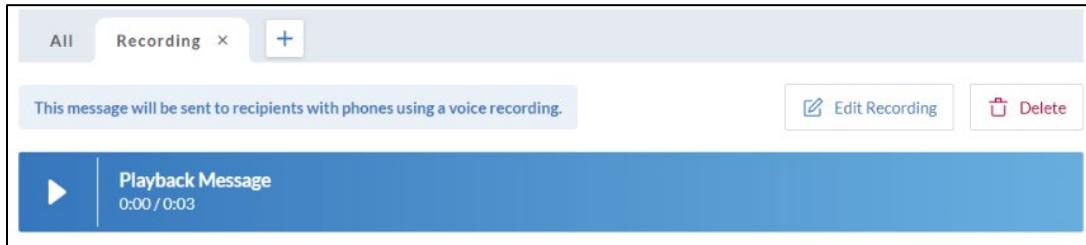
If you are a US customer:

- Within the US, dial +1 866-609-8028.
- Outside the US, dial +1 858-812-0707.

If you are an EU customer:

- Within the EU or locations outside the EU, dial +44 204 520 3004.

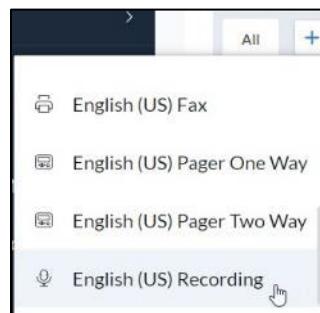
3. Follow the instructions, and when finished, the recording is displayed in the **Message Body** field.



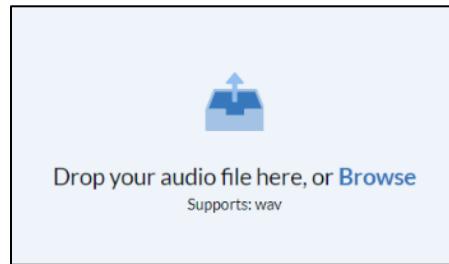
- Review the recording by selecting the arrow next to **Playback Message**.
 - Rerecord the message by selecting **Edit Recording** and repeating step 3 above.
 - Delete the recording by selecting **Delete**.
4. Continue with the Send Alert process.

To upload an audio file for the message body

1. In the **Message Body** field of the **Alert Details** page, select **Recording** from the **Customize Message** options.



2. Drag your audio file directly into the UI, or select **Browse**, navigate to your file and select **Open**.



Note: Only WAV files of size 10MB or less are accepted.

The recording is displayed in the message body field.

A screenshot of a web-based application interface titled "Recording". At the top, there are tabs for "All" and "Recording", with a "+" button to add new items. Below the tabs, a message states: "This message will be sent to recipients with phones using a voice recording." To the right are "Edit Recording" and "Delete" buttons. The main content area is titled "Playback Message" and shows a play icon, the text "Playback Message", and a timestamp "0:00 / 0:02".

- Review the recording by selecting the arrow next to **Playback Message**.
 - Rerecord the message by selecting **Edit Recording** and repeating step 2 above.
 - Delete the recording by selecting **Delete**.
3. Continue with the Send Alert process.

Response Options

If you used a voice recording in the message alert, you must use voice recordings for your response options.

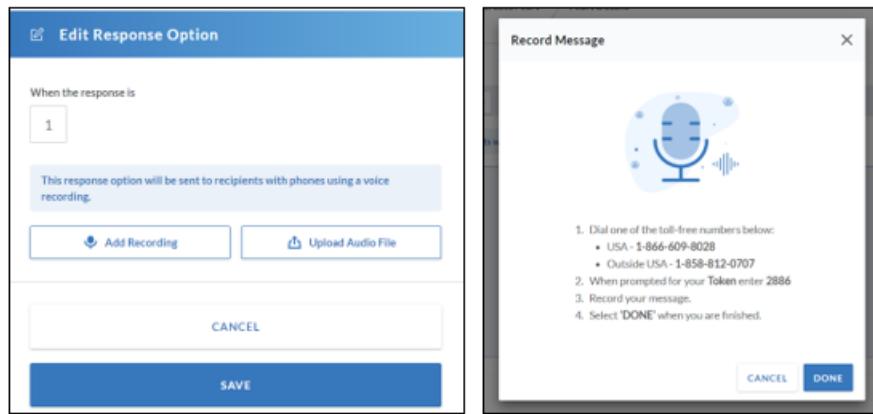
To voice record a response option

1. In the **Add Response Option** section, select the **Recording** tab.

A screenshot of a "Response Options" interface. At the top left is a back arrow and the title "Response Options". Below it is a "Preview" section with a "English (US)" language selection. The main area has tabs for "All" and "Recording", with "Recording" selected. A list shows one item: "1 No recording added". To the right are edit and delete icons.

2. Select the **Edit** icon.

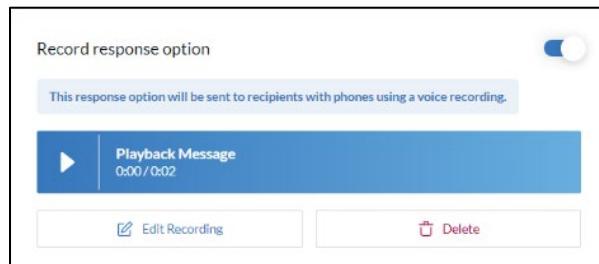
3. Select **Add Recording**. An instructional message opens.



The left screenshot shows the 'Edit Response Option' screen with a blue header. It displays a response option number '1' and a note: 'This response option will be sent to recipients with phones using a voice recording.' Below are two buttons: 'Add Recording' (with a microphone icon) and 'Upload Audio File' (with a file icon). At the bottom are 'CANCEL' and 'SAVE' buttons.

The right screenshot shows the 'Record Message' interface with a blue header. It features a microphone icon with sound waves. Below it is an instructional text: '1. Dial one of the toll-free numbers below:
• USA - 1-866-609-8028
• Outside USA - 1-858-812-0707
2. When prompted for your Token enter 2886
3. Record your message.
4. Select "DONE" when you are finished.' At the bottom are 'CANCEL' and 'DONE' buttons.

4. Follow the instructions to record the response option. When finished, the recording is displayed in the **Add Response Option** section.



Note: When recording a response option, you do not need to indicate the response option number. An automated voice lists this to recipients.

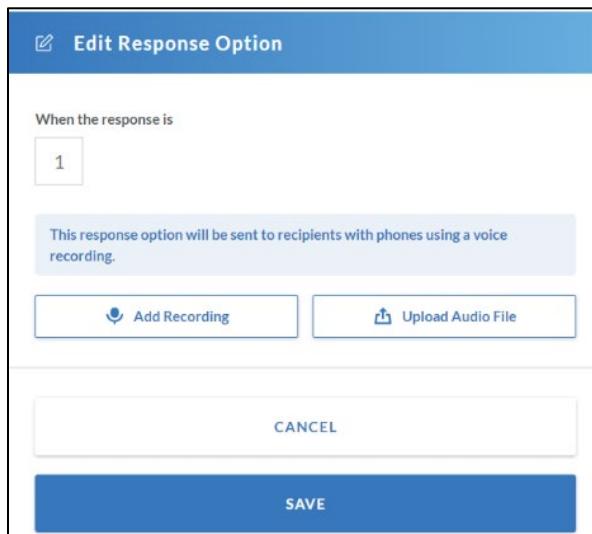
- Review the recording by selecting the arrow next to **Playback Message**.
 - Rerecord the message by selecting **Edit Recording** and repeating step 3 above.
 - Delete the recording by selecting **Delete**.
5. Repeat steps 3–4 for additional response options, and when finished, select **Save**.
6. Continue with the Send Alert process.

To upload an audio file for a response option

1. In the **Add Response Option** section, select the **Recording** tab.



2. Select the **Edit** icon.
3. Select **Upload Audio File**.



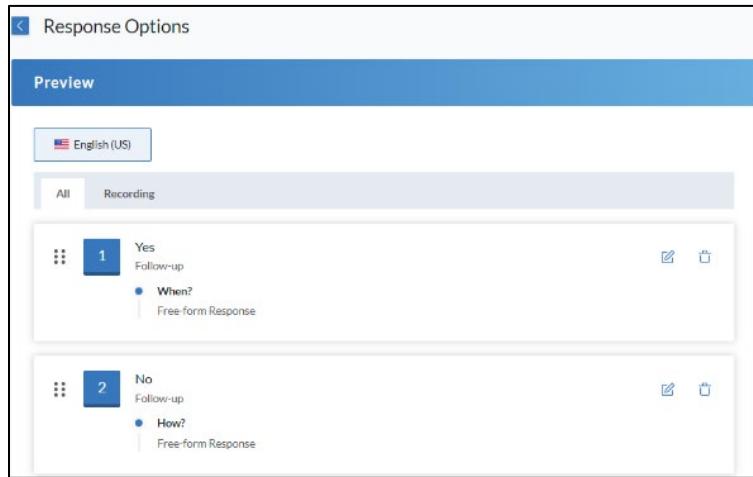
4. Drag your audio file directly into the UI, or select **Browse**, navigate to your file, select **Open**, then **Done**.
 - Review the recording by selecting the arrow next to **Playback Message**.
 - Rerecord the message by selecting **Edit Recording** and repeating step 3 above.
 - Delete the recording by selecting **Delete**.
5. Repeat steps 3–4 for additional response options, and when finished, select **Save**.
6. Continue with the Send Alert process.

Follow-Up Questions

If the response options for your alert have audio components (recorded voice or uploaded audio file), and those response options include follow-up questions, you must also provide audio components for your follow-up questions.

To voice record a follow-up question

1. In the **Preview** section of the **Response Options** page, ensure the response options in the **All** tab have their follow-up questions saved.

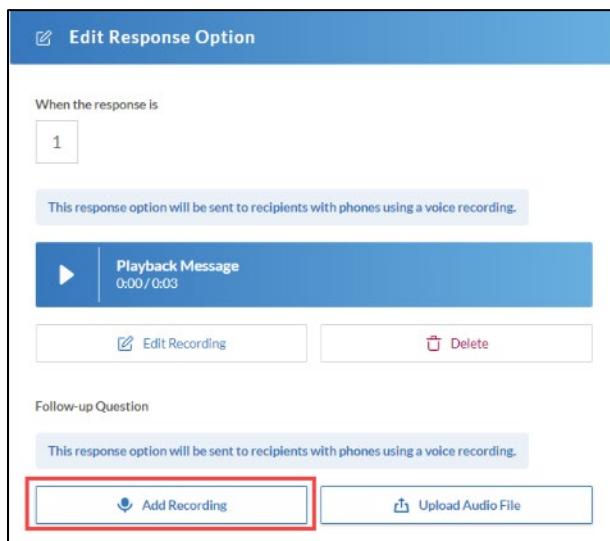


The screenshot shows the 'Response Options' interface in a web browser. At the top, there's a blue header bar with the title 'Response Options'. Below it is a blue 'Preview' bar. Underneath is a language selection dropdown set to 'English (US)'. There are two tabs: 'All' (selected) and 'Recording'. Two response options are listed:

- 1 Yes Follow-up**: A radio button is selected next to 'When?'. Below it is a 'Free-form Response' input field.
- 2 No Follow-up**: A radio button is selected next to 'How?'. Below it is a 'Free-form Response' input field.

Each response option has edit and delete icons to its right.

2. Select the **Recording** tab.
3. Select . The **Edit Response Option** section opens to the right.
4. In the **Follow-up Question** section, select **Add Recording**.



The screenshot shows the 'Edit Response Option' dialog box. At the top, there's a blue header bar with the title 'Edit Response Option'.

When the response is
1

This response option will be sent to recipients with phones using a voice recording.

Playback Message
0:00 / 0:03

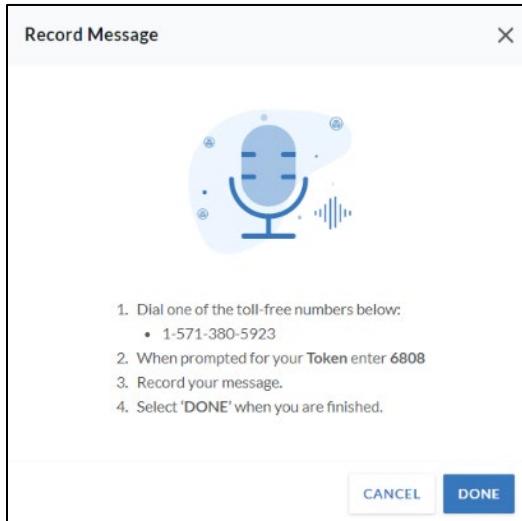
 

Follow-up Question

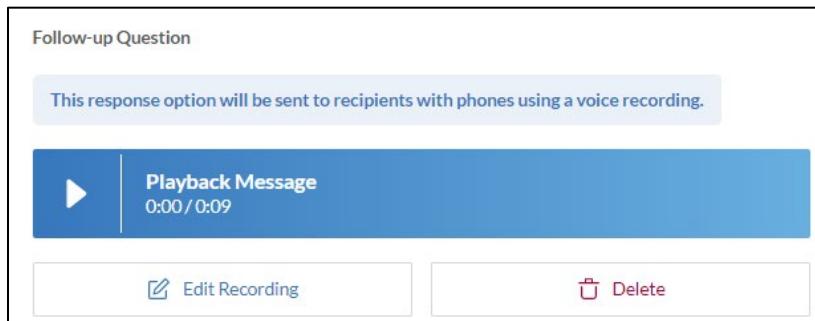
This response option will be sent to recipients with phones using a voice recording.

5. An instructional message opens. Follow the instructions.



When finished, the recording is displayed in the **Follow-up Question** section.

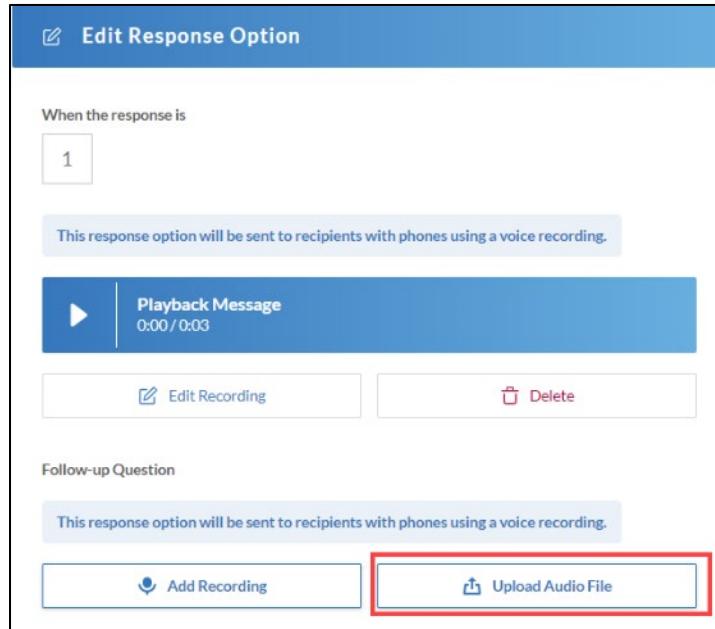


- Review the recording by selecting the arrow next to **Playback Message**.
 - Rerecord the message by selecting **Edit Recording** and repeating step 4 above.
 - Delete the recording by selecting **Delete**.
6. Select **Save**.

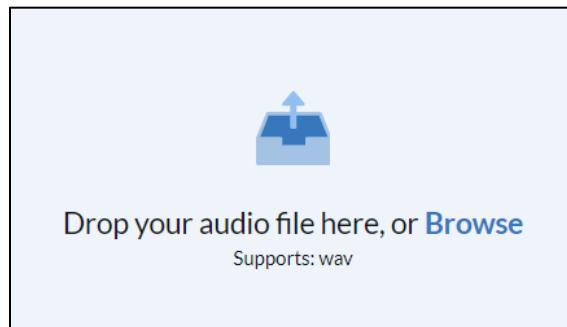
To upload an audio file for a follow-up question

1. In the **Preview** section of the **Response Options** page, select the **Recording** tab.
2. Select . The **Edit Response Option** section opens to the right.

3. In the **Follow-up Question** section, select **Upload Audio File**.

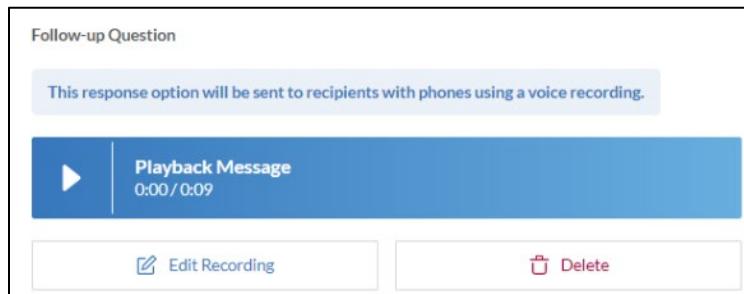


4. Drag your audio file directly into the UI, or select **Browse**, navigate to your file and select **Open**.



Note: Only WAV files of size 10MB or less are accepted.

When finished, the recording is displayed in the **Follow-up Question** section.



- Review the recording by selecting the arrow next to **Playback Message**.
 - Rerecord the message by selecting **Edit Recording** and repeating step 4 above.
 - Delete the recording by selecting **Delete**.
5. Select **Save**.

Alert Variables and Sender Instructions

Use predefined or custom alert variables for text substitution of system-created data. When you include an alert variable in your alert, the system substitutes the variable with the appropriate contact-specific data. Predefined **Contact Variables** are **First Name**, **Last Name**, **Job Title**, and **Unique ID**. Additionally, any custom fields saved in the account are available as **Custom Field Variables**. Alert variables can be placed in the **Alert Name** field and in the **Message Body**.

You can also provide instructions for all potential senders and save them to any alert.

Insert an Alert Variable

To insert an alert variable

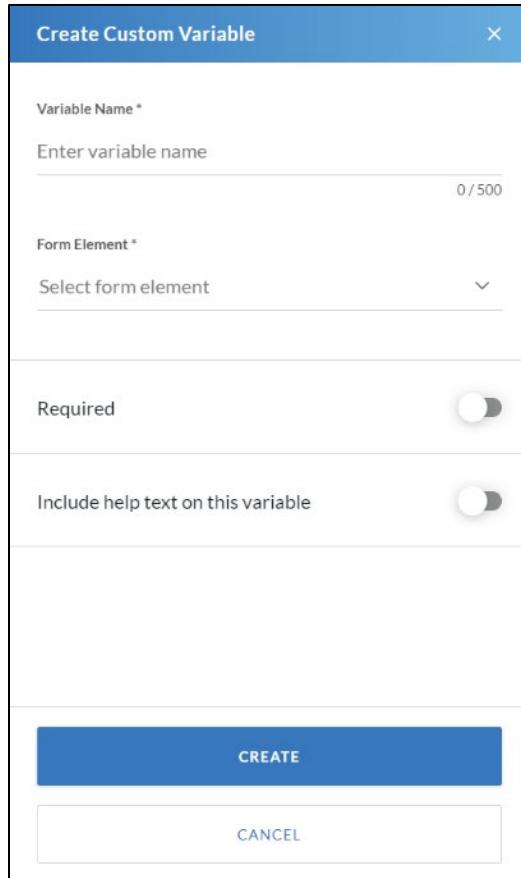
1. Place the cursor in the desired spot in the **Alert Name** or **Message Body** fields.
2. Select **+ Insert Variables**.
3. Select the desired variable. Optionally, use the search field to search by **Variable Name**.

Create a Custom Alert Variable

To create a custom alert variable

1. From the **Alert Details** page, select **+ Insert Variables**.

2. Select **Create Custom Variable**. The **Create Custom Variable** window opens.



The screenshot shows the 'Create Custom Variable' dialog box. It has a blue header bar with the title 'Create Custom Variable' and a close button 'X'. Below the header are two main input fields: 'Variable Name *' with a placeholder 'Enter variable name' and a character count '0 / 500'. Underneath is a dropdown menu labeled 'Form Element *' with the placeholder 'Select form element'. At the bottom of the dialog are two toggle switches: 'Required' (which is off) and 'Include help text on this variable' (which is off). At the very bottom are two buttons: a blue 'CREATE' button and a white 'CANCEL' button.

3. Enter a **Variable Name**. The name cannot contain periods.
4. Select the **Form Element**. Options are:
- **Single-line text:** Allows the user to create an alert variable that is a single line of text.
 - **Multi-line text:** Allows the user to create an alert variable that is multiple lines of text.
 - **Single checkbox:** Not yet available.
 - **Drop-down select:** Allows the user to add options that will appear in a drop-down list for the alert sender.
 - Select the **+** to add each option.
 - Drag and drop to reorder the options.
 - Select the trash can to delete options.

- **Advanced drop-down select:** Similar to the **Drop-down select** option but with the additional **Alternate Display** field, allowing for a second line of text in each option.



Form Element *

Advanced dropdown select

Option	Alternate Display ⓘ
Abany	New York +

5 / 200 8 / 1000

- **Date picker:** Allows the user to add a date field that the alert sender can populate.
 - **Time picker:** Allows the user to add a time field that the alert sender can populate.
5. Use the toggle to choose whether the alert variable should be **Required**.
 6. Use the toggle to choose whether to **Include help text on this variable**. If yes, include any text to aid the alert sender in using the alert variable.
 7. Select **Save**.
 8. Place the cursor in the desired spot in the **Alert Name** or **Message Body** fields and select **+ Insert Variables**.
 9. Select the desired custom variable. Optionally, use the search field to search by **Variable Name**.

Notes

Custom variables remain available for use only in the alert for which they were initially created.

Alerts that contain custom alert variables are automatically saved as templates.

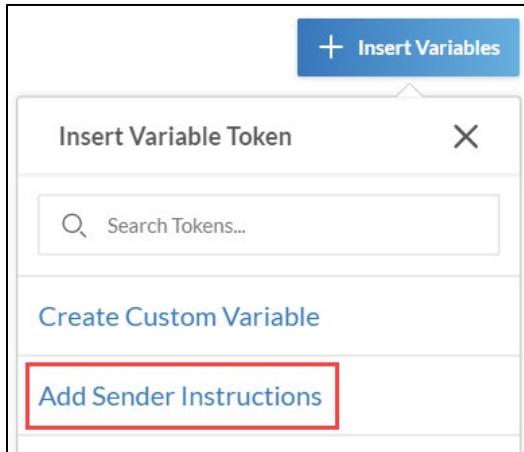
Add Sender Instructions

When creating an alert, you can include instructions for future alert senders.

To add sender instructions

1. From the **Alert Details** section of creating an alert, select **+ Insert Variables**.

2. Select **Add Sender Instructions**.



3. Enter sender instructions and select **Save**.

Note: An alert is saved as a template if it contains sender instructions.

External Conference Bridge

The External Conference Bridge feature allows recipients to seamlessly connect to a conference call when the response option they have chosen is set up to do so.

To connect recipients to an external conference bridge

1. In the **Response Option** section, select **Connect the recipient to an external conference bridge** from the **If the recipient selects this option, then** drop-down list.

If the recipient selects this option, then
Connect the recipient to an external conference bridge.

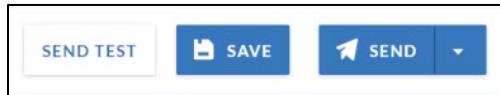
Country Code Phone Number
+1 9294362866x7054098410#

2. Select the **Country Code** and enter the **Phone Number** for the conference bridge. Optionally, enter additional syntax into the **Phone Number** field as desired. See [Appendix D](#) in this guide to learn what characters are accepted and their functions.

Note: You do not need to enter anything other than the phone number in the **Phone Number** field. If you do not, recipients must manually enter any additional required information using their phones.

Send Test, Save Alert, or Send Alert

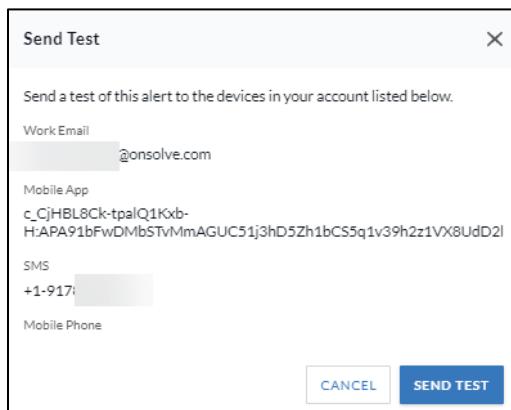
Once all required and desired components of the alert are complete, choose whether to send a test, save, or send the alert.



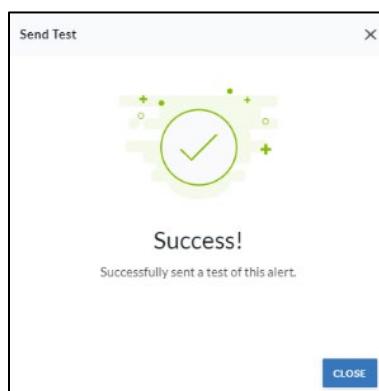
- If choosing to send a test, select **Send Test**.
 - If choosing to save the alert, select **Save**.
- Note:** If your alert contains custom variables or sender instructions, the OnSolve Platform saves the alert as a template. Otherwise, the OnSolve Platform saves it as a regular alert.
- If choosing to send the alert, select **Send**, and then **Send Now** or **Schedule to Send**.

Send Test

If choosing to send a test, a confirmation window opens with a list of the delivery methods the alert will use. The test alert will be sent to the signed-in user.

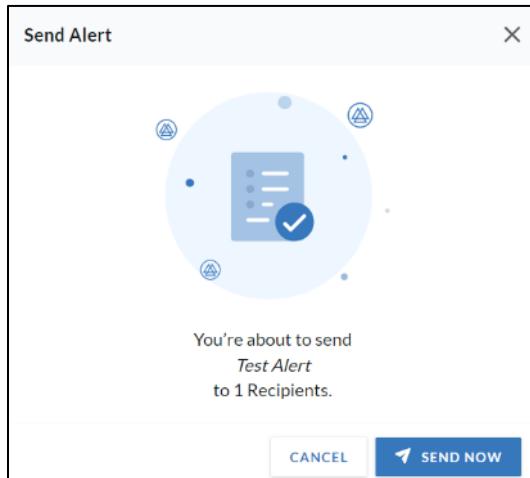


Select **Send Test**. A success message is displayed. Select **Close** to return to the alert.



Send Now

If choosing to send the alert, a confirmation window opens with the number of recipients to be contacted with this alert.



Select **Send Now**. A success message is displayed. Select **Back to Alerts** to return to the **Alerts** page, where that alert appears at the top of the **Sent** tab.

Schedule to Send

If choosing to schedule the alert, the **Schedule to Send** window opens from the right.

Select a date and time to schedule your alert to be sent later.

Start Date*

MM / DD / YYYY

Time*

00 : 00 AM

Time Zone
(-08:00) Pacific (N. America)

Repeats

Every

On the

Of every

Repeating every day(s)

End Date

1. Enter or select the date on which the alert should be sent.
2. Enter the time at which the alert should be sent.

3. If the alert should be sent repeatedly, select **Repeats**.
 - a. Choose the **Every**, **On the**, or **Repeating every** option.
 - For **Every**, select the unit of time in the right drop-down list (**Hour**, **Day**, **Week**, **Weekday**, **Weekend**, **Month**, or **Year**). Then select the interval in the left drop-down list (**First**-- through **Sixth**).
 - For **On the**, select the unit of time in the right drop-down list (**Hour**, **Day**, **Week**, **Weekday**, **Weekend**, or particular day of the week). Then select the interval in the left drop-down list (**First** through **Fourth** or **Last**).
 - For **Repeating every**, enter a number of days (1-28).
 - b. Optionally, toggle on the **End Date** and enter an end date. This end date applies to any option you choose in step 4.
4. Select **Schedule**. The alert is listed in both the **Saved** and **Scheduled** tabs of the **Alerts** page with a **Scheduled** status.

Note: You cannot cancel a scheduled alert. To prevent a scheduled alert from being sent at its scheduled time, delete it from the **Scheduled** alerts tab. It remains saved in the **Saved** alerts tab.

Save

After saving, you are returned to the **Alerts** page, where the saved alert appears in the **Saved** tab. Alerts that contain a custom variable or allow the sender to select additional recipients are saved as templates. Otherwise, they are saved as regular alerts.

	ALERT NAME	LAST MODIFIED	ALERT TYPE	STATUS	RECIPIENTS
<input type="checkbox"/>	test template 12	Edited Jul 19, 2022 at 12:52 PM by [redacted]	Broadcast	Template	
<input type="checkbox"/>	Alert from [redacted]	Edited Jul 12, 2022 at 11:03 AM by [redacted]	Quota	Template	
<input type="checkbox"/>	test additional recipients	Edited Jul 12, 2022 at 7:47 AM by [redacted]	Broadcast	Saved	

Create a Linked Alert

Users can create and send Linked Alerts via the **Critical Communications > Linked Alerts** page. The Linked Alerts feature allows authorized users to group already saved alerts so they can be sent simultaneously. Linked Alerts can fill the need to simultaneously alert different groups of recipients that require slightly different messaging. Contact your OnSolve representative to have the Linked Alert feature enabled for your account.

To create a linked alert

1. Navigate to **Critical Communications > Linked Alerts**. The **Linked Alerts** page opens.

The screenshot shows the 'Linked Alerts' page with a blue header bar containing a search bar, a magnifying glass icon, and a 'Filters' button. Below the header is a table with columns: 'LINKED ALERT NAME', '# OF ALERTS', 'LAST MODIFIED', 'DIVISION', and 'ACTION'. There are two rows of data:

LINKED ALERT NAME	# OF ALERTS	LAST MODIFIED	DIVISION	ACTION
Berge, Wunsch and Wlsozk ds 5414ts	0 Alerts	Created Jan 13, 2022 at 2:06 AM by mccruck	RomaOrg	<button>Send</button>
Breitenberg, Hickle and Lockm an67glhanx22	5 Alerts	Edited Jan 13, 2022 at 2:05 AM by mccruck	RomaOrg	<button>Send</button>

2. Select **+ Create Linked Alert**. The **Create Linked Alert** page opens.

The screenshot shows the 'Create Linked Alert' form with the following fields:

- LINKED ALERT DETAILS**
 - Linked Alert Name ***: A text input field containing "Enter linked alert name, e.g. Fire Drills".
 - Linked Alert Description**: A text input field containing "Enter linked alert description".
 - Division ***: A dropdown menu set to "RomaOrg".

3. Enter the **Linked Alert Name** (required), **Linked Alert Description** (optional), and select the **Division** to which the linked alert should belong (required).

4. Select **Next**. The **Add Alerts** table is displayed.

The screenshot shows a table titled "ADD ALERTS" with columns: ALERT NAME, ALERT TYPE, RECIPIENTS, and LAST MODIFIED. There are six rows of data:

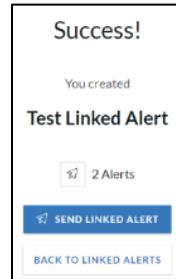
ALERT NAME	ALERT TYPE	RECIPIENTS	LAST MODIFIED
<input type="checkbox"/> Test Alert 1	Broadcast		Created Jan 14, 2022 at 12:37 PM by coloen
<input type="checkbox"/> fffffs	Broadcast		Created Jan 14, 2022 at 8:30 AM by mccruck
<input type="checkbox"/> Without Topics	Broadcast	(3)	Edited Jan 14, 2022 at 7:53 AM by mccruck
<input type="checkbox"/> dsadds	Broadcast		Created Jan 14, 2022 at 7:03 AM by mccruck
<input type="checkbox"/> sfaaaaaaaaaa	Broadcast		Created Jan 14, 2022 at 7:02 AM by mccruck
<input type="checkbox"/> սօֆթվերիք	Broadcast		Created Jan 14, 2022 at 6:58 AM by mccruck

5. Select a maximum of 200 saved alerts to be linked together. To aid in finding the desired saved alerts, you can:
- Use the **Search** field to search by alert name.
 - Filter the table by **Alert Name**, **Alert Type**, **Division**, **Last Modified**, or **Recipient Type**.
 - Sort by the **Linked Alert Name** or **Last Modified** columns.
6. When all desired saved alerts are selected, select **Next**. The table displays the selected alerts. **Edit/Add** alerts, or if done, select **Done**.

The screenshot shows a table titled "ALERTS" with columns: ALERT NAME, ALERT TYPE, RECIPIENTS, and LAST MODIFIED. There are two rows of data, both selected:

ALERT NAME	ALERT TYPE	RECIPIENTS	LAST MODIFIED
<input checked="" type="checkbox"/> fffffs	Broadcast		Created Jan 14, 2022 at 8:30 AM by mccruck
<input checked="" type="checkbox"/> Test Alert 1	Broadcast		Created Jan 14, 2022 at 12:37 PM by coloen

7. Select **Send Linked Alert** to send the linked alert now, or select **Back to Linked Alerts**.



Manage Alerts

The **Alerts** page displays the saved, scheduled, and sent alerts tabs, each with its own table. The columns in the tables differ depending on which type of alert is displayed. The number of alerts of each type is also listed.

The image shows the "Alerts" page interface. At the top, there are three tabs: "Saved" (34), "Scheduled" (1), and "Sent" (104). Below the tabs is a search bar labeled "Search Saved Alerts..." and a set of buttons for "Duplicate", "Delete", and "Filters". The main area contains a table with the following columns: ALERT NAME, LAST MODIFIED, ALERT TYPE, STATUS, RECIPIENTS, and ACTIONS. The table rows represent different alerts:

ALERT NAME	LAST MODIFIED	ALERT TYPE	STATUS	RECIPIENTS	ACTIONS
Alert from [redacted]	Edited Apr 5, 2022 at 3:35 PM by [redacted]	Quota	Template		
Alert Variable test	Created Oct 4, 2021 at 8:33 AM by [redacted]	Broadcast	Template		
First Name	Created Oct 22, 2021 at 1:17 PM by [redacted]	Broadcast	Saved		
follow up recorded response	Edited Jun 24, 2021 at 1:38 PM by [redacted]	Broadcast	Saved		
Resend alert test 2	Created Dec 17, 2021 at 3:48 PM by [redacted]	Broadcast	Saved		
test	Edited May 20, 2021 at 1:57 PM by [redacted]	Broadcast	Saved		

Cancel an Alert

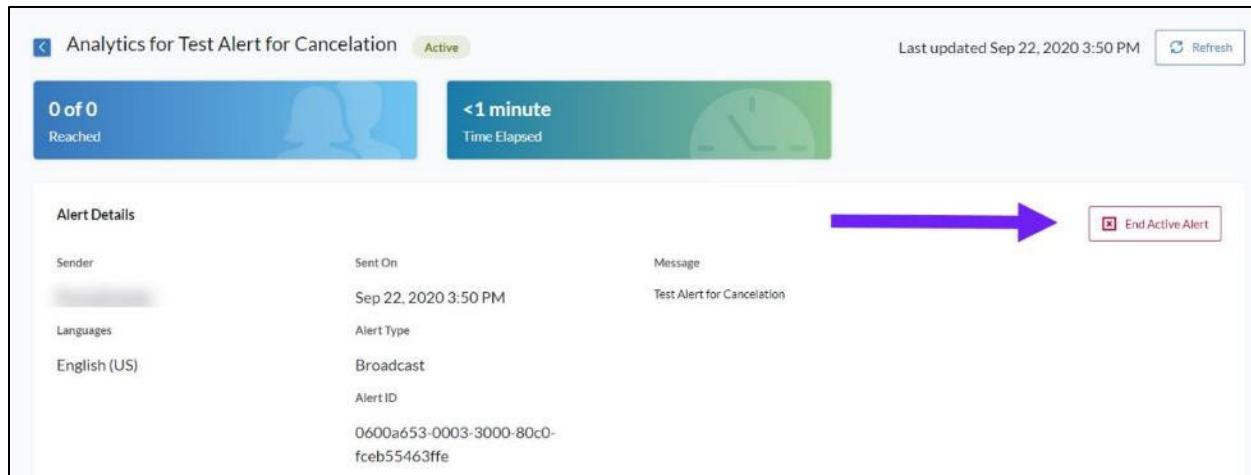
Users can cancel any sent alert that hasn't yet expired. Cancellation will stop any remaining attempts to send the alert.

To cancel an alert

1. From the **Alerts** page, select the **Sent** tab and locate the desired active alert.
2. Select the **Analytics** icon to navigate to that page.

ALERT NAME	LAST MODIFIED	ALERT TYPE	STATUS	RECIPIENTS	ACTIONS
<input type="checkbox"/> Test Alert for Cancellation	Terminated Sep 22, 2020 at 3:51 PM by [REDACTED]	Broadcast	Completed	Processing...	

3. On the **Analytics** page, select **End Active Alert**.

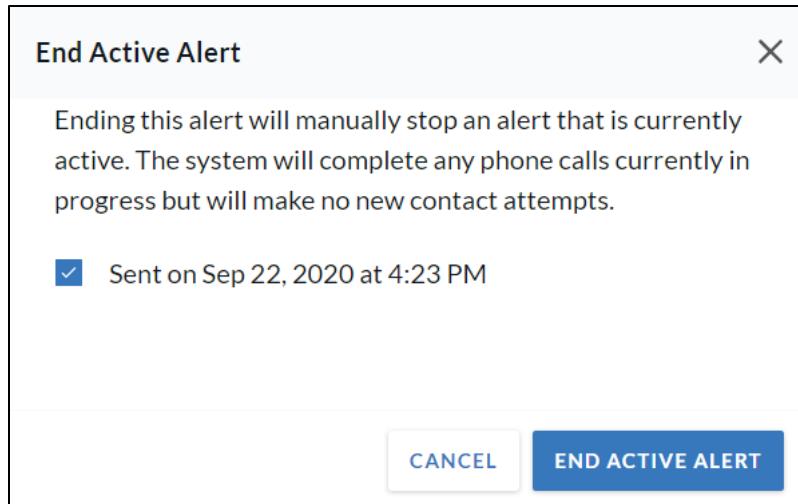


The screenshot shows the Analytics page for a test alert. At the top, it displays the alert name "Test Alert for Cancellation" (status: Active), last updated time, and a refresh button. Below this, there are two summary cards: one showing "0 of 0 Reached" and another showing "<1 minute Time Elapsed". The main section, "Alert Details", lists the following information:

Sender	Sent On	Message
[REDACTED]	Sep 22, 2020 3:50 PM	Test Alert for Cancellation
Languages	Alert Type	
English (US)	Broadcast	
Alert ID		
0600a653-0003-3000-80c0-fceb55463ffe		

A large purple arrow points from the text "On the Analytics page, select End Active Alert." to the "End Active Alert" button located in the bottom right corner of the "Alert Details" section.

4. Confirm cancelation by selecting the date and time the alert was sent and then selecting **End Active Alert**.



Manage Saved Alerts

By default, the **Alerts** page opens to the **Saved** alerts tab.

Note: These saved alerts may also have been sent.

The 'Alerts' page has tabs for 'Saved' (34), 'Scheduled' (1), and 'Sent' (104). A search bar and filter buttons ('Duplicate', 'Delete', 'Filters') are at the top. The main area shows a table of alerts:

	ALERT NAME	LAST MODIFIED	ALERT TYPE	STATUS	RECIPIENTS	ACTIONS
<input type="checkbox"/>	Alert from [redacted]	Edited Apr 5, 2022 at 3:35 PM by [redacted]	Quota	Template		
<input type="checkbox"/>	Alert Variable test	Created Oct 4, 2021 at 8:33 AM by [redacted]	Broadcast	Template		
<input type="checkbox"/>	First Name	Created Oct 22, 2021 at 1:17 PM by [redacted]	Broadcast	Saved		
<input type="checkbox"/>	follow up recorded response	Edited Jun 24, 2021 at 1:38 PM by [redacted]	Broadcast	Saved		
<input type="checkbox"/>	Resend alert test 2	Created Dec 17, 2021 at 3:48 PM by [redacted]	Broadcast	Saved		
<input type="checkbox"/>	test	Edited May 20, 2021 at 1:57 PM by [redacted]	Broadcast	Saved		

Alerts Table Details

Columns displayed for saved alerts are:

- **Favorites:** The designation of an alert as a favorite.
- **Alert Name:** The name of the alert.
- **Last Modified:** The date and time the alert was last modified, along with the username of who modified it.
- **Alert Type:** The type of alert, either **Broadcast**, **Quota**, or **Bulletin Board**.
- **Status:** The status of the alert. For saved alerts, this status is always **Saved**.
- **Recipients:** The source of the recipients. Represented by icons, the sources are “added from contacts,” “added from groups,” and “added from schedules.” If an alert contains recipients from more than one source, more than one icon is displayed.



- **Actions:** Send a saved alert. See [Send from the Alerts Page](#) for more information.

Search

Use the **Search** field to find saved alerts by keyword. This search function queries the **Alert Name** data.

Sort

Saved alerts can be sorted by **Favorite**, **Alert Name**, **Last Modified**, or **Alert Type**. Select any one of those column headers to sort by that column and select it a second time to reverse the sort order.

Filter

Saved alerts can be filtered by:

- Alert Name
- Alert Type
- Division
- Last Modified
- Recipient Type
- Status

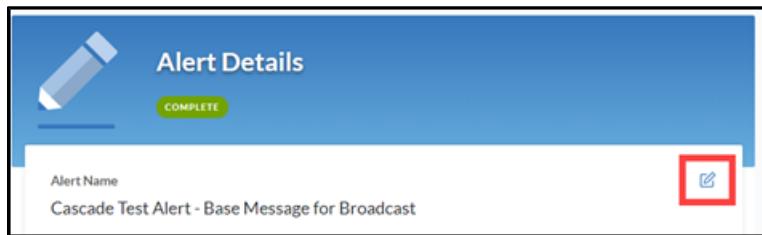
Favorite

Favoriting helps locate frequently used alerts since you can also sort by that designation. Designate an alert as a favorite by selecting the star next to it.



Edit

Saved alerts can be edited by clicking on the desired alert. That alert opens, and any section of the alert can be edited by selecting its edit icon. Save when finished.



Note: In this release of the OnSolve Platform, any schedules saved to an alert are not visible when editing that alert. To ensure that the alert will be sent to schedules, re-add the desired schedules as recipients at the time of editing.

Duplicate

Duplicate an alert—including its recipients, response options, delivery methods, and advanced settings—by selecting the checkbox next to the desired and selecting **Duplicate**. The OnSolve Platform will create a copy of that alert with the same name appended with “Copy.” Click on the new alert to make any necessary edits.

Delete

Delete a saved alert by selecting the checkbox next to it and selecting **Delete**. Look for bulk delete functionality in a future release.

Send

Recently saved alerts can be sent directly from the control center view if that option has been saved as a widget. Also, all saved alerts can be sent right from the **Alerts** page.

Send from the Control Center

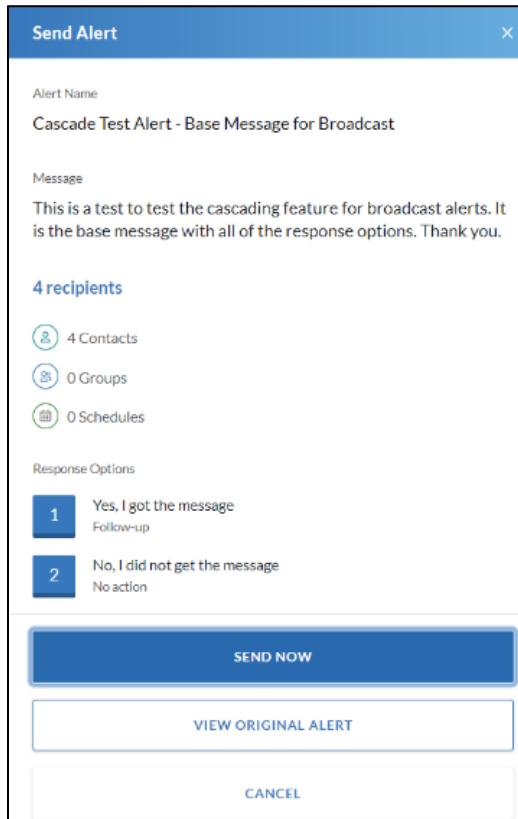
Recently saved alerts, if saved as a widget, are displayed in the control center view.

To send an alert from the Control Center

1. Find the desired alert in the **Alerts** section.
2. Select **Send** from the **Actions** column.



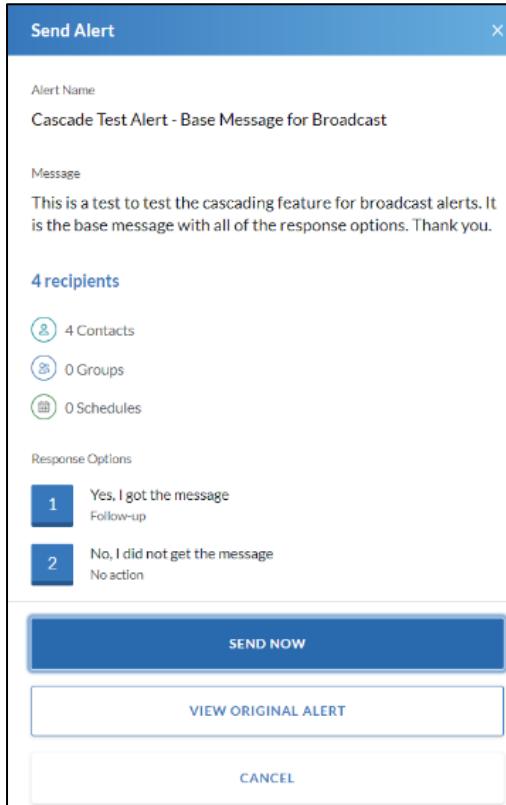
The **Send Alert** preview window opens from the right.



3. If ready to send, select **Send Now**. If the alert should be edited first, select **View Original Alert** to make any changes before sending. Edits made to the alert will be saved to that alert.

Send from the Alerts Page

1. Locate the desired alert from the **Saved** or **Sent** tab of the **Alerts** page.
2. From the **Actions** column, select **Send**. The **Send Alert** window opens and displays the **Alert Name**, **Message**, and information about the **recipients** and **Response Options** if any.



Note: Only original alerts have the resend button available. Any alerts that do not show the resend button in the **Actions** column are resent alerts themselves.

3. If any alert variables are saved to this alert, there is a **Next** button instead of a **Send Now** button. Select **Next** and complete any alert variables. Select **Preview** to see how the alert will appear with the populated alert variables.
4. If ready to send, select **Send Now**. If the alert should be edited first, select **View Original Alert** to make any changes before sending. Edits made to the alert will be saved to that alert.

Send Test

You can send any saved alert as a test. The test will be sent to the logged-in user. See [Send Test](#) for more information.

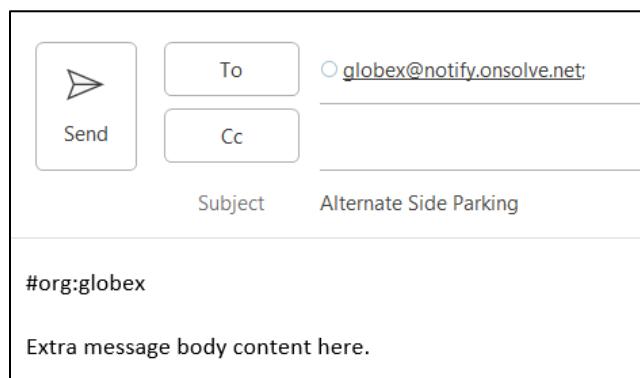
Initiate by Email

If you don't have access to the OnSolve Platform but do have access to your email, you can send a saved alert via email. Your role must have the **Email Initiation** global permission to use this feature.

To initiate an alert by email

1. Using an email account that is saved as a contact point in your account, compose an email to:
 - <username>@notify.onsolve.net if using an account in OnSolve's production environment
 - <Username>@notify.beta.onsolve.net if using an account in OnSolve's sandbox (Beta) environmentwhere <username> is your OnSolve username.

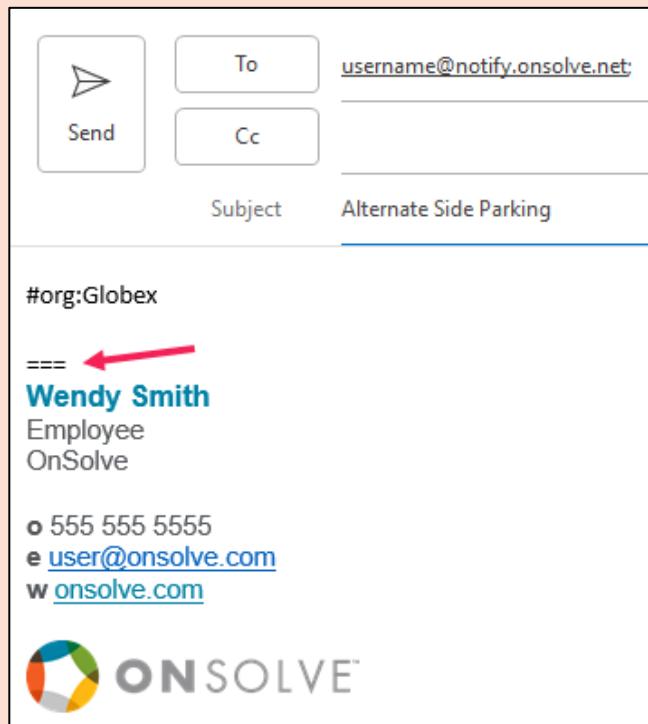
Note: Your username must not be an email address itself.
2. Enter the alert name in the subject line of the email. The subject entered here must be an exact match to the alert name of the saved alert you wish to send.
3. In the body of the email, enter #org:<workspace>, where <workspace> is your account's workspace name. Your workspace name must be all lowercase.
4. If desired, append the message body of the alert by entering content into the body of the email after the workspace name. Anything you enter here will appear at the end of the already-saved message body.



Note

When initiating an alert via email, email signatures are included as message content unless you do one of the following:

- Delete the signature before sending the email.
- Enter at least three dashes, underscores, or equal signs directly above your signature (or re-save your signature with these characters included). Using this method, you receive an email that the content below those characters was left out of the alert.



5. Send the email. The OnSolve Platform sends the alert specified in the subject line to the recipients saved to that alert in your account.

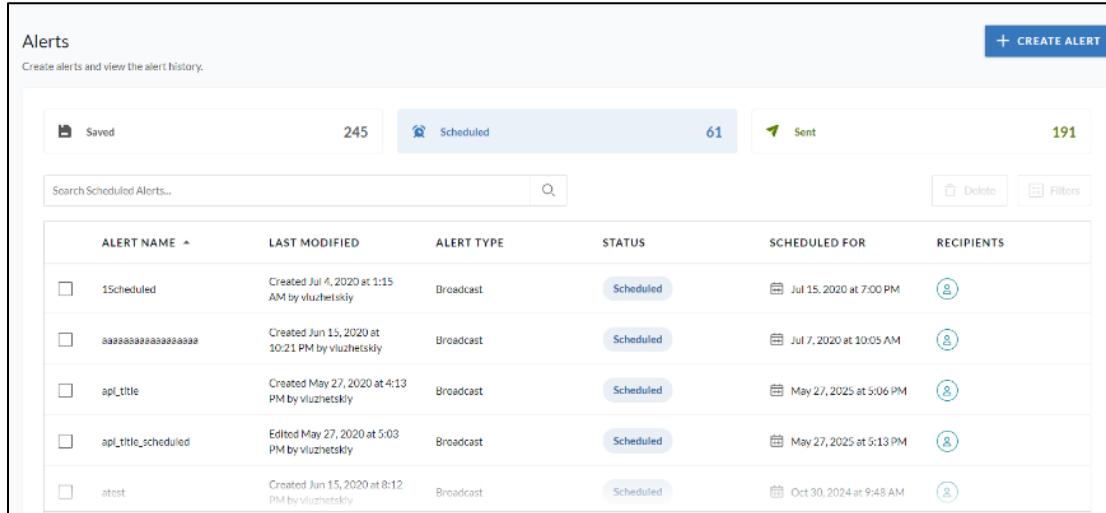
Note: You cannot add more recipients to a saved alert when using the Initiate by Email feature.

Tip

Create and save an alert in your OnSolve account with just the minimum required three characters, such as periods or underscores, in the message body. Then you can initiate an alert by email that has essentially no content but can be used as a starting point. Add the desired content in step 4 above.

Manage Scheduled Alerts

From the **Alerts** page, select the **Scheduled** tab to see all scheduled alerts.



The screenshot shows the 'Alerts' page with the 'Scheduled' tab selected. At the top, there are three tabs: 'Saved' (245), 'Scheduled' (61, highlighted in blue), and 'Sent' (191). Below the tabs is a search bar labeled 'Search Scheduled Alerts...' with a magnifying glass icon. To the right of the search bar are two buttons: 'Delete' and 'Filters'. The main area is a table with the following columns: ALERT NAME, LAST MODIFIED, ALERT TYPE, STATUS, SCHEDULED FOR, and RECIPIENTS. The table contains five rows of data:

ALERT NAME	LAST MODIFIED	ALERT TYPE	STATUS	SCHEDULED FOR	RECIPIENTS
15scheduled	Created Jul 4, 2020 at 1:15 AM by vluzhetskiy	Broadcast	Scheduled	Jul 15, 2020 at 7:00 PM	
aaaaaaaaaaaaaaaaaa	Created Jun 15, 2020 at 10:21 PM by vluzhetskiy	Broadcast	Scheduled	Jul 7, 2020 at 10:05 AM	
api_title	Created May 27, 2020 at 4:13 PM by vluzhetskiy	Broadcast	Scheduled	May 27, 2025 at 5:06 PM	
api_title_scheduled	Edited May 27, 2020 at 5:03 PM by vluzhetskiy	Broadcast	Scheduled	May 27, 2025 at 5:13 PM	
atest	Created Jun 15, 2020 at 8:12 PM by vluzhetskiy	Broadcast	Scheduled	Oct 30, 2024 at 9:48 AM	

Alerts Table Details

Columns displayed for scheduled alerts are:

- Alert Name:** The name of the alert.
- Last Modified:** The date and time the alert was last modified, along with the username of who modified it.
- Alert Type:** The type of alert, either **Broadcast** or **Quota**.
- Status:** The status of the alert. For scheduled alerts, this status is always **Scheduled**.
- Scheduled For:** The date and time the alert is scheduled to be sent.
- Recipients:** The source of the recipients. Represented by icons, the sources are “added from contacts,” “added from groups,” and “added from schedules.” If an alert contains recipients from more than one source, more than one icon will be displayed.



Search

Use the **Search** field to find saved alerts by keyword. This search function queries the **Alert Name** data.

Sort

Select the arrow next to **Alert Name** to sort A–Z or Z–A in that column.

Filter

Scheduled alerts can be filtered by:

- Alert Name (keyword)
- Alert Type (Broadcast, Bulletin Board, Quota)
- Division (choose prepopulated division)
- Last Modified (enter a date range)
- Recipient Type (Contacts, Groups, Schedules, Topics)
- Scheduled for (enter a date range)
- Status (Saved, Template)

Edit

Scheduled alerts can be edited by clicking on the desired alert. That alert opens, and any section of the alert can be edited by selecting its edit icon.

- If editing anything except the date or time the alert is scheduled, select **Save As > Save** when done editing.
- If editing the date or time, select **Send > Update Scheduled Date & Time**, make the changes, and select **Schedule**.

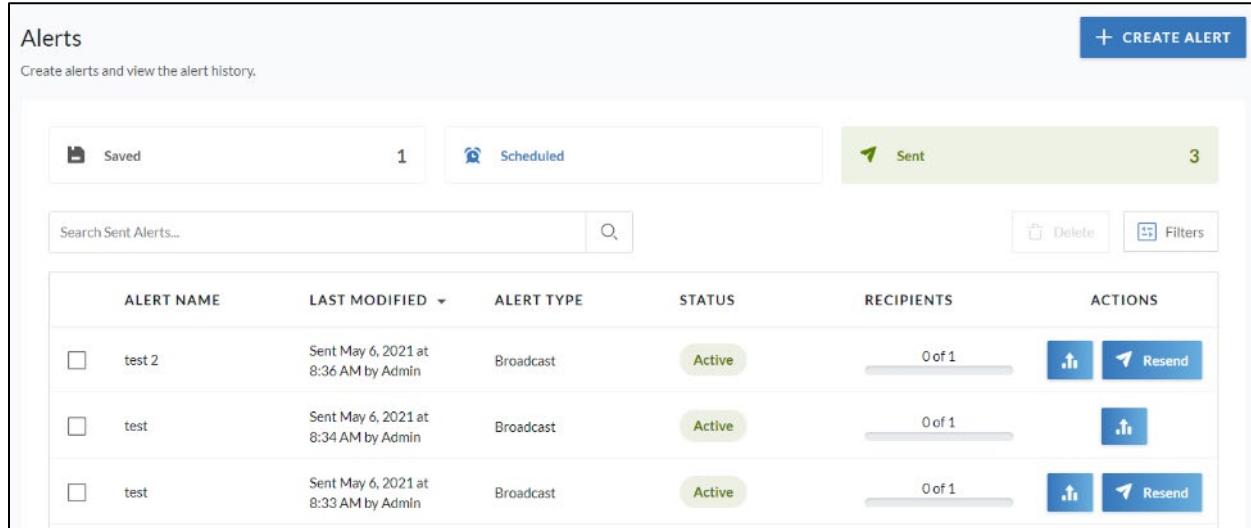
Note: In this release of the OnSolve Platform, any schedules saved to an alert are not visible when editing that alert. To ensure that the alert will be sent to schedules, re-add the desired schedules as recipients at the time of editing.

Delete (Cancel Scheduled Alert)

You cannot edit a scheduled alert once it has been saved. Instead, delete a scheduled alert by selecting the checkbox next to it and selecting **Delete**. This deletes the alert from the **Scheduled** alerts tab but does *not* delete it from the **Saved** alerts tab. Look for bulk delete functionality in a future release.

Manage Sent Alerts

From the **Alerts** page, select the **Sent** tab to see all sent alerts.

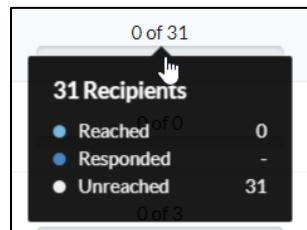


ALERT NAME	LAST MODIFIED	ALERT TYPE	STATUS	RECIPIENTS	ACTIONS
<input type="checkbox"/> test 2	Sent May 6, 2021 at 8:36 AM by Admin	Broadcast	Active	0 of 1	
<input type="checkbox"/> test	Sent May 6, 2021 at 8:34 AM by Admin	Broadcast	Active	0 of 1	
<input type="checkbox"/> test	Sent May 6, 2021 at 8:33 AM by Admin	Broadcast	Active	0 of 1	

Alert Table Details

Columns displayed for sent alerts are:

- Alert Name:** The name of the alert.
- Last Modified:** The date and time the alert was last modified, along with the username of who modified it.
- Alert Type:** The type of alert, either **Broadcast** or **Quota**.
- Status:** The status of the alert. For sent alerts, this status is either **Active** or **Completed**.
- Recipients:** The number of recipients reached out of the total number included in the alert. Hover over the recipients count to see a breakdown of how many were reached, how many responded, and how many were unreached.



- **Actions:**

- Select  to view the **Analytics** page for that alert. See [Analytics](#) in Section 4 of this guide for more information.
- Select  to resend an alert. See [Send from the Alerts Page](#) for more information.

Search

Use the **Search** field to find saved alerts by keyword. This search function queries the **Alert Name** data.

Sort

Saved alerts can be sorted by **Favorite**, **Alert Name**, **Last Modified**, or **Alert Type**. Select any one of those column headers to sort by that column and select it a second time to reverse the sort order.

Filter

Sent alerts can be filtered by:

- Alert Name
- Alert Type
- Division
- Last Modified
- Sender Name
- Status

Delete

Look for delete functionality in a future release.

View Analytics

View a sent alert's analytics by selecting the analytics icon in the **Actions** column.



Resend

Resend an alert by selecting **Resend** in the **Actions** column. See [Send from the Alerts Page](#) for more information.



Manage Linked Alerts

Manage Linked Alerts on the **Critical Communications > Linked Alerts** page.

Alert Table Details

Columns displayed for linked alerts are:

- **Linked Alert Name:** The name of the linked alert.
- **Description:** The description the creator assigned to the linked alert.
- **# Of Alerts:** The number of individual alerts associated with the linked alert.
- **Last Modified:** The date and time the link alert was last modified, along with the username of who modified it.
- **Division:** The division to which the linked alert is saved.

Edit

To edit linked alerts

1. From the **Linked Alerts** page, select the desired linked alert.
 - Edit the **Linked Alert Details** by selecting the **Edit** button. Make the desired changes and select **Save**.
 - Edit the content of the linked alert by selecting **Edit/Add**. Remove/add saved alerts as desired and select **Save**.
2. Select **Save**.

Delete

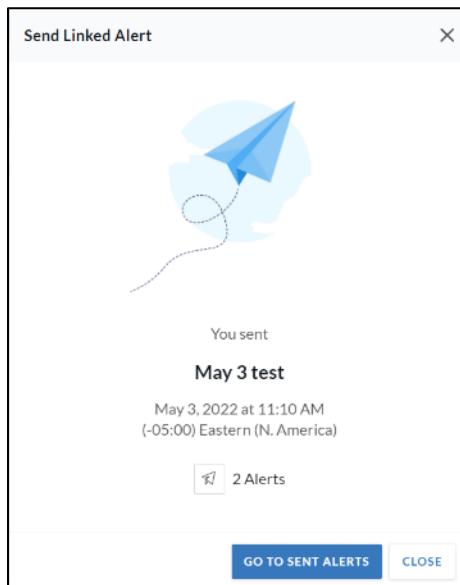
To delete linked alerts

1. Select the checkbox for the desired alerts and select **Delete** at the bottom of the page.
2. Select **Delete** to confirm.

Send

To send a linked alert

1. Select **Send** next to the desired linked alert on the **Linked Alerts** page.
2. Select **Send Now** to confirm.
3. Close the **Send Linked Alert** window to return to the **Linked Alerts** page or select **Go to Sent Alerts** to return to the **Sent** alerts tab on the **Alerts** page.



View Analytics

Sent linked alerts are listed on the **Sent** alerts tab of the **Alerts** page (**Critical Communications > Alerts > Sent**). Each of the alerts that comprise the linked alert is listed separately in the table with its own analytics page.

ALERT NAME	LAST MODIFIED	ALERT TYPE	STATUS	RECIPIENTS	ACTIONS
test SMS	Sent May 19, 2022 at 9:20 AM by portlaz	Broadcast	Active	0 of 1	
May 2 2022	Sent May 19, 2022 at 9:20 AM by portlaz	Broadcast	Active	0 of 1	

Alternate Alert Management Methods

The OnSolve Platform offers other means—other than via the UI—to send and cancel alerts. In this release, users can send and cancel active alerts via phone.

Send by Phone

The Send by Phone feature allows you to dial a toll-free or direct telephone number and navigate through an IVR to send already-saved alerts or cancel active alerts.

Notes

- Message content can be edited via the Send by Phone feature, but only for alerts sent to voice devices. See step 7 below to edit the content of your message.
- Alert templates may be sent by phone, but only if they don't require the sender to enter variable values.

To send an alert by phone

1. Sign in to your OnSolve Platform account and create and [Save](#) the alerts you anticipate sending by phone.
2. If using the OnSolve sandbox environment, dial 571-380-5922 (US/CAN). If using the OnSolve production environment, dial 1-800-330-5889 (US/CAN).
3. Press the number that corresponds to your desired language.
4. Enter your telephony ID and PIN.
5. Press 1 to send an alert (or 2 to cancel an active alert, or 3 to change your location status).
6. Press 1 to browse alert names or 2 to select an alert using the first letters of the alert name.
7. Press 1 to confirm and send, 2 to hear the names of the recipients who will be sent the alert, 3 to hear the message content, or 4 to change the message content. If choosing to change the message content, the IVR directs you to record the new message in your voice. Only recipients receiving the alert by phone can hear this newly recorded message.
8. Press 1 to confirm again.

To cancel an active alert by phone

1. Follow steps 1–4 above.
2. Press 2 to cancel an active alert.
3. Press the number that corresponds with the desired alert.
4. Press 1 to cancel that alert.

Receive an Alert

Whether a person receives an alert depends on if they are included as a recipient. They can be included by being added to the alert as an individual recipient, by being part of a recipient group, or because they subscribe to alert subscriptions such as topics or Weather & Events.

How people receive an alert depends on the sender's delivery methods and what device types are saved in recipients' people records. The available device types are:

- Voice
- TTY Phone
- Email
- Pager One Way
- Pager Two Way
- Pager Numeric
- SMS
- Fax

Reply to an Alert

Alert recipients can reply to an alert when response options are included.

Reply to an Email Alert

There are three ways to respond to an email alert that contains response options:

- Reply to the email with the number that corresponds to your response. Enter that number on the top line within the body of the email.
- Select one of the responses by clicking on the linked response option. A web browser opens with a confirmation message.
- Dial +1 866-609-8026 and use the Telephony ID provided in the email.

Reply to an SMS Alert

Depending on the features available in the sender's account, there are up to three ways to respond to an SMS alert that contains response options:

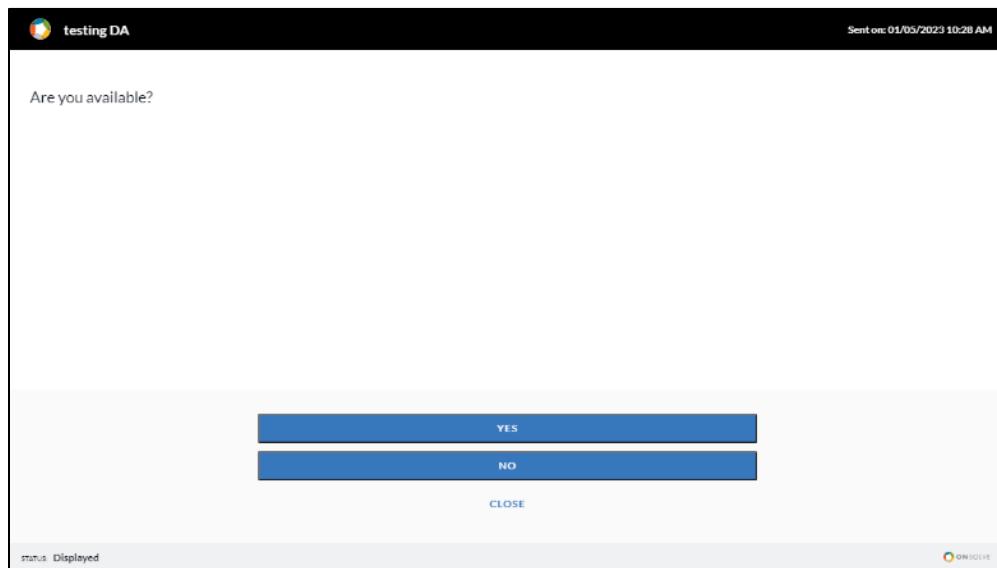
- Reply to the SMS with the number that corresponds to your response.
- If the sender has this feature enabled, select one of the responses by tapping the linked response option. A web browser opens with a confirmation message.
- Dial +1 866-609-8026 and use the Telephony ID provided in the email. Press the number that corresponds to your response.

Reply to a Voice Alert

After identifying yourself and hearing the message, press the number that corresponds to your response.

Reply to a Desktop Alert

Once the Desktop Alert opens on your screen, select your response. The window automatically closes.



Change Response

For some alerts, you may be able to change your initial response to another one if the alert is still active.

SMS and Email

- Reply to the SMS with the number that corresponds to your changed response.
- If you responded via a response link, select **Change Response** in the browser window, then in the same window, select your new response, and then **Save**.
- Dial +1 866-609-8026 again and use the Telephony ID provided in the email. Press the number that corresponds to your new response.

Voice

Dial +1 866-609-8026 from the phone that received the original alert. Press 1 to identify yourself and then the number corresponding to your new response.

Desktop Alerting

You cannot change your response via desktop alerting.

Integrations

Twitter, Slack, and Microsoft Teams alerts do not include response options. Therefore, you cannot change your response via these methods.

Reply to a Follow-Up Question

If the alert sender has added follow-up questions to an alert, you may see or hear additional questions once you choose your response option to the original alert. These additional questions allow you to choose a multiple-choice answer or write a response.

SMS and Email

Once you select a response option in the original SMS or email alert, additional questions are displayed in the web browser. You respond either by selecting a multiple-choice answer or by writing a response.

WEB REPLY

You have received the following message. Please select a response option (if any) and click Save, or click Back if no response is being requested for this message.

Would you prefer 9am-1pm or 1pm-5pm?

9am-1pm
 1pm-5pm

Back **Save**



The screenshot shows a "WEB REPLY" interface. It contains a message instructing the user to select a response option if any and click "Save" or "Back". Below this is a question: "Would you prefer 9am-1pm or 1pm-5pm?". There is a text input field for a response. At the bottom are two buttons: "Back" and "Save", with "Save" being green.

Reply via Voice

Once you select a response option in the original alert, the text-to-speech engine plays the follow-up question. Select the number on your telephone keypad that corresponds to your desired response.

Reply via Desktop Alert

You cannot view follow-up questions on the Desktop Alerting application.

Connect to a Conference Bridge

Alert senders can choose to have recipients connect to a conference bridge depending on their selected response options.

SMS

In an SMS alert, the phone number for the conference bridge is listed directly underneath the associated response option(s). Select the phone number to initiate the phone call. Select again to confirm.

Email

In an email alert, the phone number for the conference bridge is listed directly underneath the associated response option(s). Select the phone number to open a phone application on your device.

Voice

The OnSolve Platform automatically connects you to the conference bridge once you select an applicable response option. No action is necessary on your part.

Desktop Alerting

You cannot connect to a conference bridge via the Desktop Alerting application.

Retrieve an Alert

There are two ways a recipient can retrieve an alert: via the Alert Inbox in the user interface or by calling in to hear any active alert they have been sent, including bulletin board alerts.

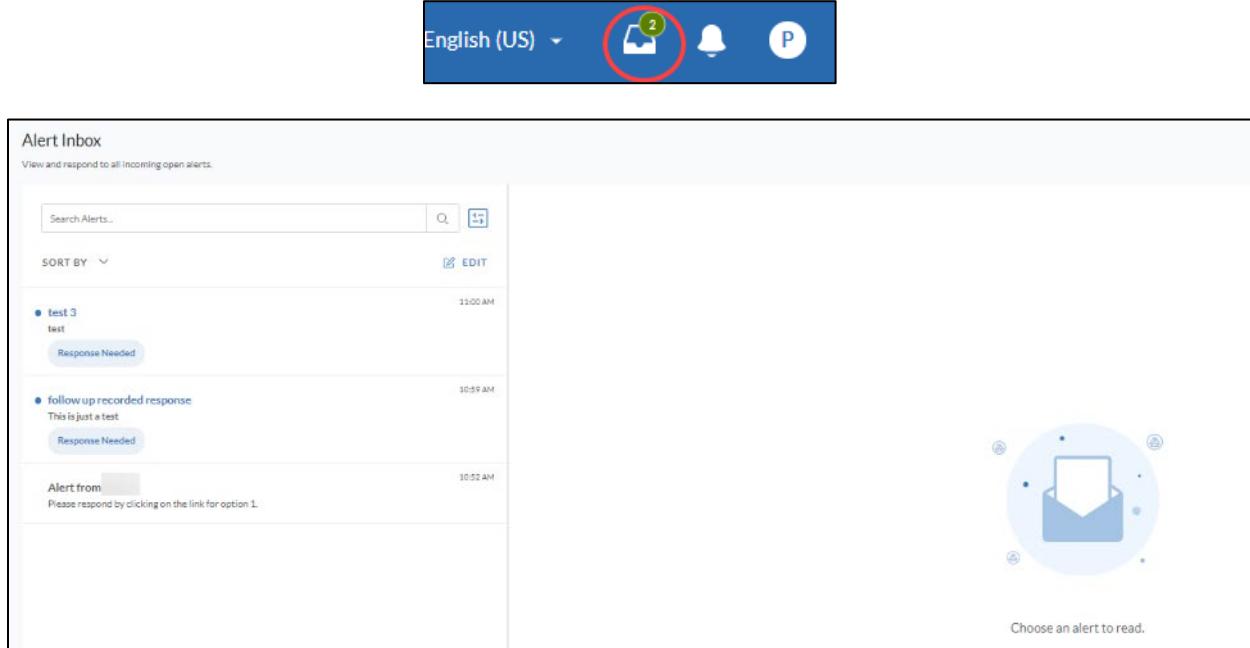
The Alert Inbox

Alert recipients with login access to the OnSolve Platform can view all active alerts via their **Alert Inbox**. Alerts are sent to recipients' Alert Inboxes no matter the delivery methods chosen when creating or saving the alert.

View an Alert

To view an alert in the Alert Inbox

Navigate to **Critical Communications > Inbox**, or select the Inbox icon from your control center view. The **Alert Inbox** is displayed.



Alert Inbox
View and respond to all incoming open alerts.

Search Alerts... EDIT

SORT BY

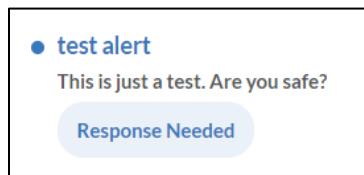
test 3
test
Response Needed

follow up recorded response
This is just a test
Response Needed

Alert from [redacted]
Please respond by clicking on the link for option 1.

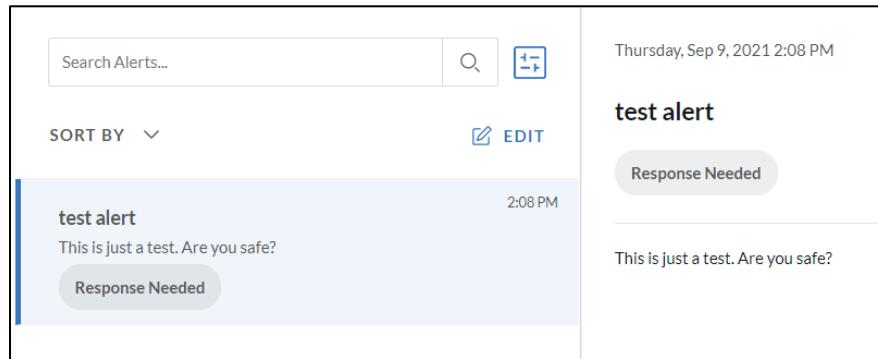
Choose an alert to read.

Unread alerts are in blue, and alerts that require a response are labeled with "Response Needed."



● test alert
This is just a test. Are you safe?
Response Needed

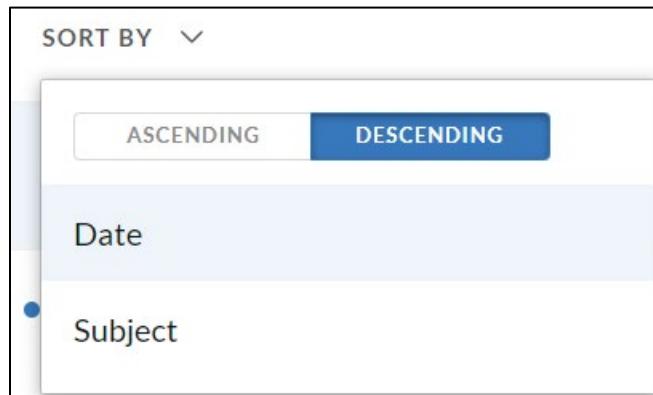
Select any alert to read it in the section to the right.



The screenshot shows a search bar at the top left with placeholder text "Search Alerts..." and a magnifying glass icon. To its right is an "EDIT" button with a pencil icon. Below the search bar is a "SORT BY" dropdown menu set to "test alert". The main list contains one item: "test alert" (Subject) from "2:08 PM". The alert content is "This is just a test. Are you safe?" and includes a "Response Needed" button. To the right of the list, a timestamp "Thursday, Sep 9, 2021 2:08 PM" is displayed above the alert details. The alert details section has a title "test alert" and a status "Response Needed". Below the alert title is the same message: "This is just a test. Are you safe?"

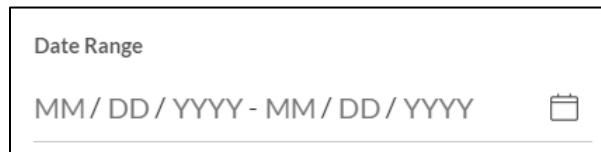
To aid in finding particular alerts, you can:

- Sort by **Date** or **Subject** in either **Ascending** or **Descending** order.



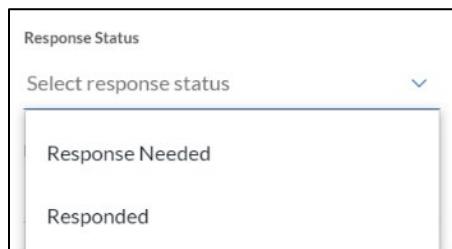
The "SORT BY" dropdown menu is open, showing two buttons: "ASCENDING" and "DESCENDING", with "DESCENDING" being highlighted. Below these buttons are two filter options: "Date" and "Subject". A blue dot indicates that "Subject" is currently selected.

- Filter by any combination of the following:
 - Date Range**



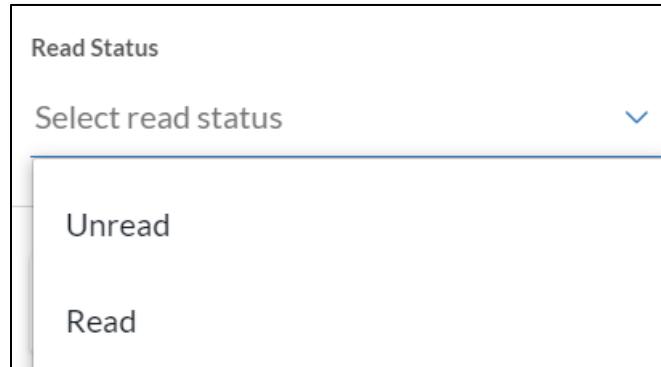
The "Date Range" input field displays the placeholder text "MM / DD / YYYY - MM / DD / YYYY" and includes a calendar icon to the right.

- Response Status**



The "Response Status" dropdown menu is open, showing a "Select response status" placeholder and two items: "Response Needed" and "Responded".

- **Read Status**

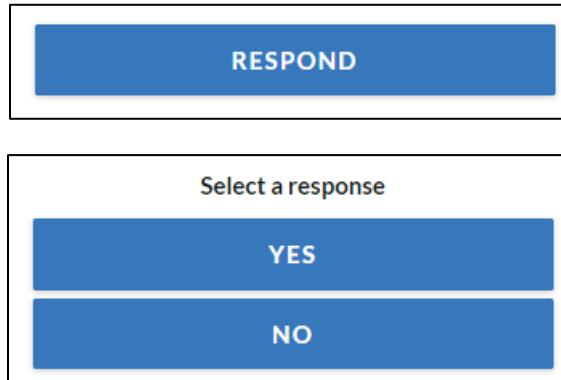


- Search by keyword in the **Search Alerts...** field.

Respond to an Alert

To respond to an alert from the Alert Inbox

1. Select the desired alert.
2. In the section on the right, select **Respond**. The response options will be displayed.

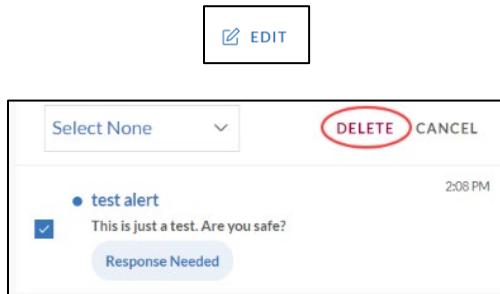


3. Select your desired response. Your response will be recorded. If necessary, change your response by selecting **Change Response**.



Delete an Alert

To delete an alert in the Alert Inbox, select the **Edit** button, select the checkbox next to the desired alert, then select **Delete**.



Calling In

You can also listen to the alerts in your Alert Inbox by calling in.

- For the OnSolve Platform's sandbox (Beta) environment, dial +1 (571) 380-5920.
- For the OnSolve Platform's production environment, dial +1 (866) 609-8026.

If you call in from a phone number saved to your account, the OnSolve Platform recognizes this but may still ask you to confirm who you are before playing your messages. If you are not calling in from a phone number saved to your account, the OnSolve Platform asks you to enter your telephony ID. Ask your account administrator for this information.

Note: Since the call-in numbers are the same for both the Alert Inbox and bulletin board alerts, users for whom there are active alerts of both types can hear them both.

Bulletin Boards

A bulletin board is a passive alert in that the OnSolve Platform does not actively attempt to contact anyone. Instead, you can call in and retrieve a posted message as needed.

- If your organization uses the OnSolve Platform's beta environment, dial +1 (571) 380-5920.
- If your organization uses the OnSolve Platform's production environment, dial +1 (866) 609-8026.

If you call in from a phone number saved to your account, the OnSolve Platform recognizes this but may still ask you to confirm who you are before playing your messages. If you are not calling in from a phone number saved to your account, the OnSolve Platform asks you to enter your telephony ID. Ask your account administrator for this information.

Note: Since the call-in numbers are the same for both the Alert Inbox and bulletin board alerts, users for whom there are active alerts of both types can hear them both.

Section 4: Reports

Overview

The **Reports** menu contains several options for viewing your account data and generating reports. Alert analytics is also covered in this section.

Analytics

The Analytics feature provides a way for authorized users to quickly and easily analyze the results of a sent alert, determine the high-level overview, manually add recipients as being accounted for, and resend alerts to all or portions of the alert recipients as needed.

Once an alert is sent, that alert's analytics can be viewed.

1. From the **Alerts** page, select the **Sent** tab.
2. Locate the desired alert and select the **View Analytics** icon from the **ACTIONS** column.

ALERT NAME	LAST MODIFIED	ALERT TYPE	STATUS	RECIPIENTS	ACTIONS
<input type="checkbox"/> Resend will soon be available by [redacted]	Sent Nov 3, 2020 at 1:27 PM	Broadcast	Completed	16 of 30	 

The **Analytics** page for that alert opens.

Analytics Details

The **Analytics** page offers snapshot tiles and details on the selected alert that parallel the completed sections when that alert is created: **Alert Details**, **Response Rate**, **Delivery Methods**, and **Recipients**.

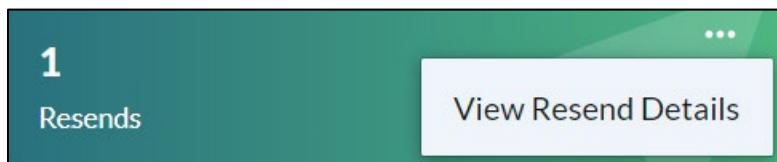
The screenshot shows the 'Analytics for test' page with a 'Completed' status. At the top, there are three summary tiles: '3 of 3 Reached' (blue), '82 minutes Time Elapsed' (teal), and '1 Resends' (green). Below these are three main sections: 'Alert Details', 'Response Rate', and 'Delivery Methods'. The 'Alert Details' section lists the sender ('portlaz'), message ('test'), language ('English (US)'), broadcast type ('Broadcast'), and alert ID ('3b9bb415-0003-3000-804e-ed867c69e121'). The 'Response Rate' section includes a donut chart showing 100% responded and a table of response counts: yes (1), no (1), Other Response (1), and No Response (0). The 'Delivery Methods' section shows a bar chart for Voice (2/2), Email (2/2), SMS (2/2), and Mobile Application (0/2).

Response	Count
yes	1
no	1
Other Response	1
No Response	0

The top of the page displays three tiles: the number of contacts **Reached**, the **Time Elapsed** since the alert was sent, and the number of **Resends**.

- If the original alert is still in progress, the elapsed time represents the elapsed time since the alert was sent.
- If the original alert is completed, the elapsed time represents the total time it was active.

Select the **Resends** ellipsis and then **View Resend Details**.



The **Resend Details** window opens, listing the original alert and any resends.

Resend Details

ALERT ID	SENDER	SENT ON ▾	COMPLETED	STATUS
3b9fc20e-0003-3000-804e-ed867c69e121	[REDACTED]	Dec 2, 2021 7:58 AM	Dec 2, 2021 8:58 AM	Completed
3b9fc20d-0003-3000-804e-ed867c69e121	[REDACTED]	Dec 2, 2021 7:57 AM	Dec 2, 2021 8:57 AM	Completed

CLOSE

Select **Refresh** to update that and any other information on the **Analytics** page.

Alert Details

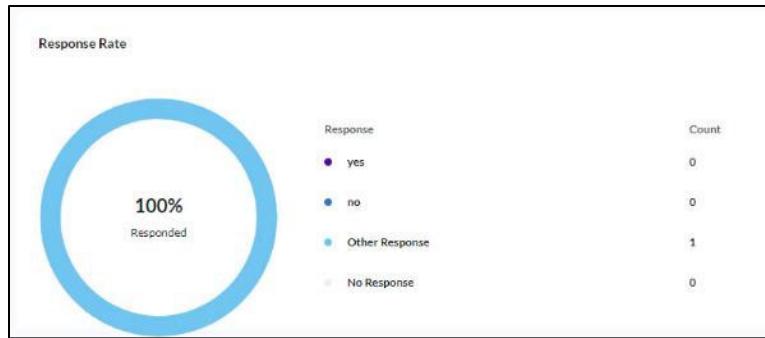
The **Alert Details** section lists:

- The **Sender**.
- The **Languages** selected when the alert was composed.
- The date and time the alert was **Sent On**.
- The **Alert Type**.
- The **Alert ID**.
- The **Message** content.

Alert Details		
Sender	Sent On	Message
[REDACTED]	Jul 8, 2020 2:42 AM	This is a test for the purpose of explaining Analytics. Are you safe?
Languages	Alert Type	
English (US)	Broadcast	
	Alert ID	
	00000255-0004-3000-8085-	
	372faf18054c	

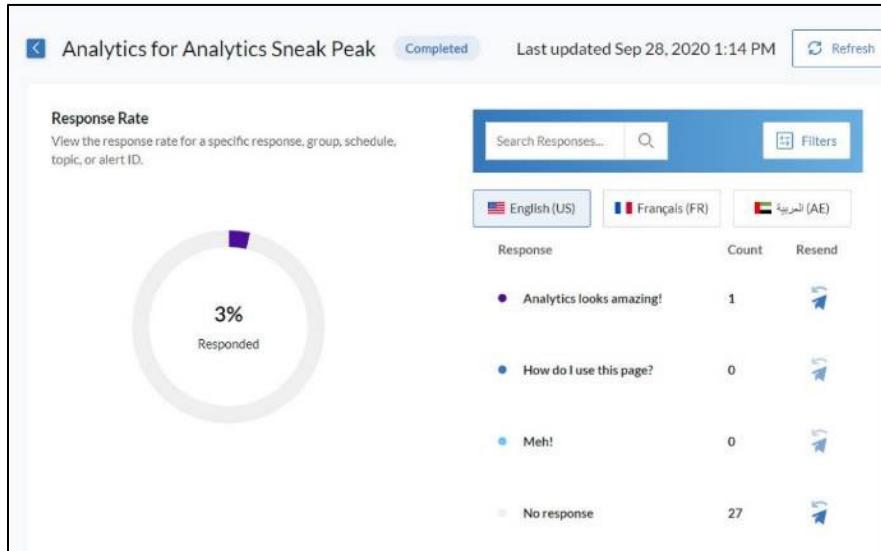
Response Rate

The **Response Rate** section lists all the available response options included in the alert, any “Other Responses,” the percentage of recipients who have responded, and the number of responses recorded for each response option. This is aggregate data, including all responses from resent alerts.



Response Rate Details

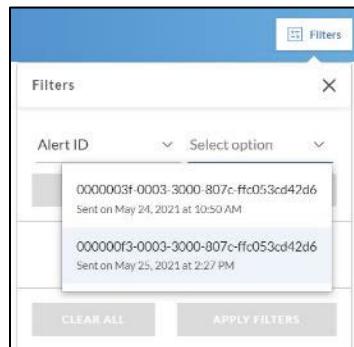
Select **View Details** to see more details on the response rate.



Here, you can:

- Search for a particular response in the **Search Responses...** field.
- Toggle between responses in all languages that were selected for this alert.
- Resend the alert to recipients who replied with a particular response option or didn't respond.
- Refresh the page to include recently received responses.

- Filter responses by **Alert ID**. This allows you to see the responses from the original alert versus any resends.



Select the back button to return to the full **Analytics** page.



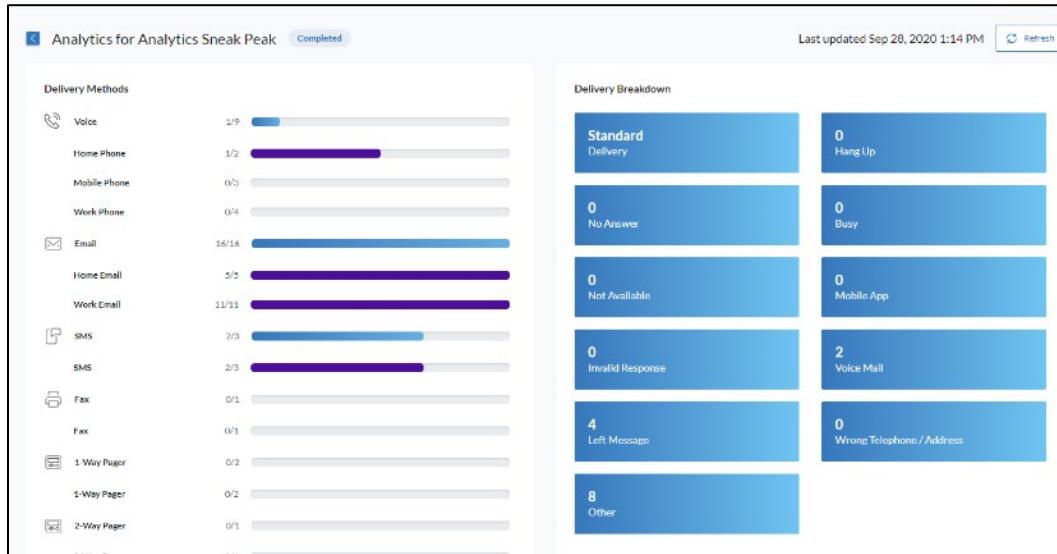
Delivery Methods

The **Delivery Methods** section displays all the delivery methods chosen for this alert and how many of each type were delivered.



Delivery Method Details

Select **View Details** to see more details on delivery methods.



Here, you can:

- View how many alerts were successfully delivered for each delivery method.
- In the **Delivery Breakdown** section, see the statuses for each alert sent via the voice delivery method.
- Refresh the page to include recently received responses.

Recipients Table

The Recipients table is towards the bottom of the **Analytics** page and tracks all the contacts that were sent the initial alert and any resends. With this table, you can easily track the status of each recipient and resend to filtered groups. You can also resend the alert to specific recipients selected from the table. See [Custom Resend](#) for more on resending from the Recipients table.



The Recipients table lists four contacts with their last name, first name, status, devices, response, other response, timestamp, resends, and unique ID.

	LAST NAME	FIRST NAME	STATUS	DEVICES	RESPONSE	OTHER RESPONSE	TIME STAMP	RESEND	UNIQUE ID
<input type="checkbox"/>	Blake	Dan	Reached				Jun 23, 2021 12:16 PM	1x	DBlack
<input type="checkbox"/>	Doe	John	Reached				Jun 23, 2021 12:17 PM	2x	JDoe2
<input type="checkbox"/>	Doe	Jane	Not Contacted						JDoe
<input type="checkbox"/>			Reached				Jun 23, 2021 12:16 PM	1x	

Search

Use the **Search** field to find recipients by keyword. This search field queries the **Last Name** and **First Name** data.

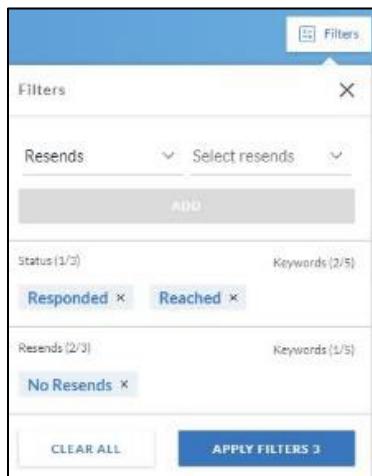
Sort

Select the arrow next to **Last Name** to sort A–Z or Z–A in that column.

Filter

The Recipients table can be filtered by **Alert ID**, **Resends**, **First Name**, **Last Name**, **Response**, **Status**, or **Time stamp**.

1. Select **Filters**.



2. Select the desired filters.

- **Alert ID**. Filter by the Alert IDs available in the drop-down list.
- **Resends**. Filter by the number of times recipients were resent the alert.
- **First Name** and **Last Name**. Enter a name as a keyword.
- **Response**. Filter by **No response** or specific responses.
- **Status**. Filter by **Responded**, **Reached**, **Not contacted**, or **Unreached**.
- **Time stamp**. Filter by the dates on which recipients were sent the alert.
- **Custom field**. Select a custom field and enter a value as a keyword.

3. Select **Apply**.

Status

The **Status** column reflects whether each recipient was **Unreached**, **Reached**, **Not Contacted**, or has **Responded**.

- **Unreached**. OnSolve attempted to reach the contact, but due to a variety of possible reasons, the alert was not delivered to the recipient. Examples of possible reasons include a contact's voicemail box not being set up, a contact's voicemail box being full, or an error preventing the alert from being delivered.
- **Reached**. The recipient received the alert but has not responded in the case of alerts with response options.
- **Not Contacted**. OnSolve did not attempt to reach the contact because the contact has none of the selected delivery methods.
- **Responded**. The contact responded to the alert with either one of the available response options or an [Other Response](#).

Resends

You can get further details about each recipient and attempts to contact them by clicking anywhere in a particular row.

	LAST NAME	FIRST NAME	STATUS	DEVICES	RESPONSE	OTHER RESPONSE	TIME STAMP	RESENGS	UNIQUE ID
	Blake	Dan	Reached				Jun 23, 2021 12:16 PM	1x	Dbake

The **Contact Attempts** window opens and displays, for each contact attempt, the **Alert ID**, **Status**, **Delivery Method**, **Details**, **Time Stamp**, and **Response**.

Contact Attempts						
has been contacted 2 times.						
ALERT ID	STATUS	DELIVERY METHOD	DETAILS	TIME STAMP	RESPONSE	
> 3d909175-0003-3000-80c0-fceb55463ffe	Responded	Work Email	Response	Mar 14, 2023 1:21 PM	No	
> 3d90918b-0003-3000-80c0-fceb55463ffe	Responded	Work Email	Response	Mar 14, 2023 1:19 PM	Yes	
> 3d90918b-0003-3000-80c0-fceb55463ffe	Reached	Home Email	Email Sent	Mar 14, 2023 1:18 PM		
> 3d909175-0003-3000-80c0-fceb55463ffe	Reached	Home Email	Email Sent	Mar 14, 2023 1:18 PM		

Edit Recipient Response

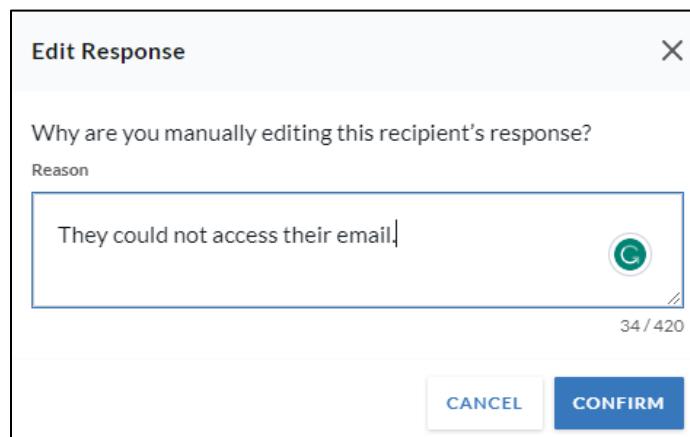
Users with the Edit Recipient Response divisional permission can change any recipient's response from within the table. This feature is helpful if, for instance, a recipient is unable to respond directly to an alert but can call and verbally provide a response.

To edit a recipient's response

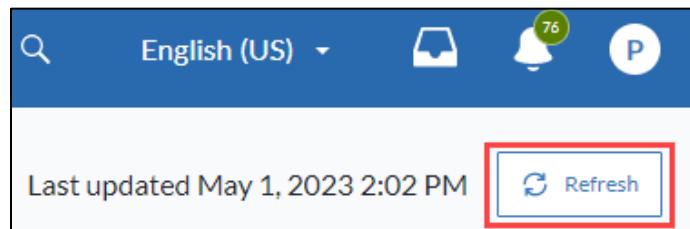
1. In the recipient's table, select the arrow next to the response you want to change.

	LAST NAME ▾	FIRST NAME	STATUS	DEVICES	RESPONSE
<input type="checkbox"/>	[REDACTED]	[REDACTED]	Responded	[REDACTED]@gmail.com	blue
<input type="checkbox"/>	[REDACTED]	[REDACTED]	Responded	[REDACTED]@gmail.com	<div style="border: 1px solid #ccc; padding: 5px;"><p>red</p><p>blue</p><p>yellow</p></div>

2. Select a new response. The **Edit Response** window opens.



3. Enter a **Reason** for why you edited the response and select **Confirm**.
4. Select the **Refresh** icon at the top right of the page to view the updated responses.



When you select that recipient from the table and the **Contact Attempts** window opens, you see that the **Delivery Method** is listed as **Admin Edit**, and the **Details** column contains the text you entered in step 3.

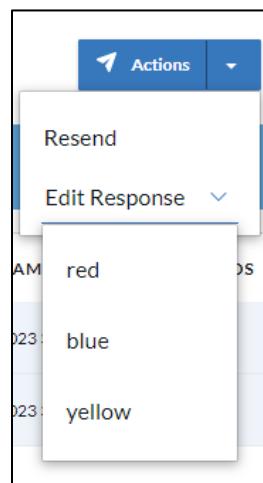
Contact Attempts					
has been contacted 1 time.					
ALERT ID	STATUS	DELIVERY METHOD	DETAILS	TIME STAMP	RESPONSE
> 3db10eb7-0003-3000-80c0-fceb55463ffe	Responded	Admin Edit	They could not access their email.	Apr 28, 2023 3:32 PM	yellow
> 3db10eb7-0003-3000-80c0-fceb55463ffe	Responded	Home Email	Response	Apr 28, 2023 3:19 PM	

To edit responses in bulk

1. In the recipient's table, check the boxes next to the recipients whose responses you want to change or select the "Select All" checkbox.

RECIPIENTS					
Search Recipients... <input style="float: right;" type="button" value="Search"/>					
	LAST NAME	FIRST NAME	STATUS	DEVICES	RESPONSE
<input checked="" type="checkbox"/>			Responded	Admin Edit	yellow
<input checked="" type="checkbox"/>			Responded	@gmail.com	red

2. Select the arrow next to **Actions** and then select the arrow next to **Edit Response**.



3. Select a new response. All selected recipients' responses update to this new response. The **Edit Response** window opens.
4. Enter a **Reason** for why you edited the responses and select **Confirm**.
5. Select the refresh icon at the top right of the page to view the updated responses.

Notes

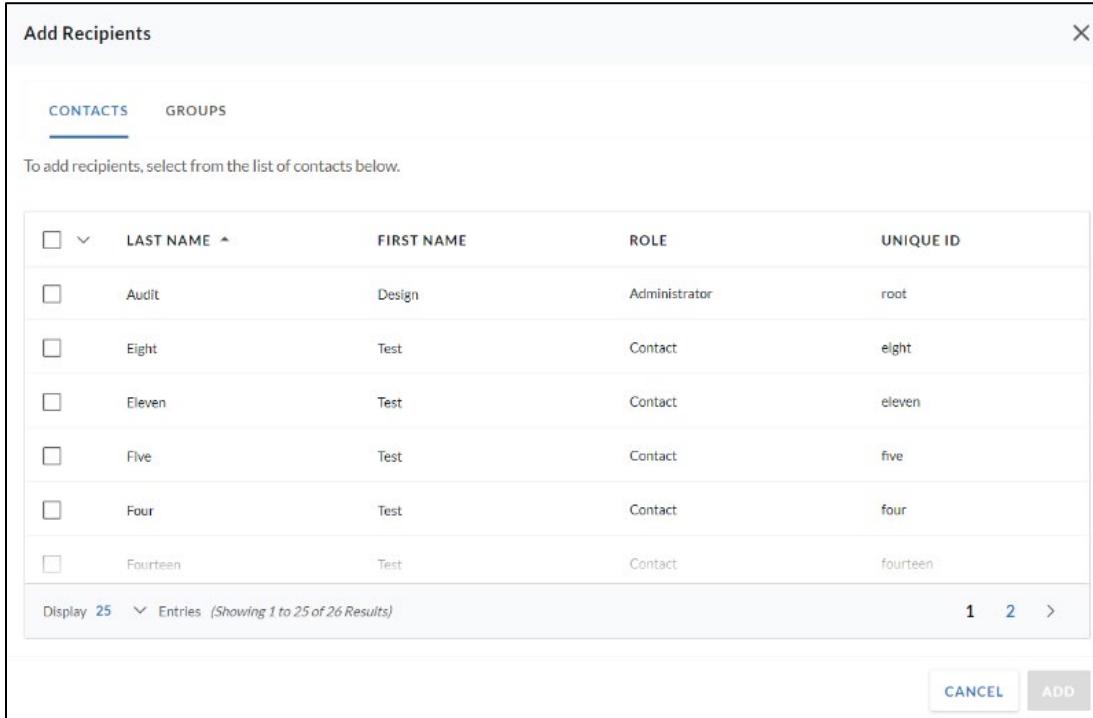
- The [Alert Analytics Report](#) includes the full history of responses from all recipients.
- In this release, you cannot mark a recipient as having not responded once they already have.
- Editing the response of a recipient who did not respond themselves does not end a broadcast alert, even if doing so means all recipients have a logged response.
- Editing a recipient's response does not trigger follow-up questions.
- Editing a recipient's response does not end a quota alert, even if the edited response causes the quota to be met.
- Editing a recipient's response does not trigger cascade alerts.
- Authorized users can edit recipients' responses after the alert duration has ended only if the Change Response advanced setting is enabled on the alert.

Manually Add Recipients

Contacts can be manually added to the Recipients table if they need to be accounted for but were not included as recipients in the alert, could not respond to the alert, or for any other reason. Additionally, contacts should be manually added to the Recipients table if the alert sender wants to include those contacts as recipients in a resent alert.

To add recipients

- From the **Analytics** page, select **+ Add Recipients**. The **Add Recipients** window opens.



The screenshot shows the 'Add Recipients' window with the 'CONTACTS' tab selected. The table lists eight contacts:

	LAST NAME	FIRST NAME	ROLE	UNIQUE ID
<input type="checkbox"/>	Audit	Design	Administrator	root
<input type="checkbox"/>	Eight	Test	Contact	eight
<input type="checkbox"/>	Eleven	Test	Contact	eleven
<input type="checkbox"/>	Five	Test	Contact	five
<input type="checkbox"/>	Four	Test	Contact	four
<input type="checkbox"/>	Fourteen	Test	Contact	fourteen

Display 25 Entries (Showing 1 to 25 of 26 Results) 1 2 >

CANCEL ADD

- Select any number of contacts to be added to the table. Groups can also be added by selecting the **Contacts** tab.
- Select **Add (N)**.

Other Response

If any recipients respond to the alert with anything other than the provided response options, the text of that response will be listed in this column.



RESPONSE	OTHER RESPONSE
Yes	
	Can someone call me?

Alert Analytics Report

You can export a summary of the Recipients table by selecting **Export Summary** or a comprehensive report by selecting **Export Details**.

The summary report includes:

- Last Name
- First Name
- Status
- Response
- Time stamp
- Resends
- Unique ID

The details report includes:

- Alert ID
- Unique ID
- First Name
- Last Name
- Division
- Username
- Job Title
- Work Addresses 1 and 2, Building, Floor, City, State, Zip, Province, and Country
- Alert Issued
- Alert Delivered
- Response Received
- Most Recent Response
- Response
- Other Response
- Device Label
- Device Status
- Device Value

Once the file is ready, select **Download**. The file downloads to your computer. The report is also emailed to you if you have a saved email address in your people record.

Resend an Alert

While alerts can be resent from the **Sent Alerts** tab, resending an alert from its **Analytics** page allows you to choose your recipients based on how they responded to the initial alert or in an ad-hoc manner.

Resend Based on Response

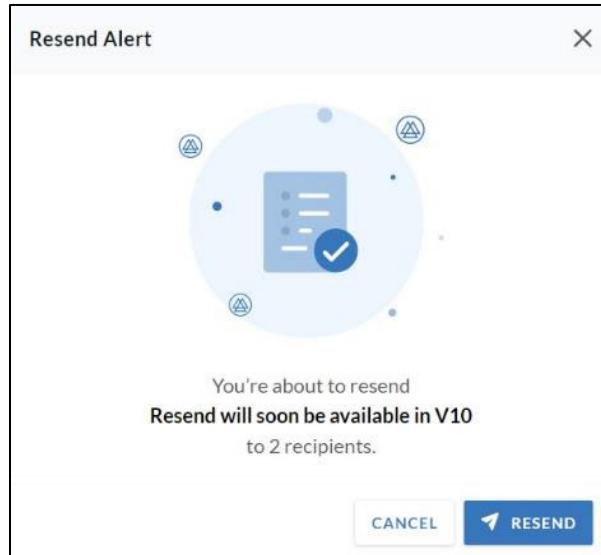
For alerts that include response options, the OnSolve Platform makes it easy for you to resend alerts to those recipients who didn't respond the first time or responded with a particular response.

To resend based on response

1. From the desired alert's Analytics page, locate the **Response Rate** section.
2. Select the **Resend** icon next to the response for the recipients you would like to resend the alert to. Or, select **Resend** next to **No Response** to resend the alert to those recipients who did not yet respond to the original alert.

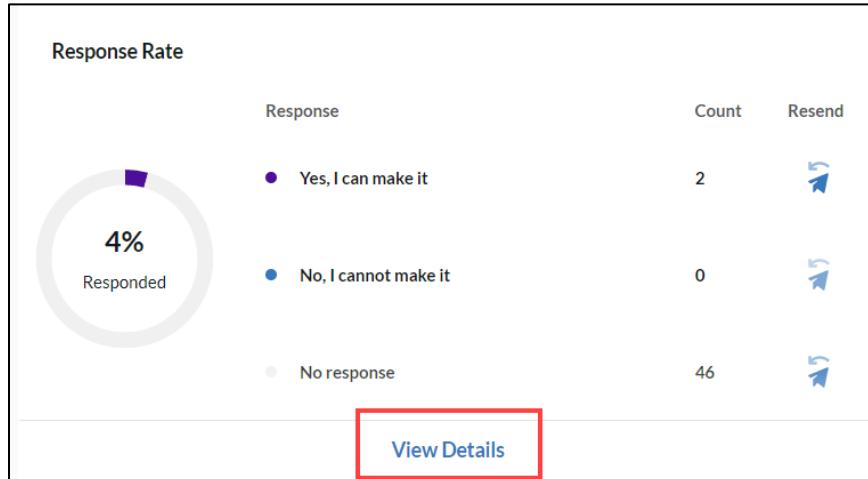


3. In the **Resend Alert** window, select **Resend**.

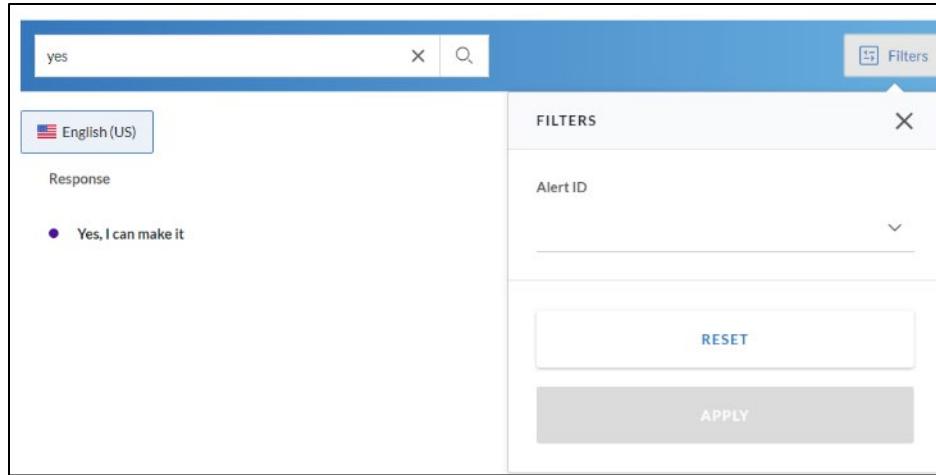


If you have a large number of responses from which to choose for your resend, you can search and filter responses:

1. From the **Analytics** page, select **View Details** in the **Response Rate** section.



2. Use the **Search Responses...** field to search responses by keyword, or use the **Filters** option to filter by **Alert ID**.



3. Once you have located the desired response, select the **Resend** icon to resend the alert to those recipients.
4. Select **Resend** to confirm.

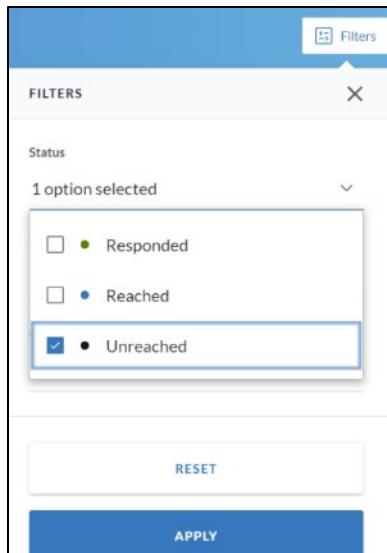
Custom Resend

Instead of resending based on responses, you can resend an alert to a custom group of recipients.

To resend to a custom group of recipients

1. From the **Analytics** page, scroll down to the Recipients table.
2. If desired, add any new recipients you'd like to include in the resend.
 - a. Select **+ Add Recipients**.
 - b. Search for and select your desired recipient(s).
 - c. Select **Add**.

3. Use the checkboxes to select each recipient to which you'd like to resend the alert. If necessary, use the **Search Recipients...** field to search by keyword, or filter recipients by **First Name, Last Name, Status** (Responded, Reached, Unreached), **Response**, or number of times **Contacted**.



Note: You can also use the table's **Select All Pages** and **Select This Page** options to select recipients in bulk, but when using **Select All Pages**, you cannot manually deselect recipients.

4. Select **Resend** again to confirm.

Ad Hoc Reports

As opposed to custom reports, ad hoc reports can be created by you, the user. Select alert-related data fields and conditions to create your criteria. In this release, you can preview the column headers in your report and run and save your report. In a future release, you will be able to preview the full data in your report before running it.

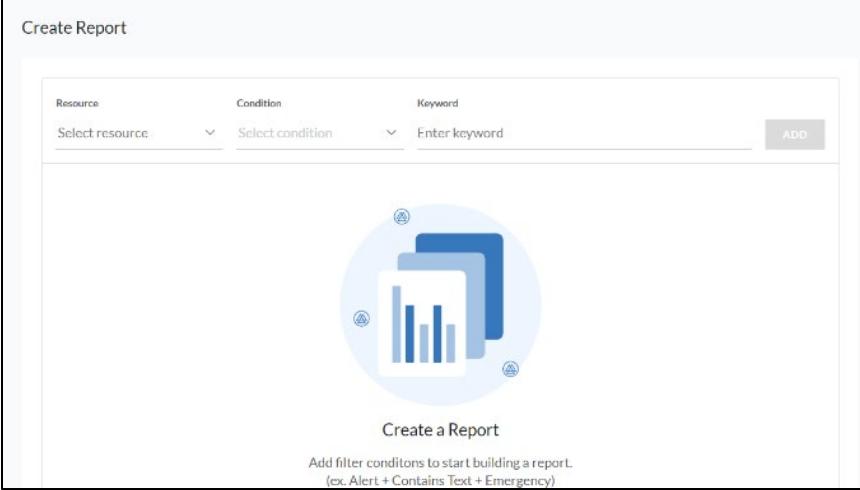
Create a New Report

Reports can be created from scratch or by duplicating a current report.

To create a new report from scratch

1. Navigate to **Reports > Reports**. The **Reporting** page opens, and any saved reports are displayed.

2. Select **+ Create Report**. The **Create Report** page opens.



Create Report

Resource	Condition	Keyword
Select resource	Select condition	Enter keyword

Create a Report

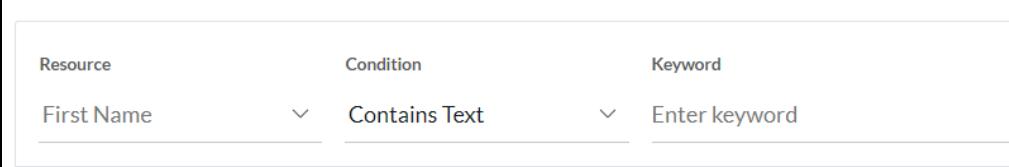
Add filter conditions to start building a report.
(ex. Alert + Contains Text + Emergency)

3. Select a **Resource** from the drop-down list as your first parameter. Over 70 data fields are available as resources and are grouped by the following categories:

- Contact
- Role
- Alert
- Sent Alert
- Group

See [Appendix B](#) in this guide for a complete list of all available resources.

4. Select a **Condition** from the drop-down list as your second parameter. The options here depend on the selected resource, but will include **Is**, **Contains Text**, or **Date Range**.
5. The final parameter again depends on your choice for the first two, but it completes the report criteria. Examples:
- If you set the first two parameters to **First Name** and **Contains Text**, you enter the final parameter as a **Keyword**.



Resource	Condition	Keyword
First Name	Contains Text	Enter keyword

- If you set the first two parameters to **Last Login** and **Date Range**, you enter the final parameter as a set of dates.

Resource	Condition	Last Login
Last Login	Date Range	MM / DD / YYYY - MM / DD / YYYY

6. Select **Add** to save that criterion.
7. Add more criteria as desired. When adding more criteria:
 - Your choice of resources will be restricted to the category from which you choose your first resource. For instance, if your first criterion is **First Name**, which is in the **Contact** category, any additional criteria resources can only be chosen from the **Contact** category.
 - You may add more criteria using the same resource as previously saved criteria. Criteria with the same resource will be displayed together with the OR condition (see [Example 2](#)). You can also change this condition to AND by editing it once saved. See [Edit Parameter Condition](#).
 - Select **AND** or **OR** as the conditions between each criterion. When **AND** is selected, the system will only return data that satisfies the criteria both before and after that condition (see [Example 2](#)).
- Note:** At any point, you can clear all criteria by selecting **Clear All Filters** at the bottom of the page.
8. When you have saved all your desired criteria, preview your report by selecting **Preview Report**. In this release, the preview displays the column headers of the report. In a future release, the data will also be displayed.
9. Choose to run the report now or only save it.
 - To only save, enter a **Report Name** and select **Save**. Your report will be saved to the Reports table. You can run a saved report at any time.
 - To run the report now, enter a **Report Name** and select **Run Report**. The report will still be saved to the Reports table. You will receive an email when your report is ready for download.
10. Follow the link in your email to download your report, which will be saved as a CSV file.

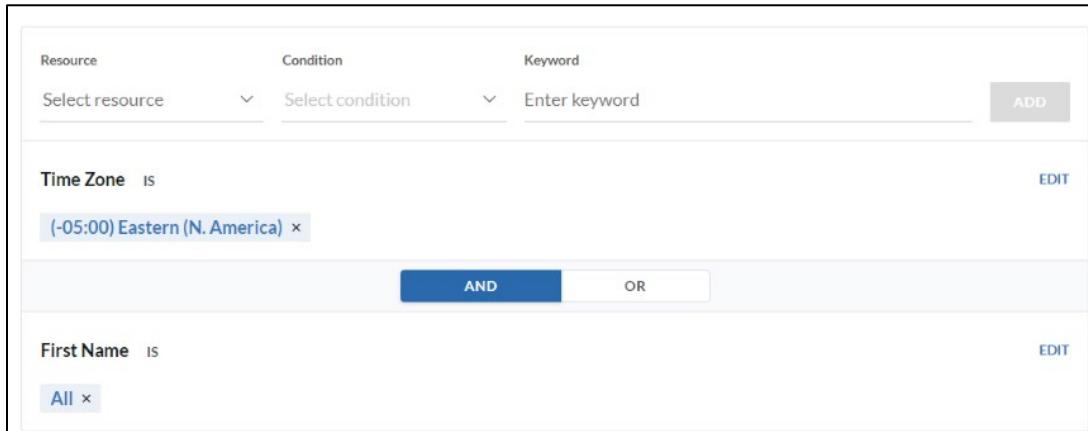
To create a new report by duplicating

1. From the Reports table, select the checkbox next to the report you want to duplicate and select **Duplicate**. The duplicated report appears in the table with "2" appended to the name.
2. Select the duplicated report's name. The report details are displayed.

3. Follow the instructions in [Edit](#) to edit your report as desired.

Example 1

In the example below, the report will list the first names of all contacts in the account that have Eastern as their time zone.



The screenshot shows the 'Edit' screen for an ad-hoc report. It features a grid for defining search criteria:

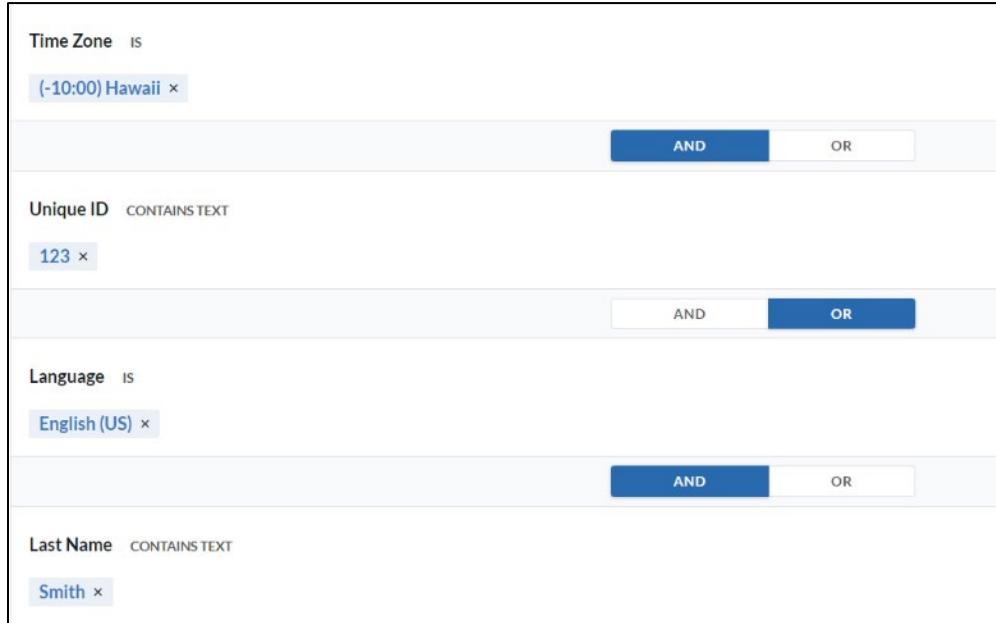
Resource	Condition	Keyword
Select resource	Select condition	Enter keyword
Time Zone IS (-05:00) Eastern (N. America) x		
First Name IS All x		

Below the grid are two buttons: **AND** (highlighted in blue) and **OR**.

Example 2

In the slightly more complex example below, the report will list all contacts:

- Whose Time Zone is Hawaii and whose Unique ID contains “123”
OR
- Whose Language is English (US) or whose Last Name contains “Smith”



The screenshot shows the Ad Hoc Report builder interface with four search criteria defined:

- Time Zone IS**: Value: (-10:00) Hawaii. Buttons: AND, OR.
- Unique ID CONTAINS TEXT**: Value: 123. Buttons: AND, OR.
- Language IS**: Value: English (US). Buttons: AND, OR.
- Last Name CONTAINS TEXT**: Value: Smith. Buttons: AND, OR.

Manage Ad Hoc Reports

All ad hoc reports can be saved in the table on the **Reporting** page.

Search

Use the **Search** field to find reports by keyword. This search field queries the **Report Name** and **Created By** data.

Sort

Select the arrow next to **Report Name** to sort A–Z or Z–A in that column.

Select the arrow next to **Last Used** to sort chronologically.

Filter

The Reports table can be filtered by **Created By**, **Last Used**, **Report Name**, or **Resource**. You can apply up to three filters with up to five keywords each.

- When filtering by **Created By**, choose from a list of all users who created any saved reports.
- When filtering by **Last Used**, enter the applicable date range.
- When filtering by **Report Name**, enter a keyword.
- When filtering by **Resource**, choose from a list of resources.

Edit

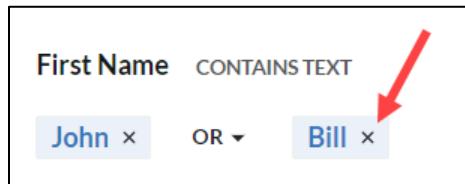
You can edit any report by clicking on its name in the Reports table. The report opens, and you can make changes as desired.

Add Criteria

Add more criteria to the report by following steps 3-6 in [Create New Report](#).

Delete Individual Parameters

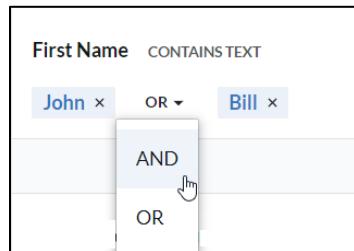
Select the **X** next to any parameters you want to delete.



Edit Parameter Condition

For criteria that contain more than one final parameter, you can change the condition from **OR** to **AND** (and vice versa):

1. Select **Edit** next to the desired criteria.
2. Use the drop-down list to select **AND** or **OR**.



3. Select **Save** to the right (where **Edit** was).



Delete Criteria

Select **Edit** and then **Delete** to delete an entire criterion from the report.



Delete

Delete a report by selecting the checkbox next to the desired report and selecting **Delete**. Select **Delete** again to confirm.

Run

You can run any saved report anytime by selecting the checkbox next to the desired report and selecting **Run Report**.

Audit Trail

The Audit Trail provides visibility into changes made directly within the User Interface, tracking all events during the OnSolve Platform account session. Administrators and authorized users can track actions and content changes, increasing accountability and insight into the account on all levels.

To view the audit trail, navigate to **Reports > Audit Trail**. The **View: Audit Logs** page opens in a new browser tab.

VIEW: AUDIT LOGS

This screen displays records from system audit logs by specifying filter criteria and clicking Search.

‣ Operations: All
‣ Performed By: All
‣ Date Range: All
‣ Target: All

Search

Audit Trail events are divided into four categories: **Operations**, **Performed By**, **Date Range**, and **Target**. Each category expands to display options for search refinement. By default, all options are selected.

Operations

The operations category includes 67 operations or events that a user in the account can take.

‣ **Operations: All**
[Check All](#) [Un-Check All](#)

Users:
 Add User
 Edit User
 Delete User

Groups:
 Add Group/Schedule
 Edit Group/Schedule
 Delete Group/Schedule

Notification:
 Add Notification
 Edit Notification
 Delete Notification

Notification Groups:
 Add Notification Group
 Edit Notification Group
 Delete Notification Group

Roles:
 Add Role
 Edit Role
 Delete Role

Templates:
 Add Template
 Edit Template
 Delete Template

Performed By

The **Performed By** section allows authorized users to search by who performed the operation. Search by **First Name**, **Last Name**, or **Employee ID** (Unique ID). When left blank, the Audit Trail returns results performed by all users. Only one name per field can be searched at a time.

▼ **Performed By:** All

First Name:	<input type="text"/>
Last Name:	<input type="text"/>
Employee ID:	<input type="text"/>

Date Range

The Date Range section allows authorized users to narrow their search results by the date the operations were performed. When left blank, the Audit Trail returns results not limited by date.

▼ **Date Range:** 10/01/2021 - 10/15/2021

Start Date:	<input type="text" value="10/01/2021"/> 
End Date:	<input type="text" value="10/15/2021"/> 

Target

The Target section allows authorized users to search by what was edited, created, deleted, etc. For example, if you want to see every event relating to a particular alert, search by that alert's name. If you want to see every event relating to a particular contact, search by that contact's name.

▼ **Target:** All

Target:	<input type="text"/>
---------	----------------------

Search the Audit Trail

To search the Audit Trail

1. In the **Operations** section, select all operations you want to be included in the search. You must select at least one operation.
2. Optionally, in the **Performed By** section, enter the **First Name**, **Last Name**, or **Employee ID** of the user whose audit trail you want to view.
3. Optionally, narrow your search by date range in the **Date Range** section.
4. Optionally, enter a **Target** to narrow your search by that which was created, edited, deleted, etc.
5. Select **Search**. Results are displayed on the bottom half of the page.

Export Audit Logs

Once you have search results, you can export those logs by selecting **Export Audit Logs**. The logs download to your computer.



Export Audit Logs

Usage Report

A usage report logs all alert traffic for an account to validate system usage and transaction bills.

To create a new Usage Report

1. Navigate to **Reports > Usage**.
2. Select **Generate Usage Report**. The **Usage Report** window opens.

Usage Report

Usage report includes the history of all alerts sent to SMS, email and mobile contact points from 12:00 AM on the start date until 11:59 PM on the end date.

Report Name

Enter report name

0 / 120

Date Range

MM/DD/YYYY-MM/DD/YYYY

CANCEL GENERATE REPORT

3. Enter a **Report Name**.
4. Enter the **Date Range** that should apply to the report.
5. Select **Generate Report**.
6. Select **Download Report**. The report is downloaded as a CSV file to the user's computer as [Report Name][Date Range].zip.

The report contains the following fields:

- | | |
|------------------------|-------------------------------|
| • Report ID | • Actual Duration (seconds) |
| • Alert Initiated At | • Billable Duration (seconds) |
| • Contact Sent At | • Initiator Division |
| • Alert Name | • Alert Division |
| • Initiator First Name | • Recipient Division |
| • Initiator Last Name | • Expedited |

- Recipient First Name
- Recipient Last Name
- Device Type
- Provider Type
- Device Address
- Contact Result
- Region
- Country
- Country Code
- Mobile Band
- Type
- SMS Messages (segments)

Call List Report

The Call List report lists all contact points for each contact in the selected division.

To generate a Call List report

1. Navigate to **Reports > Call List**.
2. Select **Call List** from the **Report Type** drop-down list.



Generate Reports

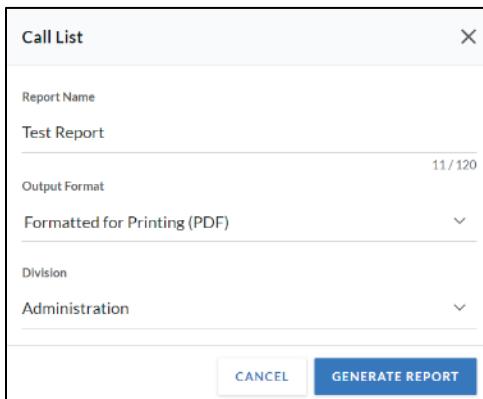
Select Report Type from the dropdown to generate reports

Report Type

Call List

Call List

3. In the **Call List** window, enter a **Report Name**.
4. Select the **Output Format** for the report. Options are PDF, CSV, XLS, and XLSX.
5. Select the **Division** to which the report should apply.
6. Select **Generate Report**.



Call List

Report Name

Test Report

11 / 120

Output Format

Formatted for Printing (PDF)

Division

Administration

CANCEL GENERATE REPORT

7. Select **Download Report**. The report downloads to the user's computer.

Custom Reports

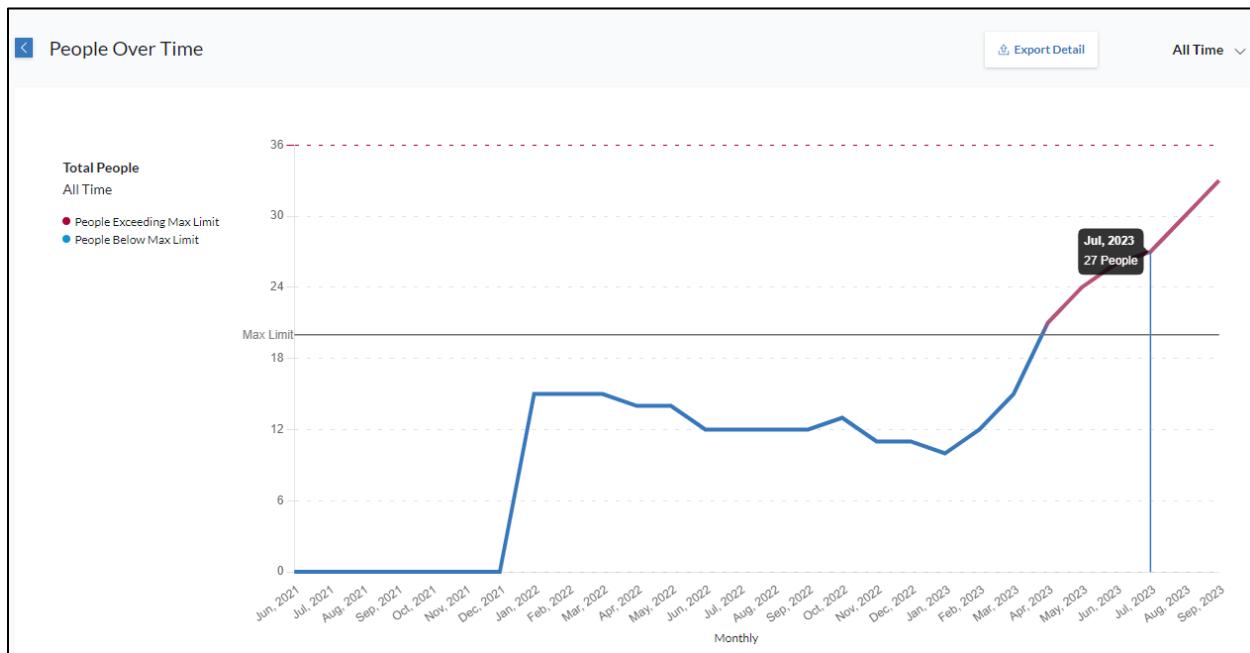
The OnSolve Professional Services Team can create custom reports specifically for your organization.

To find and run a custom report

1. Navigate to **Reports > Custom Reports**. The **Show All: Custom Reports** page opens and displays custom reports.
2. If necessary, use the available search tools to find your desired report.
3. Select the desired report and select **Display** to view it or **Export** to download it.

People Over Time

The People Over Time feature allows you to track the number of people saved in your account over a set time. Navigate to **Reports > People Over Time** to see this data in graphical form.



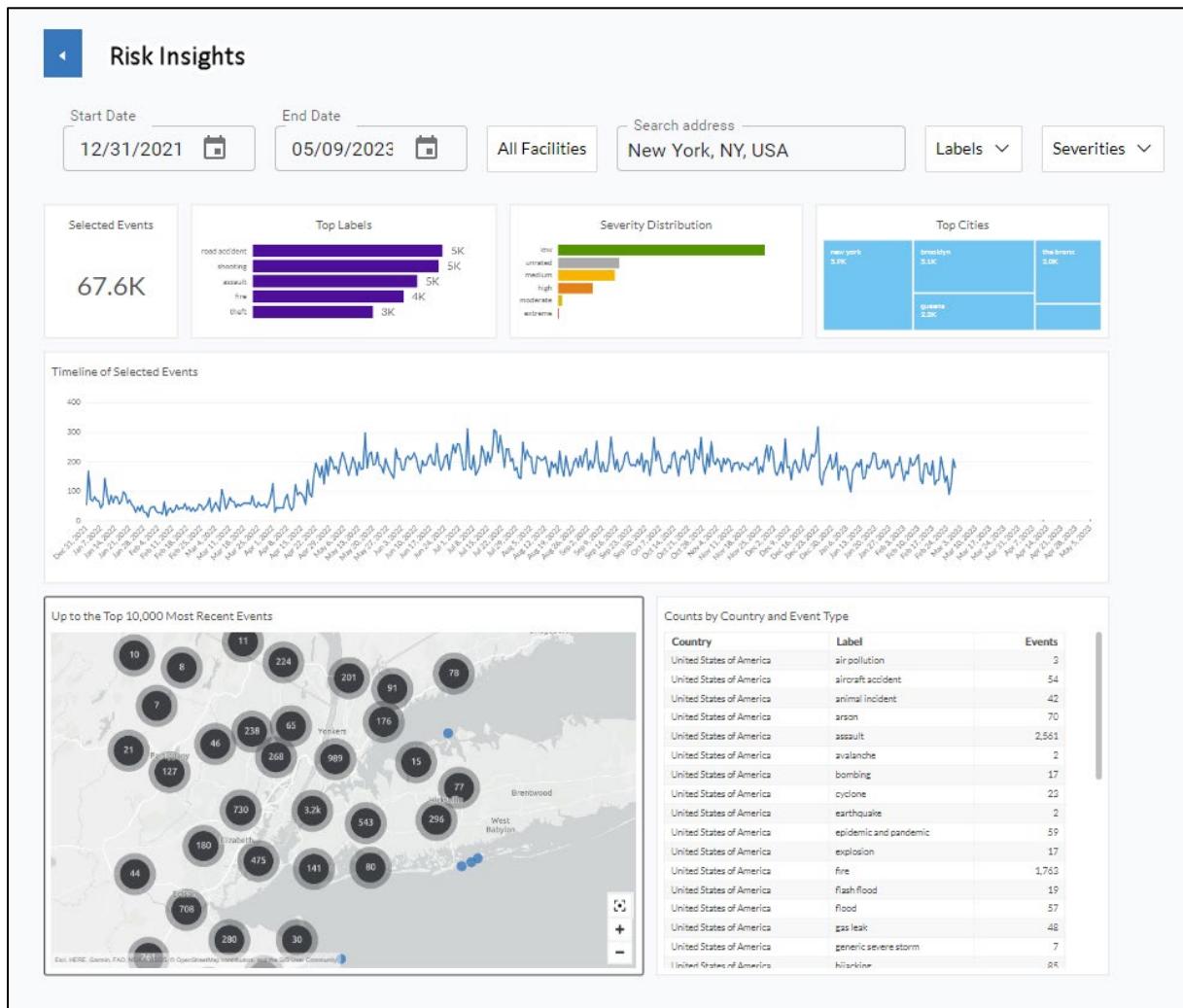
On this page, you can:

- Set the graph to display data from the **Last 7 Days**, **Last 2 Weeks**, **Last 30 Days**, **Last 3 Months**, **Last 6 Months**, **Last 12 Months**, or **All Time**.
- View your **Max Limit**. Contact Customer Support to have this limit adjusted.

- Hover over any point in the graph to see how many contacts were saved to your account as of the first of that month.
- Select **Export Detail** to download the data in the graph. The export includes your Organization ID, and for each date (the first of each month), your account's set max limit, the maximum number of contacts saved, and the difference between the two. The export covers the period of time set in the drop-down list at the top right of the page.

Risk Insights

Risk Insights is a dashboard offering powerful visualizations to reveal actionable insights around historical risks. Users can select a location, a set of assets, and a timeframe to see threat trends, comparisons, and statistics by event type and severity.



Risk Insights provides tools to access and analyze Risk Intelligence-related historical data. The aggregated data, ranging from January 1, 2021, and spanning to the previous day of the current date, contains information collected about every event that occurred worldwide from Risk Intelligence sources monitored by OnSolve. Currently, the historical data contains events captured in real-time from feeds that the OnSolve data team has validated.

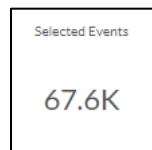
Risk Insights can be useful for customers with facilities set up in Risk Intelligence who want to understand the historical risks that have been detected around their facilities. By looking at the risk statistics, customers can see how risk breaks down by facility location and time.

Customers who do not have facilities within the system or have questions unrelated to their existing locations can also look at the breakdown of risk at a location based on an address. The ability to look at historical risk data enables customers to analyze the risk before opening a facility or an office, setting up operations, or even establishing a supply chain node at that location.

When enabled for your account, Risk Insights is an option on the OnSolve Platform left navigation menu. The Risk Insights page offers filters to hone the historical event information to visualize. Those visualizations include these statistics and charts related to the events that match the filter criteria:

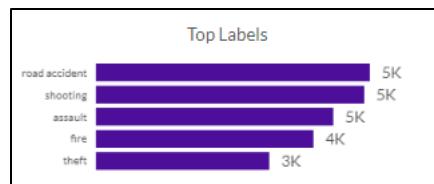
- Total Events: The number of events over the timeframe selected.

This tile gives a general idea of the number of events that occurred in the selected location and timeframe that matched the other selected criteria.



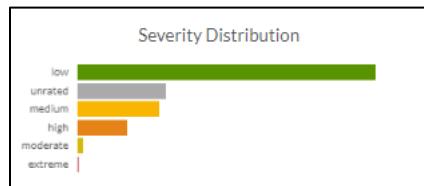
- Top Labels: The breakdown of events by event type.

This chart provides insights into the risks impacting your selected location over the selected timeframe. If no labels are specified in the **Labels** list, the chart highlights the top five risks for all possible risk labels and groups the others into one type.



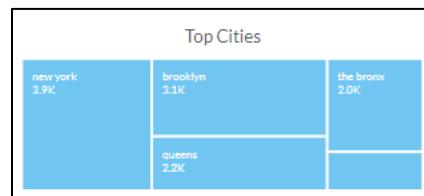
- Severity Distribution: The breakdown of event severity.

This chart indicates the severity distribution for events detected over the selected timeframe. Higher severity events indicate higher levels of identified impacts or higher risks to people and places nearby.



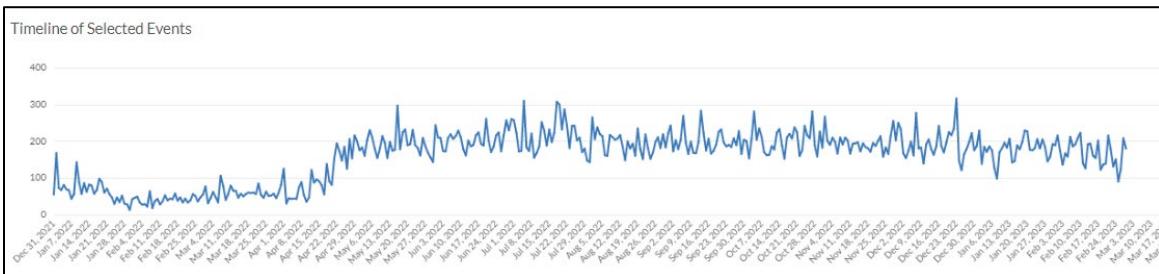
- Count of Events by City.

This chart shows the number of events broken down by the cities closest to the location of interest so that you can hone in on where events are most largely concentrated.



- Timeline: Charts event rates on a timeline.

This chart provides insights such as “Are the number of events matching my filter criteria increasing, decreasing, or staying the same for my selected timeframe?”



- Map: Shows the locations of events.

This map helps to identify areas where events occur to facilitate decision-making. For example, if you plan to put an office or facility in a particular location and the crime rate is high or where there are regular outbreaks of fires, you might want to look for areas with less impact from those events.



Once you set the filters and options that you want to focus on, the timeline and other charts update to reflect your criteria, allowing you to analyze the historical risk for those areas.

To access Risk Insights

Select **Risk Insights** from the OnSolve Platform left navigation menu to access the feature.

To filter events based on event type

1. On the **Risk Insights** page, select **Labels**. The **Labels** drop-down list is displayed.
2. Select the label(s) you want to work with.

Labels			
<input type="checkbox"/> Aircraft Accident	<input type="checkbox"/> Air Pollution	<input type="checkbox"/> Animal Incident	<input type="checkbox"/> Arson
<input type="checkbox"/> Assault	<input type="checkbox"/> Avalanche	<input type="checkbox"/> Bombing	<input type="checkbox"/> Chemical Spill
<input type="checkbox"/> Cold Wave	<input type="checkbox"/> Cyclone	<input type="checkbox"/> Drought	<input type="checkbox"/> Earthquake
<input type="checkbox"/> Epidemic and Pandemic	<input type="checkbox"/> Explosion	<input type="checkbox"/> Fire	<input type="checkbox"/> Flash Flood
<input type="checkbox"/> Flood	<input type="checkbox"/> Gas Leak	<input type="checkbox"/> Generic (Severe) Storm	<input type="checkbox"/> Heat Wave
<input type="checkbox"/> Hijacking	<input type="checkbox"/> Homicide	<input type="checkbox"/> Hostage Taking	<input type="checkbox"/> Insect Infestation
<input type="checkbox"/> Labor Strike	<input type="checkbox"/> Landslide	<input type="checkbox"/> Maritime Accident	<input type="checkbox"/> Mass Shooting
<input type="checkbox"/> Military Action	<input type="checkbox"/> NBC - Nuclear, Biological, Chemical	<input type="checkbox"/> Oil Spill	<input type="checkbox"/> Power Outage
<input type="checkbox"/> Protest	<input type="checkbox"/> Rail Accident	<input type="checkbox"/> Riot	<input type="checkbox"/> River Flood
<input type="checkbox"/> Road Accident	<input type="checkbox"/> Sexual Assault	<input type="checkbox"/> Shooting	<input type="checkbox"/> Storm Surge
<input type="checkbox"/> Structure Collapse	<input type="checkbox"/> Structure Fire	<input type="checkbox"/> Technical Disaster	<input type="checkbox"/> Terrorism
<input type="checkbox"/> Theft	<input type="checkbox"/> Tornado	<input type="checkbox"/> Tsunami	<input type="checkbox"/> Volcano
<input type="checkbox"/> Wildfire	<input type="checkbox"/> Wind	<input type="checkbox"/> Winter Storm / Blizzard	

APPLY

Note: When no labels are selected, all labels are included in the event filter.

3. Select **Apply**. The charts and statistics update based on your selections.

To filter events based on the severity

1. On the **Risk Insights** page, select **Severity**. The **Severity** drop-down list is displayed.
2. Select the severity rating(s) you want to work with.

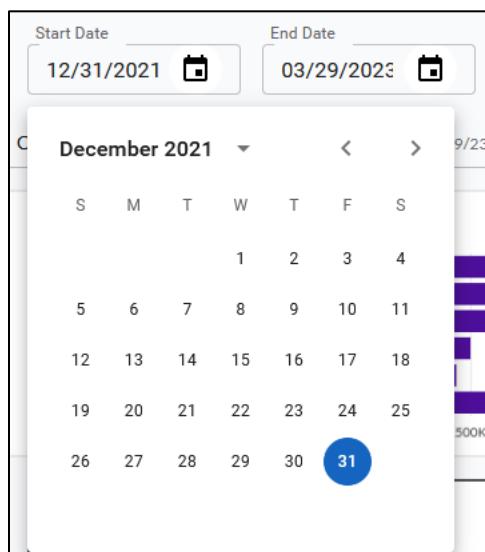


Note: When no severities are selected, all severities are included in the event filter.

3. Select **Apply**. The charts and statistics update based on your selections.

To specify a time range

1. On the **Risk Insights** page, select **Time Range**. The **Start Date** and **End Date** calendars are displayed.
2. Select the dates you want to work with.



The charts and statistics update based on your selections.

To select a location to focus on a region of interest

1. On the **Risk Insights** page, enter an address in the **Search address** field.

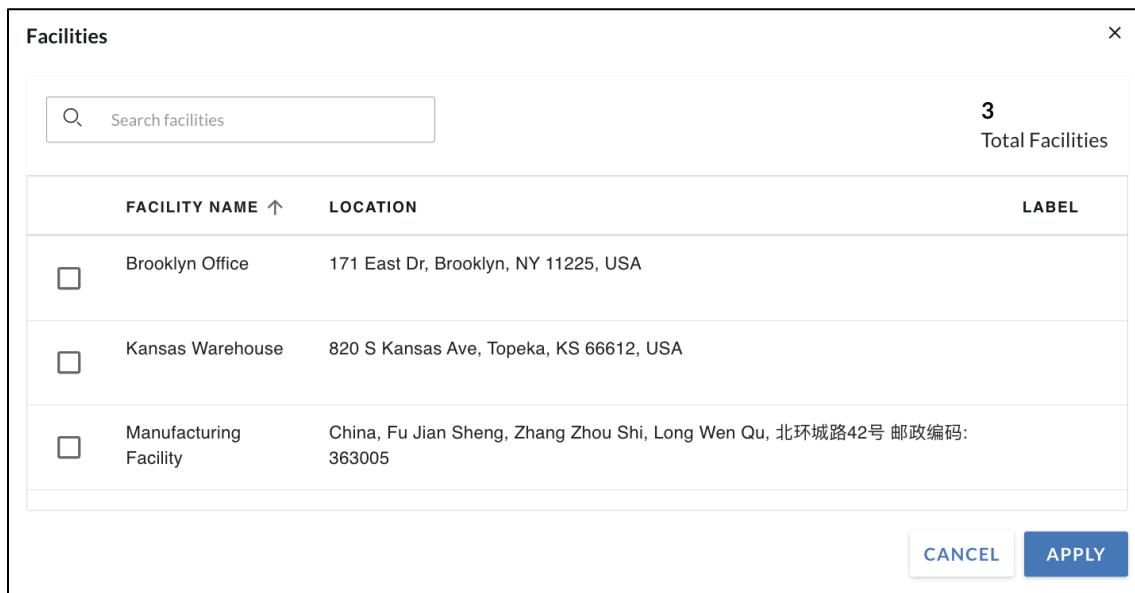


A screenshot of a search input field. The placeholder text 'Search address' is visible at the top left. Below it, the text 'New York, NY, USA' is entered. A blue rectangular border highlights the entire input field.

2. Select **Enter**. The charts and statistics update based on your selection.

To focus on risk at one or more facilities

1. On the **Risk Insights** page, select **All Facilities**. The **Facilities** dialog box is displayed.
2. Select the facility or facilities you want to work with.



A screenshot of a modal dialog box titled 'Facilities'. At the top right is a close button ('X'). Below the title is a search bar with a magnifying glass icon and the placeholder 'Search facilities'. To the right of the search bar, the number '3' is displayed above the text 'Total Facilities'. The main area is a table with three columns: 'FACILITY NAME ↑', 'LOCATION', and 'LABEL'. Each row contains a checkbox followed by the facility name, location, and a long address in China. At the bottom right of the dialog are two buttons: 'CANCEL' and 'APPLY' (which is highlighted with a blue background).

FACILITY NAME ↑	LOCATION	LABEL
<input type="checkbox"/>	Brooklyn Office 171 East Dr, Brooklyn, NY 11225, USA	
<input type="checkbox"/>	Kansas Warehouse 820 S Kansas Ave, Topeka, KS 66612, USA	
<input type="checkbox"/>	Manufacturing Facility China, Fu Jian Sheng, Zhang Zhou Shi, Long Wen Qu, 北环城路42号 邮政编码: 363005	

3. Select **Apply**. The charts and statistics update based on your selections.

Section 5: Incident Management

LookOut

The LookOut feature allows mobile users to report suspicious activities or emergency incidents and send location-specific information in real time via the mobile app.

Authorized users can assign recipients by division who will receive an alert when mobile users report a LookOut incident.

Configure LookOut Settings

Authorized users must configure all **LookOut Settings** within the user interface before app users can use the LookOut feature within the app. These include defining permissions by role and assigning alerts to divisions for incident alert recipients.

Additionally, app users must have their location enabled on their mobile devices to use the LookOut feature.

Assign Role Permissions

- Verify all divisions and roles are available, within **Configure > Divisions and Roles**, before assigning permissions for the feature.
- Mobile app users (administrators, senders, and users) will need Global Permissions added to their role to use the LookOut feature. Define the appropriate role (and role template) permissions within your organization to add **Send LookOut** within the role in **Configure> Permissions> Roles > Permissions > Mobile Interface** tab.
- Administrators who manage the LookOut feature will need divisional permissions. Divisional Permissions control what is available in the user interface, including permissions for creating and managing the LookOut feature. Add the appropriate role (and role template) permissions within your organization to **Edit** and **View LookOut** within the user interface by navigating to **Configure > Permissions > Roles > Permissions** in the **LookOut** section. Only one incident-based alert can be assigned to a division.

For more on permissions, review the [Role and Role Template Management](#) section in this guide.

Assign an Alert to a Division

Mobile users need to be part of a division to send a LookOut within the app and for the system to send LookOut-triggered alerts to users within their division. Any incident-driven alert that captures the user's triggered LookOut incident must first be assigned to a division.

To assign an alert to a division

1. Navigate to **Incident Management**. The **Incident Management** page opens.

The screenshot shows the left sidebar with 'Incident Management' selected. The main area is titled 'Incident Management' and contains two cards: 'LookOut' (Reported incidents from contacts) and 'SOS' (History of reported SOS emergencies).

2. Select **LookOut**. The **LookOut Incidents** page opens.

The screenshot shows the 'LookOut Incidents' page with a table of incidents. The columns are: INCIDENT DETAILS, LOCATION, DATE SUBMITTED, SENDER, STATUS, and ANALYTICS. Each incident row has a checkbox in the first column and a blue 'Analytics' icon in the last column.

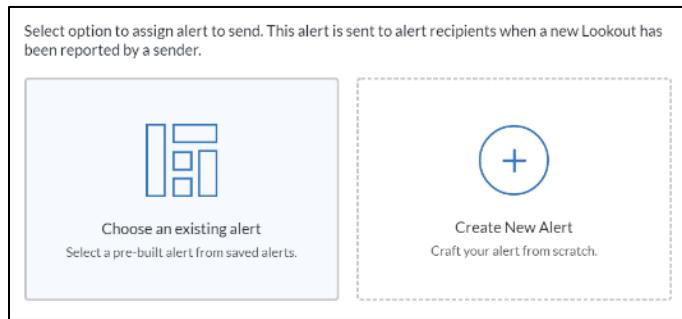
	INCIDENT DETAILS	LOCATION	DATE SUBMITTED	SENDER	STATUS	ANALYTICS
<input type="checkbox"/>	Testing only	22 Minnow Dr, Ormond Beach, FL 32174, USA	Nov 23, 2021 6:46 PM	# UserA	Completed	
<input type="checkbox"/>	Test	140 Limewood Pl, Ormond Beach, FL 32174, USA	Nov 23, 2021 11:32 AM	# UserA	Completed	
<input type="checkbox"/>	Test only	140 Limewood Pl, Ormond Beach, FL 32174, USA	Nov 23, 2021 11:29 AM	# UserA	Completed	
<input type="checkbox"/>	Is only a test	43VV+7X Chitir, Republic of Dagestan, Russia	Nov 19, 2021 3:10 PM	# UserA	Completed	
<input type="checkbox"/>	Testing	1428 Central Ave, Flagler	Sep 7, 2021 10:39 AM	# UserA	Completed	

3. Select **LookOut Settings**.

4. Select the add + icon to assign a division to a LookOut alert. Only one alert can be assigned to a division. You must select an alert that includes the variables for the LookOut feature.

The screenshot shows the 'LookOut Settings' page with a section titled 'ASSIGN ALERTS TO DIVISION'. It lists four divisions: 'OnSolve Jane Erstwhile', 'Austen Company', 'East Coast Office', and 'West Coast Office', each with a blue '+' icon to its right.

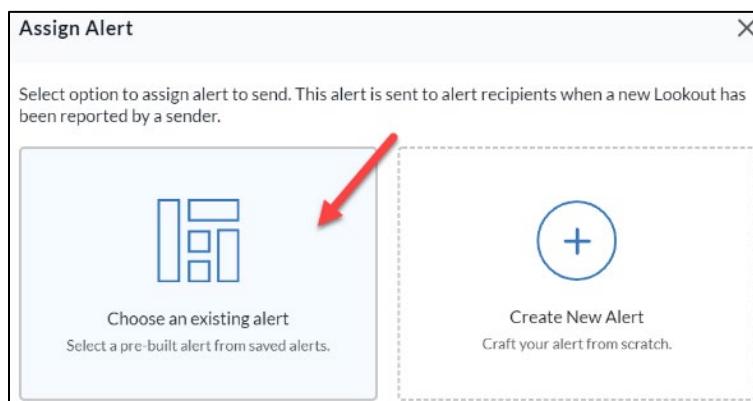
5. Choose an Existing Alert or Create New Alert.



Select Existing LookOut Alert

To choose an existing alert to link your incident to a division

- From the **LookOut Settings** page, select the +add icon next to the division. If assigning an existing alert to the division, **Choose an existing alert**.



- Choose an existing alert that includes LookOut-specific message variables from the available alerts on the **Select Alert to Send** page. Review the [Alert Variables](#) section for more information.

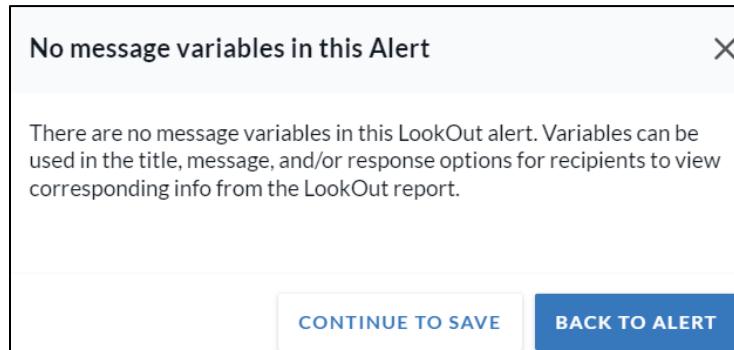
Select Alert to Send				
<input type="text" value="Search Saved Alerts..."/> Filters				
ALERT NAME	LAST MODIFIED	ALERT TYPE	STATUS	RECIPIENTS
<input checked="" type="radio"/> Earthquake	Created Nov 17, 2021 at 12:38 PM by [REDACTED]	Broadcast	Saved	
<input type="radio"/> Fire Drill	Created Nov 8, 2021 at 8:33 AM by [REDACTED]	Broadcast	Saved	
<input type="radio"/> Shots reported	Created Nov 8, 2021 at 9:15 AM by [REDACTED]	Broadcast	Saved	
<input type="radio"/> Snow Emergency	Created Nov 16, 2021 at 7:27 AM by [REDACTED]	Broadcast	Saved	

- Select **Assign** to save your choice and return to the **LookOut Settings** page. The alert is now linked to the division on the **LookOut Settings** page.

The screenshot shows the 'LookOut Settings' page. On the left is a sidebar with options: Dashboard, Alerts, Contacts, Schedules, Reports, Incident Management (which is selected), Subscriptions, and Configure. The main area is titled 'ASSIGN ALERTS TO DIVISION' with a sub-instruction: 'LookOut desktop tool & mobile app feature will be enabled for users under assigned division.' Below this, there's a list of alerts and their assignments:

- OnSolve Jane Erstwhile (selected) - Earthquake (status: Enabled)
- Austen Company (status: Enabled)
- East Coast Office (status: Enabled)
- West Coast Office (status: Enabled)

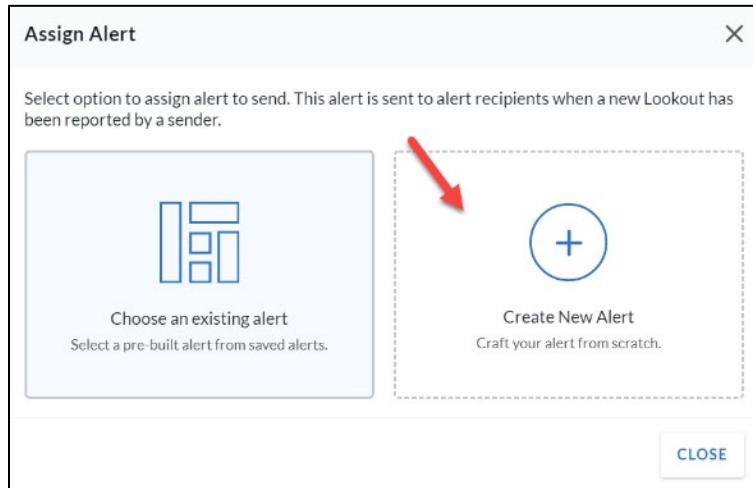
Note: If no variables are saved in your chosen alert, a warning will give you the option to edit the alert or choose another alert using the **Back to Alert** button. If you ignore the warning and no incident-based variables are included in the alert, the alert message body will be blank.



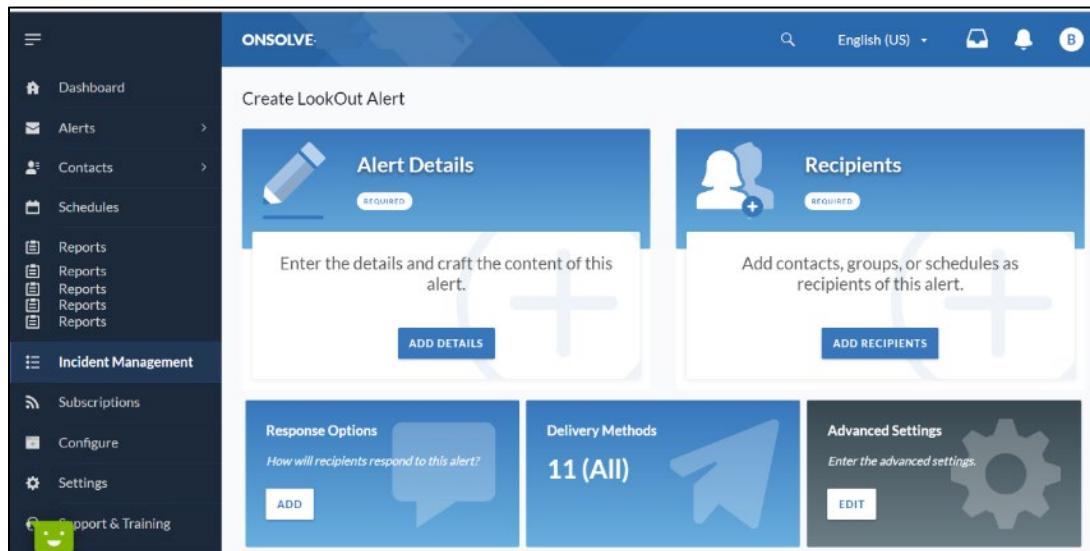
Create New LookOut Alert

To create a new alert from scratch and assign it to a division

- From the **LookOut Settings** page, select the **+** add icon next to the division and choose **Create New Alert**.



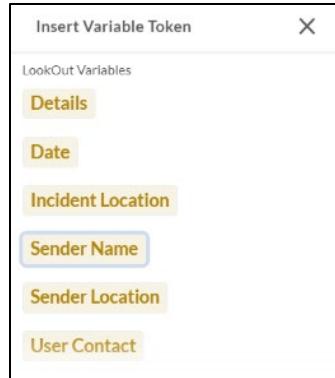
The **Create LookOut Alert** page opens.



The page has a sidebar with navigation links: Dashboard, Alerts, Contacts, Schedules, Reports, Incident Management (selected), Subscriptions, Configure, Settings, and Support & Training. The main content area is titled "Create LookOut Alert". It features four main sections: "Alert Details" (with a pencil icon), "Recipients" (with a user icon), "Response Options" (with a speech bubble icon), and "Delivery Methods" (with a megaphone icon showing "11 (All)"). There are "ADD DETAILS", "ADD RECIPIENTS", and "EDIT" buttons. The "Alert Details" section includes a note: "Enter the details and craft the content of this alert." and a "Response Options" note: "How will recipients respond to this alert? ADD".

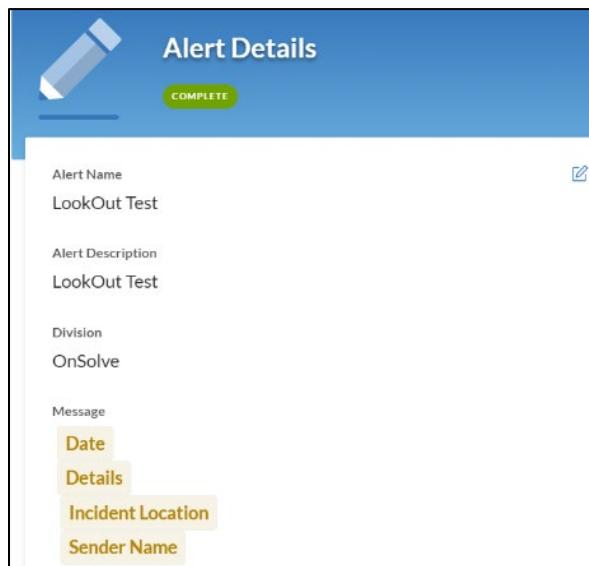
- Select **Add Details**.
- Add the **Alert Name**, **Alert Description**, and **Division**.
- Within the **Message Body** section, select **+Insert Variables** and add all tokens. All suggested variables are necessary for incident-based reporting and must be added to the alert, or the

delivered message will be blank. To add a custom variable, see [Alert Variables](#) in Section 3 of this guide for more information.



Note: You cannot create a new LookOut alert from the **Alerts** page since the incident-specific variables only exist within the **Incident Management** tool.

5. Select **Save**. The variables are now listed within **Alert Details**.



6. Add **Recipients, Delivery Methods, Response Options**, and **Advanced Settings** as desired.
 7. Select **Save** after defining the required sections. Your alert is now added to the division on the **LookOut Settings** page.
- Note:** If no variables are saved to your chosen alert, a warning will allow you to edit the alert using the **Back to Alert** button. If you ignore the warning and save the alert without the incident-specific variables, any LookOut reported with that alert will have a blank message.
8. Assign additional alerts to available divisions.

After all alerts are defined in **LookOut Settings**, when a LookOut incident is triggered via the mobile app, designated users will receive alerts with incident information, including the location.

The screenshot shows the 'LookOut Settings' page under the 'Incident Management' menu. A success message at the top says 'Successfully saved Earthquake.' Below it, a section titled 'ASSIGN ALERTS TO DIVISION' lists four divisions with their assigned alerts:

Division	Alert Type	Action	Status
OnSolve Jane Erstwhile	Fire Drill	Call	X
Austen Company	Shots reported	Call	X
East Coast Office	Snow Emergency	Call	X
West Coast Office	Earthquake	Call	X

LookOut Incidents

Review all active and completed LookOut incidents by navigating to **Incident Management > LookOut**.

The screenshot shows the 'LookOut Incidents' page. At the top, there's a search bar labeled 'Search Incidents' and a 'LOOKOUT SETTINGS' button. The main area displays a table of incidents with the following columns:

INCIDENT DETAILS	LOCATION	DATE SUBMITTED	SENDER	STATUS	ANALYTICS
Testing only	22 Minnow Dr, Ormond Beach, FL 32174, USA	Nov 23, 2021 6:46 PM	# UserA	Completed	
Test	140 Limewood Pl, Ormond Beach, FL 32174, USA	Nov 23, 2021 11:32 AM	# UserA	Completed	
Test only	140 Limewood Pl, Ormond Beach, FL 32174, USA	Nov 23, 2021 11:29 AM	# UserA	Completed	
Is only a test	43VV+7X Chitir, Republic of Dagestan, Russia	Nov 19, 2021 3:10 PM	# UserA	Completed	
Testing	1428 Central Ave, Flagler	Sep 7, 2021 10:39 AM	# UserA	Completed	

Columns displayed for LookOut Incidents are:

- **Incident Details:** The description of the LookOut incident.
- **Location:** The location of the incident.

- **Date Submitted:** The date and time the incident is reported.
- **Sender:** The mobile sender of the incident.
- **Status:** The status of the incident. This status is either **Active** or **Completed**.
- **Analytics:** Select the icon for all incident details, including images. See [Analytics](#) in Section 4 of this guide for more information.

LookOut in OnSolve Mobile

View the LookOut button and use the feature within the Recipient view. Administrators and authorized users can view and access Incident Management through the Sender app login. Review the current *OnSolve Mobile Guide* for more information on the LookOut feature within the OnSolve Mobile App.

SOS

The SOS feature allows mobile app users in an urgent situation to connect to the appropriate emergency services phone number with a tap of a button. In cases where it might not be possible to tap a button, mobile users can set Life Check to set off an SOS after a set amount of time.

Authorized users can assign incident-based alerts to divisions that capture SOS incidents as they happen. When a mobile user triggers an SOS incident or the SOS is automatically triggered by a Life Check event, assigned recipients receive an alert that shares SOS-related information, such as the mobile user's incident information and location.

Configure SOS Settings

Administrators must configure all **SOS Settings** within the user interface before app users can utilize the SOS and Life Check functionality within the app. These include defining permissions by role and assigning alerts to divisions for incident alert recipients.

Location Permissions

Though the SOS feature works with and without mobile location permission, OnSolve recommends mobile users always enable location services on their mobile device for the app.

If location permissions are enabled on the user's mobile device, the system detects and displays the user's location within the app after swiping the red **SOS** button to the right, or the Life Check timer goes off. The associated alert will share the user's location and incident information if configured with Alert Variables such as Incident Location. If location services are disabled, location information is limited to only the mobile user's country.

Assign Role Permissions

Within **Configure > Divisions and Roles**, verify all divisions and roles are created and available before assigning permissions for the feature. Only one incident-based alert can be assigned to a division.

Mobile app users (administrators, senders, and users) need Global Permissions added to their role to use the SOS feature. Define the appropriate role (and role template) permissions within your organization to add **Send SOS** and **Life Check** within a role in **Configure > Permissions > Roles > Permissions** on the **Mobile Interface** tab.

Administrators who manage the SOS feature will need divisional permissions. Divisional Permissions control what is available in the user interface, including permissions for creating and managing the SOS feature. Add the appropriate role (and role template) permissions within your organization to **Edit** and **View SOS** within the user interface by navigating to **Configure >**

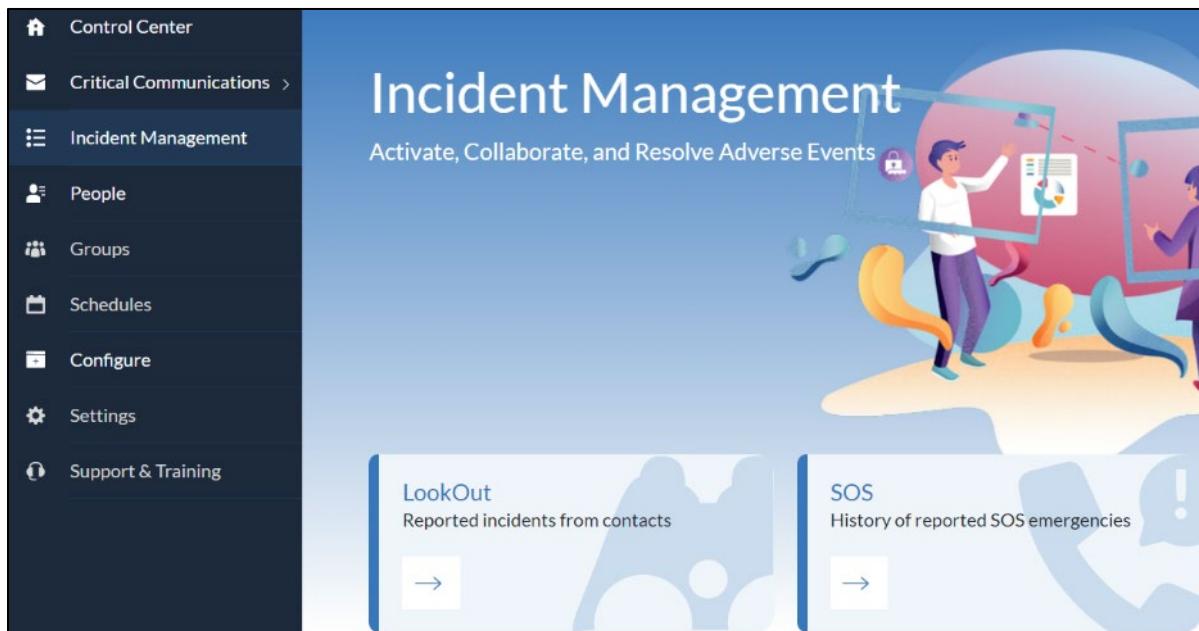
Permissions > Roles > Permissions in the **SOS** section. Review the [Role and Role Template Management](#) section in this guide for more information.

Assign an Alert to a Division

Mobile users need to be part of a division to send an SOS within the app and for the system to send SOS-triggered alerts to users within their division. Any incident-driven alert that captures the user's triggered SOS incident must first be assigned to a division.

To assign an alert to a division

1. Navigate to **Incident Management > SOS**.



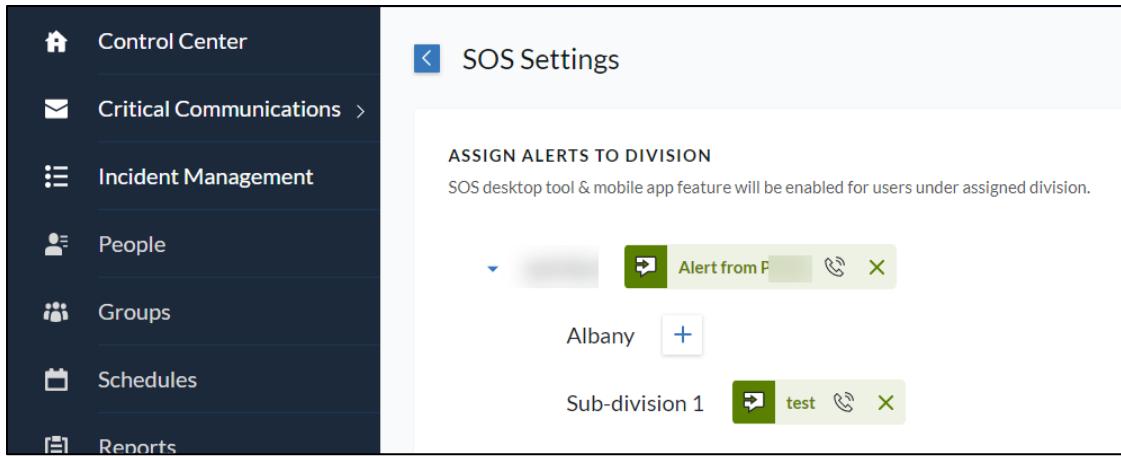
The screenshot shows the Incident Management interface. On the left is a dark sidebar menu with options: Control Center, Critical Communications, Incident Management (which is selected and highlighted in blue), People, Groups, Schedules, Configure, Settings, and Support & Training. The main content area has a blue header with the text "Incident Management" and "Activate, Collaborate, and Resolve Adverse Events". Below the header are two cards: "LookOut" (Reported incidents from contacts) and "SOS" (History of reported SOS emergencies). The "SOS" card is currently active, showing a list of recent SOS incidents.

The **SOS Incidents** page opens.

SOS Incidents							SOS SETTINGS
Search Incidents				DATE SUBMITTED	SENDER	STATUS	ANALYTICS
□	CONTACT POINT	LOCATION	DATE SUBMITTED	SENDER	STATUS	ANALYTICS	
□	SOS	47HRG96X+XC	Nov 23, 2021 6:48 PM	SOS	Completed		
□	Testing only	140 Limewood Pl, Ormond Beach, FL 32174, USA	Nov 23, 2021 6:47 PM	#UserA	Completed		
□	Testing only	140 Limewood Pl, Ormond Beach, FL 32174, USA	Nov 23, 2021 6:45 PM	#UserA	Completed		
□	Testing only	CWG3+RP Placilla, Chile	Nov 23, 2021 11:51 AM	#UserA	Completed		

2. Select **SOS Settings**.

3. Select the add + icon to assign an SOS alert to a division. Only one alert can be assigned to a division. You must select an alert that includes the variables for the SOS feature.

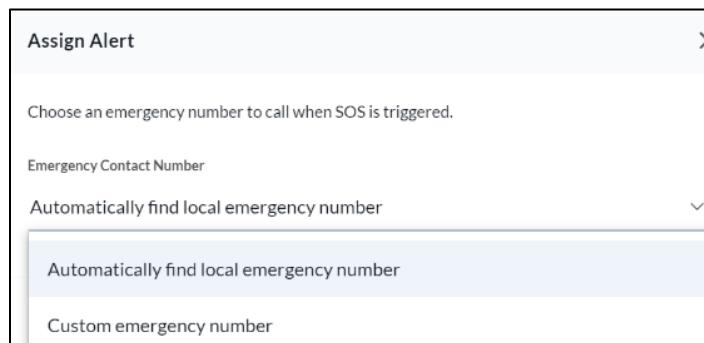


The screenshot shows the 'SOS Settings' page. On the left is a sidebar with icons for Control Center, Critical Communications, Incident Management (selected), People, Groups, Schedules, and Reports. The main area is titled 'ASSIGN ALERTS TO DIVISION' with the sub-instruction 'SOS desktop tool & mobile app feature will be enabled for users under assigned division.' Below this are two alert cards. The first card for 'Albany' has an 'Alert from F' button, a phone icon, and a close button. The second card for 'Sub-division 1' has a 'test' button, a phone icon, and a close button. A blue '+' button is located between the two cards.

4. The **Assign Alert** window opens. Assign the emergency number that allows the mobile user to connect to emergency personnel when they trigger an SOS within the app:

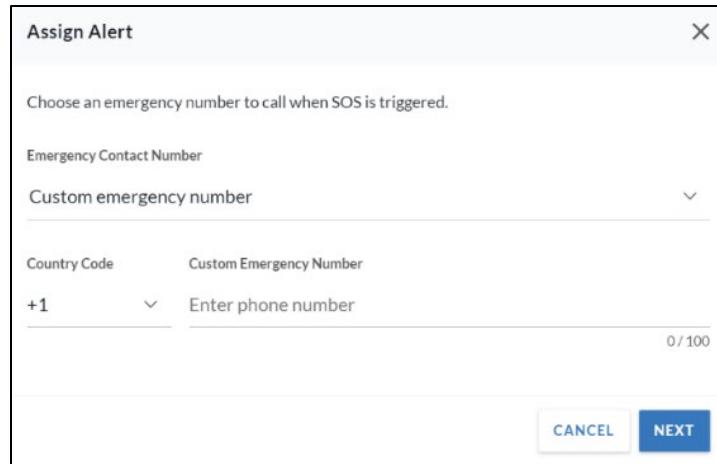
- Automatically find local emergency number:** Select **Automatically find local emergency number** from the drop-down menu. With this option, when an SOS is triggered, users are prompted to tap an Emergency Services button that dials the emergency phone number for the user's current location (911, fire, rescue, etc.). Any associated alert will share this mobile user's current location and user information associated with their login.

The system will choose the emergency number based on the user's location. If location services are off, users must select the country of their current location from a drop-down menu to prompt the Emergency Services button when an SOS is triggered. Only the selected country and app user's name will be shared in any triggered alert.



- Custom Emergency Number:** Choose the **Country code** and enter the **Phone number** in **Assign Alert**. With this option, when an SOS is triggered, users are prompted with an Emergency Services button to tap that dials a local, predefined number. The custom phone number can be an organization-specific number for a central location or a local emergency

number (sheriff or ambulance). Location information does not need to be enabled when this number is associated with the alert.



The dialog box is titled "Assign Alert". It contains a sub-instruction: "Choose an emergency number to call when SOS is triggered." Below this is a dropdown menu labeled "Emergency Contact Number" with "Custom emergency number" selected. A "Country Code" dropdown shows "+1" and a "Custom Emergency Number" input field where "Enter phone number" is typed. A character count indicator "0 / 100" is shown next to the input field. At the bottom are "CANCEL" and "NEXT" buttons.

5. Select **Next**.
6. Create a new alert or select an existing SOS alert to assign to your division.

Select an Existing SOS Alert

To choose an existing alert to link your incident to a division

1. After assigning an emergency number and selecting **Next**, **Choose an existing alert**.



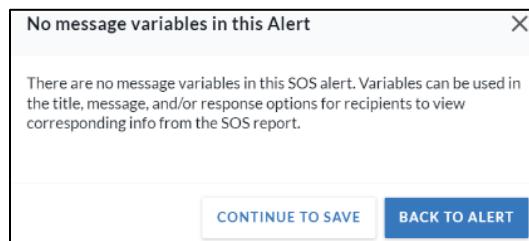
2. Select an existing alert that includes SOS-specific message variables from the available alerts on the **Select Alert to Send** page. Review the [Alert Variables](#) section for more information.

Select Alert to Send

ALERT NAME	LAST MODIFIED	ALERT TYPE	STATUS	RECIPIENTS
<input checked="" type="radio"/> Earthquake	Created Nov 17, 2021 at 12:38 PM by [REDACTED]	Broadcast	Saved	
<input type="radio"/> Fire Drill	Created Nov 8, 2021 at 8:33 AM by [REDACTED]	Broadcast	Saved	
<input type="radio"/> Shots reported	Created Nov 8, 2021 at 9:15 AM by [REDACTED]	Broadcast	Saved	
<input type="radio"/> Snow Emergency	Created Nov 16, 2021 at 7:27 AM by [REDACTED]	Broadcast	Saved	

3. Select **Assign** to save your choice and return to the **SOS Settings** page. The alert is now linked to the division on the **SOS Settings** page.

Note: If no variables are saved to your chosen alert, a message warns you there are no message variables in your selected SOS alert. You must edit the alert using the **Back to Alert** button or select a different alert with incident-specific message variables. If you ignore the warning and save the alert without the incident-specific variables, any SOS reported with that alert will have a blank message.



The linked alert next to the division on the **SOS Settings** page can also be deleted by selecting the X.

SOS Settings

ASSIGN ALERTS TO DIVISION
SOS desktop tool & mobile app feature will be enabled for users under assigned division.

- ▼ OnSolve Jane Erstwhile Earthquake
- Austen Company +
- East Coast Office +
- West Coast Office +

Create a New SOS Alert

To create a new alert from scratch and assign it to a division

1. Select the + add icon next to the division on the **SOS Settings** page and choose **+Create New Alert**.



The **Create SOS Alert** page opens.

The screenshot displays the "Create SOS Alert" page with a clean, modern design. It features three main sections: "Alert Details" (blue header), "Recipients" (blue header), and "Response Options", "Delivery Methods", and "Advanced Settings" (all grey headers). The "Alert Details" section contains fields for "Alert Name" (set to "SOS ALERT"), "Alert Description" (with placeholder "Enter alert description"), and "Division" (set to "ABC Corporation"). The "Delivery Methods" section shows "12 (All)" selected. The "Advanced Settings" section has an "Edit" button. Below the main sections, there's a summary bar with "Alert Details" expanded, showing "Alert Name: SOS ALERT", "Alert Description: Enter alert description", and a dropdown for "Division". To the right, a modal window titled "Insert Variable Token" lists tokens like "Date", "Incident Location", "Sender Name", and "User Contact".

This screenshot provides a detailed view of the "Alert Details" configuration. It includes fields for "Alert Name" (SOS ALERT), "Alert Description" (empty), "Division" (ABC Corporation), and "Delivery Methods" (12 (All)). The "Advanced Settings" section is visible at the bottom. A modal window on the right is titled "Insert Variable Token" and lists tokens such as "Date", "Incident Location", "Sender Name", and "User Contact". At the bottom, there's a "Filekick Message" section with a file upload area and a note about file size limits.

2. Select **Add Details**.

3. Add the **Alert Name**, **Alert Description**, and **Division**.
4. Within the **Message Body**, select **+Insert Variables** to add all variable tokens. All suggested variables are necessary for incident-based reporting and must be added to the SOS alert, or the delivered message will be blank. To create a custom variable, see [Alert Variables](#) in Section 3 of this guide for more information.



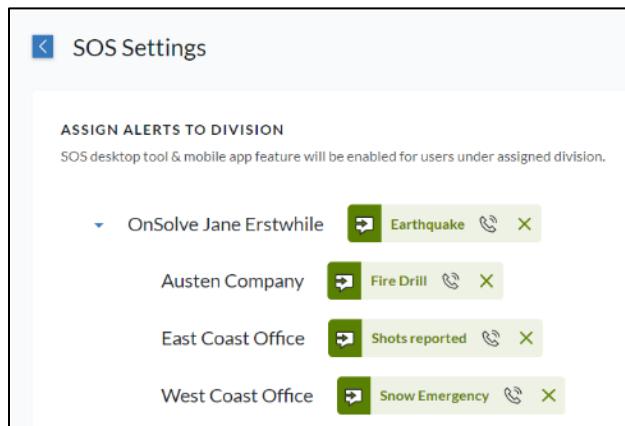
Note: If no variables are saved to your chosen alert, a warning will allow you to edit the alert using the **Back to Alert** button. If you ignore the warning and save the alert without the incident-specific variables, any SOS reported with that alert will have a blank message.

5. Select **Save**. The added variables are now associated with **Alert Details**.
6. Add **Recipients**, **Delivery Methods**, **Response Options**, and **Advanced Settings** as desired.
7. Select **Save** after defining the required sections. Your alert is added to the division on the **SOS Settings** page.

Note: You cannot create a new SOS alert from the **Alerts** page since the incident-specific variables only exist within the **Incident Management** tool.

8. Assign additional alerts to available divisions.

After all alerts have been defined in **SOS Settings**, designated users will receive alerts based on the assigned division when an SOS incident is triggered via the mobile app.



Division	Status
OnSolve Jane Erstwhile	Earthquake
Austen Company	Fire Drill
East Coast Office	Shots reported
West Coast Office	Snow Emergency

SOS Incidents

View all active and complete SOS incidents from **Incident Management > SOS**. The **SOS Incidents** page opens.

SOS Incidents							 SOS SETTINGS
Search Incidents							 
<input type="checkbox"/>	CONTACT POINT	LOCATION	DATE SUBMITTED	SENDER	STATUS		ANALYTICS
<input type="checkbox"/>	SOS - Thomas Ferg	47HRC96X+XC	Nov 8, 2021 1:48 PM	Thomas Ferg	Active		
<input type="checkbox"/>	SOS - Thomas Ferg	140 Limewood Pl, Ormond Beach, FL 32174, USA	Nov 8, 2021 1:43 PM	Thomas Ferg	Active		
<input type="checkbox"/>	SOS - britney commander	140 Limewood Pl, Ormond Beach, FL 32174, USA	Nov 8, 2021 1:41 PM	britney commander	Active		
<input type="checkbox"/>	SOS - britney commander	140 Limewood Pl, Ormond Beach, FL 32174, USA	Nov 8, 2021 1:36 PM	britney commander	Active		

Columns displayed for SOS Incidents are:

- **Contact Point:** The incident name.
- **Location:** The location of the user at the time of the incident. If location permissions are disabled on the mobile device, only the country name is reported.
- **Date Submitted:** The date and time the incident is reported.
- **Sender:** The mobile sender of the incident.
- **Status:** The status of the incident. This status is either **Active** or **Completed**.
- **Analytics:** Select the icon for all incident details. See [Analytics](#) in Section 4 of this guide for more information.

SOS in OnSolve Mobile

As stated in [Configure SOS Settings](#), you must first configure SOS from **Incident Management**. Administrators and authorized users can view and access Incident Management in the OnSolve Mobile app through the Sender app login.

Once configured, you can view the SOS button in the OnSolve Mobile and use the SOS feature within the Recipient and Sender app view. Additionally, if you access the OnSolve Mobile with a username and password, you can use the Life Check feature from the Recipient view of the Sender app.

Review the current *OnSolve Mobile Guide* for more information on the SOS and Life Check features within OnSolve Mobile.

Lockbox

The Lockbox feature allows authorized users to upload files that can then be attached to an alert. Users can upload secure, encrypted files that can be sent to mobile app users only, as well as shared files that are accessible via any text-based delivery method. Supported file types are .csv, .doc, .pdf, .xls, .xlsx, .jpeg, and .png.

Notes

Specific permissions are required to create, send, and view an alert with an attached Lockbox file:

- To create an alert with an attached Lockbox file, the creator needs the Lockbox Shared/Secured **Create** divisional permission.
- To send an alert with an attached Lockbox file, the sender needs the Lockbox Shared/Secured **View** divisional permission.
- To view a shared Lockbox file, a recipient needs the **Web Login** global permission.
- To view a secure Lockbox file, a recipient needs the **Web Login** global permission and access to OnSolve Mobile.

Upload Files to the Lockbox

To upload files

1. Navigate to **Incident Management > Lockbox** and select **Upload File**.

2. Drag and drop your file or select **Browse** to upload the file from your computer.

Notes

Accepted file types are: .csv, .doc, .pdf, .xls, .xlsx, .jpeg, and .png. The maximum accepted file size is 25MB.

While unlimited files can be added to the Lockbox, only one can be uploaded at a time.

Upload File to Lockbox

Upload a file to Lockbox to use as an attachment to an alert at a later time. Supports: .csv, .doc, .pdf, .xls, .xlsx, .jpeg, and .png



Drop your file here, or [Browse](#)

Maximum file size: 25 MB

3. Select **Next**.
4. Assign a **Security Type** to control how the file is viewed and encrypted.
 - Choose **Shared** if you want the file to be accessible by alert senders via both the OnSolve web UI and the mobile app.
 - Choose **Secure** if you want the file to be accessible by alert senders via only the mobile app.

Security Type

Select security type ▾

Shared

Lockbox shared files can be accessed through both the web version and the mobile app.

Secure

Lockbox secure files can only be accessed through the mobile app.

5. Select the division to which this file should be shared.



6. Select **Done**.

7. Select **Back to Lockbox** to see the file in the list of Lockbox files.

<input type="checkbox"/>	FILE NAME	TYPE	DIVISION	UPLOADED BY	LAST MODIFIED	HISTORY	ACTION
<input type="checkbox"/>	PT 12.28.21.png	Shared	por [REDACTED]	Por [REDACTED]	Jan 5, 2022 11:35 AM		
<input type="checkbox"/>	Receipts 12.29.21.pdf	Secure	po [REDACTED]	Por [REDACTED]	Jan 5, 2022 11:31 AM		

Manage Lockbox Files

Authorized users can manage lockbox files from the **Incident Management > Lockbox** page.

<input type="checkbox"/>	FILE NAME	TYPE	DIVISION	UPLOADED BY	LAST MODIFIED	HISTORY	ACTION
<input type="checkbox"/>	PT 12.28.21.png	Shared	portiaz	Portia Zwicker	Jan 5, 2022 11:35 AM		
<input type="checkbox"/>	Receipts 12.29.21.pdf	Secure	portiaz	Portia Zwicker	Jan 5, 2022 11:31 AM		

Search, Sort, and Filter

- Use the **Search** field to search for lockbox files by **File Name** keyword.
- **Sort** lockbox files by **File Name**, **Type**, **Uploaded By**, and **Last Modified**.
- **Filter** lockbox files by **Division**, **File Name**, **Last Modified**, **Type**, and **Uploaded By**. Select up to three filters and select **Apply Filters**.

History

Look for the History option in a future update.

Download

Under the Action column, you can download any share lockbox files. Secure files cannot be downloaded.

Delete

Delete lockbox files by selecting the checkbox next to the desired file(s) and selecting **Delete**.

View and Edit Details

Select any file to view the file's details.

File Details

Last Modified
Jan 5, 2022 11:35 AM

Uploaded By
P [REDACTED] Z [REDACTED]

File Type
PNG

File Size
433.92 KB

Security Type
Shared ▾

Division
p [REDACTED] ▾

CANCEL SAVE

Authorized users can change the **Security Type** from **Shared** to **Secure** or vice versa and edit the **Division**. When done, select **Save**.

Retrieve Lockbox Files

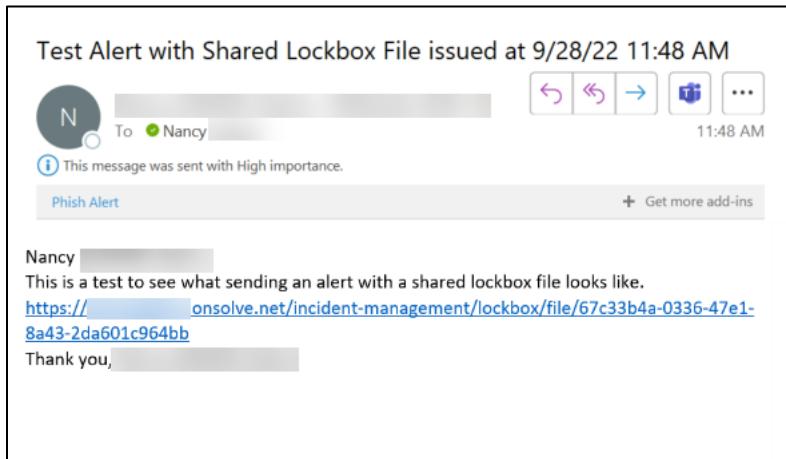
The Lockbox file retrieval experience is slightly different when retrieving a shared lockbox file compared to a secure lockbox file:

- Recipients with permission to view shared files can view and download **all** shared files saved in the Lockbox and can navigate to other pages throughout the interface that they have access to view.
- Recipients with permission to view secure files can only view the specific file attached to the alert they received and only via OnSolve Mobile. These recipients can access the secure file by opening the alert from the alert inbox and tapping on the file link under the **Attachments** heading (as long as they are logged in with their username and password).

Shared Lockbox

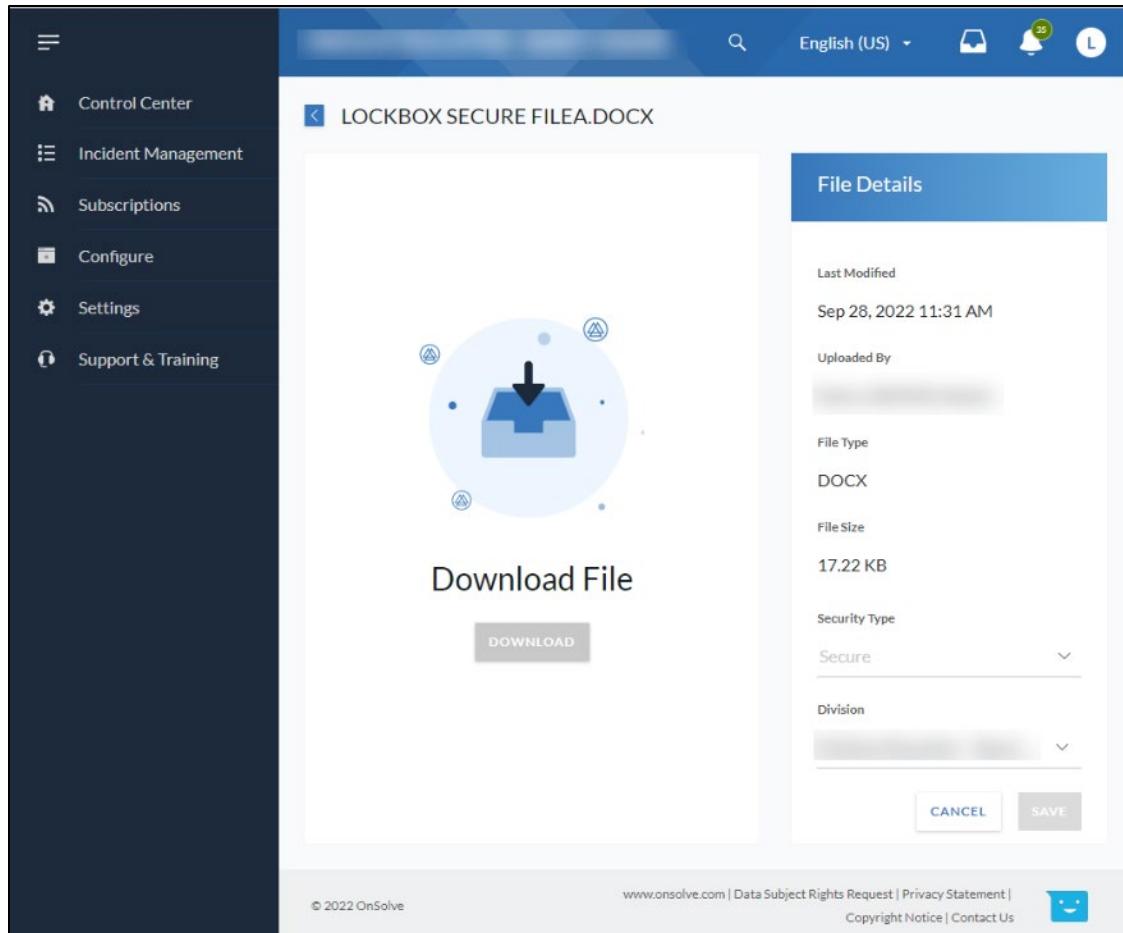
To retrieve a shared lockbox file

1. Click the link in the alert to open a browser window that displays the OnSolve login page.



2. Enter your username and password. Or, if SSO is enabled, select the **Sign in with Organization Credentials** button.

3. Once the file download page displays, select **Download** to initiate a download of the file to your computer.



The file saves to the **Downloads** folder on your computer.

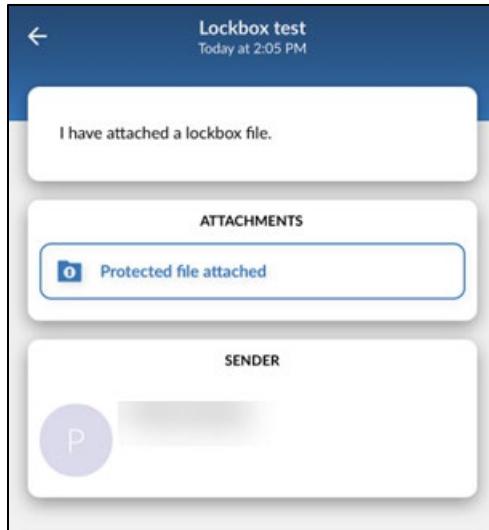
4. Select **Cancel**. The **Lockbox** page is displayed with access to all files you have permission to view.

Secure Lockbox via OnSolve Mobile

To view a secure lockbox file via OnSolve Mobile

1. Tap the push notification to view the alert. If you are logged in with a username and password, the app opens to display the alert.

2. Tap **Protected file attached** under **Attachments** to view the secure file.



If you are logged in via the SMS or email verification method, you must sign out and log in with your username and password.

- a. From the **File Protected** window, tap **Confirm, Sign Out**.



- b. Sign in with your username and password. The alert opens, and you can tap **Protected file attached** to view the secure file.

Section 6: Subscriptions

Overview

Subscriptions provide a way to send alerts according to an area of interest, be it a topic or a specific weather event. The Subscriptions page also allows administrators to set up Text-to-Keyword so that recipients can easily update their contact information or sign up to get alerts related to their location.

Weather & Events

The Weather & Events® feature is a subscription-based service that allows users to set up automated, system-generated alerts based on weather conditions in specific locations.

Weather & Events is a premium feature that must be enabled on the account. Weather & Events is on the left navigation menu under **Subscriptions > Weather & Events**.

Subscriptions combine locations and profiles to define when an alert should be sent and to whom. To receive Weather & Events alerts, at least one subscription must be enabled. Select specific options. Combine one or more profiles with one or more locations. Then determine which groups should be included in the subscription.

Create a Profile

A profile defines the specific weather or civil emergency conditions to be monitored. Profiles can be broad, including many different weather conditions or specific conditions (one for high wind conditions, one for heat conditions, etc.) Examples: Tropical Storm Warning, Severe Thunderstorm Advisory, Ice Storm Watch, etc.

Integrating with the Weather Company allows for the delivery of location-specific data with profiles unique to each region, spanning multiple countries.

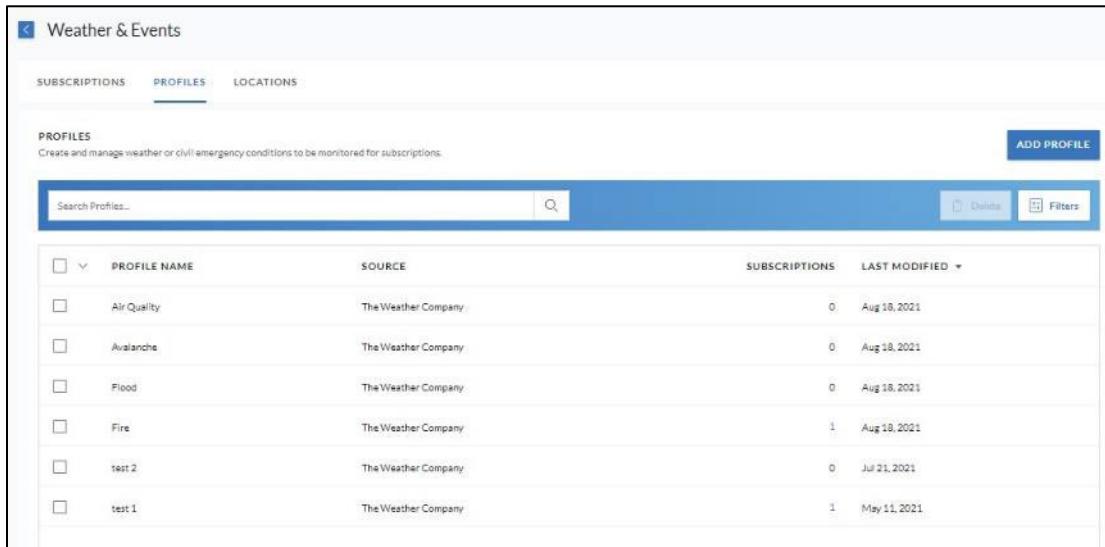
The default regions for Weather & Events are the United States, Canada, the Commonwealth of Puerto Rico, the Northern Mariana Islands, the US Territories of American Samoa, Guam, and the US Virgin Islands. Additional regions available at an added contractual cost include Australia, Japan, and Europe.

The countries included in the “Europe” region for Weather & Events are:

Belgium	Hungary	Netherlands
Bosnia-Herzegovina	Iceland	Norway
Bulgaria	Ireland	Poland
Croatia	Italy	Portugal
Cyprus	Latvia	Romania
Czech Republic	Lithuania	Serbia
Denmark	Luxemburg	Slovenia
Estonia	Macedonia	Spain
Finland	Malta	Sweden
France	Moldova	Switzerland
Germany	Montenegro	United Kingdom
Greece		

To create a profile

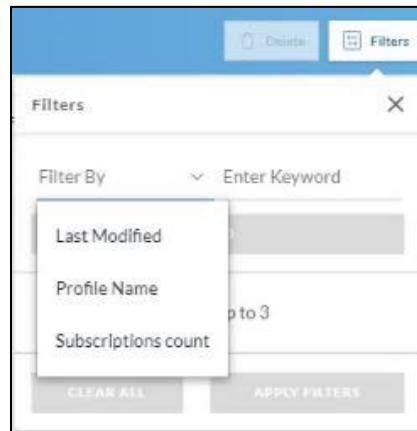
1. Select **Subscriptions > Weather & Events** on the left navigation menu and choose the **Profile** tab. The **Profiles** page opens with all profiles created for the account.



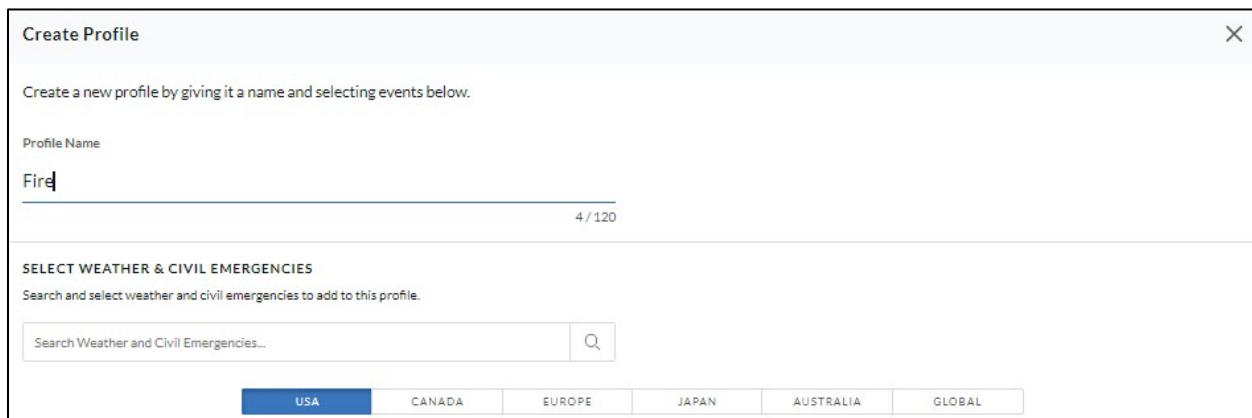
PROFILE NAME	SOURCE	SUBSCRIPTIONS	LAST MODIFIED
Air Quality	The Weather Company	0	Aug 18, 2021
Avalanche	The Weather Company	0	Aug 18, 2021
Flood	The Weather Company	0	Aug 18, 2021
Fire	The Weather Company	1	Aug 18, 2021
test 2	The Weather Company	0	Jul 21, 2021
test 1	The Weather Company	1	May 11, 2021

- Sort **Profile Name** or **Last Modified** date columns in ascending or descending order by clicking the arrow next to each column header.

- Filter profiles by **Last Modified**, **Profile Name**, or **Subscriptions count**.



- The **Source** column displays the source information for the Weather & Civil Emergencies alert subscription profile types.
 - The **Subscriptions** column displays the number of subscriptions associated with the profile.
2. Select **Add Profile** to create a new profile on the **Profiles** page or when creating a new subscription.
 3. Enter a **Profile Name** (maximum of 120 characters).



Create Profile

Create a new profile by giving it a name and selecting events below.

Profile Name

Fire 4 / 120

SELECT WEATHER & CIVIL EMERGENCIES

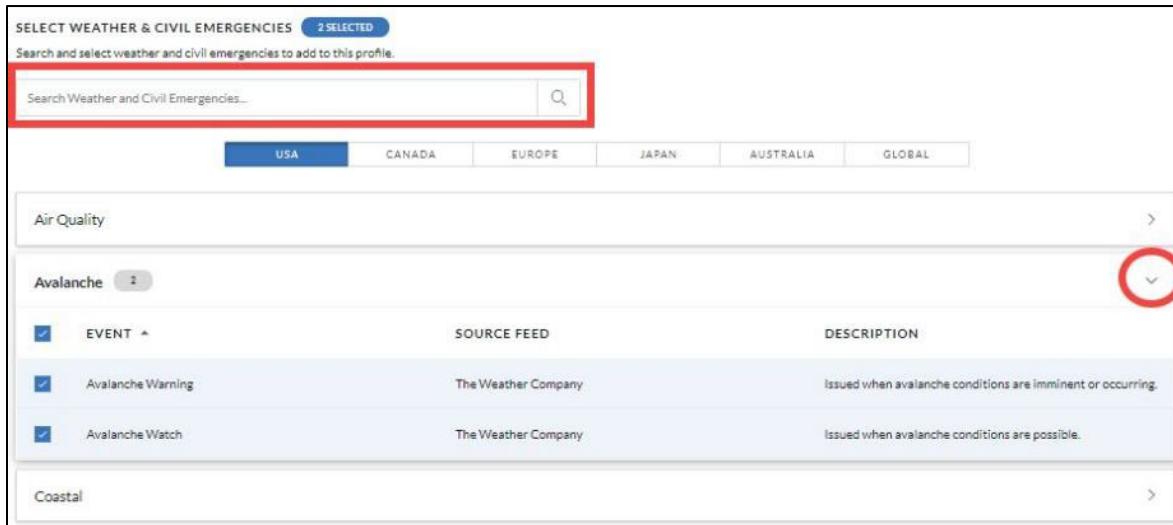
Search and select weather and civil emergencies to add to this profile.

Search Weather and Civil Emergencies...

USA	CANADA	EUROPE	JAPAN	AUSTRALIA	GLOBAL
-----	--------	--------	-------	-----------	--------

4. Choose the region(s) (USA, Canada, Europe, Japan, Australia) desired from the countries configured for the account.

5. Choose the event profiles for each region by entering keywords into the search field or by expanding each category menu by selecting the arrows to the right. Add individual events and conditions by selecting the checkbox to the left of the event. See [Appendix C](#) in this guide for a list of all Weather & Events event types.



The screenshot shows a user interface for selecting weather and civil emergencies. At the top, a header reads "SELECT WEATHER & CIVIL EMERGENCIES" with "2 SELECTED". Below it is a search bar with placeholder text "Search and select weather and civil emergencies to add to this profile." and a magnifying glass icon. A red box highlights the search bar. Below the search bar is a row of buttons for regions: USA (selected), CANADA, EUROPE, JAPAN, AUSTRALIA, and GLOBAL. The "USA" button is highlighted with a blue background. Under the "USA" section, there is a heading "Air Quality" followed by a collapsed section "Avalanche" indicated by a downward arrow. A red circle highlights this arrow. Inside the "Avalanche" section, there is a table with columns "EVENT", "SOURCE FEED", and "DESCRIPTION". Two items are listed: "Avalanche Warning" (Source: The Weather Company) and "Avalanche Watch" (Source: The Weather Company). Both rows have a checked checkbox in the "EVENT" column. The "DESCRIPTION" column provides details: "Issued when avalanche conditions are imminent or occurring." for the warning and "Issued when avalanche conditions are possible." for the watch. Below the "Avalanche" section is another collapsed section "Coastal" with a right-pointing arrow.

As you select events, the **Select Weather & Civil Emergencies** header reflects the total number of events selected for the profile by type and across all regions.

6. After you select all alerts for the individual profile requirements, select **Create** to save the profile (or **Add** to save during the create subscription process) and return to the **Profiles** page.

Once a profile is created, it can be selected for a subscription.

Alert Types

Watch

A watch is used when the risk of hazardous weather or hydrologic event has increased significantly, but its occurrence, location, or timing is still uncertain. It is intended to provide enough lead time, so those who need to set their plans in motion can do so.

Advisory

Highlights special weather conditions that are less serious than a warning. They are for events that may cause significant inconvenience, and if caution is not exercised, it could lead to situations threatening life or property.

Warning

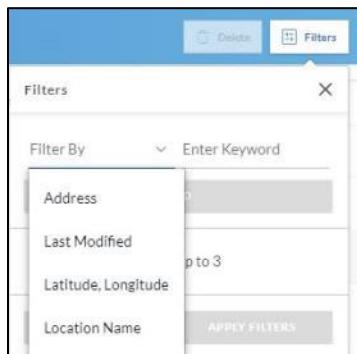
A warning is issued when a hazardous weather or hydrologic event occurs, is imminent, or has a very high probability of occurring. A warning is used for conditions posing a threat to life or property.

Create a Location

A location is any defined place where adverse weather conditions or in-progress/imminent threats to public safety need to be monitored to maintain emergency preparedness. Alerts are received when the Weather Company issues a warning, watch, or other emergency notification that corresponds to the selected events and conditions in the recipient's profile, and the recipient is within the polygon that was dynamically created for the weather event and projected path.

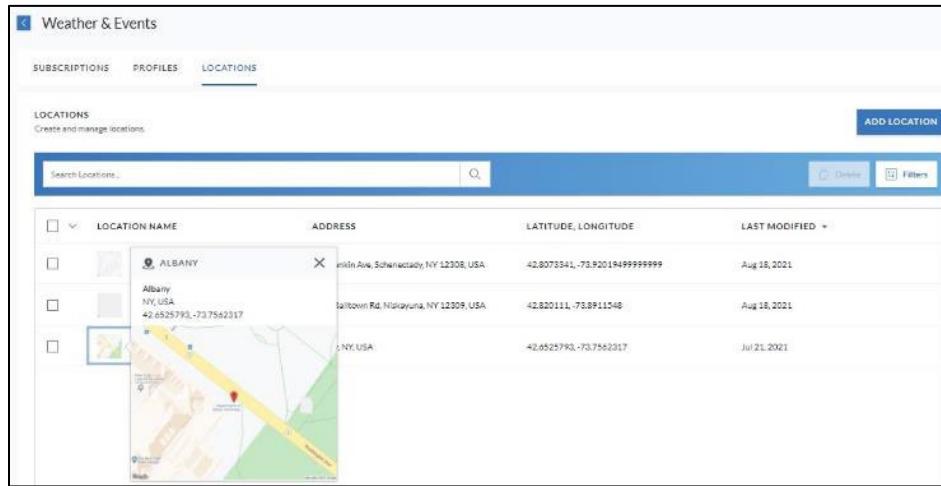
Although this varies by alert type, it is imperative to specify the location as accurately as possible to receive the appropriate alerts.

- Select **Subscriptions > Weather & Events** on the left navigation menu, and then the **Locations** tab. The **Locations** page displays all locations created for the account that can be used to create subscriptions.
- Sort **Location Name** or **Date Modified** in ascending/descending order by clicking the arrow in each column header.
- Filter locations by **Address**, **Last Modified**, **Latitude/Longitude**, and **Location Name**.



- Review **Address** information, including **Latitude** and **Longitude** for each location.

- Click on the **Locations** icon next to each address to view the map and address details for the location.



The screenshot shows the 'Weather & Events' interface with the 'LOCATIONS' tab selected. At the top, there's a search bar labeled 'Search Locations...' and a blue 'ADD LOCATION' button. Below the search bar is a table with columns: 'LOCATION NAME', 'ADDRESS', 'LATITUDE, LONGITUDE', and 'LAST MODIFIED'. The table contains three entries, all of which have a small map icon next to them. The first entry is 'ALBANY' with the address '100 Washington Ave, Schenectady, NY 12308, USA' and coordinates '42.8073341,-73.92019499999999'. The second entry is 'Talltown Rd, Niskayuna, NY 12309, USA' with coordinates '42.820111,-73.8911548'. The third entry is 'NY, USA' with coordinates '42.6525793,-73.7562317'. The bottom right corner of the screenshot shows a small map preview.

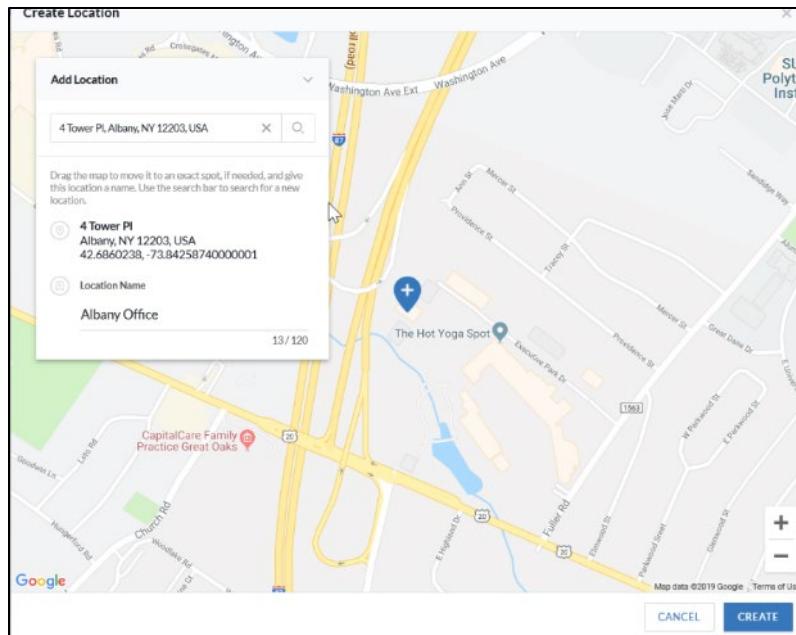
LOCATION NAME	ADDRESS	LATITUDE, LONGITUDE	LAST MODIFIED
ALBANY	100 Washington Ave, Schenectady, NY 12308, USA	42.8073341,-73.92019499999999	Aug 18, 2021
	Talltown Rd, Niskayuna, NY 12309, USA	42.820111,-73.8911548	Aug 18, 2021
	NY, USA	42.6525793,-73.7562317	Jul 21, 2021

To create a location

- Select **Add Location** on the **Locations** page. The **Create Location** page opens with a map and prompt requesting access to your location information.
 - If allowed, your location is displayed on the map.
 - If blocked, your account address from the **My Information** page is displayed on the map. If no account address exists, the OnSolve headquarters is displayed on the map:

6240 Avalon Blvd. Alpharetta, GA 30009

2. Use the predictive search bar to find an address by typing an address in the text box. Drag the map tool to move to an exact address, if necessary. The new address coordinates are displayed.

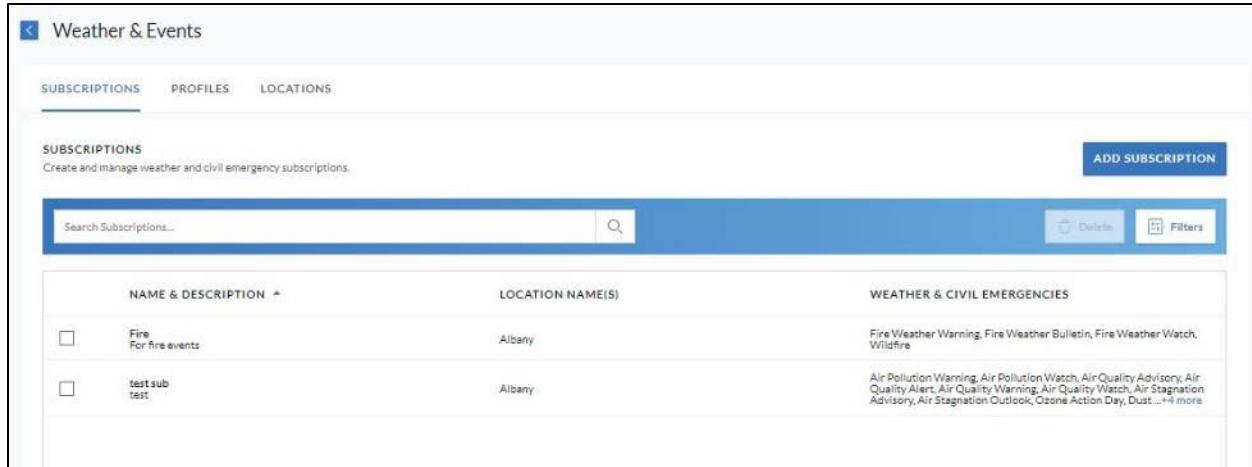


3. Add the new **Location Name** in the dialog box provided.
4. Select **Create** to save the new location (or **Add** to save during the create subscription process).

Create a Subscription

Select **Subscriptions > Weather & Events** on the left navigation menu to view a list of all existing weather subscriptions in the account on the **Subscriptions** page.

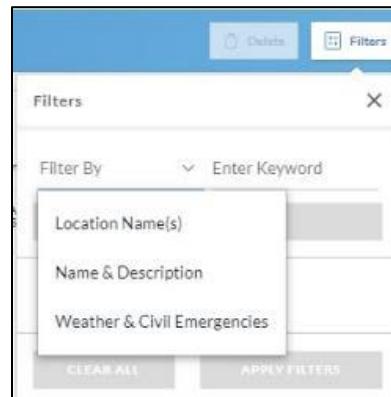
The **Subscriptions** page displays the account's subscriptions by **Name & Description**, **Location Name(s)**, and **Weather & Civil Emergencies**.



The screenshot shows the 'Weather & Events' interface with the 'SUBSCRIPTIONS' tab selected. At the top right is a blue 'ADD SUBSCRIPTION' button. Below it is a search bar and filter buttons ('Delete' and 'Filters'). The main area displays a table of subscriptions:

NAME & DESCRIPTION	LOCATION NAME(S)	WEATHER & CIVIL EMERGENCIES
<input type="checkbox"/> Fire For fire events	Albany	Fire Weather Warning, Fire Weather Bulletin, Fire Weather Watch, Wildfire
<input type="checkbox"/> test sub test	Albany	Air Pollution Warning, Air Pollution Watch, Air Quality Advisory, Air Quality Alert, Air Quality Warning, Air Quality Watch, Air Stagnation Advisory, Air Stagnation Outlook, Ozone Action Day, Dust...+4 more

- The **Name & Description** column displays the account's Weather & Civil Emergencies subscriptions. Select a subscription to view the details, including an **Overview**, **Profiles**, **Locations**, and **Groups**.
- Sort **Name & Description** in ascending or descending order by clicking the arrow in the column header.
- Filter subscriptions by **Location Name(s)**, **Name & Description**, and **Weather & Civil Emergencies**.

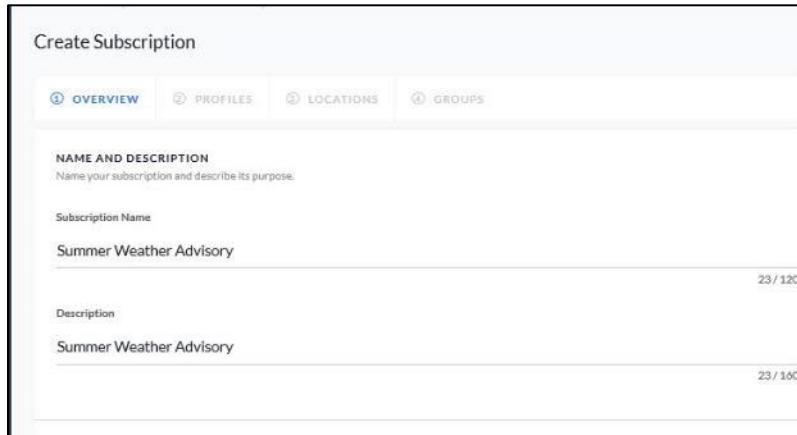


- Location Name(s)** consists of the defined Subscription location(s).

- The **Weather & Civil Emergencies** column consists of the defined alert subscription types.
- Click anywhere in a subscription row to view or modify subscription components.
- Select the **checkbox** and then **Delete** to delete a subscription.

To create a subscription

1. Select **Add Subscription** on the **Subscriptions** page. The **Create Subscription Overview** page opens.



The screenshot shows the 'Create Subscription' interface. At the top, there are four tabs: OVERVIEW (selected), PROFILES, LOCATIONS, and GROUPS. Below the tabs, under 'NAME AND DESCRIPTION', there is a placeholder 'Name your subscription and describe its purpose.' A 'Subscription Name' field contains 'Summer Weather Advisory'. To the right of this field is a character count indicator '23 / 120'. Below the name field is a 'Description' field containing 'Summer Weather Advisory', with a character count indicator '23 / 160'.

2. Enter the **Subscription Name** and **Description**. This name should be an identifier, not a specific address. The **Subscription Name** is limited to 120 characters, and the **Description** is limited to 160 characters.

3. Define Subscription Options.

Create Subscription

OVERVIEW **PROFILES** **LOCATIONS** **GROUPS**

NAME AND DESCRIPTION
Name your subscription and describe its purpose.

Subscription Name
Enter subscription name 0 / 120

Description
Enter description 0 / 160

SUBSCRIPTION OPTIONS
Set status and configure alert options for this subscription. When enabled, the subscription is active and alerts will be sent. When disabled, the subscription is inactive but saved, and alerts will not be sent.

Subscription Status

Alert Options

- Apply Delivery Options**
Select an alert to apply its device priority and alert configuration settings to this subscription. When deselected, the subscription will use default system settings.
- Ignore Updates**
When selected, no updates will be received after the initial alert. When deselected, all updates will be received as separate alerts.
- Ignore Cancellations**
When selected, notice of an alert cancellation will not be sent.
- Call to Action**
Custom text that will be appended at the end of the National Weather Service message.
- Response Options**
Include custom text, such as a question, to request a response from the alert recipient.
- Silent Periods**
Alerts are not delivered during silent periods.

a. Subscription Status

Subscription Status can be enabled or disabled. When enabled (with the **Subscription Status** toggle on), the subscription is active, and alerts are sent. When disabled (with Subscription Status toggle off), **Alert Options** cannot be selected, the subscription is saved but not active, and alerts are not sent.

SUBSCRIPTION OPTIONS
Set status and configure alert options for this subscription. When enabled, the subscription is active and alerts will be sent. When disabled, the subscription is inactive but saved, and alerts will not be sent.

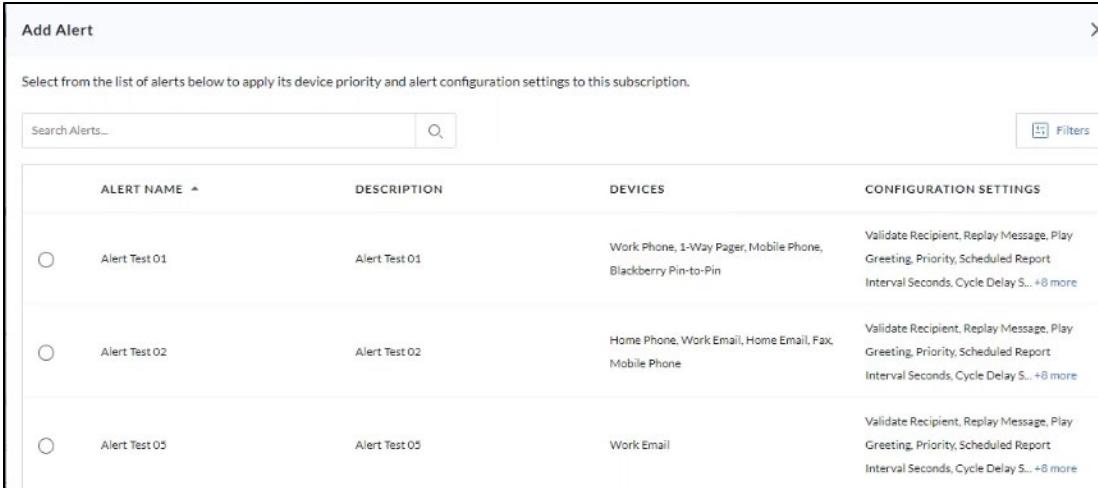
Subscription Status

b. Alert Options

- **Apply Delivery Options** allows the user to select an alert to apply its device priority and alert configuration settings to this subscription. When deselected, the subscription uses default settings. To apply an alert's settings:

1. Select the Apply Delivery Options checkbox.

2. Select **+ Add Alert**. The **Add Alert** window opens, displaying all saved alerts, their descriptions, saved devices, and configuration settings. If you do not have any saved alerts, you will have the opportunity to create one.

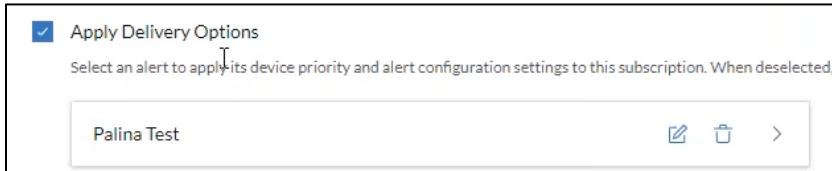


The screenshot shows the 'Add Alert' window with a title bar 'Add Alert' and a close button 'X'. Below the title bar is a search bar with placeholder 'Search Alerts...' and a magnifying glass icon. To the right of the search bar is a 'Filters' button. The main area contains a table with four columns: 'ALERT NAME', 'DESCRIPTION', 'DEVICES', and 'CONFIGURATION SETTINGS'. There are three rows of data:

ALERT NAME	DESCRIPTION	DEVICES	CONFIGURATION SETTINGS
Alert Test 01	Alert Test 01	Work Phone, 1-Way Pager, Mobile Phone, BlackBerry Pin-to-Pin	Validate Recipient, Replay Message, Play Greeting, Priority, Scheduled Report Interval Seconds, Cycle Delay S... +8 more
Alert Test 02	Alert Test 02	Home Phone, Work Email, Home Email, Fax, Mobile Phone	Validate Recipient, Replay Message, Play Greeting, Priority, Scheduled Report Interval Seconds, Cycle Delay S... +8 more
Alert Test 05	Alert Test 05	Work Email	Validate Recipient, Replay Message, Play Greeting, Priority, Scheduled Report Interval Seconds, Cycle Delay S... +8 more

3. Select an alert and select **Add**.

To change the applied alert, select the edit icon. The **Edit Alert** window opens, and a different alert can be applied. To remove the applied alert, select the delete icon.



The screenshot shows the 'Edit Alert' window. At the top left is a checked checkbox labeled 'Apply Delivery Options'. Below it is a note: 'Select an alert to apply its device priority and alert configuration settings to this subscription. When deselected, no updates will be received after the initial alert.' In the center is a list box containing 'Palina Test'. At the bottom right are three icons: a pencil for edit, a trash can for delete, and a right-pointing arrow for next.

With **Ignore Updates** selected, Weather & Events does not send multiple updates during an emergency. When this option is selected, no updates will be received after the initial alert. When deselected, all updates are received as separate alerts.

With **Ignore Cancellations** selected, Weather & Events will not send notice of an alert cancellation. For example, if The Weather Company issues a cancellation of a High Wind Warning, the cancellation alert will not be sent to the recipients who received the original warning.

The **Call to Action** option defines a custom message to be added to the received auto-generated weather alert. Calls to Action can provide organization-specific instructions (evacuation, office closures, etc.) to inform recipients how to handle the specific event. A **Call to Action** may be used with or without the **Request Response** option. There is a 250-character limit for the **Call to Action** field.

Response Options allow recipients to reply to the alert using custom text. Responses may only be received using standard two-way communication, such as live telephone calls, SMS,

and email. Select the **ADD RESPONSE OPTION** to add additional custom text. There is a 120-character limit for each field.

SUBSCRIPTION OPTIONS

Set status and configure alert options for this subscription. When enabled, the subscription is active and alerts will be sent. When disabled, the subscription is inactive but saved, and alerts will not be sent.

Subscription Status

Alert Options

Apply Delivery Options
Select an alert to apply its device priority and alert configuration settings to this subscription. When deselected, the subscription will use default system settings.

Ignore Updates
When selected, no updates will be received after the initial alert. When deselected, all updates will be received as separate alerts.

Ignore Cancellations
When selected, notice of an alert cancellation will not be sent.

Call to Action
Custom text that will be appended at the end of the National Weather Service message.

Response Options
Include custom text, such as a question, to request a response from the alert recipient.

Note: The Weather & Events alert message body for SMS and Voice has a 1000-character limit. For example, if the Call to Action has 100 characters, the message body of the Weather & Events alert is limited to 900 characters. Alerts sent to contact points other than SMS and voice do not have a character limit.

To create response options

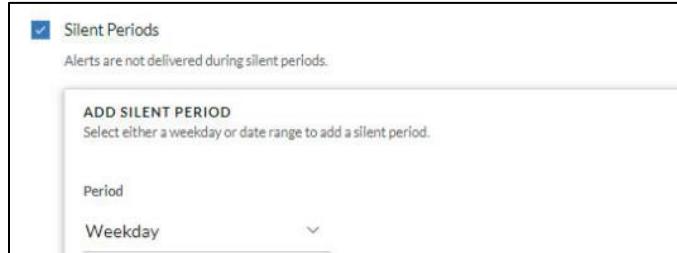
1. Select the checkbox to expand the section. As with response options, the number of response options depends on the account settings, with a maximum of five available.
2. Enter the response options, if required, for the alert. Each response can have up to 120 characters.

Note: Must be used in conjunction with Call to Action.

Define any **Silent Periods**, the specific day(s) or date range, when Weather & Events alerts should not be sent.

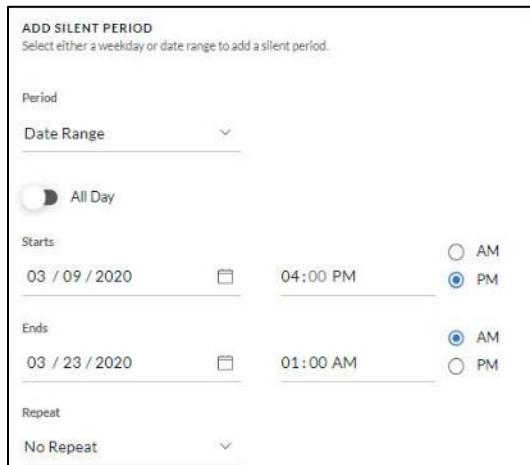
- Select the checkbox to expand the selection and choose **Weekday** for specific days of the week or a **Date Range**.

- When **Weekday** is selected from the drop-down list, choose the individual **Weekday(s)**, **All Day** (if required), **Start Time**, and **End Time**. No alerts are sent at any time during those day(s). If the **All Day** toggle is enabled, no alerts are sent at any time on the selected day(s).



The screenshot shows a configuration panel for 'Silent Periods'. A checkbox labeled 'Silent Periods' is checked, with a note below stating 'Alerts are not delivered during silent periods.' Below this is a section titled 'ADD SILENT PERIOD' with the sub-instruction 'Select either a weekday or date range to add a silent period.' A dropdown menu labeled 'Period' is open, showing the option 'Weekday'.

- When **Date Range** is selected, choose the **Starts** and **Ends** dates and times. No alerts are sent at any time during those day(s).
- From the **Repeat** drop-down list, choose whether to repeat the Silent Period **Weekly** or **No Repeat**.



The screenshot shows a configuration panel for 'ADD SILENT PERIOD'. It includes a dropdown 'Period' set to 'Date Range'. Below it are fields for 'Starts' (date 03/09/2020, time 04:00 PM, AM/PM radio button selected) and 'Ends' (date 03/23/2020, time 01:00 AM, PM radio button selected). At the bottom is a dropdown 'Repeat' set to 'No Repeat'.

- After entering all desired options for the **Subscription Options**, select **Next** to save the Subscription **Overview** and continue to the **Profiles** page.



The screenshot shows a summary of subscription options. It includes a checked checkbox for 'Silent Periods' with the note 'Alerts are not delivered during silent periods.' Below this is a summary of the silent period: 'Jul 29, 2019 to Jul 31, 2019' and '06:00 AM to 05:00 PM'. At the bottom right is a small 'Edit' icon.

- Select profile(s) to add to the subscription or follow the steps in the [Create a Profile](#) section to create a new profile for the new subscription.
- Select **Next** to choose Locations.

6. Select location(s) to be monitored for this subscription on the **Locations** page or follow the [Create a Location](#) section steps to create a new location to add to the subscription.
7. Select **Next** to navigate to the **Groups** page. A list of all groups in the account will be displayed.
8. On the **Groups** page, choose any number of groups to receive the alerts in this subscription. The **Groups** page will include the **Group Name**, **Description** of the group, group **Type**, and **Contact Count**.

Create Subscription

✓ OVERVIEW ✓ PROFILES ✓ LOCATIONS ④ GROUPS

GROUPS
Select which groups of alert recipients will receive alerts for this subscription.

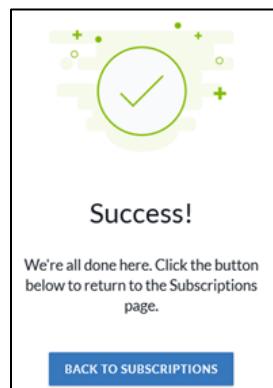
□ ▾ GROUP NAME	DESCRIPTION	TYPE	CONTACT COUNT
11111	Custom Group 1	Static	2
ABCGroup	Test Group	Static	1
AKZ195_group	Performance testing group for AKZ195	Static	0
AKZ195_group2	Performance testing group for AKZ195	Static	0
AKZ201_group	Performance testing group for AKZ201	Static	0
AKZ201_group2	Performance testing group for AKZ201	Static	0

Display 25 Entries (Showing 1 to 25 of 614 Results)

1 2 3 4 5 >

[GO BACK](#) [CANCEL](#) DONE

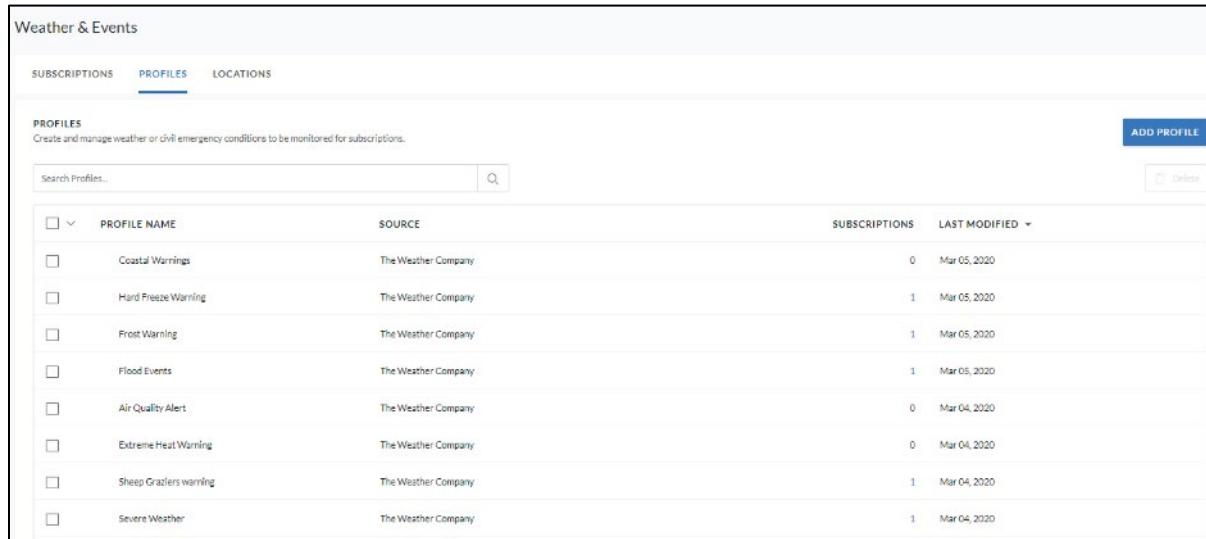
9. Select **Done** to save the new subscription. A confirmation message is displayed. Once saved, the subscription is available in the account until disabled or deleted by the administrator.



Alerts are automatically delivered to the groups specified in the subscription whenever The Weather Company (TWC) issues the corresponding alert type for the location(s) specified.

Modify a Profile

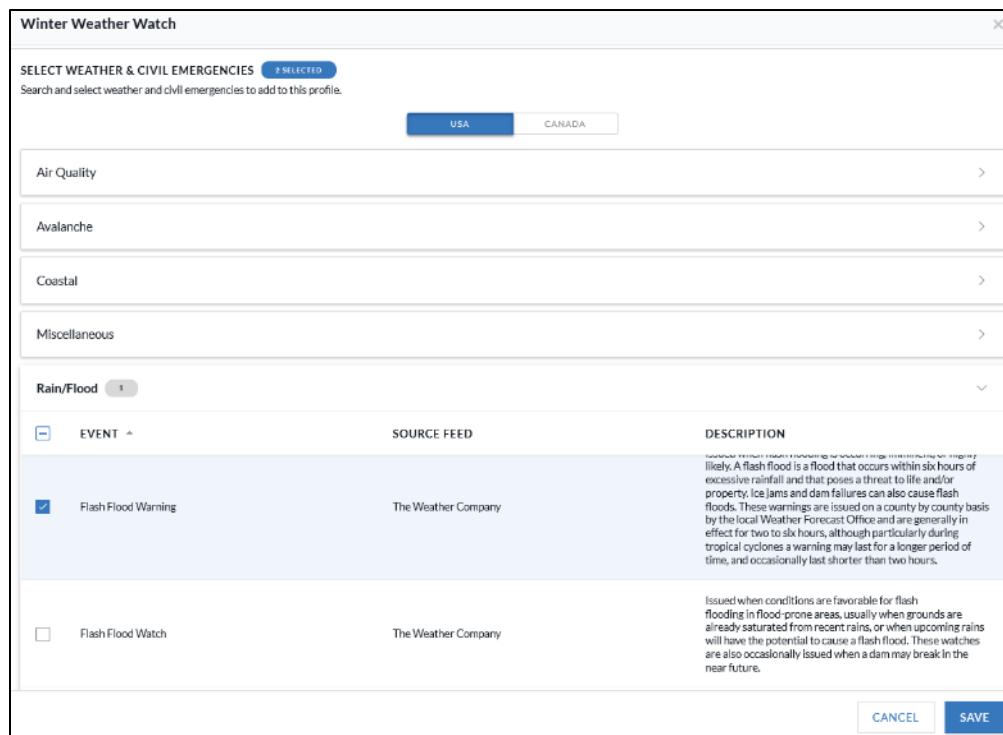
- Select the desired Profile on the **Profiles** page. The profile **Overview** window is displayed.



The screenshot shows the 'Weather & Events' interface with the 'PROFILES' tab selected. A search bar at the top allows for filtering profiles. Below the search bar is a table listing eight profiles, each with a checkbox, profile name, source, subscription count, and last modified date.

<input type="checkbox"/>	PROFILE NAME	SOURCE	SUBSCRIPTIONS	LAST MODIFIED
<input type="checkbox"/>	Coastal Warnings	The Weather Company	0	Mar 05, 2020
<input type="checkbox"/>	Hard Freeze Warning	The Weather Company	1	Mar 05, 2020
<input type="checkbox"/>	Frost Warning	The Weather Company	1	Mar 05, 2020
<input type="checkbox"/>	Flood Events	The Weather Company	1	Mar 05, 2020
<input type="checkbox"/>	Air Quality Alert	The Weather Company	0	Mar 04, 2020
<input type="checkbox"/>	Extreme Heat Warning	The Weather Company	0	Mar 04, 2020
<input type="checkbox"/>	Sheep Grazers warning	The Weather Company	1	Mar 04, 2020
<input type="checkbox"/>	Severe Weather	The Weather Company	1	Mar 04, 2020

- Edit the **Profile Name** or select additional events by checking the event box. Remove existing events by deselecting the event checkbox. A warning message is displayed when saving if no events are selected.



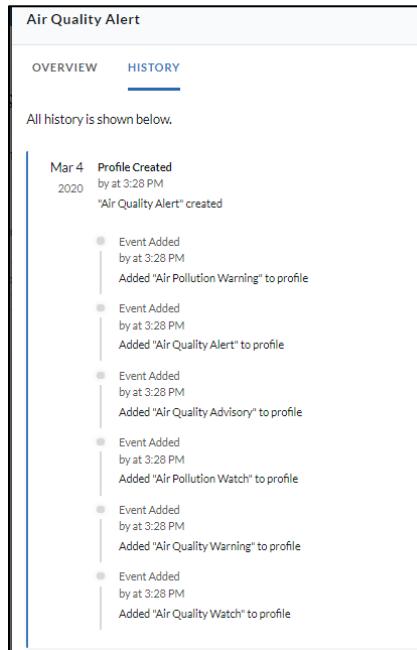
The screenshot shows the 'Winter Weather Watch' configuration window. At the top, it displays the selected weather and civil emergencies: '2 SELECTED'. Below this is a search bar and two tabs: 'USA' and 'CANADA'. The main area lists categories like Air Quality, Avalanche, Coastal, Miscellaneous, and Rain/Flood. Under the Rain/Flood category, there is a table showing events, source feed, and descriptions. The 'Flash Flood Warning' event is selected, indicated by a checked checkbox. The 'Flash Flood Watch' event is not selected, indicated by an unchecked checkbox.

<input type="checkbox"/>	EVENT	SOURCE FEED	DESCRIPTION
<input checked="" type="checkbox"/>	Flash Flood Warning	The Weather Company	Issued when there is a threat of flooding within six hours due to excessive rainfall. Flash floods can occur in urban areas and rural areas. They are issued on a county basis by the local Weather Forecast Office and are generally in effect for two to six hours, although particularly during tropical cyclones a warning may last for a longer period of time, and occasionally last shorter than two hours.
<input type="checkbox"/>	Flash Flood Watch	The Weather Company	Issued when conditions are favorable for flash flooding in flood-prone areas, usually when grounds are already saturated from recent rains, or when upcoming rains will have the potential to cause a flash flood. These watches are also occasionally issued when a dam may break in the near future.

- Select **Save** to save all changes.

View Profile History

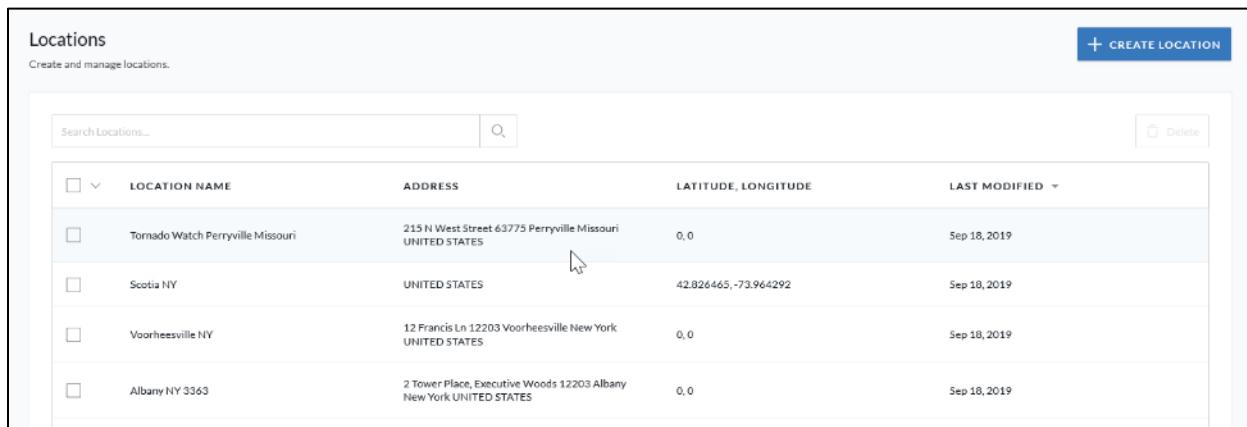
Select an individual profile on the **Profiles** page to review the history. Select the **History** tab on any existing profile to review all date and time, username, and event type modifications.



Date	Event Type	Details
Mar 4, 2020	Profile Created	by at 3:28 PM "Air Quality Alert" created
	Event Added	by at 3:28 PM Added "Air Pollution Warning" to profile
	Event Added	by at 3:28 PM Added "Air Quality Alert" to profile
	Event Added	by at 3:28 PM Added "Air Quality Advisory" to profile
	Event Added	by at 3:28 PM Added "Air Pollution Watch" to profile
	Event Added	by at 3:28 PM Added "Air Quality Warning" to profile
	Event Added	by at 3:28 PM Added "Air Quality Watch" to profile

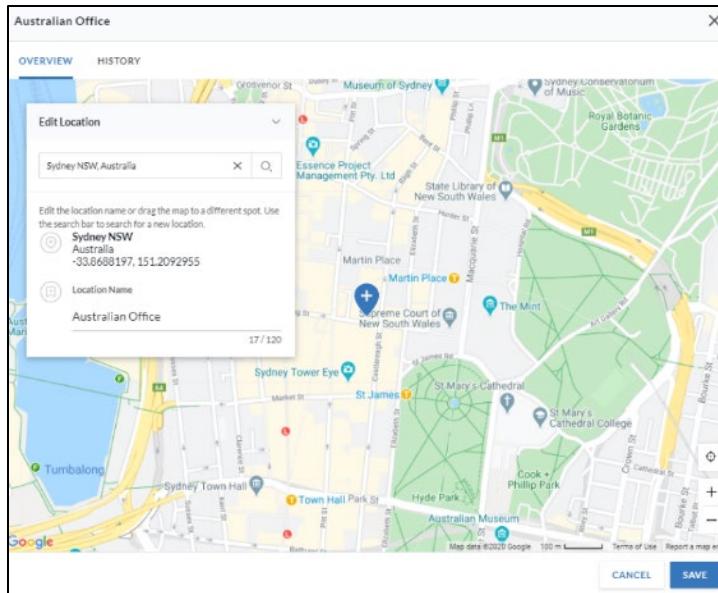
Modify a Location

1. Select the desired location on the **Locations** page. The profile **Overview** window is displayed.



<input type="checkbox"/>	LOCATION NAME	ADDRESS	LATITUDE, LONGITUDE	LAST MODIFIED
<input type="checkbox"/>	Tornado Watch Perryville Missouri	215 N West Street 63775 Perryville Missouri UNITED STATES	0,0	Sep 18, 2019
<input type="checkbox"/>	Scotia NY	UNITED STATES	42.826465, -73.964292	Sep 18, 2019
<input type="checkbox"/>	Voorheesville NY	12 Francis Ln 12203 Voorheesville New York UNITED STATES	0,0	Sep 18, 2019
<input type="checkbox"/>	Albany NY 3363	2 Tower Place, Executive Woods 12203 Albany New York UNITED STATES	0,0	Sep 18, 2019

2. Edit the location, name, or drag the pushpin to a different point on the map to choose a new location. The **Location Name** may be named/renamed using a maximum of 120 characters.



3. Select **Save** to save all changes.

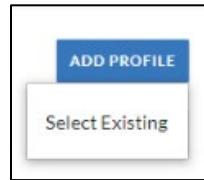
Modify a Subscription

Once created and saved, subscriptions and their components (**Subscription Overview**, **Locations**, **Profiles**, **Groups**, **History**) can be managed and accessed from the **Subscriptions** page.

From the **Subscriptions** page, click anywhere in a subscription row to view or modify subscription components. Select the **checkbox** and then **Delete** to delete a subscription.

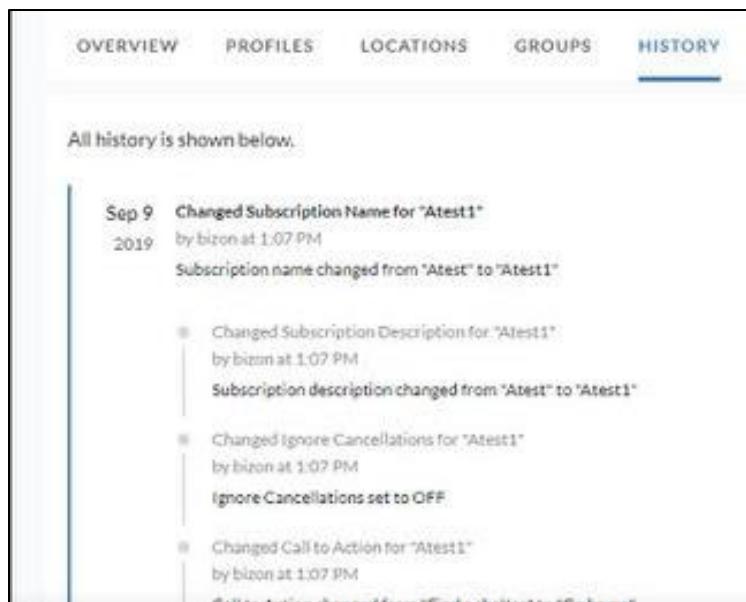
NAME & DESCRIPTION	LOCATION NAME(S)	WEATHER & CIVIL EMERGENCIES
<input checked="" type="checkbox"/> Fire For fire events	Albany	Fire Weather Warning, Fire Weather Bulletin, Fire Weather Watch, Wildfires
<input type="checkbox"/> test sub test	Albany	Air Pollution Warning, Air Pollution Watch, Air Quality Advisory, Air Quality Alert, Air Quality Warning, Air Quality Watch, Air Stagnation, Air Stagnation Outside, Ozone Action Day, Dust... + more

Note: When modifying components of a subscription, users can ONLY add existing profiles, locations, and groups. New components cannot be created on the fly when modifying a subscription.



View Subscription History

View the **History** tab on any existing subscription to review all modifications of the subscription, including date and time, username, and type of change.

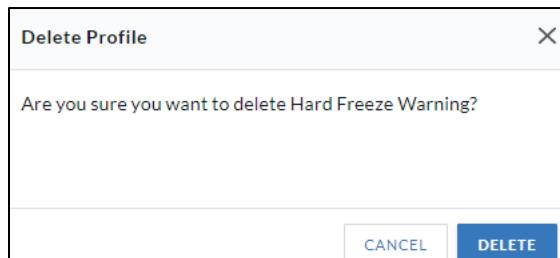


The screenshot shows a user interface for viewing subscription history. At the top, there are tabs labeled OVERVIEW, PROFILES, LOCATIONS, GROUPS, and HISTORY. The HISTORY tab is currently selected and underlined. Below the tabs, a message reads "All history is shown below." A list of changes is displayed, each with a timestamp, the user who made the change, and a brief description. The changes listed are:

- Sep 9, 2019: Changed Subscription Name for "Atest1" by bizon at 1:07 PM. Description: Subscription name changed from "Atest" to "Atest1".
- Sep 9, 2019: Changed Subscription Description for "Atest1" by bizon at 1:07 PM. Description: Subscription description changed from "Atest" to "Atest1".
- Sep 9, 2019: Changed Ignore Cancellations for "Atest1" by bizon at 1:07 PM. Description: Ignore Cancellations set to OFF.
- Sep 9, 2019: Changed Call to Action for "Atest1" by bizon at 1:07 PM. Description: Call to Action changed from "Find a solution no longer works" to "Call to Action removed from Find a solution no longer works".

Delete a Profile/Location

- From the **Profiles** or **Locations** pages, select an item(s) (or select all) and select **Delete**.
- Confirm deletion.



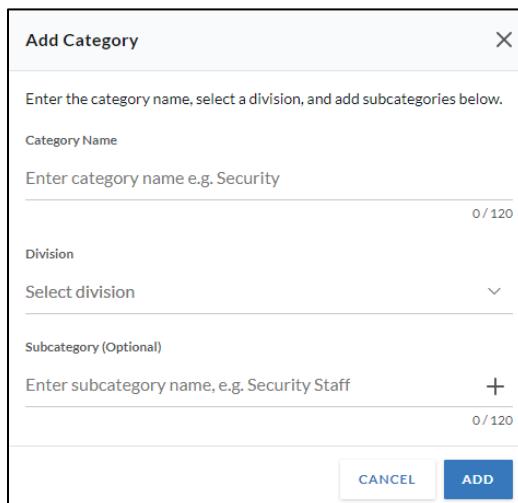
Topics

The Topics feature provides an alternate method for selecting alert recipients. Rather than selecting specific individuals or groups as the recipients, the topics feature finds its recipients based on a subscription principle. Individuals may subscribe to a particular topic, and then alerts are sent to those with matching subscriptions. Before users can create topic subscriptions, those topics must be configured. A topic consists of a category and can also include a priority or severity.

Create a New Topic

Categories

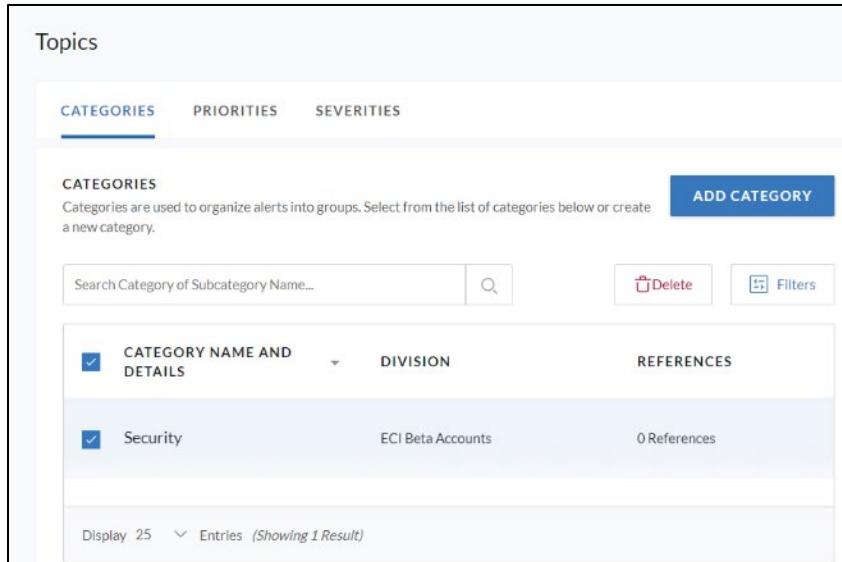
1. Navigate to **Subscriptions > Topics** in the left navigation menu. The **Topics** page opens to the **Categories** tab.
2. Select **Add Category**. The **Add Category** window opens.



The screenshot shows the 'Add Category' dialog box. It has a title bar 'Add Category' with a close button 'X'. Below the title is a descriptive message: 'Enter the category name, select a division, and add subcategories below.' There are three input fields: 'Category Name' (containing 'Security'), 'Division' (a dropdown menu showing 'Select division'), and 'Subcategory (Optional)' (containing 'Security Staff'). Each input field has a character limit indicator (0/120). At the bottom right are 'CANCEL' and 'ADD' buttons.

3. Enter a **Category Name**.
4. Choose the **Division** to which this category should be assigned.
5. Optionally, add a **Subcategory**.

- Select **Add**. The category is added to the **Categories** list.

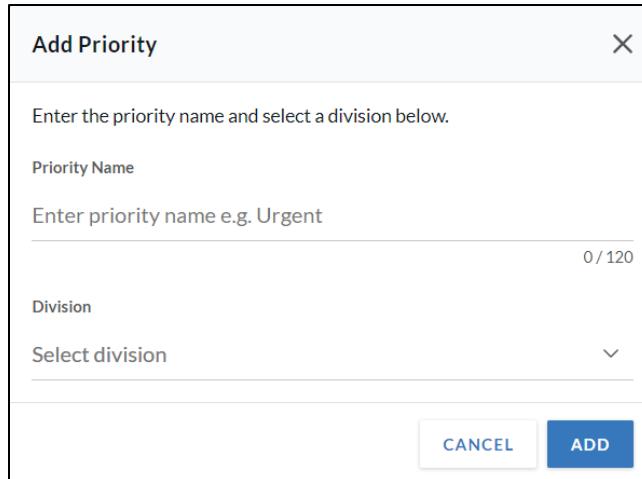


The screenshot shows the 'Topics' page with the 'CATEGORIES' tab selected. At the top right is a blue 'ADD CATEGORY' button. Below it is a search bar and filter buttons. The main area displays a table with columns: 'CATEGORY NAME AND DETAILS', 'DIVISION', and 'REFERENCES'. One entry is shown: 'Security' under 'ECI Beta Accounts' with '0 References'. At the bottom left is a pagination control 'Display 25 Entries (Showing 1 Result)'.

Priorities

The OnSolve Platform provides three predefined priorities: High, Medium, and Low. However, these can be deleted or modified. See [Manage Topics](#) for more information.

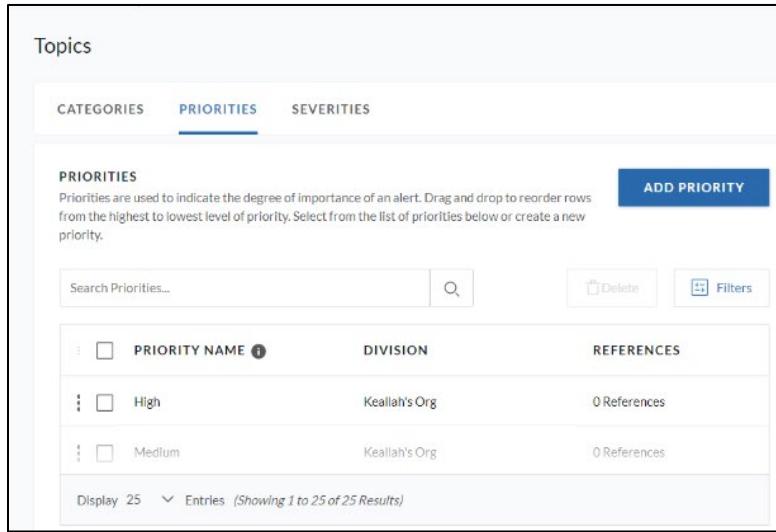
- From the **Topics** page, select the **Priorities** tab.
- Select **Add Priority**. The **Add Priority** window opens.



The screenshot shows the 'Add Priority' dialog box. It has a text input for 'Priority Name' with placeholder 'Enter priority name e.g. Urgent' and a character count '0 / 120'. Below it is a dropdown menu for 'Division' with placeholder 'Select division'. At the bottom are 'CANCEL' and 'ADD' buttons.

- Enter a **Priority Name**.
- Choose the **Division** to which this priority should be assigned.

5. Select **Add**. The priority is added to the **Priorities** list.

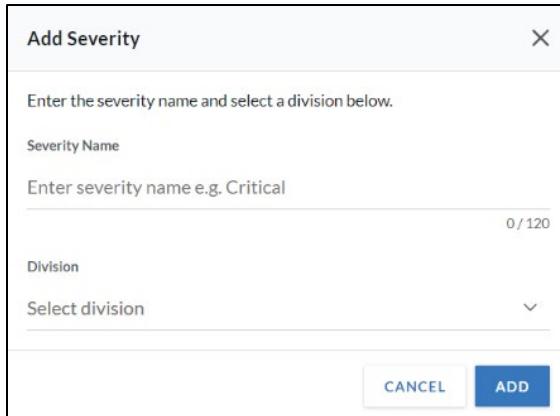


PRIORITY NAME	DIVISION	REFERENCES
High	Keallah's Org	0 References
Medium	Keallah's Org	0 References

Severities

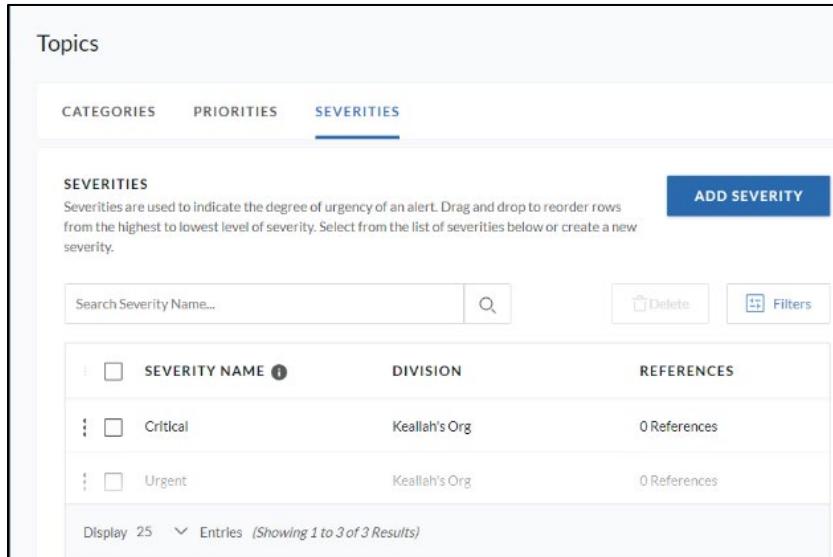
The OnSolve Platform provides three predefined severities: Critical, Urgent, and Normal. However, these can be deleted or modified. See [Manage Topics](#) for more information.

1. From the **Topics** page, select the **Severities** tab.
2. Select **Add Severity**. The **Add Severity** window opens.



3. Enter a **Severity Name**.
4. Choose the **Division** to which this severity should be assigned.

5. Select **Add**. The severity is added to the **Severities** list.



Topics

CATEGORIES PRIORITIES SEVERITIES

SEVERITIES
Severities are used to indicate the degree of urgency of an alert. Drag and drop to reorder rows from the highest to lowest level of severity. Select from the list of severities below or create a new severity.

ADD SEVERITY

<input type="checkbox"/> SEVERITY NAME <small>i</small>	DIVISION	REFERENCES
<input type="checkbox"/> Critical	Keallah's Org	0 References
<input type="checkbox"/> Urgent	Keallah's Org	0 References

Display 25 Entries (Showing 1 to 3 of 3 Results)

Manage Topics

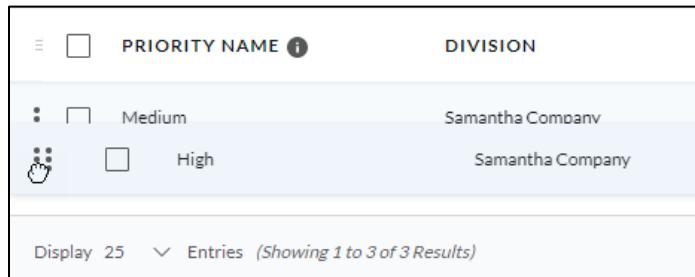
Categories, Priorities, and Severities can be modified and deleted.

Modify a Topic

Select any topic from the **Topics** page to make modifications. Select **Save** when finished.

Reorder Topics

The order in which topics appear in their respective tabs on the **Topics** page determines the order in which they appear in the drop-down lists on the **Send Alert** page. Reorder topics by dragging and dropping:



<input type="checkbox"/> PRIORITY NAME <small>i</small>	DIVISION
<input type="checkbox"/> Medium	Samantha Company
<input type="checkbox"/> High	Samantha Company

Display 25 Entries (Showing 1 to 3 of 3 Results)

Delete a Topic

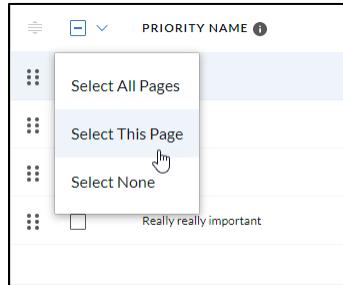
Categories, priorities, and severities can be deleted. However, when any of these topics are deleted, any subscriptions that include that topic will also be deleted.

To delete select topics

1. From the **Topics** page, select the checkbox next to the desired topic(s).
2. Select **Delete**.
3. Select **Delete** again to confirm.

To delete topics in bulk

1. From the **Topics** page, select the checkbox at the top left of the table to select all topics on the page. Or, select the arrow at the top left of the table and choose to **Select All Pages** or **Select This Page**.



2. Select **Delete**.
3. Select **Delete** again to confirm.

View References

You can view a list of all subscriptions for any topic by selecting the link in the **References** column.

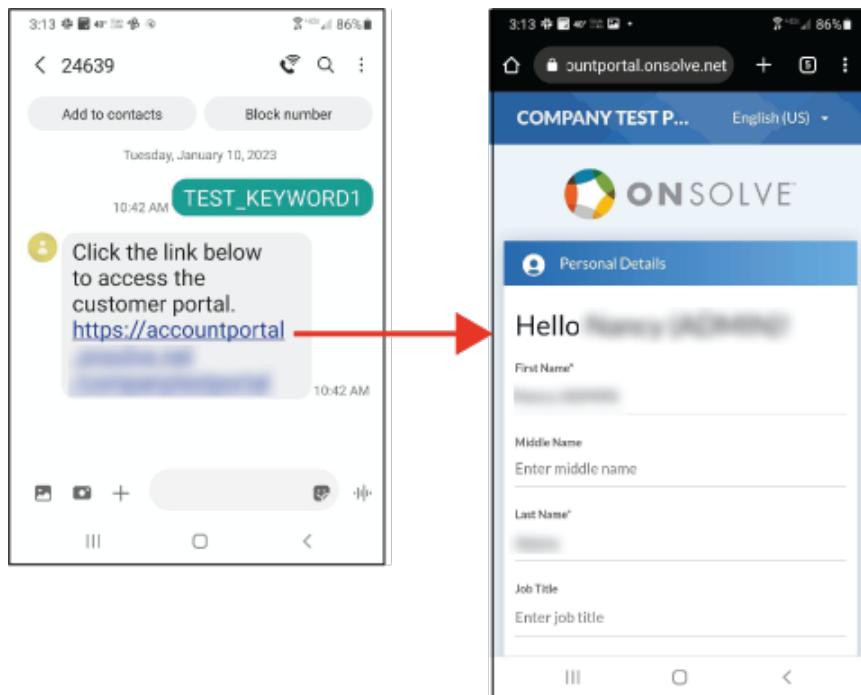
Test References		
References show all instances of alerts, groups, schedules, incidents and contacts citing this category.		
REFERENCE	TYPE	DATE ADDED
Pumpkin Cat	User subscription	October 19, 2022
Test bulletin	Alert subscription	August 16, 2021
Test subscriptions	Group subscription	July 12, 2021

The **References** window opens and lists every user, group, and alert that subscribes to that topic, the type of subscription it is (**User**, **Group**, or **Alert**), and the date the subscription started.

Test References		
References show all instances of alerts, groups, schedules, incidents and contacts citing this category.		
REFERENCE	TYPE	DATE ADDED ▾
Pumpkin Cat	 User subscription	October 19, 2022
Test bulletin	 Alert subscription	August 16, 2021
Test subscriptions	 Group subscription	July 12, 2021

Text-to-Keyword

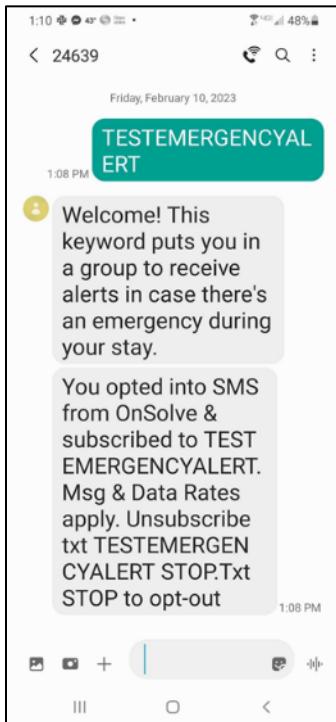
Text-to-Keyword (TTK) includes Text-to-Enroll, SMS Opt-In (Private), and SMS Opt-In (Public). The Text-to-Enroll feature enables people to send a keyword (a single SMS message) to an SMS short code to gain access to their account portal or public enrollment portal. The OnSolve Platform replies with a URL to allow people record updates via a mobile web browser.



Organizations can use Text-to-Enroll to allow existing contacts to update their contact data or use it as a way to add new contacts to their contact database through a configured account portal. Text-to-Enroll can also be used by state and local government customers who want to give people a chance to receive alerts for weather or local emergencies. After the keyword is texted, the system sends a URL directing subscribers to a public enrollment portal to register to receive alerts.

SMS Opt-In (Private) allows administrators to create a keyword that anyone can use to opt in to groups or topics to receive alerts related to those keyword topics. For example, a hotel chain might use an SMS Opt-In (Private) keyword to allow guests to opt in to get emergency alerts during their stay if an emergency occurs where they need to evacuate the premises.

SMS Opt-In (Public) allows the general public to get public-facing notifications with an SMS keyword. For example, attendees at a county fair could opt in to get alerts to learn about events happening while they are there.



The different types of TTK—Text-to-Enroll, SMS Opt-In (Private), and SMS Opt-In (Public)—all require the same steps to set up. After the OnSolve account representative enables Text-to-Keyword for the account, selects the keyword type, and assigns the number of available keywords, account administrators need to create and assign the keywords.

Note: For Text-to-Enroll, an account portal or public enrollment portal must already be set up (see [Account Portals](#) in Section 7 of this guide). For SMS Opt-In (Private and Public), the account must first have at least one topic or one group (see [Topics](#) in Section 6 and [Create and Manage Groups](#) in Section 2 of this guide). For SMS Opt-In (Public), the account must have at least one topic.

Tip

Administrators can link their keyword to a Quick Response (QR) code to make it easier for people to send the SMS text to the short code. Many free online QR code generators allow you to create custom QR codes to automatically generate an SMS message on the person's phone with the correct short code, using the configured keyword as the text. All they have to do is scan the QR code and send!

Follow these basic instructions to create a QR code:

1. Select a QR code tool. Try searching for “best free QR code generators” for the current year. That way, you eliminate older options that may not use the latest technology.
2. Choose a QR code generator that can create an SMS message that allows you to put in a specific phone number that you want to send to (the short code) and enter the message (the keyword).
3. Generate and test the QR code.
4. Download in your preferred format to put on your website or customer literature.

Create Keywords

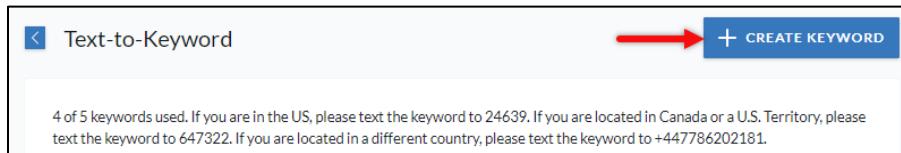
Navigate to **Subscriptions > Text-to-Keyword**. At the top of the **Text-to-Keyword** page, you see the number of keywords available in your account and the short codes people need to use. The table shows the keywords in use and information about them. Also, on this page, you can search for, filter, and delete keywords.

The screenshot shows the 'Text-to-Keyword' page with the following interface elements:

- Header:** 'Text-to-Keyword' with a back arrow icon and a '+ CREATE KEYWORD' button.
- Message:** '3 of 5 keywords used. If you are in the US, please text the keyword to 24639. If you are located in Canada or a U.S. Territory, please text the keyword to 647322. If you are located in a different country, please text the keyword to +447786202181.'
- Search Bar:** 'Search Keywords...' with a magnifying glass icon.
- Buttons:** 'Delete' and 'Filters'.
- Table Headers:** KEYWORD, TYPE, GROUP, SUBSCRIPTIONS, EXPIRATION DATE, PREVIEW.
- Table Data:** A single row for 'TEST_KEYWORD1' with Type 'Text-To-Enroll', Group '--', Subscriptions '--', Expiration Date 'Mar 9, 2023', and a 'PREVIEW' button.

To begin creating a keyword

1. From **Subscriptions** on the left navigation menu, select the **Text-to-Keyword** tile. The **Text-to-Keyword** page opens.
2. Select **+ Create Keyword** in the upper right corner of the page.

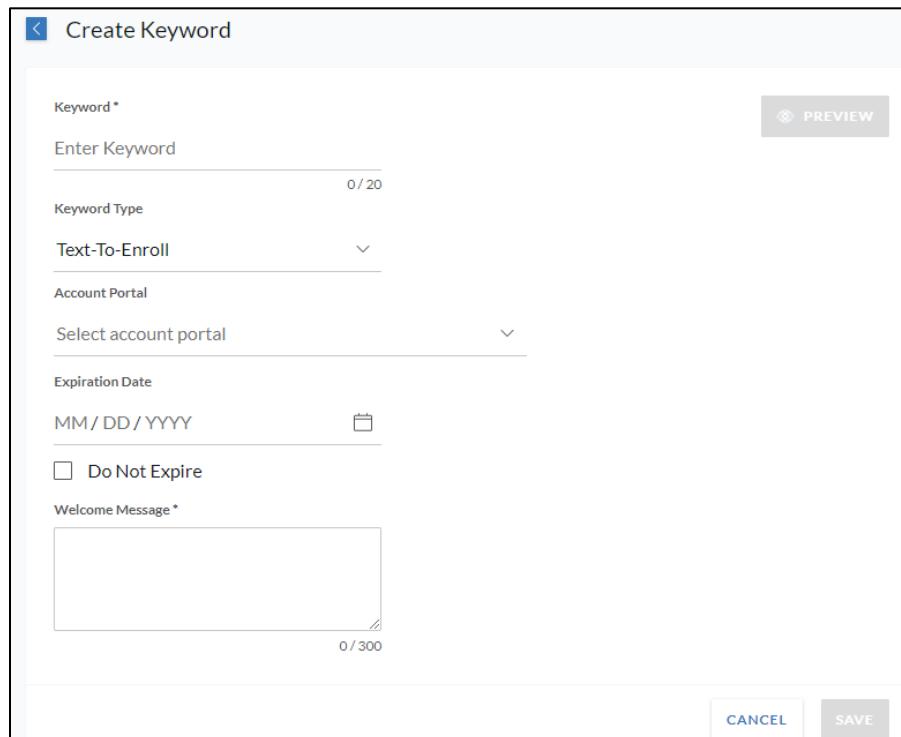


Text-to-Keyword

4 of 5 keywords used. If you are in the US, please text the keyword to 24639. If you are located in Canada or a U.S. Territory, please text the keyword to 647322. If you are located in a different country, please text the keyword to +447786202181.

+ CREATE KEYWORD

The **Create Keyword** page opens.



Create Keyword

Keyword *

Enter Keyword

0 / 20

Keyword Type

Text-To-Enroll

Account Portal

Select account portal

Expiration Date

MM / DD / YYYY

Do Not Expire

Welcome Message *

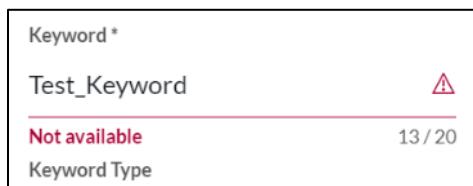
0 / 300

PREVIEW

CANCEL **SAVE**

3. Give the keyword a meaningful name (for example, CompanyXYZPortal or LakeCoOptIn) between 5 and 20 characters in length, using any characters except spaces.

Note: Keywords must be unique within the OnSolve Platform. You get a **Not available** message if the keyword is already in use. Keyword names for expired or deleted keywords can be reused after 30 days.



Keyword *

Test_Keyword

Not available

13 / 20

Keyword Type

4. Under **Keyword Type**, choose **Text-to-Enroll**, **SMS Opt-In (Private)**, or **SMS Opt-In (Public)**.
5. Once you've selected the Keyword Type, the menu options change based on your selection. Choose the next steps to follow for the type of keyword you want to create: [finish creating a keyword for Text-to-Enroll](#) or [finish creating a keyword for Private or Public SMS Opt-In](#).

To finish creating a keyword for Text-to-Enroll

1. Select from the account portals that you have previously set up.

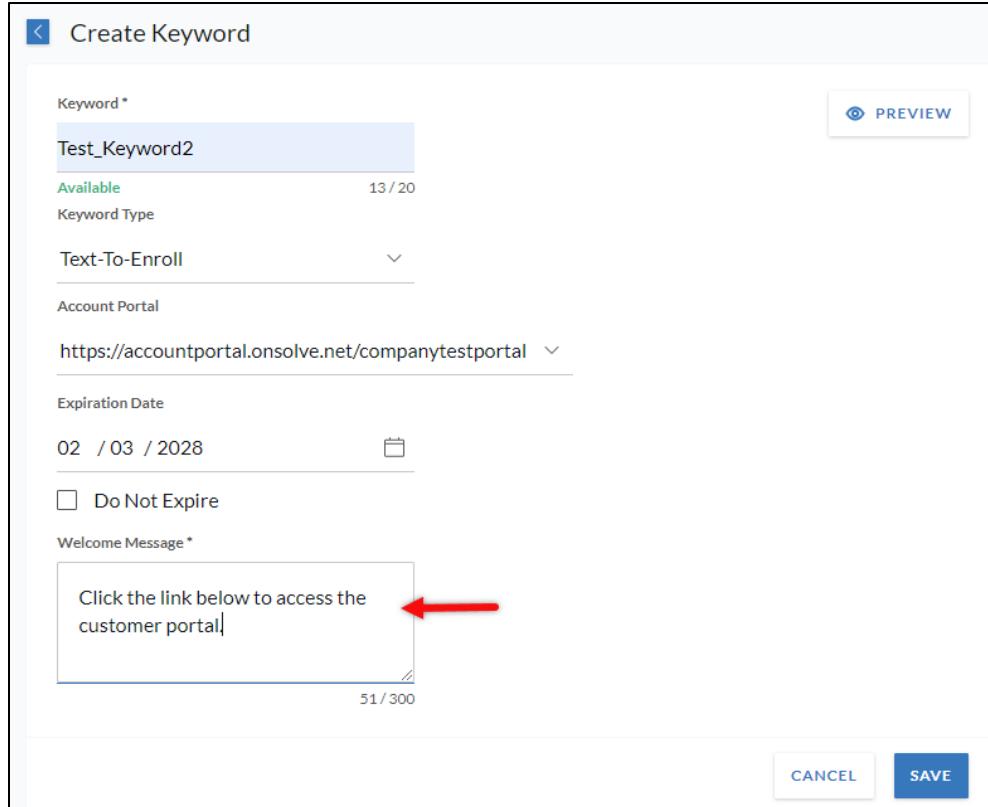
Note: If there's only one portal, the portal URL auto-fills, and the field is dimmed.

The screenshot shows the 'Create Keyword' interface. At the top, there is a back arrow and the title 'Create Keyword'. Below the title, there is a 'Keyword *' input field containing 'Test_Keyword2', which has a character count of 13 / 20. To the right of this field is a 'PREVIEW' button. Below the keyword field is a 'Keyword Type' dropdown set to 'Text-To-Enroll'. Underneath the keyword type is an 'Account Portal' dropdown. A red arrow points to the right side of this dropdown, which contains the URL 'https://accountportal.onsolve.net/companytestportal'. Below the account portal dropdown is an 'Expiration Date' section with a date input field and a calendar icon. There is also a checkbox for 'Do Not Expire'. At the bottom of the form is a 'Welcome Message *' text area with a character limit of 0 / 300. At the very bottom right are 'CANCEL' and 'SAVE' buttons.

2. Select an **Expiration Date** or select the **Do Not Expire** checkbox.

Note: For Text-to-Enroll, it may be best to select **Do Not Expire** so that the keyword is active for the lifetime of the portal. Otherwise, an expiration date is required.

3. Write a welcome message that is texted to the person after they send the keyword to the short code SMS number. For instance, “Click the link below to access the customer portal.” Or “Opt in to receive alerts from Lake County. Click below!”



Create Keyword

Keyword * PREVIEW

Available 13 / 20

Keyword Type Text-To-Enroll

Account Portal https://accountportal.onsolve.net/companytestportal

Expiration Date 02 / 03 / 2028

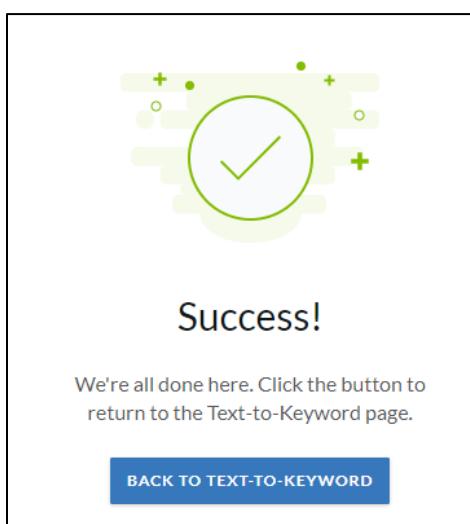
Do Not Expire

Welcome Message *

Click the link below to access the customer portal! 51 / 300

CANCEL SAVE

4. Select **Save**.
5. After the **Success** screen shows, select **Back to Text-to-Keyword**.



To finish creating a keyword for Private or Public SMS Opt-In

Note: A Private SMS Opt-In keyword requires either a group or subscription, but it can also have both. A Public SMS Opt-In keyword requires a subscription; subscribers are not placed in a group or saved to the account.

1. Next to the **Keyword Type**, select **Add Subscription**.

The screenshot shows the 'Create Keyword' interface. At the top right is a 'PREVIEW' button. Below it, the 'Keyword' field contains 'TestEmergencyAlert1'. Under 'Available' (19 / 20), the 'Keyword Type' dropdown is set to 'SMS Opt-In (Private)'. To the right of this dropdown is a blue 'ADD SUBSCRIPTION' button with a red arrow pointing to it. Below the keyword type, there's a 'Assign To Group' section with a search bar, an 'Expiration Date' field, and a 'Do Not Expire' checkbox. The 'Welcome Message' field is empty (0 / 300). At the bottom are 'CANCEL' and 'SAVE' buttons.

2. In the **Add Subscription** dialog box that opens, select a **Category**, **Priority**, and **Severity** for the subscription, and then select **Add**.

This field assigns the topic to the keyword that the person texting wishes to receive information about.

The screenshot shows the 'Add Subscription' dialog box. It has three dropdown fields: 'Category' (Select one), 'Priority' (Select one), and 'Severity' (Select one). At the bottom are 'CANCEL' and 'ADD' buttons.

Note: Care should be taken when choosing whether to include all three items together (Category, Priority, and Severity) in one subscription. When setting up related topics for the keyword, if all three are included together, all three must be included when selecting topics in the alert flow for keyword recipients to receive the alert.

3. For Private Opt-In only: In the **Assign to Group** field (see screenshot above), use the quick search or bulk add options to select a group or groups to which the person is added once they text the keyword. Alerts can then be sent to the contacts who opt in to the group(s) via the keyword.

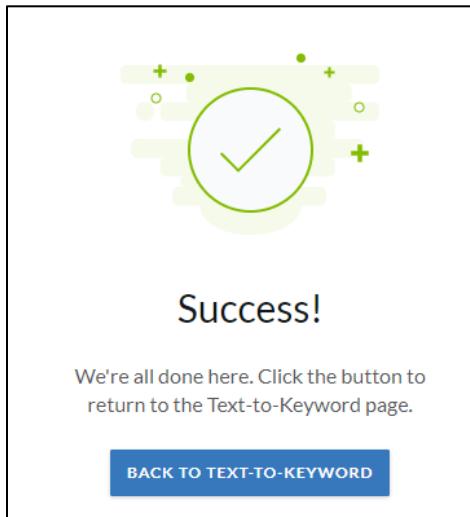
Note: OnSolve creates people records for people who opt in via private keyword and adds them to this group. If any opted-in phone number matches a contact in the account, that contact is added to the group, but a new people record is not created.

Since the only data collected about people not already in the system is the SMS phone number, the people records in the group list the SMS phone number for their first and last name. If no group is specified, but instead, a topic is used during keyword setup, contacts are added to the organization's account without being placed in a specific group.

4. Select an **Expiration Date** or select the **Do Not Expire** checkbox.
5. Write a welcome message that is texted to the person after they send the keyword to the short code SMS number. For instance, "Welcome! This keyword puts you in a group to receive alerts in case there's an emergency during your stay."

The screenshot shows the 'Create Keyword' interface. The 'Assign To Group' section is highlighted, showing 'Guest Alerts' selected. A red arrow points to the 'Welcome Message' input field, which contains the text: 'Welcome! This keyword puts you in a group to receive alerts in case there's an emergency during your stay.' The 'SAVE' button is visible at the bottom right.

6. Select **Save**.
7. After the **Success** screen shows, select **Back to Text-to-Keyword**.



Preview the Return Message for a Keyword

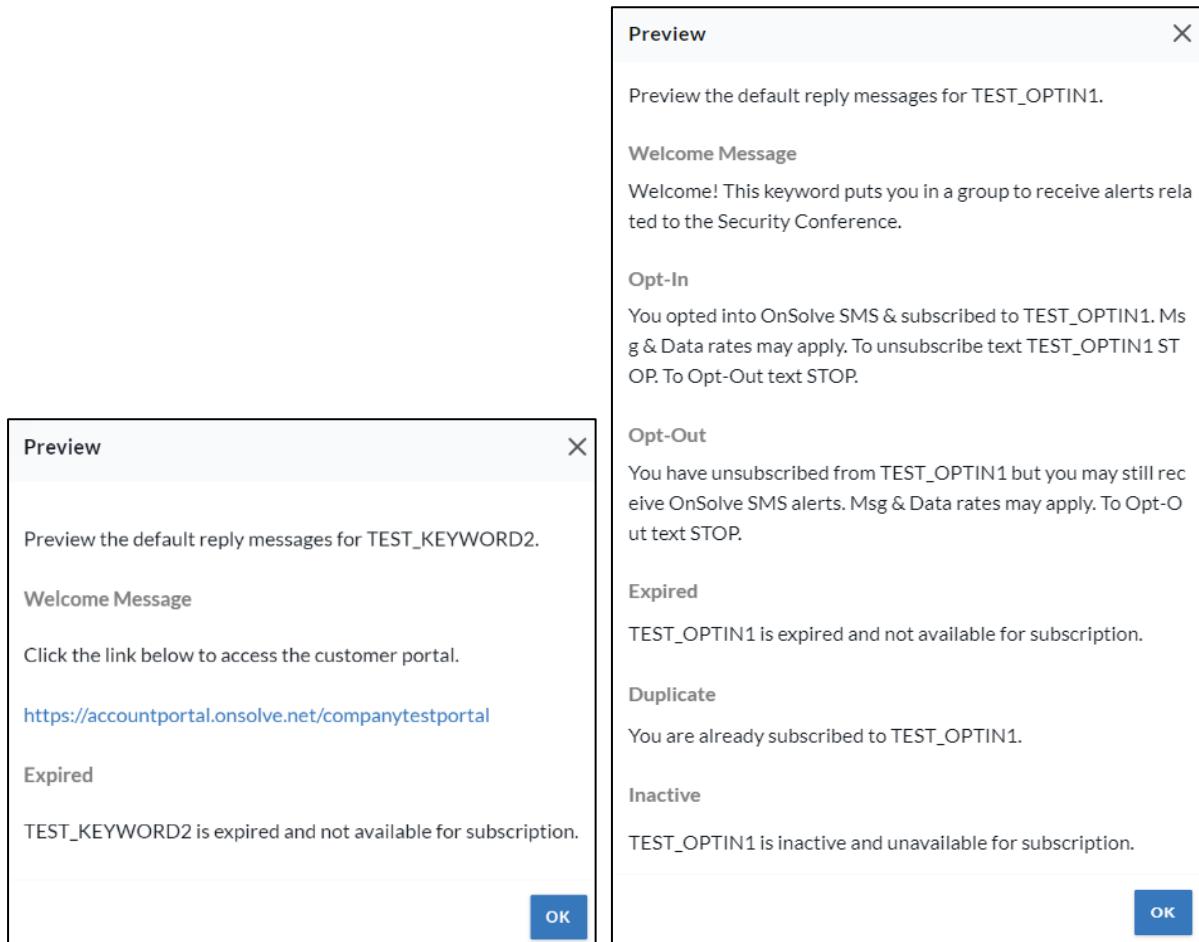
People who text the keyword receive a text back that was written when the keyword was created. Or, if the keyword is expired or deleted, a message reports that the keyword is expired. You can preview the return messages, but you can only update the Welcome Message on the **Text-to-Keyword** or **Edit Keyword** page.

A person can text the keyword five times before the system stops sending the return message. There is no message at this time that says you already texted the keyword.

The preview messages for private and public opt-in are more extensive and include the welcome message and an additional message with instructions for how to opt out from getting messages in the future. It also includes messages for when the keyword is expired, inactive, or sent more than once (duplicated).

To preview the return message

1. On the **Text-to-Keyword** page, select  for the keyword you want to preview. The **Preview** window opens.



The image displays two separate 'Preview' windows side-by-side. Both windows have a header bar with 'Preview' on the left and a close button ('X') on the right. The left window is titled 'Preview' and contains the following content:

- Header: Preview the default reply messages for TEST_KEYWORD2.
- Section: Welcome Message
- Text: Click the link below to access the customer portal.
<https://accountportal.onsolve.net/companytestportal>
- Section: Expired
- Text: TEST_KEYWORD2 is expired and not available for subscription.

The right window is also titled 'Preview' and contains the following content:

- Header: Preview the default reply messages for TEST_OPTIN1.
- Section: Welcome Message
- Text: Welcome! This keyword puts you in a group to receive alerts related to the Security Conference.
- Section: Opt-In
- Text: You opted into OnSolve SMS & subscribed to TEST_OPTIN1. Msg & Data rates may apply. To unsubscribe text TEST_OPTIN1 STOP. To Opt-Out text STOP.
- Section: Opt-Out
- Text: You have unsubscribed from TEST_OPTIN1 but you may still receive OnSolve SMS alerts. Msg & Data rates may apply. To Opt-Out text STOP.
- Section: Expired
- Text: TEST_OPTIN1 is expired and not available for subscription.
- Section: Duplicate
- Text: You are already subscribed to TEST_OPTIN1.
- Section: Inactive
- Text: TEST_OPTIN1 is inactive and unavailable for subscription.

2. Select **OK** to return to the **Text-to-Keyword** page.

Note: It is important to type the complete command to opt out of receiving messages for a particular keyword: <keyword> STOP, where <keyword> is the keyword you want to opt out of. Texting only STOP prevents you from receiving all Text-to-Keyword messages in the future. To begin receiving Text-to-Keyword messages again, text START.

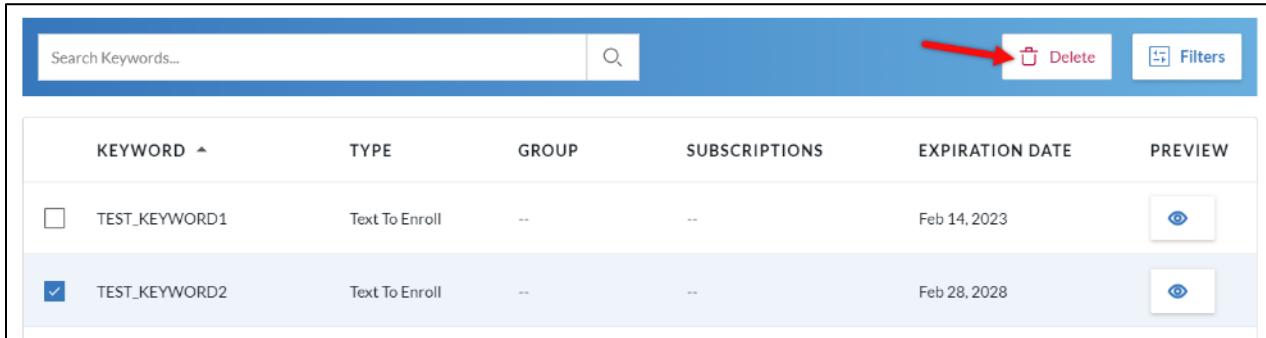
Keyword and Contact Management

You can delete keywords that are no longer needed. OnSolve Platform manages subscribers to those keywords differently depending on whether the keyword is deleted, expires, or the contacts opt out.

Delete a Keyword

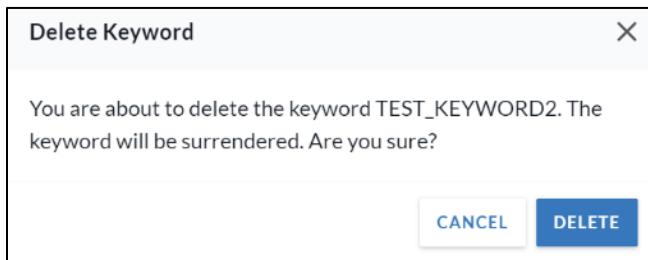
To delete a keyword

1. On the **Text-to-Keyword** page, select the keyword you want to delete.
2. Select **Delete**.



KEYWORD	TYPE	GROUP	SUBSCRIPTIONS	EXPIRATION DATE	PREVIEW
<input type="checkbox"/> TEST_KEYWORD1	Text To Enroll	--	--	Feb 14, 2023	
<input checked="" type="checkbox"/> TEST_KEYWORD2	Text To Enroll	--	--	Feb 28, 2028	

3. In the **Delete Keyword** dialog box, select **Delete**.



Contact Management

- SMS Opt-In (Public) contacts are stored anonymously as phone numbers and cannot be seen on the **People** page. When a keyword is deleted, or a contact opts out, their phone numbers are deleted. When a keyword expires, their phone numbers are deleted after 30 days.
- SMS Opt-In (Private) contacts remain in the groups they were placed in and associated with the topics they were subscribed to when a keyword is deleted or expired.
- When SMS Opt-In (Private) contacts opt out, they are removed from the groups they were placed in and unsubscribed from the topics to which they were subscribed but remain in the account.



Section 7: Configure

Integrations

The integrations feature allows authorized users to link social media and chat applications—Slack, Microsoft Teams, and Twitter—and system integrations, including Azure Active Directory and Envoy, to their OnSolve Platform account. Each third-party application below has an associated Quick Reference Guide for setting up the integration.

Social Media and Chat

Social media and chat integrations act as additional delivery methods when sending alerts. Alerts can be sent or posted to these applications by customizing the alert message body by device. Follow the instructions below to set up these integrations. See [Integrations](#) in Section 3 of this guide for instructions on sending an alert to these applications, including selecting which Slack and Microsoft Teams channels to send to.

Slack

The Slack integration allows alert senders to post alerts to a selected Slack channel. Alerts may also be customized for that delivery method. In this release, only one Slack workspace can be integrated at a time.

See the *OnSolve Platform Slack Integration Quick Start Guide* for instructions on configuring this integration.

Microsoft Teams

The Microsoft Teams integration allows alert senders to post alerts to a selected Team. Alerts may also be customized for that delivery method. In this release, only one Microsoft Teams account can be integrated at a time.

See the *OnSolve Platform Microsoft Teams Integration Quick Start Guide* for instructions on configuring this integration.

Twitter

The Twitter integration allows alert senders to post alerts to that Twitter account's feed. Alerts may also be customized for that delivery method. There is no maximum number of integrated Twitter accounts.

See the *OnSolve Platform Twitter Integration Quick Start Guide* for instructions on configuring this integration.

Systems Integrations

System integrations are general integrations that sync visitor and employee data with your OnSolve account and are not additional alert delivery methods. In this release of the OnSolve Platform, Azure Active Directory and Envoy are available to integrate with.

Entra ID (Azure AD)

The OnSolve integration with Azure Active Directory (AD) allows organizations to synchronize their Azure AD employee contact data and groups with the OnSolve Platform. Employees are managed as contacts through the OnSolve Platform without manual intervention, eliminating the need to import or export CSV files.

See the *OnSolve Platform Entra ID (Azure AD) Integration Guide* for instructions on configuring this system integration.

BambooHR

Integrating your BambooHR account allows you to sync contacts from BambooHR to the OnSolve Platform. Once BambooHR is integrated, the **People** page is populated with your BambooHR contacts.

See the *OnSolve Platform BambooHR Integration* guide for instructions on configuring this system integration.

Envoy

The OnSolve integration with the Envoy Visitor Access Management System allows organizations to track visitors accessing an organization's buildings and facilities by creating temporary contacts within the OnSolve Platform. Visitors are managed as contacts through the OnSolve Platform once they log in through Envoy's on-site kiosk, iPad, or installed software. When a critical event occurs (e.g., active shooter, fire, social unrest) near your facility, your team can alert all visitors and impacted members of your organization by sending an alert from the OnSolve Platform to ensure that all building occupants, employees, and visitors are accounted for and informed.

See the *OnSolve Platform Envoy Integration QRG* for instructions on configuring this system integration.

Kisi

Integration with the Kisi Access Control System allows customers to configure the OnSolve Platform to receive automated events based on entries to and departures from facilities protected by the Kisi Access System. When a critical event occurs (for example, a shooting or riot), an alert can be sent to employees and visitors to ensure they are adequately protected. The alert is sent to all relevant recipients to ensure that all present building occupants are notified, protected, and, if necessary, directed to safety.

See the *OnSolve Platform Kisi Mgmt Integration Quick Reference Guide* for instructions on configuring this system integration.

ServiceNow

Integration with ServiceNow is designed to send alerts to one or more recipients, chosen from ServiceNow users and contacts in the OnSolve Platform, and be able to assign incidents to these recipients within the organization's ServiceNow account.

See the *OnSolve ServiceNow Integration User Guide* for instructions on configuring this system integration.

UKG

Integration with UKG allows you to sync your UKG contacts to your OnSolve Platform account.

See the *OnSolve Platform UKG Integration Quick Reference Guide* for instructions on configuring this system integration.

Alertus

The OnSolve Alertus Integration provides you with easily visible communication methods, such as an Alert Beacon® or other digital signage to receive critical event alerts, plus panic buttons to activate an emergency alert to your OnSolve Platform account quickly. During a crisis, the OnSolve integration with Alertus devices offers additional safeguards to protect people, places, and property. When enabled for your OnSolve Platform account, the OnSolve Alertus Integration comprises a connector for inbound alerts (**Alertus**) and a connector for outbound alerts (**Alertus Outbound**).

See the *OnSolve Platform Alertus Integration User Guide* for instructions on configuring this system integration.

TDS

Integration with the TDS Access Control System allows customers to configure the OnSolve Platform to receive automated events based on entries to and departures from facilities protected by TDS access systems. When a critical event occurs (for example, a shooting or riot), an alert can be sent to employees and visitors to ensure they are adequately protected. The alert is sent to all relevant recipients so that all present building occupants are notified, protected, and, if necessary, directed to safety.

See the *OnSolve Platform TDS Visitor Integration Quick Reference Guide* for instructions on configuring this system integration.

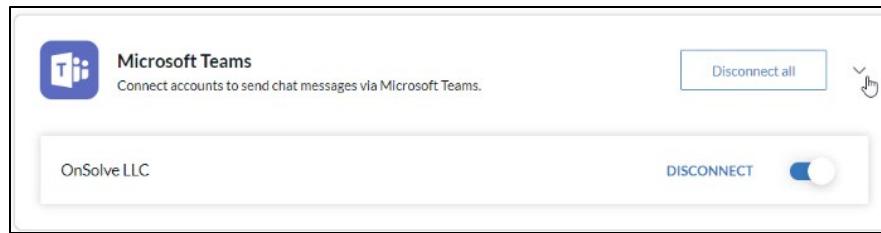
Integrations Management

For each integrated social media and chat application, accounts can be viewed, enabled/disabled, and disconnected.

Note: If an authenticated third-party account is removed, deleted, or otherwise unavailable on the application's end, they will still be listed on the **Integrations** page, but alerts cannot be sent to them.

View

To view all authenticated accounts associated with an integrated application, select the arrow to the right of that application.

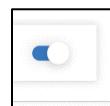


Enable/Disable

Authenticated accounts can be disabled so they are not options when customizing an alert by device yet remain integrated with the OnSolve account.

To disable a Teams account integration

Select the toggle next to the integrated Teams account. Do the same again to re-enable.



Disconnect

Integrated applications can be disconnected when needed, either one at a time or, in the case of Twitter, where you may have multiple integrations, all at once.

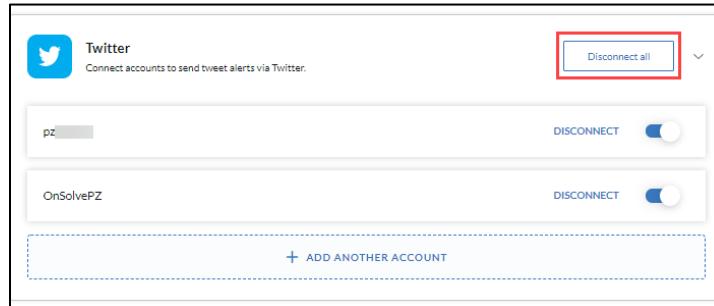
To disconnect a single account

1. Select the arrow next to the desired application.
2. Find the desired account and select **Disconnect**.



To disconnect all integrations of one type of account

Disconnect all accounts for an integration by selecting **Disconnect all**.



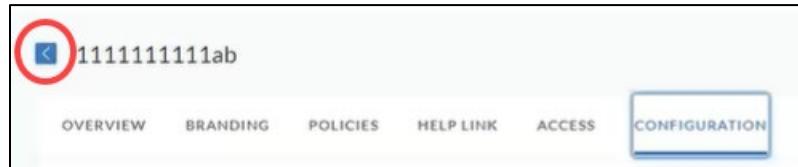
Account Portals

Recipients can opt in and create and update contact information directly in an organization-specific portal.

Only administrators can create and configure portals. In the OnSolve Platform, administrators can create up to 100 portals.

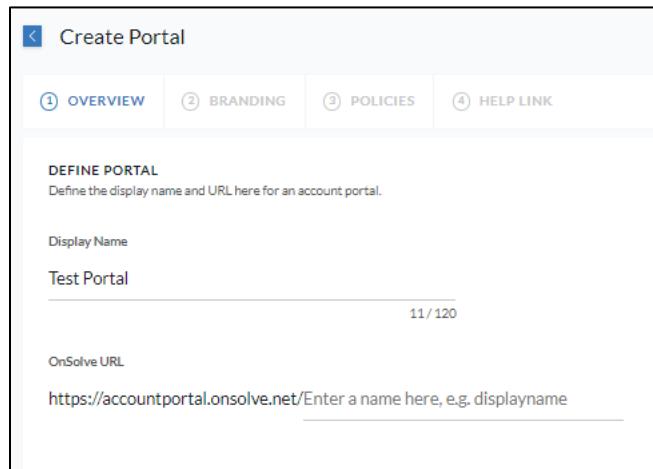
Create a Portal

Creating a portal involves six steps. At any time, select the back button to return to the previous step.



Overview

1. Navigate to **Configure > Account Portal**.
2. Select **+ Create Portal**. The **Create Portal** page opens.



The screenshot shows the 'Create Portal' interface. At the top, there's a navigation bar with a back arrow and the title 'Create Portal'. Below it is a tab navigation bar with four tabs: ① OVERVIEW (which is active and highlighted in blue), ② BRANDING, ③ POLICIES, and ④ HELP LINK. The main content area is titled 'DEFINE PORTAL' with the sub-instruction 'Define the display name and URL here for an account portal.' It contains two input fields: 'Display Name' with the value 'Test Portal' and 'OnSolve URL' with the value 'https://accountportal.onsolve.net/'. There is also a character count indicator '11 / 120' next to the URL field.

3. Enter a **Display name**.
4. Append a name, such as the Display Name, to the **OnSolve URL**.
5. Select **Next**.

Branding

Customize the look of the portal by choosing a logo and banner color.

1. Select the OnSolve logo or upload an image. Accepted file types are PNG and JPEG. The file must be no larger than 200 by 300 pixels or 2 MB.

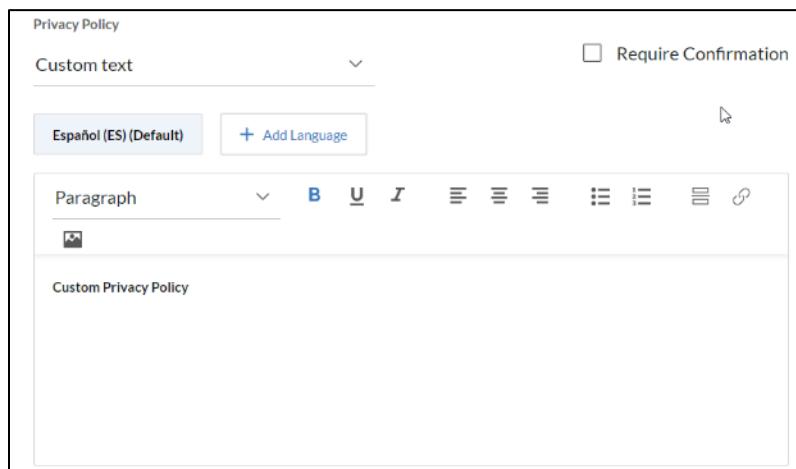


2. Select a banner color and select **Next**.

Custom Policies

Choose from a variety of policies to have displayed in the portal. For each available option:

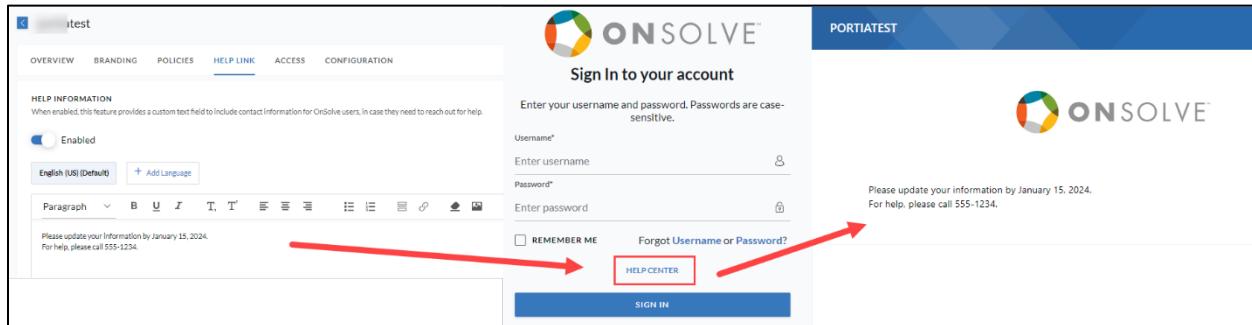
1. Select **Do Not Display** (the default), **URL**, or **Custom text** from the drop-down list.
2. If **URL**, enter the web address that will appear for registrants to follow for that policy.
3. If **Custom text**, use the WYSIWYG HTML editor to enter and format the text. If desired, select **+ Add Language** and select a language to add another text field for the chosen language. If other languages are added, it will be necessary to translate the customizable text for all languages as appropriate. For example, the English default text introduction “This is our policy” would be entered in French as “Telle est notre politique.”



4. Select whether to **Require Confirmation** of this policy by the registrant.
5. Select **Next**.

Help Link

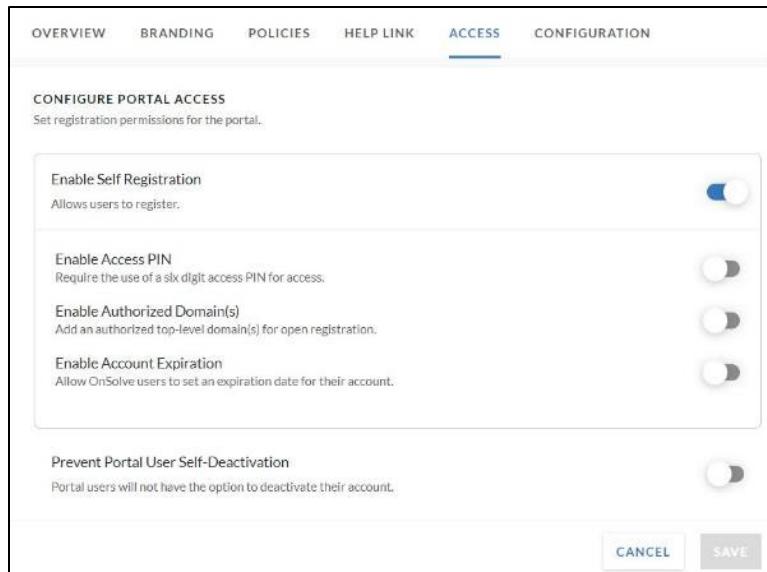
1. If desired, enable **Help Information**. When enabled, the portal administrator can add text that appears when registrants select **Help Center** on the portal sign-in page. This is an ideal place to include contact information in case registrants need help using the portal.



2. Select **Done**. The **Success** page is displayed.
3. Select **Configure Portal Now** to continue or **Back to Account Portal**. If continuing to configure, the **Access** tab is displayed.

Access

In the **Access** tab, set portal permissions for the portal.



1. Use the toggle to **Enable Self-Registration**. When Self-Registration is not enabled, the **Register** button does not show for users on the sign in page of the portal. If Self-Registration is enabled, then you can:

- a. Optionally, **Enable Access PIN**, then enter a six-digit number. When this is enabled, users must enter this six-digit PIN to access the portal. This PIN must be communicated to each user.

Enable Access PIN
Require the use of a six digit access PIN for access.

Access PIN

6 / 6

- b. Optionally, **Enable Authorized Domain(s)** to add authorized top-level domains for open registration. This allows you to restrict which email addresses can be used to self-register. For instance, allow only those with “onsolve.com” as their email domain to self-register. Enter the domain name and then press the enter key or select the **+**. The domain(s) will be listed below.

Enable Authorized Domain(s)
Add an authorized top-level domain(s) for open registration.

Domain

+

onsolve.com
trash

Notes

At any time, select the trash can to delete a domain.

You can save up to 200 authorized domains per portal, but only 40 can be saved in one batch. If you need more than 40 domains, add 40, select **Save**, and then add more, up to 200.

- c. Optionally, **Enable Account Expiration** to allow registrants to set an expiration date for their account.
- i. Enter the number of days before expiration the registrants should be warned.
 - ii. Choose an Expired Account Removal Date. Options are:
 - **Every day.**
 - **Last day of the month.**

- **Specific date.** If choosing this option, also enter a **Monthly Removal Day**.

Enable Account Expiration
Allow OnSolve users to set an expiration date for their account.

Expiration Warning Notification ⓘ
30

Expired Account Removal Date ⓘ
Last day of the month

2. Optionally, **Prevent Portal User Self-Deactivation**. When this is enabled, users will not be able to deactivate their accounts.
3. If continuing to configure, select the **Configuration** tab.

Configuration

The configuration section comprises the bulk of portal creation. It allows administrators to decide what data fields, groups, devices, and locations appear in the portal.

General Fields

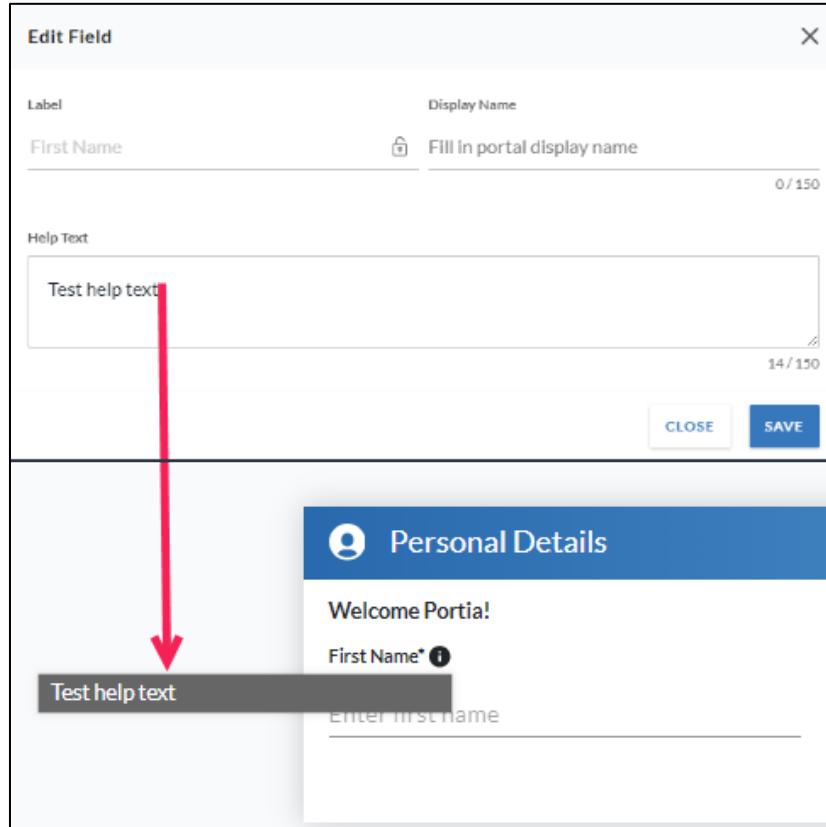
Define what general data users provide in this portal. Custom fields are managed in this section.

1. For each of the listed **General Fields**, choose whether they should be **Hidden**, **Required**, or **Locked**.

OVERVIEW					BRANDING	POLICIES	HELP LINK	ACCESS	CONFIGURATION
General Fields									
Define what general data will be collected for this portal. Custom fields are managed in this section.									
GENERAL FIELDS	REQUIRED	LOCKED	HELP TEXT						
SOME NEW NAME General Label	<input checked="" type="checkbox"/>	<input type="checkbox"/>							
Middle Name General Label	<input type="checkbox"/>	<input type="checkbox"/>							
Last Name General Label	<input checked="" type="checkbox"/>	<input type="checkbox"/>							
Job Title General Label	<input type="checkbox"/>	<input type="checkbox"/>							
First Name Custom Label	<input type="checkbox"/>	<input type="checkbox"/>	First Name 						

- Select **Hidden** for fields that shouldn't be visible.
- Select **Required** for fields that portal users must fill out.

- Select **Locked** for fields that should be viewable but not editable.
 - Reorder fields by dragging and dropping.
2. Optionally, select the **Edit** icon to write **Help Text** for any fields. This customizable text appears as a tooltip in the portal.



3. Optionally, add new fields.
- a. Select **Add General Field** underneath the list of existing fields. The **Add General Field** window opens.

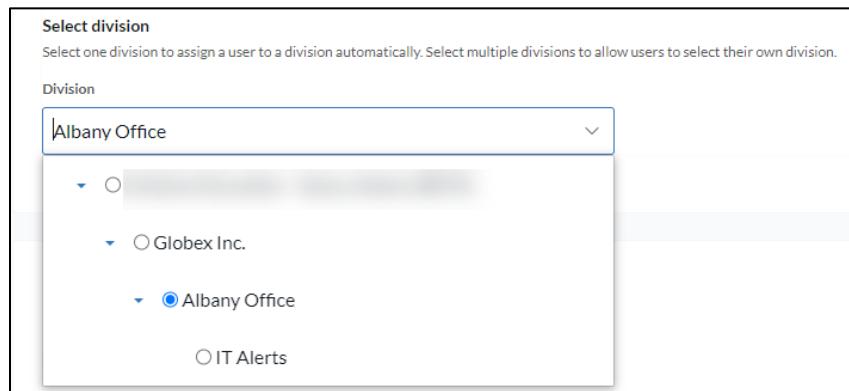


The 'Add General Field' dialog is shown. It has fields for 'Label' (Create custom label) and 'Display Name' (Department). Below these are sections for 'Custom Label' (Department) and 'Help Text' (Optional help text). The 'Help Text' section contains the placeholder 'Optional help text.' and has a character count of 19/150. At the bottom are 'CLOSE' and 'SAVE' buttons.

- b. From the drop-down list, choose a **Label** or **Create custom label**. If creating a custom label, enter a **Custom Label** name.
- c. Enter a **Display Name**.
- d. Optionally, add **Help Text**.
- e. Select **Save**.

Divisions

Using the drop-down list, select the **Division** available to the portal users from which to choose. Locate the division by either scrolling through the list or typing a division name in the text field.



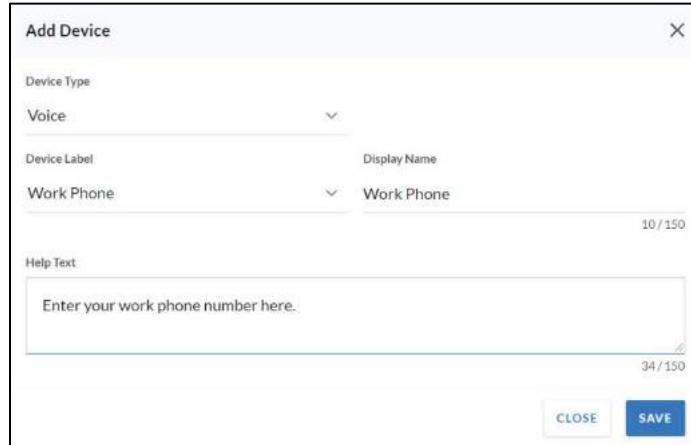
Devices

Define what devices portal users can choose to be contacted with.

1. Select a **Default Country Code** from the drop-down list. This is the default country code that registrants see when entering phone numbers.



2. Select **+ Add Device**. The **Add Device** window opens.



Add Device

Device Type: Voice

Device Label: Work Phone

Display Name: Work Phone

Help Text: Enter your work phone number here.

Save Close

3. Select the **Device Type** from the drop-down list.

4. Select the appropriate **Device Label**.

Note: Device Labels are created on the **Settings > Alert Module > Labels** page.

5. Enter a **Display Name**. Portal users see this rather than the **Device Label**.

6. Optionally, enter **Help Text**. This customizable text appears as a tooltip in the portal.

7. Select **Save**. The added device is saved to the portal.

8. Choose whether the device should be **Required** or **Locked**.

LABELS	REQUIRED	LOCKED
Work Phone Work Phone	<input type="checkbox"/>	<input type="checkbox"/>
Add Device		

9. If desired, select **Add Device** to repeat steps 2-9 and add more devices.

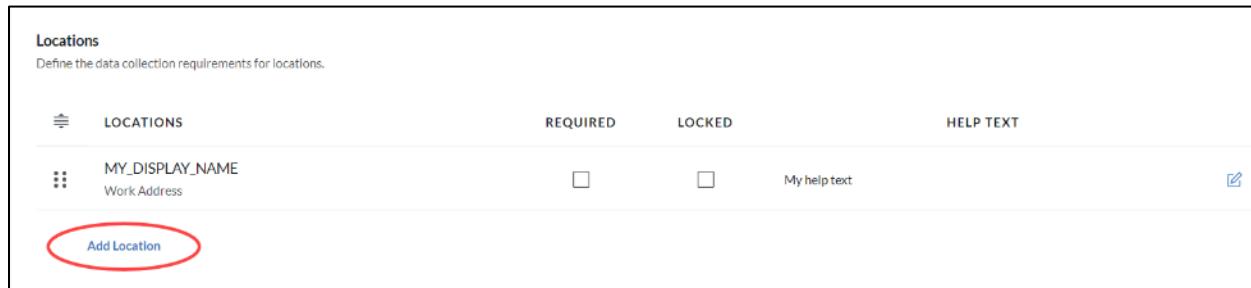
Note: Once more than one device has been added, the order in which they appear to portal users can be changed by dragging and dropping.

LABELS	REQUIRED	LOCKED	HELP TEXT
Work Phone Voice	<input type="checkbox"/>	<input type="checkbox"/>	Enter your work phone number. Edit
Office Email Email	<input type="checkbox"/>	<input type="checkbox"/>	Enter your office email. Edit
Add Device			

Locations

Portal users can provide locations that can be used for grouping and alerting purposes.

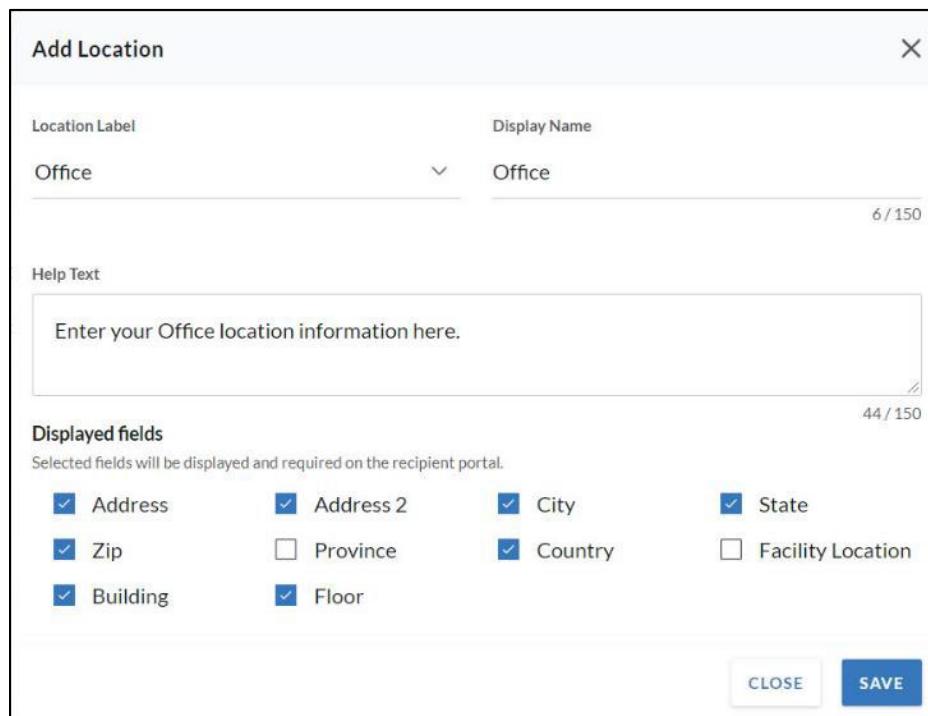
1. Select **Add Location**. The **Add Location** window opens.



Locations
Define the data collection requirements for locations.

LOCATIONS	REQUIRED	LOCKED	HELP TEXT
MY_DISPLAY_NAME Work Address	<input type="checkbox"/>	<input type="checkbox"/>	My help text

Add Location



Add Location

Location Label	Display Name
Office	Office

Help Text
Enter your Office location information here.

Displayed fields
Selected fields will be displayed and required on the recipient portal.

<input checked="" type="checkbox"/> Address	<input checked="" type="checkbox"/> Address 2	<input checked="" type="checkbox"/> City	<input checked="" type="checkbox"/> State
<input checked="" type="checkbox"/> Zip	<input type="checkbox"/> Province	<input checked="" type="checkbox"/> Country	<input type="checkbox"/> Facility Location
<input checked="" type="checkbox"/> Building	<input checked="" type="checkbox"/> Floor		

CLOSE **SAVE**

2. Select the **Location Label** from the drop-down list.

Note: Location Labels are created on the **Settings > Alert Module > Locations** page.

3. Enter a **Display Name**. Portal users see this rather than the **Location Label**.
4. Optionally, enter **Help Text**. This customizable text appears as a tooltip in the portal.
5. Select which location fields will be displayed and required for portal users.
6. Select **Save**. The added location is saved to the portal.

Note: Once more than one location has been added, the order in which they appear to portal users can be changed by dragging and dropping.

7. Choose whether the location should be **Required** or **Locked**.
8. Optionally, repeat steps 1–6 and add more locations.

Groups

Portal users may opt into groups that the portal administrator has made available. For more information on groups, see [Create and Manage Groups](#) in Section 2 of this guide.

1. Select **Add Group**. The **Add Groups** page opens.

The screenshot shows the 'Groups' page with a header 'Groups' and a sub-header 'Add and manage groups made available for users. Defaulted groups are automatically joined.' Below this is a table with columns: GROUPS, DEFAULT, HIDDEN, LOCKED, and DESCRIPTION. Two groups are listed: 'Static group with dynamic and map subgroups' and 'Tahoe Client Test 1'. At the bottom left of the table is a blue button labeled 'Add Group' with a red oval highlighting it.

GROUPS	DEFAULT	HIDDEN	LOCKED	DESCRIPTION
Static group with dynamic and map subgroups	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Tahoe Client Test 1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	test descrp. 1

The screenshot shows the 'Add groups' page with a header 'Add groups' and a back arrow icon. It features a search bar with placeholder 'Search Group Name or Description...' and a magnifying glass icon. Below the search bar is a table with columns: GROUP NAME, DESCRIPTION, TYPE, and CONTACT COUNT. Five groups are listed: DG01, Group1, NG02, NG03, and qqww. The first three groups have checked checkboxes in the 'GROUP NAME' column, indicating they are selected. The last two groups have unchecked checkboxes.

GROUP NAME	DESCRIPTION	TYPE	CONTACT COUNT
<input checked="" type="checkbox"/> DG01			--
<input checked="" type="checkbox"/> Group1	Group1		6
<input checked="" type="checkbox"/> NG02			5
<input type="checkbox"/> NG03			11
<input type="checkbox"/> qqww	qqww		2

2. Select groups to be made available in the portal and select **Add**. The selected groups are added to the **Groups** section.

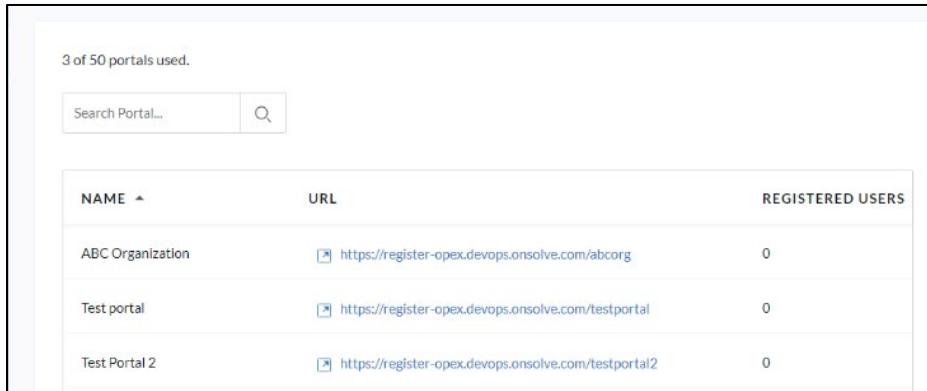
3. For each listed group, choose whether they should be **Default**, **Hidden**, or **Locked**.
 - Select **Default** for a group that users should automatically be placed into. Portal users can remove themselves from default groups unless they are locked.
 - Select **Hidden** to make a group not visible to portal users. Portal users cannot make any changes to their membership in hidden groups.
 - Select **Locked** for groups that should be viewable but not editable. Users cannot make any changes to their membership in locked groups.

Note: Once more than one group has been added, the order in which they appear to portal users can be changed by dragging and dropping.

4. If desired, edit the **Description**.

Note: By default, the **Description** is carried over from the **Groups** page. Editing the description in the portal does not carry over to the description on the **Groups** page.

5. If desired, select **Add Group** to repeat steps 1–3 and add more groups.
6. When finished, select **Save**. The list of saved portals is displayed.



3 of 50 portals used.		
NAME	URL	REGISTERED USERS
ABC Organization	https://register-opex.devops.onsolve.com/abcorg	0
Test portal	https://register-opex.devops.onsolve.com/testportal	0
Test Portal 2	https://register-opex.devops.onsolve.com/testportal2	0

Portal Management

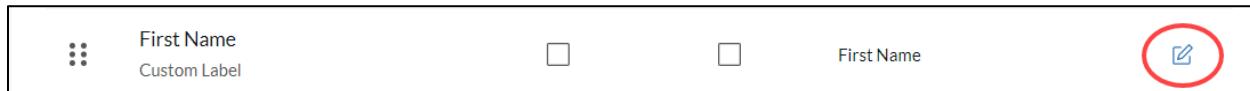
Portals can be searched by name and filtered by Name or URL. Portals can be modified and deleted.

Modify a Portal

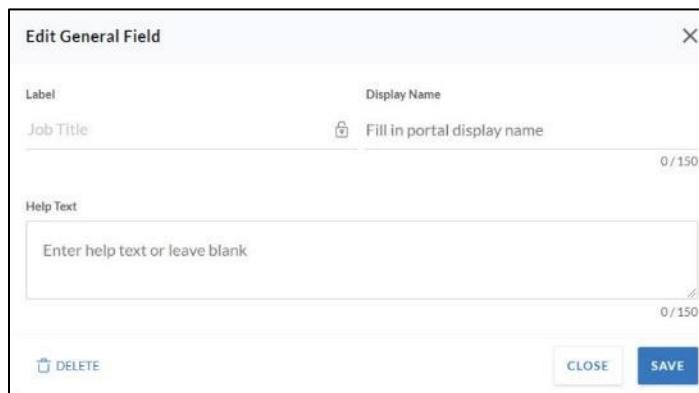
Modify a portal by clicking on the desired portal name from the account portal table. Navigate to any tab to modify any aspect of that portal. Select **Save** when finished.

Modify a General Field, Device, Location, or Group

General fields, Devices, Locations, and Groups can be modified within the **Configuration** tab by selecting the **Edit** icon.



The **Edit** window opens. Make any desired changes and select **Save**.



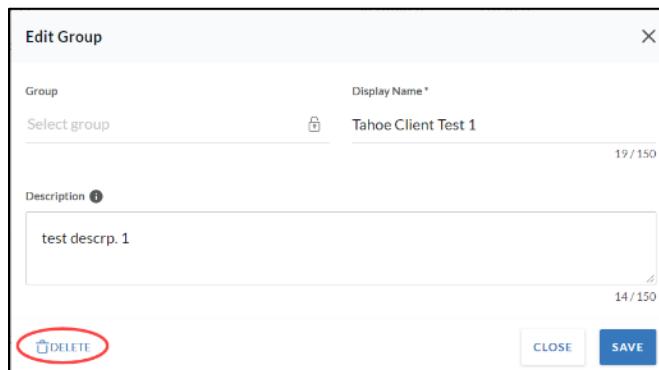
Edit General Field	
Label	Display Name
Job Title	<input type="text"/> Fill in portal display name 0 / 150
Help Text	<input type="text"/> Enter help text or leave blank 0 / 150
<input type="button"/> DELETE <input type="button"/> CLOSE <input type="button"/> SAVE	

Note: Not all fields cannot be edited.

Delete a General Field, Device, Location, or Group

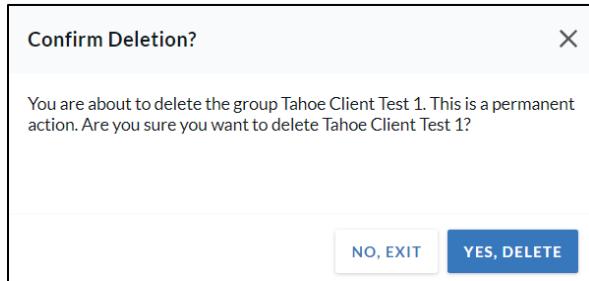
General fields, Devices, Locations, and Groups can be deleted within the **Configuration** tab.

1. Next to the desired field, device, location, or group, select the **Edit** icon and then **Delete**.



Edit Group	
Group	Display Name *
Select group	<input type="text"/> Tahoe Client Test 1 19 / 150
Description <small>ⓘ</small>	<input type="text"/> test descrp. 1 14 / 150
<input type="button"/> DELETE <input type="button"/> CLOSE <input type="button"/> SAVE	

2. Select **Yes, Delete** to confirm.



Delete a Portal

Delete a portal by selecting the checkbox next to the desired portal name and selecting **Delete**. Look for bulk delete options in a future release.

Permissions

The **Permissions** menu is where administrators and authorized users can view, manage, add roles and role templates, and view and manage divisions.

Predefined Roles

Three predefined roles with specific privilege levels are offered: Administrator, Initiator, and Recipient (Contact). These roles can be assigned directly to users. They are not deletable, and their names are uneditable. While these are predefined generic roles to get customers started, customers are encouraged to create custom roles so that the permissions given to each role are known.

Administrator

The administrator is the top-level user role responsible for administering and customizing an organization's account with little or no restrictions on system features, functions, and data. Administrators are users with access to all OnSolve role permissions.

Administrators have full access to system functionality, as well as responsibility for the operation and maintenance of the system. Administrators may create roles and divisions and, in a future release, grant access to the Billing module. Multiple administrator roles may also be created with varying levels of permissions.

Administrators for the OnSolve Platform are responsible for the day-to-day administration of the platform, where the permissions and rights are established at the highest level of the hierarchical tree (referred to as the organization). Administrator rights are inherited throughout the organization's

tree structure, so their role's permissions give them the authority to view and maintain the entire structure.

An organization's administrator(s) can create and maintain the Organization's hierarchical tree structure by using divisions and subdivisions. Divisions and subdivisions help partition senders in a specific division or subdivision (including their contacts, groups, schedules, map groups, reports, and alerts) from seeing (or accessing) other initiators and their contacts, groups, schedules, reports, and alerts. This provides security and prevents Initiators from seeing or inadvertently sending alerts to the wrong people.

Administrators can create custom user roles by applying specific permissions to the created roles. Additionally, they can import user data into the OnSolve Platform using the Import Contacts tool. See the *OnSolve Platform Import Contacts* guide for more information.

Additional responsibilities may include:

- Create custom modifications to the OnSolve Platform with pre-canned verbiage and instructions.
- Edit or protect user data fields.
- View the OnSolve Platform as other users (View as User).
- Adjust PBX Call Throttling.
- Define Automated Number Identifiers (Caller IDs).
- Establish global Extended Option defaults for the alert parameters and values.
- Build group queries and export reports.
- View billing and transaction information, and view audit logs.
- Create pronunciations (phonetic word replacements used by the TTS engine).
- Modification of the TTS delivery speed.

Initiator

Initiators or senders are users with permissions to send alerts. They may create, edit, assign, and send alerts within the system. Initiators can also view the recipients who receive the alerts.

Access to system functions usually consists of only those necessary to perform job duties. While the OnSolve Platform Organization/Division administrators are responsible for day-to-day maintenance of the platform, the Initiator is responsible for day-to-day alert activity.

An initiator's primary role is defined as a user who is authorized to create and send alerts. They can build Broadcast, Quota, and Bulletin Board alerts and send them with normal/high priority.

Initiators may also be responsible for creating contacts, groups, and schedules. In this release, data can be entered through the user interface. Future releases will include more options for data management. Initiators may also have the rights to add or remove contacts from groups and schedules.

Initiators may also be responsible for creating preconfigured alert templates and incorporating placeholders within templates, which require minimal steps before sending. They're responsible for configuring and verifying settings for contact strategies, languages, Advanced Settings, Follow-Up Questions, and Cascade before launching an alert to ensure all the features are correctly used.

More advanced Business Continuity Plans (BCP) and emergency responders (initiators) use features like the proactive Cascade for their Business Continuity Plans. They also deploy Topic Subscription for NetOps, IT, or Help Desk Users. Other initiator duties may include setting up Conference Bridge alerts for emergency meetings, creating personalized voice-recorded alerts, and possibly developing follow-up surveys to monitor and gauge the alert experience.

Specific initiator roles (e.g., limited initiator, sub-initiator, or restricted initiator) can be created based on the division, or subdivision, where the initiator resides. Some initiator roles, for example, may be limited and unable to delete contacts, alerts, or reports. Additionally, they may not be able to see user device information marked as private or to edit specific protected fields in people records. Custom roles can change because not all initiators need access to every feature or function. For security reasons or simplicity, administrators may restrict the role's permissions.

In some organizations, the initiator might assume some (or all) administrator responsibilities. Still, with most government and Fortune 500 organizations, the initiator will not have access to administrator functions, including importing and exporting contact data.

Recipient (Contact)

Recipients may receive alerts as defined by the system administrator. Recipients may or may not have access to the user interface.

Note: The name for this role is "Recipient" when managing roles from the **Configure > Permissions > Roles** or **Add Role** pages. The name for this role is "Contact" in all other places in the user interface.

Recipients are contacts who may receive alerts on multiple devices. No permissions are required to receive an alert, except for alerts sent to subscribers using the Topic Subscription feature. The recipient is the individual who receives the alert. The goal is to get the recipient to receive the alert on the devices listed in their people record and respond if requested.

While some organizations grant system login access to recipients to update and maintain their user profile, those that use DataSync or an Account Portal generally do not grant login access because the Human Resources department maintains the user data.

Role and Role Template Management

When performing initial administrative functions in the system, decisions must be made about which personnel will have access to specific functions and who will perform tasks such as defining user profiles and sending alerts. Based on these decisions, Roles and Role Templates can be defined in the system by navigating to **Configure > Permissions > Add Role/Add Role Template**.

Roles can only be tied to the division or subdivision where they were created, and permissions only apply within the division the role was created. Alternatively, Role Templates can be created and applied to any division. Role Templates are ideal for larger organizations with multiple divisions and several different roles, streamlining the process of creating and controlling user permissions.

Add a Role

Create a new role to be available to assign to users.

Enter Details

To add a new role

1. Navigate to **Configure > Permissions > Add Role**. The **Add: Access Control Role** page opens.

The screenshot shows the 'Add: Access Control Role' interface. It includes fields for the role name and division, and tabs for different permission categories. The 'Reporting' tab is selected under 'Global Permissions'. The 'Divisional Permissions' section lists several divisions, and at the bottom, there are 'Cancel' and 'Save' buttons.

2. Enter the name of the role being defined into the **Access Control Role Name** field.

3. Select the **Division** in which the role resides and has visibility to users. To make the role accessible and visible to appropriate users, it is recommended that it be assigned to the highest division possible in the hierarchy.

Note: This field is not used to identify the division in which the permissions apply.

Assign Global Permissions

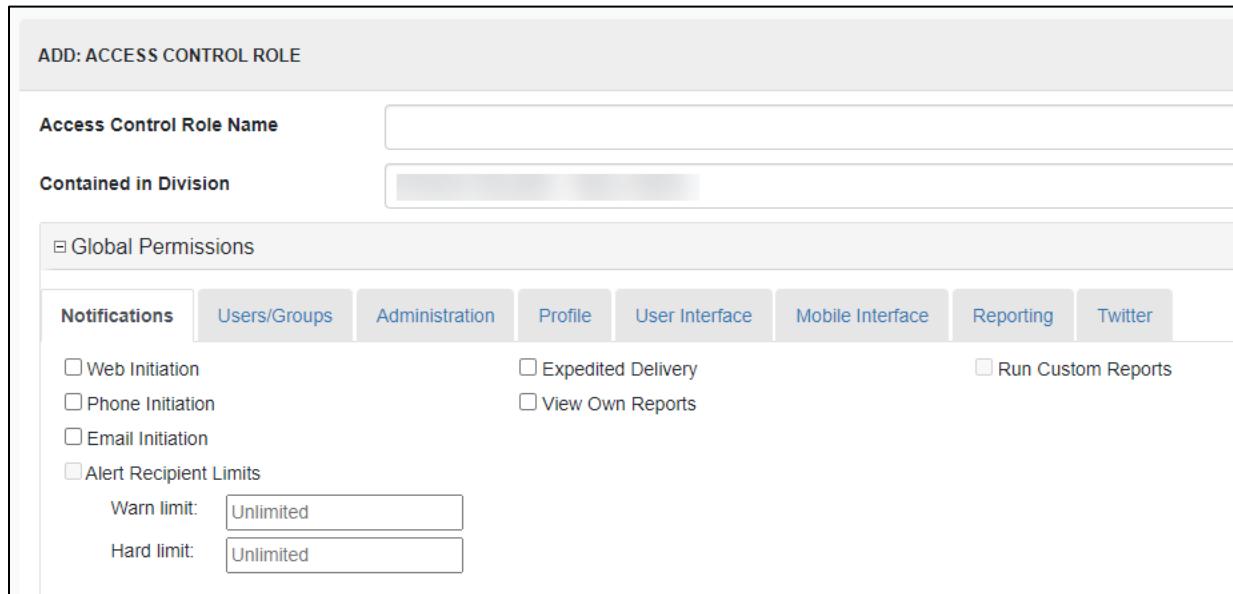
Global permissions or division-specific permissions for each defined role may be granted when defining roles. Enter global permissions into the **Notifications**, **Users/Groups**, **Administration**, **Profile**, and **Twitter** tabs. These permissions control the functionality a user can access from the related pages in the OnSolve Platform user interface.

Global permissions control the functions a user can perform at any organizational level. For example, a user assigned an IT Initiator role can send alerts but could be unable to perform administrative functions such as granting permissions to users.

Note: Several of the role permissions listed on the **Add: Access Control Role** page, while visible, are not yet applicable to the OnSolve Platform.

Notifications

On the **Notifications** tab, define global permissions that control access to the methods used to send alerts.



The screenshot shows the 'ADD: ACCESS CONTROL ROLE' page. At the top, there are fields for 'Access Control Role Name' and 'Contained in Division'. Below these, a section titled 'Global Permissions' is expanded, showing tabs for Notifications, Users/Groups, Administration, Profile, User Interface, Mobile Interface, Reporting, and Twitter. The 'Notifications' tab is selected. Under 'Notifications', there are several checkboxes for alert initiation methods: Web Initiation, Phone Initiation, Email Initiation, and Alert Recipient Limits. For 'Alert Recipient Limits', there are input fields for 'Warn limit:' (Unlimited) and 'Hard limit:' (Unlimited). Other permission checkboxes include Expedited Delivery, View Own Reports, and Run Custom Reports.

- Select **Web Initiation** to allow users with this role to send alerts. This allows users to send alerts from the OnSolve Platform interface and the OnSolve Alerts Mobile App. Requires Web Login permissions (**Global Permissions > Users/Groups tab > Web Login**).

Note: Division permissions must also be granted to send alerts for specific divisions.

- Select **Phone Initiation** to allow users with this role to send alerts by phone.
- Select **Email Initiation** to allow users with this role to send saved alerts via any email service, such as Microsoft Outlook or Gmail.
- Select **Alert Recipient Limits** and enter the number of recipients in the **Warn limit** field that, when reached, results in a warning to the sender when trying to send an alert. In the **Hard limit** field, enter the upper limit of recipients to which senders can send an alert. If left blank, an alert can be sent to unlimited recipients.
- Select the **Expedited Delivery** checkbox to allow users with this role to send high-priority alerts. Suppress in-progress OnSolve voice/telephony alerts to maximize telephony ports and prioritize a specific alert. This option pertains to telephony devices sent only to a PBX telephony system. An increased transaction fee is charged for alerts sent with Expedited Delivery enabled. Expedited Delivery does not affect text-based alerts or those sent to mobile or home phone devices.
- Select **View Own Reports** to allow users with this role to view the analytics of alerts they have sent.
- Select **Run Custom Reports** to allow users with this role to run saved custom reports carried over from a legacy OnSolve platform.

Users/Groups

On the **Users/Groups** tab, specify the global permissions that control what user profile-related functions can be accessed.

- Select **Web Login** to allow users with this role to log in to the OnSolve Platform.
Note: A user must first have **Enable User Login** toggled on in the **User Privileges** tab of their people record.
- While visible in the UI, the **Phone Login** setting is not yet applicable.
- Select **Access Role Manager** to allow users with this role access to the Role Manager function to create or edit Access Control Roles. Users must also have the divisional permission **Divisions & Roles > Edit** for specific divisions to grant or remove permissions in a role or role template.
- Select the **Import Users** checkbox to allow users with this role to access the **Import Contacts** function to import contact profile records into the OnSolve Platform. Users must also have the divisional permission **Users > Create** to add new people records to specified divisions, as well as the divisional permission **User Groups & Schedules > Create** if the import file contains new static groups that do not exist prior to the import.
- Select **Export Users** to allow users in this role to export contacts to CSV from the **People** page.

- Select **Usage Details** to allow users in this role to generate Usage Reports.
- Select **Grant Login Access** to allow users with this role to log in to obtain access to other users. This also allows those users to enable Login Access for other users they have permissions to edit. Login Access enables users to assign a username and password to log in to the OnSolve Platform user interface and OnSolve Mobile.
- Select **Edit Protected Data** to allow users with this role to edit protected data fields.

Note: The **Edit Protected Data** permission takes precedence over the Edit permission defined in the users, groups, or schedules sections of the division-specific permissions. Therefore, users cannot edit data in protected fields without permissions to Edit Protected Data. Conversely, users with Edit Protected Data permission must have Edit permissions to edit the people records.

- In a future release, select **Override SMS opt-out** to be able to send SMS alerts to recipients regardless of whether they have opted out of receiving SMS alerts.

Administration

On the **Administration** tab, define global administration permissions.

- Select **Organization Admin** to allow users with this role access to specific administrator permissions, including:
 - Reset security questions.
 - The following options on the **Alert Module** page:
 - Labels
 - Alert Options
 - Division ANI
 - Duplicate Filters
 - Alert Retrieval
 - Account Portals on the **Configure** page.
 - The **Usage** report on the **Reports** page.
 - Text-to-Keyword on the **Subscriptions** page.
- The **Manage 2FA settings** allows users with this role to access the **Configure > Security** page and configure multi-factor authentication settings.
- The **Unlock User Accounts** allows users with this role to unlock users locked out due to too many unsuccessful sign-in attempts. Used in conjunction with the Account Lockouts feature that must be enabled by your OnSolve representative.

- The **View as User** permission allows users with this role to view and act in the OnSolve Platform as other users in the account. To do so, select **View as User** on the people record of the contact you wish to view as. OnSolve recommends using this permission only as an Administrator.

Profile

On the **Profile** tab, specify global permissions that control access to profile permissions and limit the ability to edit login credentials on the user's people record.

- Select **View My Profile** to allow users with this role to view the **My Information** window.
- Select **Edit My Profile** to allow users with this role to edit the **My Profile** section.
- Select **Edit My Login** to allow users with this role to access the **Forgot My Password** link. In a future release, this permission will allow users with this role to edit their username and password.
- Select **Check-In** to allow users with this role to check in to a temporary location through the OnSolve Platform or OnSolve Mobile (if enabled in their account). Recipients may receive alerts sent to groups that include the location they have checked into.

User Interface

On the **User Interface** tab, specify global permissions that control access to elements of the user interface.

- Select **View Own Notification Inbox** to allow users with this role access to the **Critical Communications > Inbox** page.
- Select **Use Notification Groups** to allow users with this role access to the **Critical Communications > Linked Alerts** page.
- Select **Send from Show All** to allow users with this role to send alerts from the **Saved Alerts** widget and **Saved** tab of the **Alerts** page. Without this permission, users with this role instead see **View** on the aforementioned pages and can only send alerts by opening an individual saved alert and selecting **Send**.
- Select **Manage API Keys** to allow users with this role access to create and manage APIs within the Developer Portal site.

Note: API Keys are managed outside the OnSolve Platform UI in the Developer Portal.

All other permissions on this tab are not associated with OnSolve Platform functionality in this release.

Mobile Interface

On the **Mobile Interface** tab, specify global permissions that control access to the SOS and LookOut features.

- Select **Send SOS** to allow OnSolve Mobile users with this role to send SOS alerts.

- Select **Send LookOut** to allow OnSolve Mobile users with this role to send LookOut alerts.

Reporting

On the **Reporting** tab, select **View Reporting** to allow users with this role to view the **Reporting** menu in the left navigation menu.

Twitter

On the **Twitter** tab, specify global permissions that control access to the Twitter integration.

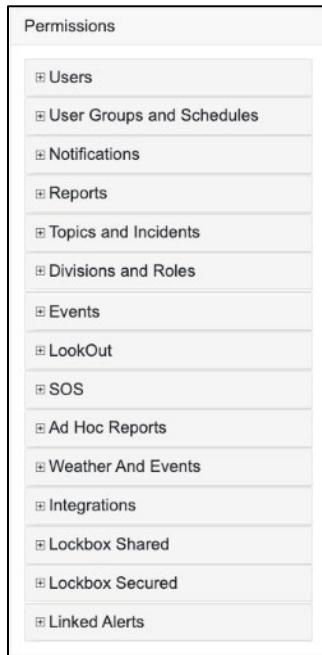
- Select **View** to allow users with this role to see any Twitter integrations in the **Configure > Integrations** menu.
- Select **Edit** to allow users with this role to edit the account's Twitter integration (such as disconnecting Twitter accounts). **View** is automatically selected by association.
- Select **Use** to allow users with this role the ability to send alerts to integrated Twitter accounts.
- Select **Configure** to allow users with this role to configure a new Twitter integration.

Assign Divisional Permissions

After setting global permissions, proceed to the **Divisional Permissions** section to grant permissions based on specific divisions. Divisional permissions are categorized into the following topics: **Users**, **User Groups and Schedules**, **Notifications**, **Reports**, **Topics and Incidents**, **Divisions and Roles**, **Events**, **LookOut**, **SOS**, **Ad Hoc Reports**, **Weather and Events**, **Integrations**, **Lockbox Shared**, **Lockbox Secured**, and **Linked Alerts**.

Note: Divisions must be created for the account before divisional permissions can be assigned. See [Divisions](#) for more information.

Once a division from the divisional tree is selected, the **Permissions** categories are displayed.



Users

- Select **Edit** to allow users in this role to edit and save existing people records; however, the users will be restricted from editing fields marked as **Protected** unless the global **Edit Protected Data** permission has been assigned in the Access Control Role. The **View Users** checkbox is automatically selected by association.
- Select **View** to allow users in this role to view existing people records. Users can view all data fields within these records except those marked **Private**; the **Private Access** checkbox must be selected to view devices marked **Private**.
- Select **Create** to allow users with this role to create new people records assigned to a division. Permission will allow a user to create a new user profile and access to data fields within that record; the **Users – View** checkbox is automatically selected by association.
- Select **Delete** to specify if users with this role can permanently delete existing people records.

- Select **Private Access** to allow users with this role to view devices marked as **Private** in people records assigned to a division.

Permissions

<input type="checkbox"/> Users
<input type="checkbox"/> Edit
<input type="checkbox"/> View
<input type="checkbox"/> Create
<input type="checkbox"/> Delete
<input type="checkbox"/> Private Access

User Groups and Schedules

- Select **Edit** to allow users with this role to edit and save the existing group or user schedules assigned to a division and the ability to access all data fields within these records.
- The **View** checkbox is automatically selected by association. Users can also add or remove users, user groups, and user schedules.
- Select **Create** to allow users in this role to create new user groups or user schedules assigned to a division and the ability to edit data fields within these records. Users can add or remove users (if they have **Users - View** permission), user groups, and user schedules.
- Select **Delete** to allow users in this role to permanently delete user groups or schedules assigned to a division. The **Groups & Schedules – View** checkbox is automatically selected by association.

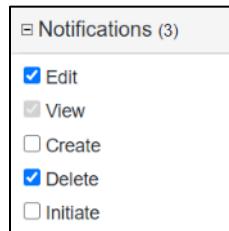
<input type="checkbox"/> User Groups and Schedules (2)
<input checked="" type="checkbox"/> Edit
<input checked="" type="checkbox"/> View
<input type="checkbox"/> Create
<input type="checkbox"/> Delete

Notifications

- Select **Edit** to allow users with this role to edit and save existing alerts assigned to this division, all data fields within these records, and designate which users (including user groups and schedules) are assigned to these alerts. The **View** checkbox is automatically selected by association. Users can also add or remove users, user groups, and user schedules for these alerts.
- Select **View** to allow users with this role to view existing alerts assigned to this division, all data fields within these records, and the users (including user groups and schedules) assigned to these alerts.
- Select **Create** to allow users with this role to create new alerts assigned to a division, edit all data fields within these records, and designate which users (including user groups and

schedules) are assigned to these alerts. The **View** checkbox is automatically selected by association. Users can also add or remove users, user groups, and user schedules for these alerts.

- Select **Delete** to allow users with this role to delete alerts inside a division. The **View** checkbox is automatically selected by association.
- Select **Initiate** to allow users with this role to send new alerts in this division. One or more of the following global permission checkboxes must be selected:
 - **Web Initiation**
 - **Phone Initiation** (Send by Phone)
 - **Email Initiation** (not yet available)



Reports

Select **View** to allow users with this role to view existing reports assigned to this division.



Topics and Incidents

- Select **Edit Topic** to allow users with this role to edit existing topic subscription records or to reorder the sequences of category/subcategory, priority, and severity items using up and down arrows in the associated data entry screens. The Topic Subscription function allows senders to tag alerts with a set of labels and then send those alerts to all users subscribed to those labels.
- Select **Use Topic** to allow users with this role to view those categories/subcategories, severities, and priorities assigned to a division to which they have subscription rights. It also allows them to subscribe to alerts. The **Use Topics** permission is required for senders who send alerts to subscribers and recipients who have subscribed to topics.
- While visible in the UI, the **Edit Incident** permission is not yet applicable.

- While visible in the UI, the **View Incident** setting is not yet applicable.

<input type="checkbox"/> Topics and Incidents
<input type="checkbox"/> Edit Topic
<input type="checkbox"/> Use Topic
<input type="checkbox"/> Edit Incident
<input type="checkbox"/> View Incident

Divisions and Roles

- Select **Edit** to allow users with this role to edit and save any division or subdivision records located below their division in the organizational hierarchy.
- Select **View** to allow users with this role to view any division or subdivision records located below their division in the organizational hierarchy.
- Select the **Set Caller ID (ANI)** checkbox to allow users with this role to edit and save Caller ID (ANI) numbers for selected divisions using the **Edit: Division ANI** page.
- Select the **Edit Verbiage** checkbox to allow users with this role to customize messaging (email, fax, pager, phone, SMS, TDD, or web reply) for a selected division via the **Configure > Branding > Custom Verbiage** page.
- Select the **Edit Pronunciation** checkbox to allow users with this role to edit and save the standard pronunciation dictionary in the system.
- Select the **View Audit Log** checkbox to allow users with this role to view the Audit Trail in **Reports > Audit Trail**.
- Select the **Set S/MIME Key** checkbox to allow users with this role to manage S/MIME keys.

<input type="checkbox"/> Divisions and Roles
<input type="checkbox"/> Edit
<input type="checkbox"/> View
<input type="checkbox"/> Set ANI
<input type="checkbox"/> Edit Verbiage
<input type="checkbox"/> Edit Pronunciation
<input type="checkbox"/> View Audit Log
<input type="checkbox"/> Set S/MIME Key

Events

While visible in the UI, the **Events** category is not yet applicable.

Lookout

- Select **Edit** to allow users with this role to edit LookOut settings. **View** is automatically selected by association.
- Select **View** to allow users with this role to view LookOut incidents.

SOS

- Select **Edit** to allow users with this role to edit SOS settings. **View** is automatically selected by association.
- Select **View** to allow users with this role to view SOS incidents.

Ad Hoc Reports

Select **Edit** to allow users with this role to edit ad hoc reports.

<input type="checkbox"/> Ad Hoc Reports (1)
<input checked="" type="checkbox"/> Edit

Weather and Events

- Select **Edit** to allow users with this role to edit and save any Weather & Events subscriptions assigned to this division. **View** is automatically selected by association.
- Select **View** to allow users with this role to view any Weather & Events locations, profiles, and subscriptions assigned to this division.
- Select **Create** to allow users with this role to create new Weather & Events locations, profiles, and subscriptions in this division.
- Select **Delete** to allow users with this role to delete any Weather & Events locations, profiles, and subscriptions.

Integrations

- Select **Edit** to allow users with this role to edit and save any Integrations in this division. **View** is automatically selected by association.
- Select **View** to allow users with this role to view any Integrations in this division.
- Select **Create** to allow users with this role to create new Integrations in this division. **View** is automatically selected by association.
- Select **Delete** to allow users with this role to delete any Integrations in this division. **View** is automatically selected by association.

Lockbox Shared

- Select **Edit** to allow users in this role to make changes to files on the **Lockbox** page, including the ability to change them from Shared to Secure and vice versa if edit permissions exist in both categories. Edit also allows the user to change the division for the file to other divisions that the user has permission to access.

- Select **View** to allow users in this role to view the **Lockbox** page and attach lockbox files to alerts.
Note: View permission is required for recipients to access and view Shared files saved in the lock box via the link included in a message (requires Web Login permission and a username and password to access the web interface).
- Select **Create** to allow users with this role to upload shared files to the **Lockbox** page (in the selected division).
- Select **Delete** to allow users with this role to delete shared files from the **Lockbox** page (in the selected division).

Lockbox Secured

- Select **Edit** to allow users in this role to make changes to files on the **Lockbox** page, including the ability to change them from Shared to Secure and vice versa if edit permissions exist in both categories. Edit also allows the user to change the division for the file to other divisions that the user has permission to access.
- Select **View** to allow users in this role to view the **Lockbox** page and attach lockbox files to alerts.
Note: View permission is required for recipients to access and view secure files saved in the lock box via the link included in a message (requires Web Login permission and a username and password to access the web interface via the Mobile App).
- Select **Create** to allow users with this role to upload secure files to the **Lockbox** page (in the selected division).
- Select **Delete** to allow users with this role to delete secure files from the **Lockbox** page (in the selected division).

Linked Alerts

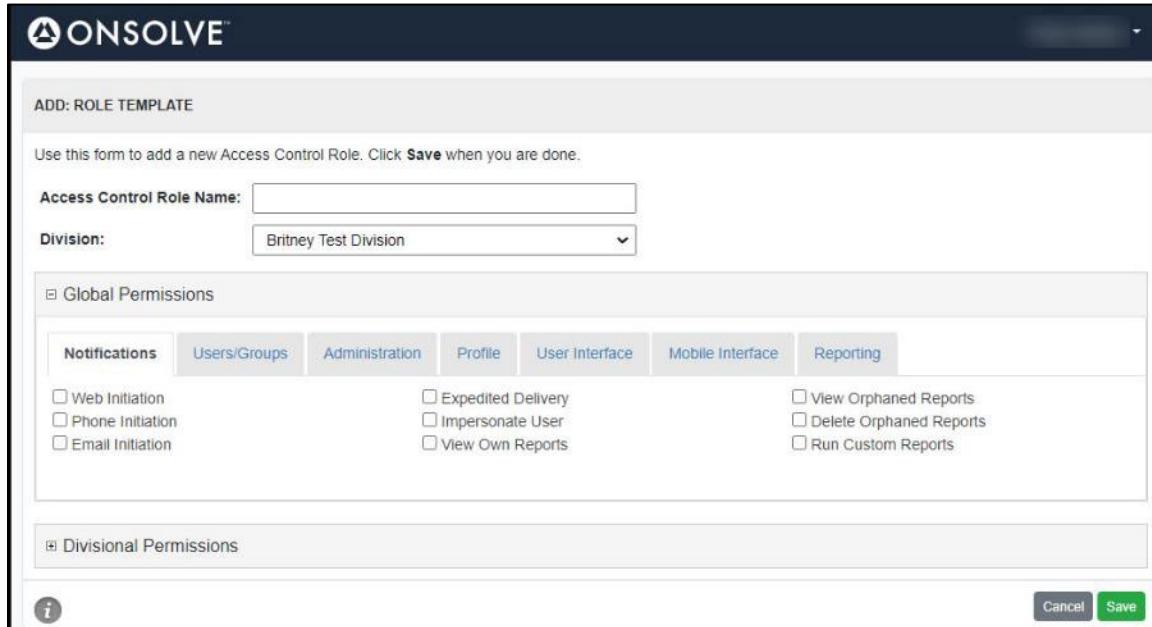
- Select **Edit** to allow users with this role to edit and save any Linked Alerts in this division. **View** is automatically selected by association.
- Select **View** to allow users with this role to view any Linked Alerts in this division.
- Select **Create** to allow users with this role to create new Linked Alerts in this division. **View** is automatically selected by association.
- Select **Delete** to allow users with this role to delete any Linked Alerts in this division. **View** is automatically selected by association.

Add a Role Template

While roles can only be tied to the division or subdivision where they were created, role templates can be created and applied to any division.

To add a new Role Template

1. Navigate to **Configure > Permissions > Add Role Template**. The **Add: Role Template** page opens.

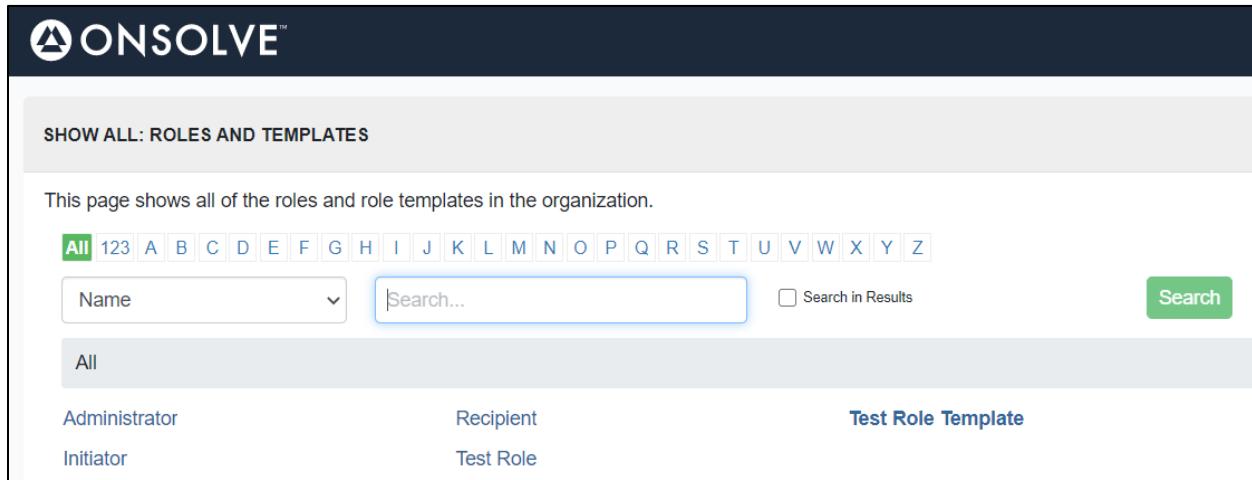


The screenshot shows the 'Add: Role Template' interface. At the top, there's a header with the ONSOLVE logo and the title 'ADD: ROLE TEMPLATE'. Below the header, a message says 'Use this form to add a new Access Control Role. Click **Save** when you are done.' There are two main input fields: 'Access Control Role Name:' and 'Division:'. The 'Access Control Role Name:' field is empty. The 'Division:' dropdown is set to 'Britney Test Division'. Under the 'Division:' dropdown, there's a link to 'Global Permissions'. This section contains a grid of checkboxes under the 'Notifications' tab. The checkboxes are: Web Initiation, Phone Initiation, Email Initiation, Expedited Delivery, Impersonate User, View Own Reports, View Orphaned Reports, Delete Orphaned Reports, and Run Custom Reports. Below the global permissions, there's a section for 'Divisional Permissions' which is currently collapsed. At the bottom right, there are 'Cancel' and 'Save' buttons, with the 'Save' button being green.

2. Enter the name of the role template being defined into the **Access Control Role Name** field.
3. Select the **Division** in which the template resides and is visible to users.
Note: This field is not used to identify the division to which the permissions apply.
4. Assign Global Permissions to the role template by following the instructions for [Assigning Global Permissions for roles](#).
5. Assign Divisional Permissions to the role template by following the instructions for [Assigning Divisional Permissions for roles](#).
6. Select **Save**.

View and Manage Roles and Role Templates

View and manage roles and role templates by navigating to **Configure > Permissions > Roles**. Role Templates are listed in **bold**.



Administrator	Recipient	Test Role Template
Initiator		Test Role

Edit a Role

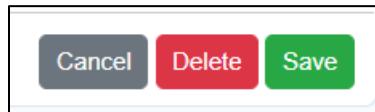
To edit a role

1. Navigate to **Configure > Permissions > Roles**. The **Show All: Roles and Templates** page opens.
2. Select the desired role.
3. Make the desired changes and select **Save**.

Delete a Role

To delete a role

1. Navigate to **Configure > Permissions > Roles**. The **Show All: Roles and Templates** page opens.
2. Select the desired role.
3. Select **Delete** at the bottom of the page.



4. Select **Delete** again to confirm.

Edit a Role Template

To edit a role template

1. Navigate to **Configure > Permissions > Roles**. The **Show All: Roles and Templates** page opens. Role templates are listed in bold.
2. Select the desired role template.
3. Make the desired changes and select **Save**.

Delete a Role Template

To delete a role template

1. Navigate to **Configure > Permissions > Roles**. The **Show All: Roles and Templates** page opens. Role templates are listed in bold.
2. Select the desired role template.
3. Select **Delete** at the bottom of the page.
4. Select **Delete** again to confirm.

Divisions

Divisions are used to partition data within an organization. Divisions and permissions are tied together in that a user's role must be granted permission to access the data saved within a particular division. That data includes alerts, contacts, groups, reports, and, eventually, certain mobile features.

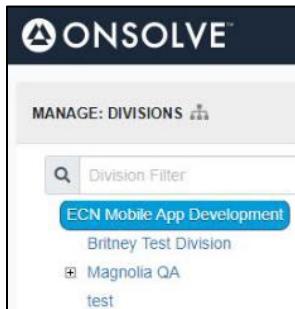
For example, an alert saved in Division A may only be accessed and sent by users with permissions to view, edit, create, delete, or send alerts saved in Division A. Additionally, a sender in Division A may only view the people records of those contacts who reside in Division A.

For each account, the OnSolve Platform can support 6,000 divisions.

Create a New Division

To create a new division or subdivision

1. Navigate to **Configure > Permissions > Divisions**. The **Manage: Divisions** page opens, displaying the name of the root organization and divisions previously defined for the organization. Only the root organization name is displayed when logging in for the first time.



2. Select the root organization to create a new division or select an existing division to create a new subdivision. The **Edit Division** fields are displayed.
3. Select **Add Sub-Division...** The **Create Division** fields are displayed.



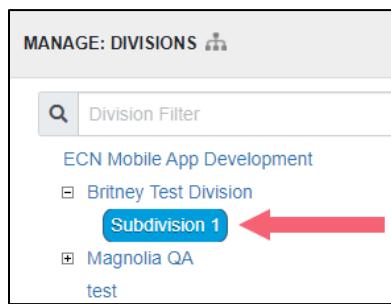
Create Division

Display Name:
Subdivision 1

Code:
Subdivision 1

Cancel Create

4. Enter a **Display Name** for the division.
5. Duplicate the display name in the **Code** field. Codes are used for automated data import methods, available in a future release.
6. Select **Create**. The new division appears in the divisional tree.



Edit a Division

To edit a division

1. From the **Manage: Divisions** page, select the desired division. The **Edit Division** fields are displayed.
2. Make any desired edits and select **Save**.

Delete a Division

To delete a division

1. From the **Manage: Divisions** page, select the desired division. The **Edit Division** fields are displayed.
2. Select **Delete**, then **Delete** again to confirm. Any groups, alerts, and contacts saved to that division will also be deleted.

Move Records Between Divisions

Groups of alerts, bulk alerts, or recipient-related records can be reassigned from their currently assigned divisions to new divisions. This process allows you to perform a mass update of a selected series of records, eliminating the need to manually reassign selected records individually.

To move records to a different division

1. Navigate to **Configure > Permissions > Move Divisions**. The **Edit: Move Division** page opens.
2. Select the type of records you want to move. The options are:
 - Notifications
 - Notification Groups
 - Users
 - User Groups/Schedules
3. Use the search functions to find and select the desired records.
4. Use the **Destination Division** drop-down list to select which division the record should be moved to and select **Move**.

Manage Division S/MIME Keys

The OnSolve Platform is designed to sign outgoing email alerts with cryptographic keys. You can enable this via the [Digitally Sign Emails](#) advanced setting. Requirements are:

- The file must be a legitimate PKCS12 file, often having a file type of P12, PFX, or PKCS12.
- It must contain at least one private key and certificate.
- It must be signed with a passphrase.
- The entire certificate trust chain should be included in the file if intermediate certificates are required.

When sending an alert with email signing enabled the OnSolve Platform signs the email using the key specified in the alert division or any parent division.

To set a signing certificate for a division

1. Navigate to **Configure > Permissions > Manage Division S/MIME Keys**.
1. Select the desired division.
2. Select **Choose File**, navigate to your key file and select **Open**.
3. Enter the **Password** and select **Save**.

Branding

Custom Verbiage

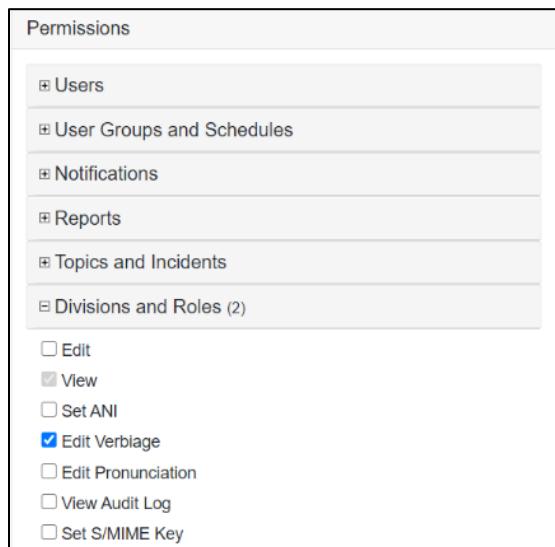
Many default system prompts and “pre-canned” messages used throughout an OnSolve alert can be modified using **Custom Verbiage**.

Verbiage may be customized to adjust the wording of instructions, add branded messages, or include additional information that pertains specifically to your company. Custom verbiage tags are categorized into 16 folders, organized mainly by the device where the verbiage is displayed or played, with over 250 individual verbiage tags that may be modified.

Access to Custom Verbiage is a role-based permission and can be granted to individual or multiple divisions and subdivisions.

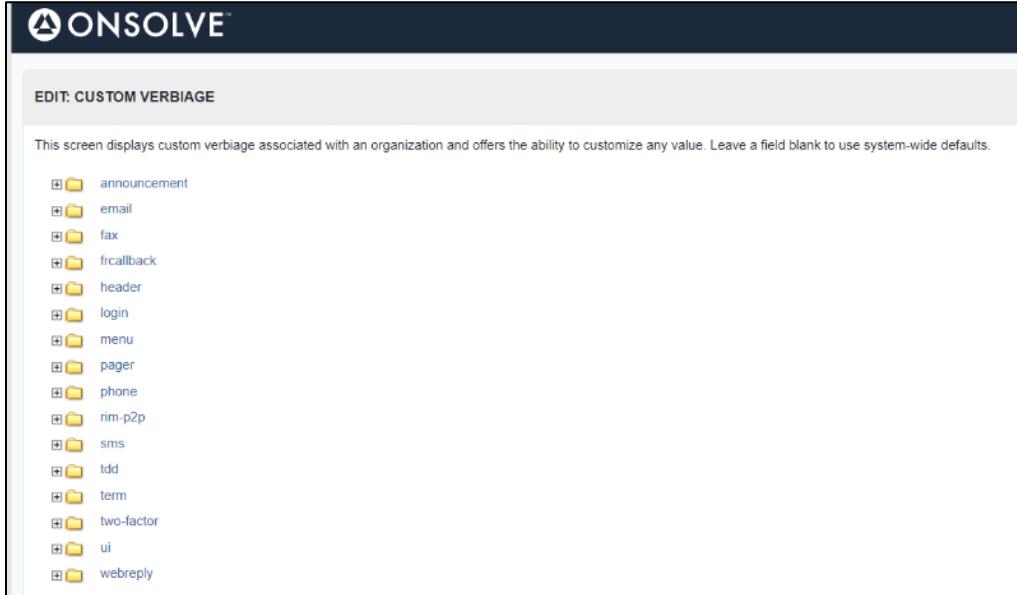
To grant access to Custom Verbiage

1. Navigate to **Configure > Permissions > Roles** and open the desired role.
2. In the **Divisional Permissions** section, select the desired division. The **Permissions** window opens to the right.
3. Under the **Divisions & Roles** category, check the box for **Edit Verbiage**.



To edit verbiage in the OnSolve Platform

1. Navigate to **Configure > Branding > Custom Verbiage**. The **Edit: Custom Verbiage** page opens.

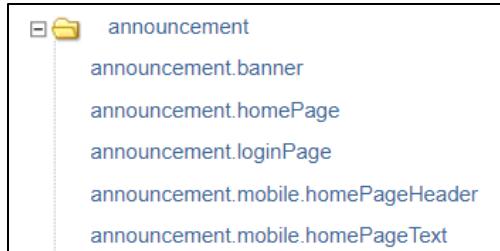


EDIT: CUSTOM VERBIAGE

This screen displays custom verbiage associated with an organization and offers the ability to customize any value. Leave a field blank to use system-wide defaults.

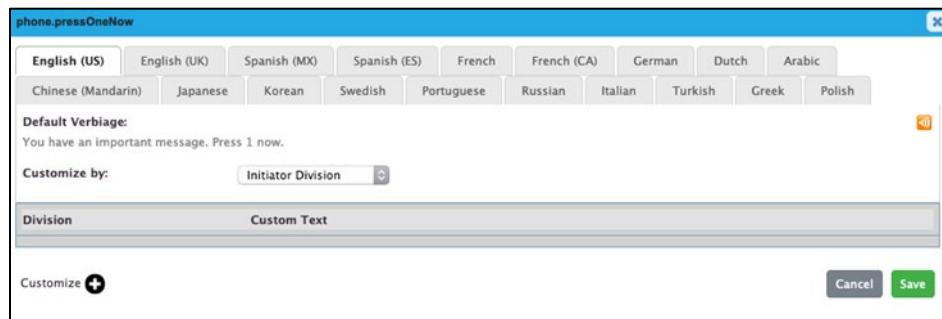
- [+] announcement
- [+] email
- [+] fax
- [+] fcallback
- [+] header
- [+] login
- [+] menu
- [+] pager
- [+] phone
- [+] rim-p2p
- [+] sms
- [+] tdd
- [+] term
- [+] two-factor
- [+] ui
- [+] webreply

2. Expand a folder by selecting the **[+]** to the left to view the individual verbiage tags available in that category.



- [+] announcement
 - announcement.banner
 - announcement.homePage
 - announcement.loginPage
 - announcement.mobile.homePageHeader
 - announcement.mobile.homePageText

3. Select a verbiage tag. The **Edit Custom Verbiage** window opens.



phone.pressOneNow

English (US)	English (UK)	Spanish (MX)	Spanish (ES)	French	French (CA)	German	Dutch	Arabic	
Chinese (Mandarin)	Japanese	Korean	Swedish	Portuguese	Russian	Italian	Turkish	Greek	Polish

Default Verbiage:
You have an important message. Press 1 now.

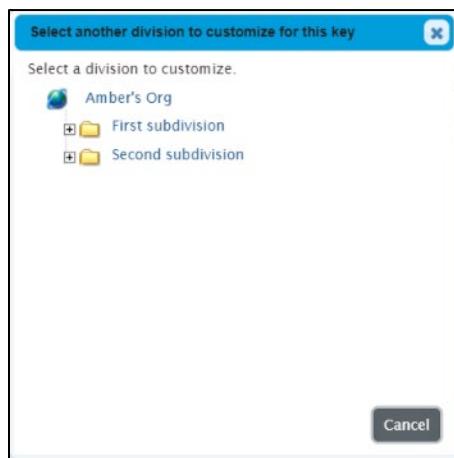
Customize by: Initiator Division

Division	Custom Text

Customize

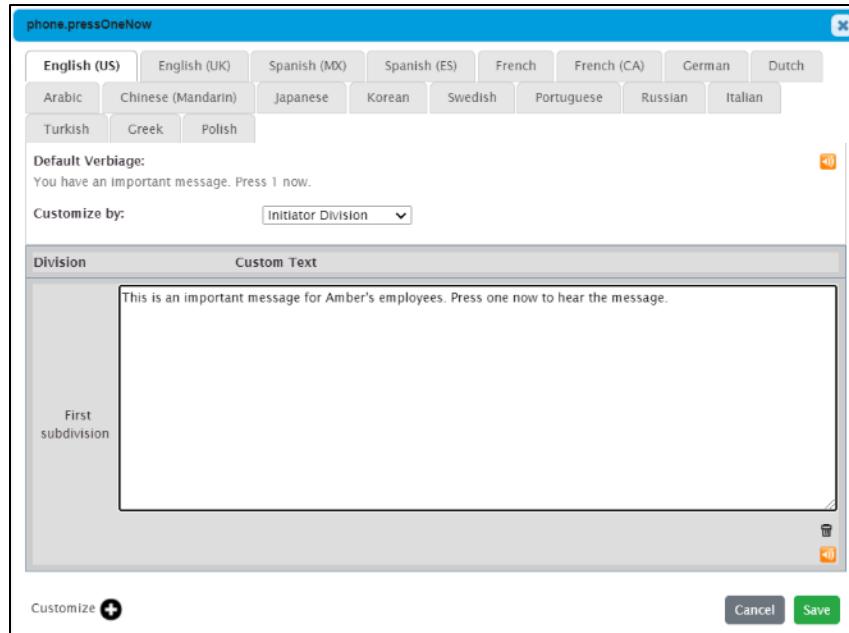
Cancel Save

4. Choose the language tab for which the custom verbiage will be applied. Each language may have its own customized verbiage. Only languages which have been provisioned for the account will be displayed.
5. Optionally, select the orange play/speaker button to hear the automated text-to-speech engine dictate this text. The speaker icon is displayed only in tags used by the text-to-speech engine.
6. Select a **Customize by** option.
 - Initiator Division: (The default and most common option) OnSolve will modify the verbiage in alerts based on the division where the Initiator (Sender) resides.
 - Recipient Division: OnSolve will modify the verbiage in alerts according to the division where the recipient resides. For example, in an alert sent from the Corporate Office to recipients in the Eastern Division and the Western Division, the Eastern Division recipients may hear the greeting “Attention Eastern Associates,” and the Western Division recipients may hear the greeting “Attention Western Associates.”
 - Notification Division: OnSolve will modify the verbiage in alerts based on the division where the alert resides. For example, an alert saved in the Security Division may be accessed and sent from initiators across multiple divisions, but the verbiage will be based on the Security Division, where the alert is saved.
7. Select **Customize**. The divisional tree opens.



8. Select the division where the customized verbiage will be stored. Custom verbiage carries down to any subdivisions below the selected division. For example, in the image above, selecting **Amber's Org** at the top modifies the verbiage for the **First subdivision** and **Second subdivision** below it.

9. In the **Custom Text** field, enter the custom verbiage that will be used instead of the default text. For text-based messages such as email, HTML source code may be entered to format text and display images within the alert's message.



10. Select **Save**.
11. If desired, repeat steps 6–10 to save another verbiage tag to another division.
12. If desired, repeat steps 4–10 for each language in which the verbiage tag should be modified.

Security

Multi-Factor Authentication

Multi-factor authentication (MFA) is an electronic authentication method by which users are granted access to the OnSolve Platform only after entering their correct username and password and then again proving their identity through one or more authentication methods. In this release of the OnSolve Platform, authorized users can set up MFA by requiring users to enter a code they receive via SMS.

Setup

Using MFA requires that users have at least one SMS device saved to their people record and that an authorized user enable the feature.

Save SMS Device

To use MFA in this release of the OnSolve Platform, users must have at least one SMS device saved to their people record. If they do not and attempt to sign in, these users receive a message telling them to be in touch with their organizational administrator to ensure they have a configured SMS device.

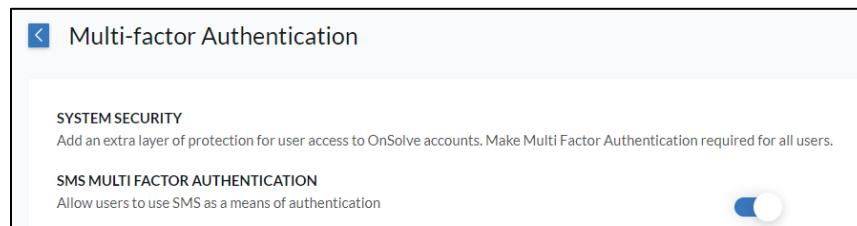
Note: SMS numbers used for MFA must be unique per user.

To save an SMS device, follow the instructions in [Devices](#), and choose **SMS** in step 3.

Enable MFA

To enable MFA

1. Navigate to **Configure > Security**.
2. Select **Multi-factor Authentication**.
3. Toggle on **SMS Multi-Factor Authentication**.



Reset MFA for a User

When MFA is configured for an organization, the first time any user with more than one SMS device saved to their people record signs in, they must choose which SMS number they'd like to use to receive their authentication code. This choice is saved for future sign-in attempts. If that SMS device is deleted, they will again choose from their available SMS numbers the next time they sign in. However, if they want to change the designated SMS number for another reason, an authorized user with the **Manage 2FA settings** global permission must complete a reset.

To reset MFA for a user

1. Navigate to that user's people record.
2. Select the **User Privileges** tab.
3. Select **Reset MFA**.

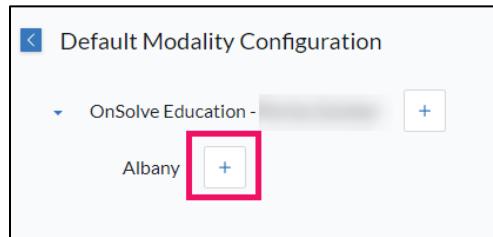


Default Modality Configuration

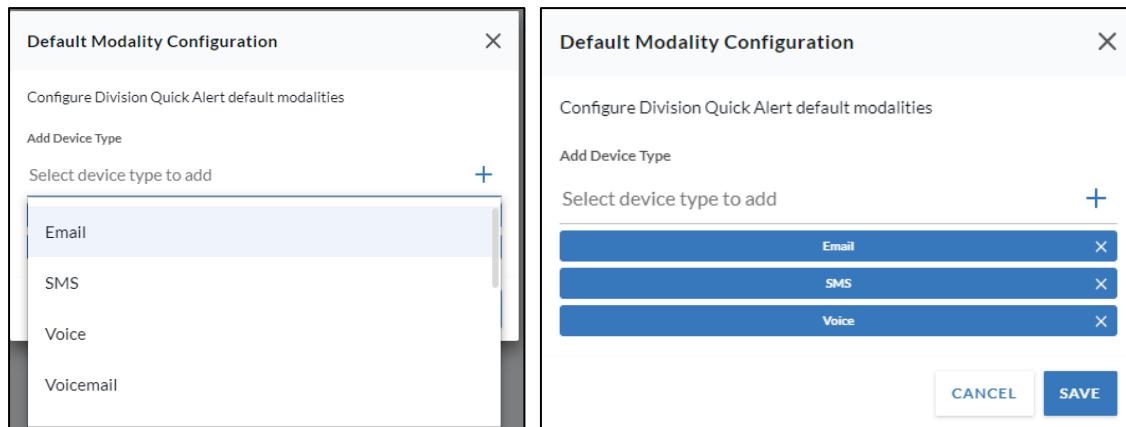
The Default Modality Configuration feature allows you to configure the default modalities for quick alerts.

To configure Quick Alert default modalities

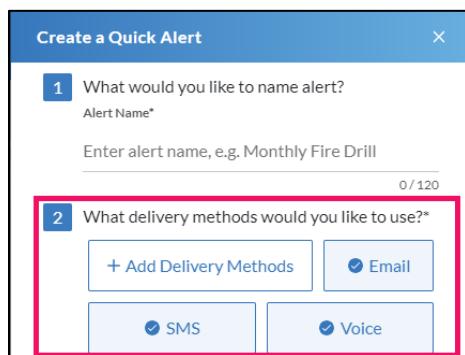
1. Navigate to **Configure > Default Modality Configuration**.
2. Select the plus next to the division to which this configuration should apply. An unconfigured subdivision inherits its parent division's configuration.



3. In the **Default Modality Configuration** modal that opens, click or tap the **Select device type to add** field and choose a device type. Repeat this until all desired device types are added.



4. Once all desired device types are added, select **Save**. The device types selected in step 3 are now preselected when you create a quick alert.





Section 8: Settings

The Settings menu houses settings that pertain to alert creation and delivery.

Note: In this release, these settings open in a new browser tab.

Alert Module

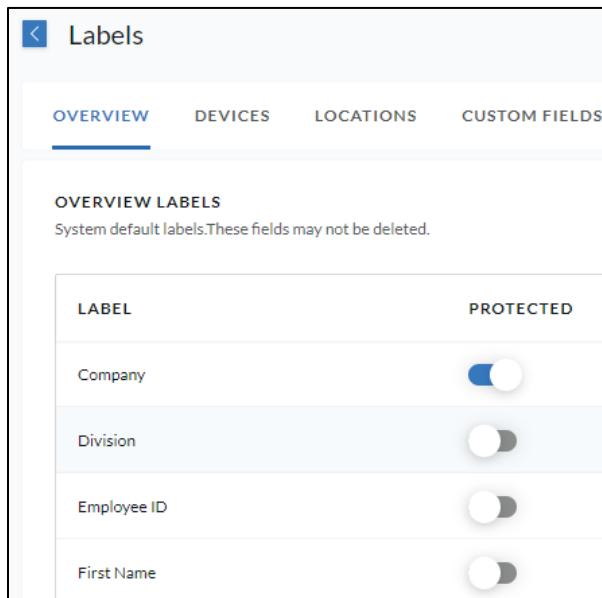
The **Alert Module** menu houses options pertaining to global default alert settings.

- For many of these settings, the authorized user can choose a default value for all alerts in the account.
- For many of these settings, the authorized user can also choose whether they are visible to senders. When a setting is *not* selected to be visible, it will not be visible to the user.

Labels

Overview Labels

Overview labels directly correlate with predefined data fields on the **Overview** and **User Privileges** tabs of a people record. On this tab of the **Labels** page, you can mark any of these fields as **Protected**. When a field or label is marked as protected, only those users with the **Edit Protected Data** permission may edit those fields.



The screenshot shows the 'Labels' page with the 'OVERVIEW' tab selected. The 'OVERVIEW LABELS' section displays four system default labels: 'Company', 'Division', 'Employee ID', and 'First Name'. Each label has a 'PROTECTED' toggle switch to its right. All four switches are currently turned on (blue), indicating that these fields are protected.

LABEL	PROTECTED
Company	<input checked="" type="checkbox"/>
Division	<input checked="" type="checkbox"/>
Employee ID	<input checked="" type="checkbox"/>
First Name	<input checked="" type="checkbox"/>

Device Labels

A device label is the naming of an associated contact point where the alert recipient may be reached (e.g., Cell Phone, Office Phone, SMS Text, TTY Device, Work Email, etc.). These labels are displayed when the "By Label" option is selected when composing an alert, which allows the alert sender to have the alert be sent only to contact points with a particular label assigned to them.

By customizing labels in the user interface, specific devices can be targeted to receive each alert. It is important to standardize these labels that describe recipient contact points. Device labels should always be identical to those used when performing data imports. Mislabeled devices can result in the wrong devices being used or intended recipients not receiving the alert.

Create a Device Label

You can define an unlimited number of device labels via the **Devices** section of the **Settings > Alert Module > Labels** option on the left navigation menu by entering the email/text and voice labels that identify the contact points.

- In addition to email, text device labels can include SMS, Fax, Pager One Way, Pager Two Way, Pager Numeric, TTY Phone, Desktop Alerts, and Mobile Application.
- Voice labels can include landlines, mobile phones, and satellite for domestic and international phone numbers.

To create a device label

1. Navigate to the **Settings > Alert Module > Labels** option on the left navigation menu. The **Labels** page opens.
2. Select **Add Device Label**.



3. The **Add Device Label** window opens.

A screenshot of the "Add Device Label" window. The window has a title bar "Add Device Label" and a close button "X".

DEVICE DETAILS
A device label is the naming of an associated contact point where the alert recipient may be reached.

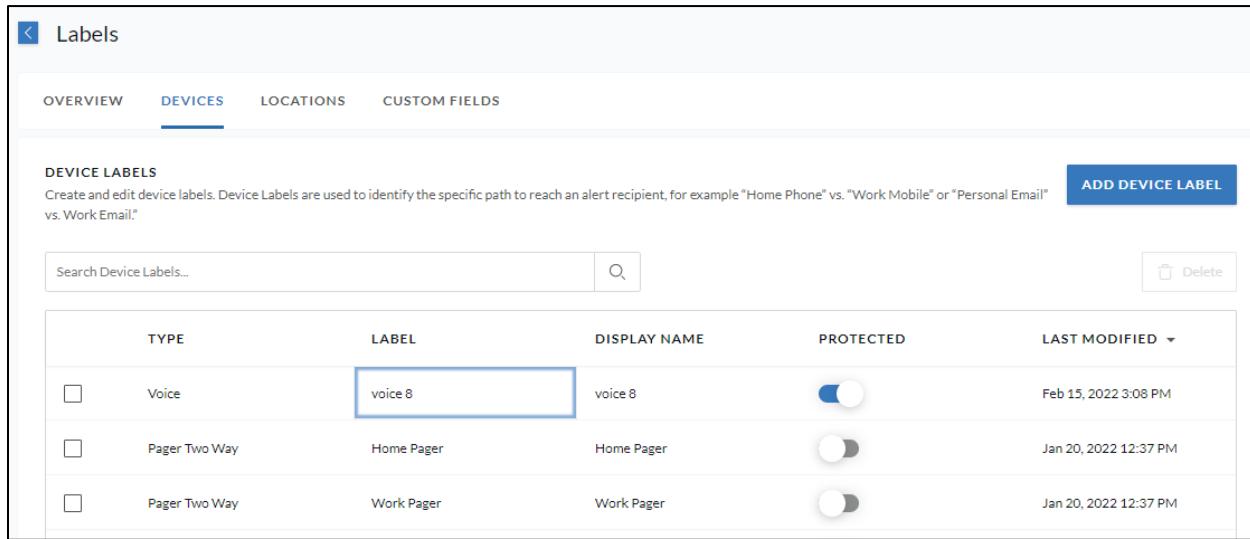
Device Type
Select type

Device Label
Enter device label
0 / 120

Display Name
Enter display name
0 / 120

Buttons: CANCEL (white text on grey background) and ADD (blue background with white text).

4. Select the **Device Type**.
5. Enter a **Device Label**.
6. Enter a **Display Name** for the label. The **Display Name** field allows assigning a custom descriptive name for the device displayed in **Device** drop-down lists throughout the system.
7. Select **Add**. The label is added to the **Device Labels** list.



Type	Label	Display Name	Protected	Last Modified
Voice	voice 8	voice 8	<input checked="" type="checkbox"/>	Feb 15, 2022 3:08 PM
Pager Two Way	Home Pager	Home Pager	<input type="checkbox"/>	Jan 20, 2022 12:37 PM
Pager Two Way	Work Pager	Work Pager	<input type="checkbox"/>	Jan 20, 2022 12:37 PM

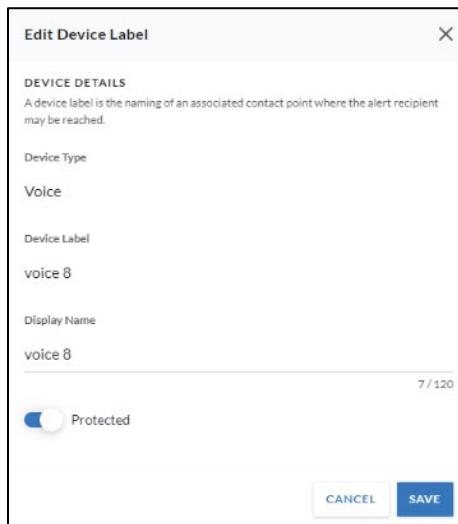
8. If desired, select the **Protected** toggle to make the label uneditable. The **Edit Device Label** window opens. Select the **Protected** toggle and select **Save**.

Modify a Device Label

Only a device label's **Display Name** can be modified. When this happens, the change is updated throughout the system: the display name change will be reflected for every contact with a device assigned that device label.

To modify a device label's display name

1. Select the desired device label. The **Edit Device Label** window opens.



2. Make any desired changes to the **Display Name** or **Protected** status and select **Save**.

Delete a Device Label

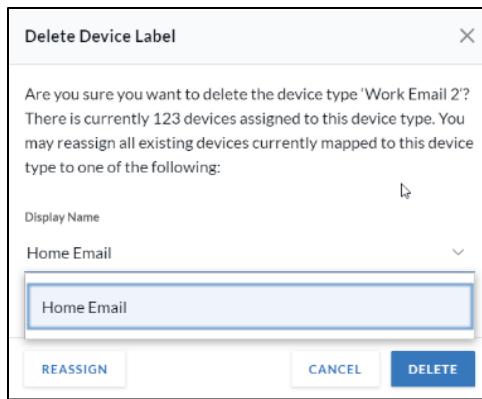
Device labels can be deleted one at a time from the **Labels** page.

1. Select the device label to be deleted.
2. Select the **Delete** icon.



3. To confirm the deletion, select **Delete**. However, if the label to be deleted is assigned to devices, users can first reassign those devices to an alternate label of the same device type. If desired, select an alternate label from the drop-down list, and select **Reassign**. All devices assigned that label will be reassigned to the chosen alternate label.

4. Back on the **Labels** page, reselect the desired label to delete, which now has zero devices assigned to it, and select **Delete**.

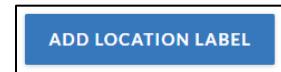


Location Labels

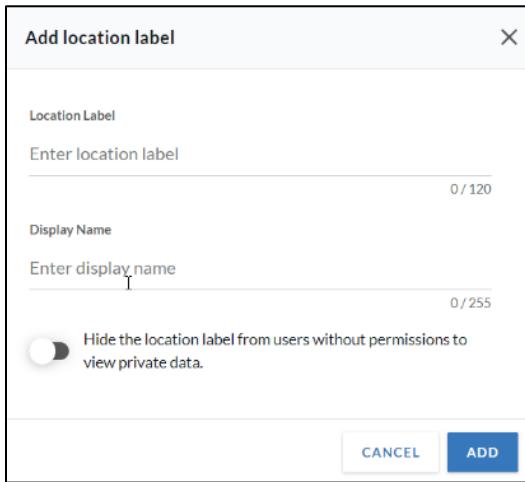
Location labels for location addresses are used in geo-enabled alerts when the Geo-Mapping feature is enabled.

Create a Location Label

1. Users can define up to eight location labels via the **Locations** section of the **Settings > Alert Module > Labels** option on the left navigation menu. The **Labels** page opens.
2. Select the **Locations** tab.
3. Select **Add Location Label**.



The **Add location label** window opens.



Add location label

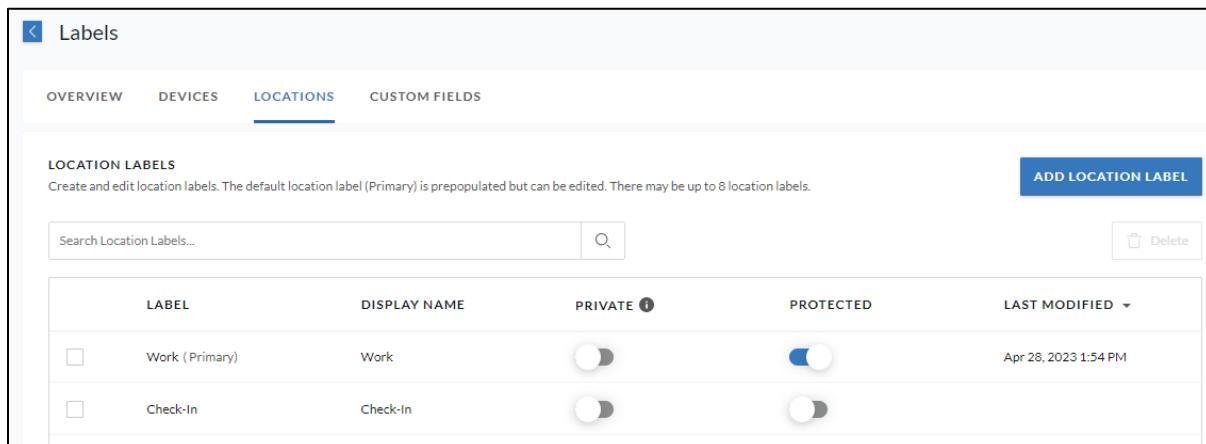
Location Label
Enter location label 0 / 120

Display Name
Enter display name 0 / 255

Hide the location label from users without permissions to view private data.

CANCEL **ADD**

4. Enter a **Location Label**.
5. Enter a **Display Name** for the label. The **Display Name** field allows assigning a custom descriptive name for the device displayed in **Device** drop-down lists throughout the system.
6. Select **Add**. The label is added to the **Location Labels** list.



Labels

OVERVIEW	DEVICES	LOCATIONS	CUSTOM FIELDS															
LOCATION LABELS Create and edit location labels. The default location label (Primary) is prepopulated but can be edited. There may be up to 8 location labels.																		
<input type="button" value="ADD LOCATION LABEL"/>																		
Search Location Labels... <input type="text"/> <input type="button" value="Search"/>																		
<table border="1"> <thead> <tr> <th>LABEL</th> <th>DISPLAY NAME</th> <th>PRIVATE <small>?</small></th> <th>PROTECTED</th> <th>LAST MODIFIED</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> Work (Primary)</td> <td>Work</td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td>Apr 28, 2023 1:54 PM</td> </tr> <tr> <td><input type="checkbox"/> Check-in</td> <td>Check-in</td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td></td> </tr> </tbody> </table>				LABEL	DISPLAY NAME	PRIVATE <small>?</small>	PROTECTED	LAST MODIFIED	<input type="checkbox"/> Work (Primary)	Work	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Apr 28, 2023 1:54 PM	<input type="checkbox"/> Check-in	Check-in	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
LABEL	DISPLAY NAME	PRIVATE <small>?</small>	PROTECTED	LAST MODIFIED														
<input type="checkbox"/> Work (Primary)	Work	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Apr 28, 2023 1:54 PM														
<input type="checkbox"/> Check-in	Check-in	<input type="checkbox"/>	<input checked="" type="checkbox"/>															

7. If desired, select the **Private** toggle to hide the label from those who do not have permission to view private data.
8. If desired, select the **Protected** toggle to make the label uneditable. The **Edit Location Label** window opens. Select the **Protected** toggle and select **Save**.

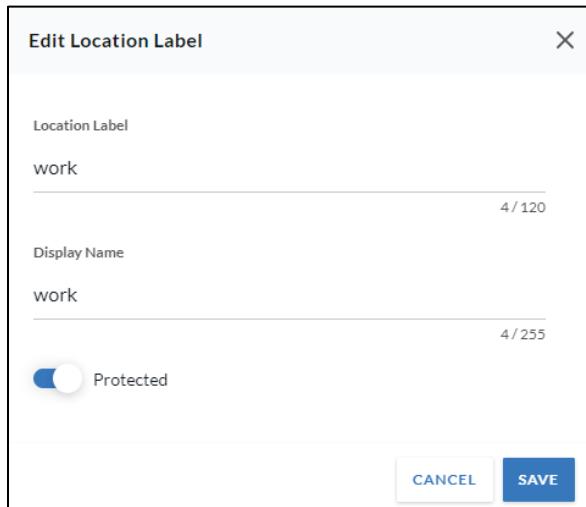
Modify a Location Label

A device label's name and **Display Name** can both be modified. When the label's name is modified, no changes are visible to contacts with locations assigned that location label since only the **Display Name** is displayed on people records. When the **Display Name** is modified, the change is updated

throughout the system: the display name change will be reflected for every contact who has a location assigned that location label.

To modify a location label

1. Select the desired location label. The **Edit Location Label** window opens.



The screenshot shows the 'Edit Location Label' dialog box. It contains two text input fields: 'Location Label' with the value 'work' and 'Display Name' also with the value 'work'. Both fields have character count indicators: '4 / 120' for Location Label and '4 / 255' for Display Name. Below these is a 'Protected' toggle switch, which is turned on (blue). At the bottom are 'CANCEL' and 'SAVE' buttons.

2. Make any desired changes to the **Location Label**, **Display Name**, or **Protected** status, and select **Save**.

Delete a Location Label

Location labels can be deleted one at a time from the **Labels** page. If the label to be deleted is assigned to locations, those locations will also be deleted.

1. Select the location label to be deleted.
2. Select the **Delete** icon.
3. To confirm the deletion, select **Delete**. If the label to be deleted is assigned to locations, those locations will also be deleted.

Custom Fields

A custom field is an optional data field (open text field) corresponding to a custom attribute for a contact (e.g., office name, department, employee status) that can be labeled and populated at the organization's preference. You can define an unlimited number of custom fields.

- These attributes are used for grouping alert recipients.

- Custom fields are also required on the people record of all alert recipients when using dynamic recipient filtering.

Create Contact

OVERVIEW DEVICES CUSTOM FIELDS LOCATIONS USER PRIVILEGES

CUSTOM FIELDS

Custom fields are used as a method of communicating with user. Add a new one or edit an existing one.

ADD CUSTOM FIELD

CUSTOM FIELD	VALUE
Home Address	2 Tower Place

Create a Custom Field

- Navigate to the **Custom Fields** tab of the **Settings > Alert Module > Labels** option on the left navigation menu. The **Labels** page opens.
- Select the **Custom Fields** tab.
- Select **Add Custom Field**. The **Add Custom Field Label** window opens.

Add Custom Field Label

Custom Field Label

Enter custom field label

0 / 120

CANCEL ADD

- Enter a **Custom Field Label**.
- Select **Add**. The label will be added to the **Custom Fields** list.

Labels

OVERVIEW DEVICES LOCATIONS CUSTOM FIELDS

CUSTOM FIELDS

Create and edit optional data fields. Custom fields can be any custom attribute of a contact based on an organization's preferences, for example Department, Title, Job Code, etc.

ADD CUSTOM FIELD

<input type="checkbox"/>	CUSTOM FIELD	PROTECTED	LAST MODIFIED
<input type="checkbox"/>	Variables	<input checked="" type="checkbox"/>	Feb 15, 2022 4:09 PM
<input type="checkbox"/>	Birthday	<input type="checkbox"/>	Sep 29, 2021 11:43 AM

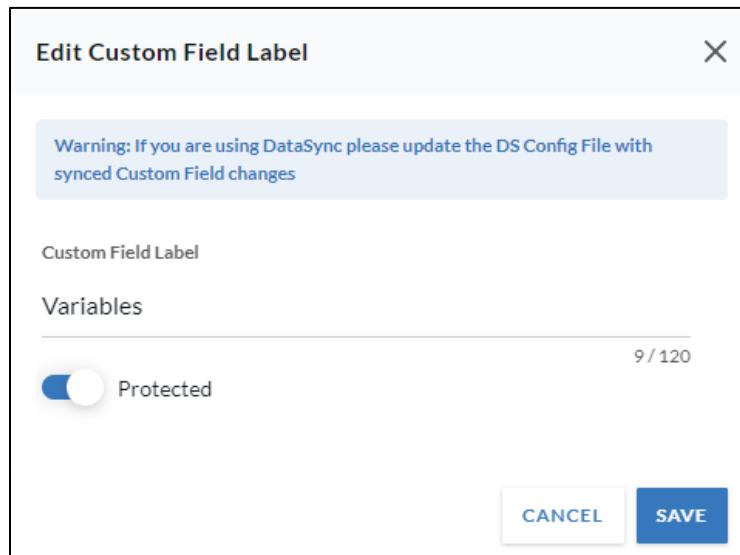
6. If desired, select the **Protected** toggle to make the custom field uneditable. The **Edit Custom Field** window opens. Select the **Protected** toggle and select **Save**.

Modify a Custom Field

When a custom field name is modified, the change is updated throughout the system: the change will be reflected for every contact who has that custom field saved to their profile.

To modify a custom field

1. Select the desired custom field. The **Edit Custom Field Label** window opens.



2. Make any desired changes to the **Custom Field Label** or **Protected** status and select **Save**.

Delete a Custom Field

Custom Fields can be deleted one at a time from the **Labels** page. These custom fields are also deleted from any people records to which they were added.

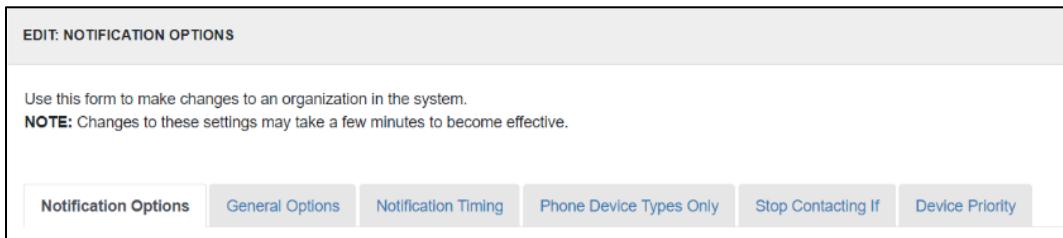
1. Select the location label(s) to be deleted.
2. Select the **Delete** icon.
3. To confirm the deletion, select **Delete**.

If a custom field is mistakenly deleted, the user can undo the deletion by selecting **Undo** in the dialog box in the upper right corner. The dialog box closes after 60 seconds, after which the deletion is permanent.



Alert Options

The Alert Options menu opens to a page with six tabs: **Notification Options**, **General Options**, **Notification Timing**, **Phone Device Types Only**, **Stop Contacting If**, and **Device Priority**. Read about each tab and its associated settings below.



EDIT: NOTIFICATION OPTIONS

Use this form to make changes to an organization in the system.

NOTE: Changes to these settings may take a few minutes to become effective.

Notification Options General Options Notification Timing Phone Device Types Only Stop Contacting If Device Priority

Notification Options

Response Options: Choose whether the option to include response options with Bulletin Board alerts appears when creating a new alert.

Broadcast Duration: Set the default duration displayed for all Broadcast alerts.

General Options

Settings in the **General Options** tab can be set as a default and made to be visible or invisible on the **Advanced Settings** page.

Initiator Alias: Define the sender name for text notifications for email sender and voice alerts when the Play Greeting or Validate Recipient options are active. When not defined, the sender of the alert is displayed.

Play Greeting: The OnSolve Platform plays an introductory message when the phone is answered that identifies the sender and recipient of the alert.

Use Alternates: When an alert is sent, the OnSolve Platform will check the recipient's people record for alternate contacts in the case that the intended recipient does not respond to the alert. Alternate contacts are managed in the recipient's people record in the **Overview** tab.

Use Topics: Allow senders to send alerts to recipients based on topics. Recipients must have **View Topics** permission in their role to receive subscription-based messages.

Send to Subscribers: Use with **Subscriptions** feature. When an alert is sent, the OnSolve Platform checks each recipient's people record for subscribed topics. The alert is delivered to the subscribed recipient if a matching Category, Severity, and Priority are found.

Note: **Use Topics** must be active, and recipients must have the **View Topics** permission to receive subscription-based alerts.

Report Recipients: Send alert reports to any contact in the system, whether or not they are a recipient of the alert. Use in combination with the **Add Report Recipients** advanced setting when creating an alert. By default, alert reports are sent to those report recipients when the alert goes from an *In-Progress* state to a *Completed* state. All report recipients must have an email address and a report format saved within the recipient's people record.

Send Periodic Reports/Send Every: Used specifically with the **Report Recipients** setting. Specify a time interval to send multiple alert reports throughout the duration of the alert. Each new report includes the latest contact and response data available.

Identical Device Suppression: When enabled, if multiple recipients share the same phone number, the system will only contact the device once rather than individually for each recipient. When disabled, the system will attempt to contact each recipient individually, regardless if they share the same phone number.

Invalid SMS Response: Activate an autoreply when an unrecognized response is received from an SMS device. The autoreply includes instructions to enter a recognizable response.

Email Priority: Allow alert senders to choose the priority level for email alerts in recipients' inboxes. Set the default to **Lowest, Low, Normal, High, or Highest**.

Digitally Sign Emails: Include a digital signature with email alerts to confirm the alert is from a trusted source. An S/MIME key must be uploaded to the system to use this feature.

Allow Response Change: Allow recipients to change their response after their initial response has been submitted.

Notification Timing

Calling Order: Used in the Quota alert method only. Set the default calling order to the Vertical Calling Matrix or the Horizontal Calling Matrix.

- **Vertical Matrix:** The OnSolve Platform cycles through every designated device for an individual, for the designated number of contact attempt cycles, before moving on to the next recipient until the Success response(s) is/are registered.
- **Horizontal Matrix:** The OnSolve Platform contacts only the Priority One device for each recipient first, then attempts the Priority 2 device, and so on, until the Success response(s) is/are registered.

Contact Attempt Cycles: Specify the number of times the alert cycles through recipient devices in the event of a non-response to the alert. Select the toggle to enable, then enter a digit in the text field.

Contact Cycle Delay: Specify the amount of time (in hours and minutes) the OnSolve Platform should wait between consecutive contact attempt cycles in the event of a non-response to the alert.

The delay begins when the first device in a recipient's device list is contacted. Contact Cycle Delay applies when Contact Attempt Cycles is set to 2 or higher.

Strict Device Delay: A fixed delay between each device in a recipient's contact cycle (both text and voice devices). If **Strict Device Delay** is checked, the **Text Device Delay** field becomes the delay time used for every device. Strict Device Delay extends the time to complete the contact cycle for each recipient.

Text Device Delay: Specify the amount of time the system should wait between consecutive contact attempt cycles for text-based devices in the event of a non-response to the alert. Select the toggle to enable, then enter the delay length in hours and minutes.

Text Contact Once: The OnSolve Platform sends the alert to text-based devices only once, ignoring further contact attempt cycles. This setting corresponds with the **Only contact once** advanced setting.

Phone Device Types Only

Validate Recipient: When **Validate Recipient** is enabled, voice alerts begin with four questions to determine if the intended recipient has answered the call.

Example: *This is <Recipient Name>. Please deliver my alert now, press 1. Please hold; I'll get <Recipient Name>, press 2. <Recipient Name> is not here right now, press 3. You have reached the wrong number; there is no <Recipient Name> at this number, press 9.* (Pressing "9" flags the number as a "Bad Address" in the user's profile, and it will not be contacted again in future alerts.)

Replay Messages: Add a voice prompt to an alert indicating the recipient can press zero to hear the alert again. Checking the box only adds the voice prompt to the alert instructions.

Confirm Response: Use the Confirm Response feature to add a voice prompt to an alert to confirm the selected response. Example: *You selected option 2. If this is correct, press 1.*

Requires PIN: Add a voice prompt to ask the recipient to enter their PIN to access and listen to the alert. The PIN is in the **Overview** tab of each recipient's people record.

Notes

The default PIN is 9999 for every contact unless it has been changed and saved in that person's record.

OnSolve does not leave voicemail messages when a PIN is required.

Select Language: Used only when an alert was created using multiple languages. If enabled, when a recipient answers the phone, they will be offered a choice of languages in which the alert will be played. Only the languages used in the alert are offered. If disabled, the OnSolve Platform will deliver the alert in the default language saved in each user's profile.

Leave Message: Determine what information is left on a voicemail if the recipient does not answer. These settings correspond to the **Leave a voicemail message** advanced setting.

Expedited Delivery: Secures additional telephony ports to prioritize an alert when ports may already be in use by other (non-urgent) alerts. Used with internal company phone tied to a PBX system only (work phones), it does not apply to mobile phones, home phones, etc. Users must have the **Expedited Delivery (Global)** permission included in their role to use this feature.

Note: Additional telephone transaction fees apply when using this feature.

Call Routing Rollover (in a future release): Used with international phone calls to deliver the voice alert from the OnSolve data center located closest to the recipient's location. Location is based on the recipient's country code of the phone number called. Most organizations leave this feature checked by default and not visible on the alert overview, so senders cannot disable it.

Stop Contacting If

Recipient Listened to Entire Message: If the recipient answers the phone and the message is played in full, OnSolve will call that a good contact and make no further attempts to contact that recipient on any device. If the recipient hangs up before the entire message is played, another contact attempt will occur during the next contact cycle (if there is one).

Recipient Listened to Partial Message: If the recipient answers the phone and the message begins to play, OnSolve will call that a good contact and make no further attempts to contact that recipient on any device. If the recipient hangs up before the entire message is played, the alert will stop, and no further attempts to contact the recipient will be made.

Partial Message Left on Voicemail: If the call goes to voicemail and the message begins to play, OnSolve will call that a good contact and make no further attempts to contact that recipient on any device. If the call is disconnected before the entire message is left on the voicemail, the alert will stop, and no further attempts to contact the recipient will be made.

Entire Message Left on Voicemail: If the call goes to voicemail and the entire message is left on the voicemail, OnSolve will call that a good contact and make no further attempts to contact that recipient on any device. If the call is disconnected before the entire message is left on the voicemail, another contact attempt will occur during the next contact cycle (if there is one).

Device Priority

When Priority defaults are set, they are reflected in the **Delivery Methods** section of creating an alert.

Device Priority: Create a standard device contact order for every alert. Choose the devices and the order in which they are contacted.

Override Default Status Only (in a future release): If using multiple Location Statuses, the alert will only override the Default Location Status with the Device Priority settings. If another Location Status is active (Weekend, Remote Office, or Holiday), the notification will honor the active Location Status, not the Device Priority settings.

Division ANI

ANI stands for Automated Number Identifier. The OnSolve Platform can display a division-specific phone number on the recipient's Caller ID when the OnSolve Platform contacts their phone device.

If a custom ANI is not set, the default Caller ID is:

Within the US:

1-866-609-8026

Note: This number is respected by US domestic telephone companies and is not changed unless a custom ANI is set up.

EU (either sent from the EU or from the US to the EU):

+1 571-380-5920

Note: This number is not necessarily respected by telephone companies in other countries and may be changed by the receiving phone carrier to another number.

To set Division ANI

1. Navigate to **Settings > Alert Module > Division ANI**. The **Edit: Division ANI** page opens.
2. Select the desired division. The division selected applies the ANI to all alerts saved to that same division. All recipients of said alerts will see the ANI specified regardless of the division the recipient resides in. The **Set ANI** section opens to the right.
3. Enter the desired phone number. This field can only accept numerals. Select **Save**.

Call Throttling

The Call Throttling setting allows management of the maximum number of concurrent telephony connections or calls allowed for a specified prefix. Call throttling ensures the lines can detect congestion and other busy/error conditions and prevent call overloads. It also prevents the system from flooding the recipient PBX, devices, or networks with calls that will fail or make emergencies worse by tying up available lines.

To set Call Throttling rules

1. Navigate to **Settings > Call Throttling**. The **Edit: Call Throttling** page opens.

Phone Prefix	Ports
+1518881	10 
<input type="text"/>	<input type="text"/> 
Add	

2. Enter the relevant **Phone Prefix**. For example:
 - +1 Area Code (+1858, +1619, etc.)
 - +1 Area Code Prefix (+1858724)
 - +1 Area Code Prefix Number (+18587241200)
3. In the **Ports** field, enter the maximum number of concurrent telephony connections or calls allowed for the corresponding phone prefix.
4. Select **Add**.
5. Optionally, add more **Phone Prefix** and **Ports** combinations.
6. Select **Save**.

Suppressed Alerts

If duplicate filter criteria have been defined in the **Edit Duplicate Filters** page, the **View Duplicate Suppression Report** page can be used to view statistics about duplicate alerts that have been suppressed in the OnSolve system. See [Duplicate Filters](#) for more on how OnSolve handles and reports duplicate alerts.

To view suppressed alerts, navigate to **Settings > Alert Module > Suppressed Alerts**. The **View: Suppressed Notifications Report** page opens with the most recent suppressed alert listed at the top.

Allowed SMS

Use this setting to send SMS alerts to contacts regardless of whether they opted out of SMS alerts. Enter the applicable phone numbers and save the page.

Note: The ability for contacts to opt out of SMS alerts will come in a future release of the OnSolve Platform.

Assign SMS Profiles

SMS Profiles, assigned per division, allow clients to use short or long SMS codes for different classes of alerts. For example, a client may use only short code 22222 in the U.S. for emergencies, but short code 33333 for regular IT alerts.

SMS short or long codes vary by country, which precludes specifying a specific source short code for certain messages—short code will not be valid for all countries. An SMS profile, therefore, consists of a set of source short/long codes on a per-country basis, plus fail-over information. A single profile called "Profile 1" may use 22222 as the source short code in the U.S., +44 4444444444 in the U.K., and it might fail over to 33333 in the U.S. and +44 5555555555 in the UK.

To assign an SMS profile

1. Select the desired division.
2. Select the desired profile or **Inherit from Parent** in the **SMS Profile** drop-down list.
3. Select **Save**.

Edit TTS Voices

The TTS setting allows you to select which “voice” is used for voice alerts that use the Text-To-Speech (TTS) engine.

To set the TTS

1. Navigate to **Settings > Alert Module > Edit TTS Voices**. The **Edit: TTS** page opens.
2. Select the desired division.
3. For each language listed, choose a voice from the drop-down list or have that division inherit its parent's TTS voice.
4. Select **Save**.

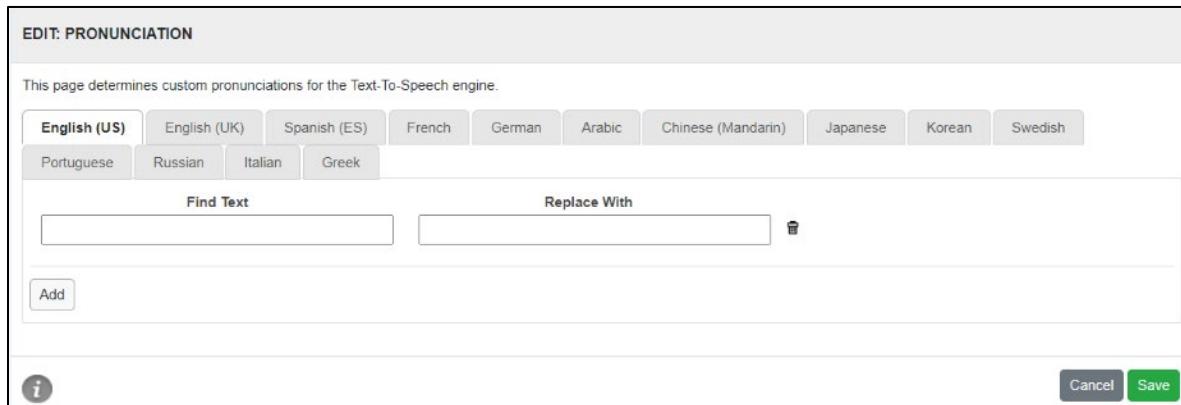
Edit Pronunciations

The Edit Pronunciation feature allows for the modification of the text-to-speech engine. Using phonetic spelling, the text-to-speech engine can be taught to pronounce specific words correctly. In addition to just words, the Edit Pronunciation feature can also be used to decipher numbers, ITSM error codes, or acronyms and translate them into common language.

To edit a pronunciation

1. Navigate to **Settings > Alert Module > Edit Pronunciations**.

2. Select the desired division. The **Edit: Pronunciation** page opens.



The screenshot shows the 'Edit: PRONUNCIATION' page. At the top, there's a header bar with the title 'EDIT: PRONUNCIATION'. Below it, a message says 'This page determines custom pronunciations for the Text-To-Speech engine.' A horizontal row of language tabs is present: English (US) (selected), English (UK), Spanish (ES), French, German, Arabic, Chinese (Mandarin), Japanese, Korean, and Swedish. Underneath these tabs are smaller buttons for Portuguese, Russian, Italian, and Greek. The main area contains two input fields: 'Find Text' and 'Replace With', with a 'Cancel' button next to them. Below these fields is a 'Add' button. At the bottom right are 'Cancel' and 'Save' buttons, with an information icon ('i') to the left of the 'Save' button.

3. Select the desired language tab.
4. Enter the name/word/acronym in the **Find Text** field as it is typically written.
5. In the **Replace With** field, enter the phonetic spelling of that word.
6. Optionally, select **Add** to add more pronunciations.
7. When finished, select **Save**.

Duplicate Filters

Users operating the OnSolve Platform in Information Technology Service Management (ITSM) environments can receive duplicate alerts about IT events that occur elsewhere in the organization. This condition is referred to as a "message flood." To prevent this and not overwhelm recipient(s) with these alerts, use the **Settings > Alert Module > Duplicate Filters** option to define automatic filtering and "throttling" of duplicate alerts for divisions.

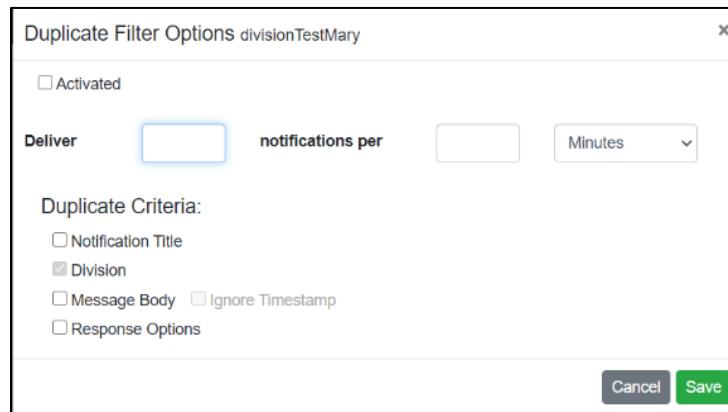
Duplicate alerts are alerts with the same title, message body, or response options (or a combination thereof) defined on the **Duplicate Filters** page.

Throttling queues/controls the flow of alerts based on time (deliver X number of alerts per second, per minute, per hour). This suppresses alert delivery within the OnSolve Platform.

Duplicate filtering affects all alerts in the OnSolve Platform, regardless of the specific mechanism used to create and send the alert. Duplicate suppression takes precedence over all other processing of incoming alerts (e.g., Message ignores and Topic Subscriptions).

To create duplicate filters

1. Navigate to **Settings > Alert Module > Duplicate Filters**. The **Edit: Duplicate Filters** page opens.
2. Select the desired division. The **Duplicate Filter Options** window opens.



Duplicate Filter Options divisionTestMary

Activated

Deliver notifications per Minutes

Duplicate Criteria:

- Notification Title
- Division
- Message Body Ignore Timestamp
- Response Options

Cancel Save

3. Select the **Activated** checkbox.
4. Enter the number of alerts to be delivered, the frequency of those deliveries, and choose the unit of frequency from the drop-down list.



Deliver 3 notifications per 1 Minutes

Minutes
Days
Weeks

5. Choose which criteria should be used for the filter. Options are:
 - Notification Title
 - Division (uneditable as Division was selected in step 2)
 - Message Body with the additional option of ignoring the timestamp
 - Response Options
6. Select **Save**.

When a filter is saved and activated, that is indicated next to the division it has been applied to.



Alert Retrieval

The Alert Retrieval setting allows authorized users to designate the order in which alerts are presented to recipients in their Alert Inbox and when they call in to retrieve alerts.

To designate an order

1. Navigate to **Settings > Alert Module > Alert Retrieval**. The **Edit: Notification Retrieval** page opens.
2. From the drop-down list, choose your desired alert retrieval order. Options are **Use System Default**, **List Oldest Notifications First**, and **List Newest Notifications First**.
3. Select **Save**.

Section 9: OnSolve Mobile

Overview

OnSolve Mobile is an app designed to provide individuals and organizations real-time critical communication and emergency alerts. The app is available for both iOS and Android devices.

There are two ways to use the OnSolve Mobile app:

- Recipients only. Authorized recipients can sign into the OnSolve Mobile app with either an SMS phone number or an email address. They can then use the app to check in, send an SOS, report an incident as it occurs (LookOut), or receive an alert.
- Authorized senders. Authorized senders sign in with the same username and password as the web UI. Almost every task that can be completed via the OnSolve Platform web user interface can also be completed using OnSolve Mobile. Additionally, authorized senders can send an SOS, use the Life Check timer, or report an incident as it occurs. When logged in as a sender, you can toggle to the Recipients interface and receive alerts.

Since all received alerts are stored in recipients' Alert Inboxes, recipients can retrieve alerts via the app no matter the alert sender's selected delivery methods. Once signed in, tap the Inbox icon at the bottom of the dashboard. However, if the sender chooses the mobile app as a delivery method, recipients with the app do not need to actively retrieve it and, instead, see the alert (or push notification) on their phones.

When creating an alert, senders can select the mobile app delivery method (if not already selected by default). Recipients then receive the alert via the app if they have downloaded it and are signed in. Recipients can even receive the alert if the app is closed, in which case a push notification is sent to the phone, so alerts are not missed.

To learn how to use OnSolve Mobile, please see the *OnSolve Mobile User Guide*.

Geofenced-Enabled Alerts

In addition to standard alerting methods where the sender selects the recipients from a list or group, OnSolve offers location-based alerts with map groups. Map groups pull recipients into a group based on location and can be created via the Groups page or the Control Center map. Map groups work in two ways, the difference being at what point the OnSolve Platform queries contacts' locations:

- **Geofence-enabled.** A map group with geofence enabled includes all contacts with static locations saved in their people record in the map shape and all OnSolve Mobile app users in the map shape, provided Mobile App is a selected delivery method. If a static location that falls within the map shape is added to a contact's record after the alert has been sent, but while the alert is still active, the contact receives the alert when their new location is saved. Likewise, if an OnSolve Mobile app user is outside the geofence when the alert is sent but enters the geofence while the alert is still active, they receive the alert once they enter the geofence.

The continuous location coordinates (latitude and longitude) are not tracked by the OnSolve Platform central application; they remain within the mobile device at all times. When a geofence-enabled alert is sent, all instances of the OnSolve Mobile application assigned to the organization receive the alert. The OnSolve Mobile app then compares its current location coordinates obtained from the mobile OS with the shape coordinates received with the alert and only displays the alert to the user if the current location is within the geofence. The app does not report the coordinates to the central Platform.

- **Geofence-disabled.** A map group with geofence disabled includes only the contacts with a location in their people record that falls in the map shape. With geofence OFF, the mobile device's location is not a factor when determining whether to display the alert in OnSolve Mobile.

Section 10: Risk Intelligence

Overview

OnSolve Risk Intelligence provides an AI-powered solution that accelerates the entire critical event management process by filtering through massive amounts of data to give you the information you need when you need it most.

During a crisis, when Every Minute Counts™, OnSolve Risk Intelligence delivers fast, accurate, and relevant intelligence so that you can make informed and proactive decisions to protect people, places, and property.

Your organization can monitor critical events before they potentially become disruptive events or incidents. Here are only a few of the OnSolve Risk Intelligence capabilities that target proactive risk awareness about local and global threats:

- AI-powered and analyst-vetted event intelligence maximizes the relevance of events.
- Validated data sources used for event detection provide timely, relevant, and comprehensive event notifications affecting locations globally.
- Determination of the location of critical events and proximity to your people and assets can be easily identified on your event feed and map view to make you aware of potential impacts.
- OnSolve Risk Intelligence allows you to filter over 50 critical event types so your organization can get alerted on those events that potentially impact you. Administrators can customize the account's default impact radius and severity rating settings for each event type in the account's risk categories Hazmat, Transportation, Natural Disaster, Crime, Weather, Infrastructure, Civil Unrest, and Geopolitical.
- Detailed filtering for facilities and teams helps you quickly identify and monitor detected events that could affect your people and assets. Event filter criteria can include event types; severity rating range of your choice; data sources; and keywords and phrases to be filtered in and out of your event filters.
- Facility labels allow you to identify critical events near your employees, whether working in offices or other facilities or from their homes.

For detailed instructions on using OnSolve Risk Intelligence, see the *OnSolve Risk Intelligence for OP User Guide*.

Section 11: Appendices

Appendix A: Glossary

Term	Definition
Administrator	The predefined user role that has full access to the account, including default configurations, feature settings, user role creation, and access to subaccounts.
Affiliations	The section of a people record that lists all instances where that contact: <ul style="list-style-type: none">• Is a member of a group (including a map group)• Is a member of a schedule• Has been listed as an alternate contact• Has been included as a recipient in an alert and the date that the affiliation started.
Alert	Voice or text communication composed by the administrator or authorized user to be delivered promptly by the OnSolve Platform to one or more designated recipients in the organization's account. Also called a message.
Alert Analytics	A feature that allows authorized users to quickly and easily analyze the results of a sent alert, determine high-level overview, manually add recipients as being accounted for, and resend alerts to all or portions of the alert recipients as needed.
Alert Duration	The length of time for which the alert is active. Once the alert duration expires, the system stops sending it out, whether or not all contact attempt cycles were completed and despite any other setting that would otherwise cause the alert to continue.
Alert Recipient	See Contact.
Alert Template	A saved alert that includes at least one custom alert variable or that allows the sender to select additional recipients.
Alert Type	The method by which recipients are contacted. Types include Broadcast and Quota.
Alert Variable	A placeholder used in parts of an alert that is replaced with recipient-specific values at the time of sending.
Alternate Contacts	Contacts who receive alerts when the primary contact cannot be reached.
Audit Trail	A log of all events that have occurred in the account.
Broadcast	The alert type that allows users to send an alert to many recipients at one time. It is used to disseminate information to many people very quickly.
Bulletin Board	The alert type that allows users to call in and listen to a posted audio recording.

Term	Definition
Cascade Alert	An alert that is sent automatically based on the response of recipients to an initial alert. Each cascade alert has its own recipients, message, response options, delivery methods, advanced settings, and generates its own report.
Contact	A person who has a record saved in the account. Sometimes referred to in the UI as People (preferred term).
Desired Response(s)	In a quota alert, the response option(s) designated as the one(s) to count toward the Number of People Needed.
Device	Any point of contact that can receive an alert, such as SMS, voice, email, Desktop Alert app, OnSolve Mobile, and Slack.
Division	A partition of an organization based on how the administrator(s) want to isolate users, particularly senders, from other users and data.
Dynamic Group	Any group that is defined by membership criteria.
Follow-up Question	One of the available actions in a response option allowing the sender to collect additional information from those recipients who have responded with a specific response.
Free-form Response	A type of response to a follow-up question when adding response options to an alert. It allows recipients to type their responses freely.
Group	A set of alert recipients or contacts. A collection ranging from one to all contacts in the OnSolve Platform account grouped to facilitate sending an alert simultaneously to a specific targeted audience; this may or may not correspond to a distribution list.
Initiator (Alert Sender)	The predefined user role that may create, edit, assign, and send alerts. Also called Alert Sender.
Integrations	A feature that allows you to connect your account with various third-party applications. Depending on the application, you can use the integration for syncing contacts or sending alerts.
Linked Alert	A group of already saved alerts that can be sent simultaneously.
Lockbox	A feature that allows authorized users to upload files that can then be attached to an alert. Users can upload secure, encrypted files that can be sent to mobile app users only, as well as shared files that are accessible via any text-based delivery method.
LookOut	A feature that allows mobile users to report suspicious activities or emergency incidents and send location-specific information in real time via OnSolve Mobile.

Term	Definition
Map Group	A group that consists of recipients based on their geographic location on a map. The Map Groups feature targets an area on a map to instantly identify and send alerts to individuals within that area.
Multiple Choice	A type of response to a follow-up question when adding response options to an alert. It allows the sender to create an unlimited number of response options from which recipients may choose.
Number of People Needed	In a quota alert, the number of recipients needed to respond with the Desired Response(s). When this number is met, the alert ends.
On-Call Scheduling	A feature that allows administrators and authorized users to set up an organized work plan. Each schedule contains one or more shifts consisting of a time period with an associated list of recipients or groups to whom alerts may be sent. When an alert is sent to a schedule, the OnSolve Platform determines which shifts are active at that time and sends the alert to the users associated with those shifts. If no users are available, no alert will be sent.
People	Contacts in the OnSolve Platform who have saved people records in the account (preferred term over contacts).
People Record	A record that contains a contact's or person's data, such as personal information, devices, user privileges, address information, custom fields, and affiliations.
Quick Alert	An alert that can be created and sent from the control center view. A quick alert does not offer as many features as an advanced alert.
Quota	The alert type that allows users to find a defined number of recipients who successfully respond to an alert. Once that number of recipients has responded, all subsequent responses will be ignored.
Recipient	A contact who has been saved to an alert or received an alert and may or may not have access to the OnSolve Platform user interface.
Recorded Response	A type of response to a follow-up question when adding response options to an alert. It allows recipients to provide their responses by recording their voices.
Response Options	A list of available choices attached to an alert. The recipient can choose an option as a response to the sender, which is then captured in Analytics and the report.
Scenario Library	A repository of commonly used alerts defined by industry and event type.
Sender Alias	An advanced setting that allows users to define the sender name in alerts where the sender's first and last name would normally be displayed.
SOS	A feature that allows mobile app users in urgent situations to connect to the appropriate emergency services phone number with a tap of a button.

Term	Definition
Shift	A schedule element defined by start and end times. When sending alerts to schedules, recipients are determined by who is assigned to the active shift at the time of sending.
Static Group	A group created by selecting specific alert recipients as members.
Tier	An escalation level within a schedule's shift.
Topics	A feature that allows alert-senders to determine their recipients based on categories, priorities, and severities to which contacts in the account have subscribed.
Unique ID	A unique identifier (such as an Employee Identification Number) optionally associated with a contact. Primary Key used to identify existing records during data maintenance. Also called Client Contact ID.
User	Any person with access to the OnSolve Platform user interface.

Appendix B: Ad Hoc Reporting Resources

Category	Resource
Contact	First Name
	Middle Name
	Last Name
	Username
	Unique ID
	Company Name
	Job Title
	Time Zone
	Language
	Last Login
	Contact Division Name
	Contact Division Path
	Contact Role Name
	Contact Group Name
	Contact Group Type
	Contact Group Division Name
	Contact Group Division Path
Role	Role Name
	Role Division Name
	Role Division Path
Alert	Alert Name
	Alert Type
	Alert Feature
	Alert Division Name

Category	Resource
	Alert Division Path
	Alert Category Description
	Alert Priority Description
	Alert Severity Description
	Sender Alias
	Contact Attempt Cycles
	Contact Cycle Delay
	Text Device Delay
Sent Alert	Sent Alert Name
	Sent Alert Type
	Sent Alert Feature
	Sent Alert Time Sent
	Sent Alert Time Ended
	Initiator First Name
	Initiator Middle Name
	Initiator Last Name
	Initiator Username
	Initiator Unique ID
	Initiator Company Name
	Initiator Job Title
	Initiator Time Zone
	Initiator Language
	Initiator Last Login
	Initiator Role Name
	Sent Alert Division Name

Category	Resource
	Sent Alert Division Path
	Sent Alert Category Description
	Sent Alert Priority Description
	Sent Alert Severity Description
	Sent Alert Recipients Summary
	Sent Alert Contacted Summary
	Sent Alert Responded Summary
	Recipient First Name
	Recipient Last Name
	Recipient Unique ID
	Recipient Language
	Recipient Username
	Recipient Time Zone
	Recipient Division
	Recipient Division Path
	Recipient Role Name
	Response Time
	Response Text
	Device Information
	Device Delivery Time
	Device Type
	Sent Alert Sender Alias
	Sent Alert Contact Attempt Cycles
Group	Group Name
	Group Type
	Group Division Name
	Group Division Path

Appendix C: Weather & Events Event Types

The US Event Types are provided by The Weather Company and include the following:

AIR QUALITY

Event Type	Description
Air Pollution Warning	Issued when conditions are observed or imminent to the formation of ground-level ozone or high levels of particulate matter leading to elevated air pollution levels.
Air Pollution Watch	Issued when conditions are possible to the formation of ground-level ozone or high levels of particulate matter leading to elevated air pollution levels.
Air Quality Advisory	Issued when conditions are observed or imminent to the formation of ground-level ozone or high levels of particulate matter leading to elevated air pollution levels.
Air Quality Alert	Issued when conditions are conducive to the formation of ground-level ozone or high levels of particulate matter leading to elevated air pollution levels.
Air Quality Watch	Issued when conditions are possible to the formation of ground-level ozone or high levels of particulate matter leading to elevated air pollution levels.
Air Stagnation Advisory	Issued when atmospheric conditions are stable enough such that the potential exists for air pollutants to accumulate in a given area and expected to last for at least 36 hours.
Air Stagnation Outlook	Issued when atmospheric conditions are stable enough such that the potential exists for air pollutants to accumulate in a given area over the next 7 days.
Dust Advisory	Issued when blowing dust is expected to reduce visibility generally with winds.
Ozone Action Day	Issued when weather conditions are likely to combine with pollution emissions to form high levels of ozone near the ground that may cause harmful health effects. People and businesses should take action to reduce emissions of ozone-causing pollutants.
Ozone Alert	Issued when weather conditions are likely to combine with pollution emissions to form high levels of ozone near the ground that may cause harmful health effects. People and businesses should take action to reduce emissions of ozone-causing pollutants.
Ozone Warning	Issued when weather conditions are likely to combine with pollution emissions to form high levels of ozone near the ground that may cause harmful health effects. Advice is to remain indoors and limit physical activity.

AVALANCHE

Event Type	Description
Avalanche Warning	Issued when avalanche conditions are imminent or occurring.
Avalanche Watch	Issued when avalanche conditions are possible.

COASTAL

Event Type	Description
Beach Hazard Statement	Issued for rip currents, chemical hazards, or biological hazards in lake or ocean waters.
Coastal Flood Advisory	Issued when minor coastal flooding is occurring or is imminent in the next 12 hours, which poses a threat to life and/or property.
Coastal Flood Statement	Issued for updates about coastal flooding situations.
Coastal Flood Warning	Issued when coastal flooding is occurring or is imminent in the next 12 hours, which poses a serious threat to life and/or property.
Coastal Flood Watch	Issued when coastal flooding is possible in the next 24 hours, which would pose a serious threat to life and/or property.
Coastal/Lakeshore Bulletin	Issued for coastal and lakeshore updates.
Gale Warning	Issued when sustained surface winds, or frequent gusts, of 34 to 47 knots (39 to 54 mph) are occurring or will be imminently experienced.
Gale Watch	Issued when there is an increased risk for a gale-force wind event, meaning sustained surface winds, or frequent gusts, of 34 to 47 knots (39 to 54 mph), but the occurrence, location, and/or timing of the event is still uncertain.
Hazardous Seas Warning	Issued when wave heights and/or wave steepness values reach certain criteria that are defined by the local forecast office.c
Hazardous Seas Watch	Issued when wave heights and/or wave steepness values are expected to reach certain criteria that are defined by the local forecast office.
High Surf Advisory	Issued when pounding surf poses a danger to those in the water.
Hurricane Force Wind Warning	Issued when sustained winds or frequent gusts of 64 knots (118 km/h, 74 mph) or greater are either being observed or are predicted to occur.
Hurricane Wind Warning	Issued when sustained winds or frequent gusts of 64 knots (118 km/h, 74 mph) or greater are either being observed or are predicted to occur.

Event Type	Description
Hurricane Force Wind Watch	Issued when sustained winds or frequent gusts of 64 knots (118 km/h, 74 mph) or greater are possible.
Hurricane Wind Watch	Issued when sustained winds or frequent gusts of 64 knots (118 km/h, 74 mph) or greater are possible.
Hurricane Warning	Issued when sustained winds of 64 kt (74 mph) or higher associated with a tropical cyclone are imminent or occurring in 36 hours or less. These winds may be accompanied by storm surge, coastal flooding, and/or river flooding. A hurricane warning can remain in effect when dangerously high water or a combination of dangerously high water and exceptionally high waves continue, even though winds may be less than hurricane force.
Hurricane Watch	Issued when a tropical cyclone containing winds of 64 kt (74 mph) or higher poses a possible threat, generally within 48 hours. These winds may be accompanied by storm surge, coastal flooding, and/or river flooding.
Lakeshore Flood Advisory	Issued when minor lakeshore flooding is occurring or is imminent in the next 12 hours, which poses a threat to life and/or property.
Lakeshore Flood Statement	Issued for updates about lakeshore flooding.
Lakeshore Flood Warning	Issued when lakeshore flooding is occurring or is imminent in the next 12 hours, which poses a serious threat to life and/or property.
Lakeshore Flood Watch	Issued when lakeshore flooding is possible in the next 24 hours, which would pose a serious threat to life and/or property.
Marine Weather Statement	Issued to provide mariners with details on significant or potentially hazardous conditions not otherwise covered in existing marine warnings and forecasts.
Rip Current Statement	Issued for a risk of rip currents present in the specified area (may be issued as a beach hazards statement).
Severe Thunderstorm Warning	Issued when a severe thunderstorm is imminent or occurring. A severe thunderstorm contains large damaging hail of 1 inch (2.5 cm) in diameter or larger, and/or damaging winds of 58 mph (93 km/h) or greater.
Small Craft Advisory	Issued when winds have reached, or are expected to reach within 12 hours, a speed marginally less than gale force. It may also be issued when sea or lake ice exists that could be hazardous to small boats.
Small Craft Advisory for Hazardous Seas	Issued for wind speeds lower than small craft advisory criteria, yet waves or seas are potentially hazardous due to wave height, wave period, steepness, or swell direction.

Event Type	Description
Small Craft Advisory for Rough Bar	Issued for specialized areas near harbor or river entrances known as bars. Waves in or near such bars may be especially hazardous to mariners due to the interaction of swell, tidal and/or river currents in relatively shallow water.
Small Craft Advisory for Winds	Issued for wave heights lower than small craft advisory criteria, yet wind speeds are potentially hazardous. Thresholds governing the issuance of small craft advisories are specific to geographic areas.
Special Marine Warning	Issued for any other weather-related phenomena which may result in a hazardous impact on local marine operations.
Storm Surge Warning	Issued when localized heavy flooding due to storm surge caused by a tropical cyclone is occurring or is imminent in the next 12 hours, which poses a threat to life and/or property.
Storm Surge Watch	Issued when life-threatening inundation from rising water being forced inland by an ongoing or potential tropical, subtropical or post-tropical cyclone is possible within the specified area, generally within 48 hours.
Storm Warning	Issued if winds of 48 to 63 knots (55 to 73 mph) are forecast.
Storm Watch	Issued if winds of 48 to 63 knots (55 to 73 mph) are possible.
Tropical Storm Warning	Issued when sustained winds within the range of 34 to 63 knots (39 to 73 mph or 63 to 117 km/h) associated with a tropical cyclone are expected in a specified area within 36 hours or less.
Tropical Storm Watch	Issued when sustained winds within the range of 34 to 63 knots (39 to 73 mph or 63 to 117 km/h) are either being observed or are predicted to occur.
Tropical Storm Wind Warning	Issued when sustained winds within the range of 34 to 63 knots (39 to 73 mph or 63 to 117 km/h) are possible.
Tropical Storm Wind Watch	Issued when sustained winds within the range of 34 to 63 knots (39 to 73 mph or 63 to 117 km/h) are possible.
Tsunami Bulletin	Issued for updates about a tsunami.
Tsunami Warning	Issued when a tsunami is imminent, expected, or occurring. Coastal regions should expect flooding.
Tsunami Warning	Issued when a tsunami is imminent, expected, or occurring. Coastal regions should expect flooding.
Tsunami Watch	Issued for areas that may be affected by an incoming tsunami.

LOCAL STORM REPORTS

Event Type	Description
1 Hour Rainfall	1 hour observed rainfall.
1 Hour Snowfall	1 hour observed snowfall.
12 Hour Rainfall	12 hours observed rainfall.
12 Hour Snowfall	12 hours observed snowfall.
24 Hour Rainfall	24 hours observed rainfall.
24 Hour Snowfall	24 hours observed snowfall.
48 Hour Rainfall	48 hours observed rainfall.
48 Hour Snowfall	48 hours observed snowfall.
6 Hour Rainfall	6 hours observed rainfall.
6 Hour Snowfall	6 hours observed rainfall.
Avalanche	Observed avalanche.
Blizzard	Observed Blizzard.
Coastal Flood	Observed Coastal Flood.
Dense Fog	Observed Dense Fog.
Downburst	Observed Downburst.
Drought	Observed Drought.
Dust Storm	Observed Dust Storm.
Flash Flood	Observed Flash Flood.
Freezing Rain	Observed Freezing Rain.
Funnel Cloud	Observed Funnel Cloud.
Hail	Observed Hail.
Heavy Rain	Observed Heavy Rain.
Heavy Snow	Observed heavy snow.
High Astronomical Tides	Observed high astronomical tides.

Event Type	Description
High Surf	Observed high surf.
High Sustained Winds	Observed high sustained winds.
Hurricane	Observed hurricane.
Ice Storm	Observed ice storm.
Lakeshore Flood	Observed lakeshore flood.
Lightning	Observed lightning.
Marine Hail	Observed marine hail.
Marine Thunderstorm Wind	Observed marine thunderstorm wind.
Non-Thunderstorm Wind Damage	Observed non-thunderstorm wind damage.
Non-Thunderstorm Wind Gust	Observed non-thunderstorm wind gust.
Rip Currents	Observed rip currents.
Sleet	Observed sleet.
Snow	Observed snow.
Snow On Ground	Observed snow on the ground.
Storm Surge	Observed storm surge.
Storm Total Rainfall	Total observed storm rainfall.
Storm Total Snowfall	Total observed storm snowfall.
Thunderstorm Wind Damage	Observed thunderstorm wind damage.
Tornado	Observed tornado.
Tropical Storm	Observed tropical storm.
Wall Cloud	Observed wall cloud.
Waterspout	Observed waterspout.
Wildfire	Observed wildfire.

MISCELLANEOUS

Event Type	Description
911 Telephone Outage Emergency	Issued for a local or state 911 telephone network outage by geographic area or telephone exchange. Authorized officials may provide alternative phone numbers in which to reach 911 or dispatch personnel.
Administrative Message	Issued for a non-emergency message that provides updated information about an event in progress, an event that has expired or concluded early, pre-event preparation or mitigation activities, post-event recovery operations, or other administrative matters pertaining to the Emergency Alert System.
Airport Weather Warning	Issued for pre-defined weather conditions that are hazardous to Airport Ground Operations that may not be specified in other NWS forecasts or warnings.
Avalanche Bulletin	Issued for avalanche condition updates.
Child Abduction Emergency	Issued to ask the public for help in finding abducted children.
Civil Danger Warning	Issued by authorized public officials for an event that presents a danger to a significant civilian population.
Civil Emergency Message	Issued to warn the public of a significant in-progress or imminent threat to public safety.
Earthquake Warning	Issued to notify adjoining regions of a substantial earthquake while it is in progress.
Evacuation Immediate Bulletin	Issued to notify the public of a mandatory evacuation due to a wildfire, approaching hurricane, or an imminent explosion due to a gas leak.
Fire Weather Bulletin	Issued for updates about fire conditions.
Fire Weather Warning	Issued when a fire is currently burning in the area and evacuation is recommended.
Fire Weather Watch	Issued when conditions are expected to become favorable for the rapid spread of wildfires.
Hazardous Materials Warning	Issued for the release of a non-radioactive hazardous material (such as a flammable gas, toxic chemical, or biological agent) that may recommend evacuation (for an explosion, fire or oil spill hazard) or shelter in place (for a toxic fume hazard).
Law Enforcement Warning	Issued when an authorized law enforcement agency may blockade roads, waterways, or facilities, evacuate or deny access to affected areas, and arrest violators or suspicious persons involved in a criminal event.

Event Type	Description
Local Area Emergency	Issued for an event that by itself does not pose a significant threat to public safety and/or property. However, the event could escalate, contribute to other more serious events, or disrupt critical public safety services.
Low Water Advisory	Issued to describe water levels that are significantly below average levels over the Great Lakes, coastal marine zones, and any tidal marine area, waterway, or river inlet within or adjacent to a marine zone that would potentially be impacted by low water conditions creating a hazard to navigation.
Network Message Notification	Issued to provide network updates.
Nuclear Power Plant Warning	Issued for an event at a nuclear power plant classified such as a Site Area Emergency or General Emergency as classified by the Nuclear Regulatory Commission (NRC). A Site Area Emergency is confined to the plant site; no off-site impact is expected. Typically, a General Emergency is confined to an area less than a 10-mile radius around the plant.
Radiological Hazard Warning	Issued for the loss, discovery, or release of a radiological hazard. Examples include the theft of a radioactive isotope used for medical, seismic, or other purposes; the discovery of radioactive materials; a transportation (aircraft, truck or rail, etc.) accident that may involve nuclear weapons, nuclear fuel, or radioactive wastes.
Red Flag Warning	Issued when conditions are favorable for the rapid spread of wildfires.
Shelter In Place Warning	Issued when the public is recommended to shelter in place (go inside, close doors and windows, turn off air conditioning or heating systems, and turn on the radio or TV for more information). An example is the release of hazardous materials where toxic fumes or radioactivity may affect designated areas.
Significant Weather Advisory	Issued when Doppler radar indicates a strong thunderstorm is producing small hail or high winds whose strength does not reach the criteria to be designated a severe thunderstorm.
Significant Weather Alert	Issued when Doppler radar indicates a strong thunderstorm is producing small hail or high winds whose strength does not reach the criteria to be designated a severe thunderstorm.
Special Weather Statement	Issued for hazards that have not yet reached warning or advisory status or that do not have a specific code of their own, such as widespread funnel clouds.
Tsunami Advisory	Issued when a tsunami could produce strong currents and waves are imminent, expected, or occurring.
Volcano Warning	Issued for current or imminent volcanic activity.
Weather Bulletin	Issued for any situation for which there is no other alert that effectively describes the conditions expected.

RAIN/FLOODS

Event Type	Description
Flash Flood Statement	Issued for updates about flash flood conditions.
Flash Flood Warning	Issued when flash flooding is occurring, imminent, or highly likely. A flash flood is a flood that occurs within six hours of excessive rainfall and that poses a threat to life and/or property. Ice jams and dam failures can also cause flash floods. These warnings are issued on a county by county basis by the local Weather Forecast Office and are generally in effect for two to six hours, although particularly during tropical cyclones a warning may last for a longer period of time, and occasionally last shorter than two hours.
Flash Flood Watch	Issued when conditions are favorable for flash flooding in flood-prone areas, usually when grounds are already saturated from recent rains, or when upcoming rains will have the potential to cause a flash flood. These watches are also occasionally issued when a dam may break in the near future.
Flood Advisory	Issued when flooding is not expected to be bad enough to issue a warning. However, it may cause significant inconvenience, and if caution is not exercised, it could lead to situations that may threaten life and/or property.
Flood Bulletin	Issued for updates about flood conditions.
Flood Warning	Issued when flooding is imminent or occurring.
Flood Watch	Issued when conditions are favorable for flooding. It does not mean flooding will occur, but it is possible.
Hydrologic Outlook	Issued for extended forecasts involving heavy rain or flooding.
Hydrologic Statement	Issued for updates about heavy rain or flooding.
River Flood Advisory	Issued when streams or rivers reaching action stage is occurring, imminent, or highly likely. These advisories are issued on a county by county basis by the local Weather Forecast Office and are generally in effect for a couple of days or longer.
River Flood Warning	Issued when flooding of streams or rivers is occurring, imminent, or highly likely. These warnings are issued on a county by county basis by the local Weather Forecast Office and are generally in effect for a couple of days or longer.
River Flood Watch	Issued when flooding of streams or rivers is possible. These warnings are issued on a county by county basis by the local Weather Forecast Office and are generally in effect for a couple of days or longer.
Wind Chill Watch	Issued when extreme wind chills that are life-threatening are possible; the criteria will vary significantly over different county watch areas.

TEMPERATURE

Event Type	Description
Excessive Heat Warning	Extreme Heat Index (HI) values forecast to meet or exceed locally defined warning criteria for at least two days. Specific criteria vary among local Weather Forecast Offices, due to climate variability and the effect of excessive heat on the local population. Typical HI values are maximum daytime temperatures above 105 to 110 °F (41 to 43 °C) and minimum night-time temperatures above 75 °F (24 °C).
Excessive Heat Watch	Conditions are favorable for an excessive heat event to meet or exceed local Excessive Heat Warning criteria in the next 24 to 72 hours.
Extreme Cold Warning (Alaska only)	Dangerously low temperatures are expected for a prolonged period of time. Frostbite and hypothermia are likely if exposed to these temperatures.
Extreme Cold Watch	Dangerously low temperatures are possible for a prolonged period of time. Frostbite and hypothermia are likely if exposed to these temperatures.
Freeze Warning	Issued when significant, widespread freezing temperatures are imminent or occurring.
Freeze Watch	Issued when it is possible for significant, widespread freezing temperatures within the next 24-36 hours.
Frost Advisory	Issued when the minimum temperature is forecast to be 33°F to 36°F degrees on clear and calm nights during the growing season.
Hard Freeze Warning	Issued for widespread temperatures at or below 28 °F (-2 °C) during the growing season. A hard freeze may occur with or without frost.
Heat Advisory	High Heat Index (HI) values are forecast to meet or exceed locally defined warning criteria for one or two days. Specific criteria vary over different county warning areas, due to climate variability and the effect of excessive heat on the local population. Typical HI values are maximum daytime temperatures above 100 to 105 °F (38 to 41 °C) and minimum night-time temperatures above 75 °F (24 °C).
Wind Chill Advisory	Issued when dangerous wind chills making it feel very cold are imminent or occurring; the criteria varies significantly over different county warning areas.
Wind Chill Warning	Issued when extreme wind chills that are life-threatening are imminent or occurring; the criteria varies significantly over different county warning areas.

THUNDERSTORM

Event Type	Description
Freezing Rain Advisory	Issued when accretion of ice up to a quarter of an inch is expected or occurring.
Freezing Spray Advisory	Issued to warn vessels that accumulation of freezing water droplets due to a combination of cold water, wind, cold air, and vessel movement is possible; however, accumulations are not expected to reach rates of 2 cm per hour.
Heavy Freezing Spray Warning	Issued to warn vessels that accumulation of freezing water droplets due to a combination of cold water, wind, cold air, and vessel movement is expected or occurring. Accumulation rates of 2 cm per hour or greater must be possible to be issued.
Heavy Freezing Spray Watch	Issued to warn vessels that accumulation of freezing water droplets due to a combination of cold water, wind, cold air, and vessel movement is possible. Accumulation rates of 2 cm per hour or greater must be possible to be issued.
Severe Thunderstorm Watch	Issued when a severe thunderstorm is possible. A severe thunderstorm contains large damaging hail of 1 inch (2.5 cm) in diameter or larger, and/or damaging winds of 58 mph (93 km/h) or greater.
Severe Weather Warning	Issued when a severe thunderstorm is imminent or occurring. A severe thunderstorm contains large damaging hail of 1 inch (2.5 cm) in diameter or larger, and/or damaging winds of 58 mph (93 km/h) or greater.
Severe Weather Watch	Issued when a severe thunderstorm is possible. A severe thunderstorm contains large damaging hail of 1 inch (2.5 cm) in diameter or larger, and/or damaging winds of 58 mph (93 km/h) or greater.
Snowfall Report	Issued to define expected snowfall or summarize the amount of snowfall in a given area.
Tornado Warning	Issued when severe thunderstorms with tornadoes are imminent or occurring.
Tornado Watch	Issued when severe thunderstorms with tornadoes are possible.
Winter Storm Warning	Issued when a significant combination of hazardous winter weather is imminent or occurring.
Winter Storm Watch	Issued when significant and hazardous winter weather is possible within 48 hours.
Winter Weather Advisory	Hazardous winter weather conditions are occurring, imminent, or likely. Conditions will cause a significant inconvenience and if caution is not exercised, may result in a potential threat to life and/or property.
Winter Weather Bulletin	Hazardous winter weather conditions are occurring, imminent, or likely. Conditions will cause a significant inconvenience and if caution is not exercised, may result in a potential threat to life and/or property.

VISIBILITY

Event Type	Description
Ashfall Advisory	Issued for conditions associated with airborne ash plume resulting in ongoing deposition at the surface. Ashfall may originate directly from a volcanic eruption, or indirectly by wind suspending the ash.
Ashfall Warning	Issued for a volcano undergoing a major eruption where the public will be affected to a significant extent, such as greater than or equal to $\frac{1}{4}$ " of ashfall accumulation, significant debris, lava or lahar flows.
Blowing Dust Advisory	Issued with strong winds and considerable blowing sand or dust reducing visibilities.
Dense Fog Advisory	Issued when widespread fog is expected to reduce visibilities to 1/4 mile or less over a large area for an extended period of time (2 or more hours).
Dense Smoke Advisory	Issued for widespread or localized smoke reducing visibilities to 1/4 mi (0.4 km) or less.

WIND

Event Type	Description
Brisk Wind Advisory	Issued when winds have reached, or are expected to reach within 12 hours, a speed marginally less than gale force.
Extreme Wind Warning	An Extreme Wind Warning is issued for surface winds of 100 knots (115 MPH) or greater associated with non-convective, downslope, derecho (NOT associated with a tornado), or sustained hurricane winds are imminent or occurring within one hour.
High Wind Warning	Issued when the following conditions are imminent or occurring: Sustained winds of 40mph or higher for one hour or more OR wind gusts of 58mph or higher for any duration.
High Wind Watch	Issued when the following conditions are possible: Sustained winds of 40mph or higher for one hour or more OR wind gusts of 58mph or higher for any duration.
Lake Wind Advisory	Issued when windy conditions on area lakes are expected to be hazardous for boaters and other recreational events on or around lakes.
Tropical Weather Statement	Issued in or near an area affected or forecast to be affected by a tropical storm or hurricane, which provides an overview of the storm's local effects, including expected weather conditions, evacuation decisions made by local officials, and precautions necessary to protect life and property.

Event Type	Description
Typhoon Local Statement	Issued for updates about typhoon conditions in a specified area.
Typhoon Statement	Issued for updates about typhoon conditions in a specified area.
Typhoon Warning	Issued when a typhoon is expected in a specified area.
Typhoon Watch	Issued when a typhoon is possible in a specified area.
Wind Advisory	Issued when there are sustained winds of 31–39 miles per hour (50–63 km/h) and/or gusts of 46–57 miles per hour (74–92 km/h) over land.

WINTER PRECIPITATION

Event Type	Description
Blizzard Warning	Issued when the following conditions are imminent or occurring within the next 12 to 18 hours: Snow and/or blowing snow reducing visibility to 1/4 mile or less for 3 hours or longer AND sustained winds of 35mph or greater or frequent gusts to 35mph or greater.
Blizzard Watch	Issued when sustained winds or frequent gusts of 35 miles per hour (56 km/h) or greater, considerable falling, and/or blowing snow reducing visibility frequently to 1/4 mile (0.40 km) or less for a period of three hours or more are possible generally within the next 48 hours.
Freezing Fog Advisory	Issued when fog develops and surface temperatures are at or below freezing. The tiny liquid droplets in the fog can freeze instantly to any surface, including vehicles and road surfaces.
Heavy Freezing Spray Advisory	Issued to warn vessels that accumulation of freezing water droplets due to a combination of cold water, wind, cold air, and vessel movement is imminent. Accumulation rates of 2 cm per hour or greater must be possible to be issued.
Ice Storm Warning	Issued when ¼ inch or more of ice accumulation is imminent or occurring.
Snow Squall Warning	Issued when two types of snow events reducing visibility in blowing snow are imminent or occurring: Lake effect snow squalls and Frontal snow squalls.

The Canadian Event Types are provided by The Weather Company and include the following:

AIR QUALITY

Event Type	Description
Air Quality and Health Advisory	Issued when conditions are observed or imminent to the formation of ground-level ozone or high levels of particulate matter leading to elevated air pollution levels.
Air Quality Warning	Issued when conditions are observed or imminent to the formation of ground-level ozone or high levels of particulate matter leading to elevated air pollution levels.
Dust Storm Warning	Issued when blowing dust is imminent or occurring to frequently reduce visibility to 1/4 mile (400 m) or less, generally with winds of 25 miles per hour (40 km/h) or more.
Smog Warning	Issued when severe air pollution is observed or expected.
Special Air Quality Statement	Issued when a high-risk Air Quality Health Index value is forecast to last for 1 to 2 hours.

COASTAL

Event Type	Description
Gale Warning	Issued when sustained surface winds, or frequent gusts, of 34 to 47 knots (39 to 54 mph) are occurring or will be imminently experienced.
High Water Level Warning	Issued when levels near bodies of water are dangerously high and could pose a risk to life or property.
Hurricane Warning	Issued when sustained winds of 64 kt (74 mph) or higher associated with a tropical cyclone are imminent or occurring in 36 hours or less. These winds may be accompanied by storm surge, coastal flooding, and/or river flooding. A hurricane warning can remain in effect when dangerously high water or a combination of dangerously high water and exceptionally high waves continue, even though winds may be less than hurricane force.
Hurricane Watch	Issued when a tropical cyclone containing winds of 64 kt (74 mph) or higher poses a possible threat, generally within 48 hours. These winds may be accompanied by storm surge, coastal flooding, and/or river flooding.
Rapid Closing of Coastal Leads Warning	Issued when the forecast combination of winds and ocean currents will result in the movement of pack ice rapidly closing any open waterways, known as leads, along the affected coastal sections.
Severe Thunderstorm Warning	Issued when a severe thunderstorm is imminent or occurring. A severe thunderstorm contains large damaging hail of 1 inch (2.5 cm) in diameter or larger, and/or damaging winds of 58 mph (93 km/h) or greater.

Event Type	Description
Special Marine Advisory	Issued for updates for any other weather-related phenomena which may result in a hazardous impact on local marine operations.
Special Marine Warning	Issued for any other weather-related phenomena which may result in a hazardous impact on local marine operations.
Special Marine Watch	Issued when conditions are conducive for the development of any other weather-related phenomena that may pose a hazard to local marine operations.
Squall Warning	Issued for forecast or observed wind gusts of 34 knots (63 km/h) or greater that are associated with a line, or an organized area, of thunderstorms.
Squall Watch	Issued for possible wind gusts of 34 knots (63 km/h) or greater that are associated with a line, or an organized area, of thunderstorms.
Storm Surge Warning	Issued when localized heavy flooding due to storm surge caused by a tropical cyclone is occurring or is imminent in the next 12 hours, which poses a threat to life and/or property.
Storm Warning	Issued if winds of 48 to 63 knots (89 to 117 km/h) are forecast.
Strong Wind Warning	Issued if winds of 20 to 33 knots (37 to 61 km/h) are forecast.
Tropical Storm Statement	Issued for updates surrounding a warm-core non-frontal synoptic-scale cyclone, originating over tropical or subtropical waters, with organized deep convection and a closed surface wind circulation about a well-defined center.
Tropical Storm Warning	Issued when sustained winds within the range of 34 to 63 knots (39 to 73 mph or 63 to 117 km/h) associated with a tropical cyclone are expected in a specified area within 36 hours or less.
Tropical Storm Watch	Issued when sustained winds within the range of 34 to 63 knots (39 to 73 mph or 63 to 117 km/h) associated with a tropical cyclone are expected in a specified area within 36 hours or less.
Tsunami Warning	Issued when a tsunami is imminent, expected, or occurring. Coastal regions should expect flooding.
Tsunami Watch	Issued for areas that may be affected by an incoming tsunami.
Waterspout Warning	Issued when a waterspout is detected on radar or is observed by trained spotters. The warning is commonly issued to warn persons on water.
Waterspout Watch	Issued when a waterspout is possible. The watch is commonly issued to warn persons on water.

MISCELLANEOUS

Event Type	Description
Ice Pressure Warning	Issued when a prolonged period of strong winds is forecast, which would cause ice pressure within the ice pack or along the coast.
Special Ice Warning	Issued for all other non-specified ice conditions that may warrant a warning being issued.
Special Weather Statement	Issued for hazards that have not yet reached warning or advisory status or that do not have a specific code of their own, such as widespread funnel clouds.
Tsunami Advisory	Issued when a tsunami could produce strong currents and waves are imminent, expected, or occurring.
Weather Advisory	Issued for any situation for which there is no other alert that effectively describes the conditions expected.
Weather Warning	Issued for extreme weather events for which there is no suitable warning type, because they rarely occur.

RAIN/FLOOD

Event Type	Description
Rainfall Warning	Issued when there is a potential for regional flooding.

TEMPERATURE

Event Type	Description
Arctic Outflow Warning	Issued for a combination of wind speed and temperatures which produce wind chills of at least -20°C (-4°F) for at least six hours during the winter when very cold Arctic air breaks from the interior mainland of British Columbia and spills out through mountain gaps and fjords.
Extreme Cold Warning	Issued when windchill, with winds of at least 15 km/h (9.3 mph), or actual temperatures ranging from -55°C (-67°F) to -30°C (-22°F) are expected to persist for at least three hours.
Flash Freeze Warning	Issued for a rapid drop in temperatures, causing freezing of residual water on roads, and sidewalks to quickly build up.
Frost Advisory	Issued when frost is expected.
Heat Warning	Issued when temperatures at least 30°C (86°F) and Humidex values over 40°C (104°F) persist for at least one hour.

THUNDERSTORM

Event Type	Description
Severe Thunderstorm Watch	Issued when a severe thunderstorm is possible. A severe thunderstorm contains large damaging hail of 1 inch (2.5 cm) in diameter or larger, and/or damaging winds of 58 mph (93 km/h) or greater.
Tornado Warning	Issued when severe thunderstorms with tornadoes are imminent or occurring.
Tornado Watch	Issued when severe thunderstorms with tornadoes are possible.
Winter Storm Warning	Issued when a significant combination of hazardous winter weather is imminent or occurring.
Winter Storm Watch	Issued when significant and hazardous winter weather is possible within 48 hours.

VISIBILITY

Event Type	Description
Fog Advisory	Issued for low visibilities in fog expected for a significant duration.

WIND

Event Type	Description
Les Suetes Wind Warning	Issued when strong winds that may cause damage are expected or occurring from Les Suetes winds.
Wind Warning	Issued when wind speeds are expected to or currently blowing steadily at 60 to 65 km/h (37 to 40 mph) or more, or winds gusting to 90 km/h (56 mph) or more.

WINTER PRECIPITATION

Event Type	Description
Blizzard Warning	Issued when the following conditions are imminent or occurring within the next 12 to 18 hours: Snow and/or blowing snow reducing visibility to 1/4 mile or less for 3 hours or longer AND sustained winds of 35mph or greater or frequent gusts to 35mph or greater.
Blowing Snow Advisory	Issued with sustained winds or frequent gusts of 25 to 35 miles per hour (40 to 56 km/h) accompanied by falling and blowing snow, occasionally reducing visibility to 1/4 mile (0.40 km) or less.

Event Type	Description
Freezing Drizzle Advisory	Issued when freezing drizzle is expected for a significant duration
Freezing Rain Warning	Issued when hazardous walking and driving conditions are expected from freezing rain or drizzle. Also, if ice is over 2 mm (0.079 in) thick and has the potential to cause damage to trees and overhead electricity and telecommunications wires.
Freezing Spray Warning	Issued whenever moderate or heavy ship icing is expected from a combination of low temperatures and strong winds causing sea spray to freeze on a ship's superstructure or on other structures either in the sea or near the water's edge.
Snow Squall Warning	Issued two types of snow events reducing visibility in blowing snow are imminent or occurring: Lake effect snow squalls and Frontal snow squalls.
Snow Squall Watch	Issued two types of snow events reducing visibility in blowing snow are possible: Lake effect snow squalls and Frontal snow squalls.
Snowfall Warning	Issued when hazardous amounts are expected to fall over a 12- or 24-hour period.

The European, Australian, and Japanese Profile Event Types are provided by The Weather Company and include the following:

COASTAL

Event Type	Description	Region
Small Craft Alert	Issued when winds have reached, or are expected to reach within 12 hours, a speed marginally less than gale force. It may also be issued when sea or lake ice exists that could be hazardous to small boats.	Australia
Strong Wind Warning	Issued if winds of 20 to 33 knots (37 to 61 km/h) are forecast.	Australia
Gale Warning	Issued when high winds are expected or observed.	Australia
Storm Force Wind Warning	Issued when very high winds are expected or occurring.	Australia
Hurricane Force Wind Warning	Issued when sustained winds or frequent gusts of 64 knots (118 km/h, 74 mph) or greater are either being observed or are predicted to occur.	Australia
Marine Wind Warning	Issued when high winds are expected or observed that could impact marine vessels.	Australia
Severe Thunderstorm Warning for Large Hail	Issued when thunderstorms are expected to produce large hail.	Australia
Severe Thunderstorm Warning for Giant Hail	Issued when thunderstorms are expected to produce very large hail.	Australia
Hazardous Surf Warning	Issued when pounding surf poses a danger to those in the water.	Australia
Severe Thunderstorm Warning for Tornadoes	Issued when thunderstorms are expected to produce tornadoes.	Australia
Severe Thunderstorm Warning	Issued when severe thunderstorms are expected.	Australia
Severe Thunderstorm Warning for Flash Flooding	Issued when thunderstorms are expected to produce flash flooding.	Australia
Severe Weather Warning for Flash Flooding	Issued when severe weather is expected to produce flash flooding.	Australia

Event Type	Description	Region
Severe Weather Warning for Abnormally High Tide	Issued when severe weather is expected to produce high tide.	Australia
Severe Weather Warning for Damaging Surf	Issued when severe weather is expected to produce damaging surf.	Australia
Tropical Cyclone Watch	Issued when a tropical cyclone is possible for a specified area.	Australia
Tropical Cyclone Warning	Issued when a tropical cyclone is observed or expected for a specified area.	Australia
Tropical Cyclone Bulletin	Issued for updates about tropical cyclone events.	Australia
Tsunami Statement	Issued for tsunami-related events.	Australia
Tsunami Watch	Issued for areas that may be affected by an incoming tsunami.	Australia
Tsunami Warning	Issued when a tsunami is imminent, expected, or occurring. Coastal regions should expect flooding.	Australia
Tsunami Bulletin	Issued for updates about a tsunami.	Australia
Marginal Fire Weather Warning	Issued when forecast fire weather conditions are slightly dangerous.	Australia

MISCELLANEOUS

Event Type	Description	Region
Fire Weather Warning	Issued when forecast fire weather conditions are dangerous.	Australia
Severe Fire Weather Warning	Issued when forecast fire weather conditions are very dangerous.	Australia
Extreme Fire Weather Warning	Issued when forecast fire weather conditions are extremely dangerous.	Australia
Catastrophic Fire Weather Warning	Issued when forecast fire weather conditions are catastrophic.	Australia
Very High Fire Weather Warning	Issued when forecast fire weather conditions are very high.	Australia
Road Weather Alert for slippery roads	Issued when rain is impacting road conditions.	Australia

Event Type	Description	Region
Road Weather Alert for icing	Issued when ice is impacting road conditions.	Australia
Road Weather Alert for snow	Issued when snow is impacting road conditions.	Australia
Road Weather Alert for flooding	Issued when flooding is impacting road conditions.	Australia
Road Weather Alert for Heavy Rain	Issued when heavy rain is impacting road conditions.	Australia
Road Weather Alert for fog	Issued when fog is impacting road conditions.	Australia
Road Weather Alert for Dust	Issued when dust is impacting road conditions.	Australia
Road Weather Alert for Smoke	Issued when smoke is impacting road conditions.	Australia
Road Weather Alert	Issued when weather conditions are impacting roads.	Australia
Road Weather Alert for Damaging Wind	Issued when wind is impacting road conditions.	Australia
Road Weather Alert for Destructive Wind	Issued when high wind is impacting road conditions.	Australia
Bushwalkers Alert	Issued to alert hikers and backpackers of potential hazards.	Australia
Bushwalkers Alert for Snow	Issued to alert hikers and backpackers of hazardous snowfall.	Australia
Bushwalkers Alert for chill conditions	Issued to alert hikers and backpackers of cold temperatures.	Australia
Sheep Graziers Warning	Issued when weather conditions may cause loss of lamb and sheep.	Australia
Severe Sheep Graziers Warning	Issued when weather conditions will probably cause loss of lamb and sheep.	Australia
Brown Rot Alert	Issued to alert of plant disease related to brown rot.	Australia
Severe Brown Rot Alert	Issued to alert of plant disease related to brown rot that is likely.	Australia

Event Type	Description	Region
Downy Mildew Advice	Issued for updates about downy mildew.	Australia
Severe Downy Mildew Advice	Issued for updates about downy mildew that is likely.	Australia

RAIN/FLOOD

Event Type	Description	Region
Initial Flood Watch	Issued when conditions are favorable for flooding. It does not mean flooding will occur, but it is possible.	Australia
Flood Watch	Issued when flooding is possible.	Australia
Initial Minor Flood Watch	Issued when conditions are favorable for minor flooding. It does not mean minor flooding will occur, but it is possible.	Australia
Minor Flood Watch	Issued when conditions are favorable for minor flooding. It does not mean minor flooding will occur, but it is possible.	Australia
Moderate Flood Watch	Issued when moderate flooding is possible.	Australia
Major Flood Watch	Issued when conditions are favorable for major flooding. It does not mean major flooding will occur, but it is possible.	Australia
Final Flood Watch	Issued when flooding is possible.	Australia
Minor to Moderate Flood Watch	Issued when conditions are favorable for minor to moderate flooding, but it is unclear.	Australia
Moderate to Major Flood Watch	Issued when conditions are favorable for moderate to major flooding, but it is unclear.	Australia
Flood Warning	Issued when flooding is observed or expected.	Australia
Initial Minor Flood Warning	Issued when minor flooding is expected or observed.	Australia
Minor Flood Warning	Issued when minor flooding is expected or observed.	Australia
Moderate Flood Warning	Issued when moderate flooding is expected or observed.	Australia
Major Flood Warning	Issued when major flooding is expected or observed.	Australia
Final Flood Warning	Issued when flooding is observed or expected.	Australia

TEMPERATURE

Event Type	Description	Australia
Frost Warning	Issued when frost is observed or expected.	Australia
Severe Frost Warning	Issued when severe frost is observed or expected.	Australia

THUNDERSTORM

Event Type	Description	Australia
Severe Weather Warning for Large Hail	Issued when severe weather is imminent or occurring with large hail.	Australia
Severe Weather Warning for Tornadoes	Issued when severe weather is imminent or occurring with tornadoes.	Australia
Severe Weather Warning for Damaging Wind	Issued when severe weather is imminent or occurring with damaging wind.	Australia
Severe Weather Warning for Destructive Wind	Issued when severe weather is imminent or occurring with destructive wind.	Australia
Severe Weather Warning	Issued when severe weather is imminent or occurring.	Australia

WIND

Event Type	Description	Region
Severe Thunderstorm Warning for Damaging Wind	Issued when a severe thunderstorm is imminent or occurring with damaging wind.	Australia
Severe Thunderstorm Warning for Destructive Wind	Issued when a severe thunderstorm is imminent or occurring with destructive wind.	Australia

WINTER PRECIPITATION

Event Type	Description	Region
Severe Weather Warning for Blizzard	Issued when a blizzard is expected or occurring.	Australia

AVALANCHE

Event Type	Description	Region
Disruption due to avalanche	Issued for major hazards due to an avalanche.	Europe
High disruption due to avalanche	Issued for major hazards due to an avalanche.	Europe
Potential disruption due to avalanche	Issued for possible hazards due to an avalanche.	Europe

COASTAL

Coastal	Description	Region
Disruption due to coastal event	Issued for hazards due to coastal situations (i.e. waterspouts or tsunamis)	Europe
High disruption due to coastal event	Issued for major hazards due to coastal situations (i.e. waterspouts or tsunamis)	Europe
Potential disruption due to coastal event	Issued for possible hazards due to coastal situations (i.e. waterspouts or tsunamis)	Europe

MISCELLANEOUS

Miscellaneous	Description	Region
Disruption due to forest fire	Issued for hazards due to fires.	Europe
High disruption due to forest fire	Issued for major hazards due to fires.	Europe
Potential disruption due to forest fire	Issued for possible hazards due to fires.	Europe

RAIN/FLOOD

Event Types	Description	Region
Disruption due to flood	Issued for hazards due to flooding.	Europe
Disruption due to rain	Issued for hazards due to heavy rain.	Europe

Event Types	Description	Region
Disruption due to rain and flood	Issued for hazards due to heavy rainfall which could cause flooding.	Europe
High disruption due to flood	Issued for major hazards due to flooding.	Europe
High disruption due to rain	Issued for major hazards due to heavy rain.	Europe
Disruption due to rain and flood	Issued for hazards due to heavy rainfall which could cause flooding.	Europe
High disruption due to flood	Issued for major hazards due to flooding.	Europe
High disruption due to rain	Issued for major hazards due to heavy rain.	Europe
High disruption due to rain and flood	Issued for major hazards due to heavy rainfall which could cause flooding.	Europe
Potential disruption due to flood	Issued for possible hazards due to heavy rainfall which could cause flooding.	Europe
Potential disruption due to rain	Issued for possible hazards due to heavy rain.	Europe
Potential disruption due to rain and flood	Issued for possible hazards due to heavy rainfall which could cause flooding.	Europe

TEMPERATURE

Event Type	Description	Region
Disruption due to extreme high temperatures	Issued for hazards due to very high temperatures.	Europe
Disruption due to extreme low temperatures	Issued for hazards due to very low temperatures.	Europe
High disruption due to extreme high temperatures	Issued for major hazards due to very high temperatures.	Europe
High disruption due to extreme low temperatures	Issued for major hazards due to very low temperatures.	Europe

Event Type	Description	Region
Potential disruption due to extreme high temperatures	Issued for possible hazards due to very high temperatures.	Europe
Potential disruption due to extreme low temperatures	Issued for possible hazards due to very low temperatures.	Europe

THUNDERSTORM

Event Type	Description	Region
Disruption due to thunderstorms	Issued for hazards due to severe thunderstorms.	Europe
High disruption due to thunderstorms	Issued for major hazards due to severe thunderstorms.	Europe
Potential disruption due to thunderstorms	Issued for possible hazards due to severe thunderstorms.	Europe

VISIBILITY

Event Type	Description	Region
Disruption due to fog	Issued for hazards due to fog.	Europe
High disruption due to fog	Issued for major hazards due to fog.	Europe
Potential disruption due to fog	Issued for possible hazards due to fog.	Europe

WIND

Event Type	Description	Region
Disruption due to wind	Issued for hazards due to high winds.	Europe
High disruption due to wind	Issued for major hazards due to high winds.	Europe
Potential disruption due to wind	Issued for possible hazards due to high winds.	Europe

WINTER PRECIPITATION

Event Type	Description	Region
Disruption due to snow and ice	Issued for hazards due to heavy snowfall with possible ice buildup.	Europe
High disruption due to snow and ice	Issued for major hazards due to heavy snowfall with possible ice buildup.	Europe
Potential disruption due to snow and ice	Issued for possible hazards due to heavy snowfall with possible ice buildup.	Europe

AIR QUALITY

Event Type	Description	Region
Dry Air Advisory	Issued when air has very low humidity.	Japan

AVALANCHE

Event Type	Description	Region
Avalanche Advisory	Issued when avalanche conditions are possible.	Japan

COASTAL

Event Type	Description	Region
Gale Advisory	Issued when high winds are possible.	Japan
High Wave Advisory	Issued when high waves are possible.	Japan
High Wave Warning	Issued when high waves are expected.	Japan
High-Wave Emergency	Issued when high waves are observed.	Japan
Storm Surge Advisory	Issued when storm surge is possible.	Japan
Storm Surge Emergency	Issued when storm surge is observed.	Japan
Storm Surge Warning	Issued when storm surge is expected.	Japan

MISCELLANEOUS

Event Type	Description	Region
Other Advisories	Issued for advisories that do not fit the criteria of existing definitions.	Japan

RAIN/FLOOD

Event Type	Description	Region
Flood Advisory	Issued when flooding is possible.	Japan
Flood Warning	Issued when flooding is observed or expected.	Japan
Heavy Rainfall Advisory	Issued when heavy rain is possible.	Japan
Heavy Rainfall Warning	Issued when heavy rain is expected.	Japan
Heavy Rain Emergency	Issued when heavy rain is observed.	Japan

TEMPERATURE

Event Type	Description	Region
Low Temperature Advisory	Issued when low temperatures are possible.	Japan
Frost Advisory	Issued when frost is possible.	Japan

THUNDERSTORM

Event Type	Description	Region
Thunderstorm Advisory	Issued when thunderstorms are possible.	Japan

VISIBILITY

Event Type	Description	Region
Dense Fog Advisory	Issued when dense fog is possible.	Japan

WIND

Event Type	Description	Region
Windstorm Emergency	Issued when storms with high winds are observed.	Japan
Windstorm Warning	Issued when storms with high winds are expected.	Japan

TEMPERATURE

Event Type	Description	Region
Frost Advisory	Issued when frost is possible.	Japan

WINTER PRECIPITATION

Event Type	Description	Region
Gale and Snow Advisory	Issued when high winds and snow are possible.	Japan
Heavy Snowfall Advisory	Issued when heavy snow is expected.	Japan
Heavy Snowfall Emergency	Issued when heavy snow is observed.	Japan
Ice Accretion Advisory	Issued when ice buildup is possible.	Japan
Snow Accretion Advisory	Issued when snow buildup is possible.	Japan
Snowstorm Emergency	Issued when a snowstorm is observed.	Japan
Snow-melting Advisory	Issued when temperatures are warm enough to cause recent snowfall to melt.	Japan
Snowstorm Warning	Issued when a snowstorm is expected.	Japan

The Global Profile Event Types are provided by The Weather Company and include the following:

FORECASTS

Event Type	Description
Altimeter Pressure	Mean sea level pressure used to calibrate aircraft altimeters. This is also known as QNH.
Cloud Ceiling	Height of the lowest cloud base for a cloud deck that covers more than 50% of the sky.
Cloud Cover	Average cloud cover expressed as a percentage.
Dew Point	Temperature which air must be cooled at constant pressure to reach saturation. The Dew Point is also an indirect measure of the humidity of the air. The Dew Point will never exceed the Temperature. When the Dewpoint and Temperature are equal, clouds or fog will typically form. The closer the values of Temperature and Dew Point, the higher the relative humidity.
Feels Like Temperature	Apparent temperature that represents what the air temperature feels like on exposed human skin due to the combined effect of the wind chill or heat index.
Forecast Description (Long)	Full summary of Forecast.
Forecast Description (Short)	Shortened summary of Forecast.
Forecast Severity	Overall severity of forecast ranging from no threat to dangerous/life-threatening.
Freezing Rain Accumulation	Forecasted freezing rain accumulation.
Heat Index	Maximum Heat Index. When the temperature is 21.1°C or higher, the Feels Like Temperature represents the computed Heat Index.
Measurable Precipitation	Forecasted measurable precipitation (liquid or liquid equivalent regardless of what type falls).
Precipitation Chance	Maximum probability of precipitation expressed as a percentage.
Precipitation Type	Expected type of precipitation.
Relative Humidity	Relative humidity of the air, which is defined as the ratio of the amount of water vapor in the air to the amount of vapor required to bring the air to saturation at a constant temperature. Expressed as a percentage.
Scattered Cloud Base	Height of the lowest cloud base for a cloud deck that covers more than 25% of the sky.

Event Type	Description
Sea Level Pressure	Mean sea level pressure
Snow Accumulation	Forecasted snow accumulation.
Temperature	Temperature of the air, measured by a thermometer 1.5 meters above the ground that is shaded from the other elements.
UV Index Description	UV Index Description complements the UV Index value by providing an associated level of risk of skin damage due to exposure.
UV Index Value	Maximum UV Index
Visibility	The horizontal visibility at the observation point.
Wind Chill	Minimum Wind Chill. When the temperature is 16.1°C or lower, the Feels Like Temperature represents the computed Wind Chill.
Wind Direction	Average wind direction.
Wind Gust	Maximum expected wind gust speed.
Wind Speed	Forecasted sustained wind speed.

TROPICAL UPDATES

Event	Description
Severe Weather	Alerts issued by agencies for information on severe tropical weather with forecasted impacts to a specific location.

Appendix D: Phone Number Formatting

Follow these protocols for entering domestic (US and Canada) and international phone numbers to ensure alerts are successfully delivered to voice devices.

International Phone Numbers

For contacts who live outside the United States and Canada, always enter the number as if it were being dialed from within the United States, even if the call is being made from an international telephony server.

After choosing the country code or GMSS (Global Mobile Satellite System) code from the drop-down list, you can enter the rest of the phone number without any spaces or symbols, with dashes, or with periods.

Country Code (Optional)	Phone number
+33	522458657
Country Code (Optional)	Phone number
+1	518-333-5000
Country Code (Optional)	Phone number
+1	518.333.5000x223

Note that some countries dial 0 first when dialing locally. This 0 must be omitted from the **Phone number** field. In the above example with the 33 country code, the 0 has been removed from the beginning of the main phone number. From within France, the number would be dialed 05 22 45 86 57.

Universal Telephony Syntax

In addition to numerical digits on a telephone keypad, there are a few characters that are read by telephony servers around the world. These characters help guide a call through the phone system, such as entering a PIN, additional data (a conference moderator code), and even pausing to allow time to advance before the next option.

These special characters can be entered into the **Phone number** field of a people record and in the **Phone Number** field when connecting a recipient to an [External Conference Bridge](#) as part of a response option.

Universal Telephony Syntax		
0 - 9	Numerical Data	
#	Pound Sign/Hashtag	The end of a requested data stream.
*	Asterisk	Personal data (PIN) will follow.
,	Comma	1/2 sec. delay before the next item.
x	Letter "x"	More requested data will follow.

- If you have a contact whose phone number includes an extension, you can do so by entering an “x” between the main number and the extension.

Country Code (Optional)	Phone number
+1	518.333.5000x223

- If your conference bridge uses a conference or meeting ID, you can include it in the **Phone Number** field so that recipients do not have to enter it manually. After the conference bridge phone number, enter an **x**, the conference ID number, and **#**, as this teleconferencing system requires.

Some teleconferencing systems require that you enter information at specific times, which means you will need to have pauses between these bits of information. You can do so by including commas in the syntax. Each comma equates to ½ second of delay.

Country Code	Phone Number
+1	5185551234x83523632#,,,,#,,,#

In the above example, the conference bridge instructions are set up for a teleconferencing system that requires a conference ID and asks for but does not require each participant to speak their name. Broken down, the instructions say to:

1. Dial 1-518-555-1234.
2. Tell the teleconferencing system that more data is to follow (X).
3. Enter 83523632 as the conference ID, followed by a required hash (#).
4. Wait 2.5 seconds to skip the name request followed by a required hash.
5. Wait 1.5 seconds while the teleconferencing bridge says, “Press hash to join the conference,” followed by that hash.

Since each teleconferencing system is different, getting the exact syntax, including counting the seconds between actions, may take several tries.