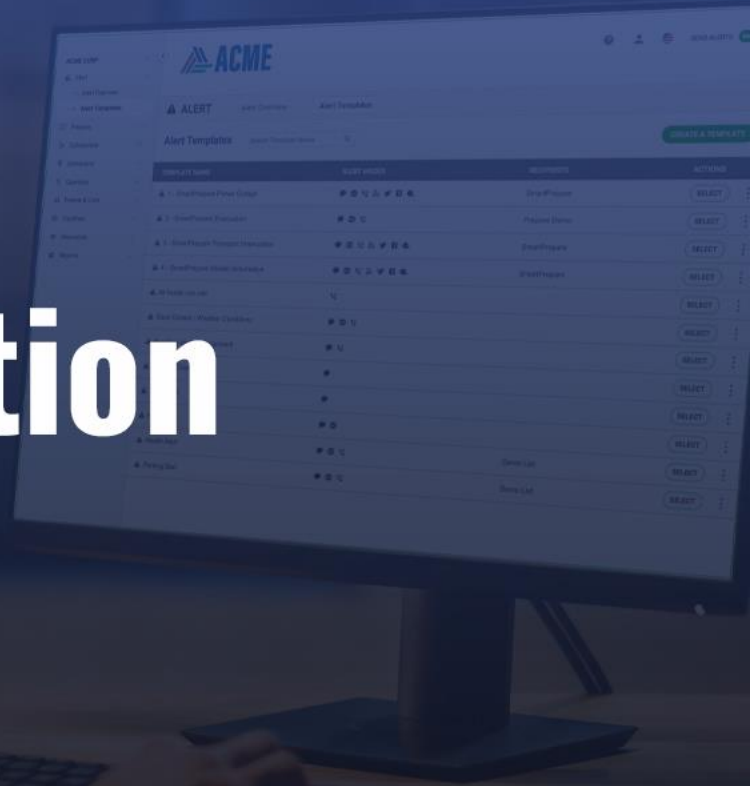




**CRITICAL COMMUNICATION
AND COLLABORATION**

Critical Communication



RAVE
MOBILE SAFETY

Role-Based Access Controls Admin Guide

Updated April 12, 2022

[See the most recent version of this document here](#)

Or through the Get Help link in Rave Alert.

Table of Contents

- What is Role-Based Access Control? 2

- 1. Combine Repeatable Roles and Flexible Individual Permissions 3
 - 1.1 What is an Admin Role? 4
 - 1.2 Individual Admin Permissions..... 5
 - 1.3 Should I Add an Override or Change the Role? 6

- 2. Rules and Examples for Planning Access Levels 8
 - 2.1 Basic RBAC Rules 8
 - 2.2 Tips for Planning Your Organization’s Roles 8
 - 2.3 Example Scenarios for Using Roles..... 9
 - 2.4 Rules for When Admins Only Have Partial Access to a Tool 10

- 3. Default Admin Roles 11
 - Legacy Roles – *Legacy Deployments Only* 12

- 4. Using Custom Administrative Roles..... 13
 - 4.1 Create a New Admin Role..... 13
 - 4.2 What Admins Can Do With Alerts – Alert Tab Options..... 19
 - Alerts Permissions 20
 - What Admins Can Do with Alerts and Templates – Permissions Checkboxes..... 22
 - Assigned Templates – Which Pre-Approved Alerts Admins Can Send 24
 - Assigned Delivery Modes – Which Modes Admins Can Send Alerts Through 25
 - Assigned Shapes – Which Locations Admins Can Target..... 27
 - Delivery Targets – Who Admins Can Send Alerts To 27
 - 4.3 Reports Tab Options..... 28
 - Reports Permissions – Which Reports Admins Can View 28

4.4 What Admins Can Do With Recipients – People & List Tab Options	30
People Permissions – What Admins Can Do with People Accounts	31
List Permissions – What Admins Can Do with Collections of People.....	33
Assigned Lists – Which People Admins Can Affect	36
4.5 System Tab Options.....	37
System Permissions – What System and Admin Functions Admins Can Set Up.....	38
4.6 SmartLoader Tab Options.....	40
SmartLoader Permissions – Which Loading Tools Admins Can Use to Manage Users.....	41
4.7 Rave Prepare Tab Permissions	42
Rave Prepare Permissions – Whether the Admin Can Change the Questions You Ask.....	42
4.8 Rave Guardian Tab Options.....	43
Guardian Permissions – Which App Tools Admins Can Access	44
Assigned Chat Categories – Which Text Tip Categories Admins Can Access.....	46
Assigned Timers – Which Locations Admins Can View Timers For.....	47
Assigned Call Categories – Which Call Directory Calls Admins Can Receive.....	48
5. Assigning a Role to An Admin	49
6. Additional Permissions for Individual Admins	53
6.1 Override Permission Rules.....	54
6.2 Add Override Permissions to an Admin.....	55
6.3 Notify an Individual Admin of Every Alert	57
7. Managing Access from Specific Alert Templates.....	58
7.1 View Which Admins Have Access to an Alert Template	58
7.2 Change Who Has Access to an Alert Template.....	62
7.2.1 Change Alert Template Permissions for Admin Roles	62
7.2.2 Change Alert Template Permissions for Individual Admins.....	65

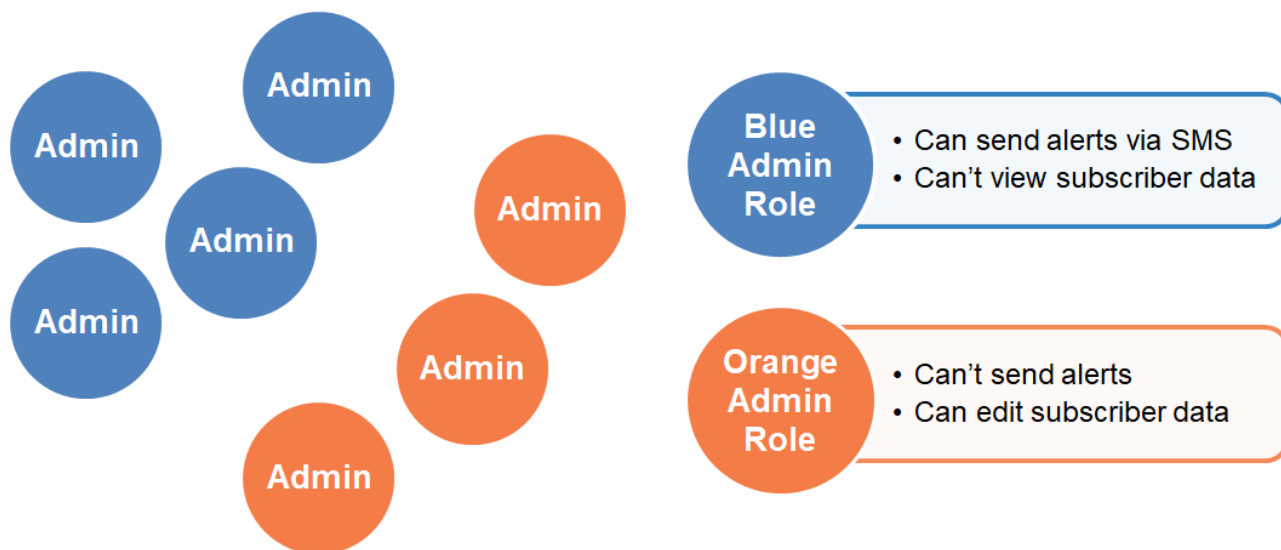
What is Role-Based Access Control?

Role-Based Access Control (RBAC) is Rave Alert's permission system. Use RBAC to configure what features and data your different administrators can access.

Customizable Reusable Roles

The basic building block for RBAC is an admin role. A role is a set of permissions you create and save. Once you create a role, you can assign it to unlimited administrators to quickly define their permissions.

This lets you easily delegate different tools and data access to different parts of your organization. You can create different roles for different departments or access levels, then quickly assign that level of access to each new admin.



Per-Administrator Adjustments If Needed

Roles let you give identical permissions to a bunch of different people. But, sometimes, you might want two people to have slightly different access.

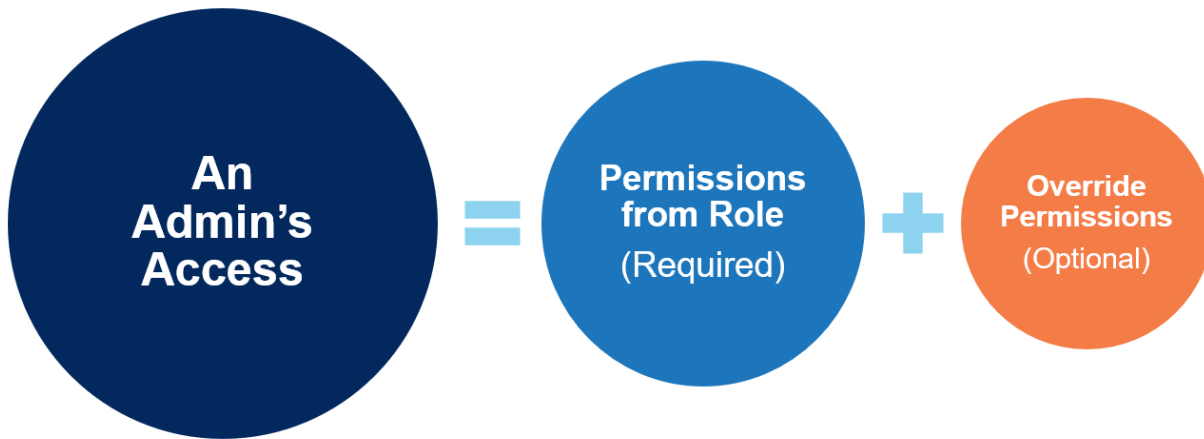
You can still assign them the same role. Once you do, you can also customize an individual administrator's permissions by adding override permissions. This lets you make small adjustments between individual administrators without spending a lot of time on repeat permissions.

This guide will help you configure admin roles and individual permissions that reflect the different access levels your organization needs.

1. Combine Repeatable Roles and Flexible Individual Permissions

Admin roles and override permissions help you delegate access to Rave Alert in repeatable, flexible ways.

An admin's access to Rave Alert depends on two components: the role you assign them and any override permissions you add in addition to their role.



The admin inherits permissions from their role. These role permissions match the permissions of every other admin assigned to that role. You can then customize a particular admin's access by adding override permissions on top of their role settings.

Permissions from Role – Shared Among Multiple Admins

Every admin in Rave Alert has a role. An Admin's role controls what areas of Rave Alert they can access, which system tools they can use, and which individual alert templates, delivery modes, sets of recipient data, or system configuration tools they can access.

Every admin with the same role has the same permissions from that role. You can assign unlimited admins to a role and they all receive the same role permissions. When you change the permission settings for a saved role all admins assigned to that role update at once.

Override Permissions – Adjust Permissions for One Admin

Admins can also have optional override permissions. You can add any tool, alert template, data list, or other setting in Rave Alert to a single admin using override permissions.

These changes only affect one and do not impact admins in the same role. Two admins in the same role can have different override permissions and slightly different access levels.

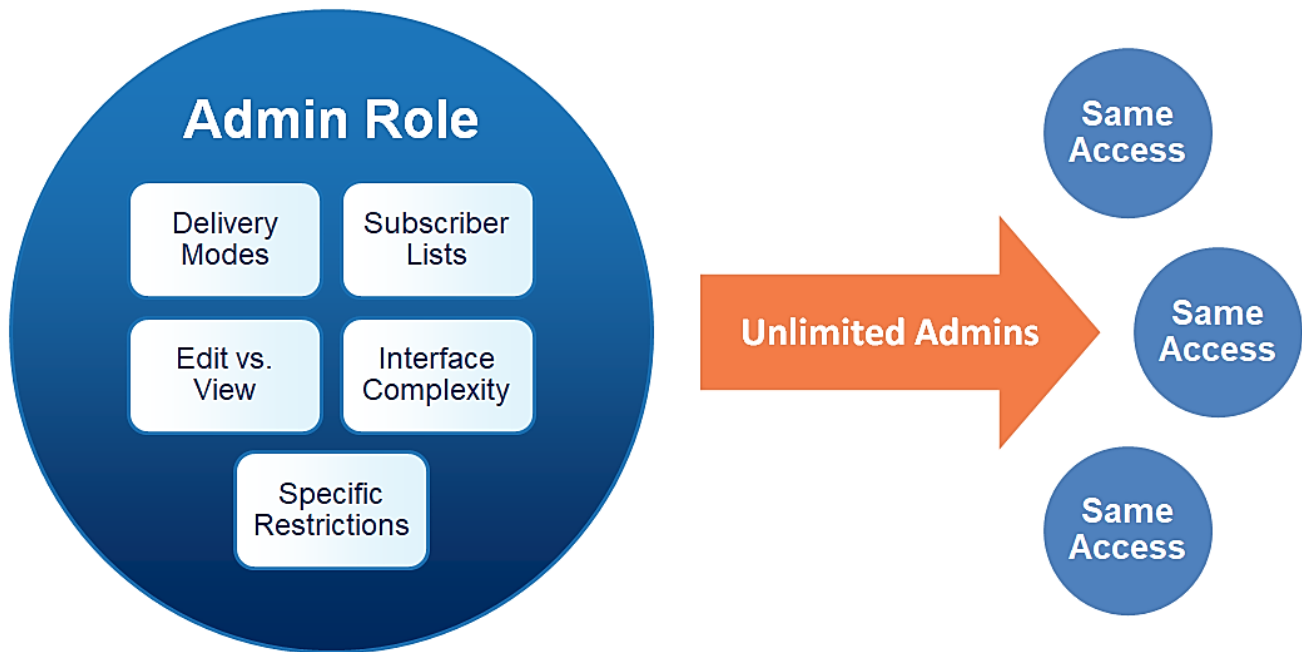
1.1 What is an Admin Role?

An admin role is a set of permissions you save ahead of time, so you can assign it to many admins.

In an admin role, you can save:

- What tools and tabs in Rave Alert admins in the role can access
- Whether they can send alerts, and what delivery modes they can send alerts through
- Who they can send alerts to
- Whether they can view recipient data, and which recipients they can view data for
- Whether they can access system configuration tools, and which ones
- Whether they can view alert reports, and how much access they have to those reports
- Whether they can create, edit, or manage other administrators
- Which alert templates, delivery lists, and other specific data objects they can use

Each admin can only belong to one role.



Roles let you create very different access levels for different people on your system. For example, you could create roles for admins where:

- They only see one Rave Alert tab – such as Alerts, Reporting, or People & Lists
- They send alerts through SnapSend, Rave Alerts simplest, cleanest interface
- They can only send alerts through certain modes – email alerts, no phone calls
- They can only send alerts using certain pre-approved alert templates
- They can only send alerts to specific people, and can't view or edit who
- They can only use specific email addresses, social media pages, or integrated systems
- They can view and edit recipient information, but can't send alerts

- They can create and update alert templates, but can't change which admins use them
- They can create and change recipient lists, but can't view a specific person's contact info

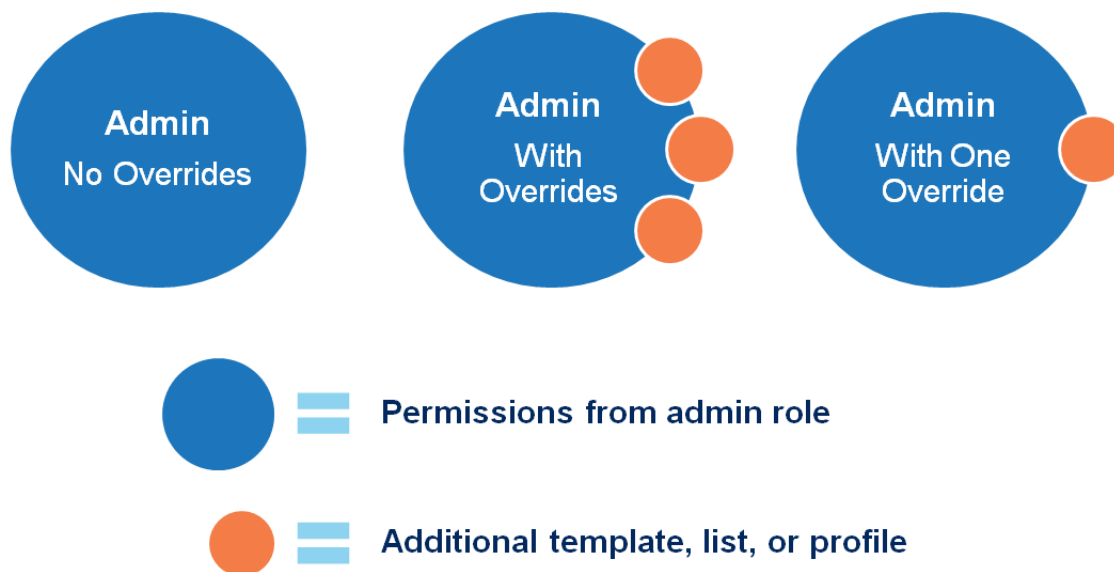
See [Chapter 4](#) how to create roles. See [Chapter 5](#) for how to assign an admin's role.

1.2 Individual Admin Permissions

All admins have permissions from their role. Sometimes, though, you want an individual admin to have extra permissions other admins in their role don't need.

To do this, you can add override permissions to that specific admin.

Override permissions only affect one admin. Other admins in the same role don't receive them, and don't lose overrides they already have.



The Two Rules of Override Permissions

These rules dictate how override permissions interact with role permissions.

Rule #1

An admin cannot have fewer permissions than those assigned to their admin role. Override permissions can only add to role permissions.

Rule #2

If you add a permission in both places, it reverts to a role permission.

For example, say an admin has an override permission. You later add that permission to their role. In this case, the permission becomes a role permission. You cannot edit it as an override on the admin's record anymore because of Rule #1.

See [Chapter 6](#) for how to configure override permissions.

1.3 Should I Add an Override or Change the Role?

Admin roles and override permissions help you meet your goals in different situations.

Ask yourself these questions to figure out which one will work best for you:

Q: How many people need this kind of access to Rave Alert now?

A: Just this one. It's a special case.

B: Multiple people. This is a standard set of needs.

If You Answered A

Consider using an override. It'll let you adjust to this special case without affecting your other admins.

If You Answered B

Consider changing the admin's role or creating a new one. It'll let you quickly apply the same access to other people with these needs, saving you time.

Q: How many people might need this kind of access in the future?

A: No one else. I expect this admin to perform this task in the future even if we grow.

B: More people depending on how many templates/people/admins we add. I expect to assign more people to this task if we grow.

If You Answered A

Consider using an override. It'll let you fit the admin's role to their task.

If You Answered B

Consider changing the admin's role or creating a new one. It'll let you easily expand the number of admins with this access in the future.

Q: Does this permission change often? How many people do you want to change it for at once?

A: This permission does not change often, and changes only affect this admin.

B: This permission changes often. It affects a few admins and impacts each one differently. I go through each one to make sure I set it right for them.

C: This permission doesn't change, except when an admin changes job.

D: This permission changes often. It affects multiple admins and impacts them all the same way. I want to update permissions for all of them at once.

If You Answered A or B

Consider using an override. It'll let you perform changes on an individual admin without affecting the others.

If You Answered C or D

Consider editing the admin's role or creating a new one. It'll let you apply consistent permission changes to multiple people at the same time and keep set job access levels.

2. Rules and Examples for Planning Access Levels

2.1 Basic RBAC Rules

Rave Alert’s Role-based Access Control (RBAC) is flexible and configurable in a lot of different ways. It has two rules to make this flexibility work correctly.

Rule #1

All admins in Rave Alert must have a role.

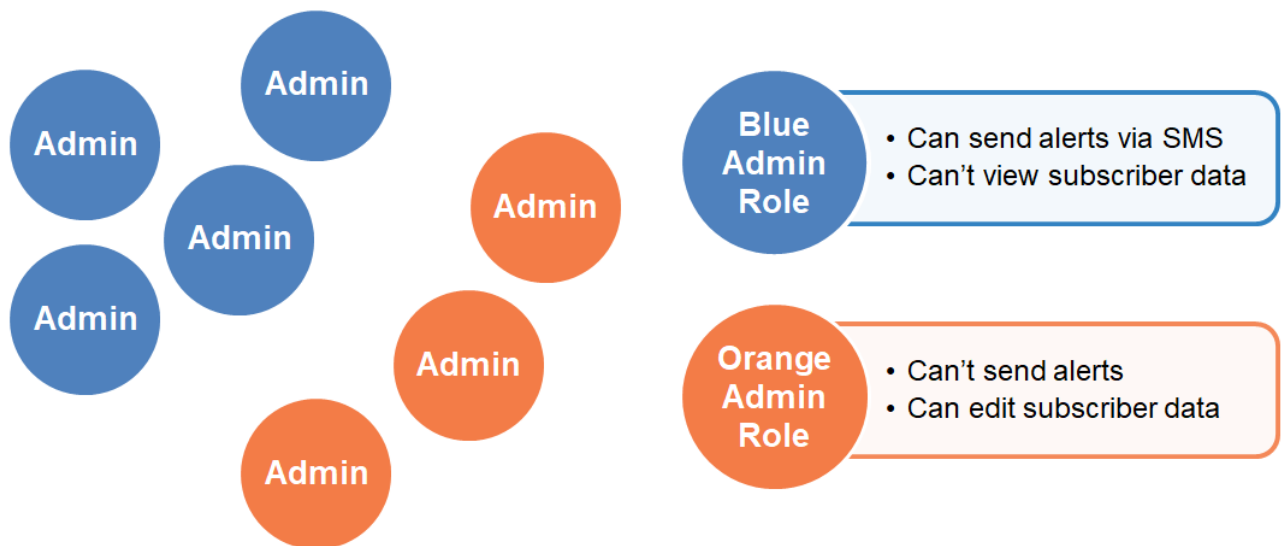
Rule #2

Admins can only have one role.

2.2 Tips for Planning Your Organization’s Roles

RBAC helps you build the right access structure for the people using your Rave Alert domain. You can limit each person to only the tools they need to fulfil their function, enhancing security and protecting from false activations.

Within RBAC, roles let you save time by grouping permissions once, then assigning them to many admins. You can build roles for groups with different tasks or data access.



Knowing which roles to make takes some detective work. Every organization is unique, and you can customize Rave’s tools to match yours.

To discover what roles your organization might need in Rave Alert:

1. **Talk to someone from each department that uses or wants to use Rave Alert.**
Find out what they use it for now and how they plan to use it in the future.
2. **Look at the data you have in Rave Alert – contact data, reports, usage.**
Think about who in your organization should and shouldn't have access to this data.
3. **Gather a list of the message types your organization wants to send.**
Identify scenarios where you want to limit who can send a message – such as emergency closure alerts or event updates.
4. **Gather a list of the delivery technology your organization wants to use.**
Identify scenarios where you want to restrict access to alarms, social media pages, email addresses, or other delivery options.

Once you have a sense of the different access needs for your organization, group them into similar needs and build roles for those needs. You can then assign each access level quickly to new admins.

2.3 Example Scenarios for Using Roles

Roles can save you time anywhere different admins should have different access levels in Rave Alert. Here are some examples where you might want to create admin roles:

- You have multiple sites or departments. Admins from one location should only message recipients associated with their group.
- Each of your sites or departments has their own emails or social media accounts. Admins from one site should only update forums associated with their group.
- You have high impact alerts, like weather closings and emergency updates. Only a small number of admins should see and use these high impact alert templates.
- You have high impact delivery methods, like sirens, alarms, or cable TV screens. Only admins with specific credentials should be able to see and use these delivery options.
- Your help-desk staff need to help recipients manage their information. These admins need to view and edit recipient information but should not see alert tools or be able to send messages.
- Your emergency response personnel need to launch emergency alerts through a simple, easy interface, without seeing any recipient information
- Your IT staff need access to configurations for setting up integrations and importing recipient data, without seeing any alerting tools

In these scenarios, you could build a role with the right access levels for the relevant admins. Once you build it, you can assign as many people that access level as needed.

If you have many roles, you may want to create a consistent naming convention for them. Having all the name structures match can help new admins quickly learn how to read them.

2.4 Rules for When Admins Only Have Partial Access to a Tool

An admin can sometimes only have access to part of a tool. In these cases, Rave Alert always restricts the admin to only the part of the tool they have permission to access.

For example, imagine an admin who has access to the SMS and email alert methods. This admin opens an alert template with SMS, email, voice call, and social media messages.

Because of their permissions, the admin only sees the SMS and email parts of the alert template. They don't see the voice or social media portions.

When the admin sends this message, Rave Alert will only send the SMS and email portion of the alert. Rave Alert automatically omits all unauthorized mode content.

Here are tables of each case where this can happen:

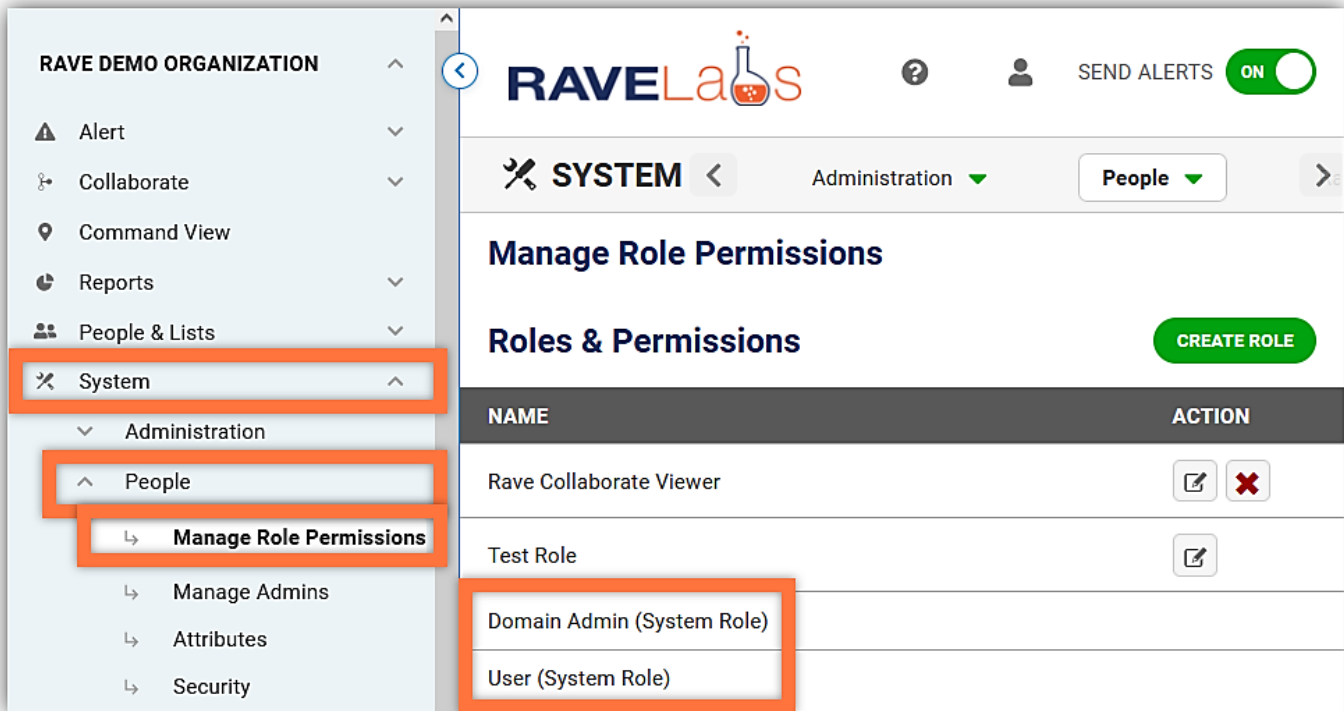
Delivery Modes in Alert Templates		
Admin Has Permission To	When They Send the Template	Can They Save the Template?
All modes in template	Message transmits through all included delivery modes	Yes. Admins can save changes to the existing templates
Some but not all modes in template	Message ONLY transmits through the modes the admin has access to	No. Admins cannot save changes over the existing template. They must copy and create a new template.

Recipient Lists		
Admin Has Permission To	When They Send the Template	Can They Save the Template?
All lists in template	Message transmits to all recipients in template	Yes. Admins can save changes over the existing template
Some but not all lists in template	Message ONLY transmits to the recipient lists the admin has permission to use	No. Admins cannot save changes over the existing templates. They must copy and create a new template.

3. Default Admin Roles

Rave Alert includes three default roles with different access levels. You can assign these roles to admins or use them for models when creating custom roles as described on page 14.

Default roles are labeled (System Role) in the role list on the Manage Role Permissions Page.



Rave Alert’s default roles are:

Domain Admin

Domain admins can access all features on your domain. They can use all alerting, data management, site configuration, and administrative tools.

User

Not an administrative role

User is the standard, default role for people in Rave Alert. A User can receive alerts and log in to the user console to manage their personal information, like adding or editing contact points. A user can’t access any alerting, data management, or site configuration tools.

Managed Contact

Not an administrative role

Managed Contact is the default role for someone your admins bulk load into the Rave Alert using the Managed Contacts loader. Managed Contacts can only receive alerts. They cannot access the user console view or change their information or contact points in the system and cannot access any administrative tools.

Legacy Roles – Legacy Deployments Only

Depending on when you started with Rave Alert, your domain might use some of our legacy roles from previous RBAC versions.

Broadcast Alert Administrator

Broadcast Admins can send alerts to any recipients and view reports related to these alerts. They can't access data management, site configuration, or administrative tools.

This simplifies the interface for them, improves site security, and supports privacy standards compliance.

List Administrator

List Admins can send alerts to a specific set of recipients and view reporting related to those alerts. They can only access specific lists.

They cannot access data management, site configuration, or administrative tools.

Legacy Faculty Role – *Legacy Deployments Only*

Not a standard role

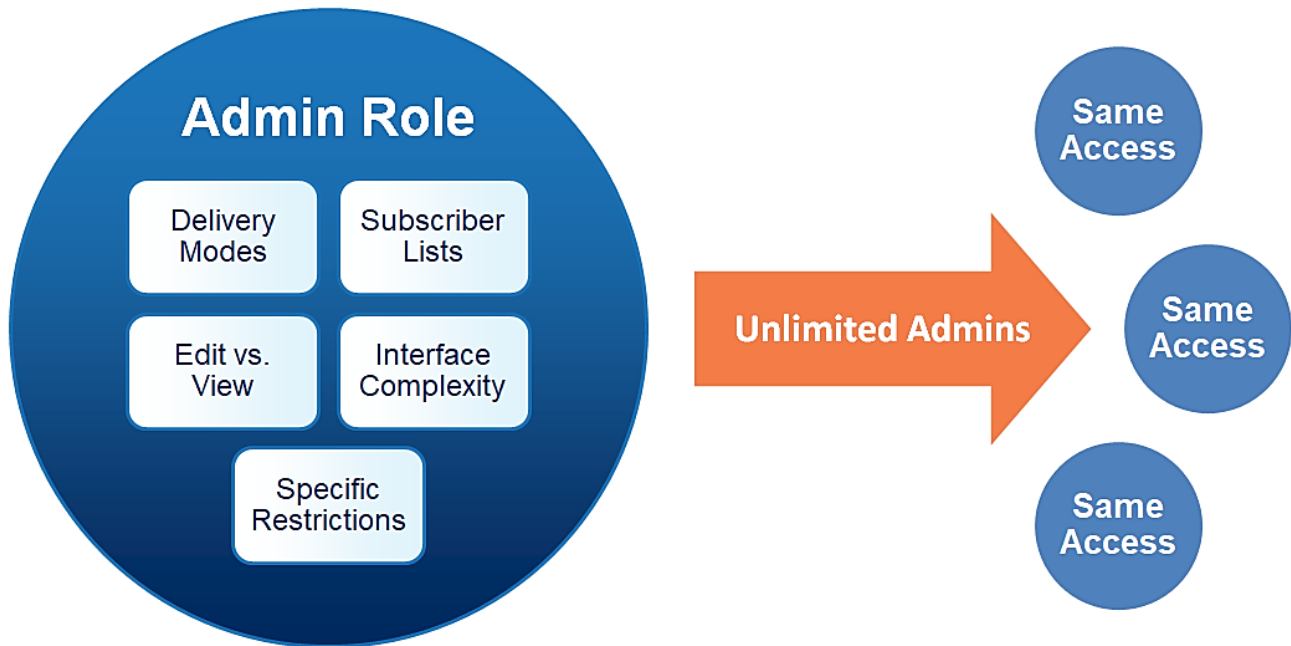
Some legacy deployments have this role; it is not included in new deployments.

Administrators in this role can access Advanced Polling features of the legacy Groups interface, without access to the Admin Console functional areas.

4. Using Custom Administrative Roles

Admin roles help you give the right people access to the right Rave Alert tools. You can configure custom roles with access to Rave Alert features, configuration tools, alert templates, recipient lists, and delivery profiles.

Once you create a role, you can assign it to unlimited administrators. This allows you to reuse the same set of permissions many times, saving time as you create administrators.



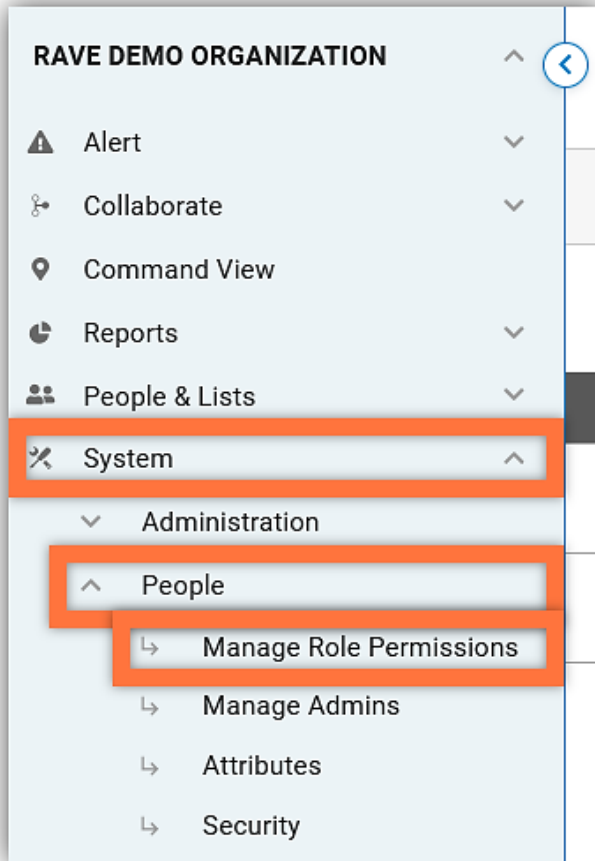
4.1 Create a New Admin Role

Each admin role saves a set of permissions so you can easily assign it to many admins. You can configure access to tools, features, and data in admin roles.

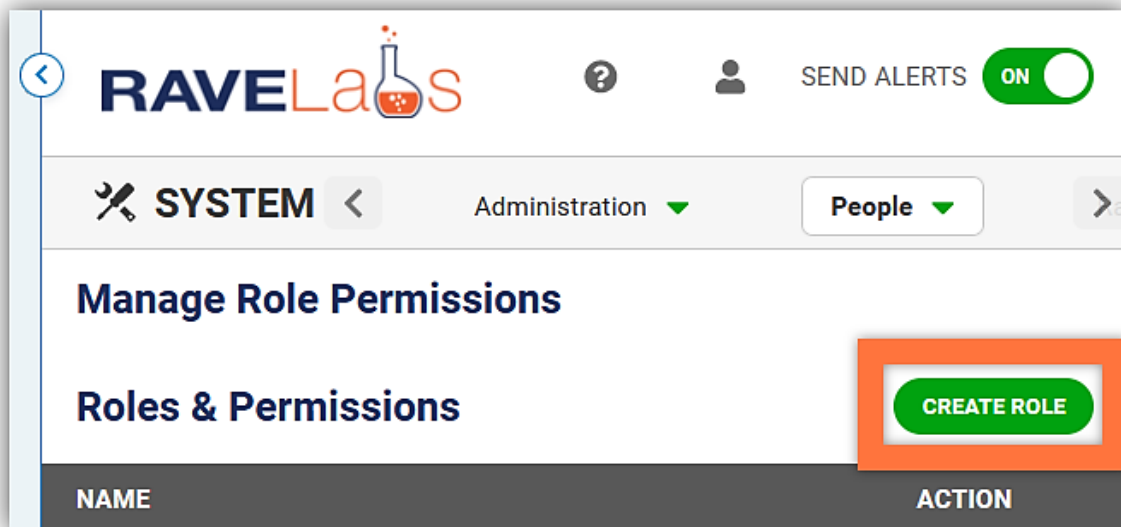
You can create unlimited custom roles with any combination of alerting, data management, and site configuration tools. Once you have a role, you can assign it to unlimited admins.

To create a custom role:

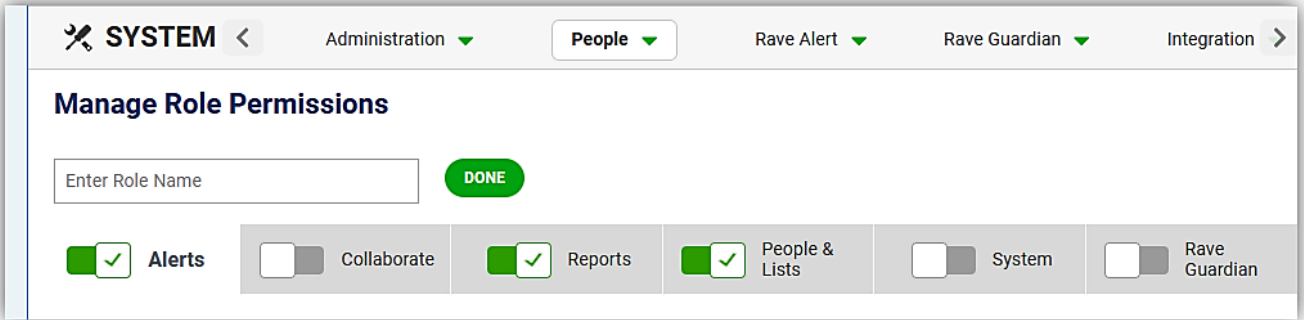
1. Open the System section, People subsection, Manage Role Permissions page.



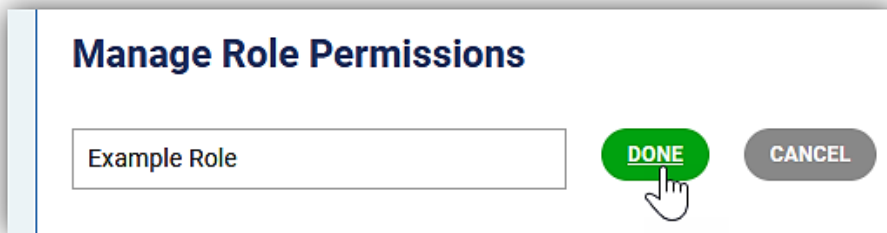
2. Select the Create Role button.



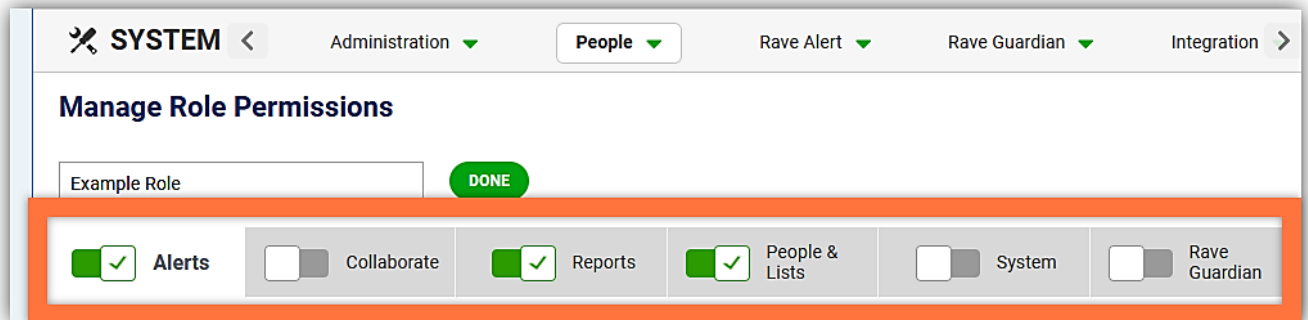
The Role Creation page opens.



3. Enter a Role Name. This name helps you recognize the role when assigning it to admins.
4. Select the Done button



5. Click a tab in the role editor pane to enable it for this role.



Each tab in this pane corresponds to a tab in the Rave Alert console. When you enable a tab here, admins in this role can view and access that tab in Rave Alert.

Depending on your domain, the available tabs are:

- **Alerts**
Permissions for sending messages, delivery modes, and assigned templates
See [Section 4.2](#) for details
- **Collaborate**
Permissions for setting up and tracking event response tasks, resources, and checklists.
See the [Rave Collaborate User Manual](#) for details
- **Reports**
Permissions for viewing at alert records, recipient confirmation, and usage data
See [Section 4.3](#) for details

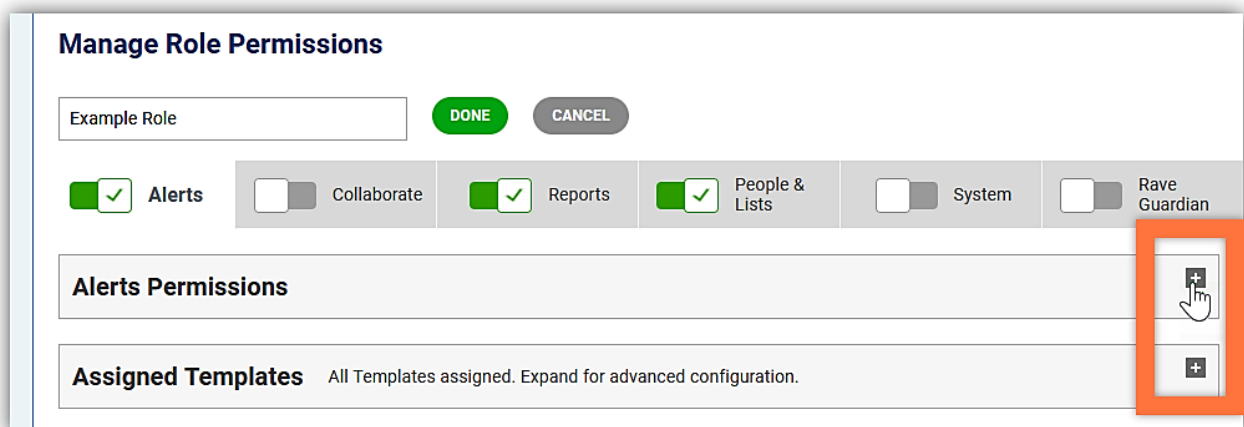
- **People & Lists**
Permissions for organizing recipients and assigned lists
See [Section 4.4](#) for details
- **System**
Permissions for setting up Rave Alert functions and managing admins
See [Section 4.5](#) for details
- **SmartLoader**
Permissions for bulk loading users
See [Section 4.6](#) for details
- **Rave Prepare**
Permissions for vulnerable needs queries
See [Section 4.7](#) for details.
- **Rave Guardian**
Permissions for the Rave Guardian™ companion app, RCV appearance, and assigned app interaction categories
See [Section 4.8](#) for details

Your Domain May Not Have Every Tab

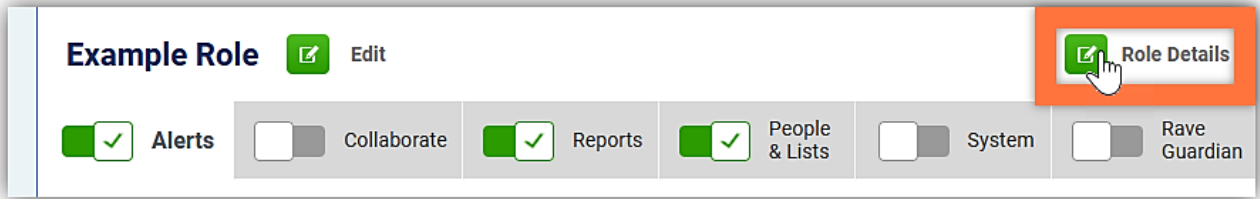
If you don't see one of the tabs shown in these screenshots, your domain does not have it enabled. No admin in your domain will have access to it.

6. Enable permissions within the tabs you've opened, as described in each tab's section. Each tab has different feature and data permissions sections.

Click the expand/collapse button in the upper right side of each section to view or hide specific permission sections.

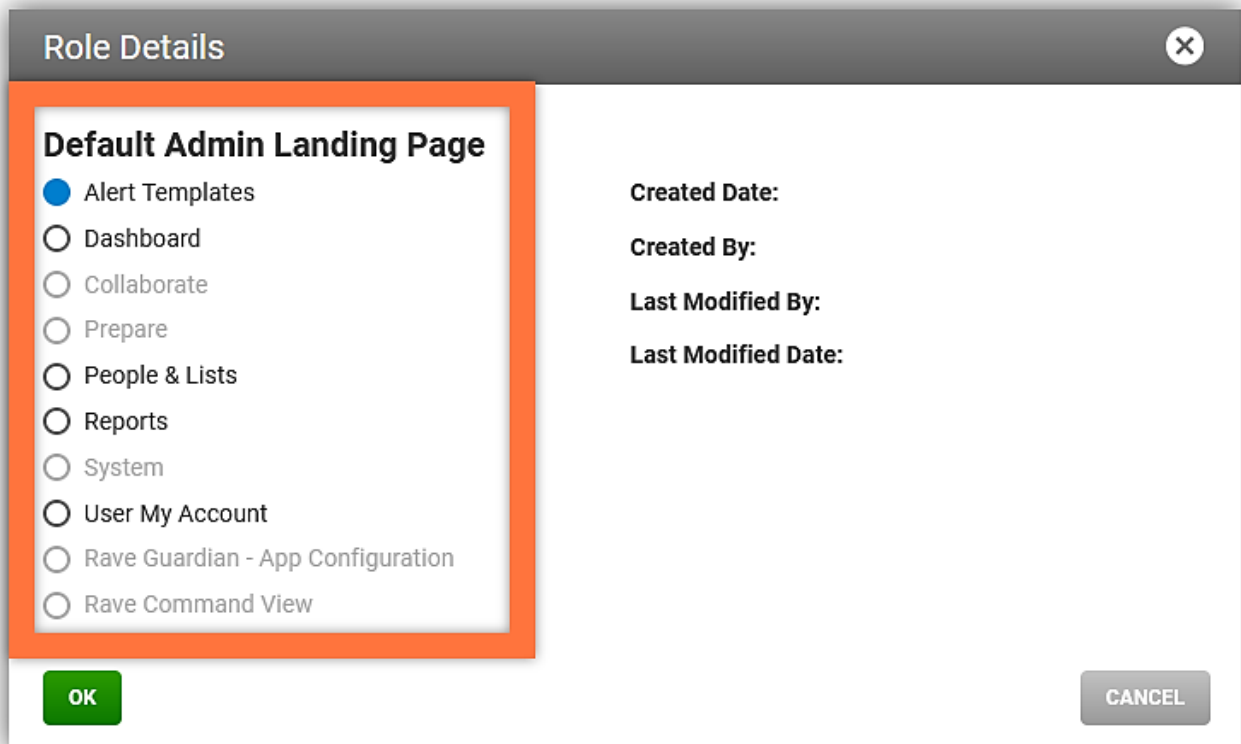


7. Select the **Role Details** button.



The Role Details window opens.

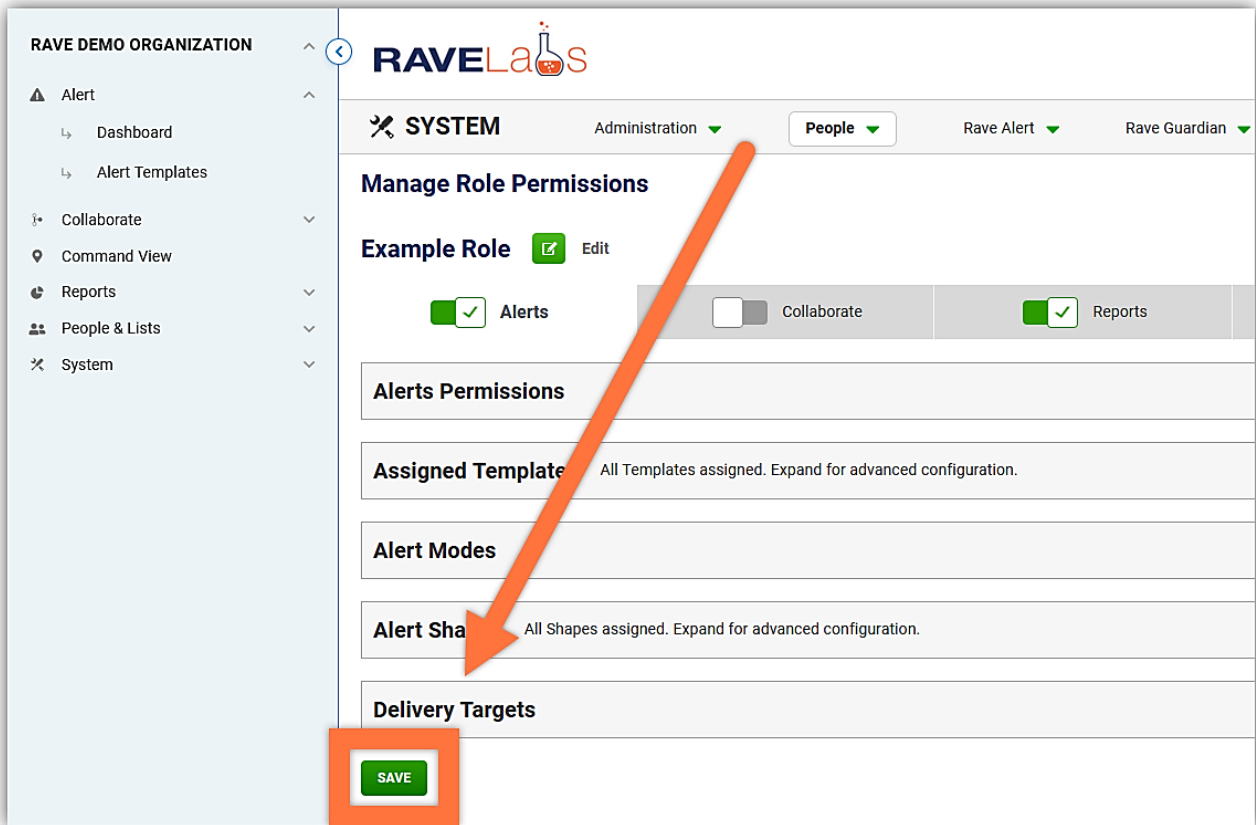
8. Select a landing tab for admins in this role. The landing tab is the first tab admins in this role see when they log into Rave Alert.



Your Landing Page Must be a Tab You Enabled in Step 5

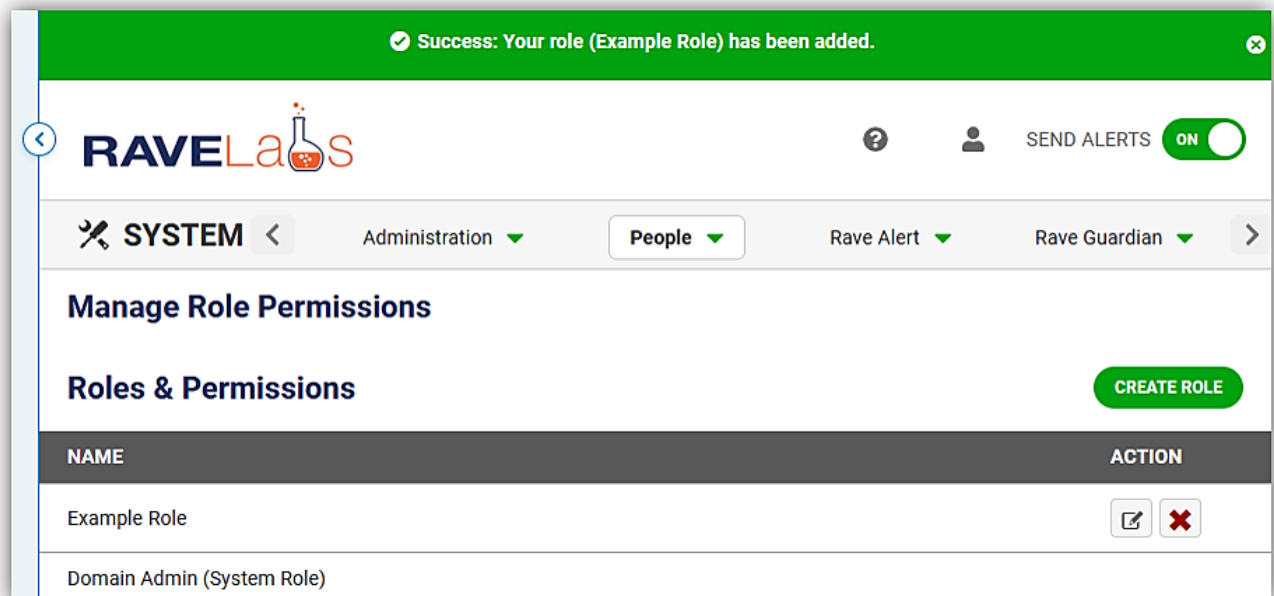
If a tab shows a greyed-out radio button, you haven't enabled it yet. Enable the tab as described in Step 5, then set the tab as the role's default.

9. Select the Ok button.
10. Select the Save button at the bottom of the page.



Congratulations, you've created a new admin role!

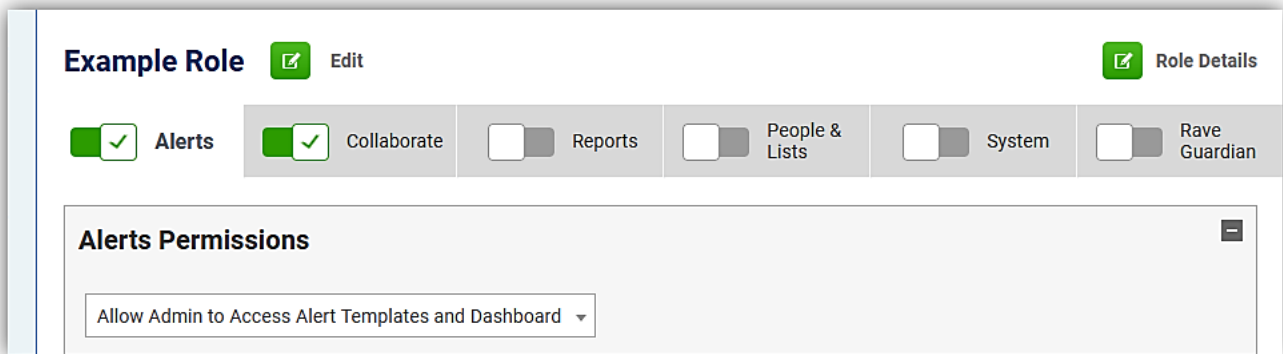
A success bar confirms we've added your new role, which shows in the role list on the Manage Role Permissions page.



You can now assign this role to existing and new admins.

4.2 What Admins Can Do with Alerts – Alert Tab Options

When you enable the Alerts Tab, admins in this role can access alert-sending tools.



In This Tab – Sending Alerts, Alert Templates, Shapes, Delivery Modes

An admin must have access to the Alerts tab to send alerts.

Once you enable this tab, you can set an admin's experience with alerts:

- How simple vs. tool-rich the alert tab looks to them
- Which tools they can use – specific templates, delivery modes, and shapes, or all of them?
- How much they can manage templates – use existing ones? Or create, edit, and delete them?
- Whether they can change other admins' alert settings
- Whether they receive notification every time anyone at your org sends an alert

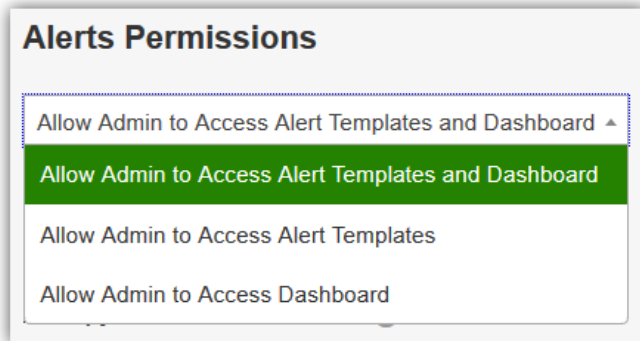
The Alerts tab contains 5 sections.

1. **Alert Permissions** –
Tab appearance, template editing, and managing other admins
2. **Assigned Templates** –
Restrictions for admins to only use specific existing alert templates
3. **Assigned Delivery Modes** –
Restrictions for admins to only use specific delivery modes for alerts
4. **Assigned Shapes** –
Restrictions for admins to only use specific geo-targeting shapes for alerts
5. **Delivery Targets** –
Direction to the correct tab to configure restrictions to creating lists

Alerts Permissions

This section controls how the alerts tab looks and what admins with this role can do with alert templates and alerts.

“Allow Admin to Access...” Menu – How the Alerts Tab Looks to Admins



What Does It Do? – Controls How Complex Alert Sending Looks

Every role needs an option from this menu. It controls complex the Alerts tab looks.

Admins who need a clean, simple interface need the Dashboard view.

Admins who need to be able to create, edit, and delete alert templates need the Alert Templates view.

Option	Effect
...to Dashboard	<p>Admins in this role can only open the Dashboard, a simplified view of ongoing alerts and a select few alert templates.</p> <p>Admins with this setting can't create, edit, or delete alert templates. They also can't assign templates to other admins. You'll see these options greyed out underneath the menu.</p>
...to Alert Templates	<p>Admins in this role can only open the Alert Templates page, a more complex and tool-rich view with a list of all alert templates the admin can access and template management tools, if they have access to them.</p>
...to Alert Templates and Dashboard	<p>Admins in this role can switch views between the streamlined dashboard and the tool-rich alert template page as needed.</p>

Alerts Tab – Simple Dashboard View

RAVE DEMO ORGANIZATION

- Alert
 - Dashboard
 - Alert Templates
- Collaborate
- Prepare
- Command View
- Reports
- People & Lists
- System
- SmartLoader

RAVELabs SEND ALERTS **ON**

ALERT Dashboard Alert Templates

SnapSend Advanced Send

Template
Active Assailant SnapSend

Recipients Edit
Admin, Jane

Short Message 80 characters left
Rave Lab 12: TEST - Active Assailant reported on Campus ... [INSERT DETAILS HERE]

Long Message 9920 characters left
Rave Lab 12: TEST - Active Assailant reported on Campus ... [INSERT DETAILS HERE]

Status
Alert will be sent to 1 Recipients.

REVIEW AND SEND ALERT **RELOAD**

Scheduled

Name	Scheduled For	Created On/By	Method	Action
There are currently no Scheduled Alerts.				

Recently Sent

Sent	Name	Status	Action
10/20/2021 02:24 PM	Leadership emergency...	Delivered	Q
10/18/2021 10:11 AM	Leadership emergency...	Delivered	Q
10/14/2021 10:41 AM	Leadership emergency...	Delivered	Q
10/14/2021 10:41 AM	Leadership emergency...	Delivered	Q
10/14/2021 10:41 AM	Leadership emergency...	Delivered	Q

Operations Notices
There are currently no Operational Notices.

Alerts Tab – Detailed Alert Template View

RAVE DEMO ORGANIZATION

- Alert
 - Dashboard
 - Alert Templates
- Collaborate
- Command
- Reports
- People & Lists
- System

RAVELabs SEND ALERTS **ON**

ALERT Dashboard **Alert Templates**

Alert Templates Search Template Name **CREATE ALERT OR TEMPLATE**

TEMPLATE NAME	ALERT MODES	RECIPIENTS	ACTION
Active Assailant on Campus	📢 📧 📞	Individual Users	SELECT ⋮
All Clear - No Further Threat is Known	📢 📧 📞	Individual Users	SELECT ⋮
Leadership emergency conference call	📞	Individual Users	SELECT ⋮

What Admins Can Do with Alerts and Templates – Permissions Checkboxes

Alerts Permissions

Allow Admin to Access Alert Templates and Dashboard ▾

User Can Create/Edit/Delete Templates

Assign Templates to Other Admins

Admins in assigned Lists and current Role All Admins

User Can Create/Edit/Delete Templates

Who Should Have It? – Admins who manage the alerts you send

This control allows admins to save changes to alert templates, create new ones, and delete existing ones.

When Enabled	When Disabled
Admins can change and create alert templates.	Admins cannot change or create alert templates.

Assign Templates to Other Admins Checkbox

Who Should Have It? – Admins who manage admins who send alerts

This setting controls whether an admin can change other admin's alert template assignments. You can use it to delegate managing the people who send your alerts.

When Enabled	When Disabled
Admins can assign other admins access to alert templates.	Admins cannot assign other admins access to alert templates.

When enabled, you can choose between:

Option	Effect
Admins in assigned lists	Admins can only manage alert assignments for a limited set of admins you assign them. Useful for delegating department or team-level management. Use Assigned Lists control in the People & Lists tab to set the limited admins.
All Admins	Admins can assign or unassign alert templates to any admin.

Assigned Templates

– Which Pre-Approved Alerts Admins Can Send

By default, admins can access all templates. Or you can restrict them to a specific set.

Who Should Have Them? – Admins who only send specific kinds of alert

Assigning specific templates lets you limit admins to preapproved alerts and delivery lists. It also keeps the alert screen simple for those admins who only send a couple alerts.

For example, you can assign just the road closure templates to a maintenance team, while your emergency response team can have many different alerts to cover your response plan.

To restrict admins in this role to specific templates:

1. Select the Specific Templates radio button. The Available Templates box opens a list of all templates on your domain.
2. Use the filter bar or scroll to find the specific templates in the All Templates box.
3. Select a template to move it into the Selected Templates box.
4. If needed, select a template in the Selected Templates box to remove it.

The screenshot displays the 'Assigned Templates' configuration page. At the top, there are two radio buttons: 'All Templates' (unselected) and 'Specific Templates' (selected, marked with a red circle '1'). Below this, the interface is split into two main sections: 'Available Templates (10)' and 'Selected Templates (3)'. The 'Available Templates' section has a 'Filter' input field (marked with a red circle '2') and a list of templates. A hand cursor is shown hovering over the 'HTML Email Alert' template, which is highlighted in blue (marked with a red circle '3'). The 'Selected Templates' section also has a 'Filter' input field and a list of three templates: 'Sample Alert', 'Sample Check-in Poll', and 'HTML Email Alert'. Each template in this section has a red 'X' icon for removal. A red circle '4' is placed over the 'HTML Email Alert' template in the 'Selected Templates' list. Navigation arrows are visible between the two lists.

Assigned Delivery Modes

– Which Modes Admins Can Send Alerts Through

SMS, email, voice call, social media, and integrations are all delivery modes.

This section controls which delivery modes admins can send alerts through.

It also controls which delivery profiles admins can apply to alerts for their assigned modes. Profiles are collections of settings that affect a specific mode, like emergency vs. operational SMS numbers, email addresses and formatting for email alerts, formatting on desktop alerts, or caller-ID and answering machine settings for voice alerts.

Assigned Delivery Modes – Which modes admins can change

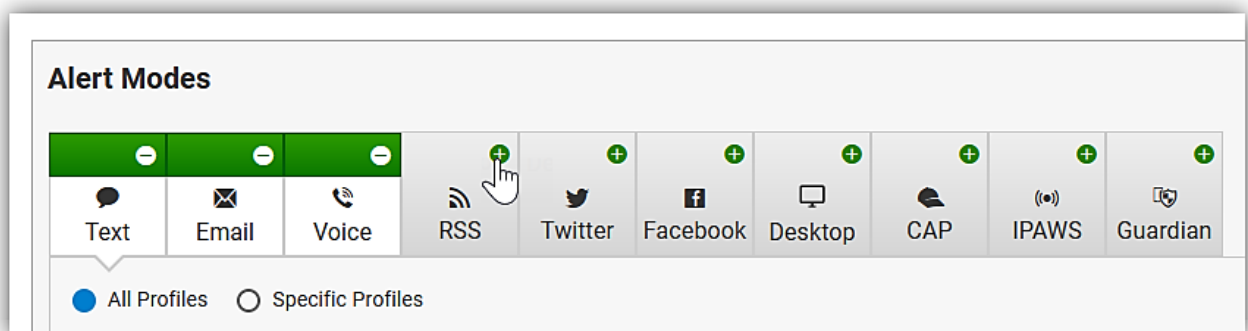
You can control which delivery modes admins can edit for alerts they send or add to alerts they create.

Who Should Have Them? – Admins who should only affect certain communication tools

For example, you could assign social media modes only to admins versed in public relations.

Only those admins could add and update social media content on your templates. And any admin can send this pre-approved content through an alert template with those settings.

To enable or disable a delivery mode, click on it in the Alert Modes section.



This Permission Affects All Alert Templates the Admin Uses

Any time an admin opens an alert template, they can only view and send the delivery modes you assign them access to here.

If they send an alert using a template with more modes, Rave Alert hides the unauthorized modes from them and only sends messages through the modes you assign here.

Assigned Delivery Profiles – Which Identifiers Admins Can Use on Alerts

Profiles are collections of settings that affect a specific delivery mode. Rave Alert has SMS profiles, email profiles, voice profiles, Twitter profiles, Facebook profiles, and desktop alerting profiles for Rave Notifier.

You can restrict admins to only using specific profiles on alerts. For example, you can restrict a role to only sending operational, not emergency, SMS messages, or only posting to a specific social media page.

Who Should Have It? – Admins who only represent part of your org

Use delivery profiles to restrict admins to certain SMS numbers, email addresses or voice call numbers. This can help you delegate messaging through appropriate channels, or separate emergency and nonemergency messaging.

By default, admins can access all profiles for a delivery mode when you assign them that mode. To restrict admins in a role to specific delivery profiles:

1. Open an assigned Delivery Mode. If the mode has profiles, a list of profiles opens beneath the mode.
2. Select the Specific Profiles radio button. A list of all mode profiles displays in the Available Profiles box.
3. Use the filter bar or scroll to find specific profiles in the All Profiles box.
4. Select a profile to move it to the Selected Profiles box.
5. If necessary, select the Delete button on the Selected Profiles box to remove a profile.

The screenshot displays the 'Alert Modes' configuration page. At the top, there are buttons for various delivery modes: Text, Email, Voice, RSS, Alertus, Twitter, Facebook, CAP, and Guardian. The 'Email' mode is selected, indicated by a red circle '1'. Below the mode buttons, there are two radio buttons: 'All Profiles' and 'Specific Profiles'. The 'Specific Profiles' option is selected, indicated by a red circle '2'. Underneath, there are two boxes: 'Available Profiles (4)' and 'Selected Profiles (2)'. The 'Available Profiles' box has a filter bar with a red circle '3'. It contains a list of profiles: 'Aa Example Profile', '</> HTML Profile', '</> HTML Profile 2', and 'Aa Site Default'. The '</> HTML Profile 2' is highlighted with a mouse cursor, indicated by a red circle '4'. The 'Selected Profiles' box has a filter bar and contains a list of profiles: '</> HTML Profile' and 'Aa Example Profile'. The 'Aa Example Profile' is highlighted with a red circle '5'. There are also red 'X' icons next to the profiles in the 'Selected Profiles' box, indicating they can be removed.

Assigned Shapes – Which Locations Admins Can Target

This section controls if and where admins can target alerts by geographic area. Saved shapes let you separate management of shapes from use of them in alerts.

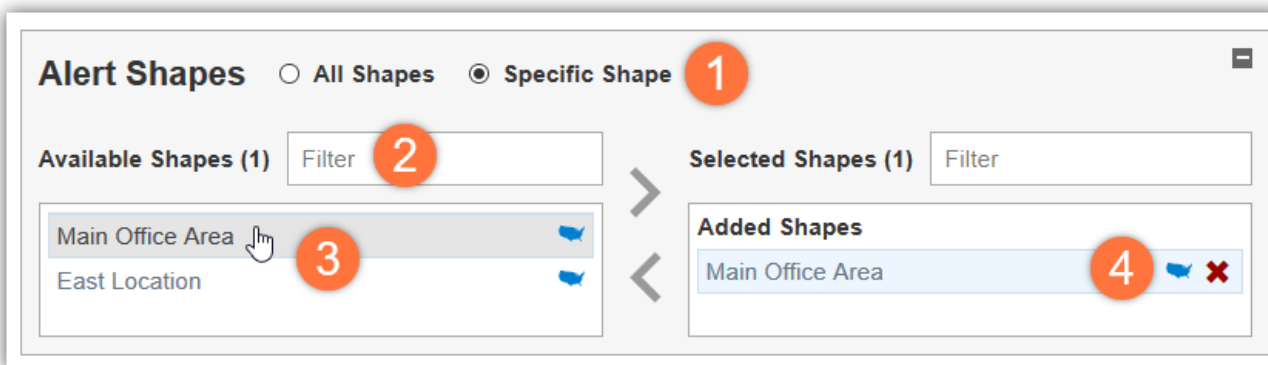
By default, a role with alerting privileges has access to all saved shapes.

Who Should Have Them? – Admins who should target specific locations

Use saved shapes to assign pre-approved jurisdiction areas to different admins. For example, you can have roles with permission to alert to specific jurisdictions or building areas.

To restrict admins with this role to specific saved shapes:

1. Select the Specific Shapes radio button. The Available Shapes box opens a list of all the saved shapes for your domain.
2. Scroll or use the filter bar to find specific shapes in the Available Shapes box.
3. Select a shape to move it to the Selected Shapes box.
4. If necessary, select a shape in the Selected Shape box to remove it.



Delivery Targets – Who Admins Can Send Alerts To

Sometimes you want to limit which people an admin can send messages to. You configure this permission in People + Lists tab, described in [Section 4.3](#).

This section on the Alerts tab reminds you where to find these permissions.

4.3 Reports Tab Options

When you enable the Reports tab, admins in this role can access reports for past alerts and statistics about Rave Alert usage.

Example Role Edit Role Details

Alerts Collaborate **Reports** People & Lists System Rave Guardian

Reports Permissions

Admin can view reports

Reports Sent by Admin Reports Sent by Admins in Role All Reports

SAVE **CANCEL**

In This Tab – Reports on In-Progress Alerts, Completed Alerts, and Usage

An admin must have access to the Reports tab to view delivery information on in-progress and completed alerts. An admin also needs access to this tab to view overall statistics about system usage.

Once enabled, you can control an admin’s experience of reports

- Whether they can view reports for alerts other admins sent
- Whether they can view reports on system usage

The Reports tab contains 1 section: **Reports Permissions**. This section contains view controls for alert reports.

Reports Permissions **– Which Reports Admins Can View**

By default, admins can access reports for every alert sent on your system and for system usage. You can restrict an admin role to only viewing reports for specific alerts, without access to usage reports.

Reports Permissions

Admin can view reports

Reports Sent by Admin Reports Sent by Admins in Role All Reports

Admin can view reports

What's It Do? – Controls Which Alert Reports Admins Can Access

All admins who can access the reports tab need an option from this menu. It controls how broadly they can access alert reports.

Admins who review all sent alerts or overall system usage need the **All Reports** setting.

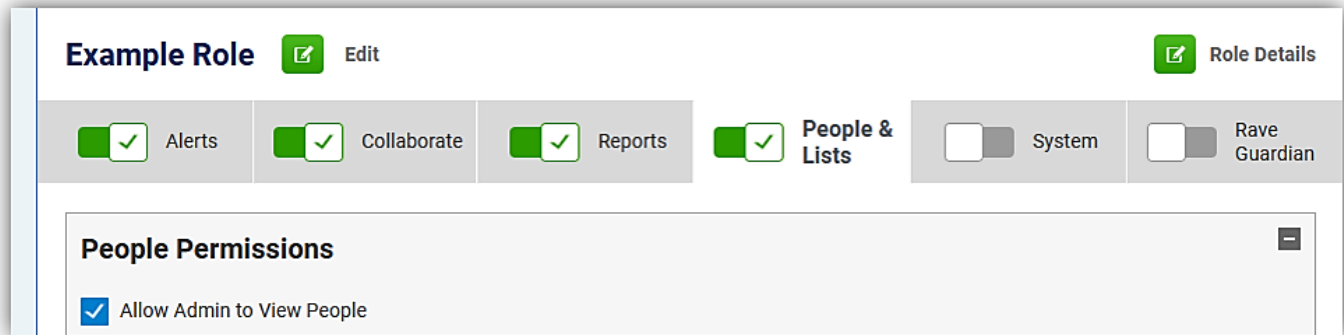
Admins who only review alerts they sent need the **Reports sent by admin** option.

Admins who review alerts sent by admins on their team need the **Reports sent by admins in role** option.

Option	Effect
Reports sent by admin	Admins can only view reports generated by alerts they launched. They cannot view any usage reports.
Reports send by admins in role	Admins can only view reports generated by alerts sent by any admin who has this role. They cannot view any usage reports
All reports	Admins can view reports for all alerts sent on your domain. They can also view all usage reports.

4.4 What Admins Can Do with Recipients – People & List Tab Options

When you enable the People & List tab, admins in this role can access recipient management tools, either for managing recipient data or collecting recipients into lists for alerting.



In This Tab – Managing Recipient Data, Managing Delivery Lists

An admin must have access to the People & Lists tab to view recipient data or create lists.

Once you enable this tab, you can set an admin's experience with recipient data:

- Whether they can view recipient accounts
- Whether they can edit recipient accounts
- Whether they can collect recipients into alert lists
- Which recipients they can view or edit
- Which recipients they can collect into alert lists
- Whether they can change these settings for other admins

On this tab, you can configure permissions related to managing people's data and recipient lists. You can also limit admins in this role to only using specific recipient lists when sending alerts.

The People & Lists Tab contains 3 sections.

1. **People Permissions**

View/Edit access to recipient accounts,

2. **List Permissions**

Create/edit access to collections of people, managing other admins' lists

3. **Assigned Lists**

Restrictions for admins to only message, edit, or affect specific sets of recipients

People Permissions – What Admins Can Do with People Accounts

This section controls whether admins in this role can view, create, or edit recipient accounts. It also lets you restrict admins to only viewing recipient accounts on specific lists.

People Permissions

- Allow Admin to View People
- Allow Admin to Modify People

When sending alerts, building lists, or managing people, admin can choose people from:

People in Assigned Lists All People

Allow Admin to View People

Who Should Have It? – Admins who check recipient information

Admins need this permission to see and search individual people’s records. Give it to admins who need to see individual names, contact information, and attribute data.

When Enabled	When Disabled
Admins can open the People page, search people records, and open individual account pages. You can restrict this function to people on specific lists.	Admins cannot access or view any people records. If admins have access to the People & Lists tab, they can only open the Lists page.

Allow Admin to Modify People

Who Should Have It? – Admins who create or correct accounts

Admins need this permission to change recipient data. Give it to admins who update recipient information, create recipient accounts, or manually delete recipients.

When Enabled	When Disabled
Admins can create, delete, and edit people records. You can restrict this function to people on specific lists.	Admins cannot change people records. If admins have access to the Manage People tab, they can only view people data, not edit it.

When sending alerts, building lists, or managing people, admin can choose people from:

What's It Do? – Controls How Broadly Admins Can Access People

All admins who can send alerts or manage people need an option from this menu. It controls the set of recipients they can access through people search tools.

Admins who need to access all recipients on your system need the **All People** setting.

Admins who need to access a limited set of recipients, without the ability to view people outside that set, need the **People in assigned lists** setting.

This Permission Affects Which People Admins Can Search in Any Tool

Settings Impact People Tools AND List Tools

Admins can interact with people in many different contexts. Even if they cannot view individual records, they might search people to add or remove from lists.

Limiting people with this permission affects all those tools. Admins will only be able to find the people you assign them here.

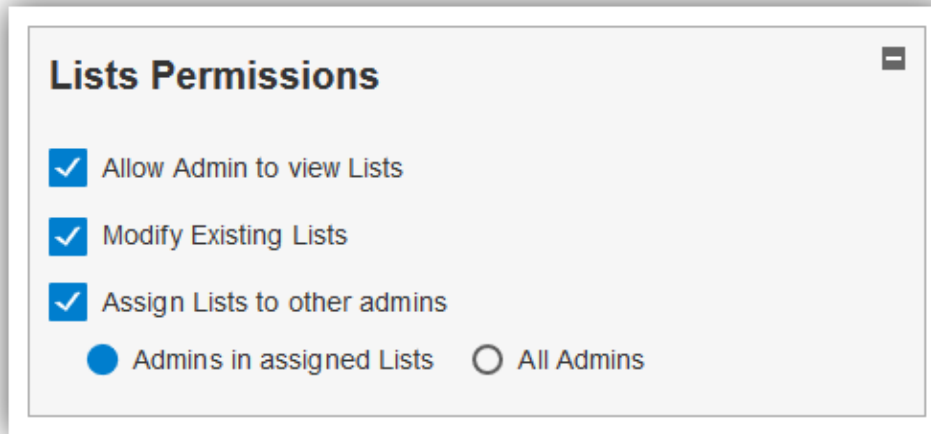
Option	Effect
People in assigned lists	Admins can only access a limited set of people records. When they send alerts, create delivery lists, or access recipient records, admins can only see recipients within their assigned lists. Assign lists to an admin with this setting in the List Permissions section.
All People	Admins can access any recipient on your system through the search tools. Depending on their other permissions, the admin can add those recipients to an alert's delivery targets, place them on a delivery list, or view their account information.

List Permissions – What Admins Can Do with Collections of People

Lists collect individual recipients into sets for admins to interact with all at once.

Your admins can use lists to quickly target many alert recipients at once. You can also assign lists of people to an admin to control which individual accounts they can access.

This section controls whether admins in this role can manage recipients lists or assign them to other admins.



Lists Permissions

- Allow Admin to view Lists
- Modify Existing Lists
- Assign Lists to other admins

Admins in assigned Lists All Admins

You Can Assign a List Without Granting Access to Individuals on That List

An admin finds and selects lists using the list name. They can't open a list to see individual recipient names or contacts unless you separately give them access to people in the People Permissions section.

You can use this to create admins to handle lists without seeing rosters, contacts, or other personal data. For example, someone who sends alerts could have access to delivery lists for certain departments or buildings, without knowing who is on each list.

Allow Admin to View Lists

Who Should Have It? –

Admins Who Need to See Names When They Open a List

Admins need this permission to open lists to see who is on them. Give it to admins who check list rosters and admins who need to change those rosters.

Admins with this permission cannot change who is on a list unless you enable the Modify Existing Lists permission.

When Enabled	When Disabled
Admins can open list records and see the roster of people on them.	Admin cannot open lists to see the roster of people on them.

User Can Create/Edit/Delete Lists

Who Should Have It? – Admins Who Control Who Receives Alerts

Admins who have access to people can build them into lists. Give this permission to admins who divide your recipient database into the right sections for people to send messages to.

You can limit which lists admins can modify by assigning them lists in the Assigned List section.

When Enabled	When Disabled
<p>Admins can create, edit, and delete lists.</p> <p>As part of managing lists, admins can view which recipients are on a list, and search for individual recipients to add or remove from lists.</p> <p>You can limit the recipients they can view to a specific set.</p>	<p>Admins can select lists on alerts, and (if they have permission) assign lists to other admins.</p> <p>Admins cannot open lists to view individual recipients. They also can't change list memberships.</p>

Assign Lists to Other Admins

Who Should Have It? –

Admins who manage admins who view or send alerts to people

This setting controls whether an admin can change other admin's access to sets of people.

Admins with this permission can change who an admin can use in other tools – sending alerts, searching and editing recipient accounts, or creating delivery lists.

When Enabled	When Disabled
Admins can assign delivery lists to other admins.	Admins can't access or edit other admins' delivery list settings.

When enabled, you can choose between:

Option	Effect
Admins in assigned lists	Admins can only manage list settings for admins included on the assigned delivery lists set on this page. Useful for delegating department or team-level management. Use Assigned Lists to set the limited admins.
All Admins	Admins can assign or unassign lists to any admin.

Assigned Lists – Which People Admins Can Affect

By default, admins with access to a tool can affect any person on the system with that tool. For example, admins with alerting permissions can send to anyone, admins with people access can edit anyone, and so on.

In this section, you can limit admins to only affecting specific people instead of everyone.

Who Should Have Them? – Admins who should only affect limited people

Assigning specific lists lets you limit admins to only affecting a limited set of people. It also keeps list or people management screens easier to navigate by removing accounts outside an admin's scope.

For example, you can assign an admin just lists of people within their department. This admin could then only.

Depending on an admin's tool access, this setting controls:

- who they can send alerts to
AND/OR
- whose accounts they can access or edit
AND/OR
- who they can add or remove from lists

To restrict admins in this role to only affecting specific people:

1. Select the Specific Lists radio button. The Available List box opens a list of all recipient lists on your domain.
2. Use the filter bar or scroll bar to find the specific lists in the All Lists box.
3. Select a list to move it to the Selected Lists box.
4. In needed, select a list in the Selected Lists box to remove it.

The screenshot shows the 'Assigned Lists Permissions' configuration screen. At the top, there are two radio buttons: 'All Lists' (unselected) and 'Specific Lists' (selected, marked with a red circle '1'). Below this, there are two main sections: 'Available Lists (11)' and 'Selected Lists (2)'. The 'Available Lists' section has a 'Filter' box (marked with a red circle '2') and a list of lists: 'Everyone', 'General Staff Notifications (200)', 'List 1 (85)', 'List 2 (100)' (highlighted with a red circle '3'), and 'List 3 (45)'. The 'Selected Lists' section has a 'Filter' box and a list of lists: 'List 2 (100)' (marked with a red circle '4') and 'General Staff Notifications (200)'. Each list in the 'Selected Lists' section has a red 'X' icon to its right. Arrows indicate the movement of lists between the two sections.

4.5 System Tab Options

When you enable the system tab, admins can access configuration tools for your domain, including global settings for delivery modes, the login page, and integrations.

On this tab, you can configure permissions for creating new admins and new admin roles.

The screenshot shows a configuration interface for a role named "Example Role". At the top, there is an "Edit" button and a "Role Details" button. Below this, there are several toggle switches for different features: "Alerts" (checked), "Collaborate" (checked), "Reports" (unchecked), "People & Lists" (unchecked), "System" (checked), and "Rave Guardian" (unchecked). Below the toggles is a "System Permissions" section with two checked checkboxes: "Allow Admin to Configure the System" and "Allow Admin to Provision Administrative Users/Roles". At the bottom, there are "SAVE" and "CANCEL" buttons.

In This Tab – Configuring Advanced System Settings, Managing Admins

An admin must have access to the System tab to change Rave Alert domain settings or configure other administrative accounts.

Once you enable this tab, you can set which advanced system tools admins can access:

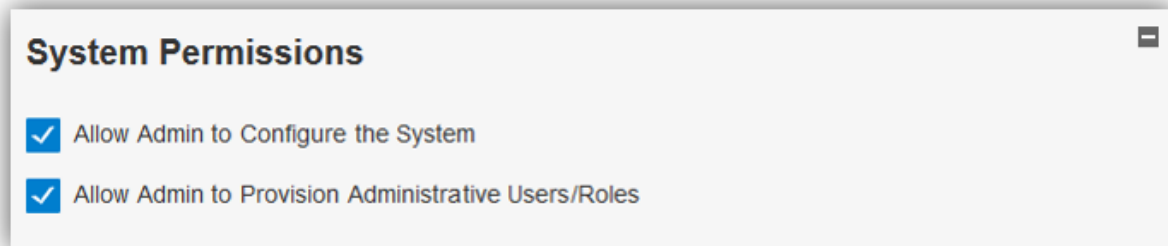
- Whether they can set up alert behaviors like CAP integrations, GIS-based geo filters, voice profiles, and email headers
- Whether they can set up the user attributes and alert categories admins use to sort data
- Whether they can set up branding, appearance, and help content on the Rave Alert site
- Whether they can create and edit admin roles
- Whether they can create admins and assign roles to them

System Permissions – What System and Admin Functions Admins Can Set Up

Rave Alert lets you set up many functions and behaviors ahead of time. This keeps sending an alert simple and consistent for alert authors.

The System tab contains 1 section: **System Permissions**.

This section controls whether admins in this role can set up system configurations – like alert settings and website branding – ahead of time. It also controls whether admins can manage other admin accounts.



Allow Admin to Configure the System

Who Should Have It? – Admins Who Make Large System Decisions

This checkbox grants access to set-ahead tools affecting many admins and recipients, including:

- Alert settings for specific modes, like caller ID, email addresses, and CAP integrations
- Data filters like geographic shapes and user data attributes
- Branding and logo of the website
- Security tools like multifactor authentication and account protection

When Enabled	When Disabled
Admins can access all system configuration tools – including those that affect alert settings, site appearance, and data filtering	Admins cannot configure broad-reaching system settings.

Allow Admin to Provision Administrative Users/Roles

Who Should Have It? – Admins who manage other admins

Admins need this permission to view admin accounts, create admin roles, and assign them to admins. Give it to admins who set up other people's admin accounts.

When Enabled	When Disabled
Admins can promote people to admin, view and edit existing admins, create admin roles, assign admin roles to admins, and view and edit existing admin roles.	Admins cannot create, view, or modify any admin accounts or roles on the system.

Admins with This Enabled Can Change Their Own Permissions (and Anyone Else's!)

This permission gives admins unlimited configuration ability for all admin permissions, including their own. They can promote any user to an admin and grant access to any part of the system to any user, including themselves.

Because they can change their own permissions, admins with this enabled can gain access to all parts of the system. Rave recommends limiting this permission to a small number of admins who set up access roles.

4.6 SmartLoader Tab Options

When you enable the SmartLoader tab, admins in this role can configure and run bulk uploads of many recipients at once.

On this tab, you can configure permissions for Rave Alert's loading tools. If your organization purchased the SmartLoader tools for integrating Rave Alert with other databases, this section controls admin access to those, too.

The screenshot shows the configuration interface for the 'Example Role'. At the top, there is a header with 'Example Role' and an 'Edit' button. To the right is a 'Role Details' button. Below the header is a row of toggle switches for various features: Alerts (checked), Collaborate (checked), Reports (unchecked), People & Lists (unchecked), System (unchecked), and SmartLoader (checked). Below this row is a section titled 'SmartLoader Permissions' with a collapse icon. This section contains two checked checkboxes: 'Smartloader Users and Lists' and 'Managed Contacts'. At the bottom of the interface are 'SAVE' and 'CANCEL' buttons.

In This Tab – Uploading Many Recipients at Once, (Paid Add-on) Auto-Updating Rave Alert based on Other Database Systems

An admin must have access to the SmartLoader tab to upload batch lists of recipients. They also need access of this tab to configure and run automated upload integrations.

Once you enable this tab, you can set which of the available loading tools admins can access:

- Whether they load and manage ad hoc lists of recipients using Manage Contacts
- Whether they manage automatic uploads of recipient data from other database systems using the SmartLoader tools.

SmartLoader Permissions – Which Loading Tools Admins Can Use to Manage Users

Rave Alert offers Managed Contacts, a manual bulk loading tool, to all domains. Using Managed Contacts, you can load a list of names, phone numbers, and email addresses to create new recipients. You can then manage those accounts through the loading tools.

If your domain purchased the SmartLoader add-on, your admins can also use this section to connect Rave Alert to other databases like ERP or SIS systems.

The SmartLoader tab contains 1 section: **SmartLoader Permissions**. This section controls which loading tools admins can access on this page.

SmartLoader Users/Lists

Who Should Have It? – Admins Who Manage Database Integrations

Admins must have this permission to access SmartLoader integration tools and reports. Give it to admins who need to set up and check the progress of automated people updates.

When Enabled	When Disabled
Admins can access automated User and List upload tools and system reports.	Admins cannot impact Rave Alert’s integration with other databases.

Managed Contacts

Who Should Have It? – Admins who handle ad-hoc lists of recipients

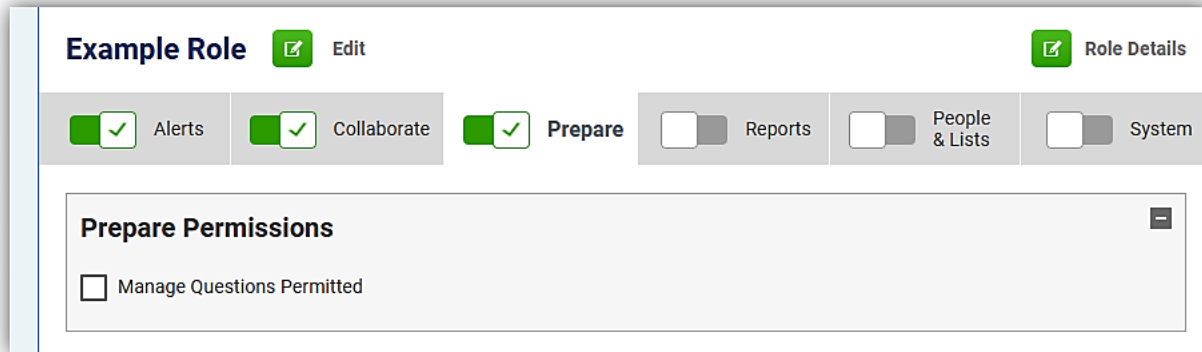
Admins need access to this page to create accounts for recipients using lists of contact information. Give it to admins who add ad-hoc sets of temporary users to the system.

When Enabled	When Disabled
Admins can perform manual, one-time loads of temporary users. They can also view and remove those temporary users.	Admins cannot perform one-time user loads or access the Managed Contact tools. They can still send messages to managed contacts who already exist in the system.

4.7 Rave Prepare Tab Permissions

Rave Prepare is an add-on to Rave Alert for public alerting clients. You will only see this tab if you have purchased Rave Prepare.

When you enable the Rave Prepare Tab, admins can view vulnerability information and messaging tools.



In This Tab – Managing Rave Prepare Questions, Running and Saving Queries

An admin must have access to the Rave Prepare tab to search recipients by vulnerability and send alerts to select groups of vulnerable recipients.

Once you enable this tab, you can set an admin's experience with vulnerability data:

- Whether they can choose which vulnerability questions you ask registrants

Rave Prepare Permissions

– Whether the Admin Can Change the Questions You Ask

The Rave Prepare tab contains 1 section: **Rave Prepare Permissions**. This section controls whether admins in this role can change the vulnerability questions on your site.

Manage Questions

Who Should Have It? – Admins Who Decide What Vulnerabilities to Map

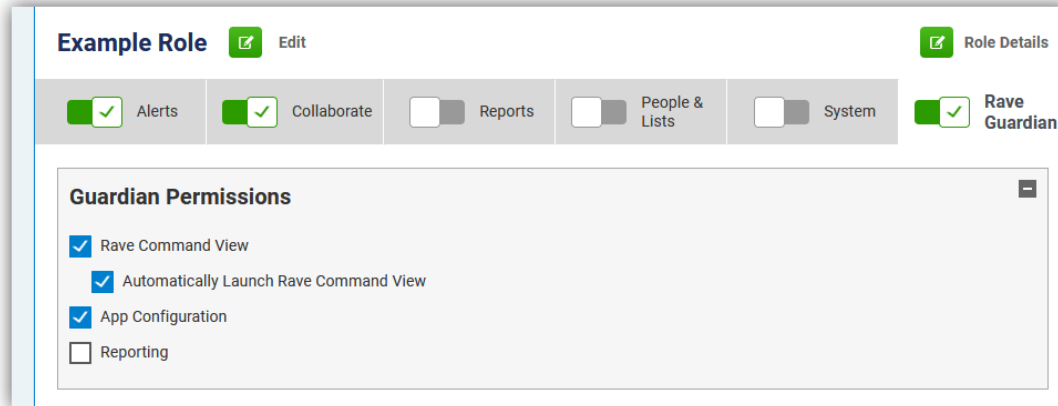
Admins must have this permission to change what information you collect from registrants on your public portal. Once enabled, admins can turn on and off specific questions in areas like dependence on electricity, no access to transportation, or other vulnerabilities.

When Enabled	When Disabled
Admins can edit the Rave Prepare questions your community views and answers.	Admins can only view data for existing questions.

4.8 Rave Guardian Tab Options

Rave Guardian™ is a mobile safety companion app to Rave Alert. You will only see this tab if your organization purchases Rave Guardian to provide your community with Safety Timers, emergency call capabilities, text tips, and app-push messages from Rave Alert.

When you enable the Rave Guardian tab, admins in this role can access Rave Command View, the console used to monitor the app, app configuration tools, and reporting.



In This Tab – Monitoring Real-Time App Activity, Setting Up App Tools, Reports

An admin must have access to the Rave Guardian tab to monitor app activity, change app settings, or view reports of historical app usage.

Once you enable this tab, you can set an admin's experience with the app:

- Whether they see any configuration tools, or automatically open to the monitoring console
- Whether they can open historical reporting
- Whether they can change the app appearance and function for different sites in your organization

On this tab, you can configure permissions for accessing Rave Command View to view app activity, customizing Guardian configurations, and viewing reports on app activity.

The Rave Guardian contains 4 sections.

- 1. Guardian Permissions**

Monitoring app activity, accessing configurations, and viewing reports

- 2. Assigned Chat Categories**

Restrictions for admins to only view and reply to specific Chat categories

- 3. Assigned Timers**

Restrictions for admins to only see Timers from specific sites

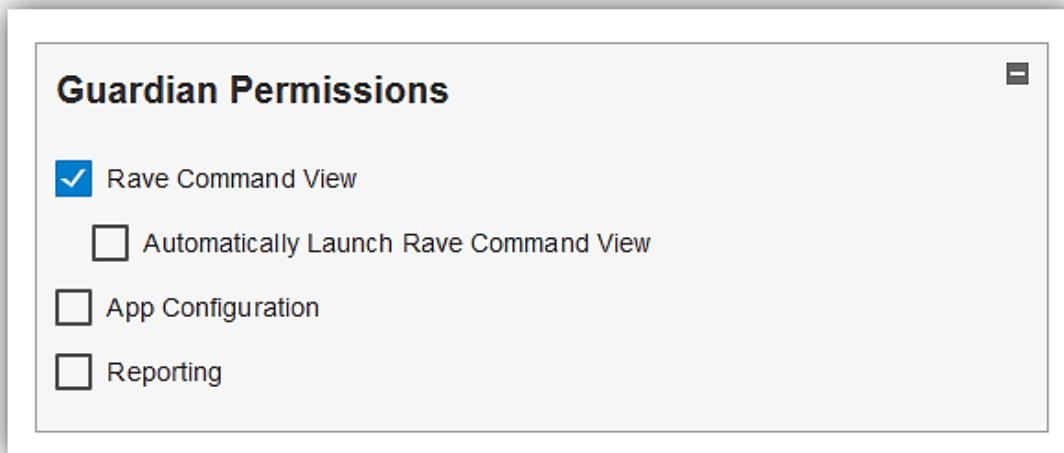
- 4. Assigned Call Categories**

Restrictions for admins to only see Call Directory calls in specific categories

Guardian Permissions – Which App Tools Admins Can Access

Admins in Rave Alert can interact with Rave Guardian in different ways. Some of your admins should monitor app usage and respond to incidents. Others need to set up how the app looks and behaves.

This section controls which app tools an admin can access, from the RCV monitoring console to changing app buttons and behavior.



Guardian Permissions

- Rave Command View
 - Automatically Launch Rave Command View
- App Configuration
- Reporting

Rave Command View

Who Should Have It? – Admins Who Monitor Realtime App Activity

Admins must have access to Rave Command View to view ongoing app activity, including incoming tips, expired Safety Timers, and emergency calls.

Through RCV, admins can see activity on a map and respond to individual incidents.

When Enabled	When Disabled
Admins can open the map-based console that displays Rave Guardian activity.	Admins cannot open RCV and do not see the RCV tab.

Automatically Launch Rave Command View

Who Should Have It? – Admins Who Should Only See Live App Activity

Admins must have access to Rave Command View to have this setting.

When enabled, admins see the map interface with ongoing app incidents as soon as they log in to Rave Alert. They don't have to interact with the navigation bar or see configuration tools.

When Enabled	When Disabled
Admins see RCV automatically when they log in.	Admins see a Rave Guardian configuration console when they log in. If they have access to it, they can navigate to the Rave Command View page.

App Configuration

Who Should Have It? – Admins Who Set Up App Behavior for One or More Sites

Admins must have access to the App Configuration settings to affect Rave Guardian's appearance and behavior for your domain.

When enabled, admins can add or remove app features, change button labels and appearance, configure categories, and set Timer functions. Admins can also save sets of app settings into Sites, offering your app users different tools at different buildings.

When Enabled	When Disabled
Admins can access global and site-specific configuration tools for the Rave Guardian app.	Admins cannot access global or site-specific configuration tools for the Rave Guardian app.

Reporting

Who Should Have It? – Admins Who Review Past App Activity

Admins must have access to Reports to view app activity in the past.

When enabled, admins can generate reports of activity by tool, activity by site, user registration over time, and more.

When Enabled	When Disabled
Admins can view historical app information and generate reports.	Admins cannot view historical app information.

Assigned Chat Categories – Which Text Tip Categories Admins Can Access

By default, admins with access to the Chat tool can view and respond to all active Chats in all Chat categories.

In this section, you can limit admins to only seeing and responding to Chats in specific categories.

Who Should Have Them? – Admins who should only handle specific conversations

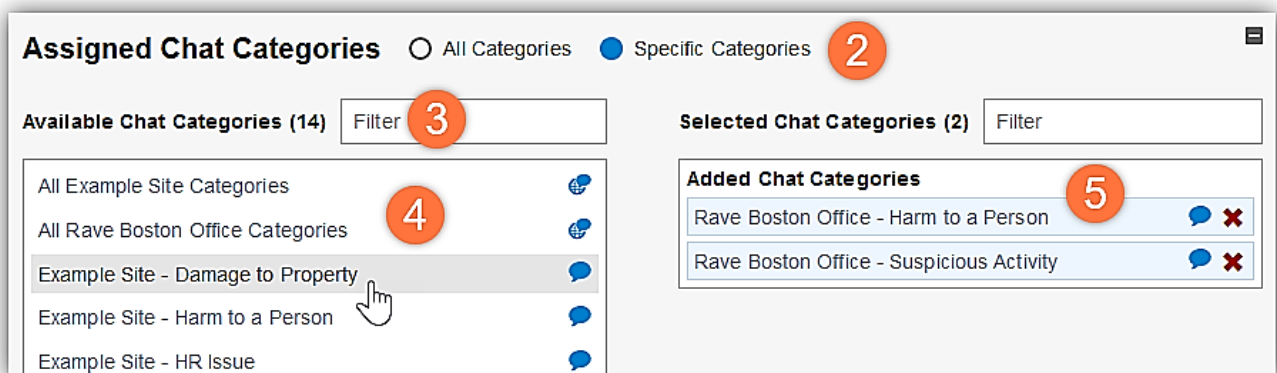
Admins must have access to RCV to view Chat categories. Assigning specific Chat categories lets you limit which message types admins see in RCV.

For example, you can restrict messages about harassment to admins with appropriate training, while directing messages about vandalism or maintenance concerns to someone else.

This setting controls which Chat messages display in RCV

To restrict admins in this role to only responding to specific Chat Categories:

1. Enable the Rave Command View option under Guardian Permissions .
2. Select the Specific Categories radio button in the Assigned Chat Categories section. A list of all chat categories opens in the Available Chat Categories box.
3. Use the filter bar or scroll bar to find the specific Chat Categories in the Available Categories box.
4. Select a category to move it to the Selected Chat Categories box.
5. In needed, select a list in the Selected Chat Categories box to remove it.



Assigned Chat Categories All Categories Specific Categories **2**

Available Chat Categories (14) Filter **3**

- All Example Site Categories
- All Rave Boston Office Categories
- Example Site - Damage to Property** **4**
- Example Site - Harm to a Person
- Example Site - HR Issue

Selected Chat Categories (2) Filter

Added Chat Categories **5**

- Rave Boston Office - Harm to a Person
- Rave Boston Office - Suspicious Activity

Assigned Timers – Which Locations Admins Can View Timers For

By default, admins with access to the Timer tool can view and respond to all active Timers for all sites.

In this section, you can limit admins to only seeing and responding to Timers for a specific site.

Who Should Have Them? –

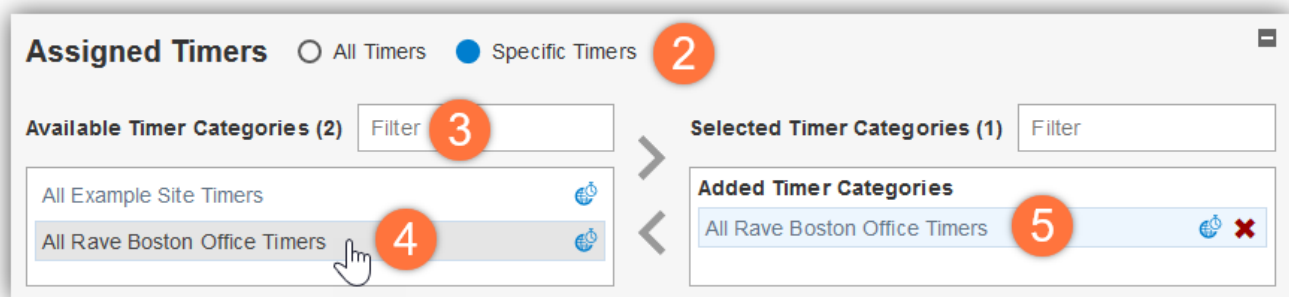
Admins who only monitor app activity for a specific location

Admins must have access to RCV to view Timer sessions. Assigning specific Timer sites lets you limit what area an admin sees Timers for.

For example, you can restrict messages about harassment to admins with appropriate training, while

To restrict admins in this role to only viewing and responding to Timers from specific sites:

1. Enable the Rave Command View option under Guardian Permissions.
2. Select the Specific Timer Categories radio button. A list of all sites for your domain appears in the Available Categories box.
3. Find the specific sites where you want admins in this role to be able to access Timers. If needed, use the search bar to filter the available sites.
4. Select a Site to move it to the Assigned Timers box.
5. In necessary, select a Site in the Assigned Timer box to remove it from admins in this role.



Assigned Call Categories – Which Call Directory Calls Admins Can Receive

By default, admins who can view Call Directory dials in RCV can see and respond to calls in all categories.

In this section, you can limit admins to only seeing and responding to specific call categories. Admins only see their assigned call categories in RCV.

Who Should Have Them? – Admins who should only respond to specific calls

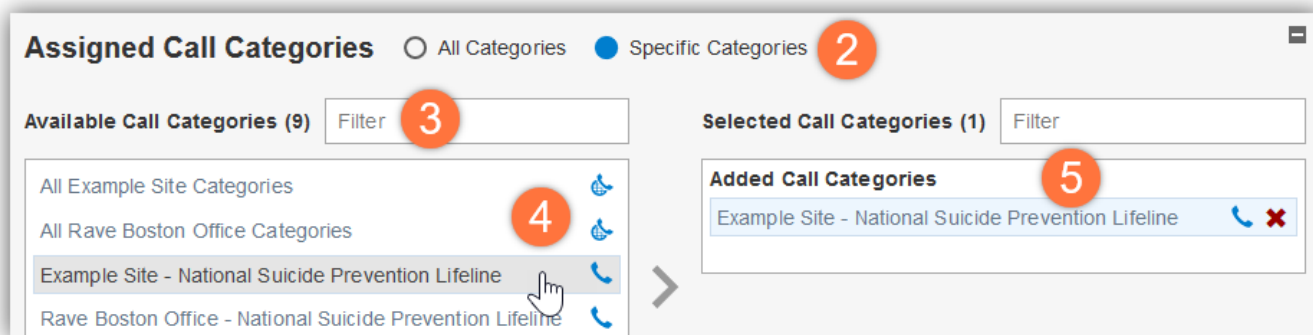
Admins must have access to RCV to view Call Directory categories. Assigning specific Chat categories lets you limit which message types admins see in RCV.

For example, you can restrict messages about harassment to admins with appropriate training, while

This setting controls which call notifications display in RCV

To restrict admins in this role to only responding to specific Call Directory calls:

1. Enable the Rave Command View option.
2. Select the Specific Call Categories radio button in the Assigned Call Categories section. A list of all recipient lists for your domain appears in the Available Categories box
3. Use the filter bar or scroll bar to find the specific Call Categories in the Available Categories box.
4. Select a category to move it to the Selected Call Categories box.
5. In needed, select a list in the Selected Chat Categories box to remove it.



5. Assigning a Role to An Admin

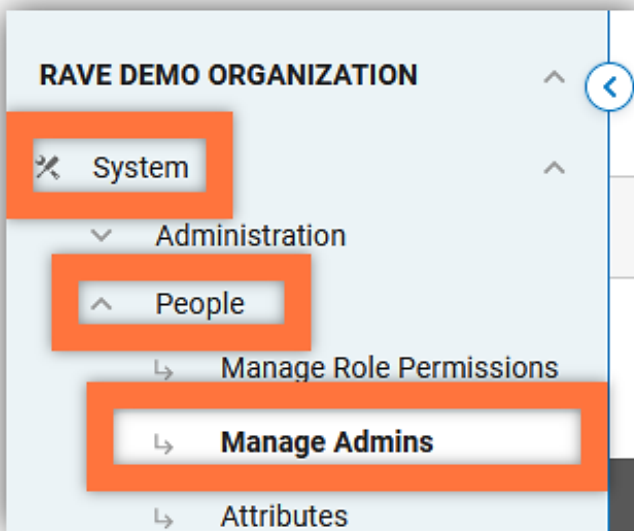
Every admin in Rave Alert must have a role. You can assign admin roles in two ways.

5.1 Assign Using the Promote to Admin Button

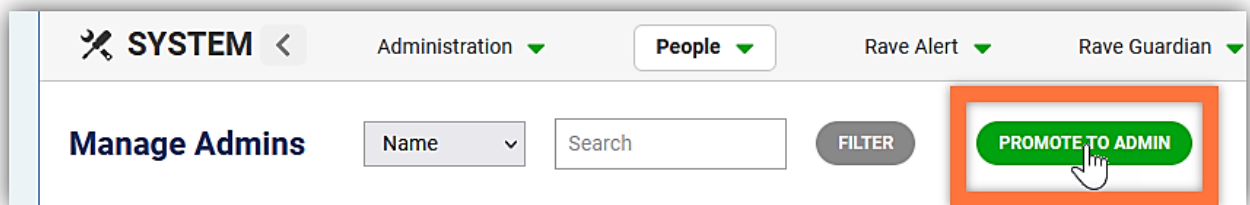
You can change an admin’s role through the Manage Admins page. Use this method if you want to promote an ordinary user to Admin status.

To change a user’s role through the admin editor:

1. Open the Open the System tab, Manage Admins Page.

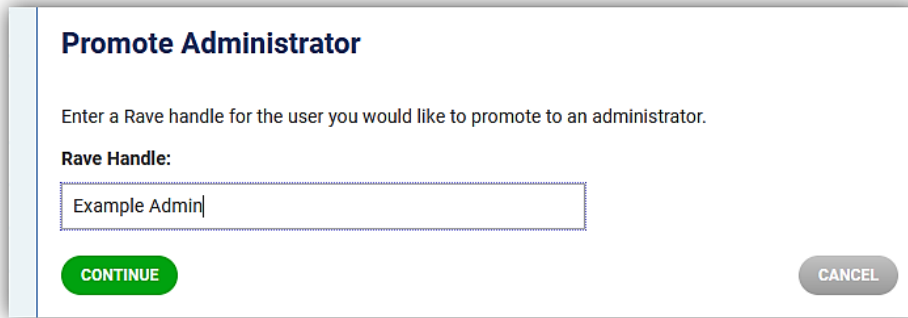


2. Click the Promote to Admin button.

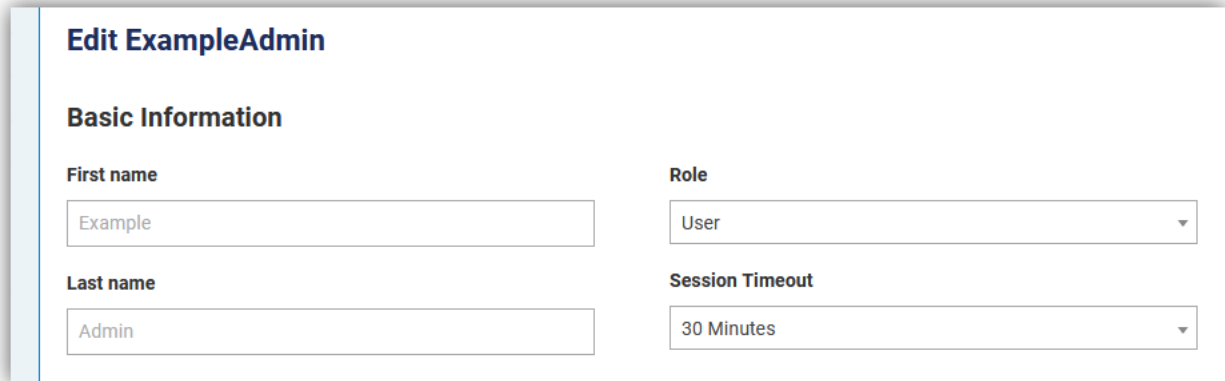


The Promote Administrator page opens.

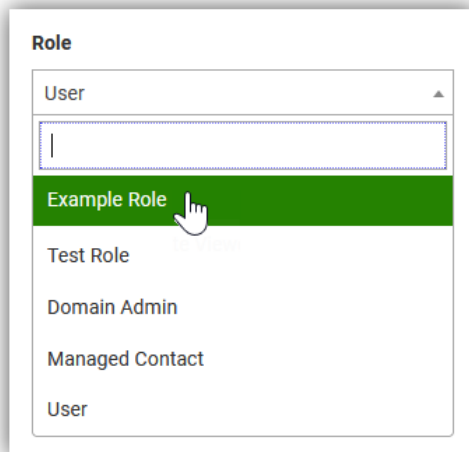
3. Enter the user's Rave Handle in the **Rave Handle:** field and click **Continue**.



The Edit Administrator page opens.



4. Select an administrative role from the **Role:** dropdown menu.



Changing an Admin's Role Can Remove Their Override Permissions

You can augment an admin's role-based permissions by adding override permissions to their record.

If you change an admin's role, it changes which tools they can access. If they lose access to a tool where they had override permissions, they will lose those override permissions.

You can add override permissions to any admin. For more information, see [Chapter 6](#).

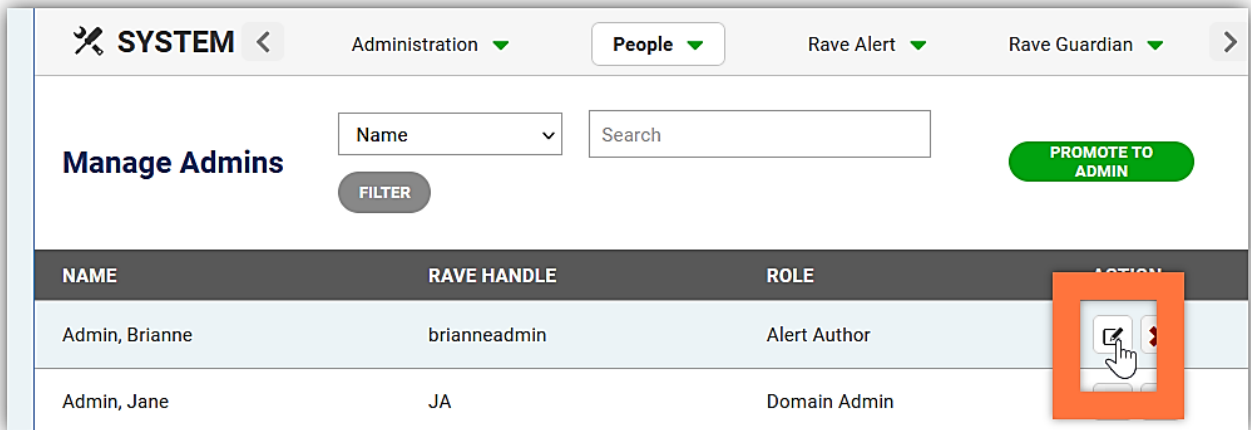
5. Select the Save Button.

5.2 Assign Through the Edit Button

You can change an admin's role directly from their record. When you change an admin's role, they have the access permissions from the new role next time they log in.

Use this method when you want to change an existing admin's access level.

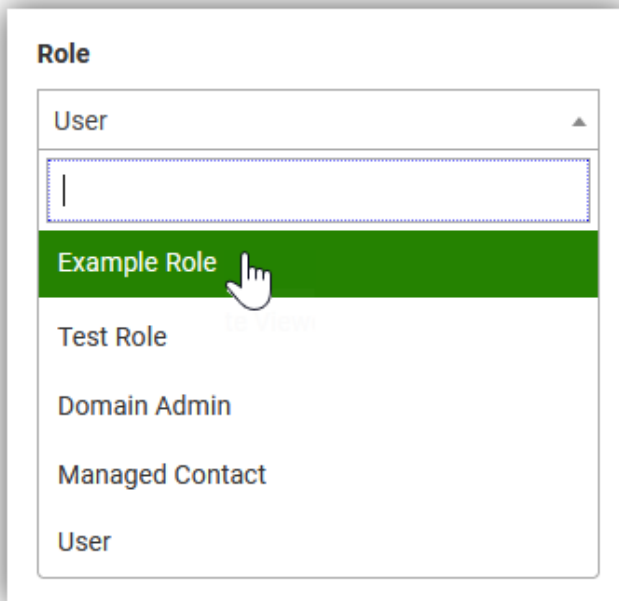
1. Open the Open the System tab, Manage Admins Page.
2. Select the **Edit** button by a user's record.



The Edit page opens.

The screenshot shows the 'Edit ExampleAdmin' page. The title is 'Edit ExampleAdmin'. Under the heading 'Basic Information', there are four fields: 'First name' with the value 'Example', 'Last name' with the value 'Admin', 'Role' with a dropdown menu showing 'User', and 'Session Timeout' with a dropdown menu showing '30 Minutes'.

3. Scroll to the **Role:** field and select an administrative role from the dropdown menu.



4. Click the Save button at the bottom of the page.



Changing an Admin's Role Can Remove Their Override Permissions

You can augment an admin's role-based permissions by adding override permissions to their record.

If you change an admin's role, it changes which tools they can access. If they lose access to a tool where they had override permissions, they will lose those override permissions.

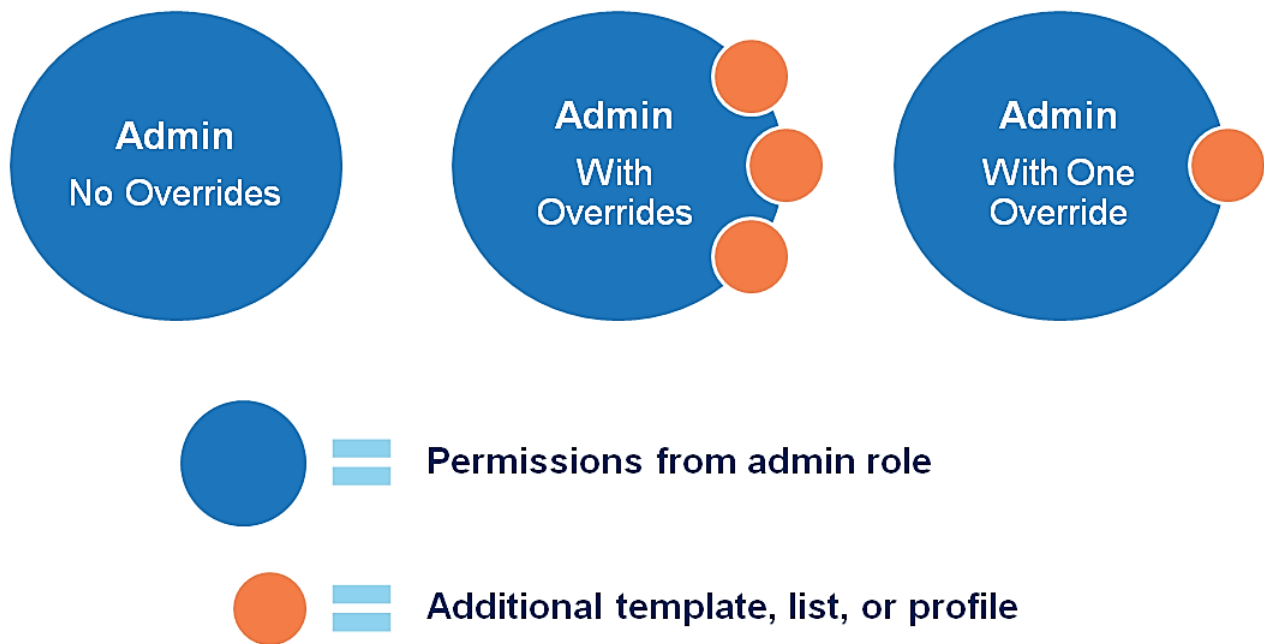
You can add override permissions to any admin. For more information, see [Chapter 6](#)

6. Additional Permissions for Individual Admins

All admins receive permissions from their roles. Admins with the same role have matching permissions.

If you want, you can give individual admins permissions beyond those from their role. These override permissions only affect one admin.

Different admins with the same role can have different override permissions.



Once an admin has override permissions, a special mark displays next to their role to show they have individual access settings.

NAME	RAVE HANDLE	ROLE	ACTION
Police, University	UPPD	Safety Official	
Admin, Jane	JA	Domain Admin	

6.1 Override Permission Rules

These rules dictate how override permissions interact with role permissions.

Rule #1

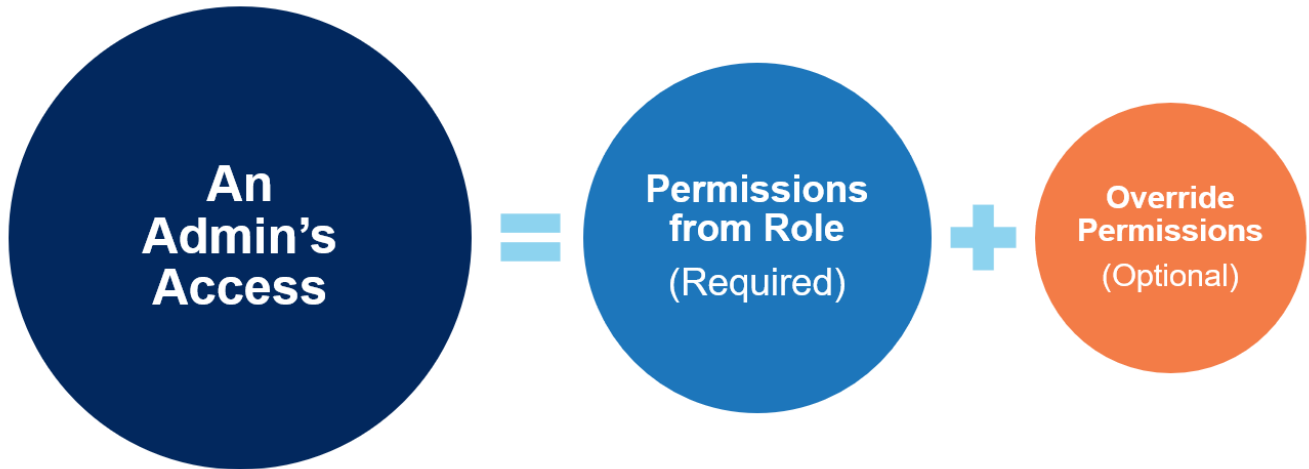
An admin cannot have fewer permissions than those assigned to their admin role. Override permissions can only add to role permissions.

Rule #2

If you add a permission in both places, it reverts to a role permission.

For example, say an admin has an override permission. You later add that permission to their role. In this case, the permission becomes a role permission. You cannot edit it as an override on the admin's record anymore because of Rule #1.

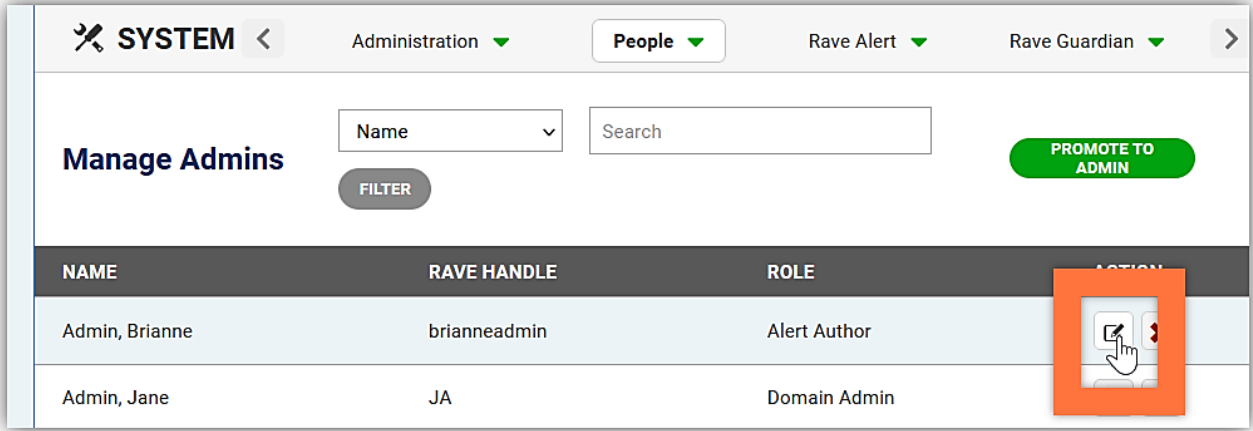
Override permissions and role permissions together allow you to create flexible access that meets each admin's specific needs.



6.2 Add Override Permissions to an Admin

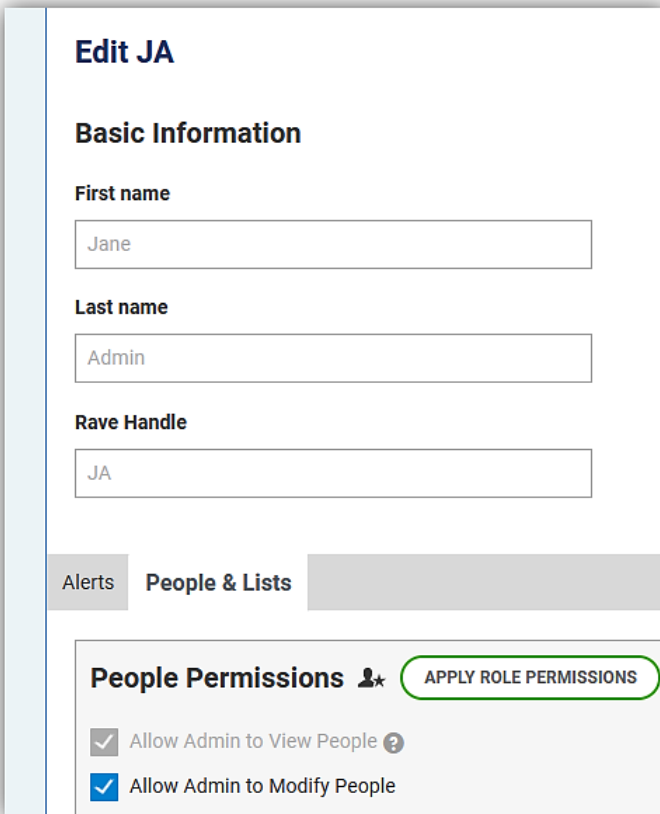
To add override permissions to an individual administrator:

1. Open the Open the System tab, Manage Admins Page.
2. Click the edit button by an admin's record.



The Edit page opens.

3. Scroll down to the permissions tabs. This section shows tabs the admin has access to because of their admin role.



You Won't See All Tabs Here

This section only shows tabs when the admin has access to from their role and the tab supports overrides.

Some tabs do not support overrides. To change an admin's access for the Reporting, System, Rave Prepare, or SmartLoader tabs, change the admin's role.

4. Open a tab to adjust the permissions. You can enable checkboxes for tool access options or add individual alert templates, delivery lists, and other specific objects.

Alerts | People & Lists

Alerts Permissions

- User Can Create/Edit/Delete Templates
- Assign Templates to Other Admins
 - Admins in assigned Lists
 - All Admins
- Copy on all Broadcast Alerts

Assigned Templates

All Templates Specific Templates

Available Templates (9)

Filter

- Attachments Example
- HTML Email Alert
- Monroe EAS

Selected Templates (0)

Filter

Added Templates

No Templates selected

The Two Rules of Override Permissions

Rule #1

An admin cannot have fewer permissions than those assigned to their admin role. Override permissions can only add to role permissions.

Rule #2

If you add a permission in both places, it reverts to a role permission.

For example, say an admin has an override permission. You later add that permission to their role. In this case, the permission becomes a role permission. You cannot edit it as an override on the admin's record anymore because of Rule #1.

5. Select the **Save** button at the bottom of the page.

SAVE

RAVE
MOBILE SAFETY

Do all you can today.™

6.3 Notify an Individual Admin of Every Alert

An individual admin can receive an email every time anyone sends an alert.

Copy on All Broadcast Alerts Checkbox



Who Should Have It? – Admins who need to know about every alert

Admins with this permission receive a summary email every time anyone sends an alert on your domain. The email includes important information like what the message said, who sent it, who received it, and when it launched.

When Enabled	When Disabled
<p>This admin receives an email notifying them of all alerts sent from this domain.</p> <p>Emails go to the admin's primary email address and include alert content and recipients.</p>	<p>Admins do not receive emails notifying them of sent alerts.</p>

Alerts Permissions

APPLY ROLE PERMISSIONS

- User Can Create/Edit/Delete Templates 
- Assign Templates to Other Admins
 - Admins in assigned Lists
 - All Admins
- Copy on all Broadcast Alerts 

7. Managing Access from Specific Alert Templates

You can quickly change which admins have access to specific alert templates right from the alerts tab.

Use these Tools Once You Have Roles and Admin Accounts Set Up

You can't create new admins or roles from this screen. Make sure the people you want already have admin accounts, and any relevant roles already exist before trying to add to them here.

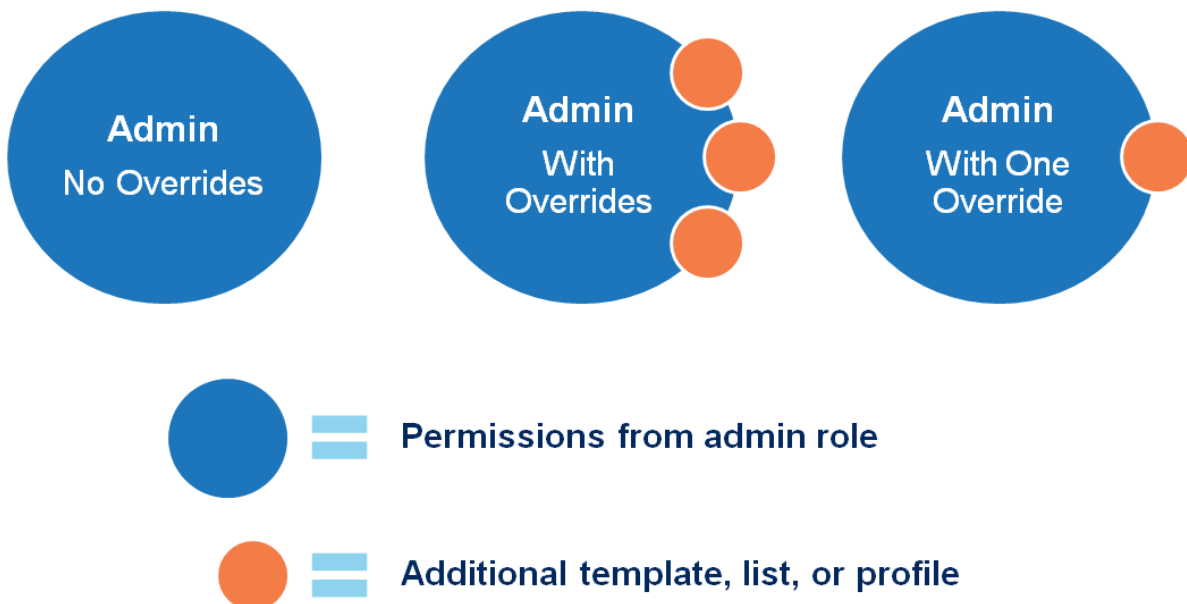
From the alerts tab, you can:

1. View who has access to the alert template right now
 - a. As part of their admin role
 - b. As part of their override permissions
2. Change who has access to the alert template
 - a. For all admins in a specific role
 - b. For individual admins

7.1 View Which Admins Have Access to an Alert Template

Admins can have access to an alert template in two ways

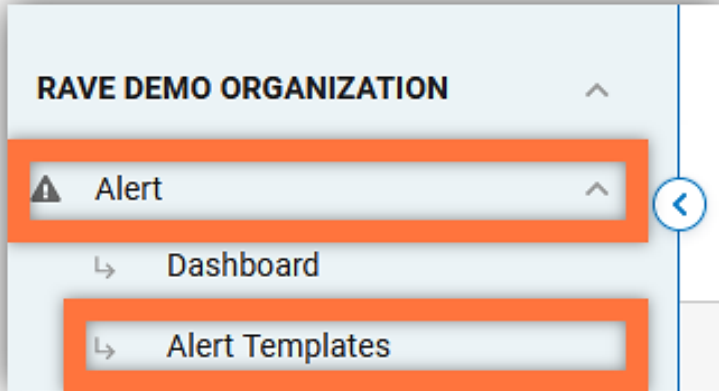
1. Their admin role contains access to the alert template, so all admins in the role have access to this template.
2. Their override permissions contain this alert template, so they individually have access to this template



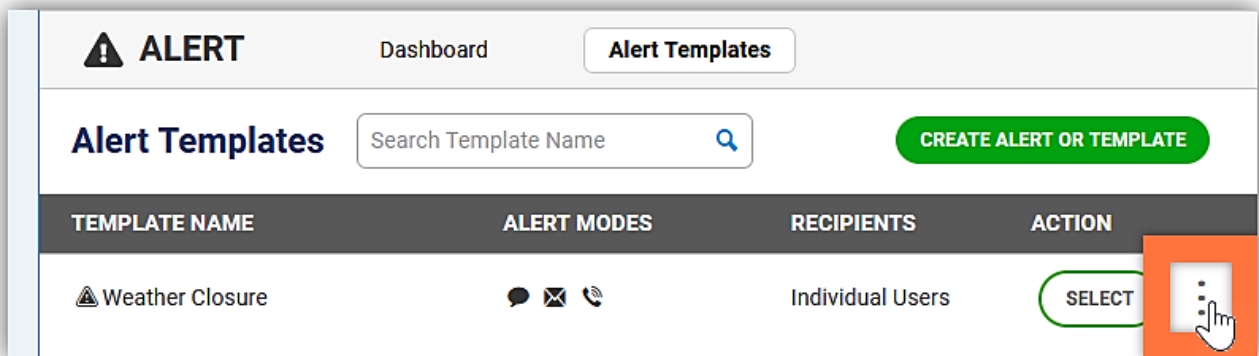
You can see admins in both these categories in the Permissions Window.

To find out who has access to an alert template:

1. Open the Alerts section of the platform menu.
2. Select the Alert Templates page.

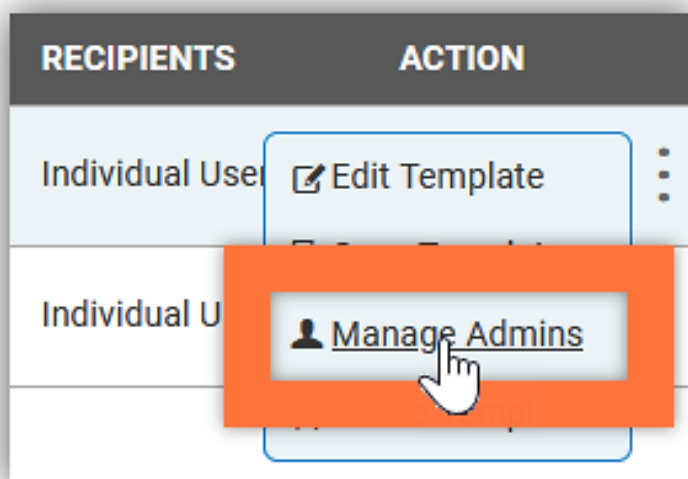


3. Select the three-dot menu icon to the right of the alert template you'd like to assign.



The template action dropdown menu opens.

4. Select the Manage Admins option.



The Alert Permissions Window Opens.

5. Open the Roles tab.

This tab shows all the admin roles with access to this alert template.

6. Click a role to see admins who have access through it.

Role name	Users
▲ Department 1 Admin	1
▼ Admin, Jane	
▼ Emergency Alert Author	2
Safety Official	4

Use the Show Roles with Access to All Templates button to view roles you can't edit here

Some admin roles have access to all templates, regardless of how individual template change. You can't edit those roles' access to an individual template from this page.

To see these roles and admins even though you can't edit them here, click the Show Roles with Access to All Templates toggle. This shows a full list of all roles with access regardless of how broad their access is.

7. Open the People tab.

This page displays individual admins who have access to this alert template. Use this page to find out which admins have override permissions containing this alert template.

8. Click on an admin row to expand their information, including contact points and attributes.

✕
Permissions for Weather Closure

ROLES
ADMINS

Current Assignments

 Show Admins Included in Roles

Name	Email(s)	Phone(s)	Role
▲ Admin, Example date: Department: Lookthisisademo: Language: English	Example@example.com eadmin@example.com		Alert Author
▲ Admin, Jane	jadmin@example.com		Domain Admin
▲ Demo, Sam	samdemo@example.com		Help Desk
▲ Officer, Safety	safety@example.com		Safety Officer

EDIT
DONE

Use the Show Admins Included in Roles button to view roles you can't edit here

Some admin roles have access to all templates, regardless of how individual template change. You can't edit those roles' access to an individual template from this page.

To see these roles and admins even though you can't edit them here, click the Show Roles with Access to All Templates toggle. This shows a full list of all roles with access regardless of how broad their access is.

The Permissions Window shows admins who have access to this alert template.

If you only have permission to edit specific admins, you will only see admins you have access to in this page.

7.2 Change Who Has Access to an Alert Template

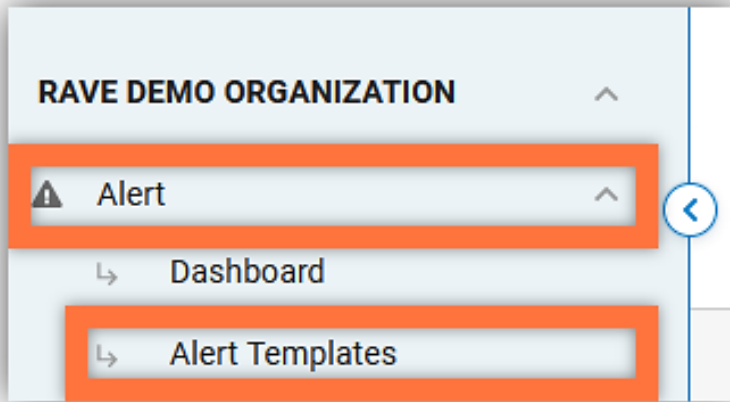
You can add or remove a template from admin permissions directly from the Permissions Window.

This tool can affect admin roles or individual admins, depending on what you need:

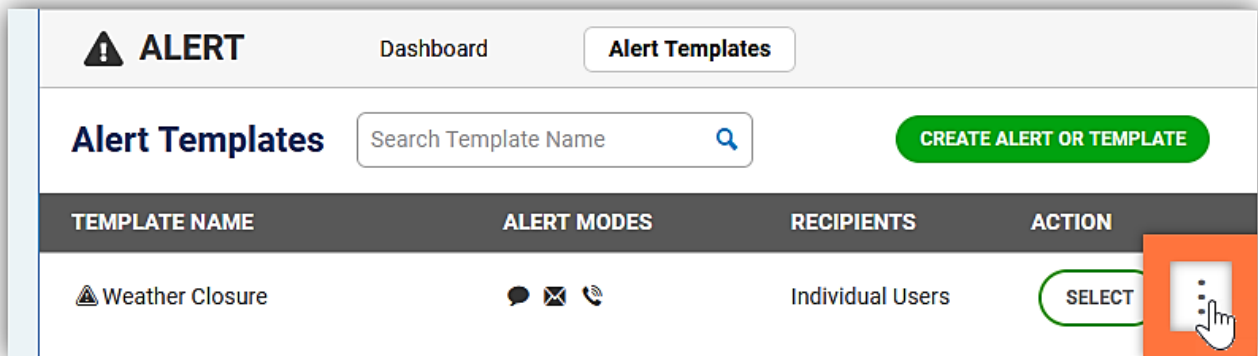
1. Change **admin roles** if you want to add this alert template to multiple admins at once, and to automatically include it for future admins when you assign them affected roles
2. Change **individual admin permissions** if you want to add this alert template to specific people right now, and not affect multiple admins at once or admins in the future.

7.2.1 Change Alert Template Permissions for Admin Roles

1. Open the Alerts section of the platform menu.
2. Select the Alert Templates page.

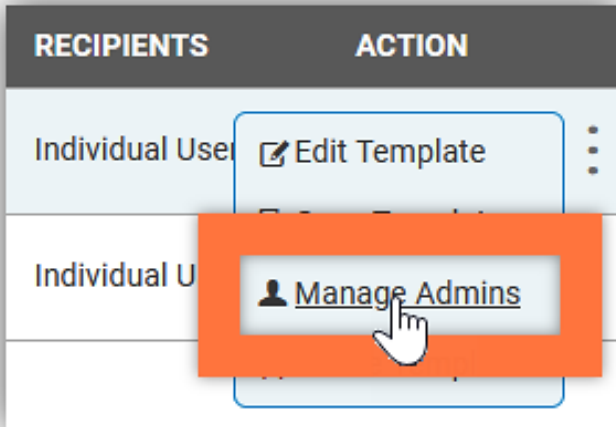


3. Select the three-dot menu icon to the right of the alert template you'd like to assign.

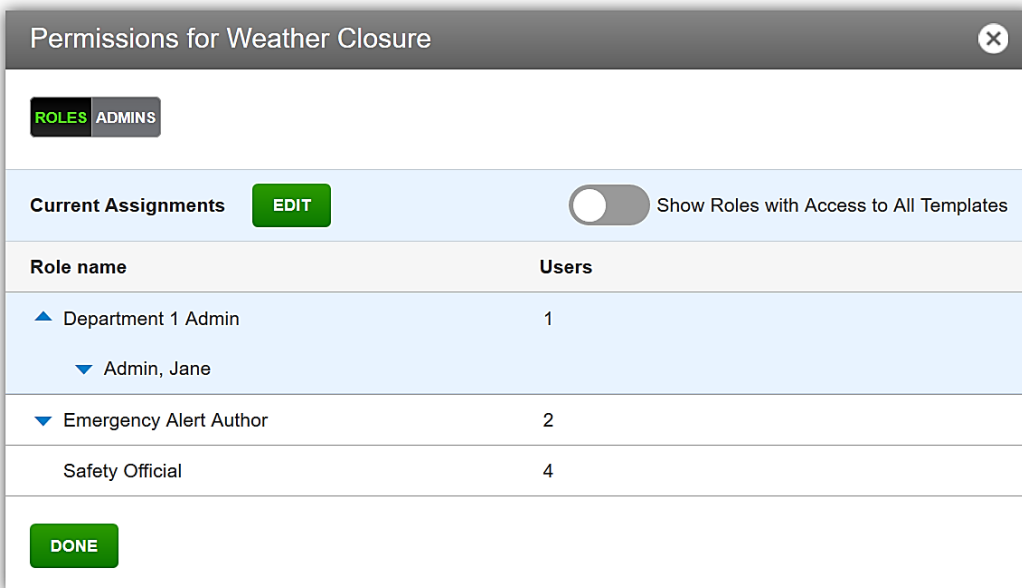


The template action dropdown menu opens.

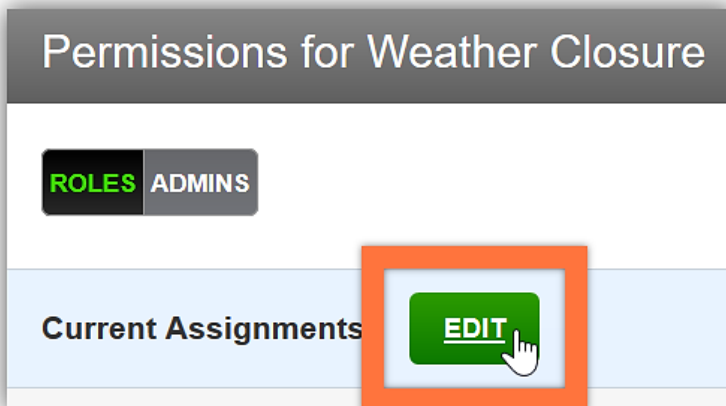
4. Select the Manage Admins option.



5. The Alert Permissions Window Opens.
6. Open the roles tab. The window displays a list of the roles with access to this template.

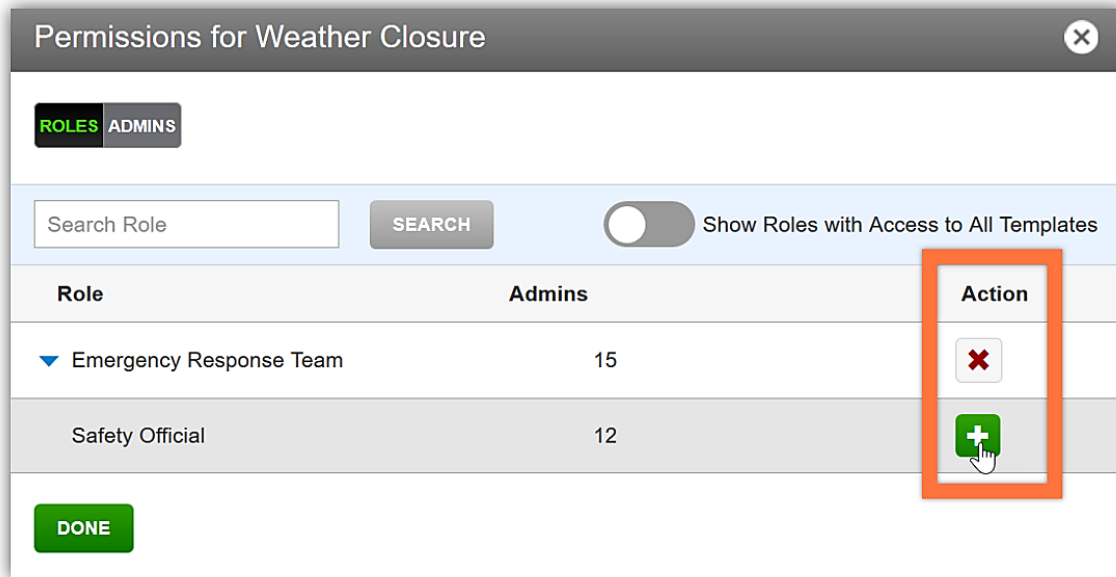


7. Select the Edit button in the Current Assignments bar.



The window displays a list of all roles in your system who could have access to this alert template.

8. Use the search bar to locate roles as needed.
9. Click the plus button to add the alert template to a role. All admins assigned this role will gain access to this alert template.

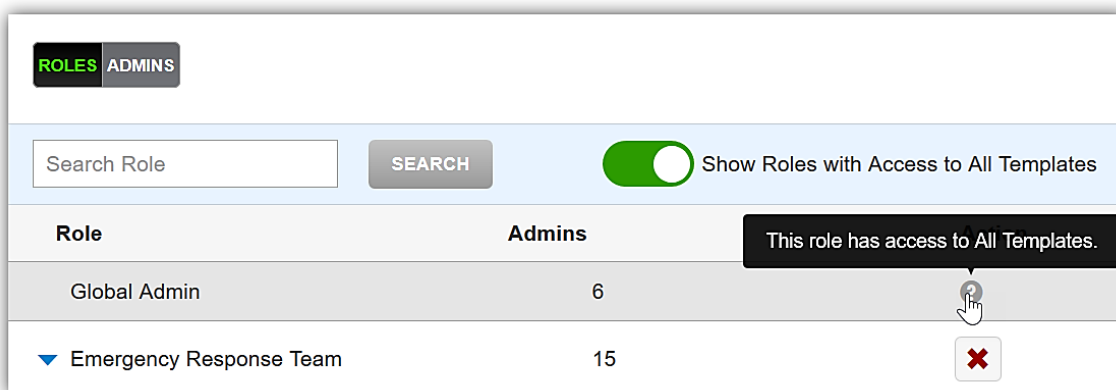


Use the Show Roles with Access to All Templates button to view roles you can't edit here

Some admin roles have access to all templates, regardless of how individual template change. You can't edit those roles' access to an individual template from this page.

To see these roles and admins, click the Show Roles with Access to All Templates toggle. This shows a full list of all roles with access regardless of how broad their access is.

Roles you can't edit here show a question mark in the Action column instead of a plus or x.

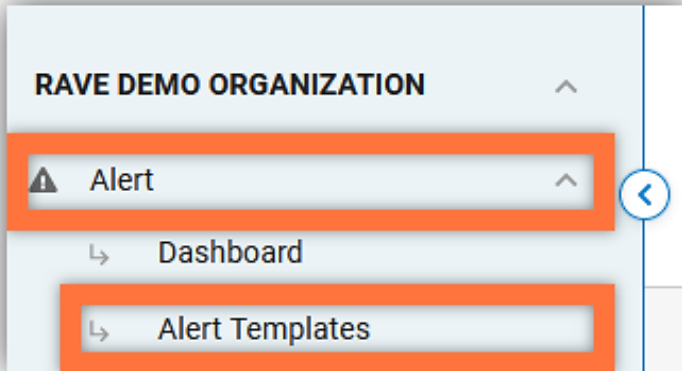


10. Click the X button to remove the template from a role. All admins in the role will lose access to the alert template.
11. Repeat steps 5-7 for any additional roles.
12. Select the Done button.

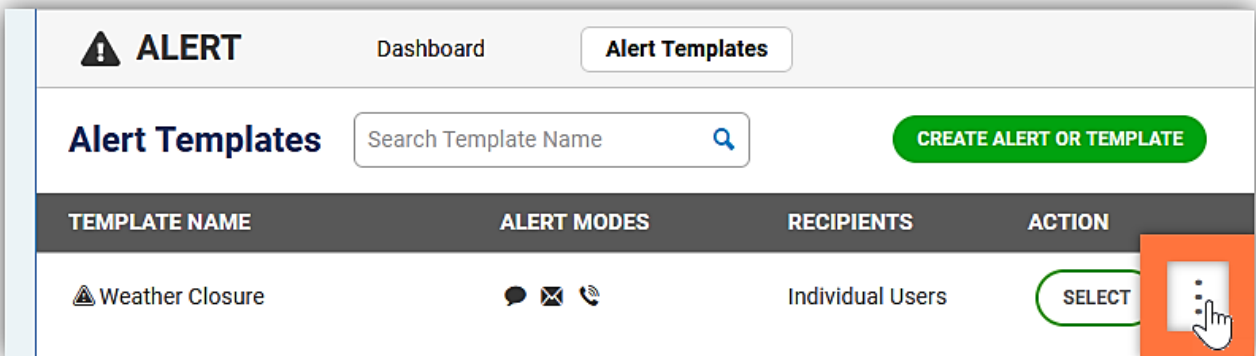
Rave Alert displays a success bar to confirm your changes.

7.2.2 Change Alert Template Permissions for Individual Admins

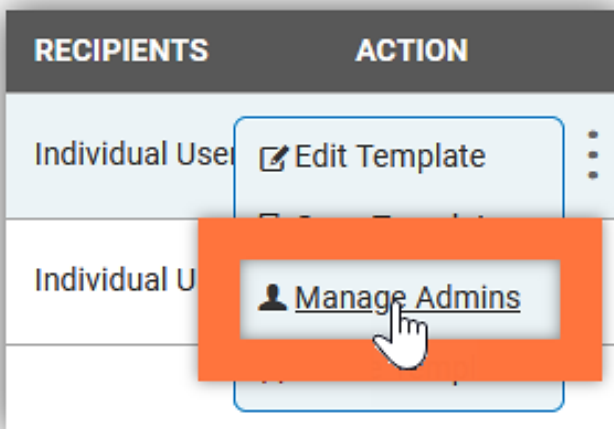
1. Open the Alerts section of the platform menu.
2. Select the Alert Templates page.



3. Select the three-dot menu icon to the right of the alert template you'd like to assign.

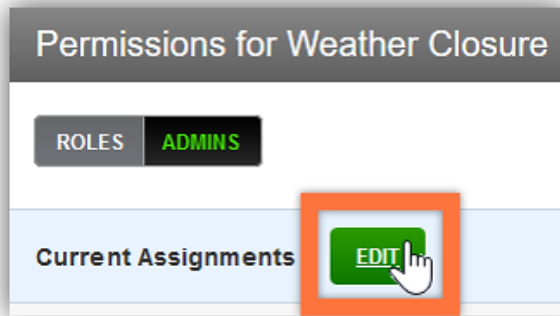


4. Select the Admins button next to an alert template.



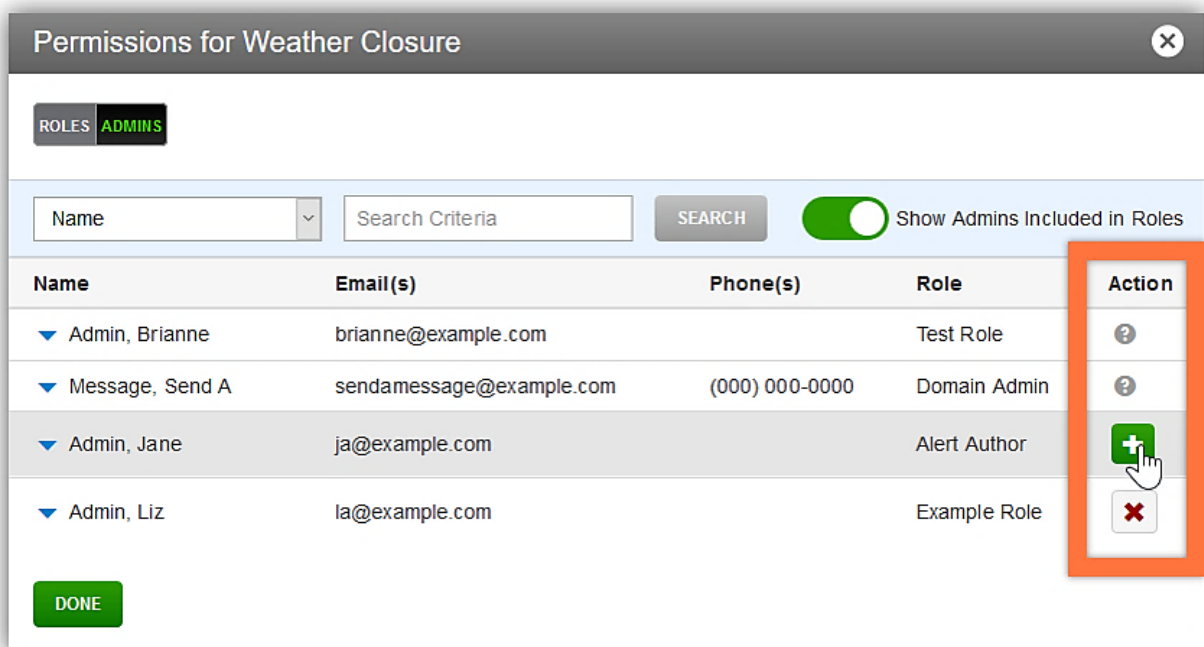
The Alert Permissions Window Opens.

5. Open the admins tab. The window displays a list of the individual admins with access to this template.
6. Click the Edit button in the current assignments section.



The window displays a list of all admins in your system who could have access to this alert template.

7. Use the search bar to locate roles as needed.
8. Click the plus button to add the alert template to an admin. Only this specific admin will gain access to this template.



Use the Show Admins Included in Roles button to view roles you can't edit from this tab

Some admins have access to specific alert templates through their roles. You can't edit those admins' access to this template from the admins page. Open the roles tab to edit the role permissions for the template.

To see these admins, click the Show Admins Included in Roles toggle. This shows a full list of all admins with access regardless of where their access comes from.

Admins you can't edit here show a question mark in the Action column instead of a plus or x.

9. Click the minus button to remove this alert template from an admin's override permissions. Only this specific admin will lose access to this template.
10. Repeat steps 5-7 for any additional admins.

11. Select the Done button. Rave Alert displays a success bar to confirm your changes.