



Custom Roles Guide

Everbridge Suite
September 2024

Everbridge Suite**2024****Printed in the USA**

Copyright © 2024. Everbridge, Inc, Confidential & Proprietary. All rights are reserved. All Everbridge products, as well as NC4, xMatters, Techwan, Previstar, one2many, SnapComms, Nixle, RedSky, and Connexient, are trademarks of Everbridge, Inc. in the USA and other countries. All other product or company names mentioned are the property of their respective owners. No part of this publication may be reproduced, transcribed, or transmitted, in any form or by any means, and may not be translated into any language without the express written permission of Everbridge.

Limit of Liability/Disclaimer of Warranty: Everbridge makes no representations or warranties of any kind with respect to this manual and the contents hereof and specifically disclaims any warranties, either expressed or implied, including merchantability or fitness for any particular purpose. In no event shall Everbridge or its subsidiaries be held liable for errors contained herein or any damages whatsoever in connection with or arising from the use of the product, the accompanying manual, or any related materials. Further, Everbridge reserves the right to change both this publication and the software programs to which it relates and to make changes from time to time to the content hereof with no obligation to notify any person or organization of such revisions or changes.

This document and all Everbridge technical publications and computer programs contain the proprietary confidential information of Everbridge and their possession and use are subject to the confidentiality and other restrictions set forth in the license agreement entered into between Everbridge and its licensees. No title or ownership of Everbridge software is transferred, and any use of the product and its related materials beyond the terms on the applicable license, without the express written authorization of Everbridge, is prohibited.

If you are not an Everbridge licensee and the intended recipient of this document, return to Everbridge, Inc., 155 N. Lake Avenue, Pasadena, CA 91101.

Export Restrictions: The recipient agrees to comply in all respects with any governmental laws, orders, other restrictions (“Export Restrictions”) on the export or re-export of the software or related documentation imposed by the government of the United States and the country in which the authorized unit is located. The recipient shall not commit any act of omission that will result in a breach of any such export restrictions.

Everbridge, Inc.

155 N. Lake Avenue, 9th Floor

Pasadena, California 91101 USA

Toll-Free (USA/Canada) +1.888.366.4911

Visit us at www.everbridge.com

Everbridge software is covered by US Patent Nos. 6,937,147; 7,148,795; 7,567,262; 7,623,027; 7,664,233; 7,895,263; 8,068,020; 8,149,995; 8,175,224; 8,280,012; 8,417,553; 8,660,240; 8,880,583; 9,391,855. Other patents pending.

Introduction.....	4
Use Cases.....	5
Roles and Permissions Scope.....	6
Configurable Permissions Areas	6
Not Within Custom Roles Scope	7
Custom Role Usage Overview	8
Creating a Custom Role	8
Validation Rules.....	15
Permission Dependency (Checking).....	15
Permission Dependency (Unchecking).....	15
Resource Impact	16
Core Permission	17
Custom Role Considerations.....	19
Interim Behavior - Configurable to Fixed Check	19
Example.....	19
Known Exceptions	20
ManageBridge	20
Custom Roles REST API.....	21
REST API Response – Role APIs	21
REST API Response – User APIs.....	23
Support Resources.....	24

Introduction

The **Custom Roles** feature allows administrators to fully configure existing feature-level permissions by using a base template from existing roles, where they can add or remove individual permissions consistent with their Organization's needs.

Use Cases

Some common use cases for expanding privileges include:

- As an Administrator, I want to create an Incident Operator to have the ability to create an Incident template.
- As an Administrator, I want to create an Incident Operator to have the ability to manage Contacts.
- As an Administrator, I want Incident Operators to have access to Universe to draw shapes and see how many Contacts are impacted.
- As an Administrator, I want to create a Dispatcher to have the ability to access Incident Communication features.
- As an Administrator, I want to create a Dispatcher to have the ability to manage Contacts.
- As an Administrator, I want a Dispatcher to be authorized to view Notification templates created by Organization Administrator roles.
- As an Administrator, I want a Dispatcher to be authorized to view Contact and group information while not able to change them.
- As an Administrator, I want to have a Group Manager role that can access Incident Communication features.

Sometimes Administrators will be interested in creating a Custom Role to restrict access to specific areas, such as:

- Creating an Incident Administrator role with the *Edit Contacts* permission disabled.
- Creating a Dispatcher role without access to Universe.

Roles and Permissions Scope

Custom Roles can be created from any of the following Role Templates:

1. Incident Operator
2. Incident Administrator
3. Group Manager
4. Dispatcher
5. Data Manager

Configurable Permissions Areas

Certain areas within Everbridge Suite have configurable permissions with Custom Roles. While more will be added over time, these currently include:

1. Universe
2. Notifications
3. Publish Options
4. Incidents
5. Contacts
6. Critical Events
7. Organization Settings
8. Reports

For a full list of configurable Custom Role permissions, see the [Custom Roles Permissions Grid](#) in the Support Center.

NOTE: The legacy Permissions Grid is still available for download in the Manager Portal on the **Roles** page.

Not Within Custom Roles Scope

The following items aren't within the scope of Custom Roles:

- The Custom Roles feature doesn't add any new permissions.
- It will not add the ability for Group Managers to Upload Contacts. Any resource allocation of contacts will disable the Upload Contact feature for all role templates.
- It will not allow Account Administrators to manage cross-Organization Contacts, Notifications, or Incidents.
- It will not limit access to Contact Record data fields.
- A role cannot manage Incidents launched by another role regardless of IC Template access (unless the role is given access to all Communication resources).

Custom Role Usage Overview

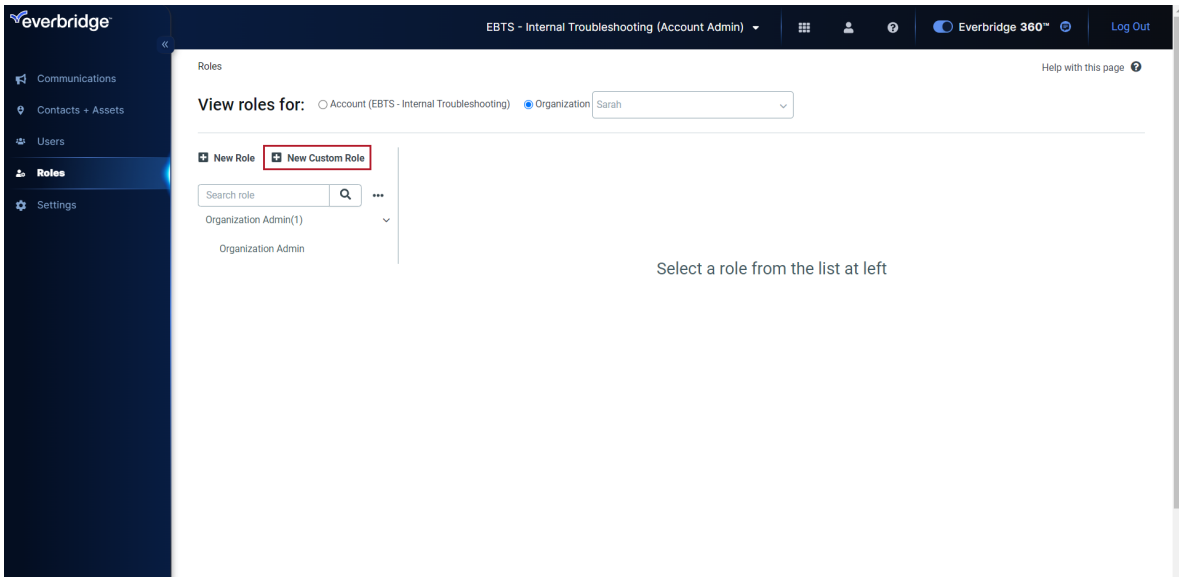
Creating a Custom Role

Custom Roles can be viewed, created, and edited from the **Roles** page.

NOTE: See [Validation Rules](#) for more details about the validation process that occurs while creating a Custom Role.

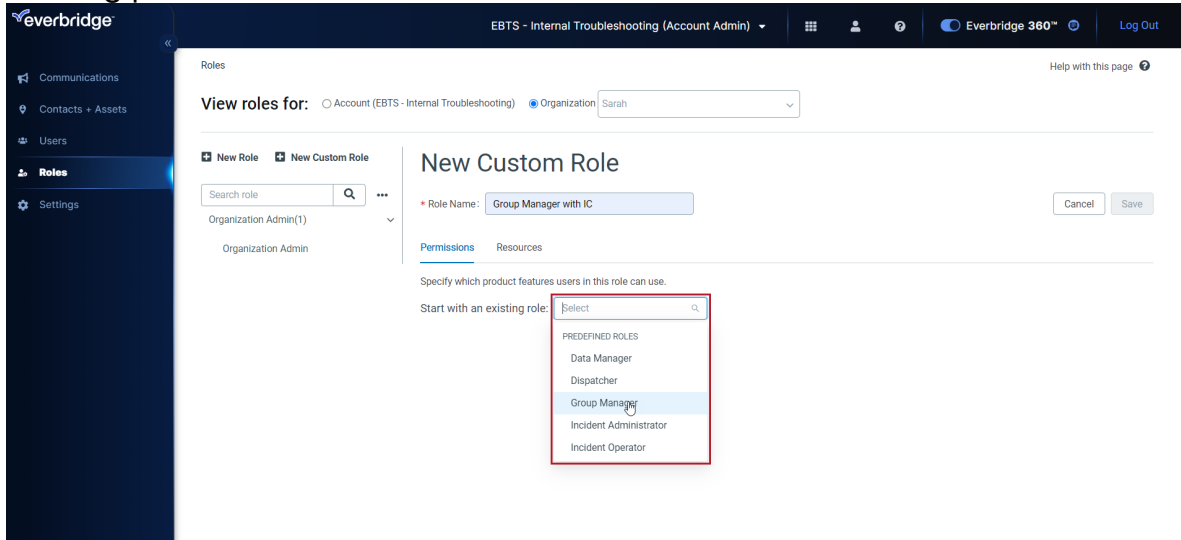
To add a Custom Role:

1. Click **New Custom Role**.

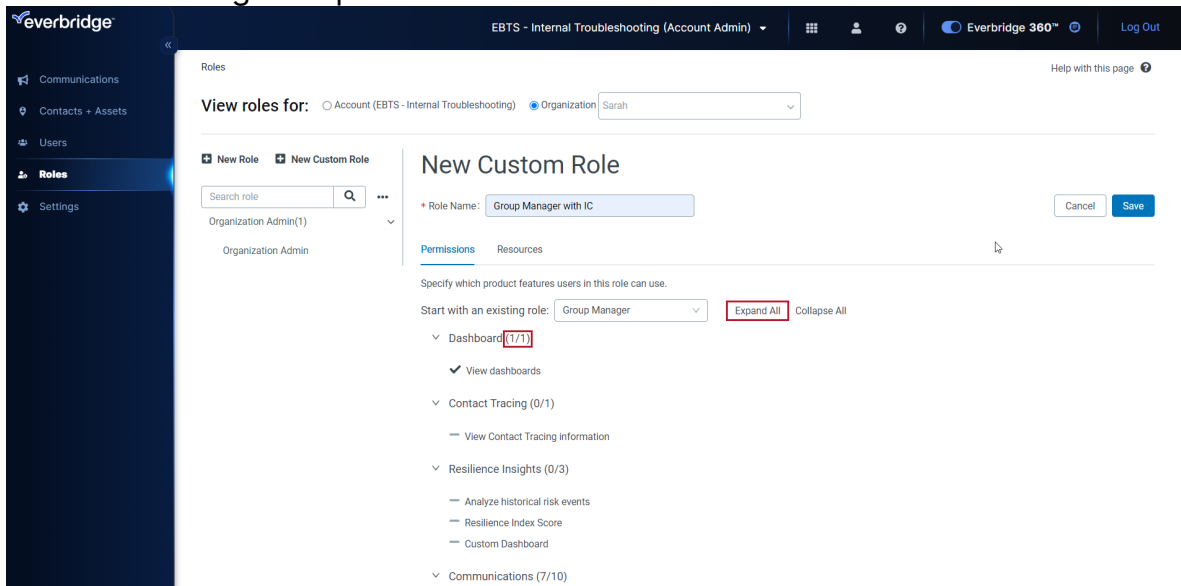


2. The **New Custom Role** page appears, where this new Custom Role can be given a name.

- Under the **Permissions** tab, select a predefined Role Template to use as a starting point for the customization.

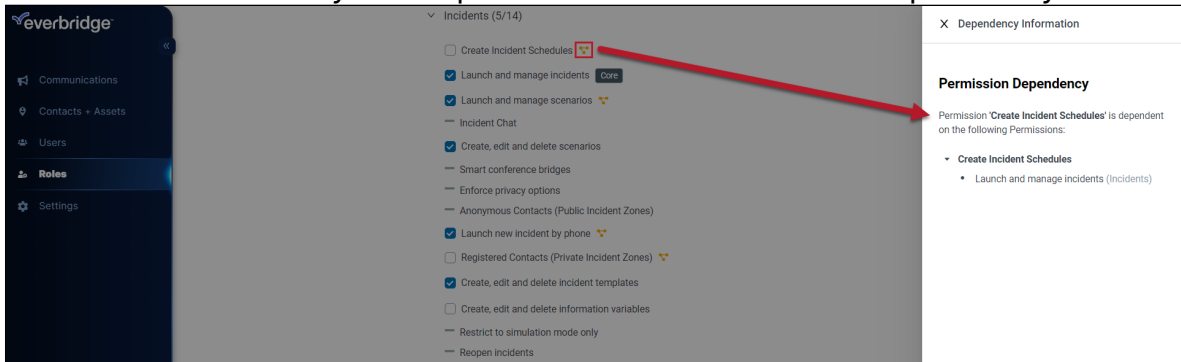


- Use the **Expand All** option to quickly see which permissions for each feature are configurable for the selected Role Template. The number of included permissions for each section is indicated next to its name for quick reference without needing to expand it.

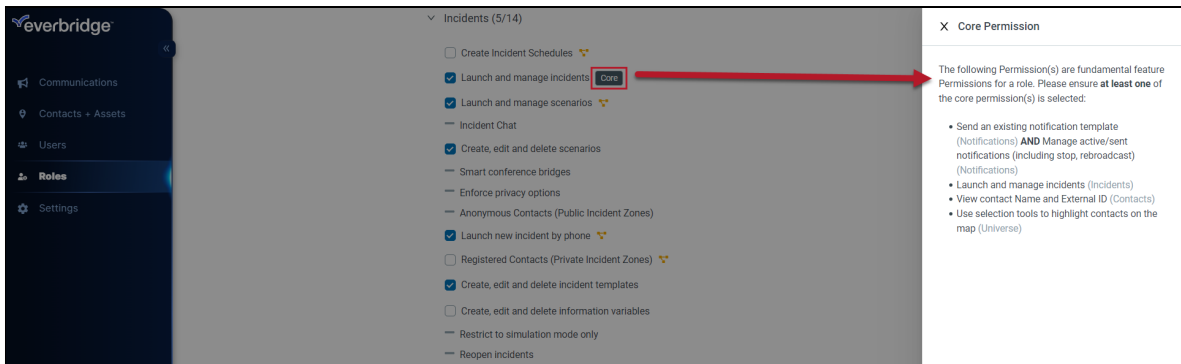


- Some permissions are dependent upon other permissions, which are denoted with the orange **Dependency** icon. Clicking this icon opens a side panel that provides a **Permission Dependency** tree for the selected permission, allowing

the user to see exactly which permissions have a related dependency.



6. Permissions featuring the **Core Permission** icon are one of the four fundamental permissions (or permission combinations), and you must enable at least one of them. Clicking the icon opens a side panel with more details about the Core Permissions.



The four Core Permissions are:

- Send an existing Notification template (Notifications) AND Manage active/sent Notifications (including stop, rebroadcast) (Notifications)
- Launch and manage Incidents (Incidents)
- View Contact Name and External ID (Contacts)
- Use selection tools to highlight Contacts on the map (Universe)

7. Once the desired permissions have been selected, click the **Resources** tab to specify which resources can be accessed or used by this new role. Note that resources can be configured independently from features they depend on but will only take effect when the feature permissions they depend on are enabled.

New Custom Role

* Role Name: Cancel Save

Permissions **Resources**

Specify which resources users of this role can use/access. Note: Resource configurations only take effect when the feature permissions they depend on are enabled.

Communication

Access to all communication resources

Notification

Access to all

Access to Notifications created by this role only

Incident

Access to all

Access to Incidents created by this role only

View Incidents created by all roles

Notification Template

Access to all ⓘ

Access to selected Templates ⓘ ▾

Edit and Delete Notification Templates created by this role only ⓘ

0 item

🔍 Search here

No Data

0 item Selected Templates ⓘ

🔍 Search here

No Data

Incident Template

Access to all ⓘ

Edit and Delete Incident Templates created by this role only ⓘ

Access to selected Templates ⓘ >

Scenario Template

Access to all ⓘ

Edit and Delete Scenario Templates created by this role only ⓘ

Access to selected Templates ⓘ >

Contacts

Organization Contacts

Access to all

Limited access ⓘ ▾

Resources are categorized into two types:

- Communication
 - Notification
 - Incident
 - Notification Template
 - Incident Template
 - Scenario Template
 - Contacts
 - Organization Contacts
8. If the new Custom Role is only intended to have access to certain resources, such as specific Notification or Incident templates, you can define this by selecting **Access to Selected Templates** and choosing the desired templates.

Notification Template

Access to all ⓘ
 Access to selected Templates ⓘ ▾
 Edit and Delete Notification Templates created by this role only ⓘ

3 Items

Q Search here

- Response Plan - Notification
- will Notification be in comms
- Excluded-Contact-Test

2 Items Selected Templates ⓘ

Q Search here

- IT Outage
- Shift Roster

Similar logic applies in the **Contacts** section, where the creator can specify both the Static and Dynamic Groups to which this new Custom Role will have

access.

Contacts

Organization Contacts

Access to all
 Limited access ⓘ ▾

Static Groups

- Remote, India
- Remote, Karnataka
- Remote, Kolkata
- Remote, Mumbai
- Remote, New South Wales
- Remote, Pune
- Responders
- Santa Clara, CA, USA (HQ)
- Spec Chars Group *)
- Staines, United Kingdom
- TIMT - India
- Test Group KJB
- TestGroup KJB
- ThisGroupDoesntexist
- ThisGroupDoestExist

Selected Groups

- Group Name ↕ 🔍
- Remote, India
- Remote, Hyderabad

[> Dynamic Group](#) [Manage](#)

- Once all of the Permissions and Resources have been configured, click **Save** to finish creating the Custom Role.

New Custom Role

* Role Name:

Permissions [Resources](#)

Specify which resources users of this role can use/access. Note: Resource configurations only take effect when the feature permissions they depend on are enabled.

Communication

Access to all communication resources

Notification

Access to all
 Access to Notifications created by this role only

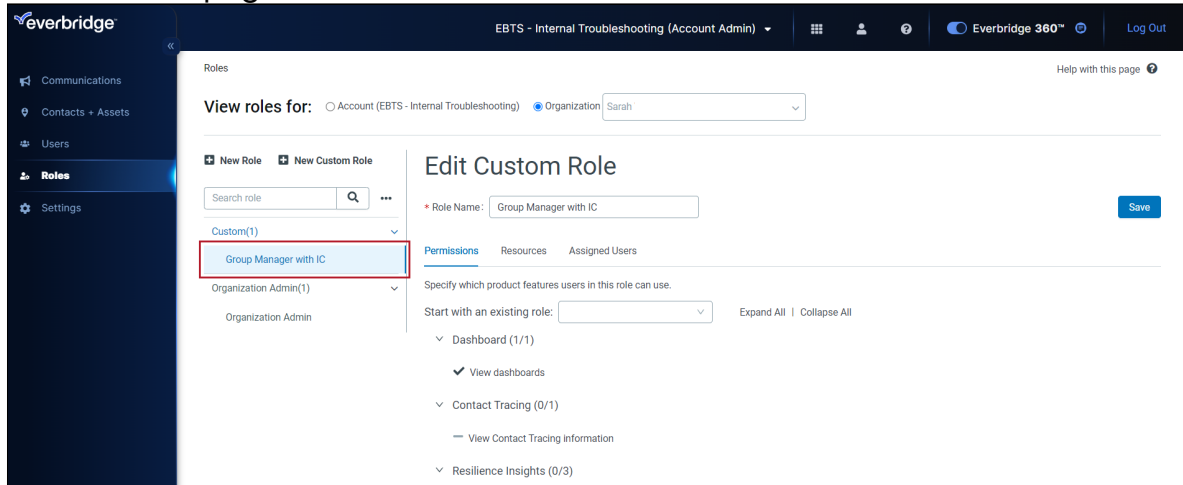
Incident

Access to all
 Access to Incidents created by this role only
 View Incidents created by all roles

Notification Template

Access to all ⓘ
 Access to selected Templates ⓘ ▾
 Edit and Delete Notification Templates created by this role only ⓘ

- The new Custom Role can now be seen and edited from the **Custom** section on the **Roles** page.



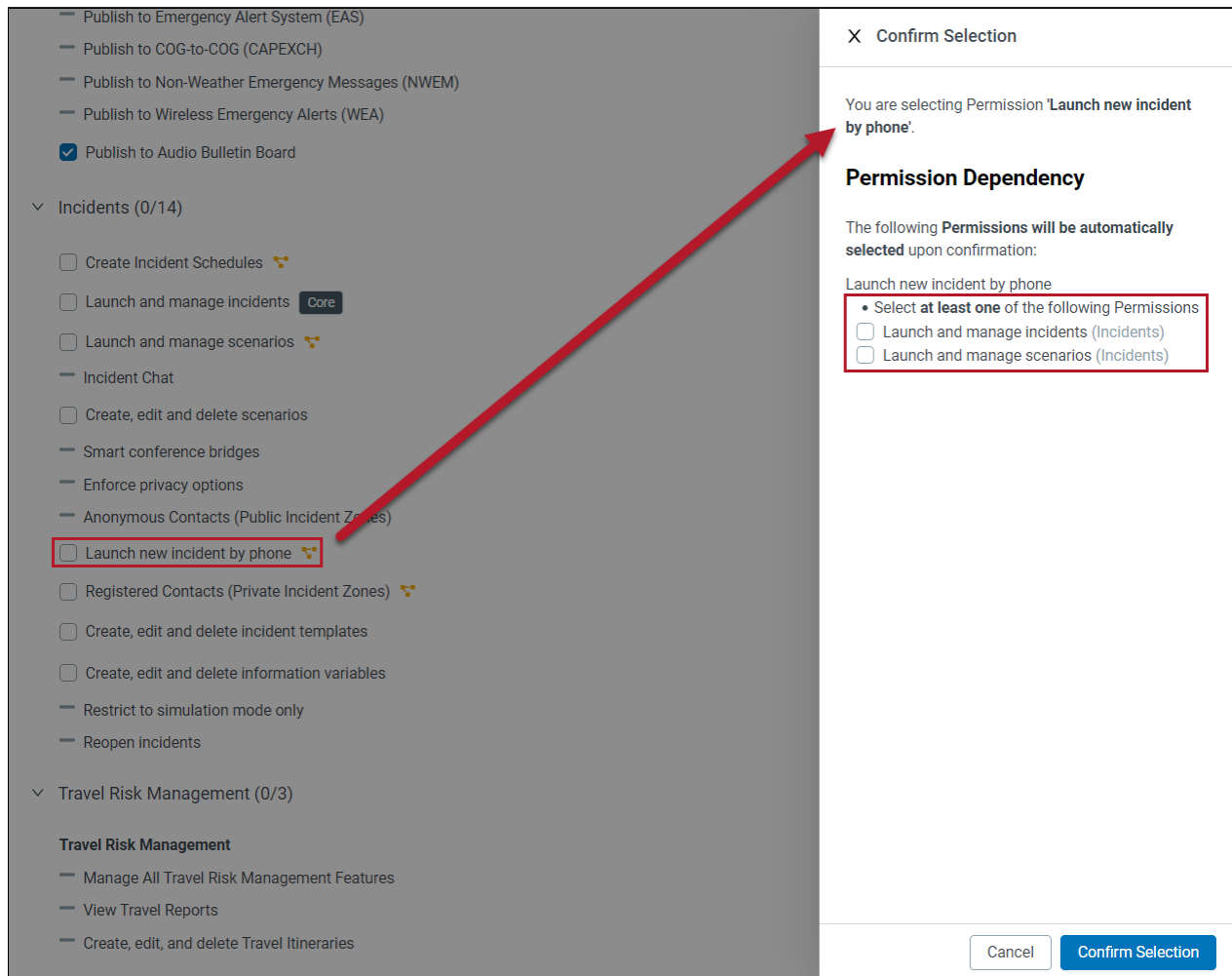
NOTE: The **New Role** button on the Roles page still functions as it did before the introduction of Custom Roles.

Validation Rules

Everbridge runs a combination of validation rules while [Creating a Custom Role](#).

Permission Dependency (Checking)

When checking a permission with dependencies, Everbridge validates if its dependent permissions are all enabled. If not, a slide-out panel with required permissions opens the user to confirm auto-selection.



Permission Dependency (Unchecking)

When unchecking a permission that has a dependency on it, the system validates if permissions dependent on it are all disabled. If not, a slide-out panel with impacted permissions appears for the user to confirm auto-deselection.

The screenshot shows a permissions configuration page on the left and a 'Confirm Deselection' dialog on the right. A red arrow points from the 'Launch and manage incidents' permission in the left pane to the dialog.

Left Pane (Permissions):

- Publish to Emergency Alert System (EAS)
- Publish to COG-to-COG (CAPEXCH)
- Publish to Non-Weather Emergency Messages (NWEM)
- Publish to Wireless Emergency Alerts (WEA)
- Publish to Audio Bulletin Board
- Create Incident Schedules ▼
 - Launch and manage incidents Core
 - Launch and manage scenarios ▼
 - Incident Chat
 - Create, edit and delete scenarios
 - Smart conference bridges
 - Enforce privacy options
 - Anonymous Contacts (Public Incident Zones)
 - Launch new incident by phone ▼
 - Registered Contacts (Private Incident Zones) ▼
 - Create, edit and delete incident templates
 - Create, edit and delete information variables
 - Restrict to simulation mode only
 - Reopen incidents
- Travel Risk Management**
 - Manage All Travel Risk Management Features
 - View Travel Reports
 - Create, edit, and delete Travel Itineraries

Right Pane (Confirm Deselection):

X Confirm Deselection

Deselecting 'Launch and manage incidents' will **automatically deselect** the following Permissions(s) that are dependent on it:

- Launch and manage scenarios (Incidents)
- Launch new incident by phone (Incidents)
- Create Incident Schedules (Incidents)

Buttons: Cancel, Confirm Deselection

Resource Impact

When checking a permission with resource impact, we validate if the required resource is configured as expected. If not, a slide-out panel with the impacted resource iopens for the user to confirm the auto-change.

The screenshot shows a configuration page for permissions. On the left, under 'Contacts (2/13)', the 'Schedule Management' section has 'Create, edit and delete schedules' checked. A red box highlights this checkbox, and a red arrow points to the 'Confirm Selection' dialog on the right. The dialog has a title 'X Confirm Selection' and a message: 'You are selecting Permission 'Create, edit and delete schedules''. Below this is a 'Resource Impact' section stating: 'The following Resource Setting will be automatically changed upon confirmation:'. It lists two items: 'Organization Contacts' and ''Access to all' will be selected'. A yellow 'Caution' box contains the text: 'Once proceed your current selection of Templates for the impacted Resources will be lost.' At the bottom of the dialog, there is a checked checkbox 'Yes, I'm aware of it' and two buttons: 'Cancel' and 'Confirm Selection'.

Core Permission

When unchecking one of the four Core Permissions, we validate if this is the only Core Permission (or permission combination) remaining on the role. If so, the user will be prevented from deselecting it and presented with a slide-out panel with Core Permissions information for troubleshooting.

Publish to Audio Bulletin Board

∨ Incidents (7/14)

Create Incident Schedules 🗑️

Launch and manage incidents Core

Launch and manage scenarios 🗑️

— Incident Chat

Create, edit and delete scenarios

— Smart conference bridges

— Enforce privacy options

— Anonymous Contacts (Public Incident Zones)

Launch new incident by phone 🗑️

Registered Contacts (Private Incident Zones) 🗑️

Create, edit and delete incident templates

Create, edit and delete information variables

— Restrict to simulation mode only

— Reopen incidents

∨ Travel Risk Management (0/3)

Travel Risk Management

— Manage All Travel Risk Management Features

— View Travel Reports

— Create, edit, and delete Travel Itineraries

∨ Contacts (0/13)

Schedule Management

Create, edit and delete schedules 🗑️

X Core Permission

The following Permission(s) are fundamental feature Permissions for a role. Please ensure **at least one** of the core permission(s) is selected:

- Send an existing notification template (Notifications) **AND** Manage active/sent notifications (including stop, rebroadcast) (Notifications)
- Launch and manage incidents (Incidents)
- View contact Name and External ID (Contacts)
- Use selection tools to highlight contacts on the map (Universe)

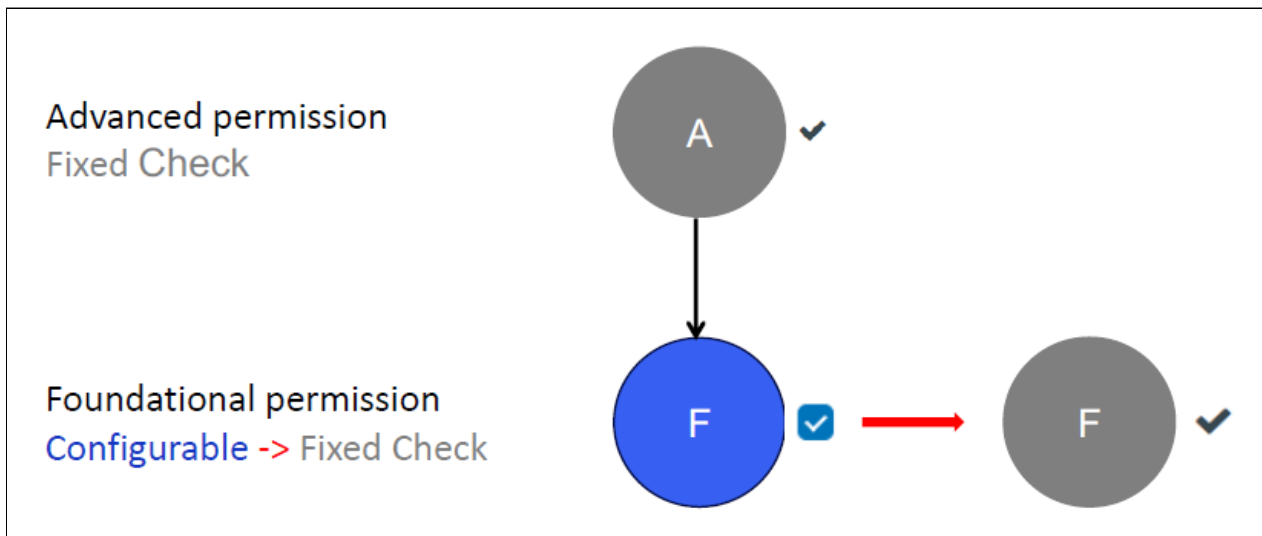
Custom Role Considerations

Interim Behavior - Configurable to Fixed Check

Advanced permissions that are enabled but not configurable and have a dependency on foundational permissions will prevent the foundational permissions from being configurable.

Example

The *Create, edit, and delete Ingestions* permission depends on *Create, edit, and delete Incident templates*. and *Create, edit, and delete Ingestions* is a fixed-check permission for the Incident Administrator role. Therefore, *Create, edit, and delete Incident templates* won't be configurable if the user starts from an Incident Administrator role template.



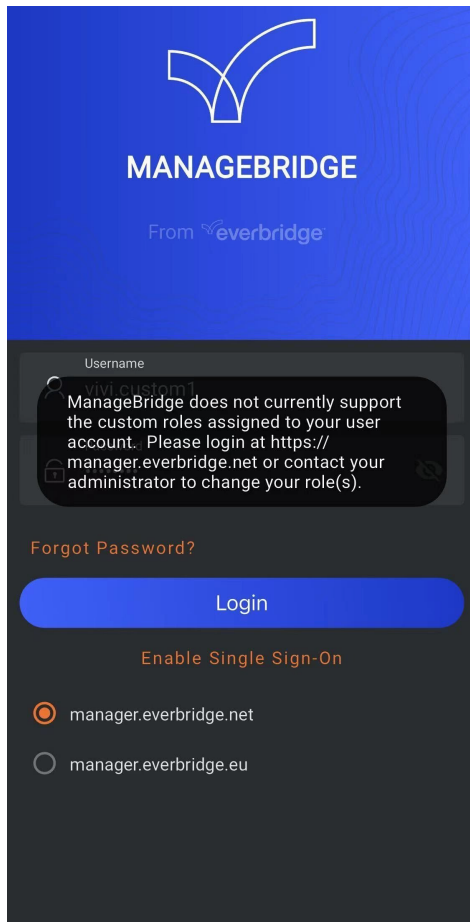
Known Exceptions

The below feature sections may not work properly for Custom Roles until later iterations:

- Smart Orchestration
- Scheduling - Manage Calendars, access Calendars in Notifications/Incidents Templates, and Notifications/Incidents launch workflows

ManageBridge

In addition to the above feature areas, ManageBridge is also currently unsupported by Custom Roles. If the user account you are logged into ManageBridge with has only Custom Roles, you will see the following error message without being able to proceed:



Custom Roles REST API

REST API Response – Role APIs

The following APIs support role-related functions within an Organization. Note that custom Roles support the GET method, but there's no **permissionScope** or **roleDataScope** field in the response. Custom roles do not support POST/PUT/DELETE and will return an error message in response.

There should be no change to Legacy Roles' behavior. See the [Everbridge Developers Hub](#) for API documentation.

Endpoint	Function	Behavior	Response Example
GET /roles/{OrganizationId}/{roleId}	Get a role for an Organization.	Return JSON response without field permissionScope and roleDataScope if the role is a custom role.	<pre>{ "id": 2526269698736143, "roleTemplate": "CUSTOMIZED", "name": "custom role 1" }</pre>
POST /roles/{OrganizationId}	Create a role for an Organization.	Error out if the role is custom.	<pre>{ "status": 400, "message": "Attribute roleTemplate value is CUSTOMIZED" }</pre>
PUT /roles/{OrganizationId}/{roleId}	Update a role for an Organization.	Error out if the role is custom.	<pre>{ "status": 400, "message": "Attribute roleTemplate value is CUSTOMIZED" }</pre>
DELETE /roles/{OrganizationId}/{roleId}	Delete a role from an Organization.	Error out if the role is custom.	<pre>{ "status": 400, "message": "Role 5743578160562301 is an ACCOUNT_ADMIN, Organization_ADMIN, or Custom Role. It cannot be deleted." }</pre>

<p>GET /roles/ {OrganizationId}</p>	<p>Retrieve all roles for an Organization.</p>	<p>Returns a JSON response without the permissionScope and roleDataScope fields for custom roles.</p>	
---	--	---	--

REST API Response – User APIs

The following APIs support the assigning and unassigning of a Custom Role for a user. See the [Everbridge Developers Hub](#) for API documentation.

Endpoint	Function	Behavior
GET /users	Retrieve all users for an account.	No permissionScope or roleDataScope fields in response for the Custom Role of the user.
GET /users/{userId}	Get a user for an account.	No permissionScope or roleDataScope fields in response for the Custom Role of the user.
POST /users	Create a user for an account.	Able to assign a custom role for a user
PUT /users/{userId}	Update a user for an account.	Able to assign/unassign a custom role for a user
DELETE /users/{userId}	Delete a user from an account.	No change to existing behavior.

NOTE: There are no **permissionScope** or **roleDataScope** fields for Custom Roles in the **GET /users** response.

Support Resources

The following Custom Roles resources are available for download in the Support Center:

- [*Custom Roles Permissions Grid*](#)
- [*Custom Roles FAQ*](#)
- [*Custom Roles Known Issues and Exceptions*](#)