Custom Roles Guide

Everbridge Suite

July 2025

Everbridge Suite
2025
Printed in the USA

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

Visit us at www.everbridge.com

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:

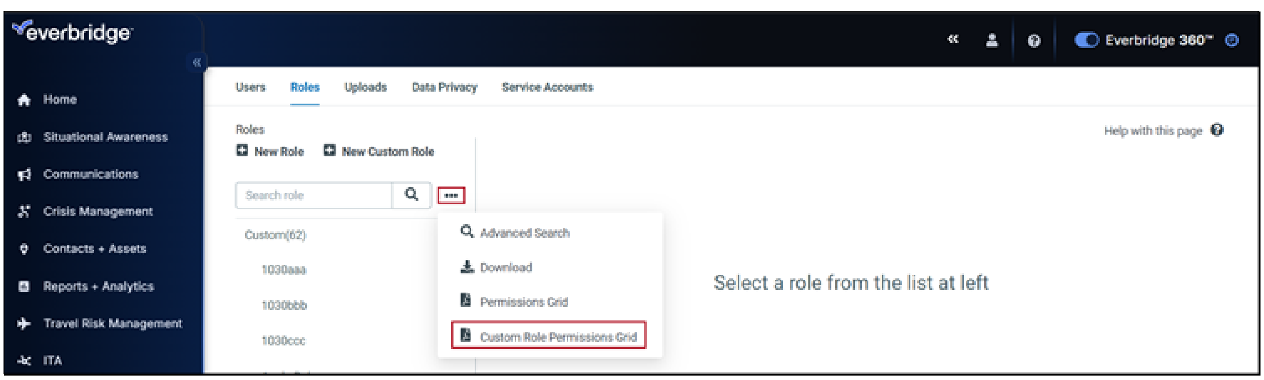
1. Incident Operator
2. Incident Administrator
3. Group Manager
4. Dispatcher
5. Data Manager

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. Visual Command Center
3. Notifications
4. Publish Options
5. Incidents
6. Contacts
7. Critical Events
8. Organization Settings
9. Reports
10. Advanced Reporting
11. Travel Risk Management
12. Asset Management

For a full list of configurable Custom Role permissions, see the Custom Roles Permissions Grid on the **Roles** page in the Manager Portal. The legacy Permissions Grid is available for download from here, as well.



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

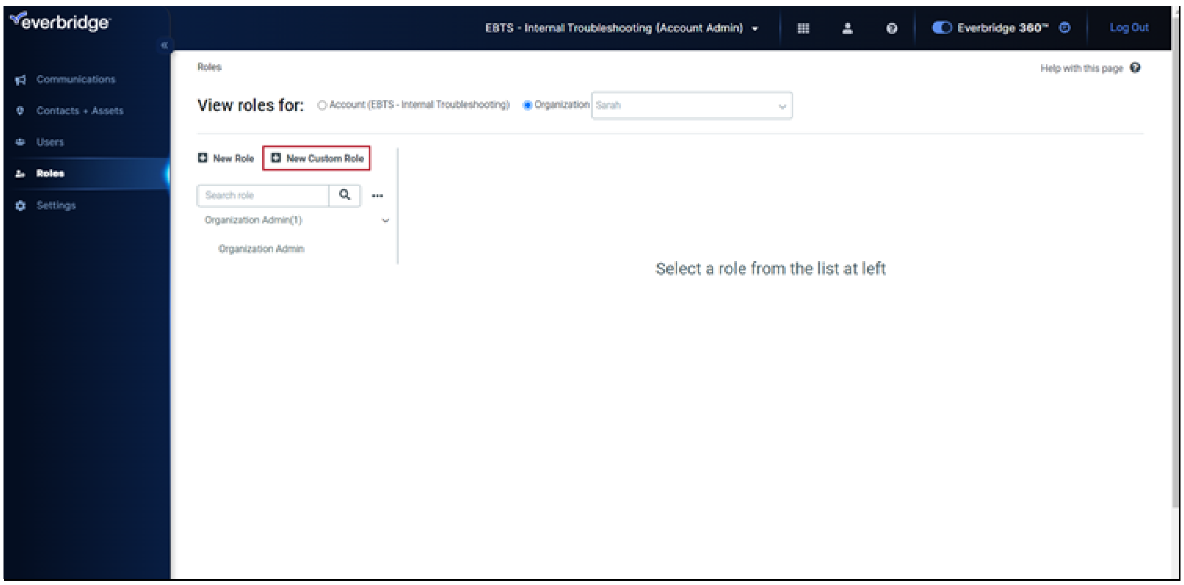
Creating a Custom Role

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.

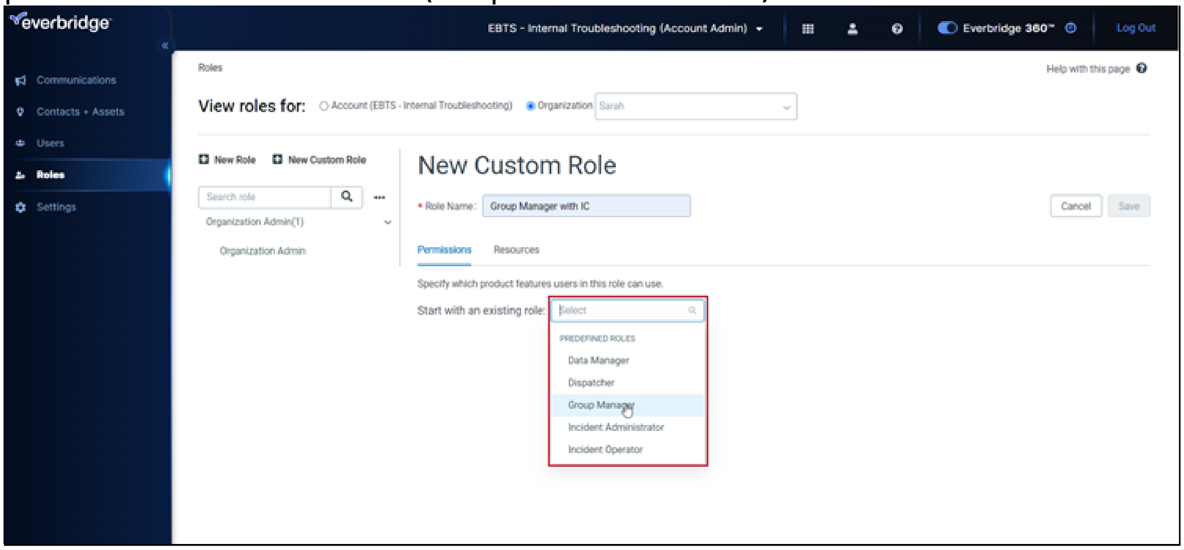
To add a Custom Role:

1. Click **New Custom Role.**

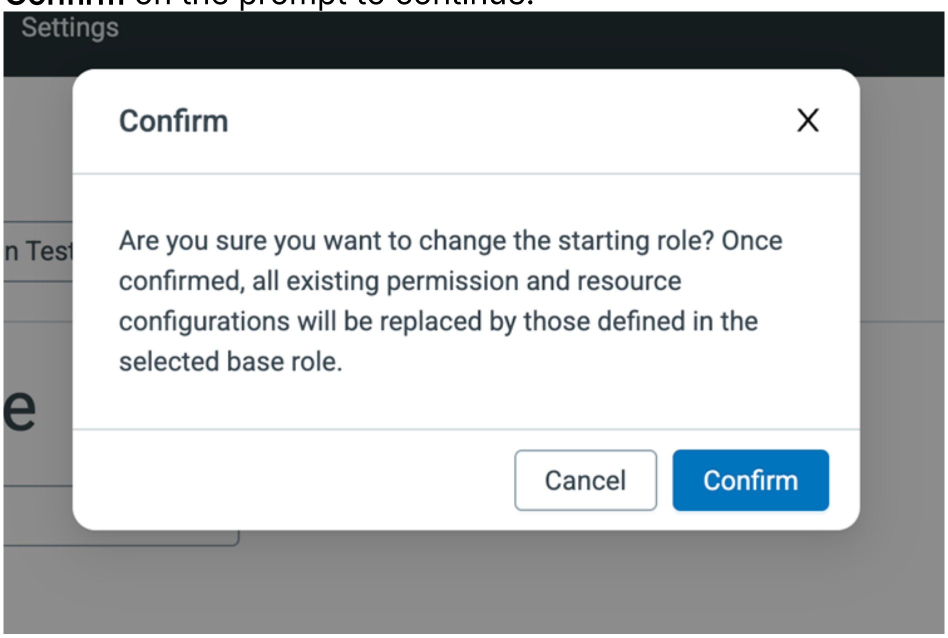


2. The **New Custom Role** page appears, where this new Custom Role can be given a name.
3. Under the **Permissions** tab, select a predefined role template to use as a starting point for the customization. The Custom Role will inherit any

permissions and resources (templates or contacts) included in the base role.

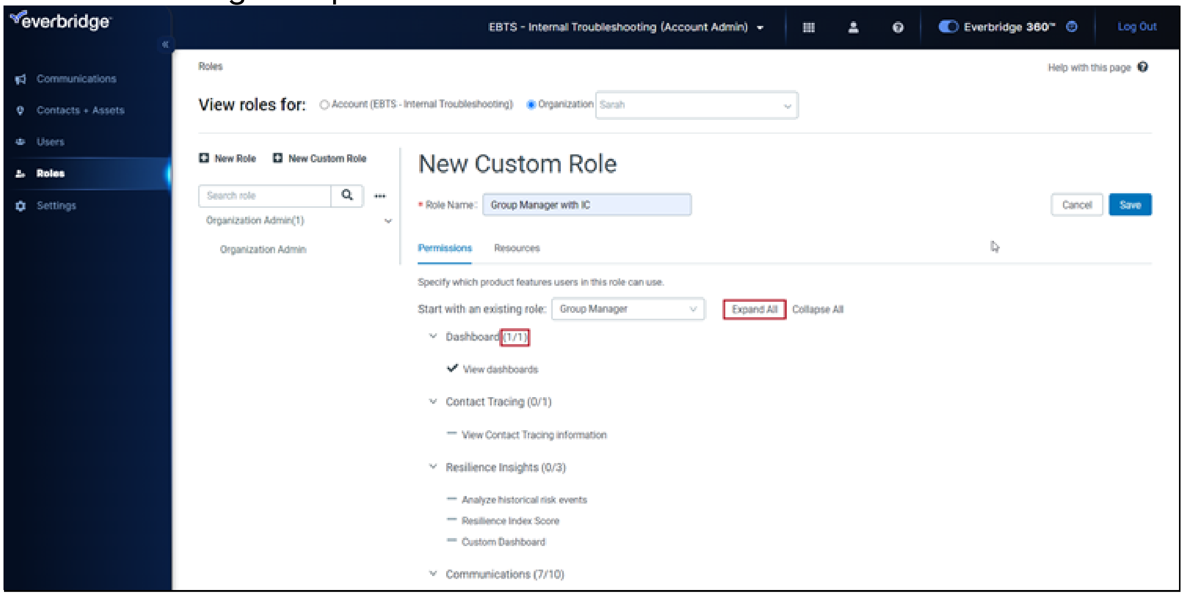


- **NOTE**: If a Custom Role is later edited to change the base role, a message will appear stating that the inherited permissions and resources will also be updated to reflect the new selection. Click **Confirm** on the prompt to continue.

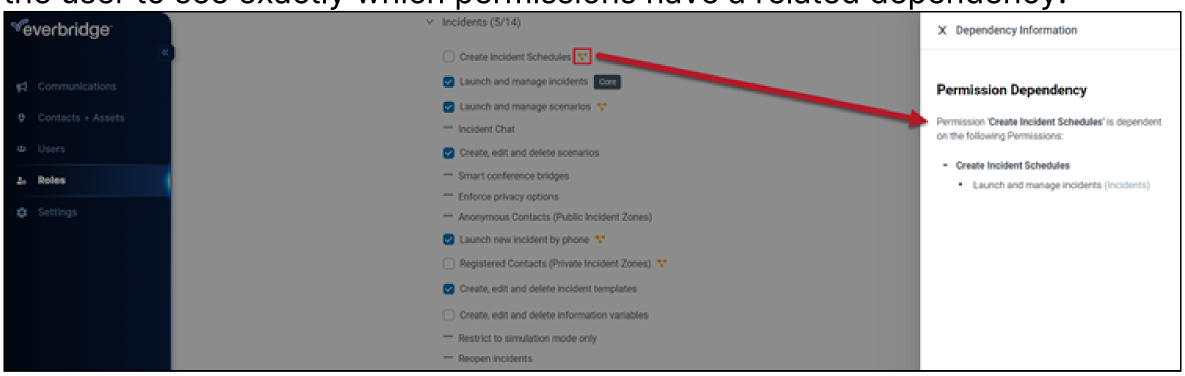


4. Use the **Expand All** option to quickly see which permissions for each feature are configurable for the selected Role Template. The number of included permissions for each section is indicated next to its name for quick reference

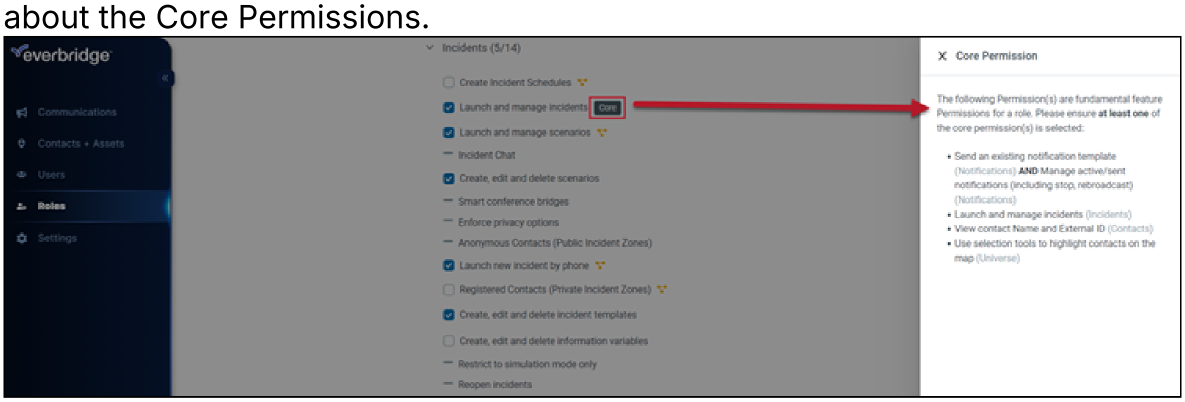
without needing to expand it.



5. 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.



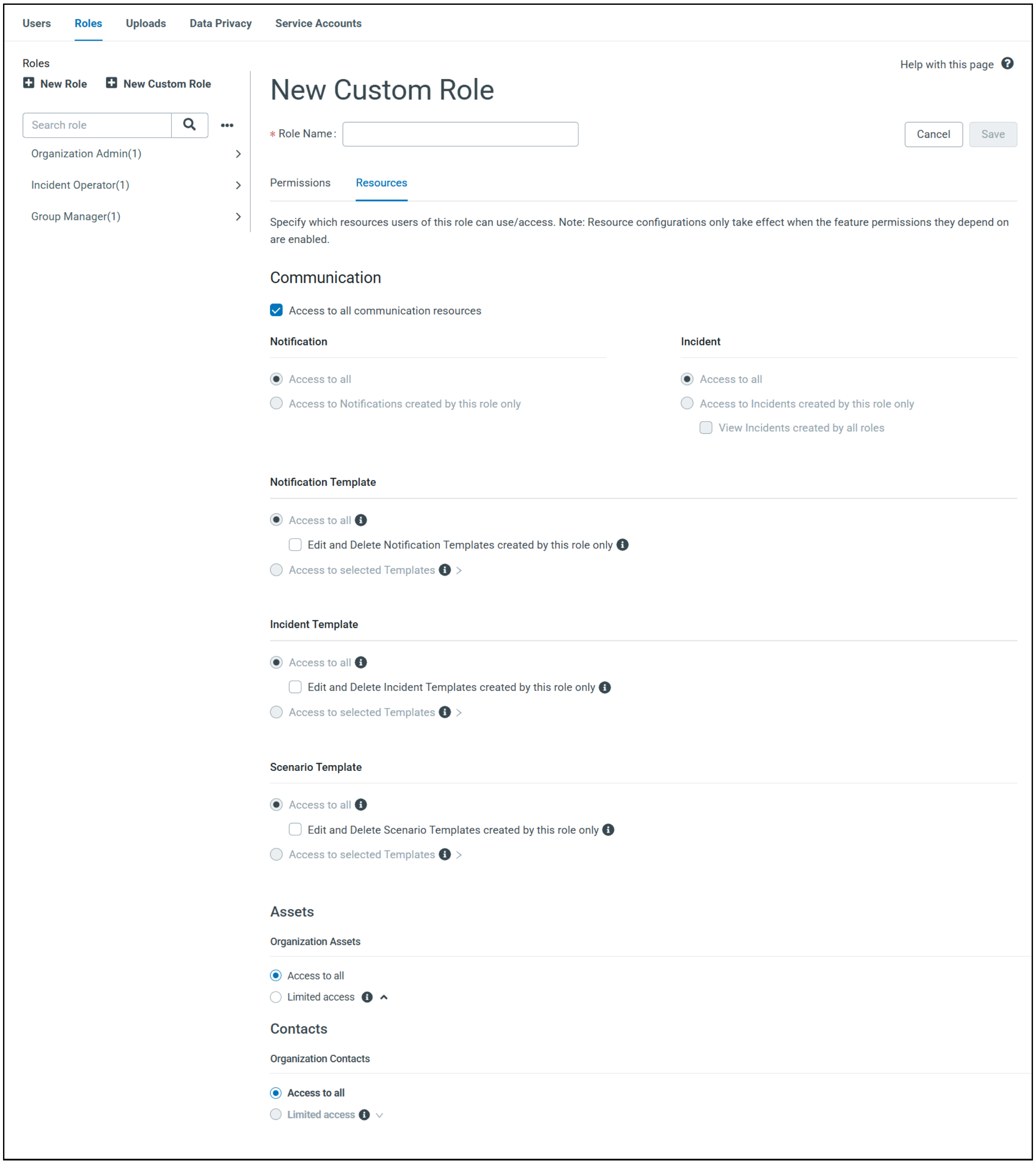
6. Permissions featuring the **Core Permission** icon are one of the four fundamental permissions (or permission combinations), and you must enable at least one of them. Clicking the icon opens a side panel with more details about the Core Permissions.



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.

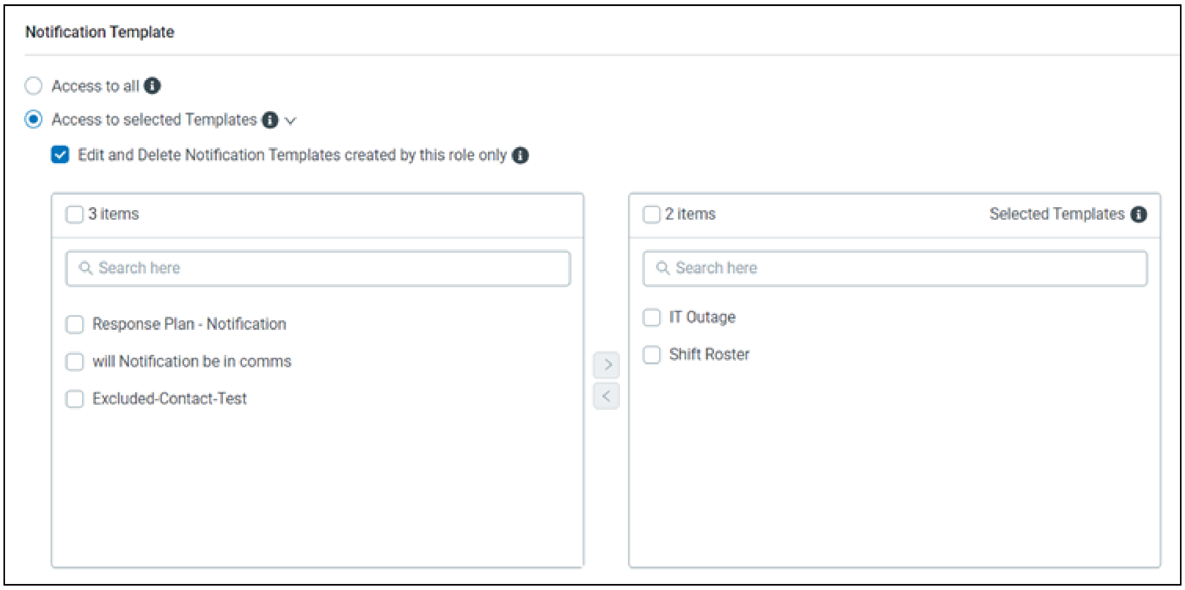


Resources are categorized into three types:

- Communication
  - Notification
  - Incident
  - Notification Template
  - Incident Template
  - Scenario Template
- Assets
  - Organization Assets
- Contacts

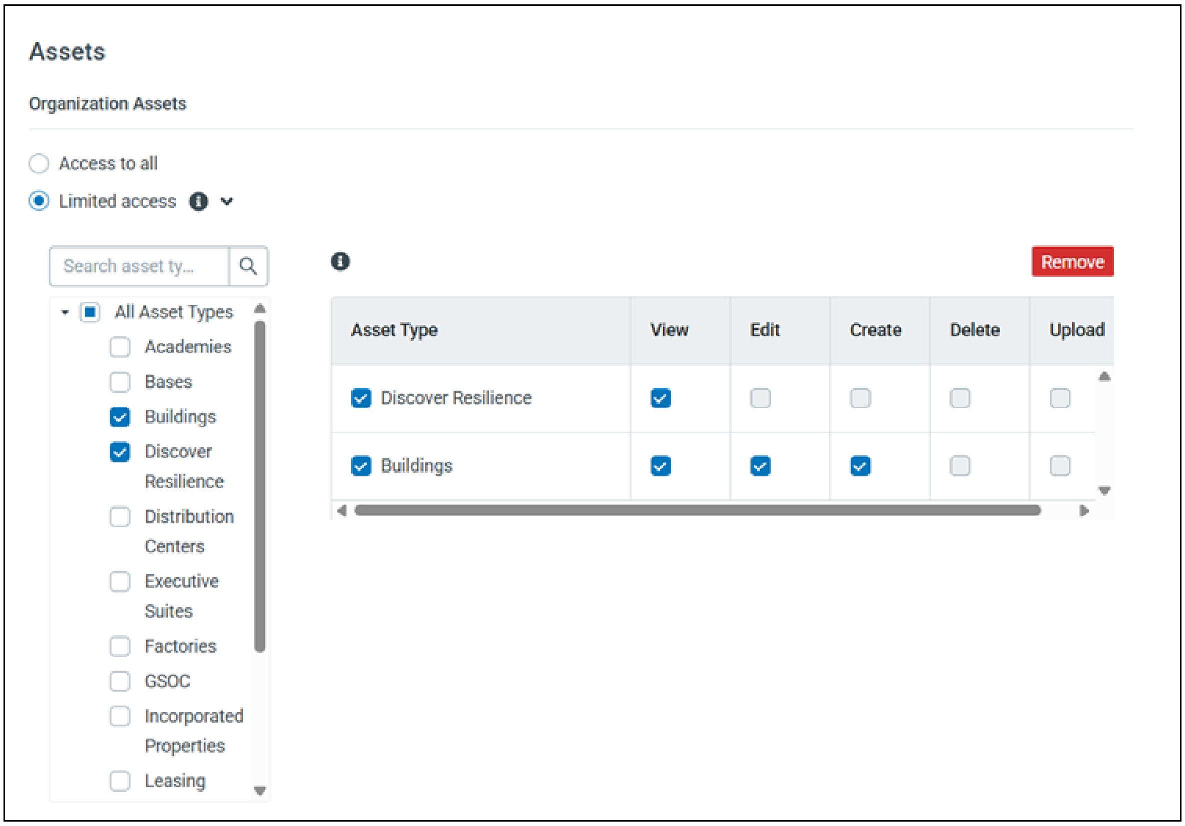
   - Organization Contacts

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. Note that the resources inherited from the chosen base role will already be selected.



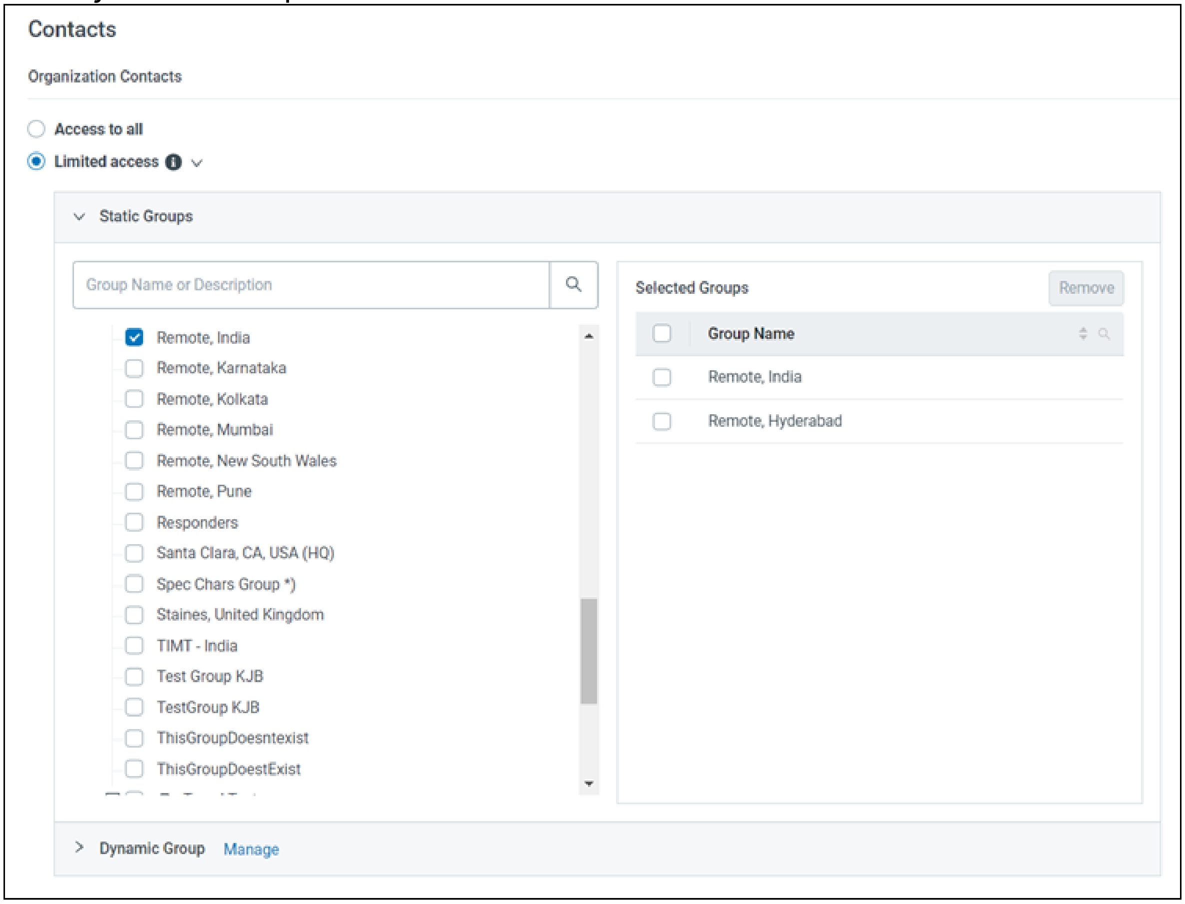
9. If the new Custom Role should only have access to Assets of a specific Type, that can be configured in the **Assets** section. Define if the role can only view these Asset Types, or if they can also edit, create, delete, or upload them, as

well.

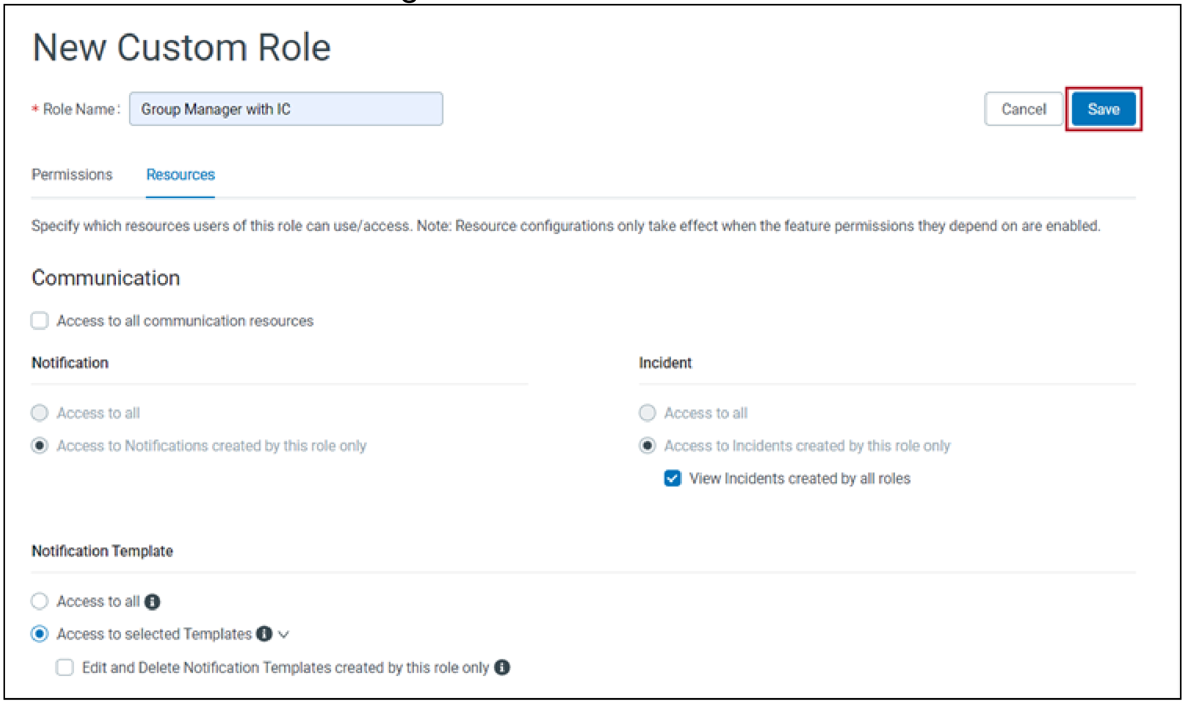


- NOTE: These rules are honored across both the Manager Portal and Visual Command Center interfaces.

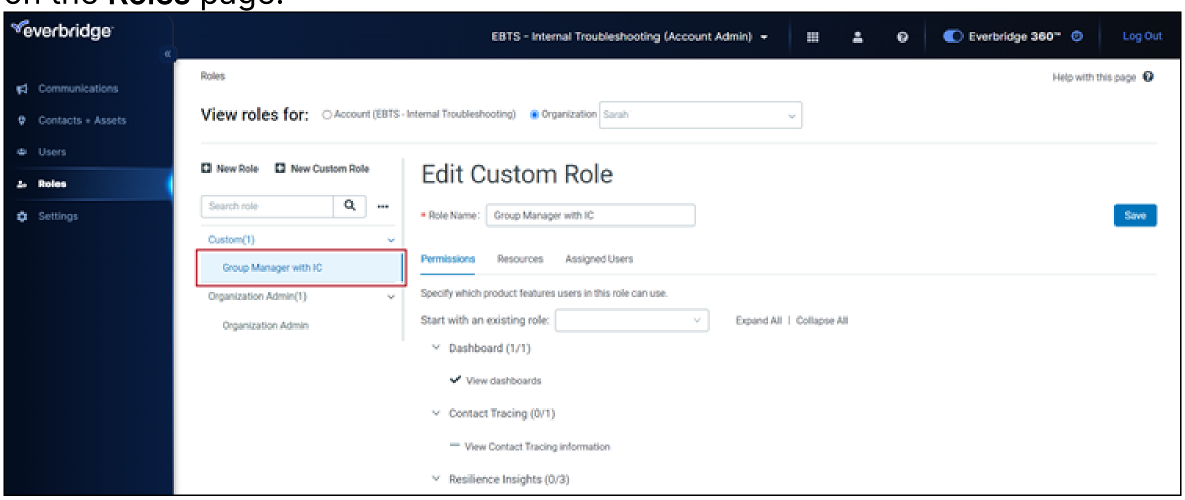
10. Next is the **Contacts** section, where the creator can specify both the Static and Dynamic Groups to which this new Custom Role will have access.



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



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



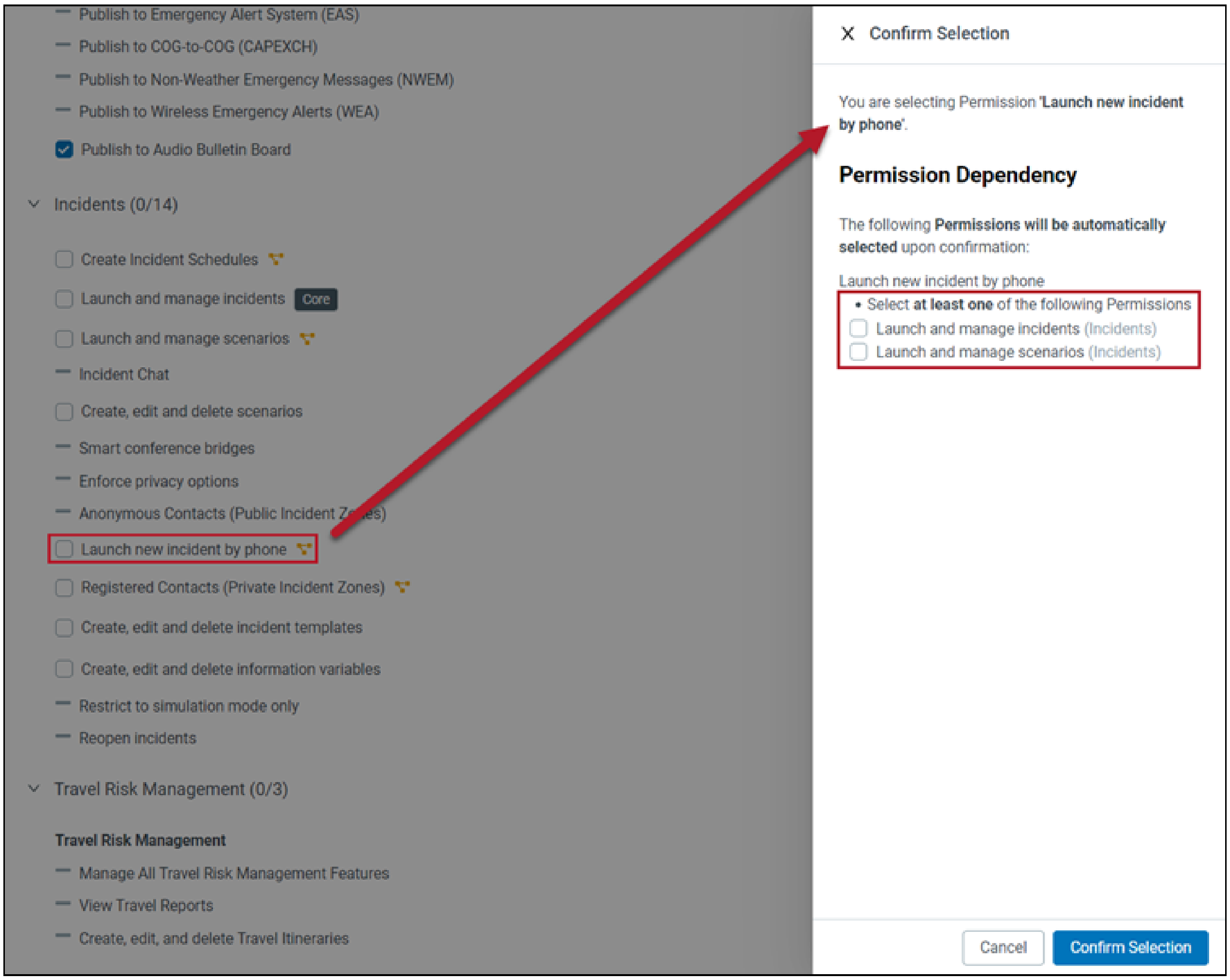
NOTE: The **New Role** button on the Roles page still functions as it did before the introduction of Custom Roles.

Validation Rules

Everbridge runs a combination of validation rules while Creating a Custom Role.

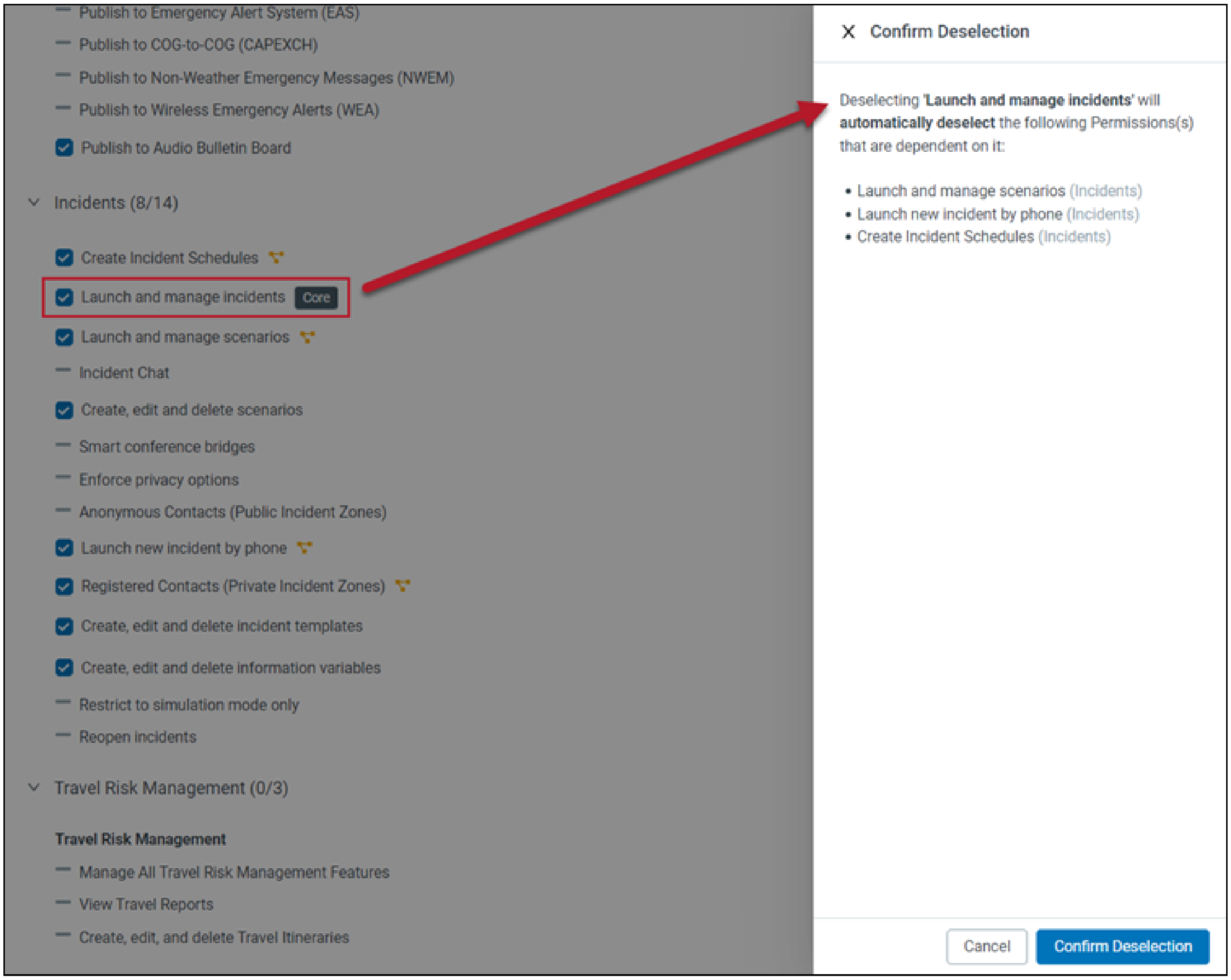
Permission Dependency (Checking)

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.



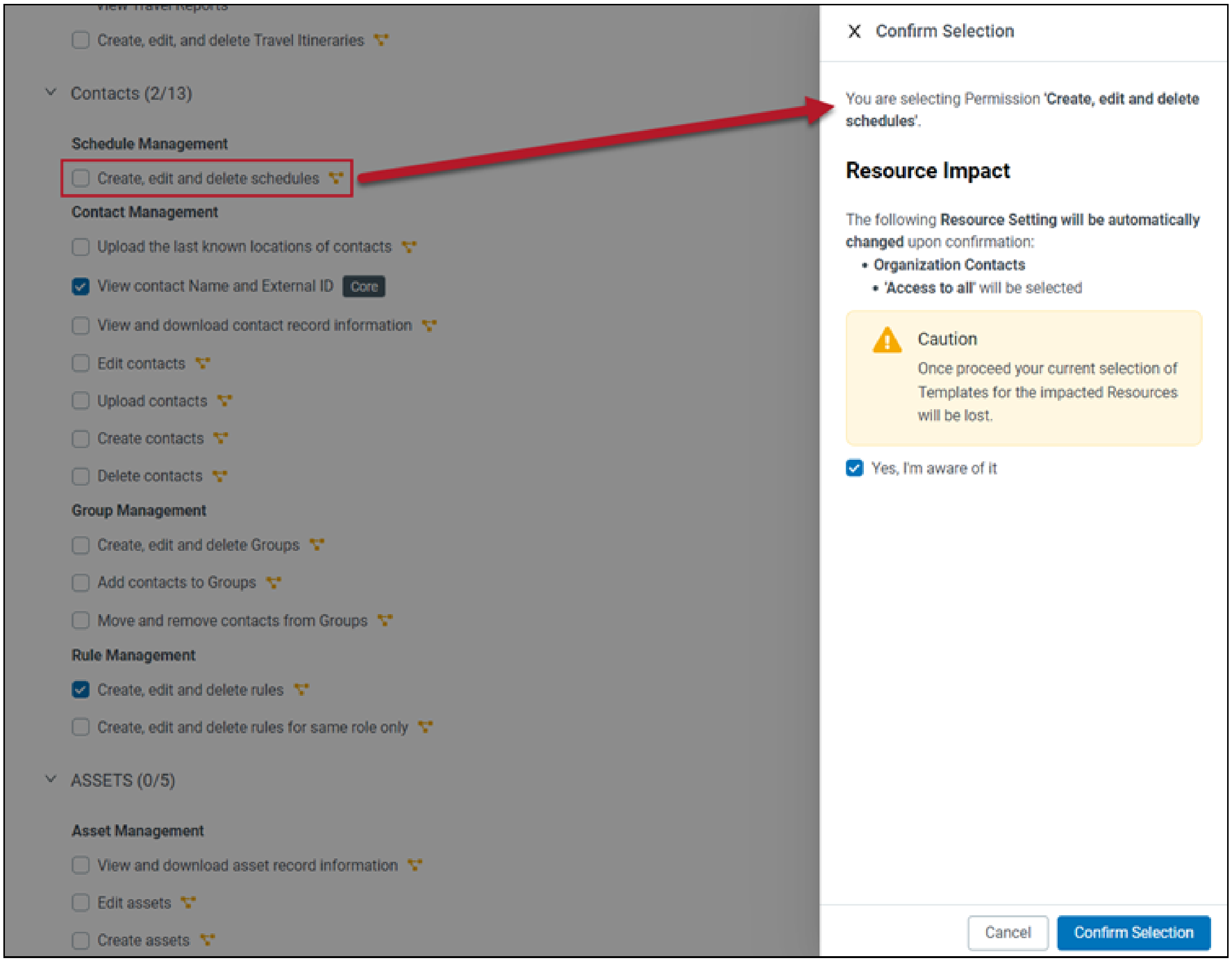
Permission Dependency (Unchecking)

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.



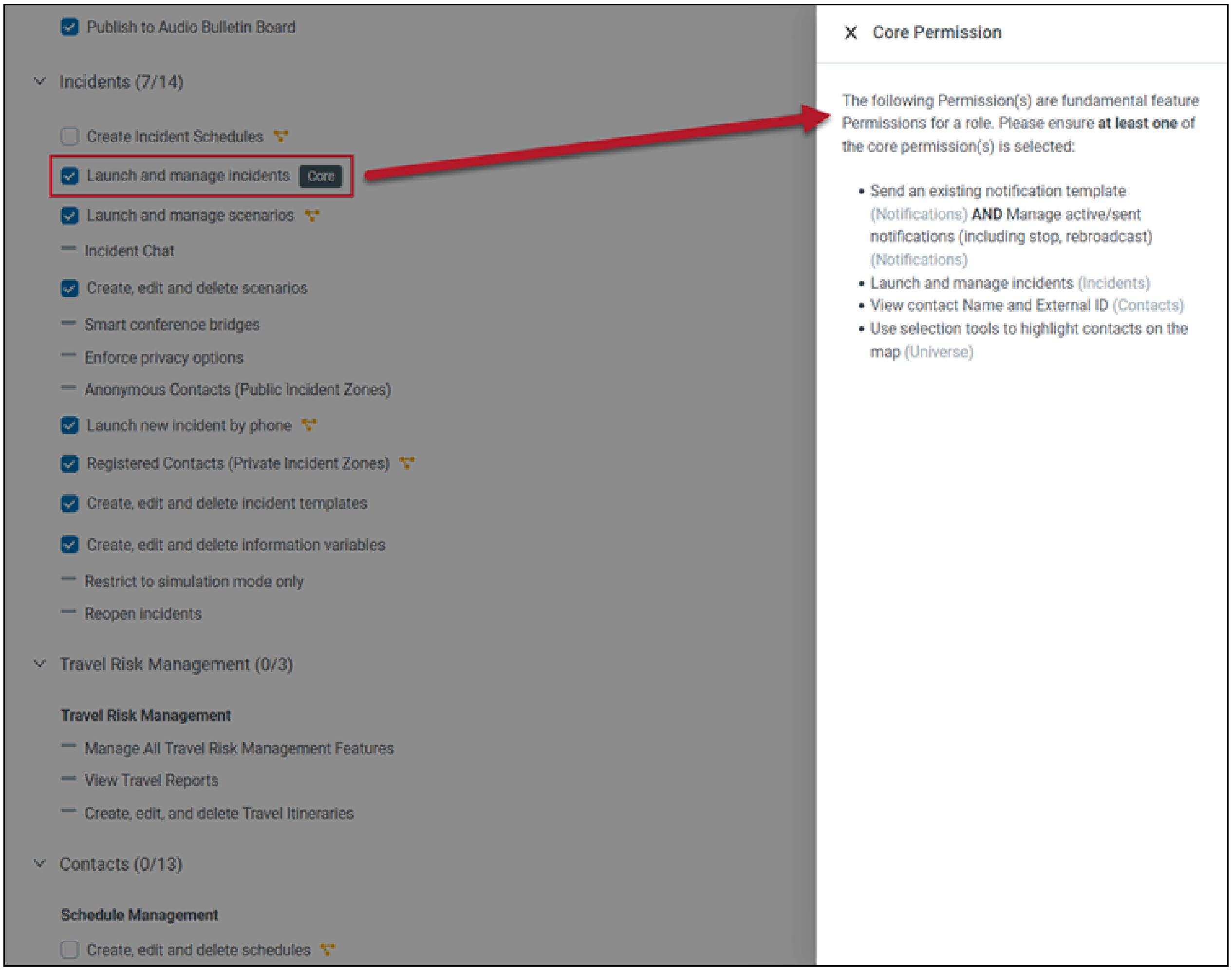
Resource Impact

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.



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
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)

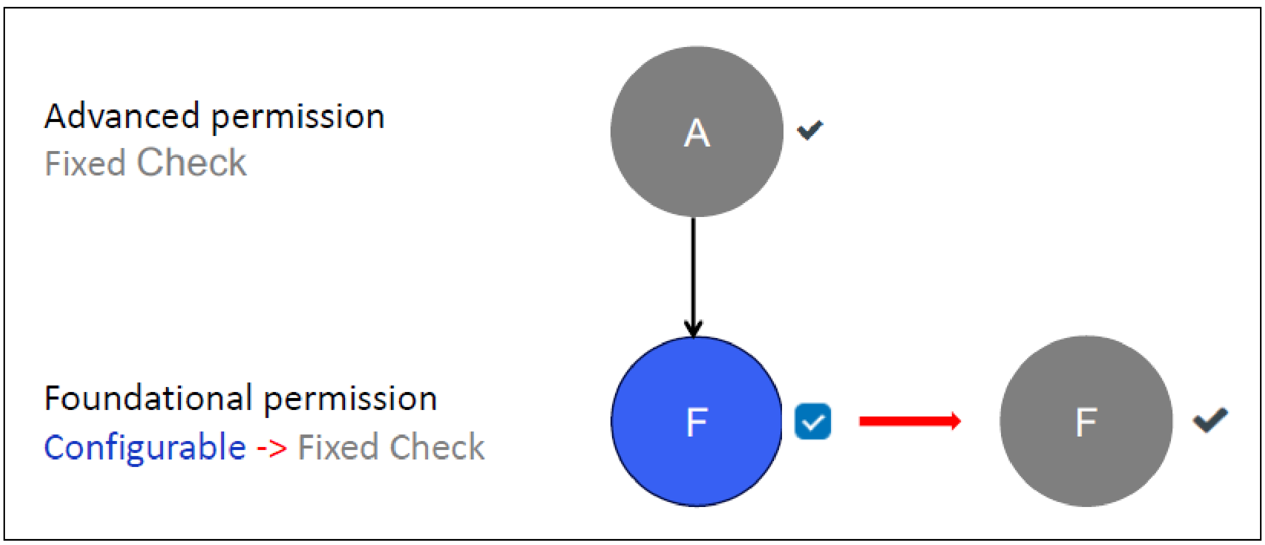
Custom Role Considerations

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.



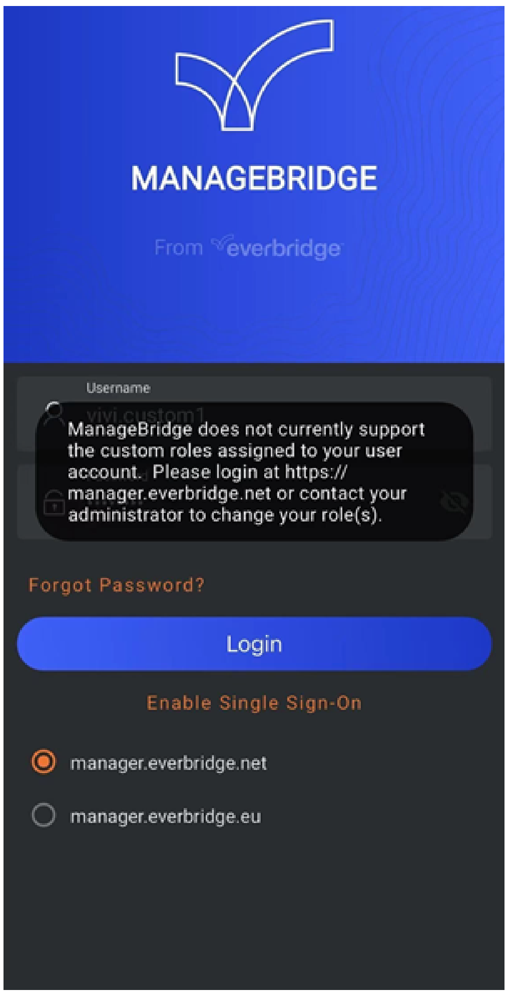
Known Exceptions

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 premissionScope and roleDataScope if the role is a custom role.	{ "id": 2526269698736143, "roleTemplate": "CUSTOMIZED", "name": "custom role 1" }
POST /roles/ {OrganizationId}	Create a role for an Organization.	Error out if the role is custom.	{ "status": 400, "message": "Attribute roleTemplate value is CUSTOMIZED" }
PUT /roles/ {OrganizationId}/ {roleId}	Update a role for an Organization.	Error out if the role is custom.	{ "status": 400, "message": "Attribute roleTemplate value is CUSTOMIZED" }
DELETE /roles/ {OrganizationId}/ {roleId}	Delete a role from an Organization.	Error out if the role is custom.	{ "status": 400, "message": "Role 5743578160562301 is an ACCOUNT_ADMIN, Organization_ADMIN, or Custom Role. It cannot be deleted." }

GET /roles/ {OrganizationId}	Retrieve all roles for an Organization.	Returns a JSON response without the premissionScope and roleDataScope fields for custom roles.	

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 FAQ
- Custom Roles Known Issues and Exceptions