CEM Orchestration Guide

Everbridge Suite

April 2026

Everbridge Suite
2026
Printed in the USA

Everbridge, Inc.
8300 Boone Blvd. Suite 800. Vienna, VA 22182
Toll-Free (USA/Canada) +1.888.366.4911

Visit us at www.everbridge.com

CEM Orchestration Overview

CEM Orchestration enables users to manage Alerting and automated communications in response to Risk Events affecting their Organization's Contacts and Assets. It supports the creation of advanced Rules within Workflows to accommodate a wide range of use cases.

For example, using CEM Orchestration, you can:

- Fine-tune your Rules based on what Risk Event is reported, who is impacted (Contacts), and what is impacted (Assets).
- Set different Alerting Rules for different Asset Types or Contact Types.
- Group all of your Risk Management Rules into Workflows.
- Manage Workflows by Risk Type rather than by Data Source.
- Utilize out-of-the-box Workflows to get started with Alerting and automated response, then customize those Workflows as needed.
- Build new Workflows and Rules via the user interface.
- Download Rules from a testing or staging Organization and upload them to your production environment.

IMPORTANT: This feature requires that you be able to access **Alert Settings Management** in Visual Command Center or have the **Orchestration Rules** permission in your user role. For more information, contact your Everbridge Account Manager.

Creating a CEM Orchestration Integration User

The **CEM Orchestration Integration User** is a user account in an Organization that is used to perform automated actions needed to execute CEM Orchestration Workflows. It can be created by an Administrator from **Workflows** > **CEM Orchestration** > **Setup**.

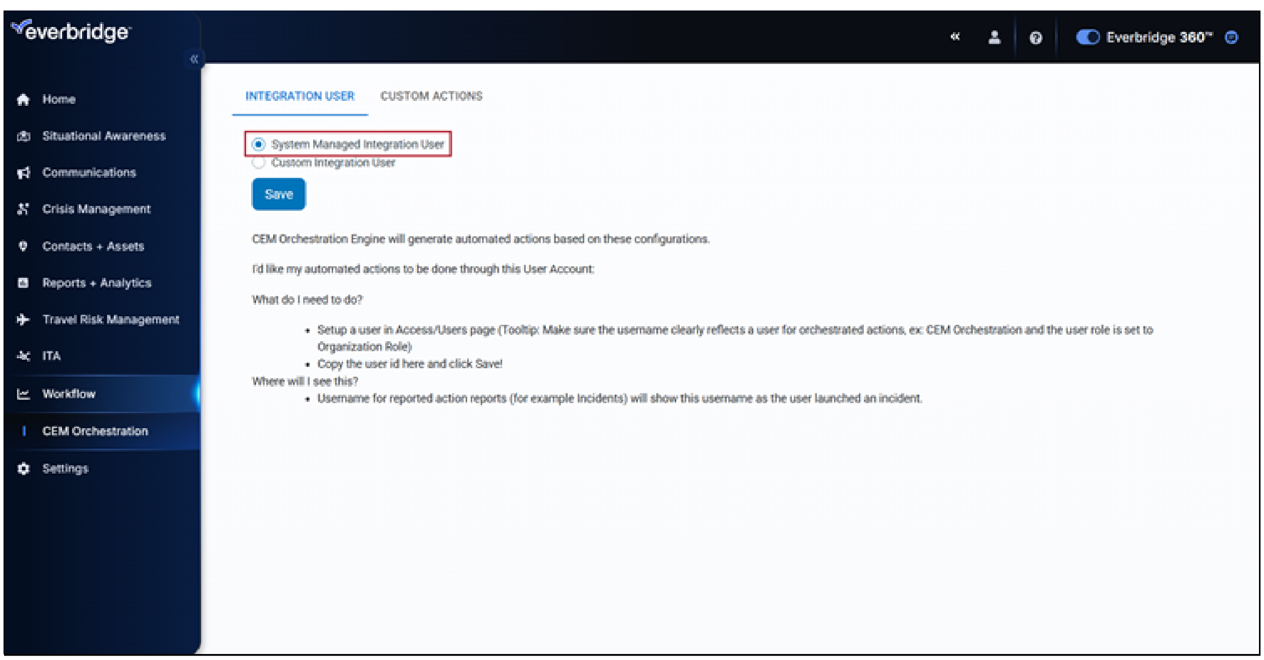
For example, a Launch Incident action in a CEM Orchestration rule will be performed automatically by the Integration User, and the Integration User's username will be associated with the action in the **Activity Log** and other reporting.

There are two types of Integration Users:

1. System-Managed Integration User
2. Custom Integration User

System Managed Integration Users

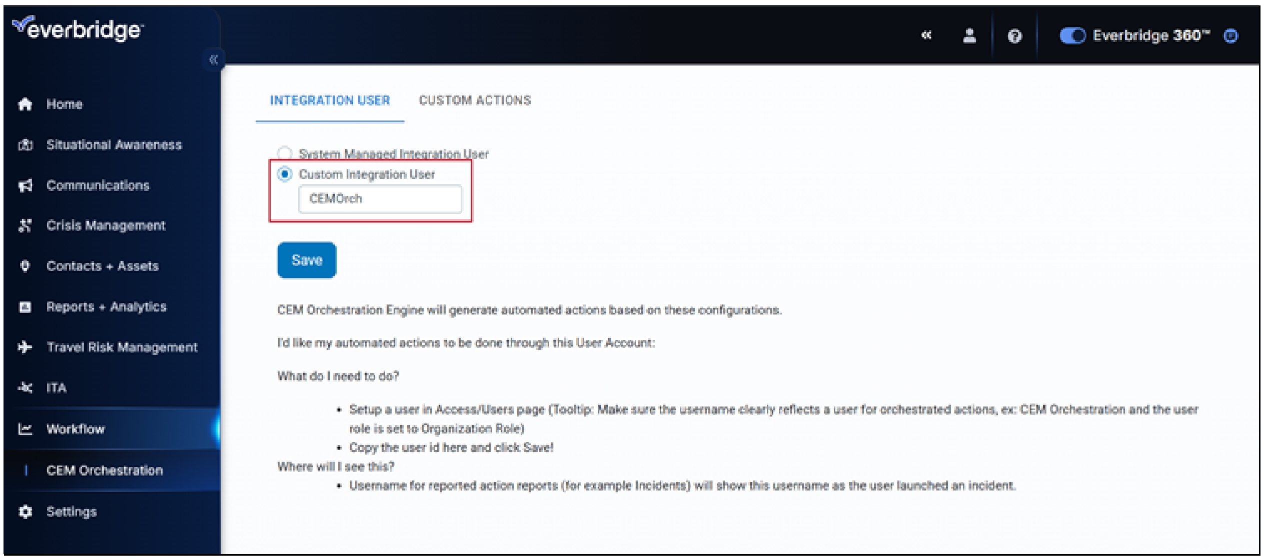
Select the **System Managed Integration User** option and click **Save** if you do not want to specify a particular account for this purpose. In this case, Everbridge will make the Integration User the same as the API User configured in **VCC Provisioning**. This is the default configuration in a new Organization.



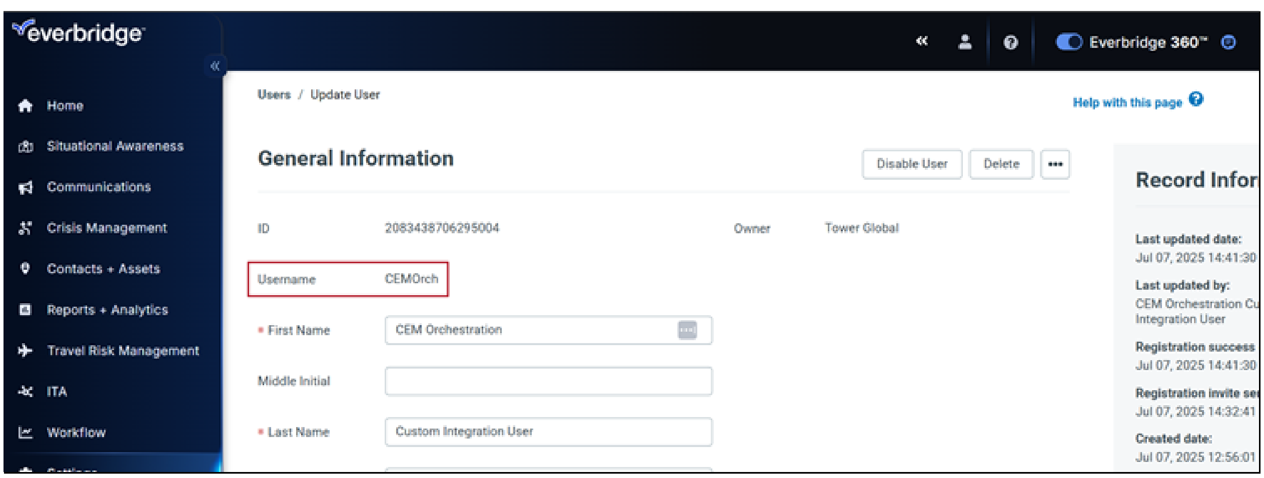
NOTE: The System Managed Integration User option is the recommended method for accuracy and ease of use.

Custom Integration User

Select the **Custom Integration User** option to assign a specific Organization Administrator as the Integration User.



Enter the exact username of the integration user (for example, "CEMOrch"), which can be found on its **Update User** page, and click **Save**.

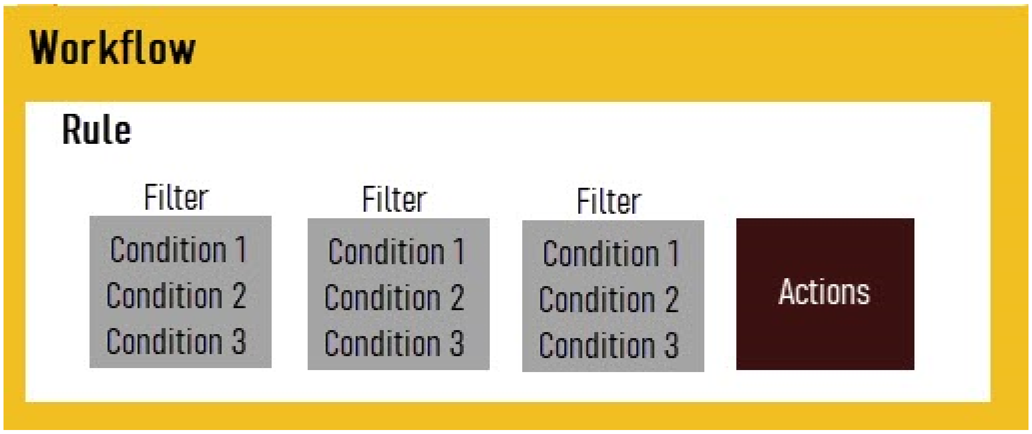


NOTE: GIve the Custom Integration User a username that can be easily identified in the logs and reporting.

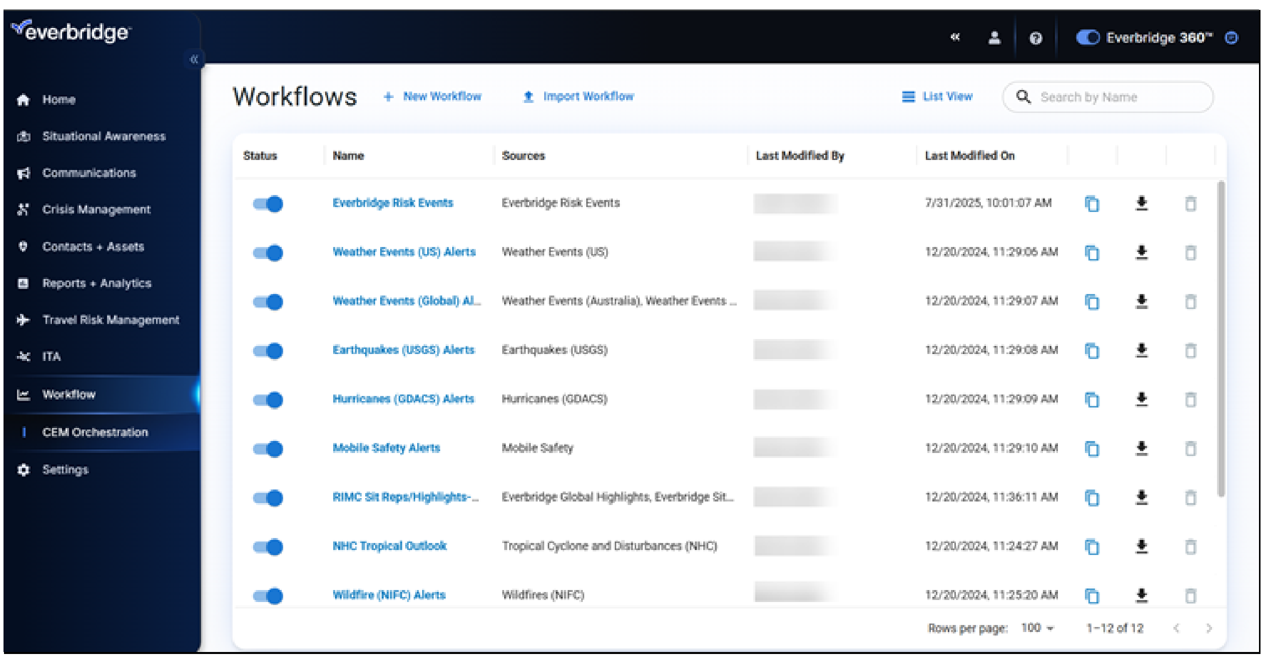
CEM Orchestration Workflows

What is a Workflow?

A **Workflow** is a container for organizing related Rules with their Filters and Actions. Each of the out-of-the-box Workflow contains the Rules for a single Risk Event Category. For example, the Weather Events (US) Alerts Workflow contains the Rules for US-based weather events.



Workflows can be created and managed from the **Workflows List** (**Workflow** > **CEM Orchestration** > **Workflow List**, where a set of default Workflows should already be configured.



NOTE: This page can also be found in the Everbridge Classic UI by navigating to **Settings** > **Everbridge Open** > **CEM Orchestration** > **Workflows**.

Rules

A **Rule** contains the settings for kicking off one or more Actions. Each Rule can contain multiple groups of settings, called Filters. If the conditions in any Filter in the Rule are met, the Rule's Action is taken. Creating Alerts is the default Action for all rules. An optional additional Action is launching an Incident. Custom Actions can also be configured and used.

Filters

A **Filter** or **Filter Set** is a set of selected conditions, such as Data Source, Event Category, and Impact Radius. When these conditions are met, CEM Orchestration takes the Action(s) specified in the Rule. Within a Rule, you can create specific Filters for different situations.

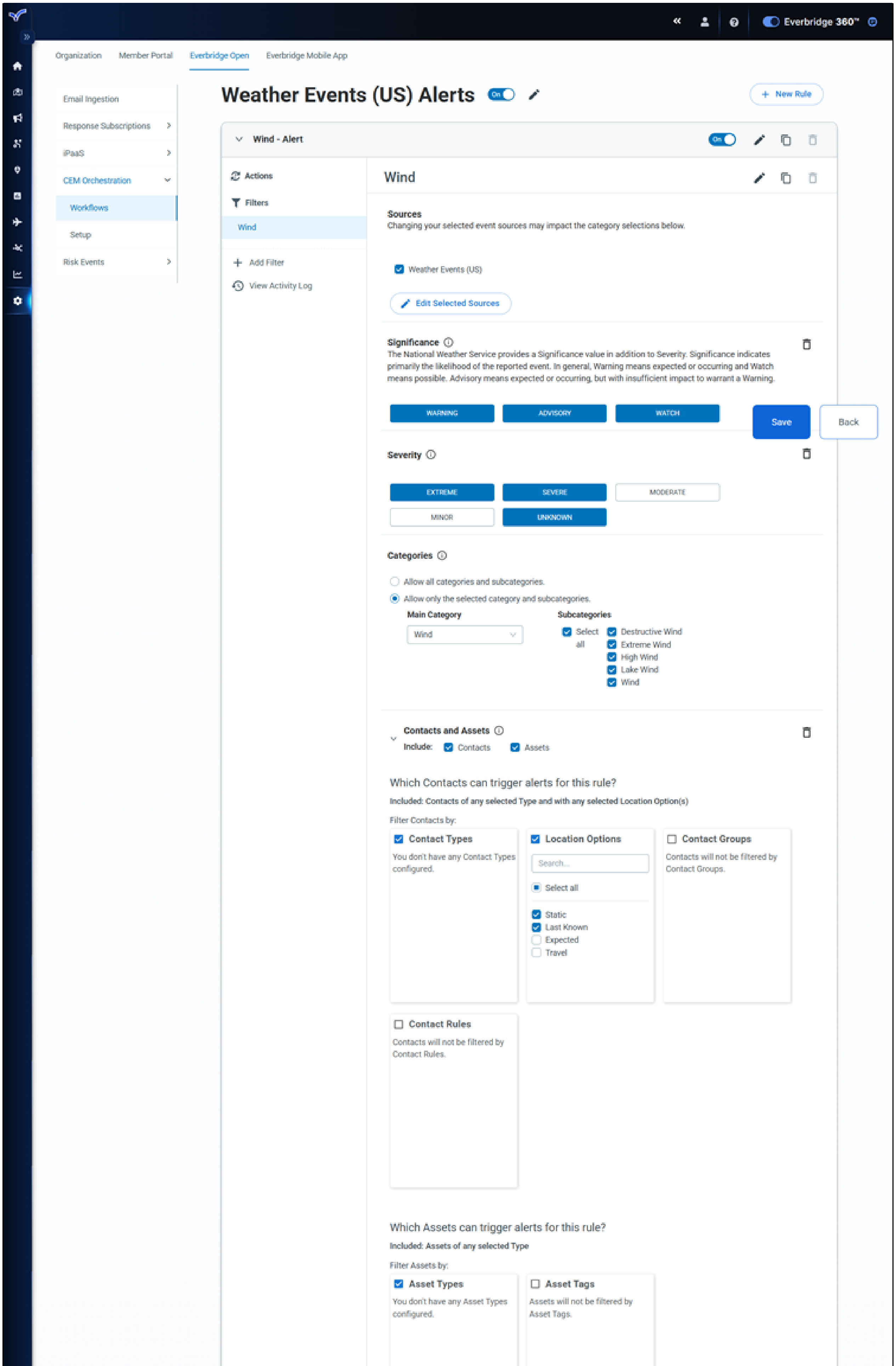
NOTE: To use different conditions, create a new **Filter**. To take different Actions, create a new **Rule**.

For example, the HAZMAT/Fire Workflow could contain an Alerting Rule. Within that Rule, you could build Filters for multiple use cases:

- Alert for all HAZMAT/Fire events—except wildfires—within one mile of any of my Assets.
- Alert for wildfires within 15 miles of any of my Assets except the "Camp" Asset Type.
- Alert for all wildfires within 20 miles of Camp Assets.

When all of the conditions for any of these Filters are met, the Rule's Action (create an Alert) is initiated.

This image shows the parts of a Workflow as they appear on the **Orchestration Workflows** page.


Everbridge 360™
Organization
Member Portal
Everbridge Open
Everbridge Mobile App
Email Ingestion
Response Subscriptions
iPaaS
CEM Orchestration
Workflows
Setup
Risk Events
Weather Events (US) Alerts
On
New Rule
Wind - Alert
On
Actions
Filters
Wind
Add Filter
View Activity Log
Wind
Sources
Changing your selected event sources may impact the category selections below.
Weather Events (US)
Edit Selected Sources
Significance
The National Weather Service provides a Significance value in addition to Severity. Significance indicates primarily the likelihood of the reported event. In general, Warning means expected or occurring and Watch means possible. Advisory means expected or occurring, but with insufficient impact to warrant a Warning.
WARNING
ADVISORY
WATCH
Save
Back
Severity
EXTREME
SEVERE
MODERATE
MINOR
UNKNOWN
Categories
Allow all categories and subcategories.
Allow only the selected category and subcategories.
Main Category
Wind
Subcategories
Select all
Destructive Wind
Extreme Wind
High Wind
Lake Wind
Wind
Contacts and Assets
Include:
Contacts
Assets
Which Contacts can trigger alerts for this rule?
Included: Contacts of any selected Type and with any selected Location Option(s)
Filter Contacts by:
Contact Types
You don't have any Contact Types configured.
Location Options
Search...
Select all
Static
Last Known
Expected
Travel
Contact Groups
Contacts will not be filtered by Contact Groups.
Contact Rules
Contacts will not be filtered by Contact Rules.
Which Assets can trigger alerts for this rule?
Included: Assets of any selected Type
Filter Assets by:
Asset Types
You don't have any Asset Types configured.
Asset Tags
Assets will not be filtered by Asset Tags.

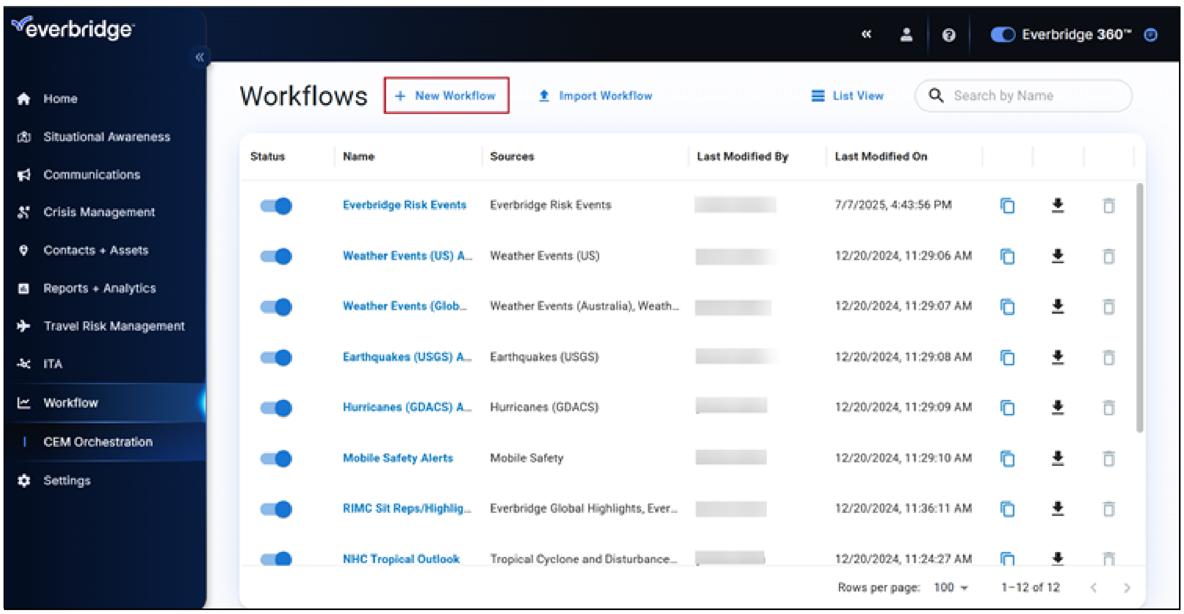
Creating Workflows

You can create or edit new Workflows on the **Workflows** page (**Workflow** > **CEM Orchestration** > **Workflow List**).

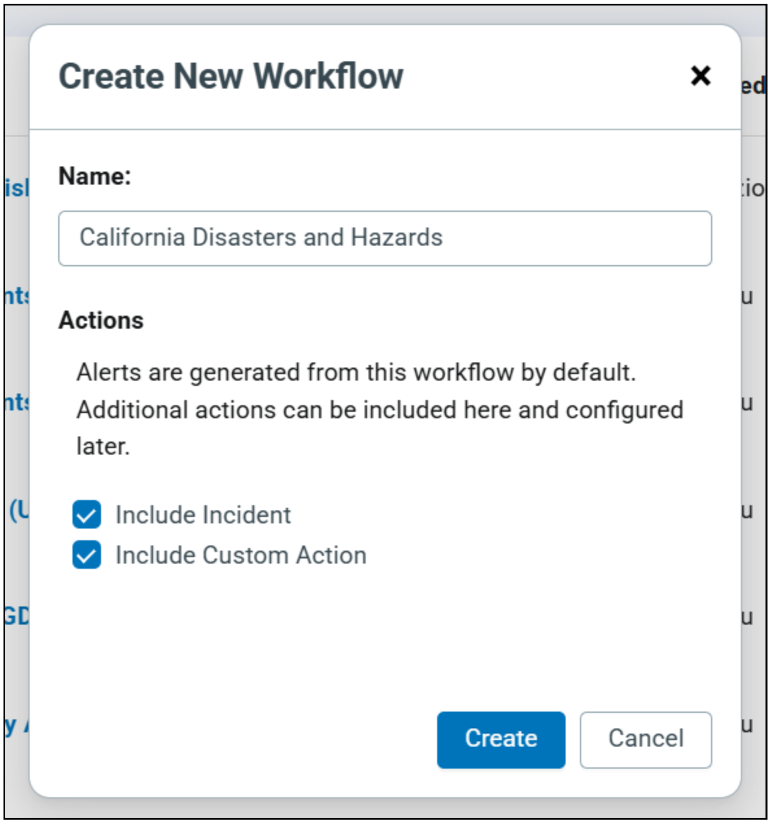
> **NOTE:** Creating custom Workflows is a Premium feature. See CEM Orchestration Limited Workflows for more information.

To create a Workflow:

1. Click **New Workflow**.



2. The **Create New Workflow** dialogue box appears. Enter a name for the Workflow in the **Name** field.



3. All Workflows can create Alerts. If you also want this Workflow to launch Incidents (to send Notifications to your contacts), select the **Include Incident** checkbox. See Setting Up Automated Incident Notifications for more details.
4. Select **Include Custom Action** if this Workflow needs to be configured to perform a specific Action. See Custom Actions for more information.
5. Click **Create**. The Workflow's Rule Configuration menu appears.

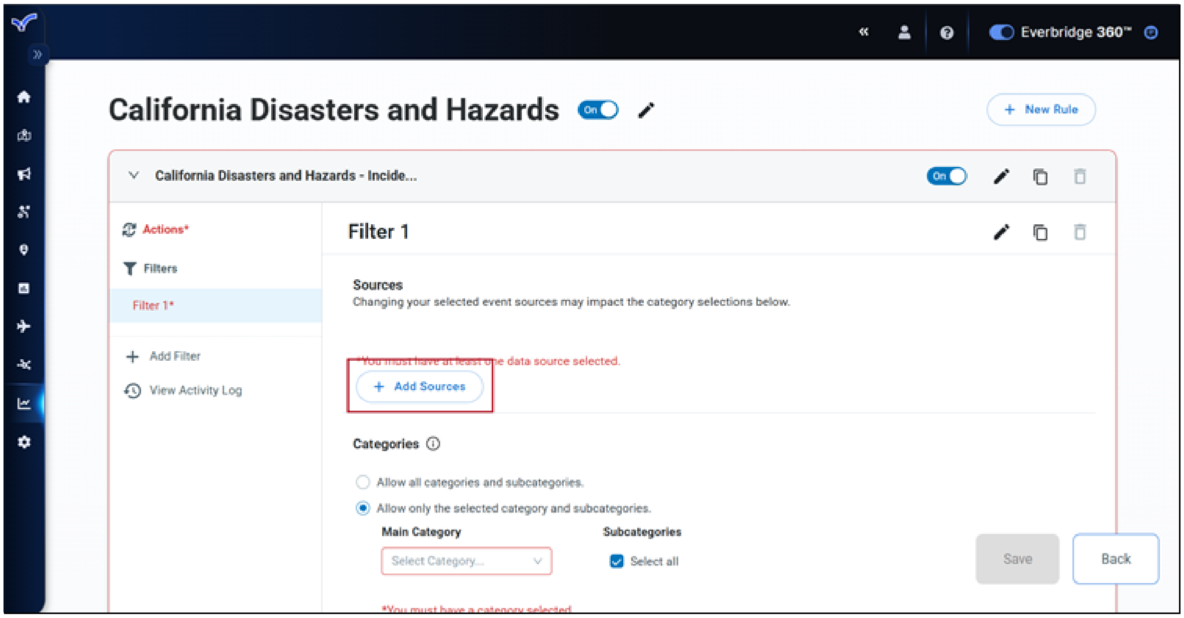
Configure Rules and Filters

After you create the Workflow, you must configure the Alerting Rules and Filters. CEM Orchestration adds one Rule by default. Each Rule can launch one set of Actions. To launch multiple sets of Actions, you can add more Alerting Rules.

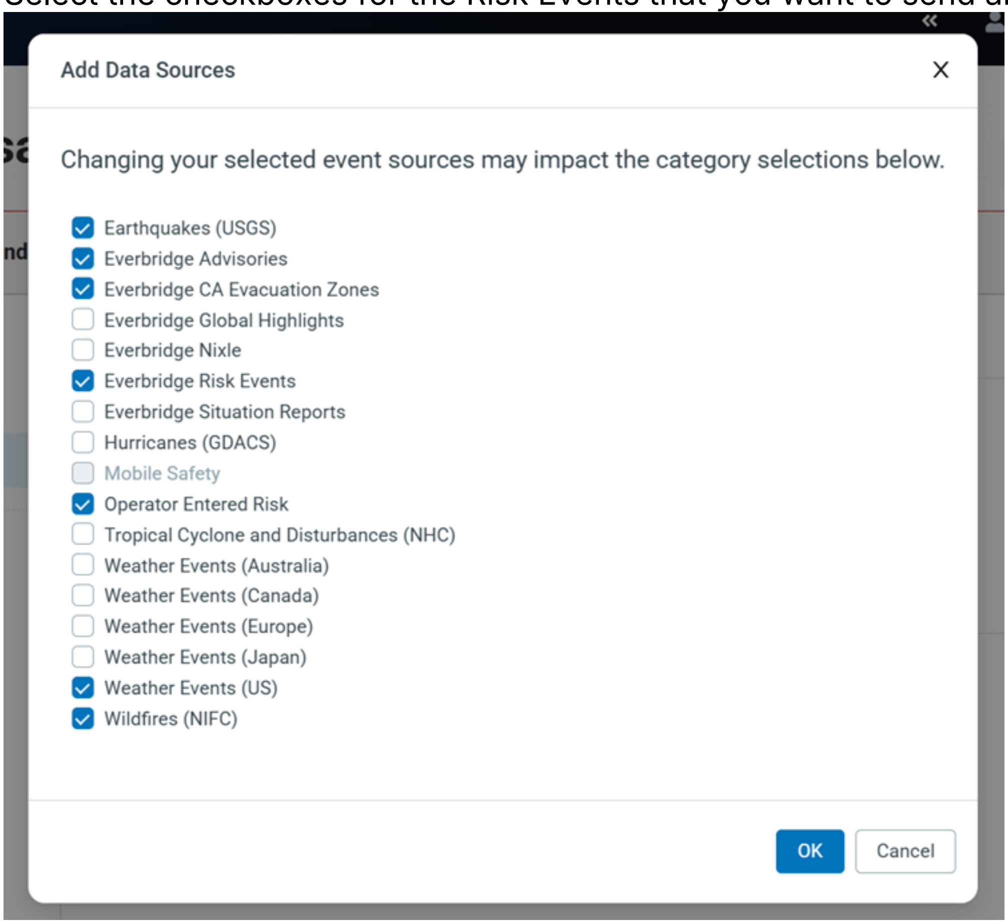
To configure a Rule:

1. Select one of its Filter Sets and change the settings described below. For examples of settings for a variety of use cases, see CEM Orchestration Use Case Examples.

2. Under the **Sources** heading, click **Add Sources**. Note that at least one Source must be added.

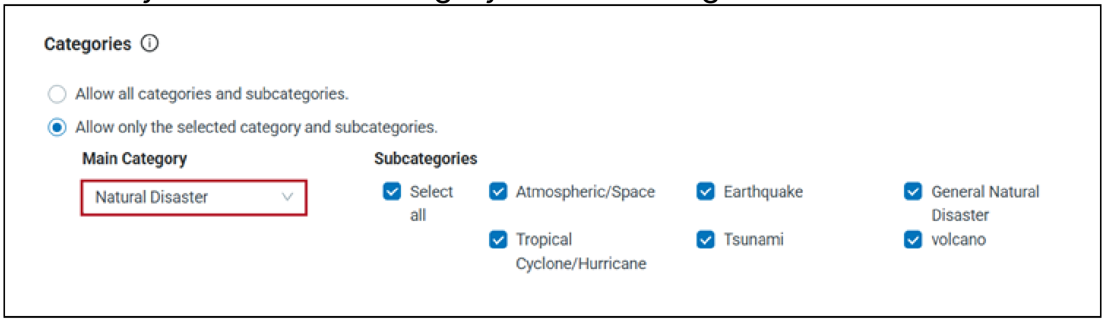


3. Select the checkboxes for the Risk Events that you want to send an Alert for.



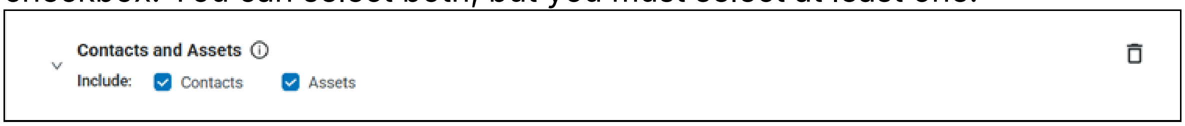
4. Choose the main Category and Subcategories by selecting either:
    - All all Categories and Subcategories

- Allow only the selected Category and Subcategories

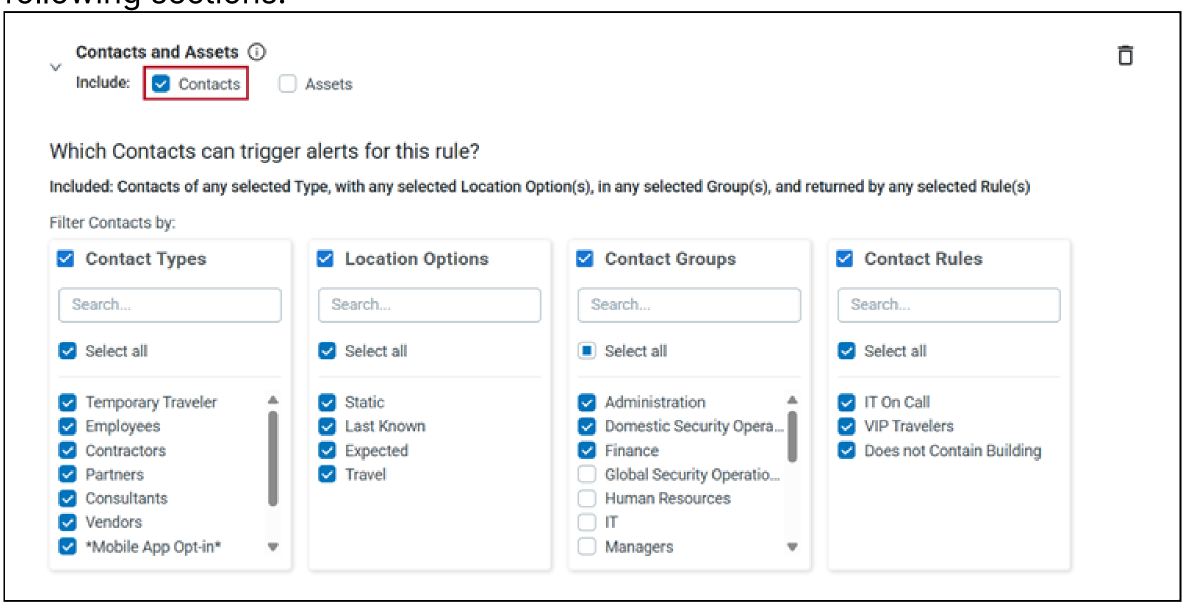


    - **NOTE**: The dropdown list only includes categories that are valid for the selected Sources.

5. Under the **Contacts and Assets** heading, select the **Contacts or Assets** checkbox. You can select both, but you must select at least one.



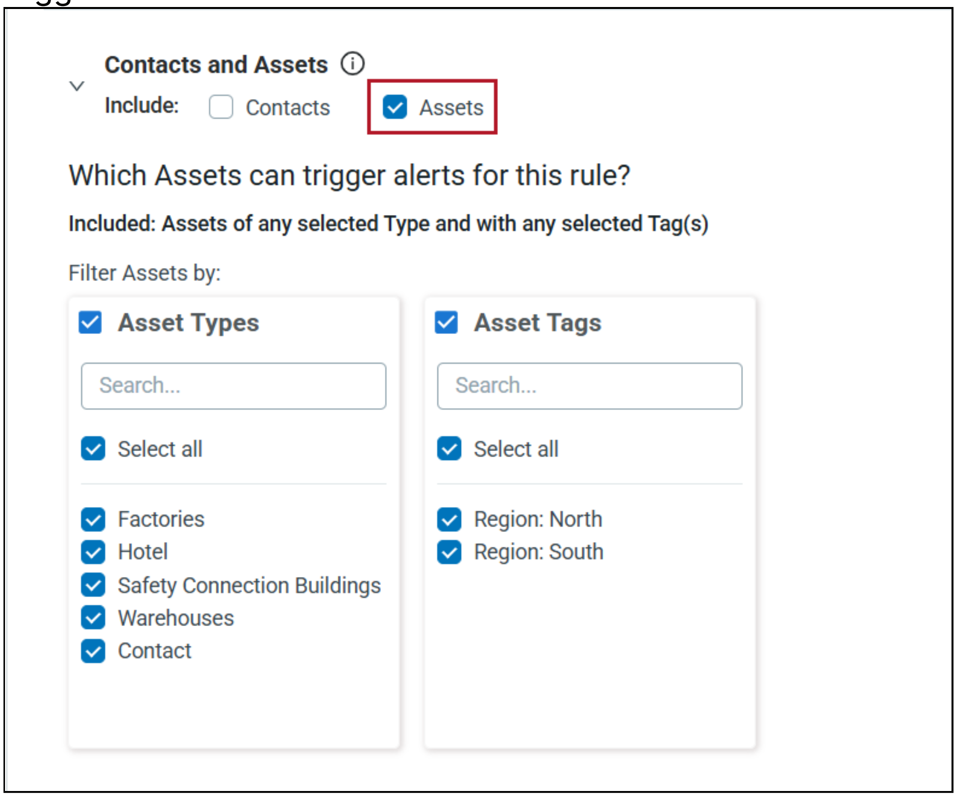
6. If you selected **Contacts**, select the Contacts who will receive Alerts in the following sections:



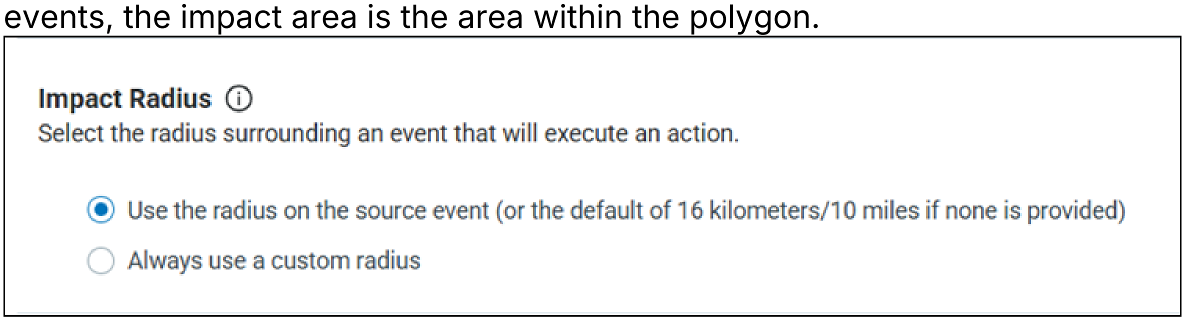
- **Contact Types** - From the list of Contact Types, select the types you want to Alert on, or **Select All** to alert for Contacts of all types.
- **Location Options** - Contains the Contacts' locations.
    - **Static**: For example, a contact’s home or office.
    - **Last Known**: A location where the Contact reported their location by (for example) swiping their ID into a building security system, checking in, or initiating an SOS from the Everbridge Mobile App or Everbridge 360 Mobile App.
    - **Expected**: For example, a temporary assignment.
    - **Travel**: A location associated with a Travel Itinerary.

- **Contact Groups** - From the list, select the Groups you want to alert or **Select all** to alert all Contacts, including those not in Groups.
- **Contact Rules** - Select a Contact Rule to leverage existing dynamic Contact Rules, which allows fine-tuning of Alerting and automated response to Risk Events based on Contact Attributes.

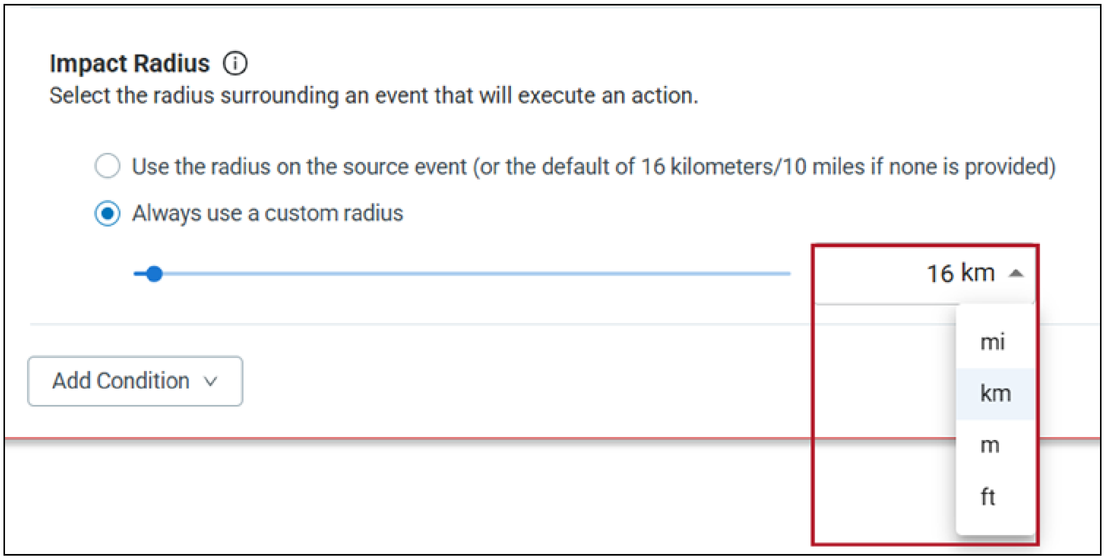
7. If you selected **Assets**, select the Asset Types and Tags that you want to trigger Alerts for this Rule.



8. Select the **Impact Radius** to send an Alert when a Contact is within a certain number of kilometers or miles of a Risk Event. The larger the Impact Radius, the more Alerts and Incidents may be generated as a result. The radius applies only when the event location is a point on the map. For polygon events, the impact area is the area within the polygon.

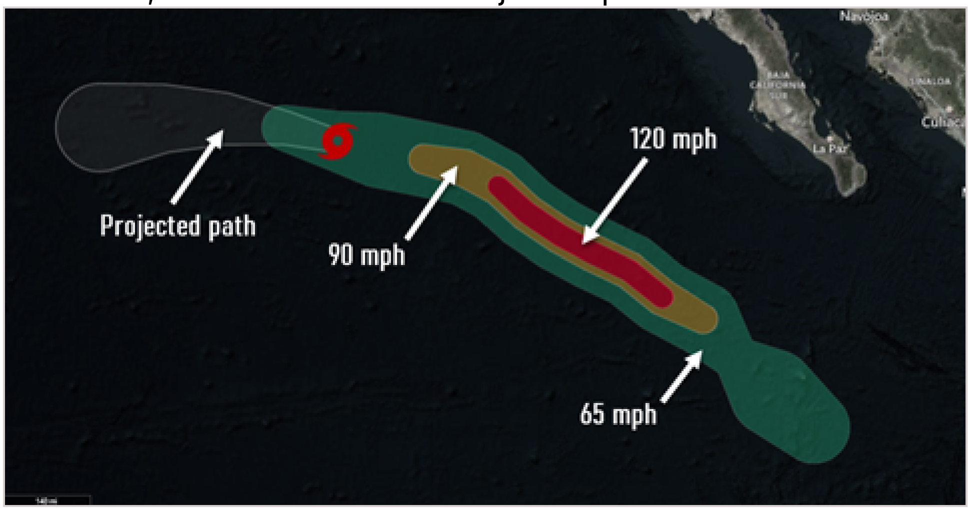


- **NOTE**: Optionally, select **Always use a custom radius** and specify the desired radius distance.



9. You can add several additional Alerting conditions to the Filter based on the selected Sources. Scroll down to the **Add Condition** menu at the bottom of the page, and select one or more of the following:
   - **Severity:** This is the Severity of the Risk Event as reported by the Risk Data Source (e.g., National Weather Service, Everbridge RIMC (Risk Intelligence Monitoring Center). Note that if this value isn't specified, then all Severities will apply.
   - **Time Frame**: By default, an Alert only results when Assets or Contacts are in the impact area between the start and end of the Risk Event. Use this setting to extend the impact duration by adding time before or after the event start time.
   - **Magnitude, Wind Swath, Significance**: These are specialized conditions that each apply only to a single Data Source:
     - **Magnitude**: Magnitude is a measure of earthquake intensity that is valid only for earthquakes reported by the Earthquakes (USGS) Data Source. For these events, you can use Magnitude in place of or in addition to Severity. Use the Magnitude in Filter Sets where Earthquakes (USGS) is the only Data Source; If you include another Data Source in the same Filter Set, the Magnitude condition will not be available. Use the **Minimum** and **Maximum** fields or the slider to select a Magnitude value between 2.0 and 10.0.
     - **Hurricane Wind Swath**: Wind swaths are geographic areas experiencing hurricane winds of different speeds. You should use Wind Swath in place of Severity for hurricanes reported by the Hurricanes (GDACS) Data Source. Use the Wind Swath condition in filter sets where Hurricanes (GDACS) is the only Data Source; If you include another Data Source in the same Filter Set, the Wind

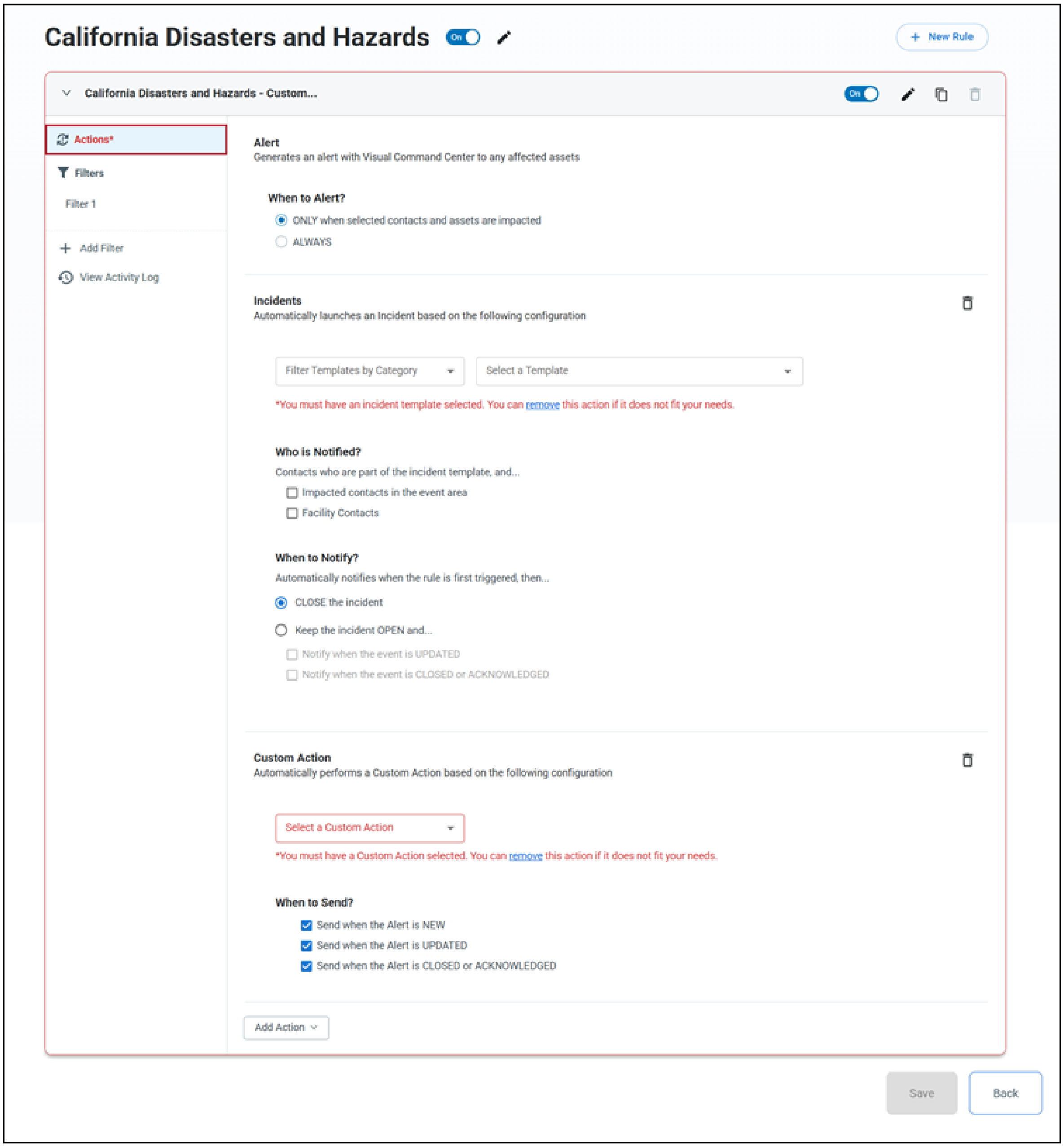
Swath condition will not be available. To get Alerts for Assets only in the area experiencing the most intense wind, choose 120mph as the value of the Wind Swath condition. To get Alerts for Assets in a wider area, choose 90 mph or 60 mph as the minimum wind speed. Or, to get Alerts for Assets in the projected path of a hurricane, choose the value "Projected path of hurricane."



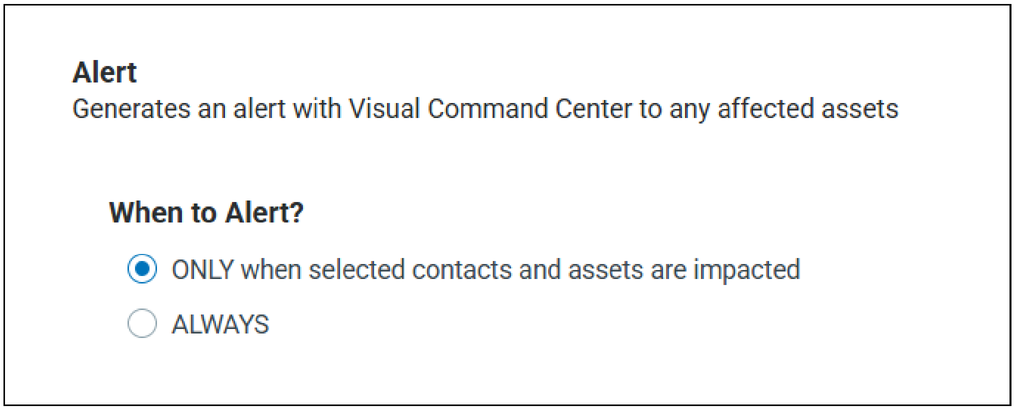
- **Significance**: A measure of probability and Severity used by the US National Weather Service (NWS). Consider using Significance in place of or in addition to Severity for events in the **Weather Events (US)** feed. Use this condition in Filter Sets where Weather Events (US) is the only Data Source. If you include another Data Source in the same Filter Set, the Significance condition will not be available. Significance values are:
  - **Watches** indicate conditions are favorable for a significant weather event to develop.
  - **Warnings** indicate hazardous conditions are expected and you may have to take action, such as delaying travel, staying indoors, dressing for extreme weather, or evacuating.
  - **Advisories** indicate a type of weather is expected that is not severe enough to merit a warning, but which may cause significant inconvenience or make travel hazardous.

10. When you have completed defining the conditions in a Filter, you can add additional Filters until all of your use cases in the current Workflow are covered. See Adding More Filter Sets to a Rule for more details.
11. Edit the Rule's Action(s). Remember that when the conditions are met for any Filter in the Rule, the defined Actions are taken. To define Actions, click the

Action tab.



12. In the **Alert** section, specify when Alerts should be generated in Visual Command Center in relation to affected Assets.

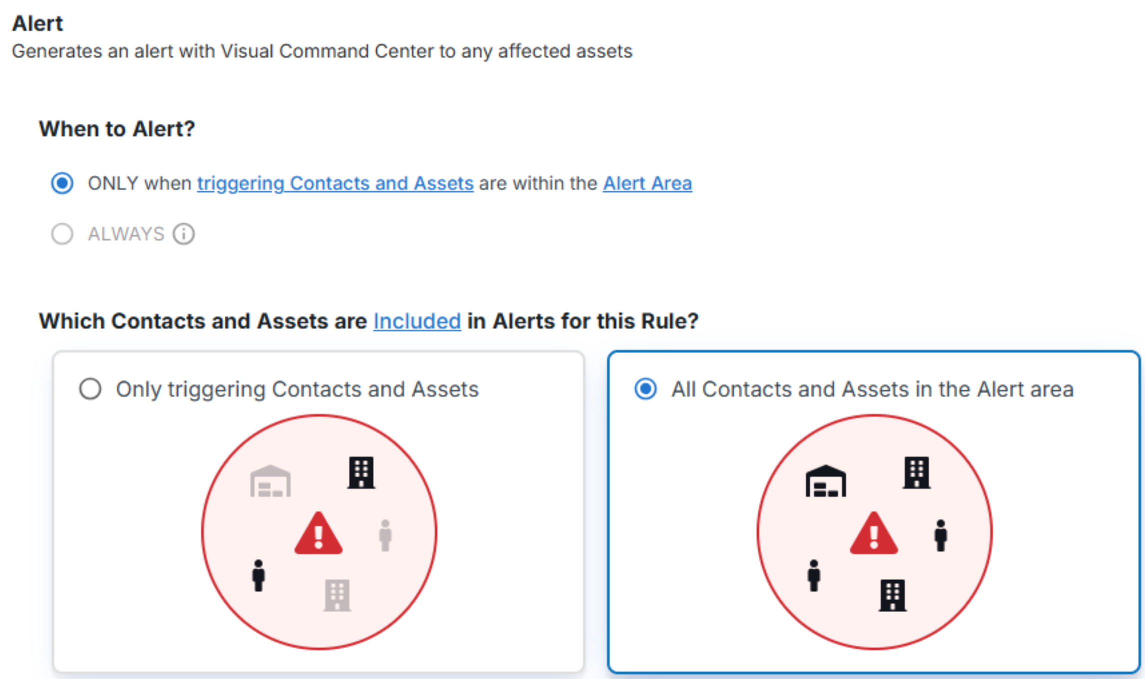


Select one of the following options for **When to Alert?**:

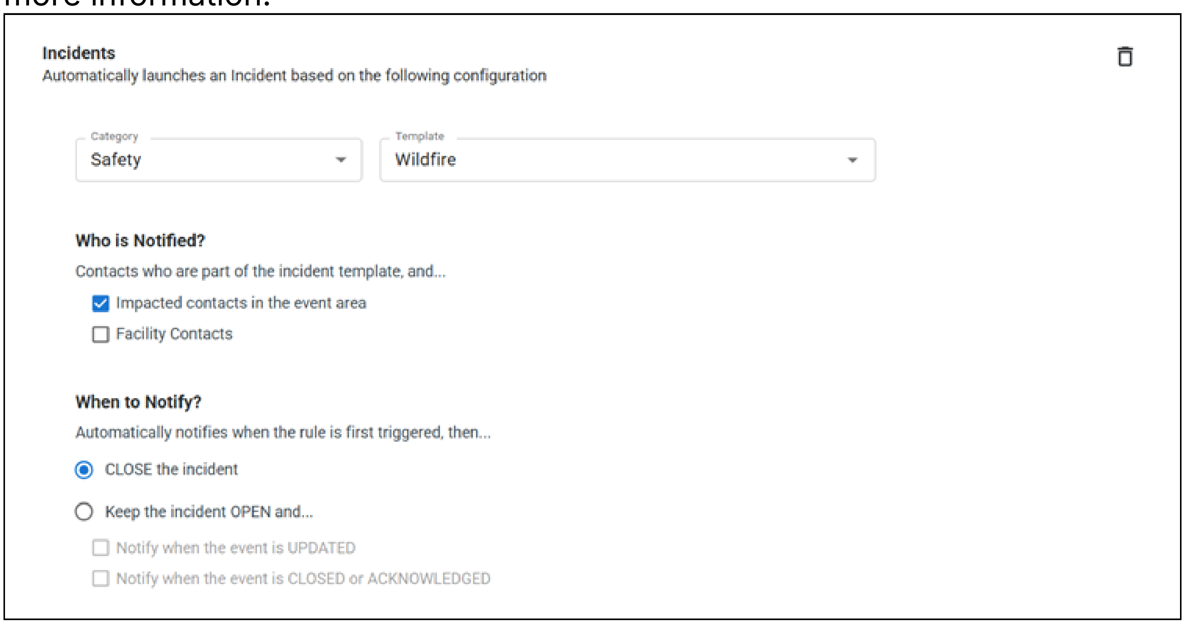
- **ONLY when selected contacts and assets are impacted** - Orchestration creates Alerts only when your selected Contacts or Assets may be affected. This is the default option.
- **ALWAYS** - Use this option if you want to enable Alerts even for Risk Events that do not affect your Contacts or Assets.
    - Note that selecting ALWAYS may result in a high volume of Alerts.
    - This checkbox can't be selected if any of the Filters in this Rule include the Self Service or Dataminr Risk Sources, as the volume of events in these Sources can create too much noise.

13. Organizations that have enabled the **Which Contacts and Assets are included in Alerts?** option from **CEM Orchestration** > **Setup** will instead see an additional modal on the **Actions** tab that allows them to specify which Contacts and Assets are included as "Affected" when an Alert is triggered. See Configuring Affected Contacts and Assets in CEM Alerts for more

details.



14. In the **Incidents** section, configure if you want to launch an Incident when the Alerting Rules are met. See Setting Up Automated Incident Notifications for more information.



15. If the **Include Custom Action** box was checked on the **Create Workflow** modal, adding a Custom Action to at least one Rule is required to save the Workflow. If that box wasn't checked, a Custom Action can still be added by clicking **Add Action** at the bottom. See Adding Custom Actions to CEM Orchestration Workflows for more information.
16. Save the Rule.

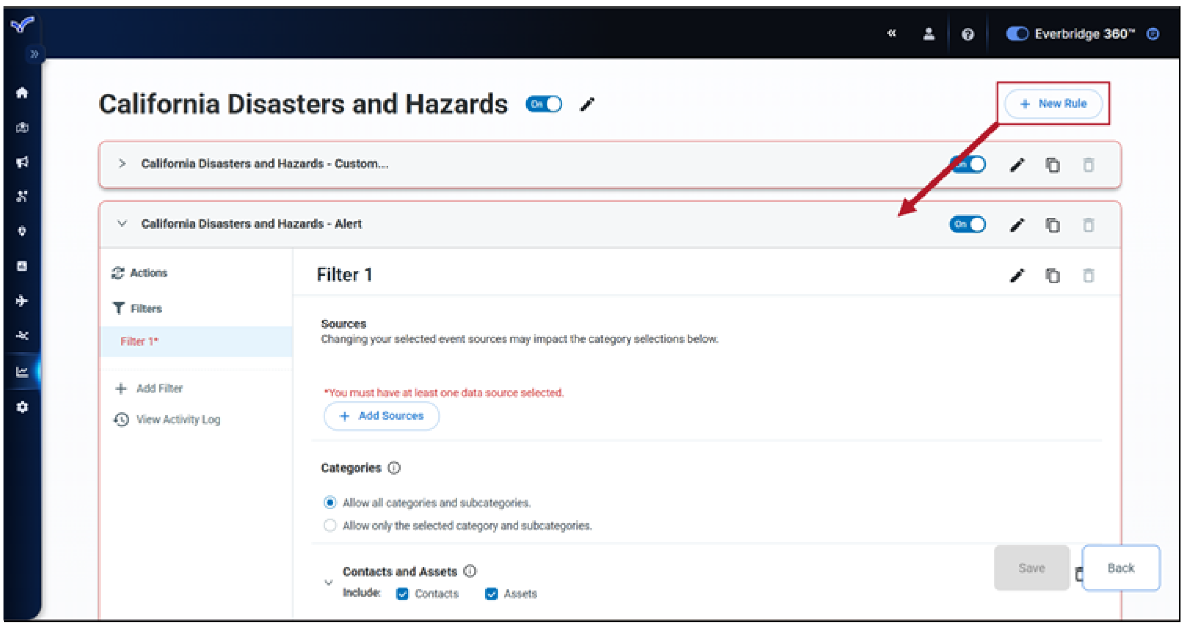
17. Add as many Rules as needed using the steps above, then save the Workflow.

> **IMPORTANT:** You **must** use a different Incident template for each instance of the **Launch Incident** action that you add to the Workflow Rule.

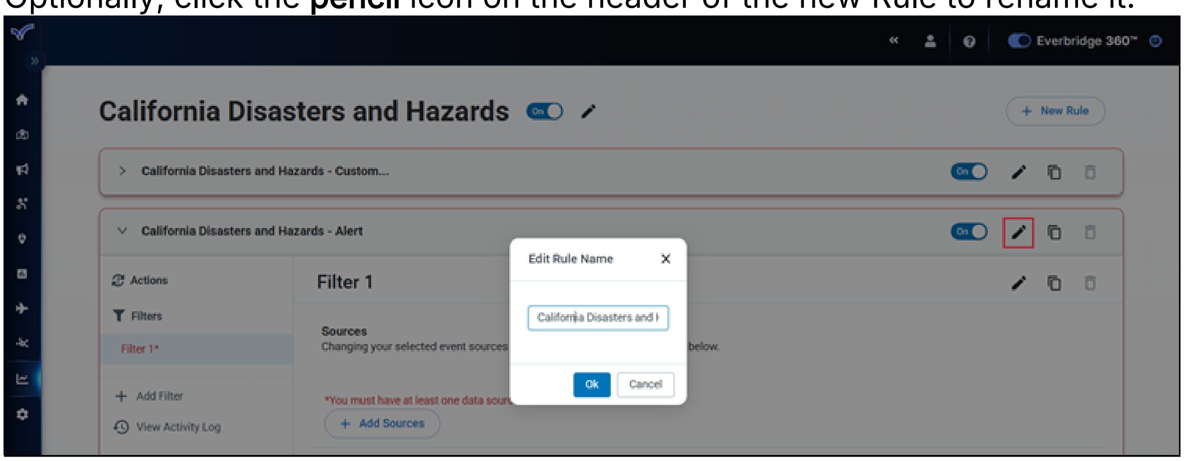
Adding More Rules to a Workflow

You can add additional Rules to a Workflow. Each Rule will have its own set of Actions. To add Rules:

1. Select a Workflow.
2. Click **New Rule** in the top-right corner. A new Rule page with a single Filter Set is created.



3. Optionally, click the **pencil** icon on the header of the new Rule to rename it.

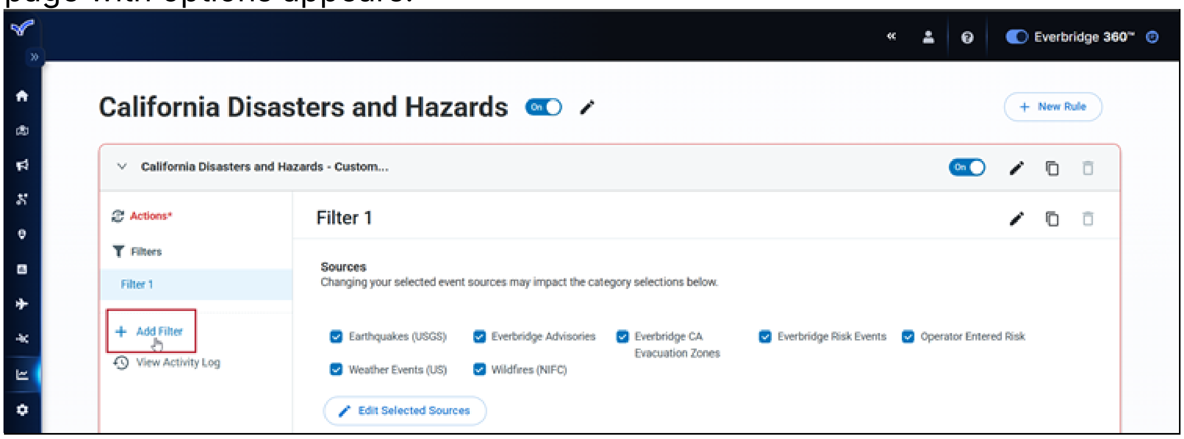


Depending on the Risk Event Feed, some Filters will appear while others will not. For example, the **Wind Swath** Filter would only appear for weather events, such as a Hurricane.

Adding More Filter Sets to a Rule

You can add additional Filter Sets to a Rule. To do this:

1. On the left-hand side of the page under **Filters**, click **Add Filter**. A new Filter page with options appears.



2. Follow the steps outlined above in Configure Rules and Filters to configure the new Filter Set.

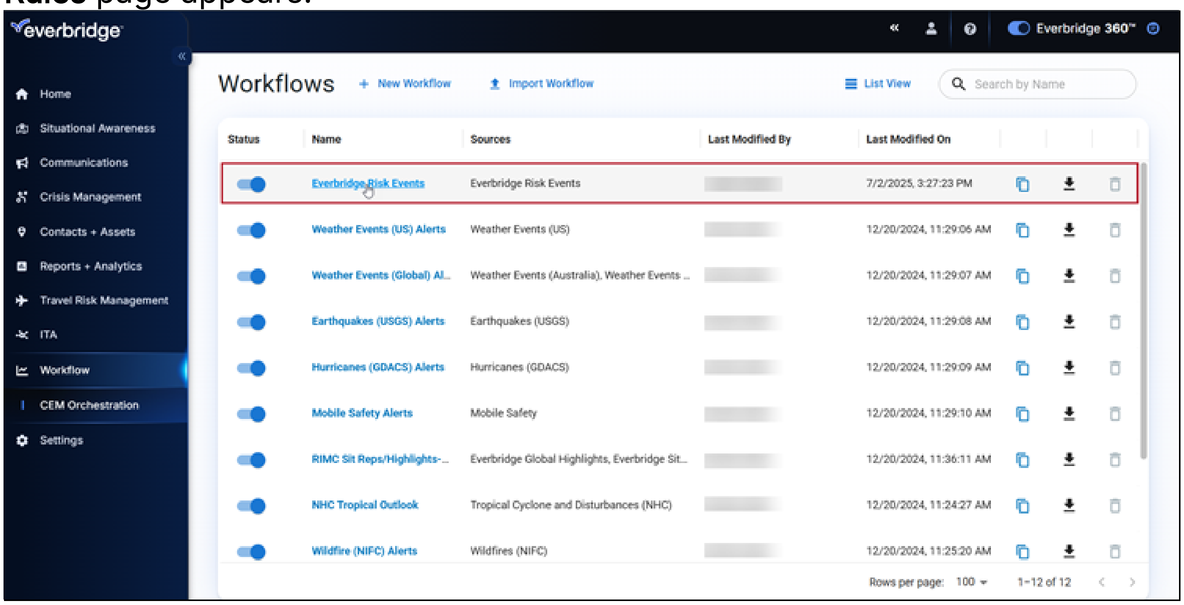
Editing a Workflow

Both Custom and preconfigured Workflows can be edited.

NOTE: Editing a Workflow or Rule is available for Premium customers. See CEM Orchestration Limited Workflows for more information.

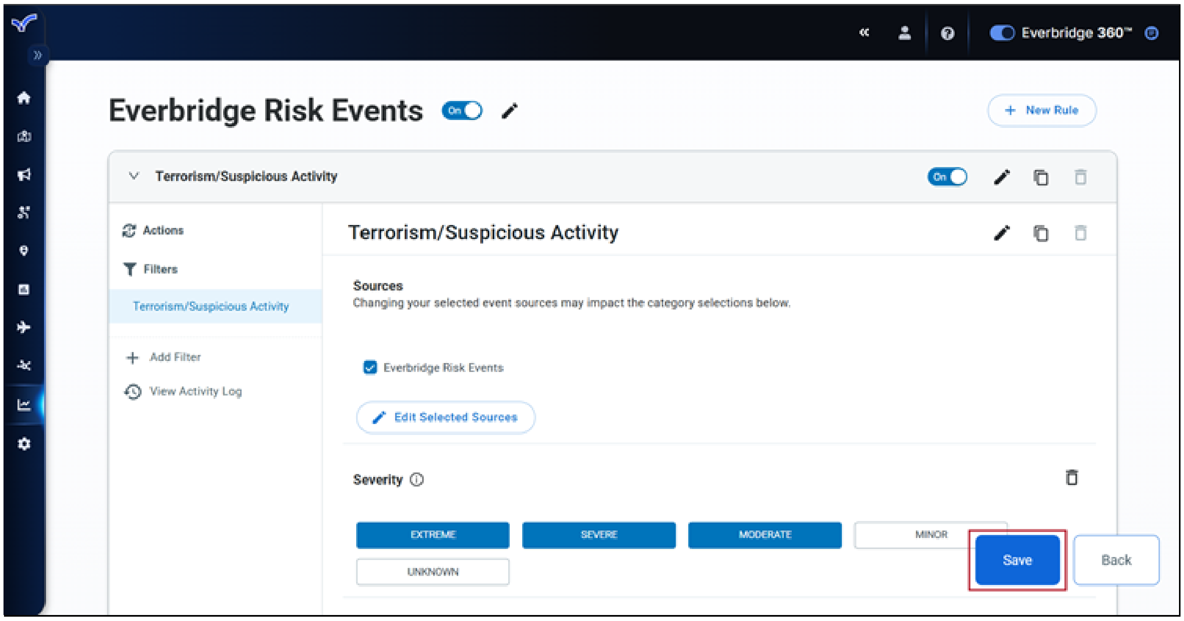
To edit a Workflow:

1. Locate the Workflow that you want to edit and click its name. The **Workflow Rules** page appears.



2. Make any necessary changes.

3. Click **Save**.


Everbridge 360™
Everbridge Risk Events
On
New Rule
Terrorism/Suspicious Activity
Actions
Filters
Terrorism/Suspicious Activity
Add Filter
View Activity Log
Terrorism/Suspicious Activity
Sources
Changing your selected event sources may impact the category selections below.
Everbridge Risk Events
Edit Selected Sources
Severity
EXTREME
SEVERE
MODERATE
MINOR
UNKNOWN
Save
Back

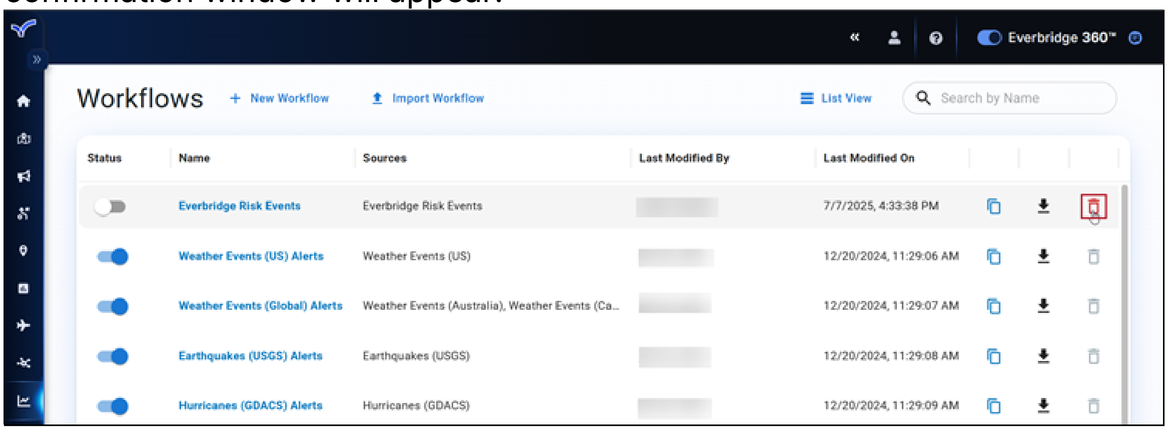
Deleting a Workflow

Both preconfigured and custom Workflows can be deleted as needed.

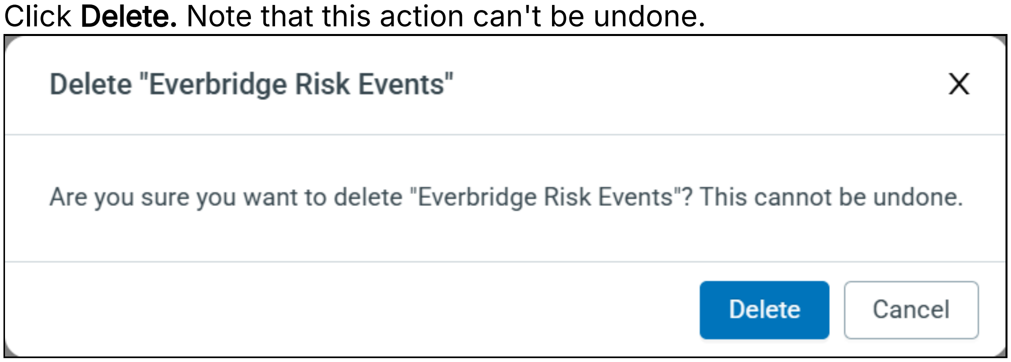
> **NOTE:** Deleting a Workflow is available for Premium customers. See [CEM Orchestration Limited Workflows]() for more information.

To delete a Workflow:

1. Locate the Workflow that you want to delete and click the **Trash** icon. A confirmation window will appear.



2. Click **Delete.** Note that this action can't be undone.



> **NOTE:** Enabled Workflows cannot be deleted. In order to delete a Workflow, first disable it.

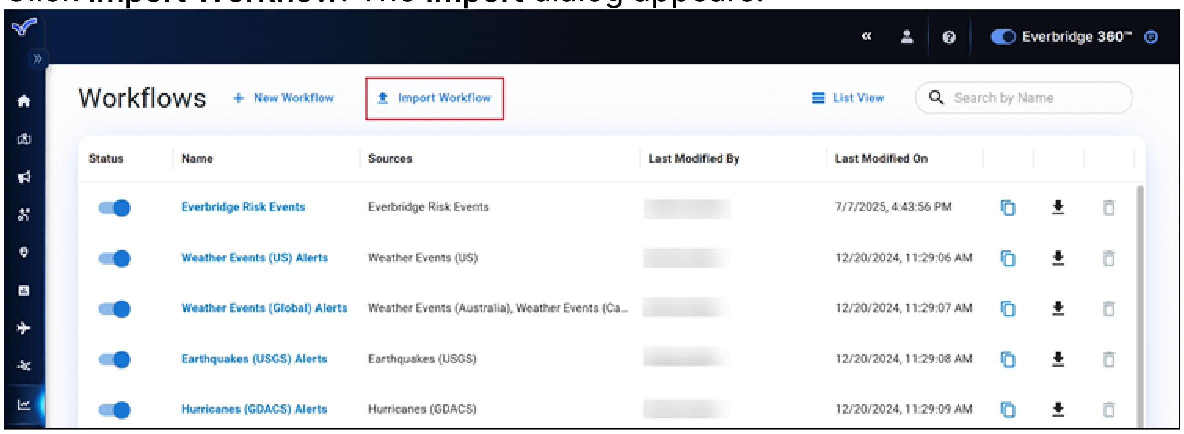
Importing a Workflow

You can use the **Import** feature to import an existing Workflow, such as a Workflow from a test Organization.

NOTE: Importing Workflows is available for Premium customers. See CEM Orchestration Limited Workflows for more information.

To import an existing Workflow into your CEM Orchestration Workflows:

1. Click **Import Workflow**. The **Import** dialog appears.



2. Click **Choose File**. Your system's file manager appears.
3. Select the file that contains the Workflow.
4. Click **Import**.
5. An onscreen message will list any Risk Sources, Contact Types, and Contact Groups that are in the imported Workflow but not in the destination Organization. These will not be included in the import.
6. **Save** the Workflow.

Settings that are retained from Imported Workflows include:

- Workflow, Rule, and Filter names
- Workflow and Rule statuses (enabled/disabled)
- Risk Sources (if they are available in the destination Organization)
- Categories and subcategories
- Impact Radius
- Most conditions, including Severity, Time Frame, Magnitude, Significance, Wind Swath
- Asset Types (if they are available in the destination Organization)
- Contact Location Options

Enabling and Disabling Workflows and Rules

Workflows and Rules each have On/Off controls; this lets you edit a Workflow or Rule while it is disabled and not generating Alerts.

When a Workflow is **Off**, all of its Rules are Off and none of the Actions in any Rule are taken.

When you toggle a disabled Workflow **On**, all of its Rules are subsequently enabled. If you want some Rules enabled and others disabled, use the On/Off toggle for each Rule.

Workflows that have some Rules enabled will appear as toggled **On**.

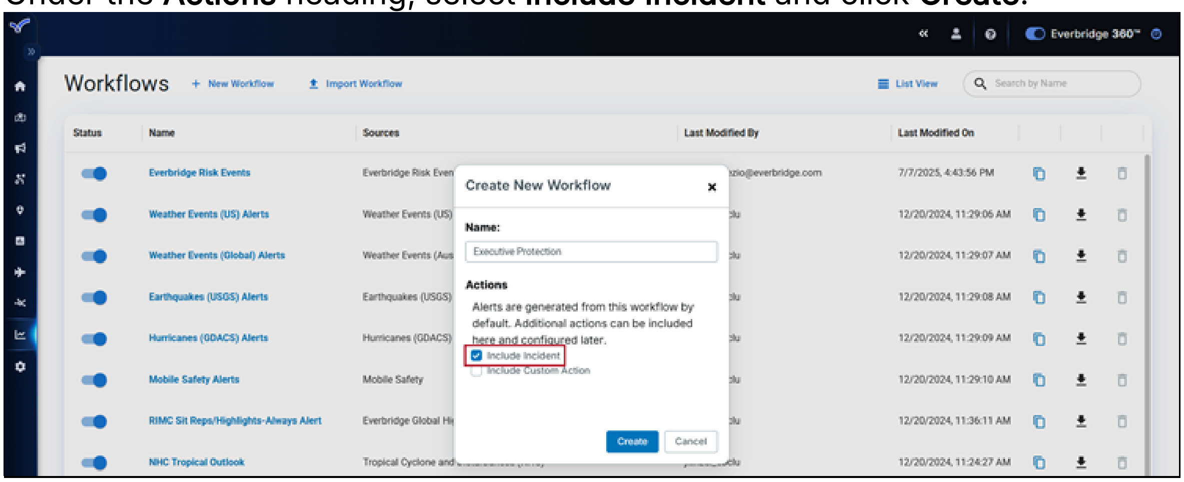
Setting Up Automated Incident Notifications

CEM Orchestration allows you to set up **automated Incident Notifications** for Risk Events that impact your Assets and Contacts. This can be done based on an Asset Type, or on a Contact’s Static, Last Known, Expected, or Travel location and allows lets users notify Contacts who may be affected by a Risk Event, and teams who are responsible for the Contact's safety.

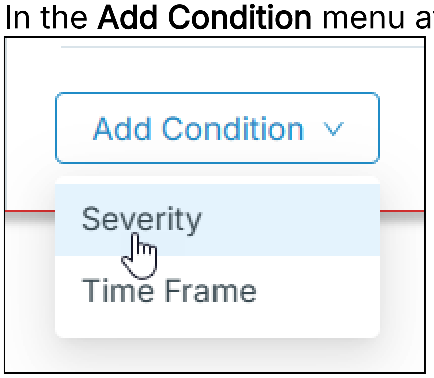
In this example, we’ll configure Orchestration to automatically notify an executive safety team when a potential terrorist event occurs at a location where an executive has used the Everbridge 360 Mobile App to check in.

To create an automated Incident Notification:

1. Click **New Workflow**. The **Create New Workflow** dialog appears.
2. Type a name for the Workflow in the **Workflow Name** field. For example, Executive Protection.
3. Under the **Actions** heading, select **Include Incident** and click **Create**.

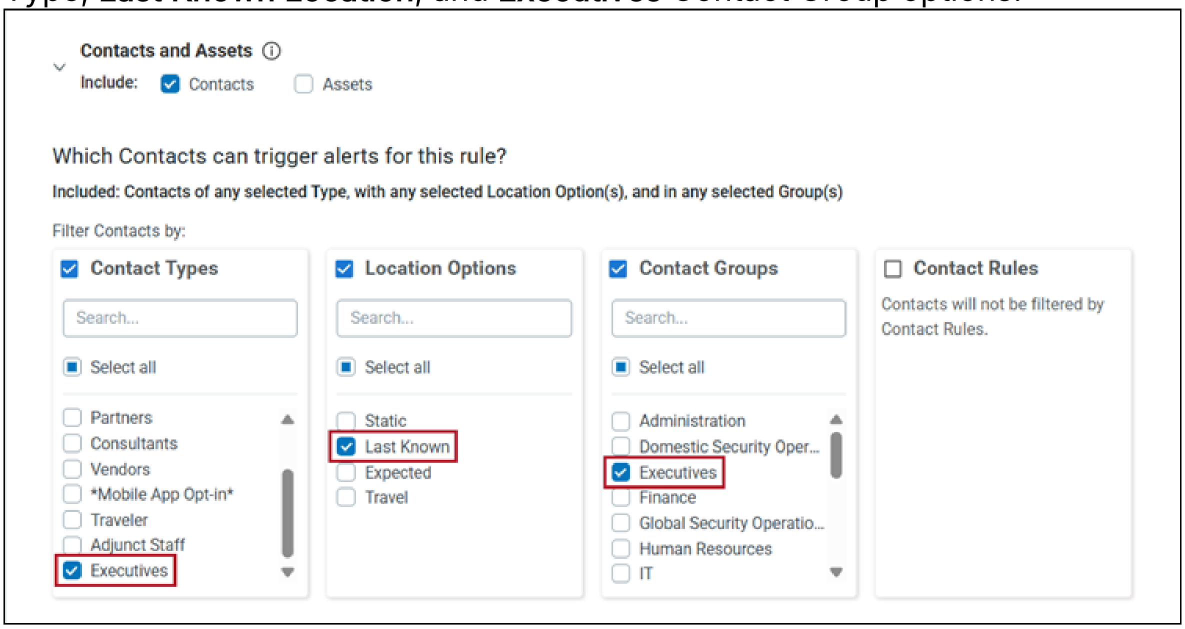


4. In the Filter, under **Sources** and **Category**, select the Risk Sources and Risk Events that you want to create Alerts for.
5. In the **Add Condition** menu at the bottom of the page, select **Severity**.

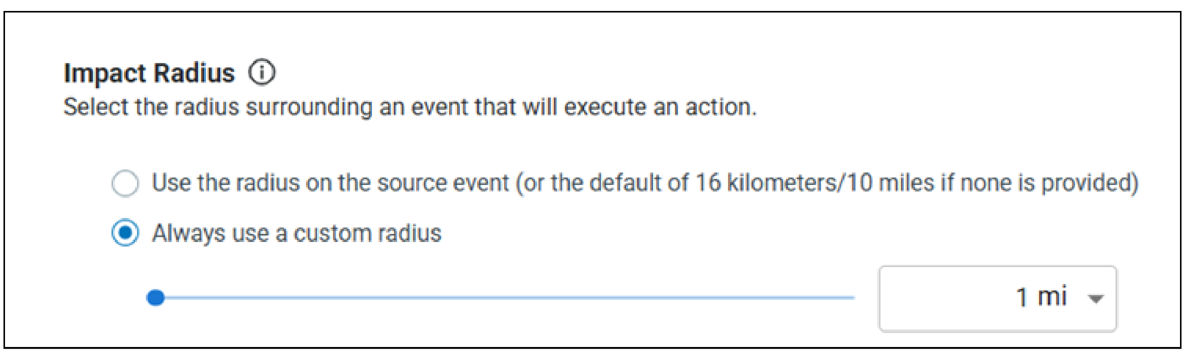


6. Select the **Severe** and **Extreme** options.

7. Under the **Contacts and Assets** heading, select the **Contacts** checkbox.
8. Under the **Which Contacts can trigger alerts for this rule?**, select the checkboxes to specify the Contact Groups, Contact Types, Contact Rules, and location options for the Alert. For example, select the **Executives** Contact Type, **Last Known Location**, and **Executives** Contact Group options.

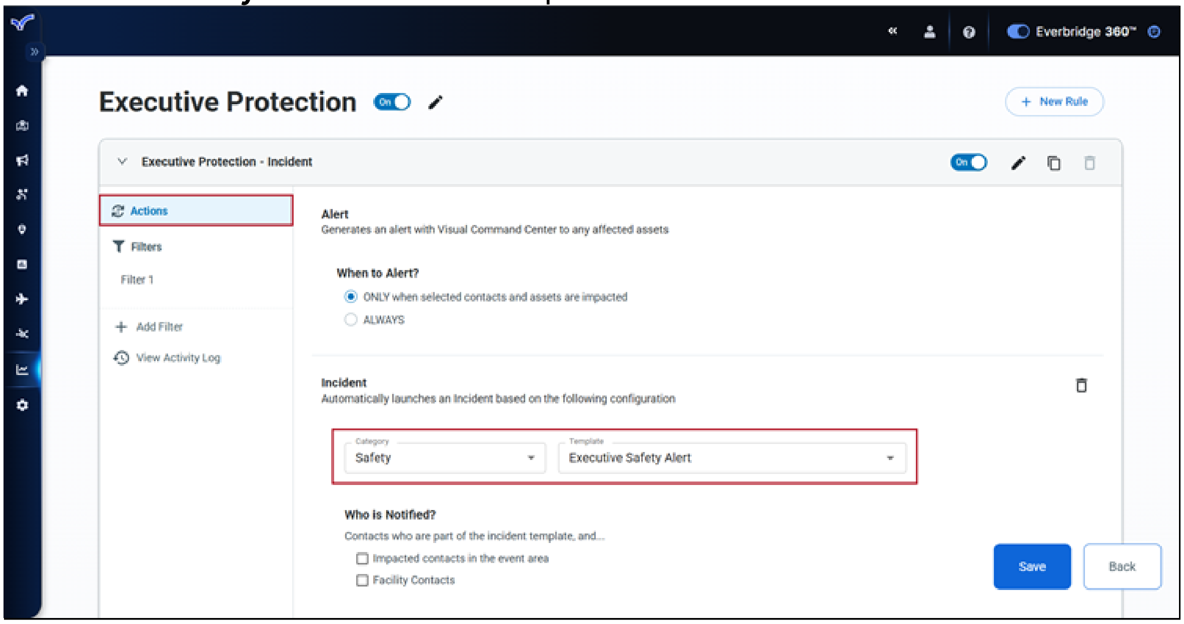


9. Select the **Impact Radius** to send an Alert when a Contact is within a certain number of kilometers of an event.

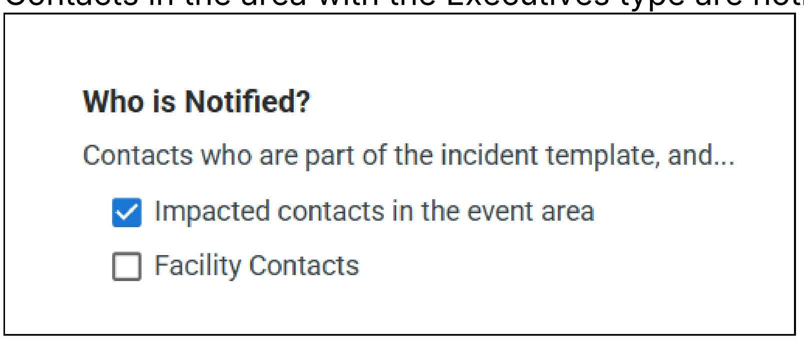


10. Click the **Action** tab and select the desired Incident template. For example, select the **Safety Communications** Incident Type and then select the

Executive Safety Alert Incident Template.

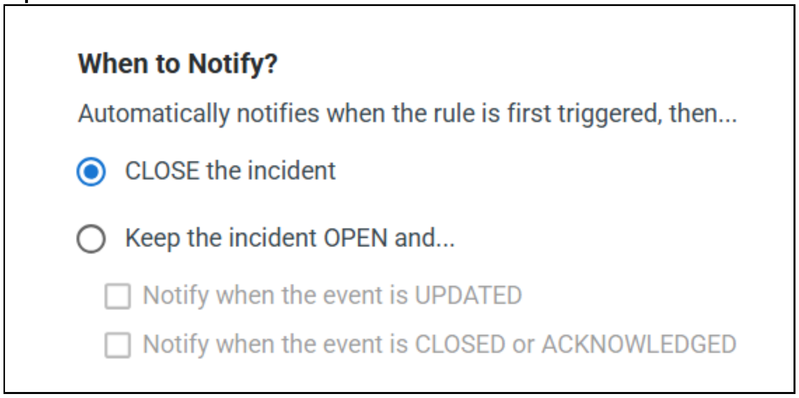


11. Optionally, select the checkboxes under **Who is Notified?** to determine how the Incident should function. When Orchestration launches an Incident, Notifications are sent to Contacts specified in the Incident template. If you also want to notify Contacts in the Alert area, select the option AND any people in the event area.
    If you have selected any Contact options (such as Contact Type, Location Type, or Groups) in your Filters, only Contacts who match the selected options are notified. So, for example, if you have selected the Contact Type **Executives** in your Filter, and chosen to notify Contacts in the Alert area, only Contacts in the area with the Executives type are notified.



12. Under **When to Notify?**, configure what automatically happens with the Incident when the Rule is first triggered. By default, when an Incident is launched, Notifications are sent and the Incident is then closed automatically. To keep the Incident open and send subsequent Notifications, select **Notify when the event is UPDATED** and/or **Notify when the event is CLOSED or ACKNOWLEDGED**. When either of these is selected, the Incident remains

open until the Risk Event is closed or the Alert is acknowledged.



13. You can add multiple Incident Actions to a Rule, so repeat the steps above for each Action that you want to add to a Workflow Rule. For example, create one Incident Action to notify Contacts in an Alert area of the potential threat and another, with different content, to notify security personnel of the threat and the closest Assets. You must use a different Incident template for each instance of the **Launch Incident** Action that you add to the Workflow rule.
14. Click **Save**.

Custom Actions

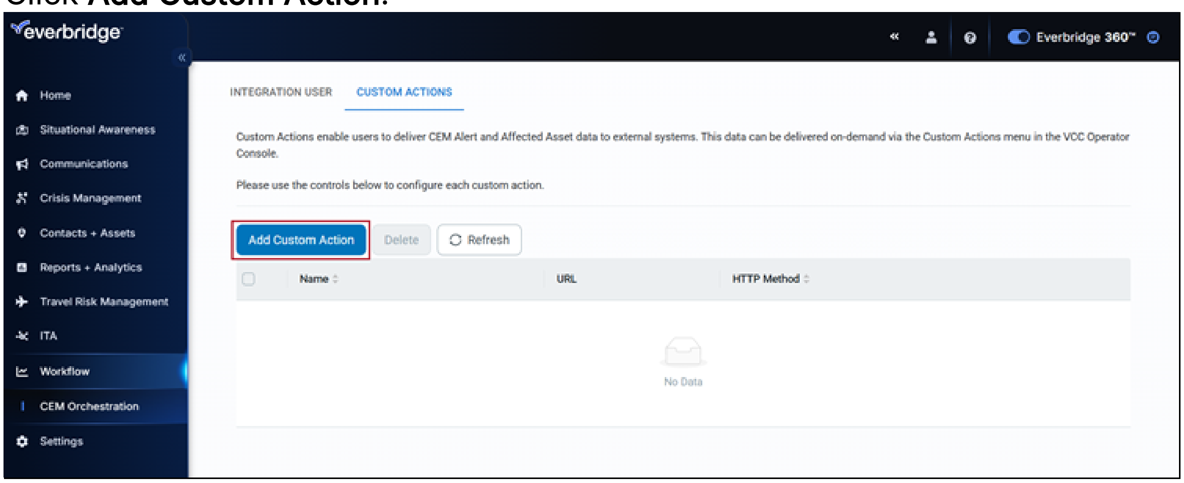
Alert Custom Actions allow operators to share the **Alert Details** from CEM Orchestration Workflows, Visual Command Center, and Alert Management to a third-party service, such as an Incident or Case Management service. They can be created and managed at the Organization level from **Workflow** > **CEM Orchestration** > **Setup**.

> **NOTE:** This page can also be found in the Everbridge Classic UI from **Settings** > **Everbridge Open** > **CEM Orchestration** > **Setup** > **Custom Actions** tab.

Creating a Custom Action

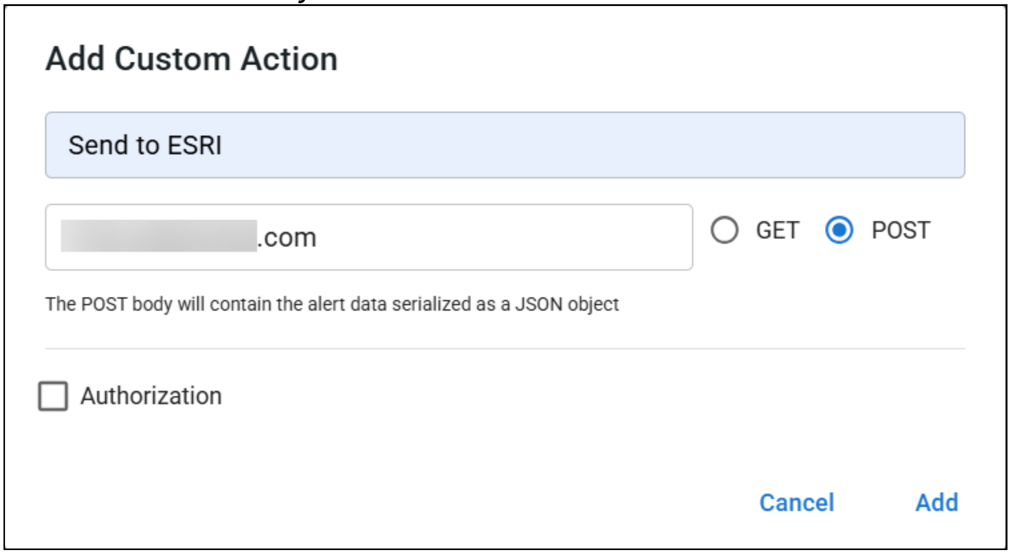
To create a new Custom Action:

1. Click **Add Custom Action.**



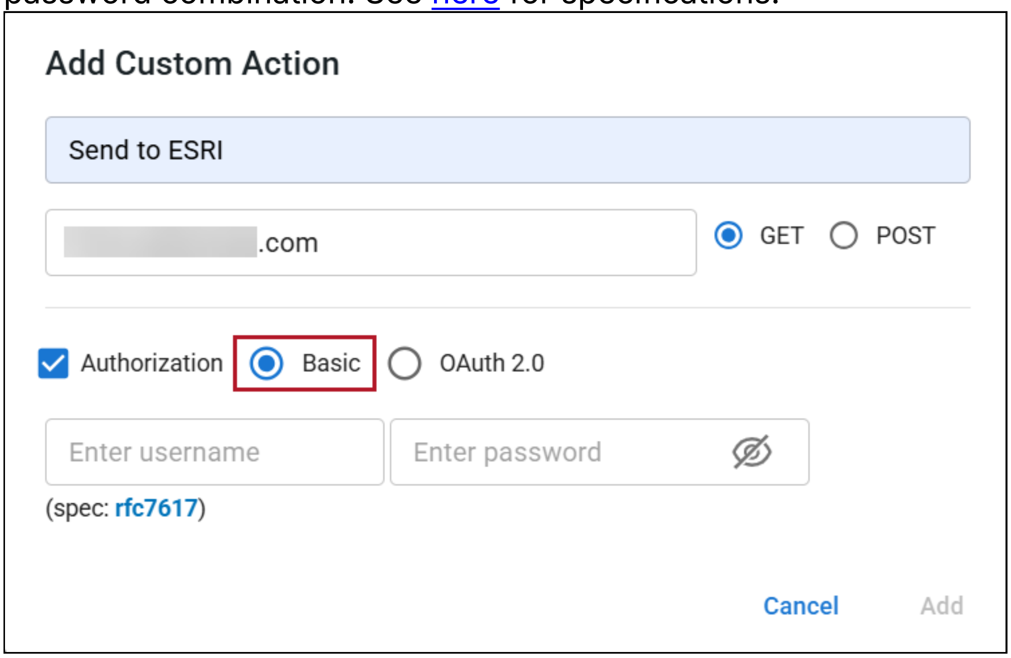
2. The **Add Custom Action** modal will appear. Add a name for the new Action.
3. Choose if this will perform a **GET** or **POST** Action, and provide an **Action URL** for the third-party service. Choose **GET** if this Action should automatically retrieve information from the Action URL, or **POST** if the Action

should automatically send information.

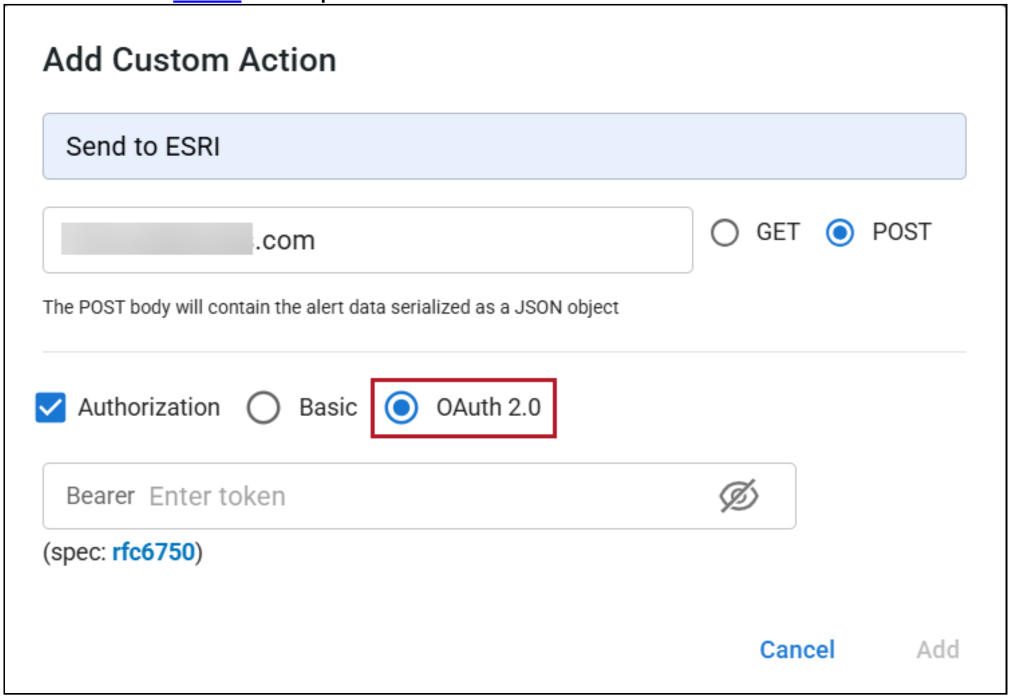


- POST Actions will send data as a JSON object.

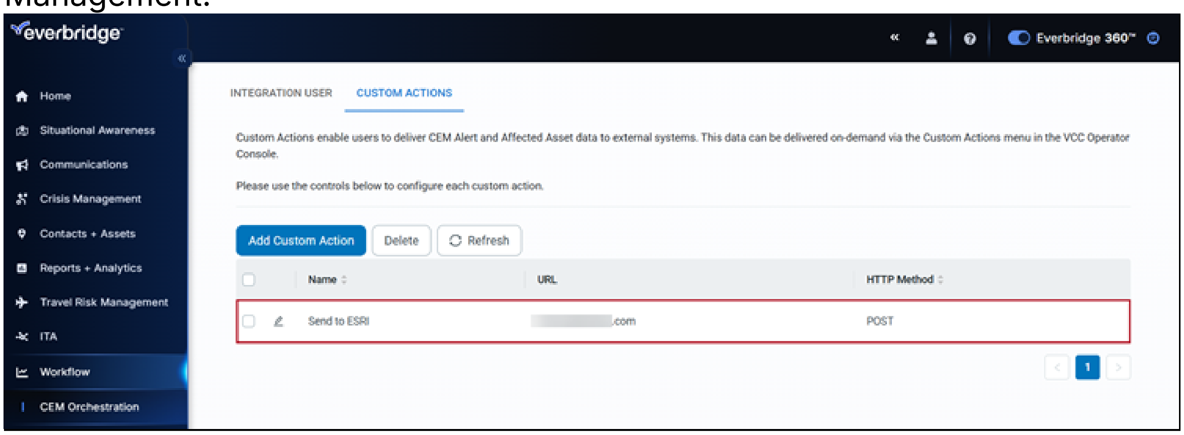
4. Optionally, click the **Authorization** checkbox, then select either:
   - **Basic** - Enforces basic HTTP Authentication with a username and password combination. See here for specifications.



- **OAuth 2.0** - Enforces authentication via OAuth 2.0 by using a Bearer token. See here for specifications.



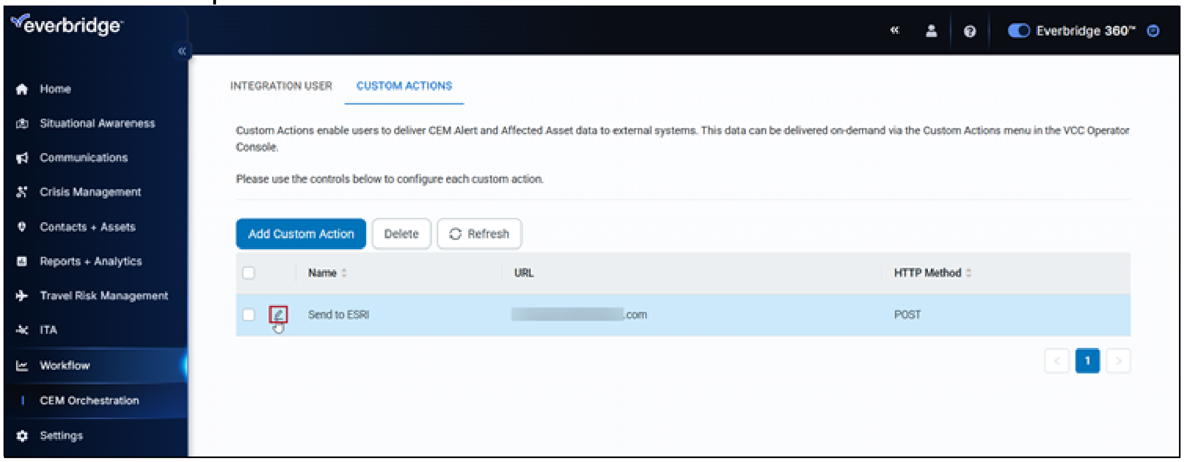
5. Click **Add**. The Custom Action will now be available to use in CEM Orchestration Workflows, the VCC Operator Console, and Alert Management.



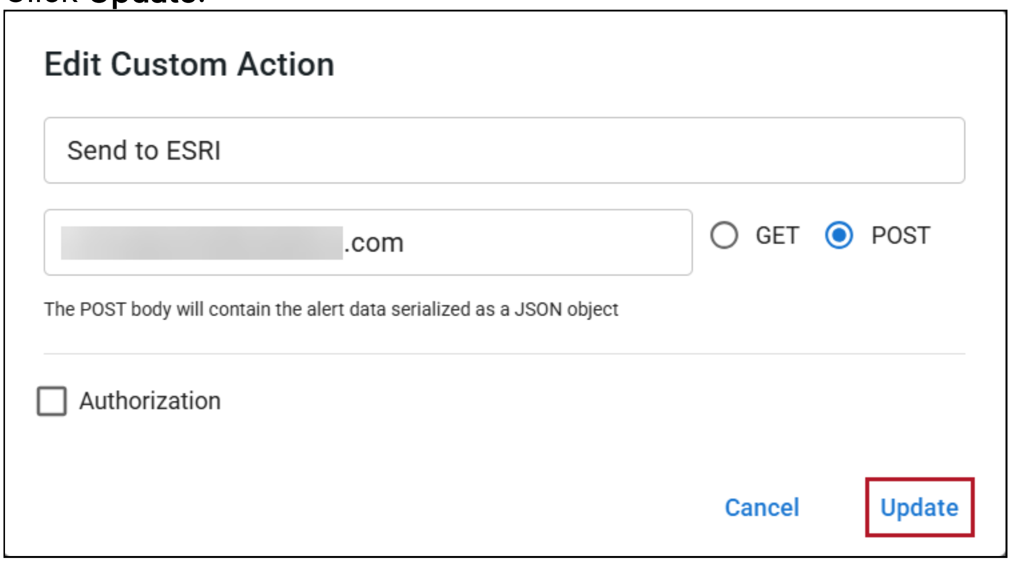
Editing Custom Actions

To edit a Custom Action:

1. Click the **Edit** pencil icon for the Custom Action that needs to be edited.



2. The **Edit Custom Action** modal will open. Make the necessary changes.
3. Click **Update**.

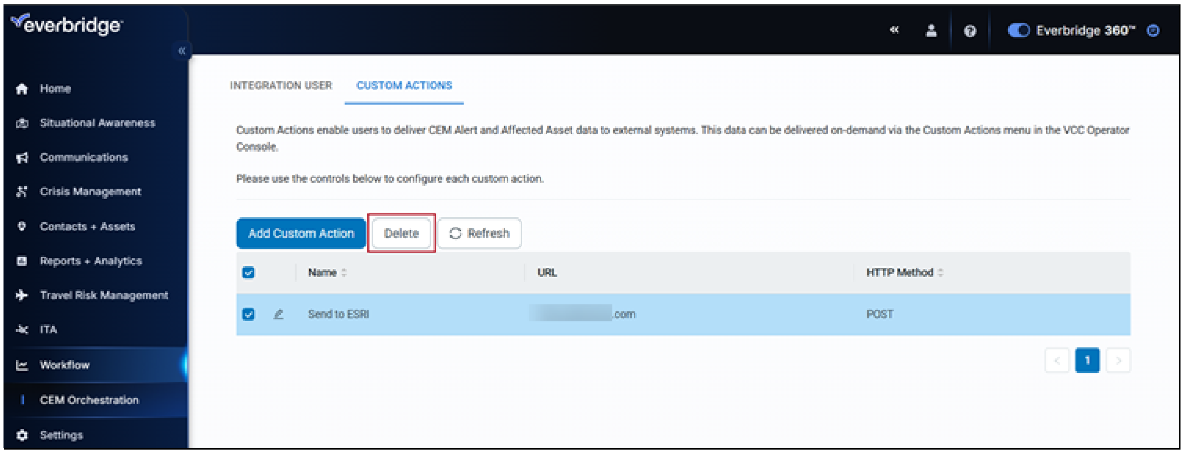


Deleting Custom Actions

To delete a Custom Action:

1. Click the checkbox next to the Custom Action that needs to be deleted.

2. Click **Delete**.

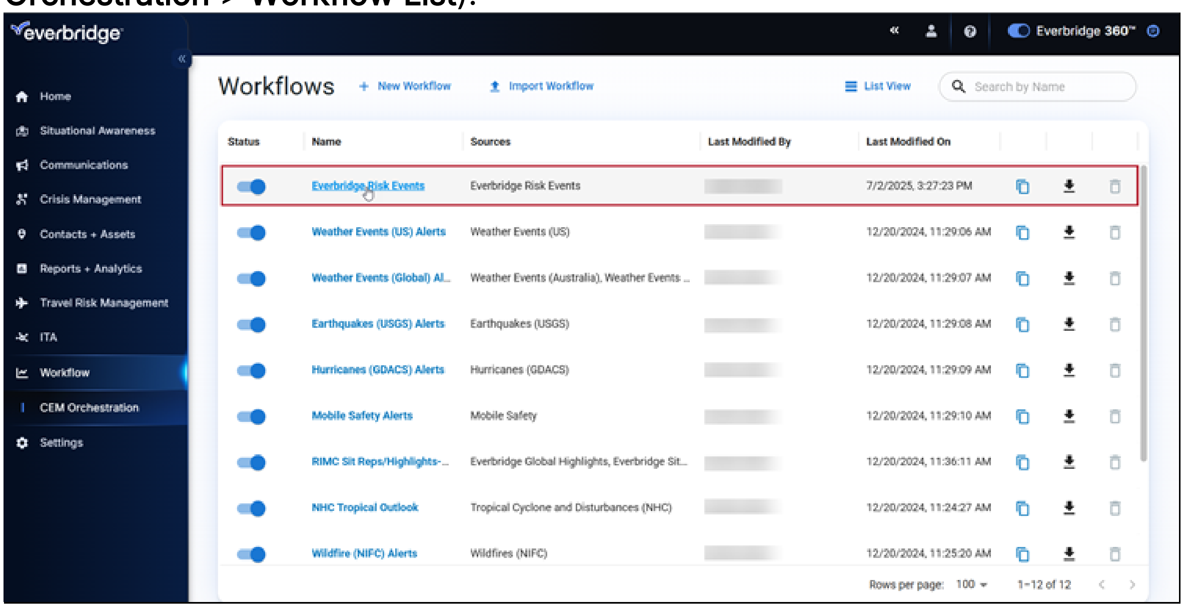


Adding Custom Actions to CEM Orchestration Workflows

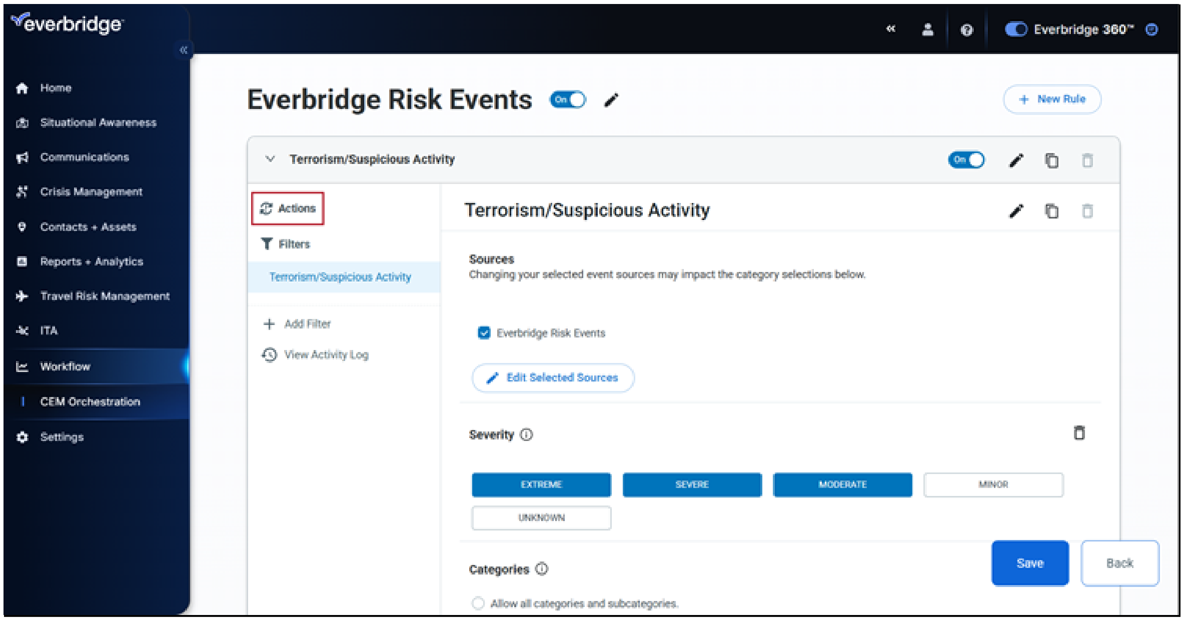
Once Custom Actions are configured, they can be launched automatically from an Alert in CEM Orchestration using Premium Workflows.

To add a Custom Action to a Workflow:

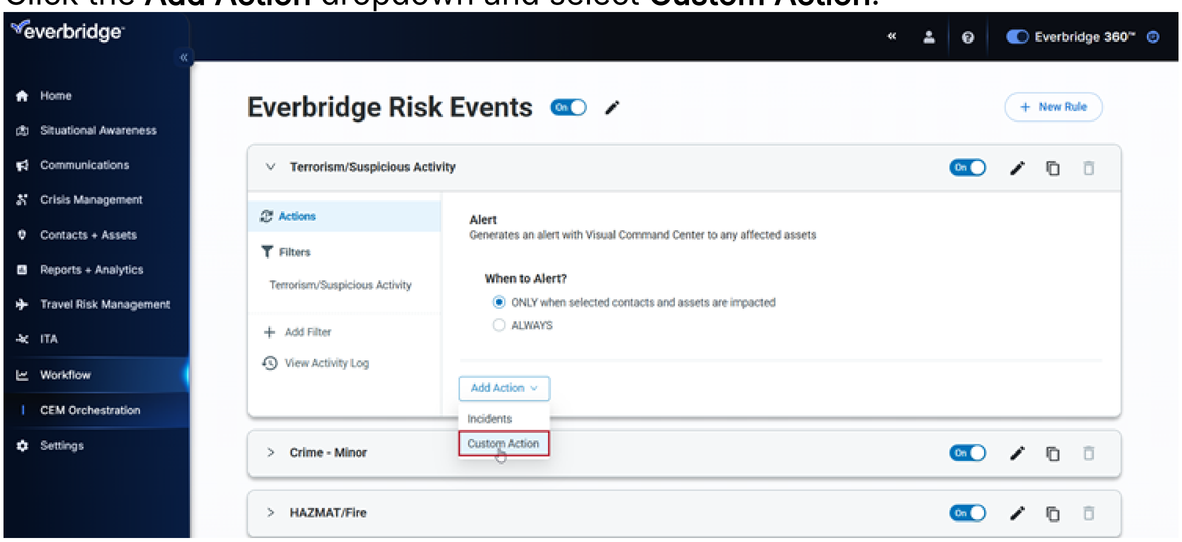
1. Select the desired Workflow from the **Workflows** page (**Workflow** > **CEM Orchestration** > **Workflow List**).



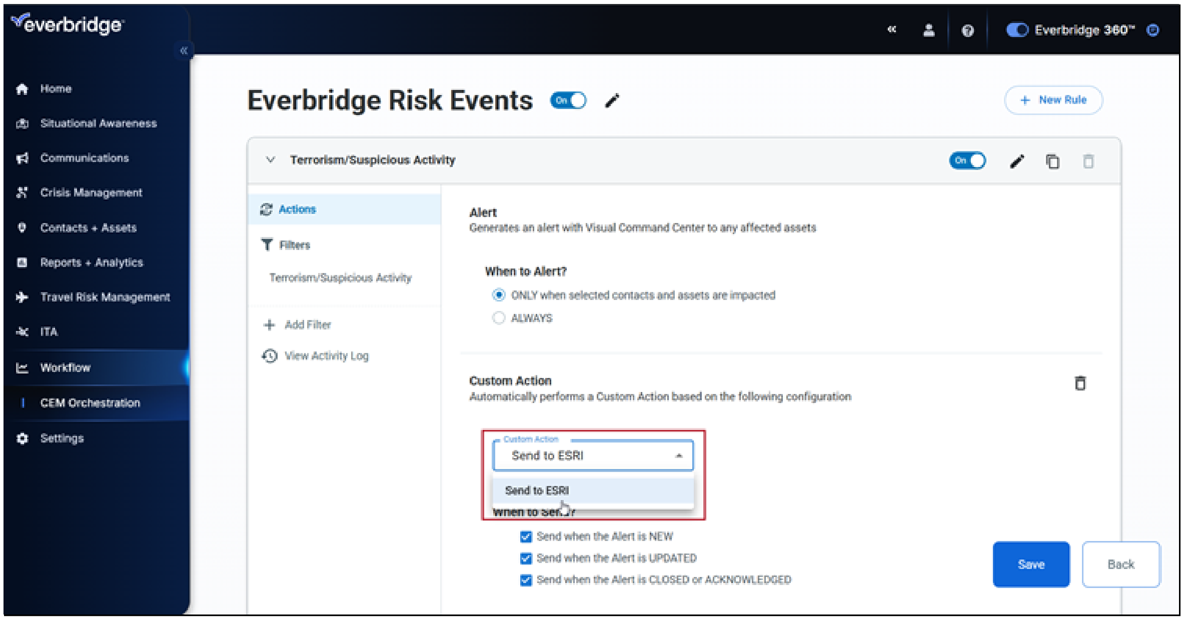
2. Select a Rule in the Workflow to expand its configuration details, and click **Actions**.



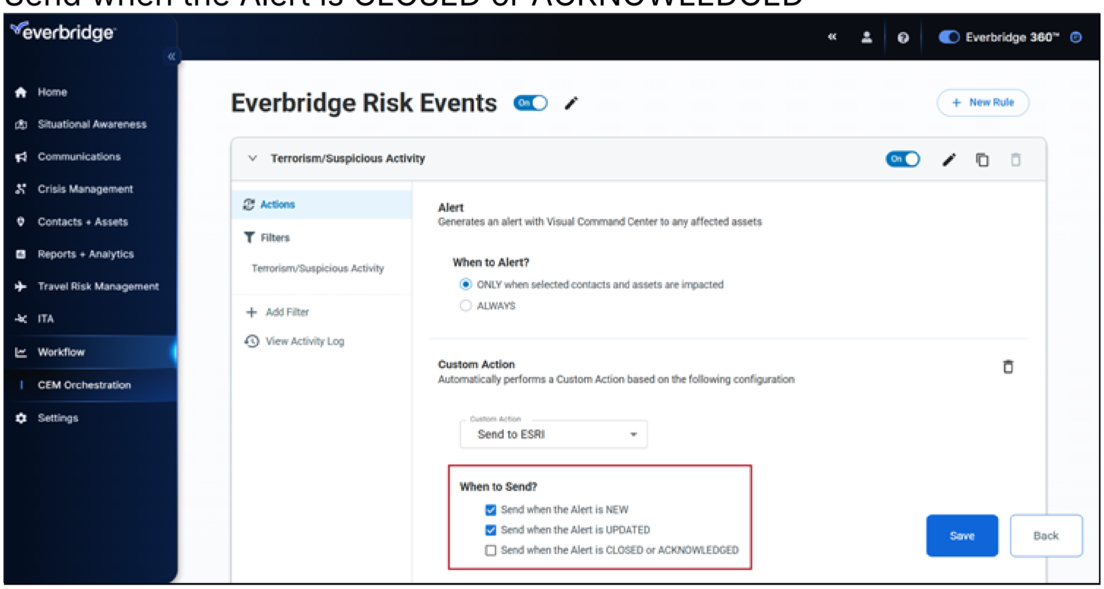
3. Click the **Add Action** dropdown and select **Custom Action**.



4. The **Custom Action** section will open. Select the Custom Action that needs to be added to this Rule.



5. Deselect Alert phases that you don't want to execute the Custom Action:
   - Send when the Alert is NEW
   - Send when the Alert is UPDATED
   - Send when the Alert is CLOSED or ACKNOWLEDGED



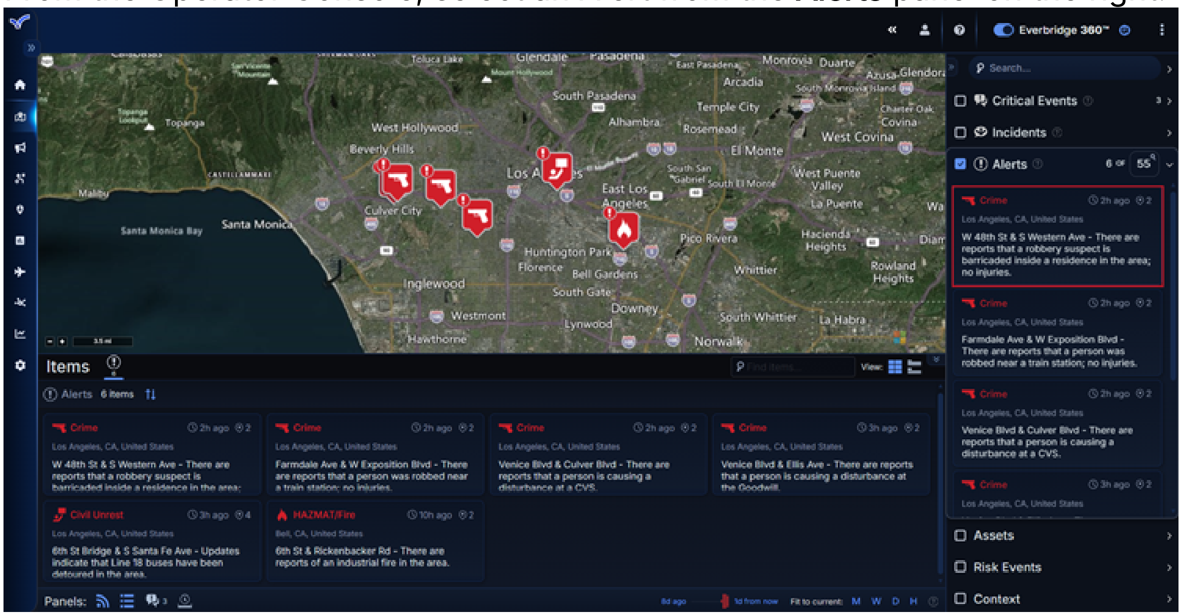
6. Click **Save**.

When the specified Alert phases are triggered by the Workflow, that Custom Action will automatically be executed. Note that operators can add multiple Custom Actions to each Workflow.

Using Custom Actions in VCC

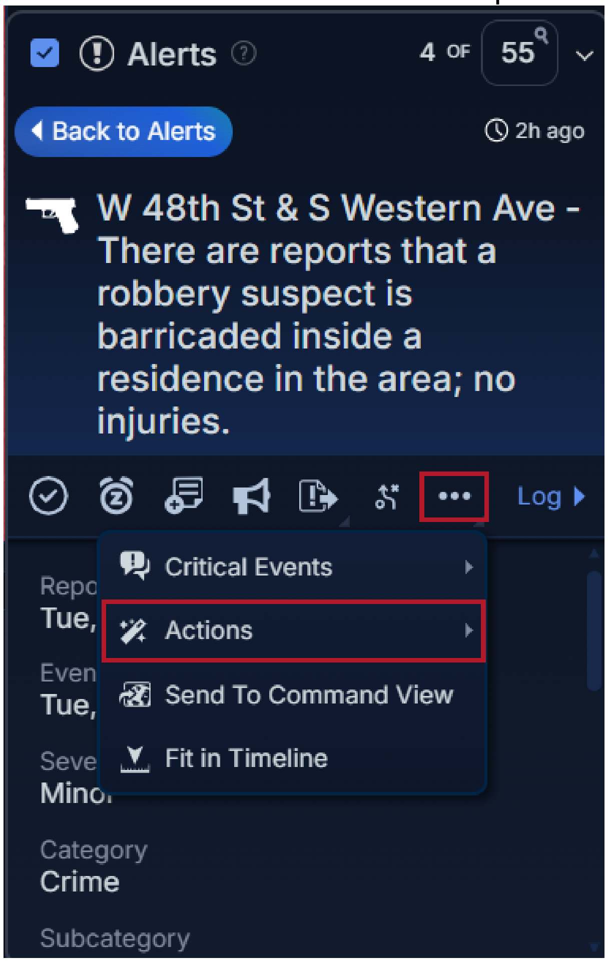
Custom Actions can be triggered from an Alert within the VCC Operator Console. To use a Custom Action:

1. From the Operator Console, select an Alert from the **Alerts** panel on the right.

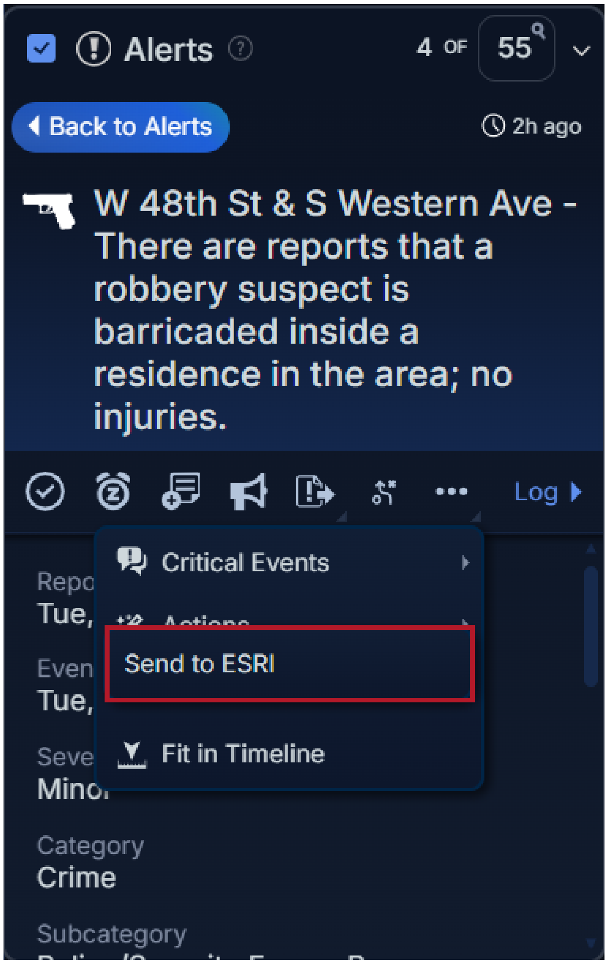


2. The **Alert Details** will open in the panel. Click **Actions.** Note that depending on the Organization's setup, the three-dot meatball menu might first need to be

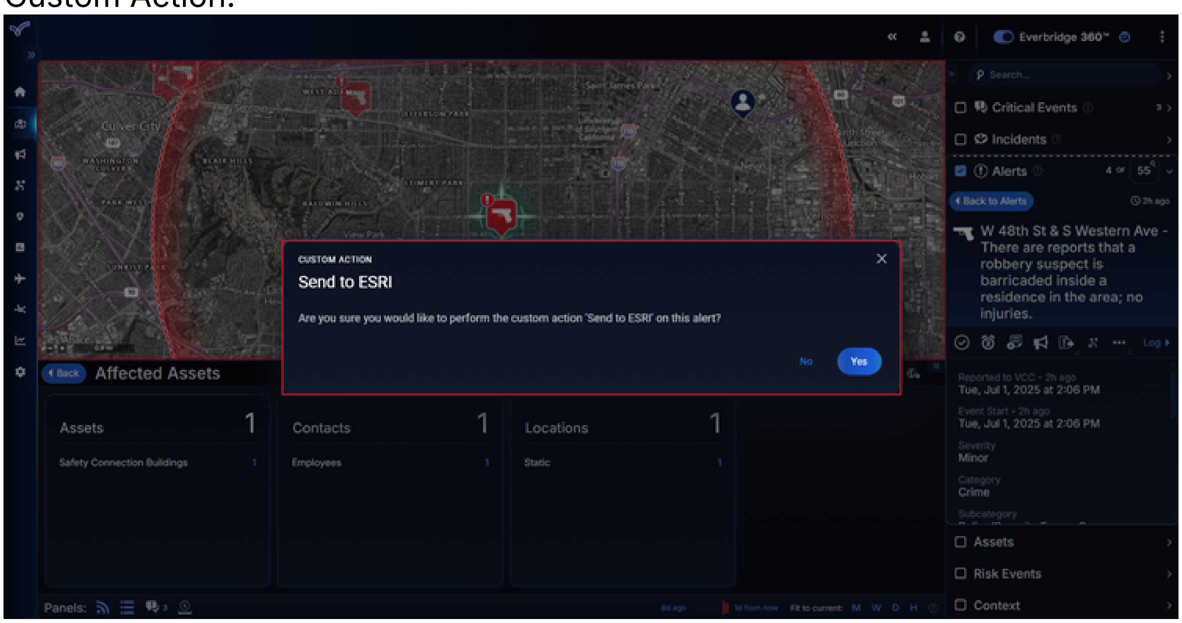
clicked to reveal the additional options.



3. Select the desired Custom Action from the menu.



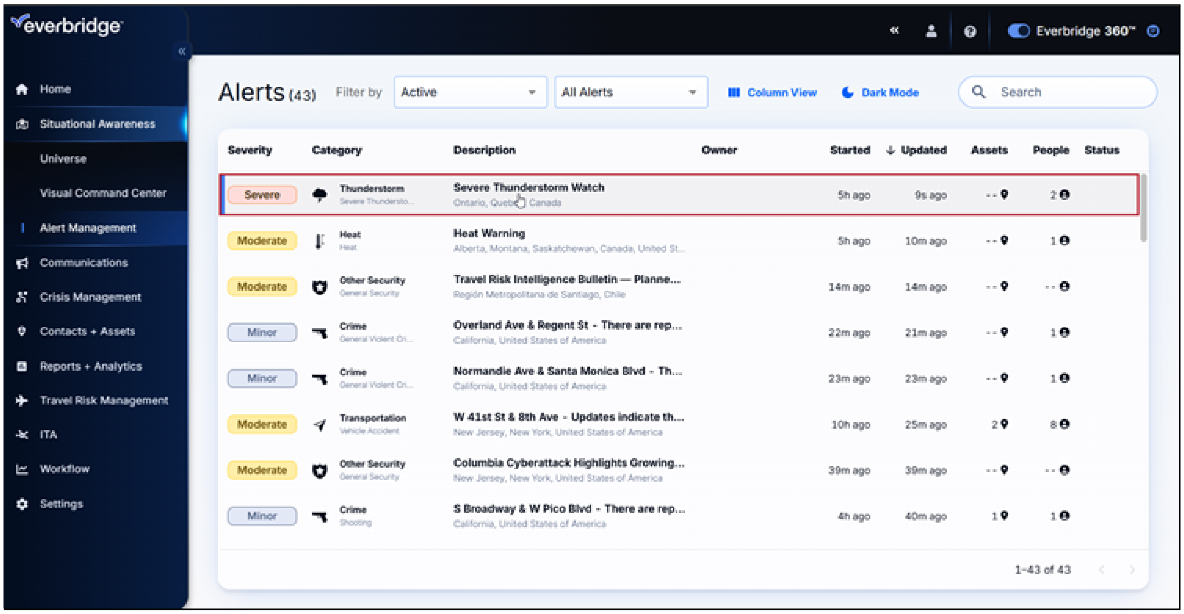
4. A confirmation prompt will appear. Click **Yes** to proceed with launching the Custom Action.



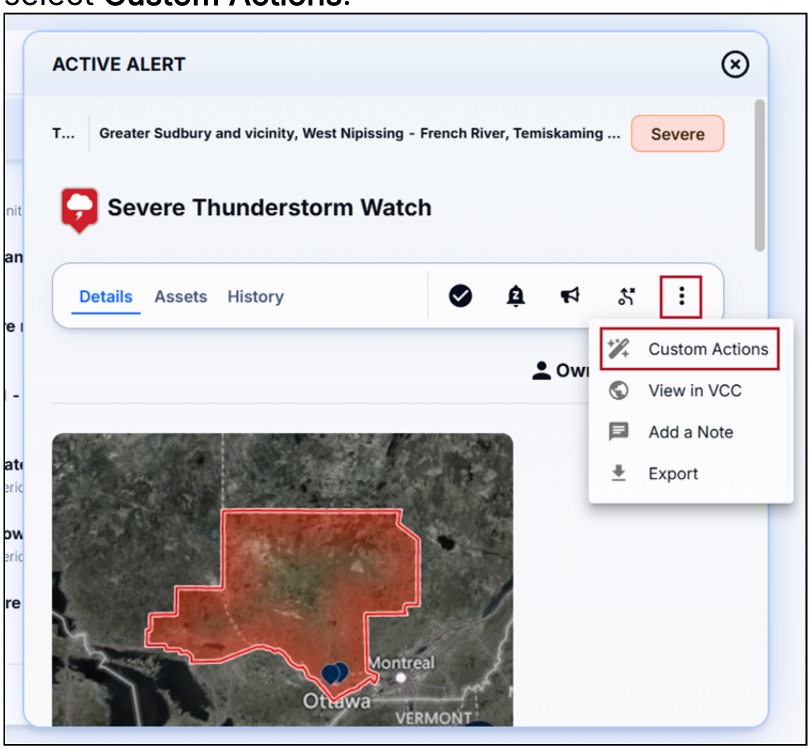
Using Custom Actions in Alert Management

Custom Actions can be triggered from the **Alert Management** page (**Situational Awareness** > **Alert Management**). To launch a Custom Action from here:

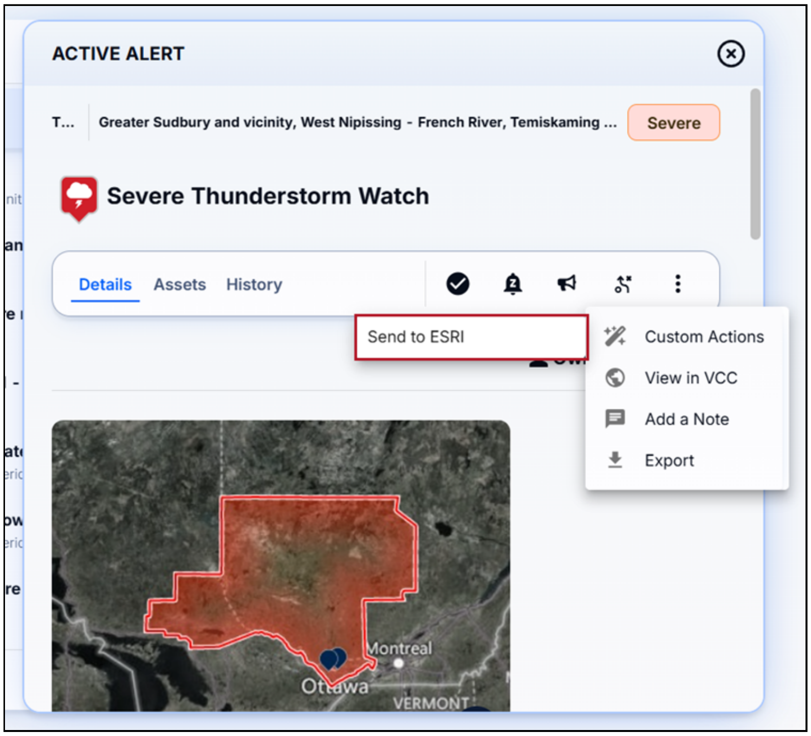
1. Click an Alert from the list view.



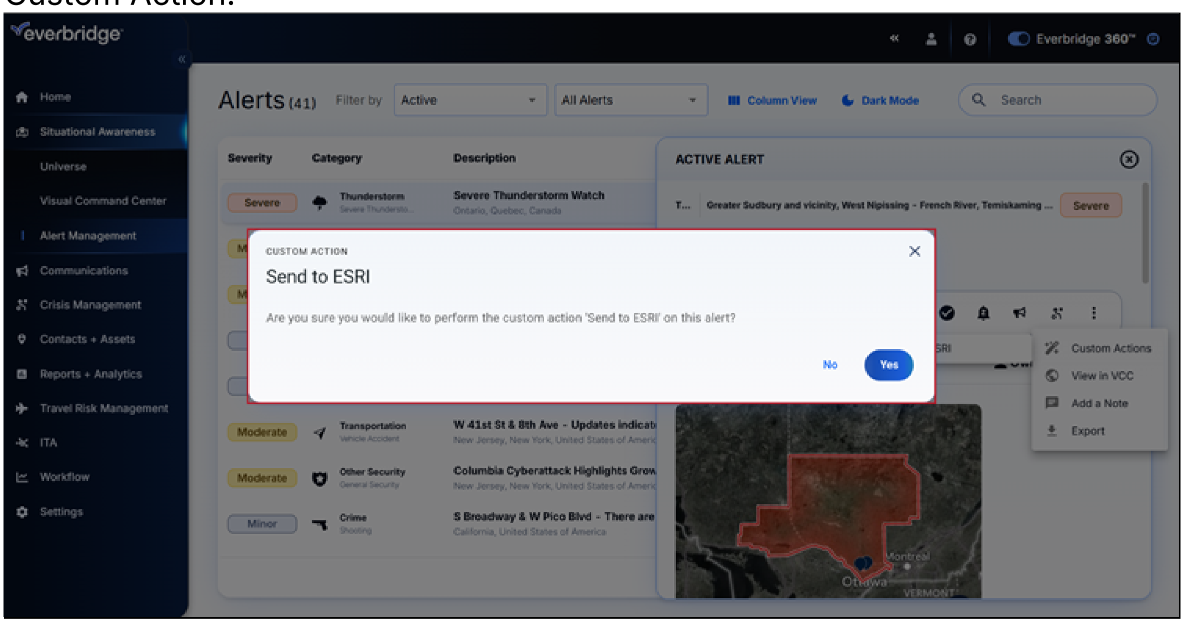
2. The **Alert Details** modal will open to the right. Click the kebab menu icon and select **Custom Actions**.



3. Select the desired Custom Action from the list.



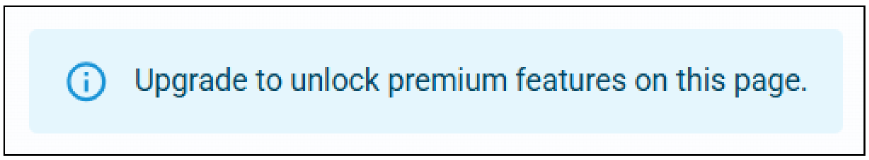
4. A confirmation prompt will appear. Click **Yes** to proceed with launching the Custom Action.



CEM Orchestration Limited Workflows

The **Everbridge 360 Professional** solution provides preconfigured **Limited Alerting Workflows**, allowing users to easily generate and automatically be notified about Alerts in Visual Command Center when a Risk Event occurs near your Contacts or Assets.

Customers with this package will see a message at the top of the CEM Orchestration pages informing them that the Premium features are available with an upgrade.



NOTE: Contact your Account Administrator if you're interested in upgrading to unlock Premium features.

Included Functionality

Customers using this solution have access to the following functionality:

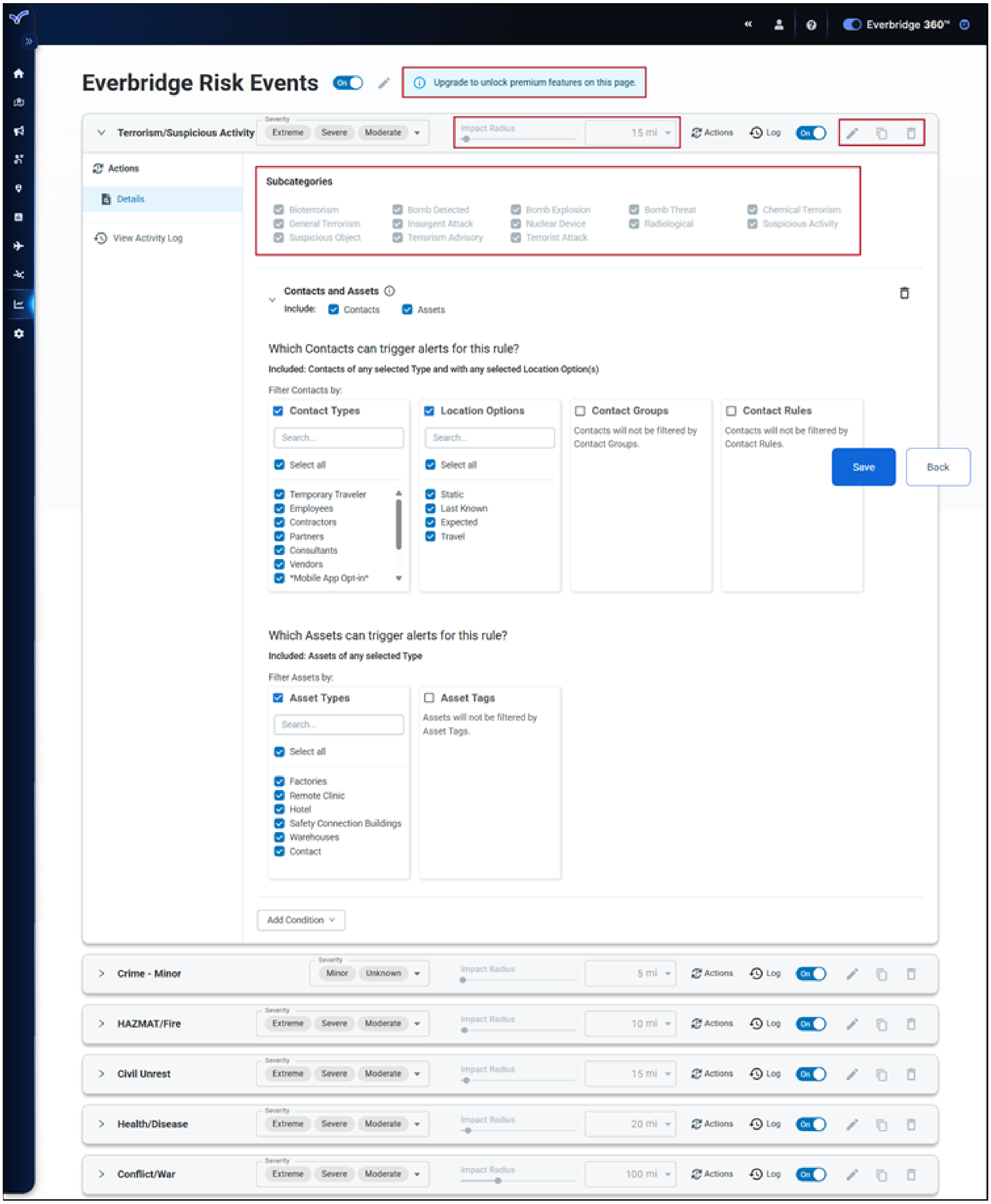
- Enable or disable preconfigured Workflows and their Rules for Alerting.
- Configure Incidents to be automatically launched when Alerting criteria is met.
- Adjust Severity for different Rules.
- Specify which Contacts can trigger Alerts for a Rule via Contact Types, Location Options, Contact Groups, and Contact Rules.
- Specify which Assets can trigger Alerts for a Rule via Asset Types and Asset Tags.
- Review the Activity Log.

Excluded Functionality

The Limited Workflow functionality doesn't include the following Premium features, which are displayed in grey in the interface:

- Create new custom Workflows or import Workflows.
- Change the selected subcategories for a Rule.
- Adjust a Rule's Impact Radius.

- Add Custom Actions to Workflows.
- Add new Filters to existing Rules.
- Rename, copy, download, or delete an existing Workflow or Rule.



Managing Assets to Align with Orchestration Workflows

Assets are the physical entities that an organization cares about other than Contacts. These could include entities like clinics, ships, airports, and schools.

CEM Orchestration allows you to set up different Alerting criteria for different Contact Types, Asset Types, and Asset Tags. You can classify your Asset Types and Tags according to how you want to define their Alerting Rules. For example, you could create Asset Types for two types of hospitals, one in a rural area and one in an urban area; this would let you configure different Alerting Rules around them.

To set up and manage your Assets, navigate to **Settings** > **Organization** > **Contacts/Assets**. For a complete set of directions on how to set up and manage assets, see the Asset Management Guide.

Creating Alerting Criteria by Asset Type

CEM Orchestration allows you to set up different Alerting Criteria for different **Asset Types.** For this example, we'll set up different Alerting Criteria for medical clinics that are located in urban areas and rural areas.

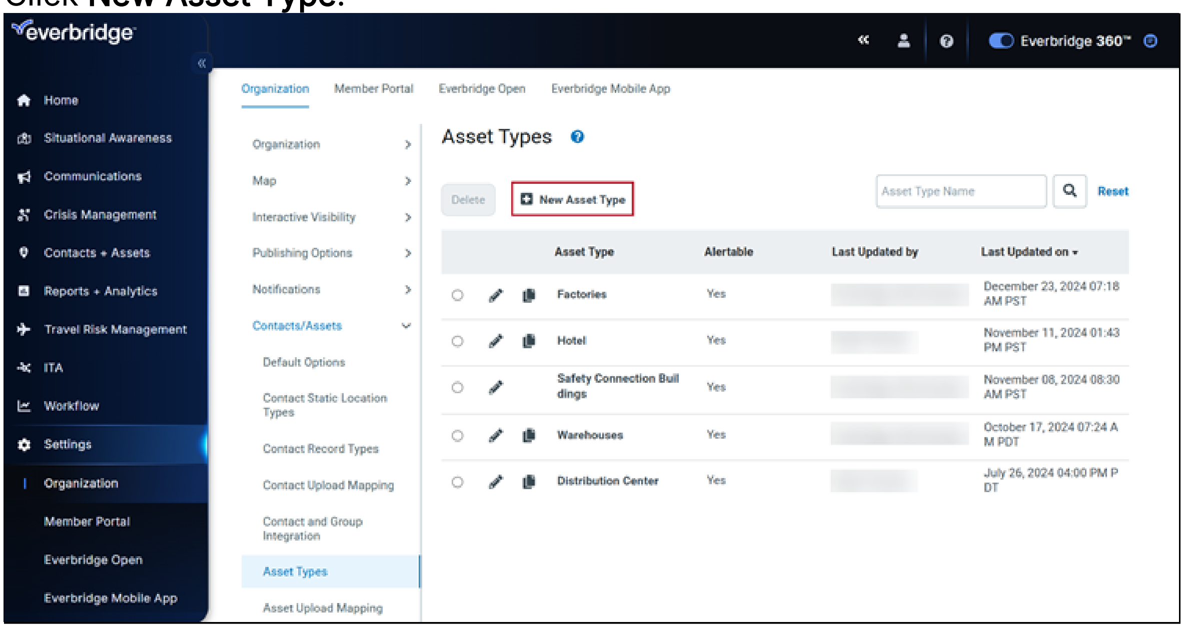
> **NOTE:** For an in-depth overview of Asset Types, see the Asset Management Guide.

Aligning Asset Types and Workflows

Before you create Workflows, you need to define your Asset Types to correspond with the way you want to Alert about them.

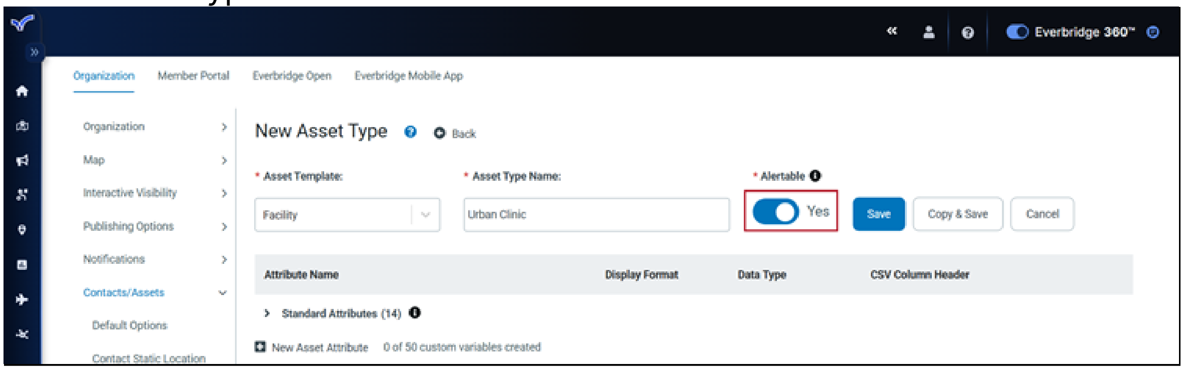
In this example, to have different alerting criteria for the clinics, you need to create separate Asset Types for the **Rural and Urban Clinics**, by following these steps:

1. Navigate to **Settings** > **Organization** > **Contacts/Assets** > **Asset Types**.
2. Click **New Asset Type**.

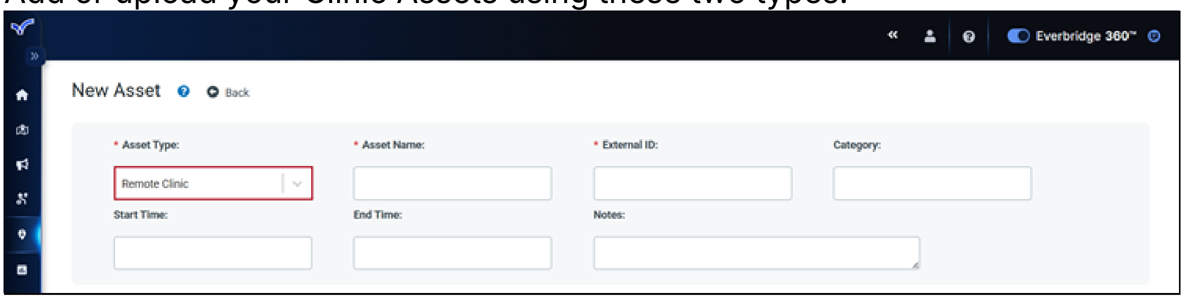


3. From the **Asset Template** menu, select **Facility**.

4. In the **Asset Type Name** field, enter **Urban Clinic**. Enable the **Alertable** setting for the new Type.



5. Click **Save**.
6. Repeat Steps 3-5 to add the **Remote Clinic** Asset Type.
7. Add or upload your Clinic Assets using these two types.

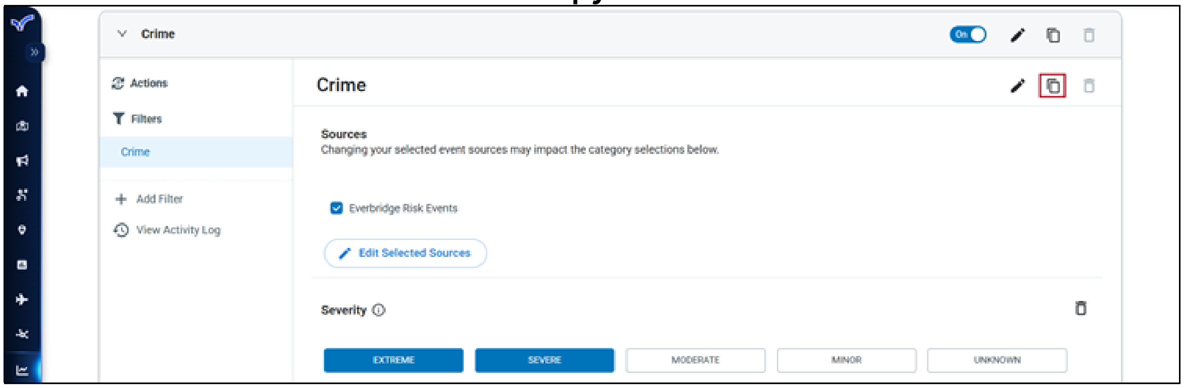


Creating Alerting Thresholds for Different Asset Types

Once you have created Asset Types that will align with your Alerting criteria, go to the **CEM Orchestration Workflows** page to create or edit a Workflow. In this example, we will edit the **Crime** Rule, creating different Filter Sets for **Urban** and **Rural Clinics**. For this example, we will use a sample Crime Workflow with one Rule that has one Filter.

1. From the **Workflows** page, select the Workflow that you want to change.
2. Select the Rule and Filter you want to change. We'll choose the **Crime** Rule for this example.

3. Click the **Copy** icon to duplicate the existing Filter. A new Filter is created with the default name **Filter Set 1 - Copy 1**.



4. Select the new Filter and click the **Edit** icon to change the Filter name. Rename it **Urban Clinics**.
5. Scroll to **Impacted Assets** to deselect Contacts and all Asset Types except **Urban Clinics**.
6. Under **Impacted Assets**, select **Urban Clinics**.
7. Adjust the **Impact Radius** and **Severity** to the values you want to apply to clinics in urban areas. To avoid over-alerting in population-dense areas, you may want to set a relatively small Impact Radius (e.g., 1 mile) and a high Severity.
8. Use the **Copy** button to create a copy of the Filter.
9. Scroll to **Impacted Assets** and deselect contacts and all Asset Types except Rural Clinics.
10. Adjust the **Impact Radius** and **Severity** to the values you want to apply to clinics in rural areas.
11. Open the original Filter. Under **Impacted Assets**, deselect **Urban Clinics** and **Rural Clinics**, since you have now created separate Filters for those Assets.
12. Click **Save**.

Configuring Asset Tags for CEM Orchestration Workflows

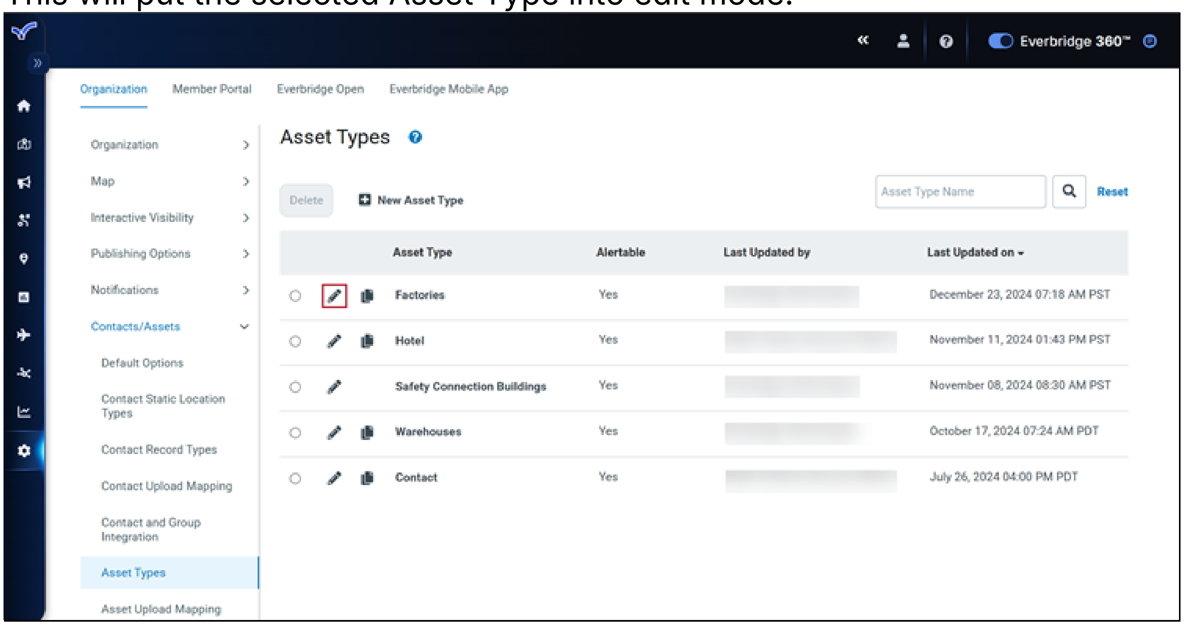
Asset Tags are highly customizable additional attributes that allow you to organize and group your Assets for Alerting and Notification purposes. Building your CEM Orchestration rules using Asset Tags increases your ability to articulate and leverage distinctions among subsets of your Assets so that you can target your Alerting more precisely.

Setting up Asset Tags for use in CEM Orchestration workflows is a three-step process involving **Asset Types**, **Assets**, and **Workflows**.

Adding a "Tags" Attribute to an Asset Type

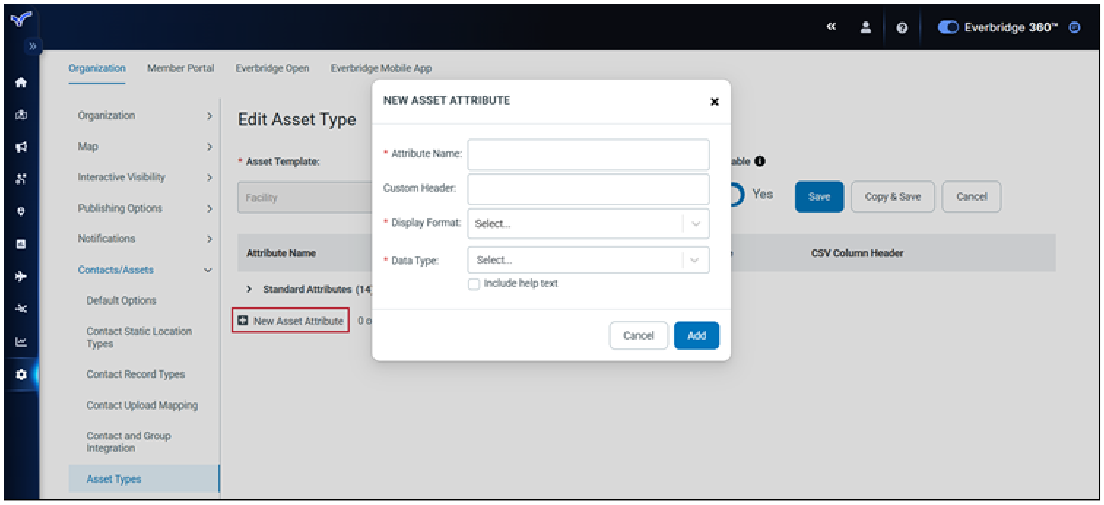
A **"Tags" Attribute** must first be configured for any Asset Type that will use tagging. To do this:

1. Navigate to **Settings** > **Organization** > **Contacts/Assets** > **Asset Types**.
2. Click the pencil icon next to the name of the Asset Type you wish to edit. This will put the selected Asset Type into edit mode.



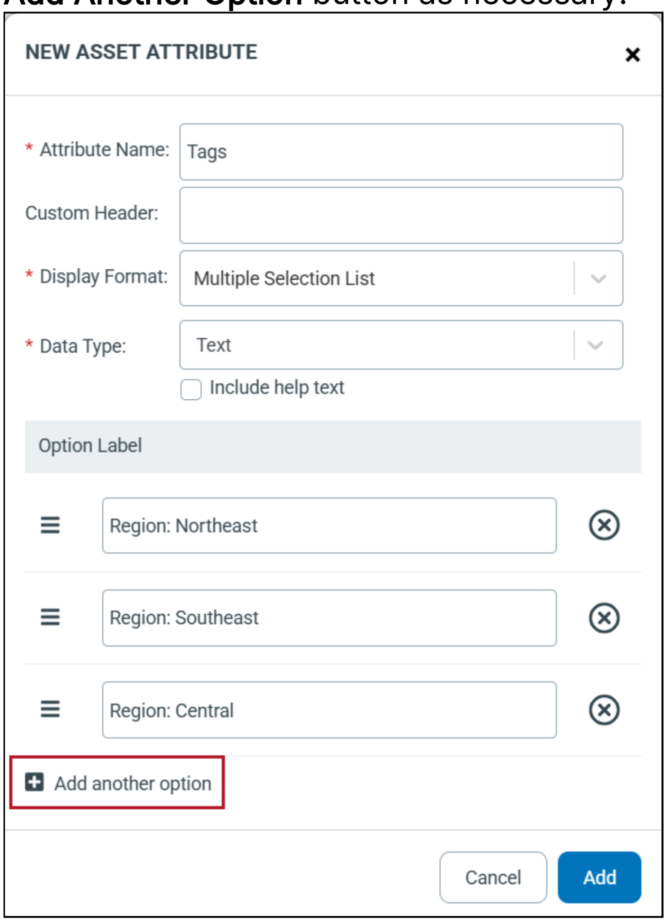
3. Add a new Asset Attribute:

a. Click the **New Asset Attribute** button at the bottom of the Asset form.



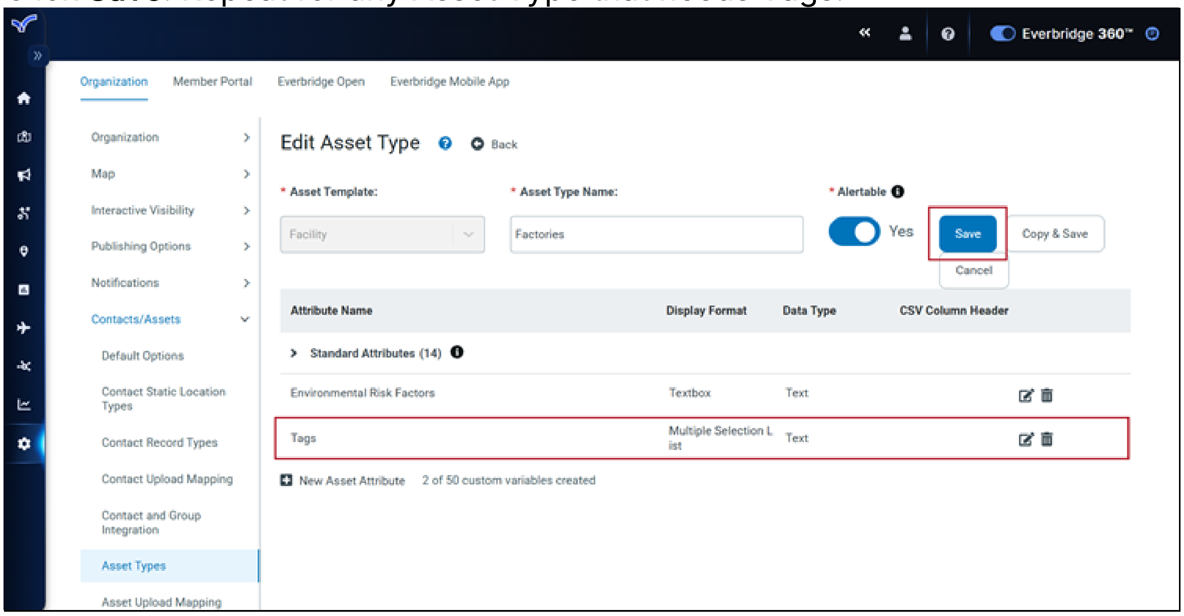
b. Fill in the required fields on the New Asset Attribute dialog:
- **Attribute Name**: “Tags”
- **Display Format**: Multiple Selection List
- **Data Type**: Text

c. Add an **Option Label** for each Asset Tag you wish to create using the **Add Another Option** button as necessary.



   d. When you have added all the Tags you want, click **Add**. The modal will close, and you'll see the new **Tags** attribute listed below the **Standard Attributes** in the list.

4. Click **Save.** Repeat for any Asset Type that needs Tags.



TIP: Tags must be configured on every Asset Type that contains Assets you wish to tag. If you have not added a “Tags” Attribute to an Asset Type according to the instructions above, no Tags will be available to assign to Assets of that Type.

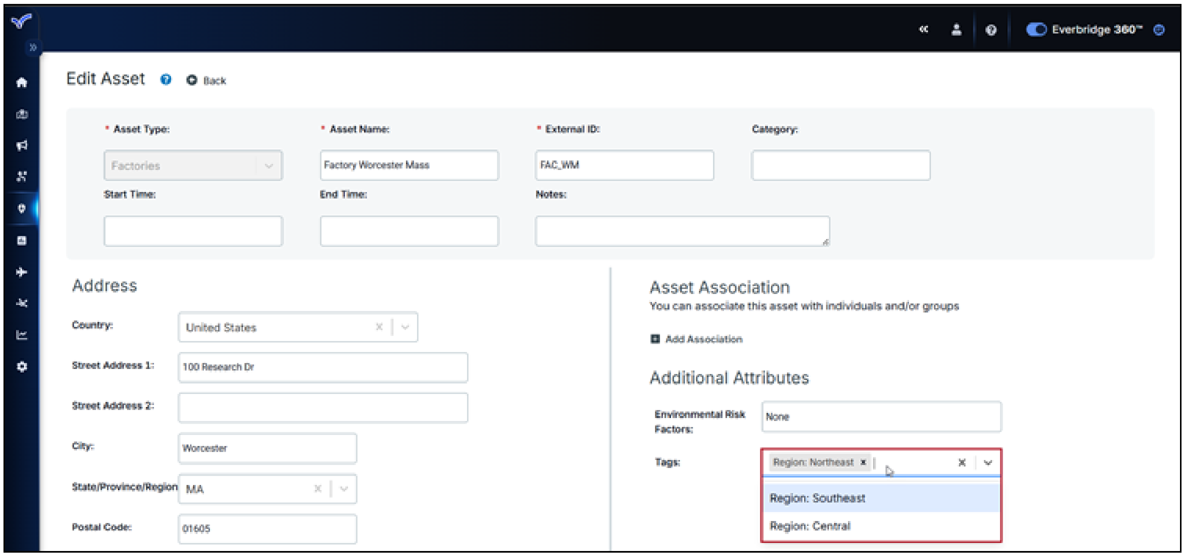
Asset Tags can be unique to a particular Asset Type or they can be shared across Types. For example, you could have a “Region: Northeast” tag on both the Offices and Data Centers Asset Types but reserve a “VIP” tag for Office-type assets. If you wish to use a Tag on more than one Type of Asset, simply include it in the Asset Type definition for every Type that will use it.

Adding Tags to Individual Assets

Once Tags have been configured, they can be added to individual Assets. To add Tags to your Assets:

1. Navigate to **Contacts/Assets** > **Assets** > **Asset List.**
2. Click the pencil icon next to the name of the Asset you wish to edit. This will put the selected Asset into edit mode.

3. Select the appropriate Tag(s) from the **Tags** dropdown menu under **Additional Attributes**.



- You can add multiple Tags to an Asset. You can also remove Tags from an Asset by clicking the **X** to the right of the tag name in the Tags control.

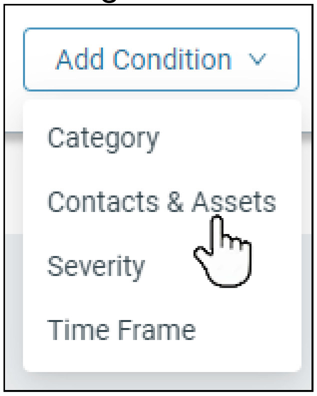
4. Once you have added all the Tags you wish to add, click the **Save** button.
5. Repeat for any additional Assets you wish to tag.

Using Tags in the Assets Filter Condition in a CEM Orchestration Workflow

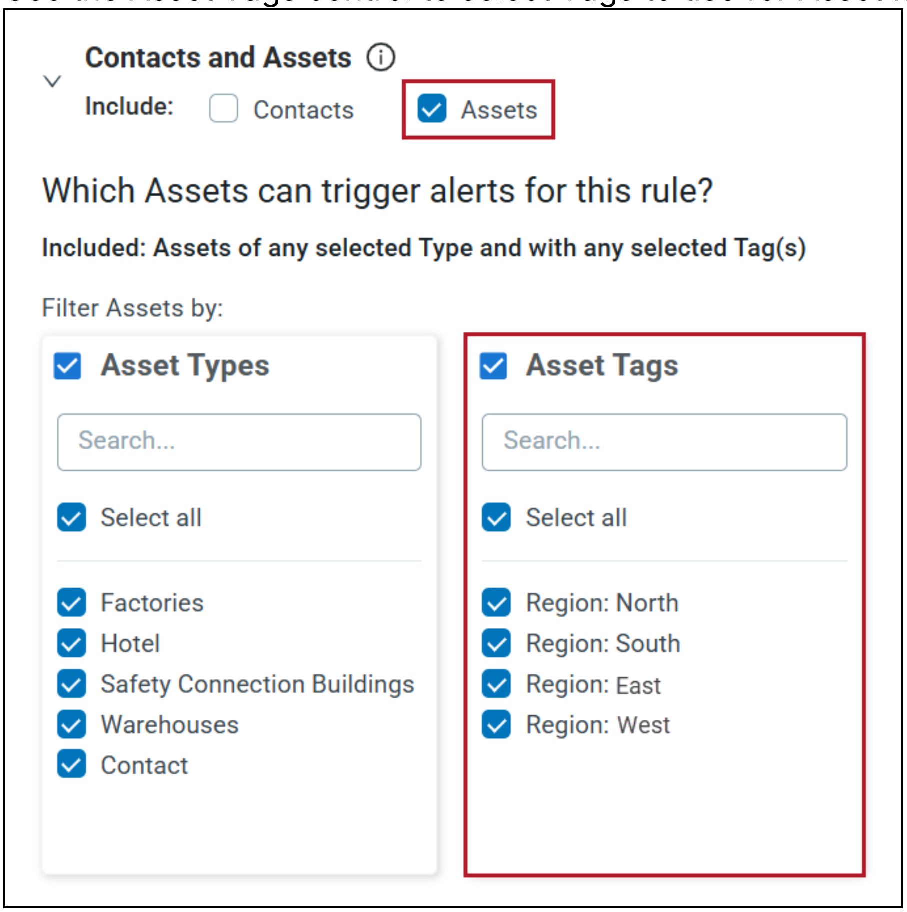
Once the Assets have been tagged, those Tags can be used in the CEM Orchestration Workflow Filter conditions to more precisely target Alerts or Notifications. To do this:

1. Navigate to **CEM Orchestration** > **Workflow List**.
2. Select the desired **Workflow**, or create a new one.
3. Expand the Filter you wish to edit and scroll to the **Contacts and Assets Condition**.

- If you do not see a Contacts and Assets Condition, you can add one by clicking the **Add Condition** button at the bottom of the form.



4. Use the Asset Tags control to select Tags to use for Asset filtering.



- To match, Assets must be of one of the selected Asset Types and have at least one of the selected Asset Tags. An Asset does not need to have all the selected Tags to match.
- If you want your filter to match Assets with no Tags, check **Select All**, as that will match all configurations of Tags, including those with no Tags.
- The **Asset Tags** filter control will always be present if you have a **Tags** Attribute configured on any Asset Type in your Organization, regardless of which Asset Types are selected for inclusion in a given

Workflow Filter. If you wish to ignore Asset Types in any Workflow, check the **Select All** option in the **Asset Tags** control.

5. Click **Save**.

Creating and Using Asset Associations

Asset Associations allow you to associate Contacts with your Assets. These associations can be leveraged in CEM Orchestration Workflows and Visual Command Center to allow precisely targeted communication to Asset stakeholders.

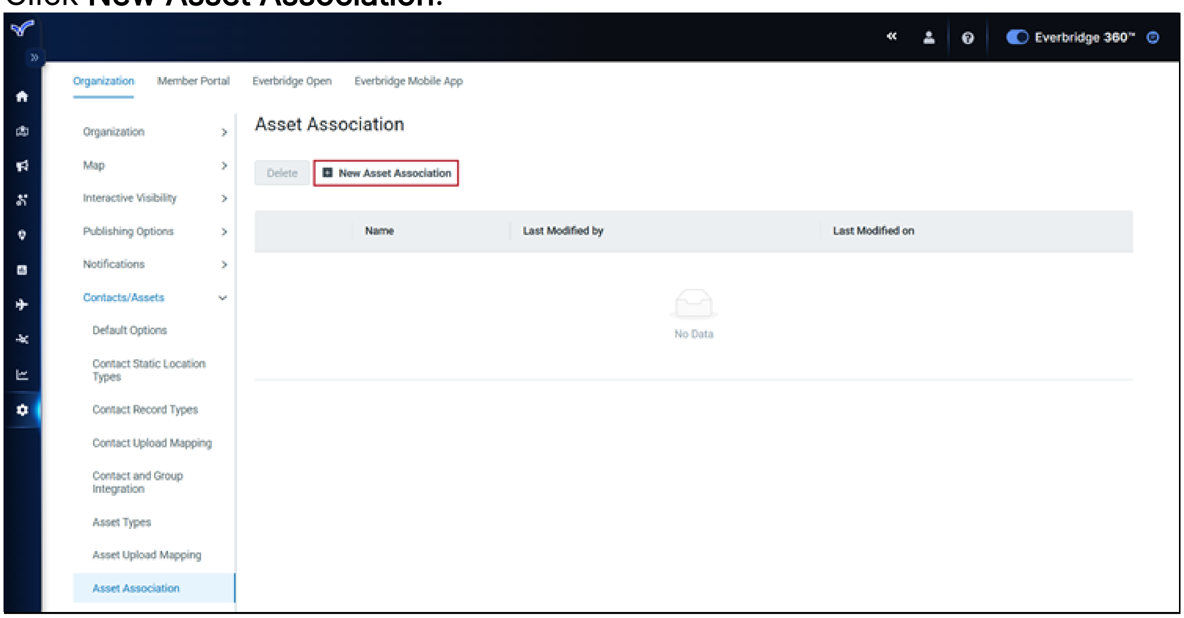
Asset Associations can be configured in three steps:

1. Create Association Types.
2. Associate Contacts or Groups to Assets.
3. Add Associations to CEM Orchestration Workflows for dynamic Notifications.

Create a New Asset Association Type

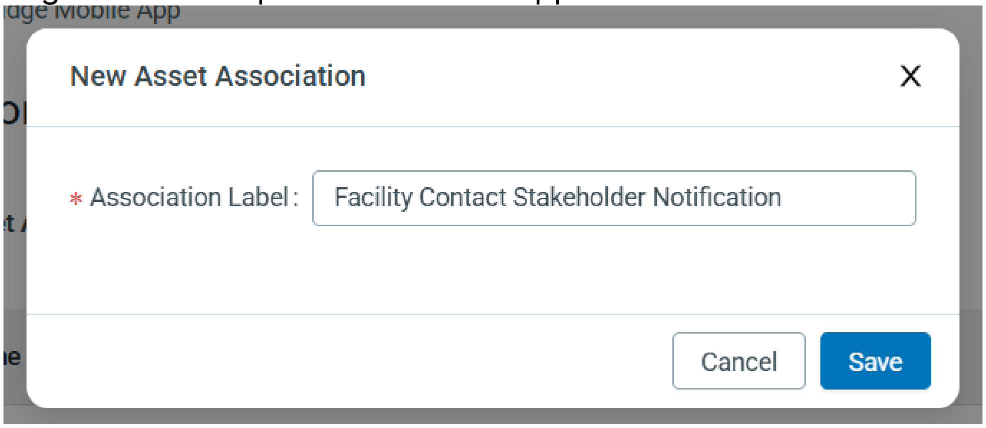
To create a new Asset Association Type:

1. Navigate to **Settings** > **Organization** > **Contacts/Assets** > **Asset Association**.
2. Click **New Asset Association**.

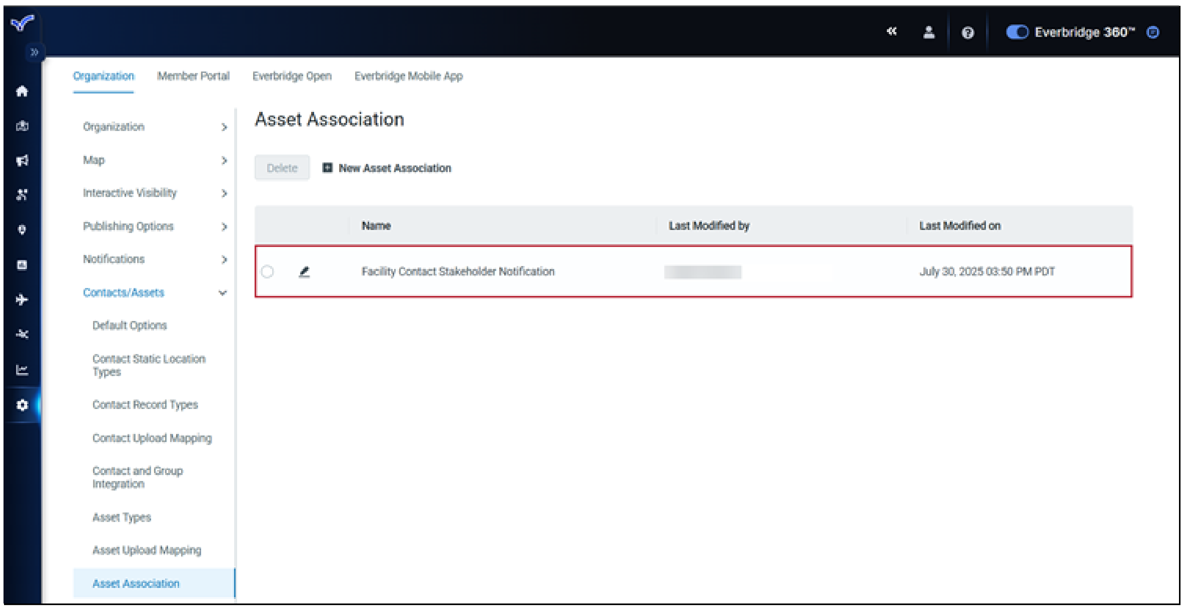


3. Add an **Association Label**, e.g., Facility Security, District Manager, Regional Manager. This can be any you choose, but each must be unique across the

Organization. Duplicates are not supported.



4. Click **Save**. The Asset Association can now be seen in the list view:

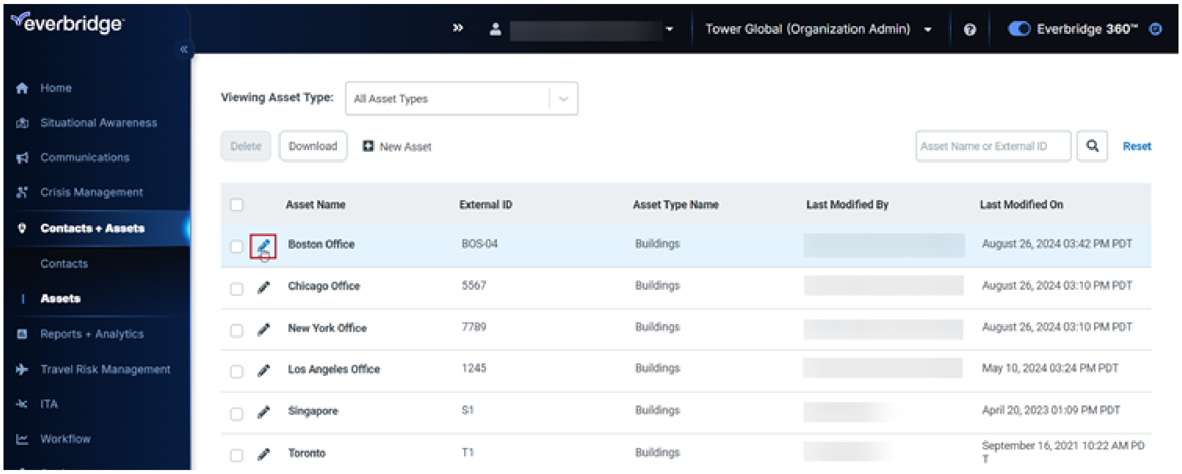


Link New Asset Association to Assets

To link the new Asset Association to an Asset:

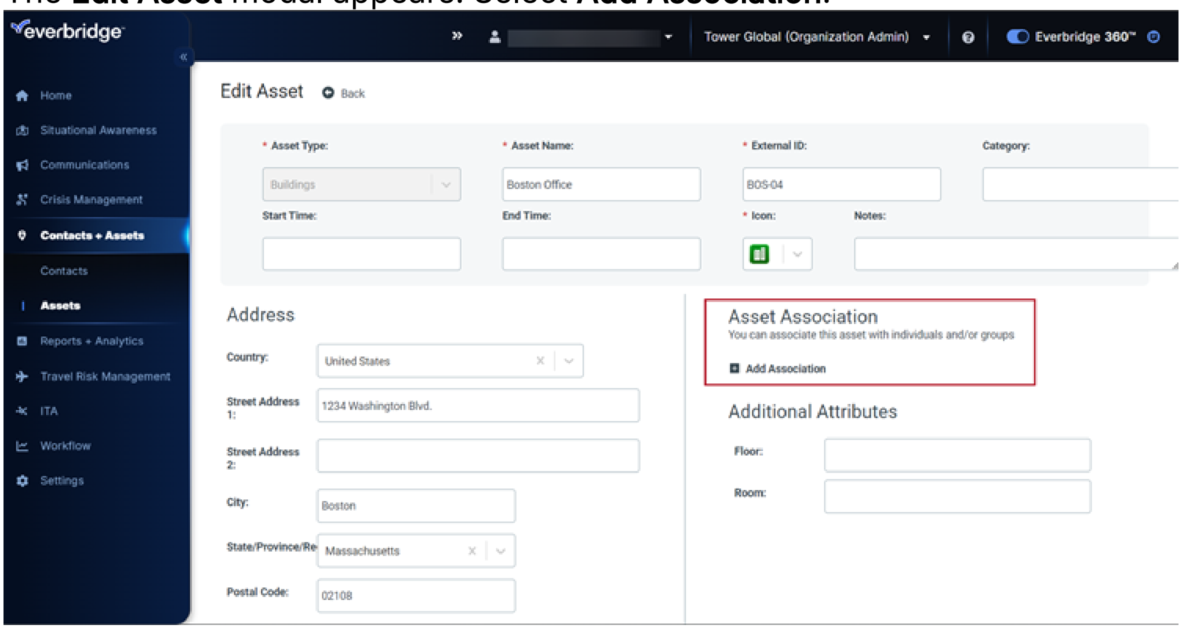
1. Navigate to **Assets** > **Asset List**.

2. Click the **Pencil** icon for the desired Asset to edit it.

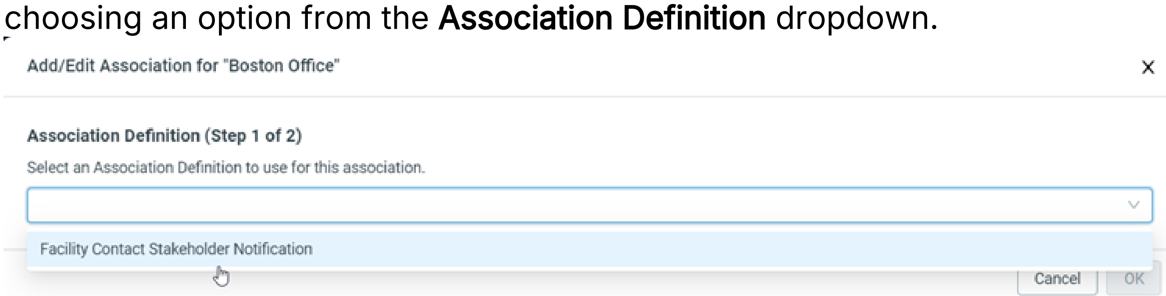


- Associations can also be linked on the **New Asset** page when creating an Asset.

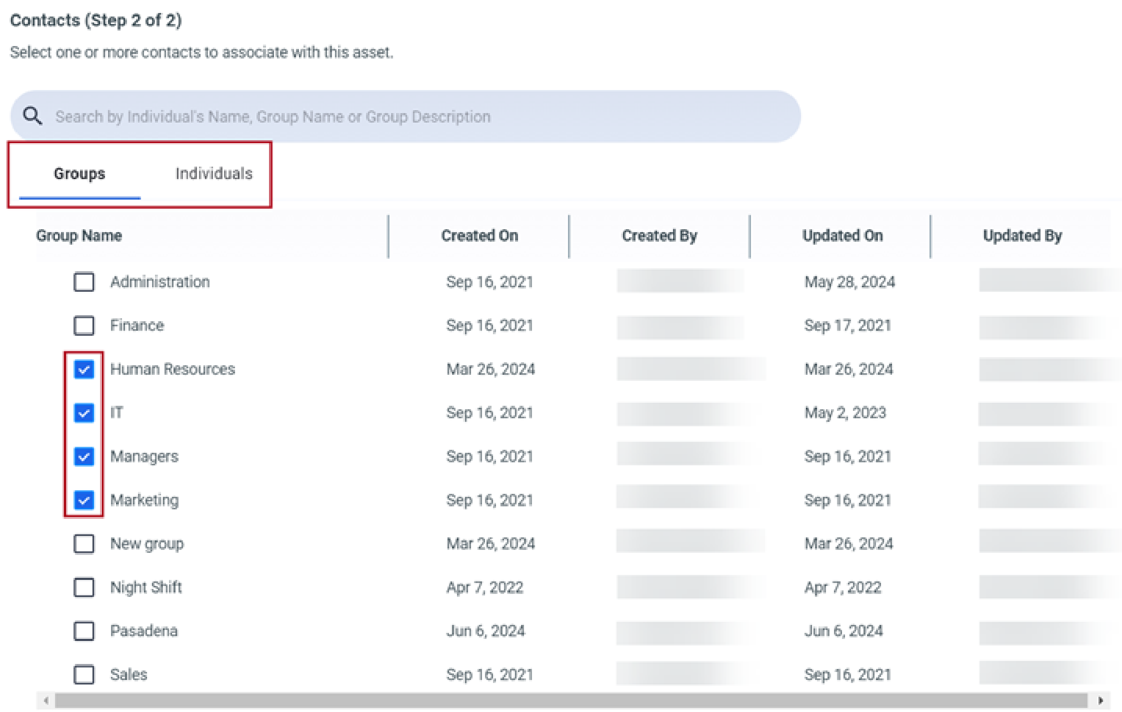
3. The **Edit Asset** modal appears. Select **Add Association**.



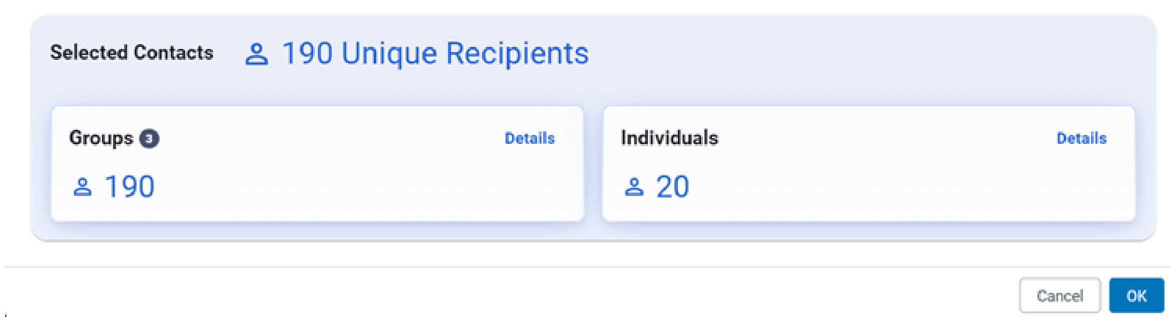
4. Select which type of association you want to define for the selected Asset by choosing an option from the **Association Definition** dropdown.



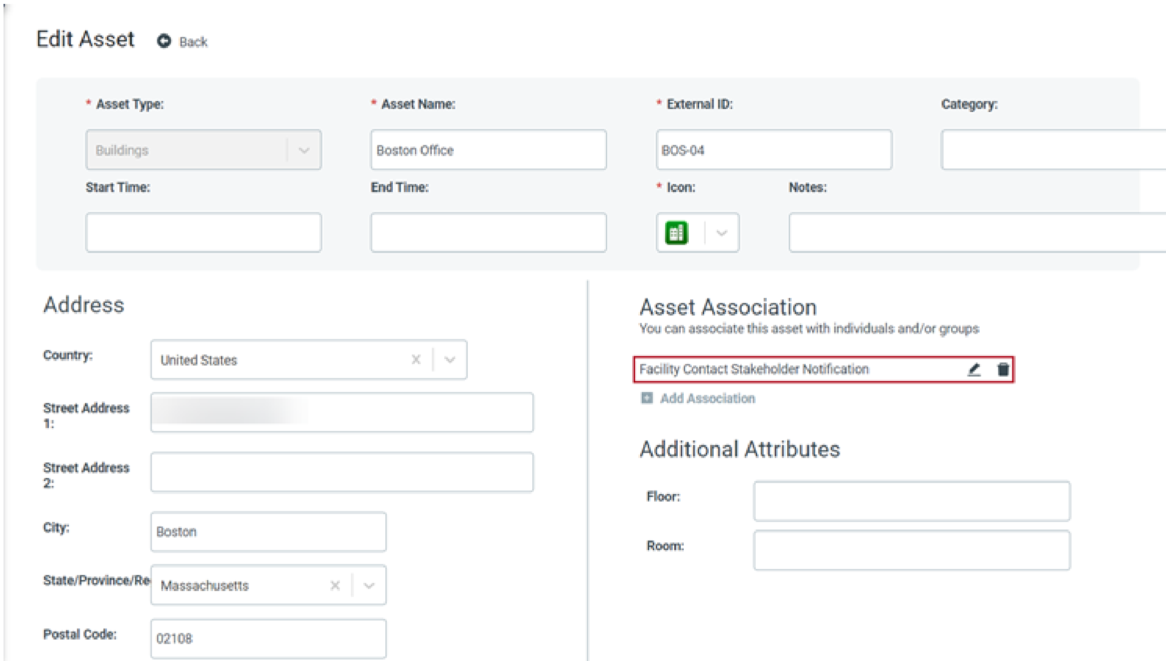
5. Choose Contacts or Contact Groups to associate with this Asset.



6. Check the preview of the targeted Contacts and Groups to make any needed changes, then click **OK**.



7. The new association will now appear in the **Asset Association** section on the selected Asset record.



Managing Asset Associations via File Upload

You can include your Asset-Contact Associations in your Asset file uploads. Once you have defined Asset Association Types in your Organization, your Asset upload templates will include two new columns for each defined Association Type: one for **Contacts** and one for **Contact Groups**.

Data Format: Associated Contacts

For Associated Contacts, the expected format is a pipe ("|")-separated list of Contact external IDs. For example, the "Site Security" Asset Association comprises two individuals, whose contact records have the external IDs "EH1002" and "Anne.Boyle@employee.com", respectively. Both Contacts will be included in "Facility Contact" communications when the associated Asset is affected.

Associated Contacts - Site Security
EH1002|Anne.Boyle@employee.com

Data Format: Associated Contact Groups

For Associated Groups, the expected format is a pipe-separated list of Group names. For example, the "District Managers" Asset Association contains two contact groups: "District 9 Managers" and "District Oversight Committee". All Contacts in either of these Groups will be included in "Facility Contact" communications when the associated Asset is affected.

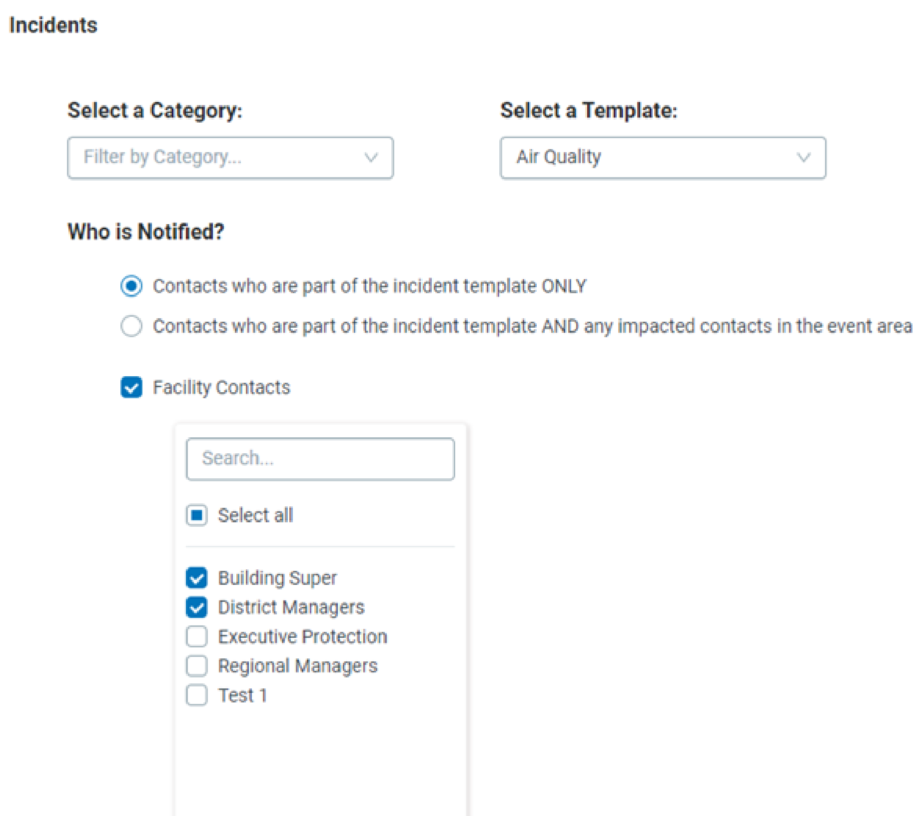
Associated Contact Groups - District Managers
District 9 Managers | District Oversight Committee

	P	Q	R	S	T	U
1	Associated Contacts - District Managers	Associated Contact Groups - District Managers	Associated Contacts - Regional Managers	Associated Contact Groups - Regional Managers	Associated Contacts - Site Security	Associated Contact Groups - Site Security
2		District 9 Managers | District Oversight Committee		East Africa Regional Security Team	EH1002 | Anne.Boyle@employee.com	Kenya Security Team | Nairobi Office Site Security Team

Using Asset Association in Alert Workflows

To use Asset Associations in Alert Workflows:

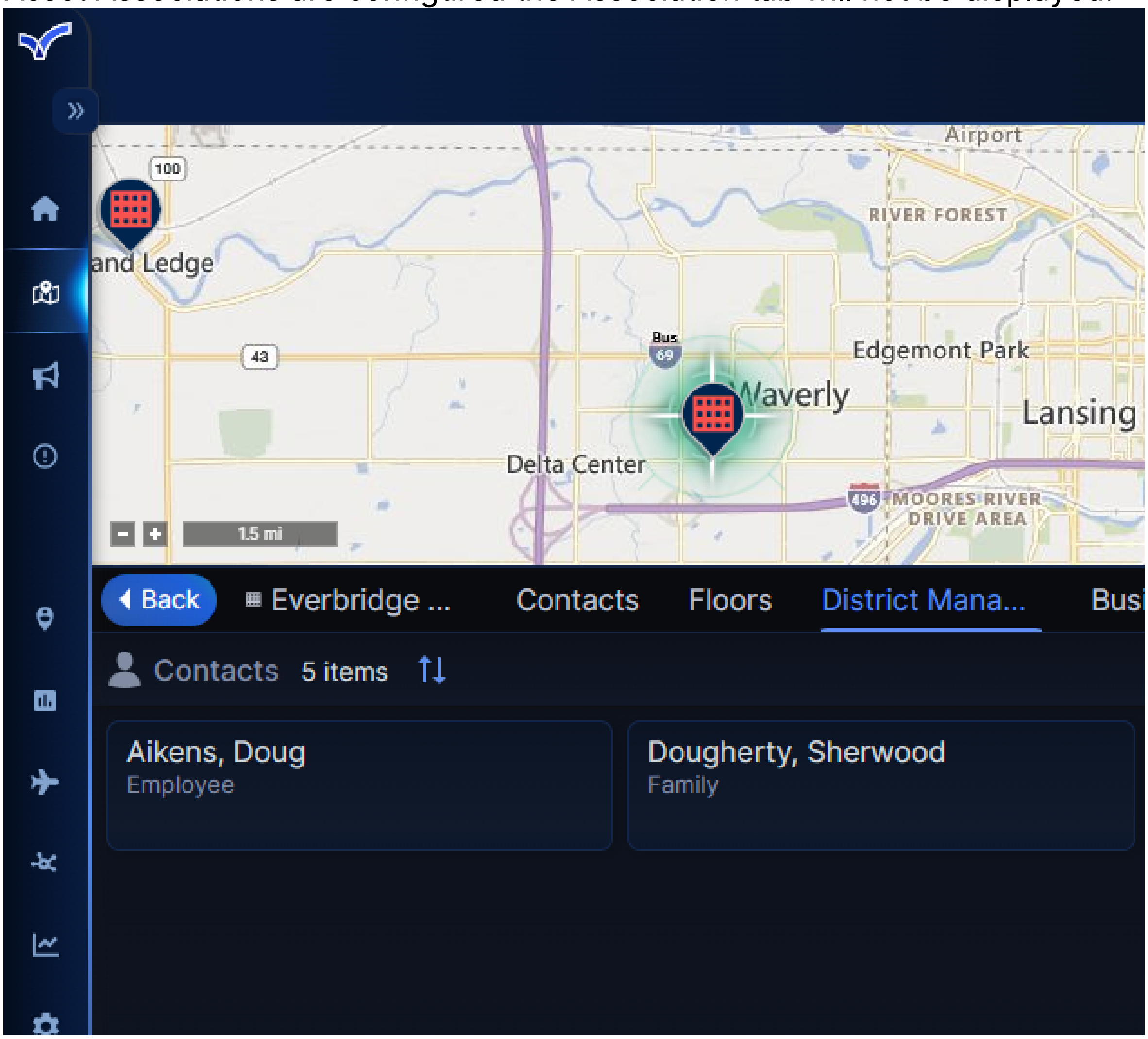
1. Navigate to **CEM Orchestration** > **Workflow List.**
    - The above path isn't available when the Legacy UI is applied, so Workflows can also be created and maintained from **Settings** > **Everbridge Open** > **CEM Orchestration** > **Workflow List**.
2. Select a specific Workflow, then click **Actions.**
3. Under **Incidents** you can select Facility Contacts to be added to your Incident Communications for the Assets affected by the alert.



Viewing Associations in Visual Command Center Operator Console

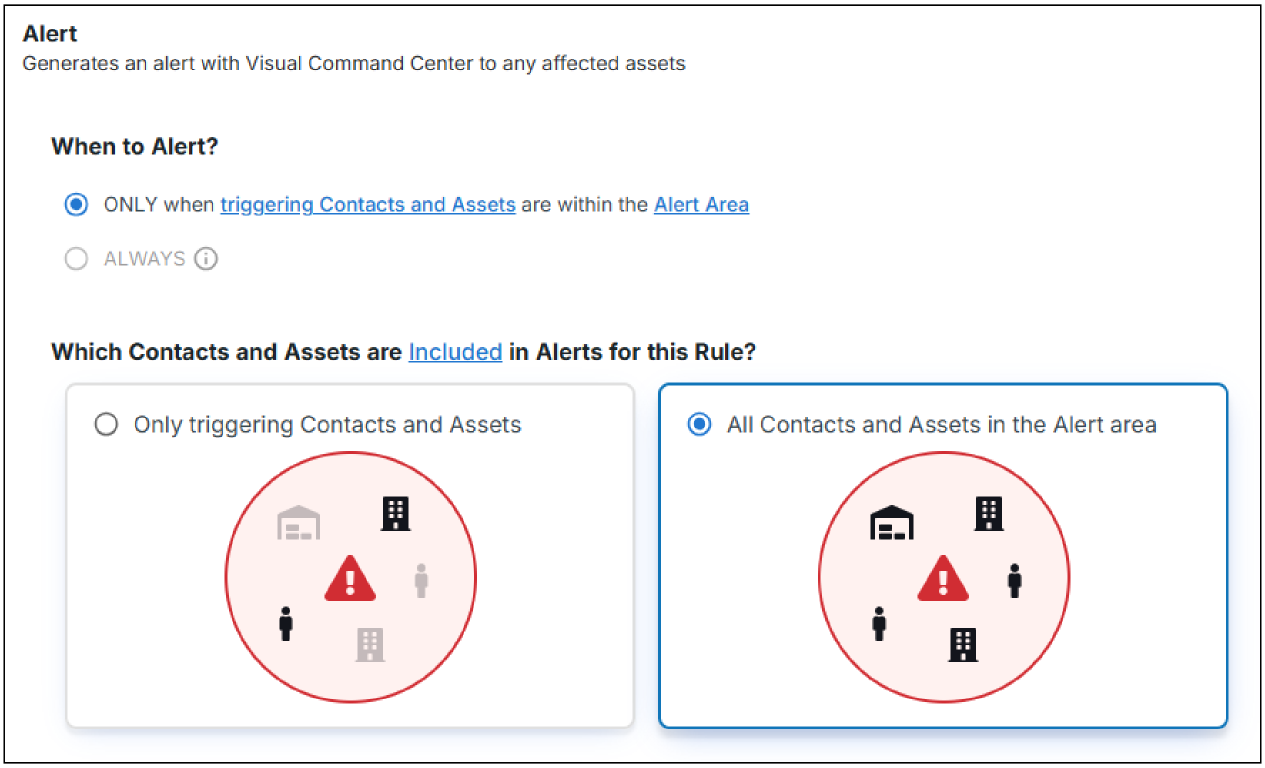
To view Associations in the VCC Operator Console:

1. Navigate to **Situational Awareness** > **Visual Command Center**.
2. Access an Asset for which you've created an Asset Association and added at least one User or Group.
3. The Asset Associations configured for that Asset will be displayed. If no Asset Associations are configured the Association tab will not be displayed.



Configuring Affected Contacts and Assets in CEM Alerts

CEM Orchestration Rules allow users to control which Contacts and Assets are included as "affected" when an Alert is triggered. This helps users understand the full impact of an Alert while maintaining precise control over what can trigger Alerts.



With this configuration, users can:

- Trigger Alerts based on specific Contacts or Assets when they meet Rule conditions
- View the full scope of impacted people and infrastructure
- Avoid overly restrictive Alert conditions

Triggering Contacts and Assets

Triggering Contacts and Assets are those that initiate an Alert when they meet the conditions defined in a CEM Orchestration Rule. They are configured in the **Contacts and Assets** condition within a Rule's Filters.

When these Contacts or Assets are within proximity to a qualifying Risk Event, they can trigger:

- An Alert
- Any additional Actions configured in the Rule

Affected Contacts and Assets

Affected Contacts and Assets are those that appear as “impacted” or “affected” by the Alert when they are located within the Alert’s Impact Area. They will appear in **Affected Assets** lists and variables for Alerts generated by CEM Orchestration Rules.

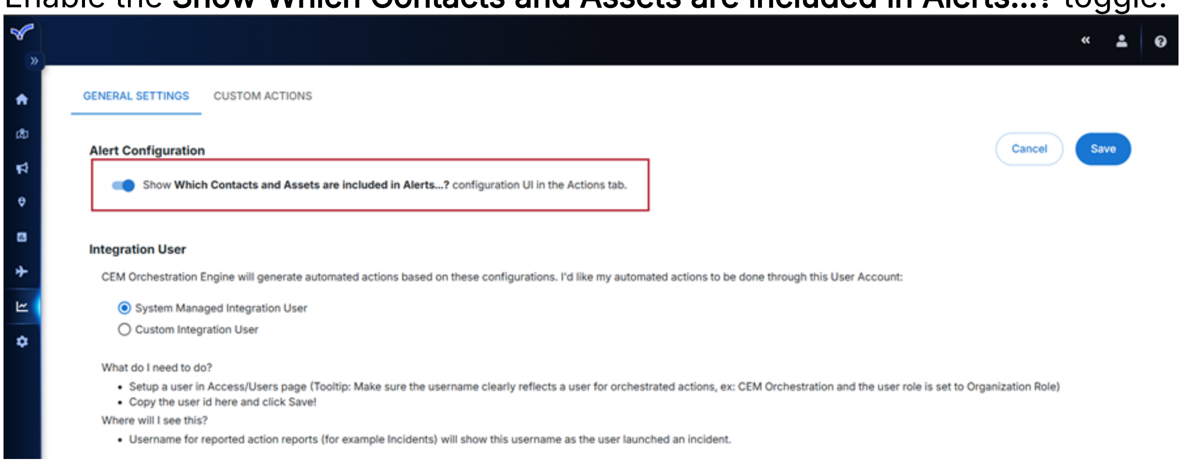
Affected Contacts and Assets do not necessarily have to be the ones that triggered the Alert, depending on how the Rule is configured. This distinction allows users to create Rules that are highly targeted for triggering Alerts while still showing the full scope of impact.

> **IMPORTANT:** Affected Contacts and Assets are determined based on their presence within the Alert area defined by the Rule.

Enabling Affected Contacts and Assets

This capability must be enabled before it is available for use when configuring a Rule. To enable:

1. Navigate to **CEM Orchestration** > **Setup**.
2. Enable the **Show Which Contacts and Assets are included in Alerts...?** toggle.



3. Click **Save**.

Configuring Alert Behavior

Once the above toggle has been turned on, users can define which Contacts and Assets should be included in Alerts by adding the specification to a Workflow's Rule. To do this:

1. Open the CEM Orchestration Workflow and select the desired Rule.
2. Go to the **Actions** tab.
3. Under **Which Contacts and Assets are included in Alerts for this Rule?**, select one of the following options. This setting determines which Contacts and Assets appear as affected in the Alert:
    - **Only Triggering Contacts and Assets (Default)** - The Contacts and Assets that triggered the Alert are shown as affected. Use this option when:
        - Alerts should only display the entities responsible for triggering the Alert
        - The Workflows require tight correlation between triggers and Alert visibility
    - **All Contacts and Assets in the Alert Area** - All Contacts and Assets within the Alert area are shown as affected, even if they did not trigger the Alert. Use this option when:
        - Visibility into the full scope of impact is necessary
        - Not all Assets or Contacts are configured to trigger Alerts
        - Strict triggering conditions with broader impact awareness are required
4. Continue creating or editing the Rule as needed. See [Creating Workflows] for more details.

Asset and Contact Requirements

Assets

Assets must have the **Alertable** flag enabled on their Asset Type to:

- Appear in CEM Orchestration Workflows
- Trigger Alerts

Contacts

Contacts do not require an **Alertable** flag. If the **All Contacts and Assets in the Alert Area** option is selected, all Contacts within the Alert area are included as affected.

Example Use Cases

Targeted Triggering with Full Impact Visibility

Scenario: Alerts trigger only when data centers are affected by a Risk Event, but you also want visibility into employees and other Assets in the area.

- **Configuration**
  - **Triggering Assets**: Data Centers
  - **Affected Assets**: All Contacts and Assets in Alert Area
- **Result**
  - Alerts trigger only for data centers
  - All impacted Contacts and Assets appear in the Alert

Highly Targeted Alert Correlation

Scenario: Alerts should remain tightly tied to specific infrastructure Assets.

- **Configuration**
  - **Triggering Assets**: Critical Infrastructure
  - **Affected Assets**: Only Triggering Contacts and Assets
- **Result**
  - Alerts show only the triggering entities
  - No additional Contacts or Assets are included

CEM Orchestration Use Case Examples

Through CEM Orchestration, you can create combinations of Workflows, Rules, and Filter sets to accommodate a wide variety of use cases. Use the sections below as models to help you create the Alert settings that meet your needs.

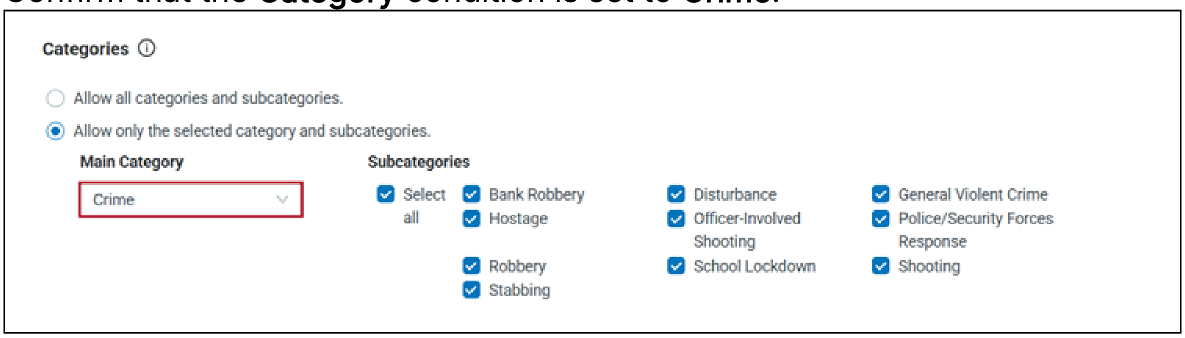
- Changing the Severity Threshold for Alerting
- Changing the Impact Radius for a Risk Event Category
- Varying the Impact Radius Depending on the Event Severity
- Applying "Always Alert" to One Risk Type
- Creating Alerting Criteria for Contacts
- Setting Up Automated Incident Notifications
- Adding Alerting Rules for a Self-Service Risk Event Feed

Changing the Severity Threshold for Alerting

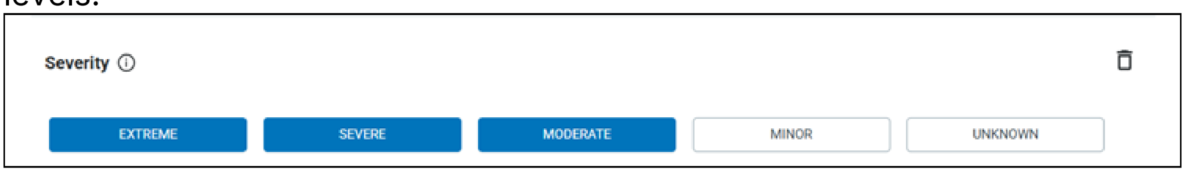
The **Severity of Risk Events** is one of several conditions you can change in your Filters. To set a new Severity threshold for Alerting, find the Workflow and Rules you want to change and then edit the Severity Threshold for each.

For example, if you need to adjust the Severity of Crime events:

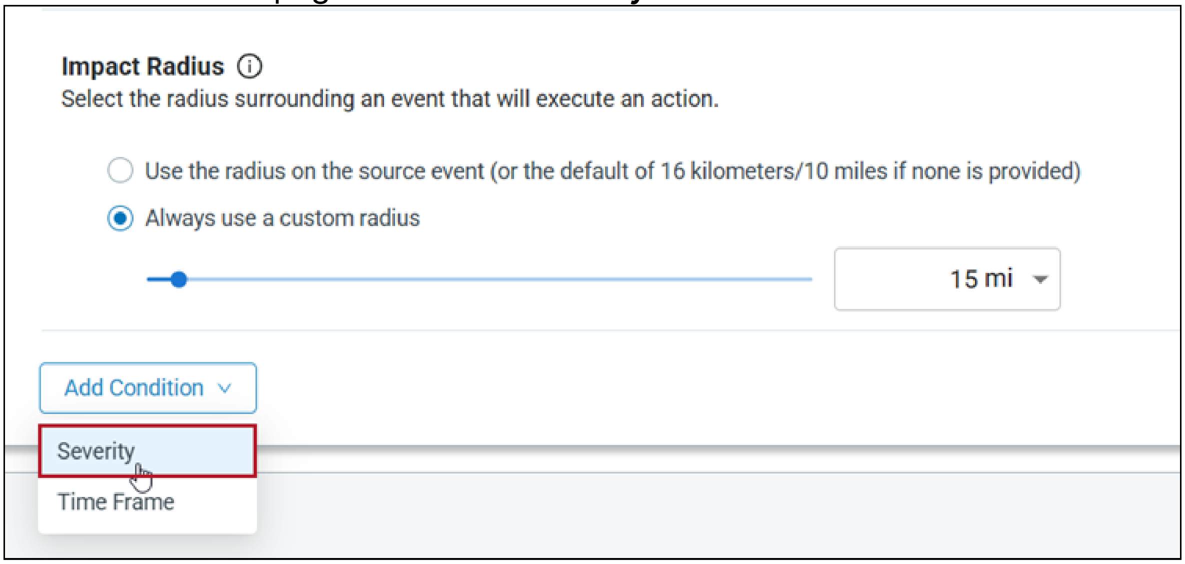
1. Navigate to **CEM Orchestration** > **Workflow List**.
2. Select a Workflow.
3. Select the **Crime** Rule. By default, this Rule will have one Rule that will open automatically.
4. Select a **Filter** tab. The default workflow will have one Filter that will open automatically.
5. Confirm that the **Category** condition is set to **Crime**.



6. Select all **Severity Levels** that apply. For example, to Alert on any Risk Events with moderate or higher Severity, select the Moderate, Severe, and Extreme levels.



7. If no Severity condition is shown, you can add one. Click **Add a Condition** at the bottom of the page and select **Severity** from the menu.



8. Click **Save**.

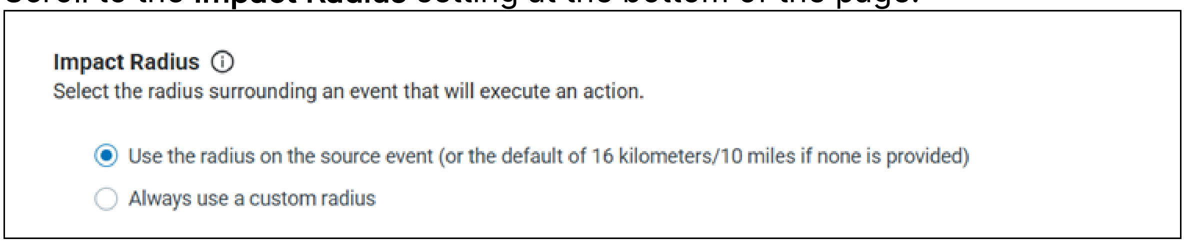
Each Rule could have more than one Filter. You need to make this adjustment for each Filter where you want to set a Severity Threshold.

Changing the Impact Radius for a Risk Event Category

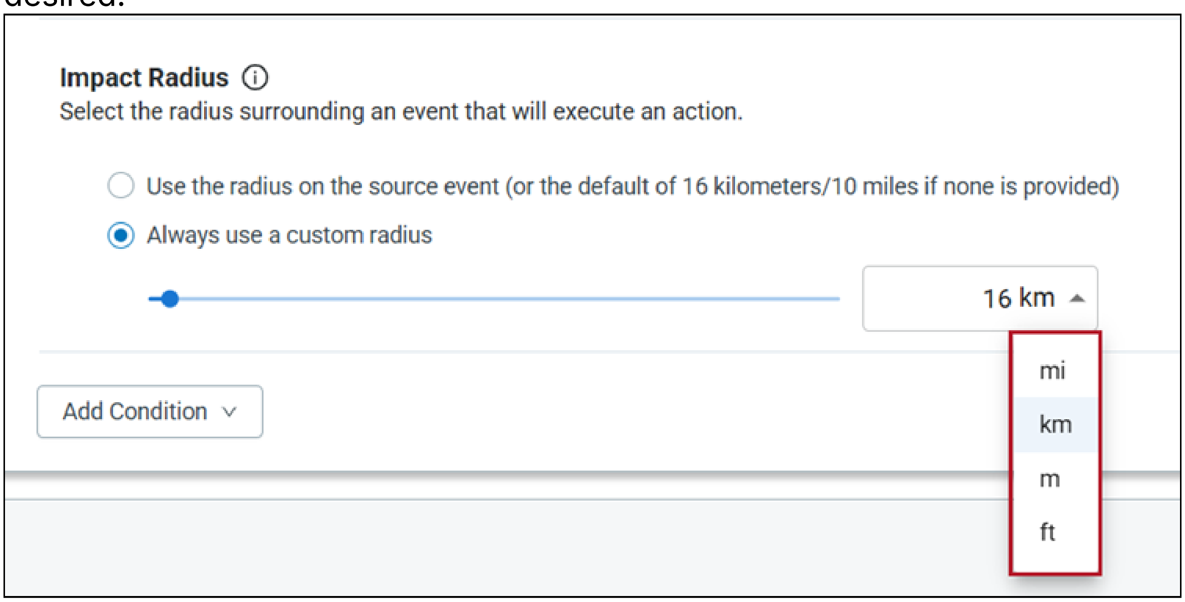
The **Impact Radius**, or Alert Radius, establishes the potential impact area for a Risk Event when the location is a point (not a polygon) on the map. When an Asset is detected within this Impact Radius during a Risk Event's duration, Orchestration creates an Alert. The larger the Radius, the more Alerts are likely to be created. The Radius does not apply to Risk Events whose location is a polygon on the map. For polygon events, the Alert Area is the area within the polygon.

The Impact Radius is one of several conditions you can change in your Filters. To change the Radius for a Risk Event Category:

1. Navigate to **CEM Orchestration** > **Workflow List** page.
2. Select the Workflow you want to change.
3. Select the Rule and Filter you want to change.
4. Scroll to the **Impact Radius** setting at the bottom of the page.



5. If the default option of **Use the radius on the source event** is selected, choose **Always use a custom radius**.
6. Use the drop-down menu to switch between miles and kilometers as desired.



7. Enter a new distance or use the **Impact Slider** to change the Radius.
8. Click **Save.**

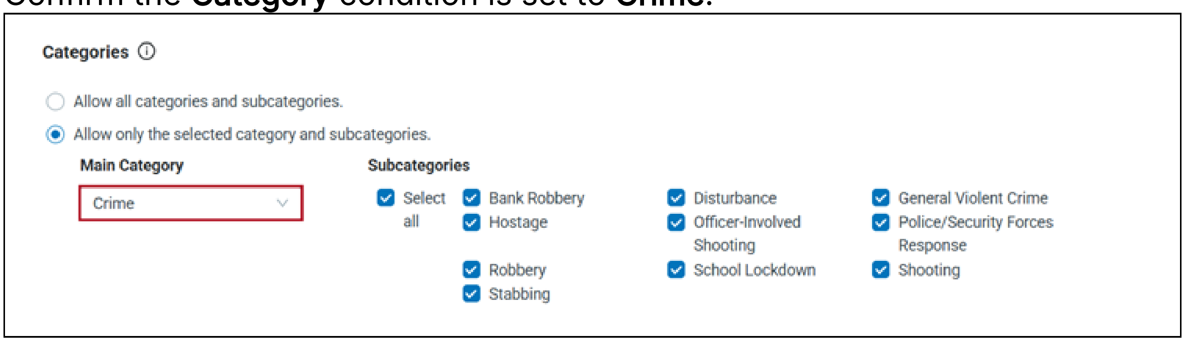
Varying the Impact Radius Depending on the Event Severity

Frequently, organizations will want to use a larger **Impact Radius** for high-Severity events than for events of lower Severity. With an Orchestration Rule, you can do this by creating separate Filters, one for the more severe events, and one for events that are expected to have a smaller, more local impact.

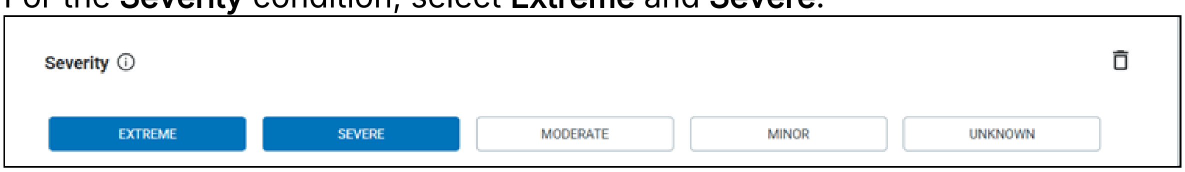
When you need to use **different conditions**, create a new **Filter**. If you need to take **different actions**, create a new **Rule**.

In this example, we want to use a different condition (a larger Impact Radius) for Crime events with a severity of Severe or Extreme, and a smaller Radius for events with a Severity of Moderate or Minor:

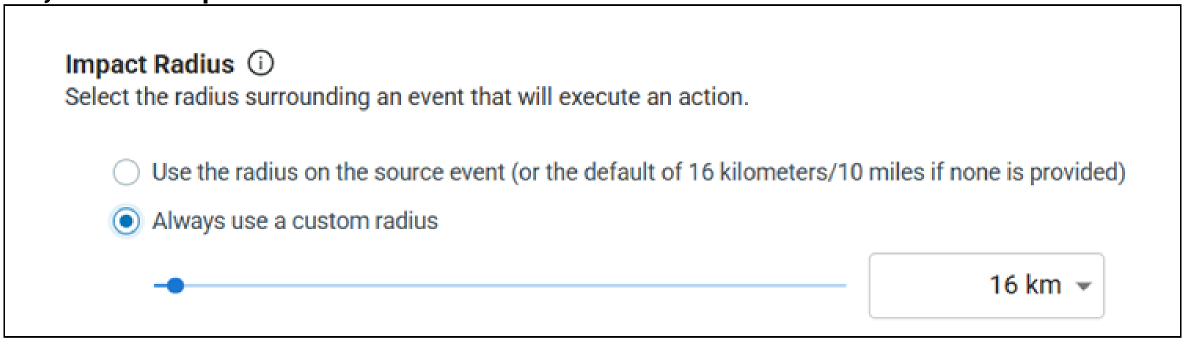
1. Navigate to **Workflow** > **CEM Orchestration** > **Workflow List** page.
2. Click on the desired Workflow.
3. Select the **Crime** Rule. By default, this Workflow will have one Rule that will open automatically.
4. Select a Filter. The default Workflow will have one Filter that will open automatically.
5. Confirm the **Category** condition is set to **Crime**.



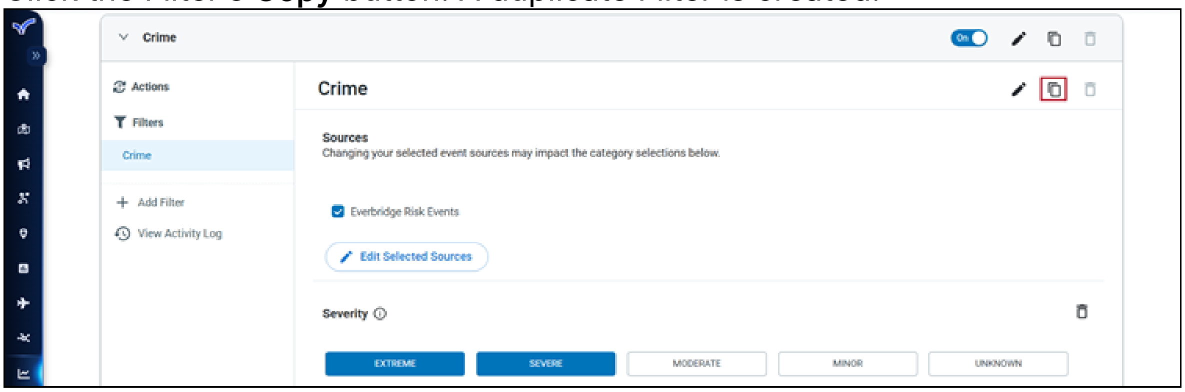
6. For the **Severity** condition, select **Extreme** and **Severe**.



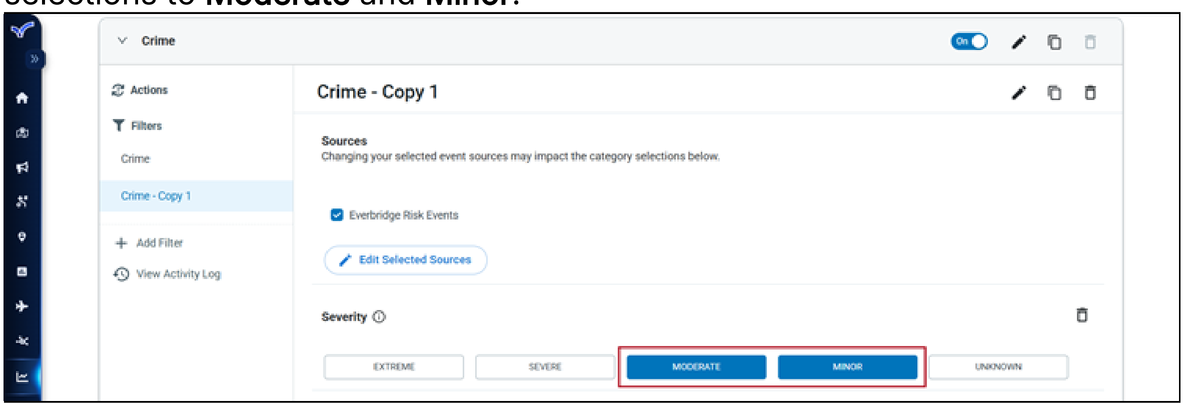
7. Adjust the **Impact Radius** condition to the desired value.



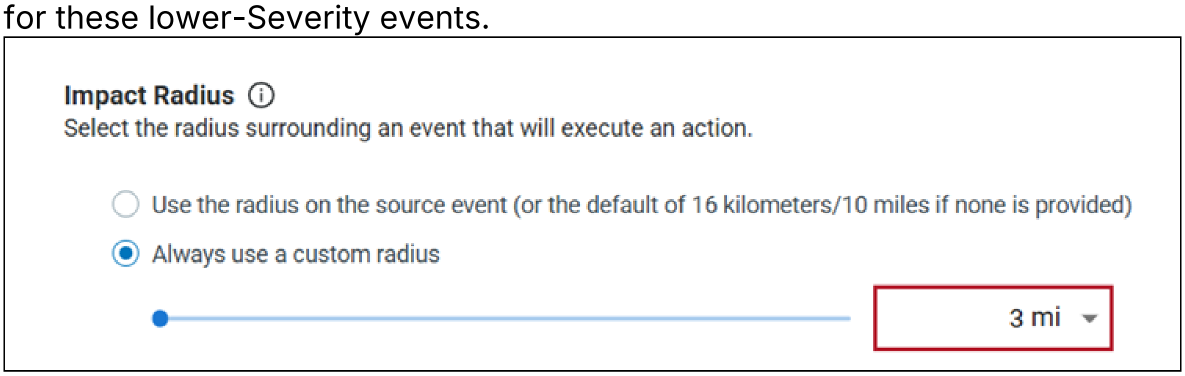
8. Click the Filter's **Copy** button. A duplicate Filter is created.



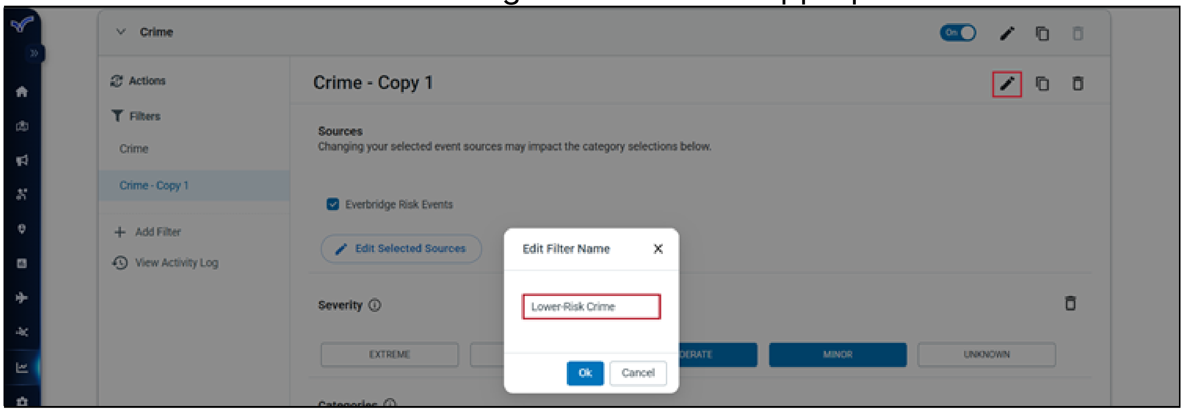
9. The copied Filter will open. Scroll to the **Severity** condition and change the selections to **Moderate** and **Minor**.



10. Adjust the **Impact Radius** condition to the desired value. Use a smaller radius for these lower-Severity events.



11. Use the **Edit** button on the tab to give the Filter an appropriate name.



12. Click **Save**.

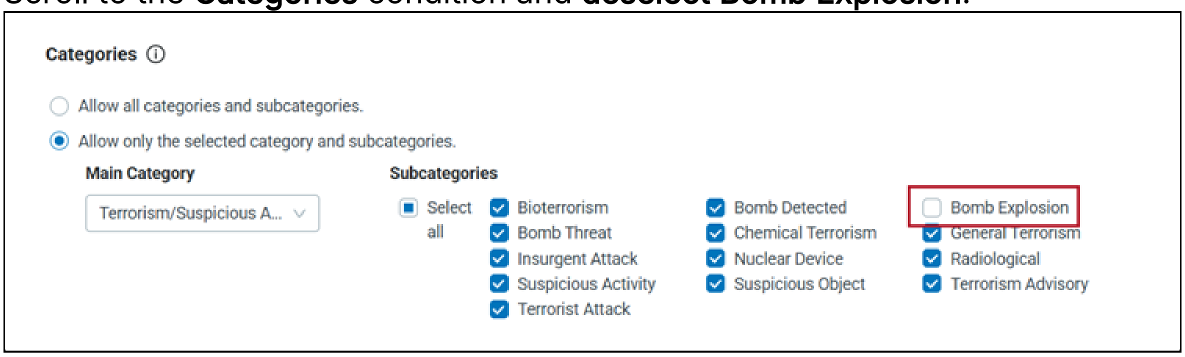
Applying "Always Alert" to One Risk Type

CEM Orchestration lets you take different Actions for different types of Risk Events. In this example, we will apply the **Always Alert** setting to the Alert Action for a single Risk Event subcategory. This means that Alerts will be created for Risk Events in that subcategory, even if there are no Assets or Contacts nearby.

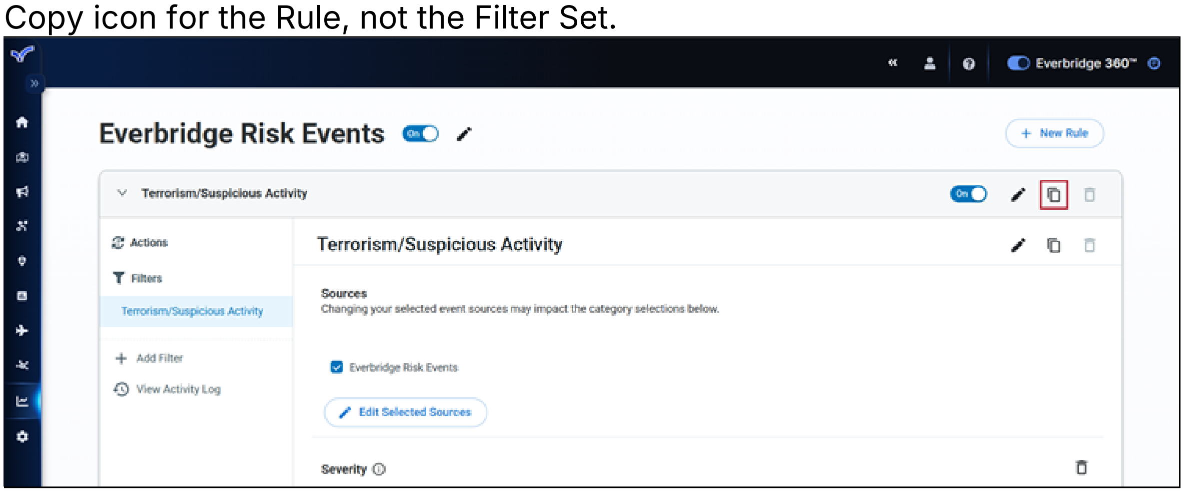
For example, because we want to take a different Alert Action, we will create a new Rule in the Everbridge Risk Events Workflow with the Category of **Terrorism/ Suspicious Activity**, and configure it to always alert only for events in the **Bomb Explosion** subcategory.

To create a new Rule:

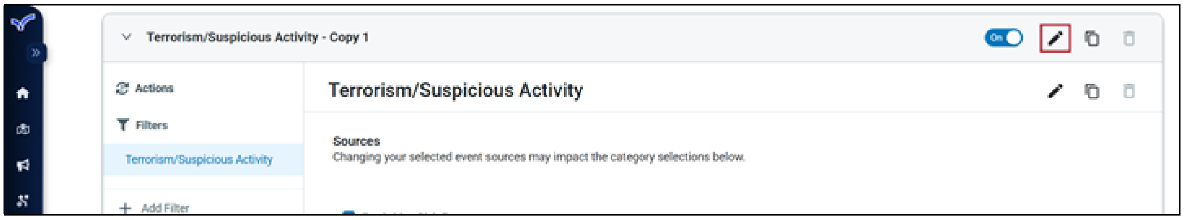
1. Select the Workflow to change. By default, the Workflow will have one Filter Set that opens automatically. If additional Filter Sets exist, select the one you want to edit.
2. Scroll to the **Categories** condition and **deselect Bomb Explosion**.



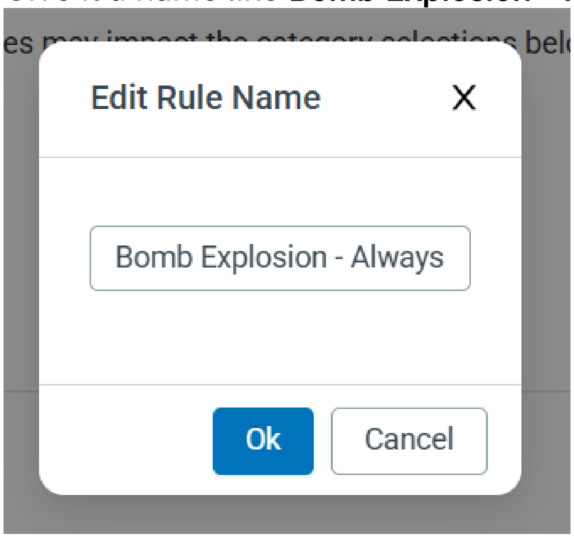
3. Scroll back up to the Rule name and click the **Copy** icon. Be sure to select the Copy icon for the Rule, not the Filter Set.



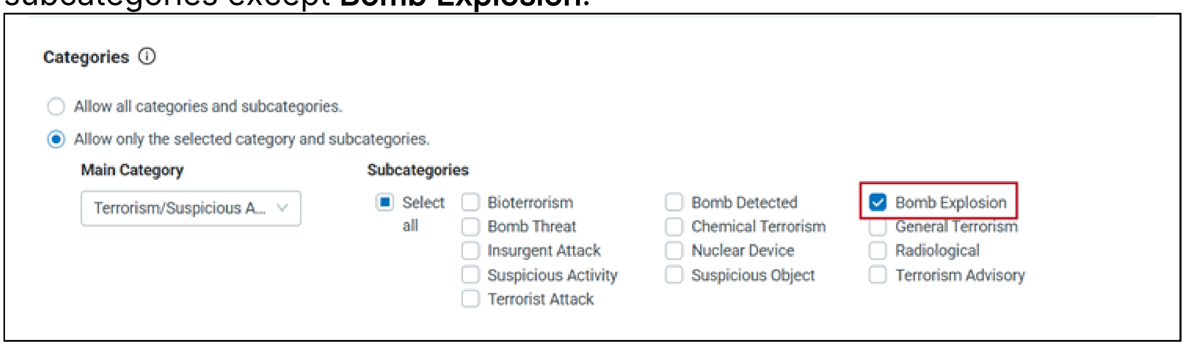
4. A new Rule is created with a default name. Click the **Pencil** icon on the Rule header.



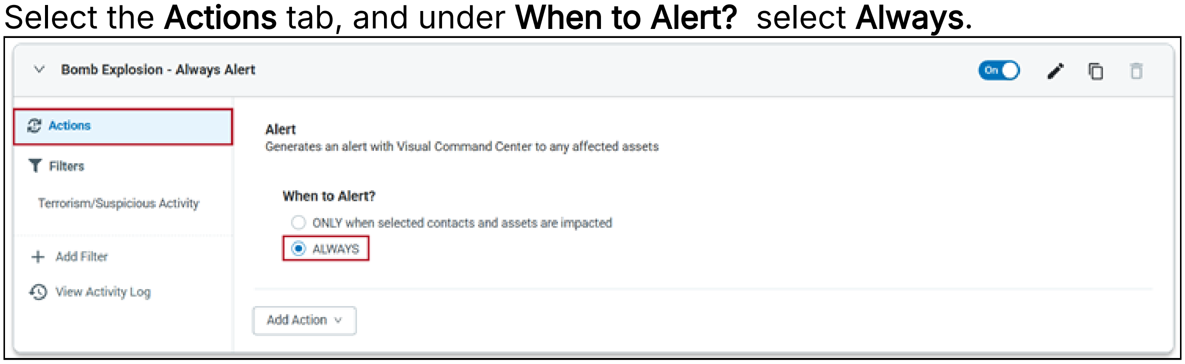
Give it a name like **Bomb Explosion – Always Alert.**



5. With a Filter selected, under the **Categories** condition, deselect all event subcategories except **Bomb Explosion**.



6. Select the **Actions** tab, and under **When to Alert?** select **Always**.



7. Click **Save**.

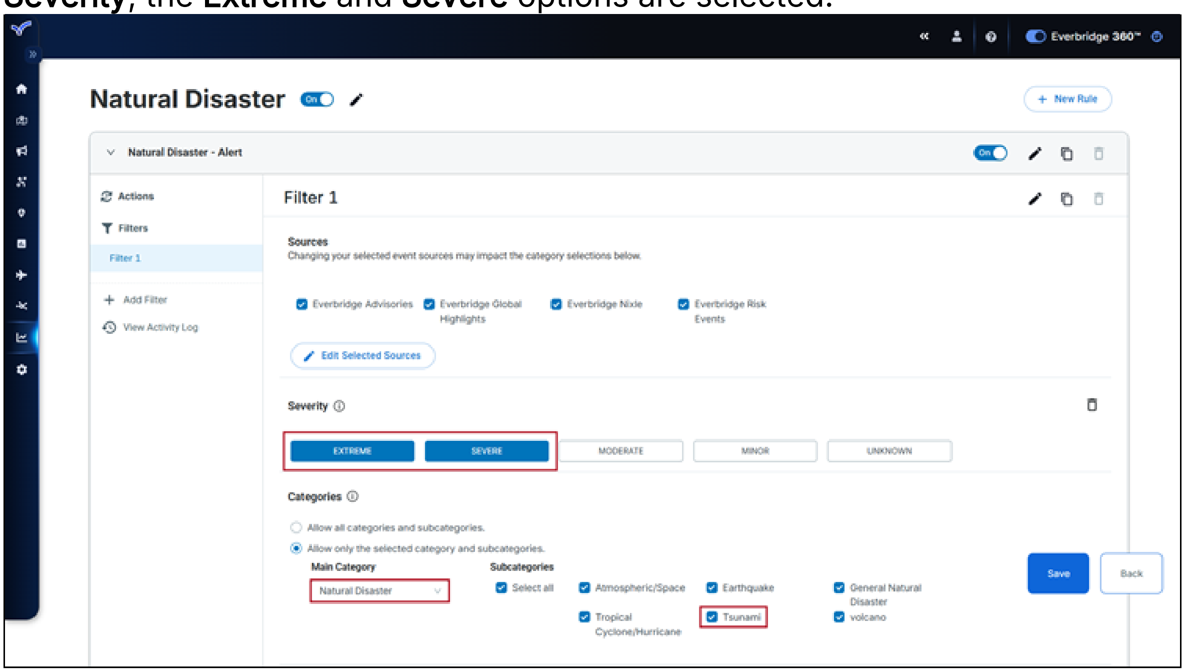
Creating Alerting Criteria for Contacts

CEM Orchestration enables you to configure Alerting for Contacts of different **Types** and **Groups** when impacted by a Risk Event in their **Static Location** (home, office, etc.), their **Last Known Location**, or their **Expected Location** when traveling. This lets you have different Alerting thresholds or launch different Incident templates that target different Contact Groups.

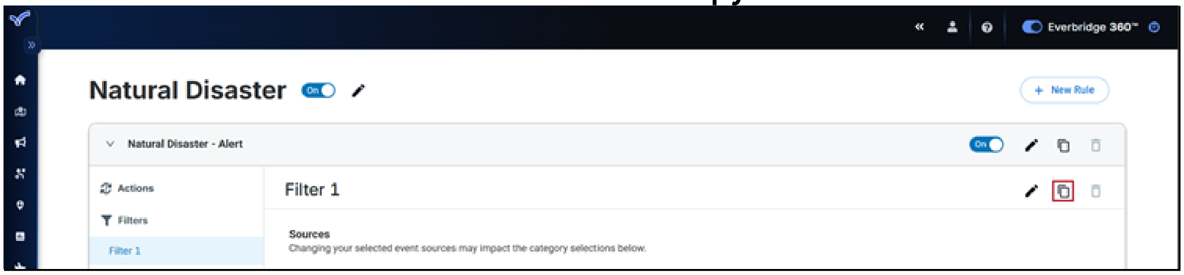
In this example, we will configure different Alerting criteria for a particular group of Contacts. We have a Workflow that is configured to generate Alerts for tsunamis of **Severe** or **Extreme Severity** near any of our Contacts, but because we are especially concerned about tsunamis affecting our employees in Japan, we want to alert on tsunamis of all Severities near these employees.

To do this, we need to create a separate Filter set in the **Natural Disaster** Workflow. We have also assigned all of our Contacts located in Japan to a Contact Group named **Japan Contacts.**

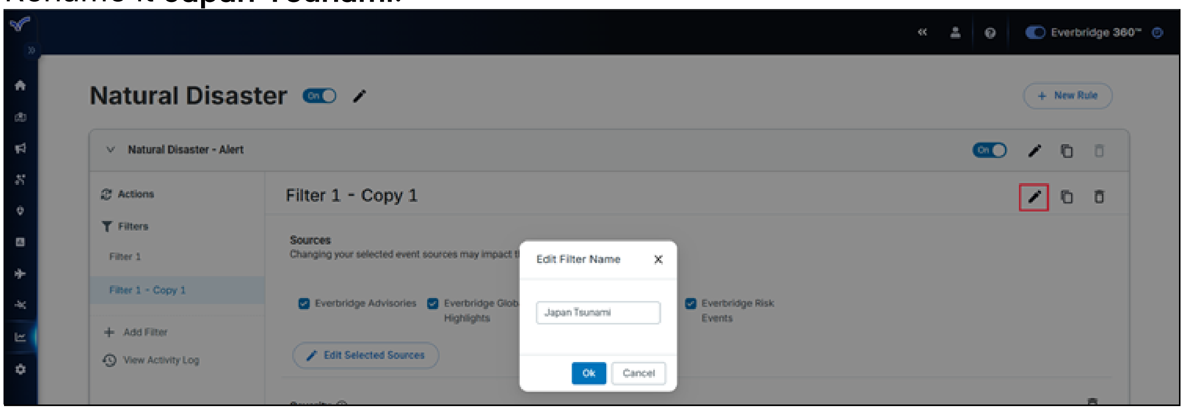
1. From the **Workflows** page, select the **Natural Disaster** workflow.
2. Select the existing Rule and the Filter.
3. Note that the subcategory **Natural Disaster** > **Tsunami** is selected, and under **Severity**, the **Extreme** and **Severe** options are selected.



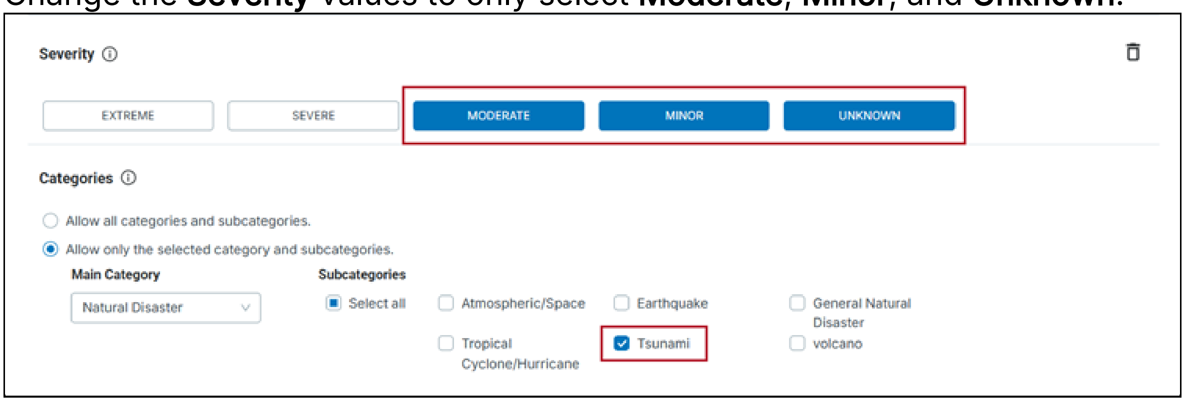
4. Click the **Copy** icon to duplicate the existing Filter. A new Filter is created in this Rule with the default name **Filter Set 1 – Copy 1.**



5. Select the new Filter and click the **Edit** icon to change the Filter name. Rename it **Japan Tsunami**.

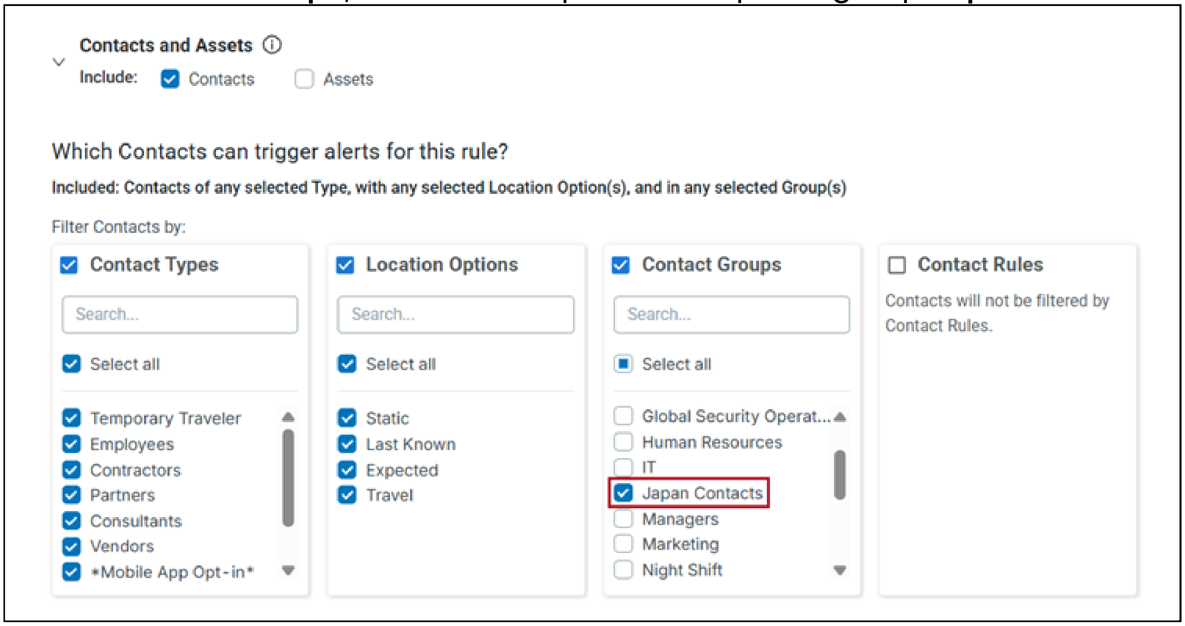


6. Under **Subcategories**, select only **Tsunami**.
7. Change the **Severity** values to only select **Moderate**, **Minor**, and **Unknown**.



8. Scroll to **Contacts** and **Assets** and deselect **Assets**.

9. Under **Contact Groups**, deselect all options except the group **Japan Contacts**.



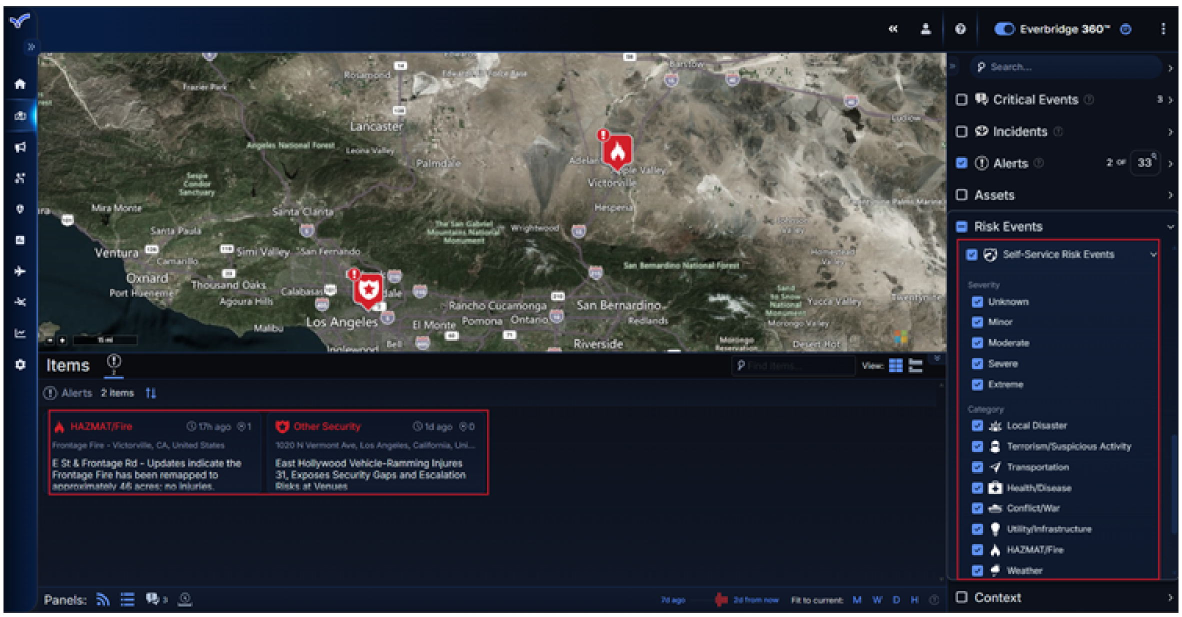
10. Click **Save.**

Adding Alerting Rules for a Self-Service Risk Event Feed

In addition to the many Risk Feeds that Everbridge offers, the **Self-Service Risk Events** feed allows you to send your exclusive Risk data or data from a third party to your Everbridge Organization using a RESTful API. For more information, see the Self-Service Risk Events Guide.

To add Alerting Rules for a Self-Service Risk Event Feed:

1. Make sure your that **Risk Event Feed** is set up correctly and that you can see the Risk Events from that feed in **Visual Command Center**.



2. Navigate to **CEM Orchestration** > **Workflow List**.

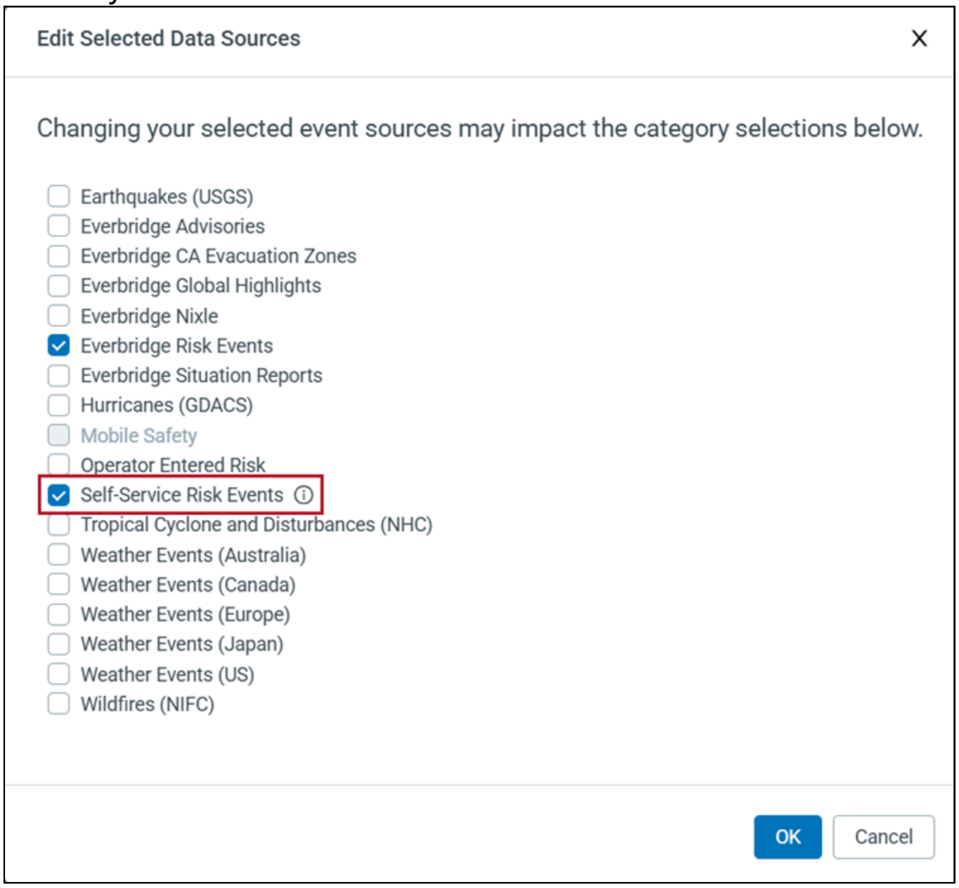
Considering the Risk data that you expect from this Self-Service Risk Feed, review the Workflows available in your Organization.

Adding the Self-Service Feed to Existing Workflows

If you expect that Risk Events from the Self-Service Feed will fall under the Categories covered by existing Workflows, follow these steps to manage Alerts for this Feed in these existing Workflows:

1. Open each Workflow you'd like to add this new Feed to.
2. Under the **Sources** section, click **Add Additional Source**.

3. Select your new source from the list and click **OK**.



4. Click **Save**.

Creating a Separate Workflow for the Self-Service Feed

To create a separate Workflow to manage Alerting for this Feed:

1. Click **New Workflow** on the **Workflow** page.
2. Name your new Workflow something that makes it easy for you and others to understand the type of Risk Event it covers.
3. Consider the **Risk Category** and the **Source Name**.
4. Under **Sources**, click the **Add Additional Source** link and select your Self-Service data source from the list.
5. Select the affected **Contacts** or **Assets** to Alert on.
6. Set the **Impact Radius**.
7. To set a threshold for another Alert attribute, for example, Severity or Category, click **Add Condition** and select the attribute.
8. Select threshold values for any attributes you add.
9. Click **Save**.