Physical Security User 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

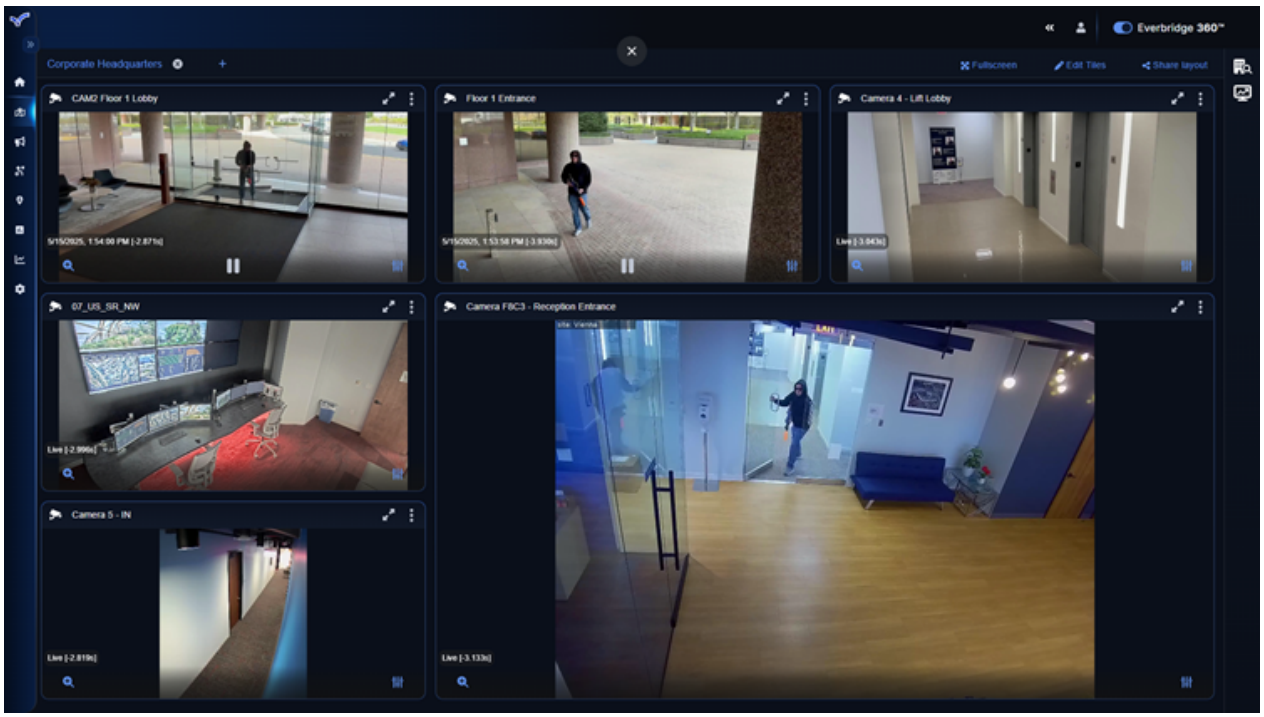
Visit us at www.everbridge.com

What is Everbridge Physical Security?

Video integration with Everbridge 360™ provides secure direct access to your Organization's security cameras when dealing with Risk Alerts. Immediate eyes on the ground:

- Improves comprehensive situational awareness
- Fosters better coordination and
- Promotes swift responses to internal and external threats impacting your Organization.

CCTV Video integration with Everbridge 360™ allows stakeholders to determine quickly and efficiently if their assets have been impacted, allowing for a more appropriate response and minimizing unnecessary disruption and time to resolution.



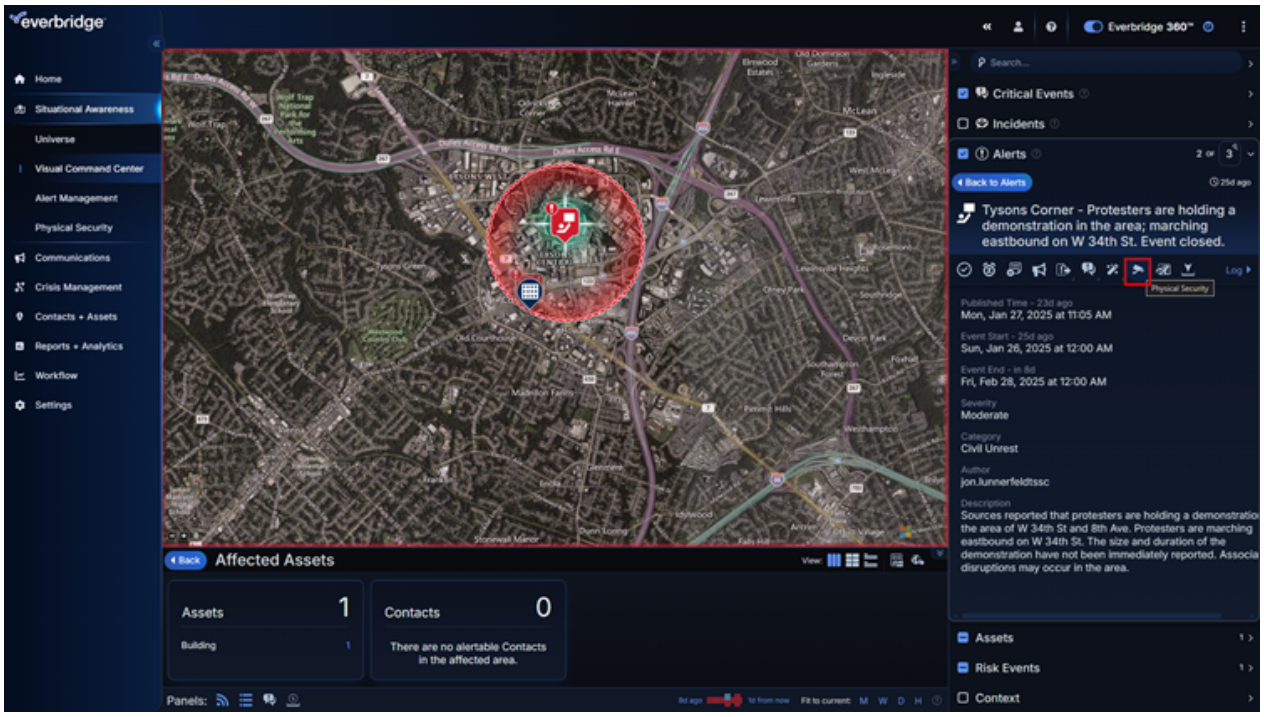
Unifying various types of video sources from multiple locations into a single, secure user interface enhances your Organization's ability to detect and respond to potential security threats or emergencies. With the seamless integration of CCTV video into Everbridge 360™, your Organization can experience the benefits of a single platform which can monitor, visualize, correlate, and alert in real-time.

NOTE: Physical Security is available as an add-on for Everbridge 360 Enterprise and Enterprise customers.

Working With Video

Viewing Cameras for an Alert

To view CCTV cameras for an Alert, select the Alert to view the **Alert** panel. Select the camera icon from the **Alert** menu. If the icon isn't visible, you might have to click **...** to reveal more Alert options.



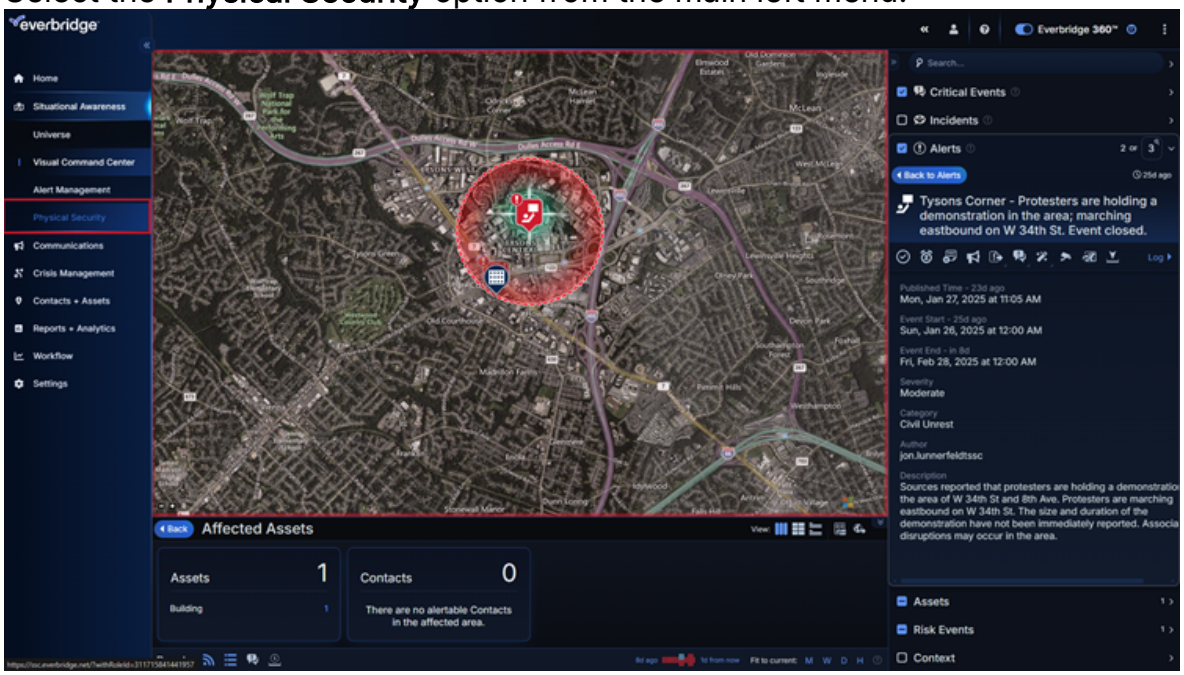
CCTV cameras are opened in a separate browser tab. You can move the tab to a separate screen or dock it to the side of the screen in order to see cameras while managing the Alert.

> **NOTE:** Cameras are only accessible if they have been associated with the asset related to the Alert. For more information about how to associate assets with Alerts, see the Configuration section.

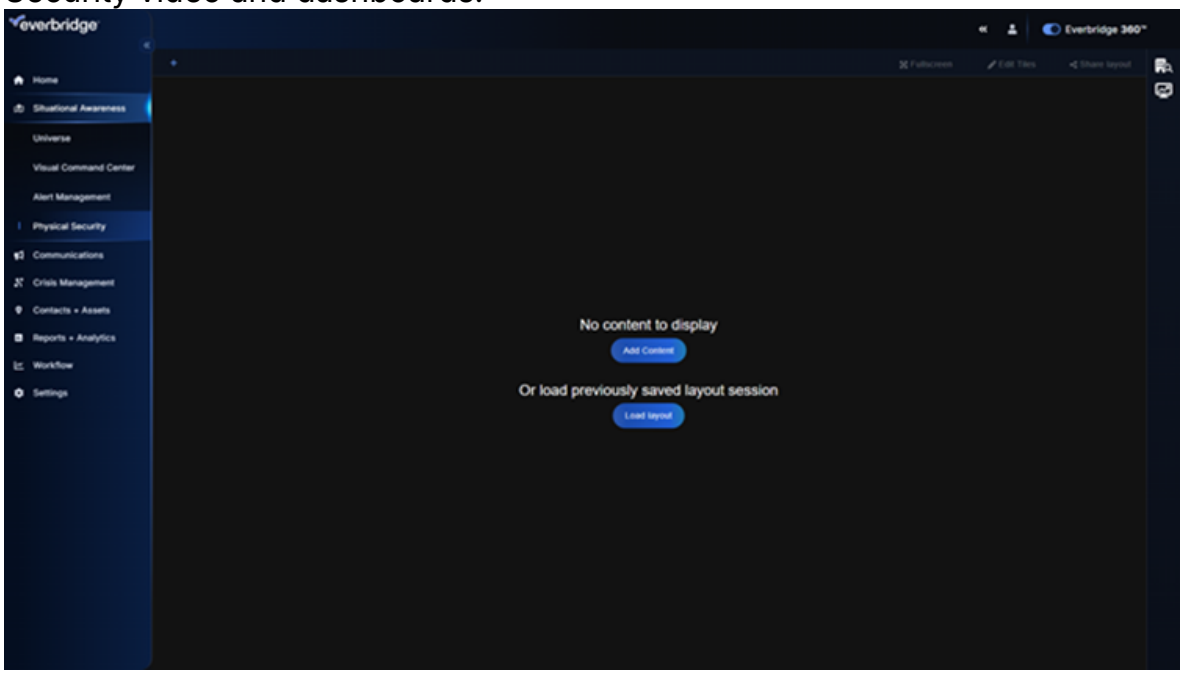
Viewing Video From Any Camera

To access video from any camera:

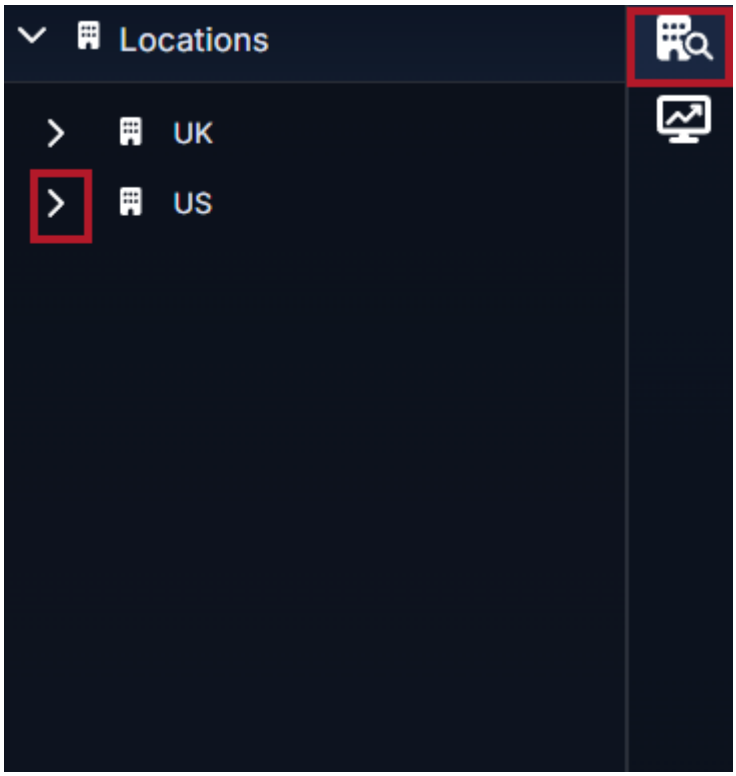
1. Select the **Physical Security** option from the main left menu.



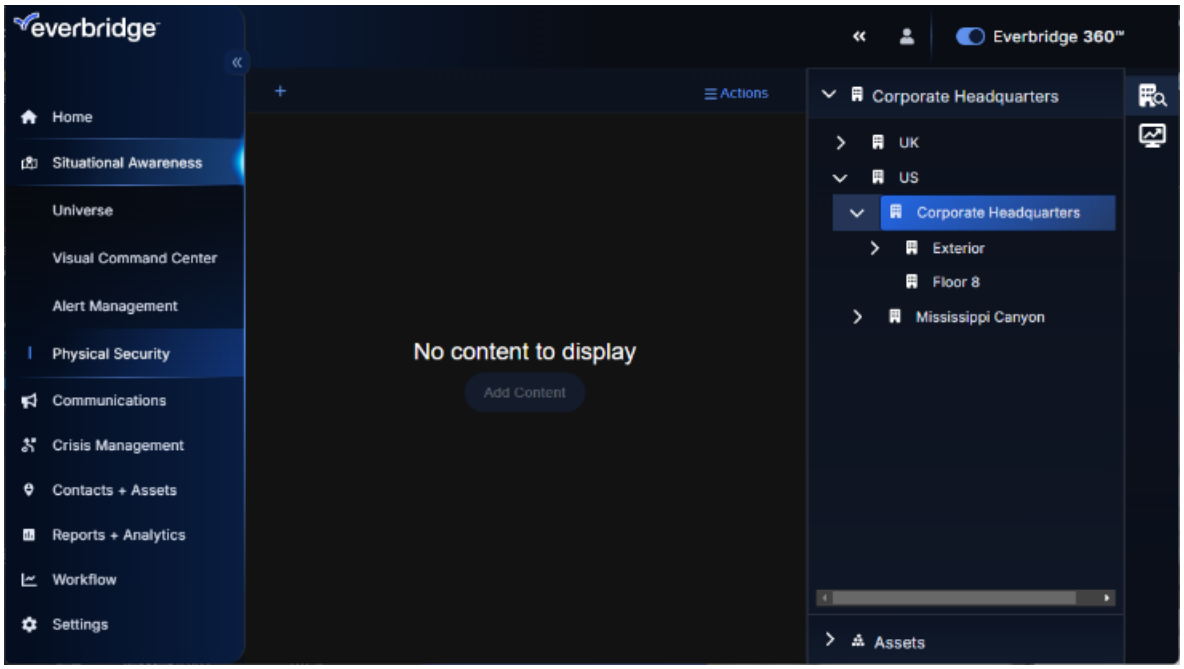
2. The **Physical Security** screen appears, where you can access Physical Security video and dashboards.

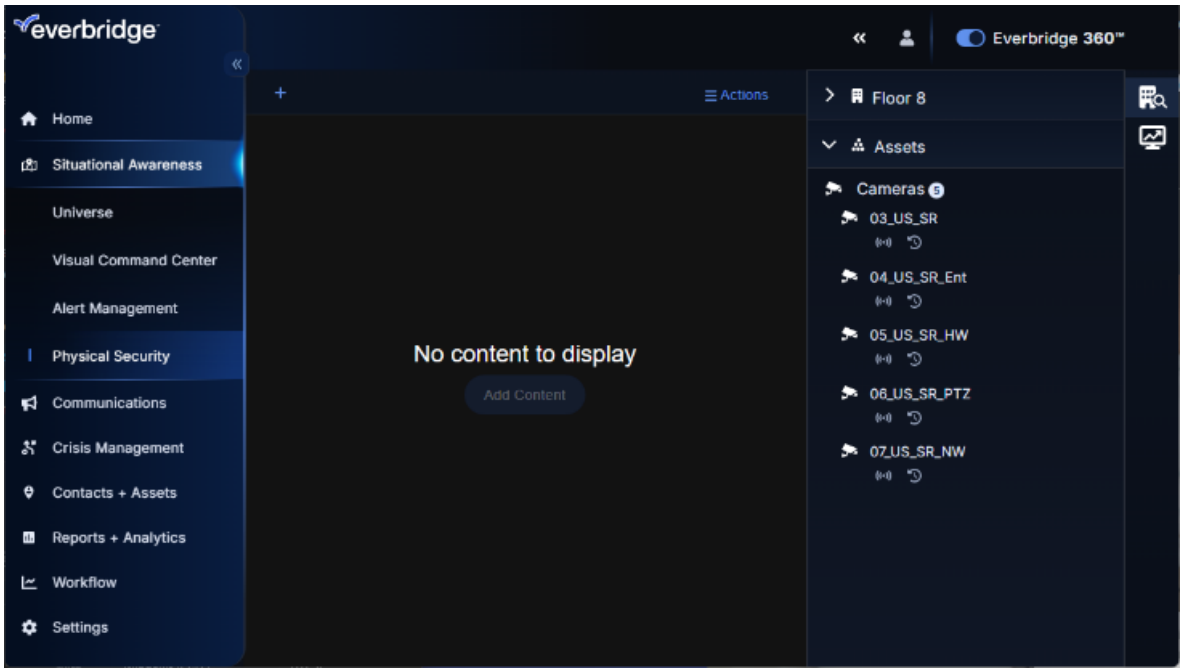


3. Select the location icon on the right and browse to the location of the cameras.

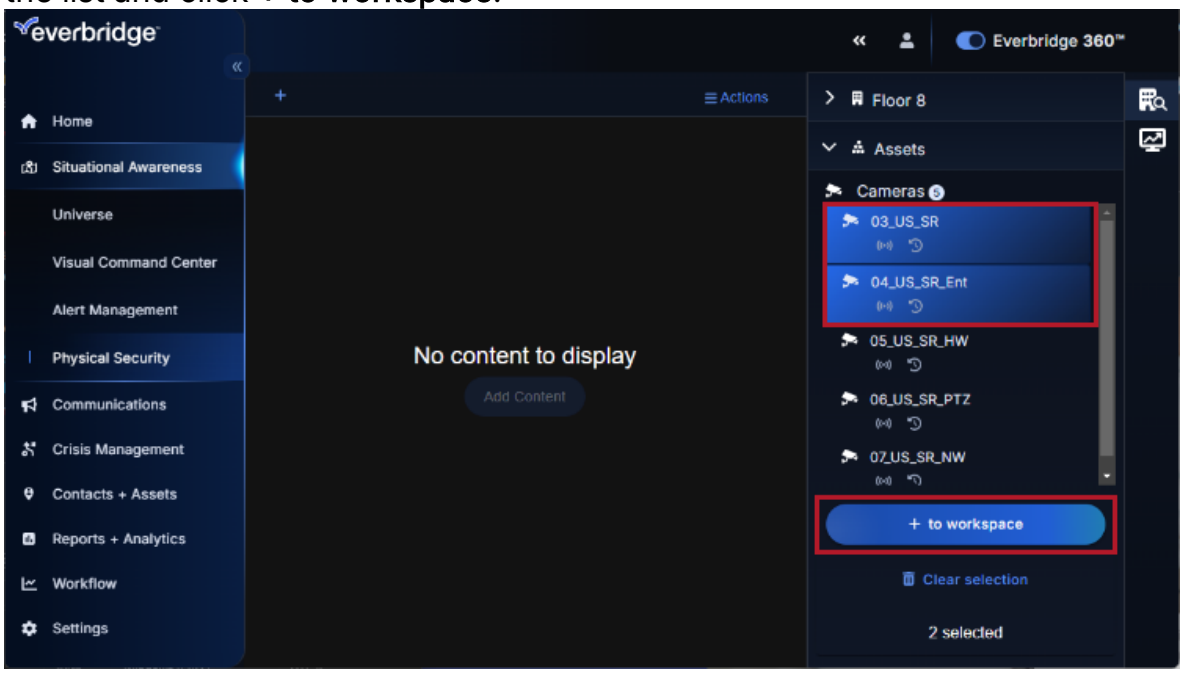


4. Browse the available locations and sub-locations. Select a location to view cameras within the location.

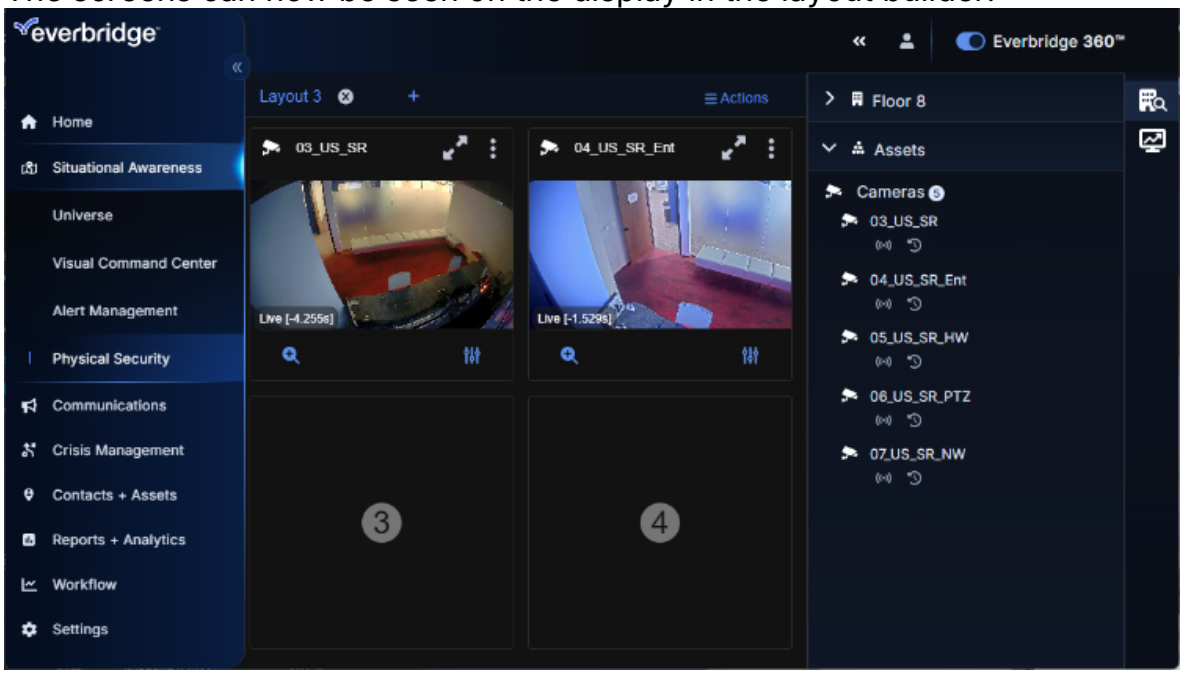

everbridge
Everbridge 360™
Home
Situational Awareness
Universe
Visual Command Center
Alert Management
Physical Security
Communications
Crisis Management
Contacts + Assets
Reports + Analytics
Workflow
Settings
Actions
No content to display
Add Content
Corporate Headquarters
UK
US
Corporate Headquarters
Exterior
Floor 8
Mississippi Canyon
Assets


everbridge
Everbridge 360™
Home
Situational Awareness
Universe
Visual Command Center
Alert Management
Physical Security
Communications
Crisis Management
Contacts + Assets
Reports + Analytics
Workflow
Settings
Actions
No content to display
Add Content
Floor 8
Assets
Cameras 5
03_US_SR
04_US_SR_Ent
05_US_SR_HW
06_US_SR_PTZ
07_US_SR_NW

5. To view video from one or more cameras, select one or more cameras from the list and click **+ to workspace**.



6. The screens can now be seen on the display in the layout builder.



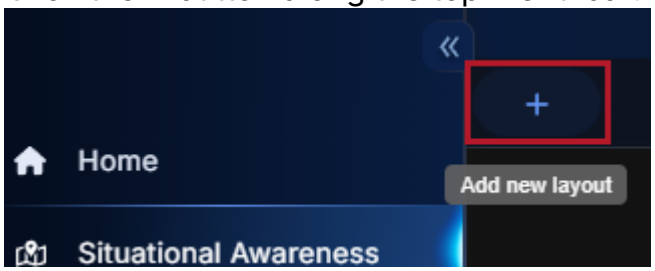
Layouts, Tiles, and Grids

The video workspace allow you to open one or more layouts. The tile grid style can be configured for each layout.

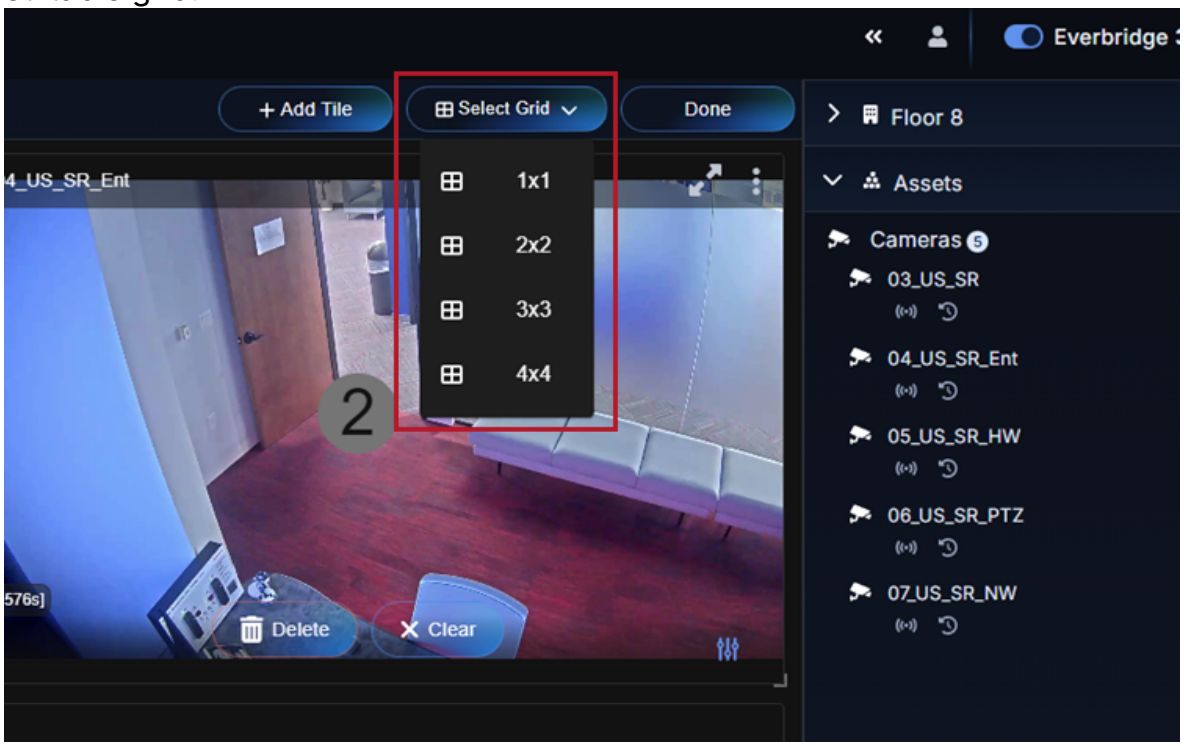
Adding New Layouts

To add layouts:

1. Click the **+** button along the top menu bar.

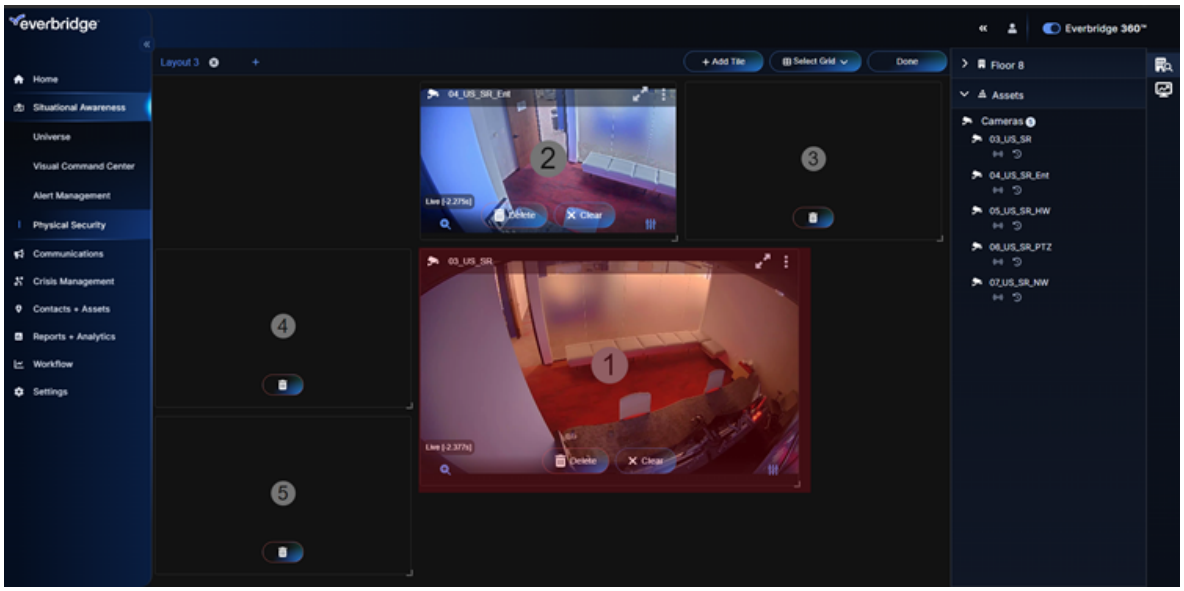


2. A new layout is added to the video layout area. To change the grid style of the layout, select **Edit Tiles**. Use the **Select Grid** drop down menu to select a suitable grid.



3. Add new tiles by clicking on the **+ Add Tile** button. If needed, they can be removed again by clicking **Delete** on the tile.

4. Assign cameras to specific tiles by dragging them from the right-hand asset tree to a tile.



5. Once satisfied with a Layout, click **Done** to exit edit mode.

Stream Options

Depending on capability, different cameras will provide additional options such as access to playback, changing stream quality, etc. To view stream options, select the **Stream Options** button.

Accessing Recorded Video

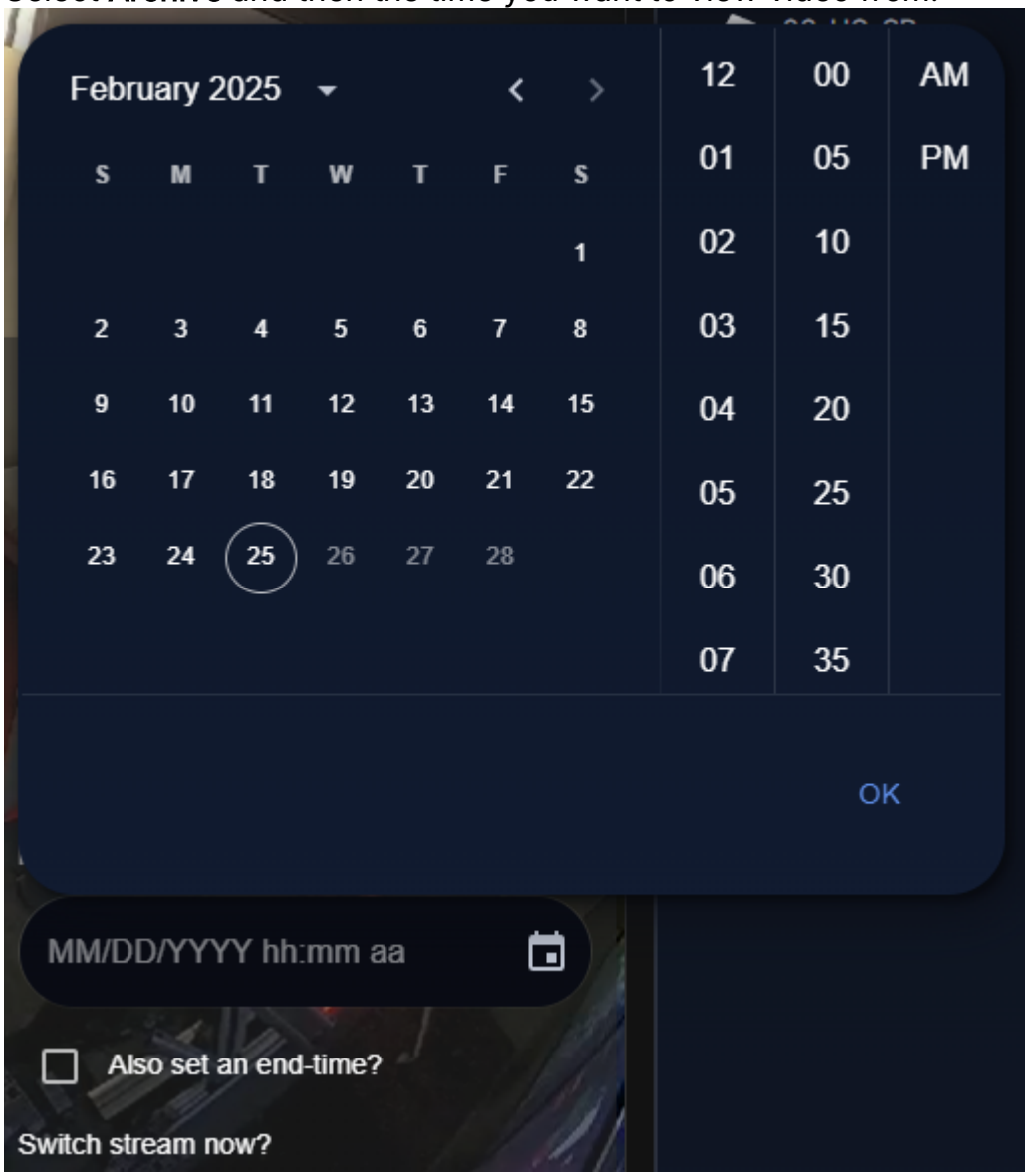
It is possible to access recorded video for cameras connected to a video system with recordings.

> **NOTE:** Recording video is a feature of the integrated Video Management System, NVR or DVR. Everbridge does not record video. If recorded video is not available, confirm that the integrated video system supports this and has been setup correctly.

To access recorded video from a camera:

1. Select the **Stream Options** button.

2. Select **Archive** and then the time you want to view video from.



3. Confirm the selection by selecting **Yes** under the **Switch stream now?** prompt.
4. The video stream from the selected date will display.

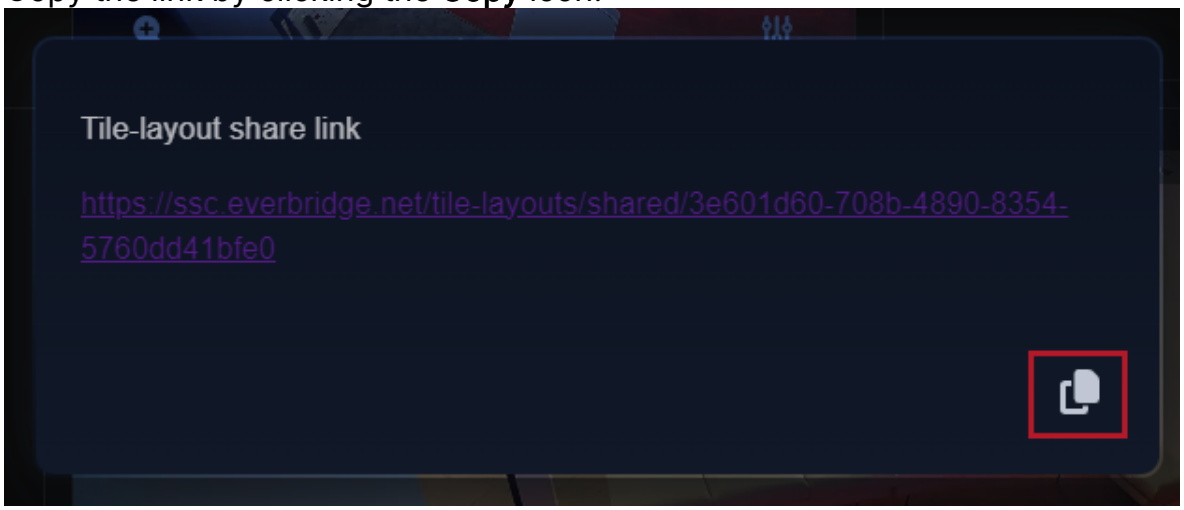
Sharing Video

Video layouts can be shared via shareable link. The recipient of the link will be presented with the selected video feeds, assuming they are able to login to Everbridge 360 and that they have permission to view the cameras.

To share video:

1. Select the **Share Layout** button.

2. Copy the link by clicking the **Copy** icon.



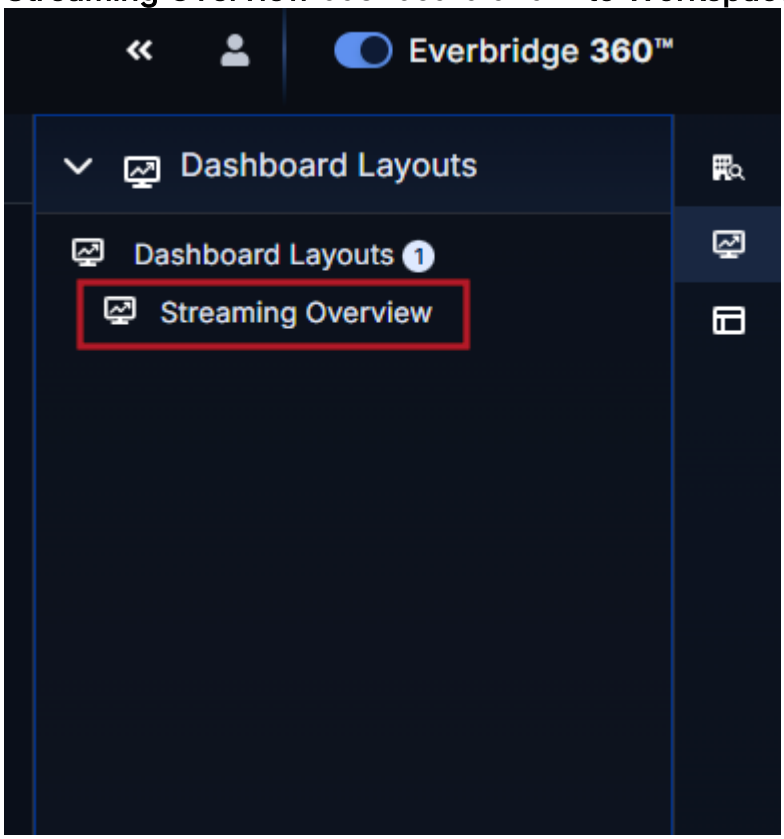
3. Share the link with anyone who needs to see the video.

Monitoring Use

Administrators can monitor who is using the system and which streams they are accessing. They can also stop active streams.

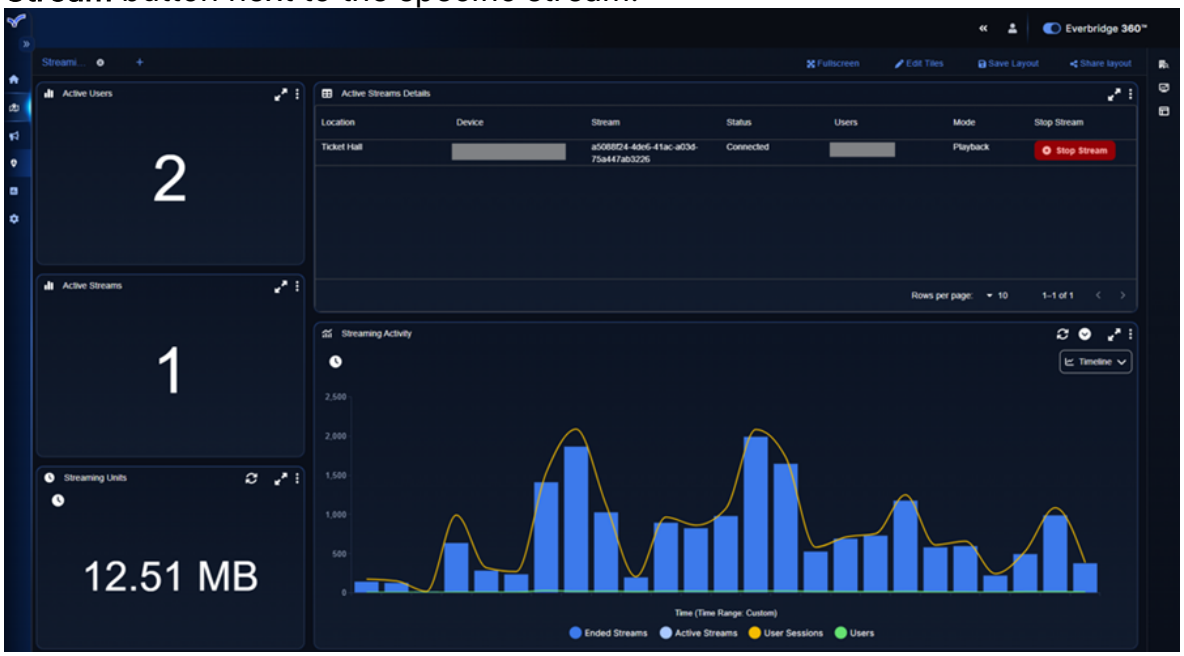
To view who is using the system:

1. Select the **Dashboard Explorer** from the right-hand menu. Then select the **Streaming Overview** dashboard and **+ to Workspace**.



2. The **Streaming Overview Dashboard** will be shown. Any active streams are listed in the grid below the number widgets. To stop a stream, select the **Stop**

Stream button next to the specific stream.



- Stop Stream permissions are only configured for elevated users. Permissions can be configured via the **Physical Security Manager Portal**.

3. Review the **Active Streams** and **Active Users** as needed.

Streaming Activity Widget

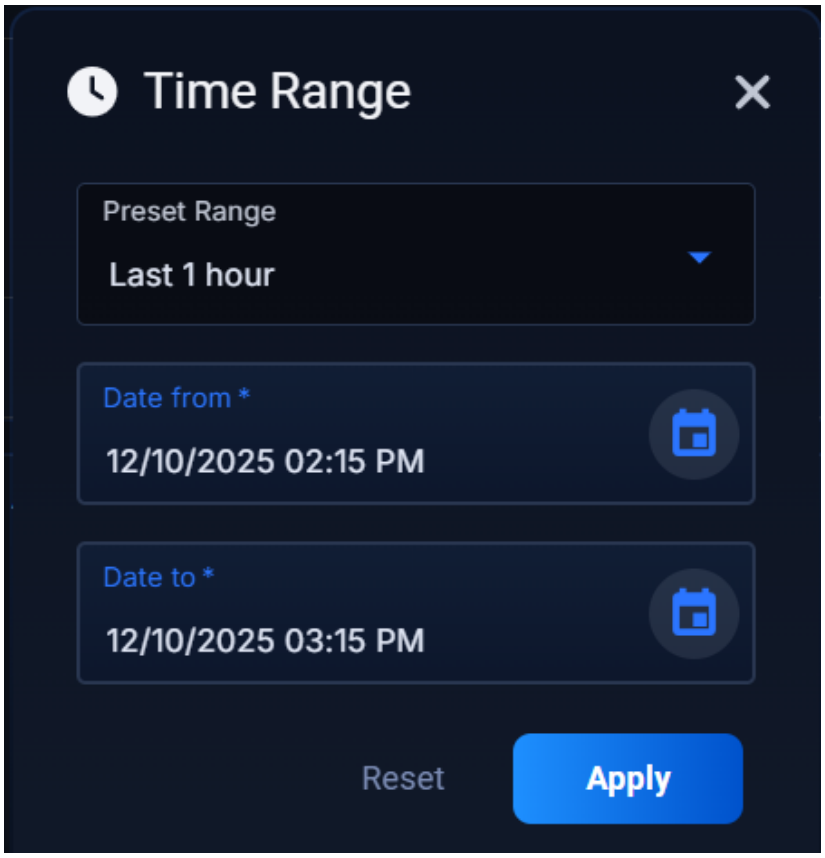
The **Streaming Activity** widget enables users to visualize and analyse streaming usage over a selected time period. It offers multiple chart views, allowing users to switch perspectives based on their reporting needs.

The following chart view options are available for the Streaming Activity widget:

- Timeline Chart
- Summary Chart
- Live vs. Playback Chart

Adjusting the Time Range

A **Time Range** selector is included at the top of the widget, allowing users to customize the period they want to analyze.



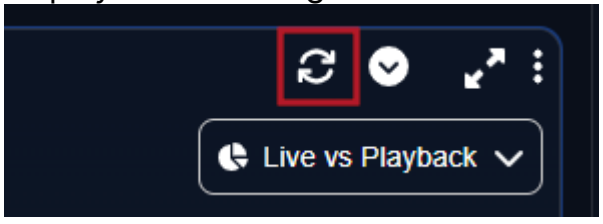
Options include:

- Last 15 minutes
- Last 1 hour
- Last 12 hours
- Last 24 hours
- Last 3 days
- Last 7 days
- Last 30 days
- Custom date range

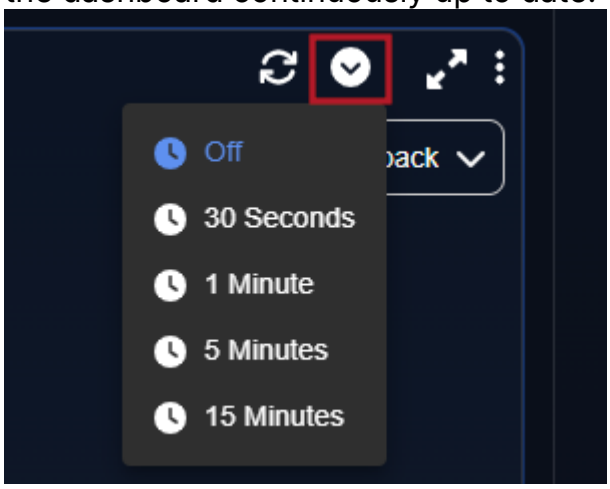
Data Refresh

The Streaming Activity widget supports both manual and automated refresh options, ensuring users can always view up-to-date streaming information.

- **Manual Refresh** - Click the **Refresh** icon to immediately reload the data displayed in the widget.



- **Automatic Refresh** - Users can choose an automatic refresh interval to keep the dashboard continuously up to date.

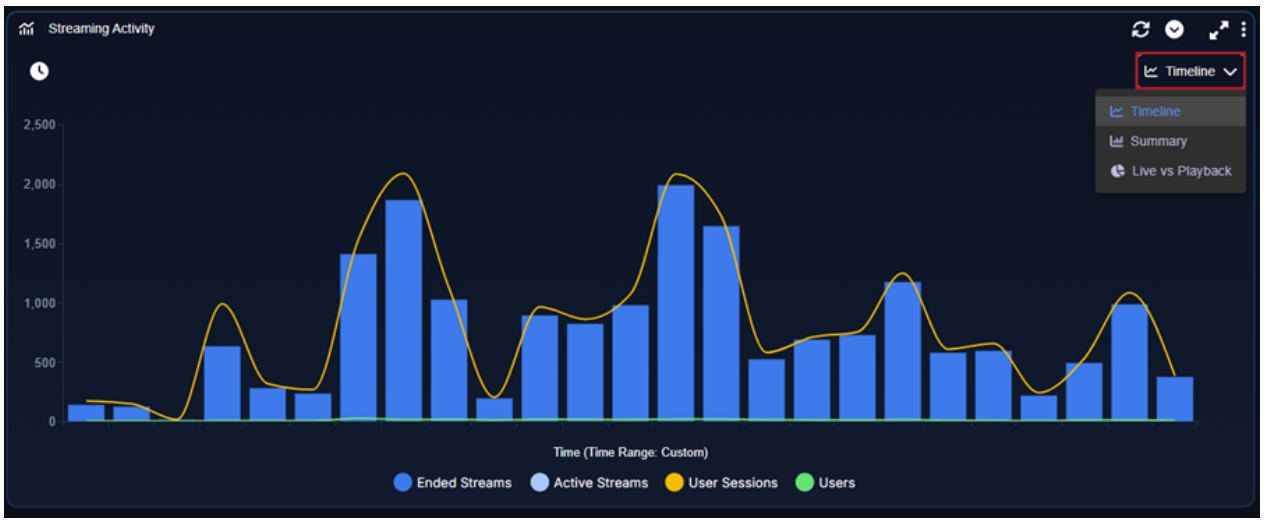


  Available options include:
  - Off
  - 30 Seconds
  - 1 Minute
  - 5 Minutes
  - 15 Minutes

Once enabled, the widget will be updated automatically without requiring further user action.

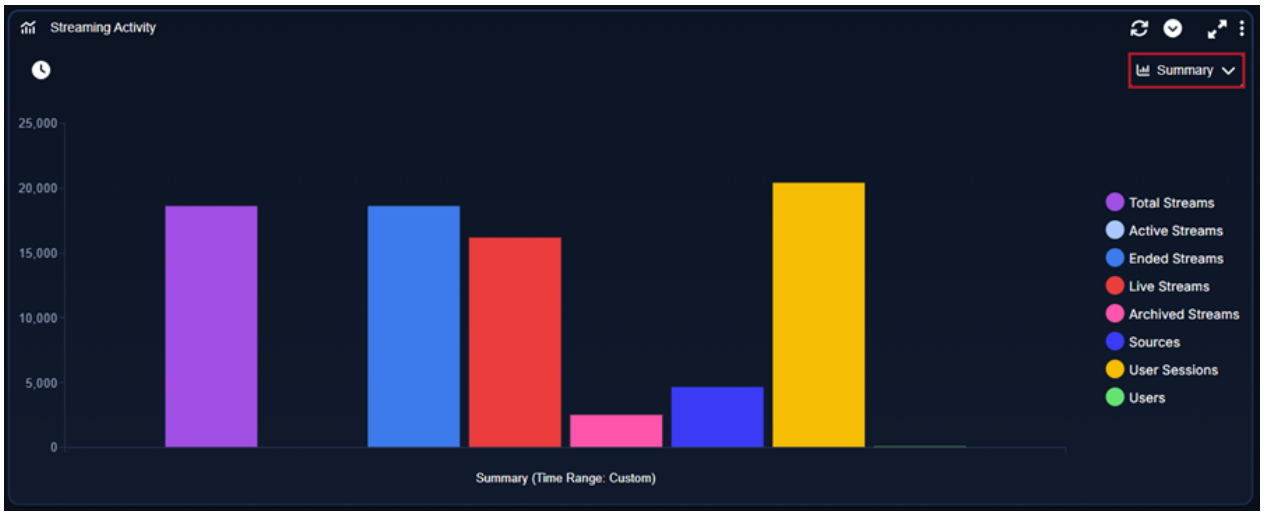
Timeline Chart

The **Timeline** chart displays streaming usage over a chosen date range. It shows total activity trends over time while highlighting usage patterns (such as high-traffic periods). Hover the cursor over the chart to view the exact values for any point in time.

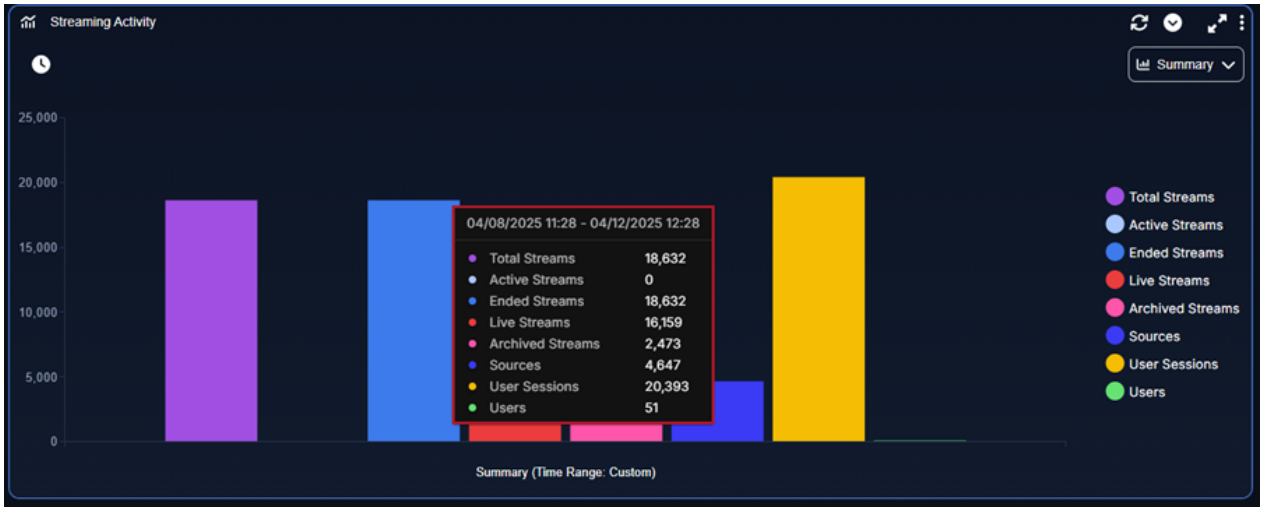


Summary Chart

The **Summary** chart provides a consolidated snapshot of overall streaming activity during the selected time range. It includes high-level totals and distribution metrics, making it ideal for quick reporting and analysis.

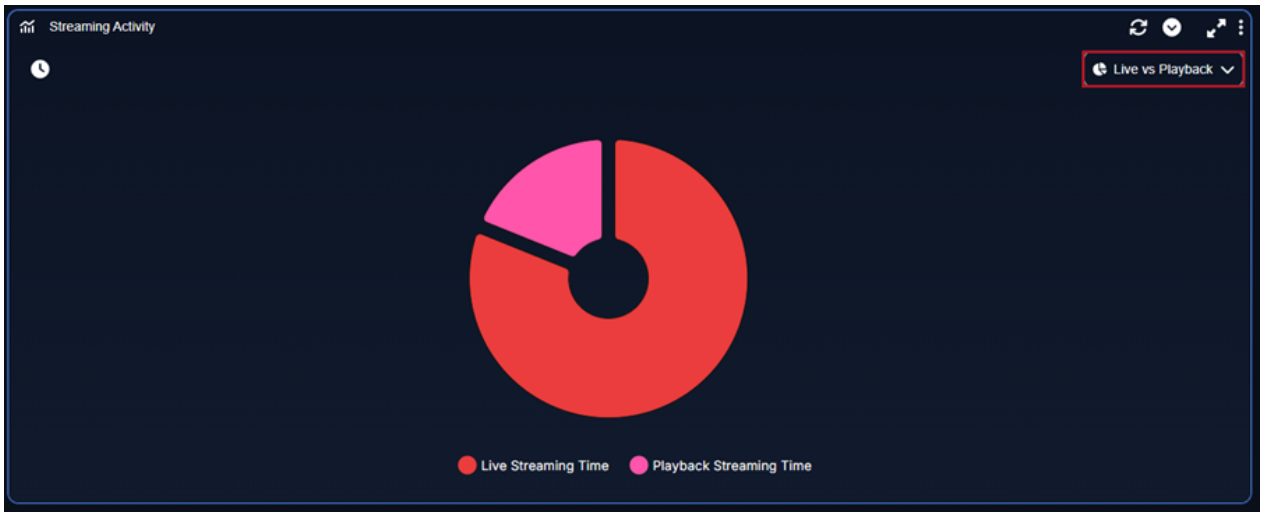


Hover the cursor over a metric to reveal its value details.

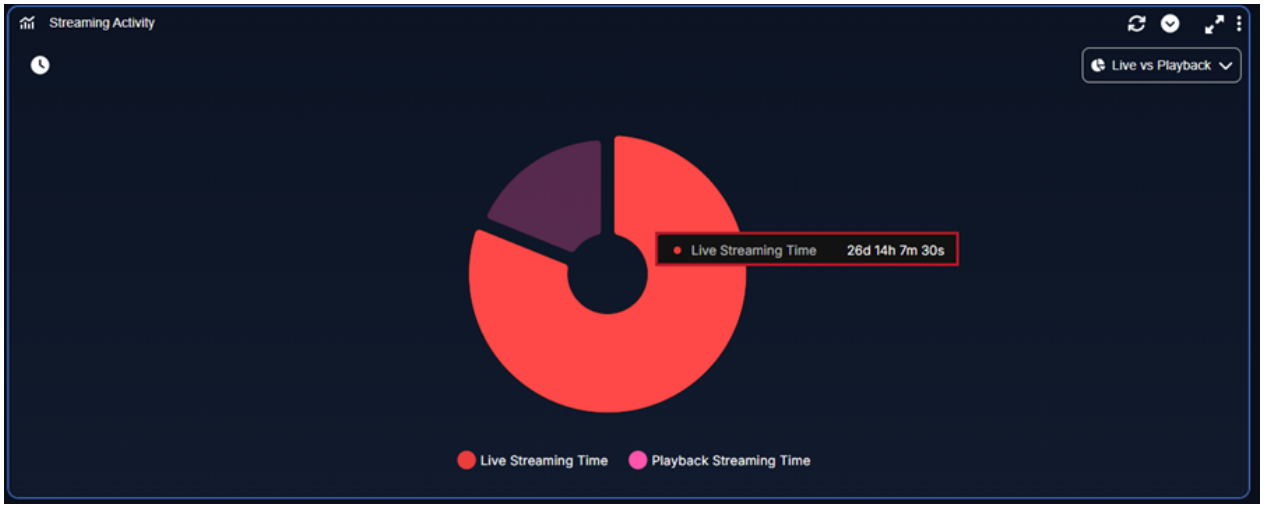


Live vs. Playback Chart

The **Live vs. Playback** chart shows how users engage with the platform by comparing live viewing to recorded playback. It provides a clear visual split between the two consumption types to help identify usage trends.



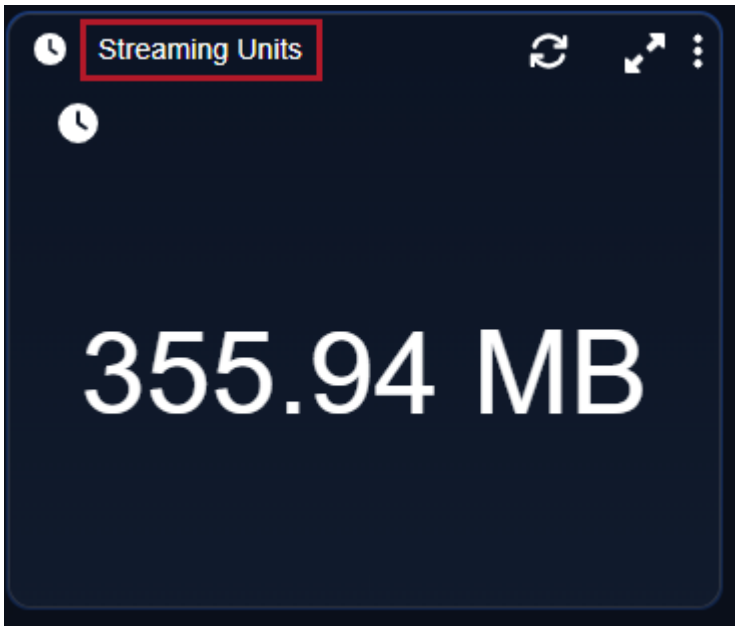
Hover the cursor over the chart to display the specific values for each category.



Streaming Units Widget

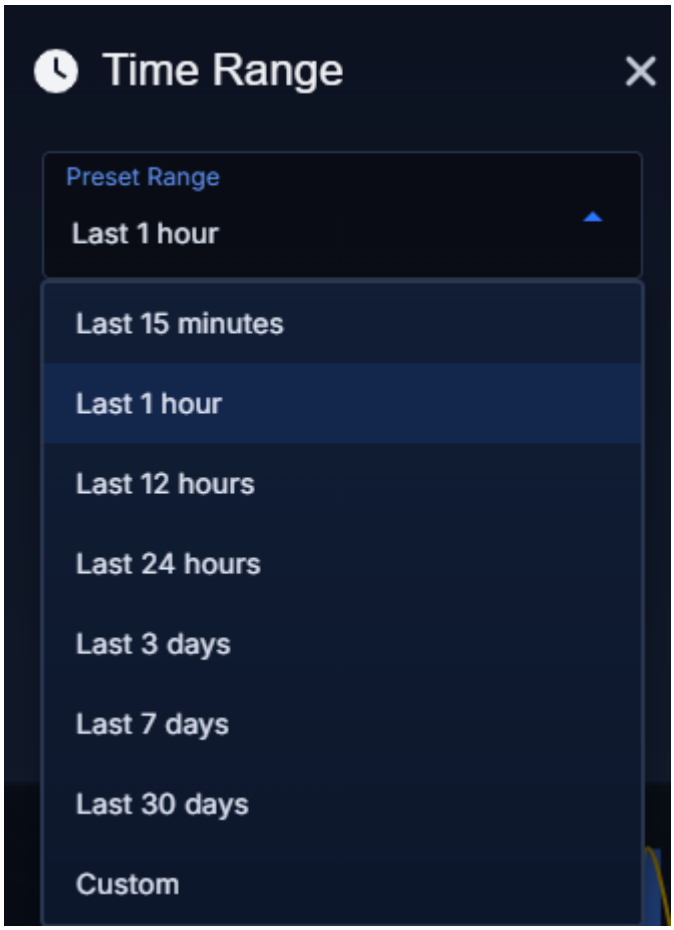
The **Streaming Units** widget provides a clear view of the total data streamed over a selected time period, helping users understand consumption levels, monitor usage trends, and assess how streaming volumes fluctuate during specific events or operational windows.

Like other dashboard widgets, **Streaming Units** includes a time-range selector and data-refresh control, ensuring users always see the most up-to-date information.



Adjusting the Time Range

A **Time Range** selector is included at the top of the widget, allowing users to customize the period they want to analyze. Adjusting the time range automatically updates the chart to reflect the selection.



Time range options include:

- Last 15 minutes
- Last 1 hour
- Last 12 hours
- Last 24 hours
- Last 3 days
- Last 7 days
- Last 30 days
- Custom date range

Data Refresh

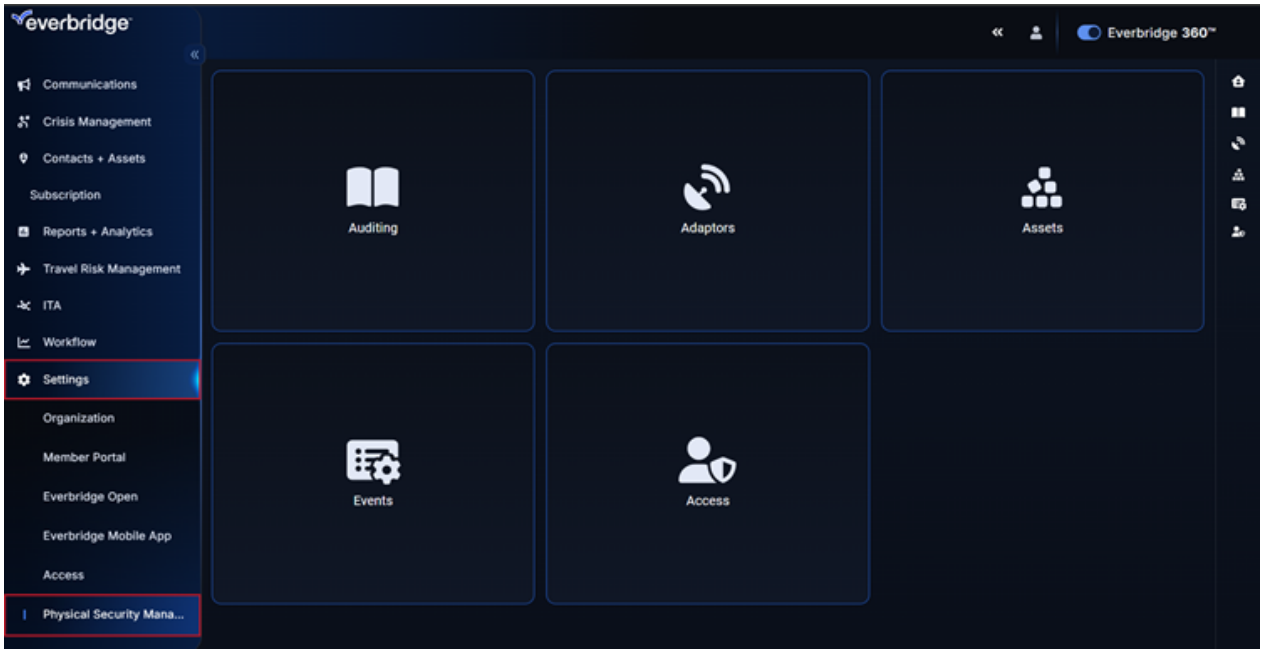
The data for the Streaming Units widget can be refreshed either manually or automatically.

- **Manual Refresh** - Users can click the **Refresh** icon to manually reload the streaming data at any time, which is especially useful when monitoring active events or real-time changes.

- **Automatic Refresh** - If globally supported at the dashboard level, users can enable an automatic refresh interval to keep the widget continuously updated without manual input.

Physical Security Management

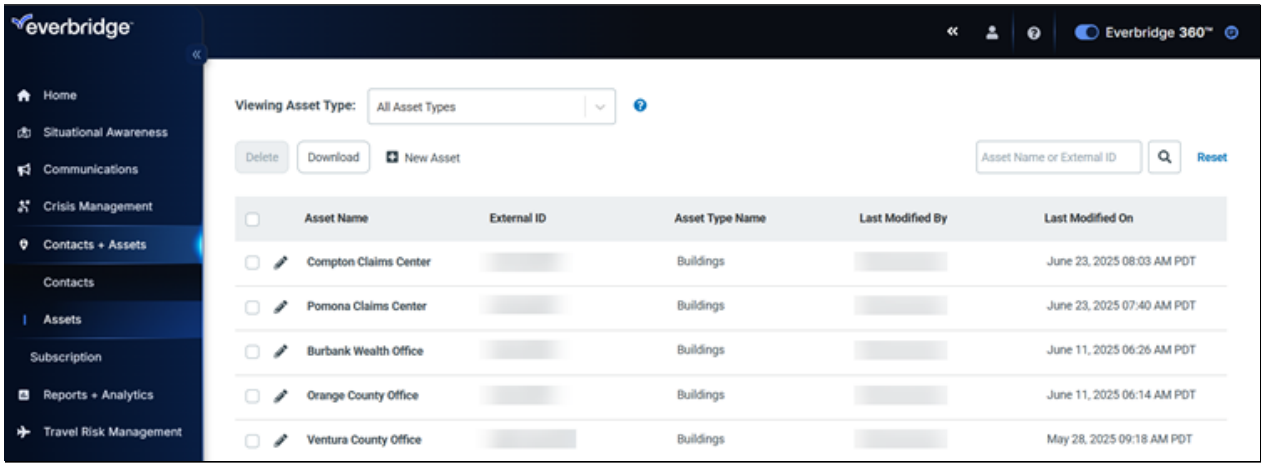
The **Physical Security Management** section under **Settings** provides the ability for Administrators to manage connections to sub-systems, permissions and assets, as well as accessing auditing information.



Asset Management

Everbridge 360 Physical Security automatically imports assets from connected subsystems. These can represent devices and the locations the devices exist in. Many physical security systems organize security assets in a location hierarchy structure.

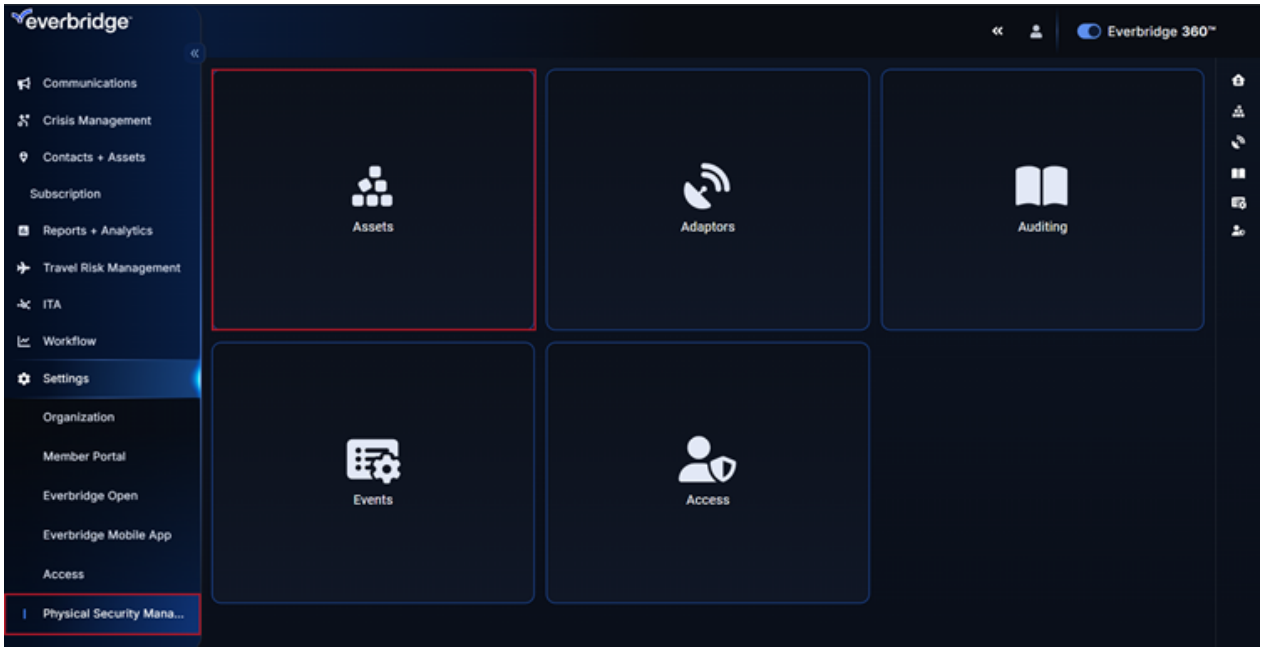
Everbridge 360 Physical Security also imports the locations configured in **Everbridge 360 Contacts + Assets**.



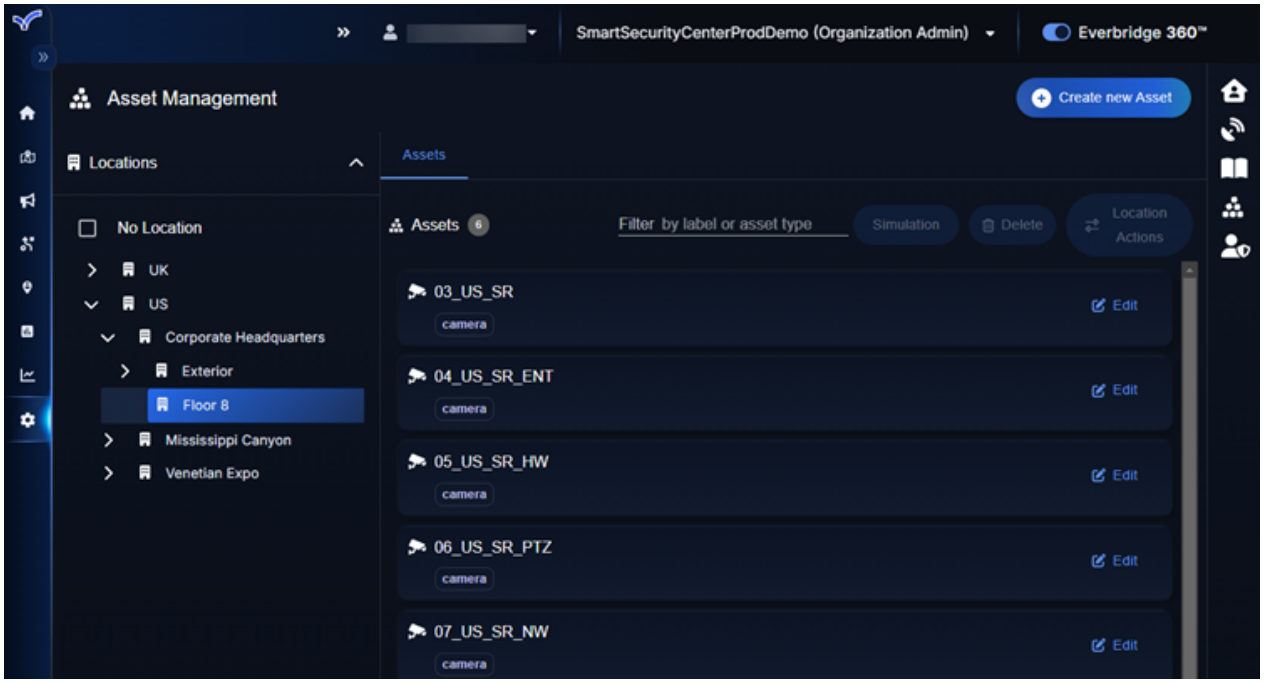
To make Cameras available to end-users, Physical Security administrators must organize imported cameras into the Locations configured with the **Everbridge 360 Contacts + Assets** section.

To do this, navigate to the **Asset Management** interface in the **Physical Security Management** section (**Settings** > **Physical Security Management**) and click the

Assets tile.



The **Asset Management** page will then open.



Preparing Everbridge 360 Locations

Everbridge 360 location assets will not have a parent location - select **No Location** to view them.

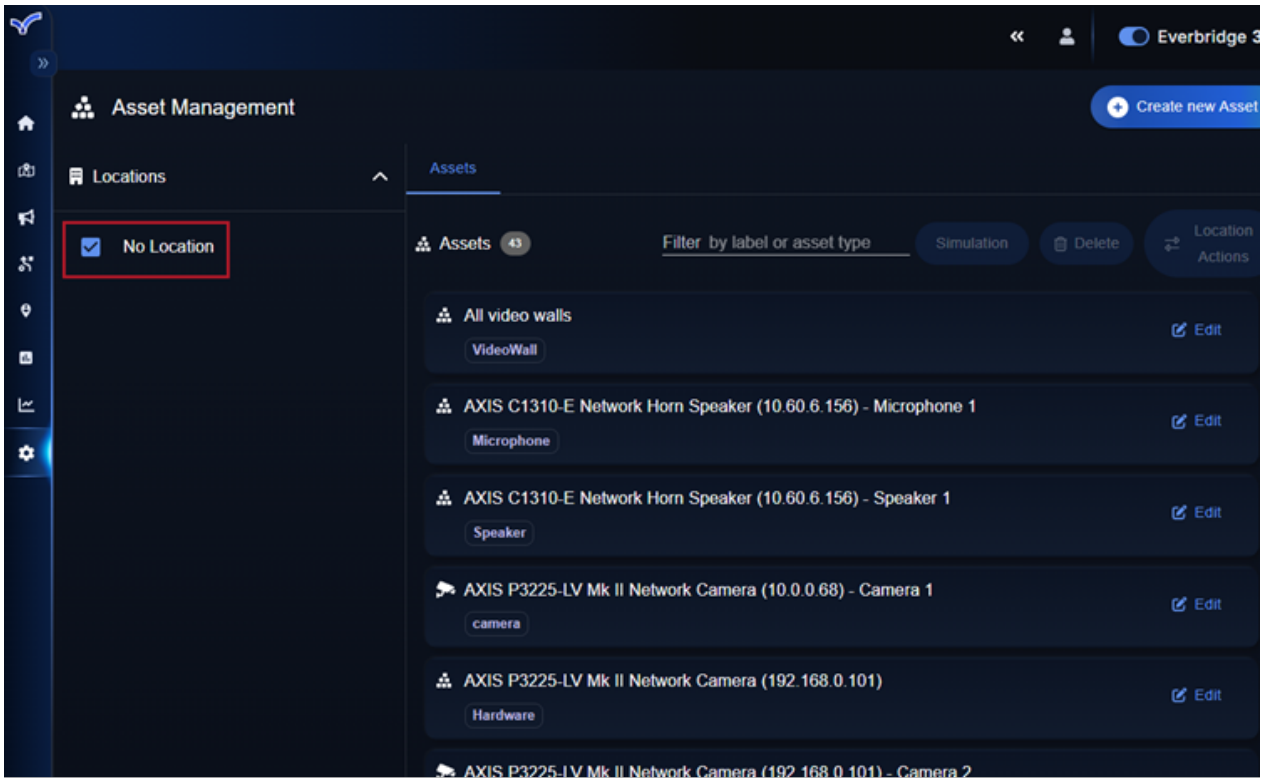
Select a location asset and then click **Location Actions** > **Set as Location** in order to make it a location that can exist in the hierarchy and have associated device assets.

Use the **Move** option to move locations into other locations. In this way, Locations can then be arranged into a hierarchy if required by moving them under a parent.

Moving Cameras Into Locations

Selecting **No Location** lists assets that do not have a parent location. This will show imported locations and top-level locations. The locations read from the Adaptor will be listed on the **Assets Management** page, when No Location is selected, and any associated devices will be listed under their respective location.

Select a camera, click **Location Actions**, and move it into desired location.

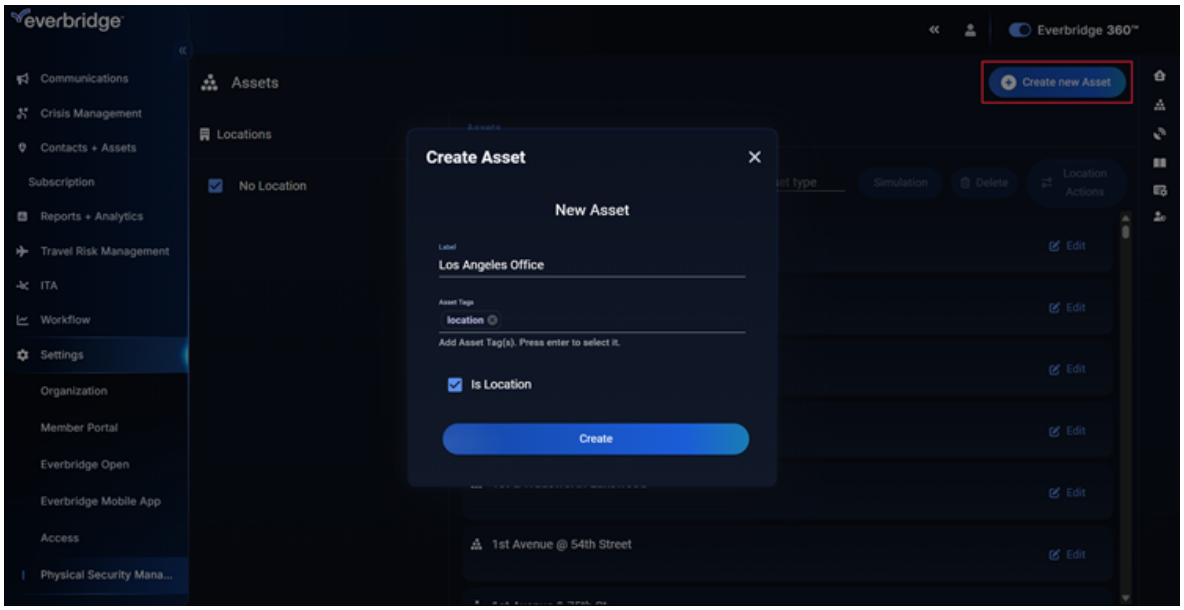


Creating Assets

It is possible to create location assets that do not exist in Everbridge 360 Contacts + Assets. To create locations:

1. Navigate to **Asset Management** in **Physical Security Manager**.
2. Select **Create new Asset**, enter a Label and any tags required.

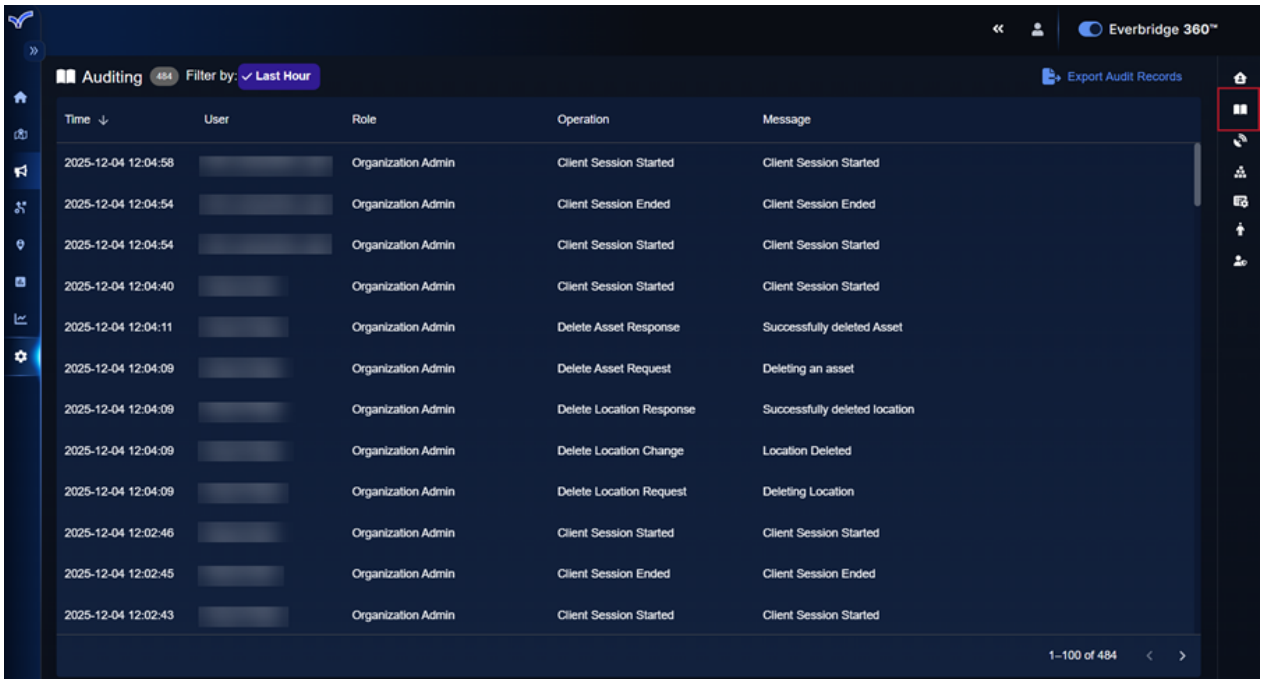
3. If the asset is a location, check the **Is Location** option.
4. Select **Create**.



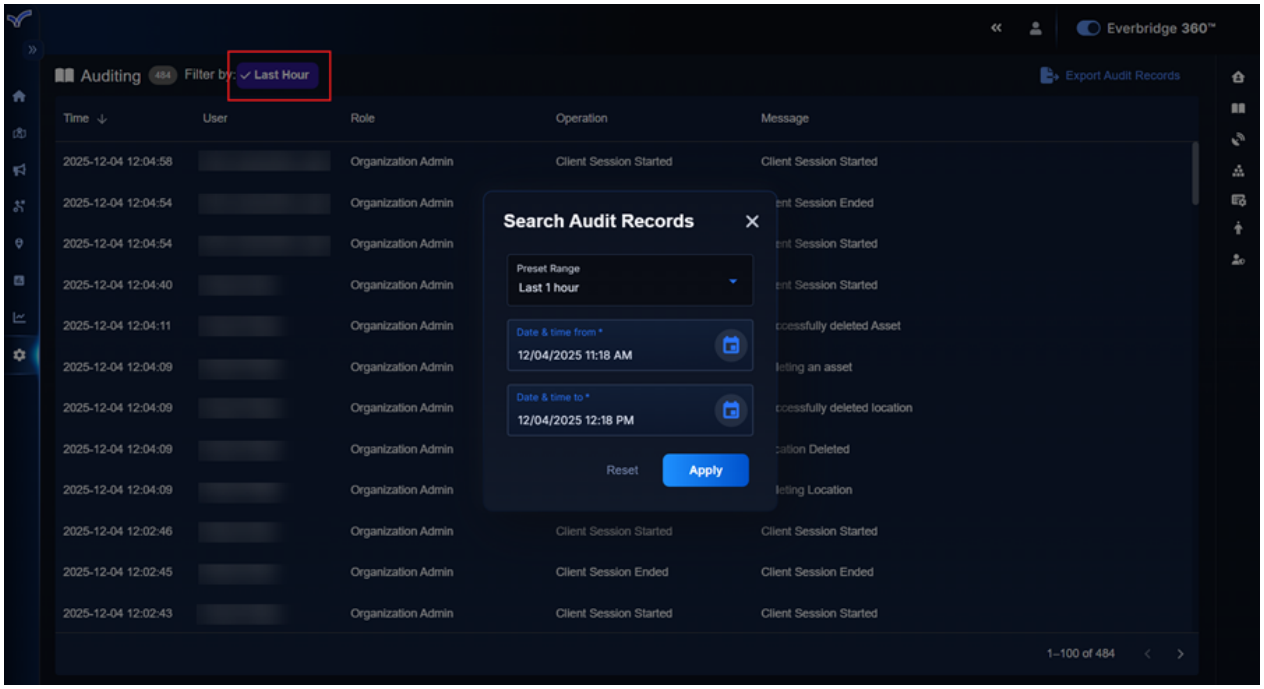
Once created, you can edit an asset by selecting **Edit** from the list.

Auditing

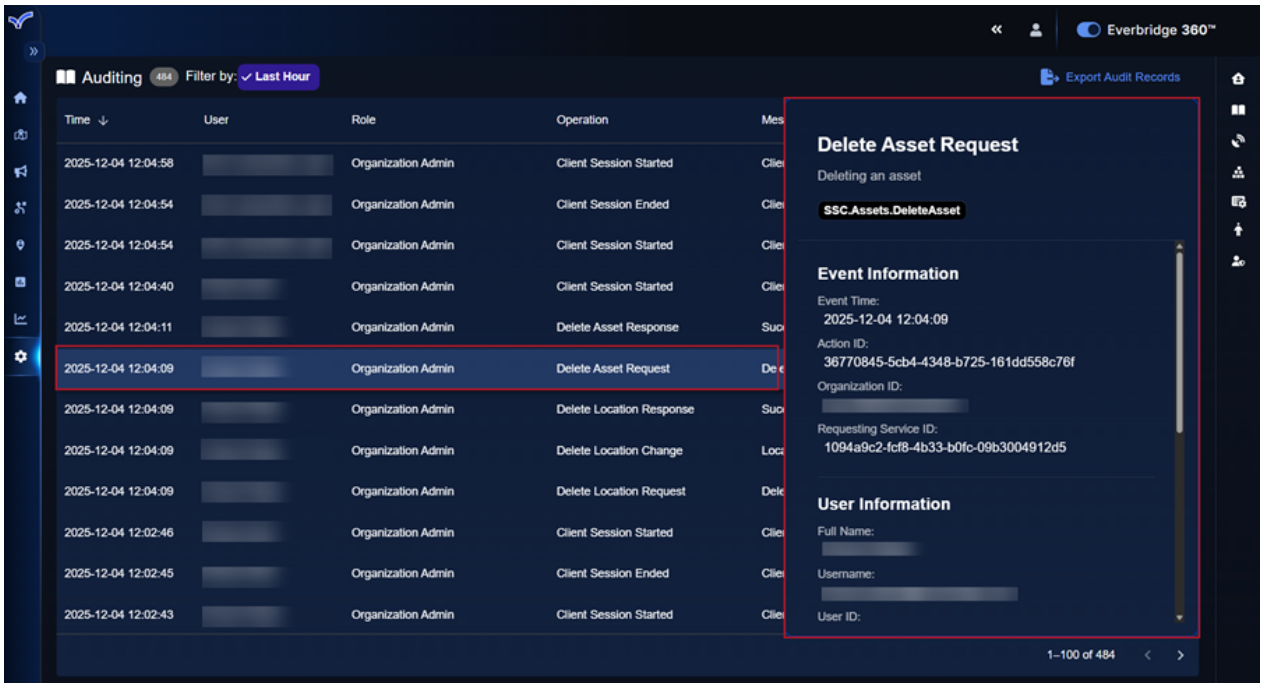
Physical Security stores information about what happens in the system, which can be viewed by clicking the **Auditing** icon on the right-hand toolbar.



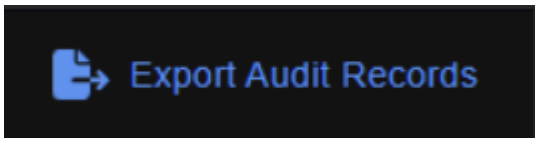
Use the **Filter By** option to select a time span to use when querying audit information.



Click on an item from the list to open its **Audit Details** panel to the right, which indludes crucial event information like time stamps and Action ID, as well as information about the user that created the event.



Audit information can be exported to a JSON file using the **Export Audit Record** button.



Advanced Configuration

The **Advanced Configuration** section provides settings used to integrate and manage third-party physical security systems within Everbridge. These configurations are typically performed by administrators or integration specialists responsible for maintaining system connectivity and data flow.

Key Concepts

Before working with these settings, it is helpful to understand how the main components relate to one another.

- **Adaptor** - A running service that connects a specific physical security system, such as a video management system, access control platform, or detection service, to Everbridge. Multiple adaptors can be used within a single group to support redundancy or increased processing capacity.
- **Adaptor Group** - A logical container used to organize one or more adaptors that connect to the same subsystem. Adaptor groups allow multiple adaptor instances to share a common configuration and operate together.
- **Connector** - Defines how an adaptor communicates with a third-party system. It determines the protocol, supported Event Types, and configuration requirements needed to establish and maintain the connection.

These components work together to enable communication between Everbridge and external systems. Adaptor groups organize connections, adaptors run the integrations, and connectors define how those integrations function.

Managing Adaptor Groups

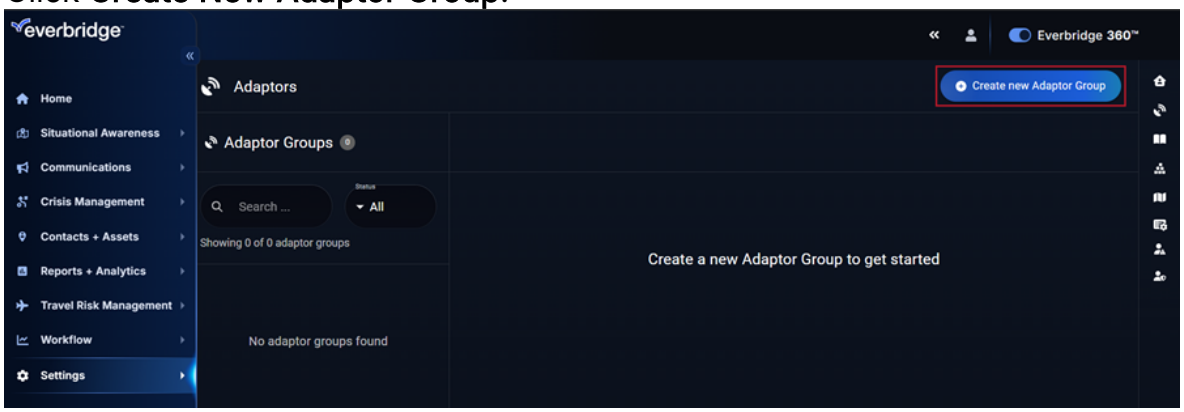
Adaptor Groups are used to organize and manage connections between Everbridge and external physical security systems. Each Adaptor Group represents a logical collection of Adaptor services that connect to the same subsystem. Grouping Adaptors in this way allows multiple Adaptor instances to share configuration settings and operate together.

Adaptor Groups are managed at the Organization level from **Settings** > **Physical Security Management** > **Adaptors**.

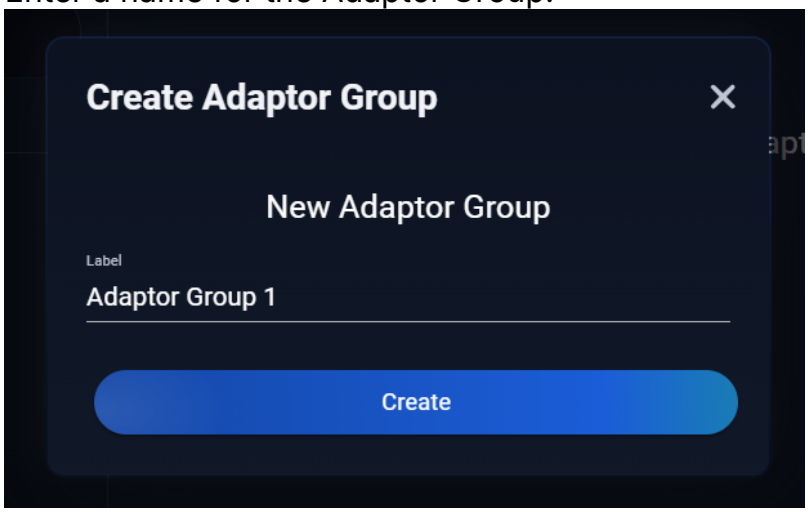
Creating an Adaptor Group

To create a new Adaptor Group:

1. Navigate to **Settings** > **Physical Security Management** > **Adaptors**.
2. Click **Create New Adaptor Group**.

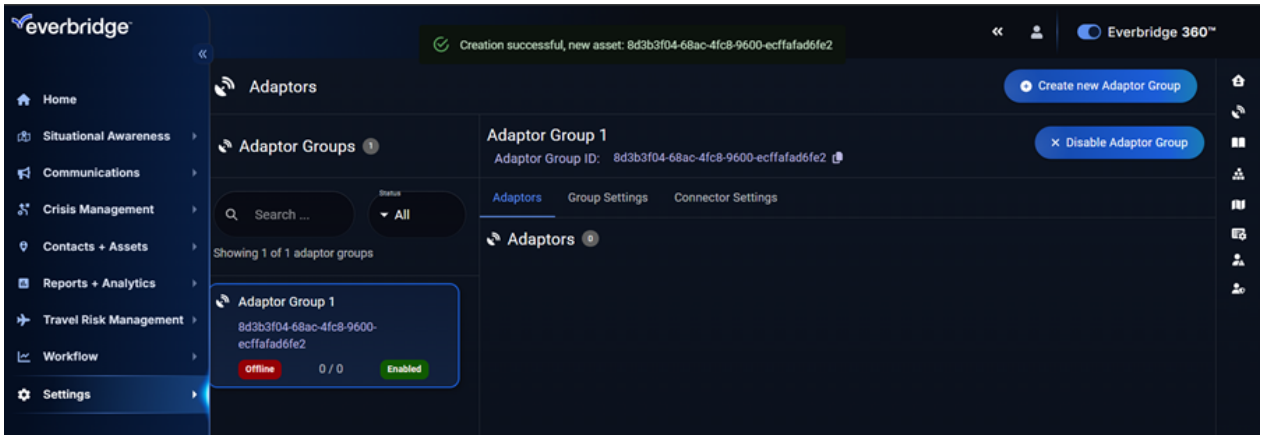


3. Enter a name for the Adaptor Group.



4. Click **Create**.

After the Adaptor Group is created, an **Adaptor ID** is generated. Record this value, as it is required when configuring Adaptor services to connect to the correct group.



Viewing Adaptor Groups

Selecting an Adaptor Group displays the Adaptor instances currently associated with that group. If no Adaptors have been configured, the list will be empty.

Enable or Disable an Adaptor Group

Disabling an Adaptor Group stops all associated Adaptor services from operating, while enabling an Adaptor Group allows services in the group to resume operation.

Use this option when temporarily suspending or restoring connectivity to a subsystem.

Configure Adaptor Group Settings

Adaptor Groups include settings that control how Assets and locations are synchronized from connected systems. When configuring an Adaptor Group, the following options are available:

- **Auto-Populate Assets** - When enabled, device Assets from the connected subsystem are automatically synchronized into Everbridge. This ensures that cameras and other devices are available without manual configuration.
- **Auto-Populate Locations** - When enabled, locations defined in the connected subsystem are automatically imported and mapped into Everbridge. Imported assets are placed within these locations during synchronization.

Synchronization begins the first time the **Assets** page is accessed for the Adaptor Group.

Editing or Reviewing an Adaptor Group

To update an Adaptor Group:

1. Navigate to **Settings** > **Physical Security Management** > **Adaptors**.
2. Select the **Adaptor Group**.
3. Modify the available settings as needed.
4. Click **Update** to apply changes.

Changes take effect immediately for all Adaptor services associated with the group.

Configuring Connectors

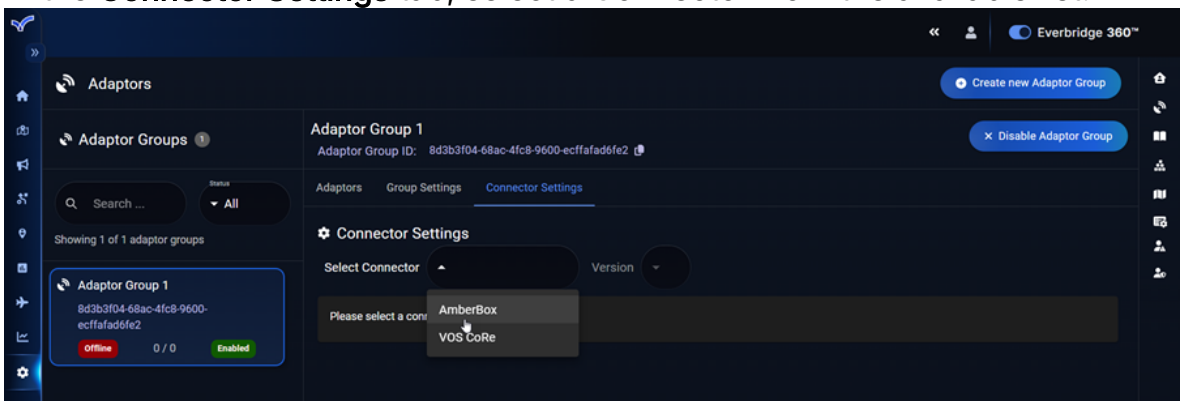
Connectors define how Adaptor services communicate with external physical security systems. Each Connector is designed for a specific subsystem and determines how data, such as video streams and Events, is exchanged with Everbridge.

Connector configuration is managed at the Adaptor Group level. When configuring a Connector, the integration type is selected, authentication details are defined, and the required configuration is provided to establish the connection.

Selecting a Connector

To select a Connector:

1. Navigate to **Settings** > **Physical Security Management** > **Adaptors**.
2. Select the Adaptor Group to configure.
3. In the **Connector Settings** tab, select a Connector from the available list.



- Only Connectors supported for the environment are displayed. Each Connector corresponds to a specific third-party system.

Configuring Connector Settings

After a Connector is selected, additional settings will be available to define how the integration operates.

Connector Version

The latest Connector version is selected by default. If required, a different version can be selected for compatibility with a specific subsystem.

Proxy User ID

The **Proxy User ID** is used for authentication when the Connector communicates with Everbridge. To create a proxy user:

1. Navigate to **Settings** > **Access** > **Users**.
2. Create a new user.
3. Use the numeric user ID shown in the user details as the Proxy User ID.

Providing the Connector Configuration

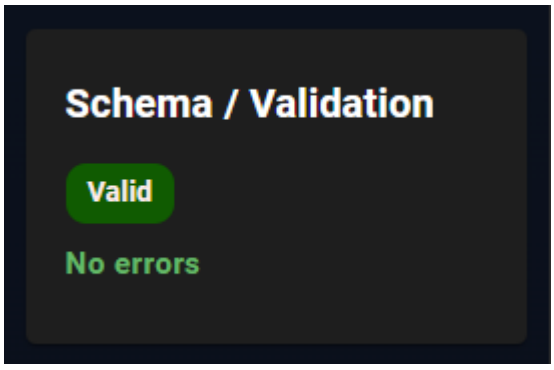
Connectors require configuration details to establish communication with the external system. This configuration is provided in JSON format.

To provide connector configuration:

1. Navigate to **Settings** > **Physical Security Management** > **Adaptors**.
2. Select the Adaptor Group.
3. Select the **Connector Settings** tab.
4. Click the **Advanced** button to open the JSON editor.
5. Enter or paste the configuration values for the selected Connector.
6. Click **Update** to save changes.

The configuration typically includes connection endpoint information, authentication credentials, polling or synchronization settings, and integration identifiers.

Ensure that the configuration is valid before saving. Validation status is displayed in the **Schema / Validation** panel.



Verify Connector Configuration

After updating the Connector Settings, confirm that the Adaptor is connected successfully. To do this:

1. Navigate to **Settings** > **Physical Security Management** > **Adaptors**.
2. Select the Adaptor Group.
3. Verify that the Adaptor status is online.

If the Adaptor does not connect, review the configuration and confirm that all required values are correct.

Hosting Adaptors

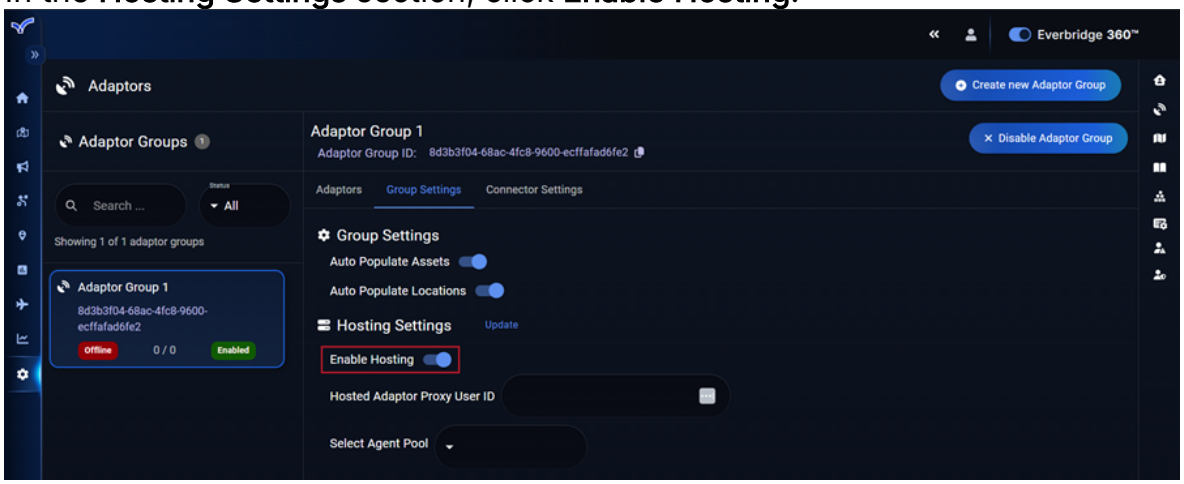
Adaptor hosting allows Everbridge to manage Adaptor services in the cloud, removing the need to deploy and maintain Adaptor infrastructure within a local environment. When hosting is enabled, Adaptor connections are established and maintained using Everbridge-managed resources.

Hosting settings are configured at the Adaptor Group level.

Enabling Adaptor Hosting

To enable hosting for an Adaptor Group:

1. Navigate to **Settings** > **Physical Security Management** > **Adaptors**.
2. Select the Adaptor Group.
3. Select the **Group Settings** tab.
4. In the **Hosting Settings** section, click **Enable Hosting**.



Enabling hosting allows Adaptor services for the selected group to run within Everbridge-managed infrastructure.

Configuring Hosting Settings

After hosting is enabled, additional settings are available to define how the hosted adaptor operates.

Hosted Adaptor Proxy User ID

The **Hosted Adaptor Proxy User ID** is used for authentication when Everbridge hosts the adaptor connection. A proxy user must be created in Everbridge before this value can be assigned. The numeric user ID associated with that user is used as the Proxy User ID.

Select the Agent Pool

The **Agent Pool** determines which Everbridge-managed resources are used to host the Adaptor. Available options depend on the environment configuration. After configuring hosting settings, select **Update** to apply changes.

Considerations for Hosted Adaptors

Adaptor hosting is only available for supported Connectors. If hosting is not supported for the selected Connector, the option may be unavailable.

When hosting is enabled, Adaptor services are managed by Everbridge. Local Adaptor deployment is not required for the associated Adaptor Group.

Updating Connector Credentials

Connector credentials are used by Adaptor services to authenticate with Everbridge and connected physical security systems. These credentials may need to be updated periodically, such as when passwords expire or API keys are rotated.

Updating Connector credentials requires modifying the Adaptor configuration file and restarting the Connector service.

Locating the Configuration File

Connector credentials are stored in the **Adaptor configuration file** on the system where the Adaptor service is installed.

The configuration file is located at:

```
C:\ProgramData\Everbridge\SSC\Connectors\<subsystem>\configuration.json
```

Updating Credentials

To update Connector credentials:

1. Navigate to the configuration file location.
2. Create a backup of the existing **configuration.json** file.
3. Open the file in a text editor.
4. Update the relevant credential values, such as:
    - Username and password

- API key and secret

5. Save the changes.

Ensure that the updated values match the credentials provided for the subsystem or Everbridge services.

Validating the Configuration

After updating credentials, confirm that the configuration file is valid by verifying that the JSON structure is correct and ensuring that all required fields are present. Invalid formatting may prevent the Adaptor service from starting.

Restarting the Connector Service

After saving the configuration file, restart the Connector service to apply the changes:

1. Restart the CEM Connector service on the Adaptor machine.
2. Confirm that the service starts successfully.

Verifying the Connection

After the service is restarted, confirm that the adaptor is operating correctly:

1. Navigate to **Settings** > **Physical Security Management** > **Adaptors**.
2. Select the Adaptor Group.
3. Verify that the Adaptor status is online.

If the adaptor does not come online, review the configuration file and confirm that the credentials are correct.

Physical Security Feed

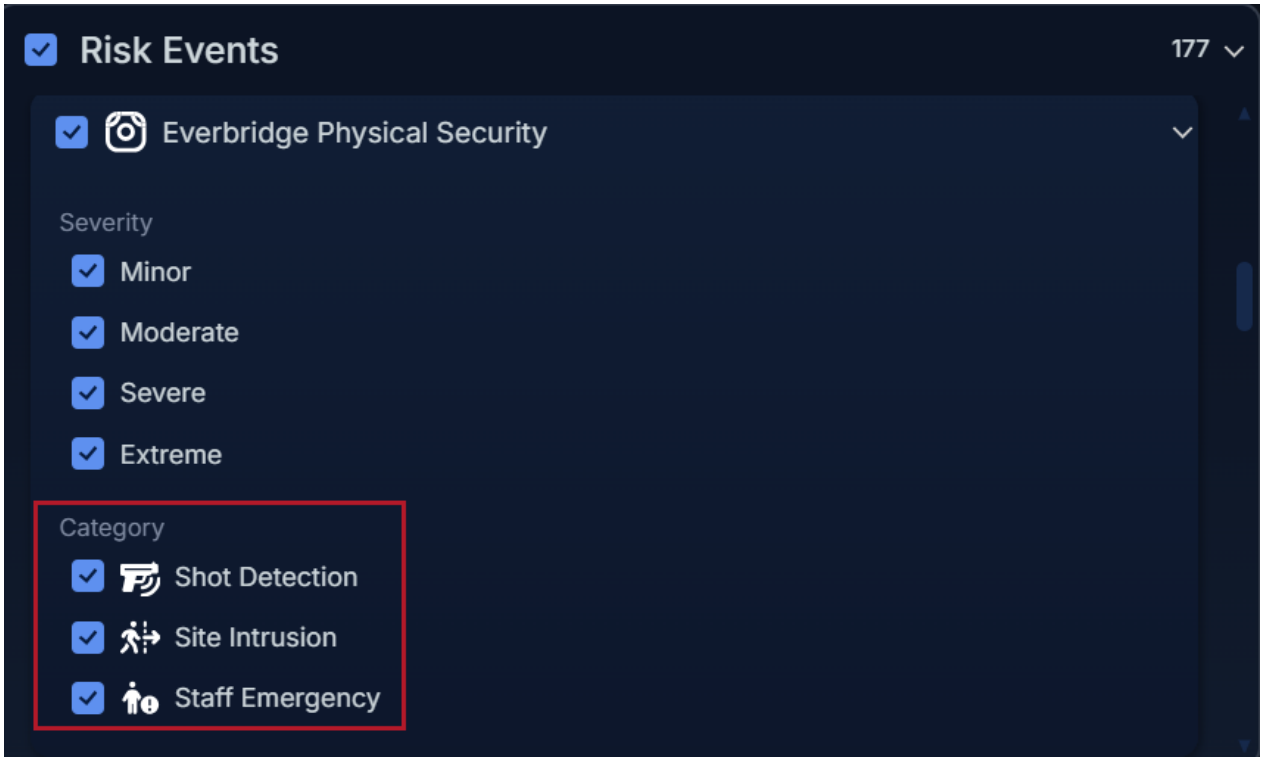
Overview

The **Everbridge Physical Security Feed** ingests and surfaces crucial event data from connected physical security systems. These events are normalized and displayed within EB360 and Visual Command Center (VCC), providing GSOCs with a unified, real-time view of Physical Security Risk Events.

Supported Event Types

The Physical Security Feed currently supports three Risk Event Types:

- Shot Detection
- Site Intrusion
- Staff Emergency



Shot Detection Events

Shot Detection Events are derived from connected gunshot detection systems. They're Immediately surfaced in VCC with contextual details, including Location and Event Type. Designed to provide high-urgency notifications for real-time situational awareness.

Site Intrusion Events

Site Intrusion Events are generated from Access Control Systems or Intrusion Detection Systems (such as Door Forced, Unauthorized Entry, Zone Breach, etc.). They're displayed in VCC with key metadata such as Location, Event Source, and timestamp while enabling GSOCs to quickly assess the severity and location of potential intrusions.

Staff Emergency Events

Staff Emergency Events are created when Panic or Duress Alerts are triggered from staff safety systems or devices. These Risk Events are prioritized automatically within the Risk Event feed for rapid awareness, supporting enhanced visibility and helping teams identify at-risk personnel to respond appropriately.

Configuring the Physical Security Feed

The **Physical Security Feed** surfaces Risk Events of the supported Risk Event Types (Intrusion, Staff Emergency, and Shot Detection) within Everbridge 360 and Visual Command Center. Workflows and their Filters can be adjusted anytime to refine Event handling or prioritization.

Prerequisites

Before configuring the Everbridge Physical Security Feed, ensure the following requirements are met:

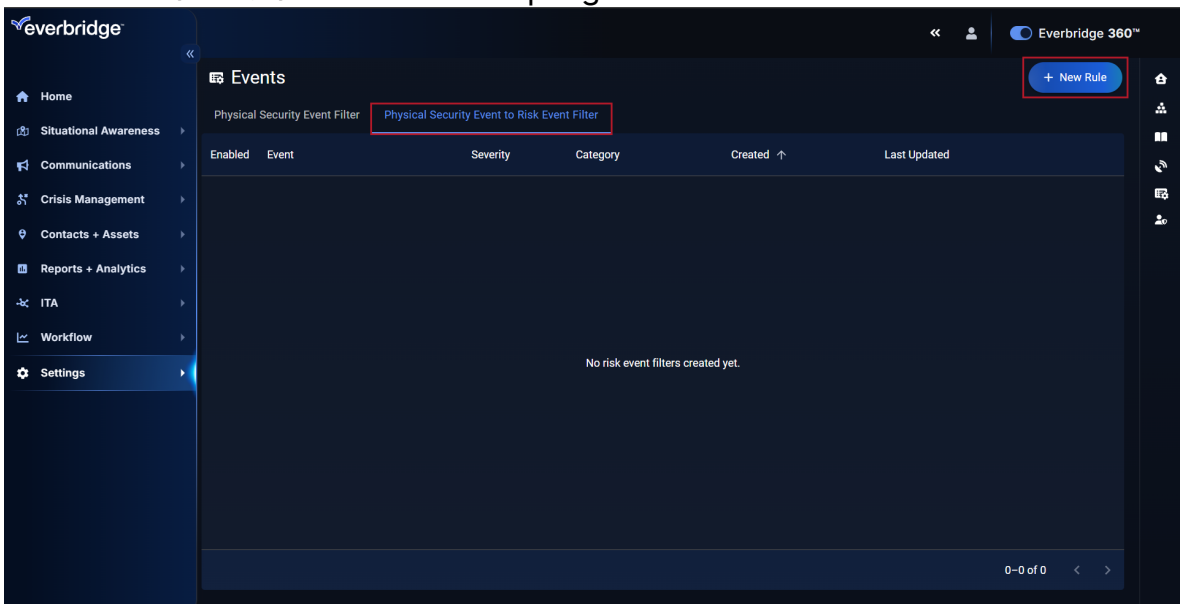
- You have an Everbridge 360 account with the **Physical Security** module enabled.
- An **Adaptor** with a connector is configured for each relevant third-party physical security system (e.g., Access Control, Intrusion, or Shot Detection systems).

Setup

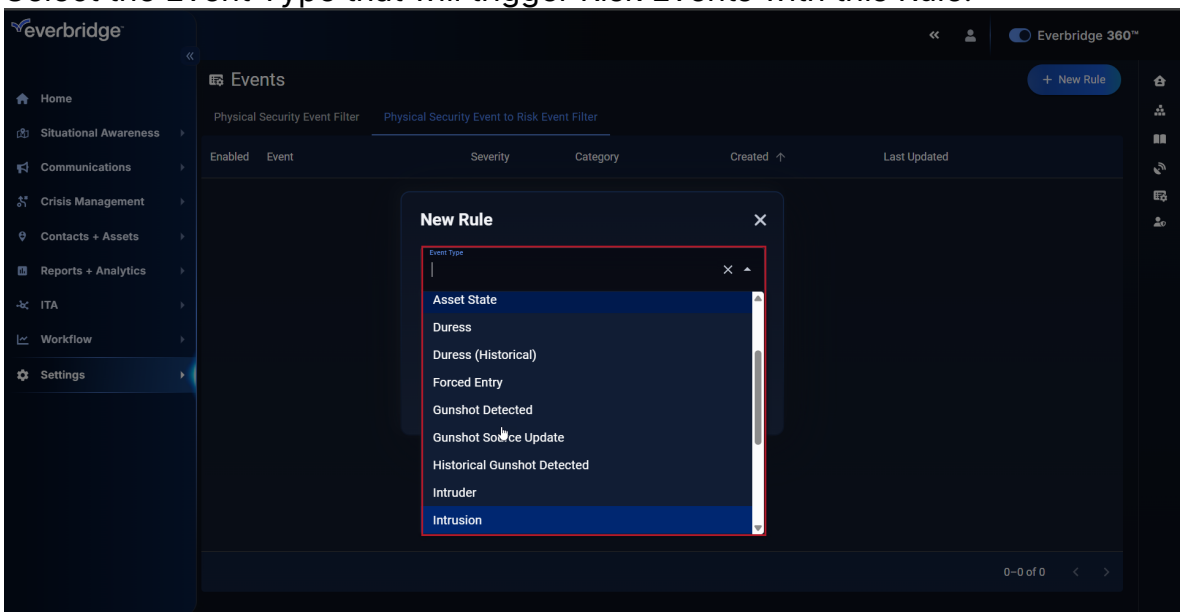
Configuring Event Filtering

To create an Event Filter:

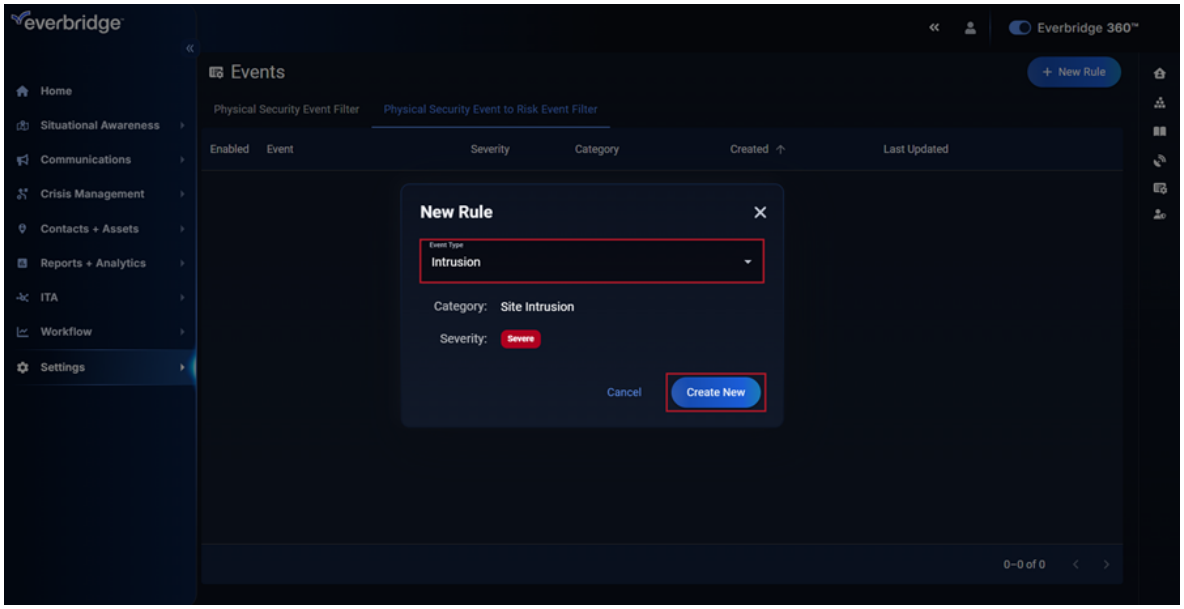
1. From the Organization level, navigate to **Settings** > **Physical Security Manager** > **Events** > **Physical Security Event to Risk Event Filter**.
2. Click the **New Rule** button in the top-right corner.



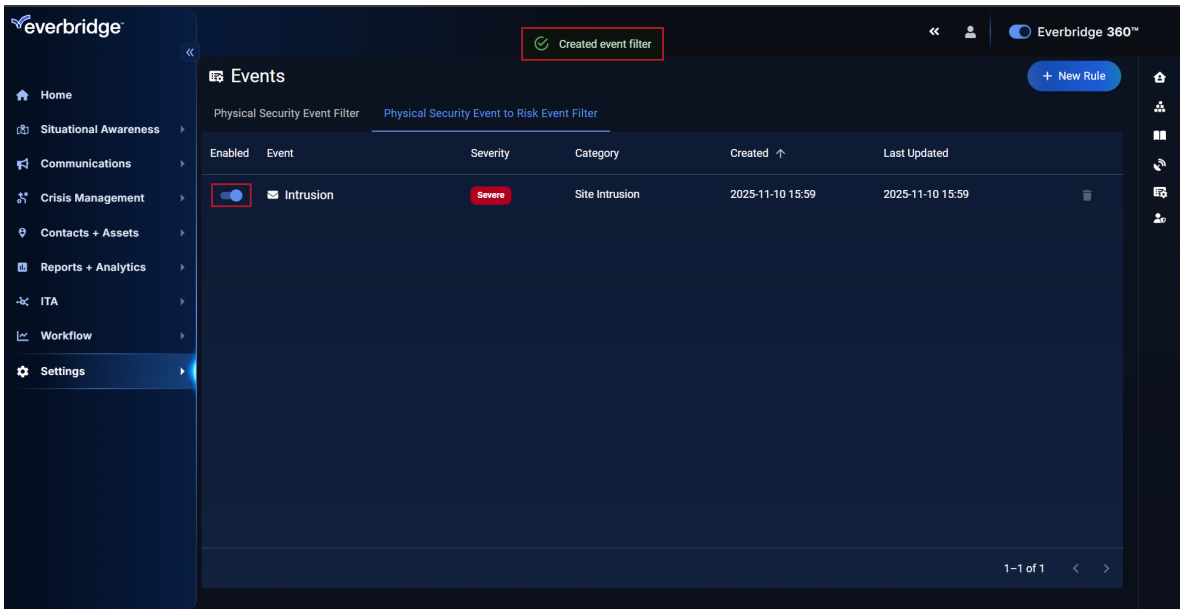
3. Select the Event Type that will trigger Risk Events with this Rule.



4. The selected Risk Event's Category and Severity will be displayed. Click **Create New**.



5. The new Risk Event Filter will appear in the list view. Click the toggle to enable or disable it as needed.



NOTE: Risk Event Filters can be deleted by first disabling them, and then clicking the **Trashcan** icon.

Creating a CEM Orchestration Workflow

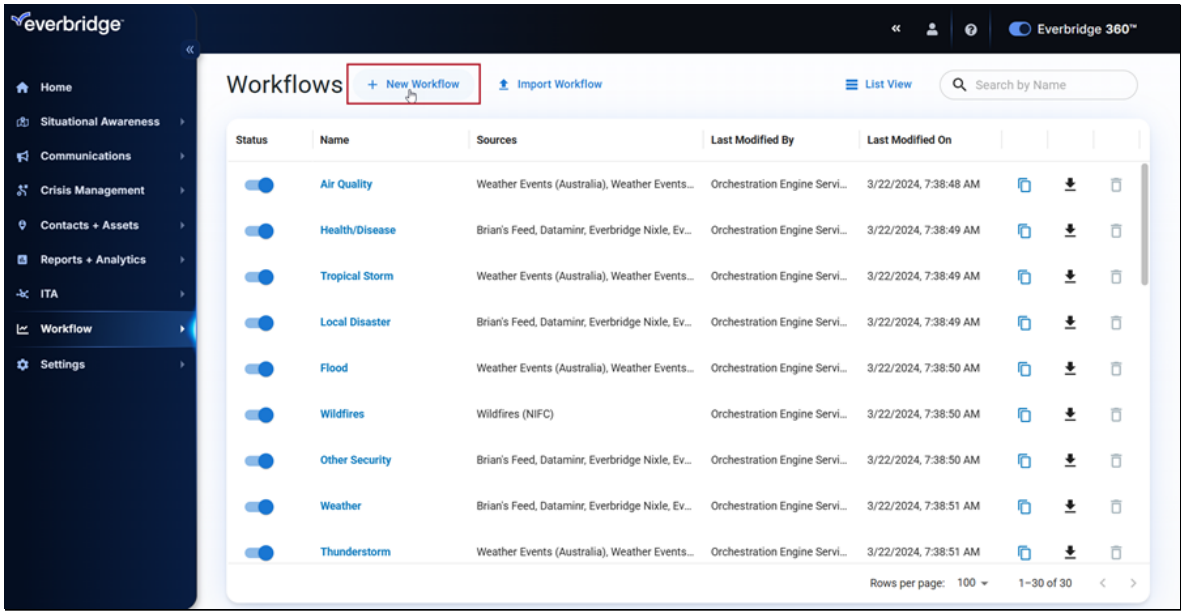
Once Event Filtering has been configured, a CEM Orchestration Workflow should be created that utilizes Everbridge Physical Security as a **Source**.

NOTE: For an in-depth explanation on creating CEM Workflows, see the CEM Orchestration User Guide.

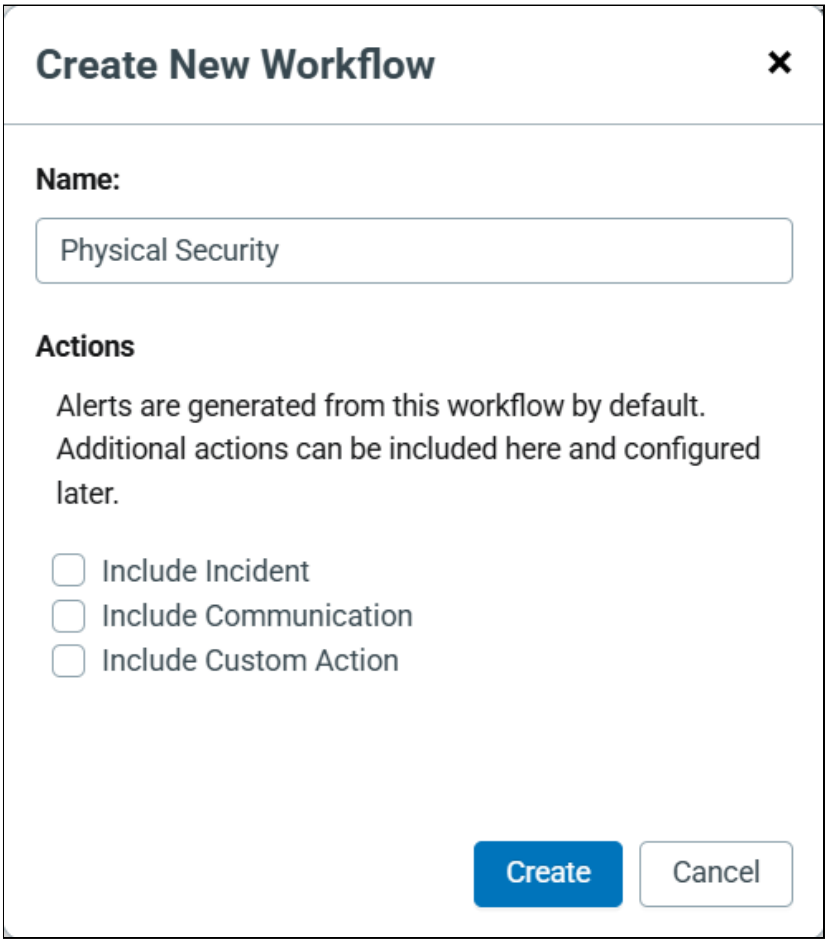
To create this Workflow:

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

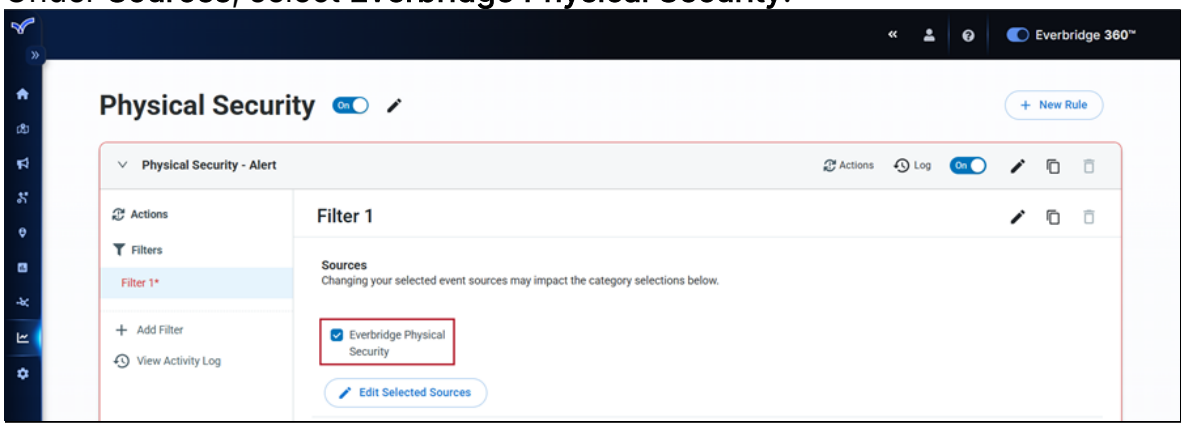
2. Click **New Workflow**.



3. Give the Workflow an appropriate name and, optionally, select the checkboxes for including an Incident, Communication, and/or Custom Action.



4. Click **Create**.
5. Under **Sources**, select **Everbridge Physical Security**.



6. Under **Categories**, select one of the following:
   - **Allow all categories and subcategories**
   - **Allow only the selected category and subcategories** - Choose one of the three categories from the dropdown menu.

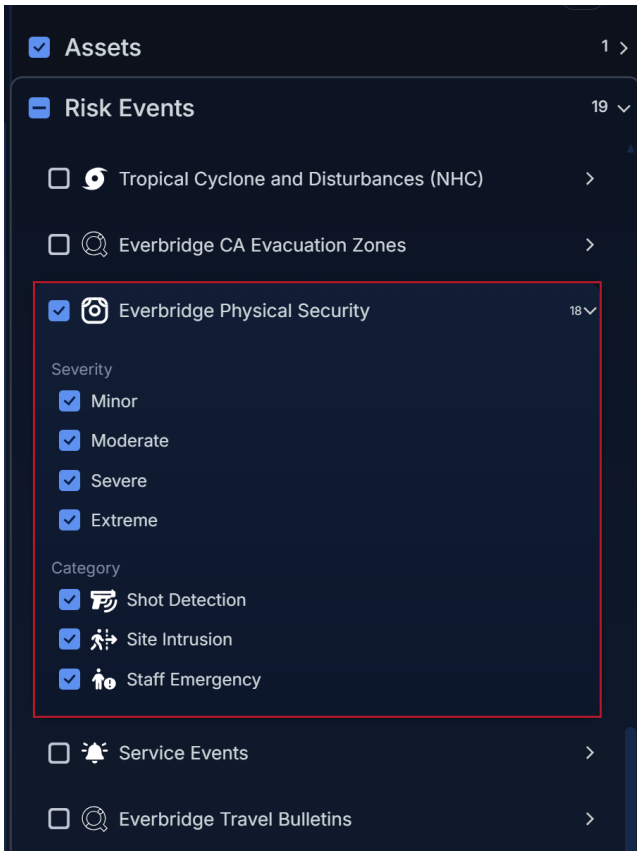
7. Continue to configure Filters as needed, then click **Save**. A confirmation message will appear indicating that the Workflow has been successfully saved.

Verifying the Feed in Visual Command Center

To verify that the Feed is configured correctly:

1. Navigate to **Situational Awareness** > **Visual Command Center**.
2. Expand **Risk Events** in the right-side menu.

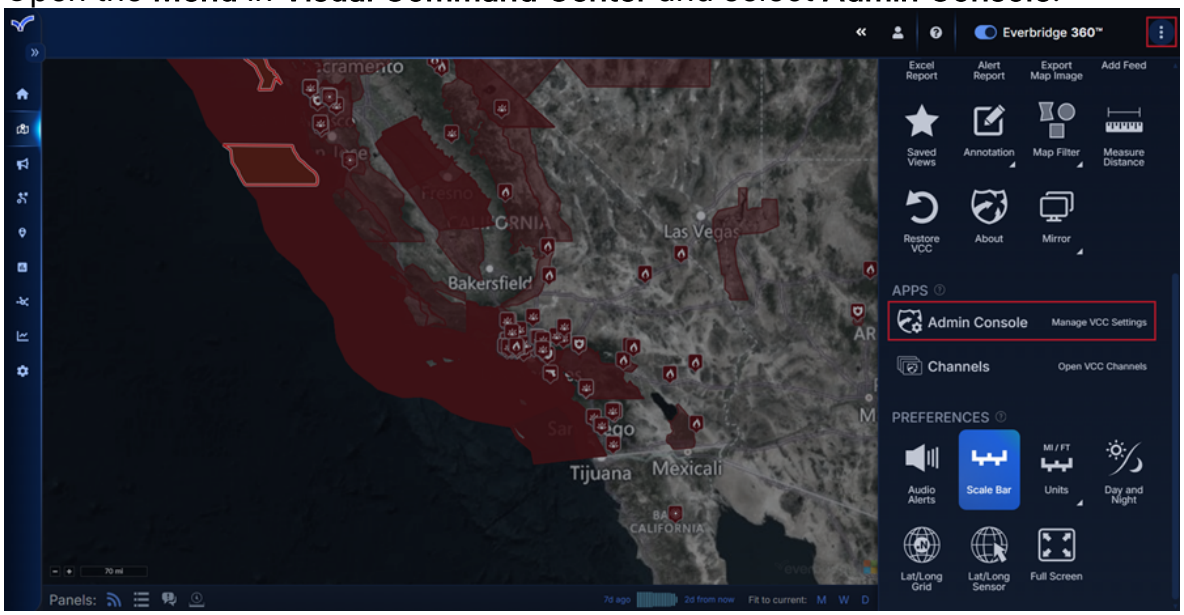
3. Confirm that **Everbridge Physical Security** is visible and enabled in the **Feeds** list.



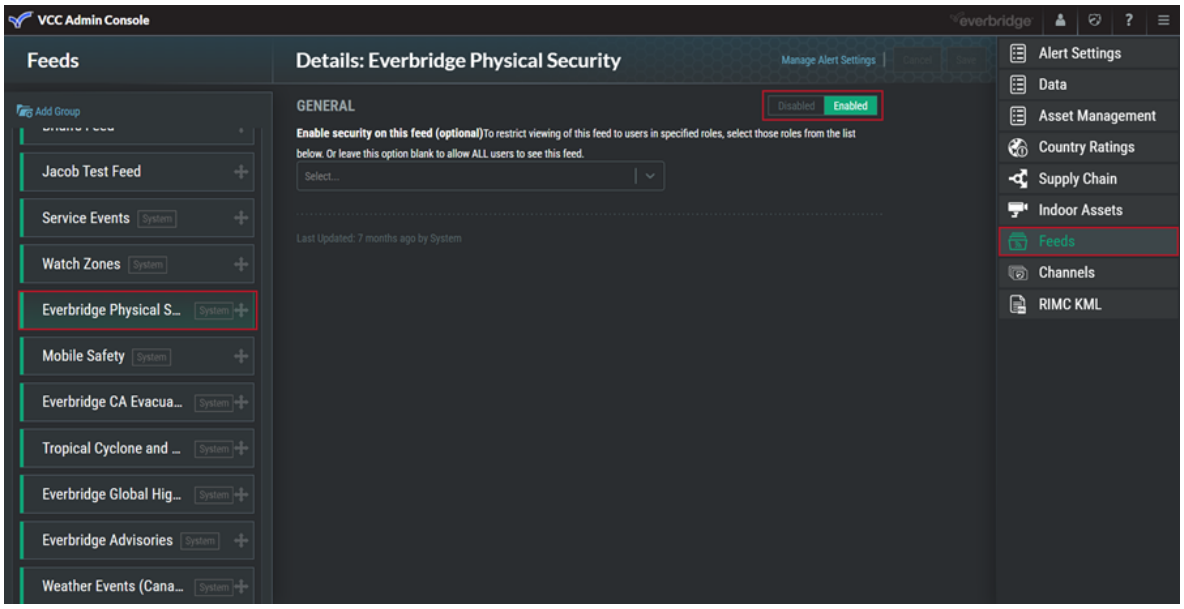
Troubleshooting Feed Visibility

If the feed doesn't appear:

1. Open the **Menu** in **Visual Command Center** and select **Admin Console**.



2. Click **Feeds** on the right.
3. Locate **Everbridge Physical Security** in the **Feeds** list to the left and ensure that it's enabled.



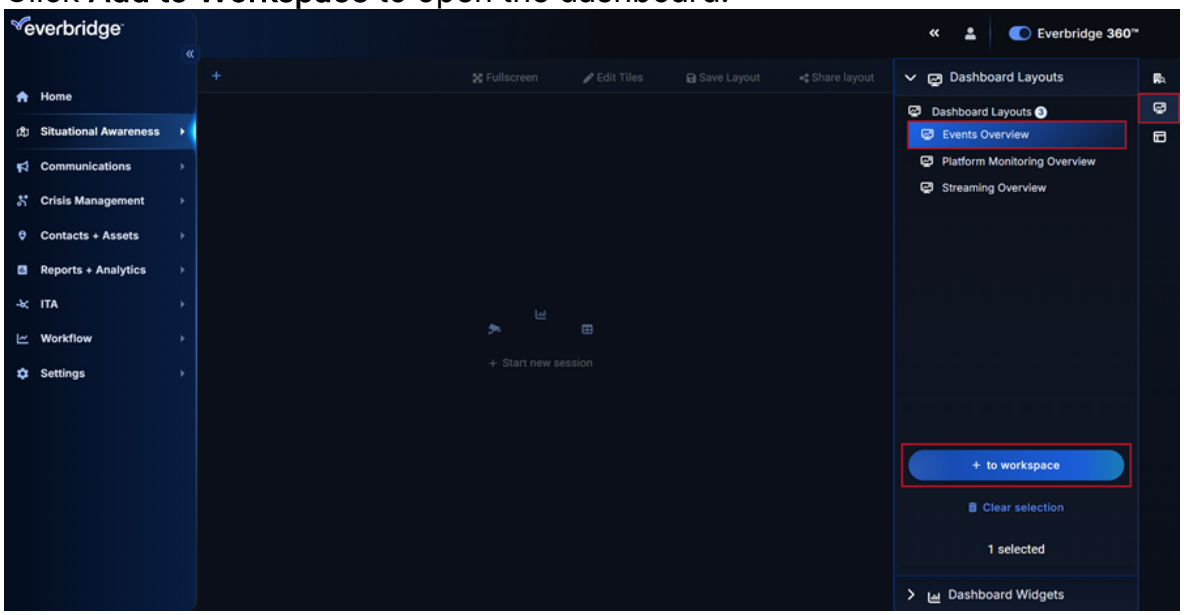
Viewing Events in Physical Security

Once configuration is complete, Events can be viewed directly within the Physical Security work space in Everbridge 360.

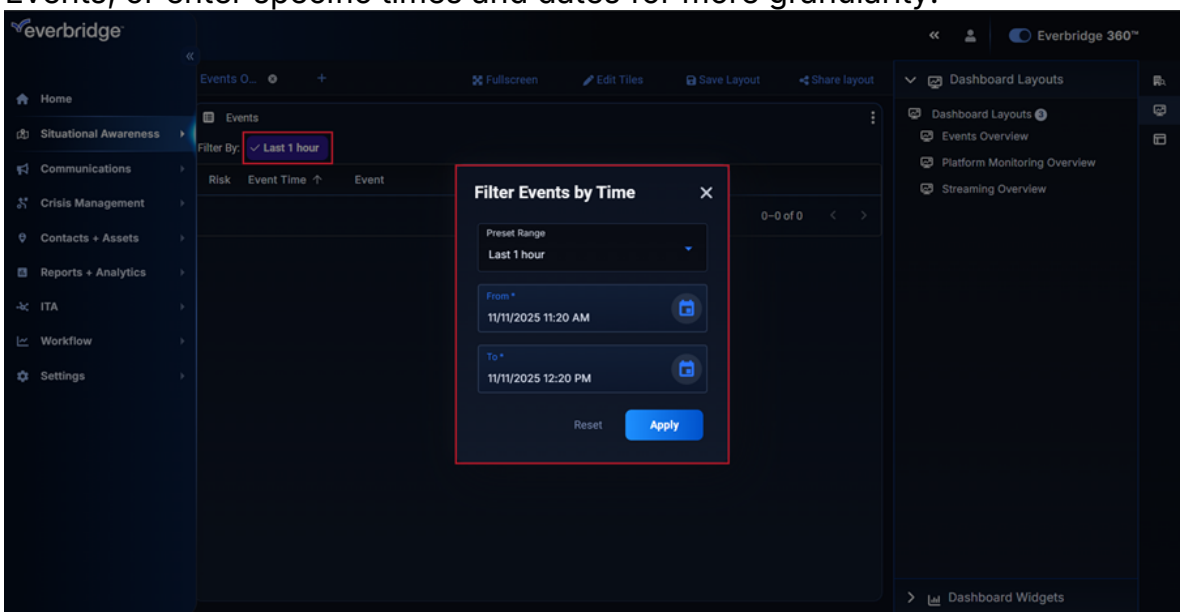
To do this:

1. Navigate to **Situational Awareness** > **Physical Security**.

2. In the right-hand menu, select **Dashboard Explorer**.
3. Choose **Event Overview** from the list of dashboards.
4. Click **Add to Workspace** to open the dashboard.



5. Click the **Filter By** value to select either a preset time range for which to filter Events, or enter specific times and dates for more granularity.

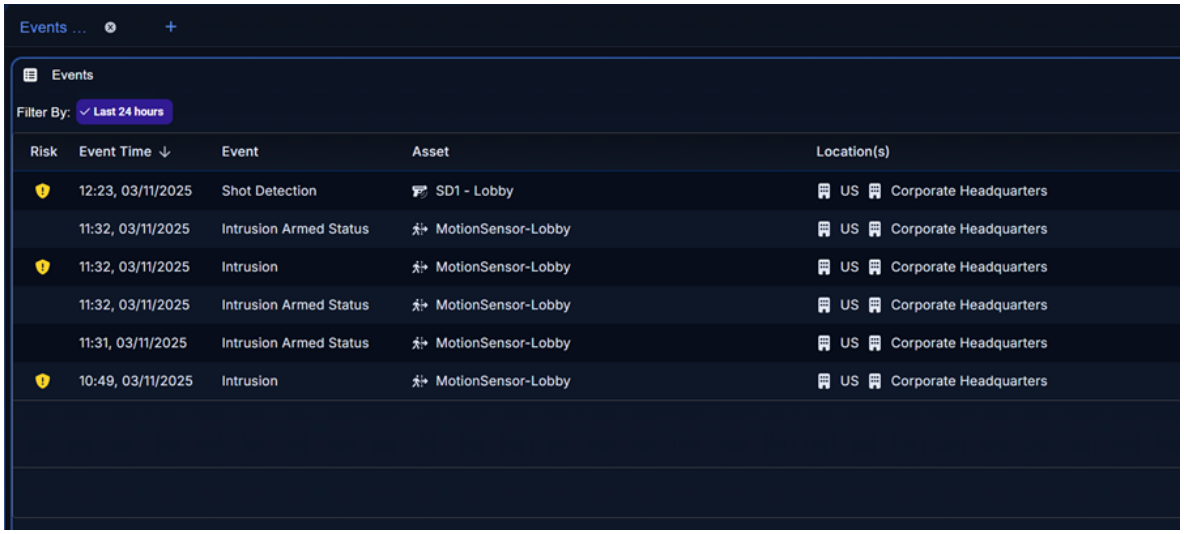


Preset ranges include:

- Last 15 Minutes
- Last 1 Hour
- Last 12 Hours
- Last 24 Hours
- Last 3 Days

- Last 7 Days
- Last 30 Days

6. Click **Apply**. Events matching the selected filter will be displayed in the results view.



NOTE: The **Yellow Shield** icon in the **Risk** column indicates that an Event has been classified as a Risk Event. This icon allows operators to quickly distinguish high-priority, Risk-relevant Events from general Physical Security Activity.

Next Steps

Organizations using additional Everbridge modules should consider linking the Physical Security Feed with the following:

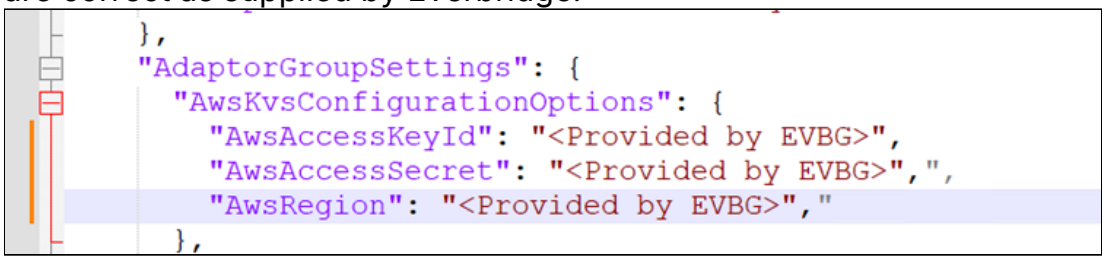
- CEM Playbooks for automated response Workflows.
- Communication Workflows for rapid alerting and stakeholder notifications.
- Incident Reports for documentation and after-action analysis.

Additional Resources

Troubleshooting

If you are unable to view streams from the cameras:

1. Open the **configuration.json** file under C:\ProgramData\Everbridge\SSC\Connectors on the media server.
   a. Check that the **AwsAccessKeyId**, **AwsAccessSecret** and **AWSRegion** are correct as supplied by Everbridge.



   b. If the adaptor is showing offline in the Manager Portal, check that the **AdaptorGroupId** matches the ones in the Physical Security Manager Portal.
   c. Check that the CEM service is running on the media server and restart if necessary.
   d. Confirm the adaptor user by logging into the Everbridge Portal using the values in **EverbridgeAdaptorUsername** and **EverbridgeAdaptorPassword**. If the password has expired, reset it and update the config file. The CEM service on the media server will need to be restarted to pick this up.
2. Check that the time on the media server is correct by referencing https://www.timesynctool.com.

For more information, see Updating Connector Credentials.

Related Documentation and Training

Resources for related Everbridge products is available from:

- **Online Help** - Provides web-based documentation for the Everbridge Suite system. In addition, users can select **(?)** on a page to access context-sensitive help.
- **Everbridge University** offers interactive courses and curriculums to empower users to learn how to use various Everbridge products.
- **Everbridge Support Center** - Hosts downloadable PDF guides, as well as release notes and Knowledge Base articles.