Cisco Cyber Vision New UI Administration Guide, Release 5.6.0

Cisco Cyber Vision
Updated July 6, 2026

Topics included

1 New and changed information

Highlights newly introduced features and significant changes in this release, providing a reference point for tracking updates and modifications to the product documentation.

This table summarizes the feature updates and enhancements available in the New UI for the Cisco Cyber Vision 5.6.0 release.

Table 1: Feature updates

Feature	Description
New UI is the default interface	Cyber Vision New UI is the default interface for Cisco Cyber Vision Center. When you sign in, Cyber Vision opens the new UI automatically.
Network Scanner alert type	The Network Scanner alert type identifies network reconnaissance and scanning attempts. IP addresses specified in the Allowed Scanner list are excluded and do not generate alerts. For more information, see Alerts on page 57.
Assets with unexpected behaviors alert type	Cisco Cyber Vision monitors the assets that are part of the alert rules, and raises an alert when any of those assets are involved in selected behaviors within the configured time window. For more information, see Alerts on page 57.
Communications page enhancement	The Communications page organizes map data by asset groups and displays communications at the asset-interface level. You can view details for asset interfaces, asset groups, and communications within an asset group. The control panel provides filter options and display settings. For more information, see Communication maps on page 80.

Feature	Description
Assets page enhancement	Asset page organizes information into the Summary, Alerts, Vulnerabilities, Communications, Behaviors, Services, Properties, and Interfaces tabs. The Summary page displays cards that provide a quick, high-level overview of the asset. For more information, see Assets on page 40.
Sensor Management extension removal	The Sensor Management extension is no longer available. Sensors that were previously deployed through the Sensor Management extension are now fully managed from the Sensors Management page in the new UI. For more information, see Sensor management frameworks on page 18.
Network detection	The Network Definition page has been enhanced to support new network definitions. Network detection runs automatically at regular intervals, with an option for manual, on-demand execution. For more information, see Network definition on page 29.
Audit logs	Cyber Vision records supported user authentication and configuration actions in the audit log. Authorized users can review and export audit records and configure the retention period from 7 through 365 days. The default retention period is 90 days.
Display themes	You can display the Cyber Vision interface using the **Light** or **Dark** theme or use the theme configured for your system. Select the display theme from the user menu.

2 Introduction to Cisco Cyber Vision New UI

Topics:

Describes the overall functionality and benefits of the Cisco Cyber Vision platform's new user interface, highlighting its innovative features and enhanced capabilities for managing and securing industrial networks, including foundational concepts of the new UI.

Cyber Vision New UI

Describes the new Cyber Vision user interface, outlining its key design improvements, navigation options, and functional enhancements that provide streamlined monitoring and management of industrial cybersecurity environments.

A Cyber Vision New UI is an asset-based user interface that

- organizes information around assets, which is a clearer representation of physical equipment, instead of discrete components or device entries,
- aggregates multiple network identities (including interfaces, IP addresses, and MAC addresses) that belong to the same physical equipment, and
- prioritizes the most relevant information, such as asset name, type, and version, to help users stay focused and reduce clutter.

User roles for the Cyber Vision Center New UI are defined in the Classic UI **Admin** > **Users** > **Role Management**.

Table 2: Feature History Table

Feature	Release Information	Feature Description
New UI	Release 5.3.x	Cisco Cyber Vision Center offers New UI that comprises simplified, structured views of assets, vulnerabilities, and alerts. The New UI includes a new method for automatically grouping assets using AI-based clustering. Click **Go to Cyber Vision New UI** in the top banner of your Center to get started.
Cisco Cyber Vision Center new UI is the default interface	Release 5.6.x	Cyber Vision New UI is the default interface for Cisco Cyber Vision Center. When you sign in, Cyber Vision opens the new UI automatically.
Display themes	Release 5.6.x	You can select the **Light** or **Dark** theme from the user menu. You can also select **System** to use your system's display theme.

Key differences between Classic UI and New UI

The Classic UI focuses on technical entities such as components and devices. Users need to manually define presets, such as baselines or monitoring sets. They often manage separate entries for each network identity, which results in complexity and confusion.

The Cyber Vision New UI connects the physical industrial environment and its digital representation. It visually groups all elements associated with a single physical equipment. Examples include production line equipment or customer installations.

Table 3: Contrast table

Feature	Classic UI	New UI
Entity focus	Components, devices	Assets–representation of physical equipment

Feature	Classic UI	New UI
Information grouping	Each network identity shown as a separate item	Multiple identities grouped by asset
User effort	Requires manual preset definitions	Provides automatic aggregation to improve clarity
Information display	Shows all details, often overwhelming	Displays only the most relevant attributes of each asset.

Change the display theme

Change the appearance of the Cyber Vision interface by selecting a light, dark, or system theme.

Select the display theme that you want to use for the Cyber Vision interface.

Cyber Vision provides the following display-theme options:

- **Light**: Displays the interface using the light theme.
- **Dark**: Displays the interface using the dark theme.
- **System**: Uses the display theme configured for your system.

Procedure

1. In the upper-right corner of the Cyber Vision interface, select your username to open the user menu.
2. Under **Theme**, select **Light**, **Dark**, or **System**.

Cyber Vision applies the selected theme to the interface.

3 Set up Cyber Vision Center

Topics:

Outlines the end-to-end setup process for Cyber Vision Center, including configuring system settings, managing sensors, defining and managing networks, establishing organization hierarchies, managing assets, and configuring filters for effective network visibility and security.

System settings

Explains how system settings ensure secure, reliable operation of Cyber Vision Center.

System settings are core configuration features that

- define external communication channels for the Cyber Vision Center,
- secure and synchronize operational parameters, and
- enable access to critical external services under controlled conditions.

Table 4: Cyber Vision Center system settings

Setting	Purpose
Date and Time	Date and time synchronization is essential for system stability. A Network Time Protocol (NTP) server ensures that the Cyber Vision Center and all connected sensors share the same time. Synchronized time is required for accurate logging and communication between devices. If an NTP server is unavailable, set the time manually. However, automated synchronization is highly recommended.
DNS (Domain Name System)	DNS operates as the network's directory service. It translates human-readable domain names into IP addresses required for communication. This setting enables Cyber Vision Center to resolve and connect to other systems by name.
Proxy	In secure environments, Cyber Vision is isolated from the internet to protect sensitive data. Some advanced features require Internet connectivity. A proxy server allows Cyber Vision to safely access required external services or updates while protecting the internal network. Cyber Vision sends requests to the proxy server instead of connecting directly to the internet. The proxy handles communication and maintains security and functionality.

Feature history table

Feature	Release Information	Feature Description
Enhanced system connectivity and security settings	Release 5.5.x	The system offers intuitive user interface based settings to simplify administrative workflow. Date and time settings allow for precise time synchronization for the center and connected sensors. DNS management streamlines system access. Proxy configurations ensure secure, controlled connectivity in isolated environments.

Configure the date and time

Configure the date and time settings for your system, either by connecting to an NTP server or manually setting the time.

Synchronize the date and time across your center and all connected sensors to ensure system stability and accurate logs.

Synchronize the date and time consistently for accurate logs and device communication. Use an NTP server to automate and maintain this process. If an NTP server is unavailable, manually configure the date and time.

Procedure

1. From the main menu, choose **Configuration** > **System** > **Date and Time**.
2. Select a method to configure the date and time.

Date and time method	Steps to be taken
(Recommended) Connect to an NTP server	**a.** Enable **NTP Servers**. **b.** Click **Add New NTP Server**. **c.** Enter the IP address or hostname of your NTP server. **d.** Optionally, enter a **Key ID** or **AES-CMAC** for secure authentication. **e.** Click **Test Connection** to verify configuration. **Note** • You can delete added NTP servers as needed. • Click **Reset changes** to revert to your last saved settings.
Manually set the time, in UTC	**a.** Enable **Manually set time (UTC)**. **b.** Set the date and time manually, or click **Get Browser Time** to fetch the current time from your browser and populate the UTC field.

3. Click **Save Changes**.

The system saves the date and time configuration.

What to do next

From the main menu, choose **Configuration** > **System** > **Date and Time** and verify the UTC time.

Configure proxy servers

Configure proxy servers for secure external network connections used by features such as Smart Licensing and SEA integrations.

Set up secure proxy connectivity for features that require external access, including Smart Licensing, SEA, XDR, and other integrations.

Many integrations and licensing features require external network access. Configuring proxy servers ensures that network traffic is securely routed to these services.

Before you begin

- Obtain the IP address and port for your proxy server.
- If your proxy requires authentication, have the username and password ready.

Procedure

1. From the main menu, choose **Configuration** > **System** > **Proxy**.
2. Enable the proxy feature.
3. Enter the IP address (IPv4 or IPv6) and port details for your proxy server.
4. If required, enter the username and password for proxy authentication.
5. Click **Test connection** to verify proxy configuration.
6. Click **Save changes** to apply the configuration.

You see a confirmation message for a successful proxy check. The system applies your proxy configuration and enables network connections through the proxy.

What to do next

- If necessary, click **Reset changes** to restore previous settings.
- Verify that external connectivity for integrations or license-related features continues to function properly.

Configure DNS servers

Configure DNS servers to enable hostname resolution for Cyber Vision Center communications.

Ensure Cyber Vision Center can resolve hostnames to IP addresses for connectivity with other systems.

Configuration of Domain Name System (DNS) servers allows Cyber Vision Center to communicate with other systems that require hostname resolution.

Before you begin

Verify that you have the IP address of the DNS server.

Procedure

1. From the main menu, choose **Configuration** > **System** > **DNS**.
2. Click **Add new DNS server**.
3. Enter the IP address of the DNS server.

   You can add up to 4 DNS servers.
4. Click **Test connection** to verify that Cyber Vision Center can reach the DNS server.

   The system provides a clear notification if the connection fails.
5. Click **Save changes** to apply the settings.

Cyber Vision Center uses the configured DNS servers to resolve hostnames to IP addresses. This setting enables Cyber Vision Center to communicate with other systems.

What to do next

If necessary, click **Reset changes** to revert to your previously saved settings. Verify external connectivity, such as integration or license connectivity, to ensure proper operation.

Audit logs

Use audit logs to review supported user authentication and configuration actions in Cyber Vision.

Understand the user actions that Cyber Vision records and the information available for each audit event.

Cyber Vision records supported user actions in the audit log. Audit records help administrators review user activity and configuration changes.

Examples of recorded actions include:

- User authentication
- Creation of an organization hierarchy level
- Assignment of a network to an organization hierarchy level

> **Note**
>
> Cyber Vision does not currently record every user action. For example, sensor onboarding actions might not appear in the audit log.

Table 5: Feature History Table

Feature	Release Information	Feature Description
Audit logs	Release 5.6.x	Cyber Vision records supported user authentication and configuration actions. Authorized users can review and export audit records and configure the audit-log retention period.

Table 6: Audit record details

Field	Description
Date	Shows when the audited event occurred.
Username	Identifies the user who performed the action.
Type	Identifies the category of the audited event.
Status	Shows whether the action succeeded or failed.
Description	Provides details about the audited action. Select **View more** to display additional information.

View audit logs

Review supported user authentication and configuration actions recorded by Cyber Vision.

View audit records to review user activity and configuration changes in Cyber Vision.

Cyber Vision displays the actions that it currently supports for auditing. The Audit page is available from the user menu.

Before you begin

Ensure that your user role has **Read** permission for Audit.

Procedure

1. In the upper-right corner of the Cyber Vision interface, select your username to open the user menu.
2. Select **Audit**.
3. Review the audit records.

   The table displays the date, username, event type, status, and description for each recorded event.
4. Use the available actions as required:
   - Select **View more** to display the complete description of an event.
   - Select the filter icon to narrow the displayed audit records.
   - Select **Export** to download the audit records.

Cyber Vision displays the available audit records. If you export the records, Cyber Vision downloads the audit data.

What to do next

Configure the audit-log retention period if you need to change how long Cyber Vision retains audit records.

Configure audit log retention

Configure how long Cyber Vision retains audit records.

Set the number of days that Cyber Vision retains audit records.

Cyber Vision retains audit records for 90 days by default. You can configure the retention period from 7 through 365 days.

Before you begin

Ensure that your user role has **Write** permission for Audit.

Procedure

1. In the upper-right corner of the Cyber Vision interface, select your username to open the user menu.
2. Select **Audit**.
3. Select the settings icon.
4. In **Retention period**, enter a value from 7 through 365 days.
5. Select **Save**.

Cyber Vision retains audit records for the configured number of days.

What to do next

Review the Audit page periodically to monitor recorded user activity and configuration changes.

Sensor management frameworks

Explains how Cyber Vision sensor management enables efficient deployment, configuration, and operation of sensors and hosts in industrial networks.

A sensor management framework is a comprehensive platform that

- coordinates the deployment, configuration, and operation of Cyber Vision sensors and hosts,
- manages industrial network environments efficiently, and
- streamlines sensor and host actions, including onboarding, monitoring, and control.

Host and sensor management

- Host management: A host is the physical platform where a sensor IOx application runs. First, onboard and validate hosts. Then, deploy sensors to each host.
- Sensor management: The sensors page allows you to manage sensors and view sensor statistics, operations, and details for each deployed sensor.

Feature history table

Feature	Release Information	Feature Description
Sensor Management extension removal	Release 5.6.0	The Sensor Management extension is no longer available. Sensors that were previously deployed through the Sensor Management extension are now fully managed from the **Sensors Management** page in the new UI.
Enhancement of sensor health monitoring	Release 5.5.x	Monitor sensor health proactively with automated updates and deep insights. The sensor management system tracks each sensor's status and provides actionable updates, helping you resolve issues before they affect your operations. Use **Advanced View** to analyze performance trends and troubleshoot efficiently.

Sensor deployment overview

Cyber Vision sensors operate as IOx applications. They perform deep packet inspection (DPI) on industrial network traffic and send metadata to the Cyber Vision Center. You can manage multiple sensors concurrently across the network.

Sensor management

Introduces the host model for managing Cisco Cyber Vision sensors. You onboard a physical host before you deploy a sensor, separating device connectivity from network traffic collection.

The Sensor management provides a host model for managing Cisco Cyber Vision sensors. A sensor host is the physical device (such as routers, switches, gateways, etc.) on which Cisco Cyber Vision deploys a sensor. The host model connects Cisco Cyber Vision to the device before the sensor begins collecting network traffic.

- A sensor is deployed on a host that corresponds to the physical device.
- Onboarding makes the host reachable to Cisco Cyber Vision; it does not begin traffic collection.
- After you onboard the host, you can deploy a sensor and configure its collection interface.
- Cisco Cyber Vision uses the Product ID to identify supported switches and routers.

Sensor deployment uses two stages:

1. Onboard hosts to Cisco Cyber Vision
2. Deploy sensor apps to hosts

The collection interface supplies the address used by the sensor to send gathered network data to Cisco Cyber Vision.

Sensors previously deployed using the sensor-management extension in the classic UI are available on the Sensor Management page in the new UI following automatic migration. Refer to Migrating sensors after system update on page 19.

Migrating sensors after system update

Describes the automatic migration of legacy sensors managed by sensor-management extension to the sensor-host model after a system update, preserving sensor identity and configuration without requiring application reinstallation.

When the Cisco Cyber Vision system is updated to version 5.6.0 and rebooted, the system identifies legacy sensor-management extension data. It then migrates the sensors to the sensor-host model on the **Sensor management** page of the new UI.

Summary

The key components involved in the process are:

- System: Detects legacy sensor-management extension data and initiates migration, including a final backup before removing the sensor management extension.
- Sensors: Preserve their identity and configuration as they transition to the sensor-host model in the new UI **Sensor management** page.

Workflow

The process involves the following stages:

1. Upon the first reboot after the Cisco Cyber Vision 5.6.0 update, the system automatically migrates legacy sensors
   - Migration is fully automated; you do not need to uninstall or reinstall the sensor application.
   - For each migrated sensor, the system automatically creates hosts by extracting the host identity attributes (host address, label, credentials, product ID, serial number, and similar data) from the internal database.

Table 7: Configuration imported into the sensor-host model

Configuration area	Imported data
Host identity and access	Host address, label, credentials, Product ID, and serial number
Traffic collection	Capture and collection interfaces, VLANs, gateway, RSPAN, capture mode, and custom filter

Configuration area	Imported data
Sensor configuration	Sensor template, Active Discovery configuration, and SRA configuration

2. Post-migration management and status updates.
   - In Classic UI, the sensor management extension is removed from the **Extension** page, but sensors installed using the extension remain visible in the **Sensor Explorer** page. Sensor management actions (reconfigure, undeploy) are no longer exposed for these sensors.
   - In new UI, the migrated sensors appear in the **Sensor Management** page with a status of **Deployment successful**. These sensors are no longer labeled as Externally managed.
   - The initial host status is QUEUED. Background discovery can update the host status to READY, UNREACHABLE, WRONG_CREDENTIALS, or NOT_READY.
   - When the host is in Ready state and the sensor deployment succeeds, redeploy, uninstall, and update actions are available.

Result

The legacy sensor-management extension is removed, and sensors are fully integrated into the sensor-host model without additional downtime.

What's next

To onboard, manage, or monitor sensors, navigate to the new UI Sensor Management page.

Host actions

Lists the available host actions and their descriptions for Cyber Vision sensor management.

Hosts can be onboarded either by uploading a CSV file for multiple hosts or by manually entering host information individually. For detailed instructions, refer to the Onboard hosts to Cisco Cyber Vision section in the *Deploy Cisco Cyber Vision Sensor on Switches and Routers* guide.

This table lists the available host actions for managing Cyber Vision sensors and describes each action:

Action	Description
Host Status	Check the host readiness status to ensure IOx is running and necessary conditions for deployment are met.
Deploy Sensor	Deploy the sensor application on the selected host.
Change Credentials	Update the username and password stored in the system to access the host.
Remove Host	Remove the host from the list.

Sensor capabilities

Provides a reference to sensor host model capabilities available after sensor migration and deployment in the Sensor management page.

This reference provides details on managing sensor capabilities through the Sensor management page.

Capabilities

On the **Sensor management** page, each sensor lists its configuration under the **Capabilities** column. You can click on a listed capability to modify its settings as needed.

The table shows the most common capabilities listed under the **Capabilities** column:

Table 8: Deployed Sensor capabilities

Capability	Configuration
Snort	Change the Snort status - Enable or Disable
Active Discovery	Configure Active Discovery
Secure Remote Access (SRA)	Change Secure Remote Access configuration: Use center as proxy, Direct, or Proxy.

Sensor actions

This reference lists the sensor actions you can use to manage Cyber Vision sensors and explains their purpose.

Cisco Cyber Vision sensor deployment follows host onboarding. The sensor collects network data from the host and sends it to Cisco Cyber Vision using a dedicated collection-interface address. For detailed instructions on deploying sensors, refer to the Deploy sensor apps to hosts section in the *Deploy Cisco Cyber Vision Sensor on Switches and Routers guide*.

This table lists the available sensor actions you can use and describes how each helps you manage Cyber Vision sensors.

Action	Description
Redeploy	Send the IOx package to redeploy the sensor. You can reconfigure parts such as IP parameters.
Update	When a new Cyber Vision Center version is deployed, a new sensor version becomes available. Use **Update** to upgrade.
Assign to Organization Hierarchy	Map sensors to an organizational hierarchy to organize asset data and operational context. See Assign sensors to the Organization Hierarchy on page 22
Change GPS Location	Manually update the GPS coordinates of the sensor to reflect its location. For more information on the GPS coordinates configuration, see Sensor geolocation data.
Configure Snort	Enable or Disable Snort.
Configure Active Discovery	Configure Active Discovery or change to Passive only to disable Active Discovery.
Configure Secure Remote Access	Enable Secure Remote Access and configure proxy setting.
Uninstall	Remove the sensor from the list and uninstall the application from IOx.

Assign sensors to the Organization Hierarchy

Assign one or more sensors to an organization hierarchy so asset creation is enabled within Cyber Vision.

Enable asset creation within Cyber Vision by mapping sensors to an organization hierarchy.

Use this task to map sensors in your environment to a defined organization hierarchy. This enables Cyber Vision to structure asset data and operational context according to organizational boundaries.

Procedure

1. From the main menu, choose **Configuration** > **Sensor Management** > **Sensors**.
2. Check the checkboxes of the sensors.
3. Select **Assign to Organization Hierarchy** from the **More actions** list.
4. Select the organization hierarchy you want to assign the sensors to.
5. Click **Assign** to confirm.

Cyber Vision assigns the selected sensors to the organization hierarchy you specified. Each assigned sensor enables asset creation within Cyber Vision based on its organizational context.

Configure Snort

Configure Snort intrusion detection on compatible Cisco sensors to monitor network traffic for suspicious activities using Snort rules.

Enable Snort to detect and alert on malicious network activity on Cisco sensors.

Snort is an intrusion detection system (IDS) that raises alerts for suspicious or malicious network activity based on predefined rules. By default, Snort is disabled on sensors but enabled on the Center's Deep Packet Inspection (DPI)

Enabling Snort on compatible sensors helps monitor assets for threats.

For further details on Snort, refer to the Snort topic in the *Cisco Cyber Vision Classic UI Administration Guide*.

For information on the Snort-related intrusion detection alert rules, refer Alerts on page 57.

Before you begin

- Ensure your sensor is deployed on a device compatible with Snort:
  - Cisco IC3000 Industrial Compute Gateway
  - Cisco Catalyst 9300 Series Switches
  - Cisco IR8340 Integrated Services Router Rugged
  - Center DPI Interface
- Configure Snort rules for the Intrusion Detection alert type.

Follow these steps to configure Snort on Cisco sensors.

Procedure

1. From the main menu, choose **Configuration** > **Sensor Management**.
2. Click the **Sensors** tab.
3. Locate the sensor on which you want to enable Snort.

4. Under **Capabilities**, click **Snort**. Alternatively, under **Action**, click the horizontal ellipsis (...) icon and choose **Configure Snort**.

   You can also select multiple sensors and then choose **More actions** > **Configure Snort**.

5. In the **Configure Snort** dialog, click **Enable Sort**.

   A check mark appears next to **Snort** under **Capabilities**, confirming that Snort is enabled.

Snort actively monitors network traffic on the selected sensors for suspicious or malicious activity according to the configured rules.

Disable Snort

Configure a sensor to disable Snort-based intrusion detection when monitoring is no longer required.

Disable Snort intrusion detection on a sensor to cease monitoring traffic for threats.

Perform this task when Snort monitoring is no longer needed for a given sensor in your environment.

Before you begin

Ensure Snort is currently enabled on the sensor.

Follow these steps to disable Snort on a sensor.

Procedure

---

1. From the main menu, choose **Configuration** > **Sensor Management**.
2. Click the **Sensors** tab.
3. Locate the sensor on which you want to disable Snort.
4. Under **Capabilities**, click **Snort**. Alternatively, under **Action**, click the horizontal ellipsis (...) icon and choose **Configure Snort**.

   You can also select multiple sensors and then choose **More actions** > **Configure Snort**.

5. In the **Configure Snort** dialog, click **Disable Snort**.

   Snort is disabled on the selected sensor(s). The check mark next to **Snort** under **Capabilities** disappears.

Configure Active Discovery on a sensor

Provides instructions to enable Active Discovery from Sensor Management, select the discovery interface, and add dedicated interfaces.

Enable active discovery to collect asset properties on the network using a compatible Cisco Cyber Vision sensor.

You can configure Active Discovery on a compatible Cisco Cyber Vision sensor after the sensor is deployed. Active discovery sends requests from the sensor to assets in the network and collects their properties.

To configure active discovery on a switch, router, or Cisco IC3000, sensors must be deployed using the IOx sensor application file that supports active discovery.

On a Cisco IC3000, you can configure Active Discovery by performing a manual configuration.

Before you begin

- Deploy a sensor with correct settings, including IP address, VLAN, gateway, or routes.
- Confirm the sensor platform supports active discovery. Supported devices include:

- Cisco IE3300, Cisco IE3400, and Cisco IE9300.
- Cisco IC3000 Industrial Compute Gateway.
- Cisco Catalyst 9300, Cisco Catalyst 9300X and Cisco Catalyst 9400.

Follow these steps to configure active discovery.

Procedure

1. From the main menu, choose **Configuration** > **Sensor Management**.
2. Click the **Sensors** tab.
3. Locate the sensor on which you want to enable or update Active Discovery.

   Note

   You can configure active discovery only if it is shown in the **Capabilities** column for that sensor.

4. Under **Capabilities**, click **Active Discovery**. Alternatively, under **Action**, click the horizontal ellipsis (...) icon and choose **Configure Active Discovery**.

   Active Discovery must be configured for each sensor individually.

5. In the **Configure Active Discovery** dialog, do the following:
   a) If you want Active Discovery to use the sensor's collection network, select **Use collection interface**.

      The collection network interface can perform discovery on the same subnet as the sensor IP address or through the sensor's collection gateway.

   b) To perform Active Discovery on additional subnets, enter **IP address**, **Prefix length**, and **VLAN number**.

      For Cisco IC3000, select a physical **Interface** from the drop-down list.

      These settings define the dedicated network interface used for active discovery.

   c) To add another network interface, click **+Add network interface**.
   d) Click **Configure Active Discovery**.

   A check mark appears next to **Active Discovery** under **Capabilities**, indicating configuration is successful.

Active discovery is enabled on the sensor, and it is now ready to scan assets using the configured interfaces.

What to do next

To complete the center-side Active Discovery configuration, set the required policy and profile in the classic UI under **Admin** > **Active Discovery**. The policy selects the protocols to use; the profile specifies the assets and sensor. Only sensors with active discovery activated appear in the sensor list. For more information, refer to *Cisco Cyber Vision Active Discovery Configuration Guide*.

Disable Active Discovery on a sensor

Guides you through changing a configured sensor to Passive only and disabling Active Discovery from the Configure Active Discovery dialog.

Ensure a sensor stops Active Discovery and operates in passive-only mode.

Active Discovery allows a sensor to actively query network assets to gather information. Disabling Active Discovery ensures the sensor remains passive and only observes network traffic.

Before you begin

Confirm you have access to a sensor currently configured with Active Discovery.

Follow these steps to disable Active Discovery for a sensor:

Procedure

1. From the main menu, choose **Configuration** > **Sensor Management**.
2. Click the **Sensors** tab.
3. Locate the sensor for which you want to disable Active Discovery.
4. Under **Capabilities**, select **Active Discovery**. Alternatively, under **Action**, select the horizontal ellipsis (...) icon and then select **Configure Active Discovery**.
5. In the **Configure Active Discovery** dialog, select **Passive only**.
6. Click **Disable Active Discovery**.

Active Discovery is disabled for the sensor, and the sensor is set to passive-only mode.

Configure Secure Remote Access on a sensor

Guides you through enabling Secure Remote Access on one deployed sensor, selecting the center, direct, or proxy connection method, and providing proxy connection details when required.

Enable Secure Remote Access on a sensor and configure its connection method to reach remote services securely.

Use Sensor Management to configure Secure Remote Access for individual sensors. The sensor uses the chosen method (center as proxy, direct, or proxy) to connect to Cisco services and the IoT Operations Dashboard.

Before you begin

Make sure center-side Secure Remote Access integration is enabled and configured for the target IoT Operations Dashboard tenant (In the classic UI, navigate to **Admin** > **Integrations** > **SRA** > **Configuration**).

Ensure Active Discovery is enabled on the sensor; this feature requires only a compatible platform. Refer to the Active Discovery configuration documentation - Configure Active Discovery on a sensor on page 23

Follow these steps to configure Secure Remote Access on a sensor.

Procedure

1. From the main menu, choose **Configuration** > **Sensor Management**.
2. Click the **Sensors** tab.
3. Locate the sensor to configure Secure Remote Access.

   Configure Secure Remote Access for one sensor at a time.

4. Under **Capabilities**, click **SRA**. Alternatively, under **Action**, click the horizontal ellipsis (...) icon and choose **Configure Secure Remote Access** .

   Configure Secure Remote Access for one sensor at a time.

5. In the **Configure Secure Remote Access** dialog, do the following:
   a) Toggle **Use SRA** to enable Secure Remote Access.

The configuration dialog identifies the sensor whose Secure Remote Access configuration you are changing. Enable SRA, and then choose the proxy or another connection method.

b) Select a connection method:

- **Use center as proxy** - If the sensor uses the Center to reach Cisco services.
- **Direct** - If a Collection gateway is specified.
- **Proxy** - If the sensor uses another server for Cisco services.

If you select **Proxy**, enter the details as shown in the table.

Table 9: Proxy settings

Field	Description
http:// or **https://**	Depending on your requirements, choose either **http://** or **https://** from the drop-down list.
Server	Enter the Server IP address.
Port	Enter the Port number.
Username and **Password**	(Optional) Enter the username and password.
Primary DNS and **Secondary DNS**	(Optional) Enter the primary and secondary DNS.

6. Click **Configure Secure Remote Access**.

A check mark appears next to **SRA** under **Capabilities**, confirming Secure Remote Access is configured.

The Center updates the sensor and IoT Operations Dashboard configuration, creates and deploys the Secure Remote Access agent as needed.

7. To validate the SEA Agent Connection, do the following:
   a) Log in to the IoT Operations Dashboard with your IoT OD credentials.
   b) In **Secure Equipment Access**, choose **System Management** > **Network Devices.**.
   c) Verify the SEA Agent Connection is **Up** for the configured network device.

When the connection is up, the sensor can access remote assets on the network.

Secure Remote Access is configured for the sensor. When the connection is established, the sensor can access remote assets through the chosen method.

Disable Secure Remote Access on a sensor

Guides you through disabling Secure Remote Access for a configured sensor from the Configure Secure Remote Access dialog.

Prevent a sensor from accessing remote assets by disabling Secure Remote Access.

Disable Secure Remote Access for a sensor when remote access is no longer needed, one sensor at a time, from Sensor Management.

Before you begin

Ensure Secure Remote Access is configured and available for the sensor under **Capabilities**.

Follow these steps to disable Secure Remote Access on a sensor.

Procedure

1. From the main menu, choose **Configuration** > **Sensor Management**.
2. Click the **Sensors** tab.
3. Locate the sensor for which you want to disable Secure Remote Access.

   Secure Remote Access can be disabled for one sensor at a time.
4. Under **Capabilities**, select **SRA**. Alternatively, under **Action**, select the horizontal ellipse (...) icon and choose **Configure Secure Remote Access**.
5. In the **Configure Secure Remote Access** dialog, disable the **Use SRA** option.
6. Click **Configure Secure Remote Access**.

Secure Remote Access is disabled for the selected sensor.

Sensor health statuses and signals

Lists and explains the key sensor health statuses and signals used in the system, including what each status and signal means, and how to interpret them for device health management.

Health statuses

You can view the current health status for each sensor. The status helps you decide when to take action.

Status	What this status means
Unknown	The sensor is managed by Classic UI.
Critical	The sensor has stopped communicating and is not sending data to the Center.
Needs Attention	The sensor is connected and sends data, but one or more health signals are outside the allowed thresholds. You may need to reconfigure the sensor or take other action.
Healthy	The sensor operates within normal parameters and no health signals are active.
Pending	The sensor is connected. The system updates the health status after it collects initial data. This process may take up to an hour.

To view the current health status for each sensor, from the main menu choose **Configuration** > **Sensor Management**.

Sensor health signals

When a sensor's health status is **Needs Attention**, the Cyber Vision Center provides these health signals to explain the issue and suggest mitigation steps.

Table 10: Health signals

Signal	What this signal means
With Time Drift	The time difference between the sensor and the Center exceeds the configured threshold.

Signal	What this signal means
Degraded Flow Health	The overall traffic from the sensor to the Center after connection is less than expected. You can use this information to decide if traffic integrity falls below the configured threshold.
Degraded Traffic Health	Unicast traffic is lower than expected. You see this signal when the ratio of unicast traffic to broadcast or multicast traffic is too low.

To view remediation details for a sensor with the **Needs Attention** health status:

- Select the sensor in **Configuration** > **Sensor Management**.
- Access the remediation card to see health signals, issue descriptions, sensor summaries, and mitigation steps.

For more information about system health, network metrics, and network interface bandwidth, see **System statistics for Center and sensors** topic in the Cisco Cyber Vision Classic UI Administrator Guide.

Features of the sensor Advanced view

Provides a comprehensive reference for the sensor Advanced view, including behavioral trends, real-time statistics, and key metrics used to monitor and troubleshoot sensor performance.

In the sensor **Advanced view**, you can:

- Examine sensor behavioral trends and performance.
- Troubleshoot sensor issues using real-time statistics.

Collection Details

Monitor sensor connection health, uptime, and network statistics, with options to filter by time periods.

Detail	Description
Connection Status	Provides sensor connection information with the Center, including online or offline status with date and time.
Link Status	Indicates two link statuses: • If the sensor is connected to the Center, the status is UP. • If the sensor is rebooted or restarted, the status is DOWN.
Time Drift	Calculates the time difference between sensor time and Center time when system information is received.
TX/RX Queue	TX and RX queues are memory buffers. They temporarily store outgoing (Transmit) and incoming (Receive) data packets. This helps manage traffic flow and prevents data loss between the network interface and the system Transmission Control Protocol/Internet Protocol (TCP/IP) stack.

Detail	Description
Retransmits	Number of TCP retransmits to resend packets lost, corrupted, or unacknowledged during initial transmission. This ensures reliable and complete delivery.
TCP Connection - Connection Reset & TCP State	Displays the TCP connection status from the Center to the sensor and shows connection reset events. These events indicate port changes or reestablishments. The connection state may change rapidly with each reset.

Data Quality

Displays information about network traffic, packet distribution, and flow statistics.

Detail	Description
Flow Count	Shows the number of traffic flows over the selected period. Receiving traffic flows indicates good sensor health.
Total Bytes	Shows the total size of each packet within the selected interval.
Total Packets	Shows the packet count within the selected interval.
Protocol Distribution	Provides the count of TCP, UDP, and other protocols detected in the traffic.
Flow Type Distribution	Shows counts for traffic flow types such as Unicast, Broadcast, and Multicast.

Access the sensor advanced view

To access advanced sensor details:

- From the main menu choose **Configuration** > **Sensor Management** and select the sensor.
- Click **Advanced view**.

Network definition

Introduces network definition in Cyber Vision, guiding you through configuring subnetworks, classifying IP addresses as internal or external, managing asset grouping and metadata, and handling exceptions for IP address classification and their impact on security assessments.

A network definition is a network configuration element that can be used to define IP ranges and classify them as internal (OT), internal (IT), or external. This configuration helps you group or exclude assets for security assessments and manage metadata by assigning custom properties network-wide to all assets.

IP address classification

By default, networks corresponding to private IP addresses are classified as OT Internal. This is a factory configuration that can be customized by the user after deployment to meet specific operational requirements.

In addition to these private ranges, the following special IP addresses and networks are also defined as Internal by default:

- Broadcast IPv4: 255.255.255.255
- Loopback IPv4 and IPv6: 127.0.0.1 and ::1
- Link Local Multicast IPv4 and IPv6: 224.0.0.0/8 and ff00::/8

All other IP addresses that do not fall into the defined internal or special categories are considered external by default.

To treat an external IP address as **OT Internal**, create a custom network containing the IP address and set its network type as **OT Internal**. This is useful for industrial sites that use public IP addresses in private networks.

Marking a set of IP addresses as **External** triggers the following system actions:

- Excludes associated assets.
- Stores external assets with limited properties and only when they are associated with communications to an internal asset.
- Suppresses component and asset creation and redirects the relationship to external communication data.

Feature history table

Feature	Release Information	Feature Description
Network detection	Release 5.6.0	The Network Definition page has been enhanced to support new network definitions. Network detection runs automatically at regular intervals, with an option for manual, on-demand execution.

Define new network

Guides you through defining new networks and subnetworks by specifying IP ranges, VLANs, network types, and custom properties to enable precise device grouping and monitoring within your network organization.

Facilitate precise management and monitoring of devices by defining networks and subnetworks.

Use this task to add a new network to your network organization. Customize IP ranges, VLANs, network types, and custom properties to improve device grouping and monitoring.

Before you begin

- Ensure you have the required IP addresses and subnets.
- Ensure you have **Network Definition** permission with **read/write** access.
- (optional) Obtain VLAN ID information if applicable.

> **Note**
>
> The VLAN ID is an advanced, optional parameter intended for specific use cases. Only configure a VLAN ID when explicitly required. Specifying a VLAN ID when not necessary may result in unexpected network behavior, such as inaccurate traffic classification or asset grouping errors.

Follow these steps to define new networks.

Procedure

1. From the main menu, choose **Configuration** > **Network Definition**.
2. Click **Define a new network**.
3. Select the **Network Type** (Options include **OT Internal**, **IT Internal**, or **External**).

   The selected network type affects Cyber Vision performance, flow storage, device risk scoring, and device license count.
4. Enter an IP address and its subnet in the **IP address/Prefix** field.
5. Enter the network **Name**.
6. (Optional) Expand **Advanced settings**, and enter the **VLAN ID** to enable overlapping networks.

   > **Note**
   >
   > Only set the VLAN ID if required.

7. (Optional) Expand **Custom properties**.

   Example
   To assign an owner name to a network, enter “Owner” as the key and the owner’s name as the value.

   When you set custom properties at the network level, those properties automatically apply to all associated assets to ensure consistency and reduce repetitive data entry.

   a) Enter a custom **Key**.
   b) Enter the corresponding **Value** for the Key.
   c) Click **Add**.
   d) To add multiple custom properties, repeat the steps and click **Add**.
8. Click **Save**.

You have added a network with the specified IP range, VLAN, network type, and custom properties. This enables accurate grouping and monitoring of assets.

Import networks

Import new networks or update existing network details by uploading a CSV template.

Enable efficient network creation and update in bulk using a standardized CSV template.

This task allows you to add multiple networks or update existing network information by importing a CSV file. Download the template, fill in the necessary network details, and upload the completed file to update your network inventory.

> **Note**
>
> You can export detected networks using the **Export** > **Recommended networks** option, update the required details in the exported CSV file, and then import the file. This approach simplifies bulk updates to multiple subnets.

Follow these steps to import networks using a CSV template.

Procedure

1. From the main menu, choose **Configuration** > **Network Definition**.
2. Click **Import** in the **Network Definition** page.

   The **Import networks** window appears.
3. Click **Download template** to download the CSV file for network import.

   The template file is saved to your local device.
4. Fill in the template with the required network details, VLAN ID, and custom properties, and then save it on your local computer.
5. In the **Import networks** window, upload the completed network template by either: click the upload icon to browse the updated network template or drag and drop the network template to the area to upload.
   - Clicking the upload icon and browsing to your updated CSV file, or
   - Dragging and dropping the template into the upload area.

   The Import completed success message is displayed.
6. (Optional) To import another CSV file of your networks, click **Import another CSV**.
7. Click **Close** to exit the import window.

The imported networks appear in the Network Definition page, and you can review the updated or newly added network entries.

Export network details

Configure options to export network and subnetwork definitions as CSV files for external analysis or record-keeping.

Export the network and subnetworks listed in the Network Definition page as CSV files.

You may need to export network details to facilitate documentation, perform external analysis, or maintain backup records.

Follow these steps to export network details.

Procedure

1. From the main menu, choose **Configuration** > **Network Definition**.
2. Click **Export** and select one of the following options:
   - **Defined networks**
   - **Recommended networks** (includes only detected networks)
   - **All networks** (includes both defined and detected networks)

   The corresponding CSV file is downloaded to your local drive.

The selected network details are exported as CSV files and saved to your local drive for further use.

Assign a network to an organization hierarchy

Configure and associate a network with a specified organization hierarchy level to align management access and policies.

Assign a specific network to a designated level within the organization hierarchy, ensuring policy controls and access are tied to organizational structure.

Use this task to organize network resources, apply hierarchical policies, or update organizational assignments for networks.

Before you begin

Ensure you have Network Definition permission with **read/write** access.

Follow these steps to assign a network to an organization hierarchy.

Procedure

1. From the main menu, choose **Configuration** > **Network Definition**.
2. In the list of available networks, locate and select the network you want to assign.
3. Click **Assign to Organization Hierarchy**.

   The **Assign to Organization Hierarchy** pane opens on the right side of the page.
4. In the right pane, search for and select the desired organization hierarchy level.
5. Click **Assign**.

The selected network is now associated with the specified level in the organization hierarchy.

Add custom properties for networks

Learn how to configure custom properties to manage metadata for assets, improving emergency response and maintenance operations.

Efficient metadata management is achieved by assigning custom properties network-wide to all assets.

Custom properties at the network level automatically propagate to all associated assets, ensuring consistency and reducing repetitive data entry. Properties defined at the network level cannot be edited at the asset level, preserving data integrity. Asset-level custom properties apply only to the individual asset and do not update or override properties defined at the network level.

Before you begin

- Ensure you have **Network Definition** permission with **read/write** access.

Follow these steps to add custom properties to a network.

Procedure

1. From the main menu, choose **Configuration** > **Network Definition**.
2. Select the network to which you want to add custom properties.
3. Click the ellipses icon (...) located at the end of the network row.
4. Click **Add Custom Properties** from the context menu.
5. Enter a custom key and its corresponding value and click **Add**.

   Example
   To add an owner name for a network, set the key to "Owner" and the value to the owner's name.

   To add multiple custom properties, repeat this step for each key-value pair.

6. Click **Save**.

The custom properties are assigned at the network level and automatically propagate to all associated assets, maintaining consistency across your environment.

> **Note**
>
> The custom properties set at the network level cannot be edited at the asset level.

Edit custom properties for networks

Configure custom properties for a network to store additional attributes, such as metadata or classification details.

Update the custom properties for a network to reflect necessary changes and maintain accurate network information.

Custom properties allow you to tag networks with metadata or other relevant information.

> **Note**
>
> Custom properties set at the network level cannot be edited at the asset level.

Before you begin

- Ensure you have **Network Definition** permission with **read/write** access.

Procedure

1. From the main menu, choose **Configuration** > **Network Definition**.
2. Select the network to which you want to edit custom properties to.
3. Click the ellipses icon (...) located at the end of the network row.
4. Click **Edit Custom Properties** from the context menu.
5. Click the edit icon associated with the properties.
6. Update the custom key or its corresponding value as needed.
7. Click **Save**.

The custom properties for the selected network are updated, and the changes are applied to the network configuration.

Edit networks

Configure and update existing network details, or perform bulk edits for multiple networks.

Update network information efficiently, including IP address, name, type, and delete networks as needed.

Use this task to manage and maintain your network definitions as your environment changes. Editing network details allows you to keep your configurations current, ensuring accurate device management.

Follow these steps to edit network details or perform bulk edits.

Procedure

1. From the main menu, choose **Configuration** > **Network Definition**

   The **Network Definition** page displays all current networks and subnetworks.

2. To edit multiple network details, click **Edit networks**.
   a) Update the fields for **IP address**, **Name**, **Type** as needed.

      Use available filters to search for networks based on criteria such as IP address, name, type, or VLAN.

      If you need to undo changes, use the revert icon.

   b) To delete networks, select the relevant check boxes and click the **Remove** button.
      Alternatively, click the trash icon next to the network.

      If you need to undo changes of the selected networks, use the **Revert** button.

   c) Click **Save changes** to apply your edits.
3. To edit an individual network, select the network check box and click **Edit**.
   a) Change the **IP address**, **Name**, **Type** as required.

      Use available filters to search for networks based on criteria such as IP address, Name, and Type.

      If you need to undo changes, use the revert icon.

   b) To delete the network, select its check box and click the **Remove** button.
      Alternatively, click the trash icon next to the network.

      If you need to undo changes of the selected network, use the **Revert** button.

   c) Click **Save changes** to apply your edits.

Manage detected networks

Configure and validate the detected network using manual detection in Cyber Vision Center.

Use this task to run the network detection, and then manage the detect networks by either accepting, updating, or discarding them.

Cyber Vision Center automatically runs network detection at regular intervals. You can also run network detection from the **Network Definition** page and review the detected networks.

Before you begin

Ensure that network traffic data is available in Cyber Vision Center. If required, use the Cyber Vision Classic UI to upload PCAP files containing OT network traffic.

Follow these steps to manually detect, review, and manage your networks

Procedure

1. From the main menu, choose **Configuration** > **Network Definition**.
2. Click **Run detection**.

   Cyber Vision Center starts the network detection process and displays a success message when the process is complete.

3. Click **Verify detected networks**.

The **Verify detected networks** window opens with a list of detected networks.

4. Review the detected networks and perform any of the following actions, as required:
   - Accept the detected networks on page 36
   - Update the detected networks on page 36
   - Discard the detected network on page 37
5. Click **Save changes**.

Accept the detected networks

Configure and verify detected networks, then accept selected networks for monitoring and management.

Use this task after running the network detection process in Cyber Vision Center to review and accept discovered networks for system integration.

Follow these steps to accept the detected networks.

Procedure

1. From the main menu, choose **Configuration** > **Network Definition**.
2. Click **Run detection**.

   Cyber Vision Center starts the network detection process and displays a success message when the process is complete.
3. Click **Verify detected networks**.

   The **Verify detected networks** window opens with a list of detected networks.
4. Accept the applicable detected networks.

   To accept individual networks:

   a) Locate the networks using available search criteria (for example, IP address, name, or type).
   b) Click the check mark icon for that network to accept the network.

      To undo the action, click the revert icon available for that network.

   Or,

   To accept multiple networks,

   a) Locate the network using available search criteria (for example, IP address, name, or type).
   b) Select the check box for each network to be accepted.
   c) Click the **Accept** button.

      To undo the action, click the **Revert** button.
5. Click **Save changes**.

Update the detected networks

Configure and update the details of detected networks before accepting them.

When networks are detected by Cyber Vision Center, you have the opportunity to review, modify, and accept the network details. This process allows you to correct any inaccuracies before accepting the networks.

> **Note**
>
> You can export detected networks using the **Export** > **Recommended networks** option, update the required details in the exported CSV file, and then import the file. This approach simplifies bulk updates to multiple subnets.

Follow these steps to review and update detected networks.

Procedure

1. From the main menu, choose **Configuration** > **Network Definition**.
2. Click **Run detection**.

   Cyber Vision Center starts the network detection process and displays a success message when the process is complete.
3. Click **Verify detected networks**.

   The **Verify detected networks** window opens with a list of detected networks.
4. Update the detected networks as required.

   To update a single network:

   a) Locate the networks using available search criteria (for example, IP address, name, or type).
   b) Update the **IP address**, **Name**, or **Type** fields as needed.

      To undo the changes, click the revert icon available for that network.

   c) Click the check mark to accept the updated network.

   Or,

   To update multiple networks,

   a) Locate the network using available search criteria (for example, IP address, name, or type).
   b) Select the check box for each network to be updated.
   c) Update the **IP address**, **Name**, or **Type** fields as needed.

      To undo the changes, click the **Revert** button.

   d) Click the **Accept** button.
5. Click **Save changes**.

Discard the detected network

Configure Cyber Vision Center to remove unwanted detected networks by selecting and discarding them from the list.

At times, network detection discovers networks that are not relevant for your environment. Discarding such networks helps ensure the inventory reflects only valid, required networks.

Follow these steps to discard detected networks:

Procedure

1. From the main menu, choose **Configuration** > **Network Definition**.
2. Click **Run detection**.

   Cyber Vision Center starts the network detection process and displays a success message when the process is complete.

3. Click **Verify detected networks**.

   The **Verify detected networks** window opens with a list of detected networks.

4. Discard the detected network that are not relevant.

   To discard individual networks:

   a) Locate the networks using available search criteria (e.g., IP address, name, or type).
   b) Click the trash icon for that network.

      To undo the action, click the revert icon available for that network.

   Or,

   To discard multiple networks,

   a) Locate the network using available search criteria (e.g., IP address, name, or type).
   b) Select the check box for each network to be discarded.
   c) Click the **Discard** button.

      To undo the action, click the **Revert** button.

5. Click **Save changes**.

   Note

   The discarded network suggestions can be restored by clicking the **Review discarded networks** button on the **Network Definition** page. This button appears only when at least one network suggestion has been discarded.

Organization hierarchies

Outlines the structure and management of organization hierarchies in Cisco Cyber Vision Center, including grouping assets and sensors, configuring hierarchical levels, nesting constraints, and administering levels for effective organization and access control.

Organization hierarchies are structural models that

- group assets, sensors, and data sources within Cisco Cyber Vision Center,
- arrange those entities in a hierarchical tree of levels (nodes), and
- enable granular organization, management, and access control across multiple subdivisions.

Hierarchy management

- Each node in the hierarchy is a level.
- The system defines the Global level and places it at the top of the hierarchy. You cannot delete this level.
- You can add, edit, or delete levels. However, if a level contains child levels or assigned entities such as sensors or PCAPs, the system prevents deletion.
- The system supports nesting up to five sub-levels; after this limit, no additional levels can be added.
- You can add, edit, or delete levels in the hierarchy through **Configuration** > **Organization Hierarchy**.

Assign multiple PCAP files to an organization hierarchy

Guides you through assigning multiple PCAP files to an organization hierarchy to organize assets and automate asset creation in Cisco Cyber Vision.

Before you begin

- Confirm you have appropriate permissions to assign PCAP files.
- Ensure the required PCAP files have already been uploaded.

Assign multiple packet capture (PCAP) files to an organization hierarchy to enable automated asset creation in Cisco Cyber Vision.

Use this task to organize and manage multiple PCAP files for asset management within an organization hierarchy.

Follow these steps to assign multiple PCAP files to the organization hierarchy:

Procedure

1. From the main menu, choose **Configuration** > **PCAPs**.
2. Select the PCAP files you want to assign to an organization hierarchy.
3. Click **Assign Selected to Organization Hierarchy**.
4. Choose the appropriate organization hierarchy.
5. Click **Assign**.

The selected PCAP files are assigned to the chosen organization hierarchy, automatically initiating asset creation in Cisco Cyber Vision.

Each PCAP initiates asset creation in Cisco Cyber Vision.

Filter PLCs by organization hierarchy

Guides you through organizing and reviewing PLC assets by applying filters based on organization hierarchy, including necessary prerequisites and step-by-step instructions for viewing PLCs at different organizational levels.

Organize and review your PLC assets based on the organization hierarchy.

Before you begin

- Create your organization hierarchy.
- Assign sensors, networks, and PCAP to your organization hierarchy.

Procedure

1. From the main menu, choose **Organization**.
2. Select **Sensors** or **Networks**.
3. Select the organization level.
4. Click **Edit** on the active view bar.
5. Apply the **Asset types** filter for PLCs.
6. Click **Apply**.

The list displays PLCs organized by the selected organization hierarchy level.

Assets

Outlines the definition, categorization, and management of assets in Cisco Cyber Vision, including modular asset structures, feature enhancements such as summary views and custom properties, asset search capabilities, CSV export improvements, and details on interface identification and visualization.

An asset is a network entity that

- serves as a core physical component within an industrial network, such as a programmable logic controller (PLC), a switch, a controller, or a server,
- may represent one or more modules with distinct identifiers, which may include serial number, reference, or type, even when MAC and IP addresses overlap; and
- is defined, categorized, and managed according to established rules in Cisco Cyber Vision to ensure effective asset inventory and operations.

Modular assets: If an asset is modular, such as a chassis with multiple modules, its summary shows details including slot, model name, type, firmware version, and serial number. Each module, such as a CPU, communication module, or I/O module, appears as a separate block in the chassis view.

Table 11: Feature History Table

Feature	Release Information	Feature Description
Assets page enhancement	Release 5.6.x	The **Assets** page includes the following tabs for each asset: **Summary**, **Alerts**, **Vulnerabilities**, **Communications**, **Behaviors**, **Services**, **Properties**, and **Interfaces** The cards on the **Summary** page provide high-level information about an asset before you open a related details tab.
Custom properties	Release 5.5.x	Add custom properties to Cisco Cyber Vision assets. You can view, add, and edit these properties, with strict validation rules enforced to maintain data integrity.

Feature	Release Information	Feature Description
Search bar	Release 5.3.x	New UI contains a search bar in the global top banner. You can search for an asset by name, IP address, or MAC address.
Asset list CSV enhancements	Release 5.3.x	The CSV that you download from Cyber Vision Center includes a column that lists the sensors that have detected assets.

Asset data management

Outlines the main functions for managing asset data on the Assets page, including filtering, searching, deleting, exporting, customizing table views, and sorting or adjusting columns to organize and review asset information effectively.

The table presents the main functions available for managing asset data in the **Assets** page. It describes the specific capabilities and behavior of each function.

Function	Description
Use widgets to filter assets table	The widgets at the top of the Assets page allow you to filter data in the asset table. You can select any of these widgets to display the corresponding data: • Active Alerts • Vulnerabilities • Discovered in last 7 days • Discovered in last 30 days
Delete assets	By default, the system deletes assets removed from the production line after 30 days. You can manually delete assets detected due to misconfiguration. If sensors detect the assets again, the system may re-add them to the inventory.
Search for assets	Enter at least three characters from an asset's name, IP address, or MAC address in the search bar to quickly locate details.
Export	Export all asset data to a CSV file. The export includes asset IDs so you can distinguish assets with the same name.

Function	Description
Manage asset table view	On the **Assets** page, you can switch among the predefined table views: • **Security** (default view) • **Network** • **Inventory** The system saves your most recently selected view and restores it when you reopen the **Assets** page in a new session. Several new columns have been added to the asset table view to display additional asset properties, such as Asset Group, OS, Firmware, Model, Behaviors, and Services. Use the table **Settings** menu to show or hide columns as needed.

Asset summary

Explains how asset summaries bring security information together so you can identify areas for further investigation.

An asset summary provides a quick view of the security information available for the asset.

The **Summary** tab includes asset metadata, and the available summary cards provide high-level information about an asset before you open a related details tab. The Summary tab includes these cards:

- **Alerts**
- **Vulnerabilities**
- **Behaviors**
- **Services**
- **Communications**
- **Rack Slot**

Information in asset summary cards

This table depicts the available cards on the **Summary** page. The cards and values that appear depend on the asset data and the features available in your deployment.

Table 12: Information in asset summary cards

Card	Information shown
Alerts	The card shows the number of active alerts. The card's visual indicator reflects the highest criticality among those alerts.
Vulnerabilities	Vulnerability information such as the total count and indicators for confirmed vulnerabilities, known exploits, a network attack vector, or the highest Common Vulnerability Scoring System (CVSS) value.

Card	Information shown
Behaviors	The card shows the number of unique behaviors observed for the asset, along with tags for the most recently observed behaviors.
Services	The service count shown for the asset.
Communications	The card shows the number of internal and external peers that communicate with the asset, when available.
Rack Slot	Available only for modular PLCs (Programmable Logic Controllers) assets. The card provides a quick inventory view of the PLC's installed modules details such as the model name, slot type, firmware version, and serial number.

View asset summary

View an asset's Summary tab to quickly assess asset metadata and high-level status cards.

Use the **Summary** tab of an asset to view essential metadata and summary cards, such as alerts, vulnerabilities, behaviors, Services, and communications. This allows you to identify the asset's status and select summary cards for more detailed analysis.

Follow these steps to view the asset's Summary page.

Procedure

1. From the main menu, select **Assets**.

   The **Assets** page lists all available assets.

2. Select an asset to open its details.

   The **Summary** tab opens by default.

3. Review the asset metadata and summary cards to assess its overall status.
4. Select a summary card, such as **Alerts**, **Vulnerabilities**, **Behaviors**, **Services**, or **Communications** to view related details.

View asset alerts

Provides instructions for reviewing alert counts, filtering and sorting the alert table, and opening related alert details for an asset.

Assets may generate multiple types of alerts. Reviewing and organizing these alerts helps users identify current issues and prioritize investigation.

The **Alerts** card depicts the total count of active alerts on the asset. The card also provide count of each alert category and the last alert detected data.

Use the asset's **Alerts** tab to review all alerts associated with an asset without opening alert instances individually.

Follow these steps to view alerts for an asset.

Procedure

1. From the main menu, select **Assets**.
2. Select an asset to open its details page.

   The **Summary** tab displays asset metadata and summary cards. The **Alert** card shows the total number of active alerts and the alert counts by category.

3. On the **Alerts** card, select an alert category, such as Communication, Intrusion Detection, Property, or Vulnerability.

   The **Alerts** tab opens and displays alerts associated with the selected asset.

   > **Note**
   >
   > In the alert table, the **Alert Type** column identifies the type of alert. The **Context** column identifies the related entity for the alert. Refer the context-related values in Alert triggers and instances in assets on page 44.

4. On the **Alerts** tab, perform any of the following actions:
   a) Review alert count widgets by **Category** or **Severity**. Category is selected by default.
      - **Category** - Communication, Intrusion Detection, Property, and Vulnerability
      - **Severity** - Critical, High, Medium, and Low

   b) Select a widget to filter the alert table by that category or severity.
   c) Sort the alert table by selecting a column header: **Alert Category**, **Alert Type**, **Severity**, or **Last detected**.
   d) Click **Details** for an alert to view additional information about that alert instance.

      The **Alerts** page opens with the alert details. If the asset is an alert instance, the page is filtered by the asset name. If the asset triggered the alert, the page displays additional information about the alert instance. For additional details, refer to Alert triggers and instances in assets on page 44.

Alert triggers and instances in assets

Explains how alert triggers and instances relate to a selected asset and why the destination that opens for an alert can vary by alert type.

An alert trigger is the condition that causes an alert. An alert instance represents an affected entity; depending on the alert type, it is usually an asset but can be another entity.

An alert can have one trigger and multiple instances. Grouping related instances under a trigger reduces the number of alert entries that you need to review.

- Depending on the alert type, the selected asset can be an alert instance or the alert trigger.
- On the **Alerts** tab of an asset, the **Context** column identifies the other entity: the trigger when the selected asset is an instance, or the instance when the selected asset is the trigger.
- The **Details** button on the **Alerts** page opens the related alert instance page. When the selected asset is an instance, the page can open with the asset filter applied; when it is the trigger, the page can open without an asset filter.

Note

The **Details** button is available only when you have the appropriate permission.

Table 13: Alert instance page destination by alert type

Alert type	Context value	Alert instance page destination
Severe vulnerabilities in monitored entities	CVE ID and CVE title	Opens the alert instance page filtered by the asset.
Prohibited vendors	Vendor name	Opens the alert instance page filtered by the asset.
Assets with unexpected external communications	Number of remote domains or addresses	Opens the alert instance page without an asset filter.
Inactive assets	Alert rule name	Opens the alert instance page filtered by the asset.
Intrusion detection	Snort rule ID and Snort rule	Opens the alert instance page filtered by the source asset.
Network Scanner	Number of scan events	Opens the alert instance page without an asset filter.
Assets with unexpected behavior	Asset name	Opens the alert instance page.

View asset vulnerabilities

View the vulnerability list for a selected asset and apply filters based on CVSS score to focus your review on priority findings.

Review vulnerabilities associated with a chosen asset in Cisco Cyber Vision to help prioritize remediation efforts.

Cisco Cyber Vision uses an internal knowledge database to match asset properties with recognized vulnerabilities, icons, and threats. For additional details on vulnerabilities, refer to the Vulnerabilities on page 75 section.

Before you begin

Ensure you have access to the Assets and Vulnerabilities dashboards in Cyber Vision Center. You may need to check your permissions under **Configuration** > **Users** > **Role Management**.

Follow these steps to view asset vulnerabilities details.

Procedure

1. From the main menu, select **Assets**.

   The **Assets** page lists all available assets.

2. Select the asset that you want to review.

The **Summary** tab opens and displays asset details and summary cards. The **Vulnerabilities** card shows confirmed and potential vulnerability counts, the highest CVSS score, network attack vector count, and known-exploit count.

3. Click the **Vulnerabilities** card.

   The **Vulnerabilities** tab opens and displays the vulnerabilities identified for the selected asset.

4. On the **Vulnerabilities** tab, perform any of the following actions as needed:
   a) Select **Cisco Security Risk Score** or **CVSS Score**, and then select a widget to apply its associated score filter to the vulnerability table.
   b) Sort the table by columns such as Alert, Vulnerability ID, Name, Risk Score, or Status.
   c) Optionally, enable **Show Acknowledged** to include acknowledged vulnerabilities.
   d) If required, **Acknowledge** or **Unacknowledge** vulnerabilities. For detailed steps, refer to the following topics:

      Acknowledge or unacknowledge vulnerabilities for a single asset on page 78

      Acknowledge or unacknowledge multiple assets for a single vulnerability on page 79

   e) Click **Export** to download the vulnerability list as a CSV file.

The vulnerability list for the selected asset is displayed. Applied filters help you identify and prioritize critical vulnerabilities.

View asset communications

Provides instructions for opening an asset communications map and using its filters and grouping options to investigate the traffic observed for the asset.

Use the **Communication** card to investigate communication patterns for a selected asset.

Use the Communications tab to examine internal and external interactions of the asset, and review communication details for monitoring or auditing purposes. For additional information on **Communication** tab, refer to Communication maps on page 80.

Follow these steps to view asset communications.

Procedure

---

1. From the main menu, select **Assets**.

   The **Assets** page lists all assets.

2. Select the asset you want to view.

   The **Summary** tab opens and displays asset metadata and summary cards. The **Communications** card shows the number of internal assets, network interfaces, external resources, ASN organization information for external communications, and last unicast days.

   > **Note**
   >
   > Investigate any external communication count greater than zero.

3. Click the **Communications** card to open the **Communication** tab.
4. On the **Communications** tab, perform the following actions as needed.
   a) Use the **Map** or **List** view to review internal and external communication patterns.

b) Apply filters, such as time, protocol, communication type, or focus filters (Asset, Network, or Country), to narrow the results.
c) Use search to find and investigate specific remote assets.
d) If external communications exist, use the **ASN Info** toggle in the **Map** view to review details about the external traffic.

The communications map displays the selected asset's network interactions based on the filters you apply.

Asset communication map features

This section lists the features of the asset communication map and their descriptions, including details about icon indicators.

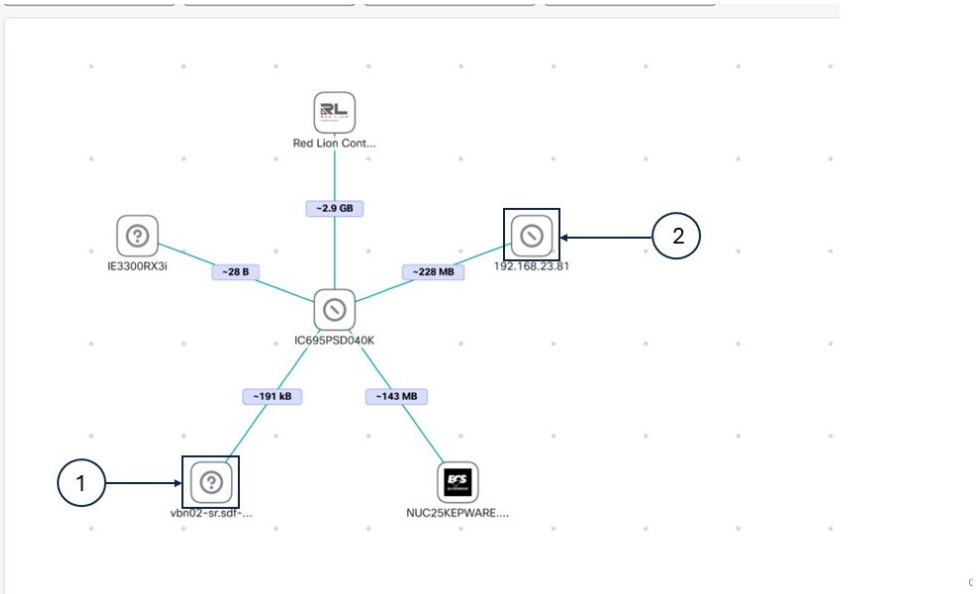
The asset communication map shows all communications between a selected asset and other individual assets in your environment. It provides a detailed view of communication patterns, offers several useful filters, and supports multiple identification methods to help you analyze network communications easily.

Table 14: Features of the asset communication map

Feature	Description
Search	Lets you search for assets within the current map and view their communication details.
Time filter	• Lets you focus on communications for specific time periods to analyze trends or activity. • The **Last 7 days** filter is enabled by default.
Group communications	• Lets you group assets by **Asset** , **Network**, or **Country** to organize the map. • Group nodes show communications between assets from the same group. Individual links show details of communication between groups: observed protocols, data exchange volumes, and information about the asset source or destination. • If an asset communicates with another asset you did not include in the active view filter, the map displays the node and links for that asset as a dotted line. • Non-communicating groups appear in grid view on the map.
Communication type	Filters the map by external or internal communications. When parent and sub-domains exist in external communications, click the parent domain node in **Map** view to display communications between sub-domains. Breadcrumbs show your current location.
Protocol filter	• Lists all protocols used between assets. • All protocols appear by default, but **Traffic-Heavy Protocols** are deselected to improve clarity.

Feature	Description
Assets identification	For each asset, the map shows the vendor icon and name. If this information is unavailable, you see the asset's IP address or MAC address.

Figure 1: Icon descriptions



Icon	Description
(1)	This icon indicates that vendor information for the asset is unavailable.
(2)	This icon indicates that the vendor is known, but its icon is unavailable.

View behaviors for an asset

Configure and review the asset behavior timeline on Cisco Cyber Vision.

Use the **Behaviors** card to analyze the distinct behaviors associated with an asset for security and operational insights.

The **Behaviors** card shows a count of distinct observed behaviors and the most recently observed behavior, such as Program Upload, Start CPU, Stop CPU, Read Var, Write Var, Restart CPU, or Network Configuration.

The **Behaviors** tab provides a view of all behaviors observed for the asset. The Behaviors Timeline displays data with daily granularity, showing date-grouped entries with the behavior name, category, description, first or last seen, and related asset when applicable. Each behavior is color coded based on its importance.

Follow these steps to view asset behaviors.

Procedure

1. From the main menu, select **Assets**.

   The **Assets** page displays a list of all assets.

2. Select the asset that you want to review.

   The asset **Summary** tab opens. The **Behavior** card shows the most recently observed behavior and when it occurred.

3. Click the **Behavior** card.

   The **Behaviors** tab opens and displays the asset's observed behaviors, grouped by date, along with a timeline.

   The **Behaviors** tab opens, displaying the list of behaviours observed for the asset grouped by date, and timeline of those behaviors.

   > **Note**
   >
   > If you select a behavior badge on the card, the timeline is filtered to show only that behavior.

4. On the **Behaviors** tab, use the available options as needed:
   a) Review timeline entries, including the behavior name, category, description, first- or last-seen time, and related asset, when applicable.
   b) Select a related asset link to open that asset's **Summary** page.
   c) Use the **Search** field to find a specific behavior.
   d) Select **Daily**, **Weekly** , or **Monthly** to change the timeline granularity.

   > **Note**
   >
   > - Daily data is retained for 31 days.
   > - Weekly data shows up to 31 days in 7-day windows.
   > - Monthly records are retained for 13 months.

   e) Filter behaviors by **Directions**.
   f) Select a behavior from the drop-down list to view its details.

      Behavior entries are color-coded to indicate their importance.

View asset services

Configure Cyber Vision to view the services detected for a selected asset using the Services tab.

In Cisco Cyber Vision, a Service refers to an active program, network infrastructure, or specialized industrial application detected on a monitored asset. Cyber Vision uses Deep Packet Inspection (DPI) to identify and display detailed information about services on each asset.

On the asset's **Summary** page, the **Services** card provides the total count of services. The most recently detected services are listed as badges on the card, such as Windows, HTTP Server, DNS Server, SSH, and engineering software like Ignition or FactoryTalk.

Use the **Services** tab to review the services displayed for a selected asset.

Follow these steps to view asset services.

Procedure

1. From the main menu, select **Assets**.

   The **Assets** page lists all available assets.

2. Select the asset you want to review.

   The **Summary** tab opens. The **Service** card shows the number of detected services and may display recently detected services, such as Windows, HTTP Server, DNS Server, SSH, Ignition, or FactoryTalk.

3. Click the **Service** card.

   The **Service** tab opens and lists the detected generic and port-based services, including when each service was first and last observed.

4. On the **Services** tab, use the available controls as needed:
   a) Use **Search** to find a specific service.
   b) Use the **Protocol** drop-down list to filter services by protocol.
   c) Use the **Service** drop-down list to select services and view their details.

You can now review the services detected for the selected asset.

View asset properties

Provides instructions to verify asset identity and review network-collected properties by protocol.

Use the **Properties** tab to review properties collected from the network for a selected asset. Reviewing asset properties ensures accurate asset identification and helps validate the information collected from the network.

Cisco Cyber Vision organizes the asset properties by protocol in the **Properties** tab.

Follow these steps to view asset properties.

Procedure

1. From the main menu, select **Assets**.

   The **Assets** page lists all available assets.

2. Select the asset you want to review.

   The **Summary** tab opens and displays asset metadata and summary information.

3. Click the **Properties** tab.
4. Review the property groups and the properties listed for each protocol.

View asset interfaces

Provides instructions for reviewing the interface values that Cisco Cyber Vision uses to identify the asset.

Use the **Interfaces** tab to review the interfaces that Cisco Cyber Vision identifies for a selected asset.

Assets use different network interfaces to communicate within the network. Interfaces may include MAC addresses, IP addresses, VLAN IDs, or combinations of these. The system collects interface properties from network traffic. It selects one interface as the primary interface for visualizations.

The **Interfaces** tab shows all interfaces for the asset, including the primary and additional interfaces. If multiple interfaces are available, you can change which interface is designated as the primary interface.

Follow these steps to view asset interfaces.

Procedure

1. From the main menu, select **Assets**.

   The **Assets** page lists all available assets.

2. Select the asset you want to review.

   The **Summary** tab opens and shows the asset metadata in the left pane.

3. In the left pane, review the **Primary Interface** details.
4. To view every interface detected for the asset, select the **View all < > interfaces** link under **Primary Interface** .

   The **Interface** tab opens and lists the primary and additional interfaces.

5. To designate a different primary interface, locate the **Primary Interface** column and select the interface you want to use.

Add custom properties to an asset

Configure custom properties to enrich metadata for individual assets, enabling improved emergency and maintenance communications.

Custom properties feature allows you to add any custom property without content limitation on assets apart from current asset information.

Add custom properties such as:

- owner name,
- email, or
- contact number

to individual assets for enhanced metadata management and operational efficiency.

Asset-level custom properties allow you to include information that is not inherited from the network, giving you granular control over asset metadata.

You cannot edit custom properties that you set for a network from the assets. Setting the custom property value at the network level overrides the value set at the asset level.

Before you begin

- Ensure you have the **Assets** permission with read/write access.

Procedure

1. From the main menu, click **Assets**.
2. Click the asset that you want to add custom properites to.
3. On **Custom Properties**, click **Add/Edit**.
4. Enter a custom key and its corresponding value.

Example
To add an owner name for an asset, set the key to "Owner" and the value to the owner's name.

To add multiple custom properties, repeat this step for each key-value pair.

5. Click **Save**.

External communications in the New UI

This section provides the criteria used to classify network communication as external in the New UI.

The system classifies and displays external communications in the New UI using specific criteria.

Criteria for classifying external communications

External communication appears in the New UI when:

- The communication is to or from networks that are explicitly marked as **External** in the New UI.
- If no external networks are defined (in the New UI under **Configuration** > **Network Definition**), any communication not assigned to an **IT Internal** or **OT Internal** network counts as external communication.

View external communications for an asset

Verify and review all external communications associated with a specific asset.

Enable you to identify and analyze all external connections for a chosen asset.

Use this task to determine which external resources a specific asset interacts with, and to analyze communication details for monitoring or auditing.

Procedure

1. From the main menu, select **Assets**.
2. Click your asset that has external communications.
3. Open the **Communications** tab for the selected asset..
4. In the **All Communications** filter, select **External** to display only external communications in either map or list view.

All external communications associated with the selected asset are displayed, including details about each connection.

Filters and map indicators for monitoring external communications

Lists the available filters and visual indicators used to monitor external communication, helping you identify network exposure and interpret the map display.

Visualization and monitoring

When you visualize external communications, you can identify unexpected network paths that might expose your organization to external threats. Available filters for external connections include:

- **Country**: Displays the country identified for the IP.
- **ASN**: Displays unique ID assigned to a network or a group of networks managed by a single organization.
- **ASN Organization**: Displays the origin organization that initiated the external communication.

Note

- Country, ASN, and ASN Organization details are available only if your local center is enrolled in Cyber Vision Site Manager (CVSM) and an active cloud connection with Cisco exists.
- In asset communications:
  - **List view**: The ASN and ASN Organization columns are disabled by default.
  - **Map view**: If external communications are available, the **ASN Info** field appears. It shows details for external communications (disabled by default).

Table 15: External communication indicators in map view

Visual indicators	Description
Single circle outside the node	Indicates one remote address communicating with your asset.
Multiple circles outside the node	Indicates that multiple remote addresses communicate with your asset.
Globe icon on the node	Indicates that IP to country mapping is unavailable or multiple countries are involved.
Node displays country's flag	Indicates that a single country has been identified.
Question mark icon in the node	Indicates an IP address without country mapping. The country column in list view shows **Unknown**. Some IPs cannot be resolved to a country based on available data feeds.

Filters

Introduces filters in Cyber Vision, explaining how they narrow displayed information, enable users to focus on specific assets, network segments, or alerts, and describes filter options by organization hierarchy, sensor, network, and other criteria across non-configuration pages.

A filter is a New UI feature that

- narrows the information displayed on core Cyber Vision pages,
- allows users to focus on specific assets, network segments, or alerts, and
- leaves configuration actions unaffected.

Table 16: Feature History Table

Feature	Release Information	Feature Description
Filter Cyber Vision Center data by organization hierarchy	Release 5.3.x	All the data views in New UI can be filtered by organization hierarchy, sensors, or networks associated with an asset. At the top of the left menu, in the **Organization** filter, choose the hierarchy level you want to focus on. **Global** is the default choice and covers all assets.
Filter data in Cyber Vision Center by active view filter	Release 5.3.x	A product-level banner in the New UI allows you to filter data on every page except configuration pages. If you have not applied any filters, **No filter applied** is displayed. Click **Edit** to apply one or more filters from functional group, network or sensor, asset type, and vendor categories.

Filter views in Cyber Vision New UI

Refines the information displayed in Cyber Vision by applying filters to the Dashboard, Alerts, Assets, Vulnerabilities, and Communications pages. This action helps focus on specific assets, network segments, or alerts.

Narrow the information displayed in Cyber Vision New UI by applying filters to the Dashboard, Alerts, Assets, Vulnerabilities, and Communications pages.

Use filters to focus on specific assets, network segments, or alerts in Cyber Vision. This action does not affect Configuration pages.

Procedure

1. From the main menu, choose **Organization** .
2. Select either **Sensors** or **Networks** .

> **Note**
>
> The **Sensors** tab is selected by default.

- To select all sensors or networks at a hierarchy level, select that level.
- To choose specific sensors or networks from a selected hierarchy level: open the organization drawer again, open **Sensor selection** or **Network selection** , select items, then click **Apply** .

> **Note**
>
> To select assets not linked to sensors or networks, choose **Unknown** .

- Use the search box to find sensors or networks by name.

3. To clear your selected sensors or networks and return to the complete organization hierarchy, open the **Organization Hierarchy** drawer again and click the **Reset selection** icon.
4. To edit the sensor or network selection for the selected organization hierarchy only, open the **Organization Hierarchy** drawer again and click the **Edit selection** icon.
5. To refine your filter, click **Edit** on the active view bar.
6. Use the **Select** buttons to add filters as needed.
7. Click **Apply** to update or **Reset** to clear the filters.

The views show only data that matches your filter criteria.

What to do next

Review the filtered data on Dashboard, Alerts, Assets, Vulnerabilities, or Communications pages.

4 Configure visibility

Topics:

Guides the configuration of visibility features, including managing alert rules and types, enabling syslog notifications, organizing asset clusters, addressing vulnerabilities, mapping communications, and activating IDS on sensors to optimize security monitoring and incident response across the network.

Alerts

Explains how alerts notify users about significant activity or irregularities in an industrial network, categorize data, and provide warnings to aid security monitoring.

Alerts are system-generated notifications that

- indicate significant activity or irregularities detected within an industrial network,
- categorize information based on type, associated data, and network components, and
- provide warnings to help with security monitoring and response.

An alert is a notification that triggers when a user-defined rule's condition is met. Cyber Vision sends alerts through Syslog when they are raised, cleared, or their status changes. For details about this configuration, see Enable or disable syslog notifications for an alert type.

Table 17: Feature History Table

Feature	Release Information	Feature Description
Pause and resume individual alert rules	Release 5.6.x	You can pause or resume individual alert rules. Pausing a rule does not affect other rules associated with the same alert type. Alert type-level pause and resume are no longer available.
MITRE ATT and CK information for Intrusion Detection alerts	Release 5.6.x	Intrusion Detection alerts display the MITRE ATT and CK tactics and techniques associated with the Snort rule that generated the alert.
Assets with unexpected behaviors alert type	Release 5.6.x	Cisco Cyber Vision monitors the assets that are part of the alert rules, and raises an alert when any of those assets are involved in selected behaviors within the configured time window.
Alert rule configuration changes	Release 5.6.x	You can no longer configure alert rules for functional groups. When you upgrade to Release 5.6.x, Cyber Vision automatically deletes existing alert rules configured for functional groups.
Network Scanner alert type	Release 5.6.x	The Network Scanner alert type identifies network reconnaissance and scanning attempts. IP addresses specified in the Allowed Scanner list are excluded and do not generate alerts.
Inactive assets alert type	Release 5.5.x	Inactive assets alert type detects assets that stop communicating due to failure or misconfiguration. Define custom rules for the inactivity period to reduce manual monitoring.

Feature	Release Information	Feature Description
Intrusion detection alert type	Release 5.5.x	Intrusion detection alert type monitors network traffic using the Snort intrusion detection system. It raises an alert when suspicious or malicious network activity is detected on monitored assets, based on Snort rules.
Assets with unexpected external communications alert type	Release 5.5.x	Assets with unexpected external communications alert type monitors asset communications. It raises an alert if an asset communicates to external IP addresses or domains.
Network-based organization hierarchy alert configuration	Release 5.4.x	You can configure alerts at the organization hierarchy level with one additional entity type: **Organization Hierarchy (Networks)**. The system changes all existing alert rules with the entity type **Organization Hierarchy** to **Organization Hierarchy (Sensors)** automatically.
Mute or unmute alert instances for prohibited vendor alert type	Release 5.4.x	You can use the mute and unmute feature to control prohibited vendor alerts. Mark alert instances as reviewed and not urgent so they remain in the system but are not active. Select the duration to mute an alert instance; after that period, the alert becomes active again.
Active and cleared alerts	Release 5.3.x	The Alerts page displays two types of alerts: • Active • Cleared
Pause alert creations	Release 5.3.x	You can pause an alert type in the **Configure** > **Alerts**
Change vulnerability scoring system for alerts	Release 5.3.x	The Cisco Security Risk Score is the default scoring system applied to alert configurations. However, you can choose to update an alert configuration to apply the CVSS scoring system instead.
Alert for severe vulnerabilities in monitored entities	Release 5.3.x	Create and edit rules for the **Severe vulnerabilities in monitored entities** alert based on the Cisco Security Risk Score or the CVSS score.

Feature	Release Information	Feature Description
Alert for prohibited vendors	Release 5.3.x	The **Configure** > **Alerts** page contains a default alert for prohibited vendors. The alert rule is based on an editable list of prohibited vendors.

Alert types

Lists the main alert types monitored by Cyber Vision and provides descriptions and associated rule information for each.

Cyber Vision provides alert types that monitor security conditions and activity across your assets and network. Each alert type contains rules that define what Cyber Vision monitors and when it generates alerts. To view and configure alert types and rules, choose **Configuration** > **Alerts**.

Alert type	Description
Severe vulnerabilities in monitored entities	• Cyber Vision Center raises alerts when it detects high-severity vulnerabilities in your assets. • The default rule for this alert type is **Default_OH_Global**. • To clear alerts for this alert type, acknowledge the vulnerabilities on the affected assets. To restore the alerts, unacknowledge the vulnerabilities. For more information, see Acknowledge or unacknowledge vulnerabilities for a single asset and Acknowledge or unacknowledge multiple assets for a single vulnerability.
Prohibited vendors	• Cyber Vision triggers alerts when your assets are linked to prohibited vendors. • The default rule for this alert type is **Prohibited_list**.
Inactive assets	• Cyber Vision automatically detects assets that have stopped communicating due to failure or misconfiguration. It then alerts you about the issue. • Define rules to set the inactivity threshold for triggering alerts, reducing manual monitoring.
Intrusion Detection	• This alert type monitors network traffic using the Snort intrusion detection system. Enable Intrusion Detection System (IDS) on a compatible sensor to activate Snort-based intrusion detection. See Enable IDS on a sensor. • The default rule for this alert type is **Default_Snort_Global**. • Detects suspicious network activity identified by Snort rules. When mapping information is available, the alert displays the associated MITRE ATT and CK tactics and techniques.

Alert type	Description
Assets with unexpected external communications	• This alert type raises an alert if assets communicate with external IP addresses. • The default rule for this alert type is **Default_Monitored_Asset_Types**, which monitors external communications for all assets with type PLC, IED, or IO.

Network Scanner	• Cisco Cyber Vision triggers alert when it detects network reconnaissance and scanning activity such as:
	  • Vertical scan - One source IP scans multiple ports on a single target host.
	  • Horizontal scan - One source IP scans a single port across multiple hosts.
	  • Combined scan - Combination of vertical and horizontal scanning, where multiple ports on multiple hosts are scanned.
	  • Industrial scan - Scan targets industrial protocol traffic and anomaly detection specific to operational technology (OT) environments.
	  • Burst scan - Large number of scan attempts in a very short period.
	  • Targeted scan - Focused reconnaissance against specific high-value assets.
	• The default rule for this alert type is **Default_Scan_Global**.

Assets with unexpected behaviors	Cisco Cyber Vision triggers an alert when an asset that is part of the alert rule is involved in one of the selected behaviors, in the configured role, within the configured time window.

Alert states and key attributes

Lists the states, alert types, rules, and key attributes used for alerts in the Cyber Vision center. This reference also provides information to help users understand alert progression and categorization.

Cyber Vision manages alerts by tracking their progression through defined states. Alerts are organized by type, and rules specify when and how alerts are triggered.

How Cyber Vision organizes alerts

Cyber Vision organizes alerts by alert type, rule, trigger, instance, and occurrence. An alert rule defines the monitored condition. A trigger identifies the condition that generated the alert. An instance identifies an affected entity or activity. An occurrence records each time Cyber Vision detects that condition for the instance.

Alert states

You can monitor alerts as they move through distinct states:

- **Active**: Displays current unresolved alerts. Alerts stay active while the underlying problem exists.
- **Muted**: When you mute alert instances related to the **Prohibited vendors**, **Inactive assets**, **Intrusion Detection**, **Assets with unexpected behaviors**, and **Assets with unexpected external communications** alert types, those alerts appear in the **Muted** tab.
- **Cleared**: After you resolve alerts, they appear in the **Cleared** tab. Cyber Vision keeps cleared alerts for a set number of days before removing them. The retention period is different for each type of alert. You can manually clear alert instances only for the **Inactive assets**, **Network Scanner**, **Assets with unexpected behaviors**, and **Assets with unexpected external communications** alert types.

Alert details

To view the alert details, from the main menu choose **Alerts**.

Name	Description
Alert Type	Specifies the category of alert generated by the system. Each type shows the nature of the underlying issue detected.
Trigger	Identifies the condition or detected object that caused the alert rule to generate an alert. The displayed information depends on the alert type.
Instances	Identifies an entity or activity affected by the trigger. One trigger can have multiple instances.
Occurrence	Records each time Cyber Vision detects the alert condition for an instance.
Severity	Severity levels include Critical, High, Medium, and Low. Use these levels to prioritize your response.
Triggered By	The alert category triggers the alert.
Last Detected	Shows the date and time when the alert was last triggered.

Note

- The **Alerts** dashboard for the **Assets with unexpected external communications** alert type is relevant for last month only.
- The trigger, instance, and occurrence information displayed in the Alerts page depends on the alert type.

Alert information by alert type

Alert type	Trigger	Instance	Occurrence
Severe vulnerabilities in monitored entities	A vulnerability that meets the configured scoring threshold	An asset affected by the vulnerability	A detection of the vulnerability on the asset

Alert type	Trigger	Instance	Occurrence
Prohibited vendors	A vendor included in the prohibited-vendor list	An asset associated with the prohibited vendor	A detection of the prohibited vendor on the asset
Network Scanner	Network reconnaissance or scanning activity from an asset or IP address that is not on the Allowed scanners list.	A target asset scanned by that source IP address.	A detection of scanner activity on the target asset, including the scanned ports.
Assets with unexpected behaviors	A behavior detected on a monitored asset.	A monitored asset that participates in the behavior in the role specified by the alert rule: Initiator, Target, or Both.	Each detection of the selected behavior involving that monitored asset during the rule's configured time window.
Inactive assets	An alert rule whose configured inactivity threshold is met.	An asset that has stopped communicating.	A detection that the asset has remained inactive for the configured duration.
Intrusion Detection	A Snort rule that detects suspicious or malicious network activity.	A source asset involved in traffic that matches the Snort rule.	Each detection of the Snort rule involving the source asset.
Assets with unexpected external communications	A monitored asset that communicates with an external address or domain.	An external IP address or domain contacted by the monitored asset.	Each detected communication between the monitored asset and the external address or domain.

MITRE ATT and CK information for Intrusion Detection alerts

Describes the MITRE ATT and CK tactics and techniques displayed for Snort-generated Intrusion Detection alerts.

Use the MITRE ATT and CK information in an Intrusion Detection alert to understand the objective and method of the activity detected by a Snort rule.

MITRE ATT and CK mapping

Cyber Vision maps the Snort rule that generates an **Intrusion Detection** alert to the corresponding MITRE ATT and CK tactics and techniques.

A Snort rule uses a GID:SID pair to identify the generator and signature that detected the activity. When a MITRE ATT and CK mapping exists for the GID:SID pair, Cyber Vision displays the mapped information in the alert preview and summary.

Cyber Vision displays the MITRE ATT and CK information in the following locations:

- The expanded alert preview displays the associated MITRE ATT and CK tactics.
- The alert **Summary** tab displays the GID:SID pair and the associated MITRE ATT and CK tactics and techniques.
- A tooltip displays the technique name when you hover over a MITRE ATT and CK technique ID.

> **Note**
>
> A Snort rule can map to one or more MITRE ATT and CK tactics. Each tactic can include one or more techniques.

MITRE ATT and CK alert details

From the main menu, choose **Alerts**, expand an **Intrusion Detection** alert, and click **View alert summary**.

Table 18: MITRE ATT and CK information

Field	Description
GID:SID	Identifies the Snort generator and signature that generated the alert.
MITRE ATT and CK Tactic	Identifies the objective that the detected activity attempts to achieve.
MITRE ATT and CK Technique	Identifies how the detected activity attempts to achieve the objective. Hover over a technique ID to view the technique name.

Supported actions for alert rules

Outlines the management actions supported for each Cyber Vision alert rule type, detailing permitted operations such as creating, editing, duplicating, deleting, pausing, or resuming rules according to alert type.

Identify the management actions that Cyber Vision supports for each alert rule type.

Alert type	Permitted alert rule actions
Severe vulnerabilities in monitored entities	Create, edit, duplicate, delete, pause, or resume alert rules.
Prohibited vendors	Edit, pause, or resume the alert rule.
Inactive assets	Create, edit, delete, pause, or resume alert rules.
Assets with unexpected external communications	Create, edit, duplicate, delete, pause, or resume alert rules.
Intrusion Detection	Pause or resume the default alert rule. You cannot create, edit, duplicate, or delete the default alert rule.
Network Scanner	Edit, pause, or resume the alert rule.
Assets with unexpected behaviors	Create, edit, duplicate, delete, pause, or resume alert rules.

Pause or resume individual alert rules

Explains how to pause or resume individual alert rules to manage alerting behavior effectively.

Starting from Cisco Cyber Vision Release 5.6.x, you can pause or resume individual alert rules.

Pausing an alert rule temporarily stops that rule from generating new alerts. Other rules associated with the same alert type remain active.

Here are few things for you to consider before pausing or resuming individual alert rules.

- Resuming a paused alert rule allows it to generate new alerts again.
- Pause and resume actions are no longer available at the alert-type level.

  Migration note: When you upgrade from Release 5.5.x to Release 5.6.x, Cyber Vision sets every rule associated with a paused alert type to **Paused**. After the upgrade, resume individual rules as needed.

Pause or resume individual alert rules

Pause or resume one or more individual alert rules and control whether they generate new alerts.

Pause one or more alert rules to temporarily stop them from generating new alerts, or resume paused rules to restart alert generation.

Pausing an alert rule affects only the selected rule. Other rules associated with the same alert type remain active. Pausing a rule does not change existing alerts.

Before you begin

- Ensure that your user role allows you to manage alert rules.
- Identify the alert type and rules that you want to pause or resume.

Procedure

1. From the Cisco Cyber Vision main menu, choose **Configuration** > **Alerts**.
2. Select an alert type.
3. Select the check boxes for one or more alert rules that you want to pause or resume.
4. Click **Pause** or **Resume**.
5. Confirm the action if prompted.

When you pause the selected alert rules, Cyber Vision stops generating new alerts for those rules. Existing alerts remain unchanged. Other rules associated with the same alert type remain active.

When you resume the selected alert rules, Cyber Vision allows them to generate new alerts again.

The status of each selected rule changes to **Paused** or **Active**.

Create alert rules for severe vulnerabilities in monitored entities

Configure alert rules to monitor asset vulnerabilities and receive timely notifications about severe threats.

Enable proactive vulnerability monitoring by creating alert rules that trigger notifications for severe vulnerabilities within monitored assets.

Starting with Release 5.6.x, you cannot configure alert rules for functional groups. When you upgrade to Release 5.6.x, Cyber Vision automatically deletes existing alert rules configured for functional groups.

Create alert rules under the **Severe vulnerabilities in monitored entities** alert type to automatically notify you when assets meet specific vulnerability criteria. This helps ensure timely response to critical security threats.

Procedure

1. From the main menu, choose **Configuration** > **Alerts**.
2. Select the **Severe vulnerabilities in monitored entities** alert type.
3. Click **Create new rule**.
4. Enter an **Alert Rule Name**, select the **Severity** and **Entity type**.

Entity types:

- **Organization Hierarchy (Sensors)**: Triggers alerts for assets linked to sensors assigned to the selected organization hierarchy levels.
- **Organization Hierarchy (Networks)**: Triggers alerts for assets linked to networks assigned to the selected organization hierarchy levels.

5. On the **Entity selection** page, select the organization hierarchy levels.
   - If you select assets based on organization hierarchy (Networks), check **Assets seen in Unknown networks** to include unidentified or unmapped assets.
   - If you select assets based on organization hierarchy (Sensors), check **Assets seen by Unknown data sources** to include unidentified or unmapped assets.

   Note

   The available **Entity selection** options depend on the **Entity type** you select in the **Rule name and entity type** step.

6. In the **Scoring system and threshold** tab, select one scoring system:
   - For **Cisco Security Risk Score**, enter a threshold number between 34 and 100.
   - For **CVSS**, enter a threshold number between 7 and 10.

   Note

   Cisco Security Risk Score is the default, but you can select **CVSS**.

7. Review your selections in the **Summary** and click **Save**.

The new alert rule appears on the **Configuration** > **Alerts** > **Severe vulnerabilities in monitored entities** page. You receive alerts when asset vulnerabilities match the new rule.

What to do next

- Regularly review the **Configuration** > **Alerts** page to manage and update alert rules as needed.
- To manage alert rules, navigate to **Configuration** > **Alerts**, select an alert type, and choose to edit, duplicate, or delete actions.

Create an alert rule for inactive assets

Configure a rule to trigger alerts when assets become inactive for a specified period.

You receive timely notifications and can take action when assets have not communicated for a set timeframe.

You can monitor asset activity and automatically generate alerts when assets are inactive for longer than a set threshold.

Before you begin

Identify the assets you want to monitor.

Procedure

1. From the main menu, choose **Configuration** > **Alerts**.
2. Select the **Inactive assets** alert type.
3. Click **Create new rule**.
4. Specify the **Alert Rule Name**, **Severity**, and the timeframe for inactivity (**Since inactive**).

   > **Note**
   >
   > You will receive an alert if an asset does not communicate within the selected period.

5. Select the assets you want to monitor.
6. View the summary and click **Save**.

When an asset is inactive for the specified period, the system triggers an alert. The **Alerts** page displays a summary of the alert and its instances.

Create an alert rule for external communications

Configure a rule to generate alerts for assets when unexpected external communications are detected.

You can establish an alert rule that enables the detection and notification of any monitored asset communicating externally, ensuring timely identification and response to potential security risks.

When an asset communicates with external IP addresses or domains, the alert rule triggers a notification in the **Alerts** dashboard. This allows you to manage asset security proactively.

Procedure

1. From the main menu, choose **Configuration** > **Alerts**.
2. Select the **Assets with unexpected external communications** alert type.
3. Click **Create new rule**.
4. Enter an **Alert Rule Name** and select **Severity** and **Entity type**.

   Entity types include:

   - **Organization Hierarchy (Sensors)**: Triggers alerts for assets linked to sensors assigned to the selected organization hierarchy levels.
   - **Organization Hierarchy (Networks)**: Triggers alerts for assets linked to networks assigned to the selected organization hierarchy levels.
   - **Asset Types**: Triggers alerts for assets linked to the selected asset types.

5. Select the relevant organization hierarchy levels or asset types in the **Entity selection** page.

   To include unidentified or unmapped assets:

- Select **Assets seen by Unknown data sources** for the **Organization Hierarchy (Sensors)** entity type.
- Select **Assets seen in Unknown networks** for the **Organization Hierarchy (Networks)** entity type.

> **Note**
>
> The available **Entity selection** options depend on the **Entity type** you select in the **Rule name and entity type** step.

6. Review your selections in the **Summary** and click **Save**.

The new alert rule appears under **Configuration** > **Alerts** > **Assets with unexpected external communications** alert type.

What to do next

- Regularly review the **Configuration** > **Alerts** page to manage and update alert rules as needed.
- Navigate to **Configuration** > **Alerts**, select the alert type, and choose the appropriate action to edit, duplicate, or delete alert rules.

Configure allowed scanner IP addresses for the Network Scanner alert rule

Guides you through adding allowed scanner IP addresses to Default_Scan_Global. Port scans from addresses on the allowed scanner list are exempt from detection and do not trigger alerts.

Use this task to manage allowed scanner IP addresses for **Default_Scan_Global**, the default **Network Scanner** alert rule.

Adding IP addresses under Allowed scanners exempts them from detection and alert generation. Port scans from IPs not included as Allowed scanners will trigger a new alert instance.

Follow these steps to configure allowed scanner IP addresses for Network Scanner alert rules:

Procedure

---

1. From the main menu, choose **Configuration** > **Alerts**.
2. On **Alerts**, select **Network Scanner**.
3. In **Alert Rules**, select **Default_Scan_Global** and then select the **Edit** under **Actions**.
4. On **Rule name and severity**, keep the default values and click **Next**.
5. Under **Allowed scanners**, enter an IP address in **Allowed scanner IP**, or search by asset name and select the associated IP address. Then click **Add**.
6. Click **Next** to open **Summary**.
7. Review the **Allowed scanners** count and IP address selection, then click **Save**.

The system updates Default_Scan_Global with the specified allowed scanner IP addresses. Port scans from these addresses are exempt from detection and do not trigger alerts.

What to do next

Next, from the main menu, select **Alerts** and review alerts for Network Scanner alerts generated by scanner activity that is not exempt from detection. Open an alert and review **Summary** to identify the scanner, scanned targets, and scanned ports. View alerts in a table and export them to a CSV file if you need to retain a trace.

Under **Assets**, open the scanner asset for more details, then review the alert from its **Alerts** tab.

Asset behavior alerts

Introduces unexpected asset behavior alerts, the rule criteria that trigger them, and the asset roles that determine how Cyber Vision matches observed behavior.

The **Assets with unexpected behaviors** alert type raises alerts when selected assets participate in a behavior selected in an active rule during its configured time window. Unexpected asset behavior refers to behavior that matches a rule you configured for this alert type.

- A rule specifies the assets to monitor, their required role for behavior, the behaviors to watch, a time window, and an alert severity.

  Note

  The time window can be from 1 to 30 days. The default is 7 days.

- An alert is raised when a matching behavior is observed. If Syslog notification is enabled for the alert type, Cisco Cyber Vision also sends a corresponding event to the configured Syslog server.

Asset roles for behavior

An asset behavior describes a meaningful action inferred from network communications, for example, Program Download, Restart CPU, Read Var, and so on. Every behavior has two roles:

- Initiator (source) - The asset that performs the behavior.
- Target (destination) - The asset on which the behavior is performed.

Note

Some behaviors are role-agnostic. They match only rules configured for both initiator and target roles.

Table 19: Asset roles for behavior alert rules

Rule role	Use it when	Example
Initiator	The configured assets must perform the selected behavior.	Monitor a jump host that initiates an OT command.
Target	The configured assets must receive the selected behavior.	Monitor a PLC that receives a program change.
Both	Either role is meaningful, or you need to include role-agnostic behaviors.	Monitor a critical asset that participates in either role.

Create an alert rule for unexpected asset behaviors

Provides instructions to create a rule that alerts when selected assets participate in selected behaviors during the configured lookback window.

Create a focused alert rule to monitor behaviors that have a clear operational or security purpose.

The alert rule includes steps for specifying identity, scope, entities, time window, and behaviors, and for conducting a final summary review.

Follow these steps to create an alert rule for unexpected asset behaviors.

Procedure

1. From the main menu, choose **Configuration** > **Alerts**.
2. Select **Assets with unexpected behaviors**, then click **Create new rule**.
3. Under **Rule name and entity type** ,
   a) Enter a descriptive **Alert Rule Name**.
   b) Select the **Severity**.

   > **Note**
   >
   > Choose severity based on operational consequence, not protocol alone.

   c) Select one **Entity type**:
      - **Organization Hierarchy (Sensors)**: Triggers alerts for assets linked to sensors assigned to the selected organization hierarchy levels.
      - **Organization Hierarchy (Networks)**: Triggers alerts for assets linked to networks assigned to the selected organization hierarchy levels.
      - **Assets**: Triggers alerts for assets linked to the selected asset types.

   d) Click **Next**.

   The selected severity applies to every instance raised by the rule.
4. Under **Entity selection**,
   a) Select the relevant organization hierarchy levels or asset types.

> **Note**
>
> The available **Entity selection** options depend on the **Entity type** you select in the **Rule name and entity type** step.
>
> - If you select assets based on organization hierarchy (Networks), check **Assets seen in Unknown networks** to include unidentified or unmapped assets.
> - If you select assets based on organization hierarchy (Sensors), check **Assets seen by Unknown data sources** to include unidentified or unmapped assets.
> - If you select Assets, you can filter assets by name, IP address, MAC address, or network. Verify the selection counter before you continue; a filter narrows the visible table but does not remove previously selected assets.

b) Click **Next**.

5. Under **Time window and scope**,
   a) Set the lookback window in **Time window**. The default time window is 7 days. You can set the time window from 1 to 30 days.

   > **Tip**
   >
   > A longer window keeps infrequent behaviors active. A shorter window makes alerts clear sooner after the last observation.

   b) Under **Match configured assets as**, select the asset role:
      - **Target**: The behavior is performed on the selected asset.
      - **Initiator**: The selected asset performs the behavior.
      - **Both initiator and target**: Both initiator and target roles match.

   c) Click **Next**.
6. Under **Behaviors**,
   a) Select one or more behaviors from the catalog. Use search as needed, and switch between **Important behaviors** and **Other behaviors** to review the category and description of each behavior.

   > **Note**
   >
   > Important behaviors are visually emphasized in alerts. Their importance does not override the severity you assign to the rule.

   b) Click **Next**.

7. Under **Summary**, review the rule name, severity, entity type, selected entities, time window, role, and behaviors, then click **Save**.

Evaluation starts automatically. Matching observations already present within the configured time window can produce alerts without waiting for a new packet.

Verify asset behavior alerts instance

Verify unexpected asset behavior alert instances and identify their source, target, behavior, and related rule context

Review active asset behavior alert instances to determine their origins, affected targets, observed behaviors, and associated rule context.

Asset behavior alerts in Cisco Cyber Vision remain active as long as the triggering behavior persists within a matching rule's time window. An alert clears when no running rule matches. This occurs, for example, when observations age out, or when the rule, asset, behavior, or applicable role changes.

- Alerts are grouped by their source asset, even when the configured assets are targets. Each instance identifies the target asset and behavior.
- If several rules match the same source, target, behavior, and orientation, Cisco Cyber Vision displays one instance and lists the applied rules.

Follow these steps to verify asset behavior alerts instance.

Procedure

1. From the main menu, select **Alerts** and click the **Active** tab.

   You can select the **Muted** or **Cleared** tab to review alerts in those states.

2. Locate and expand the Assets with unexpected behaviors alert that you want to review.

   Alert rows are grouped by source asset. This arrangement keeps the potential initiator visible as the alert trigger. Each instance also identifies the exact target and behavior.

3. Click **View alert summary** to view the behavior and the corresponding source or target details.
4. Click the **Instances** tab and review each column:
   - **Source asset** - shows the initiator.
   - **Target asset** - shows the destination.
   - **Behavior** - displays the observed action.
   - **Severity** - indicates the applicable rule severity.
   - **Alert Rules** - lists the number of matching rules.
   - **Last Detected** - shows the most recent observation.

> **Note**
>
> Repeated observations update the existing instance and its last-detected time. They do not create a new row for each occurrence.

5. Under **Alert Rules**, click the count to open the instance drawer and review comprehensive details: behavior, both source and target assets, available type, vendor, addresses, networks, sensors, applied rule, severity, configured role, and time window.

   For a target-oriented rule, the configured asset appears under **Target asset**. The source remains the initiator and is the starting point for review.

You can identify the observed behavior, affected assets, and rule context that produced each alert instance.

Mute alert instances

Mute alert instances to prevent repeated reviews of acknowledged alerts for non-critical issues.

Temporarily suppress non-critical alert instances so you do not need to review known, non-urgent alerts repeatedly.

Mute alerts for **Prohibited vendors**, **Inactive assets**, **Intrusion Detection**, **Assets with unexpected behaviors**,and **Assets with unexpected external communications** alert types. This helps you focus on critical issues. The mute feature marks specific asset alerts as reviewed and not urgent. Muted alert instances remain in the system and are inactive until the mute period ends.

Procedure

---

1. From the main menu, choose **Alerts**.
2. On the **Active** tab, find the relevant alert type and click the alert **Instances** count.
3. Select the alert instances you want to mute.
4. Click **Mute**.
5. Select the mute duration.
   - You can select from three available durations: **Forever**, **For 7 days**, or **For 30 days**.
   - To specify a custom period, select **Custom** and enter a number of days from 1 to 180.

> **Note**
>
> After the selected mute duration (except for **Forever**), alerts become active again.

6. (Optional) Add a comment.
7. Click **Mute** to confirm.

Muted alerts move from the **Active** tab to the **Muted** tab.

What to do next

- To unmute an alert instance, go to **Alerts** > **Muted**, select the alert instance, and click **Unmute**.
- After you unmute, the instance drawer of the active alert shows when it was last muted.

Clear alerts for specific assets

Clear alerts for designated assets to ensure only current, unresolved alerts remain after issues are resolved.

Clear resolved alerts from assets so the alert dashboard reflects current alerts only.

Perform this task when asset-related issues are resolved, but the system still lists alerts for those assets. Clearing alerts helps maintain accurate alert tracking.

Procedure

1. From the main menu, choose **Alerts** > **Active**.
2. Click the instance count for either the **Inactive assets**, **Network Scanner**, **Assets with unexpected behaviors**, or **Assets with unexpected external communications** alert types.
3. Select the asset you want to clear alerts for.
4. Click **Clear**.

After you clear alerts, the system moves the selected alert from the **Active** tab to the **Cleared** tab to show that its alerts are cleared.

Syslog notification details for alert types

Provides a lookup of common and alert-type-specific fields in Cisco Cyber Vision syslog notifications to help you track and investigate alert events.

Cisco Cyber Vision sends syslog notifications to the configured syslog server when an alert is raised, cleared, or its status changes. The notifications include information that helps you track and investigate events.

Cisco Cyber Vision sends alert notifications in Common Event Format (CEF). Each notification contains common alert fields and fields specific to the alert type. Some fields appear only when the associated asset or enrichment information is available.

Common alert fields

Every alert syslog notification contains the following common fields.

Field	Description	Presence
`alertId`	Identifies the alert.	Always
`alertRuleId`	Identifies the alert rule that generated the alert.	Always
`assetId`	Identifies the asset associated with the alert instance.	Always
`assetName`	Specifies the name of the associated asset.	When asset information is available

Field	Description	Presence
`sensorNames`	Lists the sensor names and packet-capture filenames associated with the asset, separated by semicolons.	When asset information is available

Alert-specific fields

In addition to the common fields, syslog notifications contain the following fields for each alert type.

Alert type	Alert-specific fields
Severe vulnerabilities in monitored entities	`vulnCSRS`, `vulnCVSSscore`, `vulnCveId`, `vulnName`
Prohibited vendors	`vendorName`
Intrusion Detection	`snortSignature`
Network Scanner	`scanEventId`, `scanType`, `scannerIP`, `targetCount`, `targetIPs`, `targetPorts`
Inactive assets	`inactiveDuration`
Assets with unexpected external communications	`asnOrganization`, `assetInterface`, `country`, `remoteAddress`, `remoteDomain`
Assets with unexpected behaviors	`behaviorId`, `behaviorLabel`, `behaviorDirection`, `sourceAssetId`, `sourceAssetName`, `targetAssetId`, `targetAssetName`

Enable or disable syslog notifications for alert types

Provides instructions for enabling or disabling syslog notifications for specific alert types in Cyber Vision Center, including prerequisites, navigation steps, and the effects of syslog notification settings on alert message delivery.

You can manage whether the Cyber Vision Center sends syslog notifications for alerts of specific alert types to your configured syslog server.

Follow these steps to enable or disable syslog notifications for an alert type:

Before you begin

- Ensure you have administrator access to Cyber Vision Center.
- Confirm that a syslog server is configured. Refer to **Configure syslog** topic in Cisco Cyber Vision Classic UI Administration Guide.

Procedure

1. From the Cyber Vision New UI, choose **Configuration** > **Alerts**.
2. Select an alert type.
3. Enable or disable **Syslog Notification**.

When you enable syslog notifications in the Cyber Vision Center, you receive syslog messages on the configured syslog server whenever the system raises (or unmutes), clears, or mutes an alert.

Vulnerabilities

This concept explains what vulnerabilities are, how they are detected within the system, and their implications for asset security.

A vulnerability is a system weakness that

- enables attackers to gain unauthorized access or perform malicious actions,
- results from flaws in system design, implementation, or configuration, and
- requires mitigation through security measures to prevent exploitation.

Feature history table

Feature	Release Information	Feature Description
Bulk vulnerability acknowledgment for assets	Release 5.5.x	You can now acknowledge or unacknowledge multiple vulnerabilities at once from the asset vulnerability table. This change removes manual processing, saving time for asset security.
Asset vulnerability insights in New UI	Release 5.5.x	Cyber Vision Center matches asset properties against the knowledge database to detect vulnerabilities. You can view the matched asset properties in the New UI. This process provides clear, actionable insights into your security posture.

Vulnerability detection in Cyber Vision Center

Provides information about how the Cyber Vision Center detects device vulnerabilities using asset properties and knowledge database rules.

Cyber Vision Center detects vulnerabilities on assets by matching their properties (such as vendor, reference, and firmware version) against a knowledge database of detection rules. This database regularly receives updates from external sources such as Computer Emergency Response Teams (CERTs), device manufacturers, and leading industry partners (e.g., Schneider and Siemens).

Key attributes of vulnerability detection:

- The vulnerability detection process is automated and relies on the latest rule database updates.
- Viewing asset vulnerability information allows security teams to assess risk exposure and prioritize remediation efforts.

To view the asset properties used for vulnerability detection in the system:

- From the main menu, choose **Assets**.
- Select the asset with vulnerabilities.
- Click **Vulnerabilities** and select the relevant vulnerability.

Vulnerability scores

Details the Cisco Security Risk Score and Common Vulnerability Scoring System, including the risk and severity categories associated with each score.

Vulnerability scores indicate the potential risk level and impact associated with specific vulnerabilities. Vulnerability scores include the following scoring systems.

Cisco Security Risk Score (CSRS)

The Cisco Security Risk Score, which is powered by Cisco Vulnerability Management, is represented on a scale from 0 to 100.

CSRS quantifies the risk of a vulnerability by looking beyond technical severity to determine how real-world attackers are leveraging the vulnerability in the wild, if at all. The score considers vulnerability and threat variables, including predictive modeling to forecast the weaponization of vulnerabilities, the availability of recorded exploits or exploit kits, the presence of near real-time exploitation, and more.

A click-through product demo supports self-paced exploration of Cisco Vulnerability Management and the Cisco Security Risk Score.

Common Vulnerability Scoring System (CVSS)

The Common Vulnerability Scoring System (CVSS) captures the principal characteristics of a vulnerability and produces a numerical score that reflects its severity. The numerical score can be translated into a qualitative representation, such as low, medium, high, and critical, to help organizations assess and prioritize vulnerability management processes.

For more information, refer to the CVSS website.

Vulnerabilities details

Outlines the details available on the Vulnerabilities page, including CVE IDs, names, Cisco Security Risk Score, CVSS scores, MITRE ATT and CK tactics, attack vectors, and affected assets for each identified vulnerability.

The **Vulnerabilities** page lists all identified vulnerabilities and their details.

Table 20: Vulnerability field descriptions

Field name	Description	Possible values/examples
CVE ID	CVE ID stands for Common Vulnerabilities and Exposures Identifier. It is a unique, standardized identifier assigned to publicly known cybersecurity vulnerabilities. This ID allows for consistent referencing of specific vulnerabilities across different security products and databases.	CVE-2023-20198
Name	This field provides a concise, descriptive title for the vulnerability.	Out-of-bounds Write Vulnerability in Rockwell ControlLogix Communication Modules

Field name	Description	Possible values/examples
Cisco Security Risk Score (CSRS)	This is a proprietary risk assessment score developed by Cisco. It provides an evaluation of the vulnerability's severity and potential impact based on Cisco's internal analysis and threat intelligence. It's typically presented as a numerical score along with a severity level (e.g., High, Medium, Low).	• 67-100: High vulnerability • 34-66: Medium severity vulnerability • 0-33: Low severity vulnerability
CVSS Score	It is the industry standard for assessing the severity of computer system security vulnerabilities. It provides a numerical score (0-10) and a qualitative severity rating (Low, Medium, High, Critical) based on various metrics like attack vector, complexity, impact on confidentiality, integrity, and availability. Security teams use CVSS scores to prioritize severe vulnerabilities and strengthen system security.	• 9-10: Critical vulnerability • 7-8.9: High severity vulnerability • 4-6.9: Medium severity vulnerability • 0.1-3.9: Low severity vulnerability
MITRE ATT and CK Tactics	Indicates whether the vulnerability can be associated with specific tactics from the MITRE ATT and CK® framework. Tactics represent the "why" of an attack (for example, gaining initial access, privilege escalation). A technique describes the specific actions or methods an attacker uses to achieve a tactic. Each tactic may be achieved through multiple techniques. To view detailed information about the tactics and techniques associated with a specific vulnerability, click the CVE ID link and review the MITRE ATT and CK section. The "3 Tactics matched" (for example) indicator suggests that the system has identified activities corresponding to three different MITRE ATT and CK tactics. Under each tactic, you can find one or more techniques used. For additional details, visit https://attack.mitre.org.	Execution, Exfiltration, Persistence
Attack Vector	Describes the path or means by which an attacker can exploit the vulnerability. It indicates the context from which the vulnerability can be exploited (example, locally, over a network, physically).	Network, Adjacent Network, Local, Physical

Field name	Description	Possible values/examples
Affected Assets	This number indicates how many of your monitored assets are currently identified as being vulnerable to this specific CVE. Clicking on the CVE ID provides a detailed list of these assets.	1 for CVE-2023-20198, 2 for CVE-2024-20437

Acknowledge or unacknowledge vulnerabilities for a single asset

Acknowledge vulnerabilities affecting an asset, or revert previous acknowledgements to manage security alerts in Cyber Vision Center.

Enable efficient management of security alerts by acknowledging or unacknowledging vulnerabilities detected for a single asset.

Perform this task to prioritize remediation efforts and maintain an accurate security dashboard. When you acknowledge a vulnerability, its alerts are removed from the **Alerts** dashboard. If you revert the acknowledgement, the alerts will appear in the **Alerts** dashboard again.

Before you begin

Ensure you have access to the **Assets** and **Vulnerabilities** dashboards in Cyber Vision Center. You may need to check your permissions under **Admin** > **Users** > **Role Management**.

Procedure

1. From the main menu, choose **Assets**.
2. Select an asset.
3. Select the **Vulnerabilities** tab.
4. To view an acknowledged vulnerability in the **Alerts** dashboard again and revert the acknowledgement:
   a. Check the checkboxes for the vulnerabilities you want to acknowledge.

      Check all the checkboxes to select all vulnerabilities at once.

   b. Click **Acknowledge**.

   c. Enter a comment if needed and confirm your acknowledgement.

5. To unacknowledge vulnerabilities:
   a. Click **Show Acknowledged** to see acknowledged vulnerabilities.

   b. Check the checkboxes for the vulnerabilities you want to unacknowledge.

   c. Click **Unacknowledge**.

- When you acknowledge a vulnerability, the system removes the alerts for that vulnerability from the **Alerts** dashboard.
- When you revert an acknowledgement, the alerts reappear in the **Alerts** dashboard.

What to do next

View the **Alerts** dashboard to verify the updated status of vulnerabilities.

Acknowledge or unacknowledge multiple assets for a single vulnerability

This task enables you to acknowledge or unacknowledge multiple assets for a single vulnerability, which helps you efficiently update remediation status and maintain accurate vulnerability records.

Simplify vulnerability management by acknowledging or unacknowledging multiple affected assets in a single operation. This reduces the time required to process vulnerability changes across several assets.

Use this task when the same vulnerability is detected across multiple devices in your environment. Bulk acknowledgment or unacknowledgment helps keep your security status accurate without repeating actions for each asset.

Procedure

1. From the main menu, choose **Vulnerabilities**.
2. Select the vulnerability you want to manage.
3. To acknowledge assets:
   a. In the **Affected** tab, check the checkboxes for the assets you want to acknowledge.
   b. Add a comment to provide context for the acknowledgment.
   c. Click **Acknowledge selected assets** and confirm.
4. To unacknowledge assets:
   a. In the **Acknowledged** tab, check the checkboxes for the assets you want to unacknowledge.
   b. Click **Unacknowledge**.

The system acknowledges or unacknowledges the selected assets for the specified vulnerability.

What to do next

Review the updated vulnerability list to confirm the changes.

Acknowledge critical vulnerabilities

Provides instructions for filtering and acknowledging critical vulnerabilities with high CVSS scores to declutter dashboards, reduce alert noise, and streamline risk management for assets.

Acknowledge critical vulnerabilities with a CVSS score greater than 9.0 to declutter dashboards, and reduce alert noise.

Use this task when you need to focus on vulnerabilities of the highest severity for an asset by filtering and acknowledging them.

Before you begin

- Ensure you have permission to view and acknowledge vulnerabilities.

Procedure

1. From the main menu, choose **Assets** and click asset name.
2. View the **Vulnerabilities** list for the selected asset.
3. Click the filter icon of the table.
4. Select **Critical** from the drop-down list in the **CVSS Score** column.

5. Click **Acknowledge**.

When you acknowledge vulnerabilities, they no longer appear in dashboard counters and alerts. This simplifies ongoing risk management.

What to do next

Review acknowledged items periodically to ensure they remain appropriate.

Communication maps

Describes how communication maps visually represent communication flows among industrial assets to help teams quickly investigate and assess risks based on abnormal flows, observed protocols, and asset relationships.

A communication map is a network visualization tool that

- Displays communication patterns at the asset-interface level.
- Organizes map data by asset groups and enables filtering of the displayed data.
- Supports investigation with details about asset interfaces, asset groups, and intra-group communications, including observed protocols, data exchange volumes, and source and destination asset-interface information.

This functionality enables operational technology (OT) and information technology (IT) teams to quickly visualize and understand the communication context of industrial assets. It provides a clear visual reference to abnormal communications and potential risks.

Feature history table

Feature	Release Information	Feature Description
Communications page enhancement	Release 5.6.x	The Communications page organizes map data by asset groups and displays communications at the asset-interface level. Asset groups can be network groups or custom groups. Functional groups are no longer supported. You can view details for asset interfaces, groups, and communications within a group. The control panel provides filter options and display settings.
External IP country mapping	Release 5.5.x	You can view the countries of external IP addresses your asset connects with. Use this map to identify geographical locations and quickly decide which communications to investigate, improving your network insight and security.

Feature	Release Information	Feature Description
ASN and ASN organization insight for external communications	Release 5.5.x	You can view ASN (Autonomous System Number) and ASN Organization information for external communications. Use this information to identify traffic sources and network owners so that you can quickly detect suspicious communications and reduce investigation time.
Communication maps and their filter enhancements	Release 5.4.x	Easily spot communications between assets, including those outside your active view. Communication maps highlight assets outside your active view filter with dotted lines.
External communications visibility	Release 5.4.x	View all communications between a selected asset and external entities. You can identify unexpected external communications that may expose your organization to attacks.
Group by network functionality in communications	Release 5.4.x	The communication map displays all communications between network groups and simplifies network interaction analysis.
See functional group-centric views of the communication map	Release 5.3.x	The communications map displays the communication activity between the configured functional groups. The communication links between groups are not actionable.
Using asset vendor names and icons	Release 5.3.x	In the New UI, communication maps include vendor icons that make asset identification easier.

Apply active view filters to the communication map

Apply filters in the communication map to focus on specific assets and their communications.

Use the common active-view filtering procedure to filter the Dashboard, Alerts, Assets, Vulnerabilities, and Communications pages. For that procedure, refer to Filter views in Cyber Vision New UI on page 54.

The active view lets you filter assets and communication links in the communication map so you can focus on specific groups. Any asset or communication outside the applied filters is shown as a dotted line, indicating it is excluded from your current view.

Follow these steps to apply active view filters to the communication map.

Procedure

1. From the main menu, select **Communications**.
2. On the **Communications** page, click the **Edit** link in the upper-right corner.
3. Under **Available filters**, configure the filters you need:

a) Click the **Select** link next to **Networks**, **Asset types**, or **Vendors** .
b) Choose the values to include for each filter.
c) Click **Apply**.

4. Click **Apply filters** to update the map.

The selected filter tags appear at the top of the **Communications** page. The map and control panel refresh to show the groups, assets, communications, and protocols associated with the active filters.

Communication map control panel

Introduces the communication map control panel, detailing features for viewing and analyzing network communications, accessing subnet details, and using panel views such as Filter Options, Settings, and Legend to filter, adjust display settings, and interpret map data.

Use the control panel on the map to view and analyze network communications and subnet details for each node on the map.

Control panel views

You can access the communication map from the **Communications** option in the main menu. The collapsible control panel appears on the left side of the map. Use it to filter map data, adjust the display, and understand map legends.

- **Filter Options**
- **Settings**
- **Legend**

The table lists the available views in the control panel and describes their uses.

Table 21: Control panel views

View	Use
Filter Options	Filter map data by time interval, Layer 2 network visibility, group, and protocol. Refer to Filter communications on the map on page 82.
Settings	Configure the map layout, visibility, communication scope, and asset labels. Refer to Configure communication map display settings on page 83.
Legend	Identify the symbols and line styles used for groups and communications. Refer to View communication map legend indicators on page 84.

You can collapse the control panel to an icon-only bar to create more space for the map. Expand it again whenever you need to update a control.

Filter communications on the map

Provides instructions for limiting the communications displayed on the map by time, L2-network visibility, group, and protocol.

Filtering communications allows you to view specific traffic and network details, making it easier to analyze patterns or anomalies.

Follow these steps to filter communications on the map.

Procedure

1. From the main menu, select **Communications**.
2. In the left control panel, click the filter icon to open **Filter Options**.
3. Under **Filter Options**, set the filters you need:

Filter Options	Use
Interval	Select the required time filter to focus on communications during specific periods. The **Last 7 days** filter is selected by default.
Show unknown (L2 Network)	Select this option to display subnets that contain MAC addresses but no IP addresses.
Groups	Select one or more asset groups to focus on their assets. Asset groups can be network groups or custom groups. Functional groups are no longer supported. IPv4 and IPv6 link-local addresses are excluded by default; select them when needed for local network discovery.
Protocols	Select the protocols to display. All protocols are selected by default, except **Traffic-heavy Protocols**, which are excluded to keep the map easier to read. Select them manually to include their data.

4. Click **Apply** to update the map.

   The **Clear** button removes the current, unapplied filter selections.

The map displays only the communications that match the selected filters.

Configure communication map display settings

Configure communication map arrangement, visibility, communication scope, and asset labels.

Use display settings to emphasize specific assets or communications, control map arrangement, and modify labels for improved clarity during investigations.

Follow these steps to configure communication map display settings.

Procedure

1. From the main menu, select **Communications**.
2. In the left-side control panel, select the Settings icon to open **Settings**.
3. Under **Settings**, configure any of the following settings:

Settings	Use
Assets & Groups	

Settings	Use
Allow rearranging	Reposition nodes on the map by dragging them. Changes are temporary and are lost when you exit the map view. This setting is enabled by default.
Hide assets outside active view	Hide assets that are outside the current active view. This setting is disabled by default.
Show only assets with communications	Display only asset interfaces with observed communications. This setting is enabled by default.
Communications	
Show all communications	Display all non-aggregated communication links at the asset-interface level. This setting is disabled by default.
Show internal communications	Display internal communications within a group. This setting is enabled by default. **Note** If you enable **Show all communications**, the **Show internal communications** setting is automatically disabled.
Asset Label	
IP address	Show only the IP address on each asset label. This option is selected by default.
Asset name (IP address)	Show the asset name and IP address on each asset label. This option is not selected by default.

The communication map updates based on your selections.

View communication map legend indicators

Identify legend indicators on the communication map to understand group types and asset status within or outside the active view.

Use the communication map legend to identify group types, assets, and communication lines shown within or outside the active view.

Follow these steps to view communication map legends indicators.

Procedure

1. From the main menu, select **Communications**.
2. In the left control panel, select the **Legend** icon.
3. Review the legend indicators.

   The legend includes the following types:

Table 22: Communication map legend

Indicator	Meaning
Asset Group Type	
Network Group	Identifies a network group.
Custom Group	Identifies a custom group.
Assets & Groups	
Within active view	Identifies assets and groups within the active view.
Outside active view	Identifies assets and groups outside the active view.
Communications	
Within active view	Identifies an asset, group, or communication that matches the active-view.
Outside active view	Identifies an asset, group, or communication that is shown for context but does not match the active-view.
Aggregated between groups	Identifies communications aggregated between two groups.

You can now clearly identify the group types and communication status of map elements.

Exploring groups in a communication map

Describes how a communication map reveals group and conduit details in place while maintaining the surrounding network communication context.

This process helps you examine asset interfaces and communications as groups are expanded or collapsed, without losing map context.

Summary

Group exploration on a communication map allows users to examine assets and communication paths within a group, without losing visibility of the overall network context.

The key components involved in the process are:

- Asset groups: Collections of assets and communication paths that can be expanded or collapsed.
- Child group: An asset group can contain child groups. When you expand a parent asset group, its child groups appear within it on the map.

- Assets interfaces: Individual interfaces within an asset group., each with associated communication and summary details. However, when **Show only assets with communications** is turned off, the map can display asset interfaces that have no observed communications.
- Conduits: Aggregated communication links between groups that display both summary and detailed information.

Workflow

The following stages describe group exploration on the communication map.

1. Select a group on the map.

   A details pop-up opens with information such as the group's assets, type, protocols, and communication summary. The map continues to show the other groups.

2. Expand the group.

   Use **Expand group** in the details pop-up to expand the group. You can also use the drop-down arrow in the group label to expand the group. The map displays the group's assets, subgroups, and internal communications while keeping nearby groups visible.

3. View asset details.

   Select an asset in an expanded group. In the details pop-up, you can select:

   - **Communication Details** to view communication details of the interface in the right pane.
   - **View assets summary** to open the asset summary page in a new tab.

4. Review inter-group communication.

   When a group is expanded, communications between groups appear as aggregated conduits. Each conduit summarizes the communication between two groups to maintain cross-group context.

5. Expand a conduit for more detail.

   Expanding a conduit shows the individual communication links, including observed protocols and total data volume. Select a communication link to view the protocol and payload size.

   Collapse the conduit to return to the aggregated view.

6. Collapse groups when finished.

   Collapsing a group returns it to a summarized node and hides its internal assets and communications. Select **Collapse All** to return the entire map to the initial group-level view.

Use the communication map context menu

Navigate the communication map using context menu actions to view groups, inspect elements, and adjust map display.

Use the context menu to navigate the communication map, view group details, and adjust how the map is displayed.

Follow these steps to access context menus and adjust the communication map display:

Procedure

1. From the main menu, select **Communications**.
2. Right-click an empty area of the map canvas to open the context menu.
3. Select the action you need:

Option	Usage
Fit to view	Display all groups and nodes in the map.

Option	Usage
Collapse All	Return every group to the group-level view.
Show all communications	Display communication links at the asset-interface level.
Show internal communications	Display communications within a group using a non-aggregated-link view.

4. To work with a specific group, right-click the group and select one of the following options:
   - **Expand group** - Shows the contents of the group.
   - **Fit group** - Focus the map on the group.
   - **Open details** - Opens the group details.

The map updates to reflect the action you select.

Enable IDS on a sensor

Enable the Intrusion Detection System (IDS) on a compatible Cisco sensor to activate Snort-based intrusion detection.

Use this task to activate Snort intrusion detection on a supported Cisco sensor for network security monitoring.

Before you begin

Ensure that your sensor is one of these compatible devices:

- Cisco IC3000 Industrial Compute Gateway
- Cisco Catalyst 9300 Series Switch
- Cisco IR8340 Integrated Services Router Rugged
- Center DPI interface

Procedure

1. From the main menu, choose **Admin** > **Sensors** > **Sensor Explorer**.
2. Select the sensor on which you want to enable IDS.
3. Click **Enable IDS**.

IDS is active on the selected sensor. Snort monitors network traffic for threats.

What to do next

To disable Snort intrusion detection, select the sensor and click **Disable IDS**.

5 Configure segmentation

Topics:

Introduces segmentation in Cyber Vision, describing segmentation concepts and workspace, enabling segmentation on switches, using Cyber Vision segmentation processes, managing asset groups, analyzing switch communications, defining and editing segmentation rules, and simulating policy impacts to enhance network security and micro-segmentation.

Cyber Vision Segmentation

Introduces Cyber Vision Segmentation in Release 5.6.0 and explains how asset groups, segmentation rules, recommendations, simulation, and switch capability fit together.

Segmentation for industrial networks is introduced in Cyber Vision Release 5.6.0 to help you define, recommend, and simulate segmentation policy on IE3300, IE3400, IE3500, and IE9300 switches.

Use Segmentation to plan policy with observed network evidence. You can review global policy objects, inspect what a switch observes, evaluate recommendations, and simulate the impact of the segmentation rules you want to apply, before applying the rules.

- Asset groups provide segmentation identities, and segmentation rules define the permissions between those identities.
- Asset group identities map to Security Group Tags (SGTs), and permissions map to Security Group ACLs (SGACLs).

You cannot deploy SGT mappings, generate switch-ready SGACL configuration, manage active policy state, or synchronize policy to switches in this release.

You can create and edit asset group membership, review and accept group recommendations, create and edit logical segmentation rules, define common-service relationships, and simulate policy impact.

You can evaluate a segmentation model against one year of observed traffic and review logical pseudo-SGACL output for training and simulation.

Cyber Vision filters the switches displayed on the **Segmentation** page according to the selected organization hierarchy level. Selecting a lower sensor-based hierarchy level limits the list to switches associated with that level and hides switches outside the selected context. If you select a network-based organization hierarchy, the **Segmentation** page does not display segmentation data. In the switches table, Cyber Vision shows whether each switch has **Simulation** or **Enforcement** capability in later releases of Cisco Cyber Vision.

- IE3300 and IE3400 only support simulation. Data from these switches can only be used for simulation.
- IE3500 and IE9300 can support enforcement. You can apply segmentation rules on these devices in later releases of Cyber Vision.
- After upgrading to Cisco Cyber Vision Release 5.6.x, wait a few days before enabling segmentation. This delay allows Cyber Vision to populate the sensor-to-communication link data required for segmentation.

Table 23: Feature History Table

Feature	Release	Feature Description
Cyber Vision segmentation	Release 5.6.0	Introduces tools to model industrial network segmentation using observed switch communications. You can create and manage asset groups, review segmentation recommendations, configure inter-group, intra-group, default, and common-service rules, and simulate policy impact on supported switches.

Segmentation workspace

Details the Segmentation entry point, global and switch-specific work areas, and organization hierarchy behavior in Release 5.6.0.

The **Segmentation** pages separate global definitions from switch detail pages.

Workspace areas

Global definitions represent reusable policy objects. In the **Segmentation** page, select the dashlets for groups or segmentation rules to view all the groups and rules available.

Switch detail pages display the rules and communications associated with the selected switch. The simulation results provided apply to the selected switch.

The switches that are listed on the **Segmentation** page are filtered by the organization hierarchy applied in Cyber Vision Center.

Only sensor-based organization hierarchies apply to **Segmentation** pages. If you apply a network organization hierarchy, the **Segmentation** pages do not display any data.

Use this table to understand the **Segmentation** pages in Cyber Vision Center.

Table 24: Segmentation workspace areas

Area	Use it to
Segmentation page	Review global definition counts and segmentation-capable switches.
Global definitions: Asset groups	Review custom groups, network groups, SGTs, and the switches that a rule is used in.
Global definitions: Segmentation rules	Review global inter-group, intra-group, and common-service rules.
Switch detail: Communications	Inspect observed group-to-group communications in map, table, and participating-groups views.
Switch detail: Segmentation rules	Review the rules that apply to the selected switch.
Switch detail: Simulation	Simulate the effect of the current policy model on observed traffic from a switch.
Disabled-switch state	Select **Enable segmentation** only when you intend to include a disabled switch in segmentation analysis.

Enable segmentation on switches

Provides instructions for enabling segmentation on switches so Cyber Vision includes device data in recommendation and simulation workflows.

You must enable segmentation on a switch to include the data from the device in the recommendation and simulation workflows.

By default, segmentation is disabled on switches.

Procedure

1. From the Cyber Vision menu, choose **Segmentation**.
2. Select one or more switches from the list.
3. Select **Enable segmentation**.

Using Cyber Vision segmentation

This topic introduces the process flow of selecting a switch, grouping assets based on observed communications, creating segmentation rules, and validating the rules before you apply any segmentation rules to a device.

Summary

Use the observed communications for a selected switch to define zones and conduits, review group-to-group communications, build rules, and simulate the rules before refining them.

Workflow

For each switch, carry out the following process.

1. Select a switch to review the communications observed on the device.
2. Use the map view to build zones and conduits, and create asset groups. The asset groups define the zones, by network group, common services, or recommended micro-segments.
3. Review the communications between asset groups.
4. Build the segmentation rules.
5. Simulate the rules and review the impact of the designed rules. You can adjust the rules as needed before finally applying them on the target device.

Result

After you adjust the rules based on the simulation, repeat the process for the next switch.

Asset groups

Explains asset groups as the segmentation identity model, including interface-based membership, custom and network groups, global and local scope, SGT precedence, and fallback behavior.

Asset groups are the segmentation identities that Cyber Vision uses to evaluate policy. When an asset interface belongs to an asset group, that group determines the SGT for the interface and the rules that can apply to its traffic.

Cyber Vision includes an asset group for a switch only after it has seen at least one asset interface from that group in traffic related to that switch.

When Cyber Vision has seen interfaces from two asset groups on the same switch, it can evaluate rules between those groups for that switch. The two groups do not need to have communicated directly with each other on that switch.

If Cyber Vision has not seen any interface from an asset group on a switch, Cyber Vision excludes that group from that switch. Rules that involve that group are not evaluated for that switch.

Group membership is based on asset interfaces, not an asset. One asset can have multiple IP addresses, and different interfaces of the same asset can belong to different groups.

Global and local group behavior

Use this table to distinguish asset group families.

Table 25: Asset group families

Group family	Source of membership	Segmentation role
Custom asset group	User-created or recommendation-derived membership from observed asset interfaces.	Explicit segmentation identity with an SGT. The group can be global or local.

Group family	Source of membership	Segmentation role
Network group	Subnet-backed membership from Cyber Vision network definitions.	Fallback segmentation identity when an interface has no effective custom group.

Global groups are the default and preferred model for shared segmentation intent. A global assignment follows the interface wherever that interface is observed.

Local groups are switch-scoped. They are visible only on the switch where they are defined and override global membership on that switch. The local SGT replaces the policy context; it does not add another permission layer on top of the global group.

An observed interface can have only one effective SGT on a switch. Cyber Vision resolves identity in this order:

Table 26: Effective identity precedence

Order	Effective identity
1	Local custom group on the selected switch.
2	Global custom group assigned to the observed interface.
3	Network group fallback for the network that contains the interface.

Use this fallback behavior to predict what happens when local or custom group membership changes.

Table 27: Fallback behavior

Situation	Effective behavior
An interface is assigned to a local custom group on the selected switch.	The local group is the effective identity on that switch, even if the interface also has a global group.
An interface has no local custom group but has a global custom group.	The global group is the effective identity.
An interface has no effective custom group.	The network group for the interface network is the fallback identity.
A local group is deleted.	Former member interfaces fall back to a global custom group when one exists. Otherwise, they fall back to the network group for their network.

Create a global asset group

Provides instructions for creating a global asset group that applies the same segmentation identity to selected asset interfaces wherever Cyber Vision observes them.

Use a global asset group when the same segmentation identity should apply to selected asset interfaces wherever Cyber Vision observes them.

> **Caution**
>
> Adding an asset interface to a group can change the segmentation identity and permissions that apply to that interface.

Before you begin

Identify the observed asset interfaces that should share the group.

Procedure

1. From the main menu, choose **Segmentation**.
2. Select the **Groups** dashlet.
3. Select **Asset groups**, select **Custom groups**, and then select **Add**.
4. Enter a unique name in **Name**.
5. Enter a description in **Description**, if needed.
6. Optional: Select a value from the **Parent group** drop-down list to filter the interfaces that belong to the selected network group.
7. Find and select the asset interfaces to add to the group from the list of **Available assets**.

   You can search or filter by **Network**, **Asset group**, **Asset type**, or **Vendor**. Review **Current group** before you select an asset interface.
8. Select **Create**.

A new global asset group is added in Cyber Vision Center. The group can be used by rules, recommendations, and simulation wherever Cyber Vision observes its member interfaces.

Switch communications views

Describes the switch communications views that show asset groups, protocols, and traffic observed for a selected switch.

On the **Segmentation** page, select a switch from the list to view the communications data observed on the switch. The **Communications** tab displays the asset groups, protocols, and traffic that Cyber Vision observed for the selected switch.

Communications views

Use this table to choose the communications view that matches what you need to inspect.

Table 28: Communications views

View	Shows	Use it to
Graph	Group relationships in a visual layout.	Understand how observed asset groups relate to each other.
Table	Group-to-group communications, protocols, and packet counts.	Inspect the protocol and traffic details behind the observed relationships.

View	Shows	Use it to
Participating groups	Asset groups observed by the switch or manually added to the switch.	Confirm which groups are available for switch-specific rule review and simulation.

Segmentation recommendations

Defines the recommendation types that Cyber Vision can propose from observed communication and explains how you can respond to each recommendation.

Cyber Vision proposes asset groups or rule changes from observed communication. You can accept, edit, or discard each recommendation.

Recommendation scope

Asset-group recommendations support microsegmentation inside one selected network group at a time. When Cyber Vision analyzes communications across a single switch, it first presents the networks that communicate across that switch. The clustering algorithm considers only assets in the selected network and checks communities using IP addresses that communicate through the switch.

Recommendations are based on observed communications, not inferred device intent. Review each recommendation before you accept it.

Cyber Vision does not need to place every interface in a new group. If it is not clear which child cluster an asset should belong to, Cyber Vision leaves that asset in the parent network group.

Existing grouped assets are not moved out of their groups. Only ungrouped assets can be recommended into existing groups.

Segmentation rules are recommendation at various levels.

Recommendation types and actions

Use this table to compare recommendation types and user responses.

Table 29: Recommendation types

Recommendation type	What you can do
Asset group recommendation	Accept as a global group, accept as a local group, edit the recommendation, or discard it.
New rule recommendation	Create an explicit rule when observed traffic would otherwise match the default rule, or discard the recommendation.
Rule update recommendation	Apply the recommended change to an existing rule, or discard the recommendation to keep the rule unchanged.

You can edit a saved rule at any time.

Create micro-segments from asset-group recommendations

Provides a source-grounded workflow for using asset-group recommendations to divide one network group into smaller logical zones.

Use micro-segmentation recommendations when you want to divide one network group into smaller logical zones before you model rules between groups.

Before you begin

Choose one network group whose observed communication patterns you want to review.

Procedure

1. In **Segmentation**, open the switch context where Cyber Vision observed communication for the network group.
2. Review the communication patterns for the selected network group.
3. Run the asset-group recommendation workflow for the selected network group.
4. Review the recommended clusters as a set.

   Cyber Vision presents the recommendations together and graphically so that you can review the relationships between the proposed groups.
5. Edit, accept, or discard each recommendation.
6. Accept a recommendation as global when the selected asset interfaces should move into a global group everywhere Cyber Vision observes those interfaces.
7. Accept a recommendation as local when the selected asset interfaces should move into a local group only in the selected switch context.
8. Leave unclear asset interfaces in the parent network group.

   Cyber Vision does not need to place every interface in a new micro-segment. Interfaces that do not form a distinct cluster continue to use the network group fallback identity.

Accepted asset-group recommendations create custom asset groups that act as micro-segments inside the selected network group. The new groups can be used by segmentation rules, recommendations, and simulation.

Segmentation rules

Provides lookup details for segmentation rule categories, actions, catch-all behavior, and default rule behavior.

Segmentation rules define permissions between asset groups. Cyber Vision models and simulates rules in Release 5.6.0, but it does not deploy them to switches.

Table 30: Rule categories

Rule category	Purpose
Inter-group rule	Defines permissions between two different asset groups.
Intra-group rule	Defines permissions within the same asset group.
Common service rule	Defines reusable service access between one service group and many subscriber groups.
Default rule	Provides the global baseline when no explicit inter-group or common-service rule applies.

Inter-group rules are unique by group pair. One pair has one shared action and one catch-all behavior, with separate directional protocol lists for each direction.

Segmentation rules table

From the main menu, choose **Segmentation**, and then select the **Segmentation rules** dashlet to manage global rules. Use the **Inter-group rules**, **Intra-group rules**, and **Common service rules** tabs to view each rule category.

Search for rules or filter them by asset group, action, protocol, or catch-all rule. Expand a rule to view the action and protocols configured for each traffic direction.

Table 31: Segmentation rule information

Field	Description
Asset group	Identifies the asset groups to which the rule applies. Inter-group rules display two different groups. Intra-group rules display the same group on both sides.
Action	Shows whether the rule allows or denies traffic that matches a configured protocol.
Protocol	Lists the protocols configured for the rule. Expand the rule to review protocols by traffic direction.
Catch all rule	Shows the action applied to traffic that does not match a configured protocol. Cyber Vision sets this value to the opposite of the configured rule action.
In use	Shows the number of switches associated with the rule. Select the number to open the **Segmentation rule in use summary** and review the switches.

Default rule behavior

The default rule is a single global baseline rule. Its default action is **Allow**, and you can edit the default action at any time.

When observed traffic hits the default rule and you create an override, Cyber Vision creates a new explicit group-pair rule instead of editing the default rule.

Select **Show** next to **Default rule** to display the group-pair rules derived from the default action. Select **Hide default rules** to display only explicit rules.

Use this table to interpret the configured action and protocol rows.

Table 32: Action and catch-all behavior

Configured action	Specific protocols	Any protocol
Allow	Allows the selected protocols and denies all other traffic between the groups.	Allows the listed protocols and denies all other traffic between the groups.
Deny	Denies the selected protocols and allows all other traffic between the groups.	Denies all traffic and locks the catch-all behavior.

Intra-group rules

Introduces how Cyber Vision models traffic inside one asset group in Release 5.6.0.

An intra-group rule defines how Cyber Vision models traffic within one asset group. The traffic uses the same effective SGT on both sides of the relationship.

In Release 5.6.0, Cyber Vision initializes each intra-group rule as an explicit allow-any rule with deny catch-all behavior. This setup permits traffic inside the group because traffic matches the allow-any rule before it reaches the catch-all behavior.

Cyber Vision creates intra-group rules for relevant asset groups. You cannot create additional intra-group rules. You can review and edit an existing rule when you need to model traffic inside a group differently.

Cyber Vision Release 5.6.0 does not generate recommendations for intra-group rules.

Edit an intra-group rule

Edit an existing intra-group rule to control how Cyber Vision models traffic within an asset group.

Edit an intra-group rule to allow or deny selected protocols between members of the same asset group.

Cyber Vision creates intra-group rules for relevant asset groups. You cannot create additional intra-group rules, but you can change the action and protocols of an existing rule.

Before you begin

Identify the asset group and the protocols that you want to allow or deny within the group.

Procedure

1. From the main menu, choose **Segmentation**.
2. Select the **Segmentation rules** dashlet.
3. Select **Intra-group rules**.
4. Open the actions menu for the asset group that you want to configure, and then select **Edit**.
5. Select **Allow** or **Deny** in **Action**.
6. Add or remove protocols for traffic within the asset group.

   Select a predefined protocol, or select **Custom rules** to define a protocol by port or port range.
7. Review the catch-all behavior and generated command preview.
8. Select **Save**.

Cyber Vision updates the intra-group rule. The rule retains the same asset group and uses the updated action and protocols in segmentation simulations.

Add an inter-group rule

Provides instructions for adding an inter-group rule that models traffic between two asset groups.

Use an inter-group rule to define how Cyber Vision models traffic between two asset groups.

Before you begin

Identify the two asset groups, the expected traffic direction, and the protocols that should be allowed or denied.

If the required protocol is not available in the predefined list, identify the transport protocol, port or port range, and optional protocol tag for the custom rule.

Review existing rules first because an inter-group rule is unique for a group pair.

Procedure

1. From the main menu, choose **Segmentation**.
2. Select the **Segmentation rules** dashlet.

3. Select **Inter-group rules**, and then select **Add**.
4. Select the first asset group in **Group A**.
5. Select the second asset group in **Group B**.
6. Select **Allow** or **Deny** in **Action**.
7. Review the **Catch all rule** that applies to traffic between the two groups that does not match a protocol row.
8. Add protocols for the direction from **Group A** to **Group B**, the direction from **Group B** to **Group A**, or both directions.

   Select protocols from the predefined list, or select **Custom rules** to define a protocol by port or port range.
9. To add a custom protocol, select **Add custom rule**, configure the protocol and port values, and then select **Save**.

   Add a protocol tag when you need a recognizable label for the custom protocol.
10. Review the generated command preview.

    Use the inline or side-by-side view to verify how the selected action and directional protocols change the logical configuration.
11. Select **Save**.

Cyber Vision adds the inter-group rule and displays it in the **Inter-group rules** table. The rule can be used in simulations for switches where both groups are relevant.

Edit an inter-group rule

Edit the action or directional protocols of an existing inter-group segmentation rule.

Edit an inter-group rule when you need to change how Cyber Vision models traffic between two asset groups.

An inter-group rule retains its Group A and Group B association. You can change its action and the protocols configured for either traffic direction.

Before you begin

Identify the inter-group rule and the protocols that you want to allow or deny.

Procedure

1. From the main menu, choose **Segmentation**.
2. Select the **Segmentation rules** dashlet.
3. Select **Inter-group rules**.
4. Select the rule that you want to change, and then select **Edit** in the rule details.
5. Select **Allow** or **Deny** in **Action**.
6. Add or remove protocols for either traffic direction.

   Select a predefined protocol, or select **Custom rules** to define a protocol by port or port range.
7. Review the catch-all behavior and generated command preview.
8. Select **Save**.

Cyber Vision updates the inter-group rule and uses the updated action and protocols in segmentation simulations.

Edit the default segmentation rule

Change the action that Cyber Vision applies when no explicit segmentation rule matches traffic between asset groups.

Edit the default rule to allow or deny traffic that does not match an explicit inter-group or common service rule.

The default rule is global. A change to its action affects the modeled behavior for all group pairs that rely on the default rule.

Before you begin

Review the explicit segmentation rules and determine whether unmatched traffic should be allowed or denied.

Procedure

1. From the main menu, choose **Segmentation**.
2. Select the **Segmentation rules** dashlet.
3. On the **Inter-group rules** tab, locate **Default rule**, and then select **Edit**.
4. Select **Allow** or **Deny** in **Action**.
5. Select **Save**.

Cyber Vision updates the default action. Group-pair traffic that does not match an explicit rule uses the updated action in segmentation simulations.

What to do next

Select **Show** next to **Default rule** to review the group-pair rules derived from the updated default action.

Common service rules

Details the common service rule model, including service groups, subscribers, local group subscriptions, and conversion warnings.

Common service rules reduce repeated pair rules for shared services such as DNS, NTP, infrastructure services, and quarantine services. A common service rule connects one service group with many subscriber groups.

Common service groups

A common service group is not a special group type. It is an asset group that has common service rules associated with it.

Common service groups are global.

Local group subscriptions

Local groups cannot themselves be common service groups. A local group can explicitly subscribe to a global common service from the switch. Local groups do not automatically inherit parent or global common-service subscriptions.

After a group is configured as a common service, relationships involving that group are managed through common service rules. Regular inter-group rules are not allowed for common service groups. Converting an existing group into a common service can replace regular rules, which can affect multiple switches.

Add a common service rule

Provides instructions for adding a common service rule when many groups need the same access to one shared service group.

Use a common service rule when many groups need the same access to one shared service group, such as a DNS or NTP server group.

> ⚠ **Caution**
>
> After an asset group is configured for common services, relationships to and from that group are managed through common service rules instead of regular inter-group rules.

Before you begin

Identify the service group, the groups that need access to that service group, and the protocols that should be allowed or denied.

Procedure

1. From the main menu, choose **Segmentation**.
2. Select the **Segmentation rules** dashlet.
3. Select **Common service rules**, and then select **Add**.
4. Select the asset group that provides the shared service in **Select group**.
5. Select **Allow** or **Deny** in **Action**.
6. Add protocols under **Outbound traffic**, **Inbound traffic**, or both.

   Use **Outbound traffic** for traffic that the service group initiates to included groups. Use **Inbound traffic** for traffic that included groups initiate to the service group.
7. Review the **Catch all rule**.

   Groups that are included in the rule use this common service rule. Groups that are not included follow the system-wide default rule.
8. Under **Inclusions**, select the groups that the common service rule applies to.
9. Select **Add**.

Cyber Vision adds the common service rule for the selected service group and included groups.

Switch-specific rules

Describes how the switch-specific segmentation rules view shows the rules associated with asset groups for the selected switch.

On the **Segmentation** page, select a switch from the list to view the segmentation rules relevant to that switch. The **Segmentation rules** tab displays the inter-group and intra-group rules associated with asset groups available on the selected switch.

Common service rules are global rules. Manage them from **Global definitions** > **Segmentation rules** > **Common service rules**.

Use this view to review the rules that apply to the selected switch and whether switch-local behavior differs from global intent. The switch-specific view limits the available asset groups and rules to those that are relevant to the selected switch.

You can add an inter-group rule from the switch-specific view. Cyber Vision limits the **Group A** and **Group B** selections to groups available for that switch.

In the global rules table, select a value in the **In use** column to identify the switches associated with a rule.

Simulate segmentation rule impact

Provides instructions for evaluating observed traffic against the current segmentation model before changing segmentation rules on a device.

Use simulation to evaluate how segmentation rules would allow or deny observed traffic before you change the rules.

Simulation is calculated on traffic observed across all segmentation-enabled switches while showing only asset groups observed on the selected switch.

Procedure

1. On the **Segmentation** page, select a switch.
2. Select the **Simulation** tab.
3. Review observed, denied, and allowed traffic totals.
4. Use **Source**, **Action**, **Protocol**, and **Destination** filters to isolate flows in the sankey chart representation.
5. Inspect high-hit source and destination flows.
6. Select **Reset to default** only when you want to clear simulation filters.

The simulation helps you understand which rules would match the observed communication, the resulting allow or deny action, whether the traffic matched an explicit protocol row or the catch-all behavior, and the switch used for evaluation.