

Cyber Vision New UI

- Cyber Vision New UI, on page 1
- Assets, on page 2
- Vulnerabilities, on page 4
- Communication maps, on page 5
- Asset clustering, on page 8
- Alerts, on page 11
- Syslog notification details for various alert types, on page 15
- Organization hierarchies, on page 16
- Filters, on page 17
- Network definitions, on page 18
- Pcap files, on page 20
- Sensor applications, on page 21
- Use Cases, on page 22

Cyber Vision New UI

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.

Table 1: 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.

Expanded explanation

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 2: Contrast table

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

Assets

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 3: Feature History Table

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 interfaces

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. If multiple interfaces exist, you can change which interface is primary. The asset list shows both the primary and additional interfaces for each asset.

Asset data management

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
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
Filter asset data	Select **Assets** and use one of the these methods to manage the asset table: • Click **Focus** to sort the asset table by **Default**, **Network**, or **Security**. • Access the table settings menu to show or hide columns as needed.

Vulnerabilities

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.

The system detects vulnerabilities when an asset or component matches a rule in the Knowledge Database. These rules come from CERTs, manufacturers, and partner manufacturers (for example, Schneider or Siemens). Vulnerabilities are identified by correlating Knowledge Database rules with normalized asset and component properties.

The Vulnerabilities page lists all identified vulnerabilities and their details, including the CSRS score, CVSS score, and the number of affected assets.

Vulnerability scores

Vulnerability scores are indicative of the potential risk level and impact associated with specific vulnerabilities. Vulnerability scores include these scoring systems:

Cisco Security Risk Score (CSRS)

The CSRS evaluates vulnerabilities beyond technical severity, focusing on how attackers might exploit them. Scores range from 0 to 100 and are based on factors such as existing vulnerabilities, threat intelligence, and the effectiveness of security controls. This score helps prioritize critical vulnerabilities and allocate resources effectively.

Table 4: CSRS categories:

Score	Vulnerability
67–100	High vulnerability
34–66	Medium severity vulnerability
0–33	Low severity vulnerability

Common Vulnerability Scoring System (CVSS)

The CVSS assigns a score out of 10 based on factors like attack complexity, attack vector, and potential impacts. Security teams use CVSS scores to prioritize severe vulnerabilities and strengthen system security.

Table 5: CVSS categories:

Score	Vulnerability
9–10	Critical vulnerability
7–8.9	High severity vulnerability
4–6.9	Medium severity vulnerability
0.1–3.9	Low severity vulnerability

Acknowledge or revert a vulnerability acknowledgement

Mark vulnerabilities as acknowledged, or undo acknowledgement as needed, to manage security alerts effectively.

Use this task when you need to acknowledge vulnerabilities affecting assets, or revert previous acknowledgements in the Cyber Vision Center.

Before you begin

Ensure you have access to the **Assets** or **Vulnerabilities** dashboards.

Procedure

Step 1 From the main menu, choose **Assets**.

Step 2 Select an asset.

Step 3 Select the **Vulnerabilites** tab.

Step 4 Select the relevant **CVE ID** to view vulnerability details.

Step 5 In the **Add/Edit Comment** field, enter a comment as needed.

Step 6 To acknowledge the vulnerability, select **Acknowledge on this asset**.

Step 7 To revert acknowledgement, select **Revert Acknowledgement**.

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

Communication maps

A communication map is a network visualization tool that

- visually displays communication patterns among industrial assets,
- enables filtering and grouping of assets by protocol, network, or functional group, and
- supports investigation by providing details such as observed protocols, data exchange volumes, and source/destination asset information.

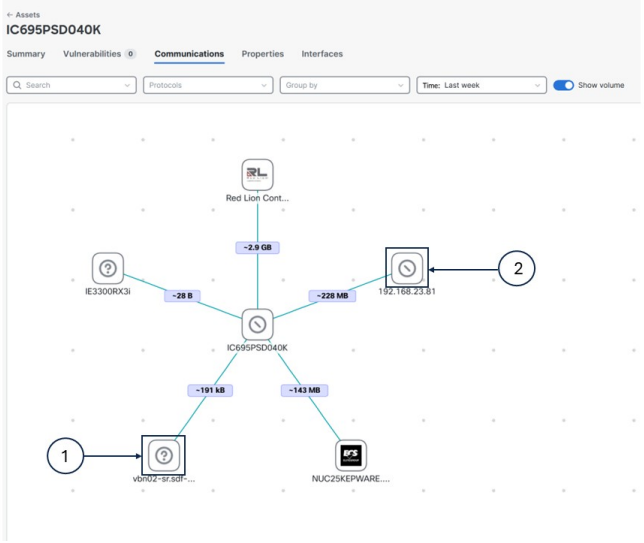
This functionality enables operational technology (OT) and information technology (IT) teams to quickly visualize and understand the communication context of industrial assets. It provides a clear visual reference to abnormal communications and potential risks.

Table 6: Feature History Table

Feature	Release Information	Feature Description
See functional-group centric views of 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 New UI, communication maps now include icons of vendors to help you identify assets more easily.

Additional reference information

- Visualization of asset communications: Use the map to view interactions between a selected asset and other internal assets. Vendor icons, IP addresses or MAC addresses, and communication volumes represent these connections. You can identify devices, vendors, or IPs involved in communications quickly.
- Filter and group communication data:
  - You can filter communications by protocol.
  - You can organize the map by grouping assets according to network (subnet) or functional group. You can expand group nodes to explore individual assets within each group.
  - You can apply a time filter to view communications during specific periods, aiding in the analysis of unusual or suspicious activity.
- The communication map shows each asset’s vendor icon and name. If a name is not available, it shows the asset’s IP address or MAC address.



Callouts	Descriptions
(1)	This icon indicates that no vendor information was assigned to the asset.
(2)	This icon indicates that the vendor is known, but its icon is unavailable.

Assets and functional group communication maps

Asset and functional group communication maps display the interaction pathways and communication details among assets and within functional groups in the system.

Table 7: Types of communication maps

Type	Description
Asset communication map	From the main menu, choose **Assets**, select an asset, and then click **Communications** to access the map. Select a communication link to view details about the observed protocols, exchange volumes, and asset source or destination information.

Type	Description
Functional group communication map	The **Communications** page from the main menu displays how accepted functional groups interact with each other. Click a functional group node to display its internal asset communications." **Note** You need to run asset clustering and accept the functional groups to see the functional group communication maps. See Cluster assets into functional groups.

Asset clustering

An asset cluster is a functional grouping that

- organizes assets based on their real-world network communication patterns,
- distinguishes between Operational Technology (OT) and Information Technology (IT) assets for grouping, and
- is generated automatically through algorithmic analysis.

Table 8: Feature History Table

Feature	Release Information	Feature Description
Receive property-based and communication-based group suggestions from asset clustering algorithm	Release 5.3.x	Asset clustering algorithms suggest property-based groups (assets that share the same definition, network, or other properties), in addition to communication-based groups (assets that primarily communicate with each other).

Additional reference information

Asset clustering simplifies asset management by creating functional groups that reflect actual communication behaviors in a network. The system suggests groupings and identifies assets that can transfer between groups. Asset clustering may suggest new functional groups or indicate when significant assets are excluded from a grouping. The asset clustering result remains stable until communication patterns in the network change.

Asset movement

- Asset clustering helps to identify assets that can move between functional groups, those that can move to an ungrouped list, and ones that can move from the ungrouped list into a group.
- The algorithm recommends which assets to transfer and then provides an updated list of functional groups.

- If you add or remove a sensor, or delete an asset, the algorithm suggests new functional groups based on the latest data.

Types of functional groups

Asset clustering suggests two types of functional groups to help organize your assets:

- Communication-based groups: Consist of OT assets that primarily communicate with each other rather than with the broader network. These groups serve as OT process function groups to align with automation stations.
- Property-based groups: Consist of assets that share common definitions, network attributes, or other properties.

Cluster assets into functional groups

Organize related assets into functional groups for easier management and monitoring.

Use asset clustering to group assets based on function or communication patterns. You can access asset clustering from configuration pages including **Functional Group**, **Sensor Applications**, **Assets**, or from an individual asset's detail page.

Follow these steps to perform asset clustering:

Procedure

Step 1 From the main menu, choose **Configuration** > **Functional Groups**.

Step 2 Click **Start asset clustering**.

The system suggests functional groups in the list.

Step 3 Click the **Functional Group** name to review group details.

Step 4 Click **Map** to view asset communications within the group.

Note
The lightning symbol indicates the most significant asset in the group.

Step 5 Click **Edit Name** to change the **Functional Group** name.

Step 6 Click **Accept** to create the functional group.

The assets are clustered into a new functional group.

What to do next

- Accept or discard the suggested functional groups before you run clustering again.
- If you click **Discard**, the system ungroups the recommended assets and includes them in the next clustering run.

Asset clustering methods

You can perform asset clustering for individual assets, groups, or sensors using several available methods. This table summarizes each method and its description:

Method	Description
For the set of assets	Use asset clustering to analyze a specific set of assets. This method excludes unrelated functional groups from the results. From the main menu, choose **Assets**. Check the checkboxes of the assets, click **More actions**, and select **Run asset clustering**.
For a functional group	Perform focused asset clustering for a specific functional group. Click the functional group name from the **Functional Group** column on the **Assets** page, click **More actions**, and select **Run asset clustering**.
For a sensor	Cluster assets detected by a specific sensor application. This process improves data organization and analysis. Select the sensor applications from **Configuration** > **Sensor Applications** and click **Run asset clustering**.
For an individual asset	Group similar assets by running the asset clustering function for a selected asset. Click the asset name on the **Assets** page, click **Functional group actions**, and select **Run asset clustering**.

Functional group actions and descriptions

Understand the available actions you can perform on functional groups, as well as the effect of each action.

The table lists the functional group actions and their descriptions.

Action	Description
Lock functional group	When you lock the group, it stays out of asset clustering. While locked, no assets can be added or removed from the group during clustering operations. From the **Assets** page, click the functional group name. Click **More actions** and select **Lock Group**.

Action	Description
Move asset from one functional group to another	You can manually adjust your functional group by moving assets between groups. The asset clustering process may not always be able to move assets automatically. From the **Assets** page, check the checkboxes of the assets. Click **More actions** and select **Add selected to group**. Select the functional group from the list and click **Add**.
Delete the functional group	Permanently removes the specified group from the system. Assets in the deleted group are no longer associated with that group. From the **Assets** page, click the functional group name and click **Delete group**.
Remove asset from functional group	Detaches an asset from its current functional group without moving it to another group. Check the checkbox of the asset from the **Assets** page, click the **More actions**, and select **Remove asset from group**. On the **Assets** page, select the checkbox for the asset. Click **More actions** and select **Remove asset from group**.



Note To access the **More actions** field, accept or discard the suggested functional groups.

Alerts

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. You can configure Cyber Vision to forward alerts through Syslog when alerts are raised, cleared, or when their status changes. For details about this configuration, see Enable or disable syslog notifications for an alert type.

You can acknowledge vulnerabilities on assets to clear corresponding alerts from the dashboard or revert acknowledgments to restore alerts.

Table 9: Feature History Table

Feature	Release Information	Feature Description
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.
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.

Additional reference information

- Active alerts: Display all current alerts. An alert remains active while the underlying issue still exists on the affected asset.
- Cleared alerts: When an issue is resolved, the alert appears in the Cleared tab, indicating that it no longer impacts the asset. The system retains cleared alerts for up to 14 days before purging them.
- Default alert types and associated rules:
  - **Severe vulnerabilities in monitored entities**: Monitors specified assets and raises alerts for high-severity vulnerabilities.

    The default rule is **Default_OH_Global**. For this alert type, you can edit, duplicate, delete, or create new rules.
  - **Prohibited vendors**: Triggers alerts for assets linked to prohibited vendors.

    The default rule is **Prohibited_list**. For this alert type, you can only edit rules; you cannot duplicate, delete, or add rules.

Alert details are as follows:

Table 10: Alert details

Name	Description
Alert Type	Types include **Severe vulnerabilities in monitored entities**, and **Prohibited Vendors**.
Trigger	Values based on alert types such as vulnerabilities or vendor names.
Instances	Number of assets impacted by the defined alert rules.
Severity	Severity levels (Critical, High, Medium, or Low).
Triggered By	Alert categories.
Last Detected	Shows last detected date and time.

Alert type management options and permitted alert rule actions

Manage the alerts that are raised for monitored entities and prohibited vendors in your system.

For each alert type, the configuration interface (**Configuration** > **Alerts**) allows control of the alert's state (**Pause** or **Resume**) and management of the associated alert rules that determine when alerts are raised. Use these management actions to maintain security awareness for your organization.

Table 11: Permitted alert rule actions for each alert type

Alert Type	Permitted alert rule actions
Severe vulnerabilities in monitored entities	Create, edit, duplicate, or delete alert rules
Prohibited vendors	Edit alert rules only

Note

- When you pause an alert type, new alerts for its associated rules temporarily stop. This does not affect existing alerts.
- When you resume a paused alert type, new alert notifications for its rules are re-enabled.
- Rule management permissions depend on the alert type:
  - For **Severe vulnerabilities in monitored entities**, all rule management actions are allowed.
  - For **Prohibited vendors**, only rule editing is permitted.

Create alert rules

Add alert rules to monitor asset vulnerabilities and receive timely notifications in the **Alerts** dashboard.

Alert rules in the **Severe vulnerabilities in monitored entities** alert type let you track severe vulnerabilities in assets. When a vulnerability matches a rule, the dashboard shows an alert.

Before you begin

- You cannot create alert rules for the **Prohibited Vendors** alert type.
- The system displays only default alert rules.

Procedure

Step 1 From the main menu, choose **Configuration** > **Alerts**.

Step 2 Select the **Severe vulnerabilities in monitored entities** alert type.

Step 3 Click **Create new rule**.

Step 4 Add an **Alert Rule Name**, then select the **Severity** and **Entity type**.

Step 5 On the **Entity selection** page, select either an organization hierarchy level or functional groups.

- If selecting assets based on functional groups, check **Include Ungrouped assets** to include assets not in any functional group.
- If selecting assets based on organization hierarchy levels, 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 chose in the **Rule name and entity type** step.

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**.

Step 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. The system generates 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 edit, duplicate, or delete actions.

Syslog notification details for various alert types

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

Common syslog message fields

- CEF:0
- vendor: cisco
- product: Cyber Vision
- version: 2.0
- event_class_id: alert_raised or alert_cleared
- event_name: alert type name
- severity id: numeric value based on the severity of the alert rule
- cat: alert category
- SCVAuthorId (optional): User ID if a user manually acknowledged an alert; empty if the system cleared the alert
- alertRuleId: Alert rule UUID
- alertId: Alert UUID
- msg: Value changes based on alert type and event_class_id
- assetId
- assetName
- assetFunctionalGroupId: Empty when the asset is ungrouped
- center-id: UUID of the center
- sensorNames

Table 12: Additional fields for specific alert types

Alert type	Fields
Severe vulnerabilities in monitored entities	• vulnNumber: For example, CVE-2023-10025 • vulnName • vulnCVSSscore • vulnCSRSscore
Prohibited vendors	• vendorName: Listed when the alert involves prohibited vendors

These syslog notification details enable effective monitoring and response to system alerts of various types.

Enable or disable syslog notifications for alert types

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. See Configure syslog.

Procedure

Step 1 From the Cyber Vision New UI, choose **Configuration** > **Alerts**.

Step 2 Select an alert type.

Step 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.

Organization hierarchies

An organization hierarchy is a structural model that

- organizes and groups assets, sensors, and data sources within Cisco Cyber Vision Center,
- uses a system-defined Global level as the root, and
- supports up to five nested sub-levels with configurable options for adding, editing, or deleting levels.

A level is a node in the hierarchy representing a logical grouping, such as a site or zone.

Additional reference information

This hierarchical structure enables users to manage industrial network assets efficiently, customize monitoring views, and streamline oversight.

Key points about organization hierarchies in Cyber Vision Center:

- Each node in the hierarchy is called a level.
- The topmost level is the Global level, which is system-defined.
- The system supports nesting up to five sub-levels; beyond this limit, no additional levels can be added.
- You can add, edit, or delete levels in the hierarchy through **Configuration** > **Organization Hierarchy**. These restrictions apply:

- The Global level cannot be deleted.
- Levels with child levels or assigned entities (such as sensors or PCAPs) cannot be deleted.

Filters

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 13: 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.

Additional reference information

Use filters on Dashboard, Alerts, Assets, Vulnerabilities, and Communications pages. Filtering does not impact configuration pages in Cyber Vision New UI.

Filter views in Cyber Vision New UI

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. Filtering does not affect Configuration pages.

Follow these steps to filter data in Cyber Vision:

Procedure

Step 1 From the main menu, choose **Organization**.

Step 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 the needed items, and click **Apply**.
- Use the search box to find sensors or networks by name.

Step 3 To clear the selected sensors or networks and return to the complete organization hierarchy selection, open the **Organization Hierarchy** drawer again and click the **Reset selection** icon.

Step 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.

Step 5 To refine the filter, click **Edit** on the active view bar.

Step 6 Use the **Select** buttons to add filters as needed.

Step 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 the Dashboard, Alerts, Assets, Vulnerabilities, or Communications pages as needed.

Network definitions

A network definition is a configuration element in Cyber Vision that

- specifies which networks (IP ranges and VLANs) should be monitored,
- allows classification of internal IT and OT assets to improve asset inventory accuracy, and
- enables exclusion or grouping of assets for focused security assessments.

Table 14: Feature History Table

Feature	Release Information	Feature Description
Assign a network to an organization hierarchy	Release 5.3.x	Assign a network to an organization hierarchy level.

Additional reference information

- Cyber Vision preconfigures network definitions with the default RFC1918 addresses 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16.
- Cyber Vision supports three principal network types:
  - OT Internal (PLCs, HMIs)
  - IT Internal (laptops, IT devices)
  - External (assets excluded from inventory)
- Network administrators choose network types and validate IP ranges to avoid duplication.
- In the Classic UI, you can create new network definitions. In the New UI, you can only view and assign existing definitions.

Example

- OT Internal networks may include subnets dedicated to industrial controllers.
- IT Internal networks may include office workstation IP ranges.
- External networks encompass public IP addresses or networks outside the organizational boundary.

Counter example:

- Networks not defined are not monitored and do not appear in the asset inventory.
- External networks are not included in asset classification.

Assign a network to an organization hierarchy

Assign a specific network to a designated level within the organization hierarchy. This action aligns management access and policy controls with the organizational structure.

Perform this task when you need to organize network resources, apply hierarchical policies, or update the organizational assignment for the network.

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

Before you begin

You must have Network Definition permission with read/write access.

Procedure

Step 1 From the main menu, choose **Configuration** > **Network Definition**.
Step 2 Locate the network you want to assign and click **Assign**.
Step 3 Select the appropriate organization hierarchy level.
Step 4 Click **Assign** to complete the assignment.

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

Pcap files

A Packet Capture (PCAP) file is a file format that:

- records raw network traffic data as captured from a network interface,
- preserves the exact communication packets exchanged between various assets, and
- enables network analysis and asset identification when imported into Cyber Vision Center.

Additional reference information:

To analyze traffic from your OT network, upload PCAP files to Cyber Vision. Use the Classic UI to upload PCAP files. For more details, see PCAP Upload.

When you import the file, Cyber Vision creates and identifies assets and associates them with their properties and communication patterns. You can then view these assets throughout the system, including on the main dashboard.

Assign multiple PCAP files to an organization hierarchy

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

Step 1 From the main menu, choose **Configuration** > **PCAPs**.

Step 2 Select the PCAP files you want to assign to an organization hierarchy.

Step 3 Click **Assign Selected to Organization Hierarchy**.

Step 4 Choose the appropriate organization hierarchy.

Step 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.

Sensor applications

A sensor application is an embedded software component that

- runs on Cisco networking devices or runs as a standalone system,
- captures industrial network traffic and performs deep packet inspection to extract relevant information, and
- securely transmits metadata to the center for storage and analytics.

Health Status: Health status describes the operational and enrollment state of a sensor. Key states are:

- New: The sensor's first status after detection by the Center; it is requesting an IP address from the DHCP server.
- Request pending: The sensor has requested a security certificate from the Center and is awaiting enrollment authorization.
- Authorized: The sensor has just been authorized by an administrator or product user and will soon transition to "Enrolled."
- Enrolled: The sensor has completed enrollment, possesses a certificate and private key, and is actively connected to the Center.
- Disconnected: The sensor was previously enrolled but is not currently connected to the Center. Possible reasons include device shutdown, network disruptions, or sensor issues.

Processing Status: Processing status reflects how the sensor processes and communicates data with the Center. Main statuses include:

- Disconnected: The sensor is enrolled but not currently connected to the Center.
- Not enrolled: The sensor is not yet enrolled; typically paired with the "New" or "Request Pending" health status.
- Normally processing: The sensor is connected and actively sending data to the Center for analysis.
- Waiting for data: The Center has processed all received data and is awaiting new data from the sensor.
- Pending data: The sensor is attempting to send data, but the Center is busy processing other incoming data.

Additional reference information

Sensor applications use Cisco's IOx platform to integrate into existing Cisco routers, switches, or purpose-built appliances. Installed sensors appear under the **Configuration** > **Sensor Applications** section of the Cyber Vision New UI. This section provides an overview of each sensor's network device, health, processing status, and organizational hierarchy context

Assign sensors to the Organization Hierarchy

Assign one or more sensors to an Organization Hierarchy to enable asset creation within Cisco Cyber Vision.

Use this task to map sensors in your environment to a defined organization hierarchy. Assignment enables Cisco Cyber Vision to organize asset data and operational context based on organization hierarchy.

Follow these steps to assign sensors to the organization hierarchy:

Procedure

Step 1 From the main menu, choose **Configuration** > **Sensor Applications**.

Step 2 To assign a single sensor, locate the sensor and click **Assign**.

Step 3 To assign multiple sensors, select the checkboxes for each sensor and click **Assign Selected to Organization Hierarchy**.

Step 4 Select the organization hierarchy.

Step 5 Click **Assign** to confirm.

Your selected sensors are assigned to the organization hierarchy. Each assigned sensor is responsible for asset creation in Cisco Cyber Vision.

Use Cases

Filter PLCs by organization hierarchy

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

Step 1 From the main menu, choose **Organization**.

Step 2 Select **Sensors** or **Networks**.

Step 3 Select the organization level.

Step 4 Click **Edit** on the active view bar.

Step 5 Apply the **Asset types** filter for PLCs.

Step 6 Click **Apply**.

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

Acknowledge critical vulnerabilities

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

Step 1 From the main menu, choose **Assets** and click asset name.

Step 2 View the **Vulnerabilities** list for the selected asset.

Step 3 Click the filter icon of the table.

Step 4 Select **Critical** from the drop-down list in the **CVSS Score** column.

Step 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.