

Cyber Vision New UI

- Cyber Vision New UI, on page 1
- Assets, on page 2
- Organization hierarchies, on page 4
- Vulnerabilities, on page 5
- Communication maps, on page 8
- Asset clustering, on page 13
- Alerts, on page 16
- Syslog notification details for various alert types, on page 21
- Filters, on page 23
- Network definitions, on page 25
- Sensor applications, on page 26
- Sensor management frameworks, on page 27
- Use Cases, on page 29

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.

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 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.

Organization hierarchies

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

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.

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.

Feature history table

Vulnerability detection in Cyber Vision Center

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.

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 Cisco Security Risk Score, which is powered by Cisco Vulnerability Management is represented on a scale from 0-100. It quantifies the risk of a vulnerability by looking beyond technical severity to understand how real-world attackers are leveraging the vulnerability in the wild—if at all. A variety of vulnerability and threat variables are considered when calculating this score, 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 much more. Explore Cisco Vulnerability Management and the Cisco Security Risk Score at your own pace through a click-through product demo.

Common Vulnerability Scoring System (CVSS)

The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes. For more information, see https://www.first.org/cvss/.

Vulnerabilities details

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

Table 4: 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
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

Field name	Description	Possible values/examples
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&CK® Tactics	Indicates whether the vulnerability can be associated with specific tactics from the MITRE ATT&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&CK® section. The "3 Tactics matched" (for example) indicator suggests that the system has identified activities corresponding to three different MITRE ATT&CK tactics. Under each tactic, you can find one or more techniques used. For additional details, visit MITRE ATT&CK®.	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 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.

Feature history table

Feature	Release Information	Feature Description
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.

Communication map features

The communication map offers multiple features to view and analyze network communications and subnet details:

You can access the communication map from the **Communications** page in the main menu. The map provides these features:

- Displays all communications between networks
- Shows subnet details for each map node

Table 5: Communication map features

Feature	Feature
Time filter	• Use the time filter to focus on communications during specific periods for trend or activity analysis. • The **Last week** filter is enabled by default.
Protocol filter	• The protocol filter lists all protocols used. • By default, all protocols are visible. However, **Traffic-heavy Protocols** are deselected to improve clarity. You can select them manually to display their data.
Show unknown (L2 Network)	Displays subnets that contain only MAC addresses without IP addresses.
Allow node rearrangement	Lets you rearrange nodes on the map for clarity. Rearrangements are temporary and are not saved after you leave the view.

Asset communication map features

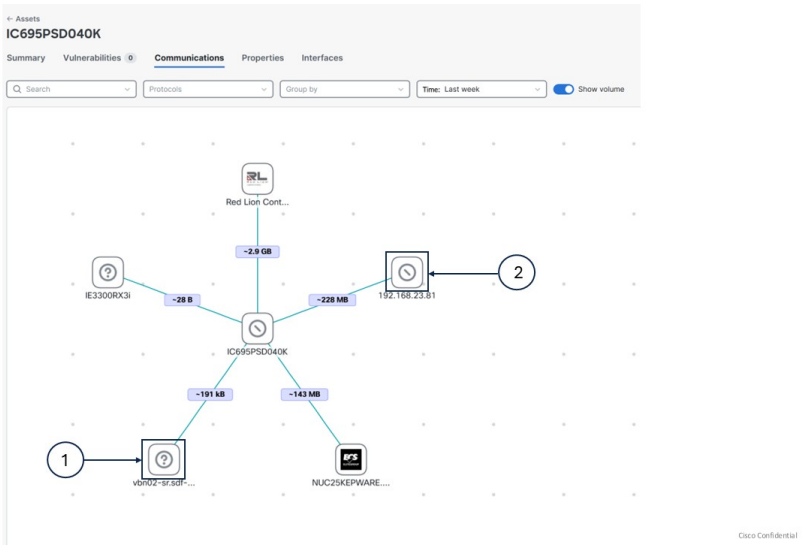
The asset communication map shows all communications between a selected asset and other individual assets in your environment. It provides a detailed view of communication patterns, offers several useful filters, and supports multiple identification methods to help you analyze network communications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

Table 6: 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 week** filter is enabled by default.

Feature	Description
Group communications	• You can group assets by **Network** (subnet) or **Functional Group** to organize the map. **Note** Before organizing, accept functional groups and define network groups. • 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.
Protocol filter	• Lists all protocols used between assets. • All protocols appear by default, but **Traffic-Heavy Protocols** are deselected to improve clarity.
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.

External communications 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 Classic UI.
- If no external networks are defined (in the Classic UI under **Admin** > **Network Organization**), any communication not assigned to an **IT Internal** or **OT Internal** network counts as external communication.

View external communications for an 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

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

Step 2 Click your asset that has external communications.

Step 3 Open the **Communications** tab for the selected asset..

Note
In the map view, external communications are grouped under the **All external communications** icon.

Step 4 To display the list of external communications with detailed information, choose one of these options:

- Click the **All external communications** icon on the communications map.
- Switch to the **List** view.

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

Asset clustering

Asset clustering 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.

Asset clustering simplifies asset management by creating groups that reflect actual communication behaviors in a network. The system suggests groupings, identifies transferable assets, and maintains cluster stability until network patterns change.

Table 7: 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).

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.

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. This process improves data organization and analysis. Select the sensors from **Configuration** > **Sensor Management** > **Sensors** and select **Run asset clustering** from **More actions** tab.
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. 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.

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

Table 8: Feature History Table

Feature	Release Information	Feature Description
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.
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

Monitor and secure your assets using the alert types provided by Cyber Vision Center. Each alert type helps you identify vulnerabilities or unusual activity with specific rules. To access alert types, from the main menu 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**.
Prohibited vendors	• Cyber Vision triggers alerts when your assets are linked to prohibited vendors. • The default rule for this alert type is **Prohibited_list**.

Alert stages and key attributes

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

Alert stages

You can monitor alerts as they move through distinct stages:

- **Active**: Displays current unresolved alerts. Alerts stay active while the underlying problem exists.
- **Muted**: When you mute alert instances related to the prohibited vendors alert type, 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** 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	The values depend on the alert type. For example, they may indicate vulnerabilities or specific vendor names.

Name	Description
Instances	The number of assets impacted by the alert rule.
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.

Alert type management options and allowed rule actions for each alert type

Alert type management options and permitted actions help you manage alerts for monitored entities and prohibited vendors.

Alert type management options include:

- You can **Pause** or **Resume** all alert types, from **Configuration** > **Alerts**.
- Pause an alert type to temporarily stop new alerts. This action does not affect existing alerts.
- Resume to re-enable new alert notifications.
- You can enable **Syslog Notification** for any alert type to send generated alerts to the Syslog server.

Table 9: 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.

Use these options to manage alert rules and maintain oversight for different alert types in your organization.

Create alert rules for severe vulnerabilities in monitored entities

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

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

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 Enter an **Alert Rule Name**, select the **Severity** and **Entity type**.

Entity types:

- **Functional Groups**: Triggers alerts for assets associated with functional groups.
- **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.

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

- If you select assets based on functional groups, check **Include Ungrouped assets** to include assets not in any functional group.
- 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.

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. 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.

Mute alert instances

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**, 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

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

Step 2 On the **Active** tab, find the relevant alert type and click the alert **Instances** count.

Step 3 Select the alert instances you want to mute.

Step 4 Click **Mute**.

Step 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.

Step 6 (Optional) Add a comment.

Step 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.

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 10: 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.

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 11: 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.

Feature	Release Information	Feature Description
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

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.

Use 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 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.

Step 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.

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 your 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 Dashboard, Alerts, Assets, Vulnerabilities, or Communications pages.

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 12: 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.

Network definition details

- Cyber Vision includes network definitions preconfigured with the default RFC1918 addresses: 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16.
- By default, all assets detected through PCAP analysis or sensors are grouped into a single network. To improve asset accuracy and relevance, assign network definitions to one of three network types:
  - **OT Internal** ((for devices such as PLCs and HMIs))
  - **IT Internal** (for laptops and other IT assets)
  - **External** (for assets that are 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.

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.

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.

Sensor applications use Cisco’s IOx platform (IOx is Cisco's software framework) to integrate into existing Cisco routers, switches, or purpose-built appliances.

Sensor health and processing states

You can view all installed sensors in the **Configuration** > **Sensor Applications** section of the Cyber Vision New UI. Use this section to understand each sensor’s network device, health status, and processing status.

Health status

The table describes each operational lifecycle step of the sensor and the impact on connectivity and management requirements.

Status	Description
New	The first status of the sensor after detection by the Center. The sensor 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.

Status	Description
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. This may occur due to device shutdown, network disruptions, or sensor issues.

Processing status

The table provides information about the communication state of the sensor and data flow with the Center.

Status	Description
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.

Sensor management frameworks

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.
- Sensors page management: The sensors page allows you to manage sensors and view sensor statistics, operations, and details for each deployed sensor.

Feature history table

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 automate sensor deployment through the Sensor Management Extension, which pushes applications to the host platform, or perform it manually. You can manage multiple sensors concurrently across the network.

Sensor actions

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.
Run Asset Clustering	Cluster assets detected by a sensor to improve data organization and analysis. See Asset clustering methods.
Change GPS Location	Manually update the GPS coordinates of the sensor to reflect its location.
Uninstall	Remove the sensor from the list and uninstall the application from IOx.

Host actions

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 enough disk space is available before you deploy sensors.
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.

Assign sensors to the Organization Hierarchy

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

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

Step 2 Check the checkboxes of the sensors.

Step 3 Select **Assign to Organization Hierarchy** from the **More actions** list.

Step 4 Select the organization hierarchy you want to assign the sensors to.

Step 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.

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.