Cisco Cyber Vision Beta Version

Introduction of the Cisco Cyber Vision Beta Version

Cisco Cyber Vision Center offers a beta UI experience, with informative, easy-to-handle dashboards that present data on assets, vulnerabilities, alerts, and organization hierarchies. You can quickly apply data filters to view necessary information.

The UI experience is a beta feature. To access the beta UI and its features, write to cv-beta@cisco.com and follow all the instructions provided in the reply. This access allows you to enable the Cisco Cyber Vision Beta UI alongside the existing classic UI.

To access the beta user interface, click **Go to Cyber Vision beta** at the top right corner of the main page. A **GO TO CYBER VISION BETA** pop-up will appear. Click **Go to Cyber Vision beta** again.

Purpose

The Cyber Vision Sensor performs the following roles:

- **Collects Industrial Network Traffic**: The Cisco Cyber Vision Sensor captures industrial network flows (passive) and queries devices (active). If the server is not accessible, it stores data locally.
- **Decodes Common Industrial Protocols**: The Cisco Cyber Vision Sensor decodes most OT and IT communication protocols to analyze packet payloads and extract meaningful information.
- **Sends Metadata to the Cyber Vision Server**: The sensor sends metadata to the server for storage, analysis, and visualization. This only adds three to five percent extra traffic to the network.

Dashboard for the New UI

The **Dashboard** appears when you log into beta version of **Cyber Vision Service**. The two dashlets, **Assets** and **Vulnerabilities**, are shown in the middle panel of the dashboard. Each number is hyperlinked to specific information. The Assets or Vulnerabilities interface appears depending on your selection. Hover over the "i" icon near either topic for definitions of terms, vulnerability categories, and value ranges.

The Vulnerabilities are categorized in the following ranges:

Rating	CVSS Score
Critical	9.0 - 10
High	7.0 - 8.9
Medium	4.0 - 6.9
Low	0.1 - 3.9

The Dashboard includes an additional Trend chart: the **Highlighted Vulnerabilities**. It shows the top five vulnerabilities.

Filter the **Highlighted Vulnerabilities** by **Affected Assets** or **CVSS Score**. The filter is available at the top right corner of the **Highlighted Vulnerabilities** field. The selection appears in the **Highlighted Vulnerabilities** table once sorted. Click any hyperlink in this panel for more information. The **CVSS Score** is the default option. You can change it to **Affected Assets** in your preferred browser. Navigate to other pages, return to the **Dashboard**, or log out and log back in using the same browser, and your settings will be retained. The vulnerability hyperlinks lead you to a new interface, which provides **Details** and **Affected Assets** information for each listed vulnerability.

Active View

The new UI provides a filter functionality called **Active View**.The **Active View** filter is available on the **Dashboard**, **Asset Visibility**, and **Alerts** pages. After you apply the filter to one page, the same data reflects on the other two pages.

There are three different ways to filter data:

- **Organization Hierarchy**: Use this field to filter the data according to **Organization Hierarchy** and its sub levels.
- **Data sources**: Use this field to filter the data according to **Data sources.**
- **Functional Group**: Use this field to filter the data according to **Functional Group**.

Filter the Data in Active View

To filter the data in **Active View**:

Procedure

Step 1 From the main menu, choose **Dashboard, Asset Visibility**, or **Alerts > Active View**.

Step 2 Click the drop-down arrow of the first filter, and check the checkboxes to select **Organization Hierarchy** and its sub-levels.

Step 3 Click the drop-down arrow of the second filter, and check the checkbox to select **Data sources**.

Step 4 Click the drop-down arrow of the third filter, and check the checkbox to select **Functional Group**.

Step 5 Click **Apply Changes**.

What to do next

After applying changes in the **Active View**, the same view becomes available on the **Dashboard**, **Asset Visibility**, and **Alerts** pages, and the assets, vulnerabilities, and alerts data are filtered accordingly.

Asset Visibility

The **Asset Visibility** tab is available in the new beta UI. The left panel displays the **Asset Visibility** function.

The **Asset Visibility** page displays two dashlets—**Assets** and **Vulnerabilities**—in the middle panel, with each number hyperlinked to specific information. The page also shows an asset list in table format and includes the **Active View** filter functionality.

Asset list

Asset Selection

From the main menu, choose **Asset Visibility**. Select the assets using the following methods:

- **To select a few assets**:
  - Check the checkbox to select a few assets one by one.
- **To select a range of assets currently on the screen**
  - To add or reduce the number of assets per page, click the drop-down arrow of **Show Records** at the bottom right of the screen.
  - Select the main checkbox at the top of the checkbox column.
- **To select all assets currently on the screen**:
  - Select the main checkbox at the top of the checkbox column.

Table Setting

Procedure

Step 1 From the main menu, choose **Asset Visibility**.

Step 2 Click the **Settings** icon at the top right of the table.

The **Table Settings** pop-up appears.

Step 3 Click **Edit Table Columns**.

Step 4 Enable the toggle switch for required fields.

Step 5 Click **Apply**.

Step 6 To display previous **Table Settings**, click **Reset All Settings**.

Asset Deletion

The system automatically deletes assets removed from the production line after 30 days. However, if the sensor or network definition is not properly configured and it detects assets not intended to be monitored by Cisco Cyber Vision, you can use the delete asset feature to remove the unnecessary assets after fixing the configuration.

To delete an asset, follow these steps:

Procedure

Step 1 From the main menu, choose **Asset Visibility**.

Step 2 Select the checkboxes of all the assets that need to be deleted.

Step 3 Click **Delete**.

A warning pop-up appears.

Step 4 Click **Delete**.

Note
An asset can reappear if sensors detect it again.

Asset Summary

An asset is a physical machine of the industrial network such as a switch, an engineering station, a controller, a PC, a server, and so on. In the UI, a single asset icon can represent multiple physical assets or multiple components. The graphic interface complies with the logic of management and inventory, focusing on users' needs. Technically, an asset is an aggregation of components with similar properties. These components share the same characteristics, such as IP address, MAC address, NetBIOS name. The aggregation of components into an asset and the definition of the asset type are based on a set of rules defined within the system.

Asset Vulnerability List

Vulnerabilities are weaknesses detected on assets that potential attackers can exploit to perform malevolent actions on the network.

Vulnerabilities are detected in Cisco Cyber Vision through rules stored in the Knowledge Database. These rules are sourced from several CERTs (Computer Emergency Response Teams), manufacturers, and partner manufacturers (such as Schneider or Siemens). Technically, vulnerabilities are generated from the correlation of the Knowledge Database rules and normalized asset and component properties. A vulnerability is detected when an asset or a component matches a Knowledge Database rule.

Vulnerability List

There are two ways to browse vulnerabilities:

Overlay Vulnerability Details: From the main menu, choose **Asset Visibility** > **Vulnerabilities**. The vulnerability list appears. It shows details such as **CVE ID**, **CVSS Score**, and the number of **Affected Assets**.

Overlay Affected Assets: Use the **Vulnerabilities** tab for a specific asset to view details related to that asset. From the main menu, choose **Asset Visibility**. Click the asset name in the **Name** column and click **Vulnerabilities**. The **Vulnerabilities** field gives the following details:

- A list of **Active Alerts**
- A list of **CVE ID**
- **Name**
- **CVSS Score**
- **Action**: You can acknowledge a vulnerability to stop alerts.

Asset Vulnerability

To measure the severity of a vulnerability, Common Vulnerability and Exposure (CVE) entries are often assigned a CVSS (Common Vulnerability Scoring System) score. The CVSS score provides a numerical evaluation, out of 10, of the overall threat raised by the presence of a given vulnerability on a computer system. The base CVSS score is computed by considering aspects such as the complexity of the attack needed to exploit the vulnerability, the attack vector (local or through a network), and the possible impacts of an exploitation on the system. Security teams use CVSS scores as part of their vulnerability management program to prioritize severe vulnerabilities and improve the security posture of computer systems. While CVSS is currently on version 3.1, version 2 is still widely used. Both versions are supported by Cisco Cyber Vision.

CVSS scores are divided into the following four 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

To see information about all vulnerabilities:

- From the main menu, choose **Dashboard** > **Vulnerabilities**.
- Hover over the "i" icon given beside the **Vulnerabilities**. Pop-up shows the **CVSS Score** ranges.

Vulnerability Acknowledgment

You can acknowledge a vulnerability to stop alerts.

Procedure

Step 1 From the main menu, choose **Asset Visibility**.
Step 2 Click the asset name from the **Name** column.
Step 3 Click **Vulnerabilities**.
Step 4 Click **Acknowledge** to acknowledge the vulnerability.

A sidebar will appear.

Step 5 **Add/Edit comment** in the box.
Step 6 Click **Acknowledge on this asset**.

Cancel a Vulnerability Acknowledgment

Procedure

Step 1 From the main menu, choose **Asset Visibility**.
Step 2 Click the asset name in the **Name** column.
Step 3 Click **Vulnerabilities** and locate the acknowledged vulnerability that needs to be canceled.
Step 4 Click **Acknowledged** to cancel the vulnerability acknowledgment.

A sidebar will appear.

Step 5 **Add/Edit comment** in the box.
Step 6 Click **Un-acknowledge**.

Primary Interface

Assets are composed of properties gathered from the network, including MAC and IP addresses. For each asset, the system lists the collected MAC and IP addresses and indicates whether a MAC address is associated with an IP address. The Interfaces section shows the collected MAC, MAC+IP, or IP addresses, representing the various interfaces of a single asset. Additionally, the system selects a primary interface for use in different visualizations within the product.

Note The user can change the primary interface.

To see the **Primary Interface**:

- From the main menu, choose **Asset Visibility.**
- Click the asset name from the **Name** column.
- Click **Interfaces**. The selected interface will appear in the **Asset Visibility** and its **Summary** page.

Properties

The Properties tab lists all the different properties collected from the network for an asset, organized by protocol.

To see **Properties**:

- From the main menu, choose **Asset Visibility.**
- Click the asset name in the **Name** column.
- Click **Properties**.

Communications (Mini Map)

The communications map shows the different communications of a given asset. It helps users assess its internal communications. The map displays all communications with other internal assets. Users can filter by protocol to see specific communications. Selecting a communication opens a side panel with details, such as observed protocols and exchange volumes, and provides information about the source or destination asset.

To see **Communications**:

- From the main menu, choose **Asset Visibility.**
- Click the asset name in the **Name** column.
- Click **Communications**.

Asset Clustering

Cisco Cyber Vision provides this new functionality in the new UI.

Manual asset grouping based on network definitions and their communications is a difficult task. Asset clustering simplifies this by organizing assets into functional groups based on their network communication patterns. Only assets that are not already assigned to a functional group will be considered. The system runs an algorithm to extract and preprocess data, perform data modeling and analysis, identify functional groups, and consolidate the results. It then suggests a list of groups.

Procedure

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

Step 2 Click**Start**.

The system shows the number of ungrouped assets and suggests a list of **Functional Groups**.

Step 3 To review, click **Functional Group** name.

Step 4 To change the **Functional Group** name, click **Edit Name**.

Step 5 Click **Accept**.

The functional group is created.

Note
When you click **Discard**, the recommended assets ungroup and are included in the next run.

Step 6 To see all the functional groups.

a) From the main menu, choose **Dashboard/Asset Visibility/Alerts**.
b) In the **Active View** area, click the drop-down arrow of **Functional Groups**.

The drop-down list will include the groups that were accepted in **Step 5**.

The system may suggest adding new assignments to the functional group. If you reevaluate the group, the system will suggest changes.

Delete the Functional Group

Procedure

Step 1 From the main menu, choose **Asset Visibility**.

Step 2 Click the group name from the **Functional Group** column.

The **View Functional Group** side panel appears.

Step 3 Click **Delete group**.

The **Delete Group** window appears.

Step 4 Click **Delete**.

Remove Asset from Functional Group

The **Remove from Group** option is disabled if any groups are pending in the recommendations. You must either accept or discard all groups to enable this feature.

To remove asset from functional group:

Procedure

Step 1 From the main menu, choose **Asset Visibility**.

Step 2 Check the checkbox to select the asset name in the **Name** column.

Step 3 Click **Remove from group**.

The **Remove From Group** pop-up appears with a note.

Step 4 Click **Remove**.

Alerts

The **Alerts** feature has a separate dashboard page in the new Cisco Cyber Vision user interface. The left panel presents the **Alerts** tab. It has **Active View** filter functionality so that the data can be filtered as per requirement. Additionally, it displays the following alert type details:

Alert Type: It shows the name of the alert type.

24h Count: It shows the number of active alerts detected in the last 24 hours.

Total Count: It displays the total number of active alerts.

Last Alert Detected: It displays the date and time of the last alert.

Action: It allows you to **Pause** or **Resume** the **Alert Type**.

Alerts are used to monitor anomalies. By default, the system includes one alert type: **Critical vulnerabilities in monitored entities**. This alert monitors vulnerabilities on assets and cannot be edited. However, you can add or edit alert rules within this alert type based on specific vulnerabilities.

The alert type, **Critical vulnerabilities in monitored entities**, has a default alert rule called **Global_OH_Critical**, which comes with the application. It monitors all vulnerabilities with a CVSS score above a set threshold of 9, impacting all assets. You can delete this alert rule if it is not required. You can edit parameters like the CVSS Score Threshold. The entity type is pre-selected and non-editable, but organization hierarchy levels can be changed. When a vulnerability matches the alert rule criteria, users will see the alerts on the Alerts tab.

Add New Alert Rule

You can add alert rules to monitor asset vulnerabilities. Adding an alert rule will affect the alert count displayed on the **Alerts** page.

Procedure

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

Step 2 Locate the alert type and click its name.

The side panel appears.

Step 3 Click **Add new rule**.

The **Add Alert Rule** panel appears.

Step 4 Add **Alert Rule Name**.

Step 5 Add **CVSS Score Threshold**.

Note

Enter a **CVSS Score Threshold** number between 7 and 10.

Step 6 Click the radio button to select an **Entity Type**.

Two entity types are available for selection. It depends on how you want to monitor your network:

a) Click **Organization Hierarchy**.

Check the checkbox for the Organizational level.

To monitor assets without data sources, check the checkbox for **Asset seen by unknown data sources**.

b) Click **Functional Groups**.

Check the checkbox to choose one or more functional groups.

To monitor assets not part of any functional group, check the checkbox for **Assets that are not part of any functional group**.

Step 7 Click **Save**.

Edit Alert Rule

You can edit alert rules to monitor asset vulnerabilities. Editing an alert rule will change the alert count displayed on the **Alerts** page.

Procedure

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

Step 2 Locate the alert type and click its name.

The side panel appears.

Step 3 Locate the alert rule and click the ellipsis (…) in the **Actions** column.

Step 4 Click **Edit**.

Change the required details.

Step 5 Click **Save**.

Delete Alert Rule

You can delete alert rules if not required. Deleting an alert rule will reduce the alert count displayed on the **Alerts** page.

Procedure

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

Step 2 Locate the alert type and click its name.

The side panel appears.

Step 3 Locate the alert rule and click the ellipsis (…) in the **Actions** column.

Step 4 Click **Delete**.

A warning pop-up appears.

Step 5 Click **Delete**.

Acknowledge Vulnerability on the Assets

Acknowledge a vulnerability to stop receiving alerts. When you acknowledge a vulnerability on an asset, the corresponding alerts are cleared, and it reduces the alert count displayed on the **Alerts** page.

Procedure

Step 1 From the main menu, choose **Asset Visibility**.

Step 2 Click the asset name that has alerts.

Step 3 Click **Vulnerabilities**.

Step 4 Click the filter icon from the top right corner of the table.

Step 5 Click the drop-down arrow of the **Active Alerts** column.

Step 6 Select **Yes** from the drop-down list.

Vulnerabilities with active alerts appear.

Step 7 Click **Acknowledge**.

A side panel will appear with details of the vulnerability.

Step 8 Add a comment in the **Add/Edit Comment** field.

Step 9 To acknowledge the vulnerability, click **Acknowledge on this asset**.

Note
Deleting an asset from the **Asset Visibility** page clears all alerts related to that asset from the system.

Pause Alert Type

You can pause an alert type to temporarily stop new alerts from being generated for all alert rules within that type. Previously generated alerts remain unaffected.

Procedure

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

Step 2 Locate alert type.

Step 3 Click **Pause** from **Actions** column.

A warning pop-up appears.

Step 4 Click **Yes**.

Resume Alert Type

Resuming the paused alert type will generate new alerts for all active alert rules.

Procedure

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

Step 2 Locate alert type.

Step 3 Click **Resume** from **Actions** column.

A warning pop-up appears.

Step 4 Click **Yes**.

Configuration

Organization Hierarchy

The organization Hierarchy represents a hierarchical structure of levels that allows for the logical grouping of entities. Each node in the hierarchy is referred to as a level. **Global** is the root level of the hierarchy. The application supports nesting up to ten sub-levels. Once you reach this limit, you cannot add more levels, as it is the system-defined nesting limit.

Create Organization Hierarchy

Procedure

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

Step 2 Locate the level in the table where you need to add a sub-level and click the ellipsis (…) under the **Action** column.

Step 3 From the drop-down list, choose **Add Level**.

Step 4 Enter the **Level Name**.

Step 5 Click **Add**.

Note
Admin must define all the organization hierarchies in the organization.

Edit Organization Hierarchy

Note The Global level does not have an edit option because it is a system-defined level.

Procedure

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

Step 2 Locate the level in the table that you need to edit and click the ellipsis (…) under the **Action** column.

Step 3 From the drop-down list, choose **Edit**.

The **Edit Level** pop-up appears.

Step 4 Edit the **Level Name**.

Note
You can only edit the name of the **Organization Hierarchy**.

Step 5 Click **Save**.

After saving, the changes to the organization hierarchy will be applied to the child levels.

Delete Organization Hierarchy

Note Global does not have a delete option because that is a system-defined level.

Note The delete option does not appear for the level if:

- The level has child levels.
- The level has a non-zero count. This means that entities, such as sensors or PCAPs, are assigned to it.

Procedure

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

Step 2 Locate the level in the table that you need to delete and click the ellipsis (…) under the **Action** column.

Step 3 From the drop-down list, choose **Delete**.

A warning appears.

Step 4 Click **Delete**.

Network Definition

To provide an accurate asset inventory and security posture assessment of your network, Cyber Vision must know which networks you want to monitor. By defining the internal IT and OT networks of your organization, you can specify the IP addresses and VLANs of your networks, thereby making the data more relevant. Cisco provides default network configurations based on RFC1918 addresses. We ship the product with default private network (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16).

The Cyber Vision Service treats all assets seen via PCAP analysis or through sensors as part of the same "network." This can lead to inaccuracies in aggregating components into physical assets or inundate you with data about assets you may not care about. Cyber Vision solves this by allowing you to define your network into the following three types:

- **OT Internal**: Assets such as PLCs or HMIs.
- **IT Internal**: Assets such as laptops and other IT-related items.
- **External**: Cyber Vision will not store assets found in this type of network and will remove them from the asset inventory.

Note The network administrator will know what type of networks you will need. They will choose the network type and check for duplicate IP ranges.

Important The network definitions are created in the Classic UI. In the new Beta UI, you can only view these definitions but cannot create or modify them.

Cyber Vision automatically defines the OT Internal network as the RFC1918 (IPv4) or RFC 4193 (IPv6) subnets, and External networks as everything else. You can edit or delete these and add your own customizable network definitions.

To define a subnetwork, use the classic UI. See Define a subnetwork.

To see all the added networks, from the main menu choose **Configuration** > **Network Definition**. The **Network Definition** page shows the total number of networks categorized into three types: **IT**, **OT**, and **External**.

PCAP

Cyber Vision allows you to upload Packet Capture (PCAP) data that captures network traffic from your OT network. You can import PCAP files to **Cisco Cyber Vision**.

A **PCAP** file captures communication packets between various assets. When imported into Cisco Cyber Vision, the assets are identified and created with their respective properties and communication patterns. Once created, assets appear not only on the dashboard but across the system on all pages.

To upload PCAP, use the classic UI. See PCAP Upload.

Important PCAP files are imported using the Classic UI. In the Beta UI, you can only view the PCAP files that have already been uploaded.

Uploaded PCAPs appear in **Configuration** > **PCAPs**.

To assign multiple PCAP files to the Organization Hierarchy, follow these steps:

Procedure

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

Step 2 Click **Assign** at the end of the row for the PCAP file you need to assign.

a) To assign multiple PCAP files to the Organization Hierarchy, follow these steps:

1. Check the checkboxes of the desired PCAP files.
2. Click **Assign Selected to Organization Hierarchy**.

Step 3 Choose the **Organization Hierarchy**.

Step 4 Click **Assign**.

Note
Each PCAP is responsible for Asset creation in **Cisco Cyber Vision**.

Sensor Applications

Cyber Vision Sensors capture network traffic and perform Deep Packet Inspection of industrial protocols to extract information. They send metadata to the center for storage and analytics. The sensor software is embedded into Cisco networking equipment as an IOx application. Sensors integrate into existing Cisco network devices such as routers and switches or can be deployed as standalone devices.

The **Sensor Applications** interface shows the **Network Device Name, Health Status, Processing Status**, and **Organization Hierarchy**.

Health status:

- **New**

  This is the sensor's first status when it is detected by the Center. The sensor is asking the DHCP server for an IP address.

- **Request Pending**

  The sensor has asked the Center for a certificate and is waiting for the authorization to be enrolled.

- **Authorized**

  The sensor has just been authorized by the Admin or the Product user. The sensor remains as "Authorized" for only a few seconds before displaying as "Enrolled".

- **Enrolled**

  The sensor has successfully connected with the Center. It has a certificate and a private key.

- **Disconnected**

  The sensor is enrolled but isn't connected to the Center. The sensor may be shut down, encountering a problem, or there is a problem on the network.

Processing status:

- **Disconnected**

  The sensor is enrolled but isn't connected to the Center. The sensor may be shut down, encountering a problem, or there is a problem on the network.

- **Not enrolled**

  The sensor is not enrolled. The health status is New or Request Pending. The user must enroll the sensor for it to operate.

- **Normally processing**

  The sensor is connected to the Center. Data are being sent and processed by the Center.

- **Waiting for data**

  The sensor is connected to the Center. The Center has treated all data sent by the sensor and is waiting for more data.

- **Pending data**

  The sensor is connected to the Center. The sensor is trying to send data to the Center but the Center is busy with other data treatment.

Installed sensors appear under **Configuration** > **Sensor Applications**.

Assign the Sensor to the Organization Hierarchy

To assign the sensor to the Organization Hierarchy, follow these steps:

Procedure

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

Step 2 Click **Assign** at the end of the network device row that needs assignment.

a) To assign the multiple sensors to Organization Hierarchy, follow these steps:

1. Check the checkboxes of the desired sensors.
2. Click **Assign Selected to Organization Hierarchy**.

Step 3 Choose the **Organization Hierarchy**.

Step 4 Click **Assign**.

Note
Each sensor is responsible for asset creation in Cisco Cyber Vision.

Use Cases

Review All PLC and SCADA Data Servers in the Paint Shop

Procedure

Step 1 Organize Network in the Old UI.

a) Define a network within the Network Organization section.

b) Ensure that the network includes the subnet for both the PLC and SCADA network.

For example, use the subnet 192.168.41.0/24.

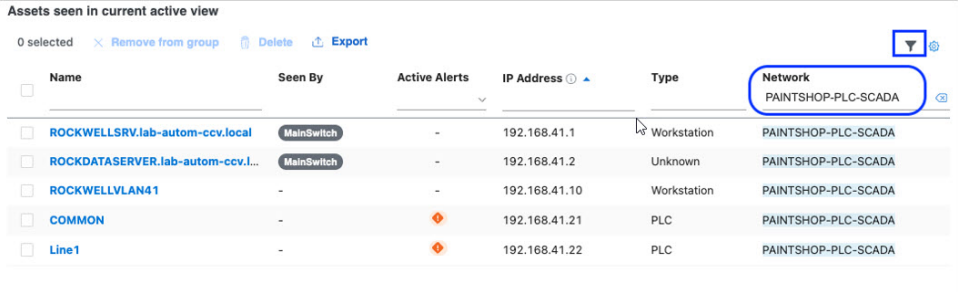
Step 2 From the main menu, choose **Asset Visibility**.

Step 3 Click the filter icon at the top-right corner of the table.

Step 4 To filter the asset list, search for the network name in the **Network** column.

Review the different assets in the paint shop.

Note
Users cannot edit the network definition information in the new UI.



Step 5 To see the details of the assets, click the asset name.

Analyze and Acknowledge All Vulnerabilities with a CVSS Score Above Nine

Users can review vulnerabilities through either the vulnerability list for each asset or the comprehensive list of vulnerabilities. Both lists include a filter to display specific CVSS scores.

Procedure

Step 1 From the main menu, choose **Asset Visibility**.

Step 2 Click the asset **Name**.

Step 3 Click **Vulnerabilities**.

Step 4 Click the filter icon at the top right corner of the table.

Step 5 Click the drop-down arrow of the **CVSS Score** column.

Step 6 Select **Critical** from the drop-down list.

This will show vulnerabilities with a CVSS score between 9.0 and 10.

Step 7 To acknowledge the vulnerability, click **Acknowledge**.

Acknowledging the vulnerability will hide it from dashboard counters, clear alerts, and make filtering easier.