Cisco Cyber Vision Administration Guide, Release 5.1.x

First Published: 2024-09-20

CONTENTS

CHAPTER 5   **Configure Cisco Cyber Vision** **83**

New and Changed Information

- New and Changed Information, on page 1

New and Changed Information

Features of Cisco Cyber Vision Release 5.1.x are as follows:

Feature	Description
Device inventory report	The Device Inventory Report is an automated summary that captures data related to devices, their risk profiles, and the inventory distribution summary for a chosen preset. See Create a Report.
Zone and conduit visualization	Cisco Cyber Vision limits the number of displayed objects to maintain performance and prevent browser issues. You can now view only top-level groups (zones) and summarized activities (conduits). The new map feature aligns zones and conduits with ISA/IEC 62443 standards. See Zones (Groups) and Conduits (Summarized Activities).
Monitor ingestion chain follow-up	The service status page shows whether all Cisco Cyber Vision processes and extensions are running smoothly, and ensures that the data queues from sensors are not congested. See Services Statistics.
Port range entry in sensor templates	When you create a sensor template, you can now enter a range of continuous port numbers in the port mapping window. See Create Templates.
Integrations removed	Cisco Firepower Threat Defense (FTD) and Cisco Firepower Management Center (FMC) are no longer available as integrations.
GUI enhancements	The Cisco Cyber Center UI pages for policy creation and licensing contain some visual changes. The functionalities and workflows remain unchanged.

Feature	Description
Beta UI	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.
	This UI experience is a beta feature. To access the beta UI and its features, write to cv-beta@cisco.com. You will receive the command to enable the Cisco Cyber Vision Beta UI in addition to the existing classic UI.
	You can also configure functional groups in the beta UI, and assign data sources to organization hierarchies.

CHAPTER 2

Introduction to Cyber Vision

Cisco Cyber Vision Installation

The GUI (graphical user interface) is an integral part of Cisco Cyber Vision center. It provides an easy-to-use, real-time visualization of industrial networks. Access to some features may depend on the license subscribed to and on the user rights assigned. The application is **collaborative**, meaning that actions performed may have an impact on the users of the platform and be visible to them. Using Cisco Cyber Vision requires the following:

1. The Center: hardware to configure network interfaces that collect data from the sensors and install Cisco Cyber Vision software.

2. Network sensors: to capture traffic and visualize data on the GUI.

If not installed yet, please refer to the corresponding quickstart guides.

At least one sensor has to be enrolled so that you can see it in the GUI. To do so, see the Sensors.

Overview

One of the aims of the GUI (Graphical User Interface) is to provide an easy-to-use, real-time visualization of industrial networks. Access to some features may depend on the license subscribed and on the user rights assigned. The application is **collaborative**; which means that actions performed may have an impact on the users of the platform and be visible to them.

Understanding Concepts

Preset

A preset is a set of criteria. Think of a preset as a "magnifying glass" in which you can see details of a big network by choosing the metadata processed by Cisco Cyber Vision that meets your business requirements. We created presets to help you navigate through the data. For example, if you are interested in knowing which PLCs are writing variables, access one Preset (e.g., OT) and select two criteria (e.g., PLC and Write Var). Several types of views are available to give you full visibility on the results and from different perspectives.

Generic presets are available by default. They were created according to the recommendations and categories listed in Cisco Cyber Vision playbooks. The following default presets are available:

- Basics: To see all data, or filter data to IT or OT components.

- Asset management: To identify and inventory all assets associated with OT systems, OT process facilities, and IT components.

- Control Systems Management: To check the state of industrial processes.

- IT Communication Management: To see flows according to their nature (OT, IT, IT infrastructure, IPV6 communications, and Microsoft flows).

- Security: To control remote accesses and insecure activities.

- Network Management: To see network detection issues.

My Preset contains customized presets. You can create presets using criteria to meet your own business logic.

Note Customized presets are persistent and impact other users.

Filters

To access the filters, follow these steps:

1. From the main menu choose **Explore**.

2. Click the drop-down arrow in the top navigation bar and click **All Data** under **Basics**.

3. Click the drop-down arrow in the third filter of the top navigation bar and click **Dashboard**.

Create presets using the following filters:

Criteria

Enter keyword(s) in the field to apply the search function. Use **Select All**, **Reject All**, or **Default** to modify the list.

- Risk score: device individual risk

- Networks: device IPs

- Device tags: devices

- Activity tags: activities

- Groups: devices

- Sensors: device "location"

Filters work differently whether they are affecting devices or activities. Their combination limits the scope of data visualized in the different views for a preset. Each category allows you to define a subset of the components, or activities for the Activity filter. If filters are defined by several categories, the resulting dataset is the intersection of the selections for each category. Parameter and filter usage is explained below.

Risk Score

Use the Risk Score to filter devices based on their score or a range of Risk scores. Risk scores can be inclusive or exclusive filters. All devices will be filtered based on this range.

Networks

Define a filter based on two network settings: IP range or VLAN ID. This filter will have an impact on the Activity List. The result will be "all activities with one end belonging to this network." Activities with at least one device in the corresponding network are selected.

Regarding the Device list, only the devices with at least one IP address in the corresponding network range are selected.

For instance, use exclusion and combination for this result:

Network filter – negative filter

Multiple negative selections are not supported on 4.0.0.

Filter combination

You can define filters in several categories simultaneously. The preset will be calculated first by filtering the activities with all the activity-based filters. Then, the devices will be filtered with their own filter criteria. The result is the preset dataset. This preset dataset is used to precompute the view that Cyber Vision presents to you. Select a time frame to further filter the preset dataset.

Device tag filters

Device tags are used to select components. Device tag filters are inclusive or exclusive. The combination of several device tags selects all the components with at least one of the selected device tags. If the device tag filter is exclusive, the system will ignore all components with the selected device tags. For example:

Device tag filters

Device tag filter definition	Device	Tags	Visible ?
☑ Controller (8) ☑ Network Switch (2) ✕ Rockwell Automation ✕ Siemens	IE4000PRP2.ccv 80:2d:bf:1e:23:8c	Network Switch	Yes
	Schneider 192.168.22.68	Controller	Yes
	Siemens 192.168.21.41	Controller , Siemens	No
	1756-L71/B LOGIX5571 (Port1-Link00)	Controller , Rockwell Automation	No

When devices are filtered the **Device view only** presents the devices corresponding to the filter. For the other displays like activity list or map, the devices which are communicating with the selected devices will be displayed too (all engineering stations or HMI in our example).

It will give the following results:

Device tag filter, example of Controllers – list of devices

In the associated map, all the components which communicate with the controllers will also be displayed. These other components are shadowed to be recognized:

Device tag filter, example of Controllers - map
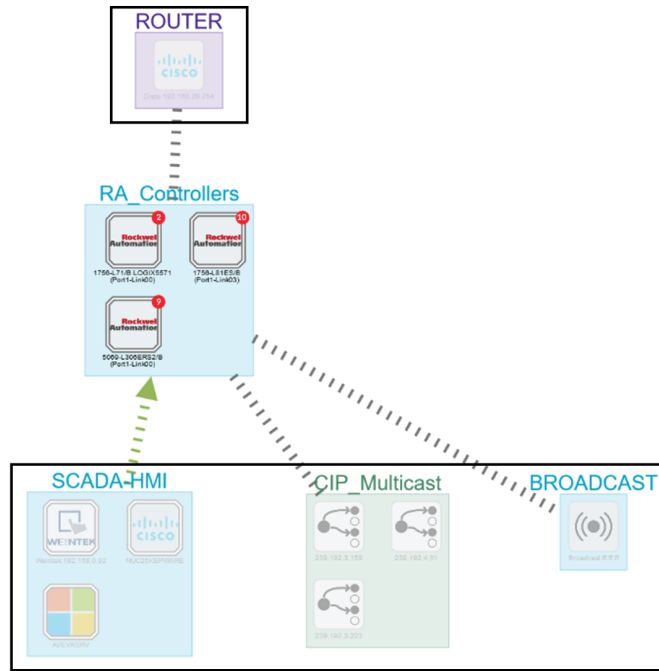
Activity Tags

Filtering on **Activity tags** will not have the same behavior than a filter based on **Devices**. Inclusive activity tag filters will be the same, but exclusive activity tag filters will remove activities only when all activity tags are included in the set of excluded tags. For example, if an activity has two tags, both tags need to be excluded to hide the activity.

For example, if an activity has two tags, both tags need to be excluded to hide the activity.

Activity filter – negative filter 1

In the example above, several activities show because the ARP tag is present, as well as other **Activity tags**. There is no exact match. The activity below is hidden.

filter 2

To remove broadcast and ARP activities, select both activity tags, as shown below.

Activity filter – negative filter 3

For very specific use cases, combine inclusive and exclusive tags. The above rules, for positive and negative selection, are combined, resulting in the following logic:

- Activities are selected as soon as at least one tag is in the set of included tags

- From this selection, activities which all tags are in the set of included AND excluded tags are hidden

Groups

Filter devices by Groups. Each group or sub-group could be added as an inclusive or exclusive filter.

Group filter
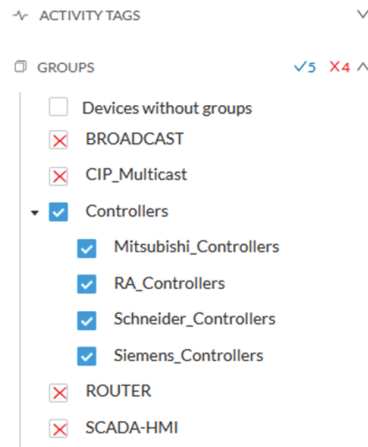
In the example above, only the devices belonging to the selected groups will be selected. Activities always involve two end points and are selected if either end point is part of a selected group, and none are part of an excluded group.

Sensors

Filter Activities based on the sensor that analyzed the associated packets. For tags, use inclusive and exclusive filters. Usually, either option is used but not both. Inclusive: selects data coming from a set of sensors. Exclusive: Ignore the data from a set of sensors.

Sensor filter

Keyword

A keyword can be used to filter devices using the "Search" section of the GUI. This keyword will be used to select devices based on their name, properties, IP, MAC and tags.

Keyword = 4c:71:0d
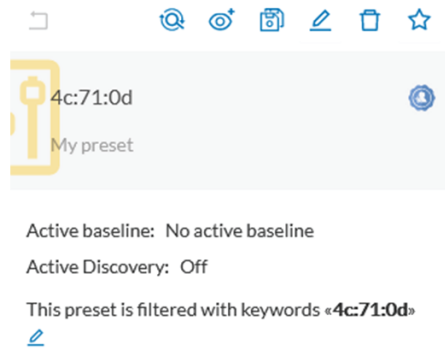
Keyword =siemens
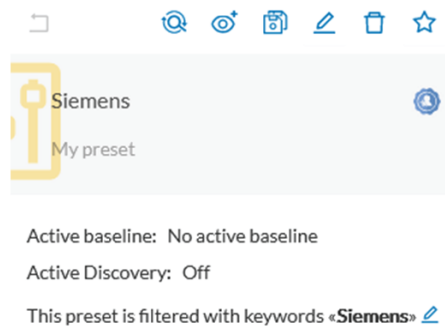
Filter combination

The user can define filters in several categories simultaneously. The preset will be calculated first by filtering the activities with all the activity-based filters. Then, the devices will be filtered with their own filter criteria. The result is the preset dataset. This preset dataset is used to precompute the view that is proposed to the user. The user can select a time frame to further filter the preset dataset.

Component

In version 4.0.0, we introduced Device, an aggregation of components. This changed how data is processed and presented. A component is an object of the industrial network. It can be the network interface of a PLC, a PC, a SCADA station, etc., or a broadcast or multicast address. In the GUI, a component is as an icon in a box, either the manufacturer icon (if detected), or a more specific icon (a known PLC model), a default cogwheel, a planet for a public IP, etc.

Some examples of icons:

Manufacturers' icons				
	SIEMENS	EMERSON	CISCO	

SIEMENS PLC icons		A S7-300 PLC.
		A Scalance X300 switch.
Default cogwheel		The manufacturer has not been detected yet by or the manufacturer has not been assigned a specific icon in 's icon library.
Public IP		
Broadcast		Broadcast destination component.
Multicast		

Components are grouped under a device. In the UI map, you see a device's components with a single border on the right side panel and technical sheet. Components that don't belong to any device display as an icon with a double border.

For more information, refer to the Device section.

Components are detected from the MAC address of the Properties and (if applicable) the IP address.

✎

Note   MAC addresses are all physical interfaces inside the network. IP addresses rely on the network configuration.

Cisco Cyber Vsion works by detecting network activity (emission or reception) by an object. Cyber Vision uses Deep Packet Inspection (DPI) technology to collate detailed information about a component. Information like IP address, MAC address, manufacturer, first and last activity, tags, OS, Model, and Firmware version depends on the data retrieved from the network. Data originates from the communications (i.e., flows) exchanged between the components.

Click a component on the map or a list. A Detail Panel with the detailed component information opens.

Device

The term **Device** is an aggregation of components with similar properties. In Cisco Cyber Vision, a **Device** is a physical machine of the industrial network such as a switch, an engineering station, a controller, a PC, a server, etc. Devices simplify data presentation, especially on the map. Devices enhance performance because a single device shows in place of multiple components. Devices comply with the logic of management and inventory, focusing on your needs.

A device shows as an icon in a double border, either the manufacturer icon (if detected), or a more specific icon (i.e., a known PLC model). If no icon is available in Cisco Cyber Vision database yet, a default cogwheel displays.

Components can share same characteristics such as the same IP address, MAC address, NetBIOS name, etc. In addition, tags and properties which are found in protocols are associated to define the type of device. Aggregation of components into a device and definition of the device type are based on a large set of rules with priorities that can be more or less complex. For example:

Click on a Schneider controller. A right side panel opens showing its components.
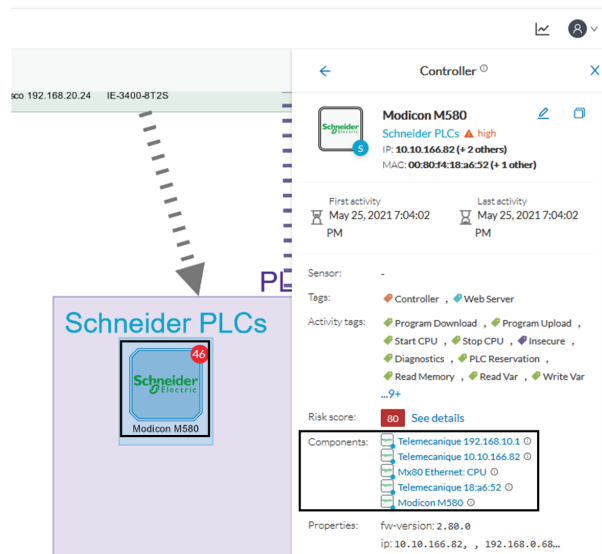
Devices can have a red counter badge. This is the number of vulnerabilities detected. For more information, refer to Vulnerability.

The list of a Rockwell Controller device's components (technical sheet > Basics > Components):

Component		First activity	Last activity	IP		MAC		Tags		Vulneral
1756-EN2T/D ⓘ		May 25, 2021 7:02:23 PM	May 25, 2021 7:02:23 PM	192.168.20.22		4c:71:0d:72:8c:57		Rockwell Automation		11
1756-RM2/A REDUNDANCY MODULE (Port1-Link01) ⓘ		May 25, 2021 7:02:23 PM	May 25, 2021 7:02:23 PM	192.168.20.22		4c:71:0d:72:8c:57		Rockwell Automation		0
1756-EN2T/D (Port1-Link02)	ⓘ	May 25, 2021 7:02:23 PM	May 25, 2021 7:02:23 PM	192.168.20.22		4c:71:0d:72:8c:57		Rockwell Automation		11
1756-EN2TR/C (Port1-Link03)		May 25, 2021 7:02:23 PM	May 25, 2021 7:02:23 PM	192.168.20.22		4c:71:0d:72:8c:57		Rockwell Automation		11
L71RED_CPU_NAME | 1756-L71/B LOGIX5571	ⓘ	May 25, 2021 7:02:23 PM	May 25, 2021 7:02:23 PM	192.168.20.22		4c:71:0d:72:8c:57		Controller , Rockwell Automation		2

All these device's components have in common activity time, IPs, MACs, and tags. The Controller tag -which is a level 2 device tag, also considered as top priority in aggregation rules to define device type- detected on one of the components is applied at the device level and define the device type as Controller. The Rockwell Automation tag is a system tag which together with other properties is detected as the brand of the device.

For detailed information about which types of devices are detected per Level, see Tags.

Activity

An activity is the representation of the communications exchanged between Device or Component. It is recognizable on the map by a line (or an arrow if the source and destination components are known) which links one component to another.

To access the map, choose **Explore** > **Control Systems Management** > **OT Activities** from the main menu. Click a component on the map to view its details.
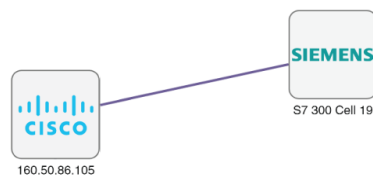
An activity between two components is actually a simplified view of the Flow exchanged. You can have many types of flows going in both directions inside an activity, represented in the map.

When you click on an activity in the map, a right side panel opens, containing:

- The date of the first and last communication between the two components.
- Details about the components (name, IP, MAC and, if applicable, the group they are part of, and their criticality).
- The tags on the flows.
- The number of flows.

• The number of packets.

• The volume of data exchanged.

• The number of events.

• A button to access the Technical Sheets that shows more details about tags and flows.
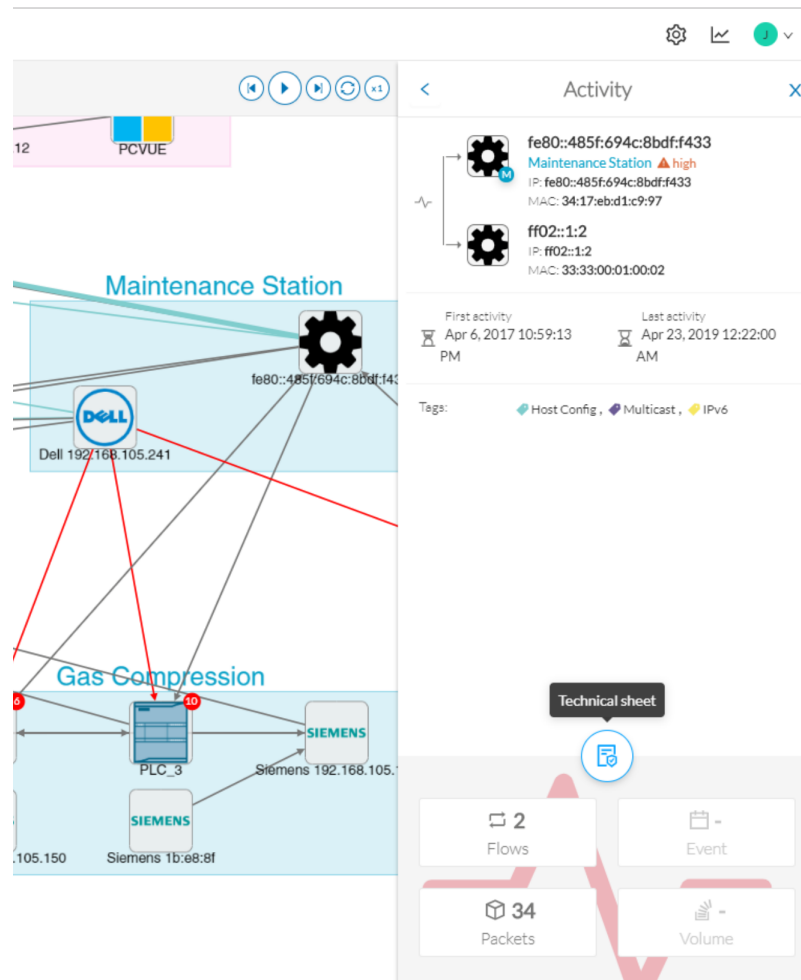
Devices or components with no activity does not mean that they did not have any interaction. In fact, a component can only be detected if it has been involved in a network activity (communication emission/reception). Lack of activity can mean that the other linked component is not part of the preset selected and so doesn't display.

Aggregated activities or conduits

When devices and components are placed inside groups, activities are aggregated to enhance visibility. Aggregated activities are called Conduit.

Use the **Show network activities** button at the lower left side of the map to turn on/off the simplified view of the activities between groups. This feature is turned on by default.
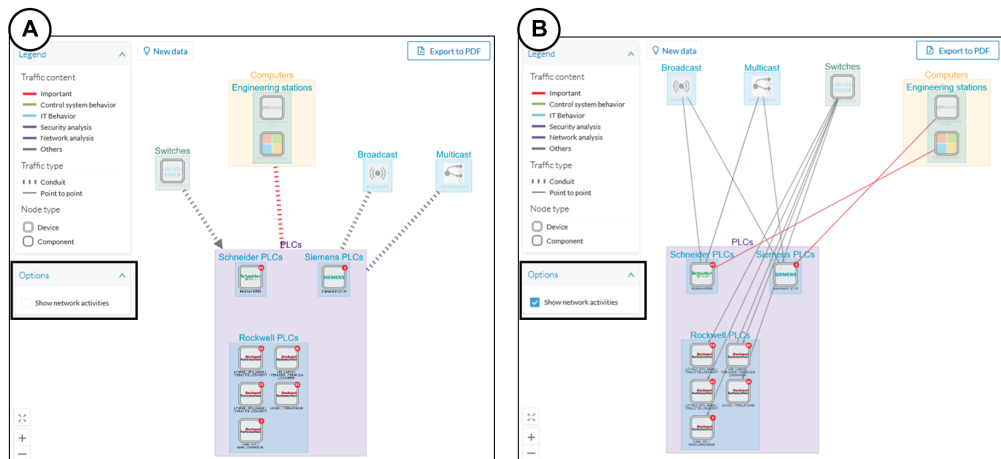
Flow

A flow is a single communication exchanged between two components. A group of flows forms an Activity, which is identifiable on the Map by a line that links one component to another.

To access a flow: click a component on the map. The side panel appears. Click the Technical Sheets icon > **Activity**. Or, click the **Flows** tile from the Detail Panel.

The Activity tab contains a list of flows which gives you detailed information about each single flow: number of flows in the activity, source and destination components (if known), ports used, first and last activity, and tags which characterize each flow.

The number of flows can be very important (there could be thousands). Consequently, filters are available in the table to sort flows by typing a component, a port, selecting tags, etc.

You can click on each flow in the list to have access to the flow's technical sheet for further information about the flow's properties and tags.

External Communication

An external communication is a communication initiated between a component/device inside a monitored network and an external component/device.

External communications are stored and listed in Cisco Cyber Vision, but not the external components/devices, nor their flows, to not obstruct the system. As a result, Cisco Cyber Vision's performances are increased, the GUI is cleared from unecessary data, and the license device count and risk scores are limited to inner devices and more accurate.

By default, external communications are defined as such through the detection of external components' IP addresses that **do not** meet with private IP address formats.

IP addresses that meet with private formats are considered as internal by default and are processed under stored components or devices and are displayed in Cisco Cyber Vision.

However, because sometimes public IP addresses are used in a private network of an industrial site, it is possible to manually define communications by declaring IP ranges as internal or external through the Network Organization administration page. For more information, refer to Cisco Cyber Vision GUI Administration Guide.

It is also possible to declare as external all or part of a private subnetwork. For example to filter some IT components/devices which are not relevant for Cisco Cyber Vision.

IP Address / subnet	VLAN ID	Network Name	Network Type	Action	
⊟ 10.0.0.0/8		10/8 private network	External	✎	🗑
10.2.0.0/22		OT range	OT Internal	✎	🗑
10.4.0.0/22		External IP within IP range	IT Internal	✎	🗑

In the GUI, a component with external communications is shown as an icon bordered in orange, or a double orange border for a device.

A device with external communications in the Map:

If you click on this component, its right side panel will appear. The **External Communications** button with the number of external communications will open the component's technical sheet directly on the external communications list.

The device's right side panel and the **External Communications** *button:*

The external communications list in the device's technical sheet:

The list shows details about external communications such as source and destination IPs, destination port, hostname, protocol, whether they are inbound or outbound, etc.

It is possible to export this list using the **Export to CSV** button.

Time Span

Cisco Cyber Vision is a real-time monitoring solution. The views are continuously updated with network data. You can view the network activity during a defined period of time by selecting a **time span**. Use **time span** to filter data, based on the time you select. This feature is available on each preset's view.

To access the timespan settings, follow these steps:

- From the main menu, choose **Explore** > **All data**.

- Click the dropdwn arrow at the top center of the page.

- Select **Device list** from the drop-down list.

- To set a time span, click the pencil icon.

  The **TIMESPAN SETTING** window appears.

- To set a **Duration**, click the drop-down arrow and select duration time (from 10 seconds to 1 day) or a custom period up to the present.

- To set a **Time window**, select a start date and (optionally) an end date.

Note If you don't select an end date, the end date will set to now.

Set a time window to see everything that has happened during the selected period of time, such as historical data or to check the network activity (in case of on-site intrusion or accident).

- Click **Refresh** to compute network data.

Note No data display is often due to a time span set on an empty period. Remember to first set a long period of time (such as 12 months) before troubleshooting.

Recommendations:

Generally, you can set the time period to 1 or 2 days. This setting is convenient to have an overall view of most supervised standard network activities. This includes daily activities such as maintenance checks and backups.

Adjust the time frame for the following:

- Set a period of a few minutes to have more visibility on what is *currently* happening on the network.

- Set a period of a few hours to have a view of the daily activity or set a time to see what has happened during the night, the weekend, etc.

- Set limits to view what happened during the night/weekend.

- Set limits to focus on a time frame close to a specific event.

Tags

Definition of Tags

	Tags are meaningful labels that succinctly describe a network. They can be applied to components or activities. Each tag has a description and an icon color which correspond to its category.
Tags 🏷️ Program Upload , 🏷️ Unite 🏷️ Program Download , 🏷️ Start CPU , 🏷️ Stop CPU , 🏷️ Unite 🏷️ Start CPU , 🏷️ Stop CPU , 🏷️ ARP , 🏷️ Unite 🏷️ Start CPU , 🏷️ Stop CPU , 🏷️ ARP , 🏷️ S7 🏷️ Read Var 🏷️ Read Var , 🏷️ Write Var , 🏷️ ARP , 🏷️ S7Plus 🏷️ Read Var , 🏷️ Multicast , 🏷️ IEC61850	

Tags are metadata on Device and Activity. Tags are generated according to the Properties of components. There are two types of tags:

- **Device tags** describe the functions of the device or component and are correlated to its properties. A device tag is generated at the component level and synthesized at the device level (which is an aggregation of components).

- **Activity tags** describe the protocols used and are correlated to its properties. An activity tag is generated at the flow level and synthesized at the activity level (which is a group of flows between two components).

Each tag is classified under categories, located in the filtering area.

The device tags categories (Device - Level 0-1, Device - Level 2, etc.) and some tags (IO Module, Wireless IO Module) in the filtering area:
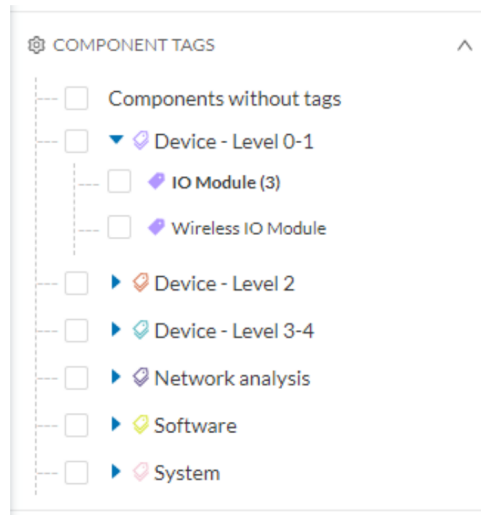
Note Device levels are based on the definitions from the ISA-95 international standard.

Tag Use

Use Cisco Cyber Vision tags primarily to explore the network. Criteria set on presets are significantly based on tags to Filters the different views.

Use tags to define behaviors (i.e., in the Monitor mode) inside an industrial network when combined with information like source and destination ports and flow properties.

Tag Location

Find tags almost everywhere in Cisco Cyber Vision, from criteria, which are based on tags to filter network data, to the different views available. Views filter and use tags differently. For example, the dashboard shows the preset's results, showing tags over other correlated data. The device list highlights devices, over data like tags. For more information, see the different types of view in Dashboard, on page 39.

For detailed information about a tag, see the **Basic** tab inside a Technical Sheets.

Below is an example of tag definitions.
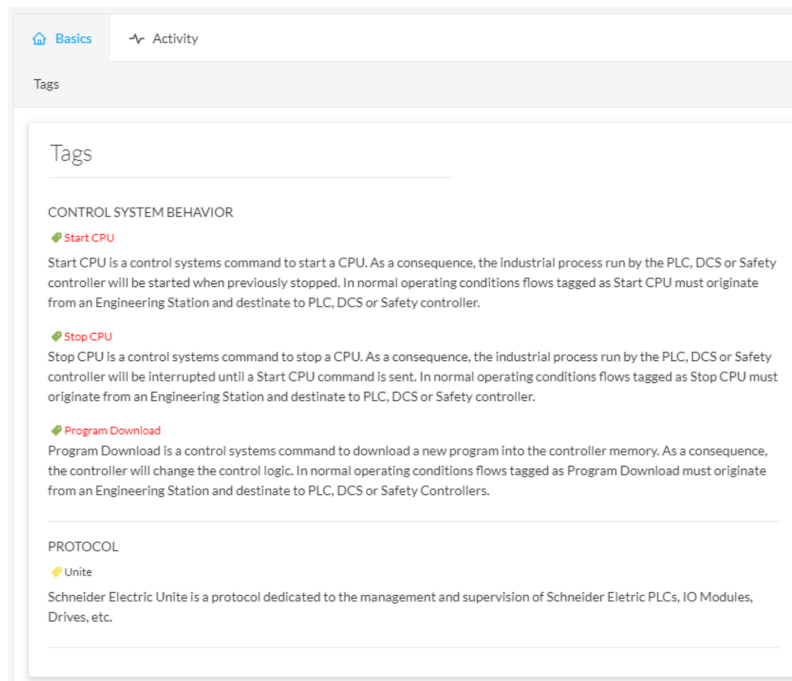
Properties

Property Definition

Properties are information such as IP and MAC addresses, hardware and firmware versions, serial number, etc. that qualify devices, components and flows. The sensor extracts flow properties from the packets captured. The Center then deduces components properties and then devices properties out of flow properties. Some properties are normalized for all devices and components and some properties are protocol or vendor specific.

Property Use

Properties provide details about devices, components and flows, and are crucial in Cisco Cyber Vision in generating Tags. A combination of properties and tags are used to define behaviors (i.e., in the Monitor mode) inside the industrial network.

Property Location

View Properties from devices and components Detail Panel and Technical Sheets under the **Basics** tab.

Below is an example of a technical sheet with normalized properties on the left column, and protocol and vendor specific properties on the right column.

Note Protocol and vendor-specific properties evolve as more protocols are supported by Cisco Cyber Vision.

Vulnerability

Definition of Vulnerabilities

Vulnerabilities are weaknesses detected on devices that can be exploited by a potential attacker to perform malevolent actions on the network.

Cisco Cyber Vision detects **Vulnerabilities** in the rules stored in the **Knowledge** database. These rules are sourced from several CERTs (Computer Emergency Response Team), manufacturers and partner manufacturers (Schneider, Siemens, etc.). Vulnerabilities are generated from the correlation of the Knowledge database rules and normalized device and component properties. A vulnerability is detected when a device or a component matches a Knowledge database rule.

Important Always update the Knowledge database in Cisco Cyber Vision as soon as possible after notification of a new version. This protects your network against vulnerabilities. See Knowledge DB to update knowledge database.

Vulnerability Use

Below is an example of a Siemens component's vulnerability. See the technical sheet, Security tab.

1. **Information** displayed about vulnerabilities includes the following: vulnerability type and reference, possible consequences, and solutions or actions to take on the network. Often, upgrading the device firmware alleviates a vulnerability. Links to the manufacturer website are also available.

2. A **score** reports the severity of the vulnerability. The score is calculated upon criteria from the Common Vulnerability Scoring System (CVSS). Criteria examples are: the ease of attack, its impacts, the importance of the component on the network, and whether actions can be taken remotely or not. Scores range from 0 to 10, with 10 being the most critical score.

3. **Acknowledge** a vulnerability if you don't want to be notified about it anymore. For example: a PLC is detected as vulnerable but a firewall or a security module is placed ahead. The vulnerability is mitigated. Cancel an **Acknowledgment** at any time. Only the Admin, Product, and Operator users can access **Vulnerabilities Acknowledgment/Cancelation**.

Vulnerability Location

Access Vulnerabilities in any of the following ways: click **Explore > All Data > Vulnerabilities**, use Vulnerabilities of a preset, or through the **Device list**. Use the **Sort arrows** to view the vulnerability column.

Find vulnerabilities on the map by a device or a component with a red counter badge. Click the badge **(4)** and the side panel opens with the number of vulnerabilities shown in red.

Click the **Vulnerabilities** in red **(5)** and the device or component's technical sheet opens.

Events

An Events occurs if a device or component gets detected as vulnerable. You receive a notification. One event is generated per vulnerable component. An event is also generated each time a vulnerability is acknowledged or not vulnerable anymore.

Credentials

Credentials are logins and passwords that circulate between components over the network. Such sensitive data sometimes carry cleartext passwords when unsafe. If credentials are visible on Cisco Cyber Vision, then they are potentially visible to anyone on the network. Credential visibility triggers awareness and actions to be taken to properly secure the protocols used on a network.

*Below is a **Details** panel of a component showing the number of credentials detected.*

Credential frames are extracted from the network in Deep Packet Inspection. Use the technical sheet of a compoent to access **Credentials**. Click the **Security** tab.

1. The number of credentials found.

2. The protocol used.

3. The user name and password. If a password appears in clear text, then action should be taken to secure it whether it is hashed or not.

4. How to reveal the credentials.

An unsafe password:
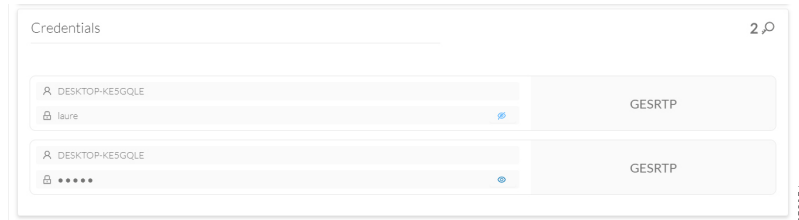
A hashed password:
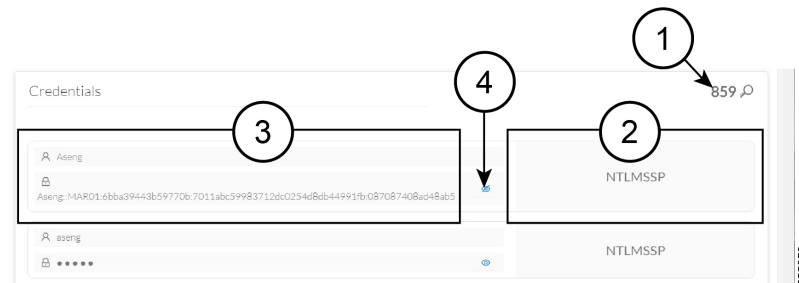
Variable Accesses

Variable Definition

A Variable is a container that holds information on equipment such as a PLC or a data server (i.e., OPC data server) for process control and supervision purposes. There are many different types of variables depending on the PLC or the server used. Access a variable by using a name or a physical address in the equipment memory. Variables can be read or written in any equipment, according to need.

For example, a variable can be the ongoing temperature of an industrial oven. This value is stored in the oven's PLC and can be controlled by another PLC or accessed and supervised by a SCADA system. The same value can be read by another PLC which controls the heating system.

Variable Use

Reading and writing variables inside a network is strictly controlled. Pay close attention if an unplanned change occurs, especially if it is a new, written variable. Such behavior could be an attacker attempting to take control of the process. Cisco Cyber Vision reports the variables' messages detected on the equipment of the industrial network.

Find details on Variable accesses in a component's technical sheet. Use **Sort arrows** to see a table containing the following:

- The name of the variable

- Its type (READ or WRITE) but not the value itself

- Which component accessed the variable

- The first and last time the component accessed the variable

The entry "2 different accesses" **(1)** indicates that two components have read the variable.

Variable Location

View the number of variable accesses per component on the component list view. Sort the var column by ascending or descending number.

For component details, click a component. The right panel opens.

For a detailed list of variable accesses, see the component's technical sheet (see the first figure above) and use the **Automation** tab or see the PLC reports.

Creating and Customizing Groups

Accessibility: Admin, Product and Operator users
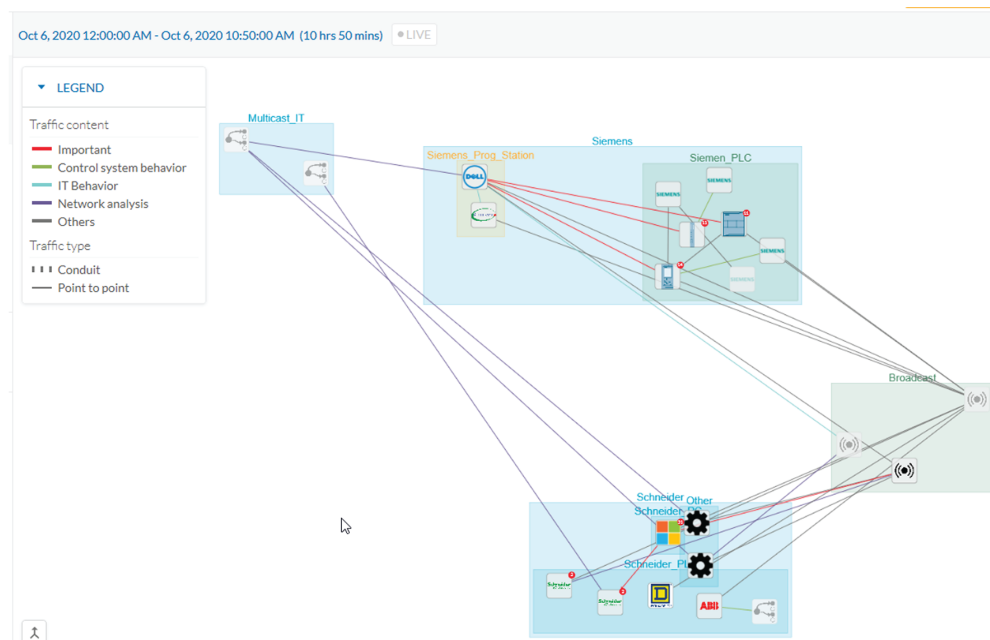
You can organize devices and components into groups to add meaning to your network representation. For example, group components according to the devices' location, process, severity, type, etc. You can also create nested groups inside a parent's group. This adds a group into another group to create several layers and structure the data.

To create a group:

Procedure

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

Step 2   Click the drop-down arrow in the top navigation bar and select **All Data** under **Basics**.

Step 3   Click the drop-down arrow in the third filter of the top navigation bar and select **Device list** or **Map**.

Step 4   Select device(s) or components from the **Map** or the **Device list** interface.

     Tip: To select multiple components in the map, press **Shift** and click the devices or components, or press **Ctrl** and draw a selection box. In the **Device list** view, use the check boxes.

     A **My Selection** right-side panel appears.

Step 5   Click **Manage selection**.

     The drop-down list appears.

Step 6   Click **Create a new parent group** from the drop-down list.

     A **CREATE A NEW PARENT GROUP** window appears.

Step 7   Enter the **Name** of the new parent group.

Step 8   Enter **Description** to customize the group and define its industrial impact.

For example, a PLC that controls a robotic arm is highly critical.

Step 9　　Change **Color** under **Customization** field.

Step 10　　Enter **Properties**.

Step 11　　Add the group to a parent group, if already created.

To create a parent group:

The following are several ways to create a hierarchy among groups:

- Select two groups and create a group, as indicated above.

- Select a device or a component and move it into a group. Use the **Move selection to existing group** button.

- Select a group and move it to another group. Use **Move selection to existing group**.

Add group properties

Adding properties to a group can be useful to store specific information. The labels available fit the 62443 standard which specifies policies and requirements for system security. You can also add custom properties.

To add properties to a group:

- Select a group in the map and click **Edit** or **Add properties**.

- Choose/define a label and add a value.
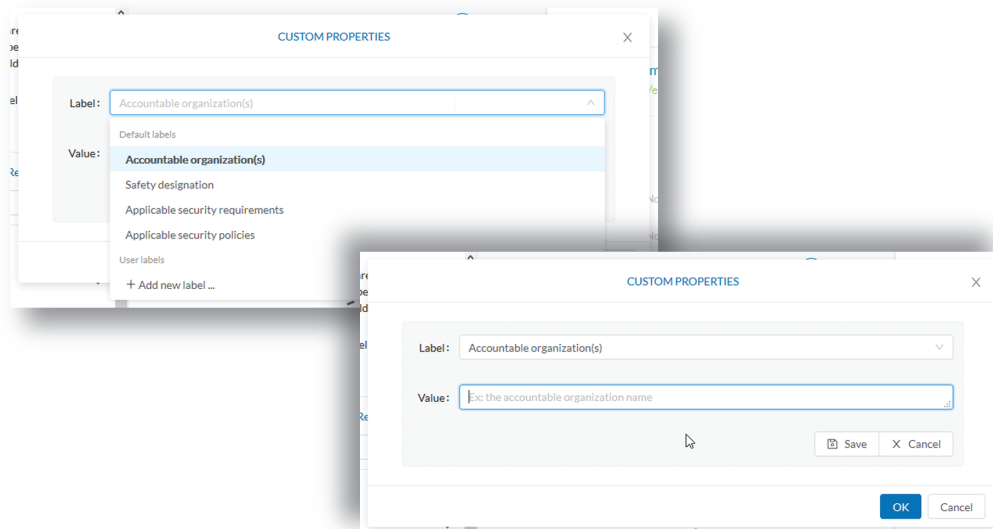
Aggregated activities are conduits

Placing devices and components inside groups aggregates the activities and enhances visibility. Aggregated activities are called Conduit.

Use the **Show network activities** checkbox at the lower left side of the map to turn on/off the simplified view of the activities between groups. This feature is on by default.
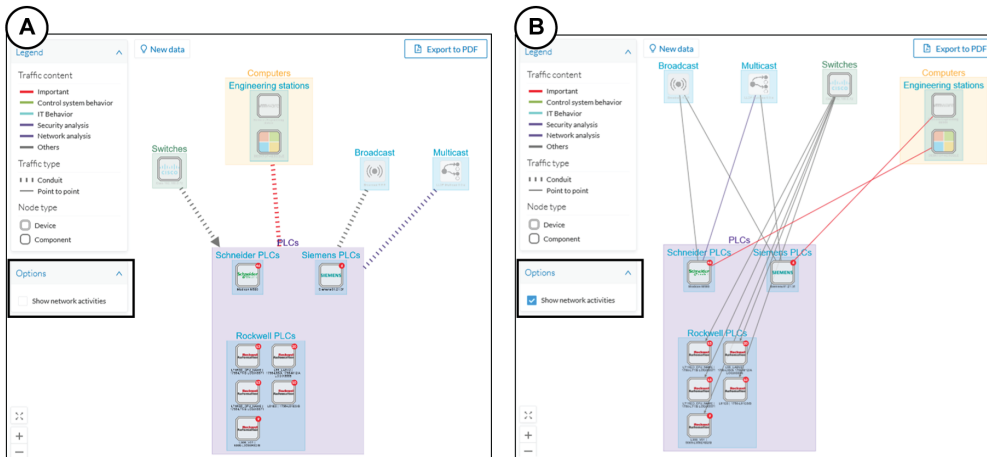
Group Lock/Unlock

Locking a group:

- Prevents adding or removing components from the group.

- Prevents a group deletion.

To switch on/off the **Lock** icon:

Step 12   Click a group. The **Group** details panel opens.

Step 13   Click the **Lock** icon on the Group's icon.

or

Click the **Edit** icon on the **Group** details panel and toggle on/off the **Lock** icon.
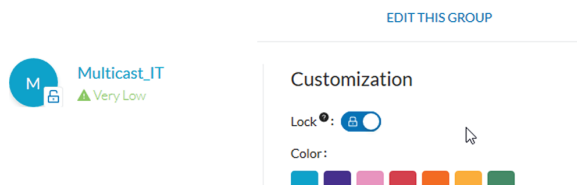
Step 14   **Groups used as criteria to filter data in Cisco Cyber Vision:**

Created groups are added into the Filters to help you refine the dataset and compose presets.
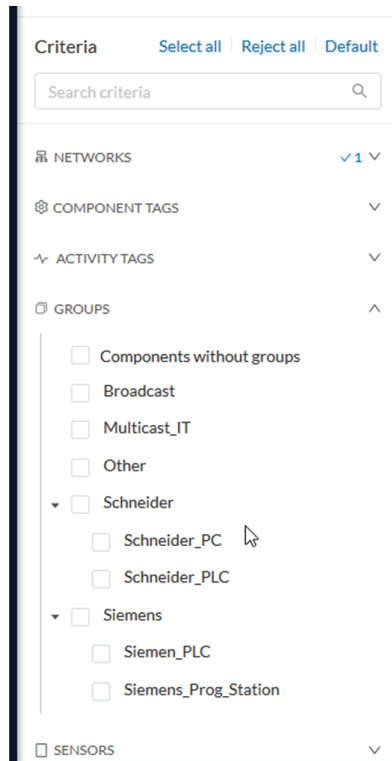
Active Discovery

Active Discovery is a feature to enforce data enrichment on the network. **Active Discovery** is an optional feature that explores traffic in an active way. All components are not found by Cisco Cyber Vision because those devices have not been communicating from the moment the solution started to run on the network. Some information, like firmware version, can be difficult to obtain because it is not exchanged often between components.

With **Active Discovery** enabled, broadcast and/or unicast messages are sent to the targeted subnetworks or devices through sensors, to speed up network discovery. Returned responses are analyzed and tagged as **Active Discovery**. Components and activitiesare clarified with additional and more reliable information than may be found through passive DPI. The following table lists the supported protocols.

Broadcast	Unicast
EtherNet/IP	EtherNet/IP
Profinet	SiemensS7
SiemensS7	SNMPv2c
ICMPv6	SNMPv3
	WMI

Active Discovery is available on the following devices:

- Cisco Catalyst IE3300 10G Rugged Series Switch

- Cisco Catalyst IE3400 Rugged Series Switch

- Cisco Catalyst IE9300 Rugged Series Switch

- Cisco Catalyst 9300 Series Switch

- Cisco Catalyst 9400 Series Switch

- Cisco IC3000 Industrial Compute Gateway

- Cisco IR8340 Integrated Services Router Rugged

Active Discovery jobs can be launched at fixed time intervals or just once.

For more information and instructions on how to configure **Active Discovery** in Cisco Cyber Vision, refer to the Active Discovery Configuration Guide.

Navigating Through Cisco Cyber Vision

Home

The Cisco Cyber Vision Center's home page displays two tabs: **Operational Overview** and **Security Overview** of the industrial network over the last month.

Use the checkboxes to edit the display. The **Operational Overview** shows the **Protocol distribution** pie chart and a list of the **Most critical events**.
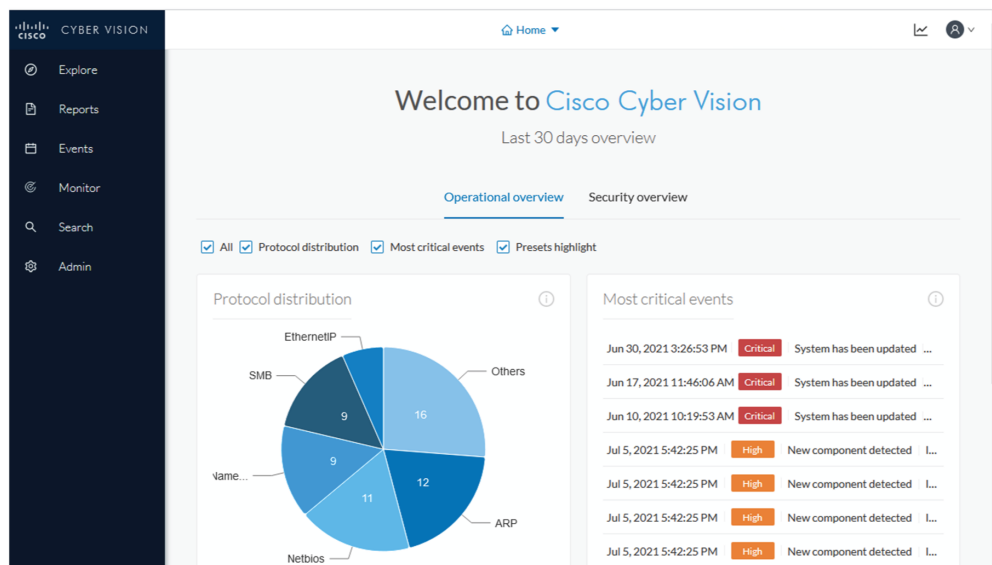
It also shows **Preset highlights**. Click **Edit favorite presets** to change what displays. Select the checkboxes of the presets and click **Save**.

Security Overview shows the **Vulnerable devices per severities** ring chart and the **Devices by risk score** ring chart.

It also shows a list of the **Most critical events**, **Events by category**, and the **Preset highlights** that you can edit.

The navigation bar on the left provides access to all main pages of the Cisco Cyber Vision Center:

1. **Explore**: Shows the overview of all presets, by defaults or configured.

2. **Reports**: Shows the Reports to export valuable information about the industrial network.

3. **Events**: Shows the Events page which contains graphics and a calendar of all events generated by .

4. **Monitor**: Shows the Monitor, on page 51 page to perform and automatize data comparisons of the industrial network.

5. **Search**: Shows the Search to look for precise data in the industrial network.

6. **Admin**: Shows how to update the system, configure exports parameters, import and export the database, update the Knowledge DB and reset data and system settings.

Explore

Explore shows an overview of all the Presets in Cisco Cyber Vision, both defaults and custom presets. Click **Explore** on the left navigation bar.

Use the top navigation bar **(1)** to access the different presets **(2)** and Preset Views.

You can also filter presets by categories.
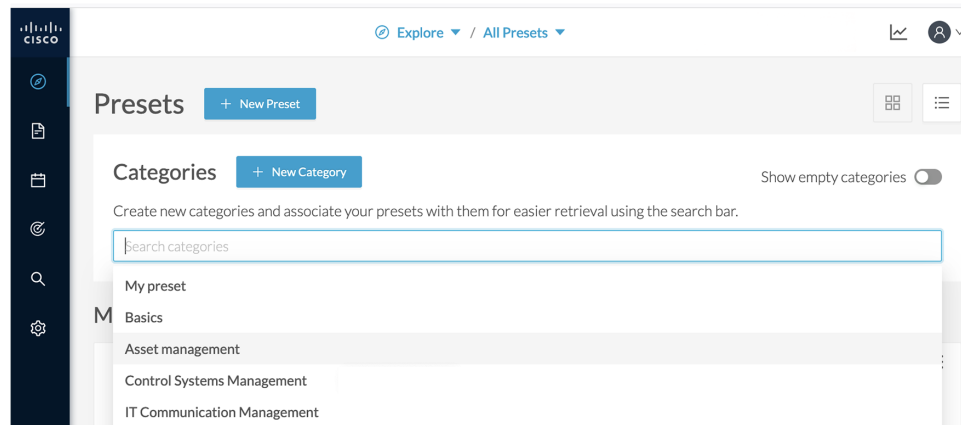
Create new categories to order and search your custom presets.
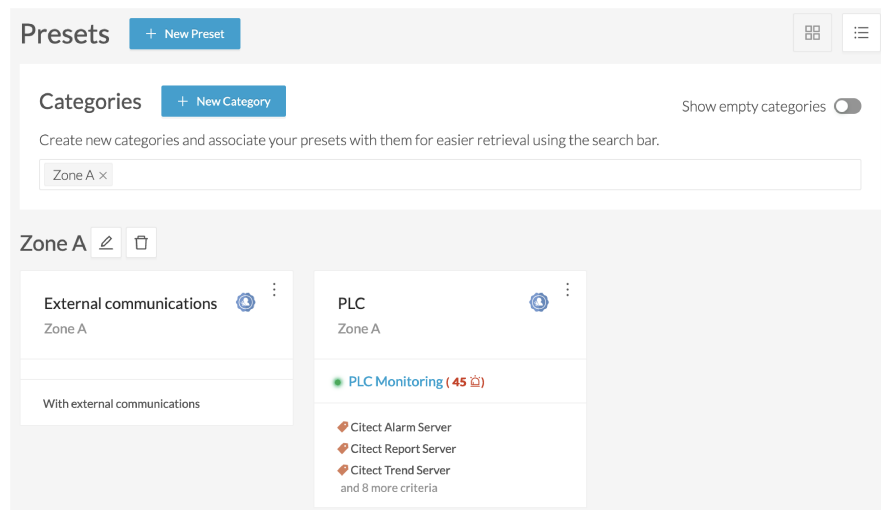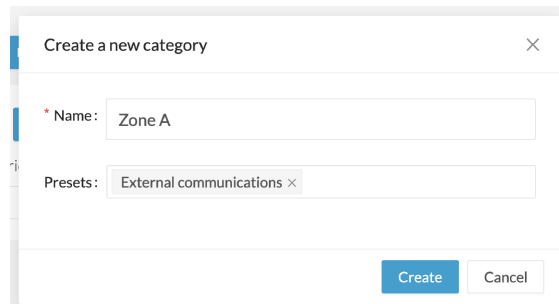
Filters included in Explore page's url allow you to save the selection in your browser's favorites.
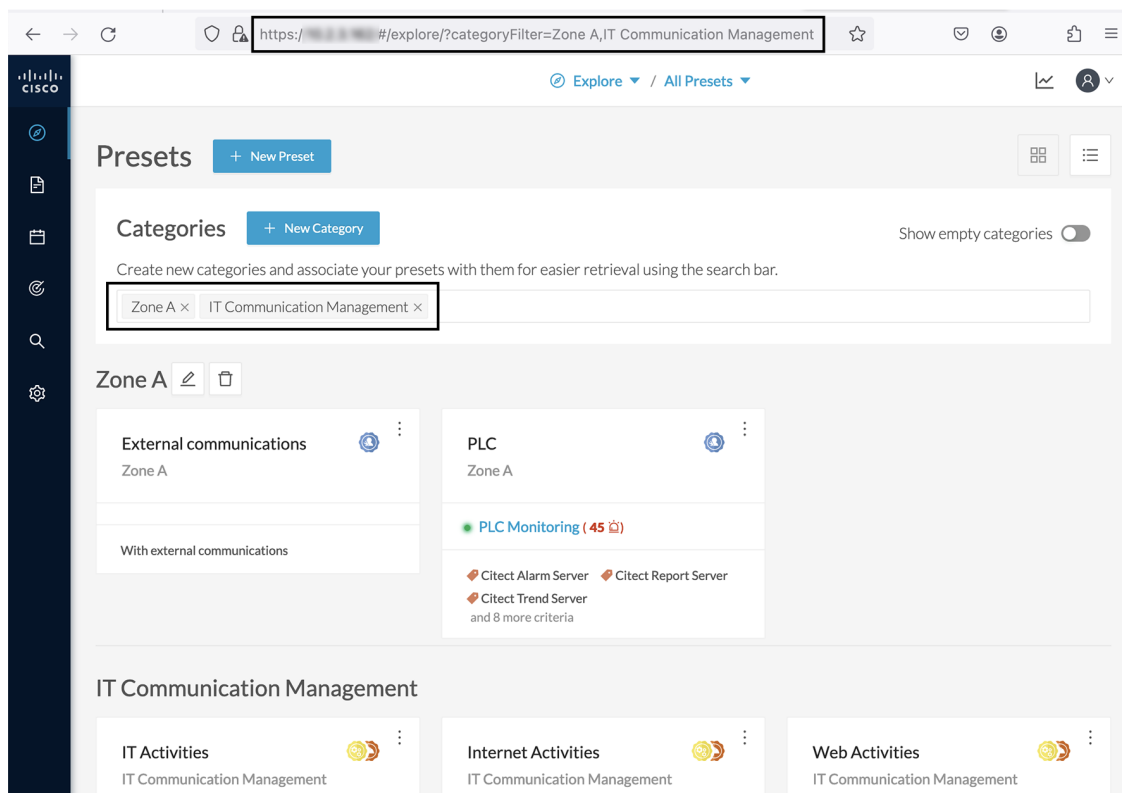
Preset Views

There are several types of views that relate to different perspectives. Use the top navigation bar to access the views. From the main menu, choose **Explore** > **All Data**. The **Dashboard** appears.

- **Dashboard** view is the default which gives the preset data overview. It is a tag-oriented view showing general insight of the network, without going into deep and technical details.

- **Map** is visual data of the industrial network that gives you a broad insight of how components are connected to each other.

- **Lists**, **Device list** or **Activity list**, show classic but powerful data filtering to match what you are looking for. For more information, refer to the Device and Activity Lists.

- **Purdue Model** shows how the components of a preset are distributed among the layers of the Purdue Model architecture.

Views are always structured as shown below:

- Use the top navigation bar and click the drop-down arrow to switch between different views, such as **Dashboard**, **Map**, **Device list**, **Activity list**, **Vulnerabilities**, **Security Insights**, and **Purdue Model**.

- Use the left panel **All data Basics** to filter, modify, and manage preset data such as **Risk Score**, **NETWORKS**, **DEVICE TAGS**, **ACTIVITY TAGS**, **GROUPS**, and **SENSORS** by adapting criteria and registering changes.

- The center panel dynamically changes as you save criteria.

The preset view is optimized to avoid lags, to solve performance issues, and to prevent the application from crashing, especially in case of large data flow. Since version 4.0.0, data elements such as components, tags and activities are stored, instead of being directly displayed in the preset views. Preset views refresh occurs only when necessary or requested. This prevents overloading the application display. The elements visible in the preset views are actually data from the *previous* computation. This means that data displayed in the GUI and data stored in the database are asynchronous, which lightens data load on preset views.

In addition, data computation adapts to the frequency of the preset consultations. That is, a preset often viewed by users computes accordingly. Conversely, the system does not compute presets that are *never* used.

When on a preset, data is regularly computed by an automatized data computation running in the background. However, this does not refresh the preset view. Two buttons are available in the preset view to act independently whether on the database or on the preset view to lighten the load on the system:

- The **New data** button appears each time a new computation is done. Click it to update the view.

> **Note** The new view may not show new data.

- The **Refresh** button forces data computation and refreshes the preset view. This task requires more resources. Use **Refresh** for the following cases:
  - If you suspect that new data was found during the most recent computation (e.g., a new device plugged into the network).
  - If custom data such as groups or names has been changed (e.g., if adding a device into a group).

In many cases, computation is forced and the view refreshes as you navigate in the application. For example, refresh happens when you access another preset or move from one view to another.

> **Note** New preset view optimization also has an impact on how criteria are handled in preset views. Save new data in a new or custom preset.

Dashboard

Dashboard is the preset default view. **Dashboard** shows an overview of the preset's global risk score, the number of devices, activities, vulnerabilities, events, variables and credentials.

Dashboard also shows **Tags**. The **Tag** pane shows all tags found, including tags set as criteria and shows the number of devices and activities found per tag.

For example:

1. From the main menu, choose **Explore** > **All Data**.

2. Click the drop-down arrow of the top navigation bar and click **Dashboard**

3. From the left panel, click the drop-down arrow of the **DEVICE TAGS**.

4. From the drop-down list, click the drop-down arrow of the **Device - Level 2**.

5. Check the checkbox of **Controller**.

6. Click **Save as**.

The **SAVE THIS PRESET AS...** pop-up appears.

7. Enter the new name in the **Name** field.

The Preset name should not be the same as previously.

8. Click the drop-down arrow of the **Category** field and select category.

9. Click **OK**.

Devices per tag: The number in brackets indicates there are 7 devices tagged as **Controller (1)**. On the **Dashboard**, you see this result **(2)**. One device is tagged as Web Server **(3)**. This means that one of the **Controllers** is a Web Server. Following this logic, we can say that five of the Controllers are Rockwell Automation devices. That leaves one remaining as "unknown."

For more details on these devices, switch to the Device and Activity Lists and access them using the filter available in the Tags column.

Activities per tag: As for activities, there is no activity tags set as criteria in the example below **(4)**. Yet, you can see that many activities have been found **(5)**. This is because the dashboard view collects all activities involved with the Controller devices found.

For details on these activities, switch to the Device and Activity Lists and access them using the filter available in the Tags column.

Device and Activity Lists

The **Device list** and **Activity list** are two specialized views. These views provide general information and advanced technical data about each element in the preset.

To access the **Device list**, follow theses steps:

1. From the main menu, choose **Explore**.

2. From the top nevigation bar, click the drop-down arrow of **All Presets** and select **All Data** from the drop-down list.

3. From the top nevigation bar, click the drop-down arrow of the third filter and select **Device list** from the drop-down list.

To access the **Activity list**, follow theses steps:

1. From the main menu, choose **Explore**.

2. From the top nevigation bar, click the drop-down arrow of **All Presets** and select **All Data** from the drop-down list.

3. From the top nevigation bar, click the drop-down arrow of the third filter and select **Activity list** from the drop-down list.

Lists can provide an in-depth exploration of the network. Use the **Search** function to find very specific data. Use the **Filter** icons in the list columns to sort data.

- Use the sort arrows to list data in alphabetical order or by ascending/descending order. Click again to cancel the sort.

- Use the filter icon opens a field to type specific data or a multiple-choice menu to filter tags.

Clicking an element in the lists opens its Detail Panel which displays more data.

Map

The **Map** view is a visual representation of data of the industrial network that gives you the broadstrokes on how devices and components are interconnected. It shows how the network is structured. **Map** helps you organize devices and components in a way that makes sense to you by creating groups.

Maps displays devices, components, and activities according to criteria set in a preset. **Grayed out devices and components** are displayed because, even if they don't correspond to the preset's criteria, they are necessary to represent the activities of the preset.
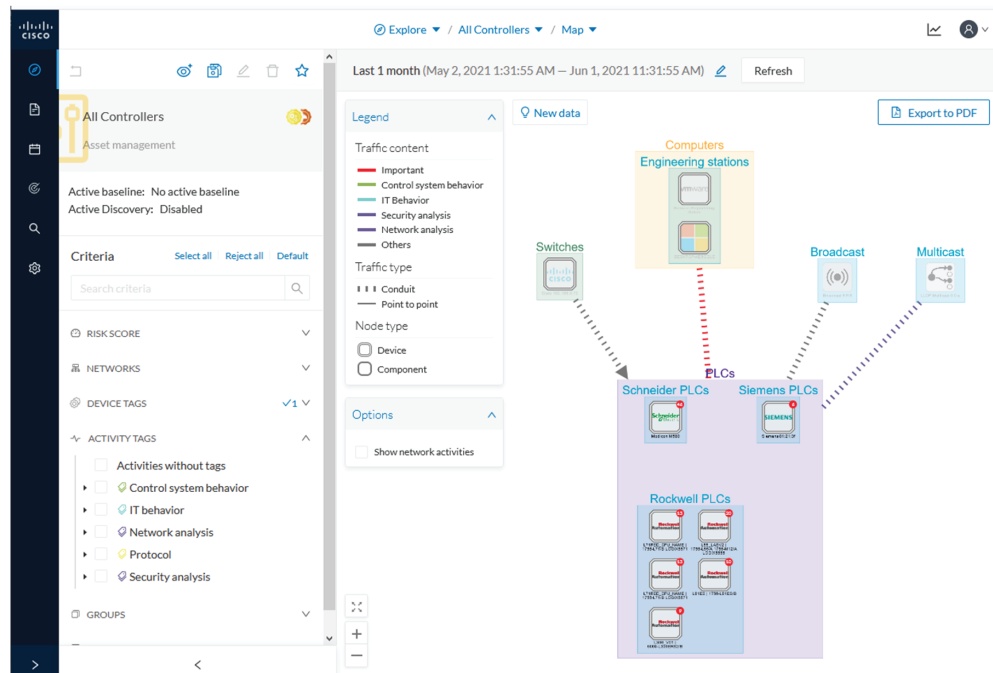
Note	The **Map** view is *self-organizing*, that is, elements are redistributed as devices, components, conduits and activities appear or disappear, and as groups are created or deleted. The **Map** automatically adapts over time and when you change a preset. This guarantees that the **Map** is always well organized and components never overlap.

By default, activities between groups are merged and displayed as Conduit. Select **Show network activities** for a more detailed view. To enhance visibility, elements here are also automatically reorganized on the **Map** .

Zones (Groups) and Conduits (Summarized Activities)

Cisco Cyber Vision limits the number of objects displayed simultaneously to maintain performance and prevent web browsers from freezing.

Users who handle large datasets or do not need detailed views can now display only groups. This option shows top-level groups (zones) and summarizes activities between them (conduits).

When a group hierarchy segments the control system, the new map option displays zones and conduits according to ISA/IEC 62443 standards.
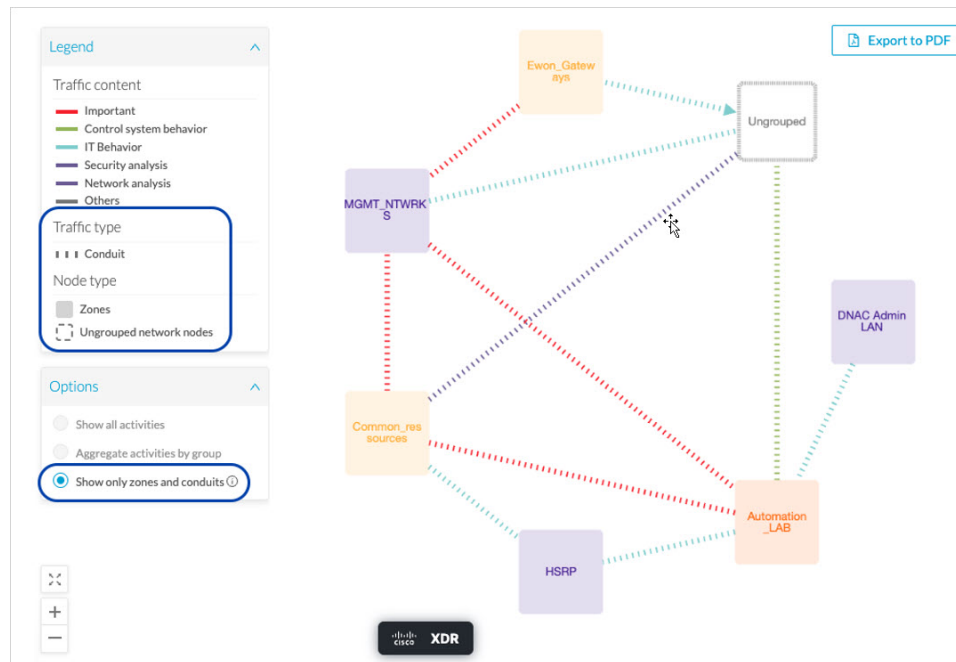
Conduit

A conduit is the representation of the communications exchanged between two Component. It is an aggregation of Activity to facilitate visibility when devices and components are inside groups. The representation of conduits in Cisco Cyber Vision fits the IEC standard, which specifies policies and requirements for system security.

On the map, a conduit displays as a thick, hyphenated line that links one group to another. If the source and destination groups are known, an arrow appears.
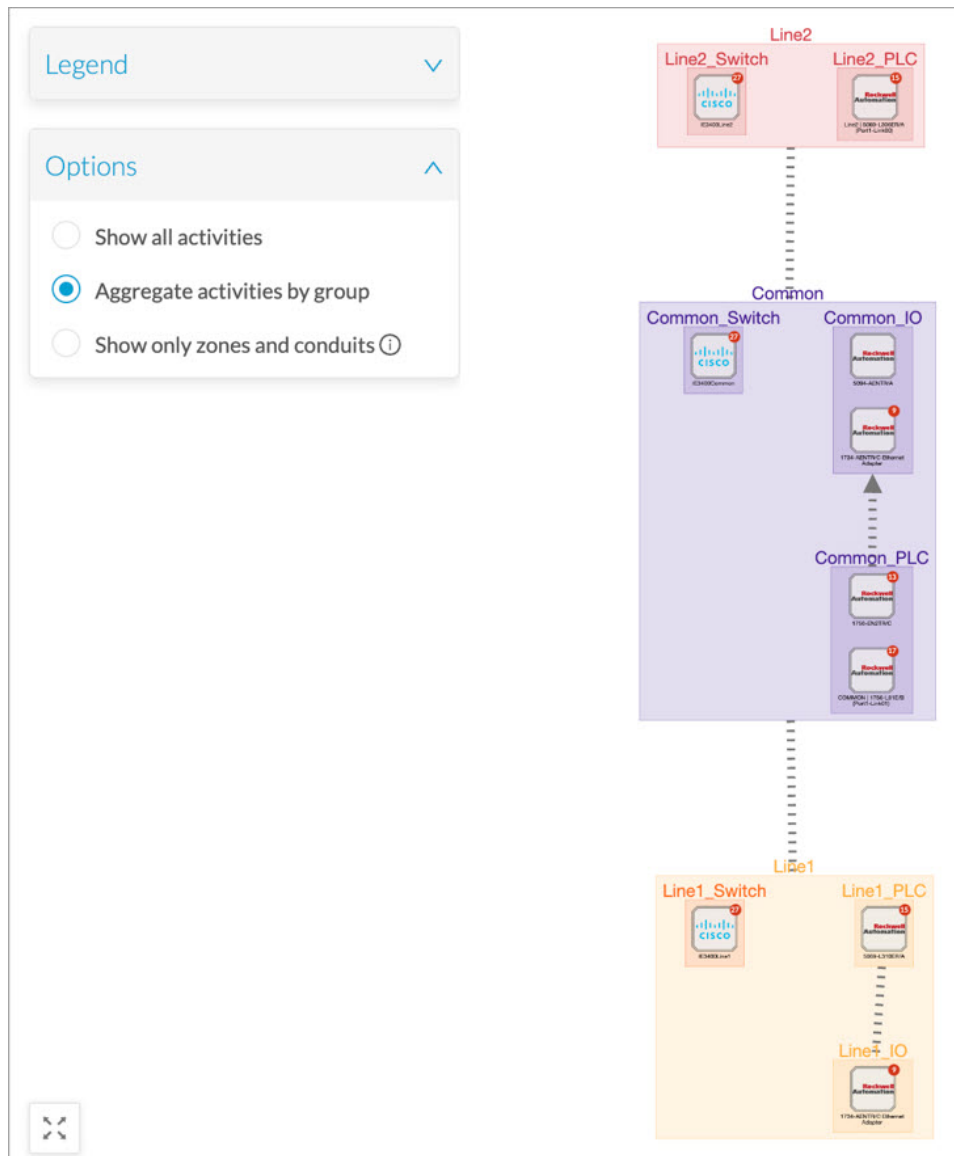
The Conduits View mode is enabled by default. Click the **Aggregate activities by group** radio button to disable it.

Vulnerabilities

To see a visual representation and a list of the Vulnerability detected within a preset, follow these steps:

1. From the main menu, choose **Explore**.

2. From the top navigation bar, click the drop-down arrow of **All Presets** and select **All Data** from the drop-down list.

3. From the top navigation bar, click the drop-down arrow of the third filter and select **Vulnerabilities** from the drop-down list.

☞

Important   If you receive a notification about a new version, update the Knowledge Database in Cisco Cyber Vision Center as soon as possible. This ensures you have the most up-to-date information about potential vulnerabilities in your network.

The pie chart shows the 10 most-matched vulnerabilities within the preset and the affected devices. The **Vulnerability severity legend** below provides the color code for severity. The center panel shows a list of the 10 most significant vulnerabilities. Click the hyperlink for an affected device to view the details panel. The right panel shows the total number of devices that are vulnerable in the selected preset.

Below is a list of all the vulnerabilities found in the preset. It has **Sort** icons to sort data by alphabetical order or by ascending/descending order, and **Filter** icons, which open a field to type specific data.

For each vulnerability, the following data is displayed in columns:

- • Vulnerability title
- • CVE ID (unique identifier for a Common Vulnerability Exposure)
- • CVSS score (Common Vulnerability Scoring System)
- • Affected devices (by the vulnerability)

Click an element in the list to open the Detail Panel. Click the link next to the **Identifier** field to view the National Vulnerability Database.

Click **Export to CSV** at the top of the vulnerability list. A report will be generated for the defined time period.

Security Insights

To access **Security Insights**, follow these steps:

1. From the main menu, choose **Explore**.

2. From the top navigation bar, click the drop-down arrow of **All Presets** and select **All Data** from the drop-down list.

3. From the top navigation bar, click the drop-down arrow of the third filter and select **Security Insights** from the drop-down list.

    Security Insights provides statistics for **DNS requests, HTTP requests, SMB Tree names** and **Flows with no tag**.

Each tab shows the top (most frequent), rarest requests, and lists all the requests. In the bottom panel, you can change the number of requests that show per page. You can see how many pages and the current page displaying. The total appears in the top right (75 in this example).

Flows with no tag

This information shows a list of all traffic that Cisco Cyber Vision Center was not able to analyze. There are various reasons for this, such as the protocol is not supported yet.

Next steps:

1. Make sure the content is supposed to be on the network.

2. Troubleshoot why it cannot be inspected.

3. Check flows with higher number of packets.

Purdue Model

This map displays the assets of a preset according to the Purdue Model architecture. Components are distributed among the layers by considering their tags. The **Purdue Model** view doesn't undergo any aggregation and is self-organizing.

To access the **Purdue Model**, follow these steps:

1. From the main menu, choose **Explore**.

2. From the top navigation bar, click the drop-down arrow of **All Presets** and select **All Data** from the drop-down list.

3. From the top navigation bar, click the drop-down arrow of the third filter and select **Purdue Model** from the drop-down list.

Assets of the preset All Controllers distributed among the layers of the Purdue model

Components are distributed according to the following different layers of the Purdue model:

- Level 0-1: Process and basic control (IO Modules).

- Level 2: Area supervisory control (PLCs, SCADA stations).

- Level 3-4: Manufacturing zone and DMZ (all others).

Detail Panel

A Detail panel is a condensed view about a device, a component, a group of components or an activity's information without changing the background device list or a map. To access a detail panel, click a device, a component or an activity on the map or a list.
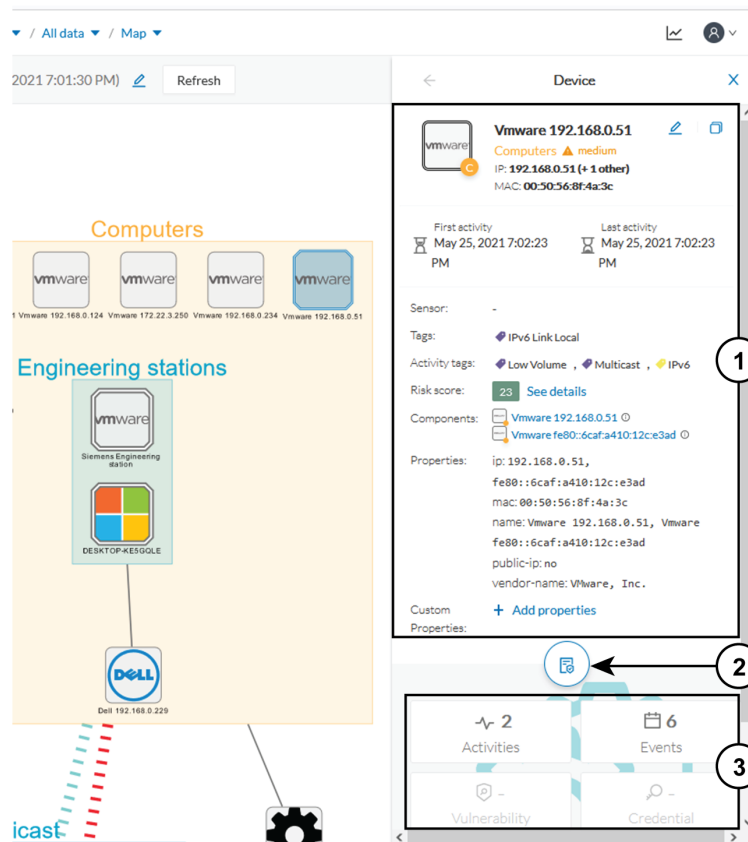
The detail panel differs depending on the type of element you select. The upper portion **(1)** gives you general information about the element. If you select a device or a component, you can edit its name an add/remove it to/from a group.

The lower part contains a round button **(2)** which opens the element's Technical Sheets with all relevant information (available for devices, components and activities).

The rectangular buttons below **(3)** redirect to the corresponding information inside the technical sheet.

Technical Sheets

A technical sheet is an interactive and complete view of all information related to a device, a component, an activity or a flow. The views differ depending on the type of element selected.

To access the **technical sheet** of a device, component or an activity's Detail Panel, follow these steps:

1. From the main menu, choose **Explore**.

2. From the top navigation bar, click the drop-down arrow of **All Presets** and select **All Data** from the drop-down list.

3. From the top navigation bar, click the drop-down arrow of the third filter and select **Map** from the drop-down list.

4. Click the **Technical sheet** icon.

The top box of the technical sheet recaps the information found in the **Detail** panel. The rectangular buttons on the right redirect to the corresponding information inside the technical sheet. In a device or a component's technical sheet, you can also edit the element's name, add/remove it to/from a group, and add custom properties.

The middle portion contains many tabs, depending on the selected element. In the above example, A **Device** detail contains the following tabs:

- **Basics** shows an element's properties and tags that are categorized with their definition. The components of the device also appear, if applicable.

- **Risk score** shows an overview and a more detailed and focused views.

- **Security** shows a component's vulnerabilities and credentials.

- **Activity** shows an activity's flows and contains a Mini Map, a view that is restricted to a device or a component and its activities. If applicable, a list of External Communication with related information appears under the corresponding tab.

- **Automation** contains variable accesses.

- More information about Properties.

- More information about Tags.

- More information about the Risk Score.

- More information about Vulnerability.

- More information about Credentials.

- More information about Flow.

- More information about the Mini Map.

- More information about External Communication.

- More information about Variable Accesses.

Mini Map

The **Mini Map** is a visual representation restricted to a specific device or component and its activities. To access **Mini Map**, follow these steps:

1. From the main menu, choose **Explore**.

2. From the top navigation bar, click the drop-down arrow of **All Presets** and select **All Data** from the drop-down list.

3. From the top navigation bar, click the drop-down arrow of the third filter and select **Map** from the drop-down list.

4. Select a device from the map.

5. Click **Technical sheet** from the **Details** panel.

6. Click the **Activity** tab.

7. To view an exploded view of the devices, check the checkbox of **Show inner components**.

8. Click any element in the Mini Map to open its Detail Panel for access to more information.

Reports

Security posture reports allow you to export industrial network data from the traffic captured and processed by Cisco Cyber Vision. You can uncover striking information like sensitive entrance points, acknowledged vulnerabilities for status reports, etc. To access **Reports**, click **Reports** from the main menu.

You must install the **Reports extension** to use this page. To install the **Reports extension**, choose **Admin** > **Extension** > **Import a new extension file** from the main menu. The extension file is available on cisco.com.

Security posture reports allow you to create reports from a Preset, (default data) in Cisco Cyber Vision, or a custom one.

Reports extensions include .docx and .pdf formats.

You can customize the report by adding a logo, such as your company's logo. By default, the report shows Cisco's logo.

The table of content menu allows you to set which content will appear in the report.

Create a Report

Note **Cyber Vision Reports Management** extension and **Cyber Vision Version** must be the same to generate the report.

Note Only users with report access and correct permission can create reports. Users with read-only access can download reports.

Procedure

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

Step 2 Click **Create and run a Report**.

Step 3 Enter **Name**.

Step 4 (Optional) Add a **Description**.

Step 5 Click the drop-down arrow of the **Type** filter and select the report type from the drop-down list.

Report types are as follows:

- **Security Posture:** This report is an automated summary that captures all the vulnerabilities, risky acivities, and security events found on the devices in the selected preset by Cisco Cyber Vision.

- **Remote Access:** This report is an automated summary that captures a list of all Remote Access Gateways and the Remote Access related activities found on the devices in the selected preset by Cisco Cyber Vision.

- **Device Inventory**: This report is an automated summary that captures the devices, their risk profile, and the inventory distribution summary found in the selected preset by Cisco Cyber Vision.

Step 6 (Optional) Add a **Customer logo**.

It will appear on the report.

Note
If no customer logo is uploaded, the default Cisco logo will be used.

Step 7   Choose the **Format**.

Step 8   Click **Next**.

Step 9   Click the drop-down arrow of **Preset** and choose a preset.

Step 10   In the Table of content, select the checkboxes of the sections and sub-sections you want to appear in the report.

Note
Content (sections and sub-sections) will vary depending on the type of report selected.

Step 11   Click **Save and Run**.

The new report appears in the list with the **Status: Processing**. When done, **Success** appears.

Step 12   To see the new report, choose **Reports** from the main menu.

Step 13   To download the report, click the name of the report under the **Name** column.

Step 14   In the **Details** panel, click the links to download the latest reports.

The **Previous Reports** tab contains older reports.

Step 15   To generate a new report, click the ellipsis (…) under the Actions column and then click **Run Again**.

Events

To access the **Events** page, choose **Admin** > **Events** from the main menu. Use Events to identify and track significant activities on the network. Events can be an activity, a property, or a change—whether it involves software or hardware components.

You can customize the severity of events on the **Events** administration page. By default, changes apply only to future events. However, you can apply new customized severities to past events by enabling the **Apply severity to existing events** option.

☞

Important   This action is irreversible and can take several minutes to complete.

Click **Reset severity to default** to reset the severity settings.

Use the toggle buttons to enable or disable **Syslog export** and **Database storage**. These two options are active by default. However, make sure Syslog Configuration before the export.

The following are examples of events:

- A wrong password entered on the GUI

- A new component connected to the network

- An anomaly detected in the Monitor Mode

- A component detected as vulnerable

The Dashboard of Events

The **Dashboard** shows event doughnut and line charts. Doughnut charts display color-coded event severity categories and percentages. To access the Events dashboard, choose **Events** from the main menu. You can use the filter at the top-right corner of the Events page to filter events by **Day**, **Week**, **Month**, or **Year**. Use the arrows for specific dates.

Doughnut charts present event numbers and percentages by category and severity.

Click a doughnut to see detailed The List of Events view filtered by the corresponding category and severity, allowing you to quickly access more event details.

To see the list of events per category, from the main menu, choose **Admin** > **Events**. See Events.

You find the Events graph at the bottom of the dashboard page. Use the filter in the top right corner to view data by **Day**, **Week**, **Month**, or **Year**. Hover over the event markers on the line chart to see event counts by category for specific dates. On the left of the graph, three tabs appear: **Cisco Cyber Vision Operations**, **Inventory Events**, and **Security Events**. Click these tabs for more details.

The List of Events

List is a chronological view in which you can see and search events. Use the search bar to find events by MAC and IP addresses, component name, destination and source flow, severity and category. You can search the Events on **Day, Week, Month** or **Year**. Use the arrows for exact dates.

To access **List**, follow these steps:

1. From the main menu, choose **Events** > **List**.

2. Click an event result for more details about the event.

   a. When an event is related to sensors, click **See Sensor Statistics** for more details.

   b. When an event is related to component or an activity, click **see Technical Sheet** for more details.

Monitor

Cisco Cyber Vision provides a monitoring tool called the Monitor mode to detect changes inside industrial networks. Because a network architecture (PLC, switch, SCADA) is constant and its behaviors tend to be stable over time, an established and configured network is predictable. However, some behaviors are unpredictable and can even compromise a network's operation and security. The Monitor mode aims to show the evolution of a network's behaviors, predicted or not, based on presets. Changes, either normal or abnormal, are noted as differences in the Monitor mode when a behavior happens. Using the Monitor mode is particularly convenient for large networks as a preset shows a network fragment and changes are highlighted and managed separately, in the Monitor mode's views.
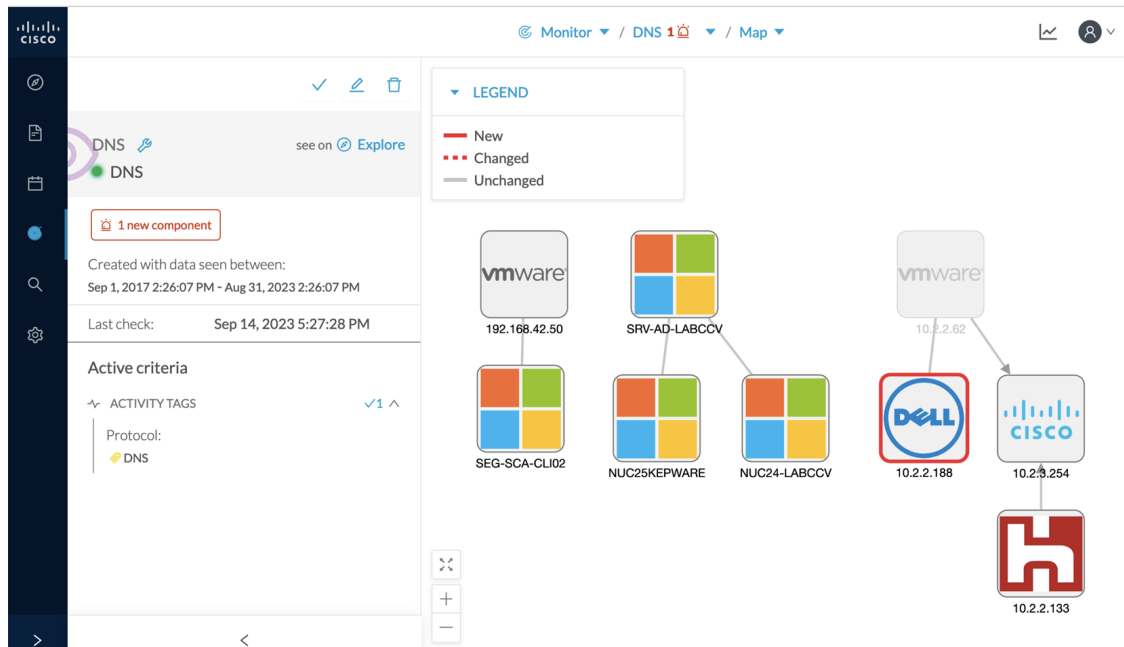
Search

Use **Search** to find components among unstructured data. Search components by name, custom name, IP, MAC, tag and property value. To access the **Search** page, choose **Search** from the main menu.

> ✎
>
> **Note**   Devices are not available in this page yet.

To search, enter the content in the search field and click **Search**.

To create a preset from your search results, click **Save this search as a Preset** . Presets will automatically update as new data is detected on the network.

For more information about a component, hover over it. The Technical Sheets **(2)** icon appears. The technical sheet gives you access to advanced data about the component.

System statistics

To access system statistics, click the **System statistics** icon in the top right corner of interface.
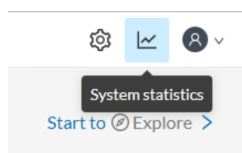
Center

The **Center** statistics view provides data about the state of the Center CPU, RAM, disk, network interfaces bandwidth and database.

Note   Use the drop-down arrow to change the time period.
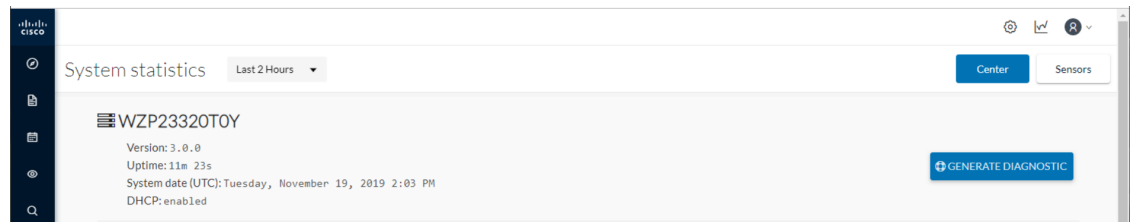
The **Center** interface shows general information about the Center (the software version, the length of time that it has been operating (i.e., uptime), the Center system date and whether DHCP is enabled or not.

Click **Generate diagnostic** to create a file to help troubleshoot issues and for produt support .
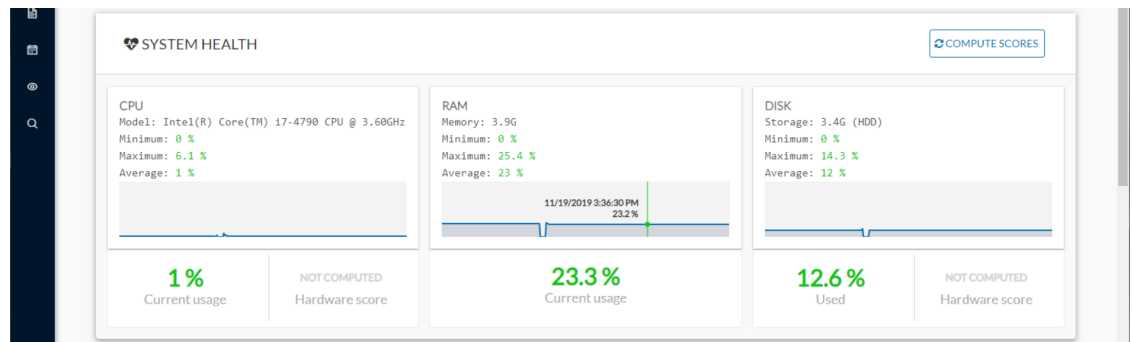
System Health

System health shows the status of the Center CPU, RAM and disk usage.

Usages (i.e., minimum, maximum and average) show for each of these system resources. For an absolute value, roll over the line chart.

The chart also shows the percentage of the system's Current usage and Hardware score, useful to product support.

The **Compute Scores** button initiates a new performance measure to compute a new score.

Network Interfaces Bandwidth
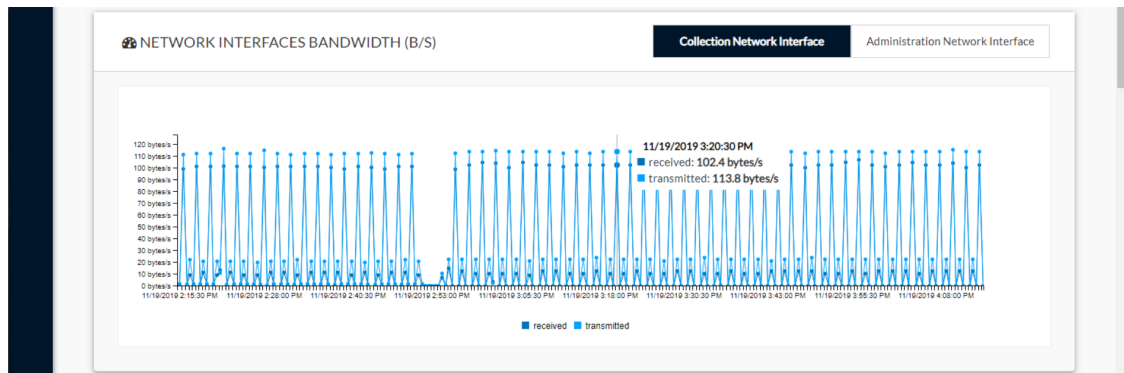
The line charts represent the Administration and Collection network interfaces bandwidth with the number of bytes received and sent by the Center per second.

For example, the Collection Network interface activity lets you see the amount of data exchanged between the Center and the sensors.

Disk I/O
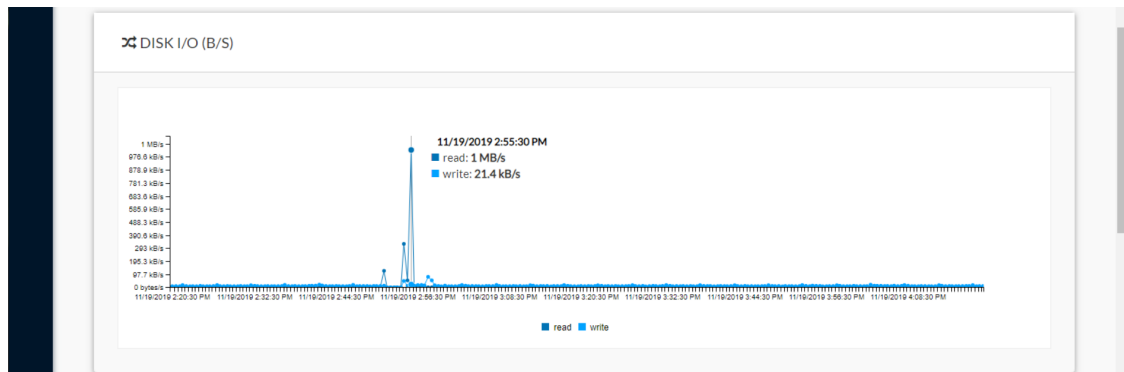
The line chart represents the Center hard disk usage in bytes/second.

Database
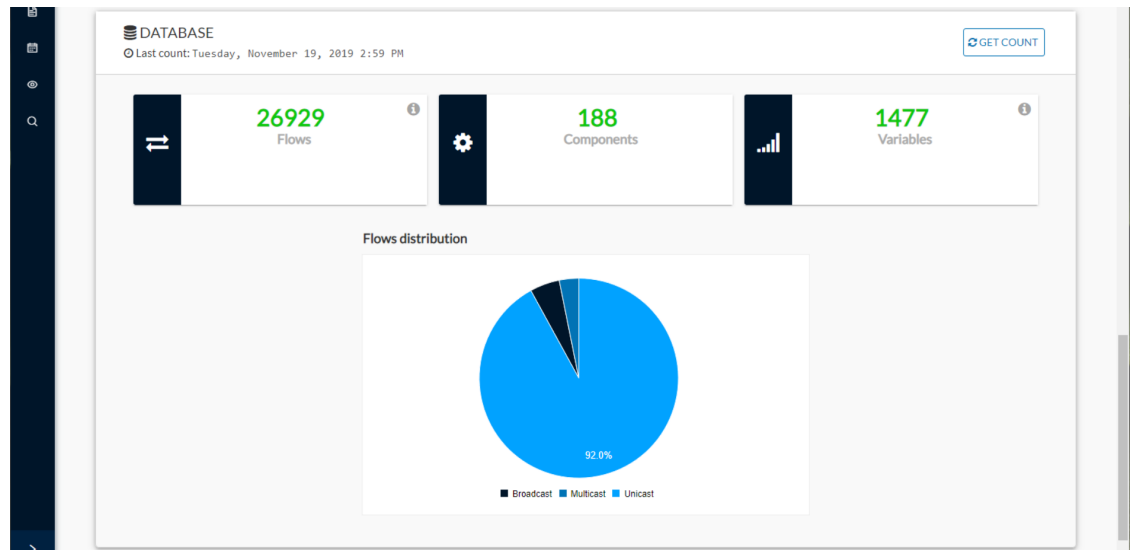
This section describes the database state by showing cards with the number of flows, components and variables that have been detected by Cisco Cyber Vision. Flows distribution is shown in a pie chart.

Data is updated each time you access the Center statistics view (the latest count is indicated on top of the database section). However, the Get Count button actualizes the database performance to the current time.

The flows card indicates the total number of flows (i.e. broadcast, multicast and unicast which are stored in the database) detected by . If you mouse over the card, you will get the number of activities and the flows evolution tendency. This information enables you to anticipate how the system load might be affected by flows in the future.

The variables card indicates the total number of variables detected by Cisco Cyber Vision. This indicator is important because an overload of variables could impact the Cisco Cyber Vision performances. If you mouse over the card you will get the number of process variables and the number of system variables.

- Process variables are the number of variables used by PLCs' software. Process variables are visible in the Monitor mode of the Cisco Cyber Vision GUI.

- System variables are the number of variables necessary to PLCs' proper operation. System variables are stored in the Cisco Cyber Vision database.
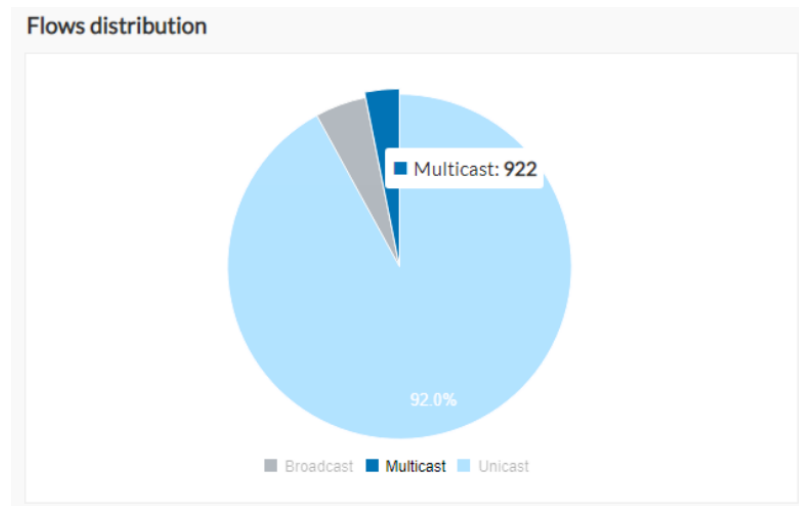
The flows distribution pie chart indicates the distribution of broadcast, multicast and unicast flows stored in the database. Mouse over the chart to see the absolute number of flows per flow type.

Services Statistics

The service status page indicates whether:

- all Cisco Cyber Vision background processes, such as services and extensions, are running correctly.

- all Cisco Cyber Vision background queues used to ingest data from sensors are not congested.

Checks are performed regularly.

Service Status:

This section shows the status of specific Cyber Vision services and extensions. Regular checks are conducted, and any service or extension that is down will be reported here.

- An **Update** button is available to refresh the services status; use it to ensure you have the latest information.

- A warning banner appears if a service is down, linking to this page, where the failing service is highlighted in red.

Queue Status:

This section shows the status of the queues. If the monitored queues drop messages, this section reports it. Only sensor queues are monitored.

A list of congested queues will be provided to indicate system performance issues. A warning banner appears at the top of the application when a queue is congested, with the queue name highlighted in red.

Sensors

The **Sensors** statistics view provides data about the CPU, RAM, disk, network interfaces bandwidth and packets captured for each sensor enrolled in Cisco Cyber Vision.

✎

Note Use the drop-down arrow to change the time period.

System statistics   Last 2 Hours ▼

FOC2222Y36C

🗗 FOC2222Y36C   Connected

S/N: FOC2222Y36C
Uptime: 5 minutes
IP address: 192.168.69.50
Version: 3.0.0+201911151747
Capture mode: Optimal

Center   Sensors

⚙ GENERATE DIAGNOSTIC

A list of the sensors appears on the left. Click a sensor name to access its statistics.

The **Sensors** statistics view shows general information about the sensor: the status (i.e., Connected), serial number, IP and MAC addresses, firmware version, the capture mode set, and the time it has been operating (i.e., uptime).

Click **Generate diagnostic** to create a file to help troubleshoot issues and for produt support.

System Health

System health shows the status of the sensor CPU, RAM and disk usage.

Usages (i.e., minimum, maximum and average) show for each of these system resources. For an absolute value, roll over the line chart.

💗 SYSTEM HEALTH

CPU
Minimum: 0 %
Maximum: 7.2 %
Average: 0 %

RAM
Minimum: 0 %
Maximum: 1.5 %
Average: 0 %

DISK
Minimum: 0 %
Maximum: 5.8 %
Average: 0 %

5.1 %
Current usage

1.5 %
Current usage

5.8 %
Used
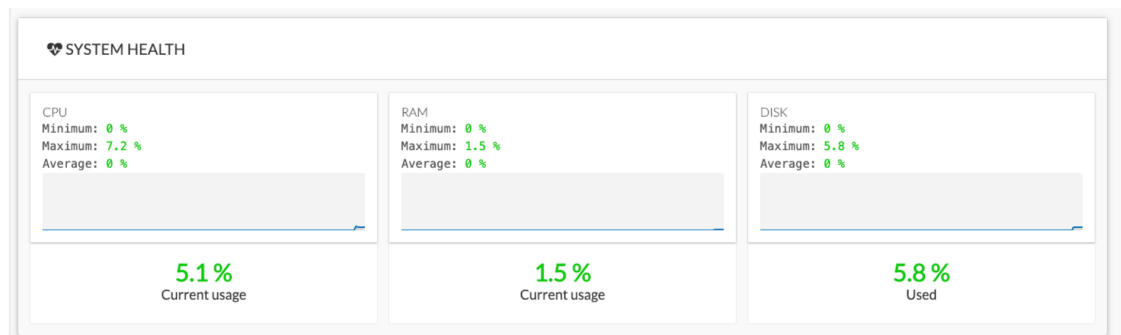
The chart also shows the percentage of the system's Current usage and Hardware score, useful to Cisco Cyber Vision product support.

Captured Packets
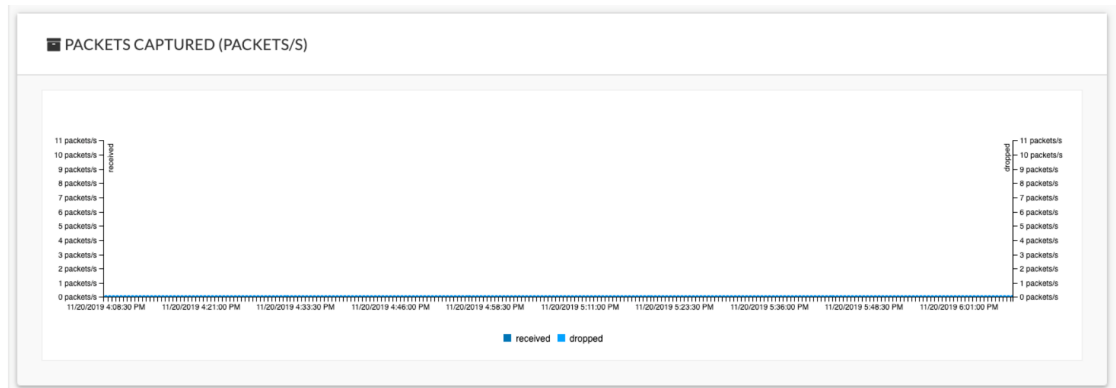
This line chart represents the number of packets that the sensor captures on the Industrial network interface (in bytes per second). It also shows dropped packets, but the value should be zero. If the dropped line shows activity, the sensor is overloaded and is not capturing traffic.

Network Interfaces Bandwidth

The line charts represent the Collection and Industrial network interfaces bandwidth with the number of bytes received and sent by the Center per second.

- The Collection Network interface activity chart shows the amount of data exchanged between the Center and the sensors.

- The Industrial cahrt shows the amount of data captured by the sensor on the industrial network through each port's couple.

  Data sent to the Industrial network is also represented, but the value should be zero. If the transmitted line shows activity, the sensor is not passive. If this happens, please contact Cisco Cyber Vision support immediately.

Disk I/O

The line chart shows the sensor hard disk usage with the number of Read-Write bytes per second.

My Settings

You must create your personal account in Cisco Cyber Vision Center. To create personal account, follow these steps:

1. Go to the user menu at the top right corner and click the drop-down arrow.

2. Click **My Settings** from the drop-down list.

    The **My Settings** page appears.

3. Enter **Firstname** and **Lastname** under the **General** fileld.

4. Click the radio button of the preferred interface language under the **Language** filed.

5. Enter your password.

    Passwords must contain at least 6 characters and comply with the rules below. Passwords:

    • Must contain a lower case character: a-z.

    • Must contain an upper case character: A-Z.

    • Must contain a numeric character: 0-9.

    • Cannot contain the user ID.

    • Must contain a special character: ~!"#$%&'()*+,-./:;<=>?@[]^_{|}.

Important   Change your password regularly to ensure platform and industrial network security.

Note   Your email will be requested for login access.

6. Select the checkbox of **Restore default parameters** to restore interface notifications.

7. Clear application cookies.

Risk Score

Risk Score Definition

A risk score is an indicator of the good health and criticality level of a device. The scale is from 0 to 100 with a color code indicating the level of risk.

Score	Color	Risk level
From 0 to 39	Green	Low
From 40 to 69	Orange	Medium
From 70 to 100	Red	High

Risk scores apply to the following:

- Filter criteria

- Device list

- Device technical sheet

- Device risk score widget (Home page)

- Preset highlight widget (Home page)

Risk Score Use

Risk score helps you easily identifying which devices are the most critical within the overall network. It provides limited and simple information on the cybersecurity of the monitored system. It is a first step in security management by showing values and providing solutions to reduce them. The goal: minimize values and keep risk scores as low as possible.

Proposed solutions are:

- Patch a device to reduce the surface of attack

- Remove vulnerabilities

- Update firmware

- Remove unsafe protocols whenever possible (e.g., FTP, TFTP, Telnet),

- Install a firewall

- Limit communications with the outside by removing external IPs

Cyber Vision allows you to define the importance of the devices in your system by grouping them and setting an industrial impact. This function increases or decreases the risk score, allowing you to focus on the most critical devices.

All these actions reduce the risk score which affect its variables, i.e., the impact and the likelihood of a risk. For example, removing unsafe protocols will affect the likelihood of the risk, but patching a device will act on the impact of the risk.

Risk score presents an opportunity to update usage and maintenance habits. However, it is NOT intended to replace a security audit.

In addition, risk scores are used in Cisco Cyber Vision to sort out information by ordering and filtering criteria in lists and to create presets.

Risk Score Computation

Risk score is computed as follows:

Risk = Impact x Likelihood

Impact is the device "criticality", that is, what is its impact on the network? Does the device control a small, non-significant part of the network, or does it control a large, critical part of the network? Impact depends on:

- Device tags: Some device types are more critical. Each device type (or device tag) or device tag category is assigned an industrial impact score by Cisco Cyber Vision. For example, the device is a simple IO device that controls a limited portion of the system or it is a Scada that controls the entire factory. These will not have the same impact if they are compromised.

- You effect the device impact by moving it into a group and setting the group's industrial impact (from very low to very high).

Likelihood is the probability of this device being compromised Likelihood of risk depends on the following:

- Device activies and the activity tags. Some protocols are less secure than others. For example, Telnet is less secure than ssh.

- The exposure of the device communicating with an external subnet.

- Device vulnerabilities, taking into account their CVSS scoring.

For detailed information about a risk, see **Details** tab inside the technical sheet.

How to take action:

1. From the main menu, choose **Explore**.

2. Click the drop-down arrow in the top navigation bar and select **All Data** under **Basics**.

3. Click the drop-down arrow in the third filter of the top navigation bar and select **Device List**.

4. In the **Risk score** column, click the sort arrow to display the highest risk scores.

5. Click a device name under the **Device** column.

   The right-side panel appears.

6. In the **Risk score**, click **See details**.

   The technical sheet appears.

   In the **Overview** tab, the **Current** risk score and the **Achievable** risk are displayed.

   The achievable risk score is the best score you can reach if you patch all vulnerabilities on the device and remove all potential insecure network activities. The score cannot be zero because devices have intrinsic risks coming from their device type and, if applicable, their group industrial impact.

The **Details** tab shows further information about the different risks impacting the device, the percentage of the risk they represent within a total risk score, and the solutions to reduce or even eliminate them.

Device type and **Group impact** affect the risk impact variable. **Activities** and **Vulnerabilities** affect the risk likelihood.
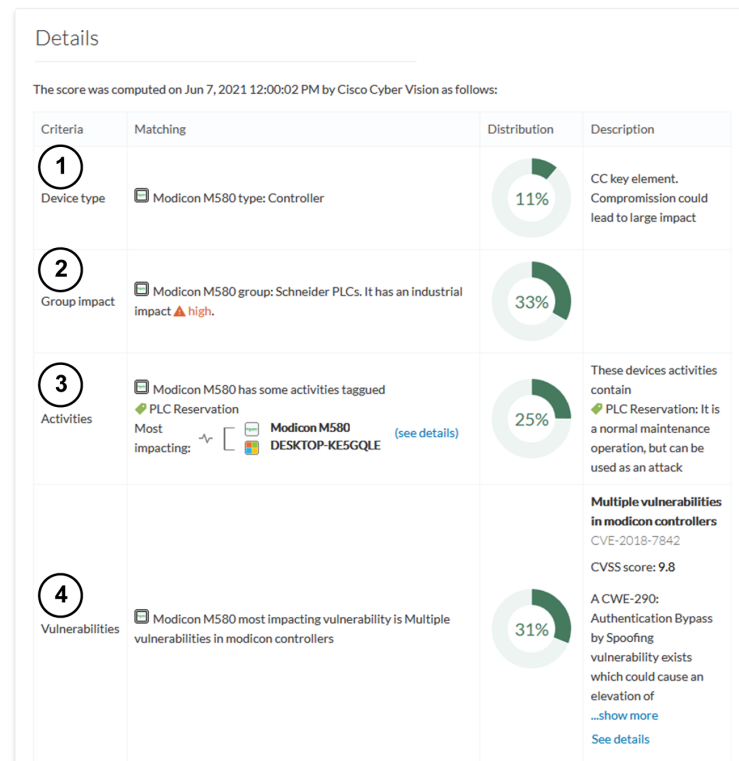
This page shows the last time the risk score was computed by Cisco Cyber Vision. Risk score computation occurs once an hour. To force immediate computation, use the following command on the Center shell prompt:

```
sbs-device-engine
```

Below is an example of the information retrieved during the last computation.

- **Device type**: Each device type corresponds to a Tags detected by Cisco Cyber Vision. No action is required at the device type level because each device tag is assigned a risk score by default.

- **Group impact**: Action is possible if the device belongs to a group. Decrease the impact by lowering the industrial impact of the group that the device belongs to.

  For example, if you set the group industrial impact to very low (previously high), the overall risk score decreases from 80 to 54.
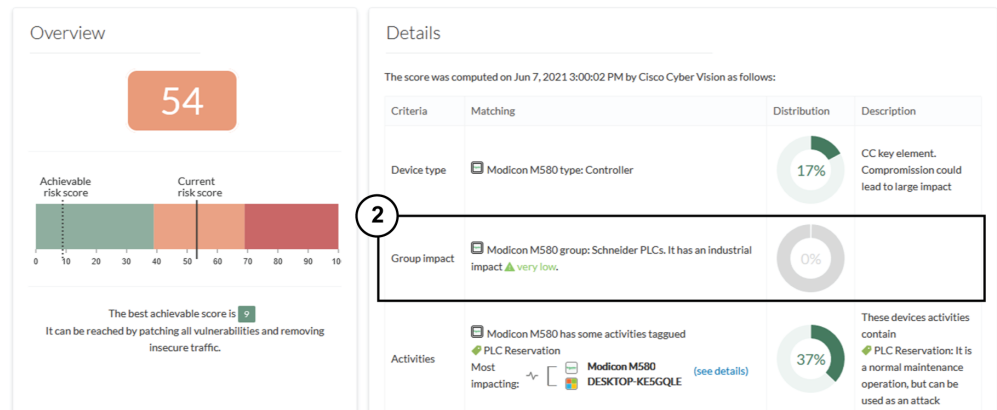
Risk Score

> **Note** The new industrial impact will factor into the next risk score computation (once an hour).

- **Activities**: The most impactful activity tag displays. To lower the risk, remove all potential insecure network activities.

- **Vulnerabilities**: Click the **See details** link for more information about how to patch the vulnerabilities and so reduce the device risk score.

By taking these actions, the risk score should decrease considerably.

Licensing

Cisco Cyber Vision Licenses

Manage your Cisco Cyber Vision smart licenses through the Cisco Smart Software Manager (CSSM), a centralized platform to track and manage all your Cisco licenses. You have real-time visibility into license usage and availability to help easily optimize and scale usage while ensuring compliance.

The set of Cisco Cyber Vision licenses include licenses for the center, sensor hardware appliances, and Talos subscriber licenses to run intrusion detection services on the sensors. For more information about the Cisco Cyber Vision license types and how to order them, see the Cisco Cyber Vision Data Sheet.

This document guides you through the registration and activation of the Cisco Cyber Vision Center licenses, Essentials, and Advantage.

You can also use CSSM satellite servers or Specific License Reservations for air-gapped networks that do not have a persistent internet connection.

Specific license reservations require special permissions. Contact your Cisco account manager if you require this license type.

Trial Licenses for Cisco Cyber Vision

When you install a Cisco Cyber Vision Center release for the first time, the evaluation mode is enabled by default. The evaluation mode is valid for 90 days and you have access to all the Cisco Cyber Vision features during this time. At the end of the 90 days, you must register a valid Cisco Cyber Vision license to continue using the center.

The evaluation mode is active automatically on a fresh install of Cisco Cyber Vision. To view the details of your evaluation mode, log in to your Cisco Cyber Vision center, and choose **Admin** > **License**. The page

displays the number of days remaining in the evaluation mode, and you can start registering your smart licenses when you are prepared to do so.

When the evaluation licenses expire, you can only access the **License** page of the Cisco Cyber Vision center. You can't access any other page until you register valid licenses.

Essentials and Advantage Licenses

Cisco Cyber Vision Center licenses are available in two tiers, Essentials and Advantage. Each tier enables a set of features, with the Advantage license enabling a wider set of features that includes the features mapped to the Essentials license.

Features enabled by Cisco Cyber Vision Essentials license

Inventory

- Device inventory

- Identify communication patterns

- Generate inventory reports

Vulnerability

- Identify device vulnerabilities

- Generate vulnerability reports

Activities

- Track control system events

- Generate device activity reports

RESTful API: REST API programming interface

Features enabled by the Cisco Cyber Vision Advantage license

It includes Essentials features, plus:

Security posture: Device Risk Scoring

Intrusion detection

- Snort IDS on supported sensors

- Talos community signatures (New rules may be added 30 days after release)

Behavior monitoring

- Create baselines for asset behaviors

- Alerts on deviations

Advanced integrations

- XDR Ribbon

- pxGrid integration with Cisco ISE

- Firepower Host Attribute integration

- SIEM Integration – Splunk, IBM QRadar

- ServiceNow OT Management integration

Licenses for Intrusion Detection System Components

The Cyber Vision intrusion detection system (IDS) components use the following licenses to enable Talos subscriber rules. Each appliance or sensor in your network that has the IDS service enabled on it consumes a license.

License ID	Purpose of License
CV-IDS-CNTR	Talos subscriber rules license for Cyber Vision Center IDS (hardware and virtual appliance)
CV-IDS-IC3000	Talos subscriber rules license for Cyber Vision IDS on IC3000-2C2F-K9 sensors
CV-IDS-IR8300	Talos subscriber rules license for Cyber Vision IDS on Cisco Catalyst IR8300 sensors
CV-IDS-C9000	Talos subscriber rules license for Cyber Vision IDS on Cisco Catalyst 9300, 9300X, or 9400 sensors

Cisco Smart Software Manager Satellite for Air-Gapped Networks

Smart licensing typically requires an active communication channel between Cisco Cyber Vision and the Cisco Smart Software Manager (CSSM). If you cannot allow a direct Internet connection for your center, you can set up a Cisco Smart Software Manager satellite on your premises.

The satellite server contains a subset of Cisco Smart Software Manager functionality and must communicate with the latter periodically to operate.

Synchronize your satellite server with the Cisco portal periodically so that the most recent license purchase and utilization data are updated in both systems. For more information, see General CSSM On-Prem Help.

Register Your Essentials or Advantage Licenses

Before you begin

After your purchased licenses are available in your Cisco Software Central account, you must make note of the product registration token and the transport gateway URL (if applicable) to register your Cisco Cyber Vision center with the organizational smart licensing account.

Product registration tokens link new product instances to a virtual account. The Cisco Software Central account for your organization would typically contain all the Cisco licenses purchased. To link a new product instance to the organizational smart licensing account, use a product registration token:

1. Log in to your Cisco Software Central account.

2. From the main menu, choose **Inventory** > **Licenses**.

3. The **Product Instance Registration Tokens** area lists all the tokens that are already generated for this smart licensing account.

   a. To use an existing token, from the **Actions** column for a token, click **Copy**.

   b. To create a new token, click **New Token**.

   c. Copy the product token.

4. (Optional) If you want to use the Transport Gateway connection method, click **Smart Transport Registration URL** to copy the registration URL.

Procedure

Step 1 Log in to your Cisco Cyber Vision center.

Step 2 From the main menu, choose **Admin** > **License**.

Step 3 To choose the license tier (Essentials or Advantage), click **View/Edit** next to the **Software Subscription Licensing** under the **Status** field.

Step 4 Enable the toggle button in the displayed dialog box to choose a license tier.

Step 5 Click **OK**.

Step 6 To choose a connection method, click **View/Edit** next to the **Transport Settings**.

The **Transport settings** pop-up appears.

Step 7 Click the radio button to select **Transport settings**.

There are three types of transport settings, as given below:

- **Direct**, to connect to Cisco licensing servers through a direct HTTP connection if you have a persistent internet connection.

- **Transport Gateway**, to connect to Cisco licensing servers through Transport Gateway. In the **URL** field, enter the Smart Transport Registration URL you copied from Cisco Software Central.

- **HTTP/HTTPS Proxy,** to connect to Cisco licensing servers through a proxy server. Enter the details of the proxy server to use for this purpose.

Step 8 Click **OK**.

Step 9 In the registration dialog box, enter the **Product Instance Registration Tokens** that you copied from Cisco Software Central account.

Step 10 Click **Register**.

Register Licenses With CSSM On-Prem

Before you begin

For information on configuring a CSSM on-premises satellite, see Cisco Smart Software Manager. After the CSSM satellite is set up, make note of the product registration token and the transport gateway URL (if applicable) to register your Cisco Cyber Vision center with the CSSM satellite.

Product registration tokens link new product instances to a smart licensing account. The CSSM on-premises satellite collects licensing data and shares the same with the Cisco Software Manager at the configured syncs.

1. Log in to your CSSM On-Prem License Workspace.

2. From the main menu, choose **Inventory** > **Licenses**.

3. The **Product Instance Registration Tokens** area lists all the tokens that are already generated for this smart licensing account.

   a. To use an existing token, from the **Actions** column, click **Copy**.

   b. To create a new token,

      1. Click **New Token**.

      2. Enter a description, an expiry date and a maximum number of token uses.

      3. Click **Create Token**.

      4. The newly created token is added to the list. To copy the token, click **Actions** and choose **Copy**.

4. (Optional) If you want to use the Transport Gateway connection method, click **Smart Transport Registration URL** and copy the registration URL.

Procedure

Step 1 Log in to your Cisco Cyber Vision center.

Step 2 Choose **Admin** > **License**.

Step 3 To choose a connection method, click **View/Edit** next to the **Transport Settings**.

The **Transport settings** pop-up appears.

Step 4 Click the radio button to select **Transport settings**.

There are three types of transport settings, as given below:

- **Direct**, to connect to Cisco licensing servers through a direct HTTP connection if you have a persistent internet connection.

- **Transport Gateway**, to connect to Cisco licensing servers through Transport Gateway. In the **URL** field, enter the Smart Transport Registration URL you copied from Cisco Software Central.

- **HTTP/HTTPS Proxy,** to connect to Cisco licensing servers through a proxy server. Enter the details of the proxy server to use for this purpose.

Step 5   Click **OK**.

Step 6   In the registration dialog box, enter the **Product Instance Registration Tokens** that you copied from Cisco Software Central account.

Step 7   Click **Register**.

Reregister Your Licenses

You may need to reregister your licenses to troubleshoot license reporting or usage issues. You can do this through the **Admin** > **License** page of the Cisco Cyber Vision center. Click the **Actions** drop-down list at the top-right corner of the License page, and click **Reregister**. Generate a registration token and follow the steps detailed in Register Your Essentials or Advantage Licenses.

Deregister Your Licenses

When you deregister your licenses, you enter the evaluation mode again. If the evaluation mode has no remaining days, the center considers your evaluation license as expired, and you have limited access to the Cisco Cyber Vision center.

You can deregister your licenses through the **Admin** > **License** page of the Cisco Cyber Vision center. Click the **Actions** drop-down list at the top-right corner of the License page, and click **Deregister**.

Use Specific License Reservation

Specific license reservation is a smart licensing method that you can use when your organization's security requirements do not allow a persistent connection between Cisco Cyber Vision center and the Cisco Smart Software Manager (CSSM). Specific license reservation allows you to reserve license entitlements on a center.

The process to create and register a specific license reservation spans across Cisco Cyber Vision center and Cisco Software Manager.

If you don't want to proceed with the license reservation after you generate the reservation request code in Cisco Cyber Vision center, in the **License** page, click **Cancel Reservation Code**.

If you lose the reservation request code you created in Cisco Cyber Vision center, in the **License** page, click **View Reservation Request Code**.

Before you begin

Specific License Reservation is not available by default. If you want to use this licensing method, contact your Cisco account team to get the permission to use specific license reservation. After you licensing method is granted, you can carry out the following task to register specific license reservation on your Cisco Cyber Vision center.

Procedure

Step 1 In the Cisco Cyber Vision center, choose **Admin** > **License**

Step 2 Click **Register**.

Step 3 In the statement **If your Smart Account is authorized for License Reservation and you wish to reserve licenses, start here.**, click **start here**.

Step 4 Click, **Yes, My Smart Account is License Reservation Enabled**.

Step 5 Click **Generation Reservation Request Code**.

Step 6 To copy the reservation code, click **Save to File** or **Copy to clipboard**.

Step 7 Log in to Cisco Software Manager, and from the main menu, choose **Smart Software Manager** > **Manage Licenses**.

Step 8 Choose **Inventory** > **Licenses** to view your purchased smart licenses.

Step 9 Click **License Reservation**.

A **Smart License Reservation** workflow dialog box is displayed.

Step 10 In the **Step 1: Enter Request Code** tab, in the field that is displayed, enter the reservation code you received from Cisco Cyber Vision center.

Step 11 Click **Next**.

Step 12 In the **Step 2: Select Licenses** tab, click the **Reserve a specific license** radio button. Then, in the **Reserve** column of the table displayed, for each license type, enter the number of license entitlements you want to reserve.

Step 13 Click **Next**.

Step 14 In the **Step 3: Review and Confirm** tab, review the details of your specific license reservation, and click **Generate Authorization Code**.

Step 15 The **Step 4: Authorization Code** tab contains a field that displays the authorization code in the XML format. This XML content includes information about the license reservation and the Cisco Cyber Vision center for which the SLR is generated. Click **Download As File** to download the .txt file to your local system.

Step 16 In the **License** page of your Cisco Cyber Vision center, click **Enter Reservation Authorization Code**.

Step 17 You can paste the contents of the .txt file in the text box, or click **Upload** and choose the .txt file that you downloaded from Cisco Software Manager.

Step 18 Click **Install Authorization Code/File**.

Update Specific License Reservation

If you need to update the details of your specific license reservation, create a new reservation code in Cisco Software Central. Then, register the license reservation through the Cisco Cyber Vision center.

Procedure

Step 1 Log in to Cisco Software Manager, and from the main menu, choose **Smart Software Manager** > **Manage Licenses**.

Step 2 Choose **Inventory** > **Product Instances** to view the product instances that report license usage to Cisco Software Central.

Step 3   Find the Cisco Cyber Vision center for which you want to update the license reservation, and click the **Actions** drop-down menu in the same row.

Step 4   Click **Update Reserved Licenses**.

Step 5   In the **Step 1: Select Licenses** tab, click the **Reserve a specific license** radio button. Then, in the **Reserve** column of the table displayed, for each license type, enter the number of license entitlements you want to reserve.

Step 6   Click **Next**.

Step 7   In the **Step 2: Review and Confirm** tab, review the details of your specific license reservation, and click **Generate Authorization Code**.

Step 8   The **Step 3: Authorization Code** tab contains a field that displays the authorization code in the XML format. This XML content includes information about the license reservation and the Cisco Cyber Vision center for which the SLR is generated. Click **Download As File** to download the .txt file to your local system.

Step 9   In the Cisco Cyber Vision center, choose **Admin** > **License**

Step 10   Click **Update Reservation**.

Step 11   Enter the authorization code for the updated license reservation.

Step 12   Click **Register**.

Return Specific License Reservation

When you return a specific license reservation, the reserved licenses are released and available in your smart licensing account for reuse. You can use them as smart licenses or as part of another license reservation.

Procedure

Step 1   In the Cisco Cyber Vision center, choose **Admin** > **License**.

Step 2   Click **Return Reserved Licenses**.

Step 3   Click **Generate Reservation Return Code**.

Step 4   Copy the code displayed in the text box.

Step 5   Click **Return License**.

Step 6   Log in to Cisco Software Manager, and from the main menu, choose **Smart Software Manager** > **Manage Licenses**.

Step 7   Choose **Inventory** > **Product Instances** to view the product instances that report license usage to Cisco Software Central.

Step 8   From the **Actions** drop-down list for your specifc license reservation, choose **Remove**.

Step 9   Enter the reservation return code that you copied in Step 4, from Cisco Cyber Vision center.

Step 10   Click **Remove Product Instance**.

Managed Services License Agreement

Managed Services License Agreement (MSLA) is a post-paid utility service model for network providers who are Cisco partners. Through the MSLA licensing method, you pay for what you use, at the end of a

monthly billing cycle. The provider holds the license entitlements and can enable or register licenses for multiple customers' centers.

In a Cisco Cyber Vision center that uses a MSLA license, you must set the center to utility mode. In the **Admin** > **License** page of the center, from the **Actions** drop-down list, choose **Change Utility Mode**.

There is no difference in the license registration process through the Cisco Cyber Vision center. The process outlined in the task Register Your Essentials or Advantage Licenses, on page 67 applies to MSLA licenses as well.

License Usage Compliance

Cisco Cyber Vision Essentials and Advantage licenses are typically term subscriptions for 1, 3, 5, or 7 years. To continue using Cisco Cyber Vision's many features and to receive product support, you must renew your licenses. If your Essentials or Advantage license expires, an alert is displayed in your Cisco Cyber Vision center to notify you of license expiry until you register new licenses.

In some noncompliance license usage scenarios, you can only access the **License** page in the Cisco Cyber Vision center until you purchase new licenses and register them. Existing configurations continue to run in your network even while your access is restricted.

- Your evaluation license has expired.

- You return your specific license reservation, and no other valid licenses are registered in your center.

- Your Essentials or Advantage licenses have expired, and you use the Cisco Smart Software satellite connection method.

If your IDS licenses expire or if overconsumption is reported because IDS is enabled on more sensors than you have licenses, a warning message is displayed in your Cisco Cyber Vision center until the issue is resolved.

Get Started with Cisco Cyber Vision

Certificate Fingerprint

Use the certificate fingerprint to register a **Global Center** with its synchronized centers and vice versa. To access the **Center Fingerprint**, choose **Admin** > **System** from the main menu. Click the copy icon to copy the **Fingerprint** and enroll your center with a global center.

For more information, refer the Centers Installation Guides.

Data Management

The **Data Management** interface allows you to do the following: manage data stored on Cisco Cyber Vision by Clear Data to optimize the Center performances, Expiration Settings, and Ingestion Configuration. To access Data Management, choose **Admin** > **Data Management** from the main menu.

The Cisco Cyber Vision update procedure will not purge data automatically. The Center's 3.2.x database will be migrated to the new 4.0.0 schema. All components, activities, flows, events, etc. will be migrated. Since the migration process can take hours (from 1 to 24 hours), you can perform a data purge in release 3.2.x to shorten the migration process. Launch the purge either from the Clear Data page or from the Command Line Interface (CLI), using the following command. Also, different options are offered.

```
sbs-db --help
```

Once migrated, the database content is managed with version 4.4.1 new data retention policies. Expiration settings apply. By default, the system will purge the following:

- Events after 6 months

- Flows after 6 months

- Variables after 2 years

☞

Important   You have 3 days once the migration from 3.2.x to 4.0.0 is done to set Expiration Settings as needed, before the default settings are applied by the system.

Clear Data

Clear data stored on Cisco Cyber Vision to optimize the Center's performances. You can clear data partially or completely, as follows:

- All data

- Components selection and associated data (refer to Purge Components, on page 76)

- Activities, Flows and Variables

- Flows and Aariables

- Variables

To clear data, choose **Admin** > **Data Management** > **Clear Data** from the main menu.

Clear data **very carefully**. Clearing any data can impact monitoring of the network. Please read the implications about all data clearance below.

Data Clearance

Use **Clear All data** as a last resort, in case of database overload issues. This action results in the deletion of the entire database content. Network data such as components, flows, events, and baselines are deleted from Cisco Cyber Vision and the GUI becomes empty. All configurations are saved. Existing users and user data configurations (such as capture modes, event severity setup, syslog configuration) persist.

Purge Components

In Cisco Cyber Vision, a component represents an object of the industrial network from a network point of view. It can be the network interface of a PLC, a PC, a SCADA station, or a broadcast or multicast address. The system protects itself by limiting the number of components stored in the database.

When the system reaches over 120,000 components, a pop-up and red banner alert appear to inform you that a purge is required. Components purge is based on several criteria.
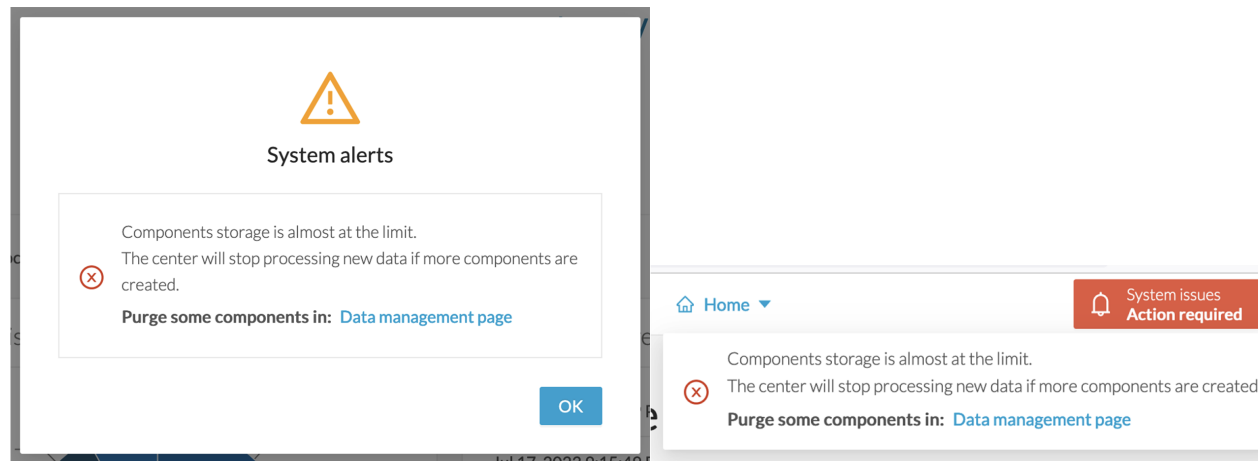
If the system reaches 150,000 components, ingestion stops. The system deletes incoming sensor data without processing or storing it. A pop-up and a red banner alert appear to inform you that a purge is required.
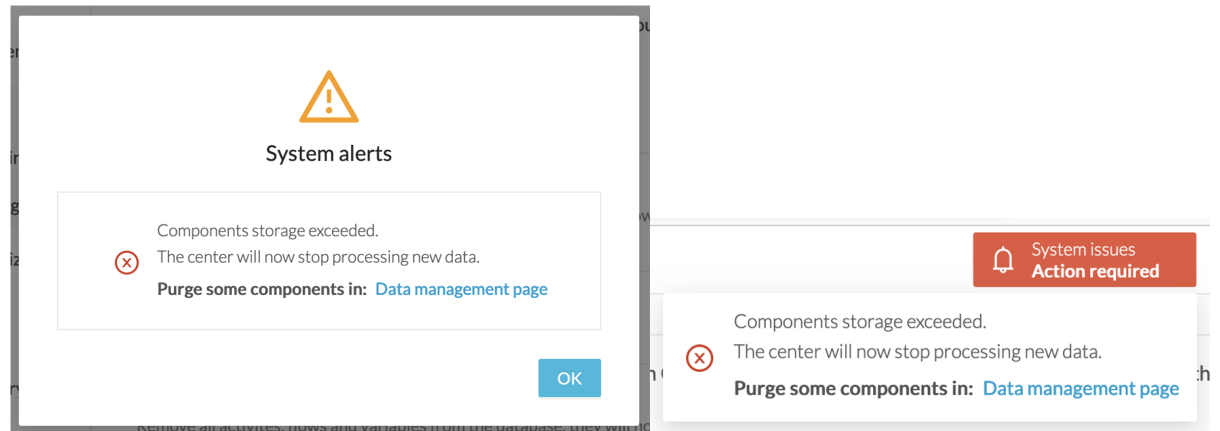
To purge components:

Procedure

Step 1   From the main menu, choose **Admin** > **Data Management** > **Clear Data**.

Step 2   Click the **Components selection** radio button.

Step 3   Select the component type (**IT** or **OT**).

Step 4   Enter the **IP Subnet**.

Step 5   Click the calendar icon to add an **Inactivity since** date.

Step 6   Click the calendar icon to add a **Creation time** date.

Step 7   Click the calender incon to add a **End Time (optional)** date.

Step 8   Click **Clear data**.

Expiration Settings

To configure the **Expiration Settings**, choose **Admin** > **Data Management** > **Expiration Settings** from the main menu.

On this page, you can manage the duration for which data and reports remain available. Select expiration times for reports and their versions. Use the drop-down menu to choose expiration periods of 3 months, 6 months, 1 year, 2 years, or 3 years. You can also set the maximum number of report versions from 1 to 100.

Note Selecting a high value may rapidly fill up storage and adversely affect system performance. The recommended value is 10 versions.

Ingestion Configuration

The **Ingestion Configuration** page allows you to configure flow and variable traffic storage. You can choose whether to store flows and variables. Flows and variables storage is disabled by default.

To access the **Ingestion Configuration**, choose **Admin** > **Data Management** > **Ingestion Configuration**from the main menu.

Messages can appear in Cisco Cyber Vision's user interface to indicate to the user that features may be limited due to absence of flows in the database. For example, in the activity technical sheet, at the top of the flows table:

In this case, you can click **Go to flow storage settings** and enable **Flow Storage**.

If **Flow Storage** is enabled, it is possible to choose from which subnetworks flows should be stored. These subnetworks can be set on the Network Organization page. The option "others" includes flows that are not part of the industrial private network.

An automatic purge will occur on selected flows when a period of inactivity exceeds 7 days.

You can click the **Flows Aggregation** and **port scan detection** toggle buttons to enable them.

Users

Management

You can create, edit and delete users through the **Users management** page. To access the **Users management** page, choose **Admin** > **Users** > **Management** from the main menu.

During their creation each user must be assigned with one of the following user roles (from full rights to read-only) or with a custom role (refer to Role Management).

- **Admin**

    The Admin user has full rights on the platform. Users who have this role assigned oversee all sensitive actions like user rights management, system updates, syslog configuration, reset and capture modes configuration on sensors.

- **Product**

    The product user has access to several features of the system administration page (i.e. the system, sensors and events administration pages). This access level is for users who manage sensors from a remote location. In addition, they can manage the severity of events and, if enabled by the Admin user, can manage their export to syslog.

- **Operator**

    This access level is for users who use the Monitor mode and manage groups but do not have to work with the platform administration. Thus, the Operator user has access to all pages, except the system administration page.

- **Auditor**

    This access level provides read-only access to the Explore, Reports, Events and Search pages. Auditors can use sorting features (such as search bars and filters) that do not require persistent changes to the data (unlike Autolayout), and generate reports.

You can create as many users as needed with any user rights. Thus, several administrators can use and administrate the whole platform. To access the **CREATE A NEW USER** window, choose **Admin** > **Users** > **Management** from the main menu. Click **Add a new user**, and the window appears.

However, each user must have their own account. That is:

- Accounts must be nominative.

- One email address for several accounts is not allowed (note that email will be requested for login access).

    Passwords must contain at least 6 characters and comply with the rules below. Passwords:

    - Must contain a lower case character: a-z.

• Must contain an upper case character: A-Z.

• Must contain a numeric character: 0-9.

• Cannot contain the user id.

• Must contain a special character: ~!"#$%&'()*+,-./:;<=>?@[]^_{|}.

Important Passwords should be changed regularly to ensure the platform and the industrial network security.

Passwords' lifetime is defined in the Security Settings.

You can create custom user roles in the Role Management.

You can map Cisco Cyber Vision user roles with an external directory's user groups in the LDAP settings page.

Role Management

In addition to the four Cisco Cyber Vision default roles (i.e. Admin, Auditor, Operator and Product), customized roles can be created and modified from the Role management page. To access the **Role management** page, choose **Admin** > **Users** > **Role Management** from the main menu.

These roles will help you defining specific privileges and accesses for each group of users.

Default roles cannot be edited or deleted.

You can map Cisco Cyber Vision custom roles with an external directory's user groups in the LDAP settings page.

Create Roles

This section explains how to create customized user roles on Cisco Cyber Vision. The user roles can later be mapped to groups in Active Directory.

Procedure

Step 1 From the main menu, choose **Admin** > **Users** > **Role Management**.

Step 2 Click the + button at the end of the user roles.

A **NEW ROLE** tab appears.

Step 3 Enter a **Role Name** and **Description** in their respective fields.

Step 4 Click the dropdown arrow from the **Search/Add existing permission** field.

Step 5 Select an existing role from the dropdown list, or click **Add New Permissions** to build the new user role from scratch.

Step 6 Check the checkboxes to select or deselect permissions from the **Administrative Rights** list as read or write.

Hover over "i" icon next to the **Administrative Rights** to know all the rights.

Step 7 Click **Save**.

A message **User role has been created successfully** appears.

The new user role is displayed in the tab list.

Note
You can modify or delete directly in the tab.

What to do next

Custom roles created can be mapped with an external directory's user groups in the LDAP settings page.

Security Settings

From the **Users security settings** page, you can configure the security settings of users' password, such as its lifetime, the number of authorized login attempts, and the number of days before a password can be reused, etc.

To access **Users security settings**, from the main menu, choose **Admin** > **Users** > **Security settings**.

Center Web Server Certificate

The **Center web server certificate** page is to configure Cisco Cyber Vision user interface security with an enterprise certificate. You will have the option to upload a .p12 or to generate a CSR.

To access **Center web server certificate** page, from the main menu, choose **Admin** > **Web Server Certificate**.

For more information, see to the corresponding Center Installation Guide.

CHAPTER 5

Configure Cisco Cyber Vision

Network Organization

Network Organization page allows you to define the subnetworks inside the industrial network by setting up IP address ranges and declaring whether networks are internal or external. To access the **Network Organization** page, choose **Admin** > **Network Organization** from the main menu.

In Cisco Cyber Vision, all private IP addresses are classified as OT internal. They appear under the **IP Address / Subnet** column on the Network Organization page.

Every other IP address is considered as external, except for:

- Broadcast IPv4: 255.255.255.255

- IPv4 and IPv6 zero: 0.0.0.0 et 0:0:0:0:0:0:0:0

- Loopback IPv4 and IPv6: 127.0.0.1 and ::1

- Link Lock Multicast IPv4 and IPv6: 224.0.0.0/8 and ff00::/8

If you want to declare a public IP address as internal, you must add an exception by changing their network type.

Declaring a subnetwork as OT internal is useful in case public IP addresses are used in a private network of an industrial site. Conversely, declaring a set of IP addresses as external will exclude their flows from the database, and exclude their devices from the license device count and the risk score.

Overall, defining subnetworks in Cisco Cyber Vision is useful for several reasons:

- It allows you to choose afterwards how related flows should be stored through the Ingestion Configuration. Excluding unnecessary flows will have positive impact on performances.

- It will impact devices' Risk Score, since a private network is considered as safer than an external one.

• Cisco Cyber Vision's license will be more accurate, because devices from an external network will be excluded from the licensing device count.

By default, Cisco Cyber Vision groups identical IP addresses detected inside the industrial network into a single device, because in most cases these belong to several components of a device. However, it can happen that the same IP address is used by several devices. In this case, you can choose to select the first option when declaring a subnetwork to prevent duplicate IP addresses from grouping within this subnetwork.

The second option is to be used when components with the same IP address are found by different sensors. This happens when same addressing parameters are used on several subnetworks, for example in case of identical production lines. By using this option, components detected by different sensors will not be aggregated into a single device.

IP ranges can be **organized into groups** which subranges can be defined like in the example below:

IP Address / subnet	VLAN ID	Network Name	Network Type	Action
— 10.0.0.0/8		10/8 private network	IT Internal	✎ 🗑
10.2.0.0/22		OT range	OT Internal	✎ 🗑
10.4.0.0/22		External IP within IP range	External	✎ 🗑

Here, the user specified that the IP range 10.2.0.0/22 is OT internal and that 10.4.0.0/22 is external.

Thus, flow storage can be specificly set in the Ingestion Configuration, on page 78 for the IP range set here as OT internal, whereas flows and devices from the IP range set as external will be excluded from the database and the license device count and risk score.

Note   It is also possible to organize subnetworks through the API.

Define a Subnetwork

To define a subnetwork:

Procedure

Step 1   From the main menu, choose **Admin** > **Network Organization**.

Step 2   Click **Add a network**.

The **ADD A NEW NETWORK** pops-up appears.

Step 3 Enter an IP address range and its subnet in the **IP address/subnet** field.

Step 4 (Optional) Enter the **VLAN ID**.

This will allow you to create overlapping networks.

Step 5 Enter the **Network name**.

Step 6 Click the dropdown arrow of the **Network Type**.

Step 7 Select the network type from the dropdown list, such as **OT Internal**, **IT Internal**, or **External**.

Note

Setting the network type can impact Cisco Cyber Vision's performances by setting flow storage, device risk scores, and the license's device count.

Step 8 Check the **Use a device engine option for this network range** checkbox.

a) If applicable, select the radio button for the first option.

Note

Enable this option if several devices share the same IP across the monitored network.

Components will not be grouped by IP.

a) If applicable, select the radio button for the second option.

Note

Enable this option in case same addressing parameters are used within different subnetworks, for example, in identical production lines.

For that particular network range, the system will not aggregate components with the same IPs detected by sensors monitoring other subnetworks. The system will aggregate the components into devices when monitored subnetworks use the same IP ranges for several machines or production lines.

In this case, for a specific IP range, a component with an IP of that range seen by a sensor will be grouped with a component with the same IP only if both components are detected by the same sensor.

Step 9 Click **Add a network**.

API Token

Cisco Cyber Vision provides a REST API. To use it you first need to create a token through the API administration page.

A token is a random password which authenticates a request to Cisco Cyber Vision to access or even modify the data in the Center through the REST API. For instance, you can request the latest 10 components detected on Cisco Cyber Vision or create new references. Requests can be used by external applications like a SOC solution.

Note Best practice: create one token per application so you can remove or expire accesses separately.

To create API token, follow these steps:

1. From the main menu, choose **Admin** > **API** > **Token**.

2. Click + **New token**.

   The **Token** window appears.

3. Enter a name.

4. Use the **Status** toggle button to disable authorization for the token if you plan to use it later and want to prevent access until then.

5. Set an **Expiration time**.

6. Click **Create**.

   After the token creation, token appears in the list available on the **API** page.

7. Click **Show** to view the token.

8. Click copy icon to copy it.

For more information about the REST API refer to the REST API user documentation available on cisco.com.

API Documentation

This page is a simplified API development feature. It contains an advanced API documentation with a list of all possible routes that can be used and, as you scroll down the page to Models, a list of possible data responses (data type, code values and meaning).

In addition to information research, this page allows you to perform basic tests and call the API by sending requests such as GET, DELETE and POST. You will get real results from the Center dataset. Specifications about routes are available such as the route's structure, and parameters and arguments that can be set. An URL is generated and curl can be used in a terminal as it is.

However, for an advanced use, you must create an application that will send requests to the API (refer to the REST API documentation).

☞

Important All routes other than GET will modify data on the Center. As some actions cannot be reversed, use DELETE, PATCH, POST, PUT with caution.

Routes are classified by 's elements type (activities, baselines, components, flows, groups, etc.).

The category "Groups" containing all possible group routes:

To authorize API communications:

Procedure

Step 1   From the main page, choose **Admin** > **API** .

Step 2   Click **Token** to create and/or copy a API Token.

Step 3   Click **Documentation**.

Step 4   Click **Authorize**.

The **Available authorizations** panel appear.

Step 5   Paste the token in **Value** field..

Step 6   Click **Authorize**.

Step 7   Click **Close**.

Close lockers displays. They indicate that routes are secured and authorization to use them is up.

To use a route:

Step 8   Click a route to deploy it.

In the example, we choose Get activity list.

Step 9   Click **Try it out**.
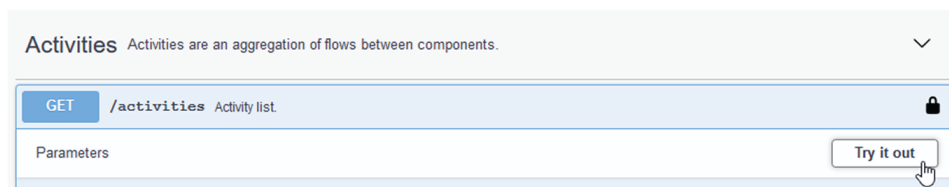
Step 10   You can set some **Parameters**.

In the example, we set page to 1 and size to 10.

Step 11   Click **Execute**.

> **Note**
> You can only execute one route at a time.

A loading icon appears for a few moments. Responses display with curl, Request URL and the server response that you can copy or even download.

Step 12   When you are finished, click the **Authorize** button.

Step 13   Log out to clear the token variable, and click **Close**.

Active Discovery Policies

Active Discovery is used to allow a sensor to send packets to the network to discover previously unseen devices and gather additional properties for known devices.

Active Discovery operates in Broadcast and Unicast, and responses received will be analyzed by .

An Active Discovery policy is a list of settings which define protocols and their parameters that will be used to scan the industrial network. The policy will be used in a preset and be applied on a list of sensors and components.

To acces the **Active Discovery policies** page, choose **Admin** > **Active Discovery** > **Policies** from the main menu.

For more information, refer to the Active Discovery Configuration Guide.

LDAP

Cisco Cyber Vision can delegate user authentication to external services using LDAP (Lightweight Directory Access Protocol), specifically to Microsoft Active Directory services.

You can enable LDAP authentication in the LDAP Settings administration page. To access **LDAP Settings** page, choose **Admin** > **External Authentication** > **LDAP**.

Configuring LDAP:

LDAP integration can be done through normal connection or securely by using certificates depending on the installation compatibility.

Mapping Cisco Cyber Vision roles with Microsoft Active Directory groups:

User groups available in the external directory can be mapped to Cisco Cyber Vision Product, Operator and Auditor user roles or custom roles. Refer to Role Management to create custom roles.

Because the Admin user role is exclusively reserved for Cisco Cyber Vision internal usage, it cannot be mapped to any external users and thus is not proposed in LDAP settings.

Testing LDAP connection:

After setting up LDAP, the connection between the Cisco Cyber Vision Center and the external directory is to be tested. On the LDAP test connection window, you will use a user login and a password set in the external directory. The Center will attempt to authenticate on the directory server with these credentials. In return, you will get either a successful authentication, or a failed one with an error message.

Login in Cisco Cyber Vision:

When logging into Cisco Cyber Vision, the login format used will determine the base (i.e. internal or external) to be queried:

- If you use an email, the Cisco Cyber Vision database is queried.

- If you use the Active Directory format <domain_name>\<user_name> (e.g. cisco\john_doe), then the external directory is used to authenticate users.

Configure LDAP

This section explains how to configure LDAP in Cisco Cyber Vision using a normal connection or a secure connection.

Procedure

Step 1 From the main menu, choose **Admin** > **External Authentication** > **LDAP**.

Step 2 Click **Edit**.

The **EDIT LDAP SETTINGS** window appears.

What to do next

Configure LDAP using a LDAP Normal Connection or a LDAP Secure Connection.

LDAP Normal Connection

After clicking the New Settings button, the following New LDAP Settings window pops up.

Procedure

Step 1 Fill in the LDAP settings in the **Edit ldap settings** window.

LDAP senttings are as follows:

a) Enter the **Primary Server Address**.
b) Enter the **Primary Server Port**.
c) (Optional) Enter the **Secondary Server Address**.
d) (Optional) Enter the **Secondary Server Port**.
e) Enter the **Base DN**.
f) Enter the **Server Response Time**.

Step 2 Click the **Role Mapping** tab.

Fill in the following fields:

a) Map one or more Cisco Cyber Vision **Default roles** with an Active Directory group.

> **Note**
> At least one default role must be mapped.

> **Note**
> Since the Admin user role is reserved for Cisco Cyber Vision internal usage, it cannot be mapped to external users and is not available in LDAP settings.

b) Map Cisco Cyber Vision **Custom roles** with Active Directory groups.

Enter the exact group names as configured in the remote directory for successful retrieval and mapping to user roles.

Step 3   Click **OK**.

Step 4   Click the **Test connection** button.

The **TEST CONNECTION** window appears.

Step 5   Enter the user credentials to test the connection between Cisco Cyber Vision and Active Directory.

Note
The Username format is domain\user.

A message Successful LDAP bind should appear.

Step 6   Click **OK**.

Step 7   Test the connection by logging out of Cisco Cyber Vision and logging in with the mapped user credentials.

Menus are displayed according to the rights granted to the user.
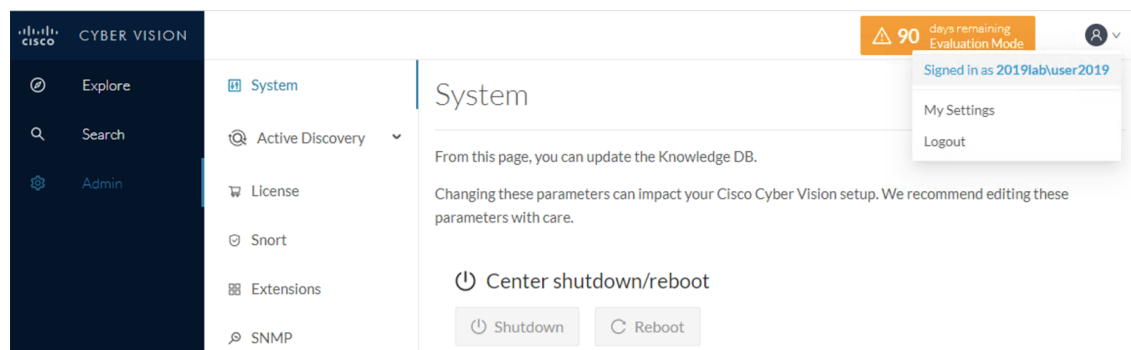
LDAP Secure Connection

After clicking the New Settings button, the following New LDAP Settings window pops up.

Procedure

Step 1   Fill in the LDAP settings in the **Edit ldap settings** window.

LDAP senttings are as follows:

a)   Check the checkbox of **LDAP over TLS/SSL**.
b)   Enter the **Primary Server Address**.
c)   Enter the **Primary Server Port**.
d)   (Optional) Enter the **Secondary Server Address**.
e)   (Optional) Enter the **Secondary Server Port**.
f)   Enter the **Base DN**.
g)   Enter the **Server Response Time**.
h)   Click **Choose a file** to upload a .pem root certificate or a chain certificate, or check the box of **Use self signed certificate**.

If you upload a certificate, a success message appears.

The certificate appears at the bottom of the New LDAP Settings window.

Step 2   Click **OK**.

Step 3   Click the **Role Mapping** tab.

Step 4   Fill in the following fields:

a) Map one or more Cisco Cyber Vision **Default roles** with an Active Directory group.

> **Note**
> At least one default role must be mapped.

> **Note**
> Since the Admin user role is reserved for Cisco Cyber Vision internal usage, it cannot be mapped to external users and is not available in LDAP settings.

b) Map Cisco Cyber Vision **Custom roles** with Active Directory groups.

Enter the exact group names as configured in the remote directory for successful retrieval and mapping to user roles.

Step 5   Click **OK**.

Step 6   Click the **Test connection** button.

The **TEST CONNECTION** window appears.

Step 7   Enter a user credentials to test the connection between Cisco Cyber Vision and Active Directory.

> **Note**
> The Username format is <domain_name>\<user_name> (e.g. cisco\john_doe).

A success message appears.

Step 8   Click **OK**.

Step 9   Test the connection by logging out of Cisco Cyber Vision and logging in with the mapped user credentials.

Menus are displayed according to the rights granted to the user.
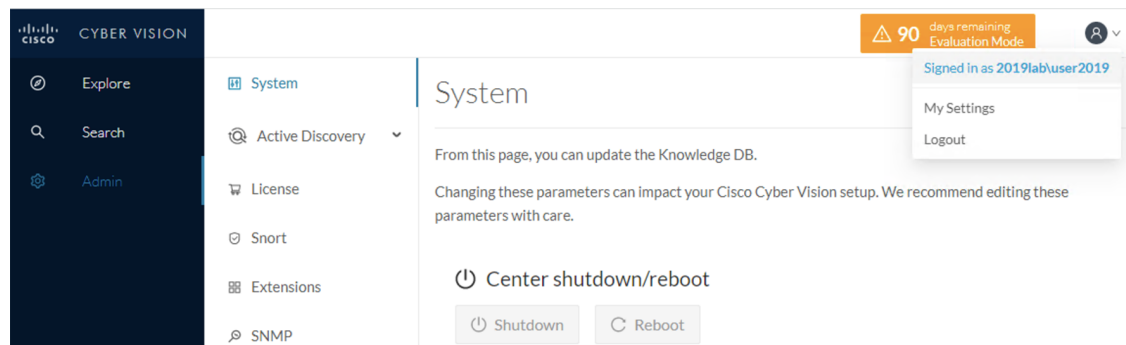
Sensors

Sensor Explorer

The **Sensor Explorer** page allows you to install, manage, and obtain information about the sensors monitoring your industrial network. To access the **Sensor Explorer** page, choose **Admin** > **Sensors** > **Sensor Explorer** from the main menu.

First, you need to know that sensors can be used in two modes, and for different purposes:

- **Online mode**: A sensor in online mode is placed at a particular and strategic point of the industrial network and will continually capture traffic.

  Applicable to: Cisco IE3400, IE3300 10G, Cisco IC3000, Catalyst 9300 and Cisco IR1101.

- **Offline mode**: A sensor in offline mode allows you to easily connect it at different points of the industrial network that may be isolated or difficult to access to occasionally make traffic captures. Traffic is captured on a USB drive. The file will then be imported in Cisco Cyber Vision.

  Only applicable to Cisco IC3000.

On the Sensor Explorer page, you will see a list of your folders and sensors (when installed) and buttons that will allow you to perform several actions.

Installation modes, features, and information will be available depending on the sensor model and the mode in which it's being used.

Additional information and actions are available as you click a sensor in the list. A right side panel will appear allowing you to see this information such as the serial number, and buttons to perform other actions.

Filter and Sort the Sensor List

Filtering

Use the Filter button to filter the folders and sensors in the list by label, IP address, version, location, health, and processing status.

To filter the sensor list, follow thses steps:

1. From the main menu, choose **Admin** > **Sensors** > **Sensor Explorer**.

2. Click the **Filter** icon from the top right corner of the table.

3. Type in the field or select from the drop-down menu to locate the folder(s) or sensor(s).

4. Click **Apply**.

Sorting

The sort icons next to the column titles allow you to organize sensors by label, IP address, version, location, health, and processing status in either alphabetical or ascending/descending order. The icons appear when you hover over them or apply them.

Sensors Status

To access the sensor status, choose **Admin** > **Sensors** > **Sensor Explorer** from the main menu.

There are two types of sensor status:

- The **Health status**, which indicates the step of the enrollment process the sensor is at.

- The **Processing status**, which indicates the network connection state between the sensor and the Center.

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.

Sensors Features

The Sensor Explorer page provides several features to manage and use your sensors. Some buttons are accessible directly from the Sensor Explorer page to manage one or more sensors, while other buttons become available when clicking a sensor in the list. To access the sensor features, follow these steps:

1. From the main menu, choose **Admin** > **Sensors** > **Sensor Explorer**.

2. Click the sensor name from the **Label** column.

   A right-side panel appears with all the features.

The features of sensors are as follows:

- The **Start recording** button records a traffic capture on the sensor. Records can be used for traffic analysis and may be requested by support in case of malfunctions. You can download the recording clicking the link below.

✎

Note This feature is targeted for short captures only. Performing long captures may cause the sensor overload and packets loss.

- The **Move to** button is to move the sensor through different folders. For more information, refer to Organize Sensors, on page 97.

- The **Download package** button provides a configuration file to be deployed on the sensor when installing the sensor manually (online mode). Only applicable to the Cisco IC3000. Refer to its Installation Guide.

- The **Capture Mode** button can be used to set a filter on a sensor sending data to the Center. Refer to the procedure for Set a Capture Mode.

- The **Redeploy** button can be used to partly reconfigure the sensor, for example to change its parameters such as its IP address.

- The **Enable IDS** button can be used to enable the SNORT engine embedded in some sensors to analyze traffic by using SNORT rules. SNORT rules management is available on the SNORT administration page.

- The **Reboot** button can be used to reboot the sensor in case of a malfunction.

- The **Shutdown** button triggers a clean shutdown of the sensor from the GUI.

✎

Note After performing a shutdown, you must switch the sensor ON directly and manually on the hardware.

- The **Uninstall** button can be used to remove an uninstalled sensor from the list or to fully uninstall a sensor. Diverse options are available according to the sensor model or deployment mode. In the case of a sensor deployed through the management extension, the IOx app can be removed from the device, whereas a reset to factory defaults can be performed in other cases. In any case, the sensor will be removed from the Center.

Install Sensor

From the **Sensor Explorer** page, you can install a sensor. To access the **Sensor Explorer** page, choose **Admin** > **Sensors** > **Sensor Explorer** from the main menu. There are three ways to install a sensor, as follows:

- Install a sensor manually.

- Install a sensor via the IOx extension. To use the Install via extension button you must first install the sensor management extension via the Extensions page.

- Capture traffic with an offline sensor (only applicable to Cisco IC3000).

For more information about how to install a sensor, refer to the corresponding Sensor Installation Guide.

Sensor Self Update

Cisco Cyber Vision now allows sensor updates regardless of the install method (i.e., without the extension). Release 4.4.1 provides the necessary foundation for sensor self-updates. However, the self-update feature will only be functional in future releases.

Starting with Cisco Cyber Vision release 4.4.1, you can update all sensors automatically. The required steps are:

- Select sensors to update.

- The Center adds a new job to the sensor queue.

- The sensor automatically collects and validates the update file.

- The sensor restarts with the new version.

Update Warnings

In the Cisco Cyber Vision Center on the Sensor Explorer page, you receive an alert to update the sensor. When this occurs, the latest version number appears in red, and a blue arrow with a tooltip indicates the sensor is upgradeable.

To update the senosr, follow thses steps:

- From the main menu, choose **Admin** > **Sensors** > **Sensor Explorer**.

- Click the sensor that is upgradeble from the **Label** column.

- The right side panel appears with sensor details.

- Click **Update**.

Update Procedure

Procedure

Step 1   From the main menu, choose **Admin** > **Senors** > **Sensor Explorer**.

Step 2   Check the checkboxes to select multiple sensors.

Step 3   Click the drop-down arrow of the **More Actions** button.

Step 4 Click **Update sensors** from the drop-down list.

The **UPDATE SENSORS** pop-up appears.

Step 5 Click **OK**.

During the update, a blue circle appears in the **Update status** column. After the update is complete, the version number turns black, and a green symbol appears in the same column.

Update Failure

If the update is unsuccessful, the **Update Status** column displays a red cross and a detailed message. To view the failure message, choose **Admin** > **Sensors** > **Sensor Explorer** from the main menu. Hover over the red cross in the **Update Status** column to see the details of the update failure.

Manage Credentials

You can use the **Manage credentials** button to register your global credentials if configured before in the Local Manager.

This feature can be used to register your global credentials in Cisco Cyber Vision. This will allow you to enter these credentials only once and they will be used when performing actions that require these credentials, that is installing and updating sensors via the IOx extension.

Only one set of global credentials can be used per Cisco Cyber Vision instance, which means that you cannot have several set of sensors accessible by different global credentials in a single instance. If there are several sensor administrators, they must use the same global credentials registered in Cisco Cyber Vision. However, you can have a set of sensors using a single global credentials and other sensors with their own single credentials.

Global credentials are stored in Cisco Cyber Vision but are set at the switch level in the Local Manager. Consequently, if you lose your global credentials, you must refer to the switch customer support and documentation.

The Manage credentials button can be used the first time you register your global credentials and each time global credentials are changed in the Local Manager. To do so, follow these steps:

1. From the main menu, choose **Admin** > **Sensors** > **Sensor Explorer**.

2. Click **Manage Cisco devices**.

3. Click **Manage credentials** from the drop-down list.

   The **SET GLOBAL CREDENTIALS** window appears.

4. Enter the **Login** and **Password**.

5. Click **Update**.

6. After you register the global credentials, the feature is enabled in the **Install via extension** procedure. Check the **Use global credentials** checkbox to use your global credentials.

Organize Sensors

You can create folders to organize your sensors more clearly. Folders can be categorized by location, person in charge, or type of sensor, such as disconnected sensors.

To create a folder and move a sensor into it, follow these steps:

Procedure

Step 1   From the main menu, choose **Admin** > **Sensors** > **Sensor Explorer**.

Step 2   Click **Organize**.

Step 3   Click + **Create folder** from the dropdown list.

Step 4   Enter the **folder name**.

Step 5   (Optional) Enter **Location** and **Description**.

Step 6   Click **Ok**.

A success message appears, and the system displays the new folder in the sensor list.

Step 7   Check the checkbox of the sensor that you want to move.

Step 8   Click **Move selection to**.

The **Move selection to** pop-up appears.

Step 9   Click the drop-down arrow of the **Destination** field.

The three options are as follows:

a) Select the required folder to move the sensor.
b) Click +**New folder** to create a new folder and move the sensor.
c) Click **Root** to move sensors back into the primary list.

Step 10   Click **Ok**.

After you move the sensor into the folder, the sensor version, health status, and processing status display in the folder line.

If you move a sensor in a disconnected state into this folder, its information displays in the folder line instead of the connected sensor's information. Less secure sensor statuses are prioritized to draw your attention.

Set a Capture Mode

The Capture mode feature lets you choose which network communications will be analyzed by the sensors. To access the **Capture mode** feature, follow these steps:

1. From the main menu, choose **Admin** > **Sensors** > **Sensor Explorer**.

2. Click the name of the sensor from the label column.

    The side panel appears with the sensor details.

3. Click **Capture mode**.

    The **CAPTURE MODE** window appears.

4. Click the radio button to select **Capture Mode**.

The aim is mainly to focus the monitoring on relevant traffic but also to reduce the load on the Center.

For example, a common filter in a firewall can consist of removing the network management flows (SNMP). This can be done by setting a filter like "not (port 161 and host 10.10.10.10)" where "10.10.10.10" is the network management platform.

By using Capture Mode, Cisco Cyber Vision performance can be improved on large networks.

Capture modes operate because of filters applied on each sensor. Filters are set to define which types of incoming packets are to be analyzed by the sensors. You can set a different filter on each sensor according to your needs.

You can set the capture mode in the installation wizard when enrolling the sensors during the Center installation. This option is recommended if you already know which filter to set. Otherwise, you can change it at any time through the Sensor Explorer page in the GUI (provided that the SSH connection is allowed from the Center to the sensors).

The different capture modes are:

- ALL: No filter is applied. The sensor analyzes all incoming flows and they will all be stored inside the Center database.

- OPTIMAL (Default): The applied filter selects the most relevant flows according to Cisco Cyber Vision expertise. Multicast flows are not recorded. This capture mode is recommended for long term capture and monitoring.

- INDUSTRIAL ONLY: The filter selects industrial protocols only like modbus, S7, EtherNet/IP, etc. This means that IT flows of the monitored network won't be analyzed by the sensor and won't appear in the GUI.

- CUSTOM (advanced users): Use this capture mode if you want to fully customize the filter to be applied. To do so you will need to use the tcpdump syntax to define the filtering rules.

Deployment Tokens

Zero Touch Provisioning allows you to automate Cisco Cyber Vision deployment on sensor batches. It is to be used with third-party tools such as Cisco Catalyst WAN Manager. Refer to its documentation on cisco.com to complete sensor deployment.

From this page, you can create, edit, enable, disable and delete deployment tokens for Zero Touch Provisioning.

To access the Deployment Tokens page, choose **Admin** > **Sensors** > **Deployment Tokens** from the main menu.

You will start with adding a deployment phase, that is a group of tokens, with a number of uses and an expiration time.

The application will request a token valid for an application type. A token contains the application name and a PSK (pre-shared key).

Once proper configuration is done on Cisco Catalyst WAN Manager, it will deploy the sensors and apply parameters which will allow each sensor to on-board itself on the Center.

Communication between the sensors and the Center starts after the sensors present the PSK to the Center and the Center delivers all necessary information for enrollment.

Deployment will fail:

- if the number of sensors exceed the number of tokens.

• if the deployment occurs after the expiration time.

If so, you can edit the deployment phase to modify the number of uses accordingly and extend the expiration time.

Table 1: Sensor applicability and correspondance table per deployment file

Sensors	Deployment files
IE3x00, IR1101, IR18xx, IE9300	cviox-aarch64.tar
IE3x00, IR1101, IR18xx, IE9300 **with Active Discovert**	cviox-active-discovery-aarch64.tar
IC3000	cviox-ic3000-x86-64.tar
IC3000 **with Active Discovery**	cviox-active-discovery-x86-64.tar
Catalyst 9300, 9400, IR8340	cviox-x86-64.tar
Catalyst 9300, 9400, IR8340 **with Active Discovery**	cviox-active-discovery-x86-64.tar

Create Deployment Tokens

To create tokens, follow these steps:

Procedure

Step 1 From the main menu, choose **Admin** > **Sensors** > **Deployment Tokens**.

The **Deployment Tokens** page appears.

Step 2 Click **Add Tokens**.

The **Add new deployment tokens** panel appears.

Step 3 Fill in the following details in **Add new deployment tokens** panel:
  a) Enter a name for the deployment phase.
  b) Add the **Number of uses** for the number of devices to be deployed.
  c) Set the token's **Expiration time**.
  d) Use the **Enabled** toggle button to enable the token to continue the deployment process.

Step 4 Click **Create**.

The deployment phase with tokens per device type appears.

Note
You can view, copy, edit, disable, and delete the token.

What to do next

Refer to Cisco Catalyst WAN Manager documentation in cisco.com to continue and complete sensor deployment.

Templates

This page allows you to create and set templates with protocol configurations and assign them to specific sensors.

Sensor templates contain protocol configurations which allow you:

- To enable or disable protocol DPI (Deep Packet Inspection) engines.

- To map UDP and TCP ports for each protocol's packet received by the sensor.

By enabling/disabling a protocol DPI engine you can decide which protocols will be analyzed.

Disabling a protocol DPI engine avoid false positives in , that is when a protocol appears on the user interface when it's actually not the case because same UDP/TCP ports can be used by other non-standardized protocols.

Some protocols are disabled in the Default template because they are not commonly used or used in specific fields such as transportation. The Default template is applied on all compatible sensors.

As previously mentioned, UDP/TCP ports default configurations are mostly standardized, but conflicts still exist among field-specific protocols or with limited usage. Mapping UDP/TCP port numbers will allow packets to be sent to the correct DPI engine so they can be accurately analyzed and correctly represented in the user interface.

If the protocol's packet is sent to the wrong port, related information will end up in Security Insights/Flows with no tag.

A sensor can be associated with a single template only. Deployment of the template can fail:

- if the sensor is disconnected,

- if there is connection issues,

- if the sensor version is too old.

Create Templates

Procedure

Step 1	From the main menu, choose **Admin** > **Sensors** > **Templates**.
Step 2	Click the **Add sensor template** button.
	The **CREATE SENSOR TEMPLATE** window appears.
Step 3	Add a name to the template.
	(Optional) You can add a description.
Step 4	Click **Next**.

The list of protocol DPI engines with their basic configurations appears.

Step 5　　　In the search bar, type the protocol you want to configure.

Step 6　　　To edit its settings, click the **pen** icon under the **Port Mapping** column, .

The protocol's port mapping window appears.

Step 7　　　Enter the port numbers you want to add.

　　　　　　Note
　　　　　　If you have continuous port numbers, you can enter a port range. For example, type 15000-15003 for ports 15000, 15001, 15002, and 15003.

Step 8　　　Click **OK**.

The port number is added to the protocol's default settings.

Step 9　　　Enable the toggle button **Displayed modified only** to quickly find the protocol.

Step 10　　Click **Next**.

Step 11　　Select the checkboxes for the sensors to which you want to apply the template.

Step 12　　Click **Next**.

Step 13　　Check the template configurations and click **Confirm**.

The configuration is sent to the sensors. Configuration deployment will take a few moments.

The OPCUA template appears in the template list with its two assigned sensors.

Export Templates

You can use this feature to define the template at one center and then migrate it to another. To export the template, follow these steps:

Procedure

Step 1　　　From the main menu, choose **Admin** > **Sensors** > **Templates**.

Step 2　　　Locate the template and hover over the ellipsis (…) in the **Actions** column.

Step 3　　　Click **Export** from the drop-down list.

Your system downloads the template to its local location.

Import Templates

To import the template, follow these steps:

Procedure

Step 1   From the main menu, choose **Admin** > **Sensors** > **Templates**.

Step 2   Click **Import sensor template**.

The system's local folder will opens.

Step 3   Select the template and click **Open**.

The system displays the imported template on the **Configuration Template** page.

Step 4   Locate the template and hover over the ellipsis (…) in the **Actions** column.

Step 5   Click **Edit** from the dropdown list.

Step 6   From the **Select sensors** tab, check the checkboxes of the sensors to which you want to apply the template.

Step 7   Click **Next**.

Step 8   Check the details and click **Update**.

The template recovers all the changes made in the previous center, and will be applied to the selected sensors.

Management Jobs

Since some deployment tasks on sensors can take several minutes, this page displays the execution status and progress for each sensor deployed with the Sensor Management Extension. The page is visible only when the Sensor Management Extension is installed in the Cisco Cyber Vision Center.

To access the **Management jobs** page, choose **Admin** > **Sensors** > **Management jobs** from the main menu.

You will find the following jobs:

- **Single deployment**:

  This job is launched when clicking the **Deploy Cisco device** button in the sensor administration page, that is when a new IOx sensor is deployed.

- **Single redeployment**:

  This job is launched when clicking the **Reconfigure Redeploy** button in the sensor administration page, that is when deploying on a sensor that has already been deployed. This option is used for example to change the sensor's parameters like enabling active discovery.

- **Single removal**:

  This job is launched when clicking the **Remove** button from the sensor administration page.

- **Update all devices**:

  This job is launched when clicking the **Update Cisco devices** button from the sensor administration page. A unique job is created for all managed sensors that are being updated.

If a job fails, you can click on the **error icon** to view detailed logs.

PCAP Upload

The PCAP Upload page allows you to upload PCAPs to view their data in Cisco Cyber Vision Center.

Procedure

Step 1 From the main menu, choose **Admin** > **Sensors** > **PCAP Upload**.

Step 2 Click **Upload a new file**.

The **UPLOAD A NEW FILE** window appears.

Step 3 Click **Choose a file or drag and drop to upload** and add the file in the box.

Step 4 Click **Upload**.

Note
During the upload, the status for DPI and Snort is displayed.

If uploading a large file, you can pause it. To resume the upload, select the same PCAP again with the browse button and click **Resume**.

SNMP

SNMP Protocol in Cisco CyberVision is used for remote monitoring purposes. To access the **SNMP Global Configuration** page, choose **Admin** > **SNMP** from the main menu.

Supported versions are:

- SNMP V2C

- SNMP V3

Older versions are not supported.

☞

Important It is highly recommended to use version 3 of the SNMP protocol. Version 2c is available due to a large number of infrastructures still using it. However, take into account that risks in terms of security are higher.

Snmp information:

- CPU % per core

- Load 0 to 100 (combination of CPU and I/O loads)

- RAM kilobytes

- Swap kilobytes

- Traffic for all physical interfaces (nb bytes in and out/interface (since the snmp service startup))

- Data storage (% - 250G)

• Packets stats (packets/sec/int)

Configure SNMP

This section explains how to configure SNMP on a CyberVision Center.

Procedure

Step 1   From the main menu, choose **Admin** > **SNMP**.

Step 2   Enable the **SNMP agent** toggle button.

A configuration menu appears.

Step 3   Enter the IP address of the monitoring host in the **Monitoring hosts (IPv4)** field.

Step 4   Click the radio buttons to select a version. Version options are as follows:

• Version 3
• Version 2c

Note
For security reasons, it is recommended to use SNMP version 3.

a) **Version 3**

• **Security type**: When the security type is **NoAuth**, only a username is required. No authentication password required.

Username: Add the username that will be used for the SNMP authentication. "ics" is used by default.

• **Security type**: When the security type is **Auth** with **NoPriv**, a username and an encrypted password are required.

Username: Add the username that will be used for the SNMP authentication. "ics" is used by default.

Authentication: Add the Hash algorithm needed and its password. It must be at least 8 characters long.

• **Security type**: When the security type is **Auth** with **Priv**, only AES encryption is available. A username, an encrypted password, and AES encryption are required.

Username: Add the username that will be used for the SNMP authentication. "ics" is used by default.

Authentication: Add the Hash algorithm needed and its password. It must be at least 8 characters long.

Privacy: Add the AES password. It must be at least 8 characters long.

b) **Version 2c**

Add the community string for the Center to communicate with the monitoring host.

Step 5   Enable the **Trap** toggle button.

The configuration menu appears:

Step 6   Set up traps to be delivered.

a) If SNMP v3 has been selected, the Engine ID field (i.e. the Center id) is displayed so you can customize it.

b) Select and set the CPU and memory rate limit and threshold according to your needs.

Step 7   Click **Save Configuration**.

SNMP MIB

Table 2:

MIB	OID prefix	Description
MIB-2	.1.3.6.1.2.1.1	System
IF-MIB	.1.3.6.1.2.1.2.2.1.1	All physical interfaces
IF-MIB	.1.3.6.1.2.1.31.1.1	All physical interfaces
HOST-RESOURCES-MIB	.1.3.6.1.2.1.25.1	System
HOST-RESOURCES-MIB	.1.3.6.1.2.1.25.2.3	Storage
HOST-RESOURCES-MIB	.1.3.6.1.2.1.25.3.3	CPU
UCD-SNMP-MIB	.1.3.6.1.4.1.2021.4	Memory
UCD-SNMP-MIB	.1.3.6.1.4.1.2021.9	Disk
UCD-SNMP-MIB	.1.3.6.1.4.1.2021.10	Load
UCD-SNMP-MIB	.1.3.6.1.4.1.2021.11	CPU
UCD-DISKIO-MIB	.1.3.6.1.4.1.2021.13.15.1	Disk IO

C H A P T E R 6

Integrate with Cisco Cyber Vision

pxGrid

From **Platform Exchange Grid** page, you can configure ISE pxGrid Cisco Cyber Vision integration.

Cisco Platform Exchange Grid (pxGrid) is an open, scalable data-sharing and threat control platform that allows seamless integration between multivendor identity, network, security and asset management systems.

To access the **Platform Exchange Grid** page, choose **Admin** > **Integrations** > **pxGrid** from the main menu.

For more information about how to perform this integration, refer to the manual "Integrating Cisco Cyber Vision with Cisco Identity Services Engine (ISE) via pxGrid".

XDR

Cisco Cyber Vision can be integrated with XDR, a cloud-native, built-in platform that connects the Cisco Secure portfolio with your infrastructure. This integration allows you to significantly reduce dwell time and human-powered tasks.

Note   SecureX reached its end of life on July 31, 2024.

Cisco XDR is an online platform that centralizes security events from various Cisco software equipments through an API. For instance, events such as those from Cisco Cyber Vision or firewall activities can be transmitted to Cisco XDR and correlated, then presented across diverse dashboards.

XDR integration enables three features in Cisco Cyber Vision:

- Without XDR SSO login, the **Investigate in XDR Threat Response** button will appear on components' technical sheets.

- With XDR SSO login, the **Report to XDR** button will appear on certain events of the event calendar page. This button is utilized to push the events to XDR.

• With XDR SSO login, an XDR ribbon featuring several functionalities can be activated within Cisco Cyber Vision.

This section details the configuration of XDR in Cisco Cyber Vision and different authorized features.

XDR Configuration

Before you begin

The Cisco XDR configuration in Cisco Cyber Vision requests:

- An Admin access to Cisco Cyber Vision Center.
- A Cisco Cyber Vision Center with internet access.
- A XDR account with an admin role.

Procedure

Step 1	From the main menu, choose **Admin** > **Integrations** > **XDR**.
Step 2	Click the dropdown arrow of the **Region** field.
Step 3	Select the region from dropdown list.
Step 4	Click **Enable XDR** to enable the link.

Once you enable the link, the button turns red to indicate **Disable XDR**.

By completing the steps above, you are now able to use the button **Investigate in XDR Threat Response** that will appear in the components' technical sheet. To install and use the XDR ribbon and the Report to XDR button, complete the steps herebelow.

Step 5	Click the user menu located in the top right corner of the GUI.
Step 6	Click **My Settings**.

A new **XDR** menu appears on the right of the **My settings** page.

Step 7	Click the **Log in** button.

A **Grant Application Access** popup appears with an authentication code.

Step 8	Click **Verify and Authorize**.

The browser opens a new page with the **Security Cloud Sign On** window to grant Cisco Cyber Vision access to **XDR**.

Step 9	Enter **Email** and click **Continue**.
Step 10	Click **Authorize Cyber Vision**.

A **Client Access Granted** popup appears.

Step 11	In **Cisco Cyber Vision Center** > **My Settings**, the XDR menu indicates that Cisco Cyber Vision is connected to XDR.
Step 12	Use the **Ribbon status** toggle button to enable the XDR ribbon.

Once you enable the **Ribbon status** toggle button, message appears.
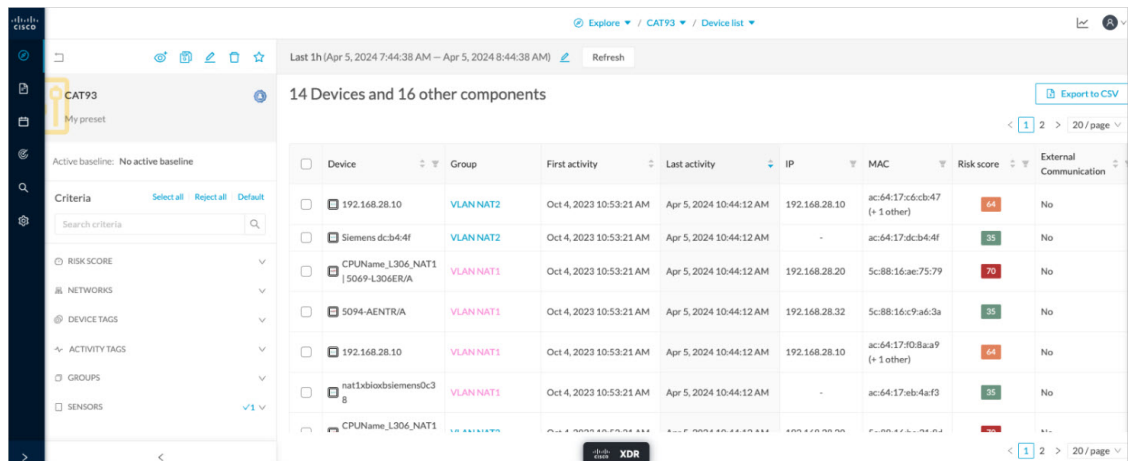
Step 13   To log out, click **Logout of XDR**.

Step 14   Click **Save settings**.

XDR Ribbon

Once configured and activated, the XDR ribbon will appear at the bottom of the Cisco Cyber Vision GUI of the Explore menu.

The XDR ribbon in the Device List view:

The Cisco XDR Getting Started Guide explains how to use the XDR ribbon.

For example, to find observables and investigate them in XDR Threat Response, click the **Find Observables** icon like below:

XDR Event Integration

Once XDR has been configured in Cisco Cyber Vision, a **Report to XDR** button appears on some events of the event calendar page. Using this button will push the event to XDR and create an incident.

The XDR button appears on three categories of event:

- Anomaly Detection
- Control Systems Events
- Signature Based Detection

The Report to XDR button on a Control Systems Events:

XDR Component Button

Once XDR has been configured in Cisco Cyber Vision, the button **Investigate in Cisco Threat Response** appears on the components' technical sheet. The component's IP and MAC addresses will be investigated in XDR Threat Response if you use this button.

External Resources for XDR Integration

Herebelow is the list of all URLs called by the Cisco Cyber Vision Center in case you need to authorize them, for example in a firewall.

Center:

North America

- Cisco XDR Platform: https://visibility.amp.cisco.com/iroh/

- Cisco XDR Private Intelligence: https://private.intel.amp.cisco.com/ctia/
- Cisco XDR Automation: https://automate.us.security.cisco.com/api/

Europe

- Cisco XDR Platform: https://visibility.eu.amp.cisco.com/iroh/
- Cisco XDR Private Intelligence: https://private.intel.eu.amp.cisco.com/ctia/
- Cisco XDR Automation: https://automate.eu.security.cisco.com/api/

Asia Pacific, Japan, and China

- Cisco XDR Platform: https://visibility.apjc.amp.cisco.com/iroh/
- Cisco XDR Private Intelligence: https://private.intel.apjc.amp.cisco.com/ctia/
- Cisco XDR Automation: https://automate.apjc.security.cisco.com/api/

Web client:

- conure.apjc.security.cisco.com
- conure.us.security.cisco.com
- conure.eu.security.cisco.com

Maintain and Monitor Cisco Cyber Vision

Center Shutdown/Reboot

You can trigger a safe shutdown and reboot of the **Center**.

Use **Reboot** to fix a minor bug, such as a system overload.

To access the **Center shutdown/reboot** page, choose **Admin** > **System** from the main menu.

Upgrade with a Combined Update File

Version releases include a **Cisco Cyber Vision Manual Update Center** update file. To access this file, choose **Admin** > **System** from the main menu.

☞

| **Important** | Rolling back to an older Cisco Cyber Version version is not supported. |

Requirements

• A combined update to retrieve from cisco.com.

Use the SHA512 checksum provided by Cisco to verify that the file you just downloaded is healthy.

Windows users:

Procedure

Step 1   Retrieve the Cisco Cyber Vision combined update from cisco.com.

Step 2   Open a shell prompt such as Windows Powershell and use the following command to retrieve the file checksum:

Get-FileHash .\CiscoCyberVision-<TYPE>-<VERSION>.<EXT> -Algorithm SHA512 | Format-List

```
PS C:\Users\        > Get-FileHash .\Downloads\CiscoCyberVision-center-3.2.3.ova -Algorithm SHA512 | Format-List

Algorithm : SHA512
Hash      : 1338BFB1A17110AF80D751AE7B450F2B29CCB4CB54F550F38B8E6B4236865EC9EDF7773FD05D1055C7F1EF76E68C2B8A96CFE69AB
            1B622E4B0BB8EBB9E94DB16
Path      : C:\Users\        \Downloads\CiscoCyberVision-center-3.2.3.ova
```

Step 3   In cisco.com, hover over the file and copy the SHA512 checksum.

Software Download

Downloads Home / Security / Network Visibility a

	Details	✕
Search...	Description :	VMware OVA (Center) - CiscoCyberVision-Center-3.2.3.ova
	Release :	3.2.3
Expand All Collapse All	Release Date :	30-Apr-2021
	FileName :	CiscoCyberVision-center-3.2.3.ova
Latest Release ⌄	Size :	382.92 MB (401520640 bytes)
	MD5 Checksum :	ad553391b4f43128ef922e1a98e7e58c ⧉
3.2.3	SHA512 Checksum :	1338bfb1a17110af80d751ae7b450f2b ... ⧉
	Release Notes for 3.2.3 Advisories ⧉	
All Release ⌄		
	VMware OVA (Center) - CiscoCyberVision-Center-3.2.3.ova	
3 ⟩	CiscoCyberVision-center-3.2.3.ova	
	Advisories ⧉	

Step 4   Compare both checksums.

  • If both checksums are identical, the file is healthy.

  • If the checksums do not match, download the file again.

  • If the checksums still don't match, please contact Cisco support.

To update the Center and all applicable sensors:

Step 5   Log in to Cisco Cyber Vision.

Step 6   From the main meu, choose **Admin** > **System**.

Step 7   Click **System update**.

Step 8   Select the update file CiscoCyberVision-update-combined-<VERSION>.dat

Step 9   Confirm the update.

As the Center and sensors update, a holding page appears. When done, click Center **Reboot**. You will be logged out.

Step 10   Log in.

If sensors were offline when the update occurred, repeat the procedure until all sensors update.

Syslog Configuration

Cisco Cyber Vision provides syslog configuration so that events can be exported and used by a SIEM. The following procedure configures to which machine the syslogs will be sent.

Procedure

Step 1   From the main menu, choose **Admin** > **System**.

Step 2   Click **Configure** under **Syslog configuration**.

Step 3   Click the drop-down arrow for the Protocol field and select a protocol from the drop-down list.

If you select **TCP** + **TLS** connection, the **Set certificate** button displays to import a p12 file. The administrator of your SIEM solution provides this file to secure communications between the Center and the syslog collector.

Step 4   Enter the **Host**.

IP address of the SIEM reachable from the Administration network interface (i.e., eth0) of the Center.

Step 5   Enter the **Port** on the SIEM that will receive syslogs. Use the arrrows.

Step 6   Click the drop-down arrow of the **Format** field to select the variant of syslog.

- **Standard**: Event messages are sent in a format specific to Cisco Cyber Vision and with legacy timestamps (one-second precision).

- **CEF**: Industry standard **Common Event Format** which is understood by most SIEM solutions (no extra configuration is needed on the SIEM). This is the recommended option.

- **Standard/CEF**: Combination of both.

- **RFC3164**: Extended syslog header format with microsecond precision for timestamps.

- **RFC3164/CEF**: Combination of both.

Step 7   Click **Save configuration**.

Import/Export

Use the System interface to import and export the Cisco Cyber Vision database. To access the **Import/Export** page, choose **Admin** > **System** from the main menu.

Regularly export the database to back up the industrial network data on Cisco Cyber Vision or if you need to transfer the database to a different **Center**.

Exports database file limitation is up to 2 GB of data. This avoids side effects related to slow database exports. If the database is larger than 2 GB, you get an error message. In this case, connect to the Center using SSH and perform a data dump. Use the command: `sbs-db dump`.

Network data, events, and users are retained, as well as all customizations (e.g., groups, component names).

Only configurations created in Cisco Cyber Vision's GUI persist. If you change **Center**, perform a basic configuration of the Center and then configure Cisco Cyber Vision again. Refer to the corresponding Center Installation Guide.

Note The **Import** process may take one hour for big databases. Refresh the page to check that the import remains active (i.e., no error message).

Knowledge DB

Cisco Cyber Vision uses an internal database which contains a list of recognized vulnerabilities, icons, and threats.

Important To remain protected against vulnerabilities, always update the Knowledge DB in Cisco Cyber Vision as soon as possible after notification of a new version.

To update the Knowledge DB:

Procedure

Step 1 Download the latest.db file available from cisco.com.

Step 2 From the main menu, choose **Admin** > **System**.

Step 3 Click **Import a Knowledge DB** under the **Knowledge DB** field.

Step 4 Select the file and click **Open** to upload the file.

Importing the new database rematches your existing components against any new vulnerabilities and updates the network data.

Certificate Fingerprint

Use the certificate fingerprint to register a **Global Center** with its synchronized centers and vice versa. To access the **Center Fingerprint**, choose **Admin** > **System** from the main menu. Click the copy icon to copy the **Fingerprint** and enroll your center with a global center.

For more information, refer the Centers Installation Guides.

Cisco Cyber Vision Telemetry

Telemetry monitors your system to provide anonymous diagnostics and usage data, helps us to understand and enhance product usage. Cisco Cyber Vision telemetry data communication occurs as HTTPS traffic through Port 443 with https://connectdna.cisco.com/.

Telemetry is enabled by default. To disable this feature, follow these steps:

Procedure

Step 1 From the main menu, choose **Admin** > **System**.

Step 2 To disable telemetry, click the **ON** toggle button under the **Telemetry Collection** field.

The switch turns **OFF**.

Reset to Factory Defaults

Only use **Reset to Factory Defaults** *as a last resort*, after all other troubleshooting attempts fail. Get help from product support.

To access the **Reset**, choose **Admin** > **System** from the main menu.

A **Reset to Factory Defaults** deletes the following:

- Some Center configuration data elements.

- The GUI configuration (such as user accounts, the setup of event severities, etc.).

- Data collected by the sensors.

- The configuration of all known sensors (such as IP addresses, capture modes, etc.).

Root password, certificates and configurations from the Basic Center configuration persist.

After a **Reset to Factory Defaults** occurs, the GUI refreshes with the installation wizard. See the corresponding Center Installation Guide.

Snort

Snort is a Network Intrusion Detection System (NIDS) software which detects malicious network behavior based on a rule matching engine and a set of rules characterizing malicious network activity. Cisco Cyber Vision can run the Snort engine on both the Center and some sensors. The Center stores the configuration rule files, pushes rules on compatible sensors, and intercepts Snort alerts to display them as events in the Cisco Cyber Vision Center's GUI.

To access the **SNORT** page, choose **Admin** > **Snort** from the main menu.

Snort is not activated by default on sensors, so you must first Enable IDS on a Sensor.

It is available on the following sensor devices:

- The Cisco IC3000 Industrial Compute Gateway

- The Cisco Catalyst 9300 Series Switches

- The Cisco IR8340 Integrated Services Router Rugged

It is also avaible on the Center DPI, and is enabled by default.

Snort Community Rules are set by default in the Cisco Cyber Vision Center. You can use the **Use Subscriber Rules** toggle button to enable snort subscriber rules. This option requires Advantage licensing and a specific IDS sensor license for each enabled sensor.

Community ruleset

- The community ruleset is a Talos certified ruleset that is distributed freely. It includes rules that have been submitted by the open-source community or by Snort integrators. This ruleset is a subset of the full ruleset available to the subscriber users. It does not contain the latest Snort rules and does not ensure coverage of the latest threats.

Subscriber ruleset

- The subscriber ruleset includes all the rules released by the Talos Security Intelligence and Research Team. The ruleset ensures fast access to the latest rules and early coverage of exploits. Compared to the Community ruleset, it contains more rules and remains in sync with the latest Talos research work on vulnerability detection.

On the **SNORT** Administration page, you can find Snort rules grouped into categories. Use the toggle buttons under the **Status** columns to enable or disable sets of rules.

Click the download buttons under the **Download Rules** column to download each category rule file.

Note that some rules are **not** enabled inside these categories. So, using the toggle button on a category won't necessarily have an effect on their rules. The ones that are considered the most useful are enabled by default, others have been disabled to avoid performance issues. Consequently, if you want to enable these rules you need to use the Enable or Disable a Rule.

It is also possible to enable/disable a specific rule from a custom rule file.

Snort rules categories:

- Browser:

  Rules for vulnerabilities present in several browsers including, but not restricted to, Chrome, Firefox, Internet Explorer and Webkit. This category also covers vulnerabilities related to browser plugins such as Active-x.

- Deleted:

  When a rule has been deprecated or replaced it is moved to this category.

- Experimental-DoS:

  Rules developed by the Cisco CyberVision team for various kinds of DoS activities (TCP SYN flooding, DNS/HTTP flooding, LOIC, etc.).

- Experimental-Scada:

  Rules developed by the Cisco CyberVision team for attacks against industrial control system assets.

- Exploit-Kit:

  Rules that are specifically tailored to detect exploit kit activity.

- File:

  Rules for vulnerabilities found in numerous types of files including, but not restricted to, executable files, Microsoft Office files, flash files, image files, Java files, multimedia files and pdf files.

- Malware-Backdoor:

  Rules for the detection of traffic destined to known listening backdoor command channels.

- Malware-CNC:

  Known malicious command and control activity for identified botnet traffic. This includes call home, downloading of dropped files, and ex-filtration of data.

- Malware-Other:

  Rules that deal with tools that can be considered malicious in nature as well as other malware-related rules.

- Misc:

  Rules that do not fit in any other categories such as indicator rules (compromise, scan, obfuscation, etc.), protocol-related rules, policy violation rules (spam, social media, etc.), and rules for the detection of potentially unwanted applications (p2p, toolbars, etc.).

- OS-Other:

  Rules that are looking for vulnerabilites in various operating systems such as Linux based OSes, Mobile based OSes, Solaris based OSes and others.

- OS-Windows

  Rules that are looking for vulnerabilities in Windows based OSes.

- Server-Other:

  Rules dealing with vulnerabilities found in numerous types of servers including, but not restricted to, web servers (Apache, IIS), SQL servers (Microsoft SQL server, MySQL server, Oracle DB server), mail servers (Exchange, Courier) and Samba servers.

- Server-Webapp:

  Rules pertaining to vulnerabilities in or attacks against web based applications on servers.

In case of mistake, or to revert to the default configuration, you can use the **RESET TO DEFAULT** button. Note that all categories status and specific rules status will be reset and any added custom rules file will be deleted.

In addition, this page allows you to import custom rules, to enable or disable rules, and reset Snort's parameters to default.

Import Snort Custom Rules

Custom rules are useful if you want to define and use your own rules in addition to the rules provided in the Cyber Vision rulesets. To do this, a file must be created containing syntactically well-formed Snort rules and imported into Cisco Cyber Vision. Refer to Snort documentation for more information about creating rules.

To import custom rules in the Center, follow these steps:

Procedure

Step 1 Prepare your custom rules file.

Step 2 From the main menu, choose **Admin** > **Snort**.

Step 3 Click **IMPORT CUSTOM RULES FILE** under the **Import custom rules** field.

Once a custom rules file is imported, it is stored in the Center, and a "Download" button appears, allowing you to view its content.

Step 4 Click **Synchronize rules on sensors**.

What to do next

You can Enable or Disable a Rule.

Enable IDS on a Sensor

To enable the Snort engine on a sensor, follow these steps:

Before you begin

To use Snort you need to enable IDS on sensors.

Snort is only compatible with sensors embedded in:

- The Cisco IC3000 Industrial Compute Gateway

- The Cisco Catalyst 9300 Series Switches

- The Cisco IR8340 Integrated Services Router Rugged

Procedure

Step 1 From the main menu, choose **Admin** > **Sensor Explorer**.

Step 2 Click a compatible sensor in the list.

The right side panel appers with sensor details.

Step 3 Click **Enable IDS**.

Enable or Disable a Rule

You can manually enable and disable any specific rule, whether it is a default or a custom one. To do so you need the sid (i.e. signature id) that you will find in the rules file.

In the following procedure, we will disable Snort rule sid 50772 as example.

sid 50772: An unverified password change vulnerability (CVE-2018-7811) exists in the embedded web servers of Schneider Electric Quantum Modicon Ethernet modules. This vulnerability could allow an unauthenticated remote user to access the "change password" functionality of the web server. Snort rule with sid 50772 detects such attempts. It monitors and analyzes HTTP flows coming from the external network and raises an alert when the HTTP URI fields contain specific keywords (ex. "passwd=",,"cnfpasswd=",,"subhttppwd=") that indicate a password change attempt targeting the web server.

Procedure

Step 1   From the main menu, choose **Admin** > **Snort**.

Step 2   Click the **download icon** in the **Download rules** column.

In the downloaded rule files, locate the rule you wish to enable or disable.

Step 3   Enter the **Rule sid** under the **Specific rule** field.

Step 4   Click **Disable**.

A success message appears.

Note
If you download the rules file again, you will find a "#" preceding the rule, indicating it is disabled.

Step 5   Click **Synchronize rules on sensors** to save and push changes to the sensors.

Risk Score

The **Risk score** page allows you to set up the time range used for risk score computation. To access the **Risk score** page, choose **Admin** > **Risk score** from the main menu. Computation occurs every hour but considers only the activities within the configured time period.

You can select a time range of 30 days (by default), 7 days, or set a custom one with a minimum of one day

For more information about risk scores, see the Risk Score.

Extensions

From this page, you can manage Cisco Cyber Vision extensions. Extensions are optional add-ons to the Center which provide more features, such as the management of new device types, additional detection engines, or integrations with external services. To access the **Extensions** page, choose **Admin** > **Extensions** from the main menu.

Currently, there are two extensions available:

- **Cyber Vision sensor management**

  For more information about this extension and how to use it, see the Sensors.

- **Cyber Vision Reports Management**

  For more information about this extension and how to use it, see the Reports.

To install an extension, retrieve the extension file on cisco.com and click **Import a new extension file** to import.

CHAPTER **8**

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.

∨ 192.168.0.0/16	–	192.168/16 private netwo...	OT Internal
192.168.41.0/24	–	PAINTSHOP-PLC-SCADA	OT Internal
192.168.42.0/24	–	PAINTSHOP-SCADA-Client	OT Internal
192.168.43.0/24	–	PAINTSHOP-admin	OT Internal

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.