

Cisco Cyber Vision Administration Guide, Release 5.3.x

First Published: 2025-09-09

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2025 Cisco Systems, Inc. All rights reserved.



CONTENTS

Short Description ?

CHAPTER 1

New and Changed Information 1

New and changed information for release 5.3.x 1

CHAPTER 2

Introduction to Cyber Vision 5

Cisco Cyber Vision Installation 5

Overview 5

Interactive Help 6

Understanding Concepts 6

Preset 6

Filters 7

Component 12

Device 13

Activity 15

Flow 17

External Communication 18

Time Span 20

Tags 21

Properties 24

Vulnerability 25

Credentials 28

Variable accesses 29

Variable accesses details 30

Enable variable processing in a sensor template 31

Creating and Customizing Groups 31

Active Discovery 35
Navigating Through Cisco Cyber Vision 36
Home 36
Explore 37
Preset Views 40
Detail Panel 48
Reports 51
Create a Report 51
Events 52
The Dashboard of Events 53
The List of Events 53
Monitor 53
Search 54
System Statistics 54
Center 55
Services Statistics 58
Sensors 58
My Settings 61
Risk Score 62

CHAPTER 3 Licensing 67
Cisco Cyber Vision Licenses 67
Trial Licenses for Cisco Cyber Vision 67
Essentials and Advantage Licenses 68
Licenses for Intrusion Detection System Components 69
Cisco Smart Software Manager Satellite for Air-Gapped Networks 69
Register Your Essentials or Advantage Licenses 69
Register Licenses With CSSM On-Prem 71
Reregister Your Licenses 72
Deregister Your Licenses 72
Use Specific License Reservation 72
Update Specific License Reservation 73
Return Specific License Reservation 74
Managed Services License Agreement 75

License Usage Compliance 75

CHAPTER 4 Get Started with Cisco Cyber Vision 77

Certificate fingerprint 77

Data Management 77

Data clearance operations 78

Purge components from the database 78

Expiration settings 79

Ingestion configuration 80

Users 81

Management 81

Role Management 82

Create a user role 83

Security Settings 83

Center Web Server Certificate 84

CHAPTER 5 Configure Cisco Cyber Vision 85

Network Organization 85

Define a Subnetwork 86

API Token 87

API Documentation 88

Active Discovery Policies 91

LDAP 91

Configure LDAP 92

Single sign-on (SSO) 93

SAML single sign-on 94

Requirement: SSO configuration for Cisco Cyber Vision Center 94

Single sign-on user accounts 95

User role mappings for SSO users 95

Azure AD single sign-on integrations 96

Add an enterprise application in Azure 96

Configure Azure SSO for Cyber Vision Center 97

Configure Cyber Vision Center for Azure SSO 98

Duo Single Sign-On solutions 99

Requirement: Prerequisites for Duo Single Sign-On setup 100
Configure Cyber Vision Center application in Duo 101
Configure Cisco Cyber Vision Center for Duo 102
Sensors 104
Sensor Explorer 104
Filter and Sort the Sensor List 104
Sensors Status 105
Sensors Features 106
Install Sensor 107
Sensor Self Update 107
Manage Credentials 108
Organize Sensors 108
Set a Capture Mode 109
Deployment Tokens 110
Create Deployment Tokens 111
Templates 112
Create Templates 112
Export Templates 113
Import Templates 113
Management Jobs 114
PCAP Upload 114
SNMP 115
Configure SNMP 115
SNMP MIB 117

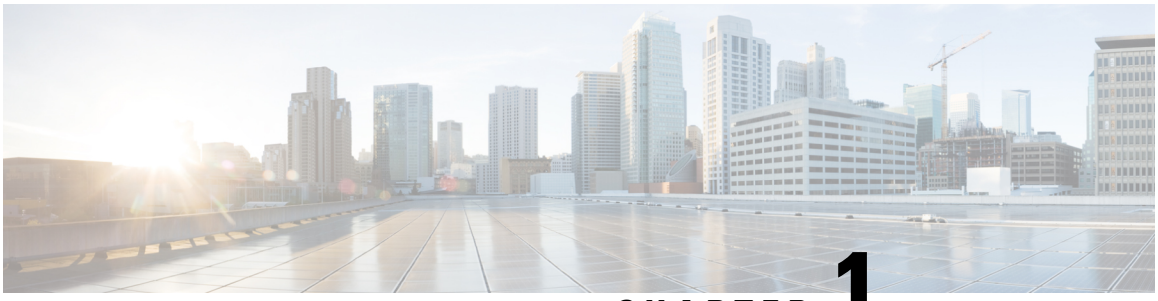
CHAPTER 6 **Integrate with Cisco Cyber Vision** 119
pxGrid 119
XDR 119
XDR Configuration 120
XDR Ribbon 121
XDR Event Integration 122
XDR Component Button 122
External Resources for XDR Integration 123
Secure Equipment Access 123

Integrate Cisco Cyber Vision Center with SEA 127
Cisco In Product Support 127
Access Cisco In Product Support 128

CHAPTER 7 **Maintain and Monitor Cisco Cyber Vision** 131
Monitored presets 131
Create categories 133
Create presets 134
Create baselines 134
Configure monitored presets 135
Manage monitored preset differences 135
Center Shutdown/Reboot 137
Upgrade with a Combined Update File 137
Syslog configurations 139
Configure syslog 139
Import/Export 140
Knowledge DB 141
Certificate fingerprint 141
Cisco Cyber Vision Telemetry 142
Reset to Factory Defaults 142
Snort 143
Snort rulesets and rule categories 143
Snort rules management features 145
Enable IDS on a sensor 145
Risk Score 146
Extensions 146

CHAPTER 8 **Cyber Vision New UI** 147
Cyber Vision New UI 147
Assets 148
Asset data management 149
Vulnerabilities 150
Vulnerability scores 150
Acknowledge or revert a vulnerability acknowledgement 151

Communication maps 151
Assets and functional group communication maps 153
Asset clustering 154
Cluster assets into functional groups 155
Asset clustering methods 156
Functional group actions and descriptions 156
Alerts 157
Alert type management options and permitted alert rule actions 159
Create alert rules 159
Syslog notification details for various alert types 161
Enable or disable syslog notifications for alert types 162
Organization hierarchies 162
Filters 163
Filter views in Cyber Vision New UI 164
Network definitions 164
Assign a network to an organization hierarchy 165
Pcap files 166
Assign multiple PCAP files to an organization hierarchy 166
Sensor applications 167
Assign sensors to the Organization Hierarchy 168
Use Cases 168
Filter PLCs by organization hierarchy 168
Acknowledge critical vulnerabilities 169



CHAPTER 1

New and Changed Information

- New and changed information for release 5.3.x, on page 1

New and changed information for release 5.3.x

Cisco Cyber Vision Release 5.3.x offers these features:

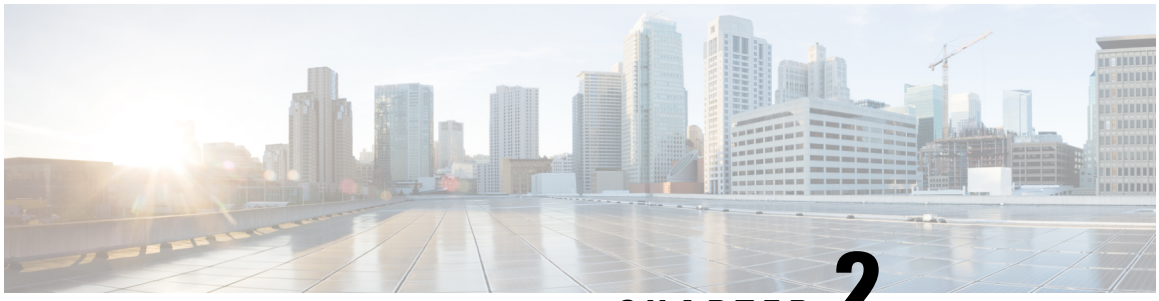
Table 1: New and changed information, release 5.3.x

Feature	Description
New UI	Cisco Cyber Vision Center offers New UI that comprises simplified, structured views of assets, vulnerabilities, and alerts. The New UI includes a new method for automatically grouping assets using AI-based clustering. Click **Go to Cyber Vision New UI** in the top banner of your Center to get started. See Cisco Cyber Vision New UI.
(New UI) Receive property-based group suggestions from asset clustering algorithm	Asset clustering algorithms suggest property-based groups (assets that share the same definition, network, or other properties), in addition to communication-based groups (assets that primarily communicate with each other). See Asset clustering.
(New UI) Filter Cyber Vision Center data by organization hierarchy	All the data views in New UI can be filtered by organization hierarchy, by sensors or networks that an asset is associated with. At the top of the left menu, in the **Organization** filter, choose the hierarchy level you want to focus on. **Global** is the default choice and covers all assets. See Filter views in Cyber Vision New UI.

Feature	Description
(New UI) Filter data in Cyber Vision Center	A product-level banner in New UI allows you to filter data on all its pages, except configuration pages. If you have not applied any filters, the value **No filter applied** is displayed. Click **Edit** to apply one or more filters from functional group, network or sensor, asset type, and vendor categories. See Filter views in Cyber Vision New UI.
(New UI) Assign a network to an organization hierarchy	Assign a network to an organization hierarchy level. See Assign a network to an organization hierarchy.
(New UI) See functional-group centric views of communication map	The communications map displays the communication activity between the configured functional groups. The communication links between groups are not actionable. Click a functional group to view the inter-asset communications within a group. Click the communication links between assets to view the details of the activities. See Assets and functional group communication maps.
(New UI) Active and cleared alerts	The **Alerts** page displays two types of alerts: • Active: alerts that are currently active in Cisco Cyber Vision and are yet to be addressed. • Cleared: alerts that are no longer considered active due to actions such as vulnerability acknowledgement or editing alert rules. A cleared alert is displayed in this list for up to 14 days. See Alerts.
(New UI) Pause alert creations	You can pause an alert type in the **Configure** > **Alerts** page to pause alert matching for the configured alert rules. You can resume alert creation from the same page at any time. See Alert type management options and permitted alert rule actions.
(New UI) Change vulnerability scoring system for alerts	The Cisco Security Risk Score is the default scoring system applied to alert configurations. However, you can choose to update an alert configuration to apply the CVSS scoring system instead. See Create alert rules.
(New UI) Alert for severe vulnerabilities in monitored entities	Create and edit rules for the **Severe vulnerabilities in monitored entities** alert based on the Cisco Security Risk Score or the CVSS score. You can edit each rule in this alert type for greater control over the alerts you see. See Alerts.

Feature	Description
(New UI) Alert for prohibited vendors	The **Configure** > **Alerts** page contains a default alert for prohibited vendors. The alert rule is based on an editable list of prohibited vendors. You cannot add any other rules to this alert type. See Alerts.
(New UI) Using asset vendor names and icons	Cisco Cyber Vision center infers device type based on device vendor name, enhancing asset identification and grouping processes. In New UI, communication maps now include icons of vendors to help you identify assets more easily. See Assets and functional group communication maps.
(New UI) Search bar	New UI contains a search bar in the global top banner. You can search for an asset by name, IP address, or MAC address. See Asset data management.
Non-CEF syslogs support removed	You can no longer use non-CEF syslog formats with Cisco Cyber Vision Center. Any existing syslog connections that are based on non-CEF formats are automatically updated to CEF formats when you upgrade to Cisco Cyber Vision Center Release 5.3.x. See Configure syslog.
SAML 2.0 SSO authentication support	Cisco Cyber Vision Center supports SAML 2.0 SSO authentication. See Single sign-on (SSO).
Clear multiple components using a VLAN ID	When you clear data, you can enter a VLAN ID to purge all the components associated with it. You can clear data for one VLAN ID at a time. See Purge components from the database.
Device list CSV enhancements	The device list CSV that you download from Cisco Cyber Vision Center includes a column to list the sensors that have seen that device.
Cisco In Product Support	Use Cisco In Product Support to manage your Cisco support cases and related tasks directly from the Center. See Cisco In Product Support.
Enable or disable Snort on a Center DPI interface	You can choose to enable or disable Snort IDS/IPS on a Cisco Cyber Vision Center DPI interface. In earlier releases of Cisco Cyber Vision Center, Snort was enabled by default and could not be modified. See Enable IDS on a sensor.

Feature	Description
Detect and process variable data	Cisco Cyber Vision sensors can capture and relay measurable variables such as pressure or temperature to Cisco Cyber Vision Center. Enable Variables Storage in the **Admin** > **Data Management** > **Ingestion Configuration** page of Cisco Cyber Vision Center to allow the center to add the variables to the database for processing. See Enable variable processing in a sensor template.
Integration with Secure Equipment Access	You can integrate Cisco Cyber Vision Center with Cisco Secure Equipment Access for remote access management of your OT assets. See Integrate Cisco Cyber Vision Center with SEA.



CHAPTER 2

Introduction to Cyber Vision

- Cisco Cyber Vision Installation, on page 5
- Overview, on page 5
- Interactive Help, on page 6
- Understanding Concepts, on page 6
- Navigating Through Cisco Cyber Vision, on page 36
- Risk Score, on page 62

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.

Interactive Help

Cisco Cyber Vision offers contextual help through the Interactive Help feature. The Interactive Help menu offers easy access to a wide range of documentation resources, and to step-by-step walkthroughs of select taskflows.

Cisco may collect some anonymous product usage behavior data in accordance with the Cisco End User License Agreement and the Cisco Privacy Statement for optimal delivery of Interactive Help.

Access Interactive Help

Interactive Help is enabled by default. To access the Interactive Help menu:

- In the classic GUI, a vertical blue ribbon is displayed in the bottom right of the Cisco Cyber Vision window. Click the ribbon.
- In the new GUI, in addition to the vertical ribbon, you can access the menu by clicking the **?** icon in the top banner, and selecting **Interactive Help**.

To disable the Interactive Help feature, carry out the following steps.

Procedure

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

Step 2 To disable the feature, in the Interactive Help area, click the toggle button.

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.

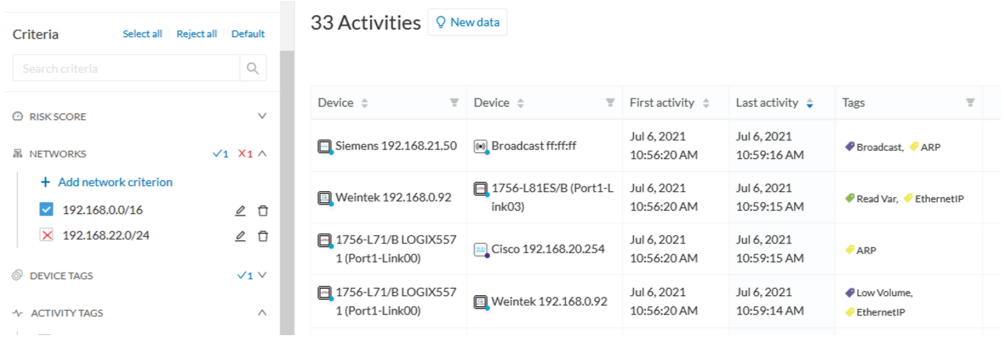
Networks

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.

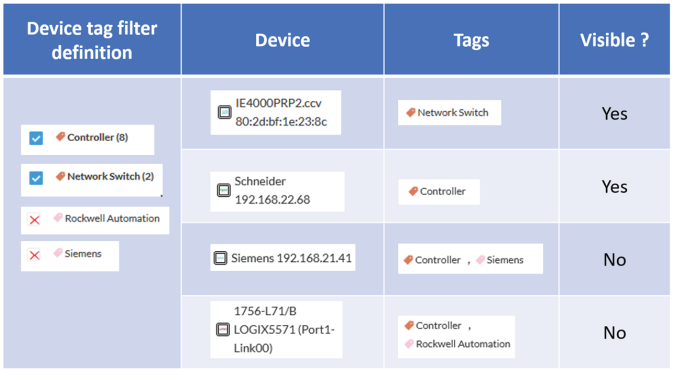
Filter combination

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:

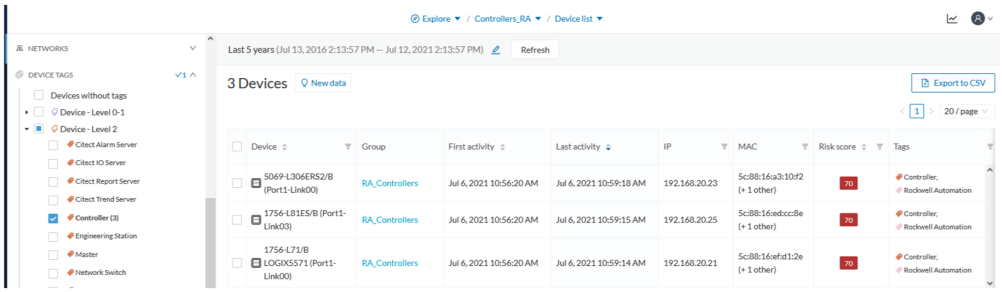
Device tag filters



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).

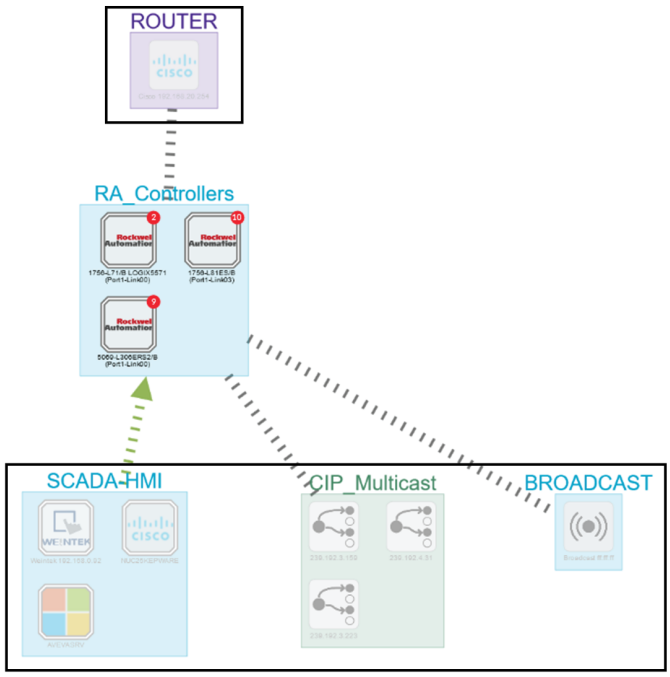
It will give the following results:

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

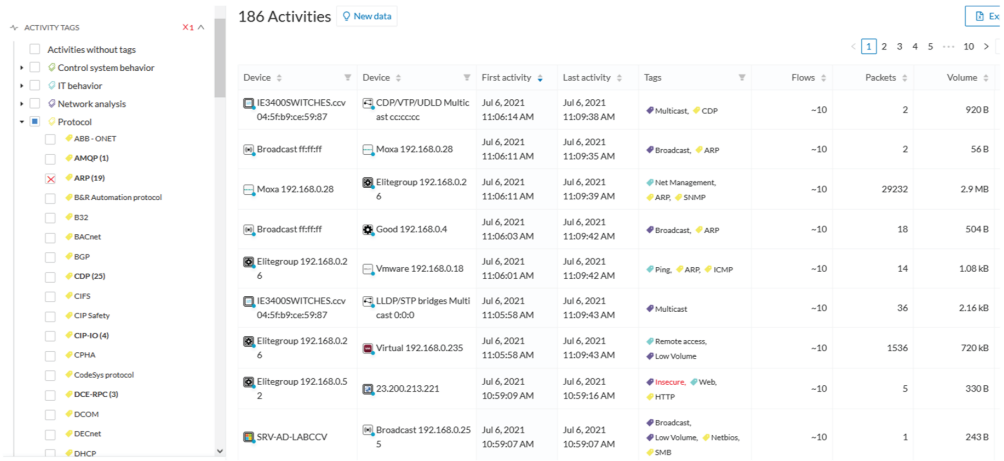


Activity Tags

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.

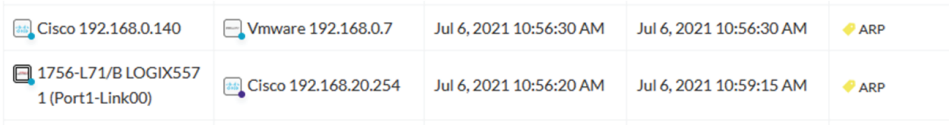
For example, if an activity has two tags, both tags need to be excluded to hide the activity.

Activity filter – negative filter 1



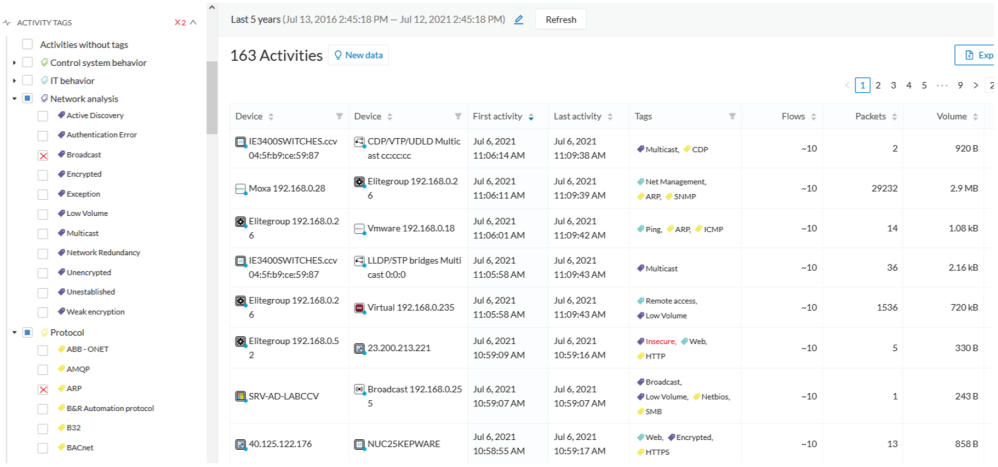
In the example above, several activities show because the ARP tag is present, as well as other **Activity tags**. There is no exact match. The activity below is hidden.

filter 2



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

Activity filter – negative filter 3



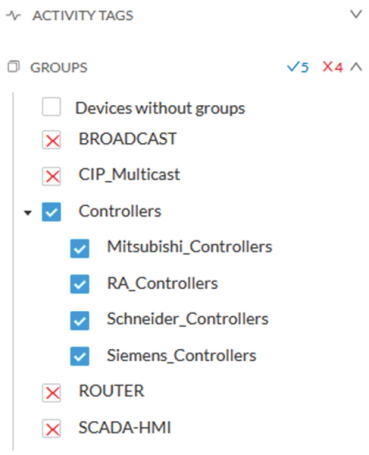
For very specific use cases, combine inclusive and exclusive tags. The above rules, for positive and negative selection, are combined, resulting in the following logic:

- 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.

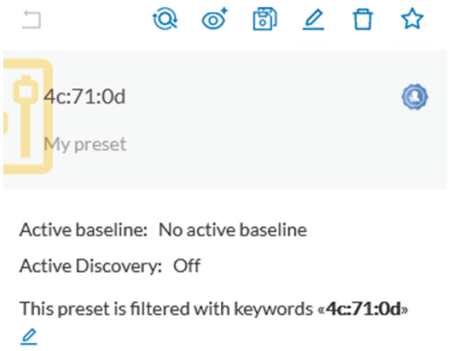
Sensor filter



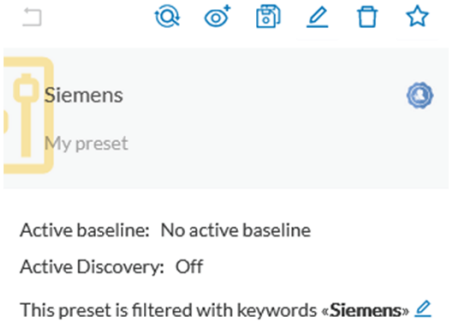
Keyword

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 side panel with the detailed component information opens.

Device

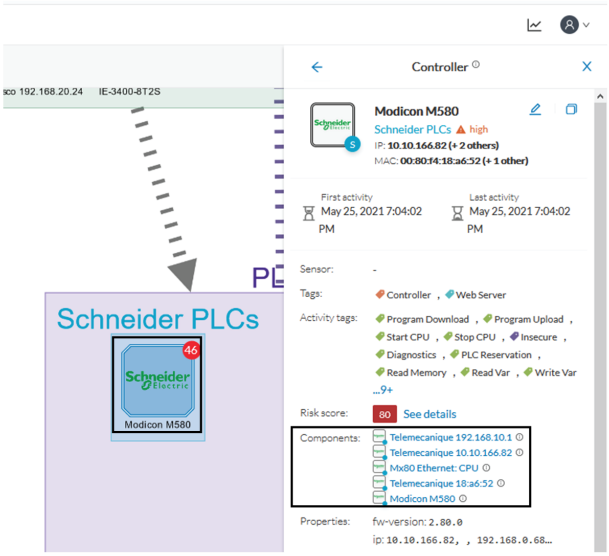
The term **Device** is an aggregation of components with similar properties. In Cisco Cyber Vision, a **Device** is a physical machine of the industrial network such as a switch, an engineering station, a controller, a PC, a server, etc. Devices simplify data presentation, especially on the map. Devices 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 Vulnerabilities.

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

5 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 devices or components. 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.

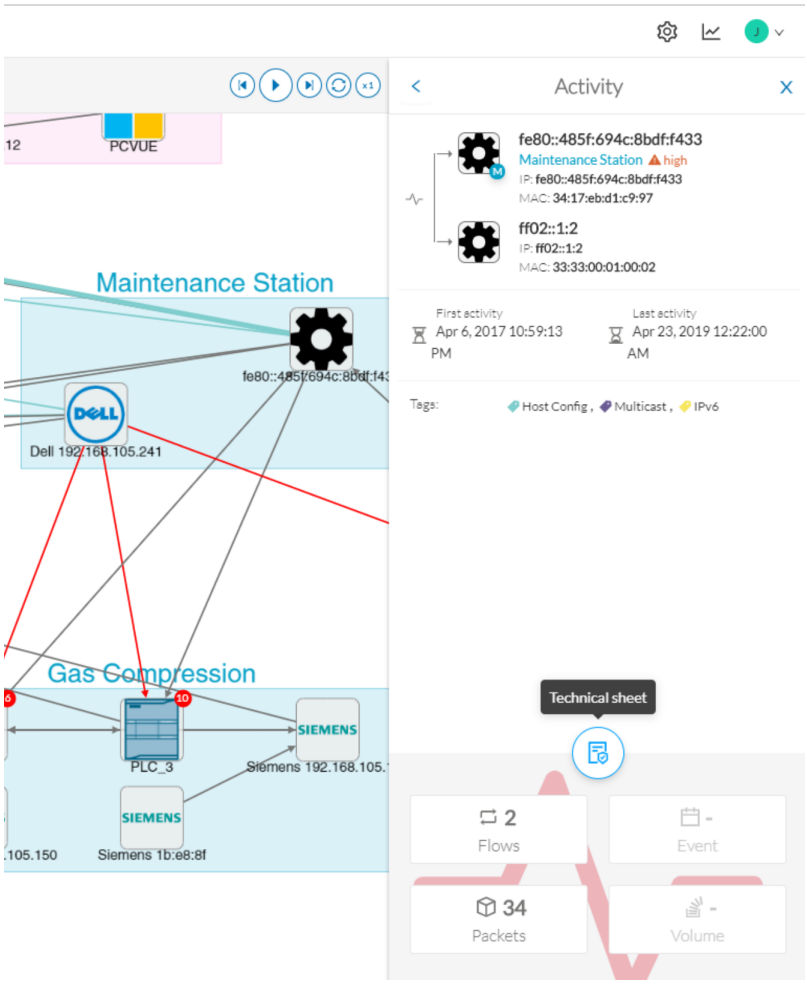


An activity between two components is actually a simplified view of the flows exchanged. You can have many types of flows going in both directions inside an activity, represented in the map.

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 sheet that shows more details about tags and flows.

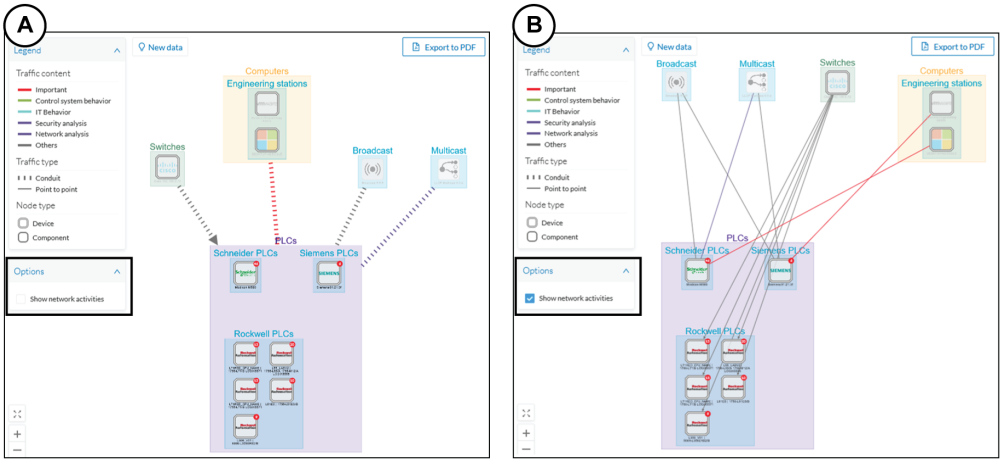


Devices or components with no activity does not mean that they did not have any interaction. In fact, a component can only be detected if it has been involved in a network activity (communication emission/reception). Lack of activity can mean that the other linked component is not part of the preset 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 conduits.

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 sheet icon > **Activity**. Or, click the **Flows** tile from the right side panel.

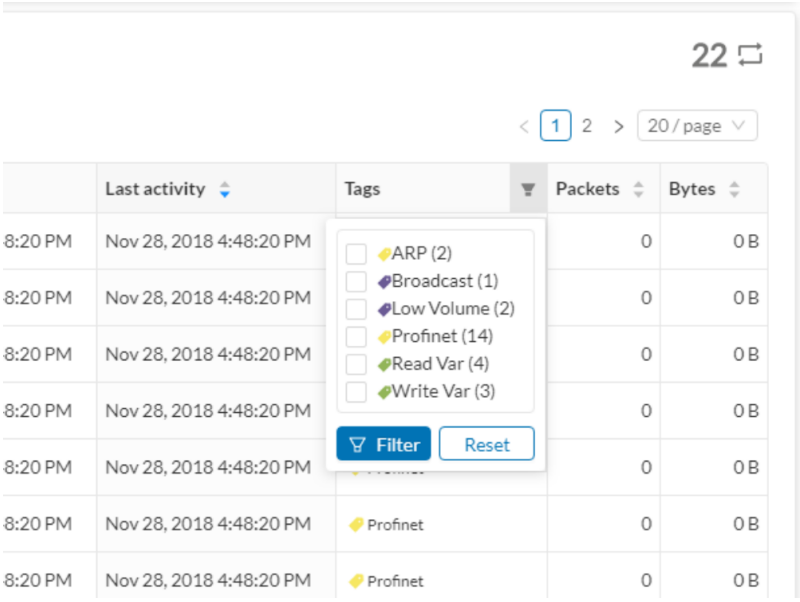
The Activity tab contains a list of flows which gives you detailed information about each single flow: number of flows in the activity, source and destination components (if known), ports used, first and last activity, and tags which characterize each flow.

Flows 12467

1 2 3 4 5 ··· 624 > 20 / page

Component	Port	Direction	Component	Port	First activity	Last activity	Tags	Packets	Bytes
PROPLUS	18507	→	Fisher 10.4.0.30	18507	Sep 25, 2019 12:06:02 PM	Sep 25, 2019 12:09:21 PM	Read Var , DeltaV protocol	409522	51.1 MB
PROPLUS	123	-	10.5.255.255	123	Sep 25, 2019 12:06:02 PM	Sep 25, 2019 12:09:21 PM	Time Management , Broadcast	2902	261 kB
Fisher 10.5.0.18	18507	-	PROPLUS	18507	Sep 25, 2019 12:06:02 PM	Sep 25, 2019 12:09:21 PM	Read Var , DeltaV protocol	105112	16.5 MB
PROPLUS	18515	-	PROPLUS	18507	Sep 25, 2019 12:06:02 PM	Sep 25, 2019 12:09:21 PM	Multicast , DeltaV protocol	5720	1.03 MB
PROPLUS	18507	→	OWS1	18507	Sep 25, 2019 12:06:02 PM	Sep 25, 2019 12:09:21 PM	Read Var , DeltaV protocol	99540	8.64 MB
PROPLUS	18507	→	Fisher 10.5.0.22	18507	Sep 25, 2019 12:06:02 PM	Sep 25, 2019 12:09:21 PM	Read Var , DeltaV protocol	135762	15.5 MB
PROPLUS	18507	→	Fisher 10.4.0.14	18507	Sep 25, 2019 12:06:02 PM	Sep 25, 2019 12:09:21 PM	Read Var , DeltaV protocol	183442	26.9 MB
							Ping ,		

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.

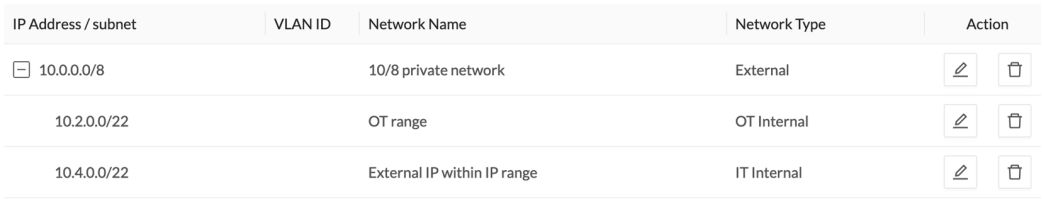
External communications are stored and listed in Cisco Cyber Vision, but not the external components/devices, nor their flows, to not obstruct the system. As a result, Cisco Cyber Vision's performances are increased, the GUI is cleared from unecessary data, and the license device count and risk scores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

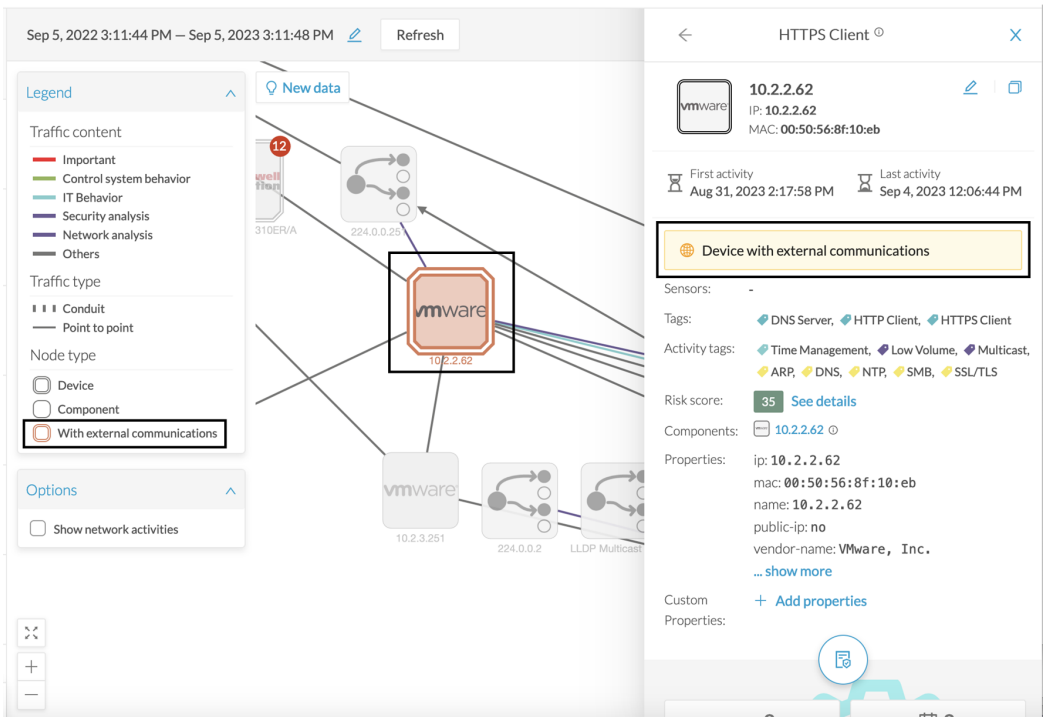
However, because sometimes public IP addresses are used in a private network of an industrial site, it is possible to manually define communications by declaring IP ranges as internal or external through the Network Organization administration page. For more information, refer to Cisco Cyber Vision GUI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



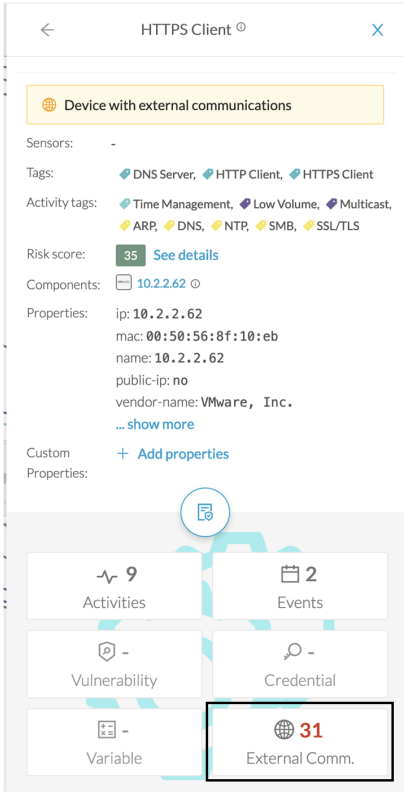
In the GUI, a component with external communications is shown as an icon bordered in orange, or a double orange border for a device.

A device with external communications in the Map:

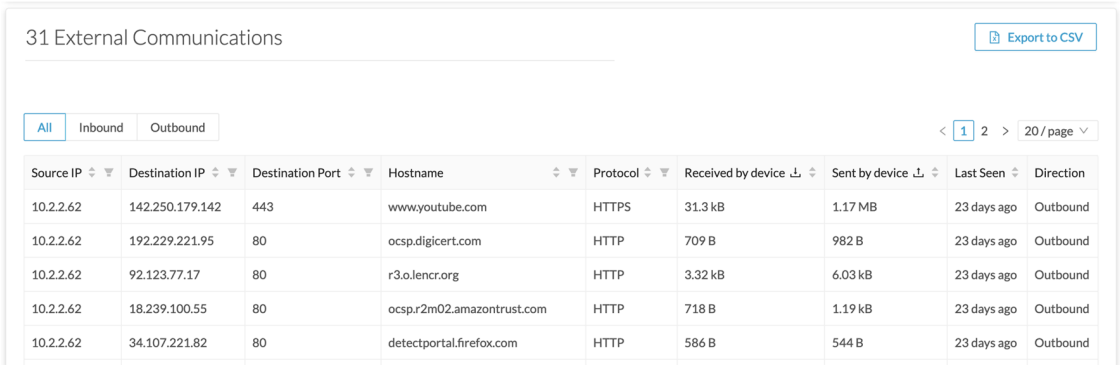


If you click on this component, its right side panel will appear. The **External Communications** button with the number of external communications will open the component's technical sheet directly on the external communications list.

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



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



Source IP	Destination IP	Destination Port	Hostname	Protocol	Received by device	Sent by device	Last Seen	Direction
10.2.2.62	142.250.179.142	443	www.youtube.com	HTTPS	31.3 kB	1.17 MB	23 days ago	Outbound
10.2.2.62	192.229.221.95	80	ocsp.digicert.com	HTTP	709 B	982 B	23 days ago	Outbound
10.2.2.62	92.123.77.17	80	r3.o.lencr.org	HTTP	3.32 kB	6.03 kB	23 days ago	Outbound
10.2.2.62	18.239.100.55	80	ocsp.r2m02.amazontrust.com	HTTP	718 B	1.19 kB	23 days ago	Outbound
10.2.2.62	34.107.221.82	80	detectportal.firefox.com	HTTP	586 B	544 B	23 days ago	Outbound

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:

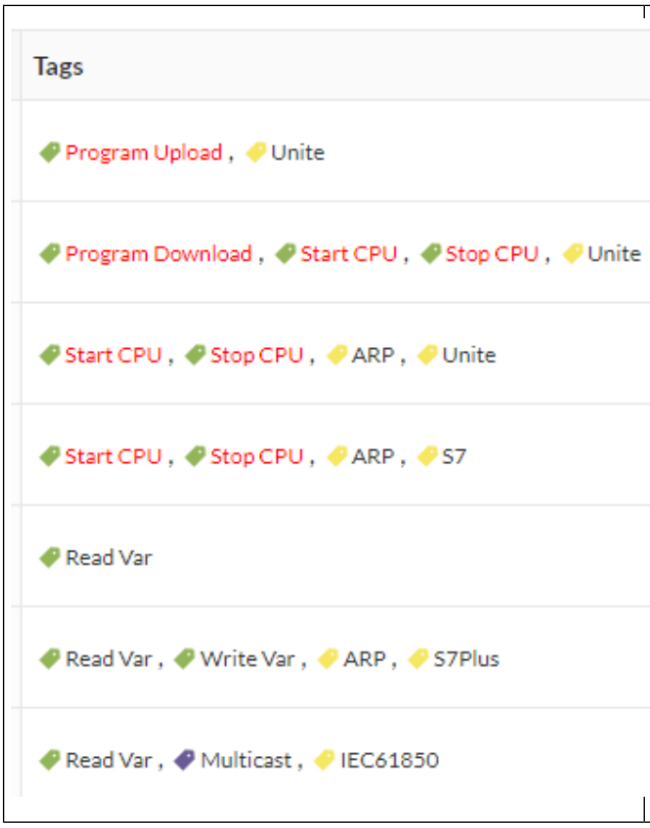
Generally, you can set the time period to 1 or 2 days. This setting is convenient to have an overall view of most supervised standard network activities. This includes daily activities such as maintenance checks and backups.

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



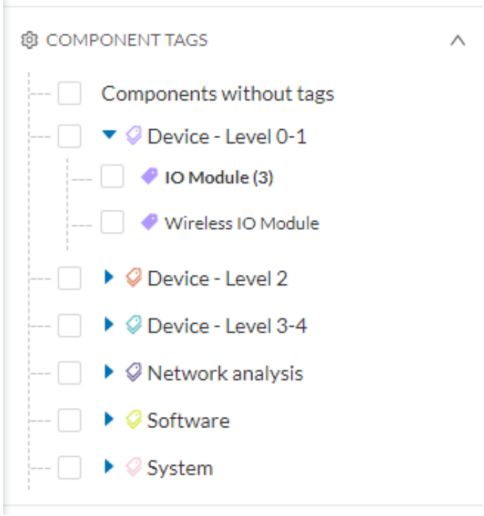
Tags are meaningful labels that succinctly describe a network. They can be applied to components or activities. Each tag has a description and an icon color which correspond to its category.

Tags are metadata on devices and activities. 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 filter the different views.

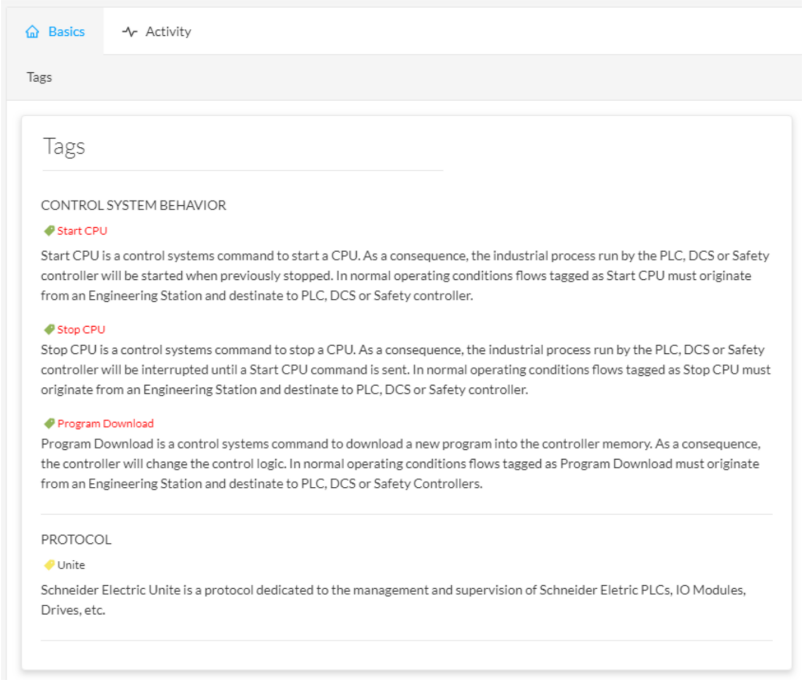
Use tags to define behaviors (i.e., in the Monitor mode) inside an industrial network when combined with information like source and destination ports and flow properties.

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 Navigating through Cisco Cyber Vision..

For detailed information about a tag, see the **Basic** tab inside a technical sheet.

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.

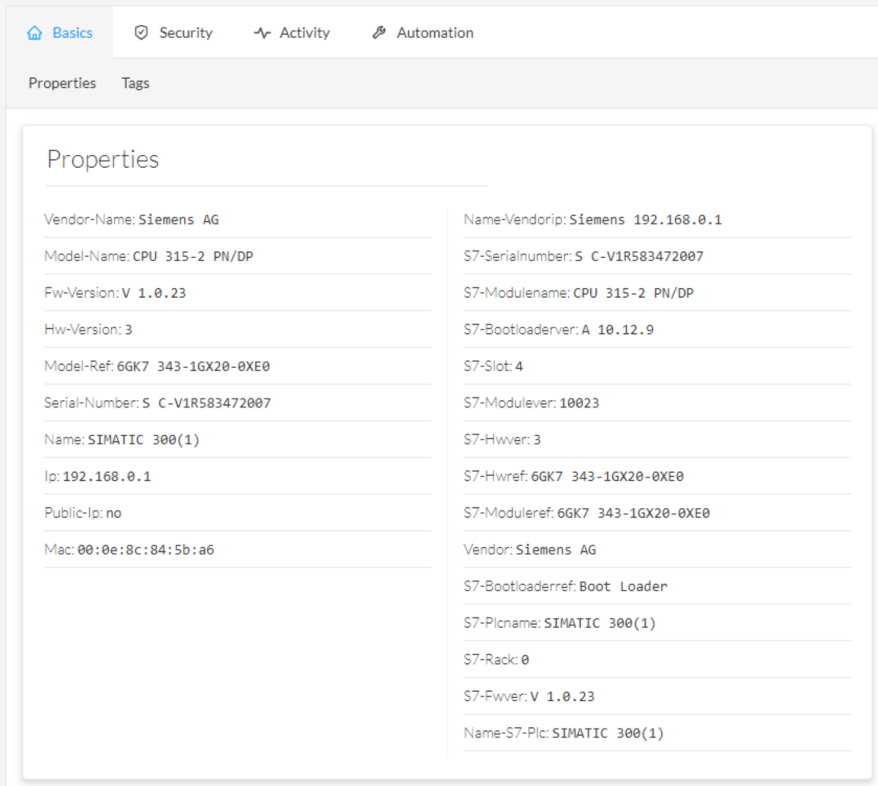
Property Use

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 right side panels 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

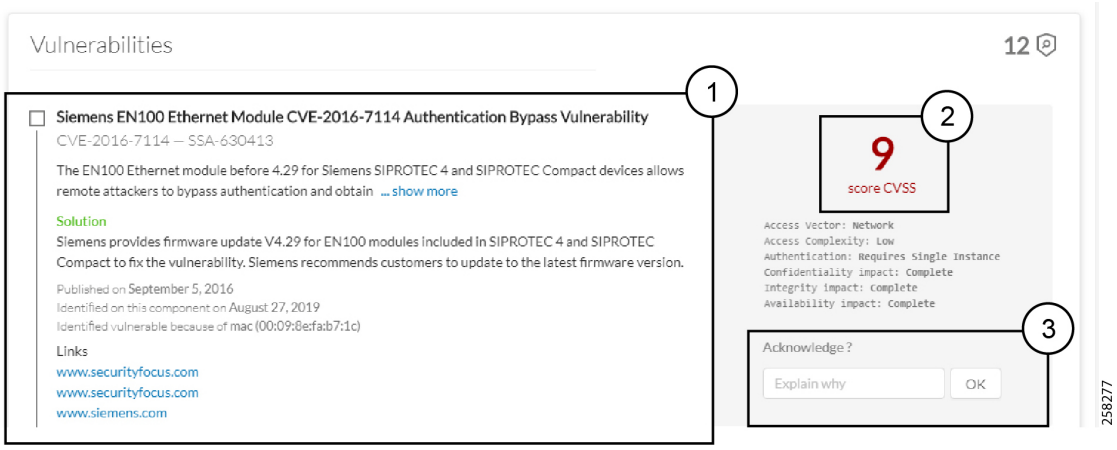
Vulnerabilities are weaknesses detected on devices that can be exploited by a potential attacker to perform malevolent actions on the network.

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

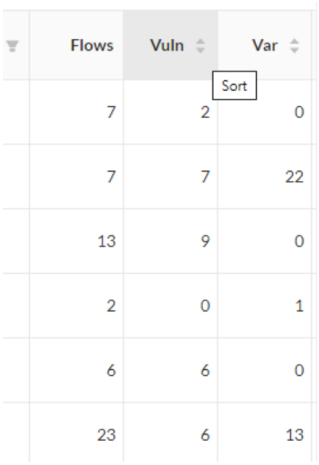
Below is an example of a Siemens component's vulnerability. See the technical sheet, Security tab.



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**.

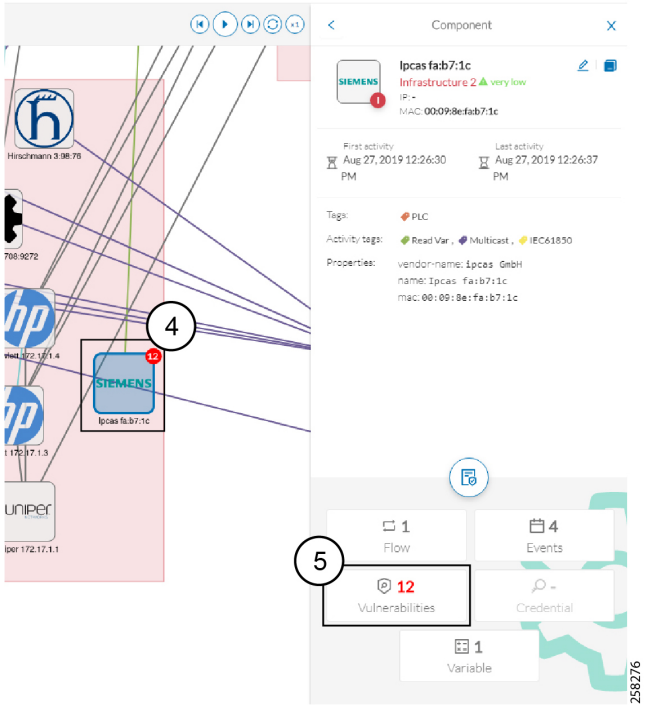
Vulnerability Location

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

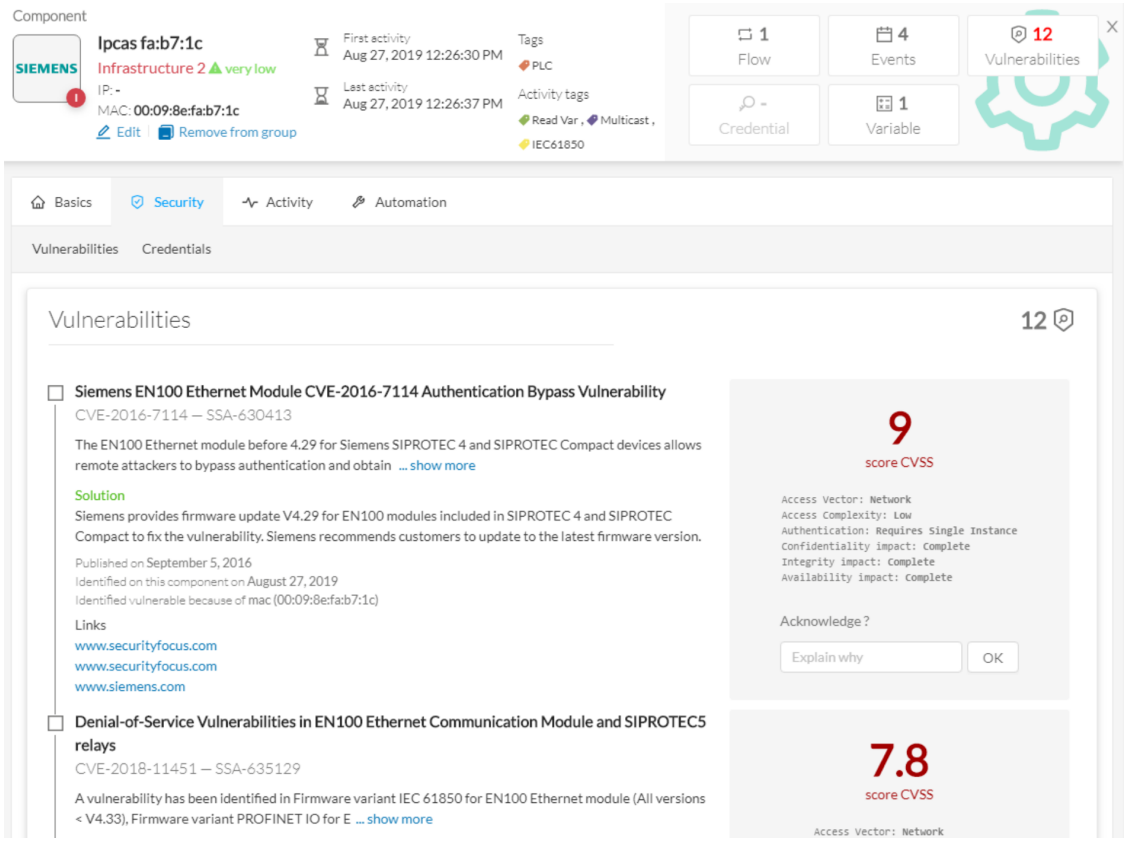




Find vulnerabilities on the map by a device or a component with a red counter badge. Click the badge **(4)** and the side panel opens with the number of vulnerabilities shown in red.



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



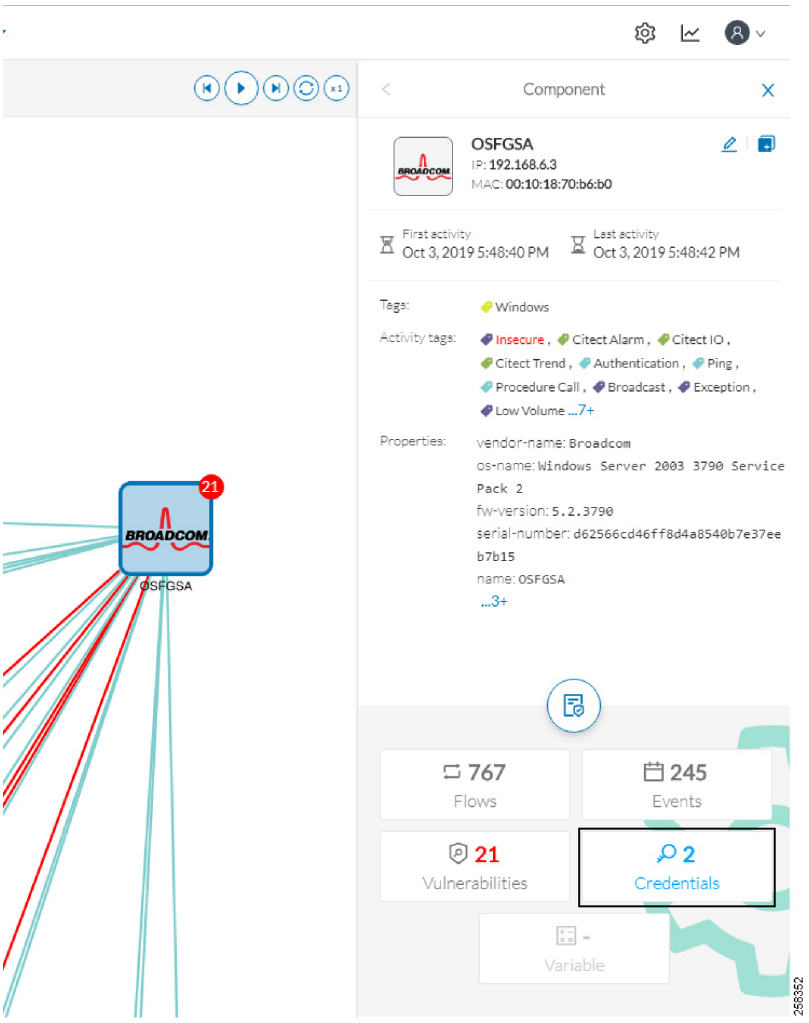
Events

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.

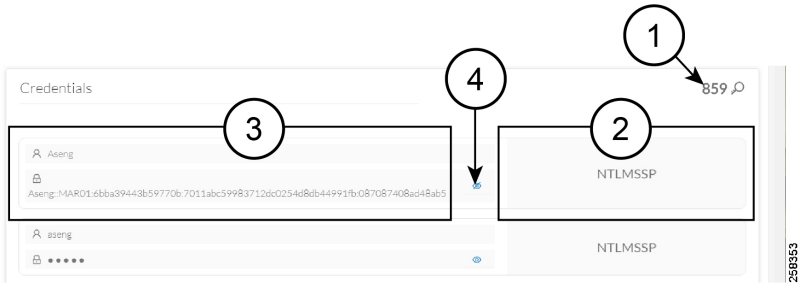
1. The number of credentials found.
2. The protocol used.

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 accesses are process control monitoring records that

- track when devices, such as PLCs or data servers, read from or write to variables,
- record which component performed each access, and
- log the timestamp of each event for operational supervision and security auditing.

Table 2: Feature History Table

Feature	Release Information	Feature Description
Detect and process variable data	Release 5.3.x	Sensors capture and relay measurable variables, such as pressure or temperature, to Cisco Cyber Vision Center. Enable Variables Storage in the **Admin** > **Data Management** > **Ingestion Configuration** page of Cisco Cyber Vision Center. This allows the center to add the variables to the database for processing.

Expanded explanation

Industrial process equipment, like PLCs and OPC data servers, use variables to store values such as temperatures, control settings, or sensor readings. A variable access occurs whenever a system component reads or writes one of these values. Each access is associated with a specific variable name and a physical memory address on the equipment.

Monitor variable accesses to maintain process integrity. Unexpected writes can indicate an attacker attempting to influence equipment operation. Solutions like Cisco Cyber Vision automatically report detected variable accesses, helping operators identify unauthorized or abnormal activity.

Examples:

- Reading the temperature of an industrial oven from its PLC controller is a variable access.
- Writing a new temperature setpoint to the oven's PLC is also a variable access.
- Multiple controllers may access the same variable, as when one PLC reads a value that another PLC writes.

Variable accesses details

The variable accesses table provides detailed information on each variable access detected on industrial network equipment. You can review, sort, and investigate variable activity for operational or security purposes.

Table 3: Fields in the variable accesses table

Field	Description
Variable name	The identifier or label of the variable accessed.
Type	Indicates whether access is READ or WRITE, but does not show the variable's value.
Component	Shows which device or system accessed the variable (for example, a PLC model or OPC server).
First accessed	The timestamp of the first access event for the variable by the component.
Last accessed	The timestamp of the most recent access for the variable by the component.

To locate variable access information

- To view more details about variable accesses, open the technical sheet for the component. For a focused view, select **Automation** or refer to PLC access reports.
- The component list view displays the total number of variable accesses per device. You can sort this list by the "var" column.
- For detailed information on a specific component's variable accesses, click the component.

Enable variable processing in a sensor template

Variable processing enables the center to detect and collect measurable variables from network traffic for monitoring and analysis. Sensors identify these variables and return them to the center.

Before you begin

Enable **Variable Storage**.

1. From the main menu, choose **Admin** > **Data Management** > **Ingestion Configuration**.
2. Enable **Variable Storage** and save changes.



Note **Variable Storage** is disabled by default.

Procedure

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

Step 2 Locate the template and select **Edit** from the **Actions** column.

Note
You can also create a new template.

Step 3 Locate the protocols with variable inspection capability.

Step 4 Check the checkbox under the **Variable Processing** column.

Step 5 Save changes.

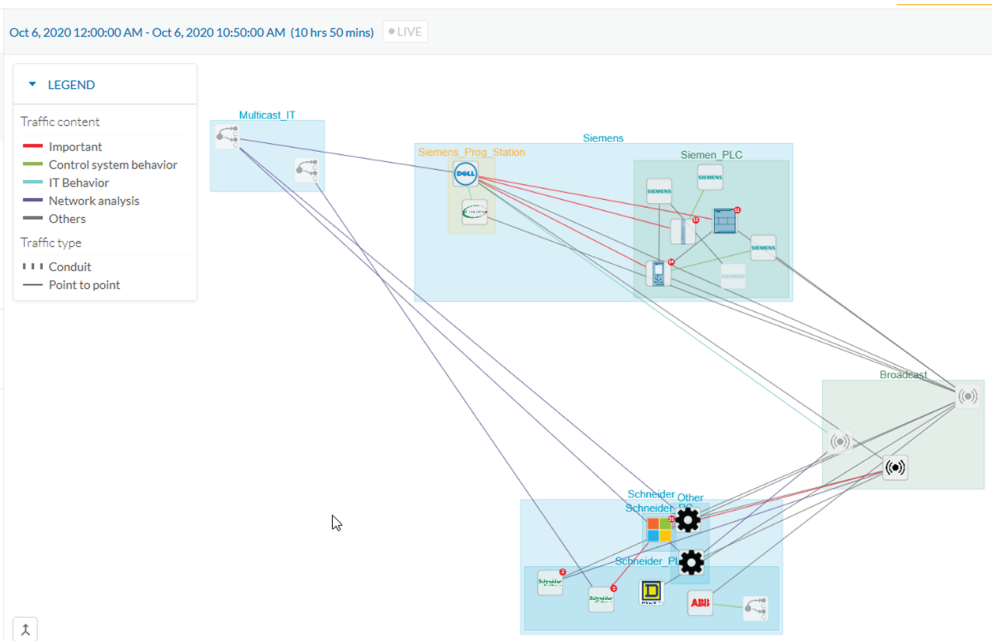
After you complete the configuration, the center sends information to the sensors. The sensors process and identify the variables. You can view detected variables in the center.

What to do next

To view **Variable accesses**, choose **Explore** > **All Data** > **Device list**, select a device, click **Variable** in the drawer, then click **Automation**.

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:

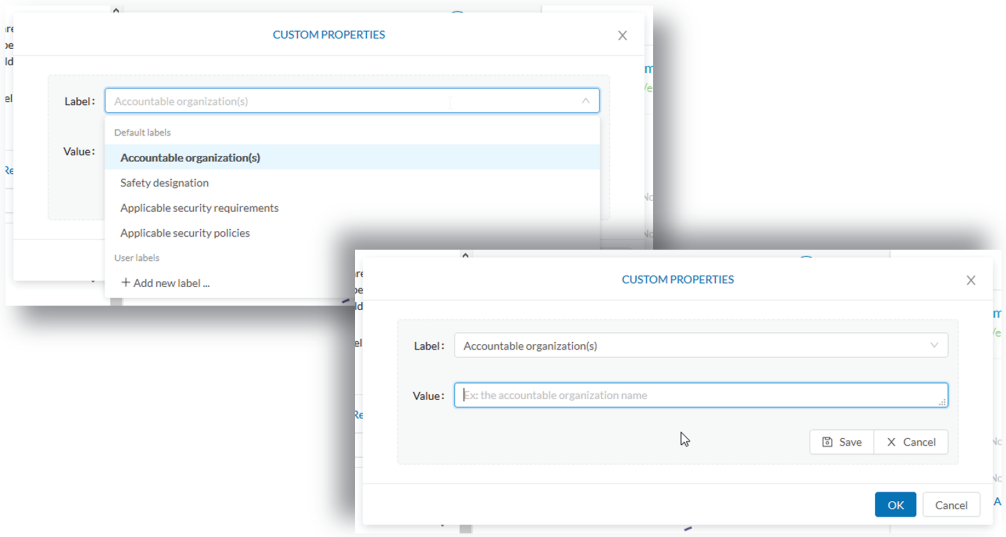
- Select two groups and create a group, as indicated above.
- Select a device or a component and move it into a group. Use the **Move selection to existing group** button.
- Select a group and move it to another group. Use **Move selection to existing group**.

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:

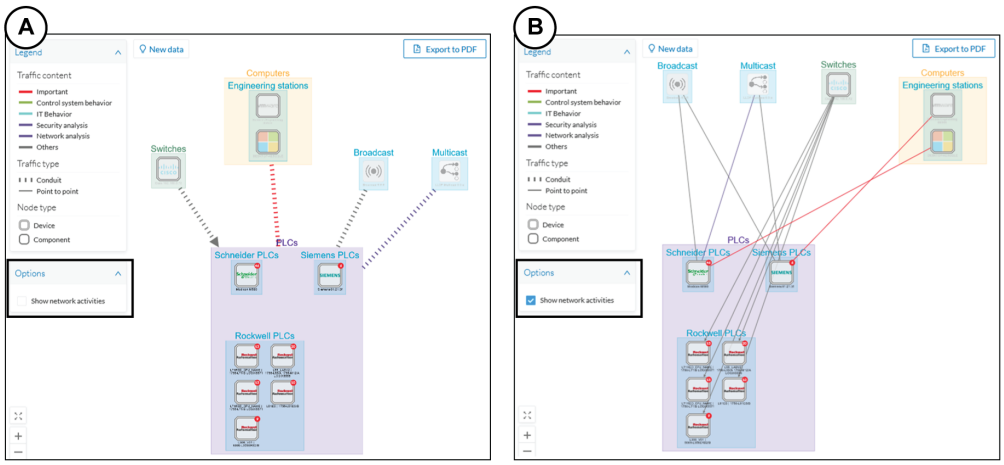
- Select a group in the map and click **Edit** or **Add properties**.
- Choose/define a label and add a value.



Aggregated activities are conduits

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

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.

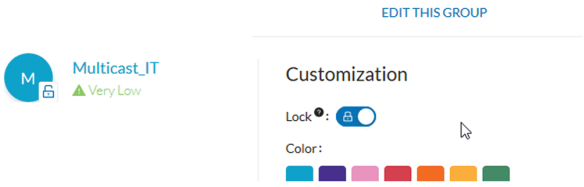
To switch on/off the **Lock** icon:

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

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

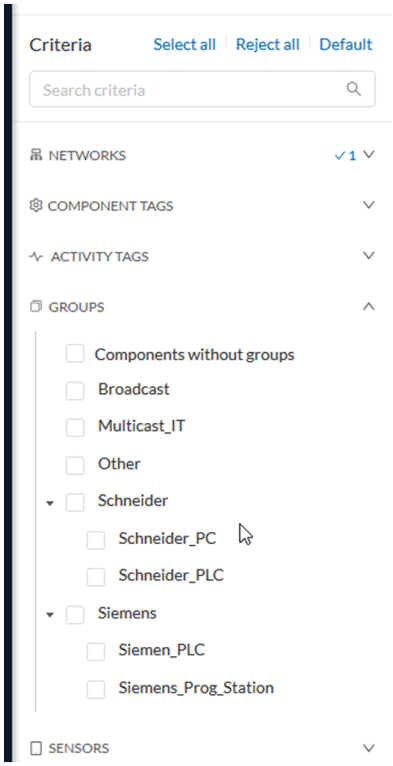
or

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

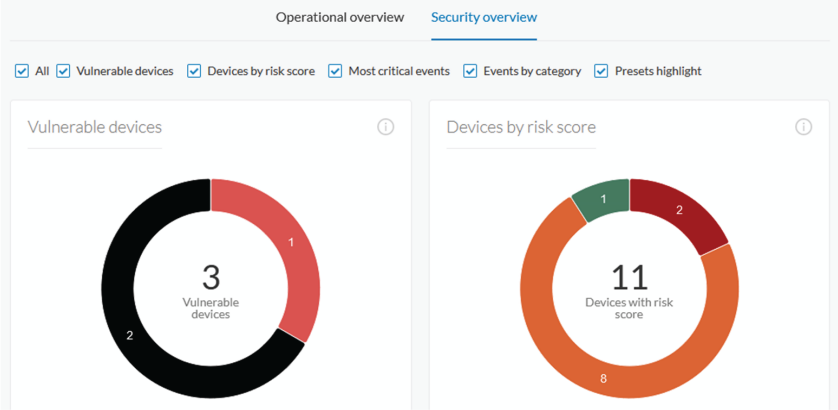
The Cisco Cyber Vision Center's home page displays two tabs: **Operational Overview** and **Security Overview** of the industrial network over the last month.

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.



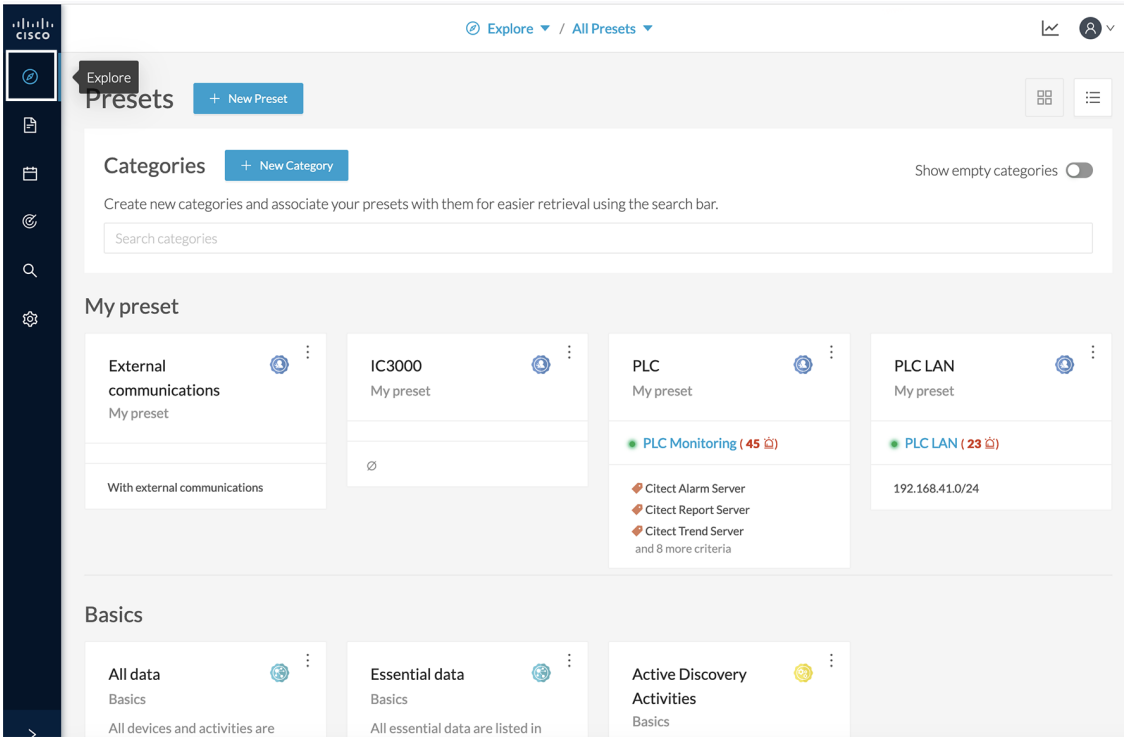
It also shows a list of the **Most critical events**, **Events by category**, and the **Preset highlights** that you can edit.

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

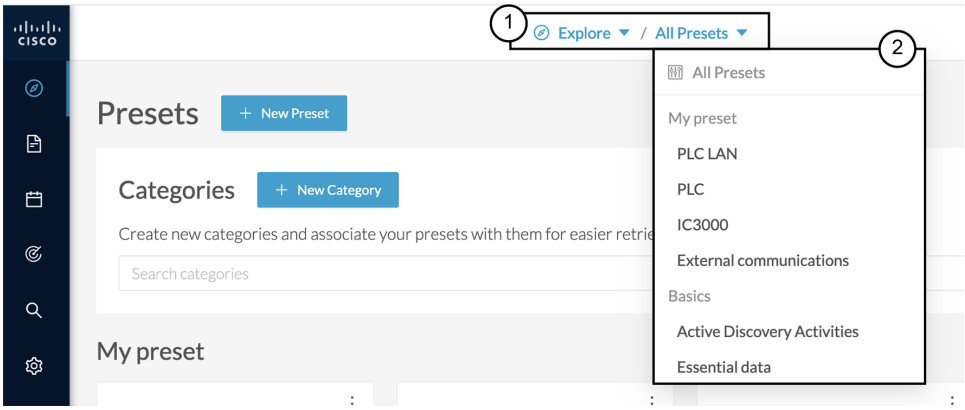
1. **Explore**: Shows the overview of all presets, by defaults or configured.
2. **Reports**: Shows the Reports page to export valuable information about the industrial network.
3. **Events**: Shows the Events page which contains graphics and a calendar of all events generated by .
4. **Monitor**: Shows the page to perform and automatize data comparisons of the industrial network.
5. **Search**: Shows the searching area 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

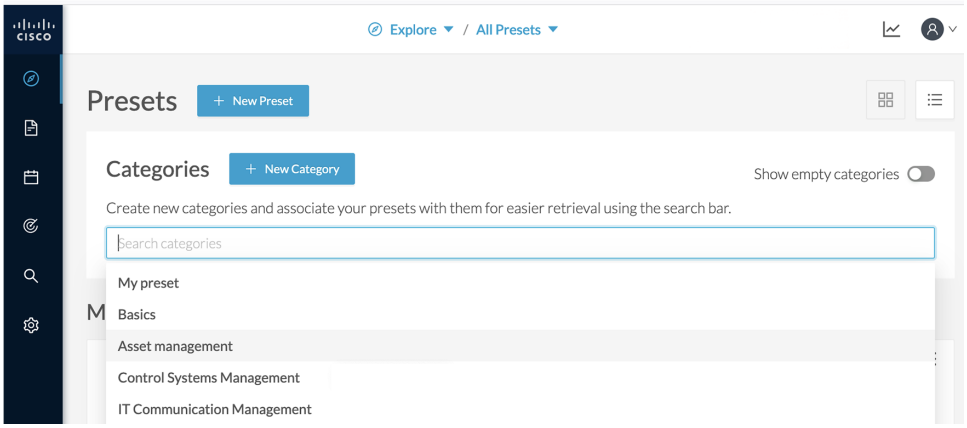
Explore shows an overview of all the Presets in Cisco Cyber Vision, both defaults and custom presets. Click **Explore** on the left navigation bar.



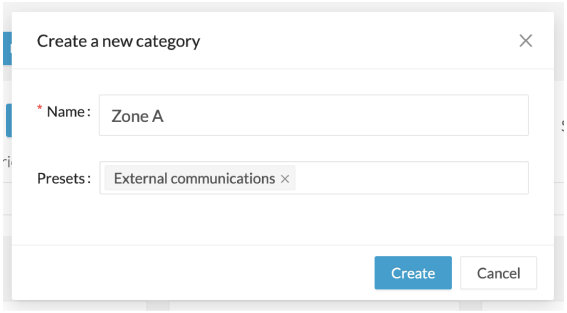
Use the top navigation bar **(1)** to access the different presets **(2)** and views.

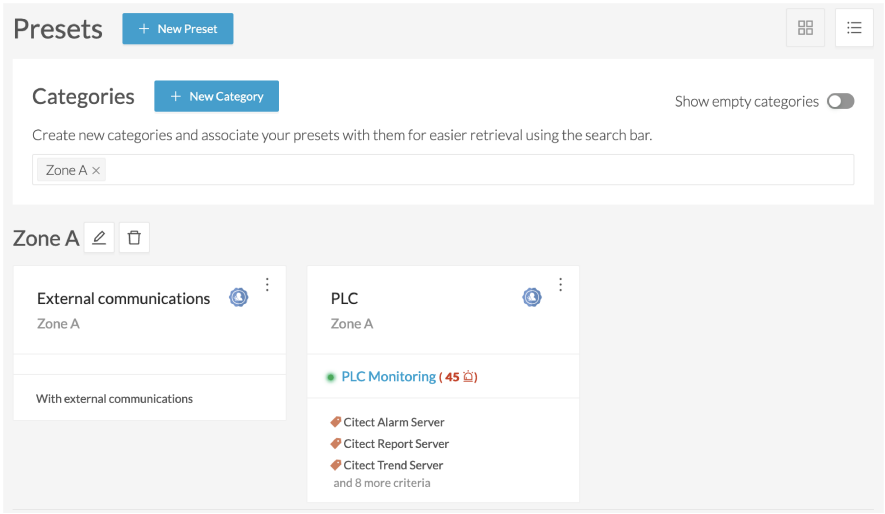


You can also filter presets by categories.

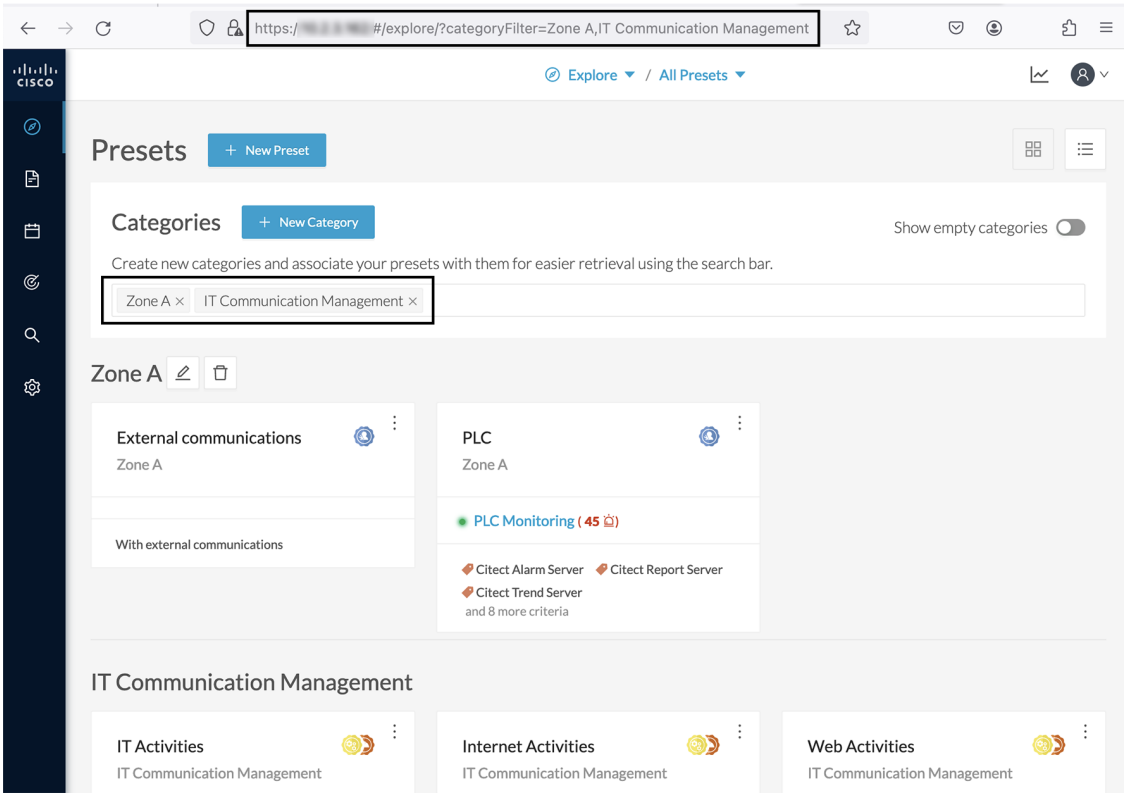


Create new categories to order and search your custom presets.





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.

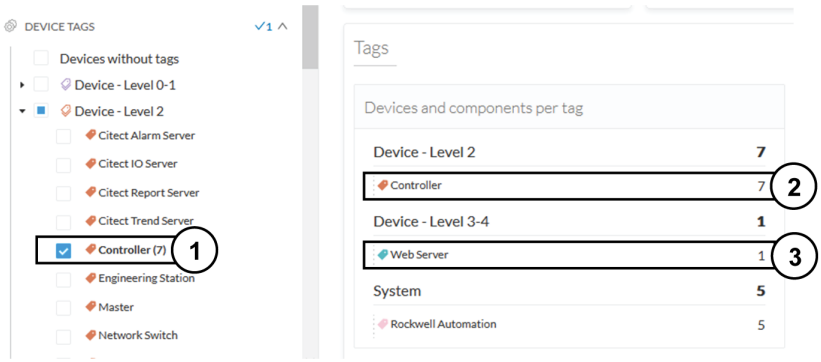
7. Enter the new name in the **Name** field.

   The Preset name should not be the same as previously.

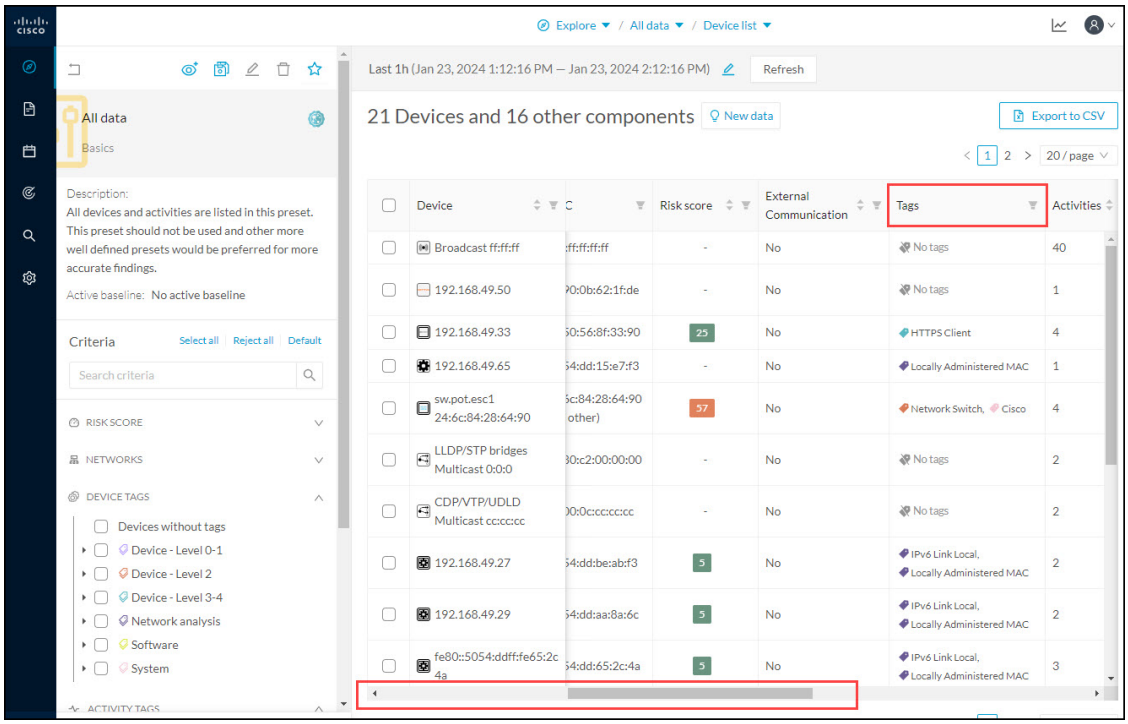
8. Click the drop-down arrow of the **Category** field and select category.

9. Click **OK**.

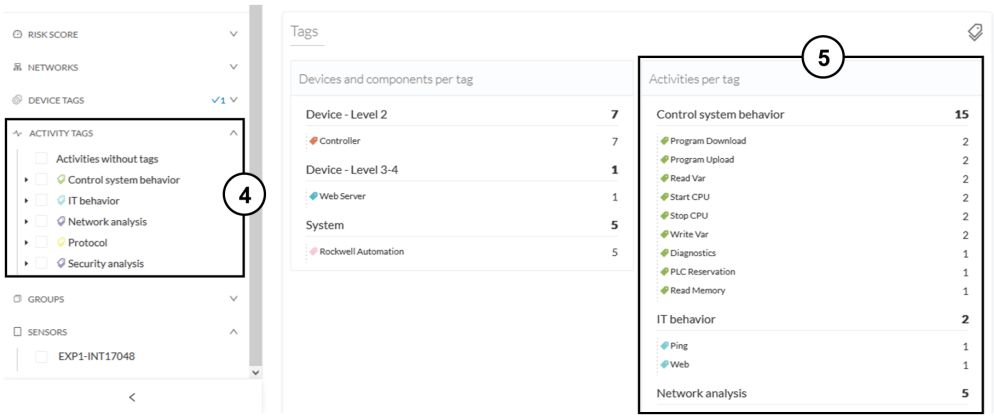
Devices per tag: The number in brackets indicates there are 7 devices tagged as **Controller (1)**. On the **Dashboard**, you see this result **(2)**. One device is tagged as Web Server **(3)**. This means that one of the **Controllers** is a Web Server. Following this logic, we can say that five of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



For more details on these devices, switch to the device list view 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 activity list view 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.

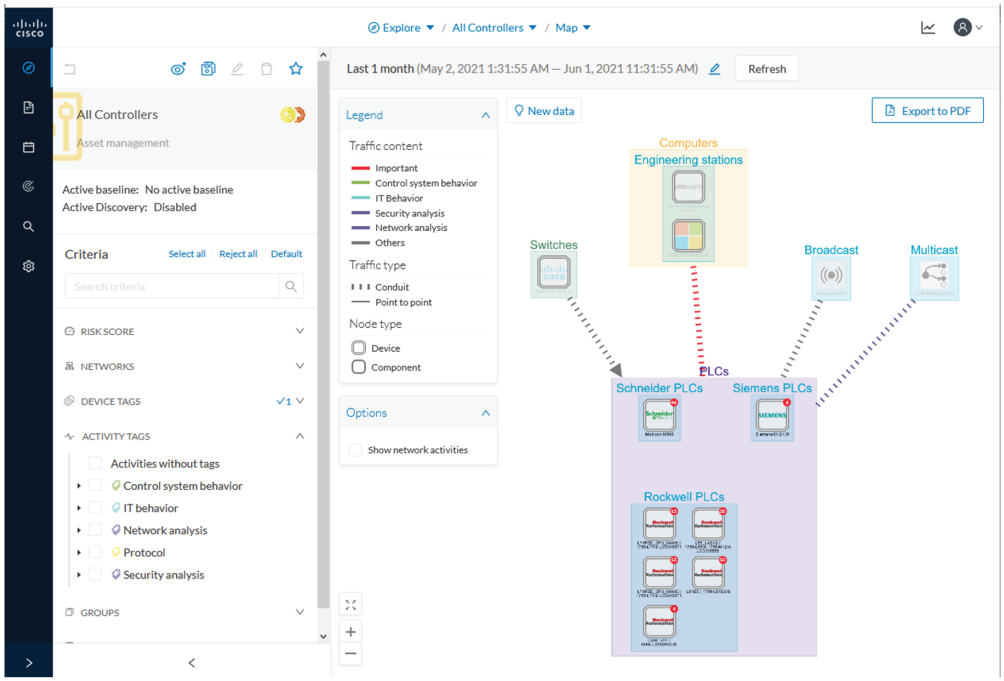
- Use the sort arrows to list data in alphabetical order or by ascending/descending order. Click again to cancel the sort.
- Use the filter icon opens a field to type specific data or a multiple-choice menu to filter tags.

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.

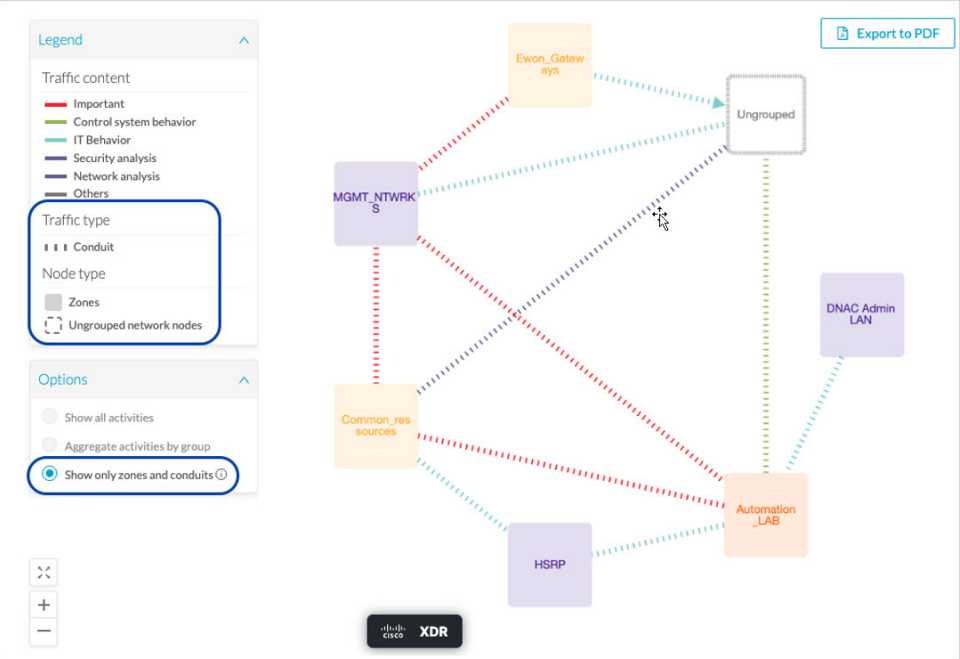
By default, activities between groups are merged and displayed as conduits. Select **Show network activities** for a more detailed view. To enhance visibility, elements here are also automatically reorganized on the **Map** .

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).

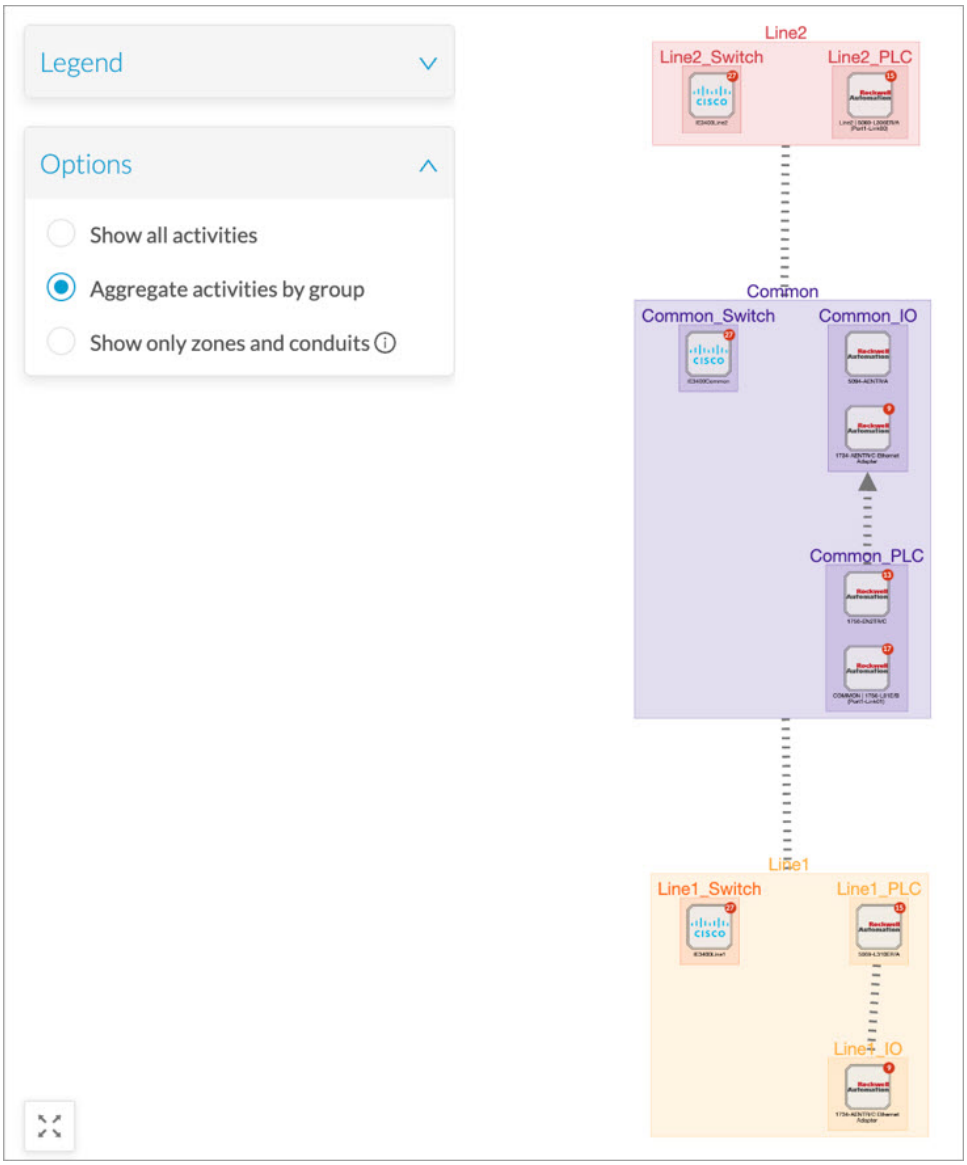
When a group hierarchy segments the control system, the new map option displays zones and conduits according to ISA/IEC 62443 standards.



Conduit

A conduit is the representation of the communications exchanged between two groups. It is an aggregation of activities 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 vulnerabilities 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.

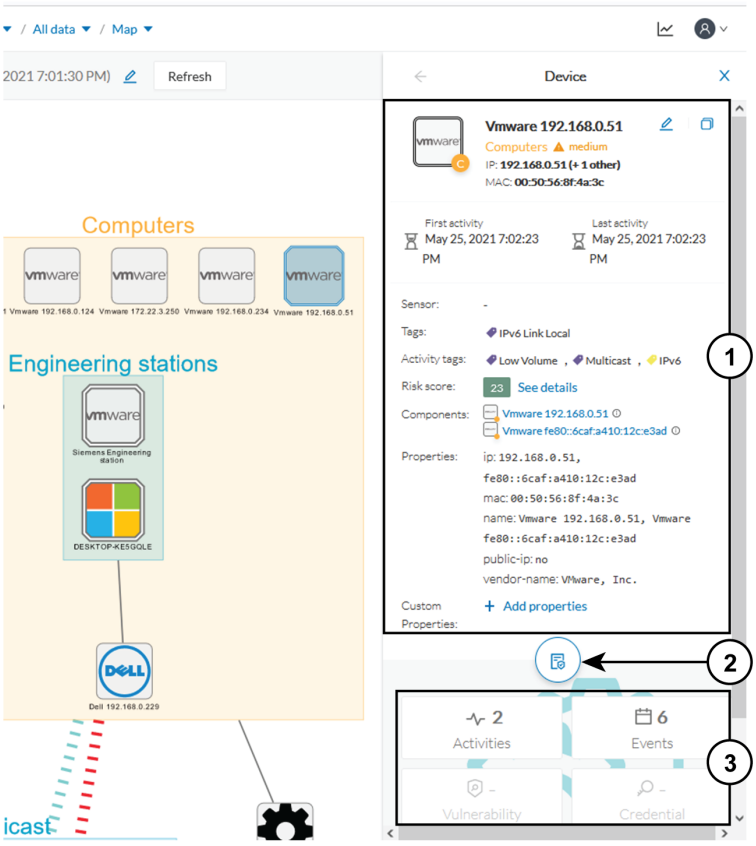
Assets of the preset All Controllers distributed among the layers of the Purdue model

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 sheet 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 communications 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 vulnerabilities.
- More information about credentials.
- More information about flows.
- More information about the Mini Map.
- More information about external communications.
- More information about variables 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

Reports enable you to export industrial network data from traffic captured and processed by Cisco Cyber Vision. You can uncover important information, such as sensitive entry points and acknowledged vulnerabilities for status reports. To access reports, click **Reports** from the main menu.

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

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.

Reports enable you to create reports from a Preset (default data) in Cisco Cyber Vision or a custom one. Reports extensions include .docx and .pdf formats.

Add a logo, such as your company's logo, to customize the report. The report displays Cisco's logo by default. Use the table of contents menu to set which content appears 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 'Reports write' permission can create reports. Users with 'Reports read' permission 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 provides an automated summary of devices, risk profiles, licensing requirements, and inventory distribution within the report's scope.

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 the syslog has been configured 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 List 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

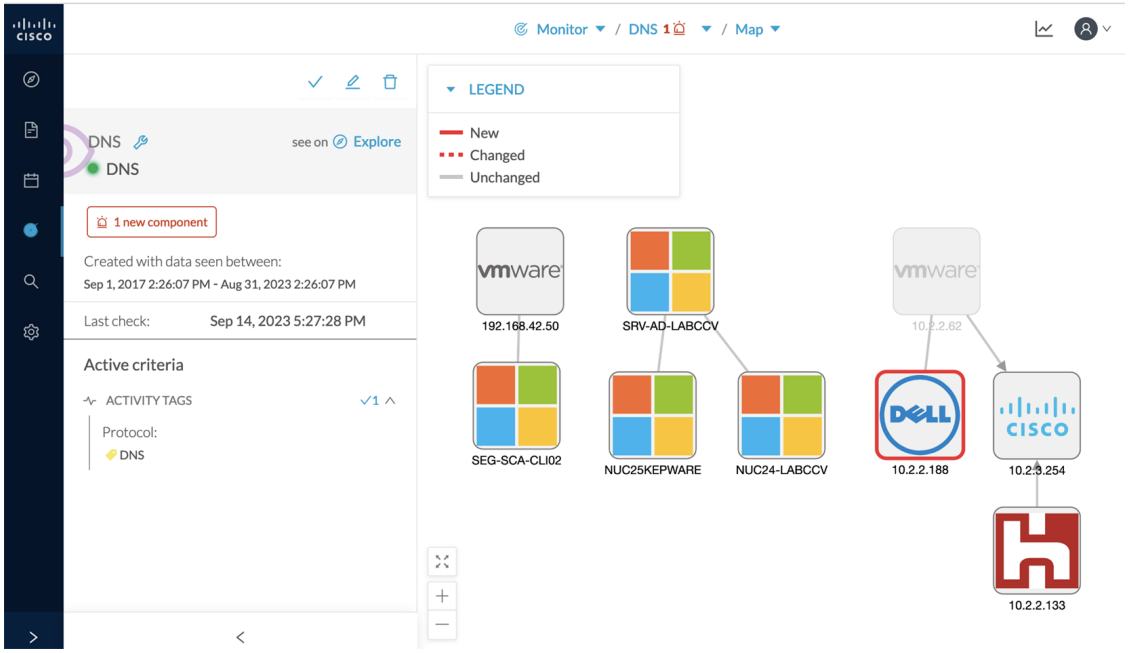
List is a chronological view in which you can see and search events. Use the search bar to find events by MAC and IP addresses, component name, destination and source flow, severity and category. You can search the Events on **Day, Week, Month** or **Year**. Use the arrows for exact dates.

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.

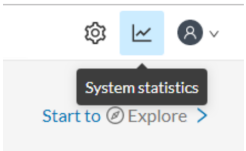
To search, enter the content in the search field and click **Search**.

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 sheet **(2)** icon appears. The technical sheet gives you access to advanced data about the component.

System Statistics

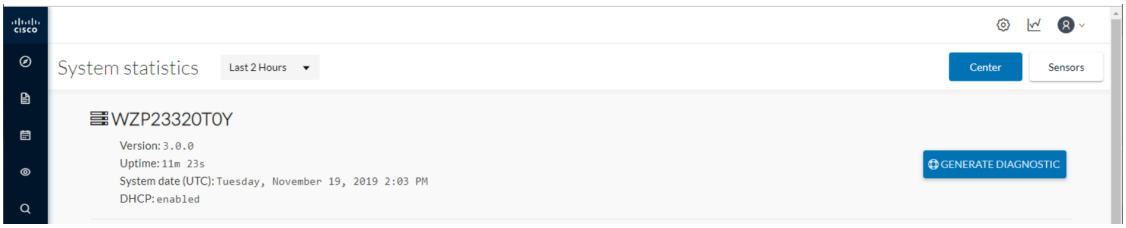
To access system statistics, click the **System statistics** icon in the top right corner of Cisco Cyber Vision interface.



Center

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

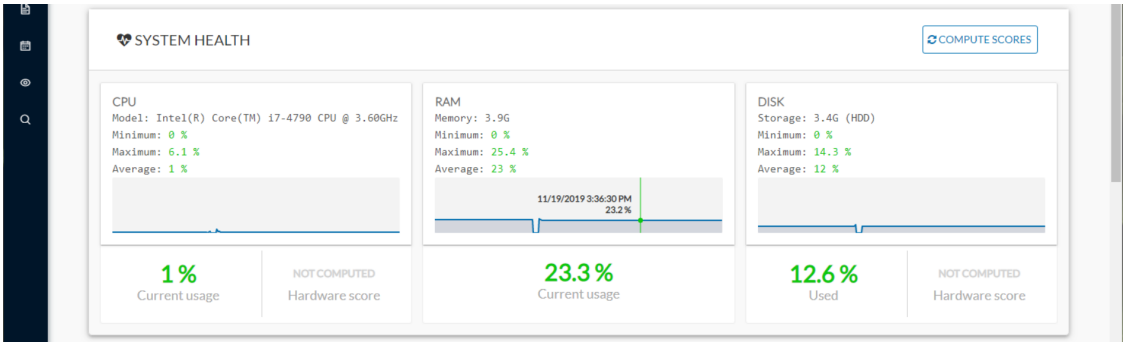
Note Use the drop-down arrow to change the time period.



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



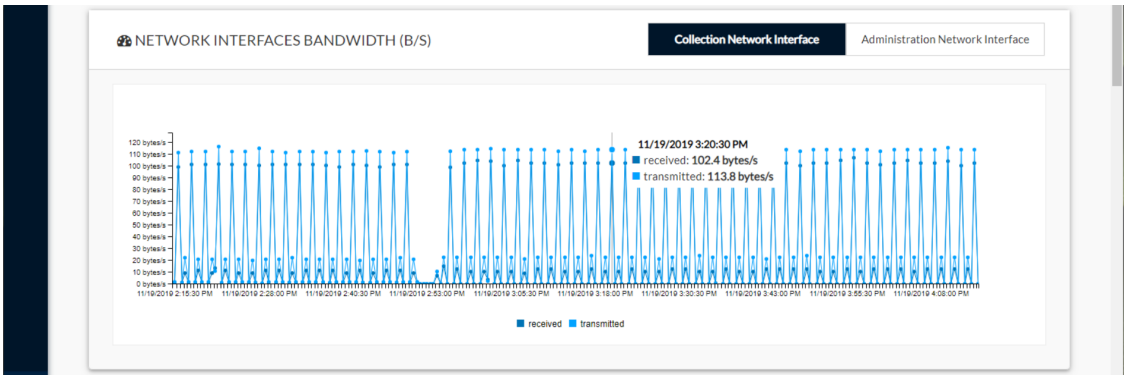
System health shows the status of the Center CPU, RAM and disk usage.

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.

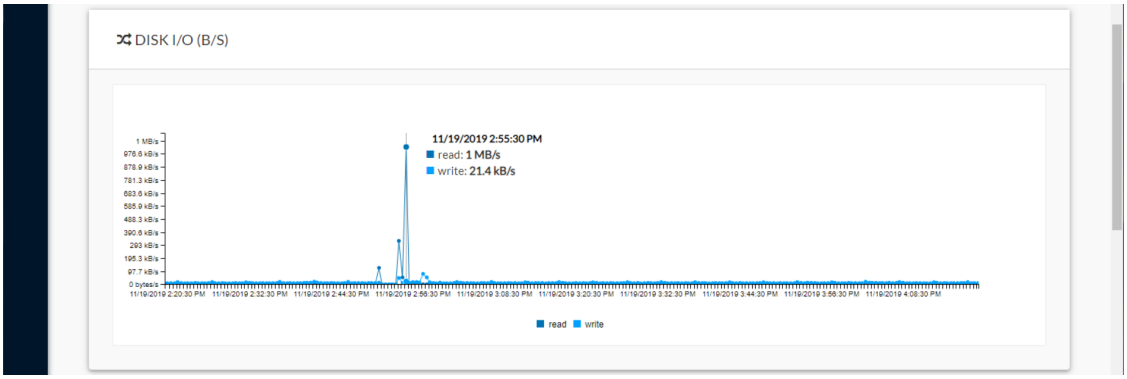
Network Interfaces Bandwidth



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

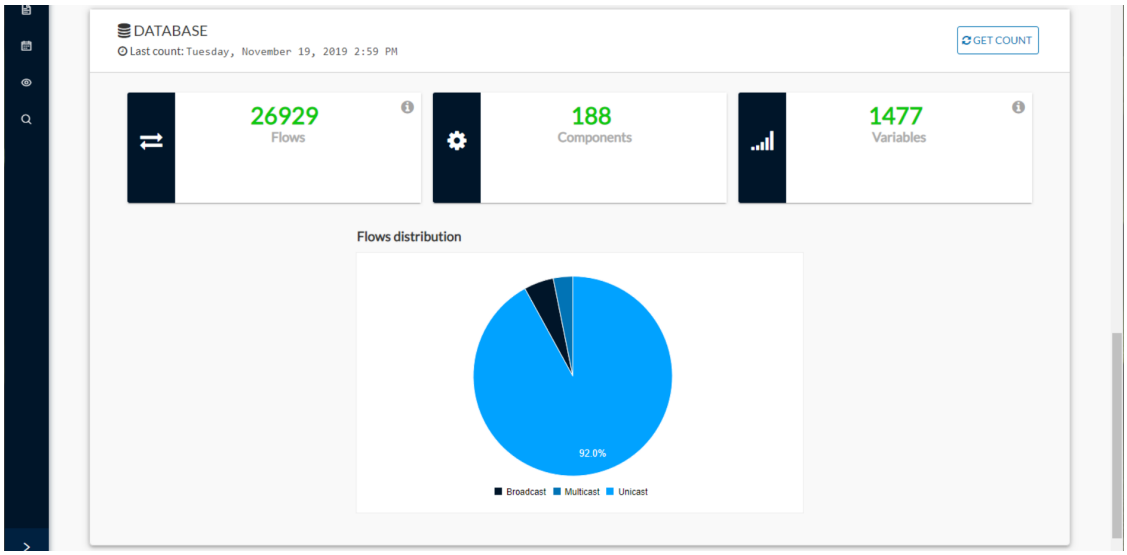
For example, the Collection Network interface activity lets you see the amount of data exchanged between the Center and the sensors.

Disk I/O



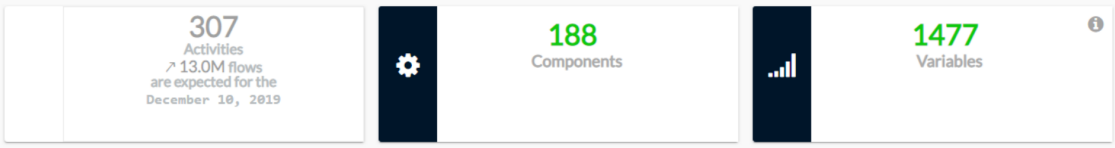
The line chart represents the Center hard disk usage in bytes/second.

Database

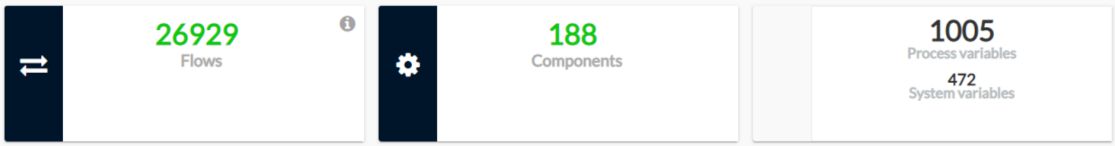


This section describes the database state by showing cards with the number of flows, components and variables that have been detected by Cisco Cyber Vision. Flows distribution is shown in a pie chart.

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.

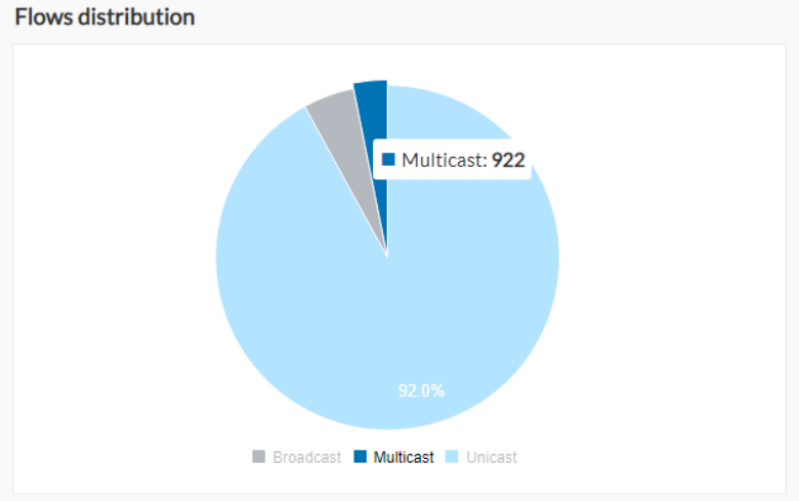


The flows card indicates the total number of flows (i.e. broadcast, multicast and unicast which are stored in the database) detected by . If you mouse over the card, you will get the number of activities and the flows evolution tendency. This information enables you to anticipate how the system load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

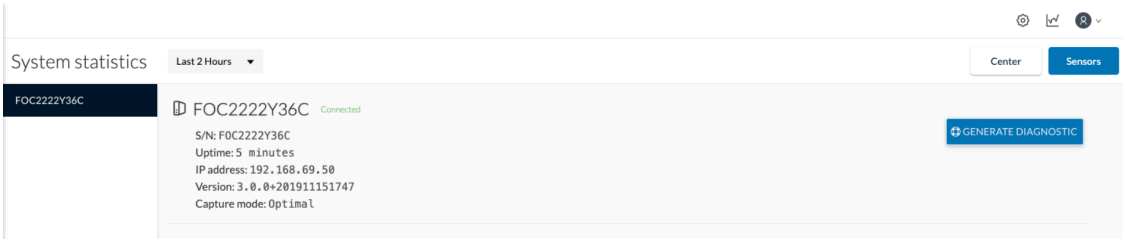
This section shows the status of the queues. If the monitored queues drop messages, this section reports it. Only sensor queues are monitored.

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.



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

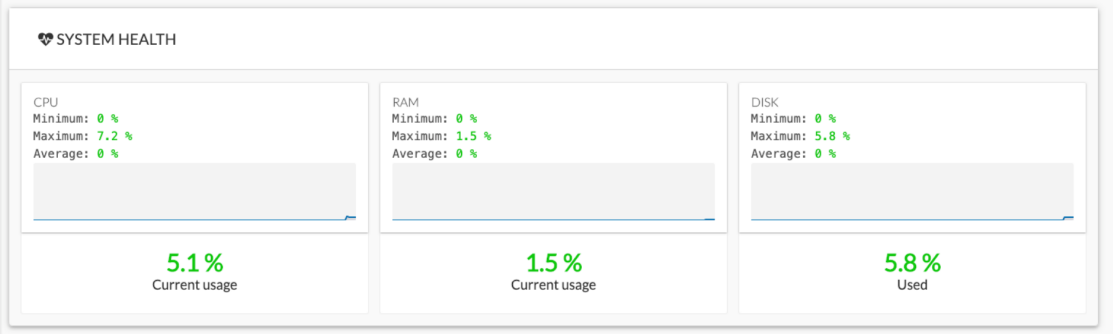
The **Sensors** statistics view shows general information about the sensor: the status (i.e., Connected), serial number, IP and MAC addresses, firmware version, the capture mode set, and the time it has been operating (i.e., uptime).

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.



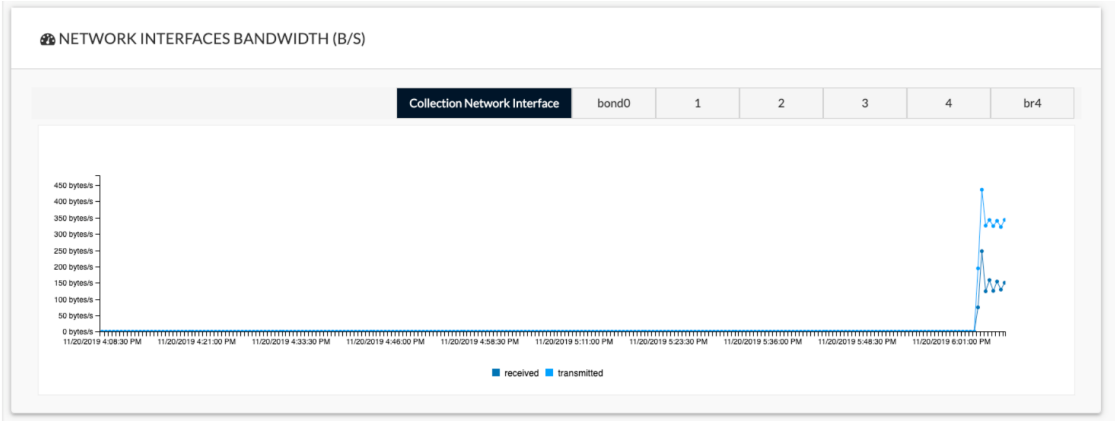
The chart also shows the percentage of the system's Current usage and Hardware score, useful to Cisco Cyber Vision product support.

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:

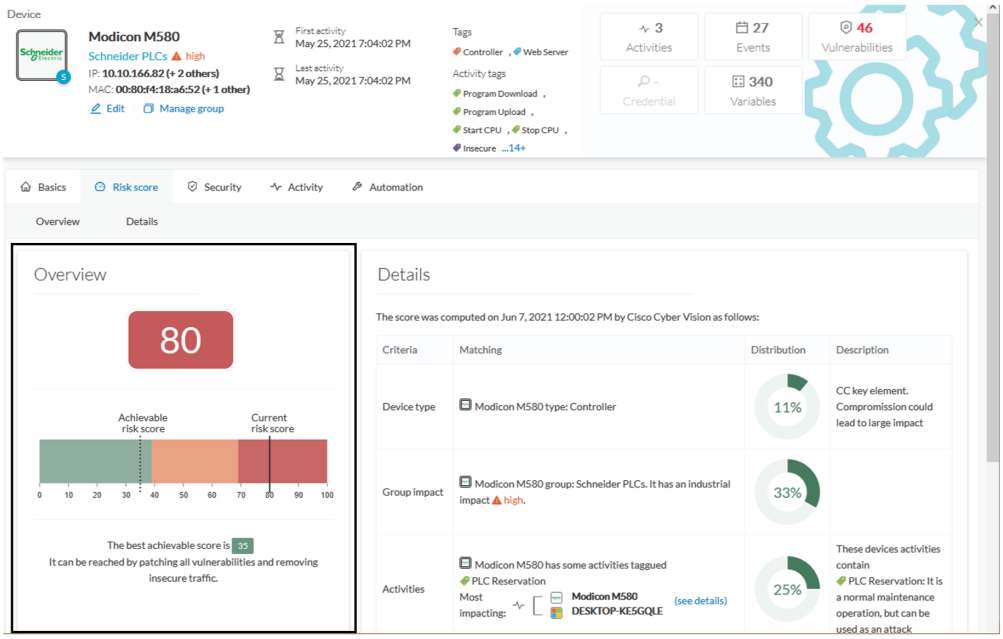
1. From the main menu, choose **Explore**.
2. Click the drop-down arrow in the top navigation bar and select **All Data** under **Basics**.
3. Click the drop-down arrow in the third filter of the top navigation bar and select **Device List**.
4. In the **Risk score** column, click the sort arrow to display 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.

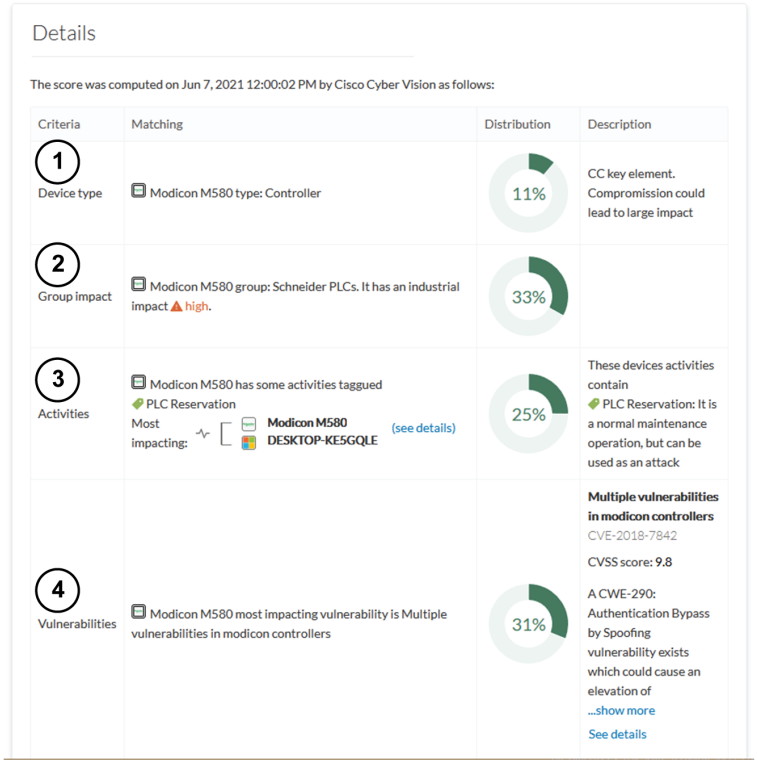
   In the **Overview** tab, the **Current** risk score and the **Achievable** risk are displayed.

   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.



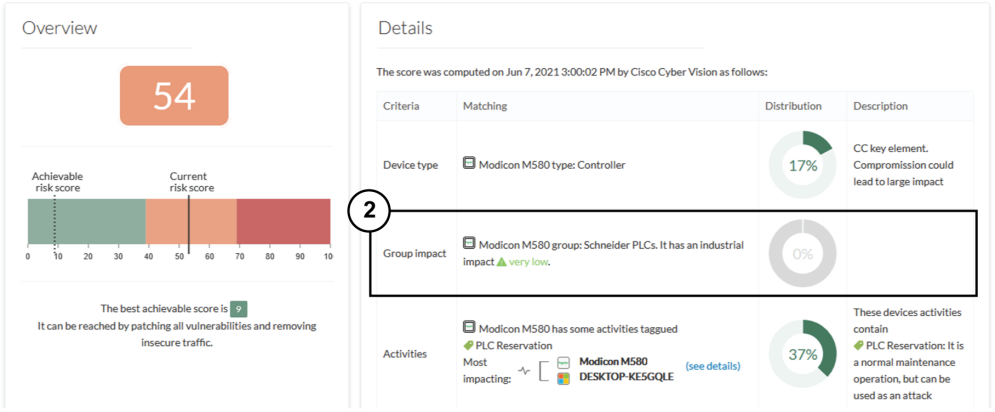
This page shows the last time the risk score was computed by Cisco Cyber Vision. Risk score computation occurs once an hour. To force immediate computation, use the following command on the Center shell prompt:

```
sbs-device-engine
```

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

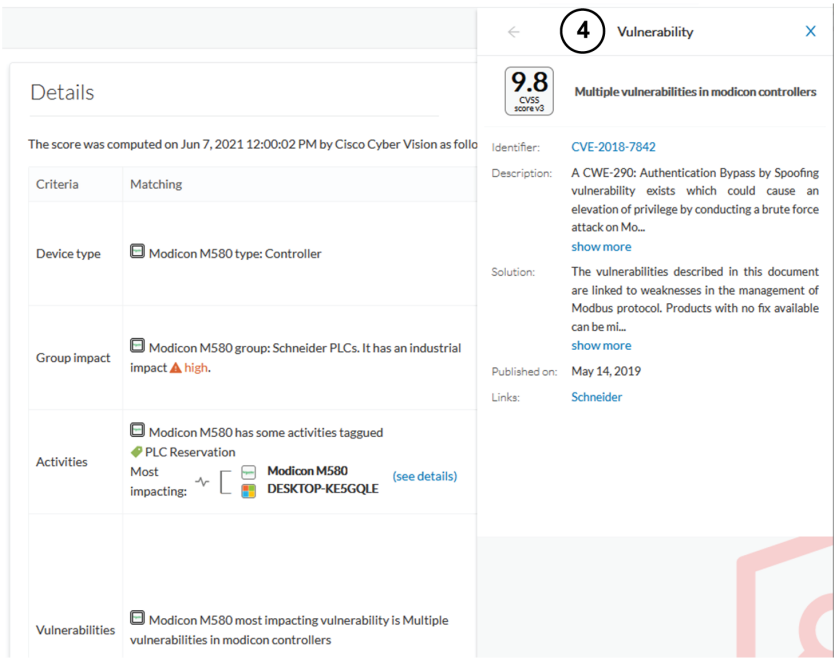
- **Device type**: Each device type corresponds to a device tag detected by Cisco Cyber Vision. No action is required at the device type level because each device tag is assigned a risk score by default.
- **Group impact**: Action is possible if the device belongs to a group. Decrease the impact by lowering 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.

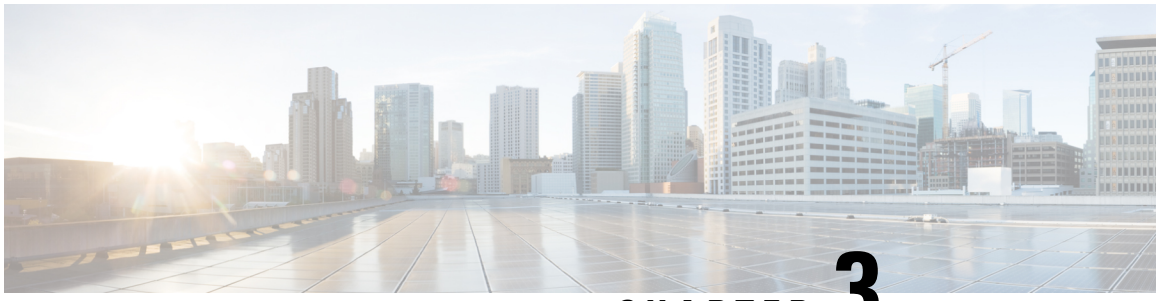


Note The new industrial impact will factor into the next risk score computation (once an hour).

- **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.



CHAPTER 3

Licensing

- Cisco Cyber Vision Licenses, on page 67
- Register Your Essentials or Advantage Licenses, on page 69
- Register Licenses With CSSM On-Prem, on page 71
- Reregister Your Licenses, on page 72
- Deregister Your Licenses, on page 72
- Use Specific License Reservation, on page 72
- Managed Services License Agreement, on page 75
- License Usage Compliance, on page 75

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 69 applies to MSLA licenses as well.

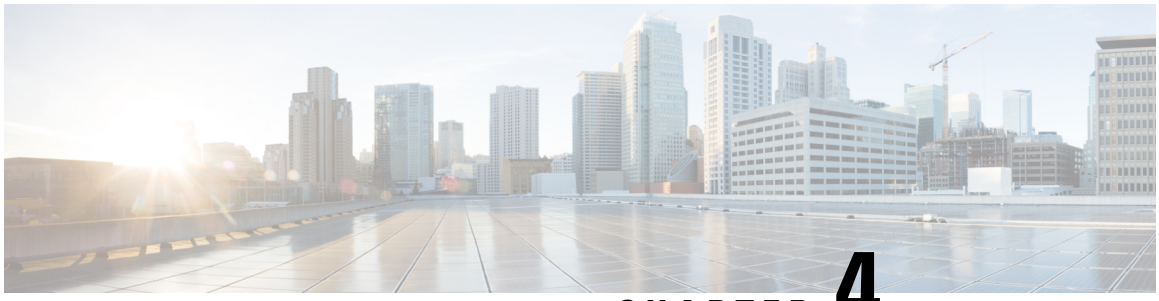
License Usage Compliance

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.



CHAPTER 4

Get Started with Cisco Cyber Vision

- Certificate fingerprint, on page 77
- Data Management, on page 77
- Users, on page 81
- Center Web Server Certificate, on page 84

Certificate fingerprint

A certificate fingerprint is a unique identifier that

- verifies the authenticity of a Center digital certificate in Cyber Vision,
- enables secure enrollment and communication between Global Centers and synchronized Centers, and
- must be updated after certificate renewal to maintain trusted connectivity.

A Center fingerprint can be retrieved in Cyber Vision from **Admin** > **System** in the main menu. Select the copy icon to save the fingerprint. Paste the fingerprint during enrollment or when updating after certificate renewal.

Additional reference information

After renewal (certificates expire every two years), update all enrolled Centers with the new fingerprint. This updates their enrollment status to "Enrolled" and their connectivity status to "Connected".

For more information, see the Centers Installation Guides.

Example

If you renew a certificate for a Global Center, you must copy the new fingerprint from the Global Center and update it in all synchronized Centers to maintain secure communication.

Data Management

The **Data Management** interface allows you to do the following: manage data stored on Cisco Cyber Vision by Data clearance operations to optimize the Center performances, setting data expiration time, and customize traffic ingestion. 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 Data clearance operations 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.

Data clearance operations

A data clearance is a maintenance operation that:

- removes stored information from Cisco Cyber Vision,
- can be performed either partially or completely, and
- affects data such as components, activities, flows, and variables.

Additional reference information

You can clear data in several ways:

- All data
- Components selection
- Activities, Flows, and Variables
- Flows and Variables
- Variables

Clearing data can impact network monitoring. Clear all data only as a last resort, for example, in cases of database overload. This action removes all network data (components, flows, events, baselines) from Cisco Cyber Vision, leaving the GUI empty. Your configurations, including capture modes, event severity, and syslog, remain intact.

Purge components from the database

Remove unnecessary or obsolete components and devices to maintain optimal database performance and prevent data ingestion issues.

The system limits the number of components (network interfaces, PCs, SCADA stations, broadcast or multicast addresses, and so on) in the database for protection.

- If the count exceeds 120,000, a pop-up and red banner alert you to purge.
- When the number of components reaches 150,000, data ingestion stops. The system deletes new sensor data without processing or storing it. A pop-up and red banner alert you to purge.

You provide selection criteria to purge components and devices. The system finds and deletes matching items. Then, the system requests synchronization with the global center.

Before you begin

Ensure you have Admin access to perform this action.

Procedure

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

Step 2 Select **Components selection**.

Step 3 Choose the **Component Type**: IT, OT, or both.

Step 4 Enter the required criteria:

- **IP Subnet** (optional)
- **VLAN** ID (optional; only one ID can be specified at a time)
- **Inactivity since** (optional)
- **Creation Start Time** (optional), and
- **Creation End Time** (optional).

Step 5 Click **Clear data** and confirm when prompted.

The system purges the specified components and related devices. The updated device count appears under **Explore** > **All Data**.

Note When you purge components by VLAN, IP, or date, the system triggers an event. If a Global Center (GC) is enrolled with the Local Center (LC), it also purges the components in the GC after synchronization.

What to do next

Review the device list to ensure the correct components were removed.

Expiration settings

An expiration setting is a configuration option that

- defines how long data and reports are retained in Cisco Cyber Vision Center,
- lets administrators manage system performance and storage by purging old data, and
- provides control over retention periods and the number of report versions kept.

Additional reference information

You can access expiration settings by navigating to **Admin** > **Data Management** > **Expiration Settings** in the Cisco Cyber Vision Center interface.

- The system allows configuration of different retention durations for data types such as events, flows, and variables.
- For reports, you can choose expiration periods such as three months, six months, one year, two years, or three years.
- The number of retained report versions can be set between 1 and 100. Setting 10 versions is recommended for balanced performance and storage use.
- High retention values can consume storage and degrade performance, so set them carefully.

Example

Suppose you set the number of report versions to five and the retention period to six months. Older reports beyond these limits are automatically deleted to free up storage and maintain system efficiency.

Analogy

Expiration settings work like a recycling schedule for your emails—after a set time or once a folder exceeds a certain number, old messages are removed so your inbox doesn't get overwhelmed.

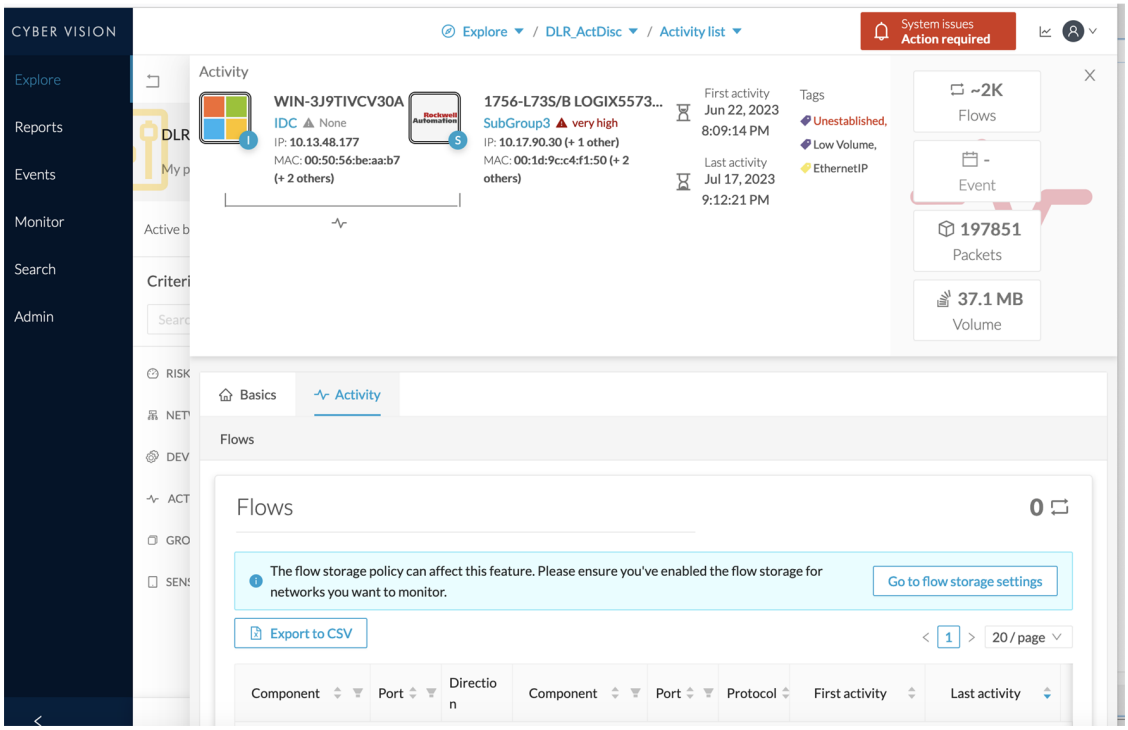
Ingestion configuration

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.

See Enable variable processing in a sensor template to enable **Variable Storage**.

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 page.

You can create custom user roles in the Role Management page.

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 a user role

Define a customized user role to assign specific permissions in Cisco Cyber Vision.

Custom roles allow administrators to tailor access control. You can later map them to Active Directory groups for role-based user management.

Before you begin

Ensure the **Cyber Vision New UI** is enabled for your center.

Procedure

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

Step 2 Click + to add a new role.

Step 3 Enter the **Role Name** and **Role Description**.

Step 4 Select existing permissions by selecting a role from **Search/Add existing permission**, or click **Add New Permissions** to define new permissions.

Step 5 Under **Classic UI Permissions**, select required permissions (**Read** or **Read + Write**).

Note
By default, the **Explore** section has read permission in Classic UI.

Step 6 Under **New UI Permissions**, select required permissions (**Read** or **Read + Write**).

Note
By default, **Assets and Vulnerabilities** and **Vulnerability Acknowledgement** have read permission, and **Dashboard** has both read and write permissions in the New UI.

Step 7 Click **Save**.

The new user role appears in the **Role Management** list.

What to do next

You can modify or delete the role in **Role Management**, or map custom roles to external directory groups in LDAP settings.

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.

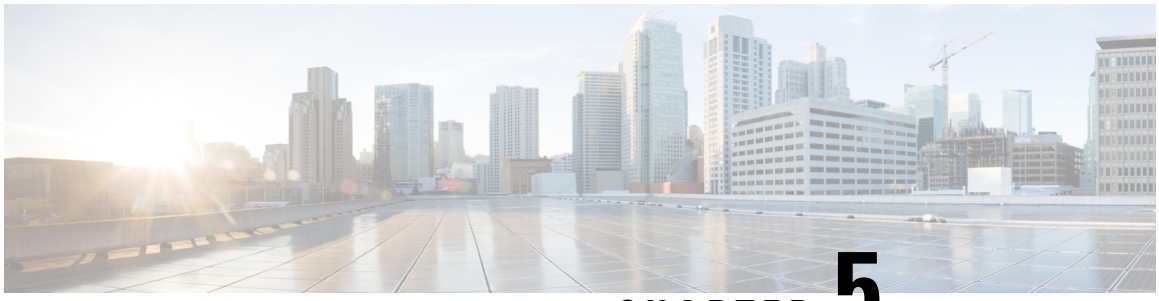
To access **Users security settings**, from the main menu, choose **Admin** > **Users** > **Security settings**.

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, on page 85
- API Token, on page 87
- Active Discovery Policies, on page 91
- LDAP, on page 91
- Single sign-on (SSO), on page 93
- Sensors, on page 104
- SNMP, on page 115

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.

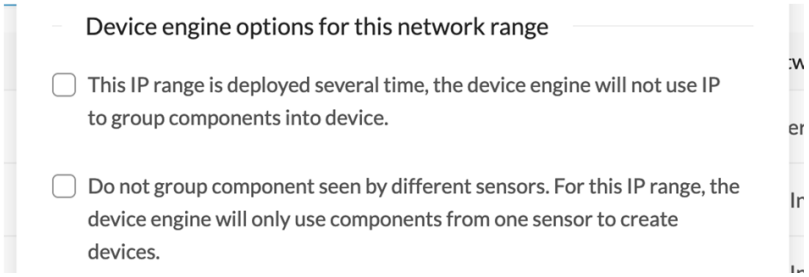
Overall, defining subnetworks in Cisco Cyber Vision is useful for several reasons:

- It allows you to choose afterwards how related flows should be stored through the Ingestion configuration page. Excluding unnecessary flows will have positive impact on performances.
- It will impact devices' risk scores, 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 80 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.

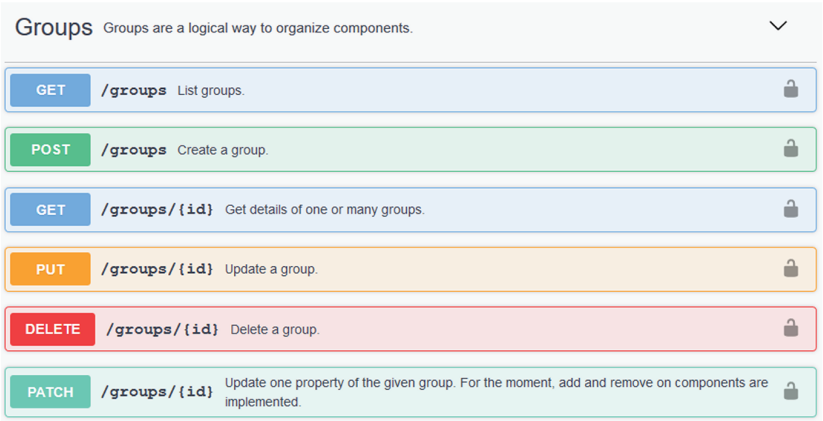
However, for an advanced use, you must create an application that will send requests to the API (refer to the REST API documentation).



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 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**.

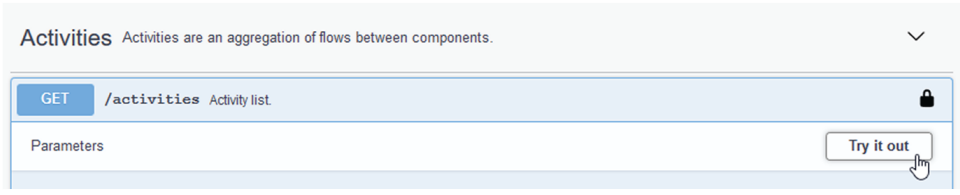
Close lockers displays. They indicate that routes are secured and authorization to use them is up.

To use a route:

Step 8 Click a route to deploy it.

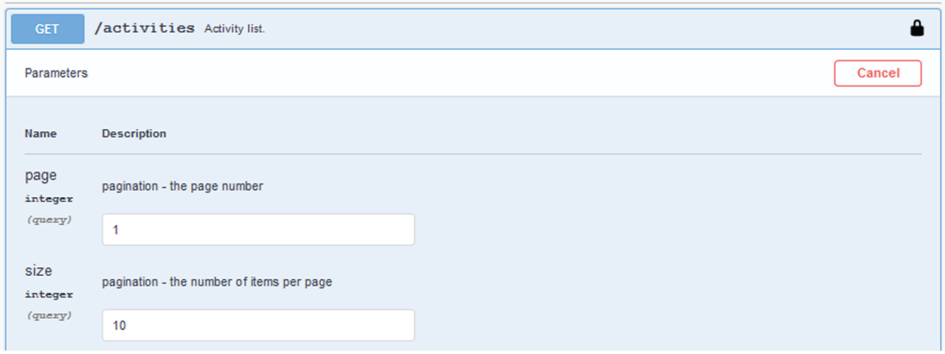
In the example, we choose Get activity list.

Step 9 Click **Try it out**.



Step 10 You can set some **Parameters**.

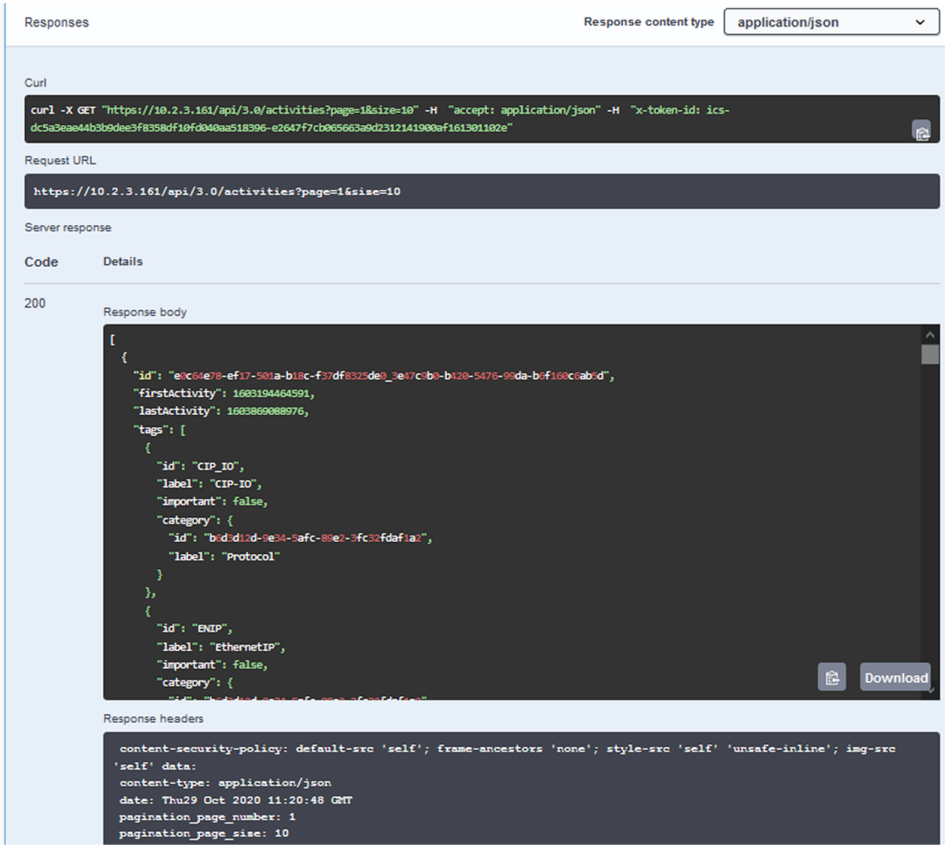
In the example, we set page to 1 and size to 10.



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 Cisco Cyber Vision.

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 that use LDAP (Lightweight Directory Access Protocol), specifically Microsoft Active Directory and AD LDS services.

To configure an LDAP connection, from the main menu, choose **Admin** > **External Authentication** > **LDAP**.

Configuring LDAP:

LDAP integration can be done through an unencrypted connection, or in a secure way by using certificates for encryption, depending on 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 intersnal 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 taskflow takes you through configuring LDAP in Cisco Cyber Vision using an unencrypted connection or a secure connection.

You can establish two types of secure connections:

- For a highly secure connection, choose the **LDAP over TLS/SSL** setting to use a CA-signed certificate with a trust chain. You must upload the certificate into the Center during the configuration task.
- For internal applications where trust is not a primary concern, choose the **Use self signed certificate** setting. The Center automatically generates and uses self-signed certificates for this connection type. You don't need to provide a self-signed certificate.

Procedure

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

Step 2 Click **New Settings**.

Step 3 In the **Settings** tab,

a) Choose **LDAP over TLS/SSL** or **Use self signed certificate**, or neither.
b) Enter **Primary Server Address**.
c) Enter **Primary Server Port**.
d) (Optional) Enter **Secondary Server Address**.
e) (Optional) Enter **Secondary Server Port**.
f) In the **Base DN** field, enter the distinguished name by which LDAP API recognize this LDAP connection.
g) (Optional) Check the **Modify search filter** check box. Then, in the **Search Filter** field, enter a search filter.

   The default search filter retrieves a user's groups by binding with the user's credentials. You can also modify the filter to target a different attribute, and the specified attribute's value is then used for both group search and binding (login).

   In the **Search Filter** field, you must include the *$user* variable. The variable is replaced with the username entered when logging in.

h) In the **Server Response Time** field, enter a timeout value, in seconds, after which the Center attempts to connect to the secondary server instead of the primary server.
i) (Optional) Check the **Use Service Account** check box. When an LDAP user doesn't have access to their own group, a service account is used. When this setting is enabled, the service account is used to search for and retrieve the user's groups.

   1. Enter a service account username.
   2. Enter a service account password.

j) If you chose **LDAP over TLS/SSL** in **Step a**, a certificate upload field is displayed. Upload or drag-and-drop a PEM file, root or chain certificate.

   The uploaded certificate is displayed at the bottom of the settings page.

Step 4 In the **Role Mapping** tab,

a) Map at least one role, default (Product, Operator, or Auditor) or custom, with an Active Directory group. You can create custom roles in the **Custom roles** area.

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

The Admin role is not listed as a default role because it is reserved for Cisco Cyber Vision internal usage and cannot be mapped to external users.

Step 5 Click **OK**.

Step 6 Click **Test connection**.

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

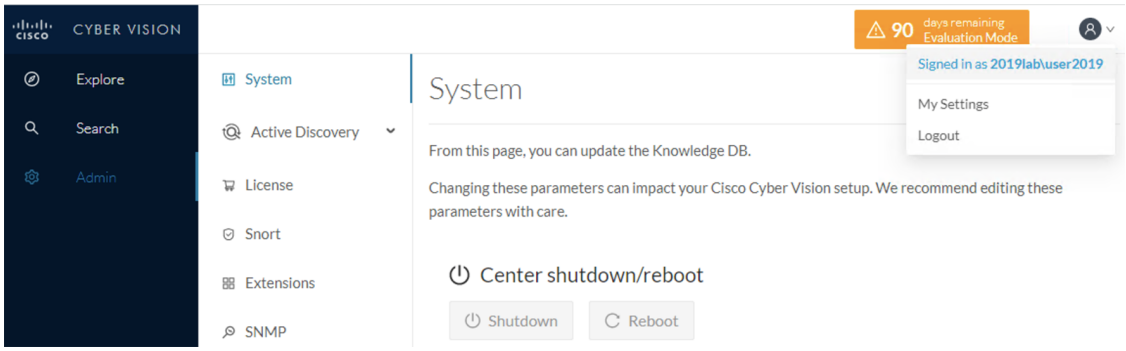
Note
For LDAP, the supported username format is <*domain_name*>\<*user_name*> (For example, cisco\john_doe).

For LDS, the supported username formats are:

- <*user_name*> (For example, john_doe).
- <*email-address*> (For example, john@example.com)

Step 8 Click **OK**.

You can also test the connection by logging out of Cisco Cyber Vision and logging in with different mapped user credentials. The Center menu changes according to the permissions granted to the user.



Single sign-on (SSO)

Single sign-on (SSO) is an authentication mechanism that

- allows users to access multiple applications using a single set of credentials,
- reduces the need for multiple logins and password management, and
- enhances security by centralizing authentication.

Table 4: Feature History Table

Feature	Release Information	Feature Description
SAML 2.0 SSO authentication support	Release 5.3.x	Cisco Cyber Vision Center supports SAML 2.0 SSO authentication.

Central authentication and authorization

This security mechanism uses a central identity provider (IdP) to manage user credentials and access permissions across multiple platforms. It consolidates authentication into a streamlined process.

Federated service provider applications

Applications configured to work with SSO, allowing users to access resources through federated authentication.

Additional reference information

With SSO, a user logs in once to access all authorized service provider applications without re-entering credentials, resulting in improved user experience and streamlined access control.

SAML single sign-on

SAML single sign-on is an authentication approach that:

- enables users to authenticate once and gain access to multiple applications through a central identity provider,
- uses Security Assertion Markup Language (SAML) 2.0 to securely exchange authentication and authorization data, and
- eliminates the need for repeated login credentials for each service.

After successful authentication by the identity provider (IdP), users are redirected back to their service. The browser manages all communication between the service and the IdP. As a result, services such as Cisco Cyber Vision Center do not require a direct network connection to the IdP.

Examples

The Cisco Cyber Vision Center supports SAML single sign-on with any single sign-on provider that uses the SAML 2.0 standard, for example, Azure Active Directory and Cisco Duo.

Reference links

- For Azure setup: See Azure AD single sign-on integrations.
- For Cisco Duo setup: See Duo Single Sign-On solutions.

Requirement: SSO configuration for Cisco Cyber Vision Center

Ensure that you meet these requirements when configuring SSO for Cisco Cyber Vision Center:

- Only admin users authenticated internally can configure SSO.

- Use only one SSO provider at a time (for example, Azure or Duo).
- Initiate SSO only from the Cisco Cyber Vision Center, not from the identity provider (IdP).
- Review audit logs to monitor login and log out events for SSO. The Cyber Vision Center records and sends these events through syslog.
- Ensure that the Cyber Vision Center host name (FQDN) is DNS resolvable.
- A center can only be configured with SSO if LDAP is disabled or not configured.

Single sign-on user accounts

A single sign-on user account is a user identity credential that

- allows access to multiple applications, systems, or services with a single set of login credentials,
- uses a central identity provider (IdP) to handle authentication, and
- simplifies the user experience by removing the need for separate logins for each system.

Role of the Identity Provider (IdP)

The identity provider (IdP) manages users and groups directly or imports them from external directories such as Active Directory, RADIUS, or LDAP. The IdP sets most account details for SSO users, including usernames and passwords.

Single sign-on (SSO) accounts on Cisco Cyber Vision Center

A single sign-on account appears on the Cisco Cyber Vision Center users page only after the user has logged in successfully for the first time.

Email address requirement

Both single sign-on accounts and the NameID attribute provided by the IdP during SAML login require valid email addresses. By default, many IdPs use the user's username as the NameID attribute. Confirm your IdP's behavior when configuring it and when creating user accounts for SSO access to Cyber Vision Center.

User role mappings for SSO users

Role mappings for SSO users are configuration mappings that:

- associate user groups from an identity provider (IdP) with roles in the Cyber Vision Center,
- use role attributes to determine user permissions dynamically, and
- enable centralized management of user access through SSO integration.

Coordination with the IdP

- Role assignment: Set up user roles at the Cyber Vision Center and coordinate them with your SSO IdP application settings. Assign roles to groups defined in the IdP.

- SSO federation understanding: Review how users, groups, and roles are organized in your IdP and configure user role mapping effectively. Consult the IdP vendor documentation for guidance on creating or importing users or groups.

Role attribute

- Role attribute at the IdP: The IdP sends a role attribute, which lists the groups a user belongs to in the IdP.
- SSO configuration details: The SSO configuration specifies the name of the role attribute and includes a list of expressions mapped to Cyber Vision Center user roles.

Email address attribute usage for SSO migration

Provide the email address attribute only if you need to migrate local users to SSO. When you configure SSO with the email address attribute, the system identifies the logged-in user's email address from the SAML assertion. If a user exists with that email address, the system removes that user from local authentication. Afterward, the user can only log in with SSO. If needed, create a new internal user.

Azure AD single sign-on integrations

Azure AD single sign-on integrations are authentication solutions that:

- use Microsoft's multi-tenant, cloud-based Azure Active Directory to manage user identities,
- enable secure and centralized access to cloud and on-premises applications (such as Cyber Vision Center), and
- allow users to authenticate with a single account across multiple services through federation.

Within Azure, a tenant is an entity that manages federated devices. A user can access these devices with their SSO account. Familiarize yourself with the Azure tenant organization before onboarding applications such as Cyber Vision Center.

Add an enterprise application in Azure

Add an enterprise application to your Azure tenant.

Before you begin

- You need an Azure account with an active subscription. Create a free account at Build in the cloud with an Azure account.
- Your account must have the "Application Developer" role or higher.

Procedure

Step 1 Sign in to the https://entra.microsoft.com/#home.

Step 2 From the main page, choose **Applications** > **Enterprise applications** > **All applications**.

Step 3 Select **New application** and click **Create your own application**.

Step 4 Enter an application name.

Step 5 Enable **Integrate any other application you don't find in the gallery (Non-gallery)**.

Step 6 Click **Create**.

Step 7 Enter the display name and select **Supported account types**.

Step 8 Click **Register**.

The application is created and appears in **Home** > **Enterprise applications** > **All applications**.

What to do next

To configure the new application, go to **Home** > **Enterprise applications** > **All applications** and open it. For further details, see Configure Azure SSO for Cyber Vision Center.

Configure Azure SSO for Cyber Vision Center

Enable authentication of Cyber Vision Center users through Azure Active Directory Single Sign-On (SSO).

Use this task to centralize user authentication and streamline role management by integrating Azure SSO with Cyber Vision Center.

Before you begin

- Create the Cyber Vision Center service provider application in Azure. See Add an enterprise application in Azure.
- Prepare your Azure tenant.
- Ensure the Cyber Vision Center hostname is a resolvable DNS entry.
- Verify that usernames and NameID attributes are valid email addresses.
- You can provide multiple groups. Roles are assigned to the user based on priority.

Note If the Cyber Vision Center has multiple accessible URLs, SSO users must always use the configured login URL.

Procedure

Step 1 Sign in to Microsoft Entra at https://entra.microsoft.com/#home.

Step 2 From the main menu, choose **Applications** > **Enterprise applications** > **All applications**.

Step 3 Select the created application.

Step 4 Click on **Single sign-on** and select **SAML**.

Step 5 Edit the **Basic SAML Configuration** section and enter:

- **Identifier (Entity ID)**: Append /saml/metadata to the Cyber Vision Center login URL.

  Format: https://{Hostname}/saml/metadata

- **Reply URL (Assertion Consumer Service URL)**: Append /saml/acs to the login URL.

  Format: https://{Hostname}/saml/acs

Step 6 Edit **Attributes & Claims**:

a. Click **Add a group claim**.

b. Select the **All groups** field to show the groups associated with the user in the **Group Claims** panel.

c. Select **Group ID** as a **Source attribute**.

d. Check the checkbox of **Customize the name of the group claim** under the **Advanced option**s.

e. Enter **Name (required)** and save.

Step 7 Assign existing Azure users and groups to the Cyber Vision Center service application.

Step 8 Record the these details from **SAML-Based Sign-On**:

- **Login URL**
- **Microsoft Entra Identifier**
- **Certificate (Base64)** file (download it)
- **Federation Metadata XML** (download it)
- **Object ID** (Group ID)

Cyber Vision Center is configured to support Azure SSO, allowing users to sign in using their Azure Active Directory credentials.

What to do next

Configure Cyber Vision Center to complete Azure SSO integration. For details, see Configure Cyber Vision Center for Azure SSO.

Configure Cyber Vision Center for Azure SSO

Enable Azure Single Sign-On (SSO) authentication for users accessing Cyber Vision Center.

Follow these steps to configure the Cyber Vision Center for Azure SSO:

Before you begin

- Use the SAML SSO management application to configure a service provider application for the Cyber Vision Center and assign users or groups to it. See Configure Azure SSO for Cyber Vision Center.
- Have the following Azure configuration details from Configure Azure SSO for Cyber Vision Center.
  - **Name (Required)**
  - **Federation Metadata XML**
  - **Login URL**

- **Microsoft Entra Identifier**
- **Certificate (Base64)**
- **Object ID** (Group ID)

Procedure

Step 1 From the main menu, choose **Admin** > **External Authentication** > **Single Sign-On**.

Step 2 Click **New Settings**.

Step 3 Add **Role Attribute** and **Email Attribute** (Optional).

For **Role Attribute**, enter **Name (Required)** used for the group claim.

Step 4 Configure Azure SSO credentials using one of these methods:

a. Upload the **Federation Metadata XML** file under the **Upload XML file** field.

b. For **Manual Configuration**:

- Enter the **Login URL** in the **Identity Provider Single Sign-On (SSO) URL** field.
- Enter the **Microsoft Entra Identifier** in the **Identity Provider (Idp) Issuer URL** field.
- Add the **Certificate (Base64)** in the **X509** field.

Step 5 Click **Role Mapping**.

Step 6 Enter the **Object ID** (Group ID) in the **Default roles** or **Customer roles** field.

Step 7 Click **OK**.

The **Login with SSO** button appears on the Cyber Vision Center login screen.

What to do next

Click **Login with SSO** to access the Cyber Vision Center using Azure SSO authentication.

Duo Single Sign-On solutions

A Duo single sign-on (SSO) is a cloud-hosted identity provider that

- facilitates inline user enrollment,
- offers self-service device management, and
- supports various authentication methods, including passkeys and security keys, Duo Push, or Verified Duo Push in the Universal Prompt.

You add two-factor authentication and flexible security policies to any SAML application with Duo Single Sign-On.

Duo Single Sign-On (SSO)

Cyber Vision Center uses Duo's strong authentication and flexible policy engine in the applications that comply with Security Assertion Markup Language (SAML) 2.0 or OpenID Connect (OIDC) authentication standards. Duo Single Sign-On serves as an identity provider (IdP). It authenticates users through existing on-premises Active Directory or any SAML 2.0 identity provider, and requires two-factor authentication before granting access to the service provider's application.

Plans and policy control

Duo Single Sign-On offers various plans for different needs:

- Duo Premier: Includes advanced features and support.
- Duo Advantage: Builds on the Basic plan with additional features.
- Duo Essentials: Provides essential security features.

Administrators can define application policies based on their plan. For example, some applications may enforce two-factor authentication at each login, while others limit login to once every seven days. Duo evaluates the user, device, and network against the application policy to determine access.

Requirement: Prerequisites for Duo Single Sign-On setup

To set up Duo Single Sign-On (SSO), ensure you meet these requirements:

- Obtain Duo Admin access with one of the following roles:
  - Owner
  - Administrator
  - Application Manager
- Configure a primary authentication source by setting up either:
  - An Active Directory connection, or
  - A Security Assertion Markup Language (SAML) 2.0 identity provider
- Complete all authentication source setup steps for Duo Single Sign-On (SSO) separately from any directory sync setup.
- If you use Active Directory as your authentication source:
  - Provide at least one standalone server (Windows or Linux) that can communicate with your Active Directory domain controllers.
  - Supply service account credentials for Active Directory.
  - Ensure access to DNS for the user email domains associated with SSO so you can add TXT records as required.
- Provide a SAML 2.0 service provider or OpenID Connect (OIDC) relying party web application to protect with Duo SSO.
- Verify the fully qualified domain name (FQDN) of the Cyber Vision Center is reachable.

Configure Cyber Vision Center application in Duo

Integrate the Cyber Vision Center application with Duo for user authentication using SAML Single Sign-On.

Use this procedure to configure Duo as a SAML identity provider for the Cyber Vision Center application.

Before you begin

- Ensure you have users and groups configured in Duo.
- Verify that Duo users have an authentication source and a proxy. For details, see https://duo.com/docs/sso#external-authentication-sources.

Procedure

Step 1 Log in to the Duo Admin Panel.

Step 2 From the main menu, choose **Applications** > **Application Catalog**.

Step 3 Locate the **Generic SAML Service Provider** labeled "SSO". Click **+ Add**.

Use the **Documentation** link to review integration requirements and steps before adding the new application.

Step 4 Enter **Application name**.

Step 5 Select **User access** option.

Note
Users cannot access new applications until user access is granted.

Step 6 Enter these details under **Service Provider**:

- **Entity ID**:
  - Use the "/saml/metadata" with the Cyber Vision Center login URL.
  - Format: https://{Hostname}/saml/metadata
- **Assertion Consumer Service (ACS) URL**:
  - Use the path "/saml/acs" with the login URL.
  - Format: https://{Hostname}/saml/acs

The Metadata section presents SAML identity provider details for Duo Single Sign-On in the table.

Name	Description
Entity ID	The global, unique name for Duo Single Sign-On. Sometimes referred to as "Issuer."
Single Sign-On URL	The authentication URL for Duo Single Sign-On. This is sometimes referred to as "SSO URL" or "Login URL". The URL is used to start IdP-initiated authentications.

Name	Description
Single Log-Out URL	This optional field specifies the logout URL for Duo Single Sign-On, sometimes referred to as the “SLO URL” or “Logout Endpoint. This field is optional.
Metadata URL	This URL can be used by service providers to download the XML metadata from Duo Single Sign-On.
SHA - 1 Fingerprint	The SHA-1 fingerprint of the SAML certificate. Sometimes service providers will request a fingerprint instead of uploading a SAML certificate.
SHA - 256 Fingerprint	The SHA-256 fingerprint of the SAML certificate. Service providers may request a fingerprint instead of a SAML certificate.
Certificate	The certificate used by the service providers to validate the signature on the SAML response sent by Duo Single Sign-On. Click **Copy certificate**.
SAML Metadata	Service providers use the XML SAML Metadata from Duo Single Sign-On to configure settings. Click the **Download XML** to download the xml file.

Step 7 In **Map attributes**:

a. Select **Email Address** in the **IdP Attribute** field.

b. Enter an attribute name in the **SAML Response Attribute** field. For example, "email".

Note
Configuring the Email attribute is optional.

Step 8 In **Role attribute**,

a. Add an **Attribute name**, for example "GroupName".

b. Map **Service Provider's Role** with **Duo groups**.

Step 9 Click **Save**.

The Cyber Vision Center application is integrated with Duo and ready to use SAML for authentication.

What to do next

Configure the Cisco Cyber Vision Center for Duo. See Configure Cisco Cyber Vision Center for Duo.

Configure Cisco Cyber Vision Center for Duo

Enable SSO login on Cisco Cyber Vision Center using Duo as an identity provider.

Use these steps to centrally configure SSO authentication after preparing Duo configuration details.

Before you begin

Obtain these Duo SSO details from Configure Cyber Vision Center application in Duo.

- **Attribute name**
- **SAML Response Attribute**
- **SAML Metadata** xml file
- **Single Sign-On URL**
- **Entity ID**
- **Certificate**
- **Service Provider's Role**

Procedure

Step 1 From the main menu, choose **Admin** > **External Authentication** > **Single Sign-On**.

Step 2 Click **New Settings**.

Step 3 Enter **Attribute name** in the **Role Attribute** field.

Step 4 Enter **SAML Response Attribute** in the **Email Attribute** field.

Note
Configuring the Email attribute is optional.

Step 5 Complete the configuration using one of these methods:

a. Upload the **SAML Metadata** XML file under the **Upload XML file** field.

b. For **Manual Configuration**:

- Enter the **Single Sign-On URL** in the **Identity Provider Single Sign-On (SSO) URL** field.
- Enter the **Entity ID** in the **Identity Provider (Idp) Issuer URL** field.
- Add the **Certificate** in the **X509** field.

Step 6 Select the **Role Mapping** tab.

Step 7 Enter **Service Provider's Role** details in the **Default roles** or **Custom roles** field.

Step 8 Click **OK**.

After you complete the configuration, the **Login with SSO** button appears on the Cyber Vision Center login screen.

What to do next

Use the **Login with SSO** button to test SSO login via Duo.

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 108.
- 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 Setting 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 installation method (for example, without the extension) and provides the necessary foundation for sensor self-updates. However, the self-update feature will only be functional in future releases. 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 allows you to select 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 right 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 on 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**: The sensor analyzes all incoming flows without applying a filter. It stores all flows in the Center database.
- **OPTIMAL (Default)**: The filter selects the most relevant flows based on Cisco Cyber Vision expertise. It does not record multicast flows. Use this capture mode for long-term capture and monitoring.
- **INDUSTRIAL ONLY**: The filter selects only industrial protocols like Modbus, S7, and EtherNet/IP. This means that the sensor does not analyze IT flows of the monitored network, and they do not appear in the GUI.
- **CUSTOM (advanced users)**: Use this capture mode to fully customize the filter. 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 5: 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.

Enable or disable a protocol DPI engine to choose which protocols to analyze.

Disable a protocol DPI engine to avoid false positives in Cisco Cyber Vision. This occurs when a protocol appears on the user interface but is not present because the same UDP/TCP ports can be used by other non-standardized protocols.

The Default template disables some protocols because they are not commonly used or are specific to fields like transportation. The Default template applies to all compatible sensors.

Although UDP/TCP port configurations are mostly standardized, conflicts still occur with field-specific or with limited usage. Map UDP/TCP port numbers to ensure packets are sent to the correct DPI engine for accurate analysis and representation in the user interface.

Sending the protocol's packet to the wrong port results in related information appearing in Security Insights/Flows without a tag.

A sensor associates with only one template. Template deployment fails

- if the sensor is disconnected,
- if there is connection issues, or
- 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.

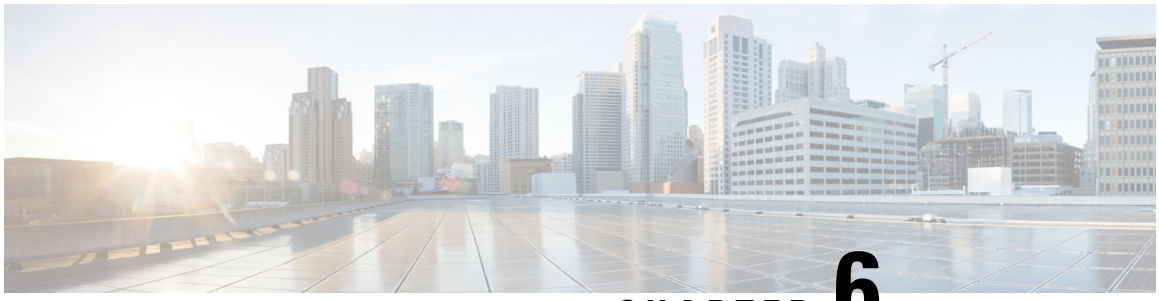
a) If SNMP v3 has been selected, the Engine ID field (i.e. the Center id) is displayed so you can customize it.
b) Select and set the CPU and memory rate limit and threshold according to your needs.

Step 7 Click **Save Configuration**.

SNMP MIB

Table 6:

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



CHAPTER 6

Integrate with Cisco Cyber Vision

- pxGrid, on page 119
- XDR, on page 119
- Secure Equipment Access, on page 123
- Cisco In Product Support, on page 127

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.

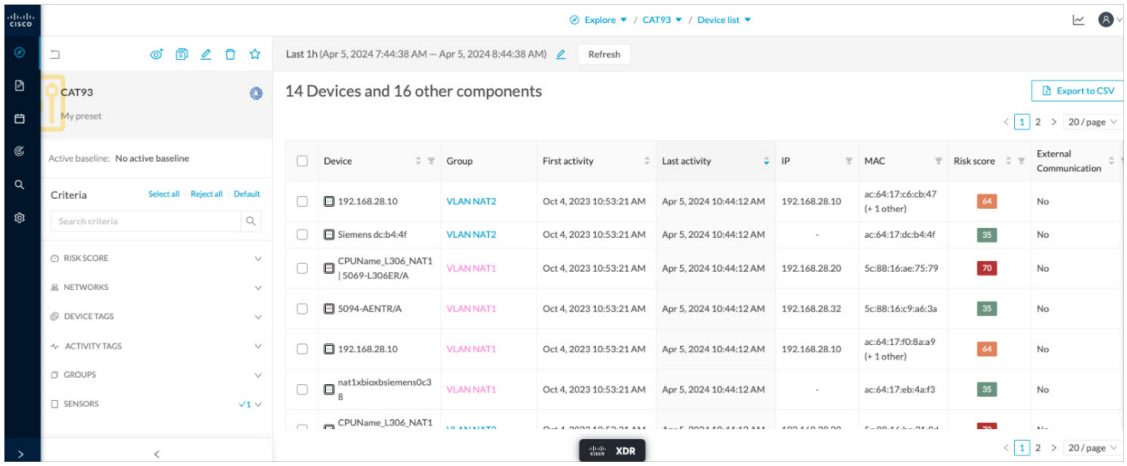
Step 13 To log out, click **Logout of XDR**.

Step 14 Click **Save settings**.

XDR Ribbon

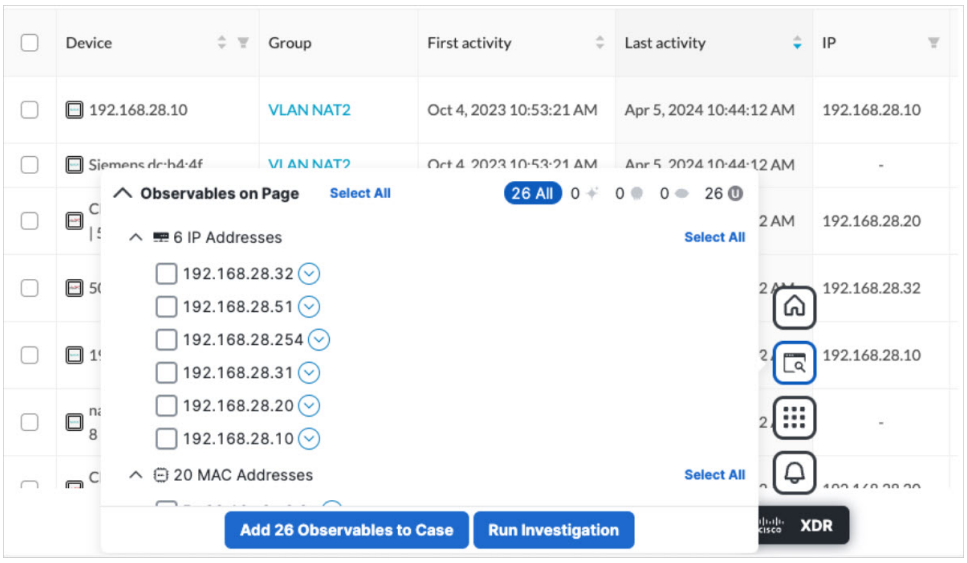
Once configured and activated, the XDR ribbon will appear at the bottom of the Cisco Cyber Vision GUI of the Explore menu.

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:



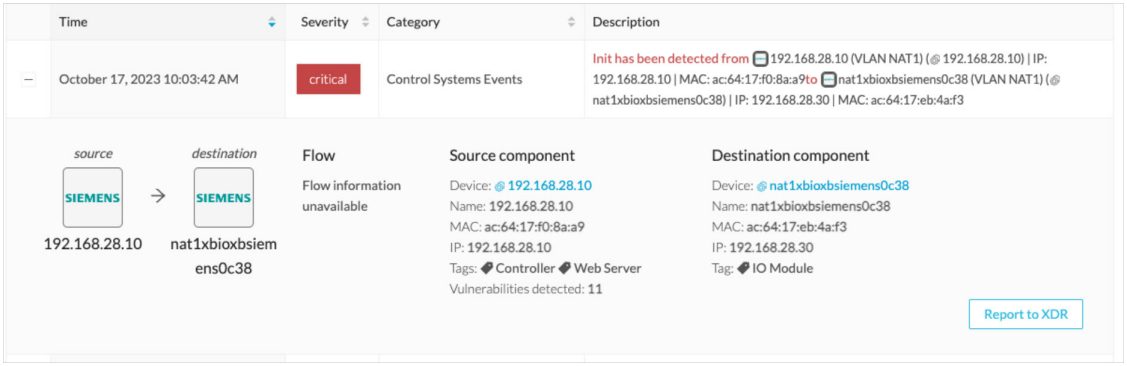
XDR Event Integration

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:

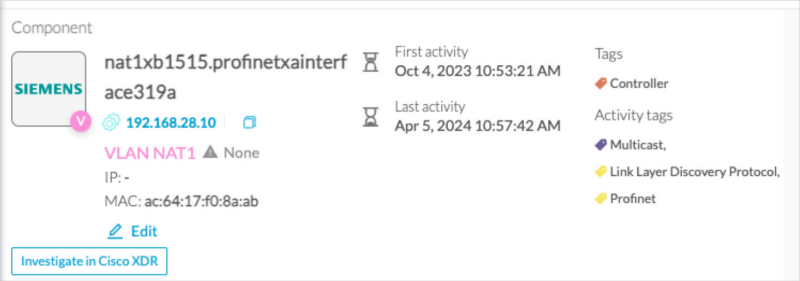
- Anomaly Detection
- Control Systems Events
- Signature Based Detection

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

Secure Equipment Access

Secure Equipment Access (SEA) is a Cisco offering that

- provides secure remote access for operations teams to manage and troubleshoot operational technology (OT) assets,

- eliminates the need for costly on-site service visits
- enables Zero Trust Network Access (ZTNA) gateway functionality.

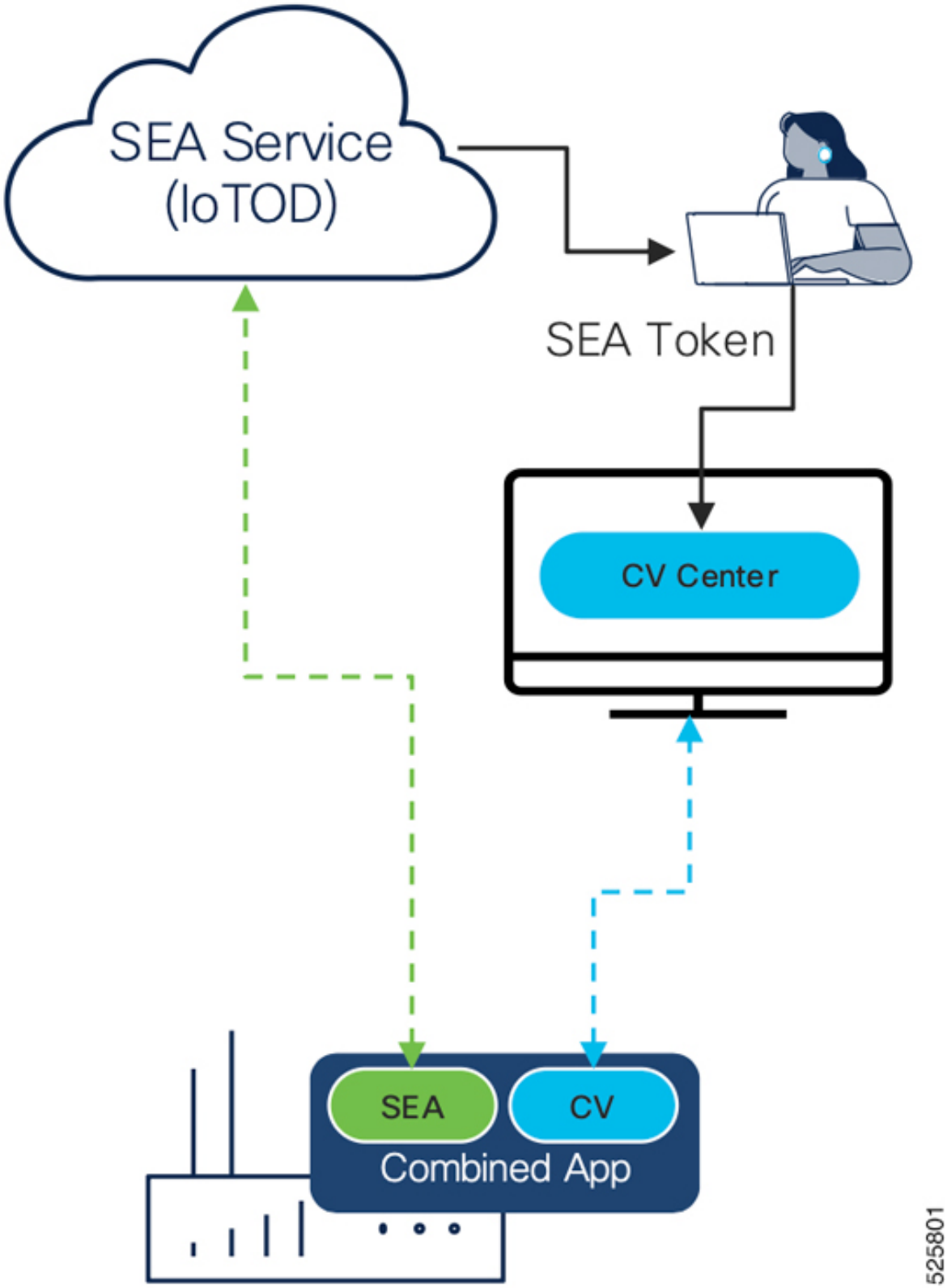
For more details, see the SEA documentation on Cisco DevNet.

You can integrate Secure Equipment Access (SEA) with Cisco Cyber Vision for unified management via the CV Center.

This integration requires the SEA agent, an IOx app, to be running on your network device. You can install the SEA agent while installing the CV sensor app using the same workflow. Both the SEA agent and CV sensor runtimes are packaged as a single IOx application.

This diagram illustrates how Cyber Vision integrates with Secure Equipment Access for industrial network management:

Figure 1: Integrate CV with SEA


SEA Service
(IoTOD)
SEA Token
CV Center
SEA
CV
Combined App
525801

Integrate Cisco Cyber Vision Center with SEA

The purpose of this integration is to enable seamless and unified management of both Secure Equipment Access (SEA) and Cisco Cyber Vision through the CV Center. This combined approach simplifies deployment and ongoing management of both components on the same device, while ensuring separation of their operations.

Before you begin

Ensure the following:

- Administrative access to Cisco Cyber Vision Center
- Tenant admin access to the SEA organization where you intend to connect with CV.

Procedure

Step 1 Log in to Cisco Cyber Vision Center, and from the main menu, choose **Admin** > **Integrations** > **SEA**.

Step 2 On the **SEA** page, in the **Configuration** section, select a region from the drop-down list and click **Connect**.

Step 3 Log in to the **IoT Operations Dashboard** with your IoT OD credentials.

Step 4 On the **IoT Operations Dashboard**, click **Connect**.

Step 5 On the **SEA** page, verify your details listed in the **Configuration** section.

Step 6 Click **Enable SEA**.

Step 7 (Optional) To validate the configuration, click **Validate configuration**.

A success message appears on the SEA page, indicating that SEA is configured.

What to do next

Install the compatible sensors. For more information, see the "Install sensors with the sensor management extension" topic in the *Cisco Cyber Vision Sensor Application for Cisco Switches Installation Guide*.

Cisco In Product Support

A **Cisco In Product Support** is a virtual assistant that:

- provides customers and partners with a unified self-service experience across multiple support domains,
- offers tools for managing cases, checking bug applicability, troubleshooting hardware, and managing licensing, and
- enables users to connect directly with case owners, managers, or Technical Assistance Center (TAC) duty managers for escalations or assistance.

Table 7: Feature History Table

Feature	Release Information	Feature Description
Cisco In Product Support	Release 5.3.x	Use Cisco In Product Support to manage your Cisco support cases and related tasks directly from the Center.

Functionality

Cisco In Product Support is designed to simplify and speed up support activities for Cisco customers and partners.

You can address technical challenges and manage support team interactions efficiently by using a single interface that consolidates multiple support services.

The tool integrates with Cisco's back-end systems to provide up-to-date case tracking, bug search, and device troubleshooting resources.

Examples

- A partner uses **Cisco In Product Support** to submit and track a hardware replacement (RMA) request.
- A customer uses the assistant to check whether a reported bug affects their installed software version.
- A network engineer leverages the self-service troubleshooting function to diagnose hardware issues without opening a formal support ticket.

Access Cisco In Product Support

Open **Cisco In Product Support** to interact with Cisco TAC support within your product.

Cisco In Product Support provides integrated access to Cisco TAC services. You can use **Cisco In Product Support** to open TAC cases, record screens, or upload files directly from your product interface.

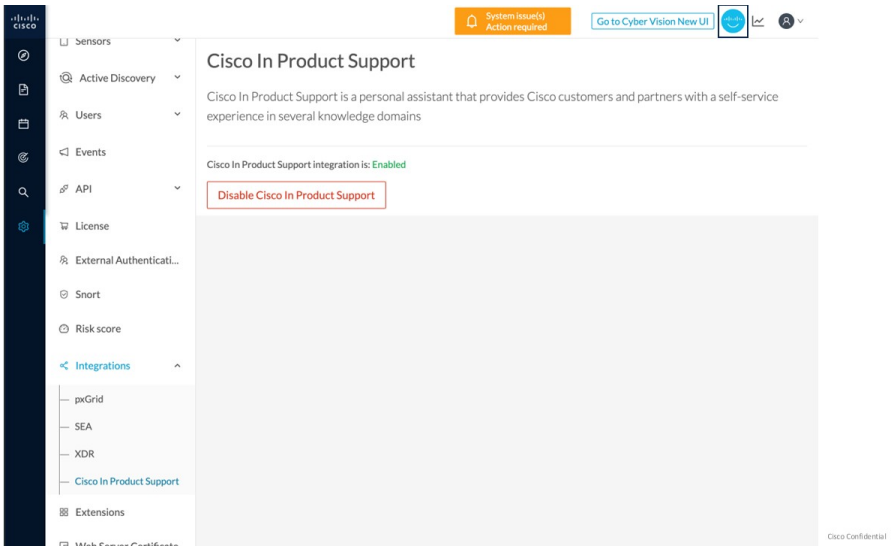
Before you begin

- Ensure you have a Cisco account with TAC access.

Procedure

Step 1 From the main menu, choose **Admin** > **Integrations** > **Cisco In Product Support**.

Note
Cisco In Product Support integration is enabled by default. Its icon is available on the page.



Step 2 Click the **Cisco In Product Support** icon.

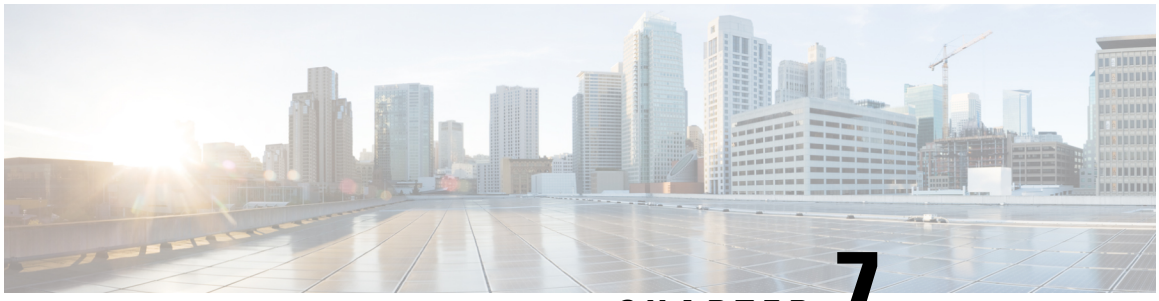
Step 3 Click **Sign In** to enable TAC's virtual assistance.

After you enable Cisco In Product Support, you can:

- **Open Cisco Support Case**
- **Record Screen**
- **Upload Local File**

What to do next

To generate and upload diagnostics, click the **System Statistics** icon.



CHAPTER 7

Maintain and Monitor Cisco Cyber Vision

- Monitored presets, on page 131
- Center Shutdown/Reboot, on page 137
- Upgrade with a Combined Update File, on page 137
- Syslog configurations, on page 139
- Import/Export, on page 140
- Knowledge DB, on page 141
- Certificate fingerprint, on page 141
- Cisco Cyber Vision Telemetry, on page 142
- Reset to Factory Defaults, on page 142
- Snort, on page 143
- Risk Score, on page 146
- Extensions, on page 146

Monitored presets

To monitor your network using Cisco Cyber Vision Center, you must set up monitored presets. A monitored preset is any preset that is monitored against a baseline.

To view the presets in your Center, from the main menu, choose **Explore**. Click a preset to view the network data that matches the preset definition. You can also export the data as a PDF file.

Presets

A preset is a customizable view that allow you to focus on specific subsets of network data. A preset filters network data based on defined criteria and gives you a focused view of an organizational network for quick, meaningful analysis.

The parameters that you can configure for a preset include:

- Time
- Risk score range
- Networks, by IP subnets or VLAN IDs
- Device tags
- Activity tags

- Groups
- Sensors

Baseline

A baseline is a snapshot of a preset. It is the reference point against which network behavior is periodically compared to detect network deviations or anomalies by identifying changes such as new devices, altered communications, or unusual activities that may indicate security issues or operational problems.

Multiple baselines for a preset

You can create multiple baselines for a preset to monitor in various known states of your network.

For example, network activity baselines may differ for weekdays and weekends. Create two baselines for these scenarios, and activate the baseline that would be an accurate monitor for your network on any given day.

To activate one of multiple baselines for a monitored preset, see Configure monitored presets, on page 135

Default presets

Some presets categories are available by default. You can make changes to the default presets and save the modified settings as new copies, but you cannot modify the default presets.

Table 8: Default presets available in Cisco Cyber Vision Center

Preset category	Presets available
Basics	• All data • Essential data • Active Discovery activities
Asset management	• OT devices • IT devices • IT infrastructure devices • All Microsoft Windows systems • All controllers
Control systems management	• OT activities • Control system activities • Process control activities

Preset category	Presets available
IT communication management	• IT activities • Web activities • Email activities • File activities • Microsoft activities
Security	• DNS activities • Remote procedure call activities • Remote access • Insecure activities • Encrypted activities • Authentication activities
Network management	• IT infrastructure activities • IT technical activities • IPv6 communications • Multicast traffic only • Broadcast traffic only

Create categories

The **Explore** page contains many default categories, including one named **My preset** in which you can place any preset that you create. You can create more categories to better organize your presets.

Procedure

Step 1 From the main menu, choose **Explore**.
Step 2 Click **New Category**.
Step 3 Enter a name for the category.
Step 4 (Optional) Select the presets you want to place in this category.
Step 5 Click **Create**.

What to do next

After you create a category, you can add a preset to the category at any time. To add a preset to a category:

1. Click the edit button for the category.
2. In the **Presets** field, select the preset you want to add to the category.

Create presets

Procedure

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

Step 2 Click **New Preset**.

Step 3 To create a preset:

a) Enter a name for the preset.
b) (Optional) Enter a description for the preset.
c) Choose a category to place your preset in.
d) Click **Create**.

Step 4 Select the newly created preset from the **Explore** page.

Step 5 In the left pane, define each criteria category. For each criteria parameter:

- Click the check box once to include the parameter
- Click the check box twice to exclude the parameter

Step 6 Click **Save**.

What to do next

After you create a preset, you can edit it at any time and update any criteria setting. These criteria settings management options are also available to you in the **Criteria** section of a preset:

- **Select all**: Include all the criteria parameters available in your Center.
- **Reject all**: Exclude all the criteria parameters available in your Center.
- **Default**: Reset all the selections such that no parameter is included or excluded.

Create baselines

Procedure

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

Step 2 To create a baseline, you can create a baseline from a preset icon () from two paths:

- The preset dashlet listed on the **Explore** page.

- The preset details page that is displayed when you click a preset dashlet.

Step 3 Enter a name and description for the preset.

Step 4 Click **Create**.

To view the newly created baseline, from the main menu, choose **Monitor**. All the baselines that are available in your Center are displayed in this page, categorized by the preset for which they were created.

Configure monitored presets

Before you begin

A monitored preset is a preset with a baseline. See Create baselines, on page 134.

In this task, you:

- Define the interval for checking the network against a monitored preset
- Choose the type of event differences you want to view alerts for

Any differences in the selected baseline and the current network status result in alerts that can review and acknowledge.

Procedure

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

Step 2 For the monitored presets you want to configure, click the vertical ellipsis icon and choose **Monitored preset settings**.

Step 3 For the monitored preset:

a) Enter a monitoring interval, in seconds.
b) If you have created more than one baseline for the preset, in the **Monitored baseline** field, choose the preset you want to activate.
c) In the **Events severity** section, choose the severity level for the alerts generated for each event type.
d) In the **Advanced settings** section, choose the component, property, and activity differences for which you want to view alerts.
e) Click **OK**.

Manage monitored preset differences

This task guides you through acknowledging or reporting a single difference entry.

- To mark a reported event as normal for the network, acknowledge the entry.
- To identify a reported event as an anomaly and create an event in Cisco Cyber Vision Center, report the entry.

After you select a baseline in the **Monitor** page, you have two bulk management options:

- To acknowledge all differences across the components and activities, click the blue tick icon in the left pane
- To acknowledge or report multiple, specific differences in the components or activities listings, select the entries and click **Acknowledge Selection** or **Report Selection**.

Procedure

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

Step 2 In the **What changed** area, for a monitored preset, click the baseline you want to examine.

Step 3 You can view the differences reported based on:

- New components
- New activities

Step 4 To view the communication flows that may have caused the reported difference, click **Investigate with flows**.

Step 5 In the components list, click an entry to view the details. You can choose from four options:

Action	Definition
Acknowledge Component	You can enter a message explaining your choice for reference. You have two acknowledgement options: • **Acknowledge and include**: Retain this alert and receive new alerts if something new happens with this component or activity. • **Acknowledge and keep warning**: Delete this alert and receive new alerts if the same event repeats.
Ack. with related activities	You can enter a message explaining your choice for reference. Click **Acknowledge and include** to retain the alert and receive alerts for any new events for the component and its activities.
Report component	You must enter a message explaining your choice for reference. You continue to receive alerts if the anomaly is detected again. Click **Report component** to create an event report for this anomaly.
Show details	View device tags and properties.

Step 6 In the activities list, click an entry to view the details. You can choose from three options:

Action	Definition
Acknowledge activity	Acknowledge the reported event as normal for the network. You can enter a message explaining your choice for reference. Two acknowledgement options are available to you: • **Acknowledge and include**: Retain this alert and receive alerts if something new happens with this component or activity. • **Acknowledge and keep warning**: Delete this alert and receive a new alert if the same event repeats.
Report activity	You must enter a message explaining your choice for reference. You continue to receive alerts if the anomaly is detected again. Click **Report activity** to create an event report for this anomaly.
Show details	View activity tags and variables.

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.

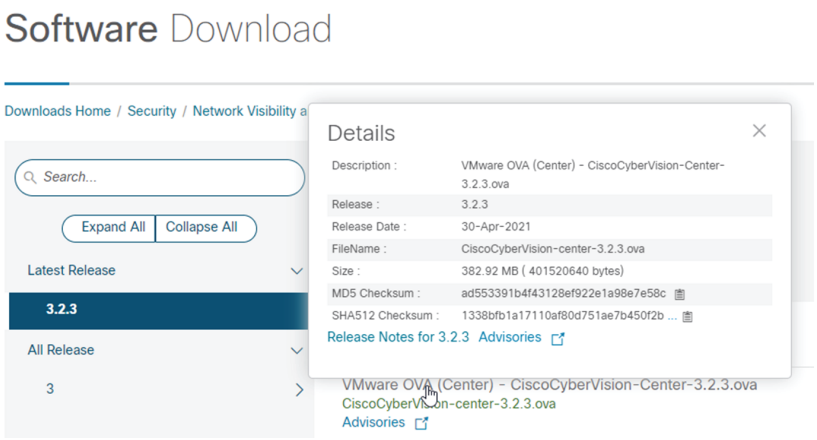
Step 2 Open a shell prompt such as Windows Powershell and use the following command to retrieve the file checksum:

Get-FileHash .\CiscoCyberVision-<TYPE>-<VERSION>.<EXT> -Algorithm SHA512 | Format-List

```
PS C:\Users\[redacted]> Get-FileHash .\Downloads\CiscoCyberVision-center-3.2.3.ova -Algorithm SHA512 | Format-List

Algorithm : SHA512
Hash      : 1338BFB1A17110AF80D751AE7B450F2B29CCB4CB54F550F38B8E6B4236865EC9EDF7773FD05D1055C7F1EF76E68C2B8A96CFE69AB
            1B622E4B0B88EBB9E94DB16
Path      : C:\Users\[redacted]\Downloads\CiscoCyberVision-center-3.2.3.ova
```

Step 3 In cisco.com, hover over the file and copy the SHA512 checksum.



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 configurations

A syslog configuration is a network logging setup that

- forwards Cyber Vision events and alerts to an external syslog server,
- enables integration with Security Information and Event Management (SIEM) platforms, and
- supports Common Event Format (CEF) for standardized message structure.

Table 9: Feature History Table

Feature	Release Information	Feature Description
Non-CEF syslogs support removed	Release 5.3.x	You can no longer use non-CEF syslog formats with Cyber Vision Center. When you upgrade to Cisco Cyber Vision Center Release 5.3.x, any existing syslog connections that use non-CEF formats are automatically updated to CEF formats.

Configure syslog

Enable forwarding of Cyber Vision events and alerts to an external syslog server to integrate with a Security Information and Event Management (SIEM) system.

To configure syslog, follow these steps:

Before you begin

- Ensure you have administrator access to Cyber Vision Center.
- Confirm that the external syslog server is accessible. Obtain the host IP address, port, and the required protocol.
- If secure communication is required, ensure you have the P12 certificate from your SIEM administrator.
- Recent syslog format changes:
  - **Standard** and **RFC3164** formats are deprecated.
  - **Standard/CEF** is now named **CEF**.
  - **RFC3164/CEF** is now named **CEF Extended Time Precision**.

Note If the deployment had **Standard** or **RFC3164** formats configured, version 5.3.x setup migrates the configuration to CEF.

Procedure

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

Step 2 Click **Configure** in the **Syslog configuration** menu.

Step 3 Select **Protocol**.

Note
If secure communication is required, select **TCP + TLS** and import the P12 certificate.

Step 4 Enter the syslog server **Host** IP address and **Port** that are accessible from Cyber Vision Center.

Step 5 Select the required **Format**.

- **CEF**: This format, based on the Common Event Format (CEF) standard, sends events with second-precision timestamps.
- **CEF Extended Time Precision**: This format, based on the Common Event Format (CEF) and an extended syslog header, sends events with millisecond-precision timestamps.

Step 6 Save the configuration.

Cyber Vision Center sends events from the Classic UI to syslog with 'Version Number = 1.0.' It sends alerts from the New UI to syslog with 'Version Number = 2.0.

What to do next

To configure notifications for specific alert types, see Enable or disable syslog notifications for alert types

To export events using syslog, see "Configure event export to syslog (Classic UI)" in the "Cisco Cyber Vision Syslog Notification Format Configuration Guide".

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

A certificate fingerprint is a unique identifier that

- verifies the authenticity of a Center digital certificate in Cyber Vision,
- enables secure enrollment and communication between Global Centers and synchronized Centers, and
- must be updated after certificate renewal to maintain trusted connectivity.

A Center fingerprint can be retrieved in Cyber Vision from **Admin** > **System** in the main menu. Select the copy icon to save the fingerprint. Paste the fingerprint during enrollment or when updating after certificate renewal.

Additional reference information

After renewal (certificates expire every two years), update all enrolled Centers with the new fingerprint. This updates their enrollment status to "Enrolled" and their connectivity status to "Connected".

For more information, see the Centers Installation Guides.

Example

If you renew a certificate for a Global Center, you must copy the new fingerprint from the Global Center and update it in all synchronized Centers to maintain secure communication.

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

A Snort instance is a network intrusion detection system (NIDS) that

- analyzes network traffic for malicious activity using a rule matching engine,
- applies a set of rules that characterize potentially harmful network activity, and
- integrates with Cisco Cyber Vision to provide real-time intrusion detection alerts and management.

Table 10: Feature History Table

Feature	Release Information	Feature Description
Enable or disable Snort on a Center DPI interface	Release 5.3.x	You can enable or disable Snort IDS or IPS on a Cisco Cyber Vision Center DPI interface. Previously, Snort was always enabled by default and could not be changed.

Additional reference information

- Cisco Cyber Vision can run the Snort engine on the Center and compatible sensors. The Center manages rule configuration and distribution. It also intercepts alerts for display in the GUI.
- Snort is disabled by default on sensors. To enable it, activate features of the Intrusion Detection System (IDS). See Enable IDS on a sensor.
- On the Center's Deep Packet Inspection (DPI), Snort is enabled by default.
- Snort is available on the following Cisco devices:
  - Cisco IC3000 Industrial Compute Gateway
  - Cisco Catalyst 9300 Series Switches
  - Cisco IR8340 Integrated Services Router Rugged
  - It is also available by default on the Center DPI.

Snort rulesets and rule categories

The Snort rules are organized into two main rulesets: the Community ruleset and the Subscriber ruleset.

Community ruleset

- Distributed freely and certified by Talos, including rules contributed by the open source community and integrators.
- Represents a subset of the full ruleset available to subscribers.
- Does not include the most recent Snort rules and does not guarantee coverage against the latest threats.

Subscriber ruleset

- Contains all rules released by the Talos Security Intelligence and Research Team.
- Provides rapid access to the newest rules and early coverage of exploits and vulnerabilities.
- Remains aligned with ongoing Talos research for maximum detection capability.
- Requires Advantage licensing and an IDS sensor license for each enabled sensor.

Snort rules are organized into categories, each targeting a specific threat type or platform.

Table 11: Rule categories

Category	Description
Browser	Detects vulnerabilities in major browsers (e.g., Chrome, Firefox, Internet Explorer) and browser plugins such as ActiveX.
Deleted	Contains deprecated or replaced rules.
Experimental–DoS	Rules targeting Denial of Service (DoS) activities such as TCP SYN flooding or DNS/HTTP flooding.
Experimental–Scada	Detects attacks on industrial control system assets.
Exploit–Kit	Tailored to identify exploit kit activities.
File	Addresses vulnerabilities in various file types (executables, Microsoft Office, images, Java, PDF, etc.).
Malware–Backdoor	Identifies traffic to known backdoor command channels.
Malware–CNC	Detects botnet command and control activity (call home, data exfiltration, download of dropped files).
Malware–Other	Covers other malicious tools or miscellaneous malware activity.
Misc	Rules address protocol-specific threats, policy violations such as spam and unwanted applications, and indicators not categorized elsewhere.
OS–Other	Looks for vulnerabilities in various operating systems (Linux, mobile OS, Solaris, etc.).
OS–Windows	Targets vulnerabilities in Windows operating systems.
Server–Other	Deals with vulnerabilities in multiple server types (web servers, database servers, mail servers, etc.).
Server–Webapp	Pertains to attacks against server-based web applications.

Snort rules management features

The Snort rules management system in Cisco Cyber Vision Center includes these features:

Table 12: Snort rules management

Feature	Description
Snort community rules	Snort community rules are set by default in the Cyber Vision Center.
Subscriber rules	Click **Use Subscriber Rules** from the **Admin** > **Snort** page to enable snort subscriber rules (requires Advantage and intrusion detection system (IDS) sensor licenses).
Category-based management	Enable or disable entire rule categories via the GUI.
Direct rule file download	Download rule files per category from the interface.
Individual rule control	Enable or disable specific rules within categories, independent of category status. In the downloaded rule files, locate the rule and get the sid (signature id). Go to **Admin** > **Snort** and enter it in the **Rule sid** and click **Disable** or **Enable**.
Custom rule import	Import and manage user-created rules via the **IMPORT CUSTOM RULES FILE** function from the **Admin** > **Snort** page.
Rule synchronization	Apply synchronized rule sets to sensors using the **Synchronize rules on sensors** feature from the **Admin** > **Snort** page.
Reset to default	Click **RESET TO DEFAULT** from the **Admin** > **Snort** page to restore the entire rule configuration to factory defaults and remove all custom rule files.

Enable IDS on a sensor

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

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

Before you begin

Ensure your sensor is one of these compatible devices:

- Cisco IC3000 Industrial Compute Gateway
- Cisco Catalyst 9300 Series Switch

- Cisco IR8340 Integrated Services Router Rugged
- Center DPI Interface

Procedure

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

Step 2 Select the sensor you want to enable IDS on.

Step 3 Click **Enable IDS**.

IDS is now active on the selected sensor. Snort will now monitor network traffic for threats.

What to do next

If required, you can disable Snort's intrusion detection capabilities. To do this, select the sensor and click **Disable IDS**.

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 Concept.

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:

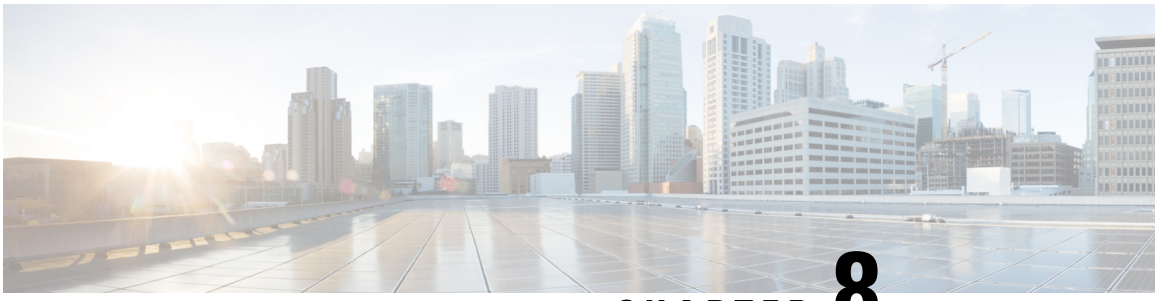
- **Cyber Vision sensor management**

  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

Cyber Vision New UI

- Cyber Vision New UI, on page 147
- Assets, on page 148
- Vulnerabilities, on page 150
- Communication maps, on page 151
- Asset clustering, on page 154
- Alerts, on page 157
- Syslog notification details for various alert types, on page 161
- Organization hierarchies, on page 162
- Filters, on page 163
- Network definitions, on page 164
- Pcap files, on page 166
- Sensor applications, on page 167
- Use Cases, on page 168

Cyber Vision New UI

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

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

Table 13: Feature History Table

Feature	Release Information	Feature Description
New UI	Release 5.3.x	Cisco Cyber Vision Center offers New UI that comprises simplified, structured views of assets, vulnerabilities, and alerts. The New UI includes a new method for automatically grouping assets using AI-based clustering. Click **Go to Cyber Vision New UI** in the top banner of your Center to get started.

Expanded explanation

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

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

Table 14: Contrast table

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

Assets

An asset is a network entity that

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

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

Table 15: Feature History Table

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

Asset interfaces

Assets use different network interfaces to communicate within the network. Interfaces may include MAC addresses, IP addresses, VLAN IDs, or combinations of these. The system collects interface properties from network traffic. It selects one interface as the primary interface for visualizations. If multiple interfaces exist, you can change which interface is primary. The asset list shows both the primary and additional interfaces for each asset.

Asset data management

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

Function	Description
Delete assets	By default, the system deletes assets removed from the production line after 30 days. You can manually delete assets detected due to misconfiguration. If sensors detect the assets again, the system may re-add them to the inventory.
Search for assets	Enter at least three characters from an asset's name, IP address, or MAC address in the search bar to quickly locate details.
Export	Export all asset data to a CSV file. The export includes asset IDs so you can distinguish assets with the same name.

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

Vulnerabilities

A vulnerability is a system weakness that

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

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

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

Vulnerability scores

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

Cisco Security Risk Score (CSRS)

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

Table 16: CSRS categories:

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

Common Vulnerability Scoring System (CVSS)

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

Table 17: CVSS categories:

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

Acknowledge or revert a vulnerability acknowledgement

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

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

Before you begin

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

Procedure

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

Step 2 Select an asset.

Step 3 Select the **Vulnerabilites** tab.

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

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

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

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

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

Communication maps

A communication map is a network visualization tool that

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

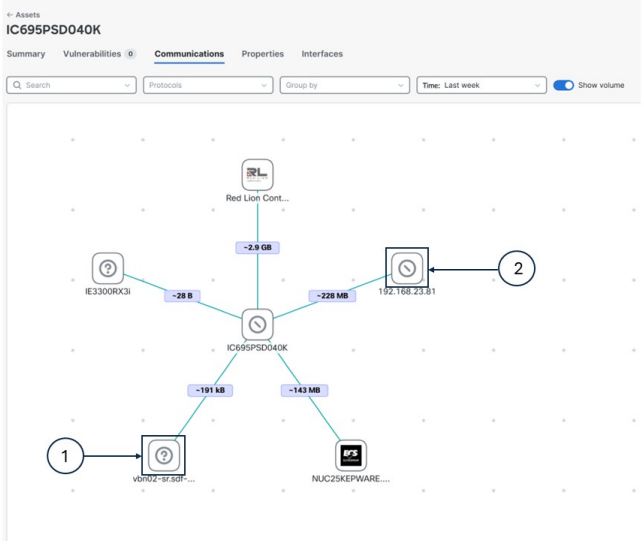
This functionality enables operational technology (OT) and information technology (IT) teams to quickly visualize and understand the communication context of industrial assets. It provides a clear visual reference to abnormal communications and potential risks.

Table 18: Feature History Table

Feature	Release Information	Feature Description
See functional-group centric views of communication map	Release 5.3.x	The communications map displays the communication activity between the configured functional groups. The communication links between groups are not actionable.
Using asset vendor names and icons	Release 5.3.x	In New UI, communication maps now include icons of vendors to help you identify assets more easily.

Additional reference information

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



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

Assets and functional group communication maps

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

Table 19: Types of communication maps

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

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

Asset clustering

An asset cluster is a functional grouping that

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

Table 20: Feature History Table

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

Additional reference information

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

Asset movement

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

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

Types of functional groups

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

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

Cluster assets into functional groups

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

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

Follow these steps to perform asset clustering:

Procedure

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

Step 2 Click **Start asset clustering**.

The system suggests functional groups in the list.

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

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

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

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

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

The assets are clustered into a new functional group.

What to do next

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

Asset clustering methods

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

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

Functional group actions and descriptions

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

The table lists the functional group actions and their descriptions.

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

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



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

Alerts

Alerts are system-generated notifications that

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

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

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

Table 21: Feature History Table

Feature	Release Information	Feature Description
Active and cleared alerts	Release 5.3.x	The Alerts page displays two types of alerts: • Active • Cleared
Pause alert creations	Release 5.3.x	You can pause an alert type in the **Configure** > **Alerts**
Change vulnerability scoring system for alerts	Release 5.3.x	The Cisco Security Risk Score is the default scoring system applied to alert configurations. However, you can choose to update an alert configuration to apply the CVSS scoring system instead.
Alert for severe vulnerabilities in monitored entities	Release 5.3.x	Create and edit rules for the **Severe vulnerabilities in monitored entities** alert based on the Cisco Security Risk Score or the CVSS score.
Alert for prohibited vendors	Release 5.3.x	The **Configure** > **Alerts** page contains a default alert for prohibited vendors. The alert rule is based on an editable list of prohibited vendors.

Additional reference information

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

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

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

Alert details are as follows:

Table 22: Alert details

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

Alert type management options and permitted alert rule actions

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

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

Table 23: Permitted alert rule actions for each alert type

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

Note

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

Create alert rules

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

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

Before you begin

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

Procedure

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

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

Step 3 Click **Create new rule**.

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

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

- If selecting assets based on functional groups, check **Include Ungrouped assets** to include assets not in any functional group.
- If selecting assets based on organization hierarchy levels, check **Assets seen by Unknown data sources** to include unidentified or unmapped assets.

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

Step 6 In the **Scoring system and threshold** tab, select one scoring system:

- For **Cisco Security Risk Score**, enter a threshold number between 34 and 100.
- For **CVSS**, enter a threshold number between 7 and 10.

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

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

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

What to do next

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

Syslog notification details for various alert types

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

Common syslog message fields

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

Table 24: Additional fields for specific alert types

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

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

Enable or disable syslog notifications for alert types

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

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

Before you begin

- Ensure you have administrator access to Cyber Vision Center.
- Confirm that a syslog server is configured. See Configure syslog.

Procedure

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

Step 2 Select an alert type.

Step 3 Enable or disable **Syslog Notification**.

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

Organization hierarchies

An organization hierarchy is a structural model that

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

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

Additional reference information

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

Key points about organization hierarchies in Cyber Vision Center:

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

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

Filters

A filter is a New UI feature that

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

Table 25: Feature History Table

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

Additional reference information

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

Filter views in Cyber Vision New UI

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

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

Follow these steps to filter data in Cyber Vision:

Procedure

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

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

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

- To select all sensors or networks at a hierarchy level, select that level.
- To choose specific sensors or networks from a selected hierarchy level, open the organization drawer again, open **Sensor selection** or **Network selection**, select the needed items, and click **Apply**.
- Use the search box to find sensors or networks by name.

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

Step 4 To edit the sensor or network selection for the selected organization hierarchy only, open the **Organization Hierarchy** drawer again and click the **Edit selection** icon.

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

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

Step 7 Click **Apply** to update or **Reset** to clear the filters.

The views show only data that matches your filter criteria.

What to do next

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

Network definitions

A network definition is a configuration element in Cyber Vision that

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

Table 26: Feature History Table

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

Additional reference information

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

Example

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

Counter example:

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

Assign a network to an organization hierarchy

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

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

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

Before you begin

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

Procedure

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

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

Pcap files

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

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

Additional reference information:

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

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

Assign multiple PCAP files to an organization hierarchy

Before you begin

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

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

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

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

Procedure

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

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

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

Step 4 Choose the appropriate organization hierarchy.

Step 5 Click **Assign**.

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

Each PCAP initiates asset creation in Cisco Cyber Vision.

Sensor applications

A sensor application is an embedded software component that

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

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

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

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

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

Additional reference information

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

Assign sensors to the Organization Hierarchy

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

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

Follow these steps to assign sensors to the organization hierarchy:

Procedure

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

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

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

Step 4 Select the organization hierarchy.

Step 5 Click **Assign** to confirm.

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

Use Cases

Filter PLCs by organization hierarchy

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

Before you begin

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

Procedure

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

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

Step 3 Select the organization level.

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

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

Step 6 Click **Apply**.

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

Acknowledge critical vulnerabilities

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

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

Before you begin

- Ensure you have permission to view and acknowledge vulnerabilities.

Procedure

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

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

Step 3 Click the filter icon of the table.

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

Step 5 Click **Acknowledge**.

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

What to do next

Review acknowledged items periodically to ensure they remain appropriate.