



Cisco Cyber Vision Administration Guide, Release 5.2.x

First Published: 2024-09-20

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	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
	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	74
License Usage Compliance	75

CHAPTER 4**Get Started with Cisco Cyber Vision 77**

- Certificate Fingerprint 77
- Data Management 77
 - Clear Data 78
 - Purge components in Cisco Cyber Vision 78
- Expiration Settings 79
- Ingestion Configuration 79
- Users 80
 - Management 80
 - Role Management 82
 - Create roles 82
 - Security Settings 83
- Center Web Server Certificate 83

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 for Cisco Cyber Vision Center 93
 - SAML single sign-on 94
 - SSO guidelines for the Cisco Cyber Vision Center 94
 - Single Sign-On user accounts 95
 - User role mapping for SSO users 96
 - Single Sign-On with Azure AD 96
 - Add an enterprise application for Azure 96
 - Configure the Cyber Vision Center service provider application for Azure 97
 - Configure the Cyber Vision Center for Azure SSO 99
- Duo Single Sign-Ons for generic SAML service providers 100
 - Requirement: Prerequisites for Duo Single Sign-On setup 100

Add authentication source for Duo	101
Create cloud application in Duo	101
Configure the Cyber Vision Center service provider application for Duo	102
Add user in service provider application	103
Configure the Cisco Cyber Vision Center for Duo	104
Sensors	104
Sensor Explorer	104
Filter and Sort the Sensor List	105
Sensors Status	105
Sensors Features	106
Install Sensor	107
Sensor Self Update	108
Manage Credentials	109
Organize Sensors	109
Set a Capture Mode	110
Deployment Tokens	111
Create Deployment Tokens	112
Templates	112
Create Templates	113
Export Templates	114
Import Templates	114
Management Jobs	115
PCAP Upload	115
SNMP	116
Configure SNMP	116
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	122
--	-----

CHAPTER 7

Maintain and Monitor Cisco Cyber Vision 125

Monitored presets	125
Create categories	127
Create presets	128
Create baselines	128
Configure monitored presets	129
Manage monitored preset differences	129
Center Shutdown/Reboot	131
Upgrade with a Combined Update File	131
Configure syslog	133
Import/Export	134
Knowledge DB	134
Certificate Fingerprint	135
Cisco Cyber Vision Telemetry	135
Reset to Factory Defaults	135
Snort	136
Import Snort Custom Rules	138
Enable IDS on a Sensor	138
Enable or Disable a Rule	139
Risk Score	140
Extensions	140

CHAPTER 8

Cisco Cyber Vision Beta Version 141

Cisco Cyber Vision Center beta version	141
Use search bar	142
Purpose	142
Dashboard	142
Filter views of dashboard, alerts, assets, vulnerabilities, and communications pages	143
Assets	144
Asset Selection	145
Table Setting	145
Asset deletion	145

Vulnerabilities	146
Acknowledge or revert vulnerability acknowledgements	147
Primary Interface	147
Properties	148
Explore communication map	148
Asset clustering	150
Perform asset clustering	150
Asset Clustering for a Limited Set of Assets	151
Asset Clustering for a Specific Functional Group	151
Asset Clustering for Selected Sensors	151
Asset Clustering for Individual Assets	152
Lock Group	152
Move Asset from One Group to Another	153
Delete the Functional Group	153
Remove Asset from Functional Group	154
Alerts dashboard	154
Alerts configuration	155
Add new alert rules	155
Manage alert rules	156
Pause and resume alert types	157
Enable or disable the syslog notifications for alert types	157
Configuration	158
Organization hierarchies	158
Add, edit, and delete levels in the organization hierarchy	159
Network definitions	159
Assign network to organization hierarchy	160
PCAP	160
Sensor Applications	161
Assign the Sensor to the Organization Hierarchy	162
Use Cases	163
Review All PLC and SCADA Data Servers in the Paint Shop	163
Analyze and Acknowledge All Vulnerabilities with a CVSS Score Above Nine	164



CHAPTER 1

New and Changed Information

- [New and Changed Information, on page 1](#)

New and Changed Information

Features of Cisco Cyber Vision Release 5.2.x are as follows:

Feature	Description
Interactive Help	<p>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.</p> <p>Interactive help is enabled by default. To disable the feature in your Cisco Cyber Vision center, go to Admin > System. The Interactive help plug-in area contains a toggle button for the feature.</p> <p>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.</p> <p>See Interactive Help Plugin.</p>
LDS support for user authentication	<p>Cisco Cyber Vision Center now supports user authentication through Lightweight Directory Services (LDS). See LDAP.</p>
Purge multiple VLAN components	<p>The sbs-db purge-components command is enhanced to allow the removal of multiple components associated with a VLAN.</p>
CEF support for syslog configuration	<p>New syslog configurations in the Cisco Cyber Vision Center require use of the Common Event Format (CEF) standard.</p>

Feature	Description
	<p>Existing syslog configurations that use non-CEF message formats are not affected in Cisco Cyber Vision Release 5.2.x.</p> <p>Non-CEF message formats may not be supported in later releases of Cisco Cyber Vision.</p>
Beta UI	<p>Cisco Cyber Vision Center offers a beta UI experience, with informative, easy-to-handle dashboards that present data on assets, vulnerabilities, alerts, and organization hierarchies. You can quickly apply data filters to view necessary information.</p> <p>This UI experience is a beta feature. To access the beta UI and its features, write to cv-beta@cisco.com. You will receive the command to enable the Cisco Cyber Vision Beta UI in addition to the existing classic UI.</p> <p>You can also configure functional groups in the beta UI, and assign data sources to organization hierarchies.</p> <p>To configure network definitions, sensors, and PCAPs, you must continue to use the classic UI. The overall task flows of Cisco Cyber Vision are currently spread across the classic and beta UIs, with the beta UI offering enhanced visualization of the center's data.</p> <p>Beta UI Enhancements</p> <p>See Introduction of the Cisco Cyber Vision Beta Version.</p> <ol style="list-style-type: none"> 1. User profile: The user profile is now displayed in the top banner of the Beta UI. The profile section displays the email id or username, or both, of a user, based on where user information is stored (Cisco Cyber Vision database or LDAP directory). 2. The left menu in the Beta UI is collapsible. 3. You can now log out from the Cisco Cyber Vision Center through the Beta UI. 4. Session expiry: If a session is inactive for an hour, you must log into the Cisco Cyber Vision Center again. <p>Communications map enhancements: The communications map displays an overview of all the communication events between connected assets. See Explore communication map. The following enhancements are now available:</p>

Feature	Description
	<ol style="list-style-type: none"> 1. Apply a time filter to the map to view communications in a specific time period. 2. Group assets by the subnet or functional group that they belong to to organize your communication map. 3. Click an asset to for a line graph representation of data flow. You can filter the graph by time and protocol. <p>Cisco Security Risk Score: Cisco Cyber Vision Center now presents a Cisco Security Risk Score for the vulnerabilities displayed. The risk score is based on Cisco Vulnerability Management's predictive model. In Cisco Cyber Vision, the risk score includes factors of exploitability and dark web activity for topical context about risk severity to help prioritize vulnerability management. See Dashboard for the New UI.</p> <p>Rack slot information for modular PLCs: The asset summary page for modular PLCs includes information on rack slots. For each slot on a modular PLC, the model name, slot type, firmware version, and serial number are displayed.</p> <p>Rerun functional group suggestions: You can regenerate functional group suggestions at any time in the Asset Visibility > <choose an asset> > Communications page. You can rerun asset data at multiple levels to receive specific functional group suggestions:</p> <ol style="list-style-type: none"> 1. Data associated with one sensor 2. Data associated with one asset 3. Data associated with an existing functional group 4. All the data in the Cisco Cyber Vision center <p>When you accept a functional group suggestion, existing functional groups may be modified to ensure an asset is part of any one functional group. .</p> <p>Heat maps for alerts: The Alerts page displays a heat map to help you quickly visualise alert trends. The map spans the last 7 days, broken into two-hour segments. Hover over a segment to view the alert count.</p> <p>Enable syslog notification for alert types: You can choose to send syslog notifications to a connected</p>

Feature	Description
	<p>syslog server for an alert type. Syslog notifications are enabled by default for new and existing alert types in your Center. You can choose to disable the notifications in the Alerts page. See Syslog notifications for alert types.</p> <p>Acknowledge vulnerabilities across assets: You can view, acknowledge, or cancel acknowledgment of a vulnerability across multiple assets. .</p>



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 Beta 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

The screenshot shows the 'Criteria' panel on the left with a search bar and a list of criteria. Under 'NETWORKS', two criteria are selected: '192.168.0.0/16' (checked) and '192.168.22.0/24' (unchecked). The '33 Activities' panel on the right shows a table of network activities.

Device	Device	First activity	Last activity	Tags
Siemens 192.168.21.50	Broadcast ffff:fff	Jul 6, 2021 10:56:20 AM	Jul 6, 2021 10:59:16 AM	Broadcast, ARP
Weintek 192.168.0.92	1756-L81ES/B (Port1-Link03)	Jul 6, 2021 10:56:20 AM	Jul 6, 2021 10:59:15 AM	Read Var, EthernetIP
1756-L71/B LOGIX5571 (Port1-Link00)	Cisco 192.168.20.254	Jul 6, 2021 10:56:20 AM	Jul 6, 2021 10:59:15 AM	ARP
1756-L71/B LOGIX5571 (Port1-Link00)	Weintek 192.168.0.92	Jul 6, 2021 10:56:20 AM	Jul 6, 2021 10:59:14 AM	Low Volume, EthernetIP

Multiple negative selections are not supported on 4.0.0.

Filter combination

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

Device tag filters

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

Device tag filters

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

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

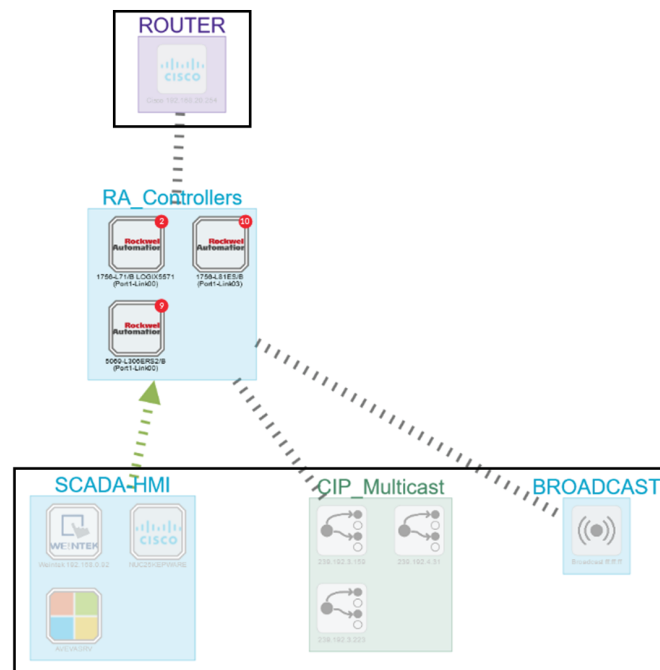
It will give the following results:

Device tag filter, example of Controllers – list of devices

Device	Group	First activity	Last activity	IP	MAC	Risk score	Tags
5069-L3046RS2/B (Port1-Link00)	RA_Controllers	Jul 6, 2021 10:56:20 AM	Jul 6, 2021 10:59:18 AM	192.168.20.23	Sc:88:16:a3:10:f2 (+ 1 other)	70	Controller, Rockwell Automation
1756-L81ES/B (Port1-Link00)	RA_Controllers	Jul 6, 2021 10:56:20 AM	Jul 6, 2021 10:59:15 AM	192.168.20.25	Sc:88:16:ed:c0:8e (+ 1 other)	70	Controller, Rockwell Automation
1756-L71/B LOGX5571 (Port1-Link00)	RA_Controllers	Jul 6, 2021 10:56:20 AM	Jul 6, 2021 10:59:14 AM	192.168.20.21	Sc:88:16:ef:d1:2e (+ 1 other)	70	Controller, Rockwell Automation

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

Filters

186 Activities [New data](#)

Device	Device	First activity	Last activity	Tags	Flows	Packets	Volume
IE3400SWITCHES.ccv 04:5f:b9:cce:59:87	CDP/VTP/UDLD Multicast ccccccc	Jul 6, 2021 11:06:14 AM	Jul 6, 2021 11:09:38 AM	Multicast, CDP	-10	2	920 B
Broadcast ff:ff:ff:ff:ff:ff	Moxa 192.168.0.28	Jul 6, 2021 11:06:11 AM	Jul 6, 2021 11:09:35 AM	Broadcast, ARP	-10	2	56 B
Moxa 192.168.0.28	Elitegroup 192.168.0.26	Jul 6, 2021 11:06:11 AM	Jul 6, 2021 11:09:39 AM	Net Management, ARP, SNMP	-10	29232	2.9 MB
Broadcast ff:ff:ff:ff:ff:ff	Good 192.168.0.4	Jul 6, 2021 11:06:03 AM	Jul 6, 2021 11:09:42 AM	Broadcast, ARP	-10	18	504 B
Elitegroup 192.168.0.26	Vmware 192.168.0.18	Jul 6, 2021 11:06:01 AM	Jul 6, 2021 11:09:42 AM	Ping, ARP, ICMP	-10	14	1.08 kB
IE3400SWITCHES.ccv 04:5f:b9:cce:59:87	LLDP/STP bridges Multicast 0:0:0	Jul 6, 2021 11:05:58 AM	Jul 6, 2021 11:09:43 AM	Multicast	-10	36	2.16 kB
Elitegroup 192.168.0.26	Virtual 192.168.0.235	Jul 6, 2021 11:05:58 AM	Jul 6, 2021 11:09:43 AM	Remote access, Low Volume	-10	1536	720 kB
Elitegroup 192.168.0.52	23.200.213.221	Jul 6, 2021 10:59:09 AM	Jul 6, 2021 10:59:16 AM	Insecure, Web, HTTP	-10	5	330 B
SRV-AD-LABCCV	Broadcast 192.168.0.255	Jul 6, 2021 10:59:07 AM	Jul 6, 2021 10:59:07 AM	Broadcast, Low Volume, Netbios, SMB	-10	1	243 B

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

Cisco 192.168.0.140	Vmware 192.168.0.7	Jul 6, 2021 10:56:30 AM	Jul 6, 2021 10:56:30 AM	ARP
1756-L71/B LOGIX5571 (Port1-Link00)	Cisco 192.168.20.254	Jul 6, 2021 10:56:20 AM	Jul 6, 2021 10:59:15 AM	ARP

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

Activity filter – negative filter 3

Last 5 years (Jul 13, 2016 2:45:18 PM – Jul 12, 2021 2:45:18 PM) [Refresh](#)

163 Activities [New data](#)

Device	Device	First activity	Last activity	Tags	Flows	Packets	Volume
IE3400SWITCHES.ccv 04:5f:b9:cce:59:87	CDP/VTP/UDLD Multicast ccccccc	Jul 6, 2021 11:06:14 AM	Jul 6, 2021 11:09:38 AM	Multicast, CDP	-10	2	920 B
Moxa 192.168.0.28	Elitegroup 192.168.0.26	Jul 6, 2021 11:06:11 AM	Jul 6, 2021 11:09:39 AM	Net Management, ARP, SNMP	-10	29232	2.9 MB
Elitegroup 192.168.0.26	Vmware 192.168.0.18	Jul 6, 2021 11:06:01 AM	Jul 6, 2021 11:09:42 AM	Ping, ARP, ICMP	-10	14	1.08 kB
IE3400SWITCHES.ccv 04:5f:b9:cce:59:87	LLDP/STP bridges Multicast 0:0:0	Jul 6, 2021 11:05:58 AM	Jul 6, 2021 11:09:43 AM	Multicast	-10	36	2.16 kB
Elitegroup 192.168.0.26	Virtual 192.168.0.235	Jul 6, 2021 11:05:58 AM	Jul 6, 2021 11:09:43 AM	Remote access, Low Volume	-10	1536	720 kB
Elitegroup 192.168.0.52	23.200.213.221	Jul 6, 2021 10:59:09 AM	Jul 6, 2021 10:59:16 AM	Insecure, Web, HTTP	-10	5	330 B
SRV-AD-LABCCV	Broadcast 192.168.0.255	Jul 6, 2021 10:59:07 AM	Jul 6, 2021 10:59:07 AM	Broadcast, Low Volume, Netbios, SMB	-10	1	243 B
40.125.122.176	NUC25KEPWARE	Jul 6, 2021 10:58:55 AM	Jul 6, 2021 10:59:17 AM	Web, Encrypted, HTTPS	-10	13	858 B

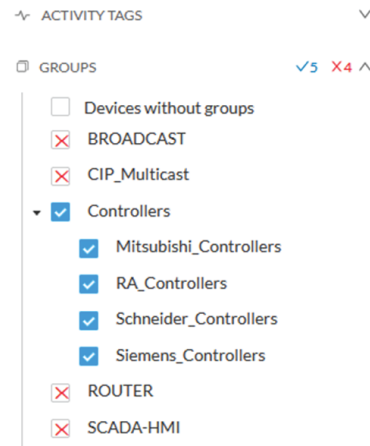
For very specific use cases, combine inclusive and exclusive tags. The above rules, for positive and negative selection, are combined, resulting in the following logic:

- 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.

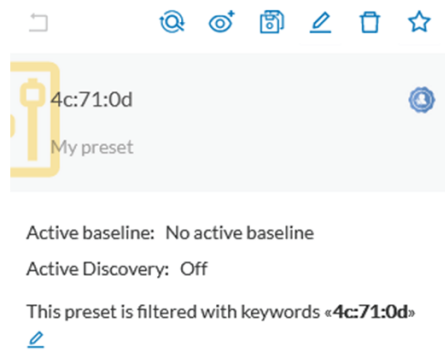
Sensor filter



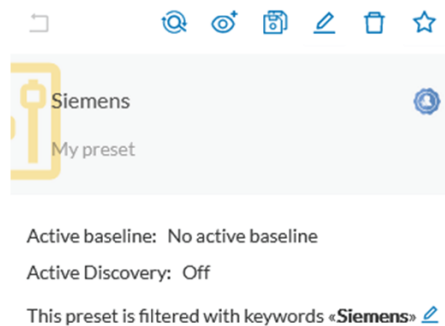
Keyword

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:



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 Vision 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

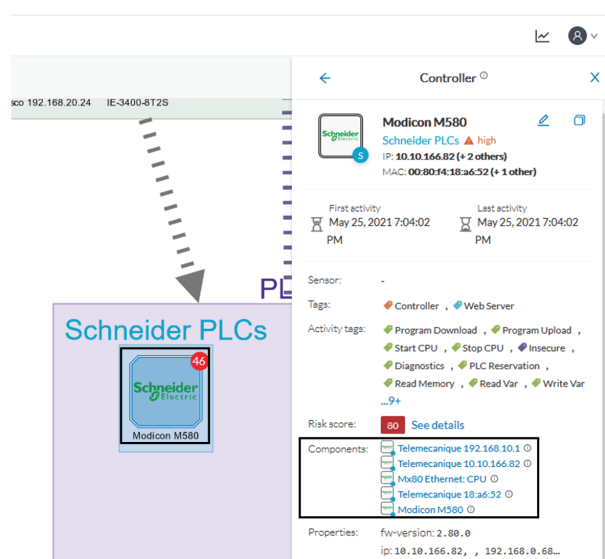
The term **Device** is an aggregation of [components](#) with similar properties. In Cisco Cyber Vision, a **Device** is a physical machine of the industrial network such as a switch, an engineering station, a controller, a PC, a server, etc. Devices simplify data presentation, especially on the map.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

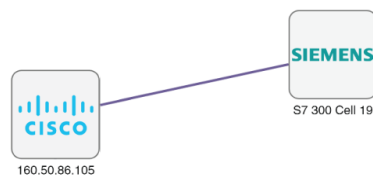
All these device's components have in common activity time, IPs, MACs, and tags. The Controller tag -which is a level 2 device tag, also considered as top priority in aggregation rules to define device type- detected on one of the components is applied at the device level and define the device type as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

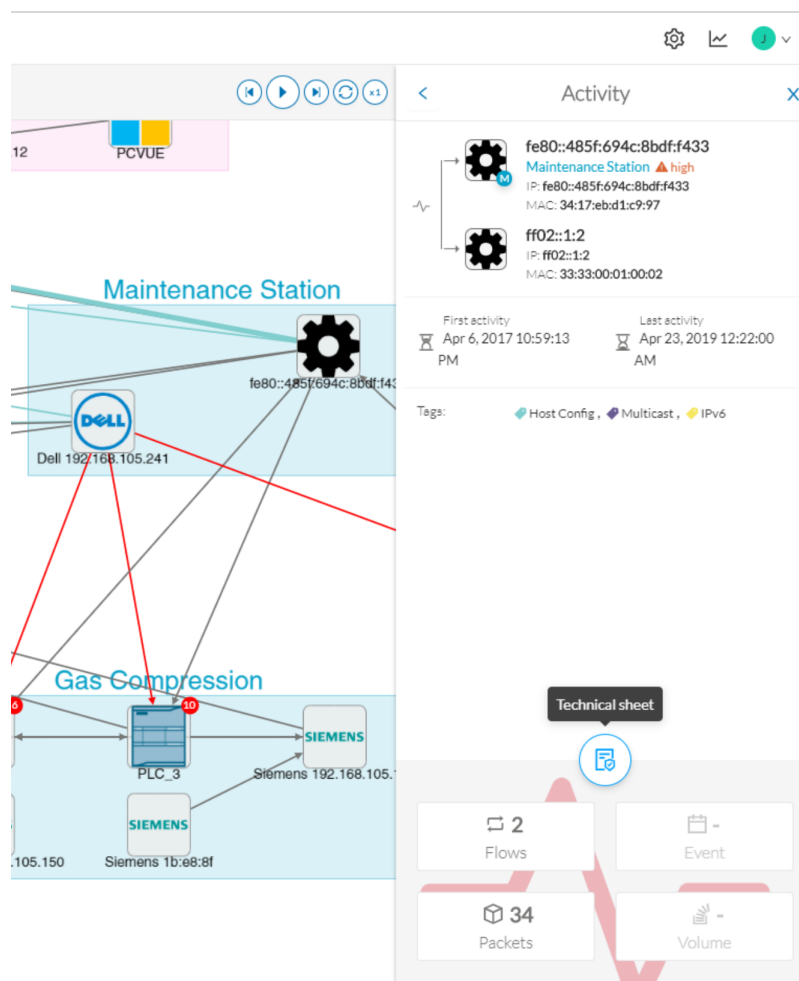


An activity between two components is actually a simplified view of the [flows](#) exchanged. You can have many types of flows going in both directions inside an activity, represented in the map.

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.

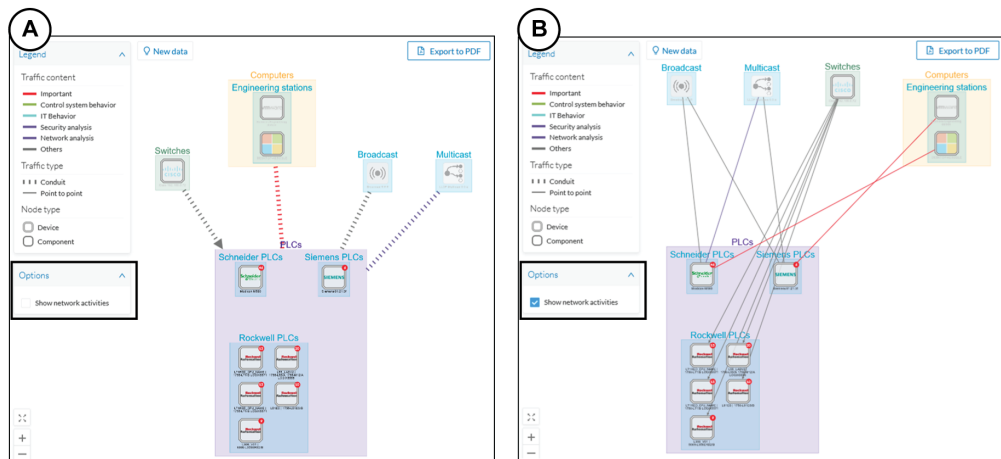


Devices or components with no activity does not mean that they did not have any interaction. In fact, a component can only be detected if it has been involved in a network activity (communication emission/reception). Lack of activity can mean that the other linked component is not part of the preset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

22

< 1 2 > 20 / page

	Last activity	Tags	Packets	Bytes
8:20 PM	Nov 28, 2018 4:48:20 PM	<input type="checkbox"/> ARP (2) <input type="checkbox"/> Broadcast (1) <input type="checkbox"/> Low Volume (2) <input type="checkbox"/> Profinet (14) <input type="checkbox"/> Read Var (4) <input type="checkbox"/> Write Var (3)	0	0 B
8:20 PM	Nov 28, 2018 4:48:20 PM		0	0 B
8:20 PM	Nov 28, 2018 4:48:20 PM		0	0 B
8:20 PM	Nov 28, 2018 4:48:20 PM		0	0 B
8:20 PM	Nov 28, 2018 4:48:20 PM		0	0 B
8:20 PM	Nov 28, 2018 4:48:20 PM	Profinet	0	0 B
8:20 PM	Nov 28, 2018 4:48:20 PM	Profinet	0	0 B

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 unnecessary data, and the license device count and risk scores are limited to inner devices and more accurate.

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

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

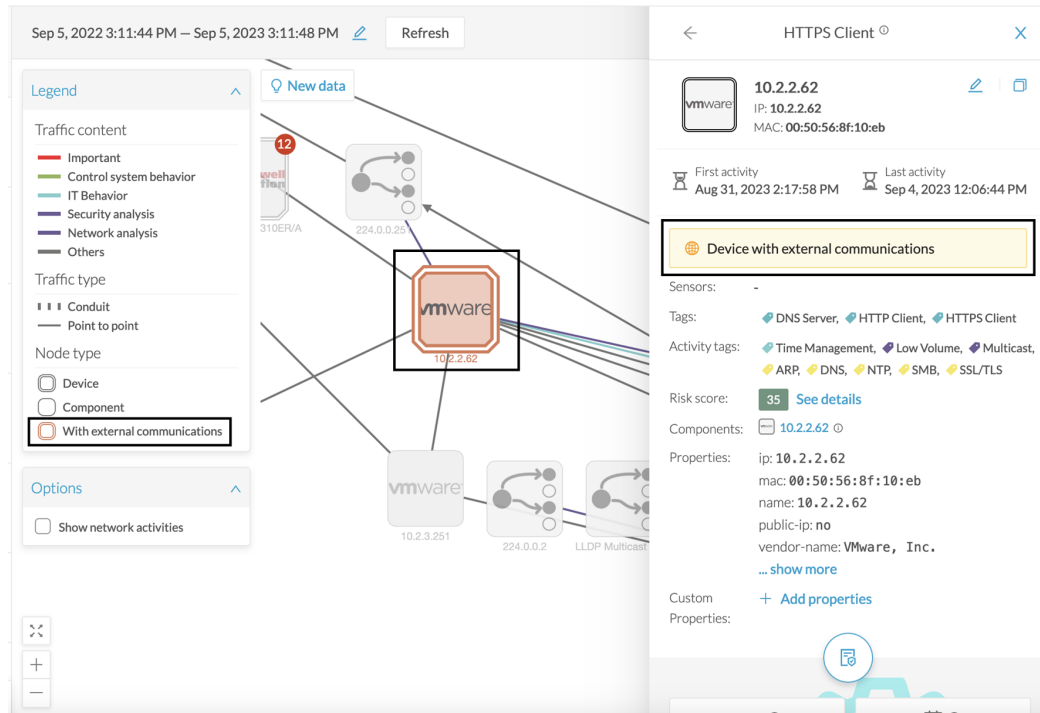
However, because sometimes public IP addresses are used in a private network of an industrial site, it is possible to manually define communications by declaring IP ranges as internal or external through the Network Organization administration page. For more information, refer to Cisco Cyber Vision GUI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

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

IP Address / subnet	VLAN ID	Network Name	Network Type	Action
<input type="checkbox"/> 10.0.0.0/8		10/8 private network	External	
10.2.0.0/22		OT range	OT Internal	
10.4.0.0/22		External IP within IP range	IT Internal	

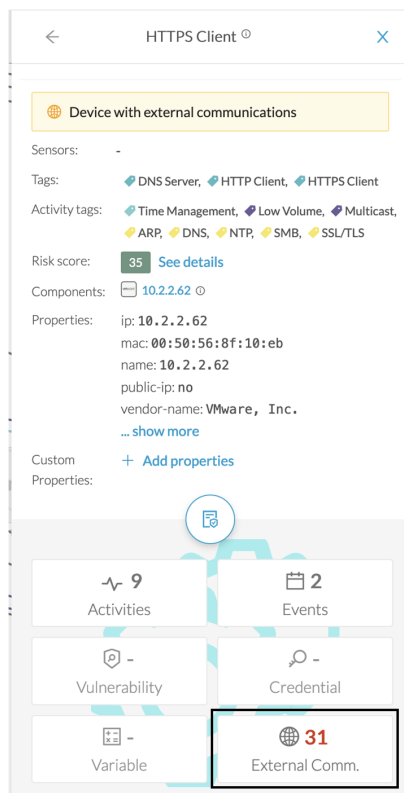
In the GUI, a component with external communications is shown as an icon bordered in orange, or a double orange border for a device.

A device with external communications in the Map:



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

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



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

									Export to CSV
All Inbound Outbound									1 2 20 / page
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 dropdw 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

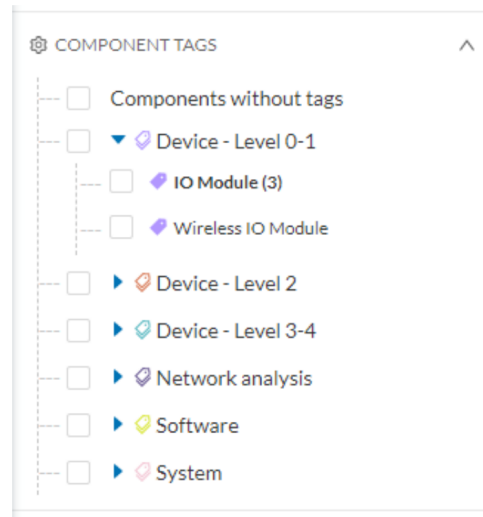
Tags	Tags are meaningful labels that succinctly describe a network. They can be applied to components or activities. Each tag has a description and an icon color which correspond to its category.
 Program Upload ,  Unite	
 Program Download ,  Start CPU ,  Stop CPU ,  Unite	
 Start CPU ,  Stop CPU , 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

Tags are metadata on [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.

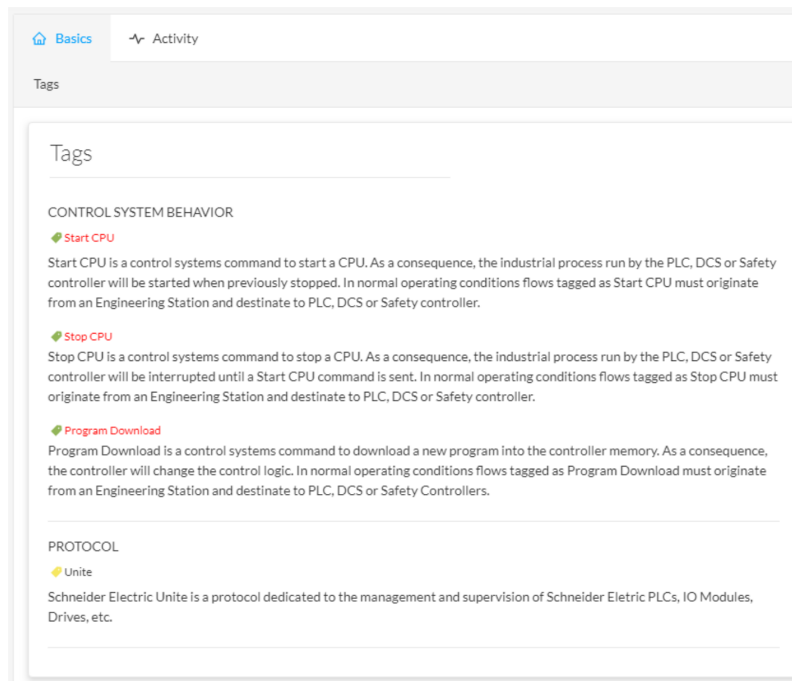
Use tags to define behaviors (i.e., in the Monitor mode) inside an industrial network when combined with information like source and destination ports and flow properties.

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 [Dashboard, on page 41](#).

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.

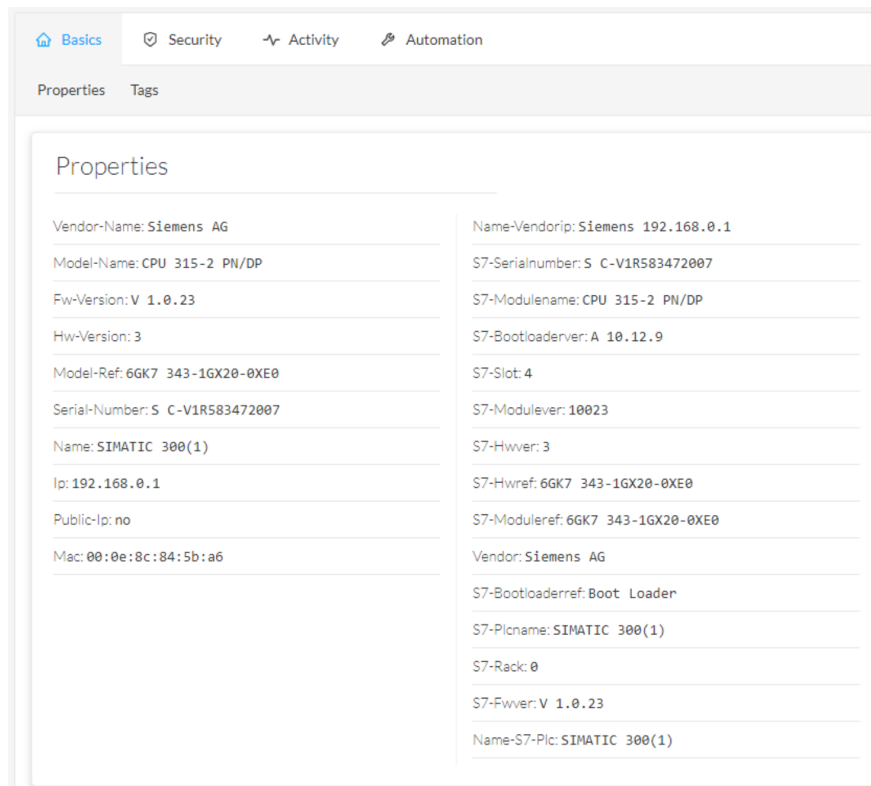
Property Use

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.



Properties	
Vendor-Name: Siemens AG	Name-Vendorip: Siemens 192.168.0.1
Model-Name: CPU 315-2 PN/DP	S7-Serialnumber: S C-V1R583472007
Fw-Version: V 1.0.23	S7-Modulename: CPU 315-2 PN/DP
Hw-Version: 3	S7-Bootloaderver: A 10.12.9
Model-Ref: 6GK7 343-1GX20-0XE0	S7-Slot: 4
Serial-Number: S C-V1R583472007	S7-Modulever: 10023
Name: SIMATIC 300(1)	S7-Hwver: 3
Ip: 192.168.0.1	S7-Hwref: 6GK7 343-1GX20-0XE0
Public-Ip: no	S7-Moduleref: 6GK7 343-1GX20-0XE0
Mac: 00:0e:8c:84:5b:a6	Vendor: Siemens AG
	S7-Bootloaderref: Boot Loader
	S7-Plcname: SIMATIC 300(1)
	S7-Rack: 0
	S7-Fwver: V 1.0.23
	Name-S7-Plc: SIMATIC 300(1)



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.

Vulnerabilities 12

1 ☐ **Siemens EN100 Ethernet Module CVE-2016-7114 Authentication Bypass Vulnerability**
 CVE-2016-7114 – SSA-630413
 The EN100 Ethernet module before 4.29 for Siemens SIPROTEC 4 and SIPROTEC Compact devices allows remote attackers to bypass authentication and obtain [show more](#)

Solution
 Siemens provides firmware update V4.29 for EN100 modules included in SIPROTEC 4 and SIPROTEC Compact to fix the vulnerability. Siemens recommends customers to update to the latest firmware version.

Published on September 5, 2016
 Identified on this component on August 27, 2019
 Identified vulnerable because of mac(00:09:8e:fab7:1c)

Links
www.securityfocus.com
www.securityfocus.com
www.siemens.com

2 **9**
 score CVSS

Access Vector: Network
 Access Complexity: Low
 Authentication: Requires Single Instance
 Confidentiality impact: Complete
 Integrity impact: Complete
 Availability impact: Complete

3 **Acknowledge?**

258277

- 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/Cancellation**.

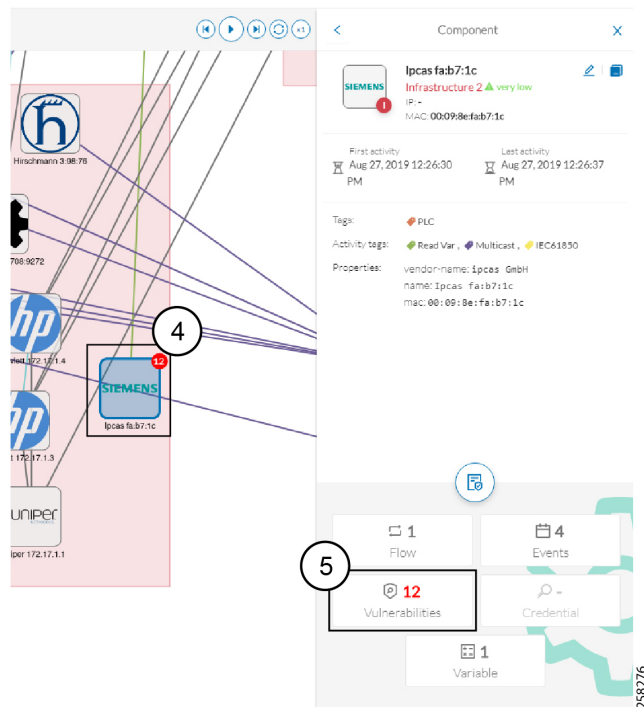
Vulnerability Location

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.

	Flows	Vuln	Var
	7	2	0
	7	7	22
	13	9	0
	2	0	1
	6	6	0
	23	6	13

	Flows	Vuln	Var
	12171	42	1
	29	13	0
	26	13	0
	1	12	2
	1	12	1
	13	9	0

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.

Component

lpcas fab7:1c
Infrastructure 2 ▲ **very low**
 IP: -
 MAC: 00:09:8e:fab7:1c
[Edit](#) [Remove from group](#)

First activity: Aug 27, 2019 12:26:30 PM
 Last activity: Aug 27, 2019 12:26:37 PM

Tags: PLC
 Activity tags: Read Var, Multicast, IEC61850

Properties: vendorname: lpcas GmbH
 name: lpcas fab7:1c
 mac: 00:09:8e:fab7:1c

1 Flow, 4 Events, 12 Vulnerabilities, 1 Variable

Basics Security Activity Automation

Vulnerabilities Credentials

Vulnerabilities

12

- ☐ **Siemens EN100 Ethernet Module CVE-2016-7114 Authentication Bypass Vulnerability**
 CVE-2016-7114 – SSA-630413
 The EN100 Ethernet module before 4.29 for Siemens SIPROTEC 4 and SIPROTEC Compact devices allows remote attackers to bypass authentication and obtain ... [show more](#)
Solution
 Siemens provides firmware update V4.29 for EN100 modules included in SIPROTEC 4 and SIPROTEC Compact to fix the vulnerability. Siemens recommends customers to update to the latest firmware version.
 Published on September 5, 2016
 Identified on this component on August 27, 2019
 Identified vulnerable because of mac (00:09:8e:fab7:1c)
 Links
www.securityfocus.com
www.securityfocus.com
www.siemens.com
- ☐ **Denial-of-Service Vulnerabilities in EN100 Ethernet Communication Module and SIPROTEC5 relays**
 CVE-2018-11451 – SSA-635129
 A vulnerability has been identified in Firmware variant IEC 61850 for EN100 Ethernet module (All versions < V4.33), Firmware variant PROFINET IO for E ... [show more](#)

9
score CVSS

Access Vector: Network
 Access Complexity: Low
 Authentication: Requires Single Instance
 Confidentiality impact: Complete
 Integrity impact: Complete
 Availability impact: Complete

Acknowledge?

7.8
score CVSS

Access Vector: Network

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.

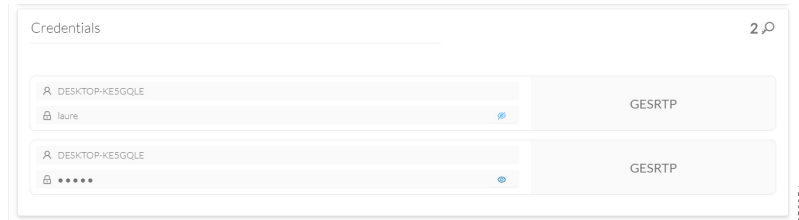
The screenshot shows the Cisco Cyber Vision interface. On the left, a network diagram highlights a component labeled 'OSFGSA' with a red circle containing the number '21'. The main panel displays the details for this component. At the top, it shows the component name 'OSFGSA', IP '192.168.6.3', and MAC '00:10:18:70:b6:b0'. Below this, it lists 'First activity' and 'Last activity' as 'Oct 3, 2019 5:48:40 PM'. The 'Tags' section includes 'Windows'. The 'Activity tags' section lists 'Insecure', 'Citect Alarm', 'Citect IO', 'Citect Trend', 'Authentication', 'Ping', 'Procedure Call', 'Broadcast', 'Exception', and 'Low Volume ...7+'. The 'Properties' section lists 'vendor-name: Broadcom', 'os-name: Windows Server 2003 3790 Service Pack 2', 'fw-version: 5.2.3790', 'serial-number: d62566cd46ff8d4a8540b7e37ee b7b15', and 'name: OSFGSA ...3+'. At the bottom, a summary bar shows '767 Flows', '245 Events', '21 Vulnerabilities', and '2 Credentials'. The 'Credentials' tab is highlighted with a red box.

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

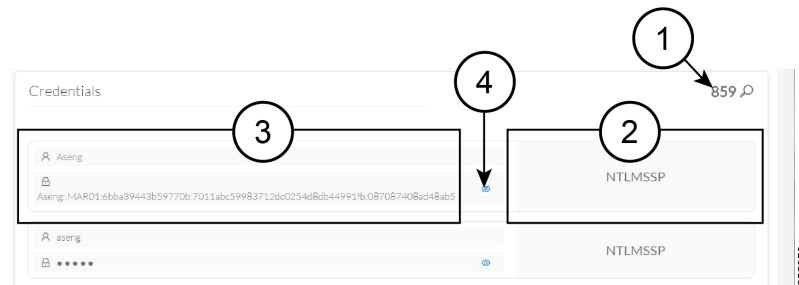
1. The number of credentials found.
2. The protocol used.

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

An unsafe password:



A hashed password:



Variable Accesses

Variable Definition

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

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

Variable Use

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

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

- The name of the variable
- Its type (READ or WRITE) but not the value itself
- Which component accessed the variable

- The first and last time the component accessed the variable

The screenshot shows the 'Variables accesses' section of the Cisco Cyber Vision interface. The table displays the following data:

Variable	Types	Accessed by	First access	Last access
DB1784.DBB 0	READ	Siemens 10.239.18.21	Sep 25, 2019 12:01:30 PM	Sep 25, 2019 12:01:31 PM
DB75.DBB 0	READ	Siemens 10.239.18.21	Sep 25, 2019 12:01:30 PM	Sep 25, 2019 12:01:31 PM
MB 0	READ	2 different accesses	Sep 25, 2019 12:01:30 PM	Sep 25, 2019 12:01:31 PM
	READ	Berneckner 10.239.18.30	Sep 25, 2019 12:01:30 PM	Sep 25, 2019 12:01:31 PM
	READ	Siemens 10.239.18.21	Sep 25, 2019 12:01:30 PM	Sep 25, 2019 12:01:31 PM
DB1784.DBX 0.6	WRITE	Siemens 10.239.18.21	Sep 25, 2019 12:01:31 PM	Sep 25, 2019 12:01:31 PM
DB75.DBB 100	READ	Siemens 10.239.18.21	Sep 25, 2019 12:01:30 PM	Sep 25, 2019 12:01:31 PM

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

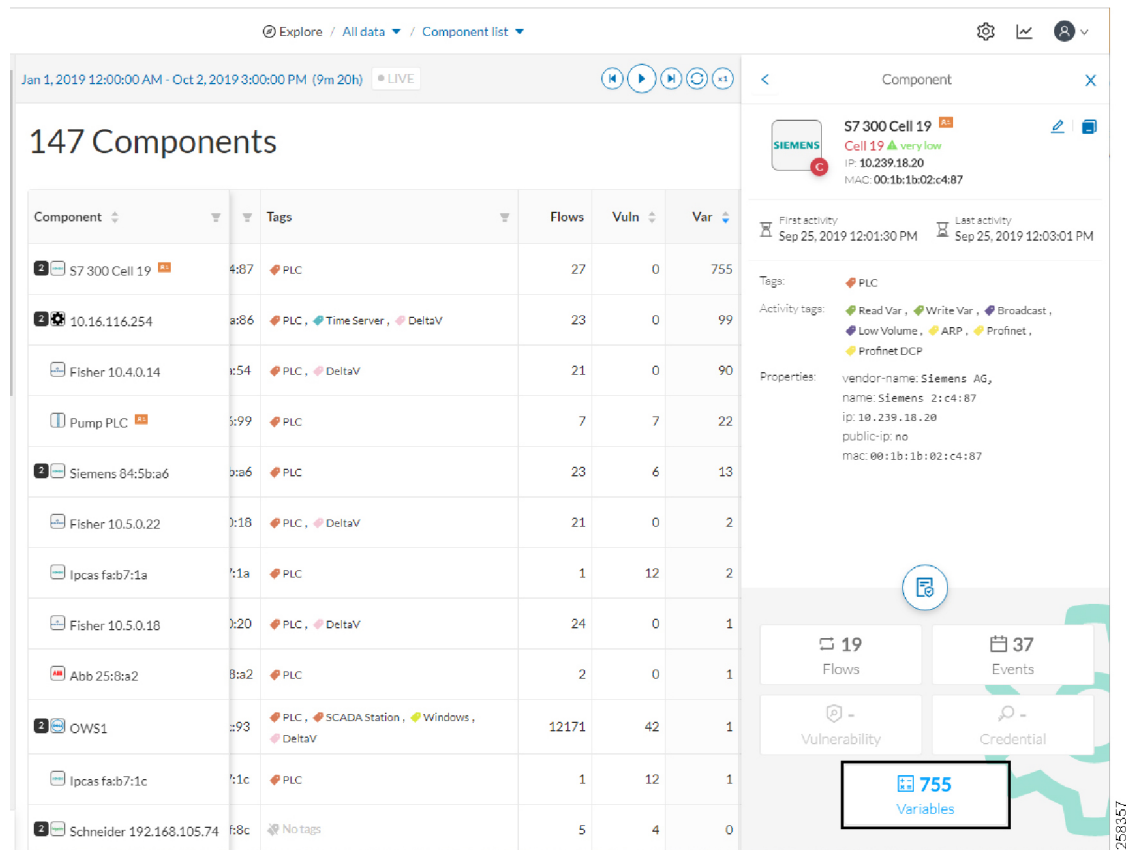
Variable Location

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

The screenshot shows the 'Component list' view of the Cisco Cyber Vision interface. The table displays the following data:

Component	Tags	Flows	Vult	Var	Vendor	OS	Model	Firmware version	Project
S7 300 Cell 19	PLC	27	0	755	Siemens AG,	-	-	-	-
10.16.116.254	PLC, Time Server, DeltaV	23	0	99	-	-	-	-	-
Fisher 10.4.0.14	PLC, DeltaV	21	0	90	Fisher-Rosemount Systems Inc.	-	-	-	-
Pump PLC	PLC	7	7	22	Siemens AG,	-	PLC 4	V 6.0.3	-
Siemens 84.5ba6	PLC	23	6	13	Siemens AG	-	-	-	-
Fisher 10.5.0.22	PLC, DeltaV	21	0	2	Fisher-Rosemount Systems Inc.	-	-	-	-

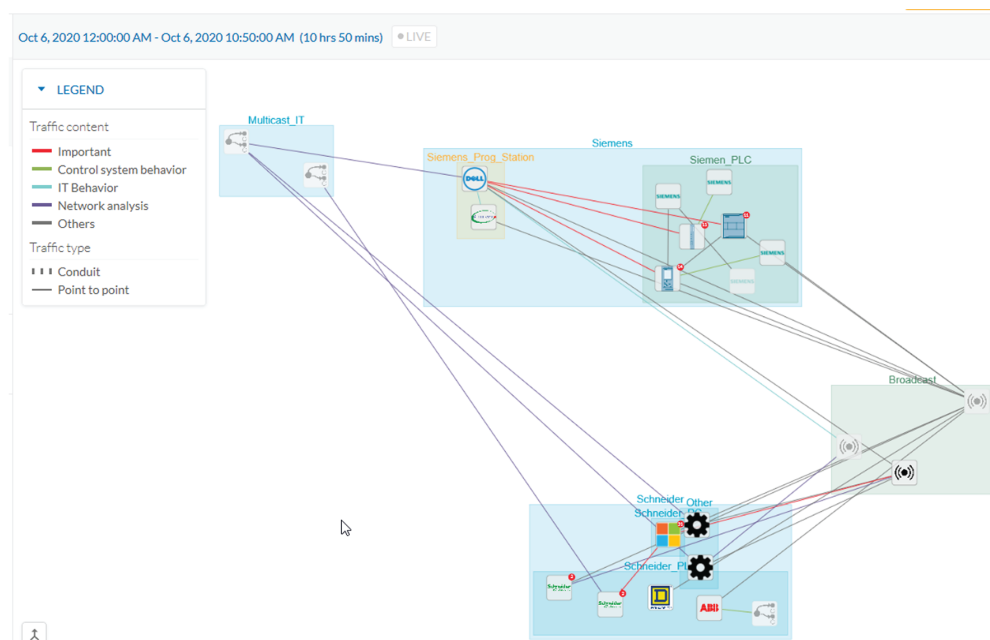
For component details, click a component. The right panel opens.



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

Creating and Customizing Groups

Accessibility: Admin, Product and Operator users



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

To create a group:

Procedure

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

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

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

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

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

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

Step 5 Click **Manage selection**.

The drop-down list appears.

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

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

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

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

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

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

Step 10 Enter **Properties**.

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

To create a parent group:

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

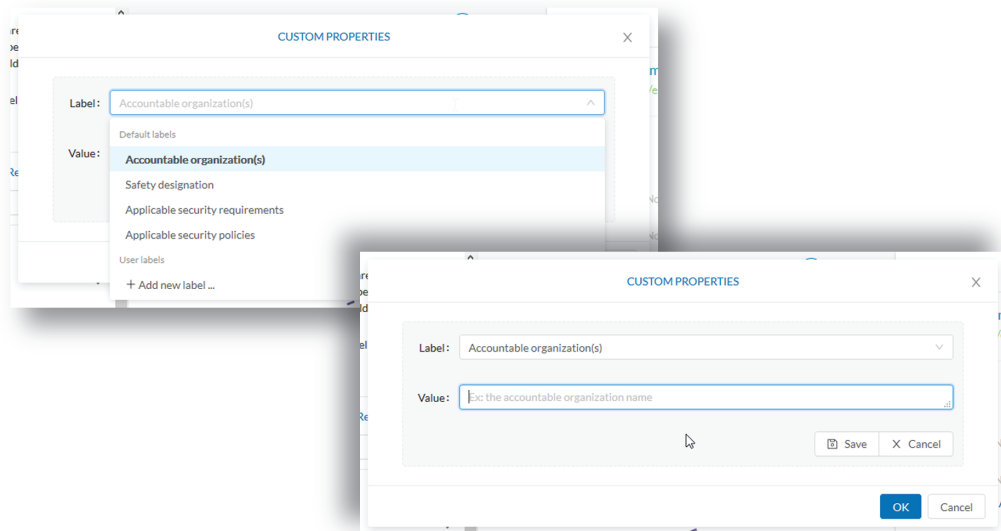
- Select two groups and create a group, as indicated above.
- Select a device or a component and move it into a group. Use the **Move selection to existing group** button.
- Select a group and move it to another group. Use **Move selection to existing group**.

Add group properties

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

To add properties to a group:

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

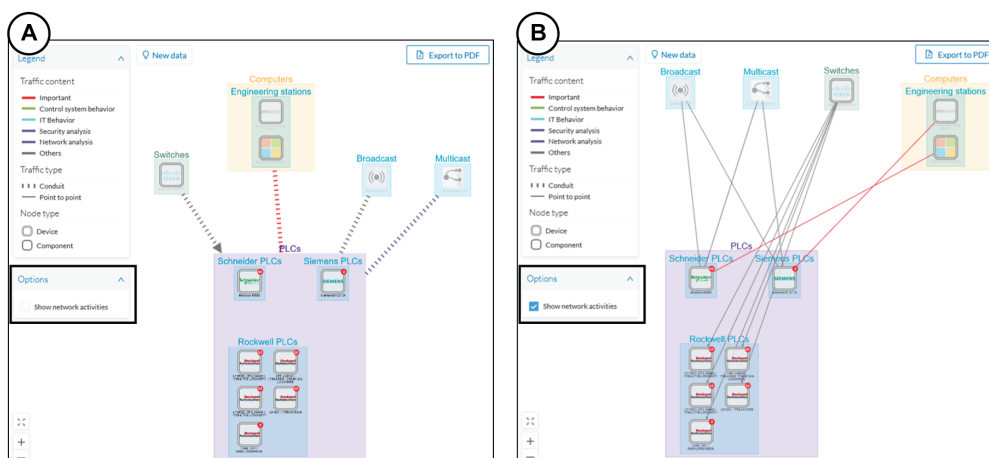


Aggregated activities are conduits

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

Creating and Customizing Groups



Group Lock/Unlock

Locking a group:

- Prevents adding or removing components from the group.
- Prevents a group deletion.

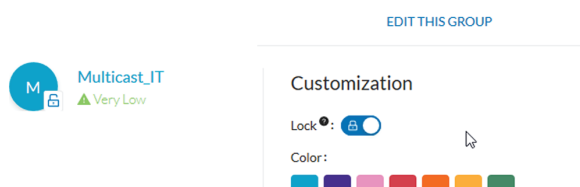
To switch on/off the **Lock** icon:

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

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

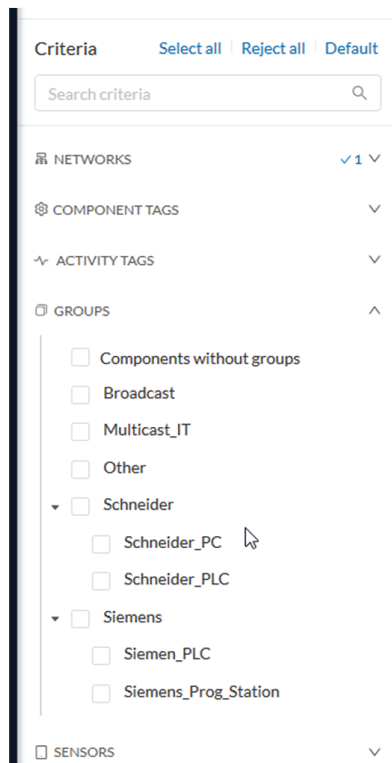
or

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 activities are 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.

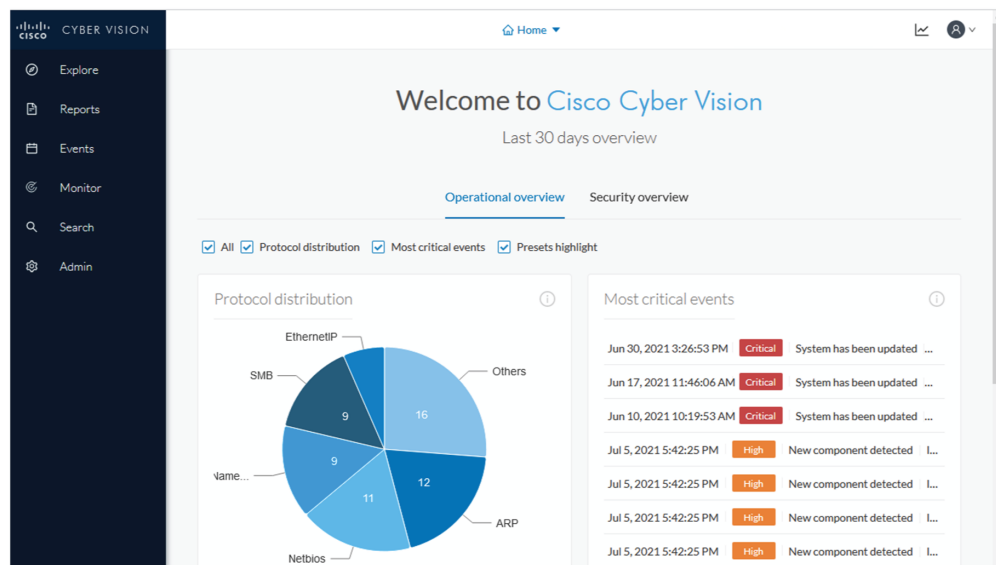
For more information and instructions on how to configure **Active Discovery** in Cisco Cyber Vision, refer to [the Active Discovery Configuration Guide](#).

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.



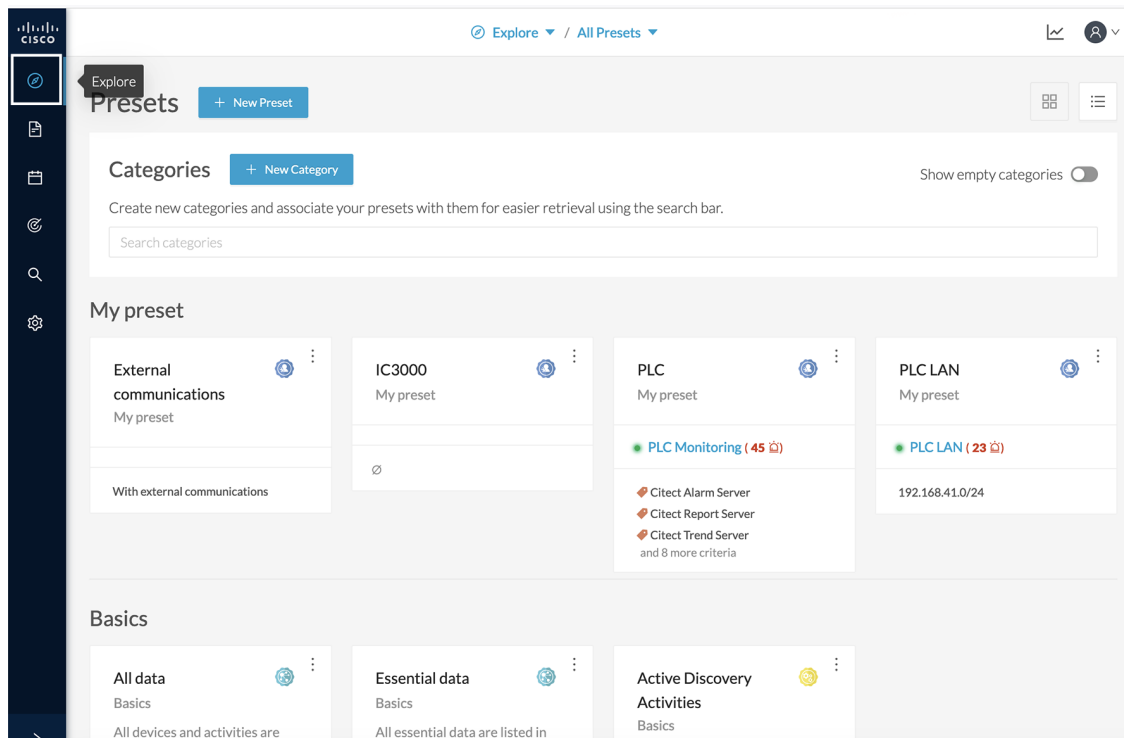
It also shows a list of the **Most critical events**, **Events by category**, and the **Preset highlights** that you can edit.

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

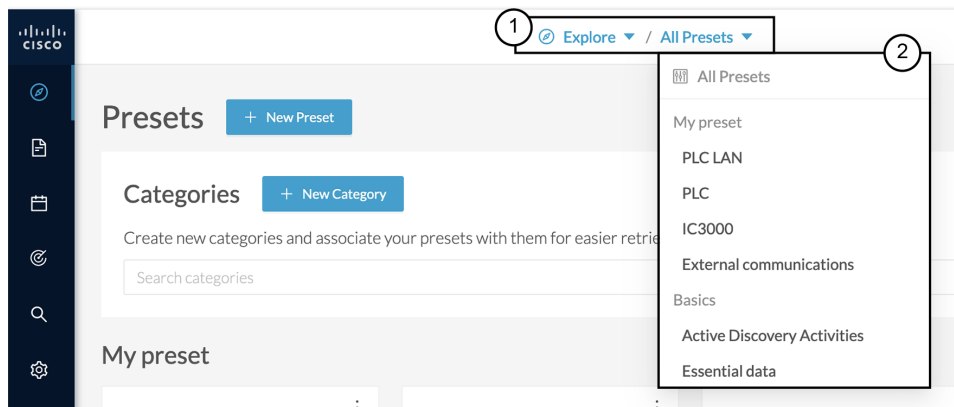
1. **Explore:** Shows the overview of all presets, by defaults or configured.
2. **Reports:** Shows the [Reports page](#) to export valuable information about the industrial network.
3. **Events:** Shows the Events page which contains graphics and a calendar of all events generated by .
4. **Monitor:** Shows the [Monitor, on page 53](#) 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

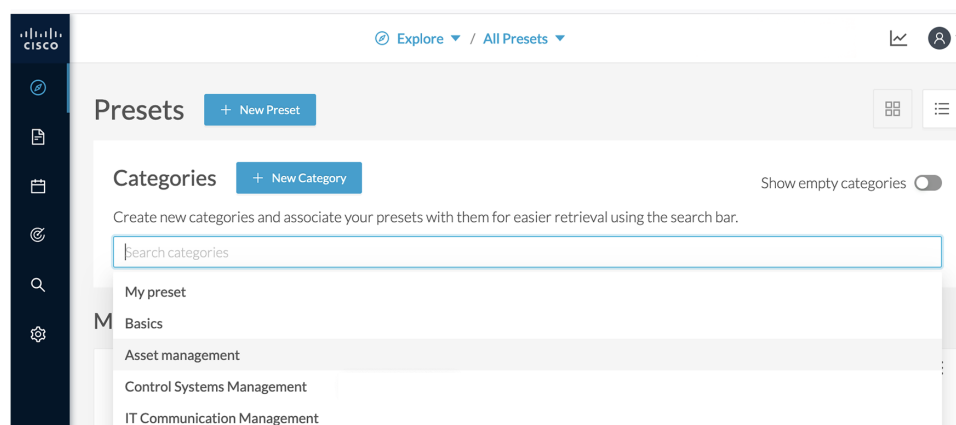
Explore shows an overview of all the Presets in Cisco Cyber Vision, both defaults and custom presets. Click **Explore** on the left navigation bar.



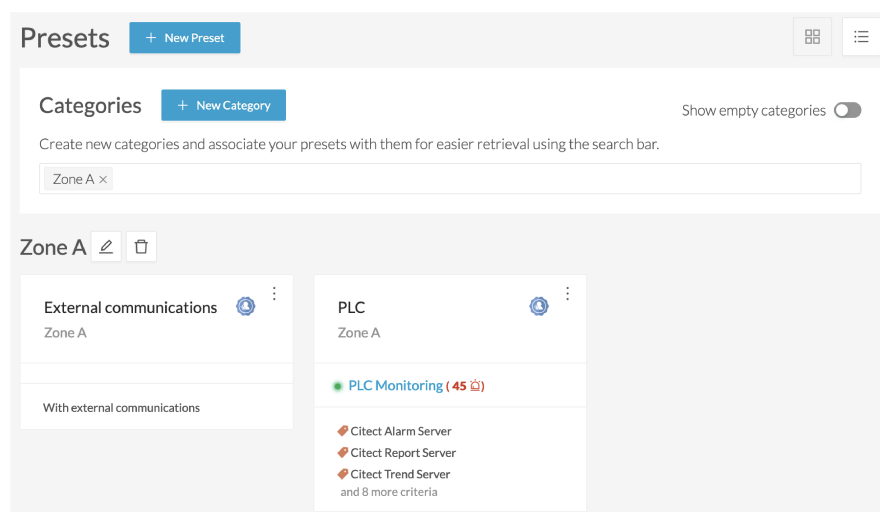
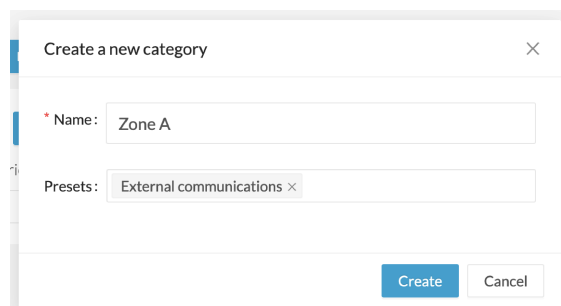
Use the top navigation bar (1) to access the different presets (2) and [views](#).



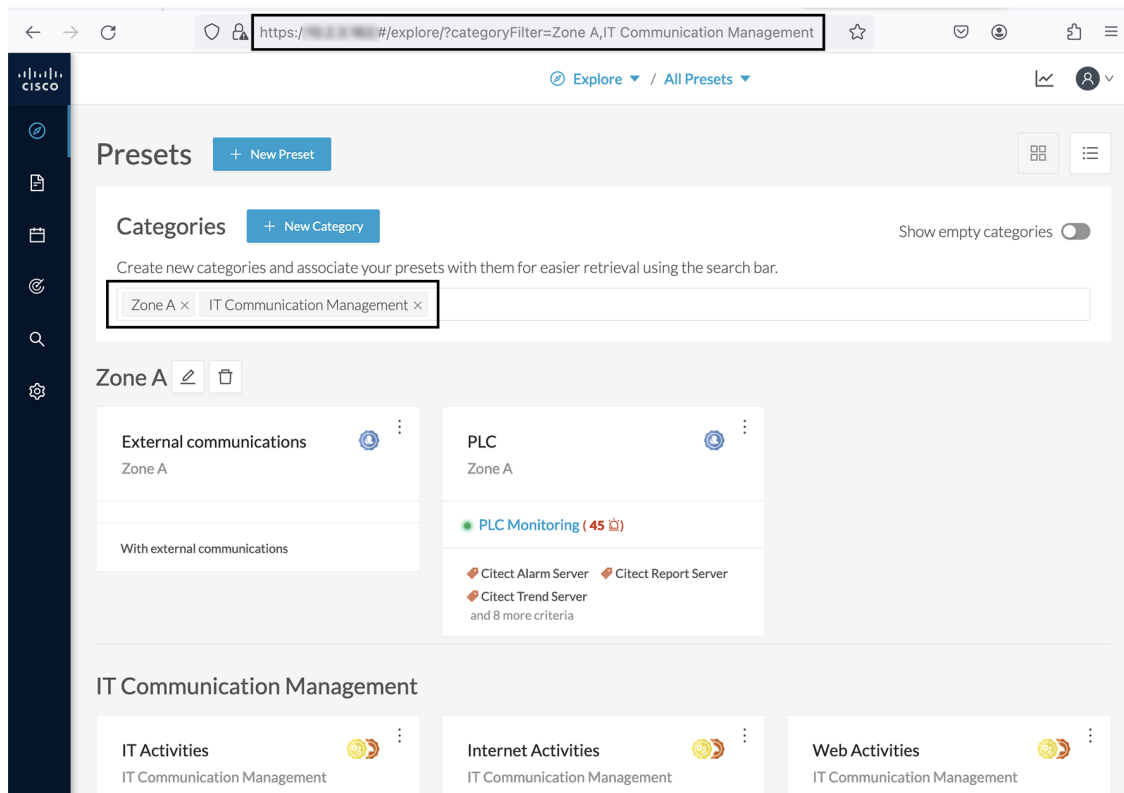
You can also filter presets by categories.



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.

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

The Preset name should not be the same as previously.

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

- 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."

DEVICE TAGS

- Devices without tags
- Device - Level 0-1
- Device - Level 2
 - Citect Alarm Server
 - Citect IO Server
 - Citect Report Server
 - Citect Trend Server
 - Controller (7)** (1)
 - Engineering Station
 - Master
 - Network Switch

Tags

Devices and components per tag	Count
Device - Level 2	7
Controller	7 (2)
Device - Level 3-4	1
Web Server	1 (3)
System	5
Rockwell Automation	5

For more details on these devices, switch to the [device list view](#) and access them using the filter available in the Tags column.

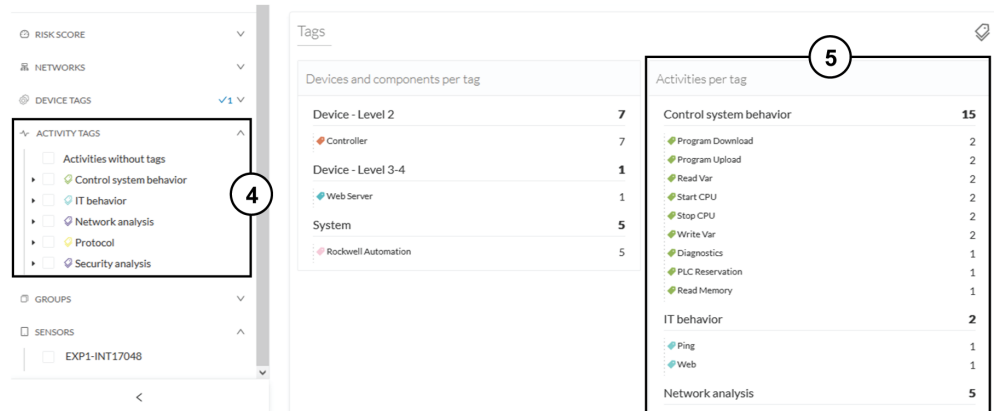
Device list

Last 1h (Jan 23, 2024 1:12:16 PM – Jan 23, 2024 2:12:16 PM) Refresh

21 Devices and 16 other components New data Export to CSV

Device	Risk score	External Communication	Tags	Activities
Broadcast ff:ff:ff:ff:ff:ff:ff:ff:ff:ff	-	No	No tags	40
192.168.49.50	-	No	No tags	1
192.168.49.33	25	No	HTTPS Client	4
192.168.49.65	-	No	Locally Administered MAC	1
sw.pot.esc1 24:6c:84:28:64:90 (other)	97	No	Network Switch, Cisco	4
LLDP/STP bridges Multicast 00:00:00:00:00:00	-	No	No tags	2
CDP/VTP/UDLD Multicast cc:cc:cc:cc:cc:cc	-	No	No tags	2
192.168.49.27	5	No	IPv6 Link Local, Locally Administered MAC	2
192.168.49.29	5	No	IPv6 Link Local, Locally Administered MAC	2
fe80::5054:ddff:fe65:2c4a	5	No	IPv6 Link Local, Locally Administered MAC	3

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

To access the **Activity list**, 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 **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.

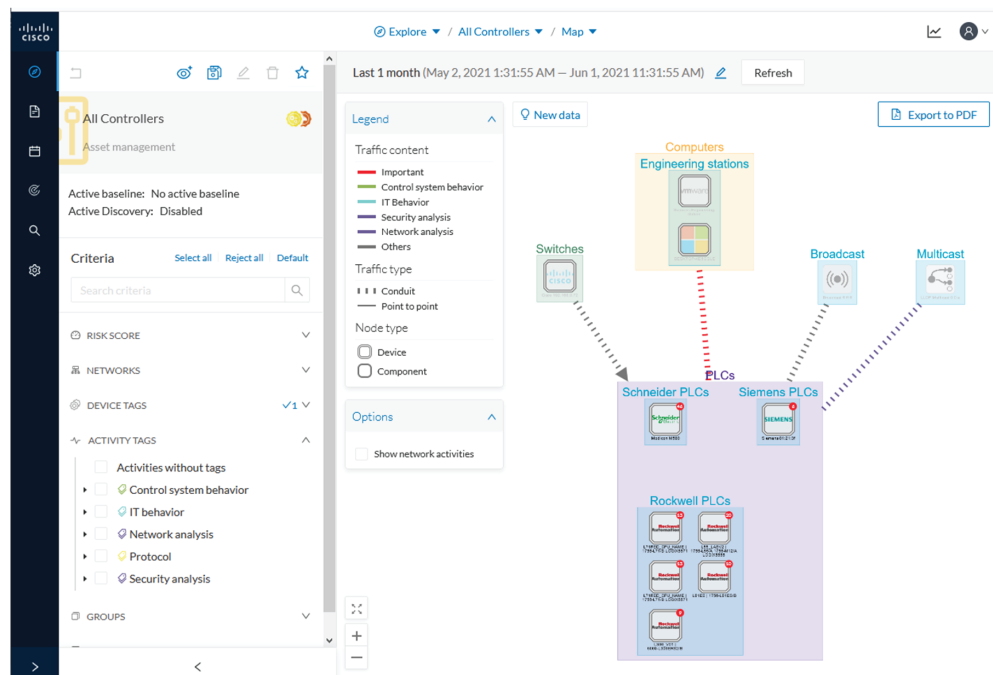
- Use the sort arrows to list data in alphabetical order or by ascending/descending order. Click again to cancel the sort.
- Use the filter icon opens a field to type specific data or a multiple-choice menu to filter tags.

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.

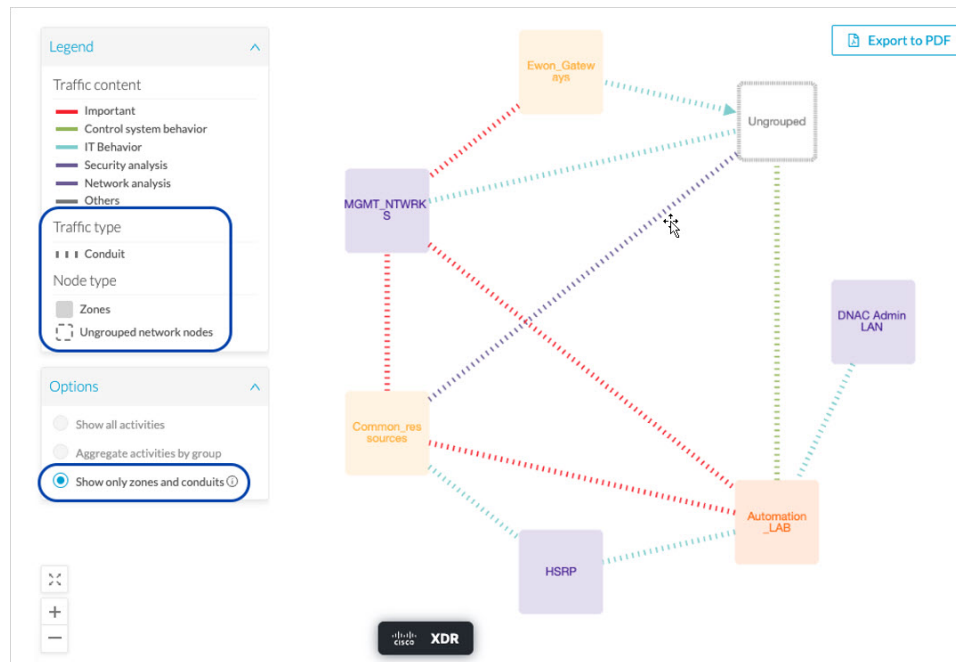
By default, activities between groups are merged and displayed as **conduits**. Select **Show network activities** for a more detailed view. To enhance visibility, elements here are also automatically reorganized on the **Map**.

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).

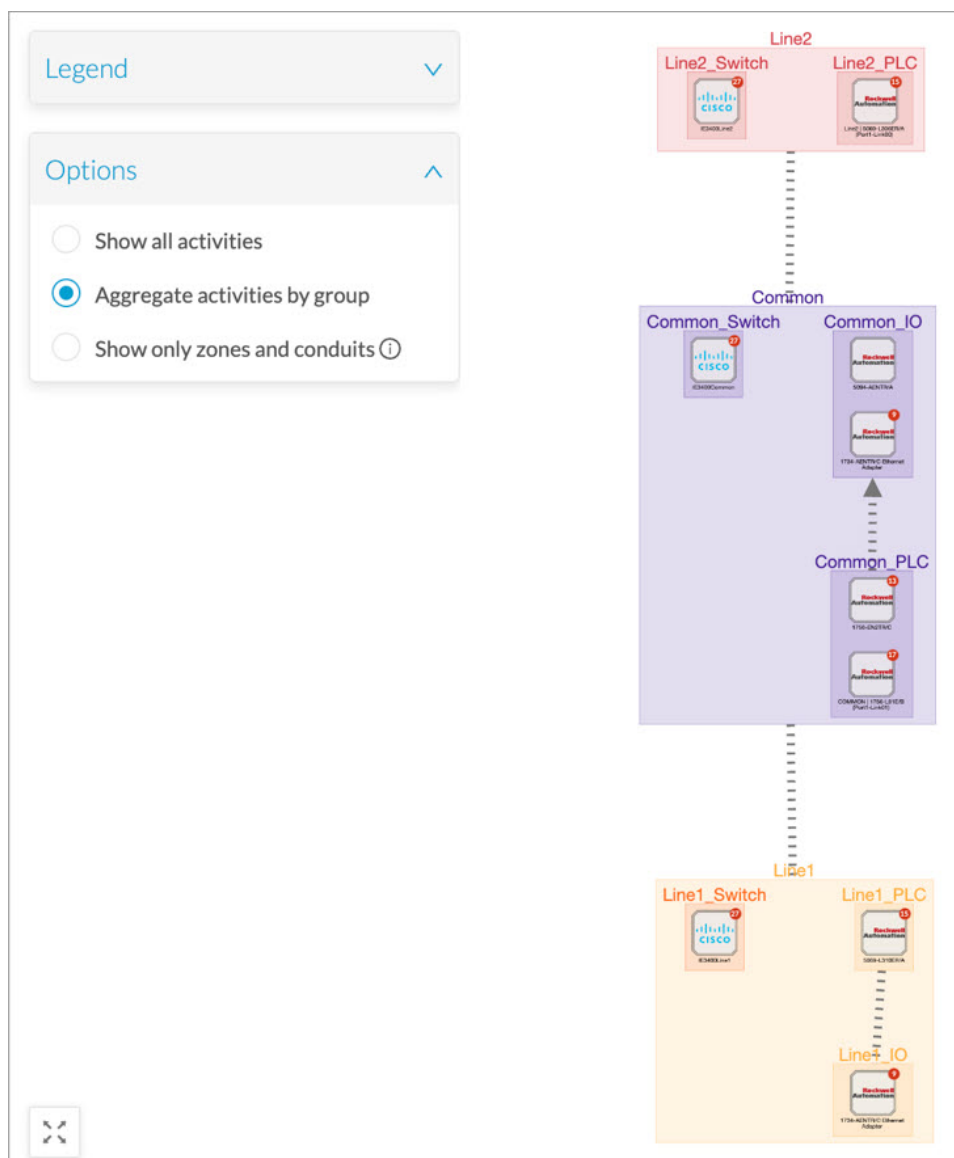
When a group hierarchy segments the control system, the new map option displays zones and conduits according to ISA/IEC 62443 standards.



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.

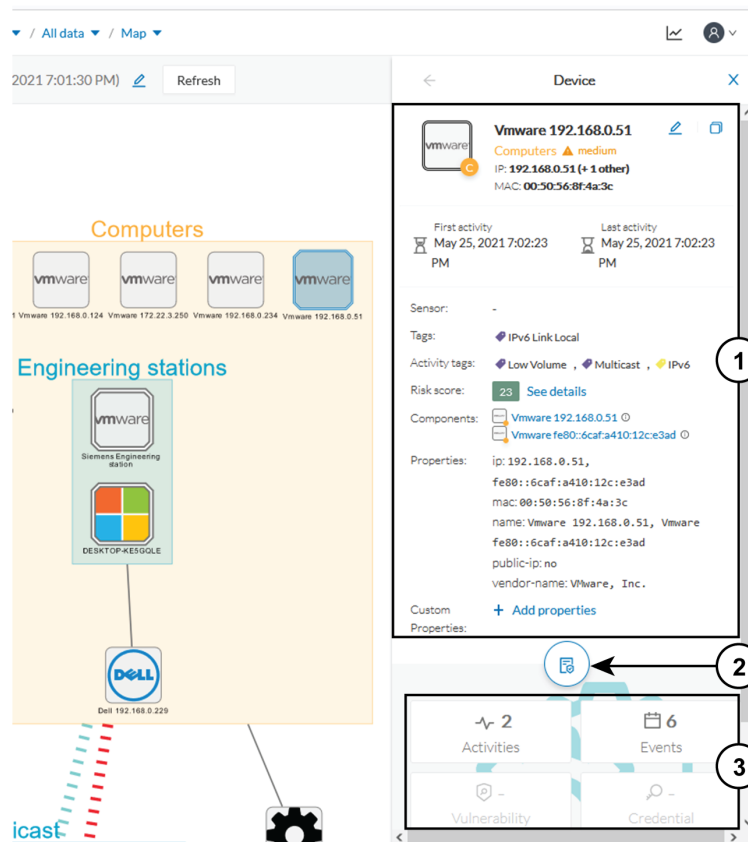
Assets of the preset All Controllers distributed among the layers of the Purdue model

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 and 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 activities, 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

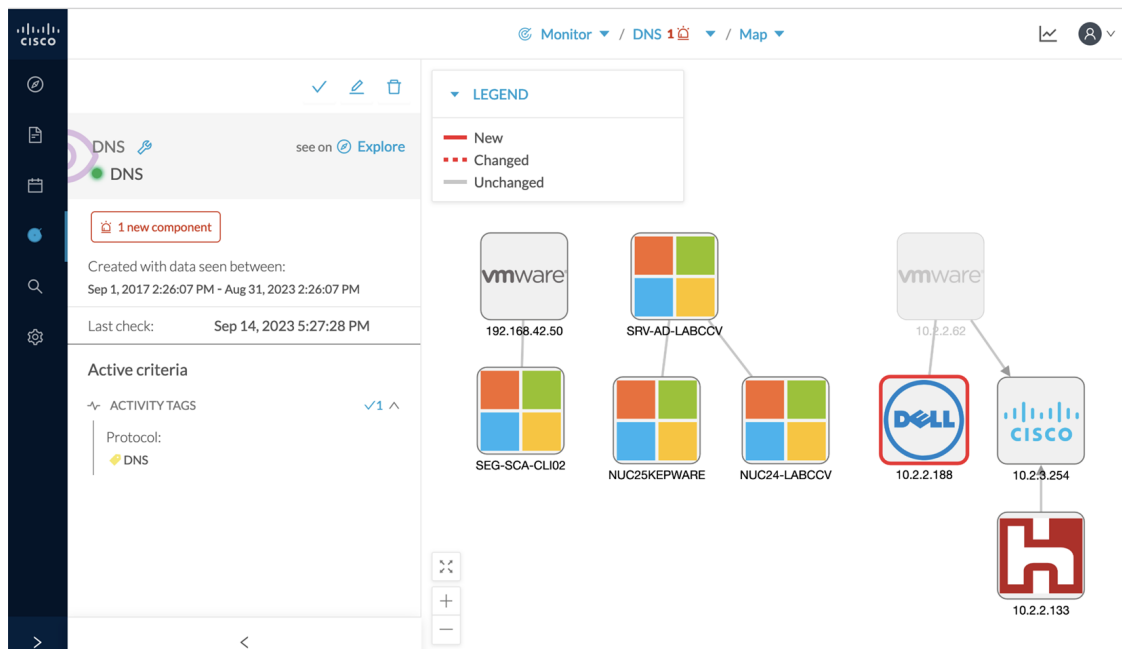
List is a chronological view in which you can see and search events. Use the search bar to find events by MAC and IP addresses, component name, destination and source flow, severity and category. You can search the Events on **Day**, **Week**, **Month** or **Year**. Use the arrows for exact dates.

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.

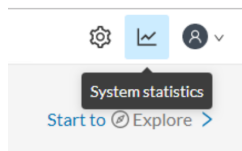
To search, enter the content in the search field and click **Search**.

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.

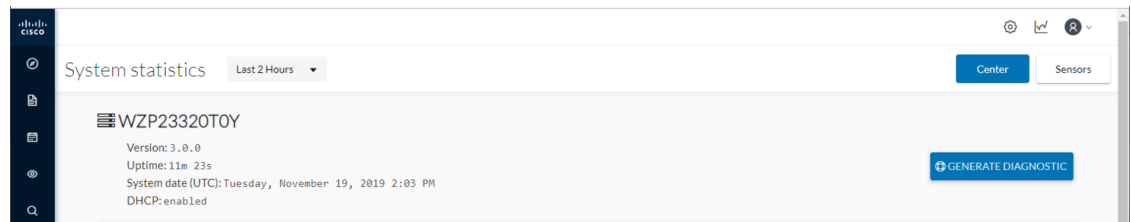


Center

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



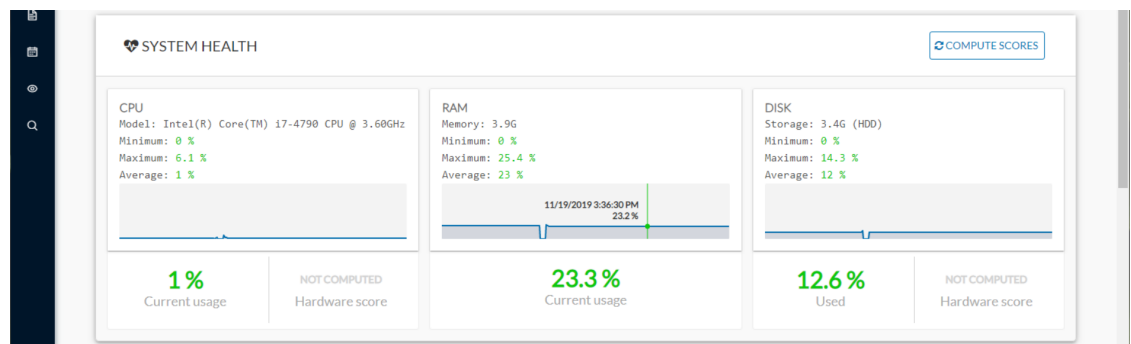
Note Use the drop-down arrow to change the time period.



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 product support.

System Health



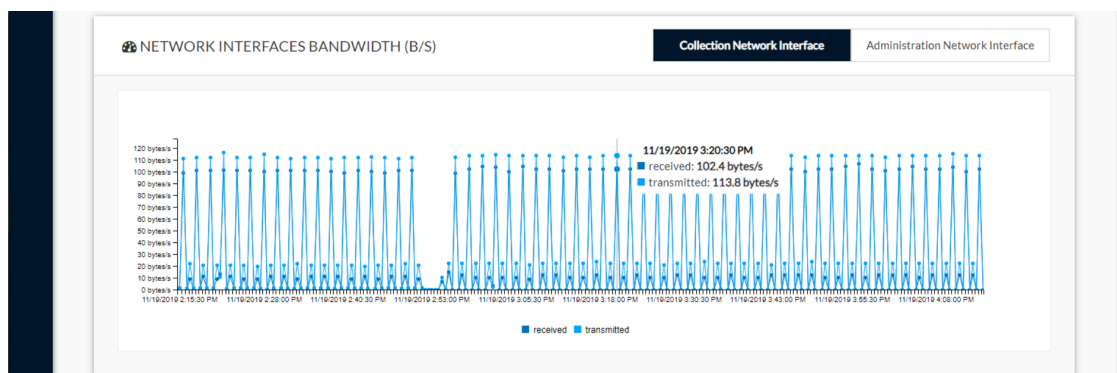
System health shows the status of the Center CPU, RAM and disk usage.

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.

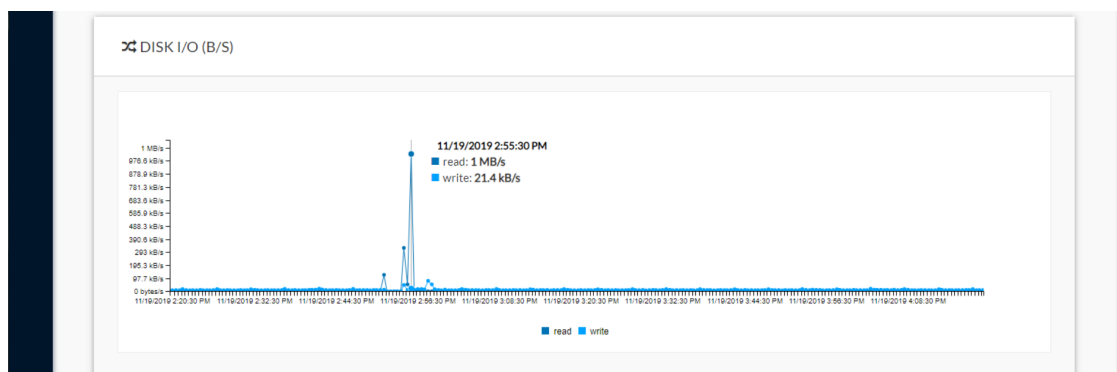
Network Interfaces Bandwidth



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

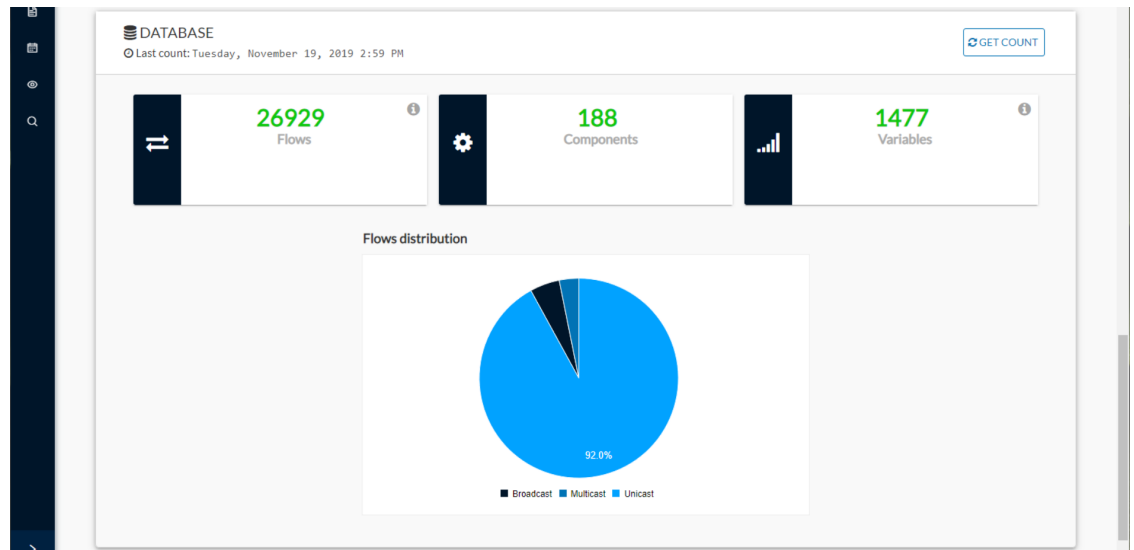
For example, the Collection Network interface activity lets you see the amount of data exchanged between the Center and the sensors.

Disk I/O



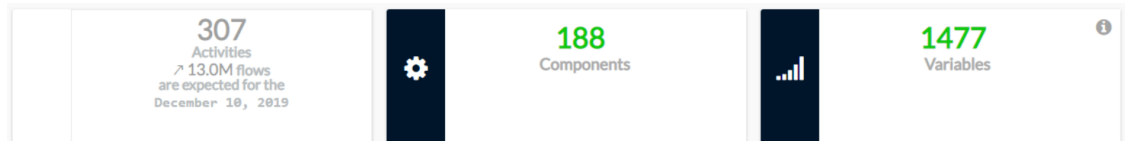
The line chart represents the Center hard disk usage in bytes/second.

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.

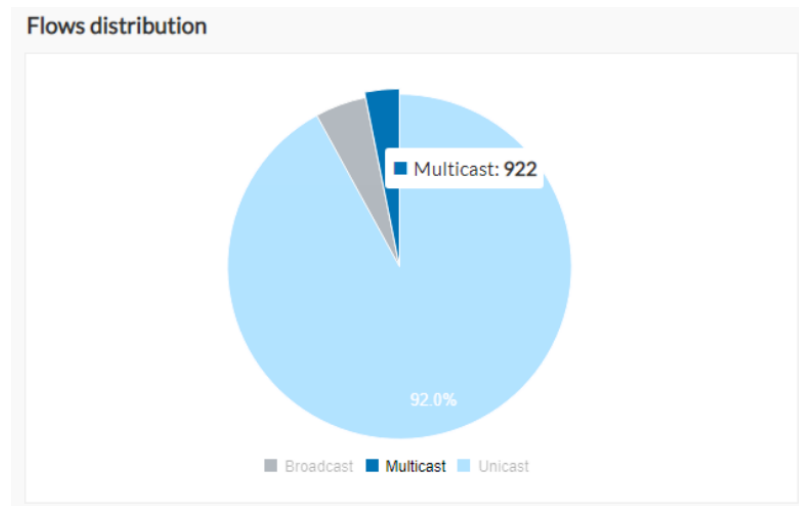


The flows card indicates the total number of flows (i.e. broadcast, multicast and unicast which are stored in the database) detected by . If you mouse over the card, you will get the number of activities and the flows evolution tendency. This information enables you to anticipate how the system load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

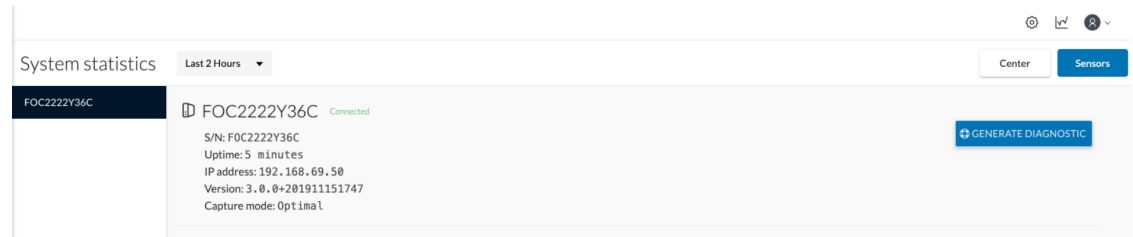
A list of congested queues will be provided to indicate system performance issues. A warning banner appears at the top of the application when a queue is congested, with the queue name highlighted in red.

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.

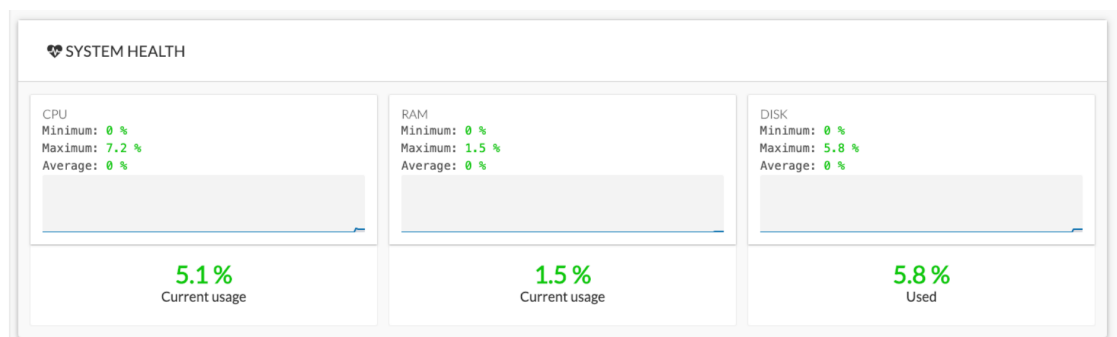
The **Sensors** statistics view shows general information about the sensor: the status (i.e., Connected), serial number, IP and MAC addresses, firmware version, the capture mode set, and the time it has been operating (i.e., uptime).

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

System Health

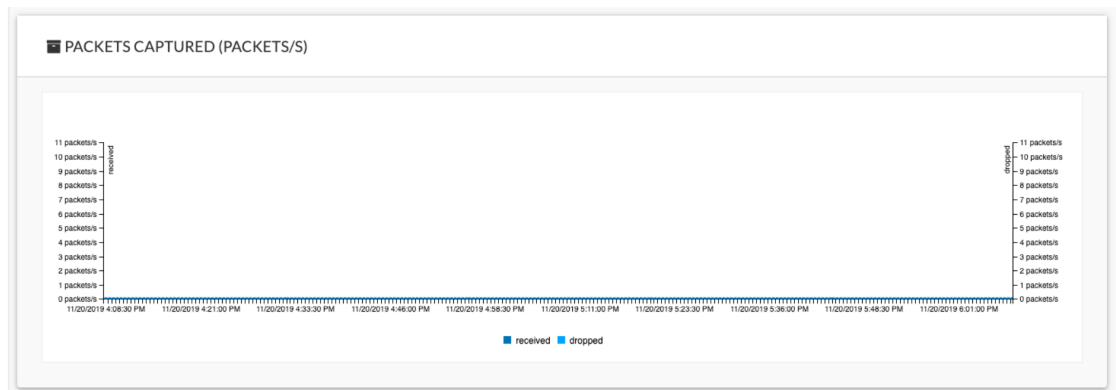
System health shows the status of the sensor CPU, RAM and disk usage.

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

$\text{Risk} = \text{Impact} \times \text{Likelihood}$

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 activities 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.

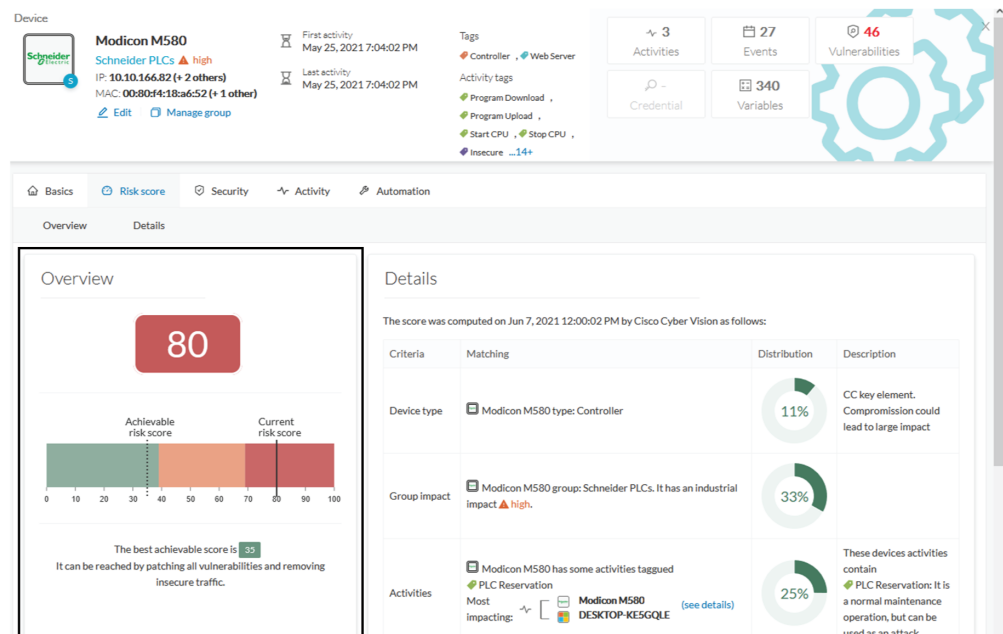
The right-side panel appears.

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

The technical sheet appears.

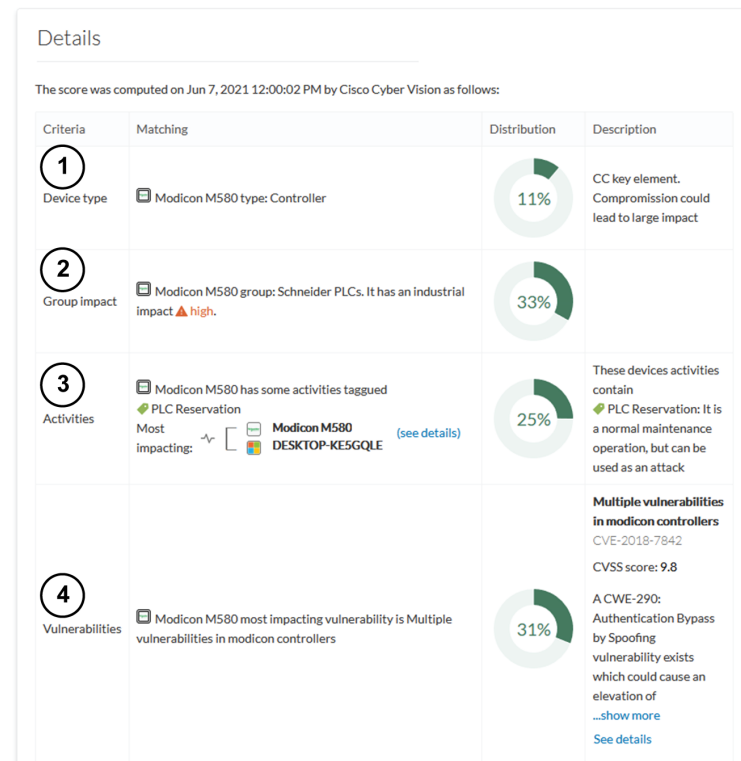
In the **Overview** tab, the **Current** risk score and the **Achievable** risk are displayed.

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.



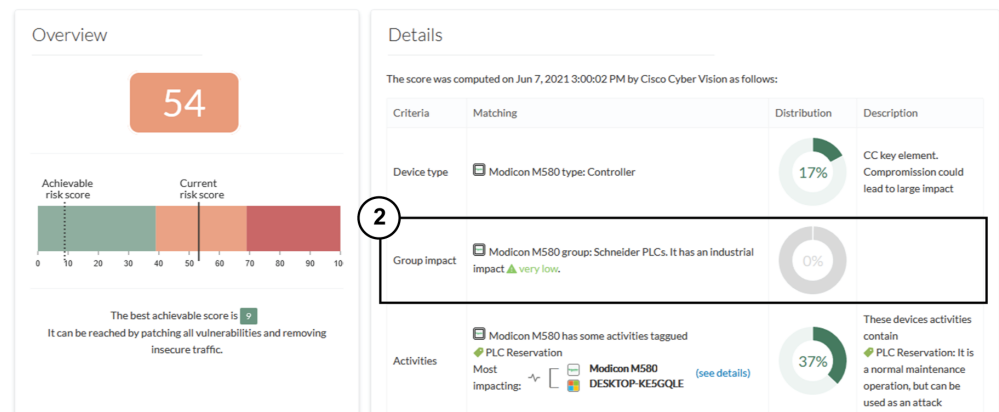
This page shows the last time the risk score was computed by Cisco Cyber Vision. Risk score computation occurs once an hour. To force immediate computation, use the following command on the Center shell prompt:

```
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.

Details

The score was computed on Jun 7, 2021 12:00:02 PM by Cisco Cyber Vision as follows:

Criteria	Matching
Device type	Modicon M580 type: Controller
Group impact	Modicon M580 group: Schneider PLCs. It has an industrial impact ▲ high.
Activities	Modicon M580 has some activities tagged PLC Reservation Most impacting: Modicon M580 DESKTOP-KE5GQLE (see details)
Vulnerabilities	Modicon M580 most impacting vulnerability is Multiple vulnerabilities in modicon controllers

Vulnerability

CVSS score v2: 9.8

Multiple vulnerabilities in modicon controllers

Identifier: CVE-2018-7842

Description: A CWE-290: Authentication Bypass by Spoofing vulnerability exists which could cause an elevation of privilege by conducting a brute force attack on Mo... [show more](#)

Solution: The vulnerabilities described in this document are linked to weaknesses in the management of Modbus protocol. Products with no fix available can be mi... [show more](#)

Published on: May 14, 2019

Links: [Schneider](#)

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 74](#)
- [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: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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 specific 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 80](#)
- [Center Web Server Certificate, on page 83](#)

Certificate Fingerprint

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

For more information, refer [the Centers Installation Guides](#).

Data Management

The **Data Management** interface allows you to do the following: manage data stored on Cisco Cyber Vision by [clearing data](#) 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 [Clear data](#) page or from the Command Line Interface (CLI), using the following command. Also, different options are offered.

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

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

- Events after 6 months
- Flows after 6 months
- Variables after 2 years

**Important**

You have 3 days once the migration from 3.2.x to 4.0.0 is done to set [expiration settings](#) as needed, before the default settings are applied by the system.

Clear Data

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

- All data
- Components selection and associated data. See [Purge components in Cisco Cyber Vision, on page 78](#).
- Activities, Flows, and Variables
- Flows and Variables
- Variables

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

Clear the data carefully. Clearing any data can impact monitoring of the network. Read the implications about all following data clearance.

Data Clearance: If database overload issues occur, clear all data as a final option. This action deletes the entire database content. It removes network data like components, flows, events, and baselines from Cisco Cyber Vision and leaves the GUI empty. Your configurations, like capture modes, event severity setup, and syslog configurations, stay intact.

Purge components in Cisco Cyber Vision

Each component represents an object in the industrial network, such as:

- Network interface of a PLC
- PC
- SCADA station
- Broadcast address
- Multicast address

The system limits the number of components stored in the database to ensure protection.

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

You can manually purge components and devices by providing the selection criteria. Once you provide the criteria, the system identifies and purges the matching components and related devices. The system then sends a request to synchronize with the global center.

Before you begin

Ensure that you have Admin access to proceed.

Procedure

Step 1 Open the main menu and select **Admin > Data Management > Clear Data**.

Step 2 Select **Components selection**.

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

Step 4 To proceed, enter the required details:

- **IP Subnet** (optional)

- **VLAN ID** (optional)

Note

You can pass only one VLAN ID at a time.

- **Inactivity since date** (optional)

- **Creation Start Time** (optional), and

- **Creation End Time** (optional).

Step 5 To proceed, click **Clear data**, and then click **Yes, remove** to confirm the action.

After you clear the data, go to **Explore > All Data** to see the updated Devices count.

Expiration Settings

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

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



Note

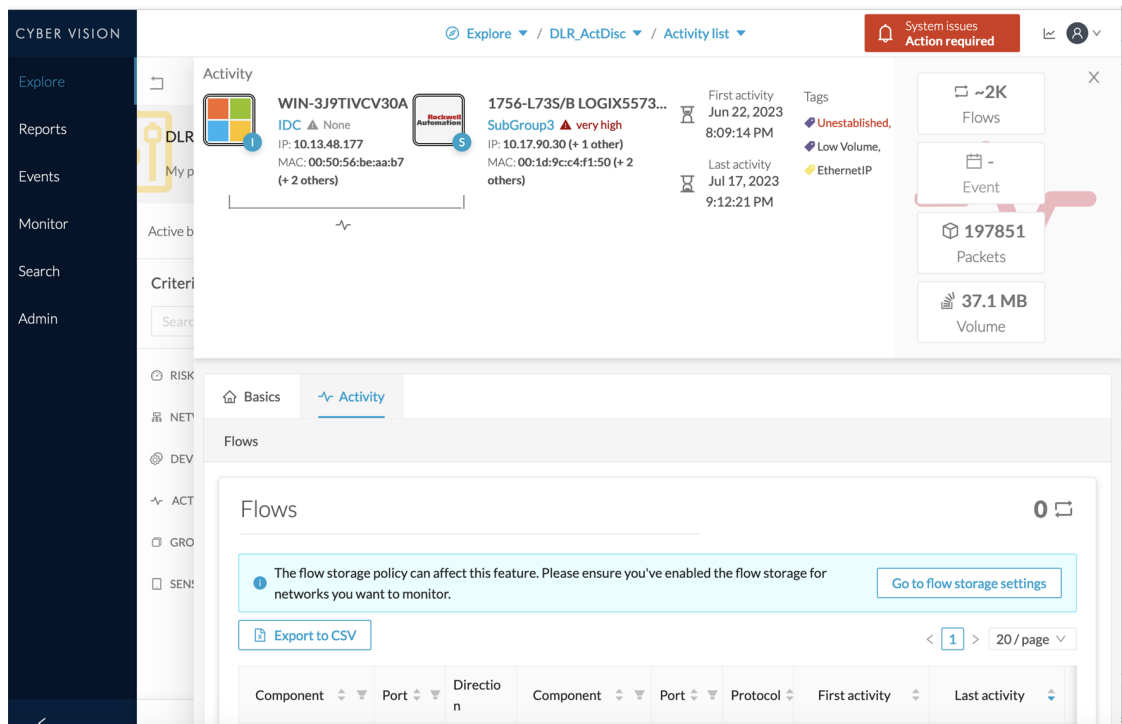
Selecting a high value may rapidly fill up storage and adversely affect system performance. The recommended value is 10 versions.

Ingestion Configuration

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

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

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



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

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

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

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

Users

Management

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

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

- **Admin**

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

- **Product**

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

- **Operator**

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

- **Auditor**

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

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

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

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

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

- Must contain a lower case character: a-z.
- Must contain an upper case character: A-Z.
- Must contain a numeric character: 0-9.
- Cannot contain the user id.
- Must contain a special character: ~!"#\$%&'()*+,-./:;<=>?@[]^_{}.



Important

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

Passwords' lifetime is defined in the [Security settings 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 roles

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

Procedure

-
- Step 1** From the main menu, choose **Admin > Users > Role Management**.
- Step 2** Click the + button at the end of listed navigation tabs.
A **NEW ROLE** tab appears.
- Step 3** Enter a **Role Name** and **Role Description** in their respective fields.
- Step 4** Click the drop-down arrow from the **Search/Add existing permission** field.
- Step 5** Select an existing role from the drop-down list, or click **Add New Permissions** to build the new user role from scratch.
- Step 6** In the **Classic Mode Permissions** drop-down list, check the checkboxes to select or deselect permissions from the list as read or write.
By default, **Explore** is enabled with read permission.
- Step 7** In the **Beta Mode Permissions** drop-down list, check the checkboxes to select or deselect permissions from the list as read or write.
- Note**
The **Beta Mode Permissions** drop-down list is enabled, only if the **Cisco Cyber Vision beta** is enabled for a center. See [Dashboard, on page 142](#) for more information.
- Step 8** Click **Save**.
A message **User role has been created successfully** appears.
The new user role is displayed in the tab list.
- Note**
You can modify or delete a role directly in the tab.
-

What to do next

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

Security Settings

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

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

Center Web Server Certificate

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

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

For more information, see to the corresponding [Center Installation Guide](#).



CHAPTER 5

Configure Cisco Cyber Vision

- [Network Organization](#), on page 85
- [API Token](#), on page 87
- [Active Discovery Policies](#), on page 91
- [LDAP](#), on page 91
- [Single Sign-On for Cisco Cyber Vision Center](#), on page 93
- [Sensors](#), on page 104
- [SNMP](#), on page 116

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.

Device engine options for this network range

☐ This IP range is deployed several time, the device engine will not use IP to group components into device.
 ☐ Do not group component seen by different sensors. For this IP range, the device engine will only use components from one sensor to create devices.

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
<input type="checkbox"/> 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 specifically set in the [Ingestion Configuration, on page 79](#) 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**.

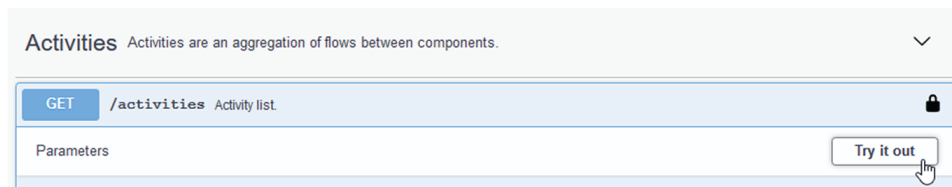
Close lockers displays. They indicate that routes are secured and authorization to use them is up.

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.

GET /activities Activity list.

Parameters

Name	Description
page integer (query)	pagination - the page number
Size integer (query)	pagination - the number of items per page

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.

Responses

Response content type: application/json

Curl

```
curl -X GET "https://10.2.3.161/api/3.0/activities?page=1&size=10" -H "accept: application/json" -H "x-token-id: ics-dc5a3eae44b3b9dee3f8358df10f3d40aa518396-e2647f7cb065663a9d2312141900af161301102e"
```

Request URL

```
https://10.2.3.161/api/3.0/activities?page=1&size=10
```

Server response

Code: 200

Details

Response body

```
[
  {
    "id": "e0c04e78-ef17-501a-b18c-f3df8325de9_e47c1b0-b420-5476-99da-bf16ac1abfd",
    "firstActivity": 1603194464591,
    "lastActivity": 1603869088976,
    "tags": [
      {
        "id": "CIP-10",
        "label": "CIP-10",
        "important": false,
        "category": {
          "id": "b1dd1dd-8e34-8afc-88e1-3fc32fdaf1a2",
          "label": "Protocol"
        }
      },
      {
        "id": "ENIP",
        "label": "ethernetIP",
        "important": false,
        "category": {
          "id": "b1dd1dd-8e34-8afc-88e1-3fc32fdaf1a2",
          "label": "Protocol"
        }
      }
    ]
  }
]
```

Response headers

```
content-security-policy: default-src 'self'; frame-ancestors 'none'; style-src 'self' 'unsafe-inline'; img-src 'self' data:
content-type: application/json
date: Thu29 Oct 2020 11:20:48 GMT
pagination_page_number: 1
pagination_page_size: 10
```

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 access 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 internal usage, it cannot be mapped to any external users and thus is not proposed in LDAP settings.

Testing LDAP connection:

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

Login in Cisco Cyber Vision:

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

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

Configure LDAP

This 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,

- Choose **LDAP over TLS/SSL** or **Use self signed certificate**, or neither.
- Enter **Primary Server Address**.
- Enter **Primary Server Port**.
- (Optional) Enter **Secondary Server Address**.
- (Optional) Enter **Secondary Server Port**.
- In the **Base DN** field, enter the distinguished name by which LDAP API recognize this LDAP connection.
- (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.

- 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.
- (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.
 - Enter a service account username.
 - Enter a service account password.
- 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,

- 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

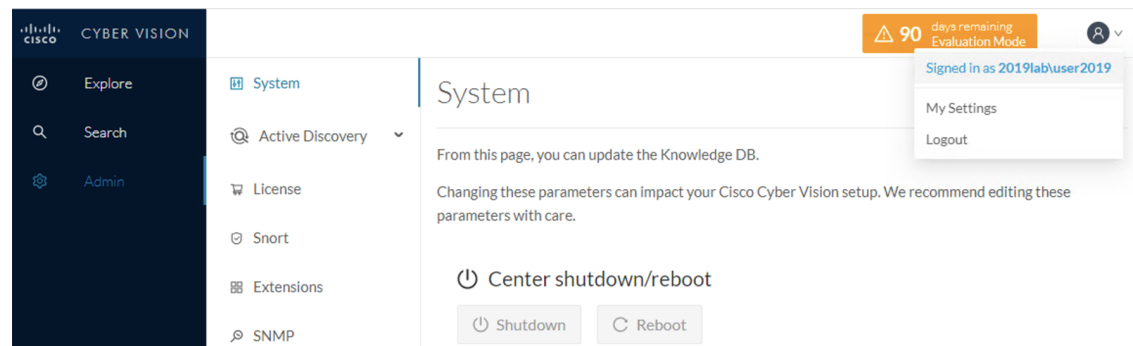
For LDAP, the supported username format is `<domain_name>\<user_name>` (For example, `cisco\john_doe`).

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 for Cisco Cyber Vision Center

A Single Sign-On (SSO) is an authentication process that:

- allows you to access multiple applications with one set of login credentials
- reduces the need for multiple logins and password management, and
- enhances security by centralizing authentication.

Central authentication and authorization

Central authentication and authorization are a security mechanism that uses a Central identity provider (IdP) to manage user credentials and access permissions across multiple platforms. This approach consolidates authentication strategies into a streamlined process, enhancing efficiency and security.

Federated service provider applications

The applications you set up for SSO are known as federated service provider applications.

Unified access for you

With SSO, you can log in just once to access all the service provider applications you are authorized to use without needing to re-enter credentials.

SAML single sign-on

Security Assertion Markup Language (SAML) is a security protocol that:

- allows users to authenticate once and gain access to multiple applications,
- uses identity providers (IdP) for authentication and authorization, and
- bypasses the need for login credentials for each service.

After successful authentication by the IdP, SSO users return to the Cisco Cyber Vision Center and log in. The browser handles communication between the Cisco Cyber Vision Center and the IdP, so the Cisco Cyber Vision Center does not need a direct network connection to the IdP.

SSO provider support

The Cisco Cyber Vision Center supports SSO with any SSO provider that uses the Security Assertion Markup Language (SAML) 2.0 standard for authentication and authorization.



Note The Cisco Cyber Vision Center does not sign SAML authentication requests. If the IdP requires signed authentication requests, SSO fails on the Cisco Cyber Vision Center.

SSO providers supported by the Cisco Cyber Vision Center

- Azure
- Cisco Duo

SSO guidelines for the Cisco Cyber Vision Center

Prerequisites

Only Admin users authenticated internally or through LDAP or RADIUS are authorized to configure SSO.

Limitations:

- No IdP-Initiated SSO: The Cisco Cyber Vision Center does not support SSO initiated from the IdP.
- No CAC Credentials: The Cisco Cyber Vision Center does not support logging in with CAC credentials for SSO accounts.
- No CC Mode: Do not configure SSO in deployments using CC mode.

Single SSO Provider Support:

The Cisco Cyber Vision Center supports only one SSO provider at a time, such as Azure or Duo.

SSO in high availability configurations:

- **Separate Configuration:** Configure SSO separately for each member of a high-availability pair, as they are not synchronized.
- **Same IdP Requirement:** Both members of the high availability pair must use the same IdP. You configure a service provider application at the IdP for each the Cisco Cyber Vision Center.

Multi-tenancy and SSO:

- **Global Domain Scope:**
 - In multi-tenancy setups, you apply the SSO configuration at the global domain level. This applies to the global domain and all subdomains.

Logging SSO activities:

Audit Logs: The Cisco Cyber Vision Center logs SSO activities, such as login and logout events, in the audit log. Each entry specifies 'Login' or 'Logout' in the Subsystem field.

Single Sign-On user accounts

A single sign-on (SSO) user account allows users to access multiple applications, systems, or services using one set of login credentials, such as a username and password. A central identity provider (IdP) handles the authentication, simplifying 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 or imports them from other applications like Active Directory, RADIUS, or LDAP. It establishes most account details for SSO users, including usernames and passwords.

SSO accounts on the Cisco Cyber Vision Center

SSO accounts appear on the Cisco Cyber Vision Center users page only after the user successfully logs in for the first time.

Email address requirement

Users for single sign-on (SSO) accounts and the NameID attribute sent by the identity provider (IdP) during SAML login must be valid email addresses. Many IdPs automatically use the username of the user attempting to log in as the NameID attribute. Confirm this behavior when configuring your IdP and creating user accounts for SSO access to the Cisco Cyber Vision Center.

Configurable account characteristics

You can configure these characteristics for SSO users from the Cisco Cyber Vision Center web interface:

- Real name
- Exempt from browser session timeout

User role mapping for SSO users

The Cyber Vision Center assigns the Security Analyst (Read Only) role to all SSO users by default. You can override the default role for specific users or groups using user role mapping.

At the Cyber Vision Center, you can configure role mapping based on either group permissions or individual user permissions.

- Test the SSO configuration.
- Define SSO user roles.

Coordination with the IdP

- Role assignment: Setting up user roles at the Cyber Vision Center and coordinating them with your SSO IdP application settings. Assign roles either to individual users or to groups defined in the IdP.
- Understanding your SSO federation: Understand your SSO federation organization of users, groups, and roles at the IdP to configure user role mapping effectively. For guidance on creating or importing users or groups in the IdP, consult the IdP vendor documentation.

Role attribute

- Role attribute at the IdP
 - The IdP maintains a role attribute for the Cyber Vision Center service provider application.
 - Each user or group accessing the Cyber Vision Center has a string or expression for this role attribute.
- SSO configuration details: The SSO configuration specifies the name of the role attribute and includes a list of expressions mapped to Cisco Cyber Vision Center user roles.
- Role matching: When you log in to the Cisco Cyber Vision Center using SSO, the system compares the role attribute value provided by your IdP (for a user or group) against expressions mapped to Cisco Cyber Vision Center roles. The Cyber Vision Center assigns all roles where the attribute value matches an expression.

Single Sign-On with Azure AD

Azure Active Directory (Azure AD) provides a multi-tenant, cloud-based identity and access the Cyber Vision Center through Microsoft Azure. Within Azure, a tenant represents the entity that includes all federated devices a user can access with a single SSO account.

Familiarize yourself with the Azure tenant organization before adding the Cyber Vision Center.

Add an enterprise application for Azure

To add an enterprise application to your tenant, use these steps:

Before you begin

- You require an Azure account with an active subscription. Create a free account at https://azure.microsoft.com/en-us/pricing/purchase-options/azure-account?icid=azurefreeaccount&WT.mc_id=A261C142F.
- The Azure account requires at least the "Application Developer" role.

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 . |
| Step 4 | Select Create your own application . |
| Step 5 | Enter the name in the Input name field. |
| Step 6 | Click Create . |
-

What to do next

You configure this newly created enterprise application. See [Configure the management center service provider application for Azure](#).

Configure the Cyber Vision Center service provider application for Azure

Before you begin

- Create the Cyber Vision Center service provider application:
 - Create the Cyber Vision Center service provider application within your Azure Active Directory tenant, and set up basic configuration settings. See [Add an enterprise application for Azure](#).
- Prepare your Microsoft Azure tenant:
 - Familiarize yourself with your Azure tenant and its users and groups. See [Single Sign-On with Azure AD](#).
 - If needed, create user accounts or groups in your Azure tenant and assign them one of these roles: Cloud Application Administrator or Application Administrator.
 - The hostname must be a resolvable DNS entry.
- Configure your IdP:
 - Ensure that SSO account usernames and the NameID attribute are valid email addresses during SAML login to the Cyber Vision Center. Verify if your IdP uses the username as the NameID attribute and confirm the login URL for the Cyber Vision Center.
- Groups and individual users:

- If you assign user groups to the Cyber Vision Center application, do not assign users within those groups as individuals.
- Role mapping:
 - Role mapping in the Cyber Vision Center for SSO is limited to one attribute. You must choose either user role mapping or group role mapping and configure a single attribute to pass user role information to the Cyber Vision Center.



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 the <https://entra.microsoft.com/#home>.
- Step 2** From the main menu, choose **Applications > Enterprise applications > All applications**.
- Step 3** Select the created application.
See [Add an enterprise application for Azure](#).
- Step 4** Click on **Single sign-on** and select **SAML**.
- Step 5** Select **Edit** in the **Basic SAML Configuration** section.
- Step 6** Enter **Identifier (Entity ID)** and **Reply URL (Assertion Consumer Service URL)**.
- **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 7** Select **Edit** in the **Attributes & Claims** section.
- Click **groups** under **additional claims**.
 - Select the groups user is associated with.
 - Check the checkbox of **Customize the name of the group claim**.
 - Add **Name (required)**.
 - Click **Save**.
- Step 8** Assign existing Azure users and groups to the Cyber Vision Center service application.
- Step 9** Note **SAML-Based Sign-On** information.
- **Login URL**
 - **Logout URL**

- Download the **Certificate (Base64)** file
- **Object ID** from Users and groups
- **Microsoft Entra Identifier**
- Download **Federation Metadata XML**



Note If you assign user groups, do not assign users within those groups as individuals.
User role mapping options: individual user permissions or group permissions (not both).

What to do next

See [Configure the Cyber Vision Center for Azure SSO](#).

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 [Add an enterprise application for Azure](#) and [Configure the management center service provider application for Azure](#).

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 the **Name (Required)**. See [Configure the management center service provider application for Azure](#) to get the **Name (Required)**.
- Step 4** Complete the configuration using one of these methods:
- Upload the **Federation Metadata XML** file under the **Upload XML file** field.
See [Configure the management center service provider application for Azure](#) to get the file.
 - For **Manual Configuration**:
 - Enter the **Login URL** in the **Identity Provider Single Sign-On (SSO) URL** field. See [Configure the management center service provider application for Azure](#) to get the **Login URL**.
 - Enter the **Microsoft Entra Identifier** in the **Identity Provider (Idp) Issuer URL** field. See [Configure the management center service provider application for Azure](#) to get the **Microsoft Entra Identifier**.
 - Add the **Certificate (Base64)** in the **X509** field. See [Configure the management center service provider application for Azure](#) to get the **Certificate (Base64)**.

Step 5 Enter the details, then select the **Role Mapping** tab.

Step 6 Enter **Object ID** in the **Default roles** field.

See [Configure the management center service provider application for Azure](#) to get the **Object ID**.

Step 7 Click **OK**.

Duo Single Sign-Ons for generic SAML service providers

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

- 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)

Cisco 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 (AD) or any SAML 2.0 IdP and requires two-factor authentication before granting access to the application of service providers.

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 policies for SSO applications based on their plans. For example, some applications may enforce two-factor authentication at every login, while others may limit login frequency 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

- A Duo Admin access with the Owner, Administrator, or Application Manager role.
- Active Directory or a Security Assertion Markup Language (SAML) 2.0 identity provider that can be used as your primary authentication source for Duo Single Sign-On (SSO).
 - You must complete all Duo Single Sign-On (SSO) authentication source setup steps separately from the directory sync setup.
- If you are using Active Directory, you need:

- At least one standalone server (Windows or Linux) that can communicate with your Active Directory domain controllers.
 - Service account credentials for Active Directory.
 - Access DNS for the user email domains associated with Single Sign-On to add TXT records.
- A Security Assertion Markup Language (SAML) 2.0 service provider or OpenID Connect (OIDC) relying party web application to protect with Duo Single Sign-On (SSO).

Add authentication source for Duo

Before you begin

You must have the owner role to add an authentication source.

Procedure

-
- Step 1** Log in to the [Duo Admin Panel](#).
- Step 2** From the main menu, choose **Applications > SSO Settings**.
- Step 3** Go to **External authentication sources**, and click **Add source**.
- Step 4** On the **Add Authentication Source** page, select an authentication source:
- Active Directory
 - SAML Identity Provider

Note

Once you add an authentication source, the system prompts you to **add an Authentication Proxy**.

What to do next

Create the SP application in Duo once your SSO source is operational.

Create cloud application in Duo

Duo's two-factor authentication system binds to your services or platforms, such as a cloud-hosted application, VPN, CMS, email system, or hardware device. Protect as many applications as needed and administer each one independently.

Before you begin

You first [sign up for a Duo account](#).

The required role to perform this task is Owner, Administrator, or Application Manager.

Procedure

-
- Step 1** Log in to the [Duo Admin Panel](#).
- Step 2** From the main menu, choose **Applications > Application Catalog**.
- Step 3** Click **Add application**. Then, click **Application**.
-

Configure the Cyber Vision Center service provider application for Duo

Before you begin

Before configuring your service provider application, you must configure a working authentication source.

Procedure

-
- Step 1** Log in to the [Duo Admin Panel](#).
- Step 2** From the main menu, choose **Applications > Application Catalog**.
- Step 3** Find the "SSO" labeled **Generic SAML Service Provider** in the catalog.
- Step 4** Click the **Documentation** link to review integration requirements and steps before adding the new application.
- Step 5** Click + **Add** to start configuring **Generic SAML Service Provider**.

Note

Users cannot access new applications until access is granted.

- Step 6** Enter **Entity ID** and **Assertion Consumer Service (ACS) URL**.
- **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 provides SAML identity provider details for Duo Single Sign-On.

Name	Description
Entity ID	The global, unique name for Duo Single Sign-On. Sometimes referred to as "Issuer."

Name	Description
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.
Single Log-Out URL	The logout URL for Duo Single Sign-On. This is sometimes referred to as "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 the Download Certificate button to download a crt file.
SAML Metadata	Service providers use the XML SAML Metadata to configure settings from Duo Single Sign-On. Click the Download XML button to download a xml file.

Step 7 Click **Save**.

Add user in service provider application

Procedure

- Step 1** Log in to the [Duo Admin Panel](#).
- Step 2** From the main menu, choose **Users**.
- Step 3** Click **Add User**.
- Step 4** Enter these details:
- **Username**
 - **Display Name**
 - **Email Address**

Step 5 Click **Add User**.

Configure the Cisco Cyber Vision Center for Duo

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 the **Name (Required)**. See [Configure the management center service provider application for Duo](#) to get the **Name (Required)**.

Step 4 Complete the configuration using one of these methods:

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

See [Configure the management center service provider application for Duo](#) to get the file.

b. For **Manual Configuration**:

- Enter the **Login URL** in the **Identity Provider Single Sign-On (SSO) URL** field. See [Configure the management center service provider application for Duo](#) to get the **Login URL**.
- Enter the **Microsoft Entra Identifier** in the **Identity Provider (Idp) Issuer URL** field. See [Configure the management center service provider application for Duo](#) to get the **Microsoft Entra Identifier**.
- Add the **Certificate (Base64)** in the **X509** field. See [Configure the management center service provider application for Duo](#) to get the **Certificate (Base64)**.

Step 5 Enter the details, then select the **Role Mapping** tab.

Step 6 Enter **Object ID** in the **Default roles** field.

See [Configure the management center service provider application for Duo](#) to get the **Object ID**.

Step 7 Click **OK**.

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 these 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 109](#).
- 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 sensor, follow these steps:

- From the main menu, choose **Admin > Sensors > Sensor Explorer**.
- Click the sensor that is upgradeable 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 > Sensors > 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 1: Sensor applicability and correspondance table per deployment file

Sensors	Deployment files
IE3x00, IR1101, IR18xx, IE9300	cviox-aarch64.tar
IE3x00, IR1101, IR18xx, IE9300 with Active Discover	cviox-active-discovery-aarch64.tar
IC3000	cviox-ic3000-x86-64.tar
IC3000 with Active Discovery	cviox-active-discovery-x86-64.tar

Sensors	Deployment files
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:

- Enter a name for the deployment phase.
- Add the **Number of uses** for the number of devices to be deployed.
- Set the token's **Expiration time**.
- 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.

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

Step 7 Click **Save Configuration**.

SNMP MIB

Table 2:

MIB	OID prefix	Description
MIB-2	.1.3.6.1.2.1.1	System
IF-MIB	.1.3.6.1.2.1.2.2.1.1	All physical interfaces
IF-MIB	.1.3.6.1.2.1.31.1.1	All physical interfaces
HOST-RESOURCES-MIB	.1.3.6.1.2.1.25.1	System

MIB	OID prefix	Description
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

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 screenshot shows the Cisco Cyber Vision GUI with the 'Device List' view selected. The left sidebar contains navigation options like 'Criteria', 'RISK SCORE', 'NETWORKS', 'DEVICE TAGS', 'ACTIVITY TAGS', 'GROUPS', and 'SENSORS'. The main area displays a table of 14 devices and 16 other components. The XDR ribbon is visible at the bottom of the table.

Device	Group	First activity	Last activity	IP	MAC	Risk score	External Communication
192.168.28.10	VLAN NAT2	Oct 4, 2023 10:53:21 AM	Apr 5, 2024 10:44:12 AM	192.168.28.10	ac:64:17:06:cb:47 (+ 1 other)	64	No
Siemens dc-b4-4f	VLAN NAT2	Oct 4, 2023 10:53:21 AM	Apr 5, 2024 10:44:12 AM	-	ac:64:17:06:cb:47	35	No
CPUName_L306_NAT1 5069-L306ER/A	VLAN NAT1	Oct 4, 2023 10:53:21 AM	Apr 5, 2024 10:44:12 AM	192.168.28.20	5c:88:16:ae:75:79	70	No
5094-AENTRA	VLAN NAT1	Oct 4, 2023 10:53:21 AM	Apr 5, 2024 10:44:12 AM	192.168.28.32	5c:88:16:c9:a6:3a	35	No
192.168.28.10	VLAN NAT1	Oct 4, 2023 10:53:21 AM	Apr 5, 2024 10:44:12 AM	192.168.28.10	ac:64:17:06:cb:47 (+ 1 other)	64	No
nat1xblakxsiemens0c3	VLAN NAT1	Oct 4, 2023 10:53:21 AM	Apr 5, 2024 10:44:12 AM	-	ac:64:17:06:cb:47	35	No
CPUName_L306_NAT1	VLAN NAT1	Oct 4, 2023 10:53:21 AM	Apr 5, 2024 10:44:12 AM	192.168.28.10	ac:64:17:06:cb:47	64	No

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:

The screenshot shows the 'Find Observables' dialog box overlaid on the device list table. The dialog box has a search bar and a list of observables. The 'Observables on Page' section shows 26 All, 0 +, 0 -, 0 0, 26 U. The 'Add 26 Observables to Case' and 'Run Investigation' buttons are at the bottom.

Device	Group	First activity	Last activity	IP
192.168.28.10	VLAN NAT2	Oct 4, 2023 10:53:21 AM	Apr 5, 2024 10:44:12 AM	192.168.28.10
Siemens dc-b4-4f	VLAN NAT2	Oct 4, 2023 10:53:21 AM	Apr 5, 2024 10:44:12 AM	-
CPUName_L306_NAT1 5069-L306ER/A	VLAN NAT1	Oct 4, 2023 10:53:21 AM	Apr 5, 2024 10:44:12 AM	192.168.28.20
5094-AENTRA	VLAN NAT1	Oct 4, 2023 10:53:21 AM	Apr 5, 2024 10:44:12 AM	192.168.28.32
192.168.28.10	VLAN NAT1	Oct 4, 2023 10:53:21 AM	Apr 5, 2024 10:44:12 AM	192.168.28.10
nat1xblakxsiemens0c3	VLAN NAT1	Oct 4, 2023 10:53:21 AM	Apr 5, 2024 10:44:12 AM	-
CPUName_L306_NAT1	VLAN NAT1	Oct 4, 2023 10:53:21 AM	Apr 5, 2024 10:44:12 AM	192.168.28.10

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:

Time	Severity	Category	Description
October 17, 2023 10:03:42 AM	critical	Control Systems Events	Init has been detected from 192.168.28.10 (VLAN NAT1) (@ 192.168.28.10) IP: 192.168.28.10 MAC: ac:64:17:f0:8aa9 to nat1xbioxbsiemens0c38 (VLAN NAT1) (@ nat1xbioxbsiemens0c38) IP: 192.168.28.30 MAC: ac:64:17:eb:4af3

source

192.168.28.10

SIEMENS

→

destination

nat1xbioxbsiemens0c38

SIEMENS

Flow

Flow information unavailable

Source component

Device: @ 192.168.28.10
Name: 192.168.28.10
MAC: ac:64:17:f0:8aa9
IP: 192.168.28.10
Tags: Controller Web Server
Vulnerabilities detected: 11

Destination component

Device: @ nat1xbioxbsiemens0c38
Name: nat1xbioxbsiemens0c38
MAC: ac:64:17:eb:4af3
IP: 192.168.28.30
Tag: IO Module

Report to XDR

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.

Component

SIEMENS

nat1xb1515.profinetxainterf ace319a

192.168.28.10

VLAN NAT1

IP: -

MAC: ac:64:17:f0:8a:ab

Edit

Investigate in Cisco XDR

First activity

Oct 4, 2023 10:53:21 AM

Last activity

Apr 5, 2024 10:57:42 AM

Tags

Controller

Activity tags

Multicast

Link Layer Discovery Protocol

Profinet

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



CHAPTER 7

Maintain and Monitor Cisco Cyber Vision

- [Monitored presets, on page 125](#)
- [Center Shutdown/Reboot, on page 131](#)
- [Upgrade with a Combined Update File, on page 131](#)
- [Configure syslog, on page 133](#)
- [Import/Export, on page 134](#)
- [Knowledge DB, on page 134](#)
- [Certificate Fingerprint, on page 135](#)
- [Cisco Cyber Vision Telemetry, on page 135](#)
- [Reset to Factory Defaults, on page 135](#)
- [Snort, on page 136](#)
- [Risk Score, on page 140](#)
- [Extensions, on page 140](#)

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 129](#)

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 3: Default presets available in Cisco Cyber Vision Center

Preset category	Presets available
Basics	<ul style="list-style-type: none"> • All data • Essential data • Active Discovery activities
Asset management	<ul style="list-style-type: none"> • OT devices • IT devices • IT infrastructure devices • All Microsoft Windows systems • All controllers
Control systems management	<ul style="list-style-type: none"> • OT activities • Control system activities • Process control activities

Preset category	Presets available
IT communication management	<ul style="list-style-type: none">• IT activities• Web activities• Email activities• File activities• Microsoft activities
Security	<ul style="list-style-type: none">• DNS activities• Remote procedure call activities• Remote access• Insecure activities• Encrypted activities• Authentication activities
Network management	<ul style="list-style-type: none">• 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 128](#).

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	<p>You can enter a message explaining your choice for reference. You have two acknowledgement options:</p> <ul style="list-style-type: none"> • 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	<p>You can enter a message explaining your choice for reference.</p> <p>Click Acknowledge and include to retain the alert and receive alerts for any new events for the component and its activities.</p>
Report component	<p>You must enter a message explaining your choice for reference. You continue to receive alerts if the anomaly is detected again.</p> <p>Click Report component to create an event report for this anomaly.</p>
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	<p>Acknowledge the reported event as normal for the network.</p> <p>You can enter a message explaining your choice for</p>

Action	Definition
	<p>reference. Two acknowledgement options are available to you:</p> <ul style="list-style-type: none"> • 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	<p>You must enter a message explaining your choice for reference. You continue to receive alerts if the anomaly is detected again.</p> <p>Click Report activity to create an event report for this anomaly.</p>
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.

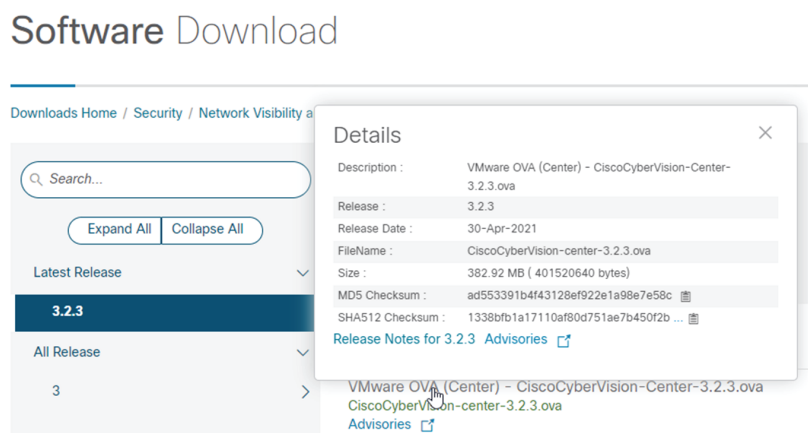
Step 2 Open a shell prompt such as Windows Powershell and use the following command to retrieve the file checksum:

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

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

Algorithm : SHA512
Hash      : 1338BF81A17110AF80D751AE7B450F2B29CCB4C854F550F3888E6B4236865EC9EDF7773FD05D1055C7F1EF76E68C2B8A96CFE69AB
           : 18622E480888E889E94DB16
Path      : C:\Users\ \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 menu, 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.

Configure syslog

Security Information and Event Management (SIEM):

It is an approach to security management that combines SIM (Security Information Management) and SEM (Security Event Management) into a single security management system.

CEF standard for syslog messages:

You must use the Common Event Format (CEF) standard for syslog configurations in the Cyber Vision Center. Update existing syslog configurations from non-CEF to CEF message formats.

Syslog messages from the Beta UI:

In Cyber Vision Center, the configured syslog server also receives messages from the Cyber Vision Center Beta UI. The syslog messages from the Beta UI contain the key-pair value 'Version Number = 2.0', and syslog notifications are generated for each alert type configured in the Beta UI of the Center.

For more information, see [Syslog notifications for alert types](#).

To add a syslog server:

Procedure

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

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

Step 3 Select **UDP**, **TCP**, or **TCP + TLS** in the **Protocol** field.

Note

Select **TCP + TLS** to secure communications with a syslog collector using a p12 certificate file provided by your SIEM administrator. Use the **Set certificate** button to import it.

Step 4 Enter the **Host**.

Enter the IP address of the SIEM that is reachable from the Administration network interface (for example, eth0) of the Center.

Step 5 Enter the **Port** on the SIEM that receives syslogs.

Step 6 Select **Format**.

- **CEF**: Based on the Common Event Format (CEF) standard, this format sends event messages with a legacy timestamp of one-second precision.
- **CEF Extended Time Precision**: Based on the Common Event Format (CEF) and an extended syslog header, this format sends event messages with a legacy timestamp of microsecond precision.

Step 7 Click **Save configuration**.

Import/Export

Use the System interface to import and export the Cisco Cyber Vision database. To access the **Import/Export** page, choose **Admin > System** from the main menu.

Regularly export the database to back up the industrial network data on Cisco Cyber Vision or if you need to transfer the database to a different **Center**.

Exports database file limitation is up to 2 GB of data. This avoids side effects related to slow database exports. If the database is larger than 2 GB, you get an error message. In this case, connect to the Center using SSH and perform a data dump. Use the command: `sbs-db dump`.

Network data, events, and users are retained, as well as all customizations (e.g., groups, component names).

Only configurations created in Cisco Cyber Vision's GUI persist. If you change **Center**, perform a basic configuration of the Center and then configure Cisco Cyber Vision again. Refer to the corresponding [Center Installation Guide](#).



Note The **Import** process may take one hour for big databases. Refresh the page to check that the import remains active (i.e., no error message).

Knowledge DB

Cisco Cyber Vision uses an internal database which contains a list of recognized vulnerabilities, icons, and threats.



Important To remain protected against vulnerabilities, always update the Knowledge DB in Cisco Cyber Vision as soon as possible after notification of a new version.

To update the Knowledge DB:

Procedure

-
- Step 1** Download the latest.db file available from cisco.com.
 - Step 2** From the main menu, choose **Admin > System**.
 - Step 3** Click **Import a Knowledge DB** under the **Knowledge DB** field.
 - Step 4** Select the file and click **Open** to upload the file.

Importing the new database rematches your existing components against any new vulnerabilities and updates the network data.

Certificate Fingerprint

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

For more information, refer [the Centers Installation Guides](#).

Cisco Cyber Vision Telemetry

Telemetry monitors your system to provide anonymous diagnostics and usage data, helps us to understand and enhance product usage. Cisco Cyber Vision telemetry data communication occurs as HTTPS traffic through Port 443 with <https://connectdna.cisco.com/>.

Telemetry is enabled by default. To disable this feature, follow these steps:

Procedure

-
- Step 1** From the main menu, choose **Admin > System**.
- Step 2** To disable telemetry, click the **ON** toggle button under the **Telemetry Collection** field. The switch turns **OFF**.
-

Reset to Factory Defaults

Only use **Reset to Factory Defaults** as a *last resort*, after all other troubleshooting attempts fail. Get help from product support.

To access the **Reset**, choose **Admin > System** from the main menu.

A **Reset to Factory Defaults** deletes the following:

- Some Center configuration data elements.
- The GUI configuration (such as user accounts, the setup of event severities, etc.).
- Data collected by the sensors.
- The configuration of all known sensors (such as IP addresses, capture modes, etc.).

Root password, certificates and configurations from the Basic Center configuration persist.

After a **Reset to Factory Defaults** occurs, the GUI refreshes with the installation wizard. See the corresponding [Center Installation Guide](#).

Snort

Snort is a Network Intrusion Detection System (NIDS) software which detects malicious network behavior based on a rule matching engine and a set of rules characterizing malicious network activity. Cisco Cyber Vision can run the Snort engine on both the Center and some sensors. The Center stores the configuration rule files, pushes rules on compatible sensors, and intercepts Snort alerts to display them as events in the Cisco Cyber Vision Center's GUI.

To access the **SNORT** page, choose **Admin > Snort** from the main menu.

Snort is not activated by default on sensors, so you must first [enable IDS in the Sensor Explorer page](#).

It is available on the following sensor devices:

- The Cisco IC3000 Industrial Compute Gateway
- The Cisco Catalyst 9300 Series Switches
- The Cisco IR8340 Integrated Services Router Rugged

It is also available on the Center DPI, and is enabled by default.

Snort Community Rules are set by default in the Cisco Cyber Vision Center. You can use the **Use Subscriber Rules** toggle button to enable snort subscriber rules. This option requires Advantage licensing and a specific IDS sensor license for each enabled sensor.

Community ruleset

- The community ruleset is a Talos certified ruleset that is distributed freely. It includes rules that have been submitted by the open-source community or by Snort integrators. This ruleset is a subset of the full ruleset available to the subscriber users. It does not contain the latest Snort rules and does not ensure coverage of the latest threats.

Subscriber ruleset

- The subscriber ruleset includes all the rules released by the Talos Security Intelligence and Research Team. The ruleset ensures fast access to the latest rules and early coverage of exploits. Compared to the Community ruleset, it contains more rules and remains in sync with the latest Talos research work on vulnerability detection.

On the **SNORT** Administration page, you can find Snort rules grouped into categories. Use the toggle buttons under the **Status** columns to enable or disable sets of rules.

Click the download buttons under the **Download Rules** column to download each category rule file.

Note that some rules are **not** enabled inside these categories. So, using the toggle button on a category won't necessarily have an effect on their rules. The ones that are considered the most useful are enabled by default, others have been disabled to avoid performance issues. Consequently, if you want to enable these rules you need to use the [specific rule field](#).

It is also possible to enable/disable a specific rule from a custom rule file.

Snort rules categories:

- Browser:

Rules for vulnerabilities present in several browsers including, but not restricted to, Chrome, Firefox, Internet Explorer and Webkit. This category also covers vulnerabilities related to browser plugins such as Active-x.

- Deleted:

When a rule has been deprecated or replaced it is moved to this category.

- Experimental-DoS:

Rules developed by the Cisco CyberVision team for various kinds of DoS activities (TCP SYN flooding, DNS/HTTP flooding, LOIC, etc.).

- Experimental-Scada:

Rules developed by the Cisco CyberVision team for attacks against industrial control system assets.

- Exploit-Kit:

Rules that are specifically tailored to detect exploit kit activity.

- File:

Rules for vulnerabilities found in numerous types of files including, but not restricted to, executable files, Microsoft Office files, flash files, image files, Java files, multimedia files and pdf files.

- Malware-Backdoor:

Rules for the detection of traffic destined to known listening backdoor command channels.

- Malware-CNC:

Known malicious command and control activity for identified botnet traffic. This includes call home, downloading of dropped files, and ex-filtration of data.

- Malware-Other:

Rules that deal with tools that can be considered malicious in nature as well as other malware-related rules.

- Misc:

Rules that do not fit in any other categories such as indicator rules (compromise, scan, obfuscation, etc.), protocol-related rules, policy violation rules (spam, social media, etc.), and rules for the detection of potentially unwanted applications (p2p, toolbars, etc.).

- OS-Other:

Rules that are looking for vulnerabilities in various operating systems such as Linux based OSes, Mobile based OSes, Solaris based OSes and others.

- OS-Windows

Rules that are looking for vulnerabilities in Windows based OSes.

- Server-Other:

Rules dealing with vulnerabilities found in numerous types of servers including, but not restricted to, web servers (Apache, IIS), SQL servers (Microsoft SQL server, MySQL server, Oracle DB server), mail servers (Exchange, Courier) and Samba servers.

- Server-Webapp:

Rules pertaining to vulnerabilities in or attacks against web based applications on servers.

In case of mistake, or to revert to the default configuration, you can use the **RESET TO DEFAULT** button. Note that all categories status and specific rules status will be reset and any added custom rules file will be deleted.

In addition, this page allows you to import custom rules, to enable or disable rules, and reset Snort's parameters to default.

Import Snort Custom Rules

Custom rules are useful if you want to define and use your own rules in addition to the rules provided in the Cyber Vision rulesets. To do this, a file must be created containing syntactically well-formed Snort rules and imported into Cisco Cyber Vision. Refer to Snort documentation for more information about creating rules.

To import custom rules in the Center, follow these steps:

Procedure

-
- | | |
|---------------|--|
| Step 1 | Prepare your custom rules file. |
| Step 2 | From the main menu, choose Admin > Snort . |
| Step 3 | Click IMPORT CUSTOM RULES FILE under the Import custom rules field. |
| | Once a custom rules file is imported, it is stored in the Center, and a "Download" button appears, allowing you to view its content. |
| Step 4 | Click Synchronize rules on sensors . |
-

What to do next

You can [enable/disable a specific rule](#).

Enable IDS on a Sensor

To enable the Snort engine on a sensor, follow these steps:

Before you begin

To use Snort you need to enable IDS on sensors.

Snort is only compatible with sensors embedded in:

- The Cisco IC3000 Industrial Compute Gateway
- The Cisco Catalyst 9300 Series Switches
- The Cisco IR8340 Integrated Services Router Rugged

Procedure

- Step 1** From the main menu, choose **Admin > Sensor Explorer**.
- Step 2** Click a compatible sensor in the list.
- The right side panel appears with sensor details.
- Step 3** Click **Enable IDS**.

Enable or Disable a Rule

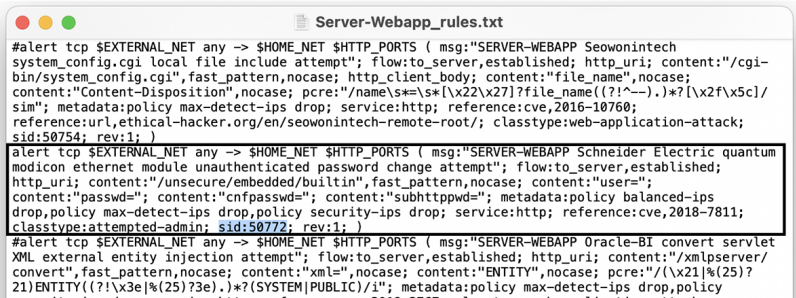
You can manually enable and disable any specific rule, whether it is a default or a custom one. To do so you need the sid (i.e. signature id) that you will find in the rules file.

In the following procedure, we will disable Snort rule sid 50772 as example.

sid 50772: An unverified password change vulnerability (CVE-2018-7811) exists in the embedded web servers of Schneider Electric Quantum Modicon Ethernet modules. This vulnerability could allow an unauthenticated remote user to access the “change password” functionality of the web server. Snort rule with sid 50772 detects such attempts. It monitors and analyzes HTTP flows coming from the external network and raises an alert when the HTTP URI fields contain specific keywords (ex. “passwd=“,”cnfpasswd=“,”subhttpwd=“) that indicate a password change attempt targeting the web server.

Procedure

- Step 1** From the main menu, choose **Admin > Snort**.
- Step 2** Click the **download icon** in the **Download rules** column.
- In the downloaded rule files, locate the rule you wish to enable or disable.



```
#alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS ( msg:"SERVER-WEBAPP Seowonintech
system_config.cgi local file include attempt"; flow:to_server,established; http_uri; content:"cgi-
bin/system_config.cgi", fast_pattern,nocase; http_client_body; content:"file_name",nocase;
content:"Content-Disposition",nocase; pcre:"/name\s*=\s*[\x22\x27]?file_name(?:!~|.)*?[\x2f\x5c]/
sim"; metadata:policy max-detect-ips drop; service:http; reference:cve,2016-10760;
reference:url,ethical-hacker.org/en/seowonintech-remote-root/; classtype:web-application-attack;
sid:50754; rev:1; )

#alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS ( msg:"SERVER-WEBAPP Schneider Electric quantum
modicon ethernet module unauthenticated password change attempt"; flow:to_server,established;
http_uri; content:"/unsecure/embedded/builtin",fast_pattern,nocase; content:"user=";
content:"passwd="; content:"cnfpasswd="; content:"subhttpwd="; metadata:policy balanced-ips
drop,policy max-detect-ips drop,policy security-ips drop; service:http; reference:cve,2018-7811;
classtype:attempted-admin; sid:50772; rev:1; )

#alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS ( msg:"SERVER-WEBAPP Oracle-BI convert servlet
XML external entity injection attempt"; flow:to_server,established; http_uri; content:"/xmlpservlet/
convert",fast_pattern,nocase; content:"xml="; nocase; content:"ENTITY",nocase; pcre:"/(\x21|%(25)?
21)ENTITY(?:\x3e|%(25)?3e).)*?(SYSTEM|PUBLIC)/1"; metadata:policy max-detect-ips drop,policy
```

- Step 3** Enter the **Rule sid** under the **Specific rule** field.
- Step 4** Click **Disable**.
- A success message appears.

Note

If you download the rules file again, you will find a "#" preceding the rule, indicating it is disabled.

Step 5 Click **Synchronize rules on sensors** to save and push changes to the sensors.

Risk Score

The **Risk score** page allows you to set up the time range used for risk score computation. To access the **Risk score** page, choose **Admin > Risk score** from the main menu. Computation occurs every hour but considers only the activities within the configured time period.

You can select a time range of 30 days (by default), 7 days, or set a custom one with a minimum of one day

For more information about risk scores, see the [Risk Score 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

Cisco Cyber Vision Beta Version

- Cisco Cyber Vision Center beta version, on page 141
- Purpose, on page 142
- Dashboard, on page 142
- Filter views of dashboard, alerts, assets, vulnerabilities, and communications pages, on page 143
- Assets, on page 144
- Vulnerabilities, on page 146
- Primary Interface, on page 147
- Properties, on page 148
- Explore communication map, on page 148
- Asset clustering, on page 150
- Alerts dashboard, on page 154
- Enable or disable the syslog notifications for alert types, on page 157
- Configuration, on page 158
- Use Cases, on page 163

Cisco Cyber Vision Center beta version

Cisco Cyber Vision Center's beta UI experience includes dashboards displaying data on assets, vulnerabilities, alerts, and organization hierarchies. You can quickly apply data filters to view necessary information.

Access beta UI

The UI experience is a beta feature. Contact cv-beta@cisco.com to access the beta UI and its features. Enable Cisco Cyber Vision Beta UI alongside the classic UI by following the instructions in the reply. To access the beta user interface, click **Go to Cyber Vision beta** from the interface menu.



Note If a session is inactive for an hour, you must log in to the Cisco Cyber Vision center again.

User profile

In the beta UI, you can find your user profile displayed in the top banner. It shows your email address, username, or both, depending on the storage location of your user information (database or LDAP).

Use search bar

Use the search bar to quickly access an asset.

Procedure

To search for an asset, enter the **Name**, **IP Address**, or **MAC Address** in the search bar.

Note

Type at least three characters to perform a search.

Exact matches appear first in the search results.

You can search for both primary and additional interfaces.

Select a search result to view the summary page of the asset.

Purpose

The Cyber Vision Sensor performs the following roles:

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

Dashboard

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

Highlighted vulnerabilities

The dashboard includes an additional trends chart in the **Highlighted Vulnerabilities**. This area displays the top five vulnerabilities.

Sort highlighted vulnerabilities

Sort the vulnerabilities by:

- Affected assets
- Cisco Security Risk Score (default selection)

- CVSS Score

The sort selection is browser-specific and your selection is retained when you are logged into the Cisco Cyber Vision Center using the same browser.

View highlighted vulnerability details

Click the vulnerabilities to view further details and the affected assets. The **Assets** area lists the affected and acknowledged assets. You can:

- Acknowledge the vulnerability for one or more assets.
- Revert acknowledgement of the vulnerability for one or more assets.

Filter views of dashboard, alerts, assets, vulnerabilities, and communications pages

You can filter the data across these pages if needed.

- Dashboard
- Alerts
- Assets
- Vulnerabilities
- Communications



Note This filter does not affect the **Configuration > Alerts** page.

Follow these steps to add, reset, or edit filters:

Procedure

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

Step 2 Select either **Sensors** or **Networks** from the **Organization Hierarchy** drawer.

- In the **Sensors** tab:
 - Click **Sensor selection**, then select the organization hierarchy based on sensors.
- In the **Networks** tab:
 - Click **Network selection**, then select the organization hierarchy based on networks.

Note

Use the search bar to find sensors and networks along with their hierarchy levels.

- Step 3** Click **Apply**.
- Step 4** Use the **Organization Hierarchy** drawer to reset or edit the selection.
- Step 5** Click **Edit** on the **Dashboard**, **Alerts**, **Assets**, **Vulnerabilities**, or **Communications** page to edit or add additional filters.
- Step 6** Use the **Select** tabs to add or remove data from the **Available filters**.

Note

In the **Organization Hierarchy**, selecting the **Sensors** tab displays the **Networks** filter, and selecting the **Networks** tab displays the **Sensors** filter in the **Edit filters** drawer.

- Step 7** Click **Apply**.
- Step 8** Click **Reset** to remove additional filters.

When you add or remove filters, the system updates the data on the **Dashboard**, **Alerts**, **Assets**, **Vulnerabilities**, and **Communications** pages.

Assets

An asset is a physical device in the industrial network, such as a switch or server. In Cisco Cyber Vision, one asset can represent multiple modules to meet management and inventory needs. Technically, an asset can consist of modules that may have the same MAC and IP addresses but differ in serial number, reference, and type. In Cisco Cyber Vision, specific rules define and categorize assets and asset types.

Asset summary

The asset summary displays detailed information about the asset. If the asset type is PLC, the Summary tab shows details like Slot, Model Name, Type, Firmware Version, and Serial Number in table format, when available. These details only appear if the PLC is modular and consists of various modules within a single chassis or backplane. These modules can include one or more CPU modules, communication modules, or IO modules. Each module is represented as a separate block within the chassis.

View of interfaces

The asset list displays both primary and additional interfaces. To view the additional interfaces, expand the rows of the primary interfaces and retrieve the information. Hover over the primary interface row to see the count of additional interfaces in a tooltip.

Search for an asset

You can search for an asset using its interface details. When you search for an additional interface, use the **IP Address**, **Network**, and **MAC Address**.

Columns and export functionality

The asset list includes new columns: **MAC Address** and **VLAN**.

The **Export** functionality allows you to export all columns to a CSV file, even if some columns are hidden in the UI.

The asset ID differentiates between two assets with the same name in the CSV file.

Asset Selection

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

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

Table Setting

Procedure

-
- | | |
|---------------|--|
| Step 1 | From the main menu, choose Assets . |
| Step 2 | Click the Settings icon at the top right of the table.
The Table Settings pop-up appears. |
| Step 3 | Click Edit Table Columns . |
| Step 4 | Enable the toggle switch for required fields. |
| Step 5 | Click Apply . |
| Step 6 | To display previous Table Settings , click Reset All Settings . |
-

Asset deletion

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

To delete an asset, follow these steps:

Procedure

-
- | | |
|---------------|--|
| Step 1 | From the main menu, choose Assets . |
|---------------|--|

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

Step 3 Click **Delete**.

A warning pop-up appears.

Step 4 Click **Delete**.

Note

An asset can reappear if sensors detect it again.

Vulnerabilities

Vulnerabilities are weaknesses in a system, manifested in these ways:

- Attackers can exploit these vulnerabilities to gain unauthorized access.
- Require mitigation through security measures.

Cyber Vision 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, 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 like existing vulnerabilities, threat intelligence, and the effectiveness of security controls. This score helps prioritize critical vulnerabilities and allocate resources effectively

Table 4: CSRS categories:

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

- **Common Vulnerability Scoring System (CVSS)**: The CVSS assigns a score out of 10 based on factors like attack complexity, attack vector, and potential impacts. Security teams use CVSS scores to prioritize severe vulnerabilities and strengthen system security. Cisco Cyber Vision supports both version 3.1 and version 2 of CVSS.

Table 5: CVSS categories:

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

The Cisco Security Risk Score is prioritized over CVSS. It helps refine security strategies.

Acknowledge or revert vulnerability acknowledgements

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

Use this procedure when you need to acknowledge vulnerabilities affecting assets or revert previously acknowledged vulnerabilities within the Cyber Vision Center. You can acknowledge vulnerabilities and revert acknowledgments from both the **Assets** and **Vulnerabilities** dashboards.

Procedure

-
- | | |
|---------------|--|
| Step 1 | From the main menu, choose Assets . |
| Step 2 | Select an asset. |
| Step 3 | Select the Vulnerabilities tab. |
| Step 4 | Click a CVE ID to view vulnerability details. |
| Step 5 | Enter a comment in the Add/Edit Comment field. |
| Step 6 | To acknowledge the vulnerability, select Acknowledge on this asset . To revert an acknowledgement, select Revert Acknowledgement . |
-

When you acknowledge a vulnerability, the Cyber Vision Center clears the alerts from the **Alerts** dashboard. When you revert the acknowledgment, the alerts reappear on the **Alerts** dashboard.

Primary Interface

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



Note The user can change the primary interface.

To see the **Primary Interface**:

- From the main menu, choose **Assets**.
- Select an asset.
- Click **Interfaces**. The selected interface will appear in the **Assets** and its **Summary** page.

Properties

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

To see **Properties**:

- From the main menu, choose **Assets**.
- Select an asset.
- Click **Properties**.

Explore communication map

The communications map displays the various interactions of an asset. It helps you assess the internal communications of an asset.

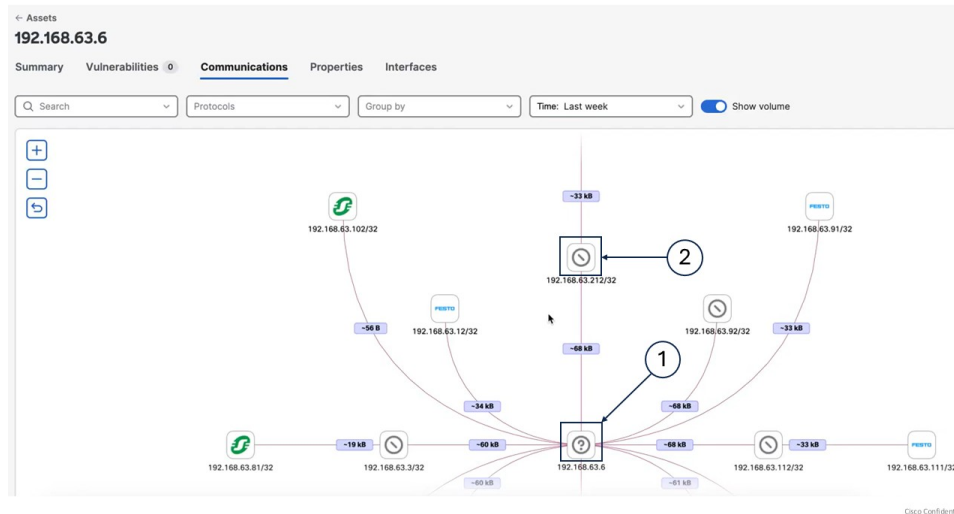
You can filter the data to see specific communications. When you select a communication, a side panel opens showing observed protocols, exchange volumes, and source or destination asset information.

Procedure

- Step 1** From the main menu, choose **Assets**.
- Step 2** Select the asset name.
- Step 3** Click **Communications**.
- Step 4** To organize asset communications:
- Use the **Time** field to sort by the required time period.
 - Use the **Group by** field to sort by **Network** or **Functional Group**.

If you select	Then
Network,	the filter groups all assets that communicate with the selected asset by their subnets. It shows only the subnet information, not the individual assets.
Functional Group,	the filter groups all assets that communicate with the selected asset by their functional groups. It shows only the functional groups, not the individual assets.

The **Communication** page displays asset vendor icons along with their IP or MAC addresses.



Callouts	Descriptions
(1)	It indicates that an asset does not have a vendor.
(2)	It indicates that the vendor is known, but its icon is unavailable.



Note

You can click group nodes to explore groups. This shows assets within each group and lets you investigate further.

Asset clustering

Manual asset grouping based on network definitions and communications is difficult. Asset clustering simplifies this process by organizing assets into functional groups according to their network communication patterns.

The system uses an algorithm to distinguish between OT and IT assets and includes all OT assets in asset clustering. It then suggests a list of functional groups.

Asset movement

Asset clustering identifies assets that can move between functional groups, move to an ungrouped list, or move from the ungrouped list to a group. The algorithm recommends which assets to transfer and 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. The asset clustering result does not change until the communication pattern changes.

Types of functional groups

Asset clustering suggests two types of functional groups: communication-based groups and named groups. A named group can have only one asset, while a communication-based group must have at least two assets. Asset clustering may suggest new functional groups that exclude the most significant assets.

Perform asset clustering

You can perform asset clustering on a specific asset, a functional group, or a sensor. Access this feature from the **Functional Group** page, **Sensor Applications** page, **Assets** page, or the individual asset detail page.

Procedure

-
- | | |
|---------------|--|
| Step 1 | From the main menu, choose Configuration > Functional Groups . |
| Step 2 | Click Start asset clustering .

The system then suggests functional groups in the list. |
| Step 3 | To review, click the Functional Group name. |
| Step 4 | To view communications between assets in a functional group, click Map .

The lightning symbol shows the most significant asset in the group. |
| Step 5 | To change the Functional Group name, click Edit Name . |
| Step 6 | Click Accept to create the functional group. |
-

What to do next

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

Asset Clustering for a Limited Set of Assets

This function allows you to perform focused asset clustering on a limited set of assets. Select assets to define the scope of your asset clustering. The results suggest functional groups that are impacted by the selected assets and exclude unrelated groups.

Procedure

-
- Step 1** From the main menu, choose **Assets**.
 - Step 2** Check the checkboxes next to the asset names in the **Name** column.
 - Step 3** Click the **More actions** drop-down arrow.
 - Step 4** Click **Run Asset Clustering** from the drop-down list.
The **Functional Group Asset Clustering** pop-up appears.
 - Step 5** Click **Start**.
The asset clustering scope is the selected assets.
-

Asset Clustering for a Specific Functional Group

This function allows you to perform focused asset clustering for a specific functional group. The selected functional group defines the scope of the asset clustering. The system runs asset clustering on all assets, and once complete, only the impacted functional groups and asset information appear. The results suggest which assets should be part of the functional group and which should be removed.

Procedure

-
- Step 1** From the main menu, choose **Assets**.
 - Step 2** Click the group name in the **Functional Group** column.
The **View Functional Group** panel appears.
 - Step 3** Click the **More actions** drop-down arrow.
 - Step 4** Click **Run Asset Clustering** from the drop-down list.
The **Functional Group Asset Clustering** pop-up appears.
 - Step 5** Click **Start**.
-

Asset Clustering for Selected Sensors

This function allows you to perform focused asset clustering for a specific sensor. The selected sensor serves as the scope for clustering. It runs asset clustering for assets detected by the selected sensor.

Procedure

- Step 1** From the main menu, choose **Configurations > Sensor Applications**.
- Step 2** Check the check-box of sensor application.
- Step 3** Click **Run Asset Clustering**.
The **Functional Group Asset Clustering** pop-up appears.
- Step 4** Click **Start**.
-

Asset Clustering for Individual Assets

This function allows you to perform focused asset clustering for a individual asset. The selected assets serve as the scope for clustering.

Procedure

- Step 1** From the main menu, choose **Assets**.
- Step 2** Click the asset name in the **Name** column.
- Step 3** Click the drop-down arrow of the **Functional group actions** field.
- Step 4** Click **Run Asset Clustering** from the drop-down list.
The **Functional Group Asset Clustering** pop-up appears.
- Step 5** Click **Start**.
-

Lock Group

When you lock the group, it stays out of asset clustering. While it's locked, no assets get added or removed during asset clustering.

Procedure

- Step 1** From the main menu, choose **Assets**.
- Step 2** Click the group name in the **Functional Group** column.
The **View Functional Group** panel appears.
- Step 3** Click the **More actions** drop-down arrow.
- Step 4** Click **Lock Group** from the drop-down list.
The **Lock Group** pop-up appears.

Step 5 Click **Lock**.

Move Asset from One Group to Another

You can adjust your functional group by moving assets between groups, even if the algorithm cannot add a specific asset to your group.

Procedure

- Step 1** From the main menu, choose **Assets**.
- Step 2** Check the checkbox next to the assets.
- Step 3** Click the **More actions** drop-down arrow.
- Step 4** Click **Add selected to group** from the drop-down list.

The **Add Selected To Group** panel appears.

- Step 5** Click the **Functional Group** drop-down arrow.
- Step 6** Choose the group from the drop-down list.
- Step 7** Click **Add**.

The **Add Selected to Group** warning appears.

- Step 8** Click **Add**.

Note

After you move assets from one group to another, the system deletes any group that is left with a single asset automatically.

Note

You can also move an asset to another group from its individual detail page.

Delete the Functional Group

Procedure

- Step 1** From the main menu, choose **Assets**.
- Step 2** Click the group name from the **Functional Group** column.
- The **View Functional Group** side panel appears.
- Step 3** Click **Delete group**.
- The **Delete Group** window appears.

Step 4 Click **Delete**.

Remove Asset from Functional Group

To remove asset from functional group:

Procedure

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

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

Step 3 Click the **More actions** drop-down arrow.

Note

Accept or discard the suggested functional groups to access **More actions** field.

Step 4 Click **Remove asset from the group** from the drop-down list.

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

Step 5 Click **Remove**.

Alerts dashboard

An **Alerts** dashboard is a monitoring interface that allows you to:

- filter alerts by severity (Critical, High, Medium, or Low),
- access alert summaries and instance details, and
- configure alert types from the summary page.

Active and cleared alerts

- **Active:** The Active tab shows all active alerts from the Cyber Vision Center.
- **Cleared:** When an alert is no longer valid, it appears in the **Cleared** tab.



Note Cleared alerts stay available for up to 14 days.

Alert table

- **Alert Type** column lists alert types such as **Severe vulnerabilities in monitored entities** and **Prohibited Vendors**.

- **Trigger** column lists vulnerabilities.
- **Instances** column lists impacted asset count.
- **Severity** column lists severity levels.
- **Triggered By** column lists categories.

Alerts configuration

You configure alerts by managing alert rules and types.

Alert types

Cyber Vision Center, by default, includes two alert types:

- **Severe Vulnerabilities in Monitored Entities**: Monitors assets within selected entities and raises alerts for high-scoring vulnerabilities.
- **Prohibited Vendors**: Raises alerts for assets associated with prohibited vendors.



Note You can enable Syslog notifications to send alerts generated for a specific alert type to the Syslog server.

Alert rules

Each alert type includes a default alert rule:

- The **Severe Vulnerabilities in Monitored Entities** alert type uses the **Default_OH_Global** rule. You can add, duplicate, or delete this rule. See [Edit, duplicate, and delete alert rules](#).
- The **Prohibited Vendors** alert type uses the **Prohibited_list** rule. You can only edit this rule. See [Edit, duplicate, and delete alert rules](#).

Add new alert rules

You add new alert rules to monitor asset vulnerabilities. When a vulnerability matches the rule, the alert appears on the Alerts dashboard.

Adding rules under the **Severe vulnerabilities in monitored entities** type changes the number of alerts on the dashboard. The **Prohibited Vendors** alert type does not include a **Create New Rule** option.



Note You cannot add new alert rules to the **Prohibited Vendors** alert type.



Note Upgrading the Cyber Vision Center purges old alert rules. 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 **Alert Rule Name** and select the **Severity** and **Entity type**.
- Step 5** Select either organization hierarchy level or functional groups in the **Entity selection** page.

Note

Entity selection depends on the **Entity type** selected in the **Rule name and entity type** page.

- Select the organization hierarchy level. Check the **Assets seen by Unknown data sources** checkbox.
- Select one or more functional groups. Check the **Include Ungrouped assets** checkbox.

- Step 6** Select one of these scoring systems in the **Scoring system and threshold** tab.
- **Cisco Security Risk Score**: enter a Cisco Security Risk Score threshold number between 34 and 100.
 - **CVSS**: enter a CVSS score threshold number between 7 and 10.

Note

Cisco Security Risk Score is the default scoring system, but you can switch to **CVSS**.

- Step 7** Review the **Summary** and then click **Save**.
-

Manage alert rules

You can manage alert rules for **Severe vulnerabilities in monitored entities** by editing, duplicating, or deleting them. For the **Prohibited Vendors** alert type, you can only edit the alert rules.

Procedure

-
- Step 1** From the main menu, choose **Configuration > Alerts**.
- Step 2** Select the alert type.
- Step 3** Locate the alert rule and click the ellipsis (...) in the **Actions** column.
- Step 4** To manage alert rules:
- For the **Severe vulnerabilities in monitored entities** alert type, choose **Edit**, **Duplicate**, or **Delete**.
 - For the **Prohibited Vendors** alert type, select **Edit**.
- Step 5** Change settings as needed and click **Save**.
- For **Severe Vulnerabilities in Monitored Entities**, you can update the **Alert Rule Name**, **Severity**, **Entity selection**, and **Scoring system and threshold**.

- For **Prohibited Vendors**, you can update the **Alert Rule Name**, **Severity**, and **Vendors**.

The alert rule updates the alert count displayed on the **Alerts** page accordingly.

Pause and resume alert types

Pause an alert type to temporarily stop creating new alerts for all rules under it. Existing alerts stay the same. Resume a paused alert type to restart creating new alerts for all rules.

You can manage the alerts by pausing and resuming the alert types.

Procedure

-
- Step 1** From the main menu, choose **Configuration > Alerts**.
Identify the alert types you wish to pause or resume.
- Step 2** Click **Pause** or **Resume** in the **Actions** column.
- Step 3** Click **Yes** in the **Warning** pop-up window.
-

Enable or disable the syslog notifications for alert types

The system sends syslog notifications to the configured syslog server by default whenever an alert is raised, cleared, or its status changes.

- The syslog message includes these details, which are common to all alert rules:
 - CEF:0
 - vendor: Cisco
 - product: Cyber Vision
 - version: 2.0
 - event_class_id: alert_raised OR alert_cleared OR alert_muted
 - event_name: alert type name
 - severity id: 2 (The value changes based on the severity of the alert rule.)
 - cat=alert category
 - SCVAuthorId=user uuid (optional): populated only if user acknowledged an alert manually, empty when system cleared the alert
 - alertRuleId=alert rule uuid
 - alertId=alert uuid
 - msg=The value changes based on the alert type and the event_class_id.

- assetId
 - assetName
 - assetFunctionalGroupId (empty when ungrouped)
 - center-id=uuid of center
 - sensorNames
- The syslog message includes these details for **Severe vulnerabilities in monitored entities**:
 - vulnNumber: for example, CVE-2023-10025
 - vulnName
 - vulnCVSSscore
 - vulnCSRSscore
 - The syslog message includes "vendorName" for **Prohibited Vendors**.

Procedure

-
- | | |
|---------------|--|
| Step 1 | From the menu, choose Configure > Alerts . |
| Step 2 | Select an alert type. |
| Step 3 | Enable or disable the Syslog Notification button. |
-

Configuration

Organization hierarchies

The Organization Hierarchy represents a structured arrangement of levels that logically group entities.

Hierarchy structure

- Each node in the hierarchy is called a level.
- The root level of the hierarchy is referred to as Global, and it is a system-defined level.

Nesting limit

The Cyber Vision Center supports nesting of up to five sub-levels. Once this limit is reached, you cannot add more levels due to the system-defined restriction.

Add, edit, and delete levels in the organization hierarchy

Procedure

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

Step 2 Locate the level and click the ellipsis (...) under the **Action** column.

Step 3 From the drop-down list:

- Select **Add Level**, enter the level name, and click **Add** to create the new level.
- Select **Edit**, modify the level name, and save the changes to edit the level.
- Select **Delete** and confirm to remove the level.

Note

The **Delete** option does not appear for a level if:

- It is a global level.
 - It has child levels.
 - It has a non-zero count, meaning entities such as sensors or PCAPs are assigned to it.
-

Network definitions

Cyber Vision identifies the networks you want to monitor to provide an accurate asset inventory and security posture assessment. You specify the IP addresses and VLANs of your networks by defining your organization's internal IT and OT networks. This approach makes the data more relevant.

Cyber Vision Center offers default network configurations based on RFC1918 addresses and ship the product with default private networks (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16).

Asset detection and network types

The Cyber Vision Service treats all assets detected through PCAP analysis or sensors as part of the same "network." This may result in inaccuracies when aggregating components into physical assets or may lead to irrelevant asset data. Cyber Vision resolves this by allowing you to define your network into three network types:

- **OT Internal:** includes assets like PLCs or HMIs.
- **IT Internal:** includes assets like laptops and other IT-related items, and
- **External:** excludes and removes assets found in this network type from the asset inventory.

Network administrator role

The network administrator determines the type of networks needed. The administrator chooses the network type and checks for duplicate IP ranges.

Network definition in classic and new UI

The network administrator determines the type of networks you need. They choose the network type and check for duplicate IP ranges.

- Classic UI: You can create network definitions. See [Define a subnetwork](#) for more information.
- New UI: You can view existing network definitions and assign them to specific organization hierarchy level, but cannot create or modify them. See [Assign network to organization hierarchy](#) for more information.

Default network definitions

Cyber Vision automatically defines:

- OT Internal networks: based on RFC1918 (IPv4) or RFC 4193 (IPv6) subnets, and
- External networks: defined as everything else.

Assign network to organization hierarchy

To assign a network to an organization hierarchy, follow these steps:

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 organization hierarchy level. |
| Step 4 | Click Assign to complete the process. |
-

PCAP

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

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

To upload PCAP, use the classic UI. See [PCAP Upload](#).



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

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

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

Procedure

-
- Step 1** From the main menu, choose **Configuration > PCAPs**.
- Step 2** Click **Assign** at the end of the row for the PCAP file you need to assign.
- a) To assign multiple PCAP files to the Organization Hierarchy, follow these steps:
1. Check the checkboxes of the desired PCAP files.
 2. Click **Assign Selected to Organization Hierarchy**.
- Step 3** Choose the **Organization Hierarchy**.
- Step 4** Click **Assign**.

Note

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

Sensor Applications

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

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

Health status:

- **New**

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

- **Request Pending**

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

- **Authorized**

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

- **Enrolled**

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

- **Disconnected**

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

Processing status:

- **Disconnected**

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

- **Not enrolled**

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

- **Normally processing**

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

- **Waiting for data**

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

- **Pending data**

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

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

Assign the Sensor to the Organization Hierarchy

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

Procedure

-
- Step 1** From the main menu, choose **Configuration > Sensor Applications**.
- Step 2** Click **Assign** at the end of the network device row that needs assignment.
- a) To assign the multiple sensors to Organization Hierarchy, follow these steps:
1. Check the checkboxes of the desired sensors.
 2. Click **Assign Selected to Organization Hierarchy**.
- Step 3** Choose the **Organization Hierarchy**.
- Step 4** Click **Assign**.

Note

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

Use Cases

Review All PLC and SCADA Data Servers in the Paint Shop

Procedure

Step 1 Organize Network in the Old UI.

- Define a network within the Network Organization section.
- Ensure that the network includes the subnet for both the PLC and SCADA network.

For example, use the subnet 192.168.41.0/24.

192.168.0.0/16	-	192.168/16 private netwo...	OT Internal
192.168.41.0/24	-	PAINTSHOP-PLC-SCADA	OT Internal
192.168.42.0/24	-	PAINTSHOP-SCADA-Client	OT Internal
192.168.43.0/24	-	PAINTSHOP-admin	OT Internal

Step 2 From the main menu, choose **Assets**.

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

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

Review the different assets in the paint shop.

Note

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

Assets seen in current active view

0 selected [Remove from group](#) [Delete](#) [Export](#)

Name	Seen By	Active Alerts	IP Address	Type	Network
<input type="checkbox"/> ROCKWELLSRV.lab-autom-ccv.local	MainSwitch	-	192.168.41.1	Workstation	PAINTSHOP-PLC-SCADA
<input type="checkbox"/> ROCKDATASERVER.lab-autom-ccv.l...	MainSwitch	-	192.168.41.2	Unknown	PAINTSHOP-PLC-SCADA
<input type="checkbox"/> ROCKWELLVLAN41	-	-	192.168.41.10	Workstation	PAINTSHOP-PLC-SCADA
<input type="checkbox"/> COMMON	-		192.168.41.21	PLC	PAINTSHOP-PLC-SCADA
<input type="checkbox"/> Line1	-		192.168.41.22	PLC	PAINTSHOP-PLC-SCADA

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

Analyze and Acknowledge All Vulnerabilities with a CVSS Score Above Nine

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

Procedure

- Step 1** From the main menu, choose **Assets**.
 - Step 2** Click the asset **Name**.
 - Step 3** Click **Vulnerabilities**.
 - Step 4** Click the filter icon at the top right corner of the table.
 - Step 5** Click the drop-down arrow of the **CVSS Score** column.
 - Step 6** Select **Critical** from the drop-down list.
This will show vulnerabilities with a CVSS score between 9.0 and 10.
 - Step 7** To acknowledge the vulnerability, click **Acknowledge**.
Acknowledging the vulnerability will hide it from dashboard counters, clear alerts, and make filtering easier.
-