



## **Cisco Cyber Vision GUI User Guide, Release 4.1.0**

**First Published:** 2021-01-01

**Last Modified:** 2021-01-01

### **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





## CONTENTS

---

<b>CHAPTER 1</b>	<b>About this documentation</b>	<b>1</b>
	Document purpose	1
	Warnings and notices	1

---

<b>CHAPTER 2</b>	<b>Introduction</b>	<b>3</b>
	Cisco Cyber Vision Installation	3
	Cisco Cyber Vision overview	3

---

<b>CHAPTER 3</b>	<b>Understanding concepts</b>	<b>5</b>
	Preset	5
	Filters	6
	Component	12
	Device	13
	Activity	15
	Conduit	17
	Flow	18
	Time span	19
	Tags	21
	Properties	23
	Risk score	24
	Vulnerability	31
	Events	34
	Credentials	35
	Variable accesses	36
	Creating and customizing groups	38
	Active Discovery	43

---

<b>CHAPTER 4</b>	<b>Navigating through Cisco Cyber Vision</b>	<b>49</b>
	Home	49
	Explore	54
	Preset views	55
	Dashboard	57
	Device and activity lists	59
	Map	60
	Vulnerabilities	62
	Security Insights	64
	Purdue Model	65
	Right side panel	65
	Technical sheets	66
	Reports	69
	Events	71
	The Dashboard	71
	The Calendar	72
	Monitor	73
	Monitor mode	73
	Monitor mode's views	74
	New and changed differences	78
	Review differences	79
	Acknowledge differences	79
	Report differences	80
	Remove and keep warning	80
	Individual acknowledgment	81
	Investigate with flows	81
	Create a baseline from a default preset	81
	Create a baseline from a group	81
	Create a weekend baseline	82
	Enable a baseline monitoring	82
	Use cases	84
	Detection of assets newly connected to the network	84
	Tracking sensitive assets properties	93

Detect changes that impact availability and integrity	98
Search	102
Admin	104
System	104
Center shutdown/reboot	104
Upgrade with a combine update file	104
Syslog configuration	106
Import/Export	107
Knowledge DB	107
Certificate fingerprint	108
Reset	109
Data management	109
Clear data	110
Expiration settings	110
Ingestion configuration	111
Network organization	112
Sensors	113
Sensor Explorer	113
Management jobs	126
PCAP Upload	128
Users	129
Management	129
Role Management	131
Security settings	134
Events	135
API	136
Token	136
Documentation	138
License	141
External Authentication	141
LDAP	141
Snort	150
Risk score	153
Integrations	153

- pxGrid 153
- FMC 153
- FTD 155
- SecureX 156
- Extensions 163
- Center certificate 164
- SNMP 165
  - Configure SNMP 165
  - SNMP MIB 168
- System statistics 169
  - Center 169
  - Sensors 172
- My settings 174



# CHAPTER 1

## About this documentation

---

- [Document purpose, on page 1](#)
- [Warnings and notices, on page 1](#)

### Document purpose

This user guide presents the [Understanding concepts](#) you will meet in Cisco Cyber Vision and how to [Navigating through Cisco Cyber Vision](#) within the application by explaining available features.

It takes into consideration the GUI with the highest license level (Advantage) and involves all available users roles (from full rights to read-only).

This manual is applicable to **system version 4.1.0**.



---

#### Important

Cisco Cyber Vision EAP is a snapshot of the ongoing development process and is in the qualifying phase. Testing for this program is under progress and may contain features that are incomplete or may change before the next full release.

---

### Warnings and notices

This manual contains notices you have to observe to ensure your personal safety as well as to prevent damage to property.

The notices referring to your personal safety and to your property damage are highlighted in the manual by a safety alert symbol described below. These notices are graded according to the degree of danger.



---

#### Warning

Indicates risks that involve industrial network safety or production failure that could possibly result in personal injury or severe property damage if proper precautions are not taken.

---



---

**Important** Indicates risks that could involve property or Cisco equipment damage and minor personal injury if proper precautions are not taken.

---



---

**Note** Indicates important information on the product described in the documentation to which attention should be paid.

---





## CHAPTER 2

# Introduction

---

- [Cisco Cyber Vision Installation](#), on page 3
- [Cisco Cyber Vision overview](#), on page 3

## Cisco Cyber Vision Installation

The Cisco Cyber Vision GUI (Graphical User Interface) is an integral part of Cisco Cyber Vision. Thus, you cannot use it without prior installation and initialization of:

1. The sensors, to capture traffic and visualize data on the GUI.
2. The Center, to configure network interfaces that collect data from the sensors and install Cisco Cyber Vision software.

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

If everything is ready to start using the GUI, note that at least one sensor has to be enrolled so that you can enjoy your first experience with the GUI. To do so, please refer to [Sensor Explorer](#) section in this documentation.

## Cisco Cyber Vision overview

One of the aims of the Cisco Cyber Vision 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.





## CHAPTER 3

# Understanding concepts

---

- [Preset, on page 5](#)
- [Filters, on page 6](#)
- [Component, on page 12](#)
- [Device, on page 13](#)
- [Activity, on page 15](#)
- [Conduit, on page 17](#)
- [Flow, on page 18](#)
- [Time span, on page 19](#)
- [Tags, on page 21](#)
- [Properties, on page 23](#)
- [Risk score, on page 24](#)
- [Vulnerability, on page 31](#)
- [Events, on page 34](#)
- [Credentials, on page 35](#)
- [Variable accesses, on page 36](#)
- [Creating and customizing groups, on page 38](#)
- [Active Discovery, on page 43](#)

## Preset

As knowing an industrial network can be really challenging, presets have been created to help you navigating through its numerous data.

A preset is a set of criteria. This concept is a fundamental of Cisco Cyber Vision that will allow you to explore the network in its details from what you need to see. For example, if you are an automatician you could be interested in knowing which PLCs are writing variables. To reach this data, you just need to access one Preset (e.g. OT) and select two criteria (e.g. PLC and Write Var). Think 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 meet your business requirements. Several types of view are available to give you full visibility on the results and from different perspectives.

Some generic presets are available by default. You can start by playing with these ones to see what they have to offer. They have been created according to the recommendations and big categories listed in Cisco's playbooks which are the following:

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

- Asset management, to identify and make an inventory of all assets associated with OT systems, OT process facilities and IT components.
- Communications management, to see flows according to their nature (OT, IT, IT infrastructure, IPV6 communications, Microsoft flows).
- Security, to control remote accesses and insecure activities.
- Control system integrity, to check the state of industrial processes.
- Network quality, to see network detection issues.

The category My Preset contains customized presets. You can create presets using criteria to meet your own business logic. However, as Cisco Cyber Vision is a collaborative application, it shouldn't be forgotten that customizations on presets are persistent and impact other users.

## Filters

Cyber Vision data can be filtered to build a preset per:

- Device tags: devices
- Risk score: device individual risk
- Groups: devices
- Activity tags: activities
- Sensors: device “location”
- Networks: device IPs
- Keyword: device properties including IP, MAC, names, vendor, etc...

Filters work differently whether they are affecting devices and/or activities. Their combination will limit the scope of data visualized in the different views for a preset:

Each category allows 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 intersect of the selections for each category.

The way each parameter can be used in filters is explained in the next sections.

### Device tags

Device tags can be used to select components. Device tag filters can be inclusive or exclusive. The combination of several device tags will select 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) <input checked="" type="checkbox"/> Network Switch (2) <input checked="" type="checkbox"/> Rockwell Automation <input checked="" type="checkbox"/> Siemens	IE4000PRP2.ccv 80:2d:bf:1e:23:8c	Network Switch	Yes
	Schneider 192.168.22.68	Controller	Yes
	Siemens 192.168.21.41	Controller , Siemens	No
	1756-L71/B LOGIX5571 (Port1-Link00)	Controller , Rockwell Automation	No

When devices are filtered the “Device view” only presents the devices corresponding to the filter. For example, only the Controllers if the tag “Controller” is selected.

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).

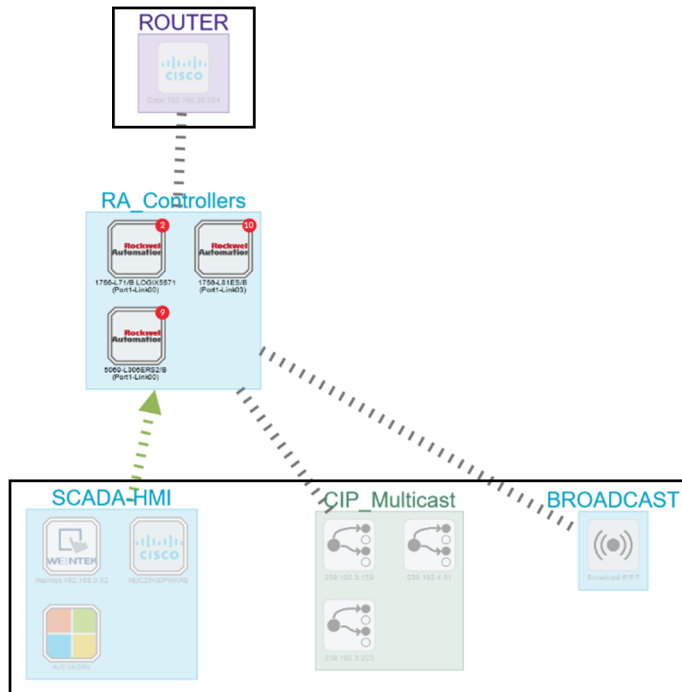
It will give the following results:

*Device tag filter, example of Controllers – list of devices*

Device	Group	First activity	Last activity	IP	MAC	Risk score	Tags
5069-L306ERS2/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-Link03)	RA_Controllers	Jul 6, 2021 10:56:20 AM	Jul 6, 2021 10:59:15 AM	192.168.20.25	Sc-88:16:ed:ccc:8e (+ 1 other)	70	Controller, Rockwell Automation
1756-L71/B LOGIX5571 (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*



### Risk score

The risk score will be used to filter devices based on their score. A range of Risk score can be defined and used as inclusive or exclusive filter. All devices will be filtered based on this range.

#### *Risk score, filter definition*

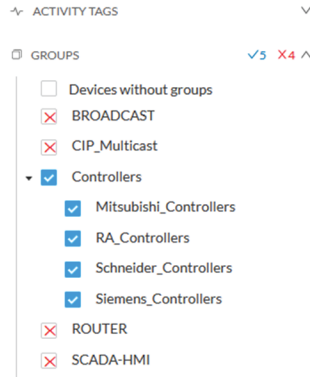
#### *Risk score – inclusive filter*

In the example above, only the devices with a risk score in the selected range will be selected.

### Groups

Groups can be used to filter devices. Each group or sub-group could be added as inclusive or exclusive filter:

#### *Group filter*



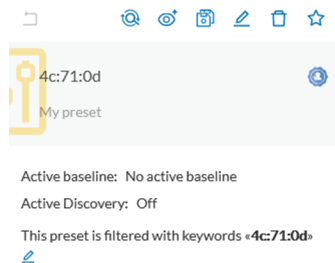
In the example above, only the devices belonging to the selected groups will be selected.

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.

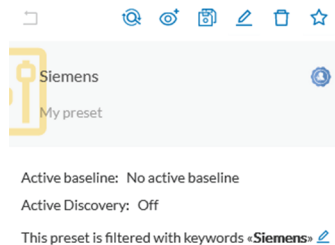
**Keyword**

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*



**Sensors**

Activities can also be filtered based on the sensor that analyzed the associated packets. As for tags, inclusive and exclusive filters can be used. Usually either option is used, inclusive only to select data coming from a set of sensors, or exclusive only, to ignore the data from a set of sensors.

### Sensor filter

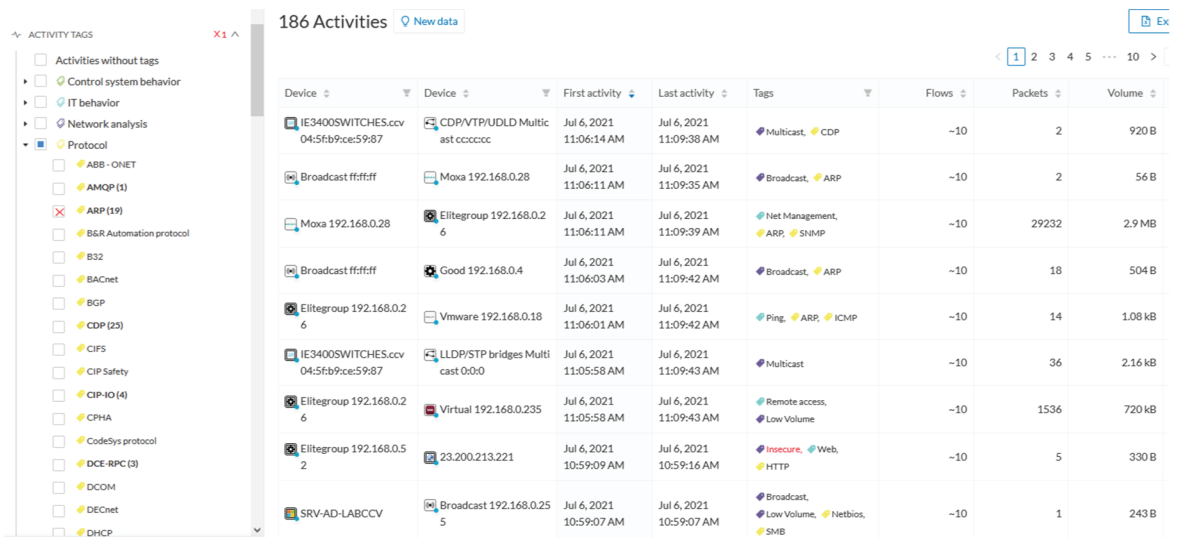


### Activity tags

Filtering on activity tag will not have the same behavior than a filter based on devices. Inclusive activity tag filters will be the same, but exclusive 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.

### Activity filter – negative filter 1



In the example above, several activities are kept because the ARP tag is present as well as other activity tags. There is no exact match. But 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 LOGIX557 1 (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, both activity tags need to be selected like below:

### Activity filter – negative filter 3



The screenshot displays a table of network activities. On the left, a sidebar shows 'ACTIVITY TAGS' with various categories like 'Network analysis', 'Protocol', and 'Authentication Error'. The main table lists activities with columns for Device, First activity, Last activity, Tags, Flows, Packets, and Volume. The table is filtered to show activities from July 6, 2021.

Device	Device	First activity	Last activity	Tags	Flows	Packets	Volume
IE3400SWITCHES.ccv 04:5fb9:ce:59:87	CDP/VTU/DLD Multicast cc0cccc	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	Elttegroup 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
Elttegroup 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 04:5fb9:ce: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
Elttegroup 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
Elttegroup 192.168.0.5	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

Combined inclusive and exclusive tags are seldom used, but for very specific use cases.

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

### Networks

A filter can be defined based on network settings: IP range or VLAN ID can be used. 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 will be selected.

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

Exclusion and combination also can be used, for instance:

*Network filter – negative filter*

The screenshot shows a 'Criteria' panel on the left with a search bar and a list of filters. Under 'NETWORKS', two IP ranges are selected: 192.168.0.0/16 (checked) and 192.168.22.0/24 (unchecked). Under 'DEVICE TAGS', 'Broadcast' is selected. The main table shows 33 activities filtered by these criteria.

Device	Device	First activity	Last activity	Tags
Siemens 192.168.21.50	Broadcast ffffff	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

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

As of version 4.0.0, the notion of [Device](#), which is an aggregation of components, is introduced in Cisco Cyber Vision and changes how data is processed and presented.

A component represents an object of the industrial network from a network point of view. It can be the network interface of a PLC, a PC, a SCADA station, etc, or a broadcast or multicast address.

In the GUI, a component is shown as an icon in a box, either the manufacturer icon (if detected), or a more specific icon (for instance for a known PLC model), a default cogwheel, a planet for a public IP, etc.

Some examples of icons:

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



Whenever it's possible, components will be grouped under a device, and represented as such. For example, in the map, you will be able to see a device's components through its right side panel and technical sheet. Other components, that is the ones that don't belong to any device, will be displayed in the map, with the difference that a device is represented with an icon squared with a double border, whereas a component will have a single border.

For more information, refer to the [Device](#) section.

In Cisco Cyber Vision, components are detected from the [Properties](#) MAC address and (if applicable) IP address.



**Note** MAC addresses are all physical interfaces inside the network. Instead, attribution of IP addresses relies on the network configuration.

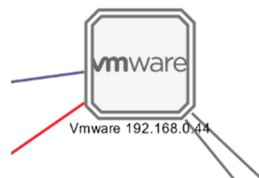
To be detected by Cisco Cyber Vision, an object needs to have some network activity (emission or reception). Thanks to Deep Packet Inspection technology, detailed information about a component is provided in the GUI. Thus, information like IP address, MAC address, manufacturer, first and last activity, tags, OS, Model, Firmware version depends on the data retrieved from the network. Data originates from the communications (i.e. [Activity](#)) exchanged between the components.

When you click a component on the map or a list, a [Right side panel](#) opens on the right with the component detailed information.

## Device

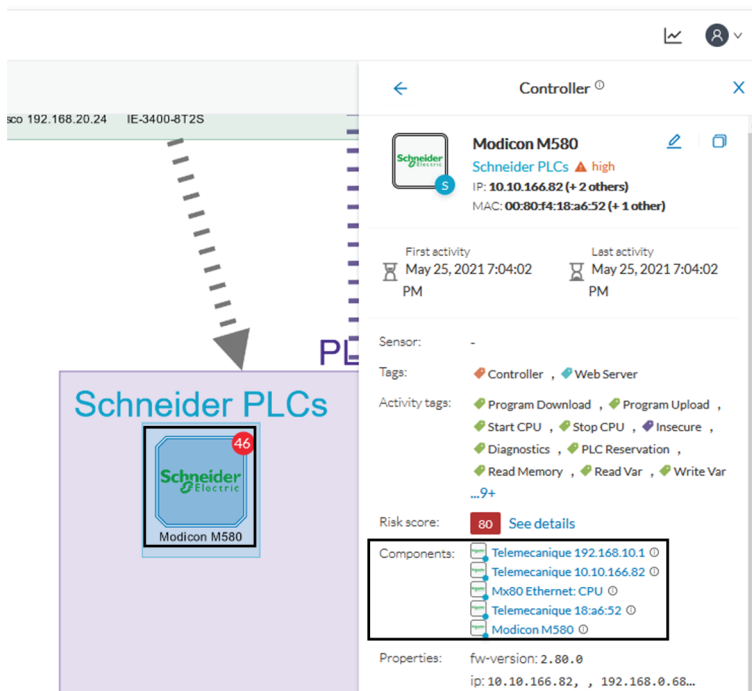
The concept of device has been developed to show the network from a physical point of view (in Cisco Cyber Vision versions older than 4.0.0 only components and aggregated components were used). A device represents in Cisco Cyber Vision a physical machine of the industrial network such as a switch, a engineering station, a controller, a PC, a server, etc. Thus, devices simplify data presentation, especially in the map, and enhance performances; because a single device will be shown in place of multiple components. Besides, it complies with a logic of management and inventory, which focuses on users needs.

In the GUI, a device is shown as an icon in a double border, either the manufacturer icon (if detected), or a more specific icon (for instance for a known PLC model), or even a default cogwheel if no icons is available in Cisco Cyber Vision database yet.



Technically, a device is an aggregation of **Component** that have been brought together because they have similar properties. In fact, components can share same characteristics such as same IP address, same MAC address, same 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.

As you click on a device -on the left, a Schneider controller-, a right side panel opens showing its components:



Devices can have a red counter badge which display the number of vulnerabilities detected. For more information, refer to **Vulnerability**.

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

5 Components

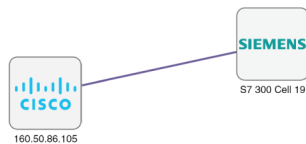
Component	First activity	Last activity	IP	MAC	Tags	Vulnerat
1756-EN2T/D	May 25, 2021 7:02:23 PM	May 25, 2021 7:02:23 PM	192.168.20.22	4c:71:0d:72:8c:57	Rockwell Automation	11
1756-RM2/A REDUNDANCY MODULE (Port1-Link01)	May 25, 2021 7:02:23 PM	May 25, 2021 7:02:23 PM	192.168.20.22	4c:71:0d:72:8c:57	Rockwell 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.

To know which types of device Cisco Cyber Vision is capable of detecting, take a look at the device [Tags](#) classified per level in the Cisco Cyber Vision application.

## Activity

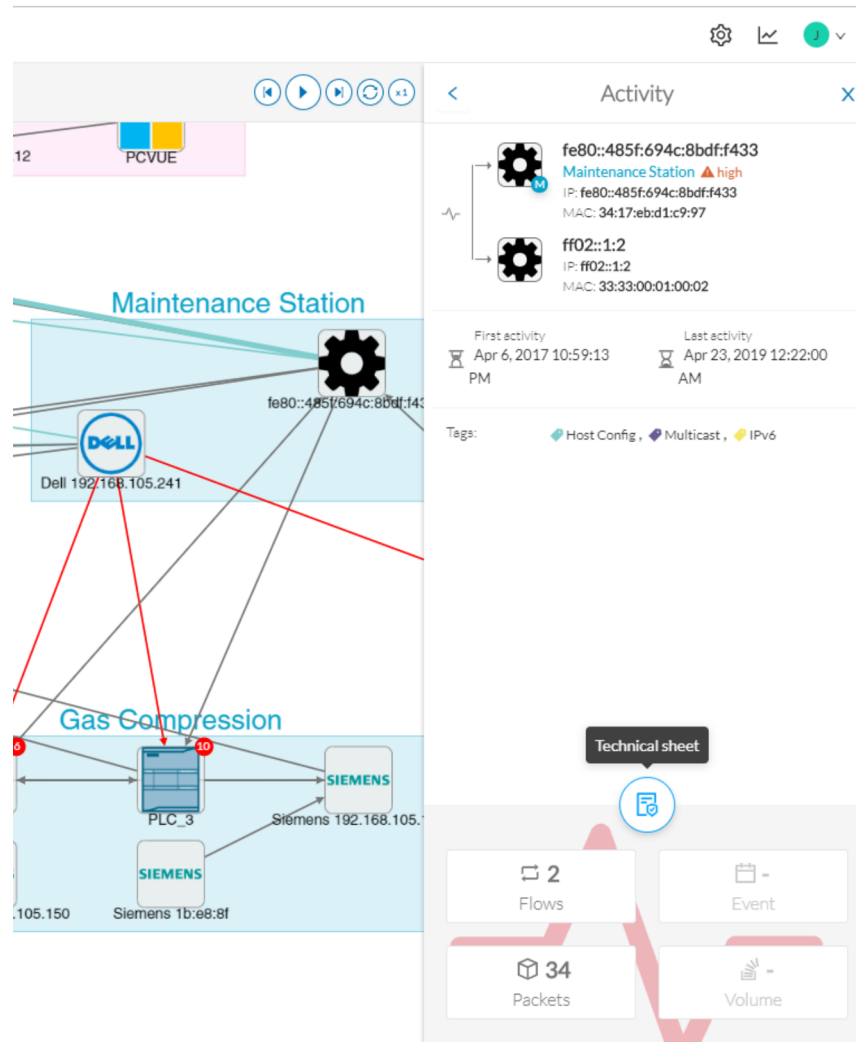
An activity is the representation of the communications exchanged between [Device](#) or [Component](#). It is recognizable on the map by a line (or an arrow if the source and destination components are known) which links one component to another:



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

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

- The date of the first and last communication between the two components.
- Details about the components (name, IP, MAC and if applicable the group they are part of, their criticality).
- The tags on the flows.
- The number of flows.
- The number of packets.
- The volume of data exchanged.
- The number of events.
- A button to access the [Technical sheets](#) that shows more details about tags and flows.

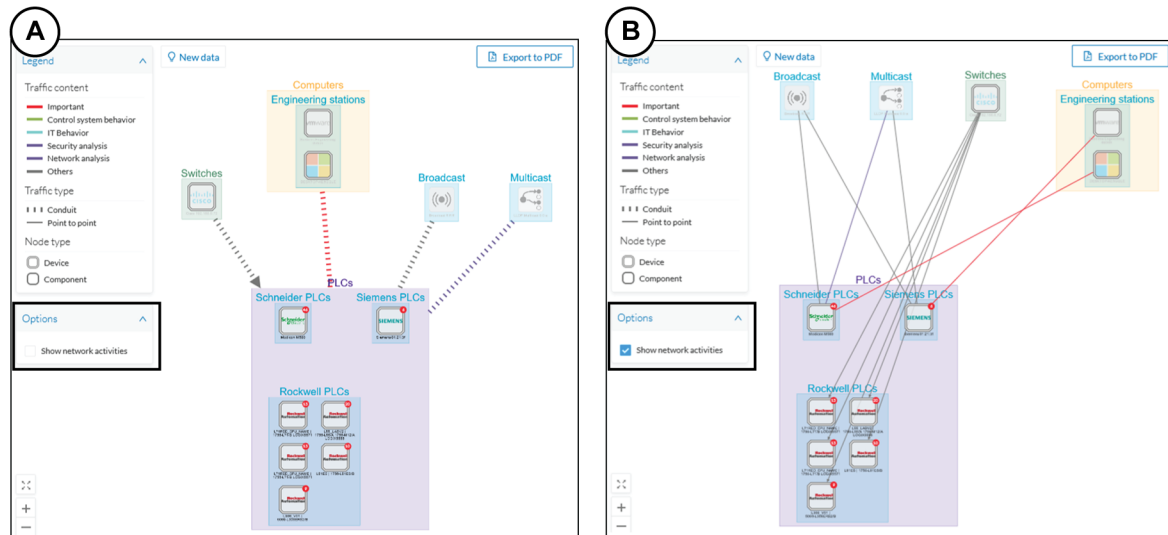


Devices or components with no activity does not mean that it did not have any interaction. In fact, a component can only be detected if at some point it has been involved in a network activity (communication emission/reception). Lack of activity can mean that the other linked component is not part of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

#### Aggregated activities or conduits:

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

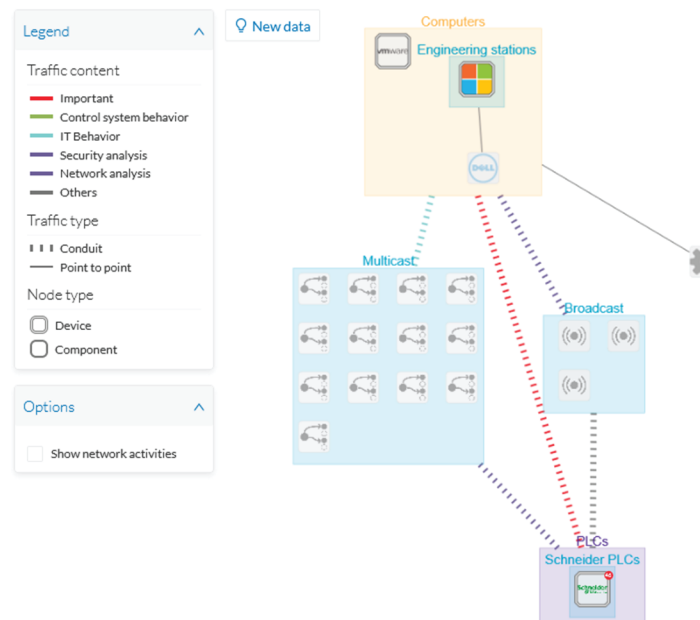
Use the Show network activities button at the lower left side of the map to turn on/off the simplified view of the activities between groups. This feature is turned on by default.



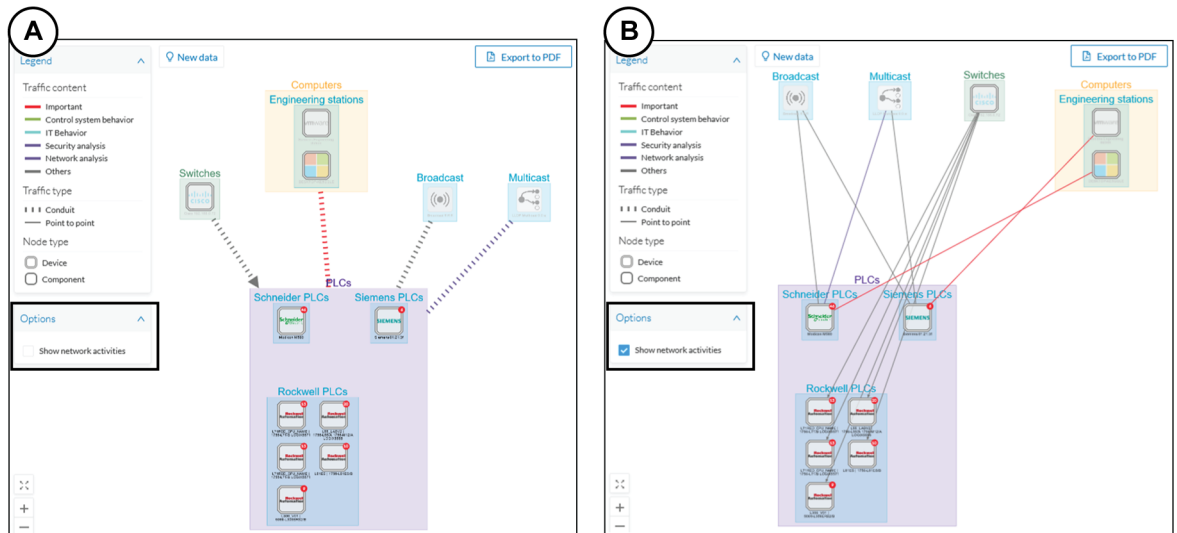
# Conduit

A conduit is the representation of the communications exchanged between two **Component**. It is in fact an aggregation of **Activity** to facilitate visibility when devices and components are inside groups. Conduits representation in Cisco Cyber Vision fit the 62443 standard which specifies policies and requirements for system security

A conduit is recognizable on the map by a thick, hyphenated line -which can have an arrow if the source and destination groups are known- that links one group to another:



Conduits view mode is enabled by default. You can disable it by using the Show network activities button at the lower left side of the map.



# Flow

A flow is a single communication exchanged between two components. A group of flows forms an **Activity**, which is identifiable in the Maps by a line that links one component to another. You can see flows by accessing a **Technical sheets** and then by clicking the Activity tab, or directly by clicking the number of flows on 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.

The screenshot shows a table with columns: Last activity, Tags, Packets, and Bytes. The table contains several rows of data. A filter dropdown menu is open over the 'Tags' column, showing a list of tags with checkboxes and counts: ARP (2), Broadcast (1), Low Volume (2), Profinet (14), Read Var (4), and Write Var (3). There are 'Filter' and 'Reset' buttons at the bottom of the dropdown.

	Last activity	Tags	Packets	Bytes
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		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.

## Time span

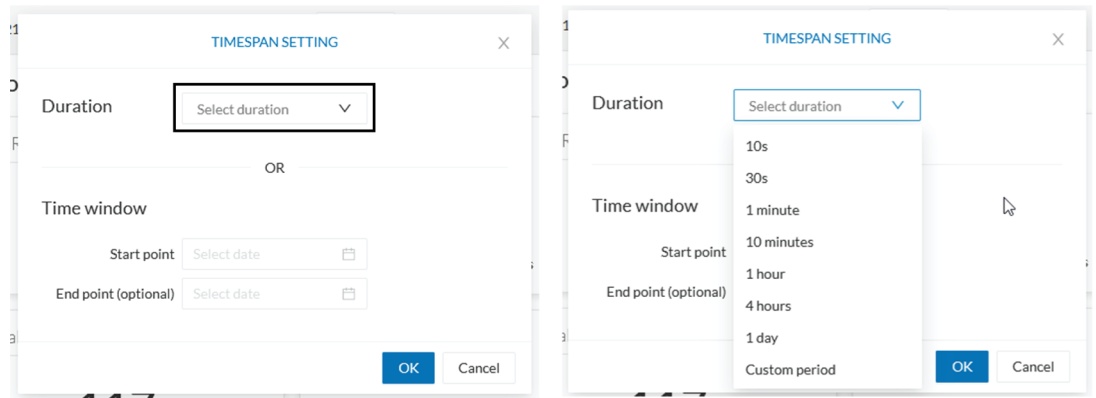
Because Cisco Cyber Vision is a real-time monitoring solution, views are continuously updated with network data. Thus, you can visualize the network activity during a defined period of time by selecting a time span. Time span is used to view less data on the view you're on, or filter data based on time. This feature is available on each preset's view.

The screenshot shows the Cisco Cyber Vision GUI. A time span filter is set to 'Last 1 year (Jun 3, 2020 5:50:32 PM – Jun 3, 2021 5:50:32 PM)'. The main view displays '14 Devices and 32 other components'. A table lists devices with columns for Device, Group, First activity, and Last activity.

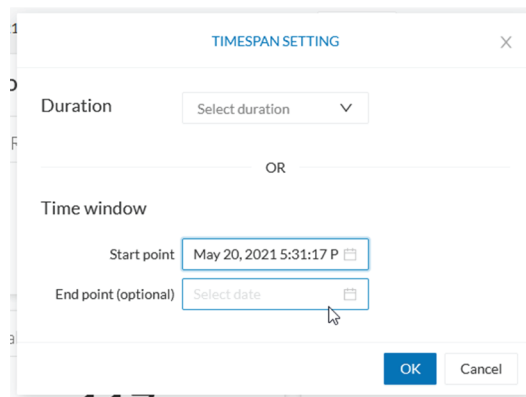
Device	Group	First activity	Last activity
Dell 192.168.0.229	Computers	May 25, 2021 7:06:29 PM	May 25, 20
Siemens 192.168.0.46	Siemens PLCs	May 25, 2021 7:06:29 PM	May 25, 20
Siemens Engineering	Engineering	May 25, 2021 7:06:29 PM	May 25, 20

To set a time span, click the pencil button. A window pops up and gives you two options:

- To set a duration, selecting a period of time (from 10 seconds to 1 day) or a custom period up to now.

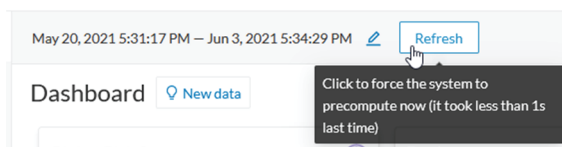


- To set a time window, selecting a start date and optionally an end date. If you don't select one the end date will be set to now.



You can 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.

Once the time span set, click the Refresh button 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 12mo) before considering a troubleshooting.

### Recommendations:

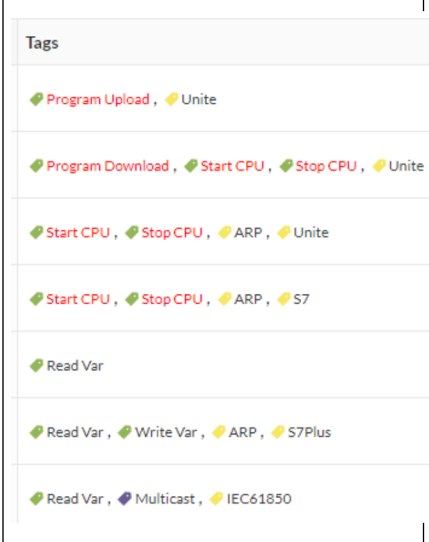
Generally, you can set the time period to 1 or 2 days. This setting is convenient to have an overall view of most supervised standard network activities. This includes daily activities such as maintenance checks and backups.

However, there are many cases where the time frame should be adjusted:

- 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 week-end, etc.
- Set limits to visualize what happened during the night/week-end.
- Set limits to focus on a time frame close to a specific event.

## Tags

### What are tags?

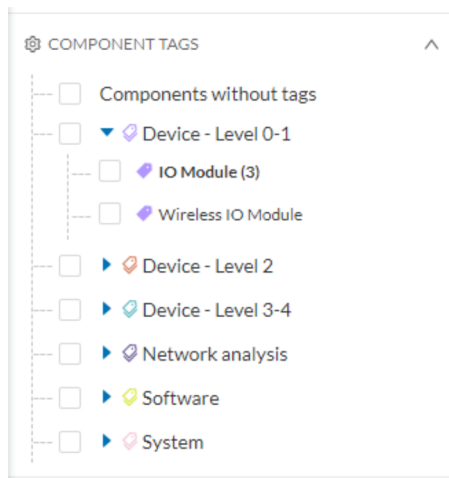
	<p>Tags are meaningful labels that succinctly describe a network. They can be applied to components or activities. Each tag has a description and an icon color which correspond to its category.</p>
--	---

More specifically, tags are metadata on [Device](#) and [Activity](#). Tags are generated according to the [Properties](#) of components -which are then applied to devices- and activities. Thus, there are two types of tags:

- Device tags **(1)** which 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 **(2)** which 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, which you can find in the filtering area, and applies to a device or an activity.

*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 presented in the ISA-95 international standard.

---

### What are tags used for?

Exploration of the network and Cisco Cyber Vision is mainly lead by tags. Criteria set on presets are significantly based on tags to [Filters](#) the different views.

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

### Where to find tags?

You will 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 take different perspectives and have different approaches concerning tags. For example, the dashboard shows the preset's results bringing out tags over other correlated data, while the device list highlights devices over data like tags. Refer to the [Navigating through Cisco Cyber Vision](#) to know more about them.

If you want to know more about a tag, access the Basic tab inside a [Technical sheets](#) to see the tags' definition marked on a component and an activity.

*Some definitions of tags inside an activity's technical sheet:*

The screenshot shows the 'Tags' section in the Cisco Cyber Vision GUI. It is organized into two main sections: 'CONTROL SYSTEM BEHAVIOR' and 'PROTOCOL'. Under 'CONTROL SYSTEM BEHAVIOR', there are three tags: 'Start CPU', 'Stop CPU', and 'Program Download'. Each tag has a brief description of its function. Under 'PROTOCOL', there is one tag: 'Unite', which is described as a protocol for managing and supervising Schneider Electric PLCs, IO Modules, and Drives.

## Properties

### What are properties?

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 flows properties from the packets captured. The Center then deduces components properties and then devices properties out of flows properties. Some properties are normalized for all devices and components and some properties are protocol or vendor specific.

### What are properties used for?

Besides from providing further details about devices, components and flows, properties are crucial in Cisco Cyber Vision to generate [Tags](#). And combination of properties and tags are used to define behaviors (i.e. in the Monitor mode) inside the industrial network.

### Where to find properties?

Properties are visible from devices and components [Right side panel](#) and [Technical sheets](#) under the tab Basics.

*A component's properties inside its technical sheet with normalized properties on the left column, and protocol and vendor specific properties on the right column:*

The screenshot shows the 'Properties' tab in the Cisco Cyber Vision GUI. The interface includes navigation tabs for 'Basics', 'Security', 'Activity', and 'Automation'. Below these are 'Properties' and 'Tags' sub-tabs. The main content area is titled 'Properties' and contains two columns of key-value pairs. The left column lists general device information, and the right column lists S7-specific details.

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

## Risk score

### What is a risk score?

A risk score is an indicator of the good health and criticality level of a device, on a scale from 0 to 100. It has a color code associated to 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

The notion of risk scores appears in several parts of Cisco Cyber Vision. For example, you will find them in:

- The filter criteria.
- The device list.
- The device technical sheet.
- The device risk score widget (Home page).
- The preset highlight widget (Home page).

### **What is a risk score used for?**

The risk score is meant to help the user 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 intended as a first step in security management to take actions by showing the causes of high scores and providing solutions to reduce them. The goal is to minimize and keep risk scores as low as possible.

The solutions proposed can be:

- to patch a device to reduce the surface of attack,
- to remove vulnerabilities,
- to update firmware,
- to remove unsafe protocols whenever possible (e.g. FTP, TFTP, Telnet),
- to install a firewall,
- to limit communications with the outside, by removing external IPs.

In addition, it is necessary to define the importance of the devices in your system by grouping devices and setting an industrial impact. Thereby, increasing or decreasing the risk score, which will allow you to focus on most critical devices.

All these actions will reduce the risk score which affect its variables, i.e. the impact and the likelihood.

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 represents 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.

### **How is the risk score computed?**

The risk score is computed as follows:

Risk = Impact x Likelihood

Impact:

The impact answers the question: What is the device “criticality”, that is, what is its impact on the network? Does it control a small, non-significant part of the network, or does it control a large critical part of the network? To do so, the impact depends on:

- The device tags, because some device types are more critical. Each device type (or device tag) or device tag category has been assigned an industrial impact score by Cisco Cyber Vision. For example, is the

device a simple IO device that controls a limited portion of the system, or is it a Scada that controls the entire factory? These will obviously not have the same impact if they are compromised.

- The user has the possibility to act on the device impact by moving it into a group and setting the group's industrial impact (from very low to very high).

Likelihood:

The likelihood answers the question: What is the likelihood of this device being compromised? It depends on:

- Device activities, more precisely on the activity tags. Because 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.

These criteria are visible under Details in the device's technical sheet.

### How to take action:

1. In the device list, in the risk score column, click the sort icon to get the highest risk scores.

The screenshot shows a web interface for device management. At the top, there are navigation links: "Explore", "All data", and "Device list". Below this is a date range filter for "Last 1 year (Jun 3, 2020 5:50:32 PM – Jun 3, 2021 5:50:32 PM)" and a "Refresh" button. The main content area displays "14 Devices and 32 other components" with an "Export to CSV" button and a pagination control showing "1 / 2" and "40 / page". Below the pagination, it indicates "1 / 46 Devices selected" with options to "Select all devices" or "Clear selection". The table below has the following columns: Device, Group, First activity, Last activity, IP, MAC, and Risk score. The first row is selected and has a risk score of 80. The other three rows have a risk score of 75.

Device	Group	First activity	Last activity	IP	MAC	Risk score
<input checked="" type="checkbox"/> Modicon M580	Schneider PLCs	May 25, 2021 7:04:02 PM	May 25, 2021 7:04:02 PM	192.168.0.68 (+ 2 others)	00:80:f4:18:a6:52 (+ 1 other)	80
<input type="checkbox"/> L71RED_CPU_NAME   1756-L71/B LOGIX5571	Rockwell PLCs	May 25, 2021 7:02:23 PM	May 25, 2021 7:02:23 PM	192.168.20.21	4c:71:0d:72:8c:57	75
<input type="checkbox"/> L81ES   1756-L81ES/B	Rockwell PLCs	May 25, 2021 7:02:23 PM	May 25, 2021 7:02:23 PM	192.168.20.25	4c:71:0d:72:8c:57	75
<input type="checkbox"/> L306_V01   5069-L306ERS2/B	Rockwell PLCs	May 25, 2021 7:02:23 PM	May 25, 2021 7:02:23 PM	192.168.20.23	4c:71:0d:72:8c:57	75

2. Click a device in the list. Its right side panel opens.
3. Click the risk score's "see details" button.



The screenshot displays the Cisco Cyber Vision GUI. On the left, a table lists 14 devices and 32 other components. The table has columns for Device, Group, First activity, and Last activity. The first device is a Modicon M580, which is selected. The right pane shows the detailed view for this device, including its risk score (80) and a list of components.

Device	Group	First activity	Last activity
<input checked="" type="checkbox"/> Modicon M580	Schneider PLCs	May 25, 2021 7:04:02 PM	May 25, 2021 7:04:02 PM
<input type="checkbox"/> L71RED_CPU_NAME   1756-L71/B LOGIX5571	Rockwell PLCs	May 25, 2021 7:02:23 PM	May 25, 2021 7:02:23 PM
<input type="checkbox"/> L81ES   1756-L81ES/B	Rockwell PLCs	May 25, 2021 7:02:23 PM	May 25, 2021 7:02:23 PM
<input type="checkbox"/> L306_V01   5069-L306ERS2/B	Rockwell PLCs	May 25, 2021 7:02:23 PM	May 25, 2021 7:02:23 PM
<input type="checkbox"/> L71RED_CPU_NAME   1756-L71/B LOGIX5571	Rockwell PLCs	May 25, 2021 7:02:23 PM	May 25, 2021 7:02:23 PM

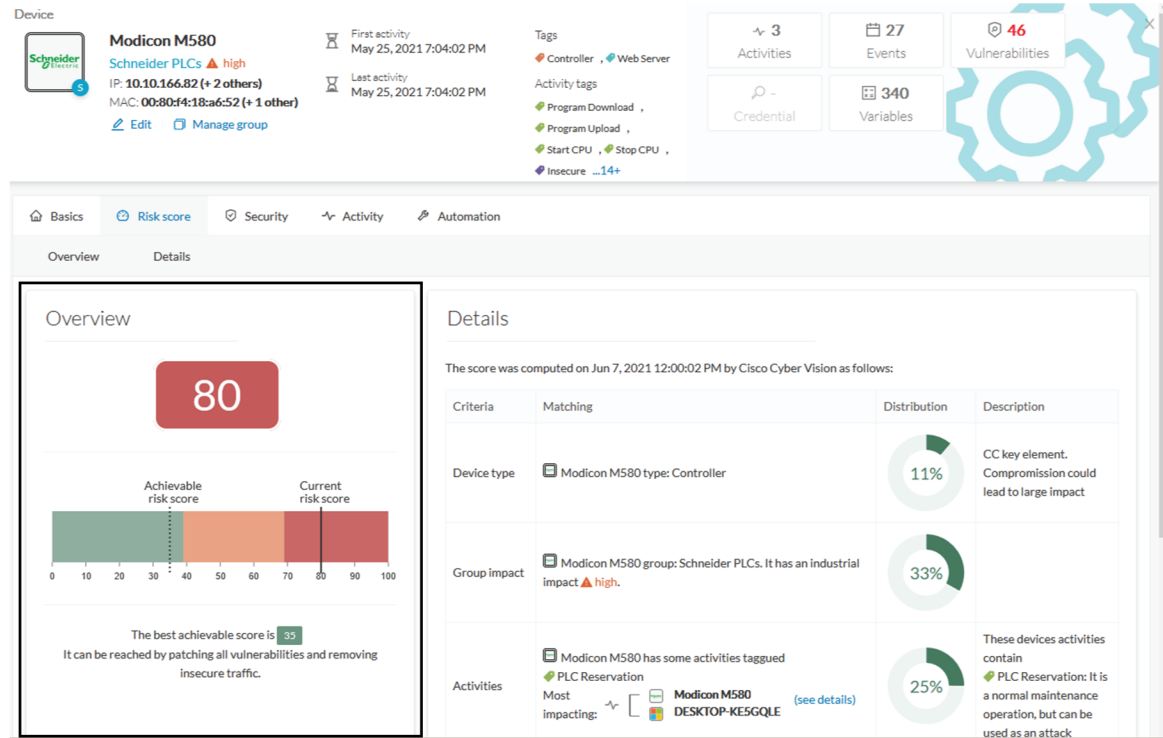
The detailed view for the Modicon M580 shows the following information:

- Device:** Modicon M580 (Schneider PLCs)
- Risk score:** 80 (See details)
- Components:**
  - Telemecanique 192.168.10.1
  - Telemecanique 10.10.166.82
  - Mx80 Ethernet: CPU
  - Telemecanique 18.a6:52
  - Modicon M580
- Properties:** fw-version: 2.80.0

The device's technical sheet opens on the risk score's menu.

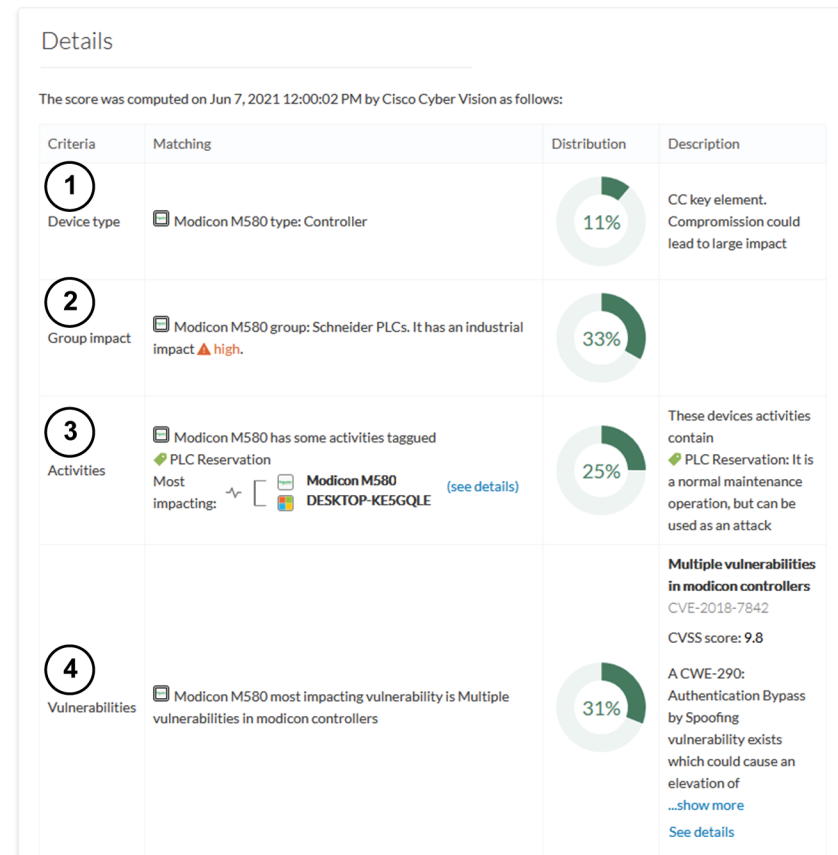
Under overview, you can see the current risk score and the achievable risk score.

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.



Under Details, you have 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 (1) and group impact (2) affect the risk impact variable, meanwhile activities (3) and vulnerabilities (4) affect the risk likelihood.



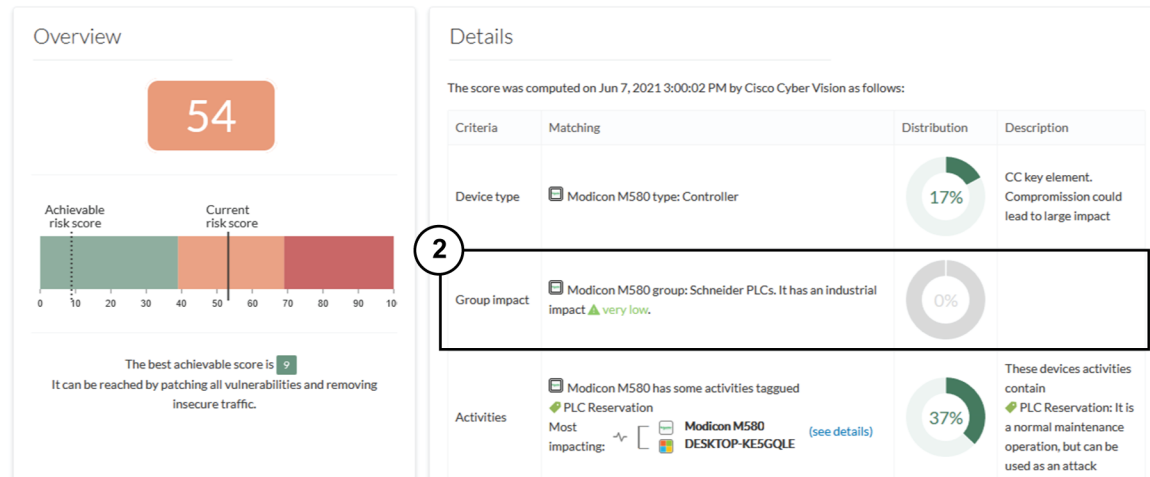
As first information, you have the last time the risk score was computed by Cisco Cyber Vision. Risk score computation occurs once an hour. However, you can force computation by using the following command on the Center shell prompt:

```
sbs-device-engine
```

Below, appears the information retrieved during the last computation.

- Device type **(1)**: Each device type corresponds to a [Tags](#) detected by Cisco Cyber Vision. There is no action to be done at the device type level, because each device tag is assigned with a risk score by default in Cisco Cyber Vision.
- The group impact **(2)**: Action is possible if the device belongs to a group. You can decrease the impact by lowering the industrial impact of the group that the device belongs to.

For example, if I 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 be taken into account at the next risk score computation (once an hour).

- **Activities (3):** The most impactful activity tag is displayed. The risk can be lowered if all potential insecure network activities are removed.
- **Vulnerabilities (4):** Click the "see details" button for more information about how to patch the vulnerabilities and so reduce the device risk score.

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 <span style="color: red;">▲</span> high.
Activities	Modicon M580 has some activities tagged <ul style="list-style-type: none"> <li>PLC Reservation</li> <li>Most impacting: Modicon M580 DESKTOP-KE5GQLE (see details)</li> </ul>
Vulnerabilities	Modicon M580 most impacting vulnerability is Multiple vulnerabilities in modicon controllers

**9.8** CVSS score v2

**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.

## Vulnerability

### What are vulnerabilities?

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

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

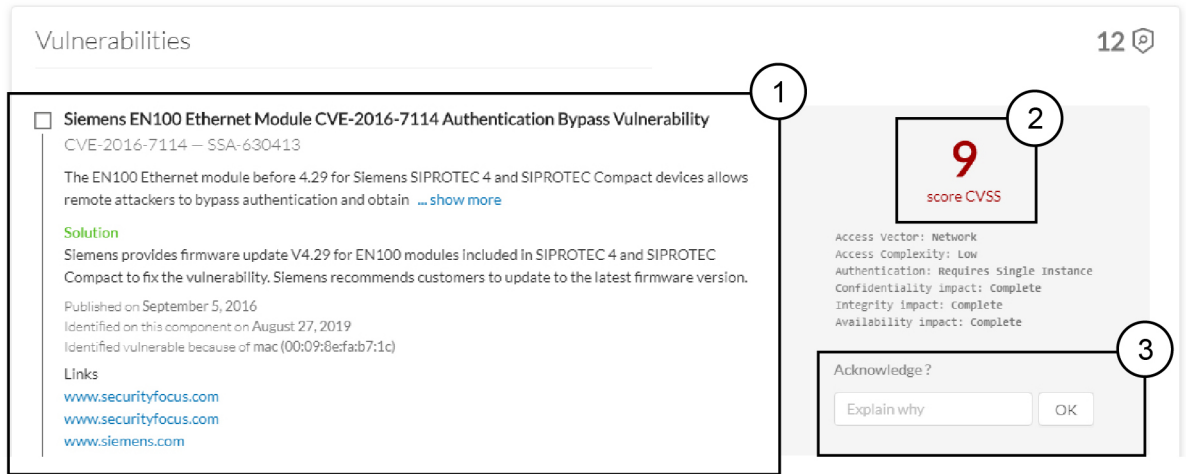


#### Important

It is important to [Knowledge DB](#) in Cisco Cyber Vision as soon as possible after notification of a new version to be protected against vulnerabilities.

### What are vulnerabilities used for?

*Example of a Siemens component's vulnerability visible on its technical sheet under the Security tab:*



Information displayed about vulnerabilities (1) includes the vulnerability type and reference, possible consequences and solutions or actions to take on the network. Most of the time though, it is enough to upgrade the device firmware. Some links to the manufacturer website are also available for more details on the vulnerability.

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

You also have the option to acknowledge a vulnerability (3) if you don't want to be notified anymore about it. This is used for example when a PLC is detected as vulnerable but a firewall or a security module is placed ahead. The vulnerability is therefore mitigated. An acknowledgment can be canceled at any time. Vulnerabilities acknowledgment/cancelation is accessible to the Admin, Product and Operator users only.

**Where to find vulnerabilities?**

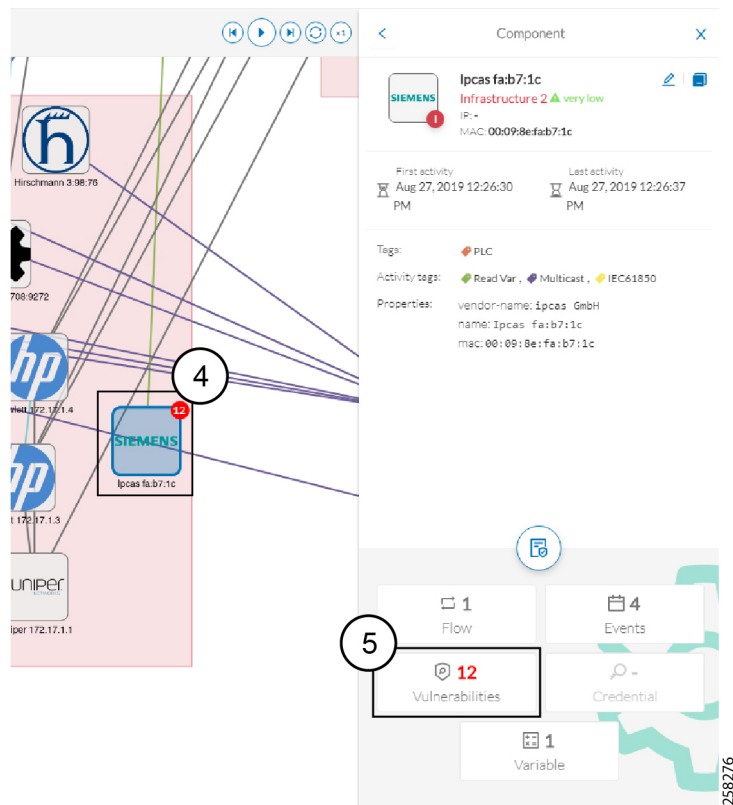
Vulnerabilities are accessible through the [Vulnerabilities](#) of a preset.

Also, you can see vulnerabilities through the Device list. Sort the vulnerability column to bring vulnerable components up:

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

Moreover, vulnerabilities are pointed out in the map by a device or a component with a red counter badge (4). If you click it, its side panel opens on the right with the number of vulnerabilities evidenced in red (5).



Clicking the vulnerabilities displayed in red (5) (in the figure above) opens the device or component's technical sheet with further details about all its vulnerabilities:

Component

**Ipcas fa:b7:1c**  
 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

1 Flow | 4 Events | 12 Vulnerabilities

Credential | 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](http://www.securityfocus.com)  
[www.securityfocus.com](http://www.securityfocus.com)  
[www.siemens.com](http://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

However, you'll be notified each time a device or component is detected as vulnerable by [Events](#). One event is generated per vulnerable component. An event is also generated each time a vulnerability is acknowledged or not vulnerable anymore.

## Events

Events are used to identify and keep track of significant activities on the network and on Cisco Cyber Vision. It can be an activity, a property or a change whether it concerns software or hardware parts.

For instance, an event can be:

- A wrong password entered on Cisco Cyber Vision's GUI.
- A new component which has been connected to the network.
- An anomaly detected on the Monitor Mode.
- A component detected as vulnerable.

Events are visible in the [Events](#).



New events may be generated when the database is updated (in real-time or each time an offline capture is uploaded to Cisco Cyber Vision) with a severity level (Critical, High, Medium and Low) customizable through the [Events](#).

## Credentials

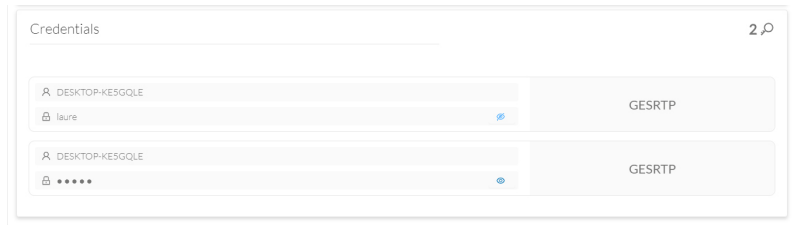
Credentials are logins and passwords that circulate between components over the network. Such sensitive data sometimes carry cleartext passwords when unsafe; and if credentials are visible on Cisco Cyber Vision, then they're potentially visible to anyone on the network. Credentials visibility on Cisco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

*A component's right side panel showing the number of credentials detected:*

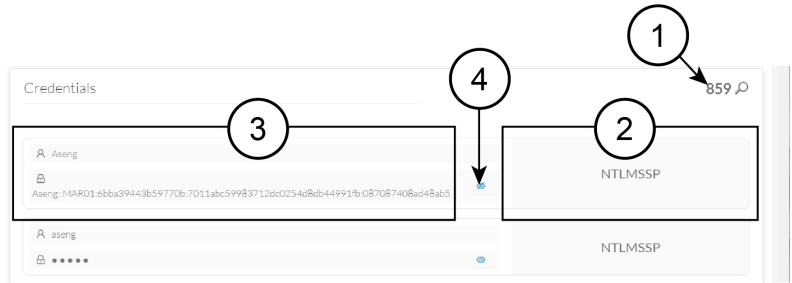
The screenshot displays the Cisco Cyber Vision interface. On the left, a network diagram shows a component labeled 'OSFGSA' with a red '21' badge indicating the number of vulnerabilities. On the right, the 'Component' technical sheet is open for 'OSFGSA'. The sheet includes fields for IP (192.168.6.3), MAC (00:10:18:70:b6:b0), and activity timestamps. Below these are 'Tags' (Windows) and 'Activity tags' (Insecure, Citect Alarm, Citect IO, Citect Trend, Authentication, Ping, Procedure Call, Broadcast, Exception, 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: d62566cd46ff8d4a8540b7e37eeb7b15, and name: OSFGSA. At the bottom, a summary dashboard shows 767 Flows, 245 Events, 21 Vulnerabilities, and 2 Credentials (highlighted with a red box). A 'Variable' section is also visible.

Credential frames are extracted from the network thanks to Deep Packet Inspection. Credentials are then accessible from a component's technical sheet under the security tab. You will find the number of credentials found (1), the protocol used (2), and the user name and password (3) with a button to unveil it (4). If a password appears in clear text, then action should be taken to secure it whether it is hashed or not.

*An unsafe password:*



A hashed password:



## Variable accesses

### What are variable accesses?

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

A variable can be for example the ongoing temperature on an industrial oven. This value is stored in the oven's PLC and can be controlled by another PLC or accessed by a SCADA system for supervisory purpose. The same value can be read by another PLC which controls the heating system.

### What are variable accesses used for?

Reading and writing variables inside a network is strictly controlled. Particular attention should be paid when an unplanned change occurs, especially when it comes to a new written variable. Indeed, such a behavior could be symptomatic of an attacker attempting to take control of the process. Cisco Cyber Vision reports the variables' messages detected on the equipment of the industrial network.

Variable accesses are detailed inside component's technical sheet under a sortable table list, containing:

- The variable's name.
- Its type (WRITE or READ, but not the value itself).
- Which component have accessed the variable.
- The first and last time the component has accessed the variable.

Component: S7 300 Cell 19 (AS)  
 Cell 19 very low  
 IP: 10.239.18.20  
 MAC: 00:1b:1b:02:c4:87

First activity: Sep 25, 2019 12:01:30 PM  
 Last activity: Sep 25, 2019 12:03:01 PM

Tags: PLC  
 Activity tags: Read Var., Write Var., Broadcast., Low Volume., ARP ...2+

19 Flows, 37 Events, 755 Variables

Variables accesses: 755

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

**Where to find variable accesses?**

You can see the number of variable accesses per component on the component list view. You can sort the var column by ascending or decreasing number.

147 Components

Component	Tags	Flows	Vuln	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 84:5ba26	PLC	23	6	13	Siemens AG	-	-	-	-
Fisher 10.5.0.22	PLC, DeltaV	21	0	2	Fisher-Rosemount Systems Inc.	-	-	-	-

Clicking a component from any view opens its right side panel where the number of variables on this component is indicated.

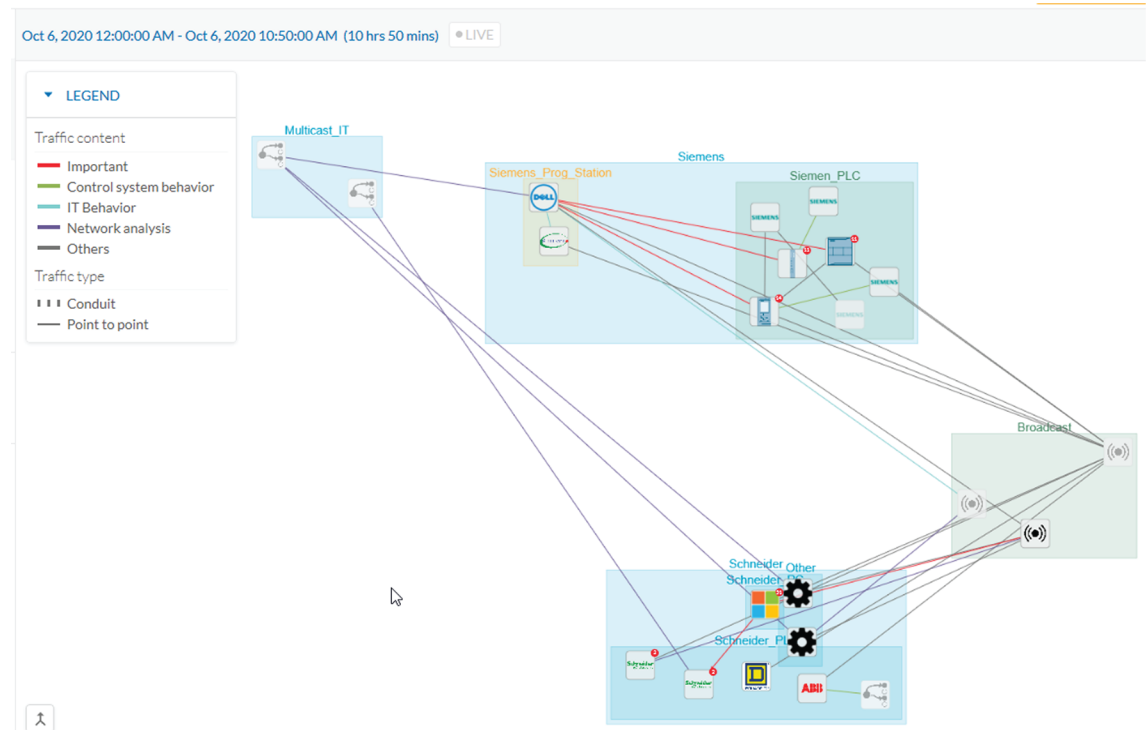
The screenshot displays the Cisco Cyber Vision interface. The top navigation bar shows 'Explore / All data / Component list'. The main area is titled '147 Components' and contains a table with the following columns: Component, Tags, Flows, Vuln, and Var. The table lists various components, including 'S7 300 Cell 19', '10.16.116.254', 'Fisher 10.4.0.14', 'Pump PLC', 'Siemens 84:5b:a6', 'Fisher 10.5.0.22', 'Ipcas fab7:1a', 'Fisher 10.5.0.18', 'Abb 25:8:a2', 'OWS1', 'Ipcas fab7:1c', and 'Schneider 192.168.105.74'. Each row shows associated tags, flow counts, vulnerability scores, and variable counts.

On the right, a detailed view for 'S7 300 Cell 19' is shown. It includes the Siemens logo, component name, status (Cell 19 very low), IP (10.239.18.20), and MAC (00:1b:1b:02:c4:87). It also displays activity logs for 'First activity' and 'Last activity' on Sep 25, 2019. Below this, there are sections for 'Tags' (PLC), 'Activity tags' (Read Var, Write Var, Broadcast, Low Volume, ARP, Profnet, Profnet DCP), and 'Properties' (vendor-name: Siemens AG, name: Siemens 2:c4:87, ip: 10.239.18.20, public-ip: no, mac: 00:1b:1b:02:c4:87). At the bottom right, a summary box shows '19 Flows', '37 Events', 'Vulnerability -', 'Credential -', and a highlighted '755 Variables'.

A detailed list of variable accesses is available under the automation tab on the component's technical sheet (see the first figure above) and on PLC reports.

## Creating and customizing groups

Accessibility: Admin, Product and Operator users



You can organize devices and components into groups as you wish to add meaning to your network representation. For example, this can be done according to the devices' location, process, severity, type, etc. You can also create nested groups inside a parents group, that is, add a group into another group to create several layers and structure the data.

You can use this feature inside the map and the device list views.

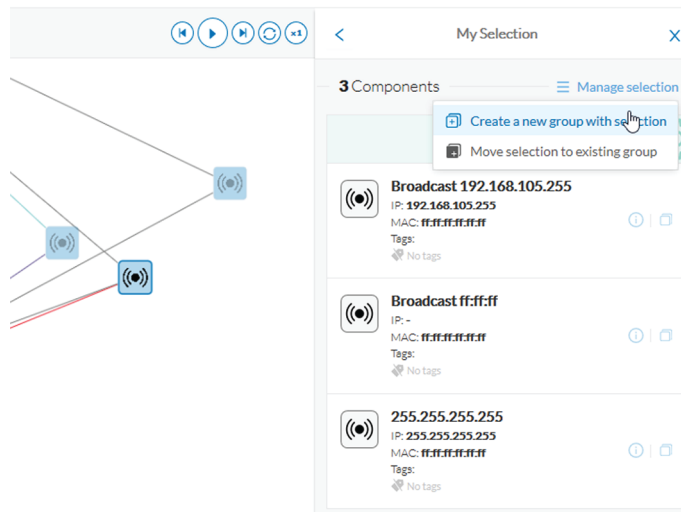
To create a group:

## Procedure

**Step 1** Select one or more devices or components in the map or the device list view.

Tip: To select several components at once in the map, click the devices or components while pressing Shift, or draw a selection box while pressing Ctrl. In the device list view, use the check boxes.

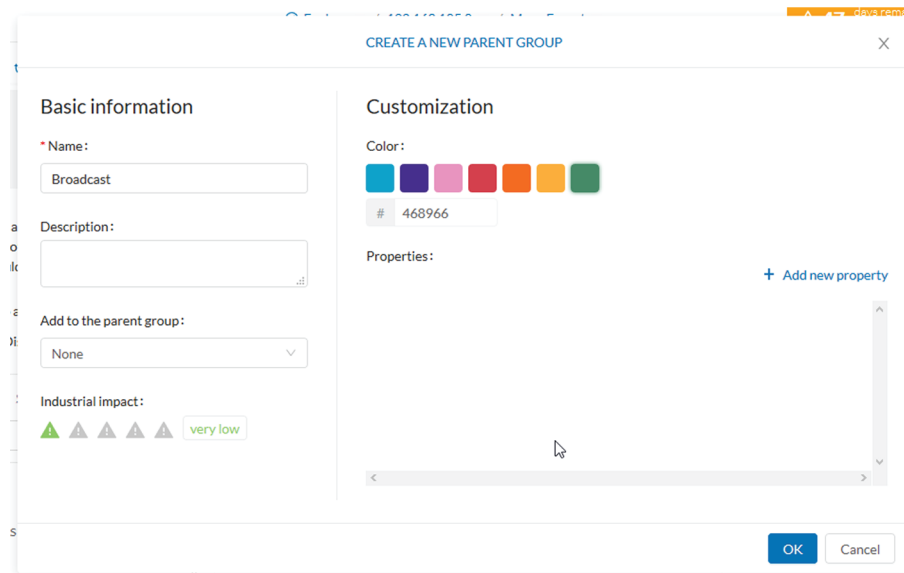
A My Selection panel opens on the right.



**Step 2** Click Manage selection.

**Step 3** Click Create a new parent group.

A Create a new parent group window pops up:



**Step 4** Customize the group by giving it a description, defining its industrial impact (e.g. as opposed to a print server, a PLC that controls a robotic arm is highly critical), changing its color and adding properties.

**Step 5** In addition, you can add the group to a parent group if already created.

#### To create a parent group:

There are several ways to create a hierarchy among groups:

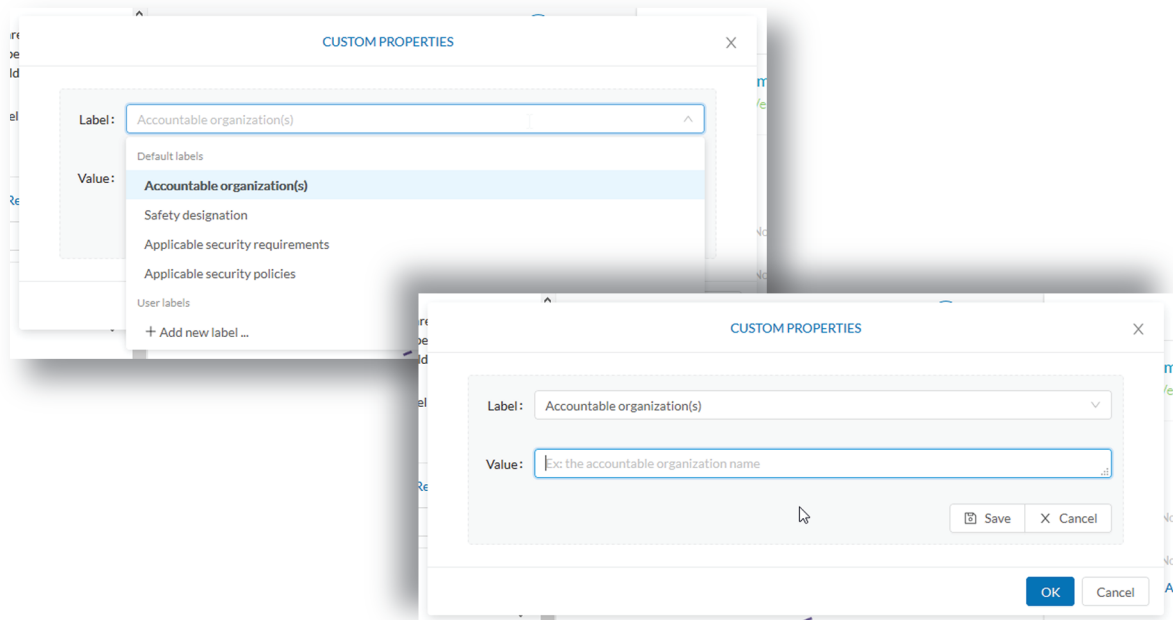
- Select two groups and create a group as indicated before.
- Select a device or a component and move it into a group clicking the Move selection to existing group button.

- Select a group and move it to another group clicking the same button.

### 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.

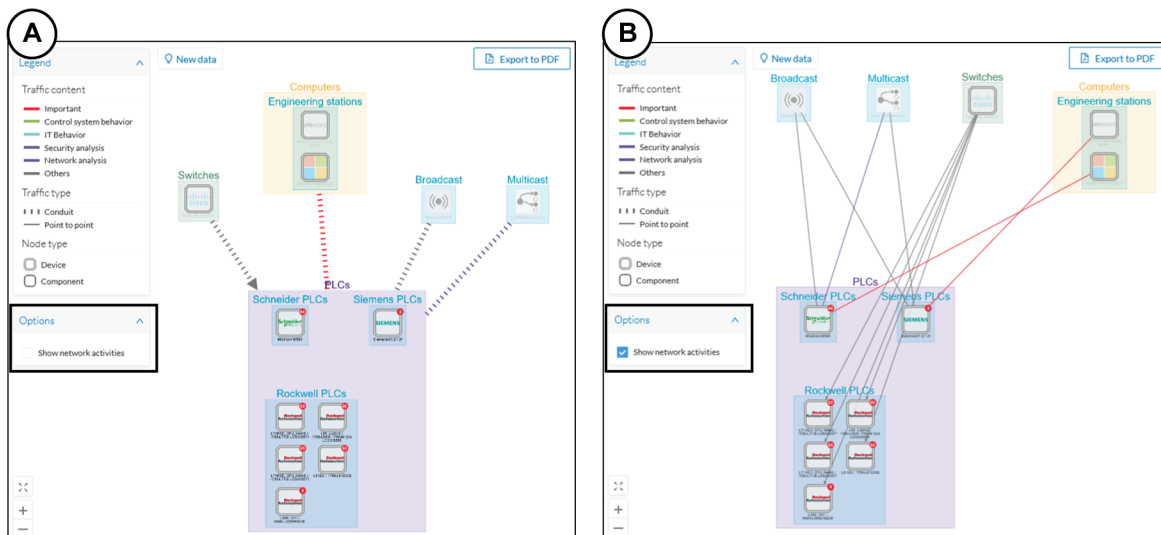
To add properties to a group, select a group in the map and click Edit or Add properties. Then, choose/define a label and add a value.



### Aggregated activities or conduits:

When devices and components are placed inside groups, activities are by default aggregated to enhance visibility. Aggregated activities are called [Conduit](#).

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



Lock/unlock a group:

Locking a group:

- prevents components from being added to or removed from the group.
- prevents a group to be deleted.

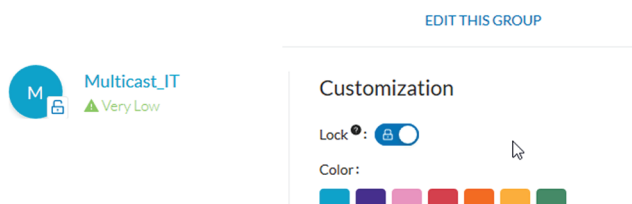
To switch on/off the Lock toggle button,

**Step 6** Click a group.

**Step 7** Click the Lock button on the group's icon.

or

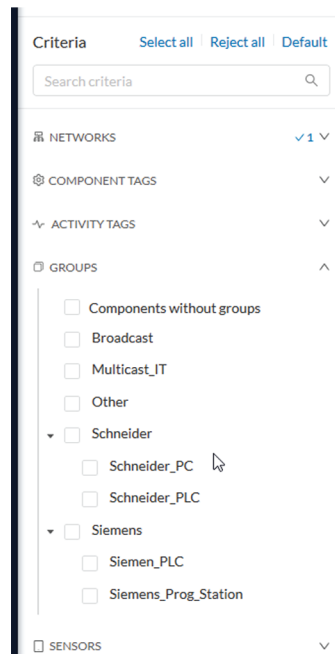
Click the Edit button on the group's right side panel and toggle on/off the Lock button.



**Step 8** **Groups used as criteria to filter data in Cisco Cyber Vision:**

Any groups created will be 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. As opposed to passive traffic capture principles on which Cisco Cyber Vision is relying on and was originally built around, Active Discovery is an optional feature that explores traffic in an active way. The reason is, some components are sometimes not found by Cisco Cyber Vision because those devices haven't been communicating from the moment the solution started to run on the network. Moreover, some information like firmware version can be difficult to obtain because they are not exchanged often between components.

With Active Discovery enabled on selected presets, broadcast messages will be sent to the targeted subnetwork through the sensors to speed up network discovery. Then, returned responses will be analyzed through Deep Packet Inspection and tagged as Active Discovery and additional information. Thus, components and activities will be clarified with additional and more reliable information than what is usually found through passive DPI.

Active Discovery's jobs are launched every 10 minutes. In case Active Directory is enabled on several presets that use the same sensor, the job is executed only once to avoid traffic load. You can also choose which broadcast protocol will be active on the subnetwork.

Active Discovery supports three broadcast protocols, which are EtherNet/IP (Rockwell), and Profinet and S7 Discovery (Siemens).

Active Discovery is available on:

- Cisco Catalyst 9300 Series Switches.
- Cisco Catalyst IE3400 Rugged Series Switches.

- Cisco Catalyst IE3300 10G Rugged Series Switches.
- Cisco IC3000 Industrial Compute Gateway.

To use Active Discovery, you must first perform a few configurations:

## Procedure

**Step 1** Enable the feature on a sensor, and set the subnetwork to be monitored.

**Step 2** Enable Active Discovery on a preset using the sensor set with Active Discovery and choose which protocols to be broadcasted on the subnetwork.

To enable Active Discovery on sensors:

**Step 3** On Cisco Cyber Vision, navigate to Admin > Sensors.

The sensors list displays.

**Step 4** Check the sensors' Active Discovery status:

- **Unavailable:** This sensor model does not support Active Discovery (i.e. Cisco IR1101 Integrated Services Router Rugged); The Cisco Cyber Vision IOx Application is not up-to-date on the device (version must be 3.2.0 or newer); The IOx Application installed does not include Active Discovery (two packages are available, one includes Active Discovery, the other does not). For more information, refer to the relevant Cisco Cyber Vision Network Sensor Installation Guide.
- **Available:** IOx app's version is up-to-date on the device and using Active Discovery is possible.
- **Running:** The sensor is scanning the network sending broadcast at the moment.  
The sensor's Active Discovery status must be in Available to continue the procedure.

**Step 5** Click the Active Discovery button.

Name	IP	Version	Status	Processing status	Active Discovery status	Capture Mode®	Uptime
IE3400_ActivDisc	192.168.0.161	3.2.0+202010190818	Connected	Pending data	Available	All	13d 6h 43m 51s

S/N: FOC2401V07N  
 Name: IE3400\_ActivDisc  
 IP address: 192.168.0.161  
 Version: 3.2.0+202010190818  
 System date (UTC): Tuesday, October 20, 2020 1:44 PM  
 Status: Connected  
 Processing status: Pending data  
 Active discovery: Available

Deployment: Sensor Management Extension  
 Uptime: 13d 6h 43m 51s  
 Capture mode: All  
 ● Start recording sensor  
 📶 No statistics available. Is the sensor clock synchronized?

Remove
Active Discovery
Capture Mode

UPDATE CISCO DEVICES
+ DEPLOY CISCO DEVICE
+ INSTALL SENSOR MANUALLY
IMPORT OFFLINE FILE

The Active Discovery configuration window pops up.

**Step 6** Set the interface corresponding to a subnetwork monitored by the sensor filling the following information:

- The subnetwork IP address.
- The subnet mask.
- The VLAN.

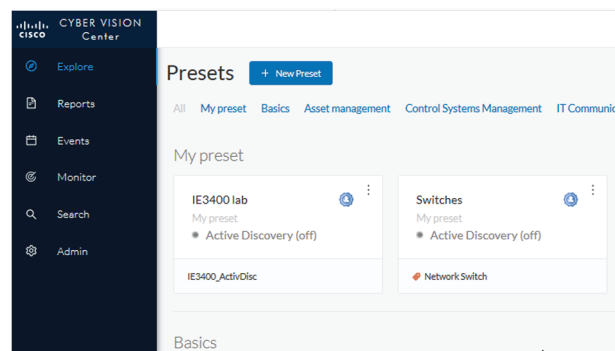
You can set as many interfaces as subnetworks monitored by the sensor.

**Step 7** Click Configure.

To enable Active Discovery and set protocol scanning on a preset:

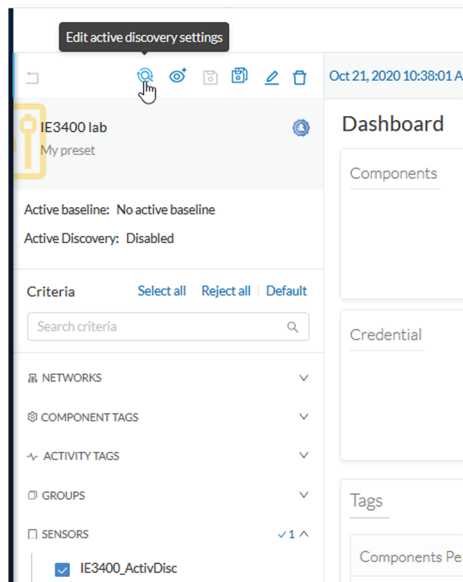
Active Discovery is not available on default presets (under Basics). To use it, you must use a custom preset (under My Presets) or create a new preset. You can create it from a default preset.

**Step 8** Access or create a custom preset in the Explore menu.

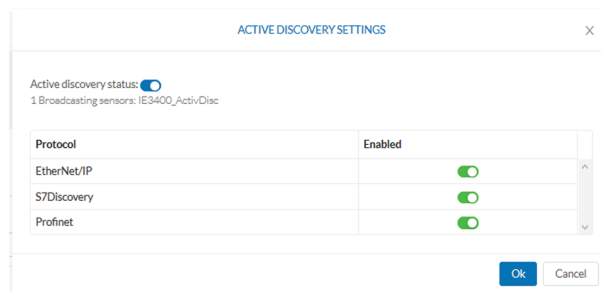


In the example, we use the IE3400 lab preset that we created with the sensor filter selected, previously configured with Active Discovery.

**Step 9** Click the Edit Active Discovery settings button on the top left corner.



The Active Discovery settings window pops up.



**Step 10** Use the toggle button to enable Active Discovery.

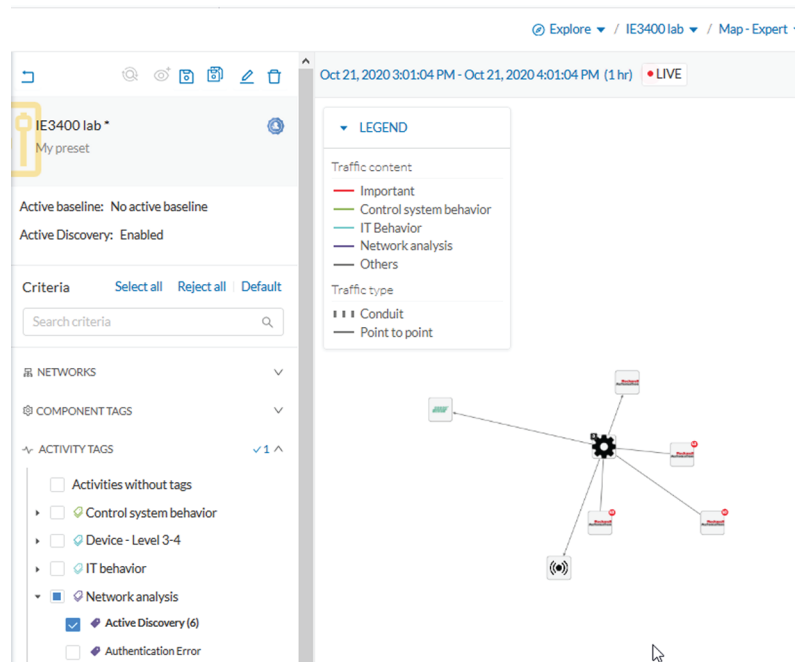
**Step 11** Use the toggle buttons to enable the protocols you want the subnetwork to be scanned with.

To identify elements detected by Active Discovery:

**Step 12** In the criteria area > Activity tags > Network Analysis, select the Active Discovery tag.

All components and activity tagged as Active Discovery, and so detected thanks to the feature, display.

*Elements found and other related elements detected by Active Discovery in the Map - Expert view:*



Components, activities and sensors detected by Active Discovery are tagged as Active Discovery.

*Components related to Active Discovery scanning in the Component list view:*

Explore / IE3400 lab / Component list

89 days remaining Evaluation Mode

Oct 21, 2020 3:13:34 PM - Oct 21, 2020 4:13:34 PM (1 hr) LIVE

7 Components

Export to CSV

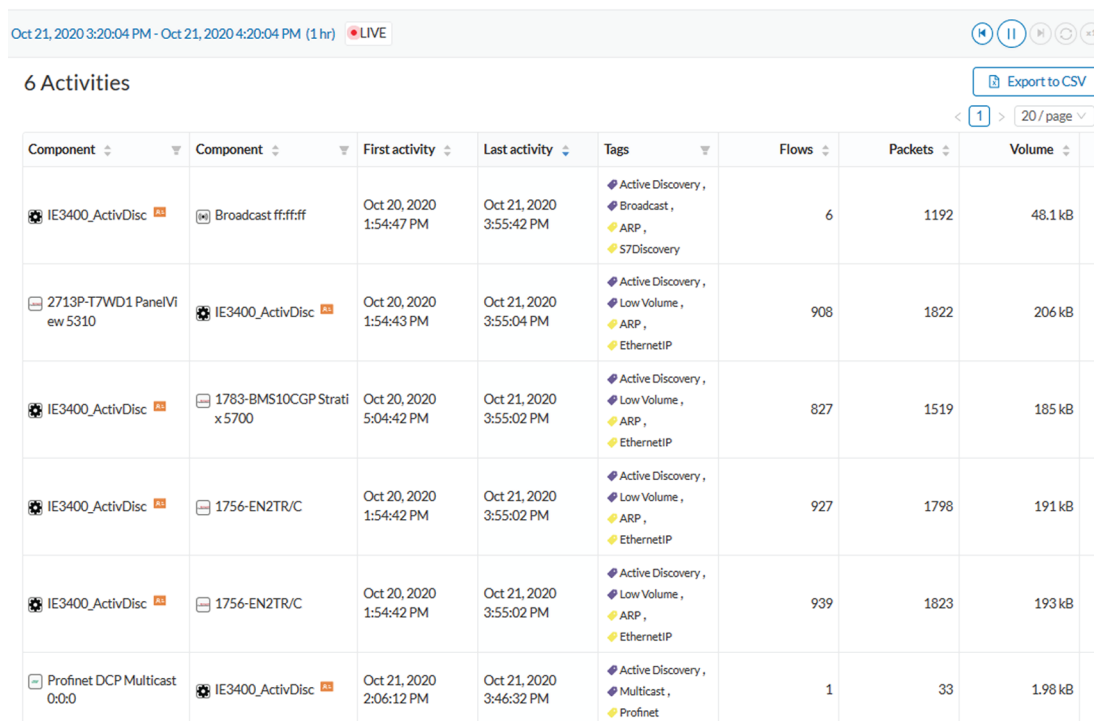
Component	Group	First activity	Last activity	IP	MAC	Tags
255.255.255.255	-	Oct 20, 2020 1:47:45 PM	Oct 21, 2020 3:49:46 PM	255.255.255.255	ff:ff:ff:ff:ff:ff	IPv4 Link Local
Rockwell f0:30:1f	-	Oct 20, 2020 1:49:29 PM	Oct 21, 2020 3:48:53 PM	172.16.0.201	5c:88:16:f0:30:1f	Rockwell Automation
Rockwell dd:55:c8	-	Oct 20, 2020 1:48:29 PM	Oct 21, 2020 3:48:40 PM	172.16.0.205	00:1d:9c:dd:55:c8	Rockwell Automation
Rockwell 82:b2:f9	-	Oct 20, 2020 1:48:28 PM	Oct 21, 2020 3:48:31 PM	172.16.0.203	f4:54:33:82:b2:f9	Rockwell Automation
IE3400_ActivDisc	-	Oct 20, 2020 1:54:42 PM	Oct 21, 2020 3:46:32 PM	-	52:54:dd:67:7d:09	IPv6 Link Local, Cyber Vision Sensor
Profinet DCP Multicast 0:0:0	-	Oct 21, 2020 1:54:39 PM	Oct 21, 2020 3:46:32 PM	-	01:0e:cf:00:00:00	No tags
1783-BMS10CGP Stratix 5700	-	Oct 20, 2020 1:54:42 PM	Oct 21, 2020 3:45:02 PM	172.16.0.200	5c:88:16:45:0e:c0	Rockwell Automation

**Step 13**

- Components discovered thanks to Active Discovery are tagged as Active Discovery. This is not the case here because these components had already been detected thanks to passive traffic capture. However, they are shown here because their activities have been detected through Active Discovery.

- Sensors are in passive traffic capture often tagged as Engineering Station or Scada Station, which is incorrect. With Active Discovery, these tags are removed and the sensor is tagged as Cisco Cyber Vision Sensor.

*Activities related to Active Discovery scanning in the Activity list view:*



Component	Component	First activity	Last activity	Tags	Flows	Packets	Volume
IE3400_ActivDisc	Broadcast ffff:ff	Oct 20, 2020 1:54:47 PM	Oct 21, 2020 3:55:42 PM	Active Discovery, Broadcast, ARP, S7Discovery	6	1192	48.1 kB
2713P-T7WD1 PanelView 5310	IE3400_ActivDisc	Oct 20, 2020 1:54:43 PM	Oct 21, 2020 3:55:04 PM	Active Discovery, Low Volume, ARP, EthernetIP	908	1822	206 kB
IE3400_ActivDisc	1783-BMS10CGP Stratix 5700	Oct 20, 2020 5:04:42 PM	Oct 21, 2020 3:55:02 PM	Active Discovery, Low Volume, ARP, EthernetIP	827	1519	185 kB
IE3400_ActivDisc	1756-EN2TR/C	Oct 20, 2020 1:54:42 PM	Oct 21, 2020 3:55:02 PM	Active Discovery, Low Volume, ARP, EthernetIP	927	1798	191 kB
IE3400_ActivDisc	1756-EN2TR/C	Oct 20, 2020 1:54:42 PM	Oct 21, 2020 3:55:02 PM	Active Discovery, Low Volume, ARP, EthernetIP	939	1823	193 kB
Profinet DCP Multicast 0:0:0	IE3400_ActivDisc	Oct 21, 2020 2:06:12 PM	Oct 21, 2020 3:46:32 PM	Active Discovery, Multicast, Profinet	1	33	1.98 kB

Activities detected by Active Discovery, which is meant to enrich data, are tagged as Active Discovery and as S7 Discovery, EtherNet/IP or Profinet in addition to other tags detected by passive traffic capture.

Tip: Register this selection as a preset to be informed about any new Active Discovery's elements found on the subnetwork.

Tip: You can see all Active Discovery effects on the network consulting the Active Discovery Activities preset. You will see activities tagged as Active Discovery, the components involved, and the sensors.



## CHAPTER 4

# Navigating through Cisco Cyber Vision

---

- [Home](#), on page 49
- [Explore](#), on page 54
- [Reports](#), on page 69
- [Events](#), on page 71
- [Monitor](#), on page 73
- [Search](#), on page 102
- [Admin](#), on page 104
- [System statistics](#), on page 169
- [My settings](#), on page 174

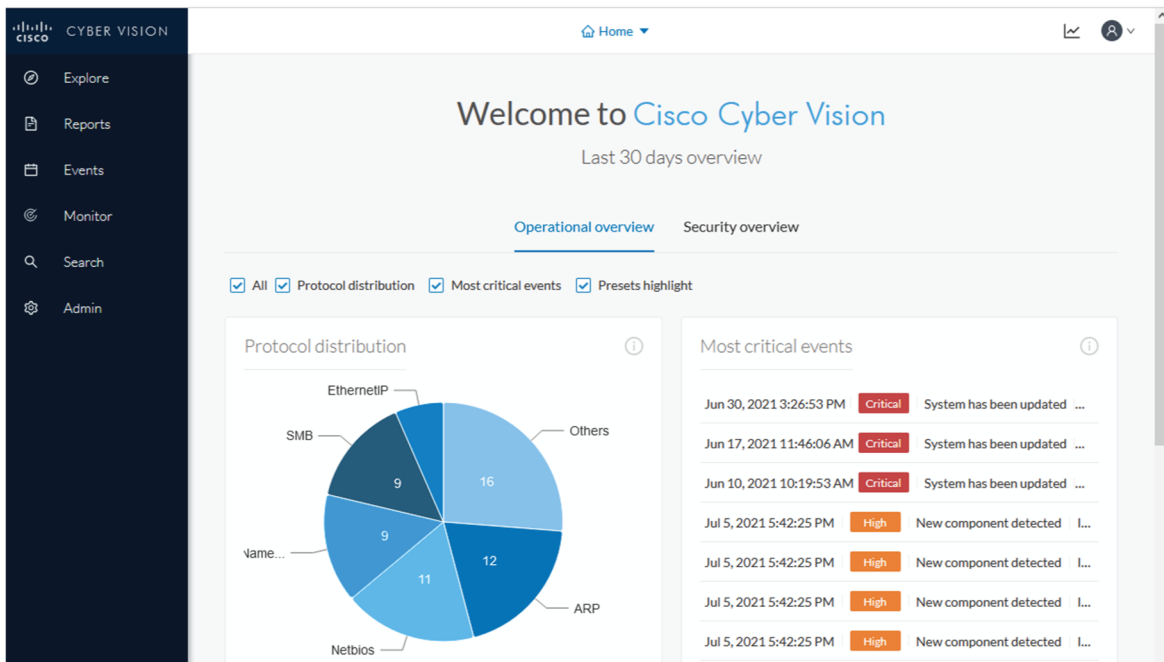
## Home

This page is where you'll land as logging in Cisco Cyber Vision.

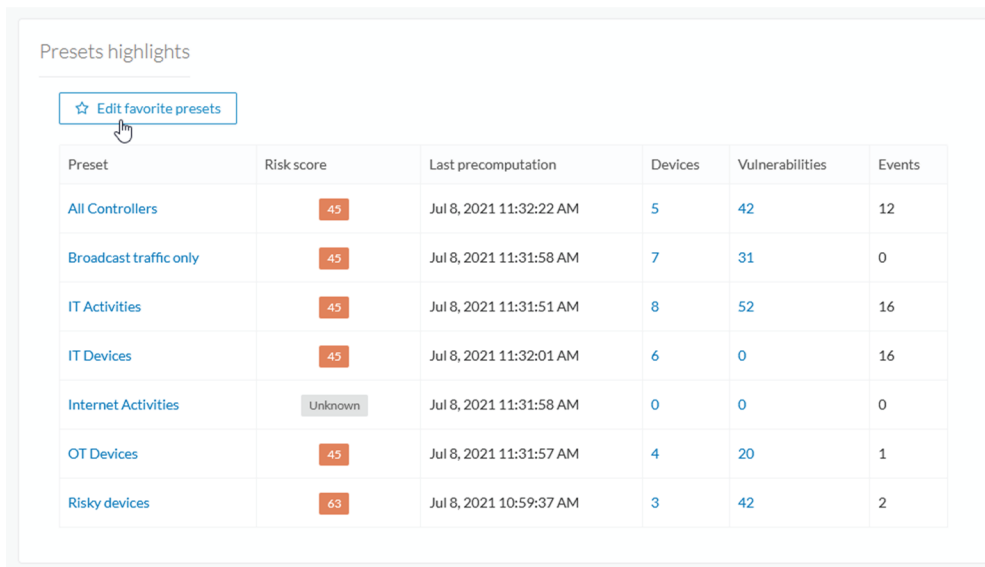
The home page displays an operational and a security overview of the industrial network over the last month.

You can edit which information is displayed by ticking/unticking the different boxes available.

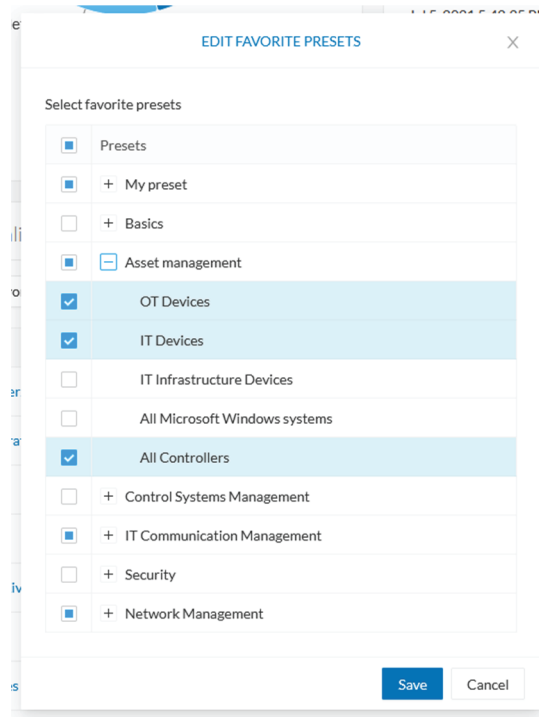
In the operational overview, you will find a pie chart with the protocol distribution and a list of the most critical events.



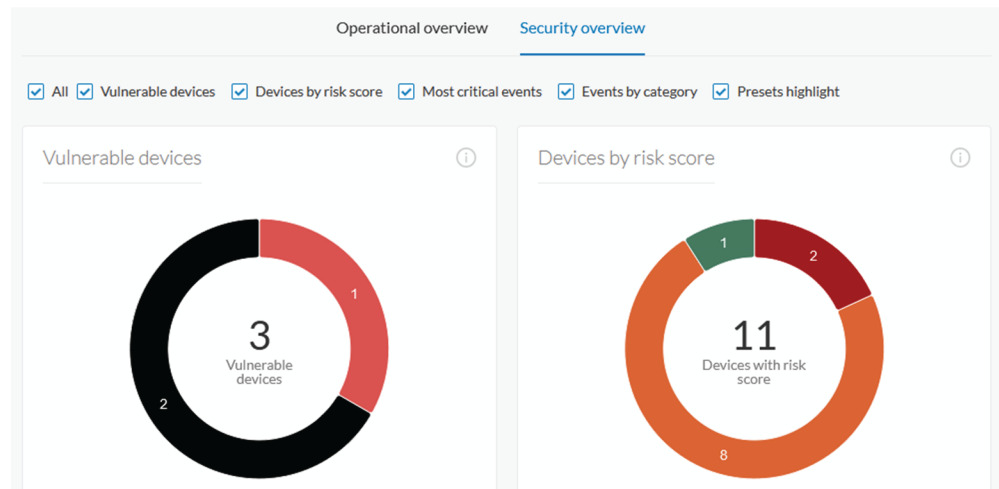
Below, a preset highlight you can edit to display your favorite presets.







In the security overview, you will find a pie chart representing the vulnerable devices per severities, and a pie chart representing the devices per risk score.



Below, a list of the most critical events, and events classified per category, as well as a preset highlight that you can edit.

### Most critical events

- Jun 30, 2021 3:26:53 PM Critical System has been updated ...
- Jun 17, 2021 11:46:06 AM Critical System has been updated ...
- Jun 10, 2021 10:19:53 AM Critical System has been updated ...
- Jul 5, 2021 5:42:25 PM High New component detected L...
- Jul 5, 2021 5:42:25 PM High New component detected L...
- Jul 5, 2021 5:42:25 PM High New component detected L...
- Jul 5, 2021 5:42:25 PM High New component detected L...
- Jul 5, 2021 5:42:25 PM High New component detected L...
- Jul 5, 2021 5:42:25 PM High New component detected L...
- Jul 5, 2021 5:42:25 PM High New component detected L...

### Events by category

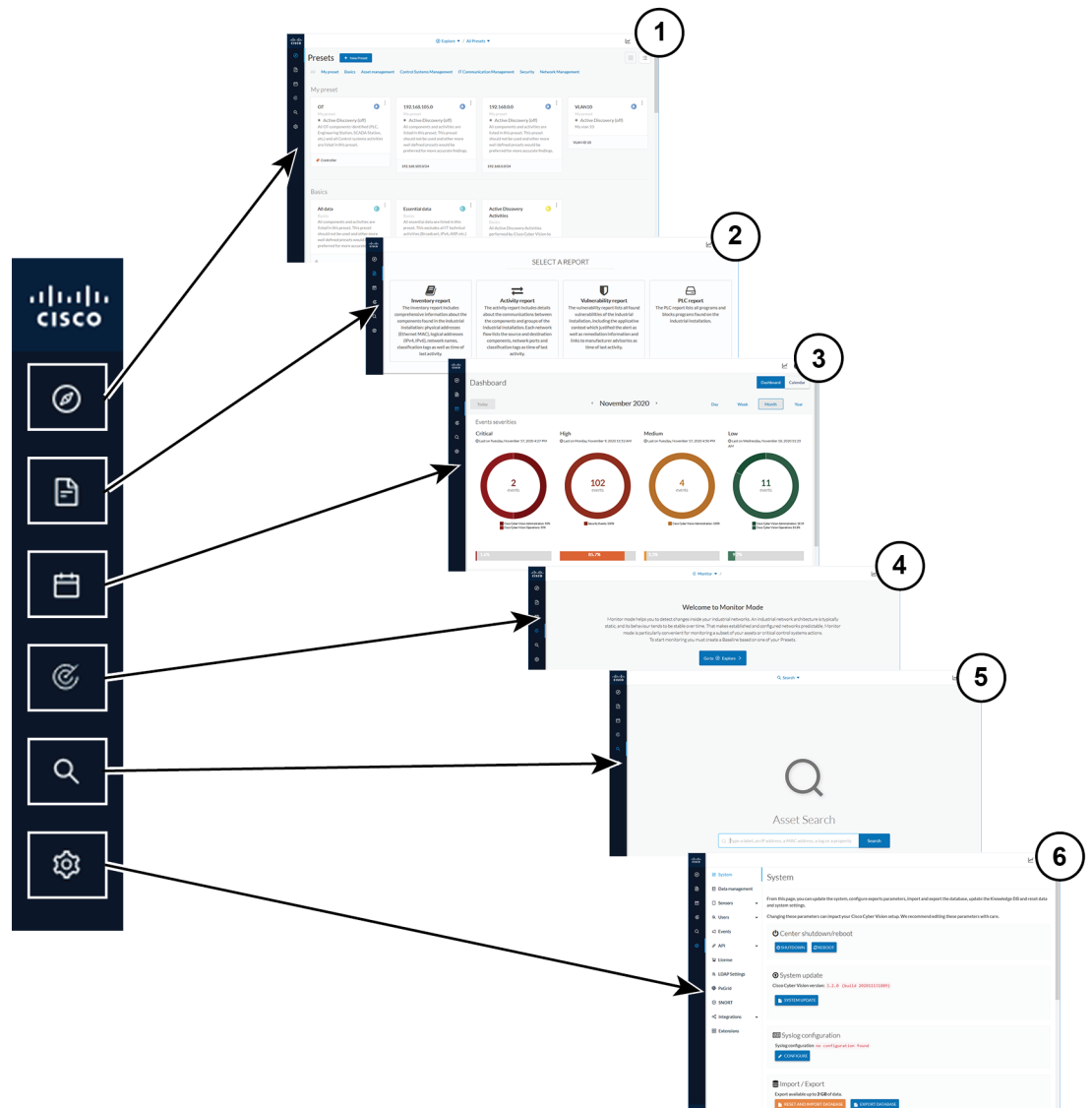
Category	Count
Security Events	19

### Presets highlights

☆ Edit favorite presets

Preset	Risk score	Last precomputation	Devices	Vulnerabilities	Events
All Controllers	45	Jul 8, 2021 11:32:22 AM	5	42	12
Authentication Activities	Unknown	Jul 8, 2021 11:31:58 AM	0	0	0

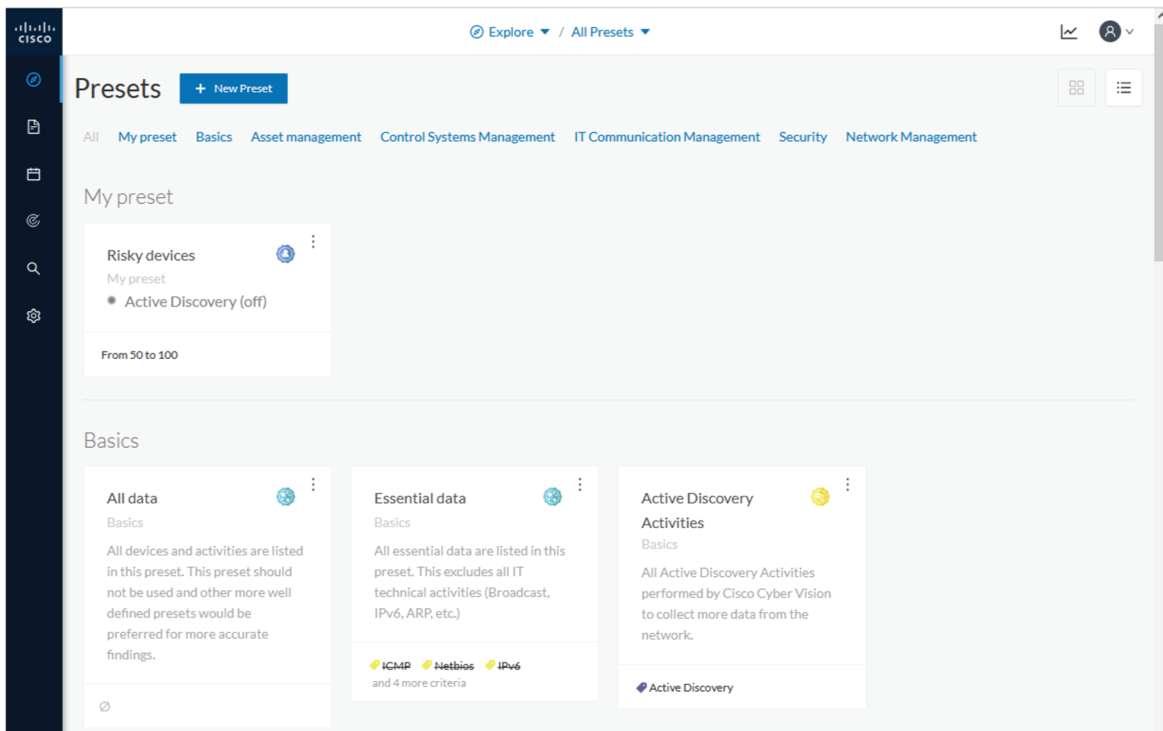
The navigation bar on the left gives access to all other main pages of Cisco Cyber Vision:



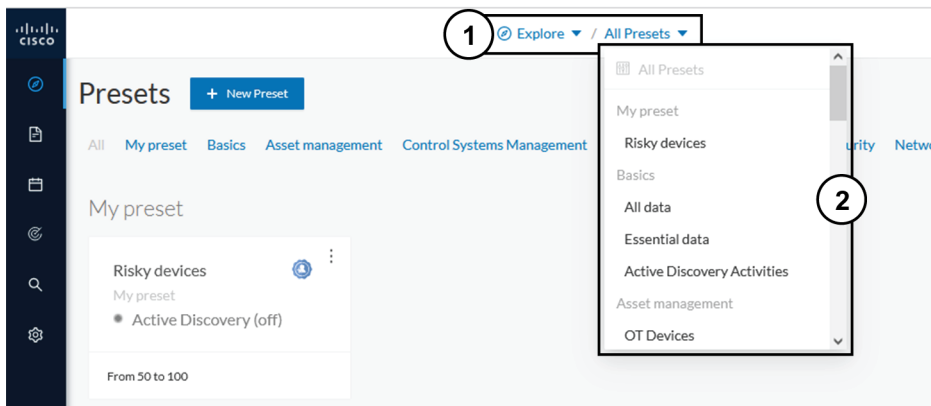
- Explore (1): This button leads to the overview of [Explore](#) by defaults or configured.
- Reports (2): This button leads to the [Reports](#) to export valuable information about the industrial network.
- Events (3): This button leads to the [Events](#) which contains graphics and a calendar of all events generated by Cisco Cyber Vision.
- Monitor (4): This button leads to the [Monitor](#) to perform and automatize data comparisons of the industrial network.
- Search (5): This button leads to the [Search](#) to look for precise data in the industrial network.
- Admin (6): This button leads to the [Admin](#).

# Explore

Presets is a page containing an overview of all presets existing in Cisco Cyber Vision whether they are present by default or part of users' customizations. You can access this page by clicking the Explore button on the left navigation bar.



The top navigation bar (1) allows you to access the different presets (2) and then reach their different Preset views.



## Preset views

There are several types of views which relate to different perspectives:

- The dashboard:

The [Dashboard](#) is a unique view which is displayed by default when accessing a preset. It offers an overview of data found by the preset. The fact that it's a tag-oriented view allows you to have a general insight of the network without going into deep and technical details.

- The map:

The [Map](#) is a visual data view of the industrial network that gives you a broad insight of how components are connected to each others.

- Lists:

Lists are views specialized whether on devices or activities. These views provide classic but powerful data filtering to match what you are looking for. For more information, refer to the [Device and activity lists](#).

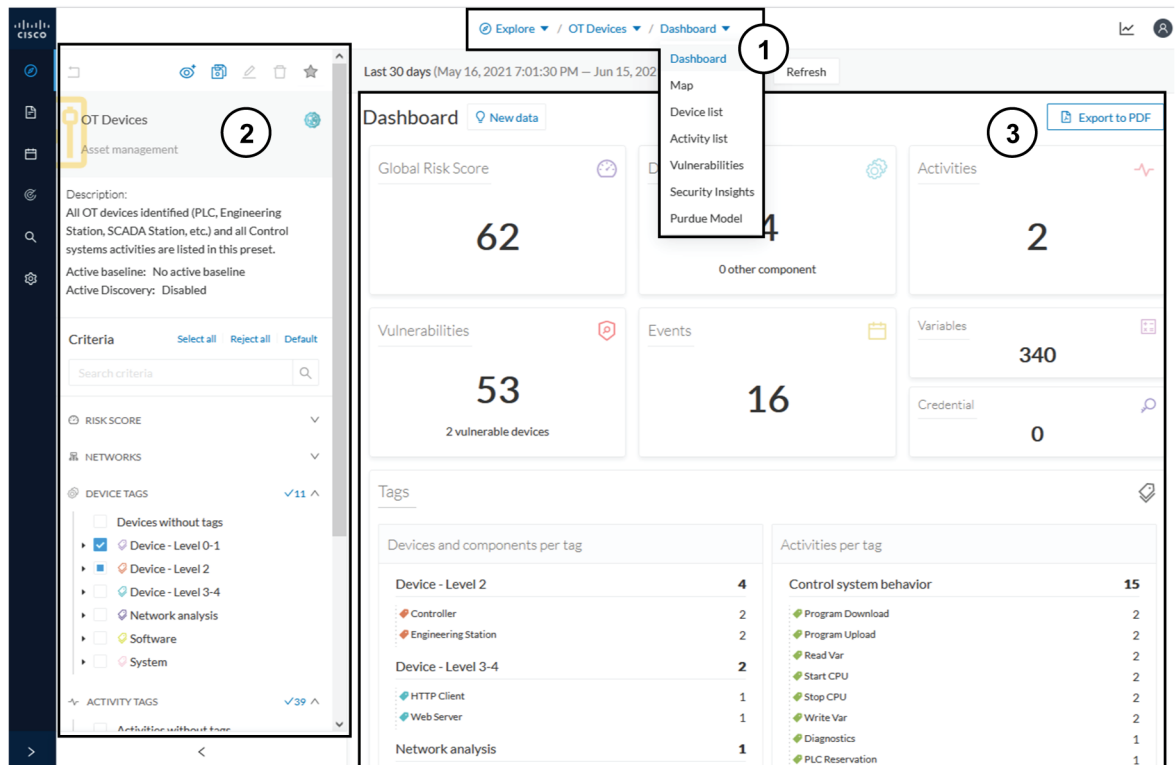
- The Purdue Model:

In this map, the components of a preset are distributed among the layers of the [Purdue Model](#) architecture.

Views are always structured as shown below:

- The top navigation bar **(1)**, which allows you to easily switch between the different views thanks to its menu.
- The filtering area on the left **(2)**, which allows you to modify and manage the preset by adapting criteria and registering changes.
- The view you're on **(3)**, which dynamically evolves as you change and save criteria.

*Example of the OT Devices preset on the dashboard view:*



Display of preset views has been optimized to avoid lags, solve performance issues and prevent the application from crashing, especially in case of large data flow.

The entire database used to be checked over and over. Elements such as components, tags and activities were counted repeatedly and displayed simultaneously in the preset views, which were continuously refreshed.

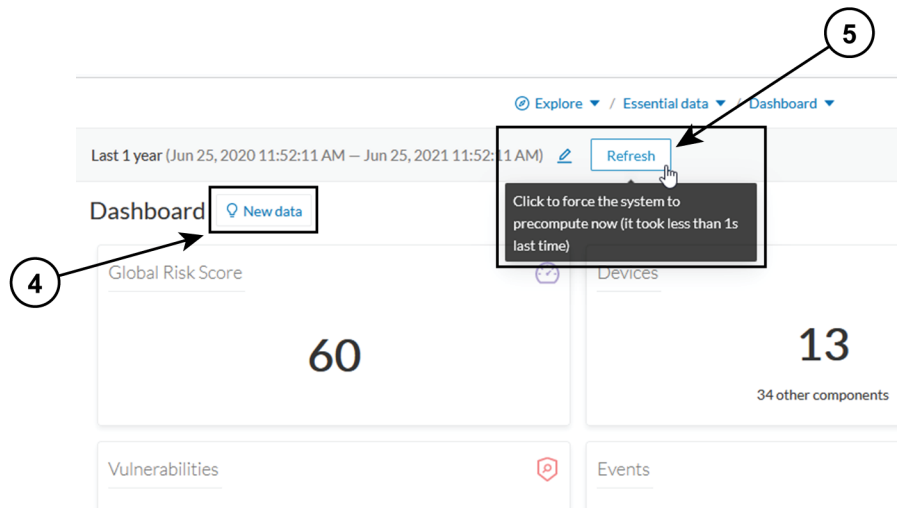
As of Cisco Cyber Vision version 4.0.0, data found is stored instead of being directly displayed in the preset views. Preset views refresh occurs only when necessary or requested to not overload the application display. The elements visible in the preset views are actually data from the previous computation, which means that data displayed in the GUI and the data stored in the database, are asynchronous. This actually lightens data load on preset views.

In addition, computation adapts to the preset consultation frequency. That is, a preset often viewed by users will be computed accordingly. Instead, the system will not compute presets that are never used.

When on a preset, data are regularly computed thanks to an automatized data computation running in the background. However, this will 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 (4) appears each time a new computation is done and refresh the view as you click on it. The view will be updated to the last computation done in the system, which means that using this button won't necessarily show new data.
- The Refresh button (5) forces data computation and refresh the preset view. This task requires more resources and should be used in the following cases:
  - If you expect that new data has been found during the most recent computation (e.g. a new device plugged into the network).

- If custom data such as groups or names have been changed (e.g. if adding a device into a group).



In any cases, the computation is forced and the view is refreshed as you navigate in the application. For example, when accessing another preset or when moving from one view to another.

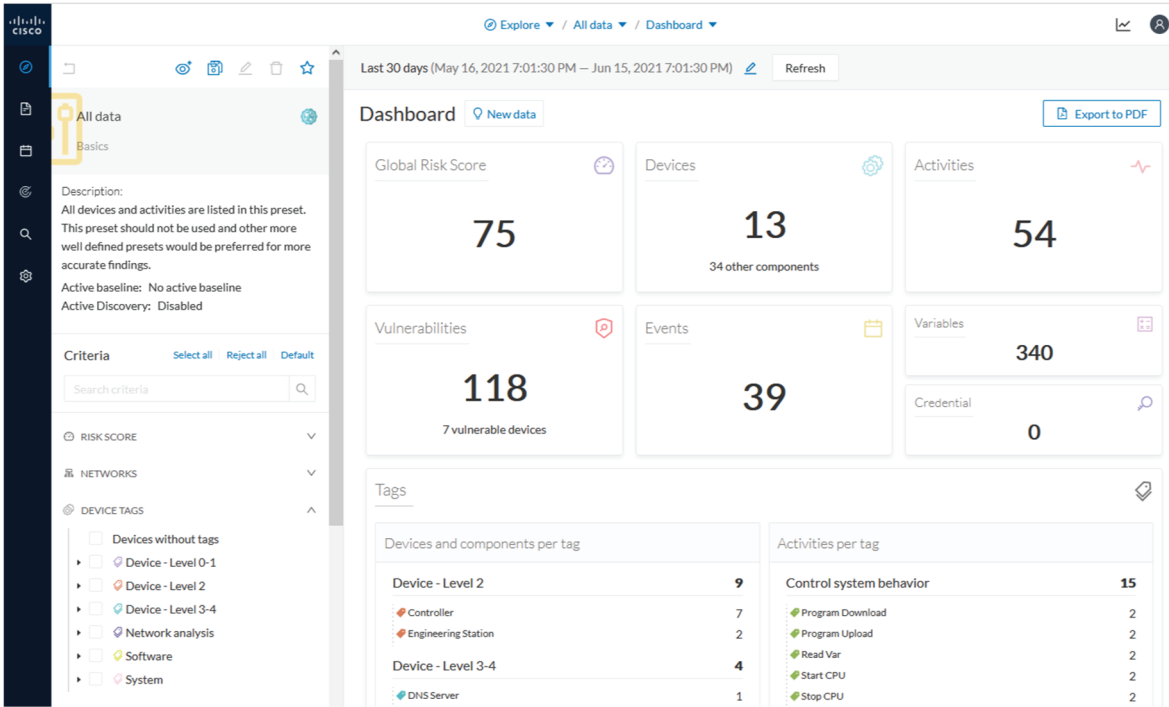


**Note** New preset view optimization has also an impact on how criteria are handled in preset views. To be taken into account and thus for the computation to be forced, criteria must be saved as a new preset if acting from a default preset, or saved if in a custom preset.

## Dashboard

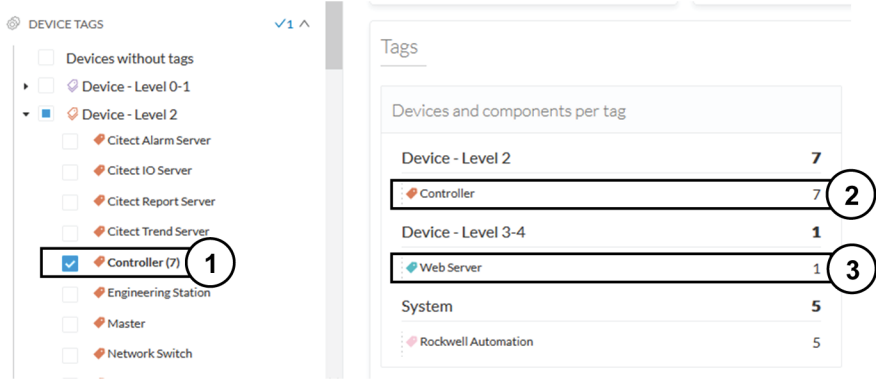
The dashboard is the view by default when opening a preset. It gives you an overview of the preset's global risk score, number of devices, activities, vulnerabilities, events, variables and credentials.

The dashboard is also a tag-oriented view. It's an overview of all tags found -independently of the ones set as criteria- with the number of devices and activities found per tag.



**Example:** For the purpose of the whole example given below, we access the All data preset, select the Controller tag as criteria (under Device - Level 2), and save the selection as "Example: Controller tag".

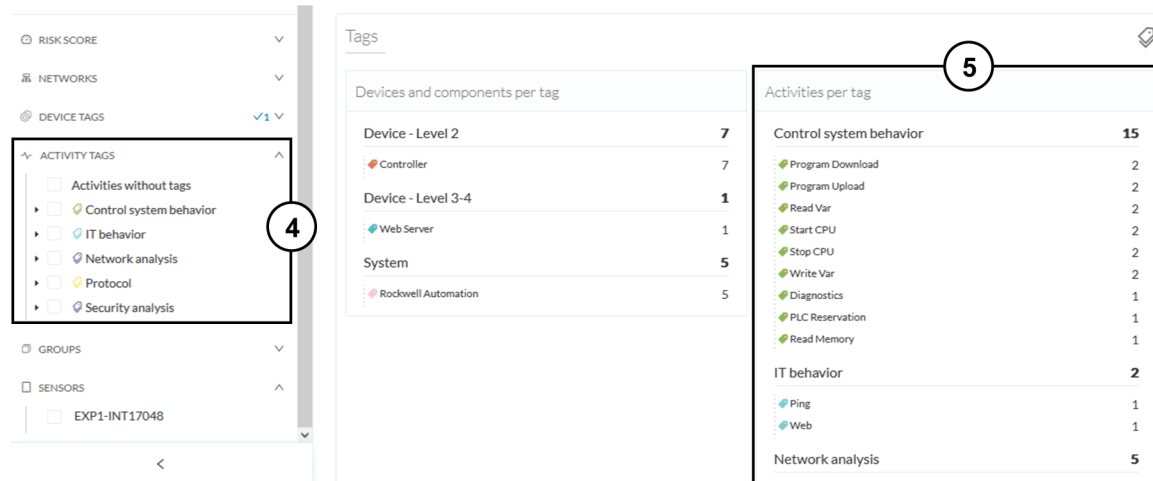
**Devices per tag:** The number in brackets indicates there are 7 devices tagged as Controller (1). On the dashboard, you see this result accordingly (2). One device is tagged as Web Server (3). This means that one of the Controller is a Web Server. Following this logic, we can say that five of the Controllers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



If you want to know more about one of these devices, switch to the [Device and activity lists](#) and reach them using the filter available in the tags column.

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





If you want to know more about one of these activities, switch to the [Device and activity lists](#) and reach them using the filter available in the tags column.

## Device and activity lists

The device and activity lists are two specialized and oriented views. Even though they are legated and share a large number of data, devices and activities are split in two different views to facilitate comprehension and visualization of data.

These views provide general information and advanced technical data about each element found in the preset. Check at the differences between the device and activity views.

*The All Controllers preset in the device list view:*

Explore / All Controllers / Device list

Last 30 days (May 16, 2021 7:01:30 PM – Jun 15, 2021 7:01:30 PM) Refresh

7 Devices [New data](#) [Export to CSV](#)

Device	Group	First activity	Last activity	IP	MAC	Risk score	Tags	Activities	Vuln
Siemens 192.168.0.46	Siemens PLCs	May 25, 2021 7:06:29 PM	May 25, 2021 7:06:29 PM	192.168.0.46	ac:64:17:81:21:3c (+ 1 other)	73	Controller	3	7
Modicon M580	Schneider PLCs	May 25, 2021 7:04:02 PM	May 25, 2021 7:04:02 PM	192.168.0.68	00:80:f4:18:a6:52 (+ 2 others)	80	Controller, Web Server	3	46
L306_V01   5069-L306ERS2/B	Rockwell PLCs	May 25, 2021 7:02:23 PM	May 25, 2021 7:02:23 PM	192.168.20.23	4c:71:0d:72:8c:57	75	Controller, Rockwell Automation	1	9
L81ES   1756-L81ES/B	Rockwell PLCs	May 25, 2021 7:02:23 PM	May 25, 2021 7:02:23 PM	192.168.20.25	4c:71:0d:72:8c:57	75	Controller, Rockwell Automation	1	10
L71RED_CPU_NAME   1756-L71/B	Rockwell PLCs	May 25, 2021 7:02:23 PM	May 25, 2021 7:02:23 PM	192.168.20.22	4c:71:0d:72:8c:57	75	Controller	1	13

*The All Controllers preset in the activity list view:*

Explore / All Controllers / Activity list

Last 30 days (May 16, 2021 7:01:30 PM – Jun 15, 2021 7:01:30 PM) Refresh

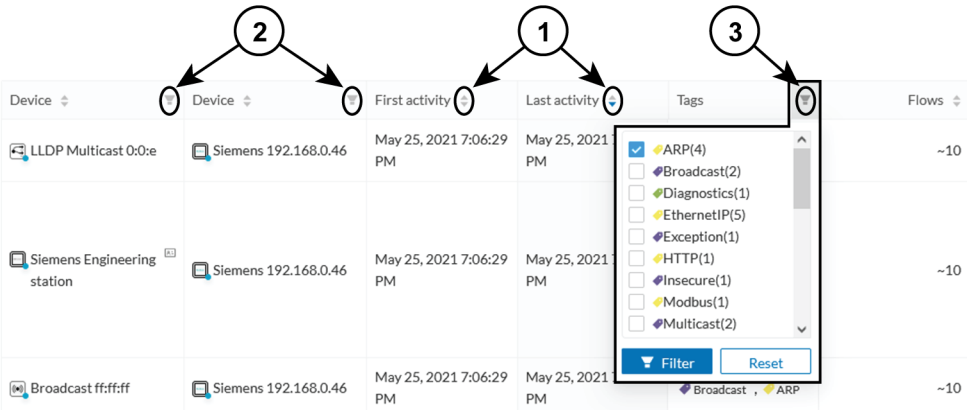
11 Activities [New data](#) [Export to CSV](#)

1 / 40 page

Device	Device	First activity	Last activity	Tags	Flows	Packets	Volume	Events
LLDP Multicast 0:0:e	Siemens 192.168.0.46	May 25, 2021 7:06:29 PM	May 25, 2021 7:06:29 PM	Multicast, Profinet	-10	101	12 kB	0
Siemens Engineering station	Siemens 192.168.0.46	May 25, 2021 7:06:29 PM	May 25, 2021 7:06:29 PM	Program Download, Program Upload, Start CPU, Stop CPU, Read Var, Write Var, ARP, S7Plus	-10	1296	591 kB	6
Broadcast ffffff	Siemens 192.168.0.46	May 25, 2021 7:06:29 PM	May 25, 2021 7:06:29 PM	Broadcast, ARP	-10	1	28 B	0
LLDP Multicast 0:0:e	Modicon M580	May 25, 2021 7:04:02 PM	May 25, 2021 7:04:02 PM	Multicast	-10	14	2.34 kB	0
Broadcast ffffff	Modicon M580	May 25, 2021 7:04:02 PM	May 25, 2021 7:04:02 PM	Broadcast, ARP	-10	298	8.34 kB	0

Lists are meant to perform an in-depth exploration of the network. Using this type of view is especially convenient when searching for a very specific data. To do so, different filters are available inside the lists to sort data:

- The sort icon (1) is to sort data by alphabetical order or by ascending/descending order.
- The filter icon (2) opens a field to type a specific data in, or a multiple choice menu (3) to filter tags.

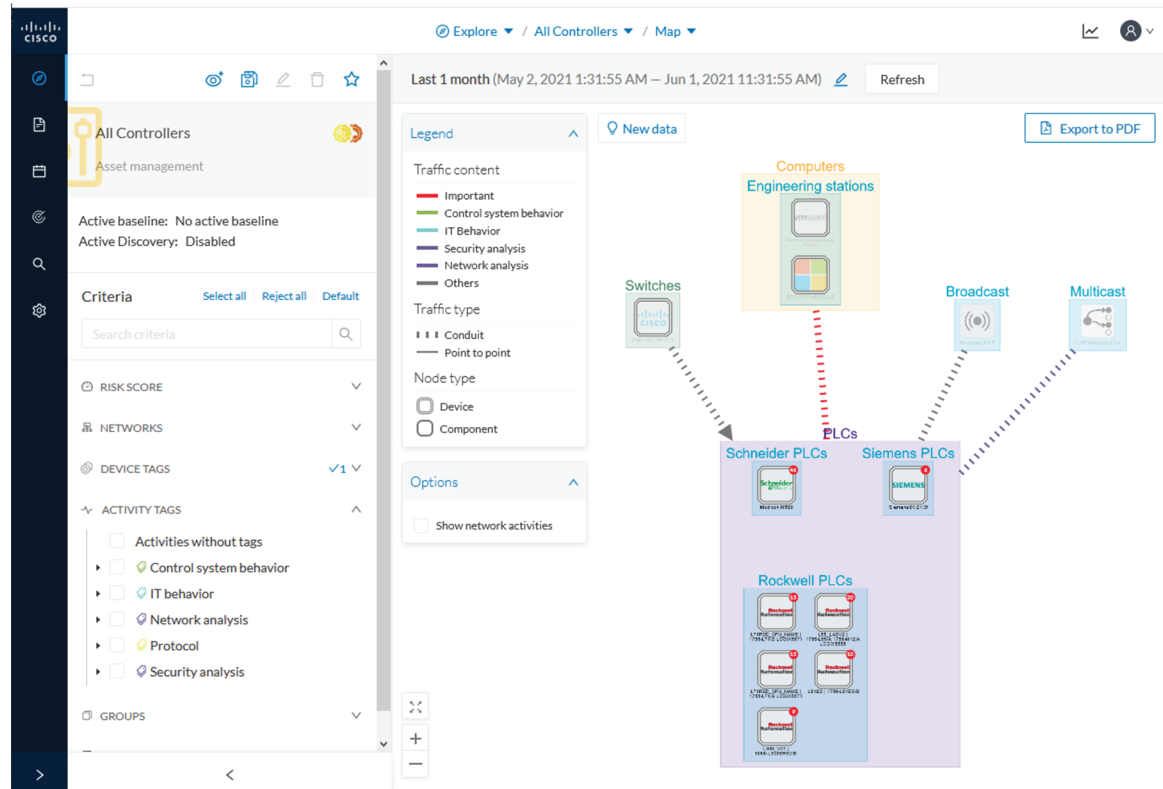


Clicking an element in the lists opens its [Right side panel](#) which leads to more advanced data.

## Map

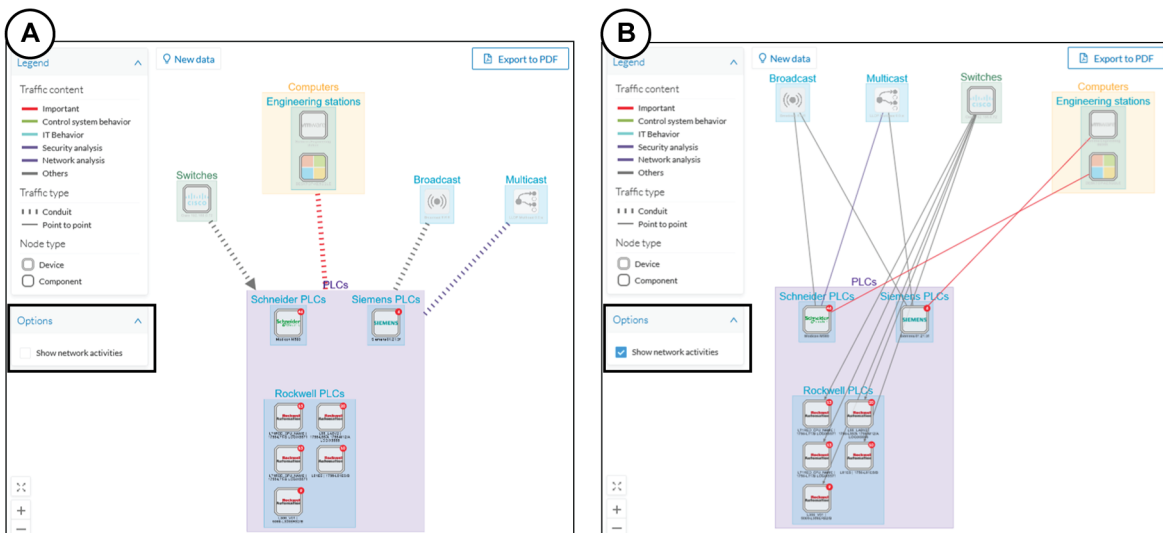
The Map is a visual representation of data of the industrial network that gives you a broad insight on how devices and components are interconnected. It's a good input to get to know how the network is structured. You can start organizing components in a way that makes sense to you by creating groups.

Maps display 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 is **self-organizing**, that is, elements are redistributed as devices, components, conduits and activities appear or disappear, and as groups are created or deleted. Moreover, the map automatically adapts over time and when changing preset. This way, it is guaranteed that the map is always well organized and components never overlap.

By default, activities between groups are merged and displayed as **Conduit (A)**. You can tick the option "Show network activities" to see activities, which gives a more detailed view **(B)**. Elements are here also automatically reorganized in the map to enhance visibility.



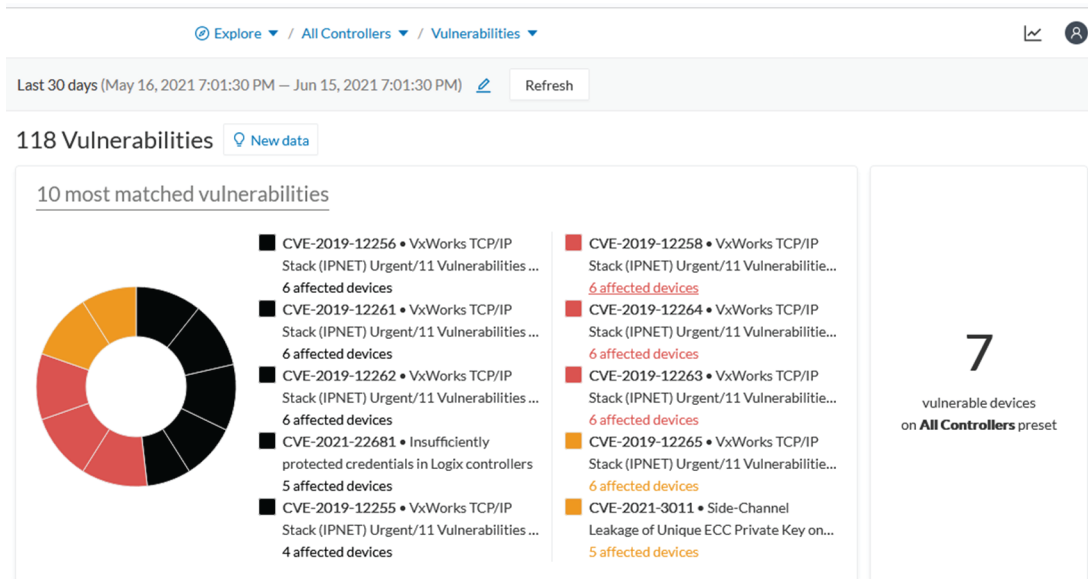
## Vulnerabilities

The vulnerability dashboard gives you a visual representation and a list of the **Vulnerability** detected within a preset.



### Important

It is important to **Knowledge DB** in Cisco Cyber Vision as soon as possible after notification of a new version to be protected against vulnerabilities.



The pie chart presents the 10 most matched vulnerabilities within the preset, that is, the vulnerabilities that have affected more devices. You can click the number of devices detected to see the devices affected.

On the right, you'll see a summary of the total number of devices that are vulnerable in the preset selected. Below, you have a list of all the vulnerabilities found in the preset with sort icons to sort data by alphabetical order or by ascending/descending order, and filter icons which opens a field to type a specific data.

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

- The vulnerability name
- Its CVE ID (world unique identifier for a Common Vulnerability Exposure)
- Its CVSS score (Common Vulnerability Scoring System)
- The devices affected by the vulnerability

Vulnerability title	CVE	CVSS score	Affected devices
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - DoS of TCP connection via malformed TCP options	CVE-2019-12258	7.5 (v3)	6 devices
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - IGMP Information Leak via IGMPv3 specific membership report	CVE-2019-12265	5.3 (v3)	6 devices
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - TCP Urgent Pointer State Confusion during connect() to remote host	CVE-2019-12261	9.8 (v3)	6 devices
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - TCP Urgent Pointer State Confusion due to Race Condition	CVE-2019-12263	8.1 (v3)	6 devices
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - Stack Overflow in parsing of IPv4 packets' IP options	CVE-2019-12256	9.8 (v3)	6 devices
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - Logical Flaw in IPv4 assignment by the ipdhcpc DHCP client	CVE-2019-12264	7.1 (v3)	6 devices
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - Handling of	CVE-2019-12262	9.8 (v3)	6 devices

Clicking an element in the lists opens its **Right side panel** which leads to more details about the vulnerability, including its link to the National Vulnerability Database.

Last 30 days (May 16, 2021 7:01:30 PM – Jun 15, 2021 7:01:30 PM) [↗](#)
Refresh

Vulnerability title	CVE	CVSS score
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - DoS of TCP connection via malformed TCP options	CVE-2019-12258	7.5 (v3)
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - IGMP Information Leak via IGMPv3 specific membership report	CVE-2019-12265	5.3 (v3)
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - TCP Urgent Pointer State Confusion during connect() to remote host	CVE-2019-12261	9.8 (v3)
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - TCP Urgent Pointer State Confusion due to Race Condition	CVE-2019-12263	8.1 (v3)
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - Stack Overflow in parsing of IPv4 packets' IP options	CVE-2019-12256	9.8 (v3)
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - Logical Flaw in IPv4 assignment by the ipdhcpc DHCP client	CVE-2019-12264	7.1 (v3)
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - Handling of unsolicited Reverse ARP replies (Logical Flaw)	CVE-2019-12262	9.8 (v3)
Insufficiently protected credentials in Logix controllers	CVE-2021-22681	10 (v3)
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - Heap	CVE-2019-12267	9.8 (v3)

← Vulnerability
×

9.8  
CVSS score v3

**VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - TCP Urgent Pointer State Confusion during connect() to remote host**

Identifier: CVE-2019-12261

Description: Wind River VxWorks 6.7 through 6.9 and vx7 has a Buffer Overflow in the TCP component (issue 3 of 4). This is an IPNET security vulnerability: TCP Urge... [show more](#)

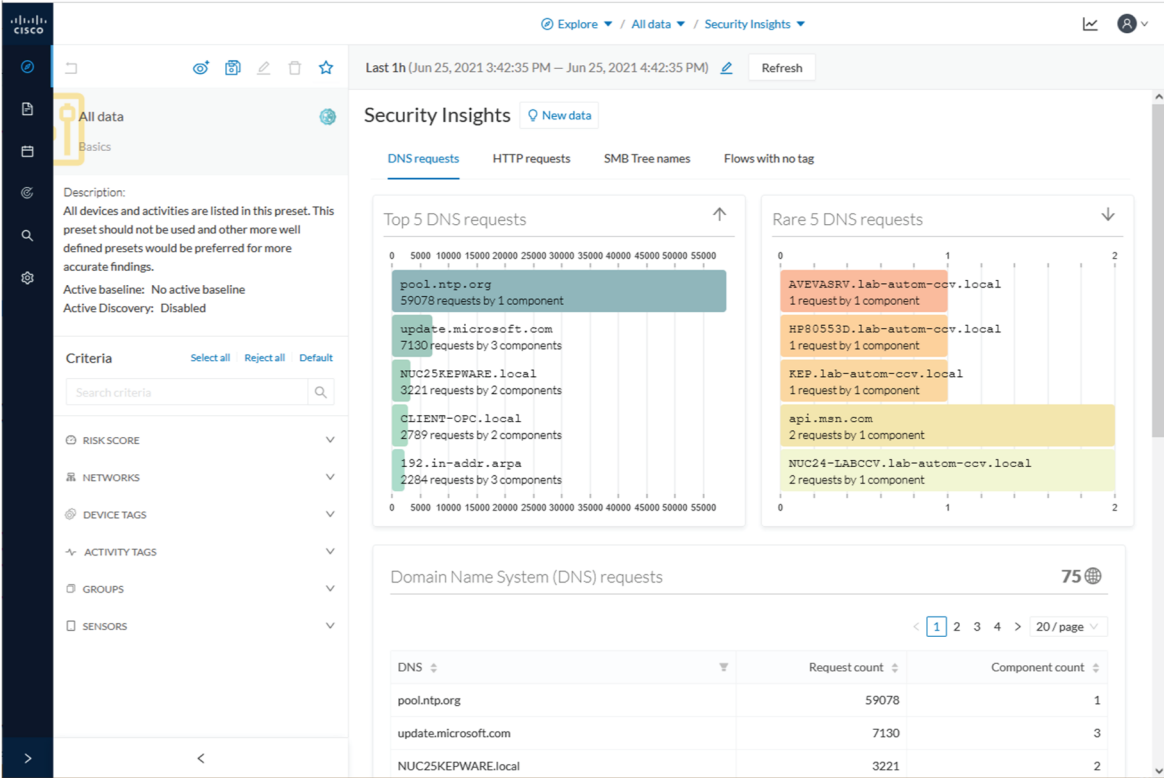
Solution: Please refer to the associated manufacturer's advisory.

Published on: August 9, 2019

Links: [Schneider support2.windriver.com](#)  
[support.f5.com](#)  
[security.netapp.com](#)  
[psirt.global.sonicwall.com](#)  
[cert-portal.siemens.com](#)  
[support2.windriver.com](#)  
[www.windriver.com](#)  
[Rockwell](#)

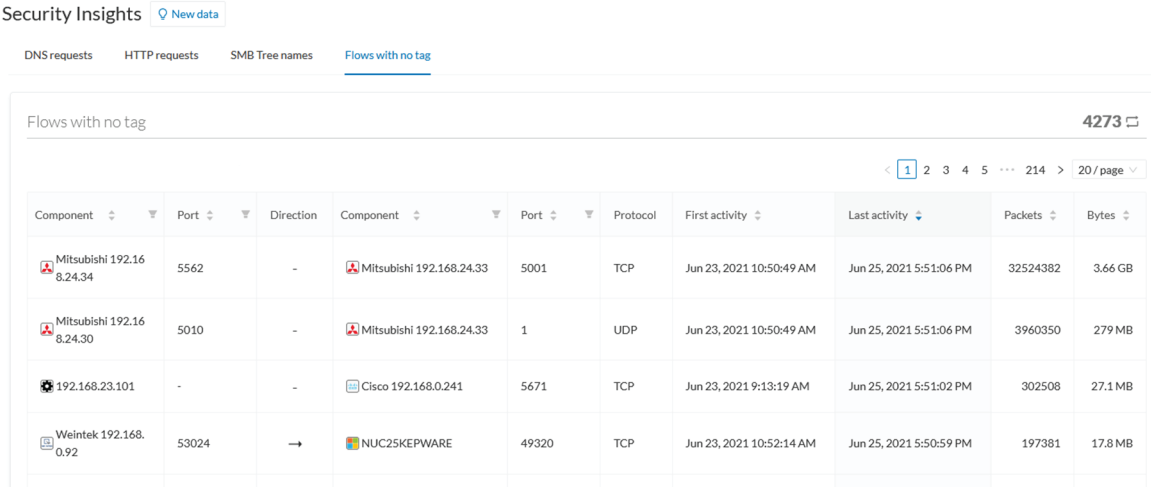
# Security Insights

Security Insights is a view that provides statistics for DNS requests, HTTP requests, SMB Tree names and flows with no tag.



For each category, you will find the most frequent and rarest requests, and the list of all these requests.

### Flows with no tag:

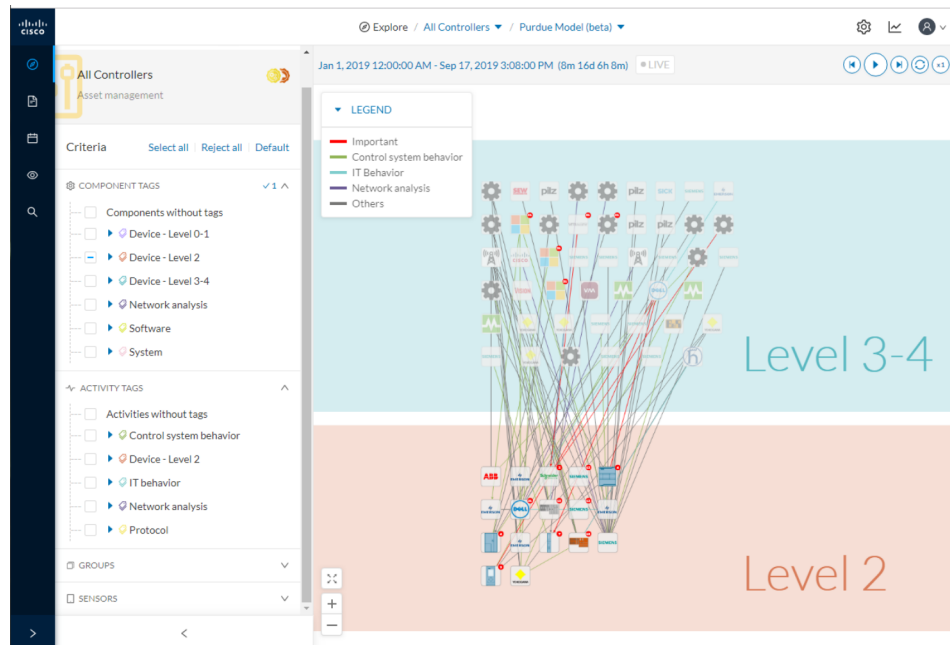


In this category, you will find a list of all flows with no tags, that is, traffic that Cisco Cyber Vision wasn't able to analyze. The reason can be that the protocol is not supported by Cisco Cyber Vision yet. However, this list is interesting from a security standpoint to make sure if such content is really supposed to be on the network and search why it cannot be inspected. A good starting point is to 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.

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

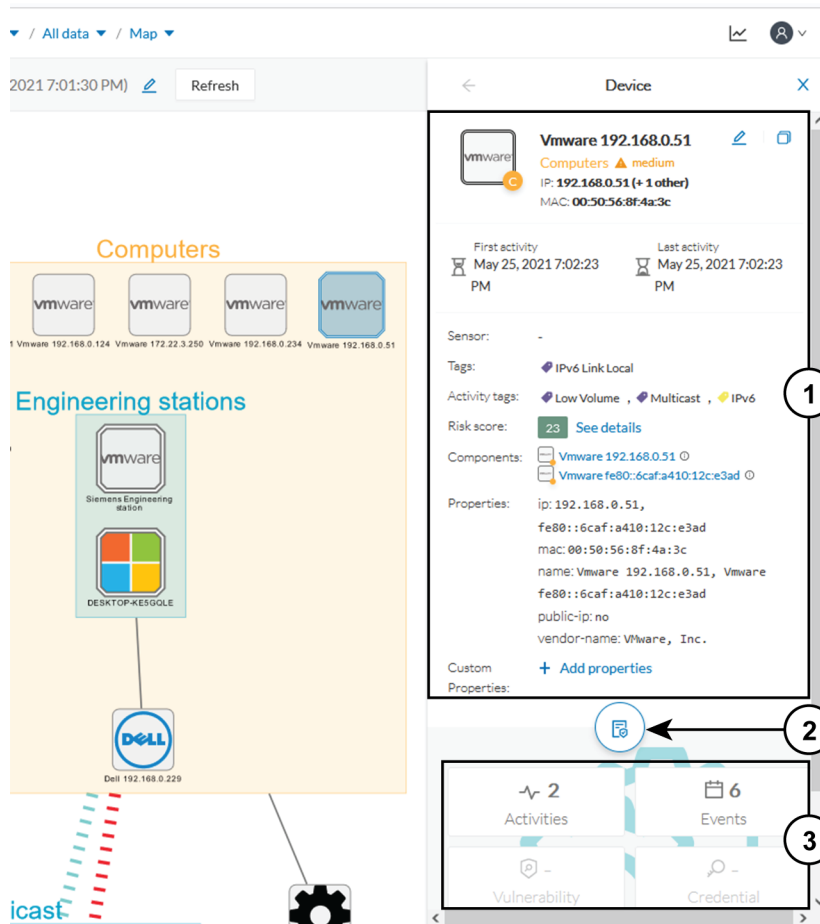


Components are distributed according to the different layers of the Purdue model:

- 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).

## Right side panel

A right side panel is a condensed view about a device, a component, a group of components or an activity's information. This view allows you to quickly scan general information about an element meanwhile you're keeping an eye on a broader view such as a device list or a map.



Right side panels differ depending on the type of element consulted. The higher part (1) of the right side panel gives you general information about the element. If consulting a device or a component, you can edit its name or add/remove it to/from a group.

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

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

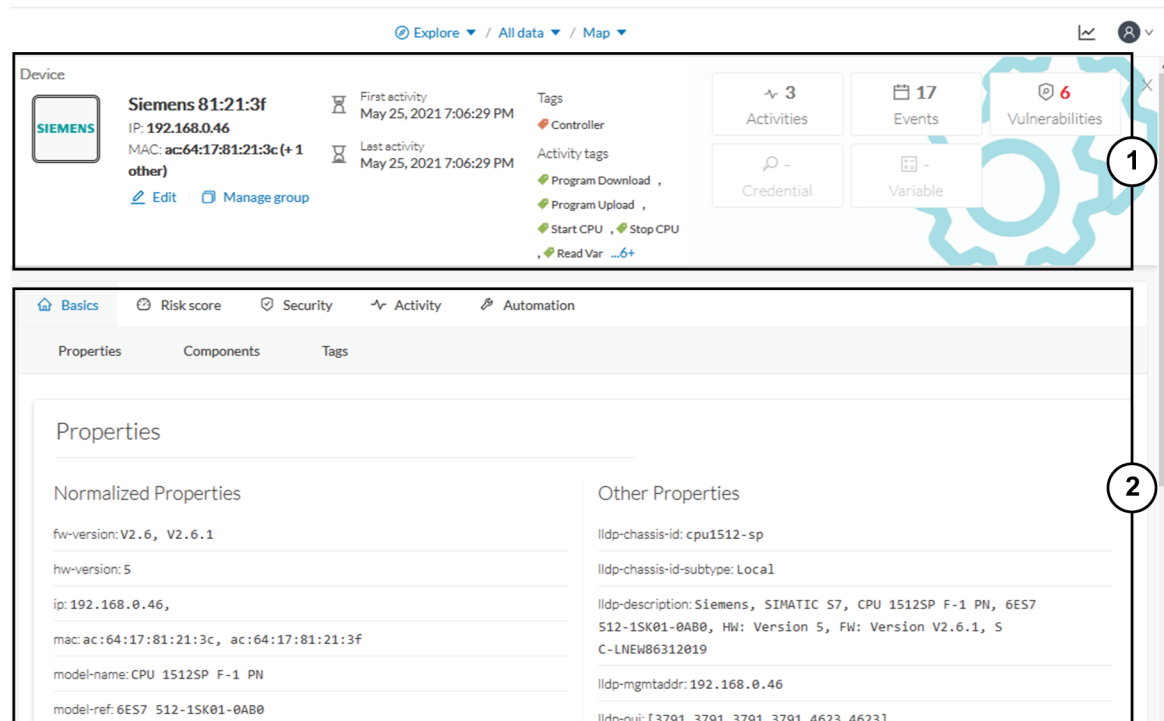
To access a right side panel you just need to click a device, a component or an activity on the map or a list.

## 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 consulted.

*A device's technical sheet:*





A technical sheet is composed of a top bar and of a list of tabs. The higher part (1) recaps the information found in the right side 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 lower part (2) contains detailed information classified under tabs, displaying or not according to the element you're on:

- Basics contains an element's properties and tags that are categorized with their definition. Device's components also appear if applicable.
- Risk score with an overview and a more detailed and focused views.
- Security contains a component's vulnerabilities you can acknowledge and credentials.
- Activity is about an activity's flows and contains a [Mini map](#) which is a view that is restricted to a device or a component and its activities.
- Automation contains variable accesses.

You can access technical sheets through a device, component or an activity's [Right side panel](#), clicking the technical sheet button. A flow's technical sheet is visible when clicking on a particular flow.

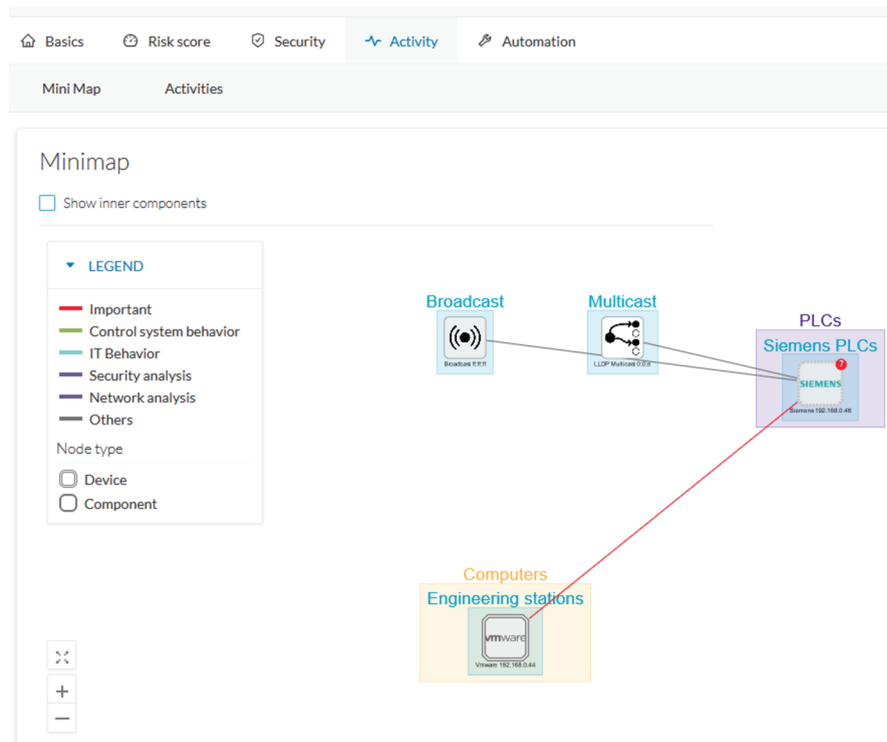
- More information about [Properties](#).
- More information about [Tags](#).
- More information about the [Risk score](#).
- More information about [Vulnerability](#).

- More information about [Credentials](#).
- More information about [Flow](#).
- More information about the [Mini map](#).
- More information about [Variable accesses](#).

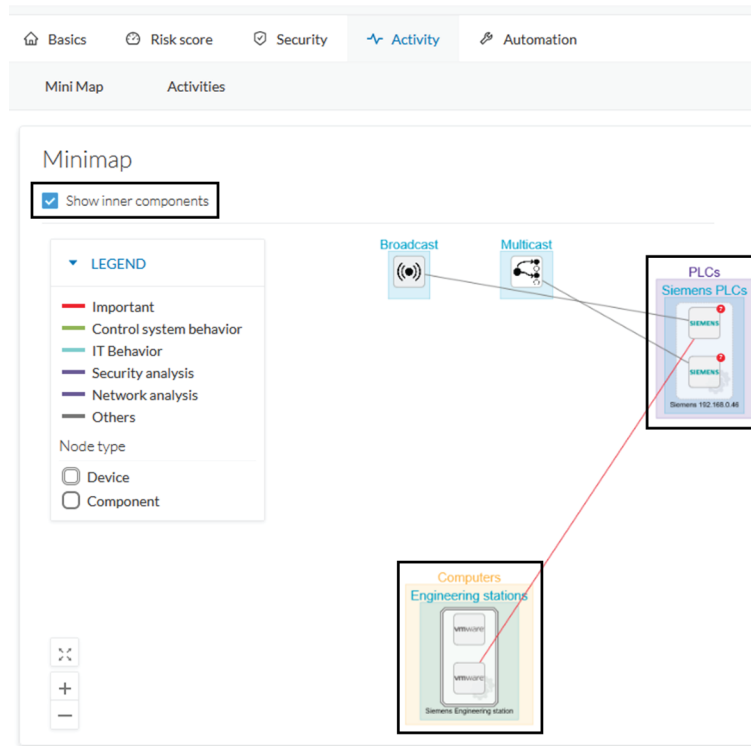
## Mini map

The Mini Map is a visual representation restricted to a specific device or component and its activities.

This view is accessible through the Activity tab of a Component's [Technical sheets](#).



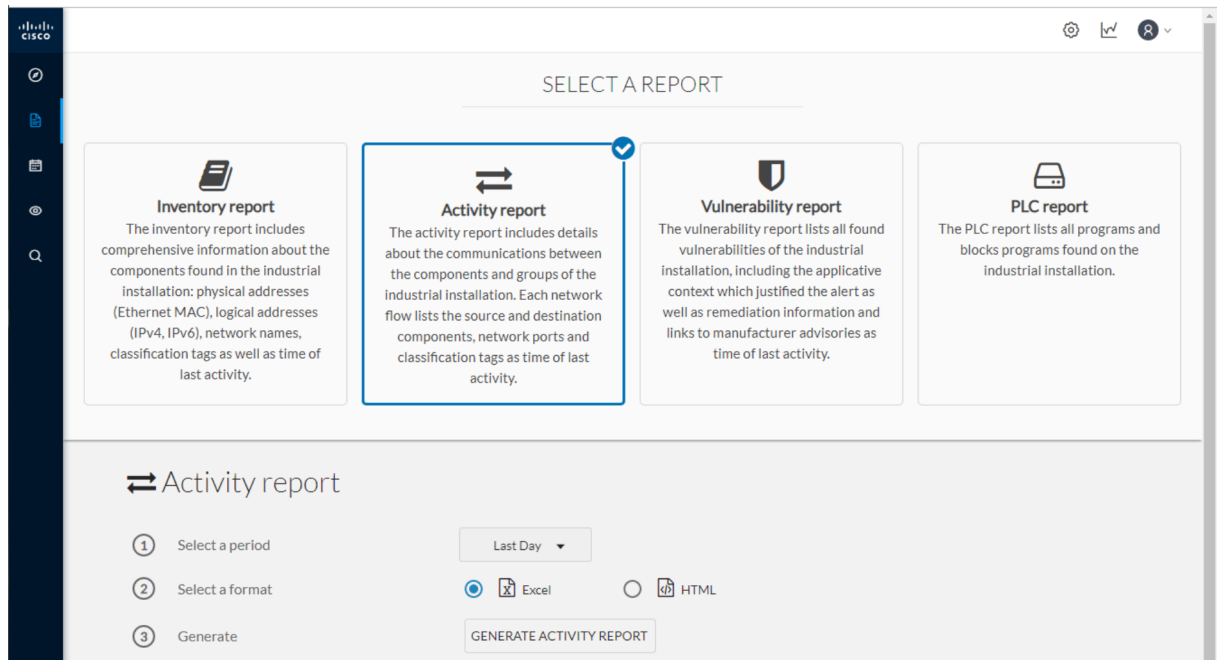
The option "Show inner components" enables an exploded view of the devices.



Clicking any element in the Mini Map will open its [Right side panel](#) so you can have access to further information.

## Reports

Reports are exportable files which improve your visibility of valuable information about your industrial network. Information is collected and categorized according to different perspectives which are components, flows, vulnerabilities and PLCs. Reports can be generated for a time period you define into spreadsheets (XLSX) or printable (HTML that you can export to PDF).



Below is the description of the four types of reports available:

- The **inventory report** lists and details all components of your industrial network. They are sorted by group. For each component different information is given like the component name, when it was active for the first and the last time and tags that qualify its activity. If available, you will also find technical details such as its MAC and IP addresses, hardware and firmware versions, the serial number and extra properties.
- The **activity report** lists and details all communications exchanged between the components of your industrial network. They are sorted by group and by direction (inner, incoming and outgoing communications regarding a group). Information provided includes the protocol, which source and destination ports have been used and tags that qualify its activity.
- The **vulnerability report** lists all components detected as vulnerable and gives further details about vulnerabilities. Vulnerabilities are based on the Knowledge DB provided by Cisco. So, the more you keep the Knowledge DB up to date, the better you will be notified about new known vulnerabilities. The report contains information about the vulnerability, its impact level, its CVSS (Common Vulnerability Scoring System) and solutions. A vulnerability is often about outdated software parts. It is strongly recommended to fix outdated states as soon as possible. Links to manufacturers' websites are provided for this purpose.
- The **PLC report** lists all PLCs in your industrial network. For each PLC, the report lists and details properties, events, programs, program blocks and variable accesses, if there are any.

All reports generated are displayed in the History section from which you can rename, download and delete reports.



## Events

Cisco Cyber Vision provides many [Events](#) significant for the network security especially the ones which relate to the industrial activity (such as New program downloaded/uploaded, New start/stop CPU command, New init command...). Many other events are also available such as events related to [Vulnerability](#), comparison results, sensors activity, etc.

Refer to the [Events](#) on the GUI to see all events available.

The Events page provides two views to give high visibility on these events:

- The [The Dashboard](#): a visual and continuously-updated view of the current state of the installation based on the number of events (by severity and over time).
- The [The Calendar](#): a chronological and continuously-updated view of the events within which you can search events.

## The Dashboard

Events are presented in the Dashboard under doughnut and line charts.

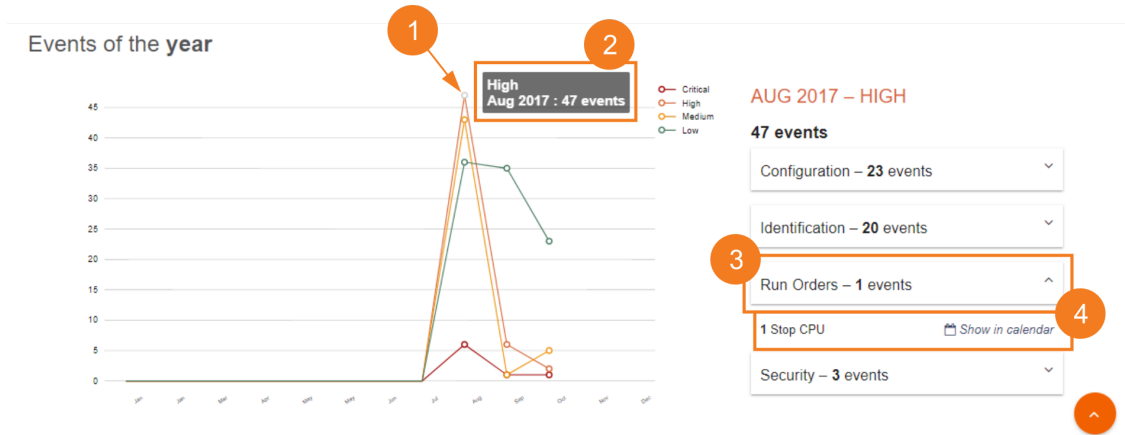
Doughnut charts present events numbers and percentages per categories and severities.



You can see the list of events per categories in the [Events](#).

Clicking the doughnut redirects you to the [The Calendar](#) view that is filtered with the corresponding category and severity so you can quickly access more events details.

Below, the line chart puts an emphasis on the number of events per severity over time.



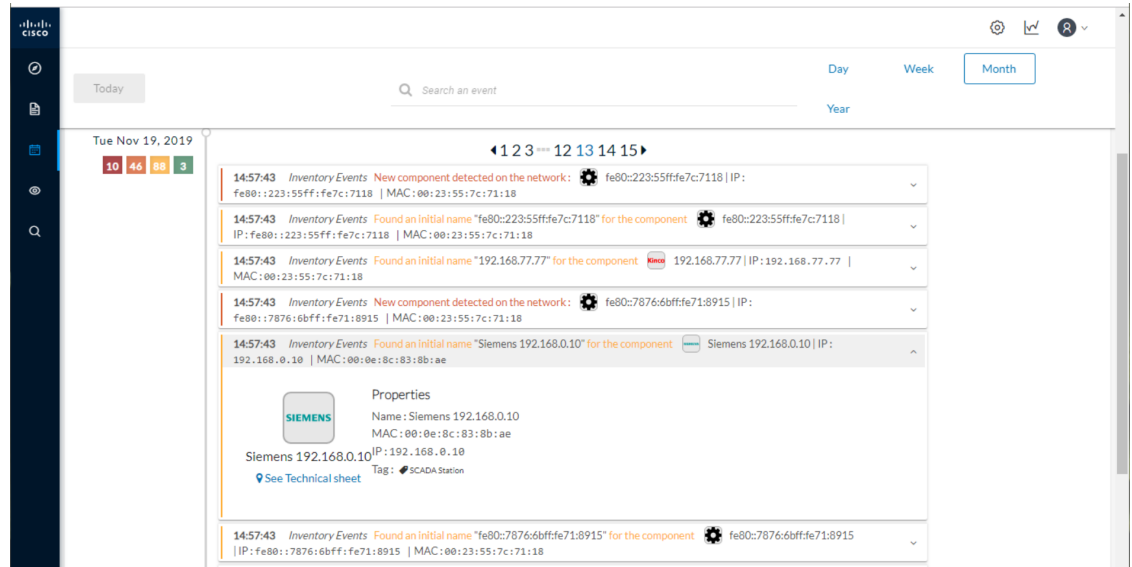
Clicking event markers (1) on the line chart lets you see the number of events per category according to a specific time (2).

Click a category event tab (3) to see events details in the Calendar view by means of the link "Show in calendar" (4). Events will be filtered with the corresponding category, severity and event type.

## The Calendar

The Calendar is a chronological view in which you can see and search events. Use the search bar to search events by MAC and IP addresses, component name, destination and source flow, severity and category.

You can also see events that have happened during the day, week, month and year.



Clicking on a result event will show you details about the event.

When an event is related to a component or an activity, you can jump to its technical sheet by clicking See technical sheet.

When a Monitor event is generated, the short description includes a link to view the differences in the Monitor page.



# Monitor

## Monitor mode

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.

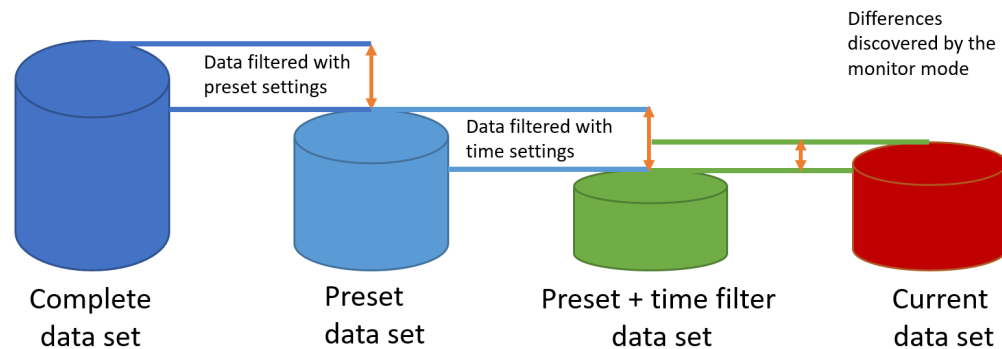
### Baselines as Preset's normal states

A Preset is a set of criteria which aims to show a detailed fragment of a network. To start monitoring a network, you need to pick up a preset, and to define what would be its normal, stable state. This will represent the

preset's baseline. A state may rely on a period, as a network fragment may be subject to several states. Hence, it is possible to create several planned, controlled and time-framed baselines per preset, and to monitor the whole network. For example, a normal state of the network can be a typical weekday operating mode, in which numerous processes are performed iteratively. During weekends, these processes may be slowed down, different, or even stopped. Any network phase can be saved as a baseline by selecting the time span in which it occurs, and monitored. Other examples of baselines can be a regular maintenance period, a degraded mode, a weekend and night mode, and so forth. A baseline is created for a situation considered as part of a normal operating process in which all network behaviors (components, activities, properties, tags, variable accesses) will be taken into account for review.

### Review and assignment of differences

A difference is a new or changed behavior happening within a fragment of a network. Any difference detected is highlighted in the Monitor mode through several views such as a map, a component list and an activity list. When reviewing these, they can be acknowledged or reported. It depends on whether you consider them as normal or not, and their level of criticality. That is, you can include these changes into your baseline if it is part of a normal network development process, or take action in case of suspicious behavior. By doing so, each baseline will be refined bit by bit over time and become more compliant with your needs.



## Monitor mode's views

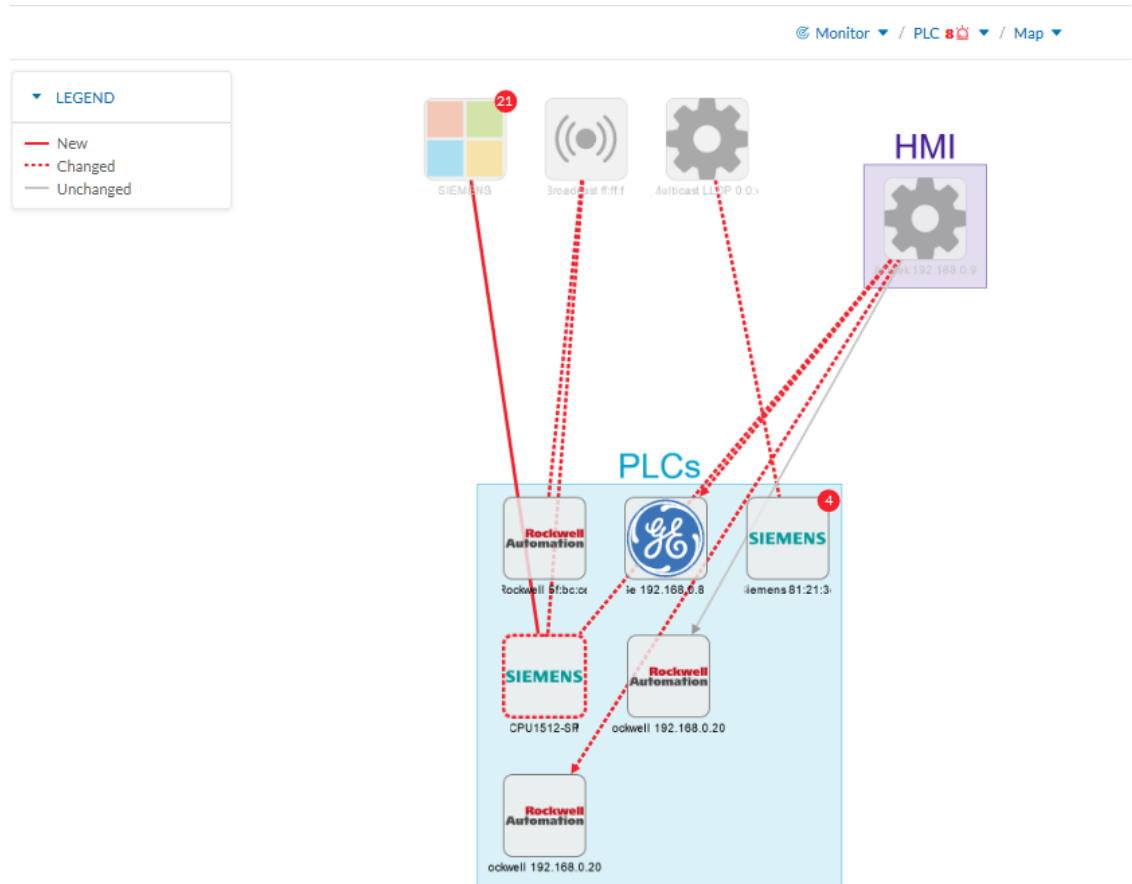
Like in the Explore mode, the Monitor mode offers several views of data so you can see them through different representations. The difference, though, is that in the Monitor mode views new and changed detected elements are highlighted in red.

For more information about the views listed below, refer to the Explore chapter.

The map view:

non-aggregated components





The component list view:

Monitor / PLC 8 / Component list

6 Component  
1 changed

STATUS	Component	Group	First activity	Last activity	IP	MAC
CHANGED	Siemens 192.168.0.46	PLCs	Apr 7, 2020 12:11:14 PM	Apr 7, 2020 12:11:14 PM	192.168.0.46	ac:64:17:81:2
-	Ge 192.168.0.81	PLCs	Apr 7, 2020 12:11:14 PM	Apr 7, 2020 12:11:14 PM	192.168.0.81	00:09:91:01:6
-	Rockwell 192.168.0.200	PLCs	Apr 7, 2020 12:11:14 PM	Apr 7, 2020 12:11:14 PM	192.168.0.200	00:00:bc:5f:bc
-	Rockwell 5f:bc:ce	PLCs	Apr 7, 2020 12:11:14 PM	Apr 7, 2020 12:11:14 PM	-	00:00:bc:5f:bc
-	Siemens 81.21:3d	PLCs	Apr 7, 2020 12:11:14 PM	Apr 7, 2020 12:11:14 PM	192.168.0.46	ac:64:17:81:2
-	Rockwell 192.168.0.200	PLCs	Apr 7, 2020 12:11:14 PM	Apr 7, 2020 12:11:14 PM	192.168.0.200	00:00:bc:5f:bc

The activity list view:

Monitor / PLC 8 / Activity list

### 8 Activity

1 new 6 changed

STATUS	Component	Component	First activity	Last activity	Tags
NEW	SIEMENS	Siemens 192.168.0.46	Apr 7, 2020 6:04:58 PM	Apr 7, 2020 6:04:58 PM	Read Var , Write
CHANGED	Ge 192.168.0.81	Weintek 192.168.0.91	Apr 7, 2020 12:11:14 PM	Apr 7, 2020 12:11:14 PM	No tags
CHANGED	Weintek 192.168.0.91	Siemens 192.168.0.46	Apr 7, 2020 12:11:14 PM	Apr 7, 2020 12:11:14 PM	No tags
CHANGED	Multicast LLDP 0:0:e	Siemens 81:21:3d	Apr 7, 2020 12:11:14 PM	Apr 7, 2020 12:11:14 PM	No tags
CHANGED	Rockwell 192.168.0.200	Weintek 192.168.0.91	Apr 7, 2020 12:11:14 PM	Apr 7, 2020 12:11:14 PM	No tags
CHANGED	Siemens 192.168.0.46	Broadcast ff:ffff	Apr 7, 2020 12:11:14 PM	Apr 7, 2020 12:11:14 PM	No tags
CHANGED	Rockwell 5f:bc:ce	Broadcast ff:ffff	Apr 7, 2020 12:11:14 PM	Apr 7, 2020 12:11:14 PM	No tags
-	Rockwell 192.168.0.200	Weintek 192.168.0.91	Apr 7, 2020 12:11:14 PM	Apr 7, 2020 12:11:14 PM	No tags

In any view, on the left side, there is:

- a fixed panel with a summary of the elements that have been detected in the Monitor mode,
- the last time this baseline has been checked,
- the preset it belongs to along with the list of criteria selected.

You can also modify the baseline settings. And the Explore button redirects you to the corresponding preset in the Explore mode.

Monitor / PLC 8 / Activity list

PLC
see on Explore

1 new activities
1 changed components

6 changed activities

Last check: Apr 7, 2020 7:03:12 PM

---

Active criteria

GROUPS v 1 ^

- PLCs

### 8 Activity

— 1 new — 6 changed

STATUS	Component	Component
NEW	SIEMENS	Siemens 192.168.0.4
CHANGED	Ge 192.168.0.81	Weintek 192.168.0.9
CHANGED	Weintek 192.168.0.91	Siemens 192.168.0.4
CHANGED	Multicast LLDP 0:0:e	Siemens 81:21:3d
CHANGED	Rockwell 192.168.0.200	Weintek 192.168.0.9
CHANGED	Siemens 192.168.0.46	Broadcast ff:ff:ff
CHANGED	Rockwell 5f:bc:ce	Broadcast ff:ff:ff
-	Rockwell 192.168.0.200	Weintek 192.168.0.9

In any view, if you click one of the elements, for example below the activity marked as new in the activity list, a right side panel opens. It gives you:

- information about the activity such as the two components it belongs to,
- the date of the first and the last activity,
- its tags,
- buttons to perform several [Review differences](#).

The screenshot shows the 'Monitor' interface with a navigation bar at the top indicating 'PLC' and 'Activity list'. A notification banner shows '84 day remaining Evaluation Mode'. The main area is titled '8 Activity' with a sub-header '1 new 6 changed'. Below this is a table of activity entries:

STATUS	Component	Component	First activity
NEW	SIEMENS	Siemens 192.168.0.46	Apr 7, 2020 6:04:58 P
CHANGED	Ge 192.168.0.81	Weintek 192.168.0.91	Apr 7, 2020 12:11:14
CHANGED	Weintek 192.168.0.91	Siemens 192.168.0.46	Apr 7, 2020 12:11:14
CHANGED	Multicast LLDP 0:0:e	Siemens 81:21:3d	Apr 7, 2020 12:11:14
CHANGED	Rockwell 192.168.0.200	Weintek 192.168.0.91	Apr 7, 2020 12:11:14
CHANGED	Siemens 192.168.0.46	Broadcast ff.ffff	Apr 7, 2020 12:11:14
CHANGED	Rockwell 5f:bc:ce	Broadcast ff.ffff	Apr 7, 2020 12:11:14
-	Rockwell 192.168.0.200	Weintek 192.168.0.91	Apr 7, 2020 12:11:14

To the right of the table is a 'New Activity' panel for the selected entry. It shows details for a SIEMENS device (IP: 192.168.0.44, MAC: 00:0c:29:d2:45:53) and a CPU1512-SP (IP: 192.168.0.46, MAC: ac:64:17:81:21:3c). The PLCs are marked as 'very low'. Below the details are buttons for 'Read Var', 'Write Var', 'ARP', and 'S7Plus', along with 'Approve activity' and 'Report activity' buttons, and a 'Show details' button.

Clicking the Show details buttons opens a window on top with more information, in the example below, it shows the activity tags with the category they belong to and their description.

The screenshot shows the 'Activity in details' window. It contains a 'New Activity' panel on the left with the same device information as the previous screenshot. The main area is titled 'Activity in details' and contains a table of 'Activity tags':

Status	Tag	Category	Description
NEW	ARP	PROTOCOL	The Address Resolution Protocol (ARP) is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given network layer address, typically an IPv4 address. Source: <a href="https://en.wikipedia.org/wiki/Address_Resolution_Protocol">https://en.wikipedia.org/wiki/Address_Resolution_Protocol</a>
NEW	Read Var	CONTROL SYSTEM BEHAVIOR	Read Var is a control systems command to read process variables from the PLC, DCS or Safety controller memory. It enables the reading component to acquire data. In normal operating conditions flows tagged as Read Var must originate from a SCADA Station, HMI, OPC Server or Historian and destinate to PLC, DCS or Safety controller.
NEW	S7Plus	PROTOCOL	Siemens S7 Plus is a protocol dedicated to the management and supervision of Siemens SIMATIC S7 PLCs, IO Modules, Drives, etc.
NEW	Write Var	CONTROL SYSTEM BEHAVIOR	Write Var is a control systems command to write process variables to the PLC, DCS or Safety controller memory. The writing component set new data such as setpoints or orders. In normal operating conditions flows tagged as Write Var must originate from a SCADA Station, HMI, OPC Server and destinate to PLC, DCS or Safety controller.

The window also includes 'Approve activity' and 'Report activity' buttons, and a 'Show details' button.

Click the collapse button to come back to the initial view.

However, to go deeper into analysis, click the Investigate with flows button.

## New and changed differences

When a difference is detected, it appears in red in the Monitor mode. There are two types of differences: new and changed ones. A component, an activity, a tag, a property and a variable access can appear (new) or evolve (change). Here below are a few examples of how differences are represented in the Monitor mode:

A new component (plain red) and a changed component (hyphenated red)

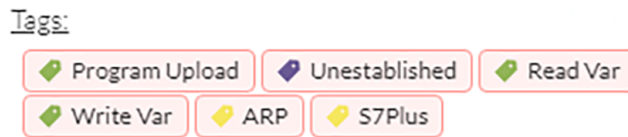


Changed component's properties, with the former crossed out property:

Properties: 2 differences [Investigate with flows](#)

```
lldp-description: Siemens, SIMATIC S7, CPU 1512SP F-1 PN, 6ES7 512-1SK01-0AB0, HW: Version 5, FW: Version V2.8.1, S C LNEW86312019 Siemens, SIMATIC S7, CPU 1512SP F-1 PN, 6ES7 512-1SK01-0AB0, HW: Version 5, FW: Version V2.6.1, S C LNEW86312019
fw-version: V2.8.1 V2.6.1
```

New and changed component and activity tags:



New and changed activity's variable access:

Variables:

```
process. Dint DB4/lid=11 read Weintek 192.168.0.91
process. Dint DB3/lid=11 read Weintek 192.168.0.91
```

Each difference must be reviewed to identify a potential threat and refine the baseline. Refer to the section [Review differences](#).

## Review differences

When differences are detected by the Monitor mode, what one wants to do is to review them to see if they are a potential threat to the network, and clear their data from any red-alarming elements. Several actions are available to help you do so, which will, moreover, allows you to enrich the current baseline, clean it, or report abnormalities. These are available at different levels depending on whether you want to perform a deep behavior review on a component or activity particulars, or at a higher macro level for a quick review. Thus, you can perform these actions on tags, properties, variable accesses, components, activities and baselines.

In any case, any action taken on the Monitor mode will generate an event that you can see on the Events page.

## Acknowledge differences

### Acknowledge in the Monitor mode

"Acknowledge" is an action to be used to indicate that determined behaviors -or differences- are safe and normal. In fact, by doing this action, the difference will be included in the baseline. You can acknowledge

differences on any element of the Monitor mode: tags, properties, variable accesses, components, activities and baselines.

### Acknowledge a component or an activity

Acknowledge will display as such if the behavior is notified as changed. However, if the behavior concerning a component or an activity is notified as new, an additional action is required when clicking the button "Acknowledge" because a distinction has to be made according to whether the behavior in question is exceptional or part of an iterative process.

- **Acknowledge & Include**

This action is to be used for a behavior which is part of a normal process and is meant to happen regularly over time. By using this button, the behavior will be included into the current baseline. If later the component or the activity changes -because for example a new tag has been detected on them- you will be alerted through the Monitor mode: it will turn to "changed" and appear hyphenated and red. This action is useful to refine a baseline as it evolves over time.

Ex: You can perform this action on a new machine installed in the network, or a new activity due to a new supported protocol.

- **Acknowledge & Keep Warning**

This action is to be used when a behavior is punctual and not part of a process. In this case, such behavior must not be considered as abnormal but rather as an unusual one, which doesn't have a bad impact on the network. By using this button, the behavior will be acknowledged and so cleared, but will not be included into the baseline. Consequently, you'll be notified if it happens again as a new behavior in the monitored baseline.

Ex: You can perform this action on a new component and a new activity due to an exceptional maintenance act.

## Report differences

This action is to be applied on a difference you consider to be an anomaly, that is, a behavior that is abnormal and may compromise the operating capability and security of the network. However, before reporting the anomaly, the first thing to do is to investigate, and, if possible, to resolve it. In any case, when reporting an anomaly, you must fill in a message of incident response or acknowledgment (in which context the incident has happened, potential threats, or how it has been fixed). Once an anomaly is reported, it is cleared and not included in the baseline, and an event is generated with a default severity level higher than the acknowledge action. You will be alerted in the Monitor mode if the incident occurs again.

## Remove and keep warning

This action will remove the component or activity from the current baseline. This is to be used when you consider an element should not appear in a baseline, or you don't want to see it anymore. However, you will be alerted if the component or activity comes back, and the difference will appear as new. This action is also available on variable accesses through [Individual acknowledgment](#).




---

**Note** If a difference keeps coming back in a baseline and you don't want to see it, you should modify the preset instead.

---

## Individual acknowledgment

Individual acknowledgment is an advanced usage of Cisco Cyber Vision. This feature is available on changed components and activities, that is, on elements already included in a baseline. It allows you to access their details to perform a deep behavior review by [Acknowledge differences](#) and [Remove and keep warning](#) one by one the differences detected on the network. Thus, individual acknowledgment is available on components' properties and tags, and on activities' tags and variable accesses.

- **Component properties**

New and changed properties display in red. Concerning changed properties, the former one is crossed out and the new one displays next to it. They will always display in red, unless you acknowledge them.

- **Component and activity tags**

New and changed tags display in red. They will be cleared as you acknowledge or report them (i.e. they are no longer displayed in red).

- **Activity variable accesses**

New and changed variable accesses display in red. A variable access can be acknowledged, reported, and, in addition to other elements, deleted (i.e. button "**Remove and keep warning**"). Deleting a variable access is to be used when you consider that it should not be part of the current baseline and you don't want to see it. It will be removed from the baseline and disappear. If, however, the variable access happens again, you will be alerted and it will display in red.

Once all component or activity's elements are reviewed (i.e. acknowledged, reported, or removed), the entity they belong to is cleared (the component or activity itself is no longer displayed in red). Any action performed in the Monitor mode will appear in the Event page.

## Investigate with flows

This button is not an action but an option to get more information and context about the differences detected on the network. In fact, each difference found, since it belongs to a component or an activity, is related to a flow. This view allows you to perform forensic analysis and may give you some clues to understand what happened.

Ex: You can search from which flow exactly a tag comes from.

## Create a baseline from a default preset

1. Access the Explore page.
2. In Basics, click the preset Essential data.
3. Click the button Add a new baseline from preset.
4. A pop-up appears to invite you to check your new baseline. Click Go check it out.
5. All elements displays. Some components and activities may already appear in red as new or changed.

## Create a baseline from a group

To create groups:

## Procedure

---

- Step 1** Access the All data preset.
- Step 2** Create two groups of components.
- Step 3** Click the Autolayout button.

### Example:

We create a group HMI and a group PLC.

To create presets from groups:

- Step 4** In criteria, access the groups filter, and select the first one of the group you created.

### Example:

We select the HMI group in the filter.

The HMI group displays in the map with its related activities.

- Step 5** Create a preset from this view.
- Step 6** Click Save as and name the preset HMI.
- Step 7** Repeat the previous steps for the PLC group.
- Step 8** Go to All Presets. You will see your two new presets.

To create a baseline from presets:

- Step 9** Access the HMI preset.
- Step 10** Click the button "Add a new baseline from preset".
- Step 11** Name it HMI.
- Step 12** Repeat the previous steps for the PLC preset.
- Step 13** Access the Monitor mode. You will see your two new baselines.
- 

## Create a weekend baseline

Create another baseline to monitor the network during weekends.

1. Access the All data preset.
2. Set the period for the weekend. For example, from Friday 5 p.m. to Monday 4 a.m.
3. Click the button "Add a new baseline from preset".
4. Name the baseline "All data weekend" and add the description "Must be active from Friday 5pm till Monday 4am".

## Enable a baseline monitoring

To make the most of the Monitor mode, it is sometimes insightful to create several baselines per preset. However, only one baseline can be active at a time per preset. This is because a baseline is to be used to monitor a well-defined network process during a specific period of time (e.g. baselines Normal operating

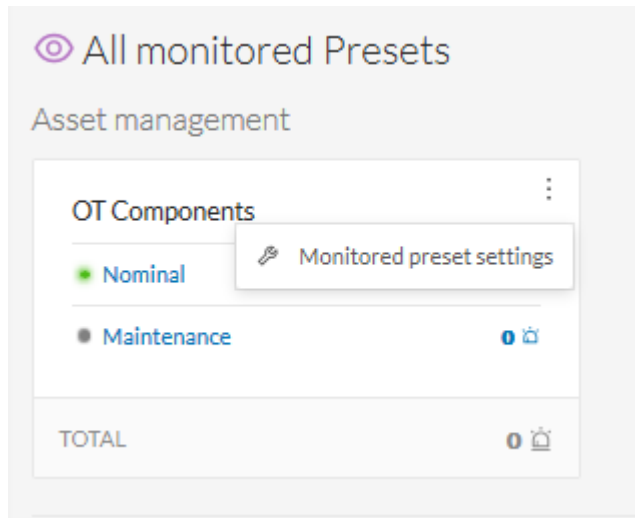


mode, Maintenance, Week-end, Night). Two baselines cannot happen at the same time on a preset, and you need to enable the proper baseline as the network enters a new operating phase. Consequently, when you enable a baseline on a preset, the active one is automatically disabled.

To enable a baseline:

**Procedure**

- Step 1** Access the Monitor page.
- Step 2** Click the monitored preset settings menu on the preset you want to monitor.



- Step 3** Under Monitored baseline, select the baseline you want to enable.

**Step 4** Click Ok.

The baseline selected turns to green and is enabled.

## Use cases

### Detection of assets newly connected to the network

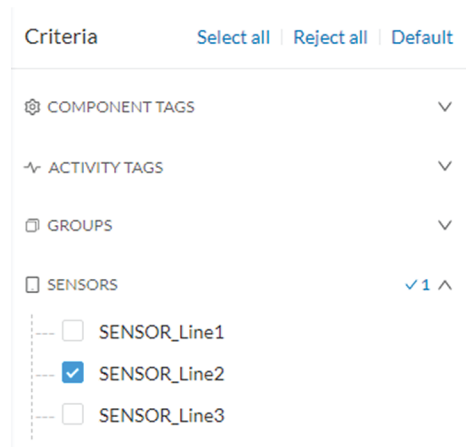
A basic use case in Cisco Cyber Vision is to detect if and when a new equipment connects to the industrial network being monitored. However, the first thing to do when using Cisco Cyber Vision is to organize components in an intelligible way. In this use case, we choose to organize components according to the network's topology, that is, per production chain. In fact, a network can be divided into several areas, such as several production chains with different criticality levels, where a Cisco Cyber Vision Sensor is placed to capture and monitor its traffic. This topology can be reflected in Cisco Cyber Vision by creating groups which represent a production chain and contain its components. In clear, here we intend to detect a new component and its related activities within a specific area. Thus, it will be possible to see whether a component connects with this production chain. Its related activities will also be highlighted in the Monitor mode.

**Key Differences:** New components and their related activities on the network

**Aim:** Monitor the production line 2 of the industrial network.

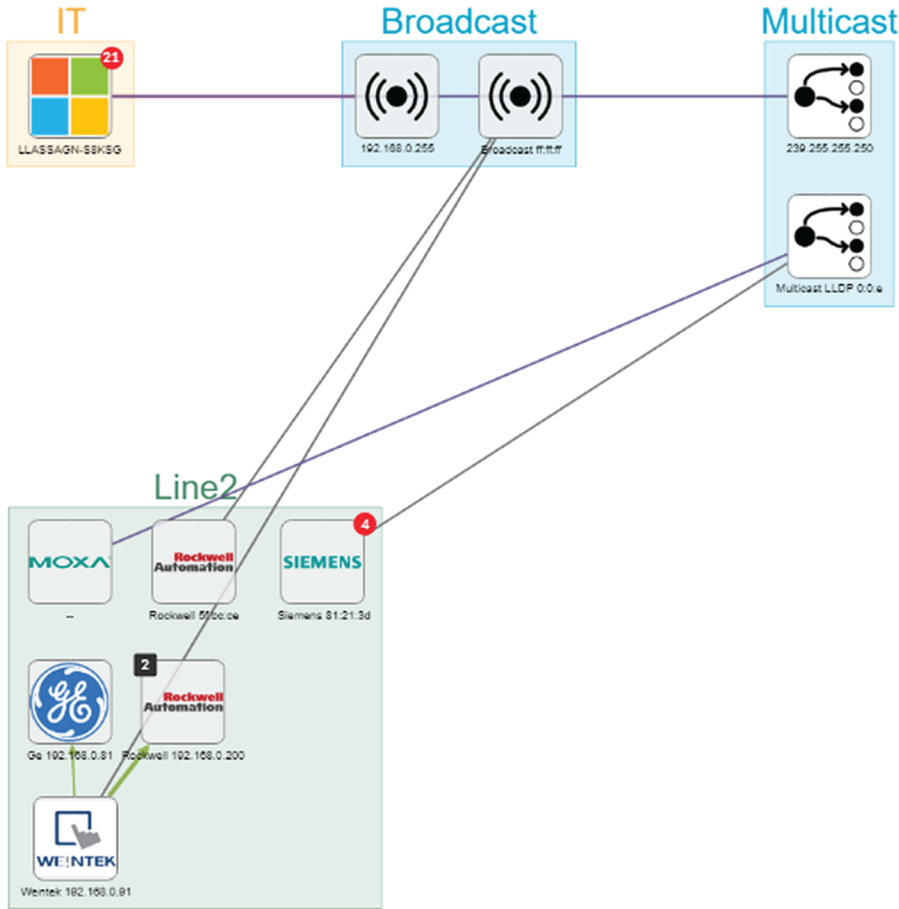
Since a sensor is placed on each production chain, we use the sensor filter to display each production chain. In our example, the industrial network we're monitoring has 3 production lines on which we have positioned a sensor. We want to see and monitor what is happening on production line 2. To do so, we access the Preset

All data in the Explore mode and we select the filter SENSOR\_Line2 (it is possible to rename sensors to identify which area of the network they're monitoring) so only traffic captured on Production Line 2 appears.



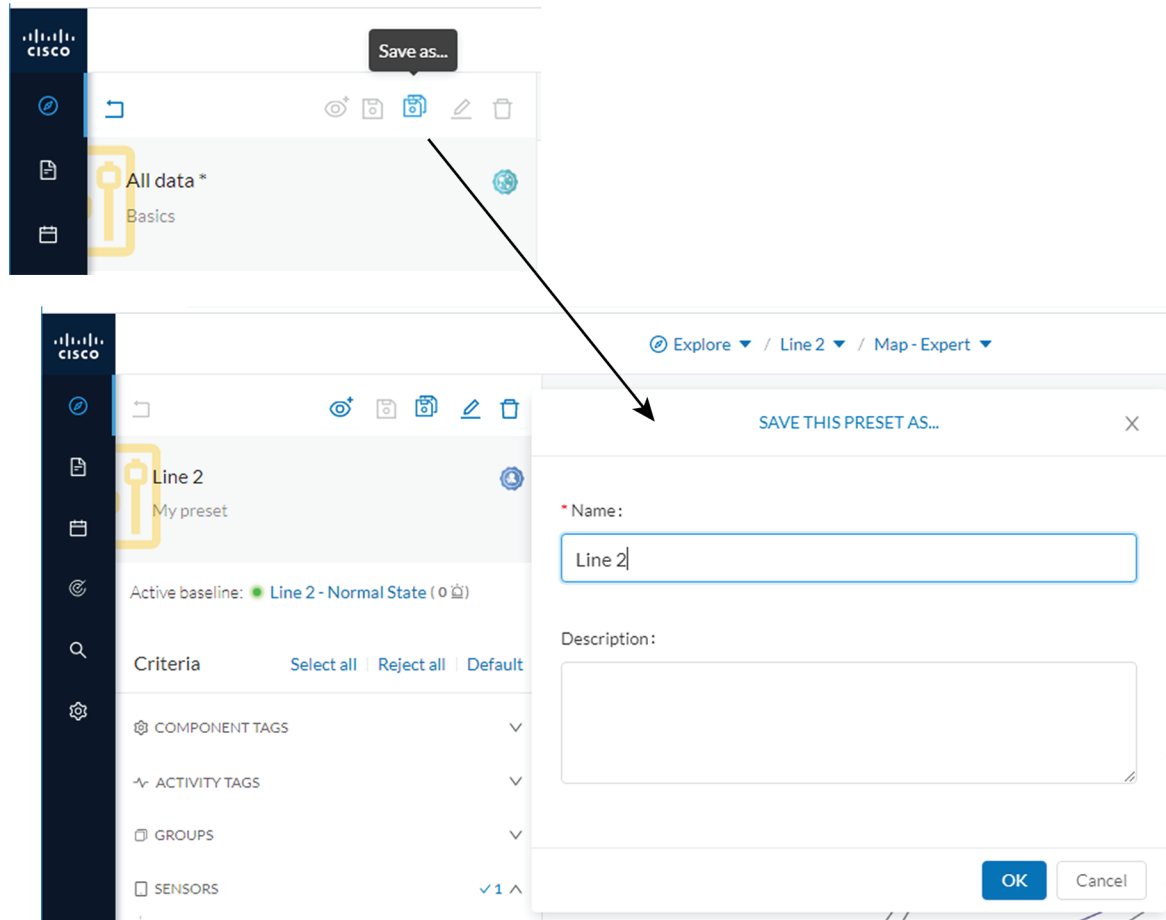
What we need to do then, is to organize the components into groups, per function:

- PLCs in Line 2
- IT
- Broadcast
- Multicast

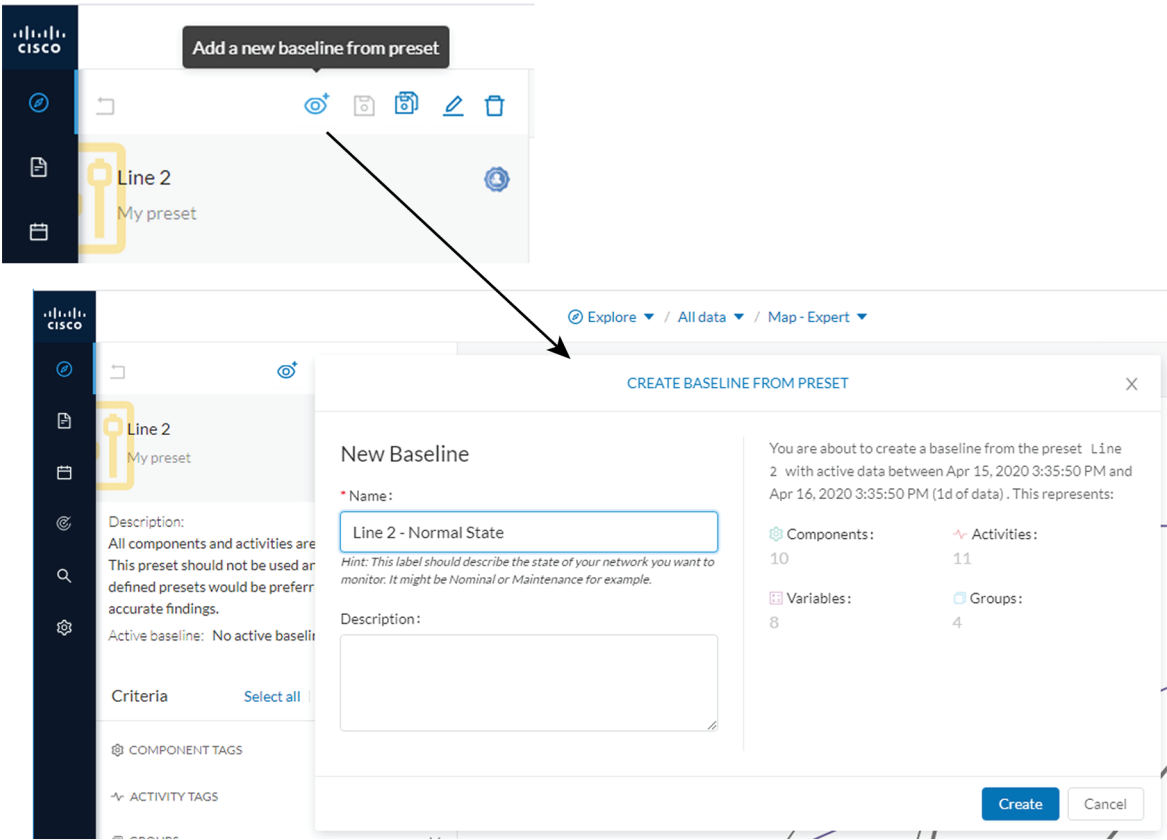


As a result, we have a filtered and organized view of production chain 2.

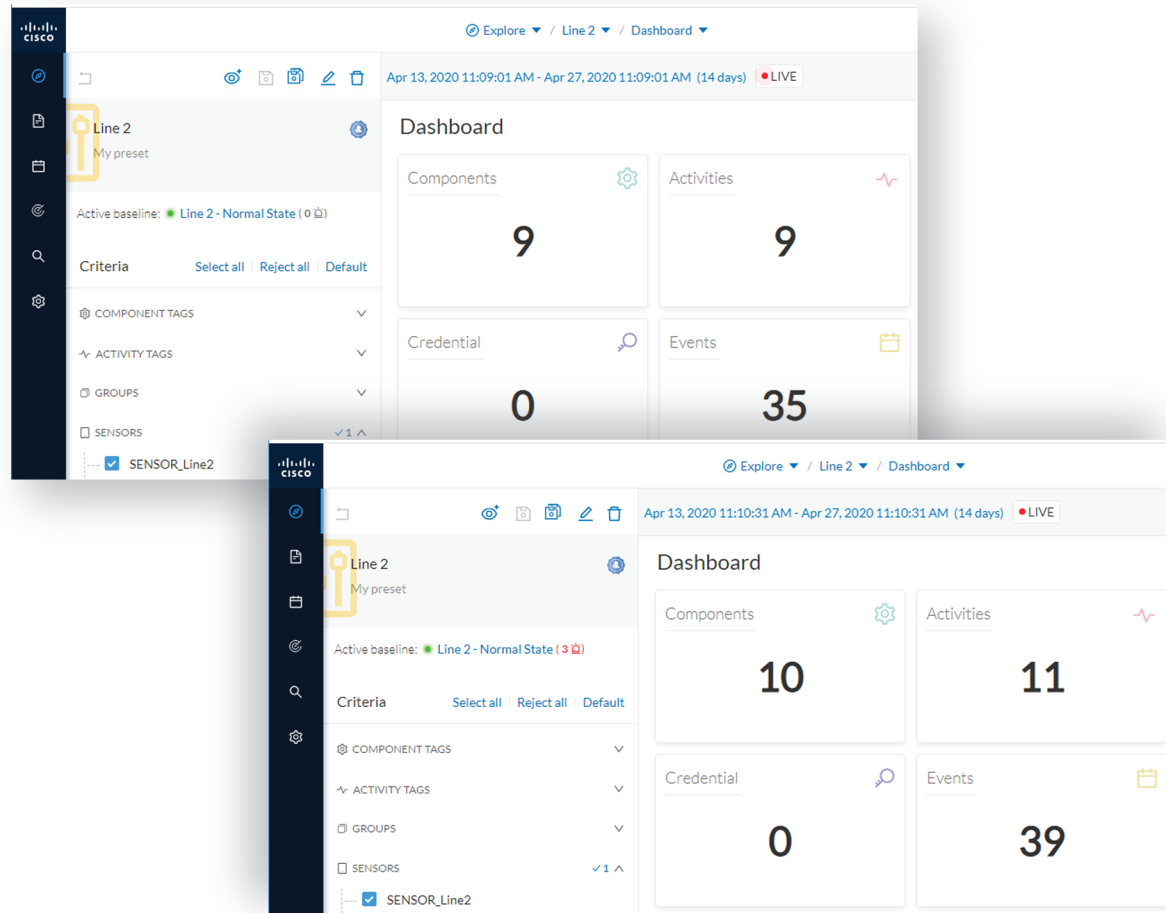
Now that the network data is filtered and grouped, we save the selection as a new preset that we name Line 2.



The preset Line 2 contains components and activities we consider to be interacting in a normal way, that is, production line 2 is in normal operating state. We save the preset's normal state as a baseline that we name Line 2 - Normal State.



We come back later to check Production Line 2. As we access the Explore mode we notice that there are 10 components instead of 9. Number of activities and events have increased too. The baseline Line 2 - Normal State reports 3 alerts.



To understand what had happened exactly, we access the baseline in the Monitor mode.

The left panel indicates that 1 new component and 2 new activities have been found.

As we click the new component, the right side panel opens with the component's detailed properties.

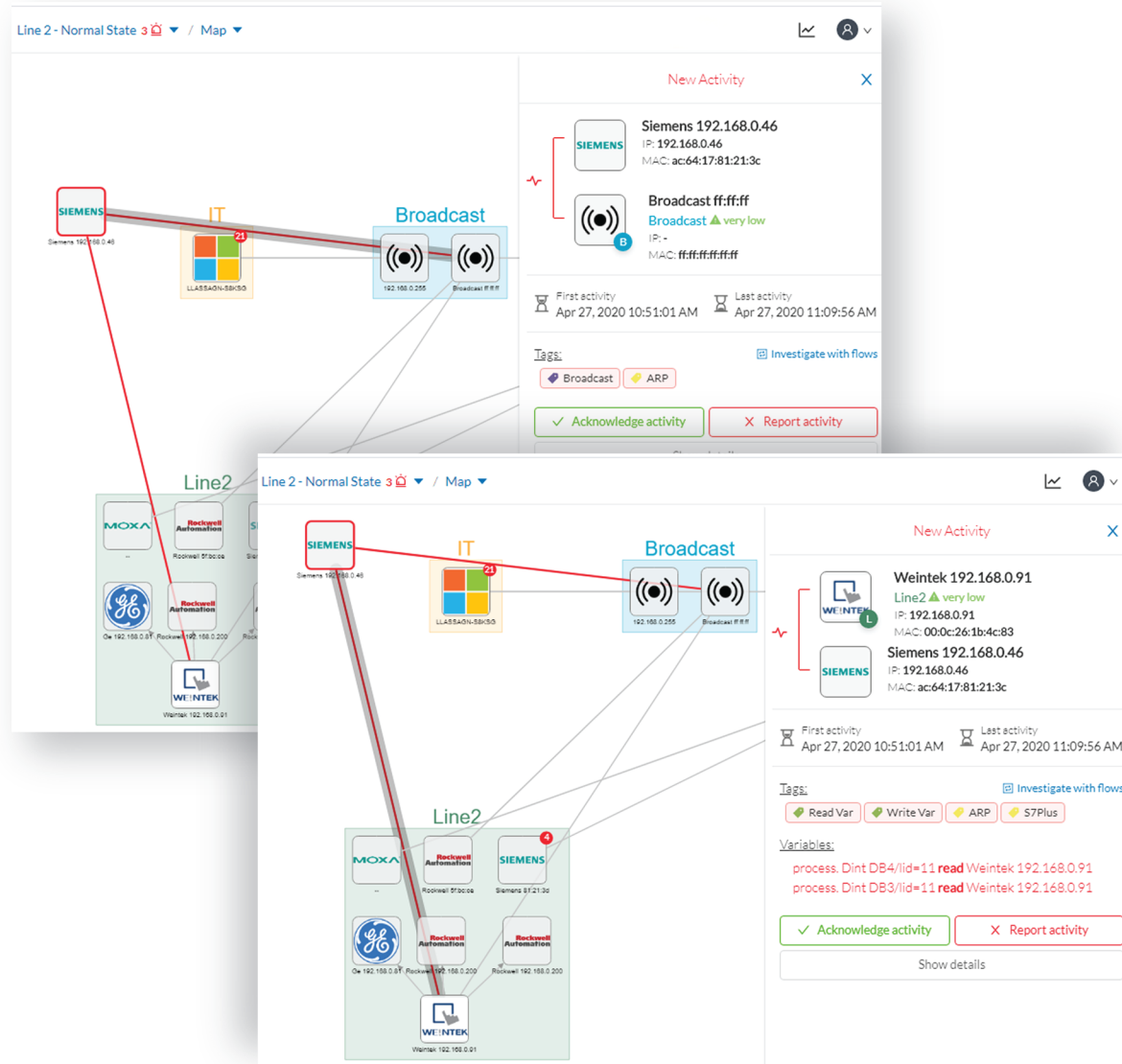
As we observe the component's details, we learn that it is in fact a controller, and properties look like what we're already used to see on the network regarding other components' characteristics. After confirming on site, we discover that a new PLC has been connected to the network to enlarge Production Line 2.

Detection of assets newly connected to the network

The screenshot displays the Cisco Cyber Vision interface for monitoring a network segment labeled 'Line 2'. The main view shows a network map with several components: a Siemens component (IP: 192.168.0.46), an IT component (LLASDAQV-SB-00), a Broadcast component (IP: 192.168.0.255), and a Line2 component containing Moxa, Rockwell Automation, and Weintek devices. A legend indicates that the Siemens component is 'New' (red outline). A 'New Component' panel on the right provides details for the Siemens component: IP: 192.168.0.46, MAC: ac:64:17:81:21:3c. The interface also shows a 'SENSOR Line2' and various activity counts (4 Flows, 4 Events).

Then, we check that this new component behaves normally by looking at its activities. It has been identified because it has sent a broadcast packet (probably ARP) and then has connected to the Weintek machine using a legitimate protocol. Actions like Read variable accesses look normal too.





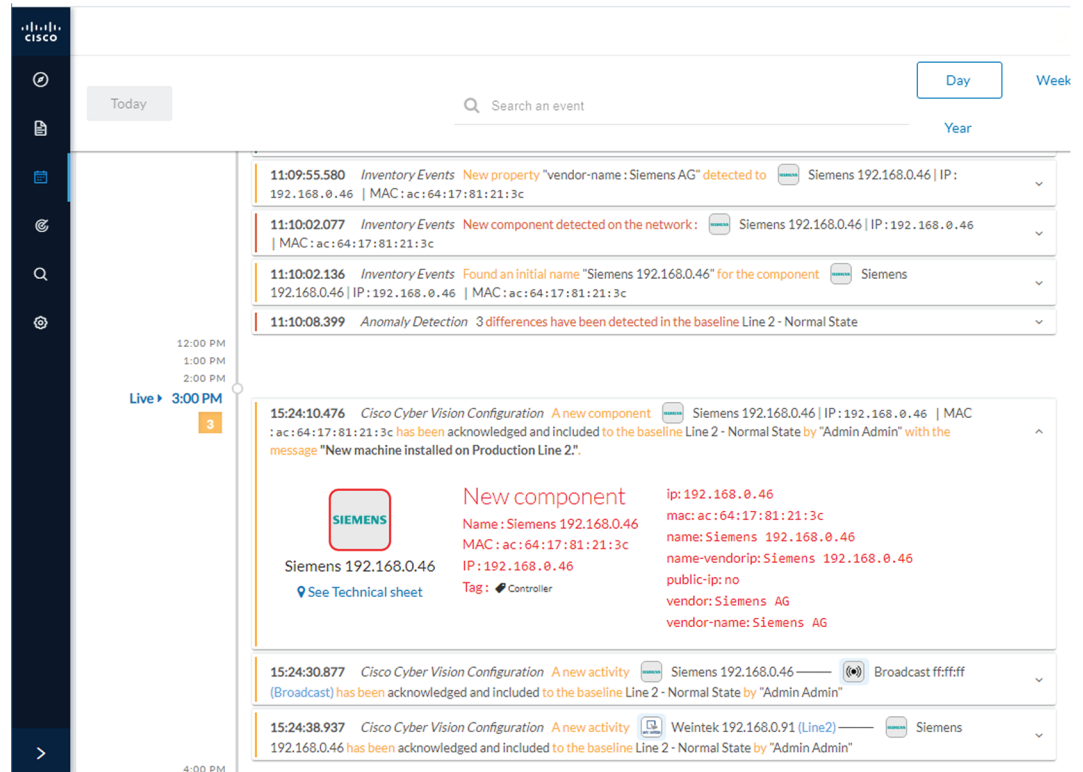
Since the component and activities will be part of the normal operating process of Production Line 2, the differences can be acknowledged and included in the baseline to be notified if any change occurs.

The screenshot displays two overlapping windows in the Cisco Cyber Vision interface. The background window, titled 'New Component', shows details for a Siemens device with IP 192.168.0.46. It includes activity timestamps (Apr 27, 2020), a 'Controller' tag, and various properties like vendor-name, name, ip, public-ip, and mac. At the bottom of this window are buttons for 'Acknowledge component' and 'Report component', along with a 'Show details' link.

The foreground window is an 'ACKNOWLEDGE' dialog box. It contains a green checkmark icon and text explaining the action: 'You are about to acknowledge this difference in your network. It means you consider it as normal.' Below this, there is a text area for a message, with the example text 'New machine installed on Production Line 2.' At the bottom of the dialog are three buttons: 'Acknowledge & Include', 'Acknowledge & Keep warning', and 'Cancel'.

We return to the Explore mode and add the component into the Line 2 group.

Eventually, we access the Events page and see that all previous actions are reported here, from the detection of a new component and activities on the network, to adding the component into the group Line 2.



## Tracking sensitive assets properties

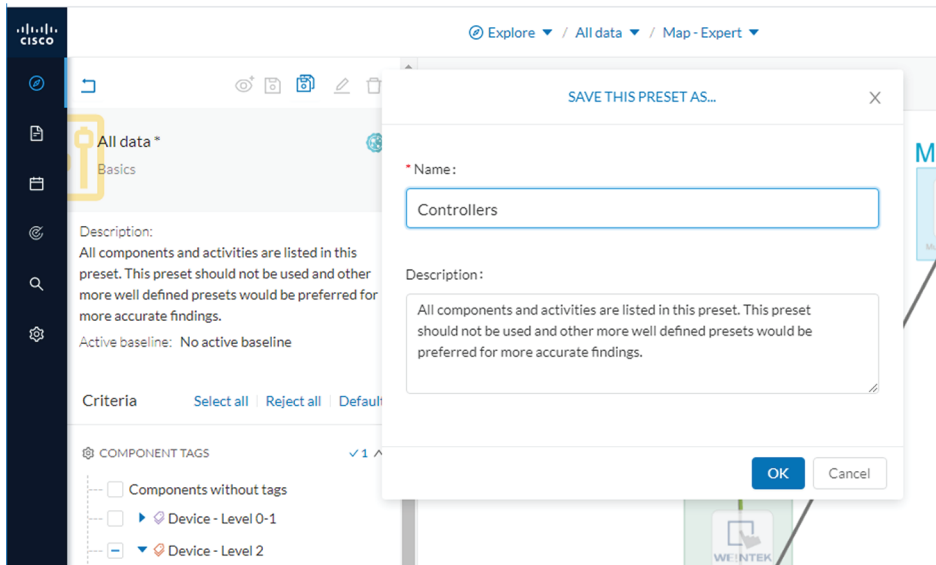
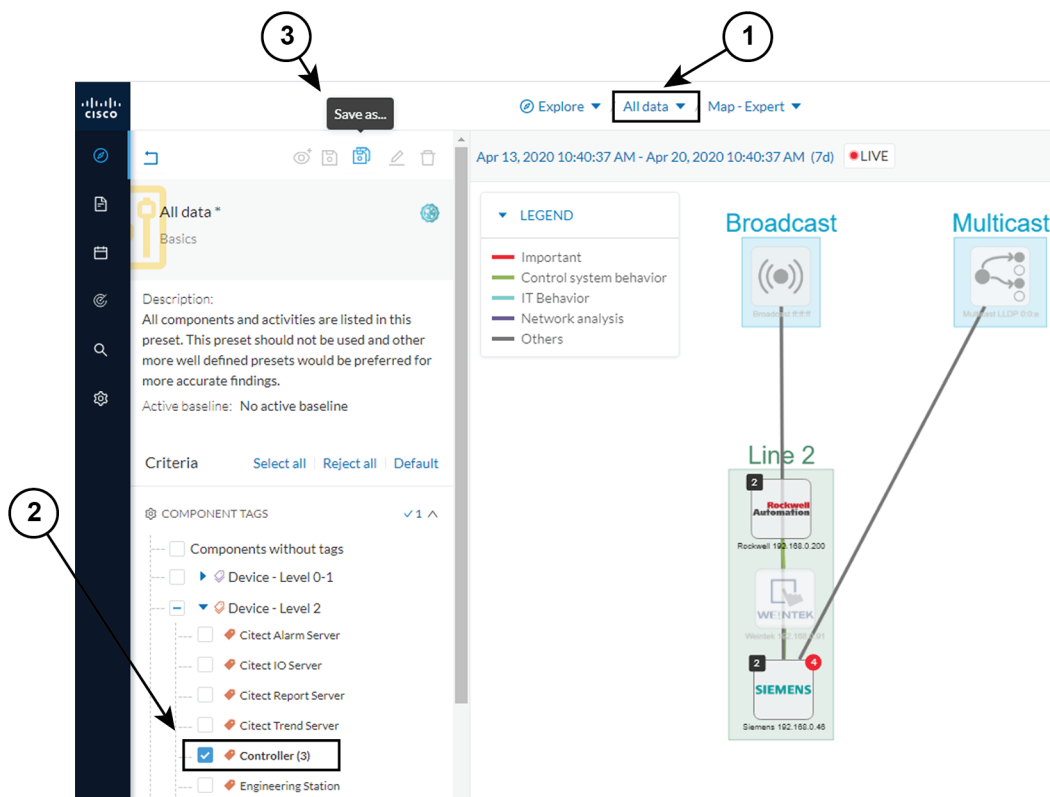
To ensure a network's security, its critical assets need to be monitored closely. Usually, critical assets are controllers which ensure the plant's operation. To monitor them, we're going to check its properties. The properties to keep an eye on are programs and firmware versions changes that might cause malfunctions or even stop a production line.

Preset Definition: Preset need to be defined per Group or multiple Group

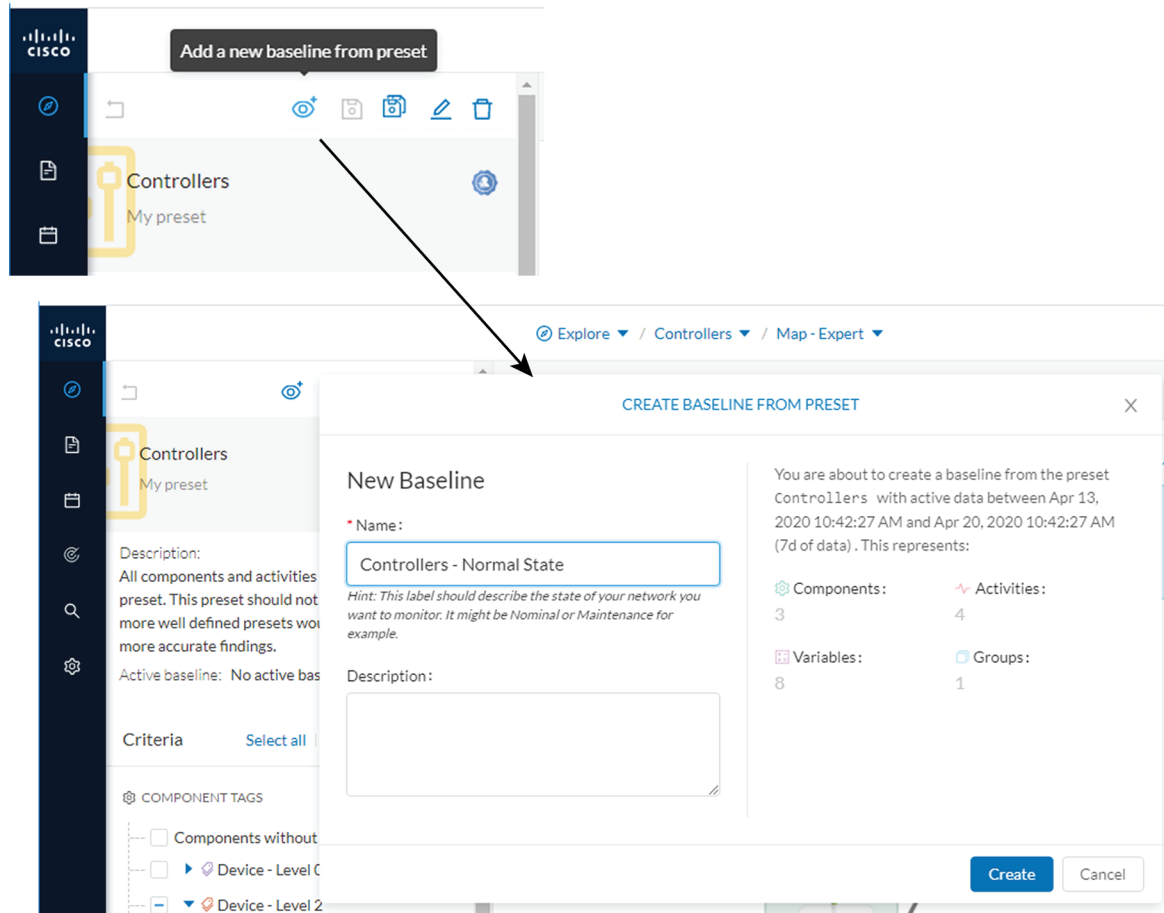
Key Differences: New properties or changed properties on components

In the Explore mode, we access the Preset All data (1). We group the components per function (Broadcast, Multicast, Production Line 2) to organize our data. We select the Controllers component filter (2), so only the components marked with the Controller tag, their activities and related components display.

Now that the network data is filtered and grouped, we save the selection as a new preset (3) that we name Controllers.

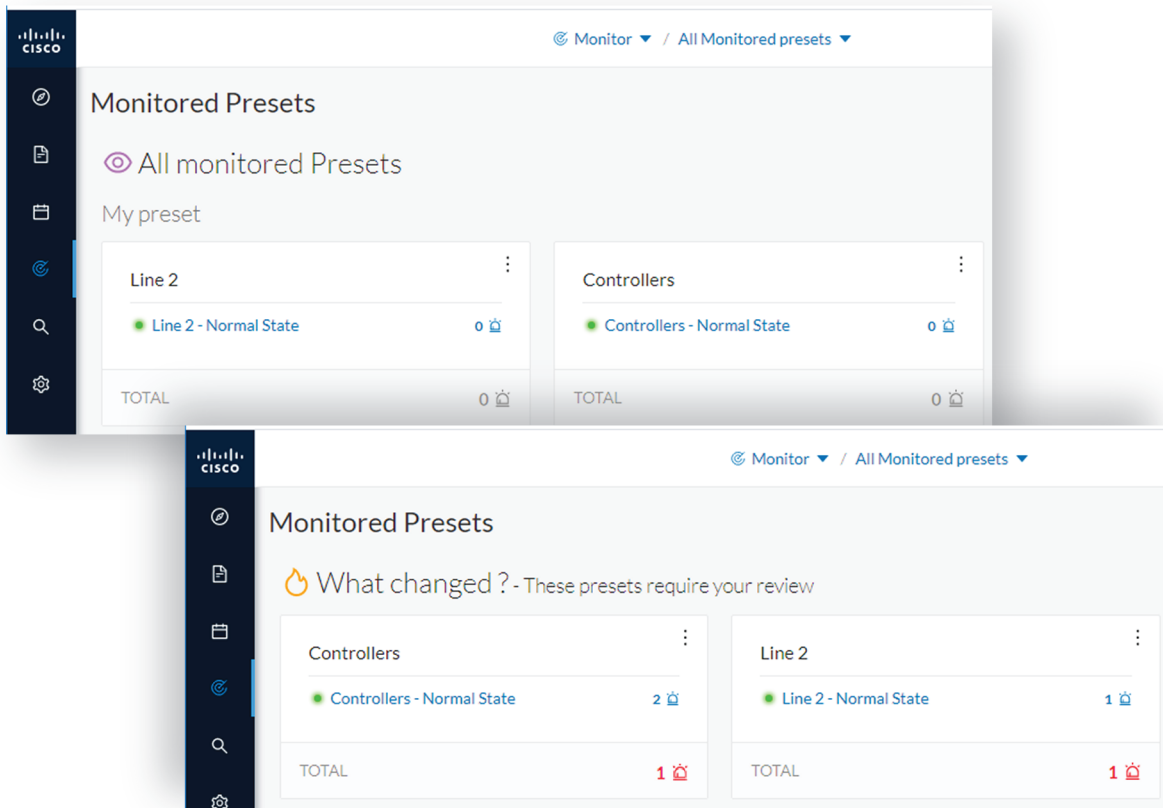


The preset Controllers contains components and activities we consider to be operating in a normal way. We save the preset's normal state as a baseline that we name Controllers - Normal State.



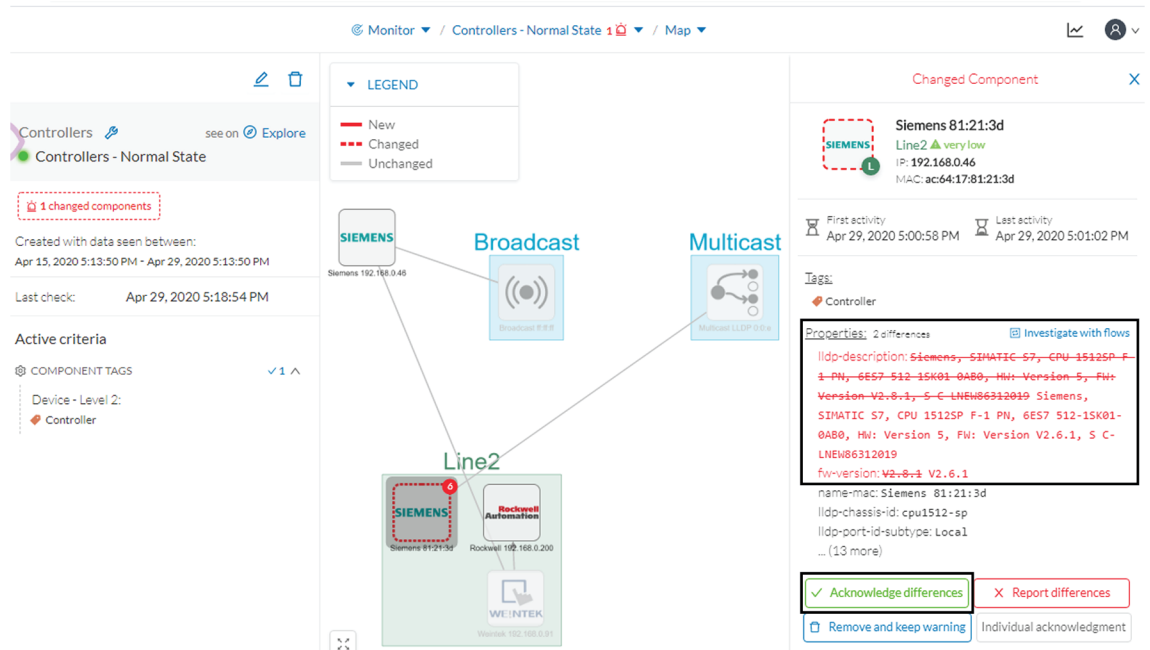
We access the Monitor mode. The new baseline Controllers - Normal State displays.

A few moments pass and two alerts are reported in the Controllers preset. We access the baseline to see what happened.

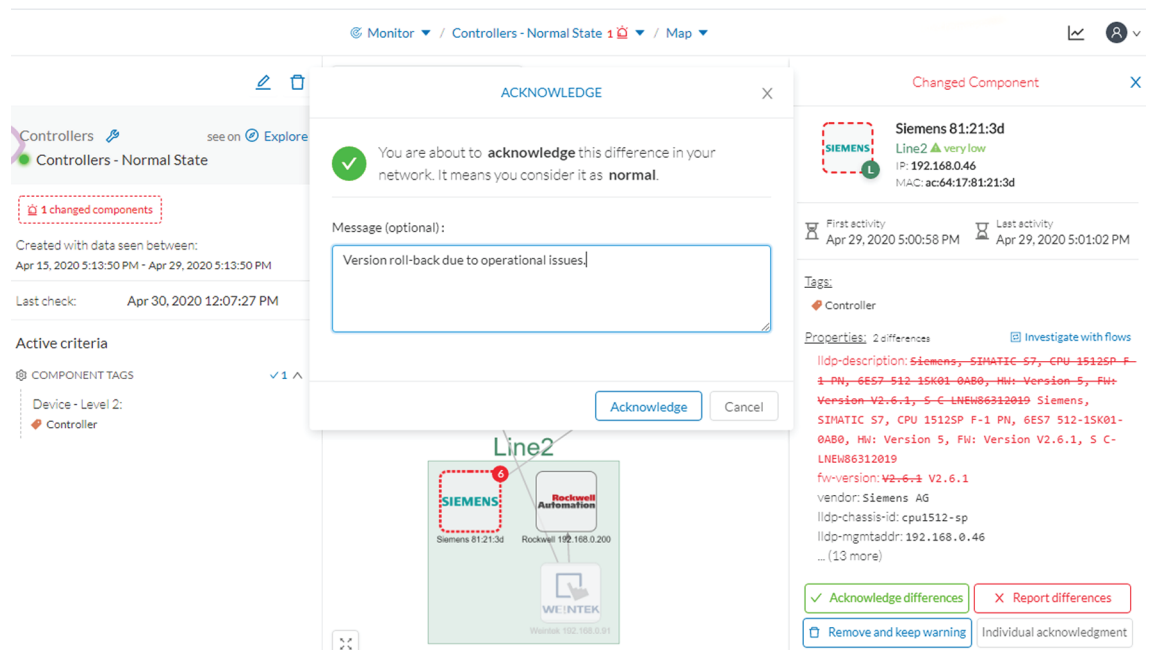


The left panel reports that one component and one activity have changed in the scope of the preset.

As we click on the changed component in the map, a right side panel opens with more information. Changes appear in red. The tag indicates that it's a controller. The properties lldp-description and firmware version have changed and the former version is crossed off.

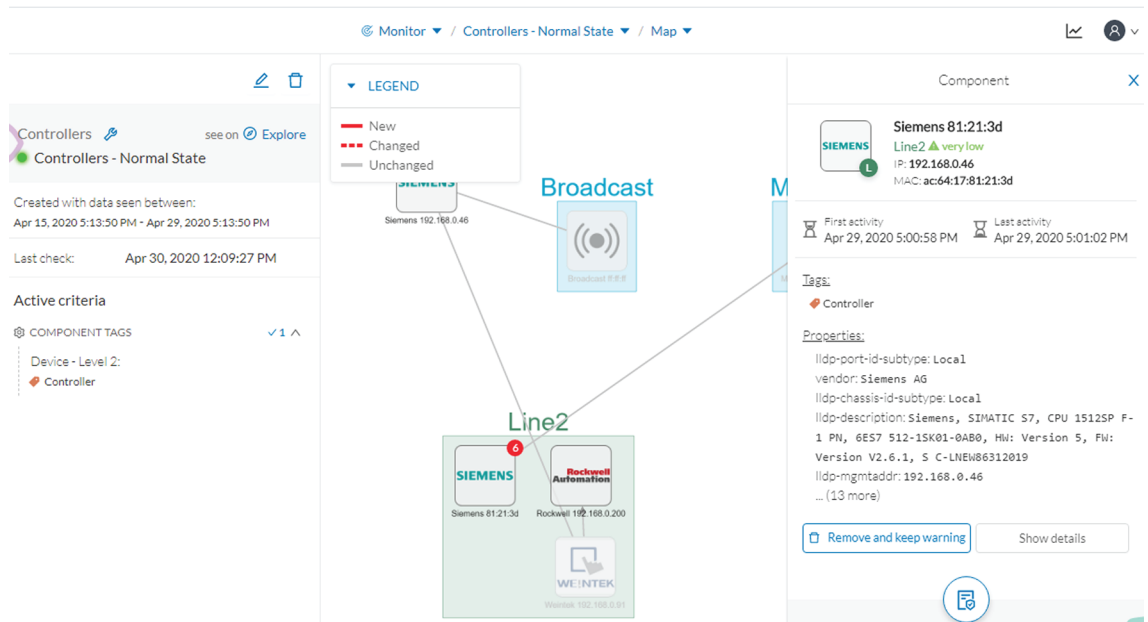


The particularity here is that no activity on the network seems to explain why the SIEMENS component's firmware version rolled back. To figure this out, we meet with the technical operator in charge of the production line. This person informs us that the latest version was causing several issues on the network. Consequently, a rollback has been performed by a maintenance operator to solve these until a new fix comes out. We conclude that this was part of a normal maintenance act and we acknowledge the differences.

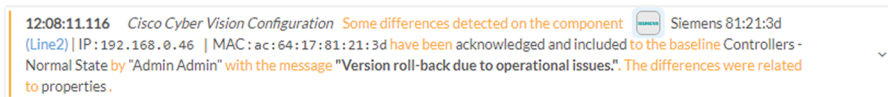


**Detect changes that impact availability and integrity**

Once differences are acknowledged, they are considered as normal and do not appear in red anymore. If a new change happens such as the version update, the component will appear as changed again in the Monitor mode.



An event is generated accordingly to the previous behaviors that have happened on preset Controllers and actions.



**Detect changes that impact availability and integrity**

First evidence that someone might have hacked your industrial control system and is trying to disrupt your industrial processes are Stop CPU orders or new programs sent into a Controller's memory. A station that starts to send such content inside a network must be detected as soon as possible. It is possible to monitor a network by watching all control system behaviors.

This can be done in Cisco Cyber Vision by using the Control System Activities preset, which is a default preset and will check all activity tags categorized as Control System Behavior and consequently all related components. Key differences in such use case are new or changed activities. Moreover, components' tags and properties will give further context to help understanding of what is happening in the network.

Preset Definition: Preset need to be defined per activities tag like "Control Systems Behaviors"

Key Differences: New or changed activities

To do so, we access the preset Control System Activities (1) and we create a baseline from this preset (2) that we name Control System Activities - Normal State (3).



The screenshot displays the Cisco Cyber Vision interface. At the top, a callout box labeled '2' points to the 'Add a new baseline from preset' button. To its right, the 'Control System Activities' dropdown menu is highlighted with a callout labeled '1'. The main dashboard area shows a legend for activity types and a network diagram titled 'Line 2'. The diagram includes nodes for Rockwell Automation (IP: 192.168.0.200), Weintek (IP: 192.168.0.91), Siemens (IP: 192.168.0.46), and GE (IP: 192.168.0.81). A red '6' is visible on the Siemens node.

The 'CREATE BASELINE FROM PRESET' dialog box is shown. The 'Name' field is filled with 'Control System Activities - Normal State'. A hint below the name field reads: 'Hint: This label should describe the state of your network you want to monitor. It might be Nominal or Maintenance for example.' The 'Description' field is empty. Summary statistics are displayed: Components: 4, Activities: 3, Variables: 8, and Groups: 1. 'Create' and 'Cancel' buttons are at the bottom right.

As we access the Monitor mode we can access and see the Control System Activities's baseline we just created. Nothing has happened yet on the preset.

The screenshot displays the Cisco Cyber Vision interface. On the left, a sidebar contains navigation icons. The main panel is titled 'Control System Activities - Normal State' and shows a 'Last check' of 'Apr 22, 2020 11:51:59 AM'. Below this is a list of 'Active criteria' under 'ACTIVITY TAGS', including items like 'Alarm Acknowledgement', 'Block Download', 'Citect Alarm', etc. To the right, a 'LEGEND' box indicates that a solid red line represents 'New', a dashed red line represents 'Changed', and a solid grey line represents 'Unchanged'. The network diagram on the right shows a 'Broadcast' component connected to a 'Line 2' network. The 'Line 2' network includes several devices: two 'Rockwell Automation' units (IPs 192.168.0.200 and 192.168.0.201), a 'GE' unit (IP 192.168.0.81), a 'WEINTEK' unit (IP 192.168.0.91), and a 'SIEMENS' unit (IP 192.168.0.46). Arrows indicate connections between the 'Broadcast' component and the 'Rockwell Automation' and 'WEINTEK' units.

After a few moments, new differences are detected on the preset. The left panel and the Map help identifying what has happened: a new component had an activity which changed another component and its activity with another component (1).

Clicking the new component (2) opens a right side panel which offers more information. The tag Windows indicates that the new component is a Windows machine (3). Below, its properties are listed and give more information about the machine.

The screenshot displays the Cisco Cyber Vision interface. On the left, the 'Control System Activities - Normal State' section shows a legend with 'New' (red solid line), 'Changed' (red dashed line), and 'Unchanged' (grey solid line). Below this, a list of 'Active criteria' includes various system behaviors like 'Alarm Acknowledgement', 'Block Download', and 'Firmware Download'. The central network diagram shows a 'Line 2' connection between a 'Broadcast' node and an 'IT' node (LLASSAGN-S8KSG). The IT node is highlighted with a red dashed border, indicating a change. The right-hand panel provides details for this component, including its IP (192.168.0.231), MAC (00:e0:4ca8:69:db), and a list of activity tags such as 'Windows', 'Firmware Download', 'Start CPU', and 'Stop CPU'. At the bottom right, there are summary statistics for 'Flow' (39) and 'Event' (11).

Clicking the new activity between the new machine and the CPU opens its right side panel and gives more information about what happened. New tags such as Firmware Download, Start CPU, Stop CPU, Read and Write Var, which are suspicious, indicate the type of actions the new Windows machine has performed on the CPU.

The screenshot displays the Cisco Cyber Vision Monitor interface. On the left, there are panels for 'Control System Activities' with filters for '1 new components', '1 new activities', '1 changed components', and '1 changed activities'. Below this is a list of 'Active criteria' under 'ACTIVITY TAGS'. The central area shows a network diagram with nodes for 'Broadcast', 'IT', and 'Line 2'. A legend indicates that red dashed borders represent 'New' components, red solid borders represent 'Changed' components, and grey solid borders represent 'Unchanged' components. On the right, a 'New Activity' panel shows details for 'LLASSAGN-SBKSG', including IP (192.168.0.231), MAC (00:e0:4c:a8:69:db), and CPU (CPU1512-SP). Below the activity details are tags for 'Firmware Download', 'Start CPU', 'Stop CPU', 'Read Var', 'Write Var', and 'S7Plus', along with 'Approve activity' and 'Report activity' buttons.

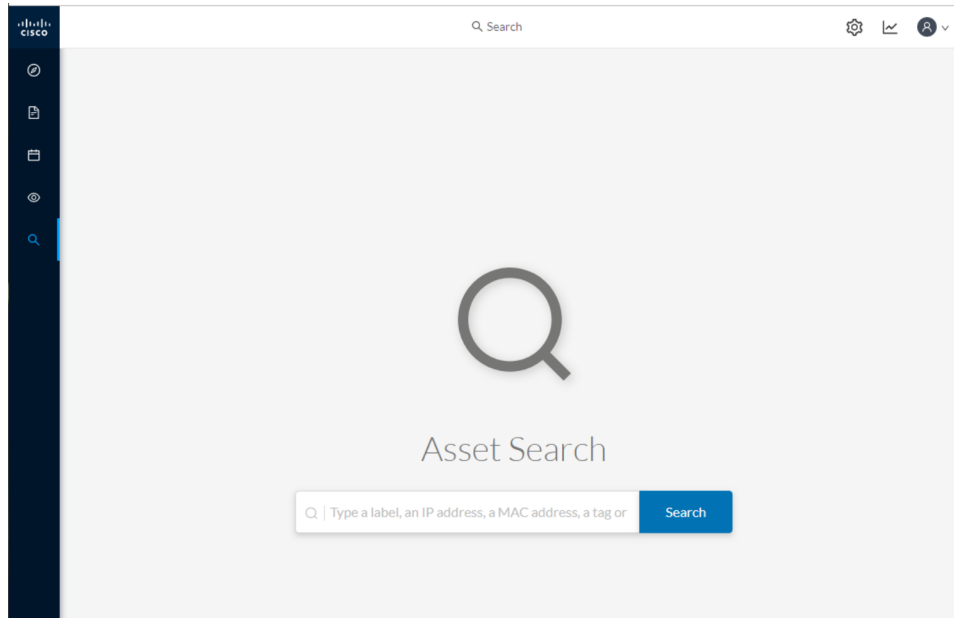
These elements let us think that this is actually an attack. We report this issue and start to counter the attack immediately with the security team. If other suspicious changes happen, the Monitor mode will notify them.

## Search

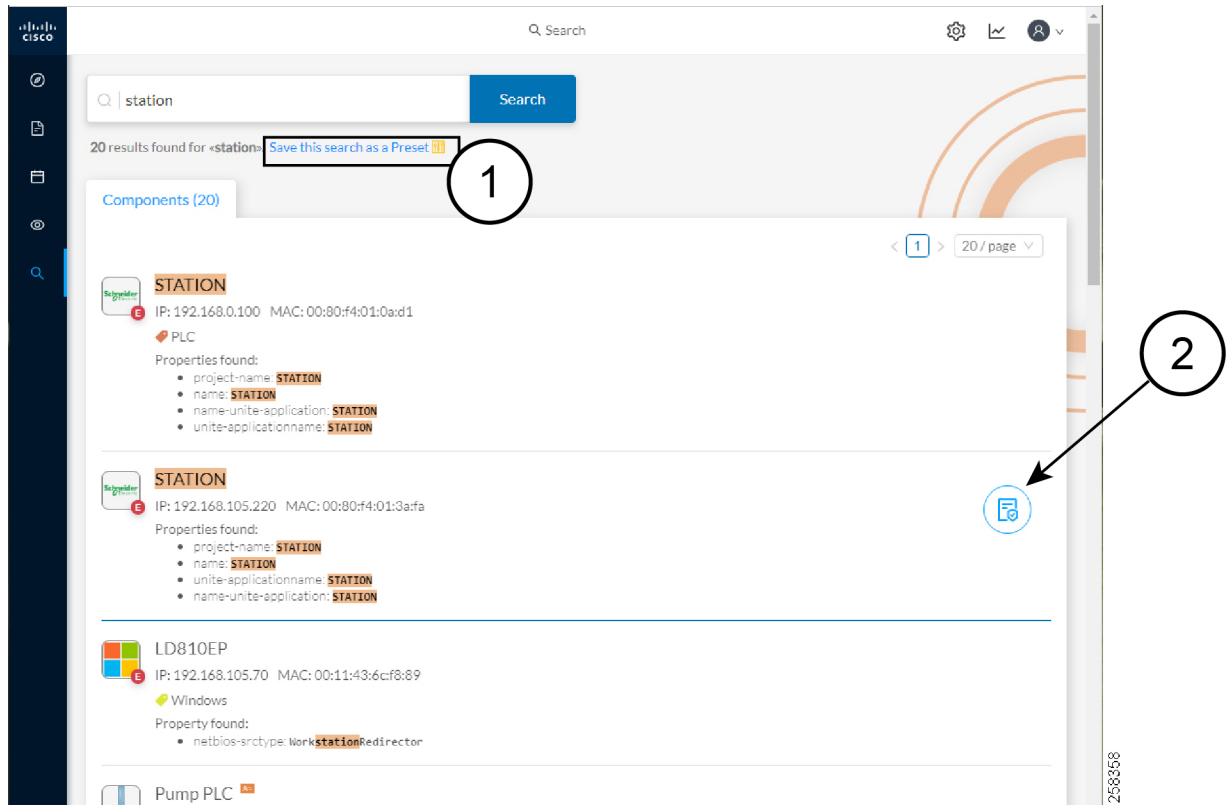
This page is available to search for components among unstructured data. You can search components by name, custom name, IP, MAC, tag and property value.



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



Results out of a Station research:



In the example above, 20 components have been found with the mention "station" in their name, property values and tags.

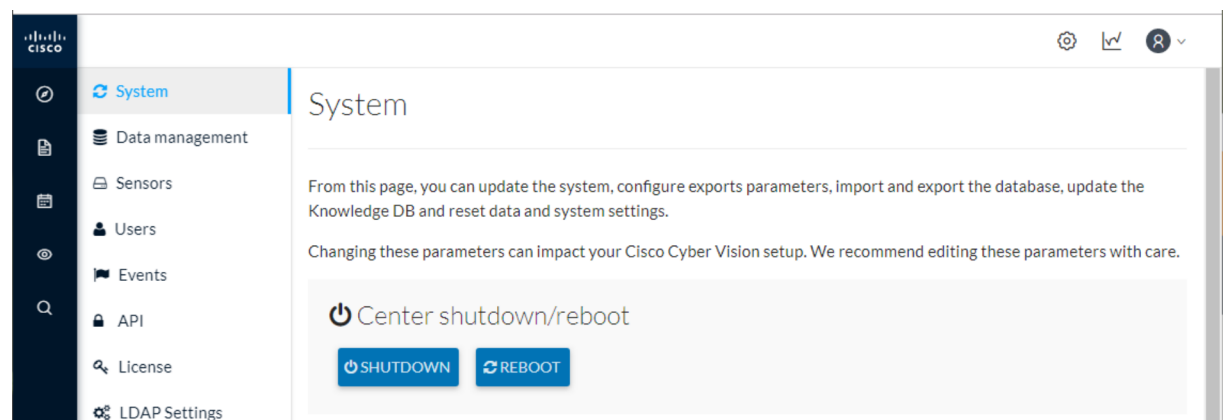
It is possible to create a preset out of your research results (1). Presets created out of results will automatically update as new data are detected on the network.

If you mouse over a component, the button that gives access to its [Technical sheets](#) (2) appears. This view will give you access to advanced data about the component.

# Admin

## System

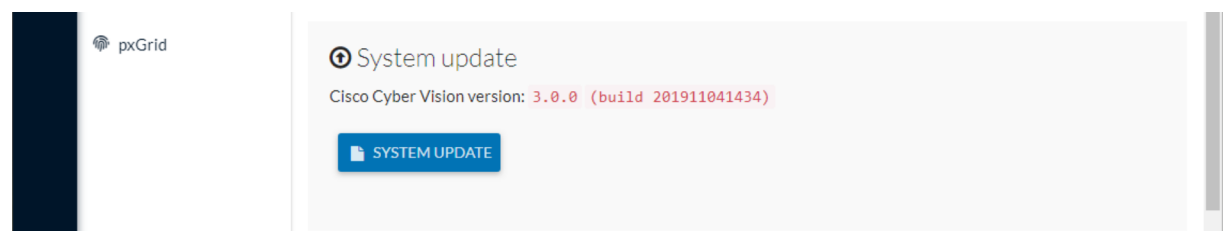
### Center shutdown/reboot



You can trigger a safe shutdown and reboot of the Center from the System administration page.

The reboot can be used in case of a minor bug. For instance, in case of a system overload.

### Upgrade with a combine update file



Version releases usually include updates for both the sensors and the Center (i.e. combined updates). If operating conditions make it possible, you can update the Center and all its online sensors at once from the user interface. You can proceed to a combined update without opening a shell prompt and using SSH.



**Note** Combined updates are applied to the Center and all its online sensors. Make sure (by accessing the sensor administration page) that all your sensors are connected and SSH is authorized between the Center and the sensors before proceeding to a combined update.



**Important** Rolling back to an older Cisco Cyber Vision version is not possible.

Requirements:

- 
- A combined update.

To verify that the file you just downloaded is healthy, it is recommended to use the SHA512 checksum provided by Cisco.

To do so (Windows users):

**Procedure**

**Step 1** Access Cisco Cyber Vision download page.

**Step 2** Download the file.

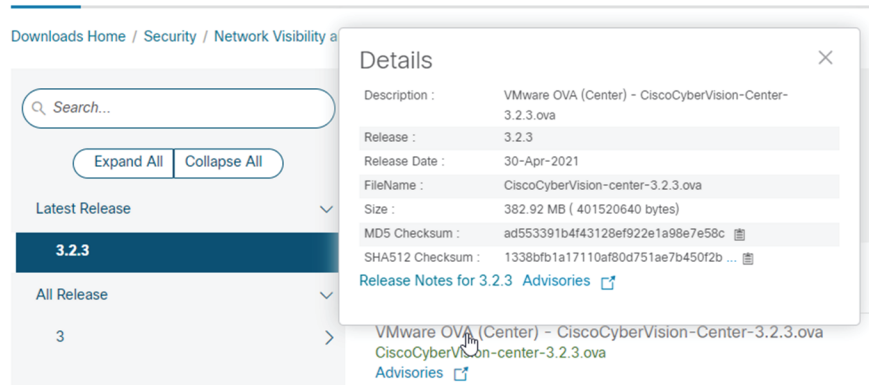
**Step 3** Open a shell prompt such as Windows Powershell and use the following command to retrieve the file checksum:

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      : 13388FB1A17110AF80D751AE7B450F2B29CC84CB54F550F38BBE6B4236865EC9EDF7773FD05D1055C7F1EF76E68C2B8A96CFE69AB
          : 1B622E4B08B8E8B9E940816
Path      : C:\Users\ \Downloads\CiscoCyberVision-center-3.2.3.ova
```

**Step 4** In the download page, mouse over the file and copy the SHA512 checksum.

## Software Download



**Step 5** Compare both checksums.

- If both checksums are identical it means the file is healthy.
- If the checksums do not match try to download the file again.

- If, after downloading the file again the checksums still don't match, please contact Cisco support.

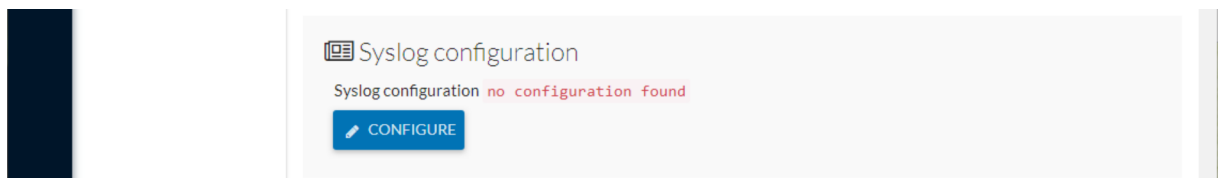
To update the Center and all its online sensors:

- Step 6** Access the Cisco Cyber Vision's user interface.
- Step 7** Access System administration > System and use the System update button.
- Step 8** Select the update file CiscoCyberVision-update-combined-<VERSION>.dat
- Step 9** Confirm the update.

As the Center and sensors updates proceed, you are redirected to a holding page. Once the update is finished the Center and the sensors need to reboot and you will be logged out from the user interface.

- Step 10** Log in again to the user interface.
- Step 11** If there were offline sensors when the update occurred, the same procedure can be used as many times as necessary to update all sensors.

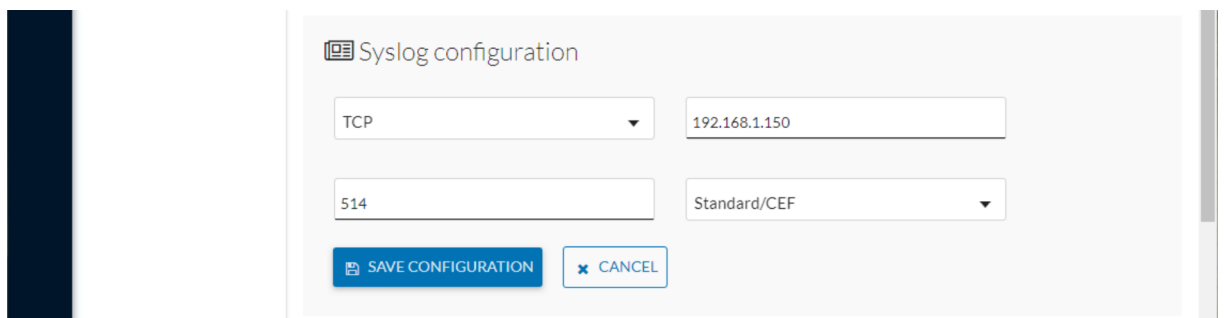
## Syslog configuration



Cisco Cyber Vision provides syslog configuration [Events](#) and used by a SIEM. To configure which machine the syslogs will be sent to:

### Procedure

- Step 1** Click Configure.



- Step 2** Select a protocol.
- Step 3** Enter the IP address of the SIEM reachable from the Administration network interface (i.e. eth0) of the Center.
- Step 4** Enter the port on the SIEM that will receive syslog.
- Step 5** Select the variant of syslog format:



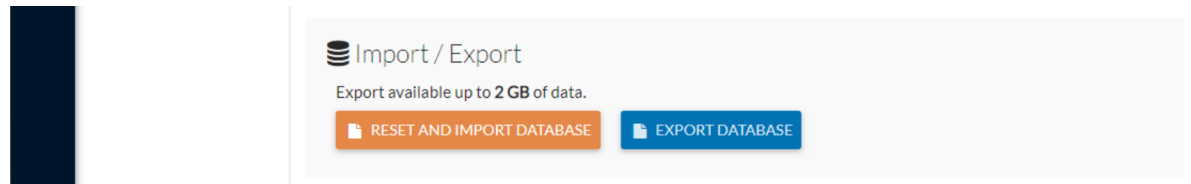
- Standard: event messages are sent in a format specific to Cisco Cyber Vision and with legacy timestamps (one-second precision).
- CEF: industry standard ("Common Event Format") which is understood by most SIEM solutions (no extra configuration is needed on the SIEM). This is the recommended option.
- RFC3164: extended syslog header format with microsecond precision for timestamps.

**Step 6** If you select TCP + TLS connection an additional "set certificate" button displays to import a p12 file. This file is to be provided by the administrator of your SIEM solution to secure the communications between the Center and the syslog collector.

## Import/Export

You can import and export the Cisco Cyber Vision database from the System administration.

This can be used on a regular basis to backup the industrial network data on Cisco Cyber Vision or if you need to transfer the database to a different Center.



Exports are possible up to 2 GB of data to avoid side effects related to slow database exports. If the database is larger than 2 GB, you will get an error message. In this case, you must connect to the Center using SSH and perform a data dump using the command `sbs db dump`.

Network data, events, users will be kept as well as all customizations (e.g. groups, component names).

As for configurations, only those made in the Cisco Cyber Vision user interface will be kept. Thus, if you change Center you will have to perform a basic configuration of the Center and then configure Cisco Cyber Vision again (refer to the Center Quickstart Guide).



**Note** Import can last up to one hour for big databases. However, you can refresh the page from time to time to check that the import keeps going on normally (i.e. no error message).

## Knowledge DB

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

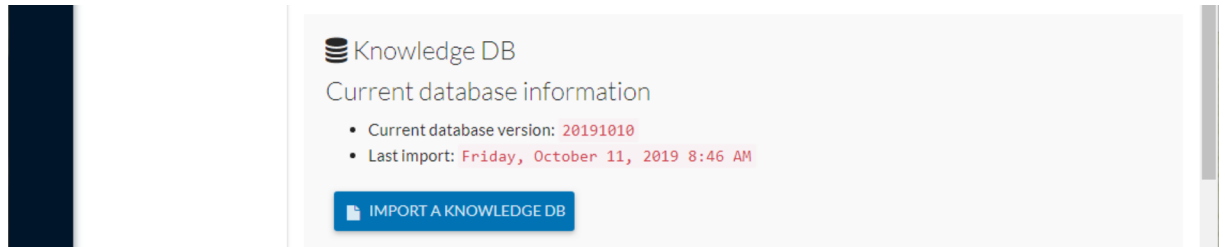


**Important** It is important to update the Knowledge DB in Cisco Cyber Vision as soon as possible after notification of a new version to be protected against vulnerabilities.

To update the Knowledge DB:

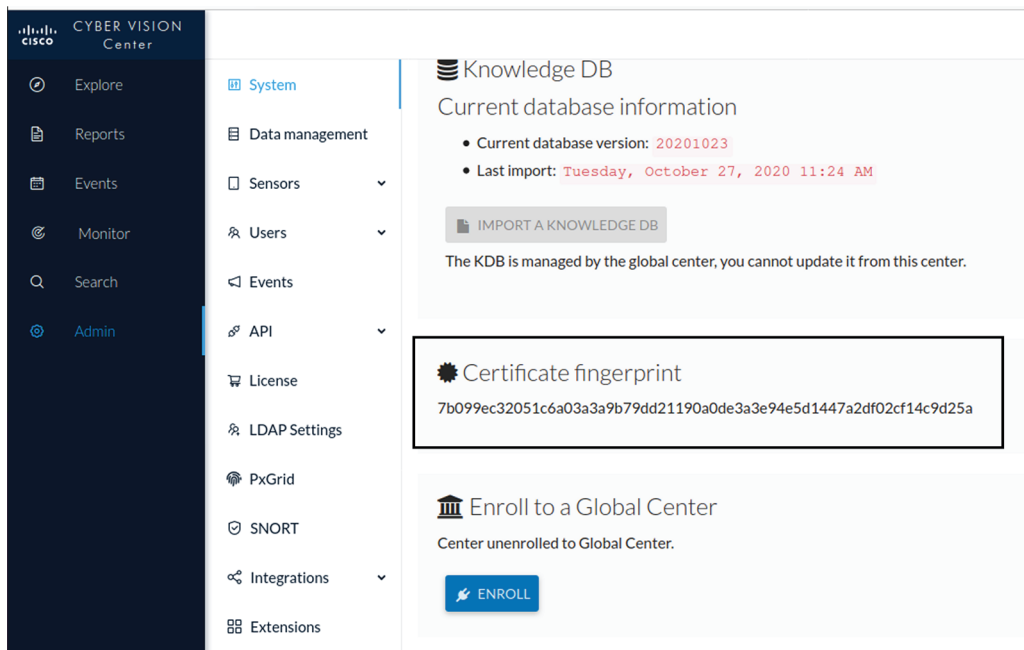
**Procedure**

- Step 1** Download the latest.db file available.
- Step 2** From the Cisco Cyber Vision system administration page click the Import a knowledge DB button to upload the file.
- Step 3** Importing the new database will rematch your existing components against any new vulnerabilities and update network data.



**Certificate fingerprint**

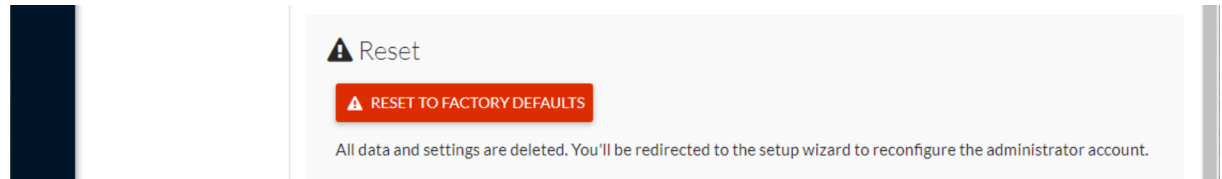
The certificate fingerprint is used to register and enroll a Global Center with its synchronized Centers and vice versa.



For more information, refer the the Centers installation guides.

## Reset

A Reset to Factory Defaults should be performed carefully with the help of Cisco product support and be used only as a last resort when all other troubleshooting attempts have failed. Please read below all implications of taking this action.



Reset to Factory Defaults is to be used as a last resort to clear all existing data from the Center.

Proceeding to a Reset to Factory Defaults will lead to the deletion of:

- 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 will be kept.

Once a Reset to Factory Defaults has been performed, the GUI page refreshes with the Cisco Cyber Vision installation wizard (refer to the Center Quickstart Guide).

## Data management

From the system administration page, you can manage data stored on Cisco Cyber Vision by [Clear data](#) to optimize the Center performances, [Expiration settings](#), and [Ingestion configuration](#).

Cisco Cyber Vision update procedure will not purge any 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 24hours), it is possible to proceed to a data purge in release 3.2.x to shorten the migration process. This purge can be launched either from the [Clear data](#) page in the Graphic User Interface (UI), or from the Command Line Interface (CLI), using the following command where different options will be offered:

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

Once migrated, the database content will be managed with version 4.0.0 new data retention policies. Expiration settings will be applied, and the system will purge by default:

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

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

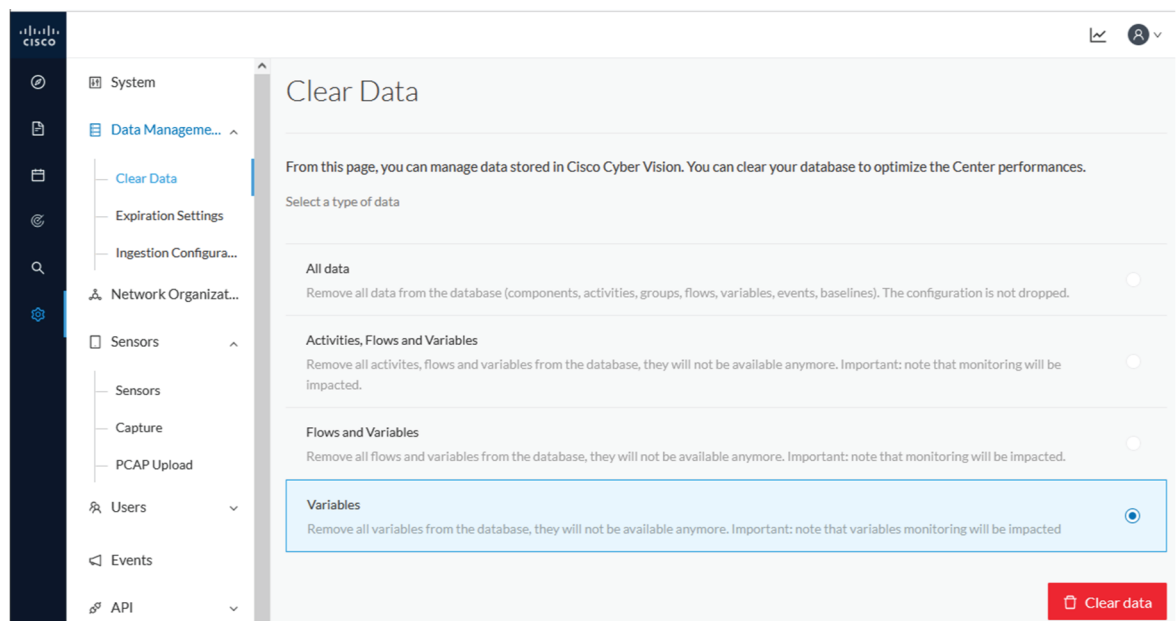
## Clear data

From this page, you can clear data stored on Cisco Cyber Vision to optimize the Center's performances.

You can clear data partially or totally, like below:

- all data
- activities, flows and variables
- flows and variables
- variables

Clearing data should be performed carefully with the help of Cisco Cyber Vision product support and be used only as a last resort when all other troubleshooting attempts have failed. Clearing any data can impact monitoring of the network. Please read below all implications about all data clearance.



About all data clearance:

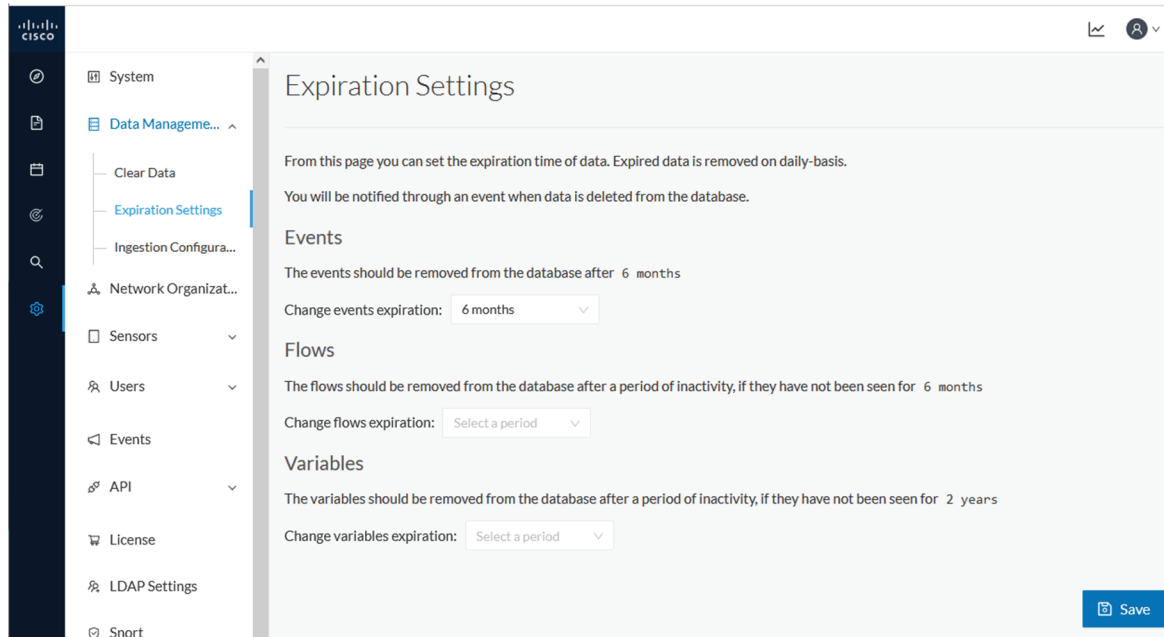
Clearing all data is to be used as a last resort in case of database overload issues.

This will result in the entire database content deletion. Network data such as components, flows, events and baselines will be deleted from Cisco Cyber Vision and the GUI will be emptied.

All configurations will be saved. Existing users and user data configuration (such as capture modes, events severity set up, syslog configuration) will remain unchanged.

## Expiration settings

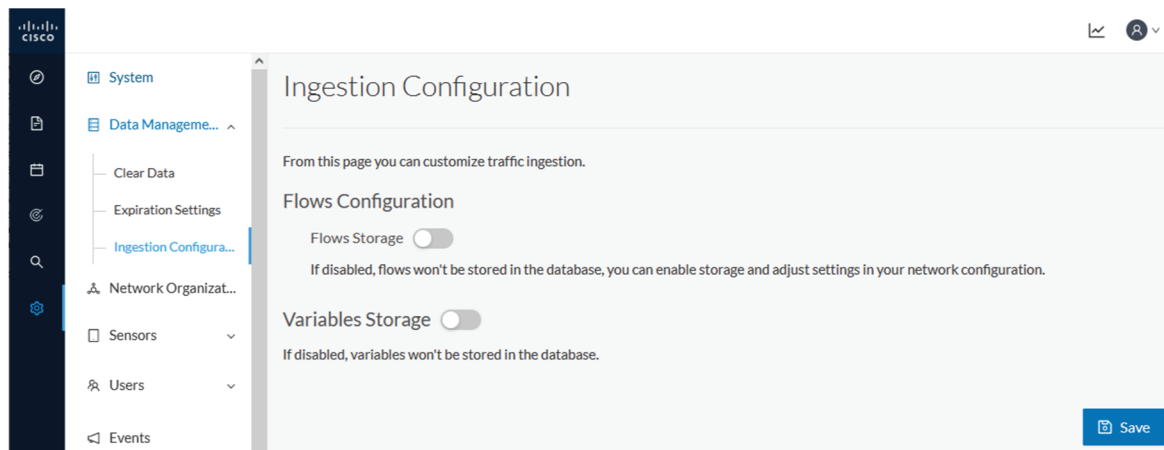
From this page, you can set data expiration time. Data is removed on a daily-basis once they expire. You can set an expiration time to events, flows and variables independently, and for a period of 7 days, 1 month, 3 months, 6 months or 1 year.



## Ingestion configuration

The ingestion configuration page allows you to configure flow and variable traffic storage.

You can choose whether to store flows and variables.



If flows 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", that is, flows that are not part of the industrial private network, is disabled by default.

**Flows Configuration**

Flows Storage

If disabled, flows won't be stored in the database, you can enable storage and adjust settings in your network configuration.

Network Name	Flow Storage
Others	<input type="checkbox"/>
Endpoints without IP address	<input checked="" type="checkbox"/>
10/8 private network	<input checked="" type="checkbox"/>
172.16/12 private network	<input checked="" type="checkbox"/>
192.168/16 private network	<input checked="" type="checkbox"/>
FC00::/7 IPv6 local unicast	<input checked="" type="checkbox"/>

It is also possible to choose if enabling flows aggregation and port scan detection.

Flows Aggregation

Cisco Cyber Vision stores every individual network flow that has been seen by the sensors with full details (including the client/server ports for each flow).  
For some TCP/UDP based protocols, the client port is dynamically generated by the client and thus Cisco Cyber Vision will store multiple similar copies of the flow for each spotted client port.  
When enabling flow aggregation, Cisco Cyber Vision will instead discard the client port, thus limiting the number of flows in the database.

Only the following protocols are concerned by flow aggregation: DNS, NTP, SSH, SNMP, Syslog, RabbitMQ, HTTP(S), IEC104, EtherNet/IP.  
Flows for other protocols are always stored with full details.

Port scan detection

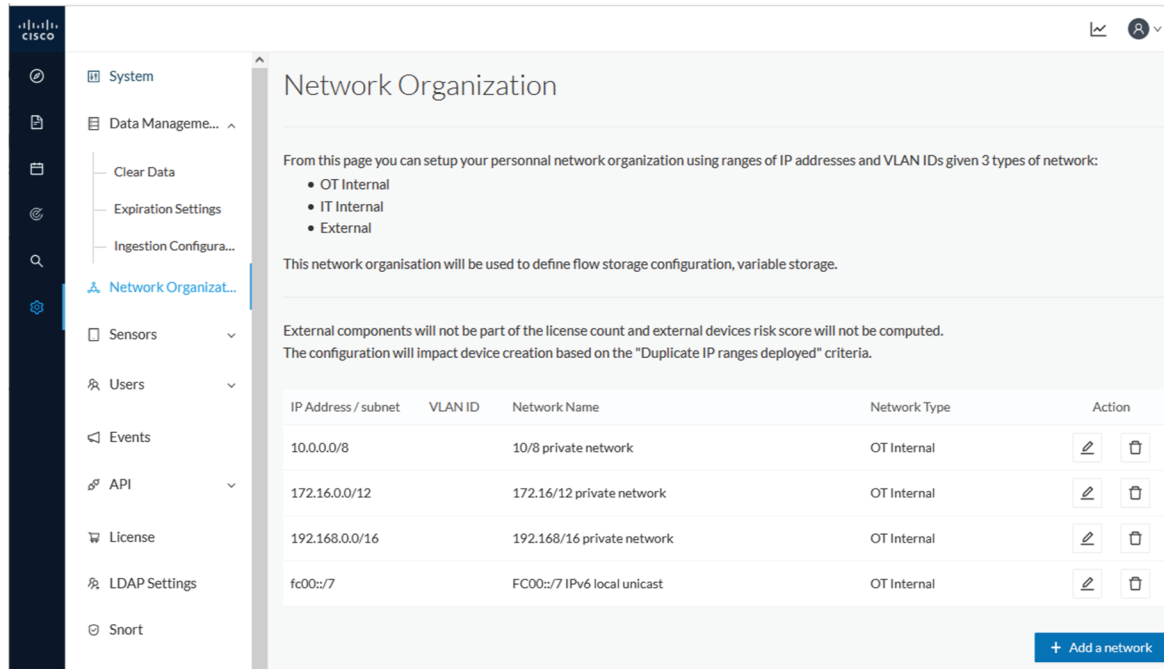
## Network organization

This page allows you to setup the subnetworks inside the industrial network by defining IP address ranges and declaring whether networks are internal or external.

Defining subnetworks is useful for several reasons:

- It allows you to choose afterwards how related flows should be stored through the [Ingestion configuration](#).
- It will impact devices' [Risk score](#), since a private network is considered as safer than an external one.
- Cisco Cyber Vision license will be more accurate, because devices from an external network will be excluded from the [License](#).

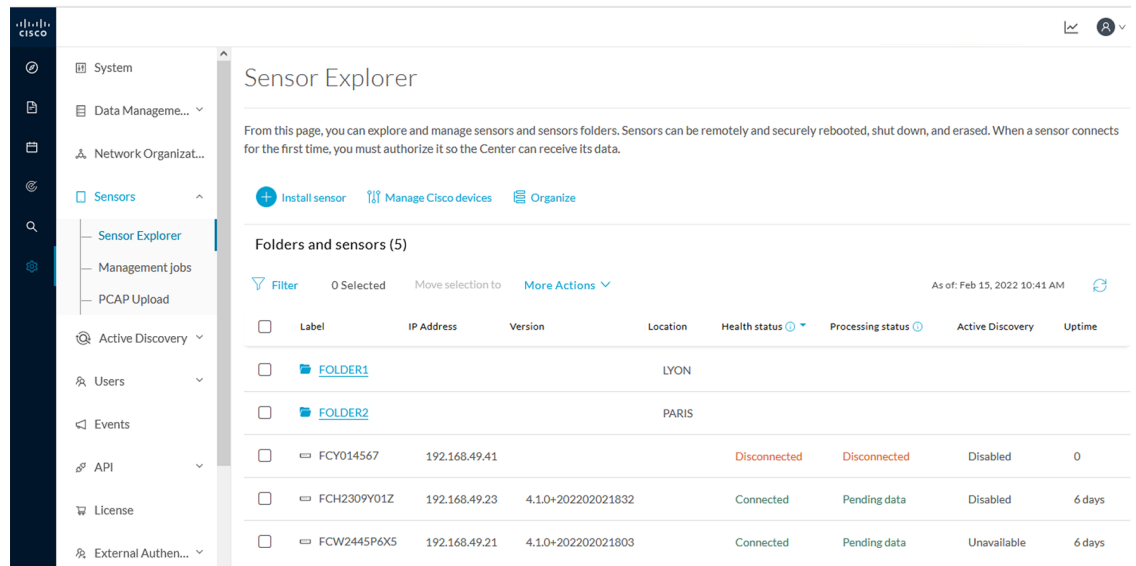
To define a subnetwork, you must click the Add a network button and give it a name, an IP address range, and a network type such as OT internal, IT internal or external.



# Sensors

## Sensor Explorer

The Sensor Explorer page allows you to install, manage, and obtain information about the sensors monitoring your industrial network.



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

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

*The folders and sensors list without filtering:*

Folders and sensors (5)

<input type="checkbox"/>	Filter	0 Selected	Move selection to	More Actions	As o	
<input type="checkbox"/>	Label	IP Address	Version	Location	Health status	Processing status
<input type="checkbox"/>	FOLDER1			Lyon		
<input type="checkbox"/>	FOLDER2			Paris		
<input type="checkbox"/>	FCH2309Y01Z	192.168.49.23	4.1.0+202202151504		Connected	Pending data
<input type="checkbox"/>	FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Connected	Normally processing
<input type="checkbox"/>	FCY014567	192.168.49.41			Disconnected	Disconnected

Type in the field or select from the drop down menu to reach the folder(s) or sensor(s) and click the Apply button:



Folders and sensors (5)

Filter 0 Selected Move selection to More Actions

Label	IP Address	Version	Location	Health status	Processing status
FCH			Lyon		
			Paris		
		.1.0+202202151504		Connected	Pending data
		.1.0+202202151440		Connected	Pending data
				Disconnected	Disconnected

Filter dialog box:

- Label: FCH
- IP Address: \_\_\_\_\_
- Version: \_\_\_\_\_
- Location: \_\_\_\_\_
- Health status: \_\_\_\_\_

Buttons: Cancel, Apply

The folders and sensors list after filtering by label:

Folders and sensors (1)

Filter 0 Selected Move selection to More Actions

Label is FCH

Label	IP Address	Version	Location	Health status	Processing status
FCH2309Y01Z	192.168.49.23	4.1.0+202202151504		Connected	Pending data

**Sorting**

Sort icons allow you to sort sensors by label, IP address, version, location, health and processing status by alphabetical or by ascending/descending order. Sort icons appear when applied or as you hover over them.

Folders and sensors (5)

Filter 0 Selected Move selection to More Actions

<input type="checkbox"/>	Label	IP Address	Version	Location	Health status	Processing status
<input type="checkbox"/>	FOLDER2			Paris		
<input type="checkbox"/>	FOLDER1			Lyon		
<input type="checkbox"/>	FCY014567	192.168.49.41			Disconnected	Disconnected
<input type="checkbox"/>	FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Connected	Pending data
<input type="checkbox"/>	FCH2309Y01Z	192.168.49.23	4.1.0+202202151504		Connected	Pending data

Sensors status

There are two types of sensor status:

- The health status, which indicates at which step of the enrollment process the sensor is.
- The processing status, which indicates the network connection state between the sensor and the Center.

<input type="checkbox"/>	Label	IP Address	Version	Location	Health status	Processing status	Active Discovery	Uptime
<input type="checkbox"/>	FCY014567	192.168.49.41			Disconnected	Disconnected	Disabled	N/A
<input type="checkbox"/>	FCH2309Y01Z	192.168.49.23	4.1.0+202202151504		Connected	Pending data	Enabled	3 days
<input type="checkbox"/>	FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Connected	Pending data	Enabled	6 hours

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**

You will find in the Sensor Explorer page several features to manage and use your sensors. Some buttons are accessible from the Sensor Explorer page itself to manage one or more sensors. Other buttons are available when clicking a sensor in the list. A right side panel opens with additional sensor information and actions that are available or not depending on the sensor model, mode (online or offline) and the installation type performed.

FCH2309Y01Z
✕

Label: FCH2309Y01Z ✎

Serial Number: FCH2309Y01Z

IP address: 192.168.49.23

Version: 4.1.0+202202151504

System date: Feb 16, 2022 10:07:45 AM

Deployment: Sensor Management Extension

Active Discovery: Disabled

Capture mode: All

**System Health**

Status: Connected

Processing status: Pending data

Uptime: 7 minutes

[Go to statistics](#)

[Start Recording](#)

Last recording: Feb 10, 2022 3:36:54 PM

[Download \(49 bytes\)](#)

[Move to](#)

<a href="#">Download package</a>	<a href="#">Capture mode</a>
<a href="#">Redeploy</a>	<a href="#">Enable IDS</a>
<a href="#">Reboot</a>	<a href="#">Shutdown</a>
<a href="#">Uninstall</a>	

- The **Start recording** button records a traffic capture on the sensor. Records can be used for traffic analysis and may be requested by Cisco 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 121](#).
- The **Download package** button provides a configuration file to be deployed on the sensor when installing the sensor manually (online mode). Only applicable to the Cisco IC3000. Refer to its Installation Guide.
- The **Capture Mode** button can be used to set a filter on a sensor sending data to the Center. Refer to the procedure for [Set a capture mode](#).
- The **Redeploy** button can be used to partly reconfigure the sensor, for example to change its parameters such as its IP address.

- The **Enable IDS** button can be used to enable the SNORT engine embedded in some sensors to analyze traffic by using SNORT rules. SNORT rules management is available on the SNORT administration page.
- The **Reboot** button can be used to reboot the sensor in case of a malfunction.
- The **Shutdown** button triggers a clean shutdown of the sensor from the GUI.



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

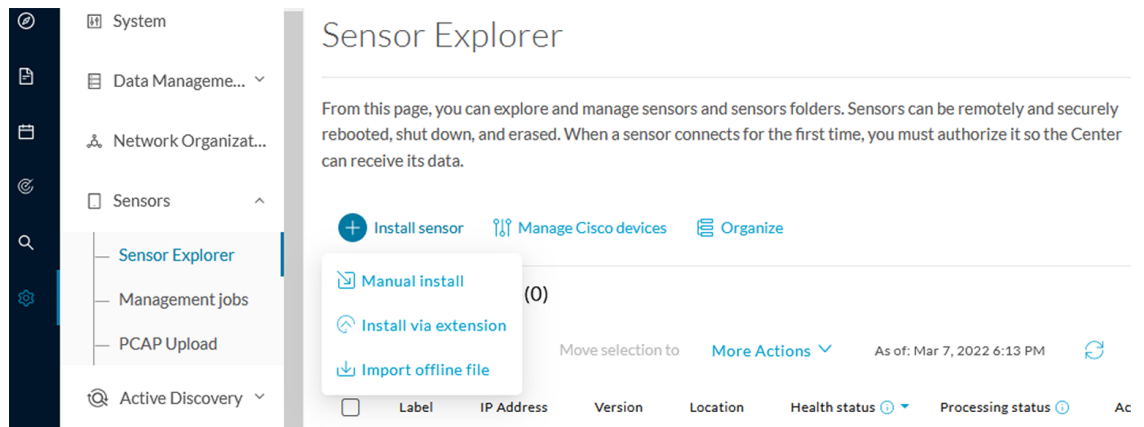
- The **Uninstall** button can be used to remove an uninstalled sensor from the list or to fully uninstall a sensor. Diverse options are available according to the sensor model or deployment mode. In the case of a sensor deployed through the management extension, the IOx app can be removed from the device,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

### Install sensor

From the Sensor Explorer page, you can:

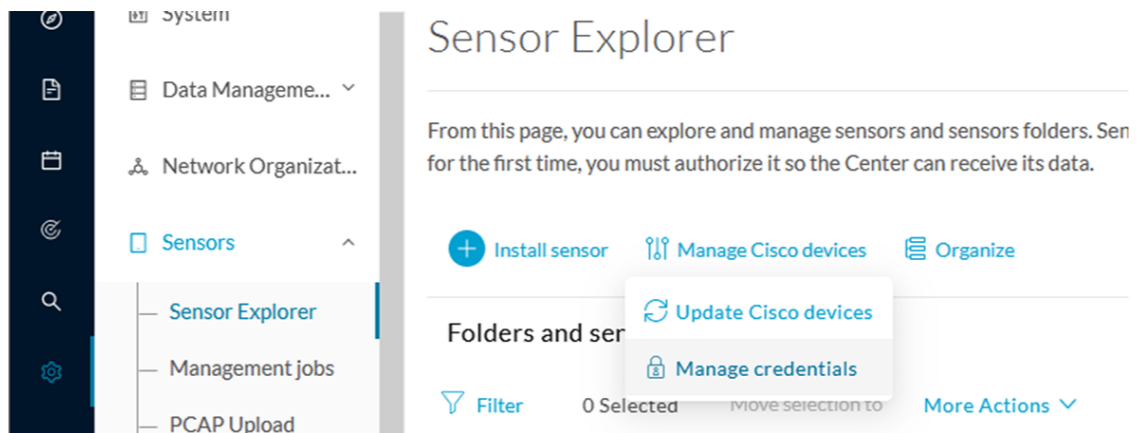
- Install a sensor manually.
- Install a sensor via the IOx extension. To use the Install via extension button you must first install the sensor management extension via the [Extensions](#) page.
- Capture traffic with an offline sensor (only applicable to Cisco IC3000).

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



### Manage credentials

The Manage credentials button, which you can have access by clicking Manage Cisco devices in the Sensor Explorer page, is 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, enter the login and password and click Save.

SET GLOBAL CREDENTIALS
×

You can define "global credentials" which can be used as default credentials when deploying a new Cisco device. When you update these "global credentials" it affects both new and deployed sensors.

Login \*

Password \*

Save
Cancel

Once the global credentials are registered, the feature will be enabled in the Install via extension procedure. Select the Use global credentials option to use your global credentials.

Install via extension

### Reach Cisco device

Please fill the fields below to enable Cisco Cyber Vision to reach your device.

IP address\*  Port\*

For example 443 or 8443

Center collection IP

leave blank to use current collection IP

Credentials

Use global credentials

Capture mode

- Optimal (default): analyze the most relevant flows

## Organize sensors

You can create folders and move your sensors into the folders for more clarity. Folders can correspond to a location, a person in charge, a set of disconnected sensors, etc.

To create a folder and move a sensor in it:

1. Click the Organize button and click Create folder.

The screenshot shows the 'Sensor Explorer' page in the Cisco Cyber Vision GUI. On the left, a dark sidebar contains a menu with 'Sensors' expanded to show 'Sensor Explorer', 'Management jobs', and 'PCAP Upload'. The main content area has a title 'Sensor Explorer' and a sub-header 'Folders and sensors (4)'. Below this, there are buttons for 'Install sensor', 'Manage Cisco devices', and 'Organize'. The 'Organize' button is highlighted with a red box, and a sub-menu is open showing a '+ Create folder' button, also highlighted with a red box. Below the buttons, there is a table with columns 'Label', 'IP Address', and 'Version'. One row is visible with a folder icon and the label 'FOLDER1'.

2. Write a folder name, and, if needed, a location and a description.

The new folder is displayed in the sensor list.

Folders and sensors (5)

Filter 0 Selected Move selection to More Actions As...

<input type="checkbox"/>	Label	IP Address	Version	Location	Health status	Processing status
<input type="checkbox"/>	<a href="#">FOLDER1</a>			Lyon		
<input type="checkbox"/>	<a href="#">FOLDER2</a>			Paris		
<input type="checkbox"/>	FCY014567	192.168.49.41			Disconnected	Disconnected
<input type="checkbox"/>	FCH2309Y01Z	192.168.49.23	4.1.0+202202151504		Connected	Pending data
<input type="checkbox"/>	FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Connected	Normally processing

3. Select a sensor in the list and click the button Move selection to.

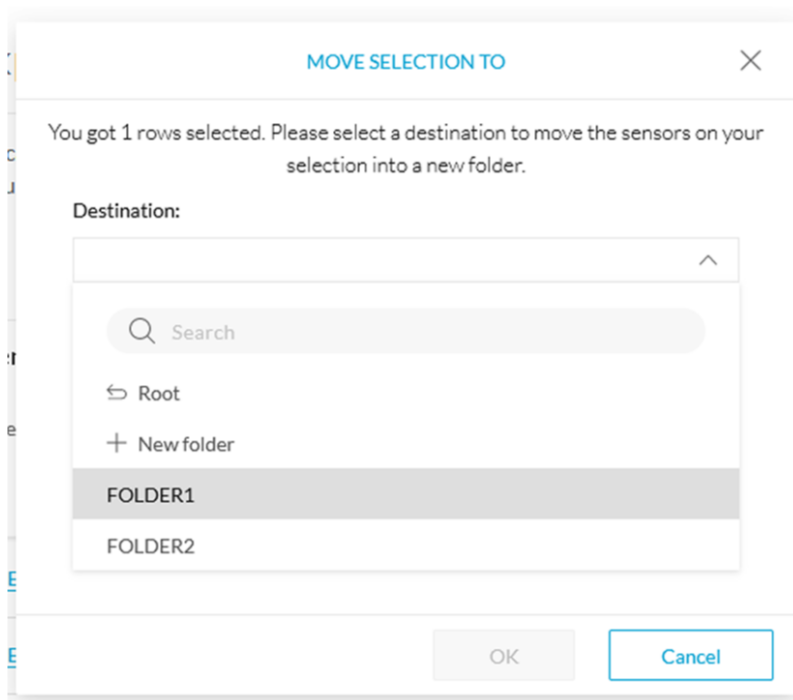


Folders and sensors (5)

Filter 1 Selected **Move selection to** More Actions ▾ As

<input type="checkbox"/>	Label	IP Address	Version	Location	Health status ⓘ ▾	Processing status ⓘ
<input type="checkbox"/>	<a href="#">FOLDER1</a>			Lyon		
<input type="checkbox"/>	<a href="#">FOLDER2</a>			Paris		
<input type="checkbox"/>	FCY014567	192.168.49.41			Disconnected	Disconnected
<input checked="" type="checkbox"/>	FCH2309Y01Z	192.168.49.23	4.1.0+202202151504		Connected	Pending data
<input type="checkbox"/>	FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Connected	Normally processing

- Select the folder you want to place the sensor in or create a new folder. Root can be used to move sensors back into the primary list.



The sensor is moved into the folder. The sensor version, health status and processing status are displayed in the folder line.

Folders and sensors (4)

Filter 0 Selected Move selection to More Actions

<input type="checkbox"/>	Label	IP Address	Version	Location	Health status	Processing status
<input type="checkbox"/>	<b>FOLDER1</b>		4.1.0+202202151504	Lyon	Connected	Pending data
<input type="checkbox"/>	<b>FOLDER2</b>			Paris		
<input type="checkbox"/>	FCY014567	192.168.49.41			Disconnected	Disconnected
<input type="checkbox"/>	FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Connected	Pending data

If you move a sensor in a disconnected state inside this same folder, then its information will be displayed in the folder line rather than the sensor in connected state. Less secure sensor status are showcased in priority to drag your attention.

Folders and sensors (3)

Filter 0 Selected Move selection to More Actions

<input type="checkbox"/>	Label	IP Address	Version	Location	Health status	Processing status
<input type="checkbox"/>	<b>FOLDER1</b>		- 4.1.0	Lyon	Disconnected	Disconnected
<input type="checkbox"/>	<b>FOLDER2</b>			Paris		
<input type="checkbox"/>	FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Connected	Pending data

The sensors inside a folder:

FOLDER1

📍 Lyon

[✎ Edit](#) [🗑 Delete](#)

Folders and sensors (2)

Filter 0 Selected Move selection to More Actions

<input type="checkbox"/>	Label	IP Address	Version	Health status	Processing status
<input type="checkbox"/>	FCY014567	192.168.49.41		Disconnected	Disconnected
<input type="checkbox"/>	FCH2309Y01Z	192.168.49.23	4.1.0+202202151504	Connected	Pending data

### Set a capture mode

The Capture mode feature lets you choose which network communications will be analyzed by the sensors. You can set it by clicking an online sensor in the sensors list of the Sensor Explorer page or during a sensor installation.

*Setting the capture mode on a sensor from the right side panel:*

The screenshot shows the 'Sensor Explorer' interface. On the left, there's a table titled 'Folders and sensors (5)'. The table has columns for Label, IP Address, Version, Location, and Health status. One sensor, 'FCH2309Y01Z', is highlighted. On the right, a detailed view of this sensor is shown, including its label, serial number, IP address, version, system date, deployment type, and active discovery status. At the bottom of this panel, there are several action buttons: 'Move to', 'Download package', 'Capture mode' (which is highlighted with a red box), 'Redeploy', 'Enable IDS', 'Reboot', 'Shutdown', 'Uninstall', and 'Active Discovery'.

*Capture modes:*

The screenshot shows a dialog box titled 'CAPTURE MODE'. It contains the text 'Please select an option to filter the flows analyzed by this sensor.' Below this, there are four radio button options under the heading 'Capture mode:':
 

- Optimal (default): analyze the most relevant flows
- All: analyze all the flows
- Industrial only: analyze industrial flows
- Custom: you set your filter using a packet filter in tcpdump-compatible syntax

 At the bottom of the dialog, there are two buttons: 'OK' and 'Cancel'.

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.

Using Capture mode Cisco Cyber Vision performance can be improved on large networks.

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

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



---

**Note** You can set a capture mode to offline sensors from a file containing the filter and registered on the USB drive. This will be then plugged on the Offline USB port of the device. For more information about setting a capture mode on an offline sensor contact the support.

---

The different capture modes are:

- **ALL:** No filter is applied. The sensor analyzes all incoming flows and they will all be stored inside the Center database.
- **OPTIMAL (Default):** The applied filter selects the most relevant flows according to Cisco expertise. Multicast flows are not recorded. This capture mode is recommended for long term capture and monitoring.
- **INDUSTRIAL ONLY:** The filter selects industrial protocols only like modbus, S7, EtherNet/IP, etc. This means that IT flows of the monitored network won't be analyzed by the sensor and won't appear in the GUI.
- **CUSTOM (advanced users):** Use this capture mode if you want to fully customize the filter to be applied. To do so you will need to use the tcpdump syntax to define the filtering rules.

## Management jobs

As some deployment tasks on sensors can take several minutes, this page shows the jobs execution status and advancement for each sensor deployed with the sensor management extension.

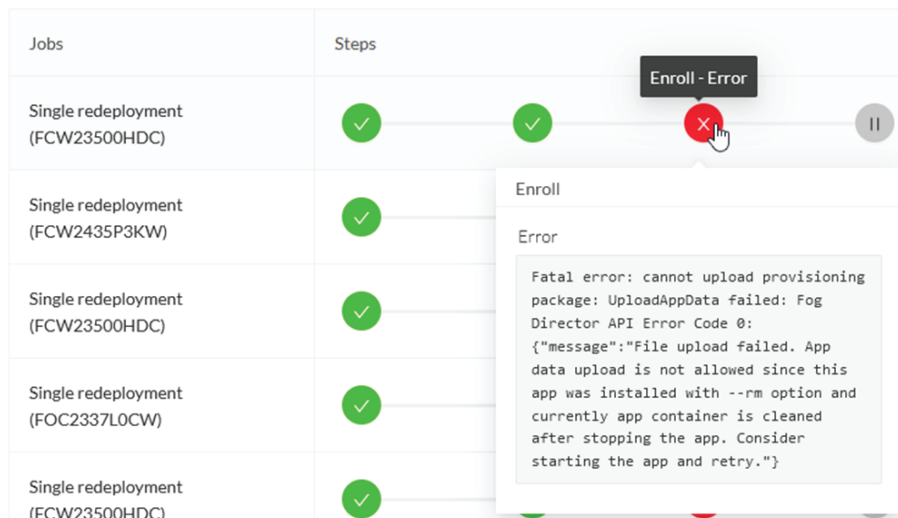
This page is only visible when the sensor management extension is installed in Cisco Cyber Vision.

Jobs	Steps	Duration
Single redeployment (FCW2435P3KW)	✓ — ✓ — ✓ — ✓	1m 11s
Single redeployment (FCW23500HDC)	✓ — ✓ — ✗ —	41s
Single redeployment (FOC2337LOCW)	✓ — ✓ — ✓ — ✓	1m 33s
Single redeployment (FCW23500HDC)	✓ — ✓ — ✗ —	35s
Single redeployment (FCW23500HDC)	✓ — ✓ — ✗ —	39s
Single redeployment (FCW23500HDC)	✓ — ✓ — ✗ —	43s
Single redeployment (FOC2334V045)	✓ — ✓ — ✓ — ✓	6m 52s

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.

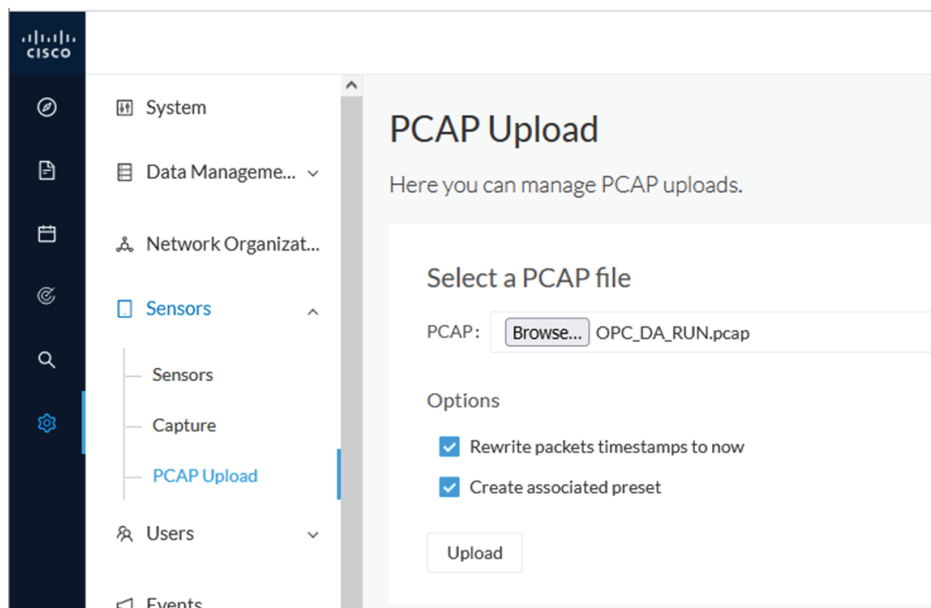


## PCAP Upload







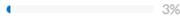





This page allows you to upload pcaps to view their data in Cisco Cyber Vision.

When selecting a pcap, two options are available:

- You can choose to use the timestamp of the pcap or the current timestamp instead. Choosing the current timestamp can be useful if the pcap timestamp is old and searching for its data in Cisco Cyber Vision is thus easier.
- You can define a preset from the pcap. Once the pcap is uploaded you'll just have to click the pcap link to be redirected to its preset.



Note that during the upload that the status for the DPI and Snort are displayed.

Name	Size	Upload status	Processing status	Packets first timestamp
<a href="#">OPC_DA_RUN.pcap</a>	7.3 MB	 ✓	DPI:  Snort: 	Jul 5, 2021 5:42:20 PM
<a href="#">smb_putty_xfer.pcap</a>	726.5 kB	 ✓	DPI:  Snort: 	Jun 30, 2021 4:23:24 PM
MergedFile.pcapng	815 MB	 3%	DPI:  Snort: 	
<a href="#">DAN_Rockwell_With_Variables.pcap</a>	1.5 MB	 ✓	DPI:  Snort: 	Jun 30, 2021 11:28:37 AM

If uploading a large file, you have the possibility to pause it. To relaunch the upload, you just need to select the same pcap again with the browse button and click Resume.



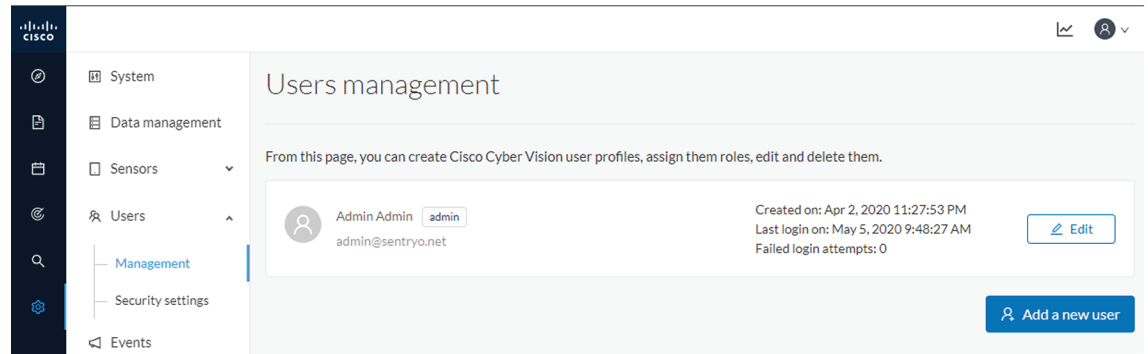
**Note**

pcap data cannot be erased individually from Cisco Cyber Vision. You will need to use the [Clear data](#) button and it will affect the whole database. Upload pcaps with caution.

## Users

### Management

You can create, edit and delete users through the users administration page.



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 Cisco Cyber Vision 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 Cisco Cyber Vision 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.

CREATE A NEW USER ×

Firstname <sup>\*</sup> :

Lastname <sup>\*</sup> :

Email <sup>\*</sup> :

Password <sup>\*</sup> :

Great ⓘ

Suggested password:  
 AwsLWumTPjpv4FrNGB : [9]

📄
🔄

Confirm password <sup>\*</sup> :

Role <sup>\*</sup> :

Auditor
▼

[🔍 Learn more about users roles >](#)

Admin: has access to the Admin page and can set users roles. ×

Product: has access to the sensor panel and the events panel in the Admin page

Operator: has access to the Monitor mode and can edit groups and acknowledge vulnerabilities.

Auditor: has access to the Map and Events pages.

OK
Cancel

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: ~!#\$%&'()\*+,-./:;<=>?@[^\_{}.



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

Passwords' lifetime is defined in the [Security settings](#).

You can create custom user roles in the [Role Management](#).

You can map Cisco Cyber Vision user roles with an external directory's user groups in the [LDAP](#).

## 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.

Administrative Rights		read	write		read	write
Active Discovery	<input type="checkbox"/>	<input checked="" type="checkbox"/>	API	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Center Certificate	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Data Management	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Events	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Events Settings	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Explore	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Extensions	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
External Authentication	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Integrations	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
License	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Monitor	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Network Organization	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Reports	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Risk Score	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Secure X	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Security Settings	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Sensors	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
SNMP	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Snort	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
System	<input type="checkbox"/>	<input checked="" type="checkbox"/>	User Admin	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Vulnerability Management	<input type="checkbox"/>	<input checked="" type="checkbox"/>				

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](#).

## Create roles

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

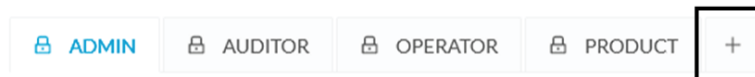
### Procedure

**Step 1** In Cisco Cyber Vision, navigate to Admin > Users > Role Management.

**Step 2** Click the + button next to default user roles.

## Role management

From this page, you can create Cisco Cyber Vision user roles, edit and delete them.

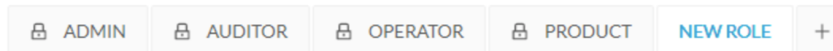


A new role tab appears.

**Step 3** Type a role name and a description.

## Role management

From this page, you can create Cisco Cyber Vision user roles, edit and delete them.



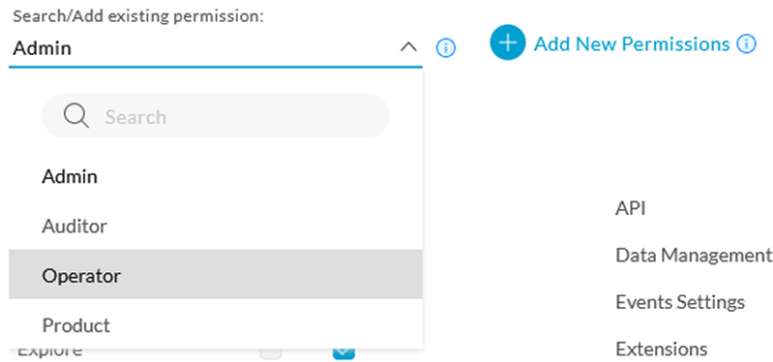
Role Name \*

Role Description \*

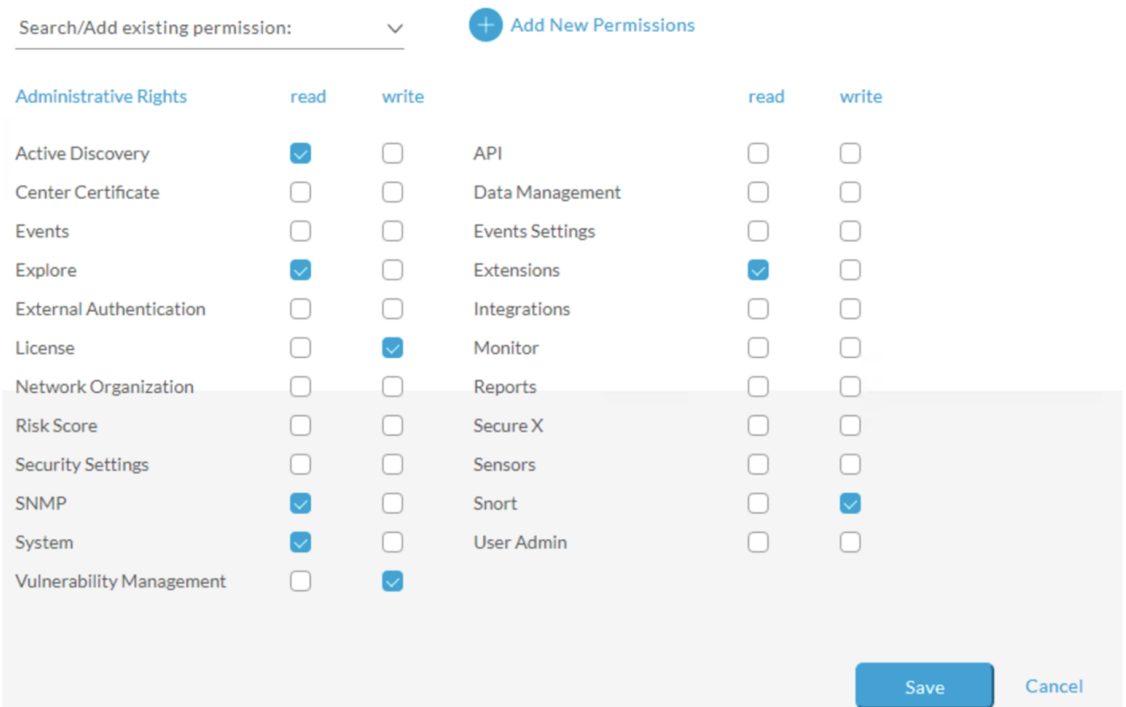
Search/Add existing permission:

[+ Add New Permissions](#)

**Step 4** Select an existing role from the Search/Add existing permissions drop down menu, or click the Add New Permissions button to build the new user role from scratch.



**Step 5** Select/unselect permissions from the list as read or write



**Step 6** Click save.

A message saying that the user role has been created successfully appears.

The new user role is displayed in the tab list.

TESTAD2019  ADMIN  AUDITOR  OPERATOR  PRODUCT  +

TestAD2019  

TestAD2019 

Administrative Rights ⓘ	read	write		read	write
Active Discovery	<input checked="" type="checkbox"/>	<input type="checkbox"/>	API	<input type="checkbox"/>	<input type="checkbox"/>
Center Certificate	<input type="checkbox"/>	<input type="checkbox"/>	Data Management	<input type="checkbox"/>	<input type="checkbox"/>
Events	<input type="checkbox"/>	<input type="checkbox"/>	Events Settings	<input type="checkbox"/>	<input type="checkbox"/>
Explore	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Extensions	<input checked="" type="checkbox"/>	<input type="checkbox"/>
External Authentication	<input type="checkbox"/>	<input type="checkbox"/>	Integrations	<input type="checkbox"/>	<input type="checkbox"/>
License	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Monitor	<input type="checkbox"/>	<input type="checkbox"/>
Network Organization	<input type="checkbox"/>	<input type="checkbox"/>	Reports	<input type="checkbox"/>	<input type="checkbox"/>
Risk Score	<input type="checkbox"/>	<input type="checkbox"/>	Secure X	<input type="checkbox"/>	<input type="checkbox"/>
Security Settings	<input type="checkbox"/>	<input type="checkbox"/>	Sensors	<input type="checkbox"/>	<input type="checkbox"/>
SNMP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Snort	<input type="checkbox"/>	<input checked="" type="checkbox"/>
System	<input checked="" type="checkbox"/>	<input type="checkbox"/>	User Admin	<input type="checkbox"/>	<input type="checkbox"/>
Vulnerability Management	<input type="checkbox"/>	<input checked="" type="checkbox"/>			

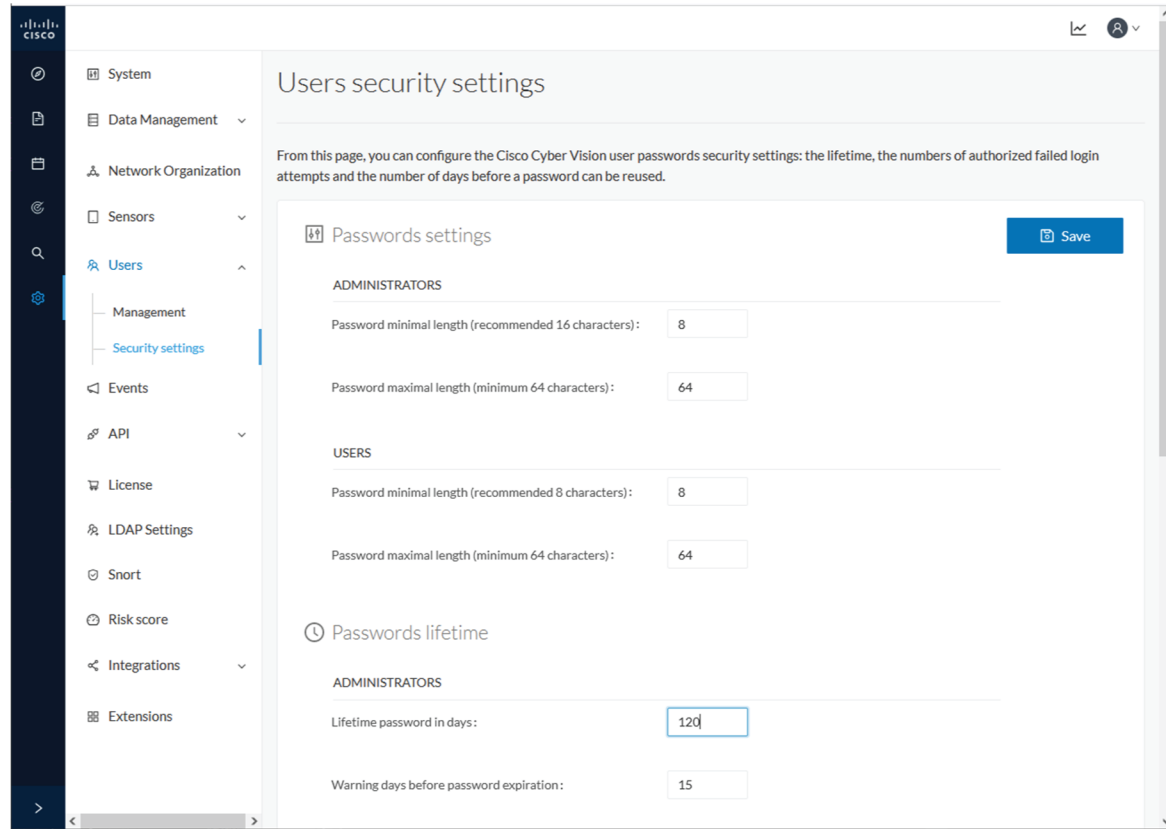
You can modify or delete directly in the tab.

**What to do next**

Custom roles created can be mapped with an external directory's user groups in the [LDAP](#).

**Security settings**

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



## Events

The severity of [Events](#) can be customized on the events administration page. By default, changes will be applied to future events only. However, you can apply new customized severities to past events by enabling [Apply severity to existing events](#).

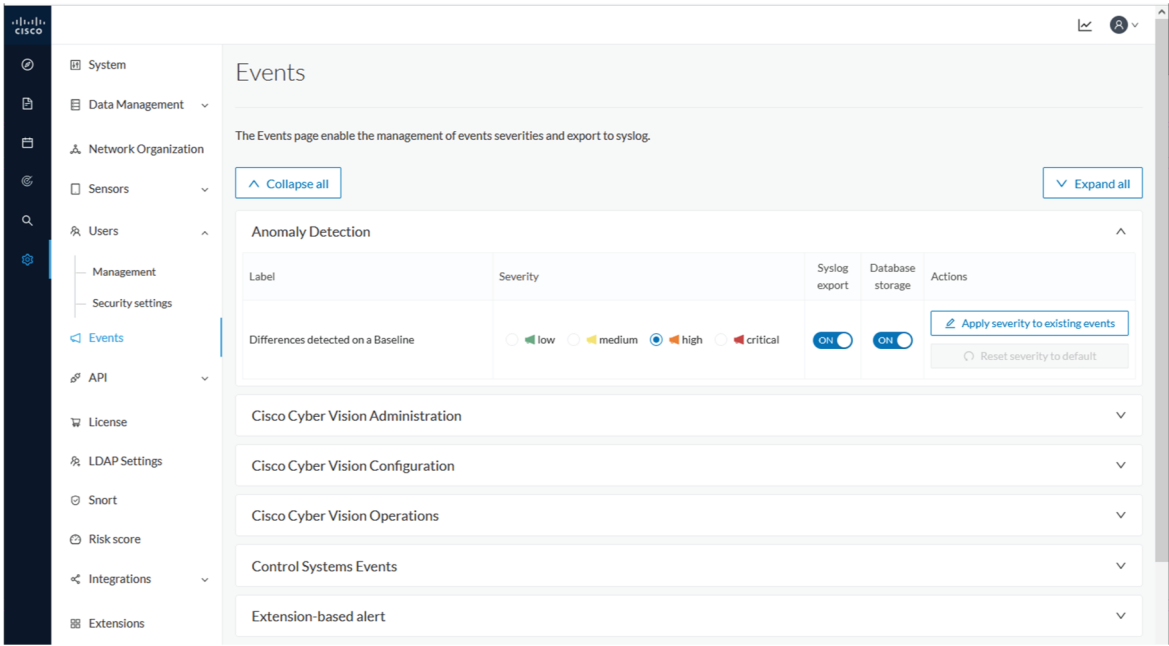


**Important**

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

You can reset the severity to default.

You can enable or disable the export of events to syslog and database storage. These two options are active by default. However, make sure [Syslog configuration](#) before the export.



# API

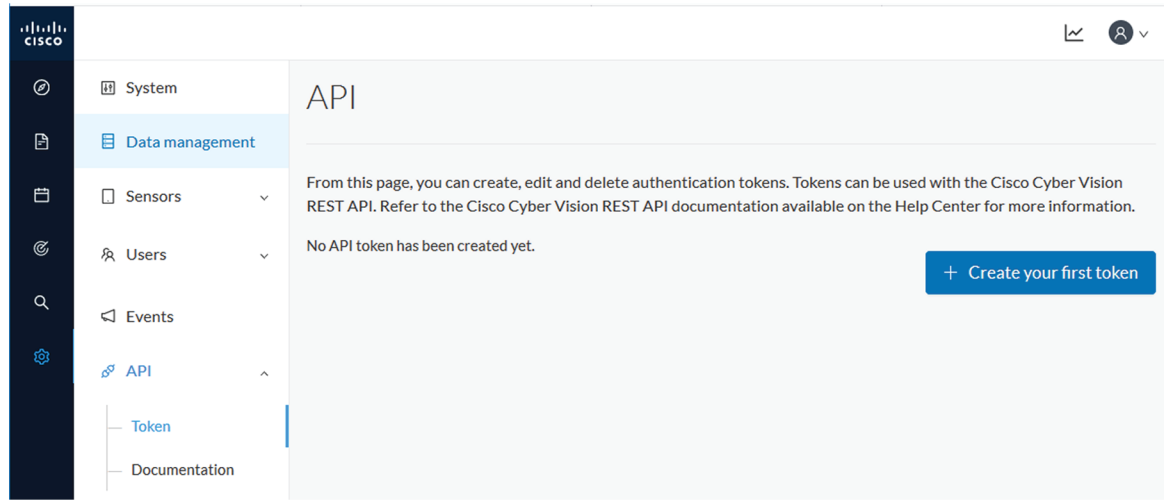
## Token

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

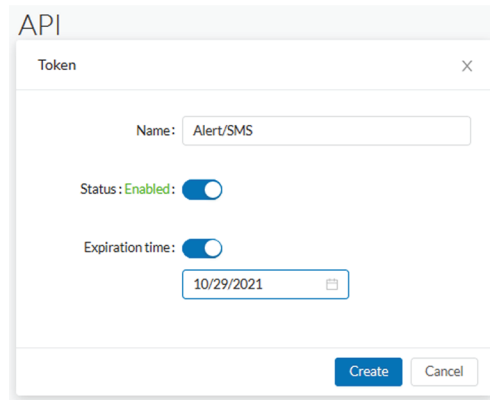
A token is a random password which authenticates a request to Cisco Cyber Vision to access or even modify the data in the Center through the REST API. For instance, you can request the latest 10 components detected on Cisco Cyber Vision or create new references. Requests can be used by external applications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



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



Create your first token and enter a name that will help you identifying the token. For security reasons you can also use the status toggle button to disable authorization to use the token (for example, if the token created is to be used later and you want to prevent access until then) and set an expiration time.



Once the token is created click show to see and copy the token to the clipboard.

Name	Token	Status	Creation Date	Expiration Date	Actions
Alert/SMS	ics-806ad94c9d70d05a0483f2eb1edc842488f53bc4-4390bf0c8b56670ce142913a458380e18ec12abf <a href="#">Hide</a>	Enabled	Oct 29, 2020	Oct 29, 2021	<a href="#">Edit</a> <a href="#">Refresh</a> <a href="#">Delete</a>
Analyzer API	Hidden <a href="#">Show</a>	Enabled	Oct 29, 2020	None	<a href="#">Edit</a> <a href="#">Refresh</a> <a href="#">Delete</a>
IoC	Hidden <a href="#">Show</a>	Disabled	Oct 29, 2020	None	<a href="#">Edit</a> <a href="#">Refresh</a> <a href="#">Delete</a>

[+ New token](#)

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

## 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 Cisco Cyber Vision's elements type (activities, baselines, components, flows, groups, etc.).

*The category "Groups" containing all possible group routes:*

**Groups** Groups are a logical way to organize components. ▼

<b>GET</b>	/ <b>groups</b> List groups.	🔒
<b>POST</b>	/ <b>groups</b> Create a group.	🔒
<b>GET</b>	/ <b>groups/{id}</b> Get details of one or many groups.	🔒
<b>PUT</b>	/ <b>groups/{id}</b> Update a group.	🔒
<b>DELETE</b>	/ <b>groups/{id}</b> Delete a group.	🔒
<b>PATCH</b>	/ <b>groups/{id}</b> Update one property of the given group. For the moment, add and remove on components are implemented.	🔒

To authorize API communications:

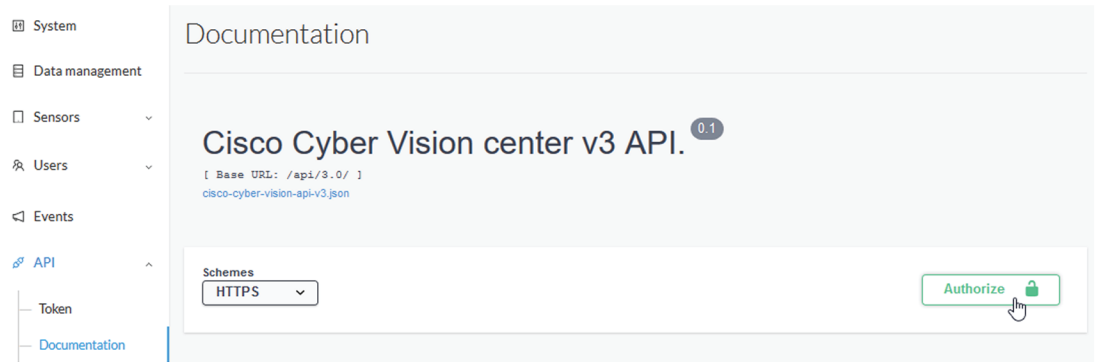
### Procedure

#### Step 1

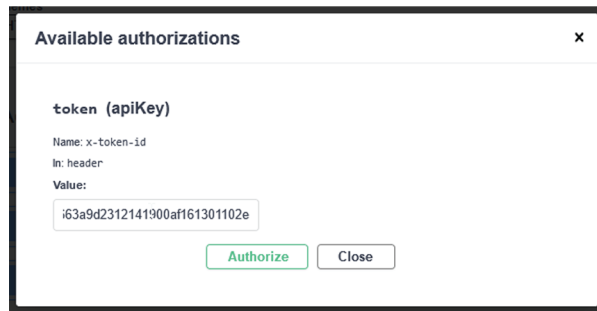
Access the API Token menu to create and/or copy a [Token](#).

Access the API Documentation page and click the Authorize button.

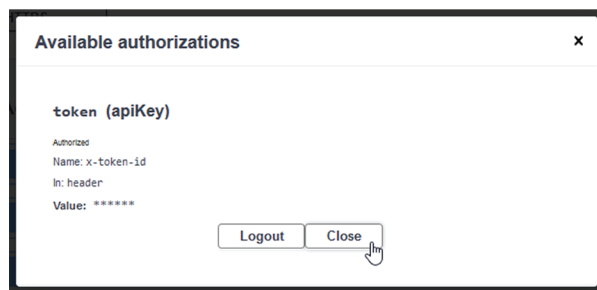




- Step 2** Paste the token.
- Step 3** Click Authorize.



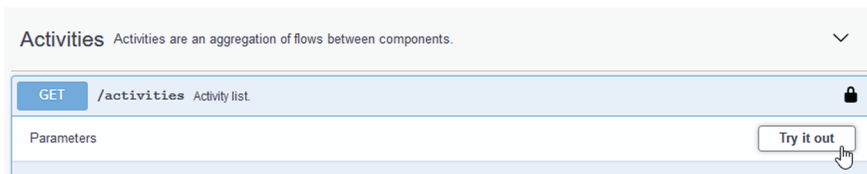
- Step 4** Click Close.



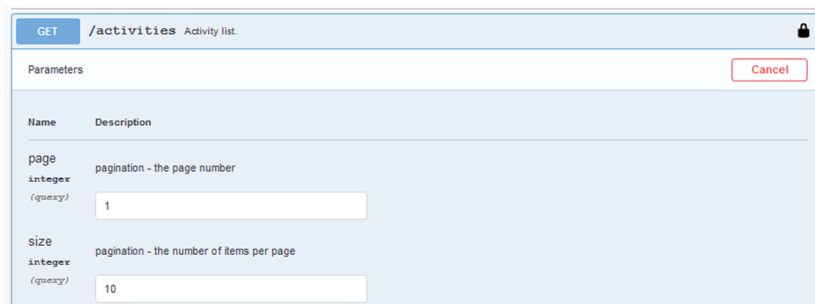
Closed lockers displays. They indicate that routes are secured and authorization to use them is up.

To use a route:

- Step 5** Click a route to deploy it. In the example, we choose Get activity list.
- Step 6** Click Try it out.



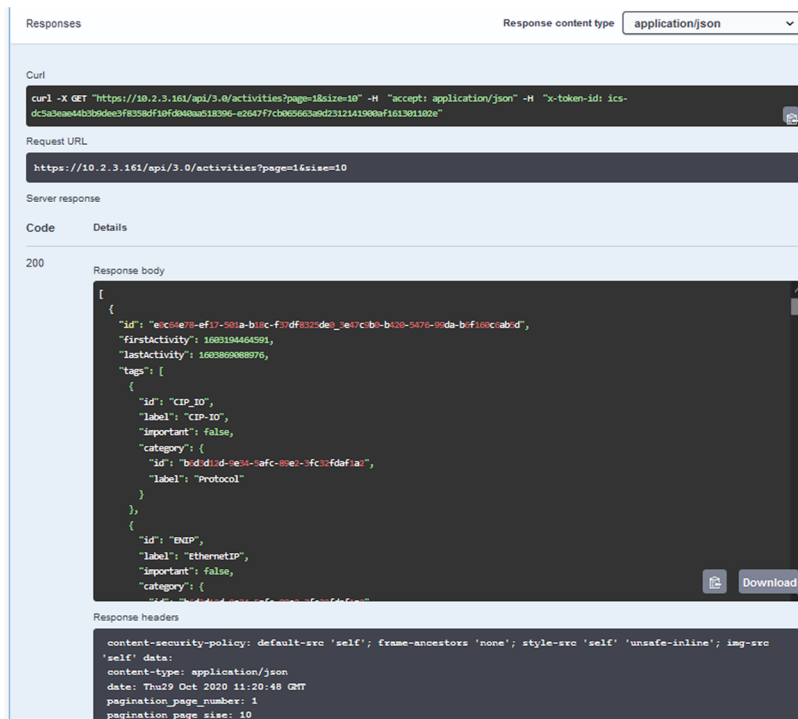
**Step 7** You can set some parameters. In the example, we set page to 1 and size to 10.



**Step 8** Click Execute.

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

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

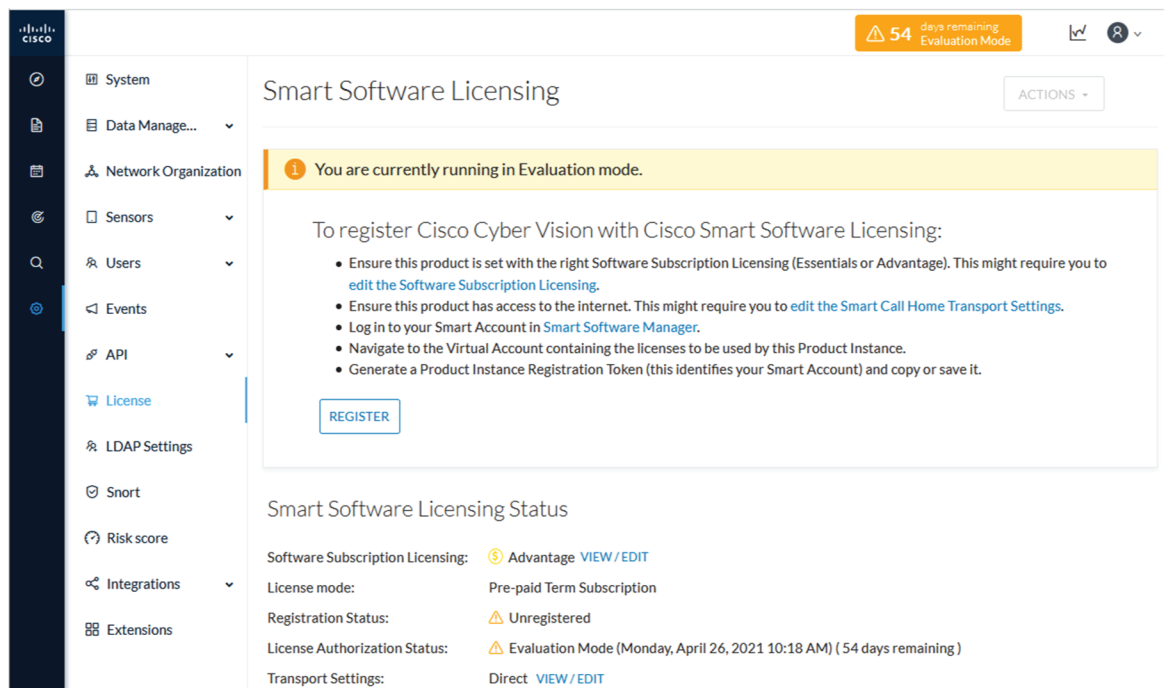


- Step 9** When you're finished, click the Authorize button.
- Step 10** Logout to clean the token variable, and click Close.

## License

You can install a license in Cisco Cyber Vision in the License administration panel.

Licensing is based on device count. For device count to be more accurate, it is advised to setup the subnetworks of the monitored industrial network through the [Network organization](#). By doing so, you will declare which subnetworks are internal, and which are external. Devices from external subnetworks will be excluded from the license count and related costs would be reduced.



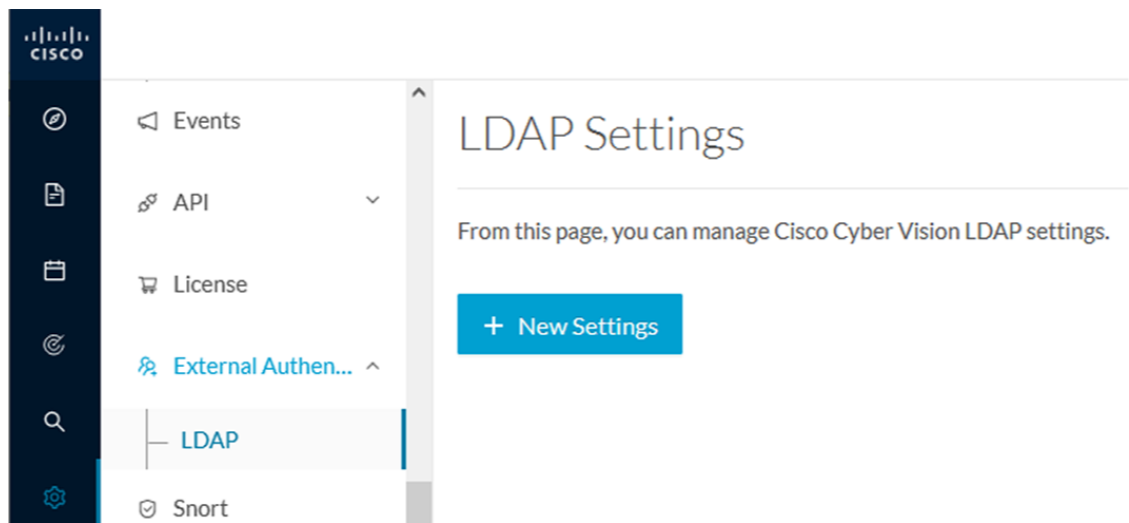
For more information about how to install a license, refer to the Cisco Cyber Vision Smart Licensing User Guide.

## External Authentication

### LDAP

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

You can enable LDAP authentication in the LDAP Settings administration page.



### Configuring LDAP:

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

### Mapping Cisco Cyber Vision roles with Microsoft Active Directory groups:

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

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

### Testing LDAP connection:

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

### Login in Cisco Cyber Vision:

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

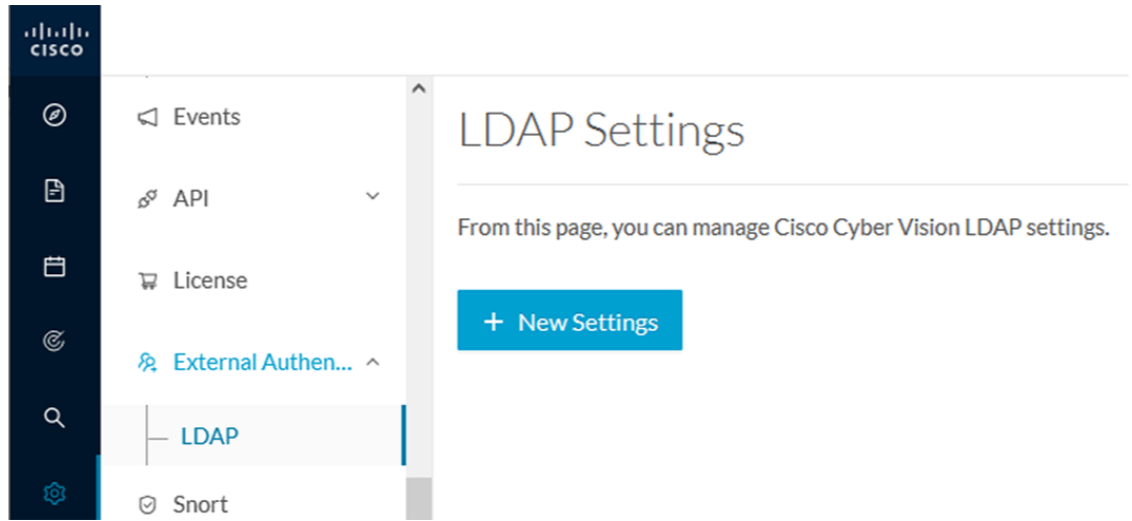
- If you use an email, the Cisco Cyber Vision database is queried.
- If you use the Active Directory format <domain\_name>\<user\_name> (e.g. cisco\john\_doe), then the external directory is used to authenticate users.

## Configure LDAP

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

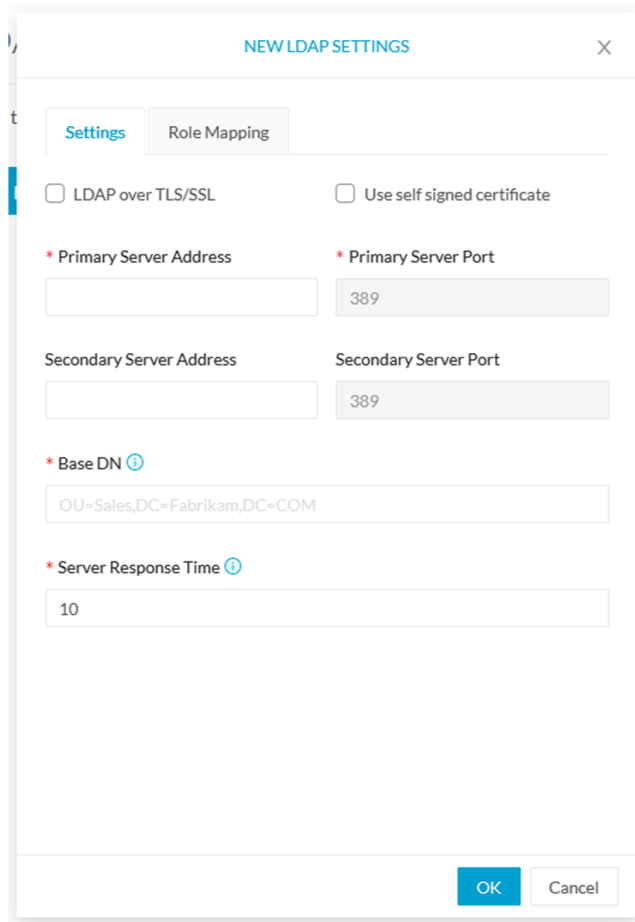
### Procedure

- 
- Step 1** In Cisco Cyber Vision, navigate to Admin > External Authentication > LDAP.



**Step 2** Click New Settings.

The New LDAP Settings window pops up.



**What to do next**

Configure LDAP using a [LDAP normal connection](#) or a [LDAP secure connection](#).

*LDAP normal connection*

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

**Before you begin**

**Procedure**

**Step 1** Fill in the LDAP settings.

The screenshot shows a dialog box titled "NEW LDAP SETTINGS" with a close button (X) in the top right corner. It has two tabs: "Settings" (active) and "Role Mapping". Under the "Settings" tab, there are several configuration options:

- Two checkboxes: "LDAP over TLS/SSL" and "Use self signed certificate", both of which are unchecked.
- Two rows of fields for server information:
  - Primary Server Address: dc01.2019lab.local
  - Primary Server Port: 389
  - Secondary Server Address: dc01.2019lab.local
  - Secondary Server Port: 389
- Base DN: DC=2019lab,DC=local
- Server Response Time: 10

At the bottom of the dialog, there are "OK" and "Cancel" buttons.

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

**Step 3** Fill in the following fields:

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

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

**Note** 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.

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

You must type the exact group names as configured into the remote directory so they can be retrieved and mapped to user roles.

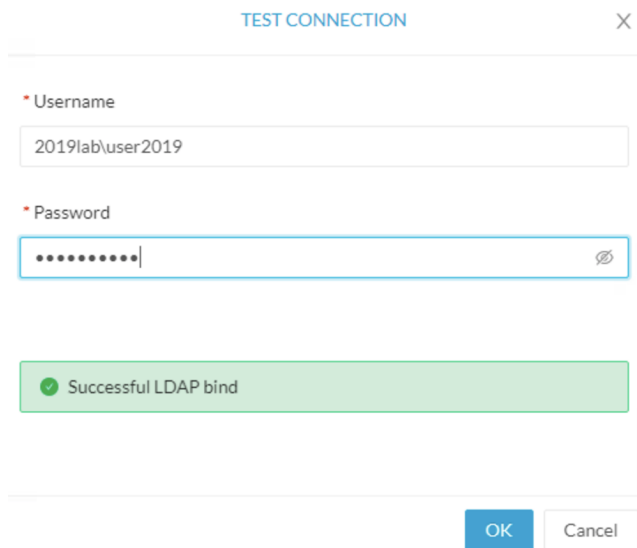
The screenshot shows a dialog box titled "NEW LDAP SETTINGS" with a close button (X) in the top right. It has two tabs: "Settings" and "Role Mapping" (which is active). Under "Default roles", there are three rows: "Product" mapped to "Domain Users", "Operator" with an empty text box, and "Auditor" with an empty text box. Below this is a "+" icon. Under "Custom roles", there is one row: "TestAD2019" mapped to "TestAD2019", with a red trash icon to its right. At the bottom of the dialog are "OK" and "Cancel" buttons.

**Step 4** Click OK.

**Step 5** Click the Test connection button.



The Test Connection window pops up.



**Step 6** Enter a user credentials to test the connection between Cisco Cyber Vision and Active Directory.

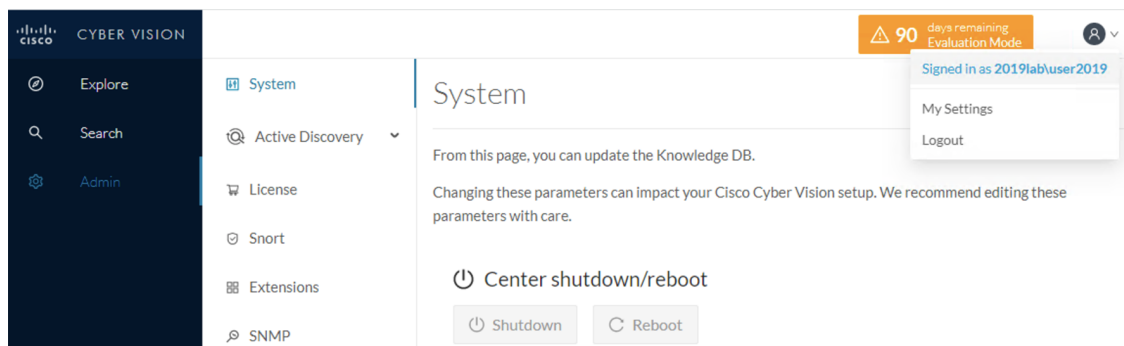
**Note** The Username format is domain\user.

A message Successful LDPA bind should appear.

**Step 7** Click OK.

**Step 8** Test the connection by logging out of Cisco Cyber Vision and logging in with the mapped user credentials.

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



**What to do next**

*LDAP secure connection*

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



### Before you begin

### Procedure

**Step 1** Fill in the following fields:

NEW LDAP SETTINGS X

Settings

Role Mapping

LDAP over TLS/SSL

Use self signed certificate

\* Primary Server Address

\* Primary Server Port


Secondary Server Address

Secondary Server Port

\* Base DN ⓘ

\* Server Response Time ⓘ

\* CA Trust Chain

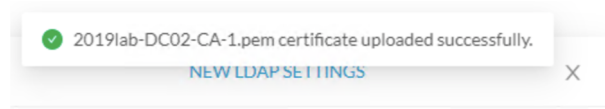
  
Choose a file or drag and drop to upload  
Accepted files: .pem

OK

Cancel

- a) Tick LDAP over TLS/SLL.
- b) Fill in the LDAP settings.
- c) Upload a .pem root certificate or a chain certificate, or tick Use a self-signed certificate.

If you upload a certificate, a message indicating that the certificate has been uploaded successfully appears.



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

NEW LDAP SETTINGS ×

Settings Role Mapping

LDAP over TLS/SSL  Use self signed certificate

\* Primary Server Address \* Primary Server Port

dc01.2019lab.local 636

Secondary Server Address Secondary Server Port

dc02.2019lab.local 636


\* Base DN ⓘ

DC=2019lab,DC=local

\* Server Response Time ⓘ

10

\* CA Trust Chain



Choose a file or drag and drop to upload

Accepted files: .pem

📎 2019lab-DC02-CA-1.pem

OK Cancel

**Step 2** Click OK.

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

**Step 4** Fill in the following fields:

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

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

**Note** 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.

- b) Map Cisco Cyber Vision custom roles with Active Directory groups.

You must type the exact group names as configured into the remote directory so they can be retrieved and mapped to user roles.

NEW LDAP SETTINGS X

Settings

Role Mapping

Default roles ⓘ

Product ▼	Domain Users
Operator ▼	
Auditor ▼	

+

Custom roles ⓘ

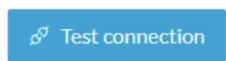
TestAD2019 ▼	TestAD2019	✖
--------------	------------	---

OK

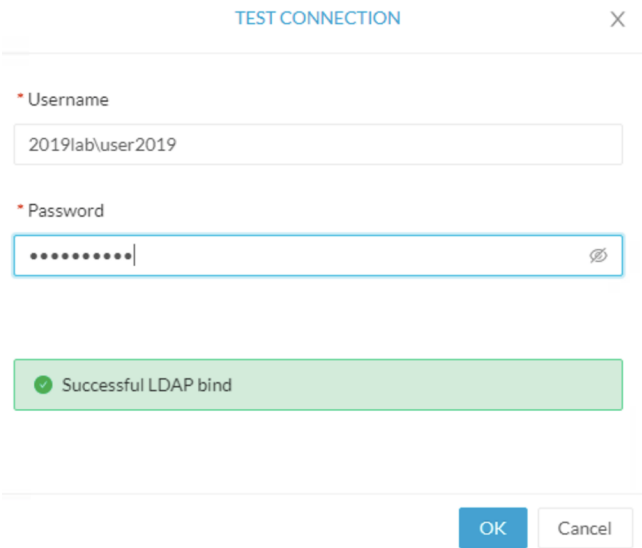
Cancel

**Step 5** Click OK.

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



The Test Connection window pops up.



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

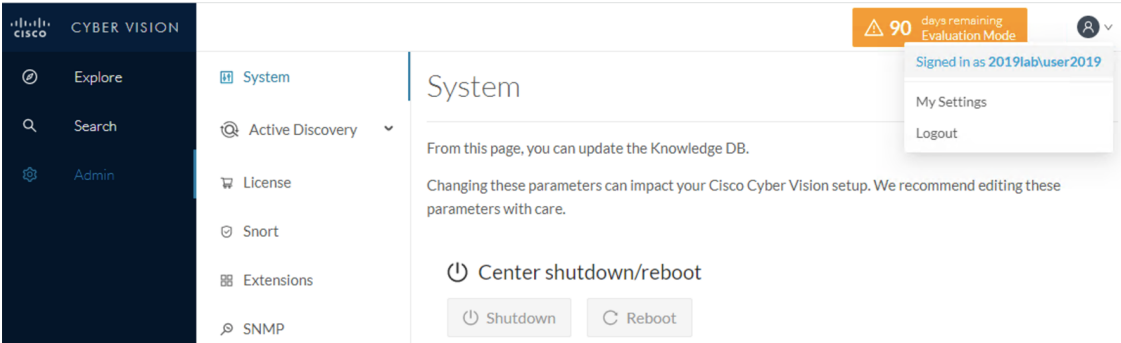
**Note** The Username format is <domain\_name>\<user\_name> (e.g. cisco\john\_doe).

A message Successful LDPA bind should appear.

**Step 8** Click OK.

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

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

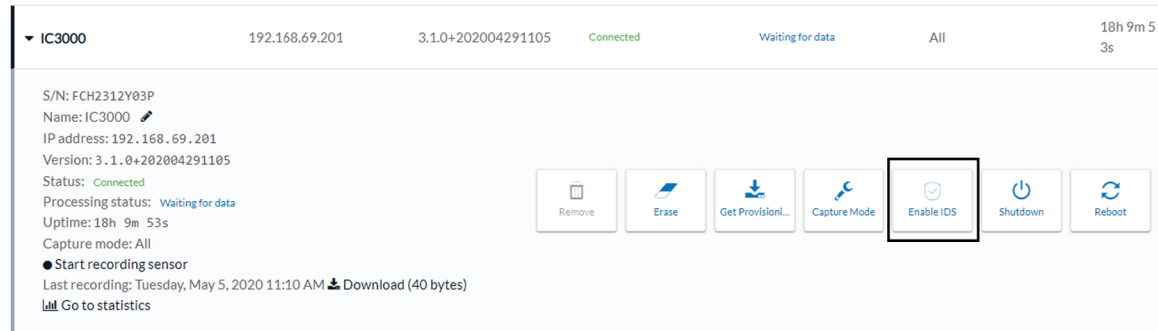


**What to do next**

# Snort

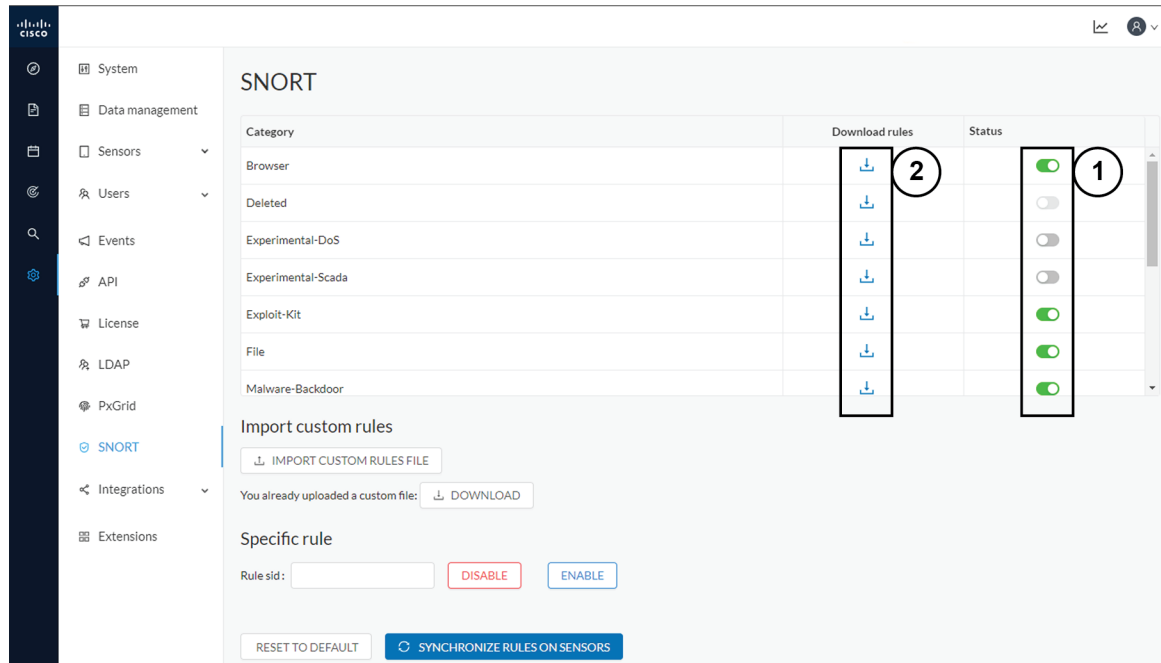
Snort is a network intrusion detection system (NIDS) software based on a text rules engine. It is provisioned in some Cisco Cyber Vision sensors like the sensor embedded in the IC3000, but not activated by default. Cisco Cyber Vision Center stores the rules and configuration files but also intercepts Snort alerts and display them as event.

To activate the Snort engine in the sensor, the button "Enable IDS" from the sensors management page needs to be used:



The rules and the basic configuration of Snort are packaged in the Cisco Cyber Vision Knowledge Database and managed from the SNORT menu. This package is updated regularly by Cisco and need to be updated by retrieving the updated KDB from the official Cisco repository. By default standard rules are configured and some of them are enabled, others are disabled.

In the SNORT administration menu, rules coming from Cisco could be consulted and enabled or disabled. To simplify the usage rules were grouped in categories in order to enable or disable an entire category. The status button (1) column could be used to enable or disable the corresponding category. All category rules could be consulted by downloading the set of rules (2)



Categories list:

- Browser
- Deleted

- Experimental-DoS
- Experimental-Scada
- Exploit-Kit
- File
- Malware-Backdoor
- Malware-CNC
- Malware-Other
- Misc
- OS-Other
- OS-Windows
- Server-Other
- Server-Webapp

Some custom rules could be used in order to generate specific alerts. To do this, a file needs to be generated with a defined syntax as the base rule files. Snort also provides some help to generate rules (Snort\_rule\_infographic.pdf).

The screenshot shows a web interface for managing Snort rules. At the top, there's a section titled 'Import custom rules' with a button labeled 'IMPORT CUSTOM RULES FILE'. Below that, it says 'You already uploaded a custom file:' followed by a 'DOWNLOAD' button. The next section is 'Specific rule', which contains a text input field for 'Rule sid:', a red 'DISABLE' button, and a blue 'ENABLE' button. At the bottom of the interface, there are two buttons: 'RESET TO DEFAULT' and 'SYNCHRONIZE RULES ON SENSORS'.

Custom rules file could be imported in the center by using the button "IMPORT CUSTOM RULES FILE". All custom rules are stored in the center, they could be downloaded for review by using the button "DOWNLOAD".

The predefined rules available in categories could be enabled or disabled individually by using the rule signature id (sid). To retrieve the sid the category file need to be downloaded and consulted, the sid is present at the end of the rule line. When a rule is disabled a "#" is added in front of the rule line to comment it. When a rule is enabled the "#" in front of the rule line is deleted. The 2 buttons "DISABLE" and "ENABLE" are used to do those actions.

When the configuration is done the rules definition (standard and custom) could be sent to the sensors by using the button "SYNCHRONIZE RULES ON SENSORS".

In case of mistake, or to initialize the configuration, the button "RESET TO DEFAULT" could be used. All rules settings will be reset to the default Cisco Cyber Vision configuration.

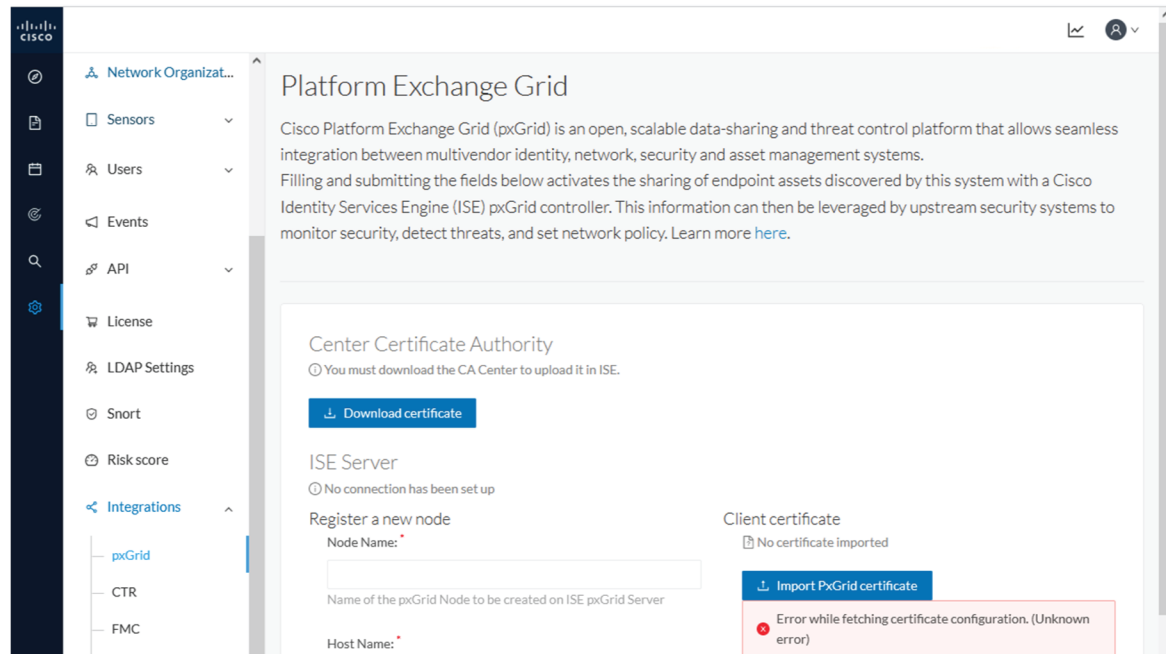
## Risk score

## Integrations

### pxGrid

From this 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.



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".

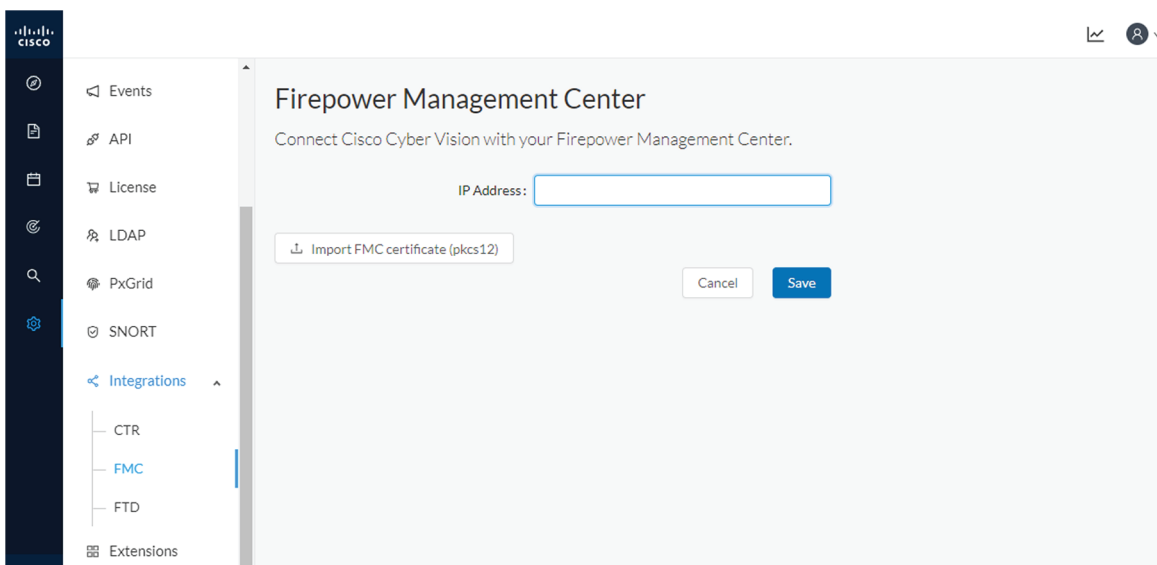
### FMC

FMC administration page permits to configure a link between Cisco Cyber Vision with your Firepower Management Center. This connection will permit to send regularly (every 10 seconds) the components discovered by Cisco Cyber Vision. Every 10 seconds a list of new discovered components will be sent with the following properties in Cisco Cyber Vision:

- Name
- Id
- Ip
- Mac
- And if they are available:

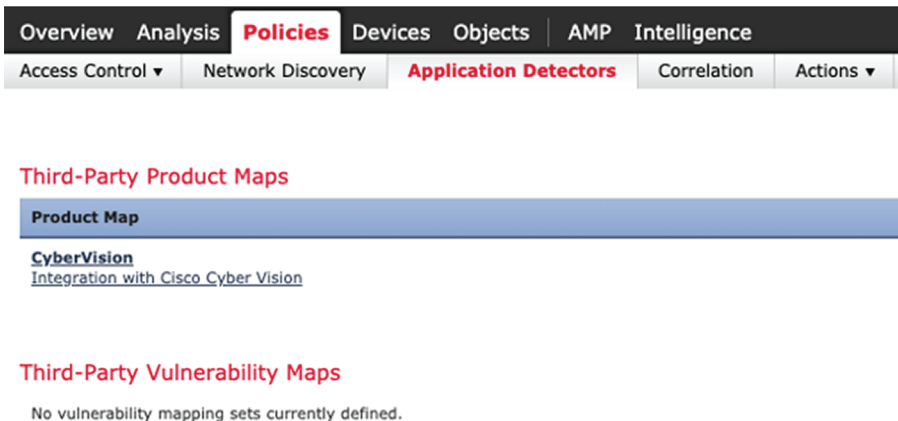
- hw\_version
- model-ref
- serial\_number
- fw\_version
- tags

The configuration of this connection consists of adding the IP address of FMC, then importing a certificate in Cisco Cyber Vision.



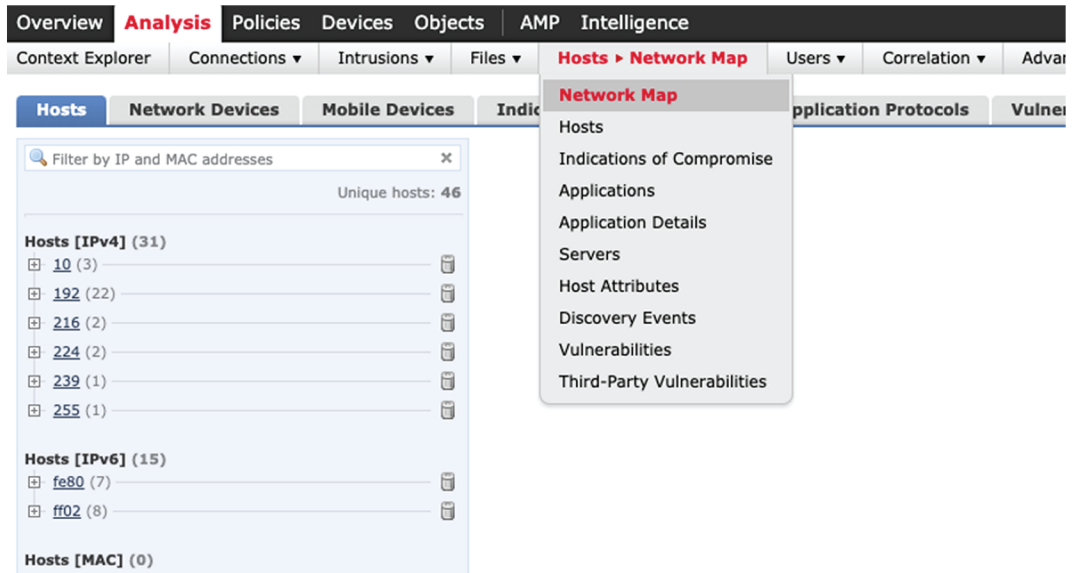
In FMC, to download the necessary certificate, please navigate to "System" then to "Integration" and open the "Host Input Client" tab. In the tab create a new Client with the button "Create Client". Add the Cisco Cyber Vision Center IP address as host name, then download the pkcs12 certificate.

Then, in FMC, menu "Policies", "Application Detectors" add a new Product Map with the button "Create Product Map Set". Please create the new product Map with the exact name and case as presented below:





The created hosts could be consulted in FMC, menu "Analysis", tab "Hosts – Network Map":



## FTD

FTD administration page permits to connect Cisco Cyber Vision with your Firepower Threat Defense. It will allow to automatically kill anomalies detected by monitor mode and snort events. The corresponding session found in FTD will be killed.

Every 10 seconds Cisco Cyber Vision will browse the new monitor and SNORT events and send the corresponding action to the firewall. To enable that functionality, the user needs to add the following parameters in the FTD administration page:

- Ip address of the firewall
- Login: admin login, an ssh connection will be established between the center and the firewall
- Password: corresponding password
- Hostname: is the name of the device, by default "firepower"

Two options are available: kill session from monitor difference detection events and kill session from snort events.

**Firepower Threat Defense**

Connect Cisco Cyber Vision with your Firepower Threat Defense. It will allow us to automatically kill anomalies detected by monitor mode and snort events

IP Address:

Login:

Password:

Hostname:

Kill session from monitor difference detection events:

Kill session from snort events:

## SecureX

Cisco SecureX is an online platform that centralizes security events from different Cisco software equipments through an API. For example, events like Cisco Cyber Vision events or firewall events can be sent to Cisco SecureX and correlated to be presented through different dashboards.

The integration with SecureX will enable 3 features in Cisco Cyber Vision:

- with SecureX SSO login, a button "Report to SecureX" will appear in some events of the [The Calendar](#). this button will push the events to SecureX.
- with SecureX SSO login, a SecureX Ribbon could be activated and associated features could be used in Cisco Cyber Vision.
- without SecureX SSO login, a button "Investigate in SecureX Threat Response" is displayed in component technical sheet.

The different topics below will cover the configuration of SecureX in Cisco Cyber Vision and the usage of the different features authorized.

### SecureX configuration

#### Before you begin

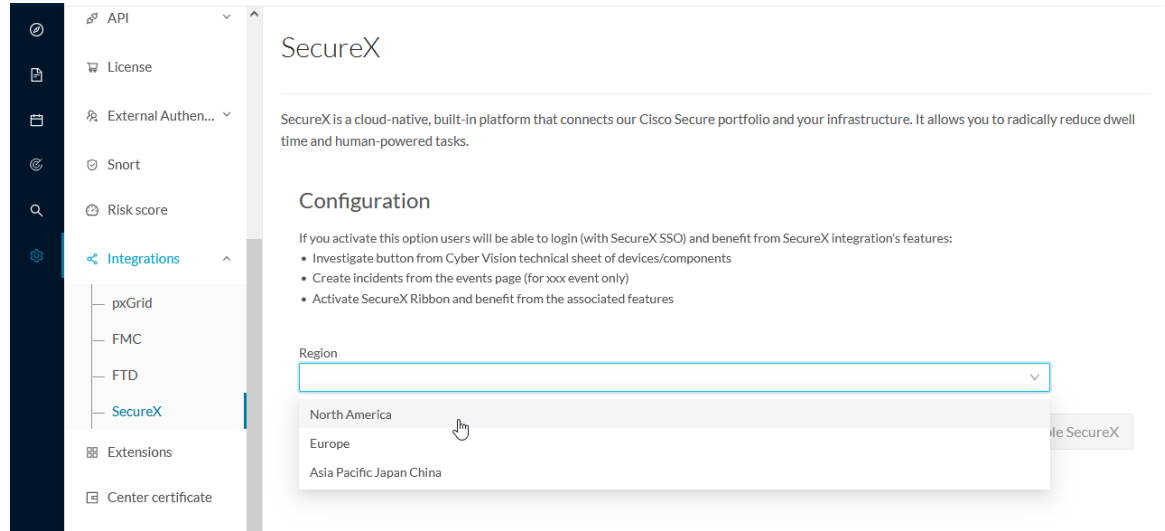
The Cisco SecureX configuration in Cisco Cyber Vision requests:

- An Admin access to Cisco Cyber Vision
- A Cisco Cyber Vision Center with internet access
- A SecureX account with an admin role.

**Procedure**

**Step 1** To start the configuration, in Cisco Cyber Vision navigate to the **Admin** menu, then **Integrations** and finally **SecureX**.

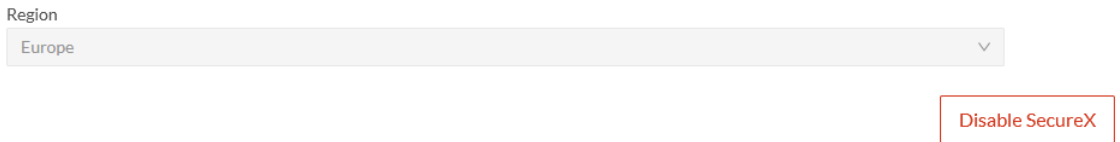
**Step 2** Then on the **SecureX** page select the Region to be used:



**Step 3** Once the **Region** selected, the button Enable SecureX becomes available, click on it to enable the link.

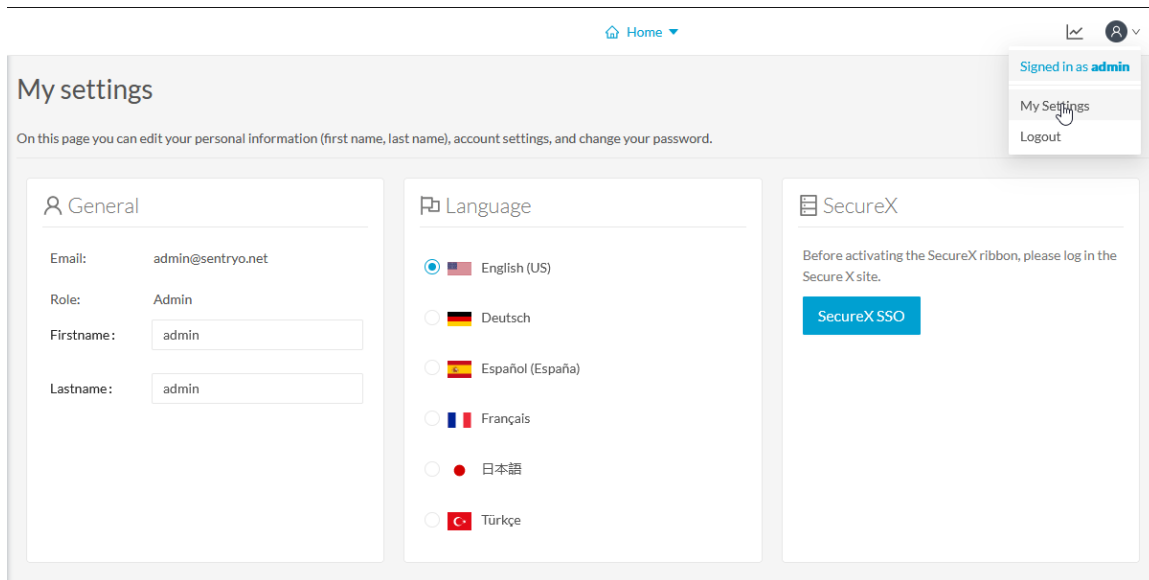


Once enabled the button becomes red:

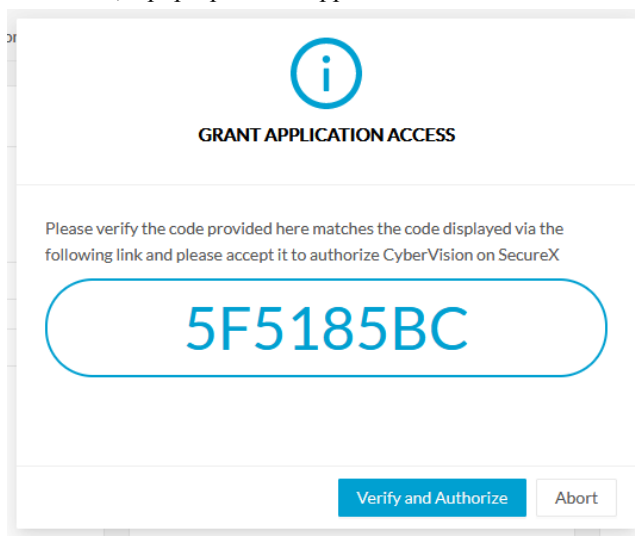


Reaching this step is enough to use the button "Investigate in SecureX Threat Response" in component technical sheet. The other 2 features need some extra steps explained below:

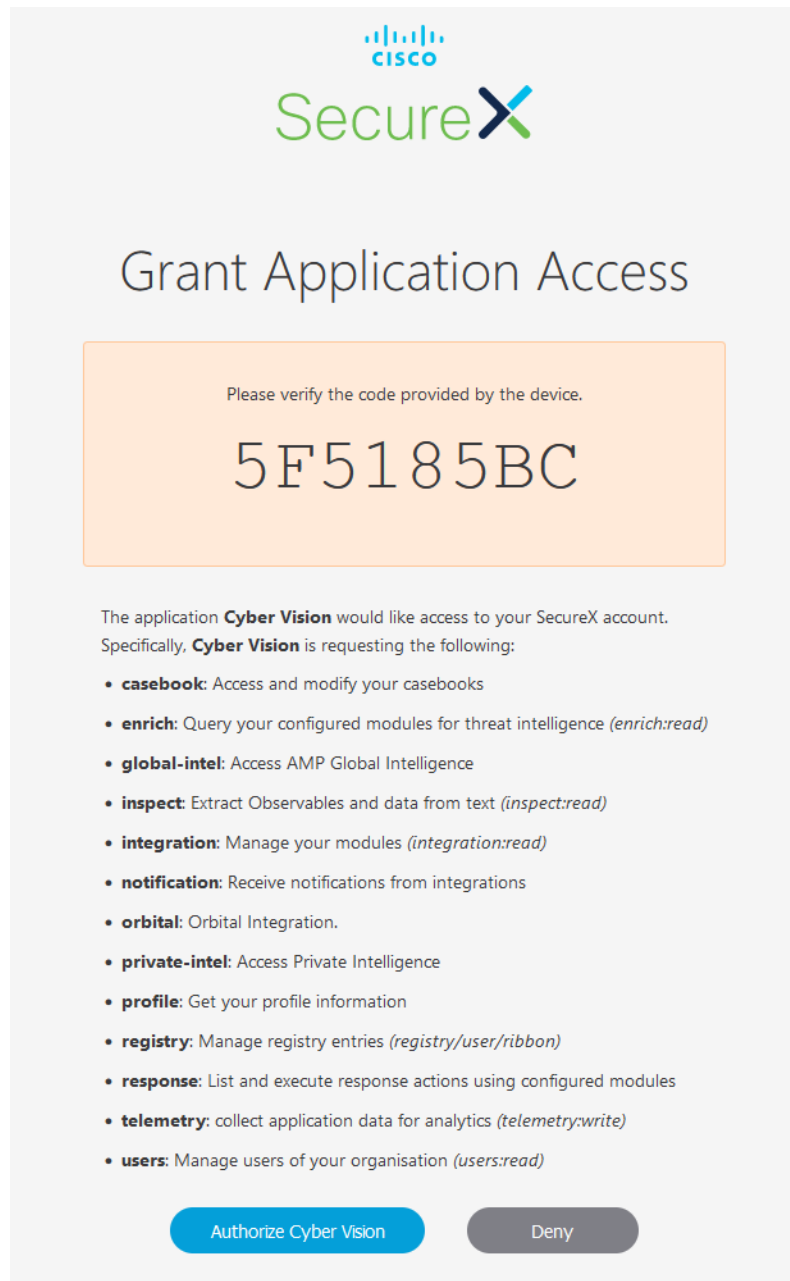
**Step 4** Navigate to the user **My Settings** menu (on the top right corner of the user interface). A new menu **SecureX** is available on this page when SecureX is enabled.



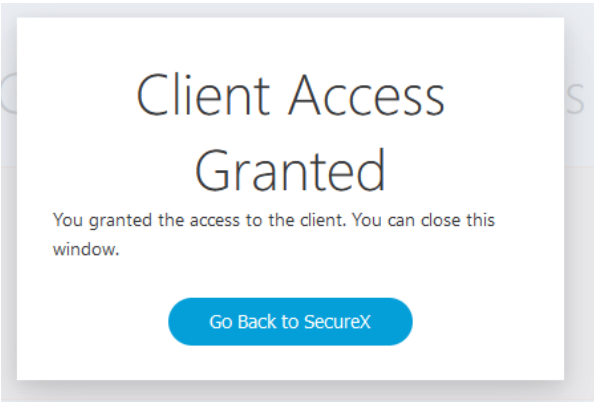
**Step 5** Click on the **SecureX SSO** button, a pop-up should appear with an authentication code:



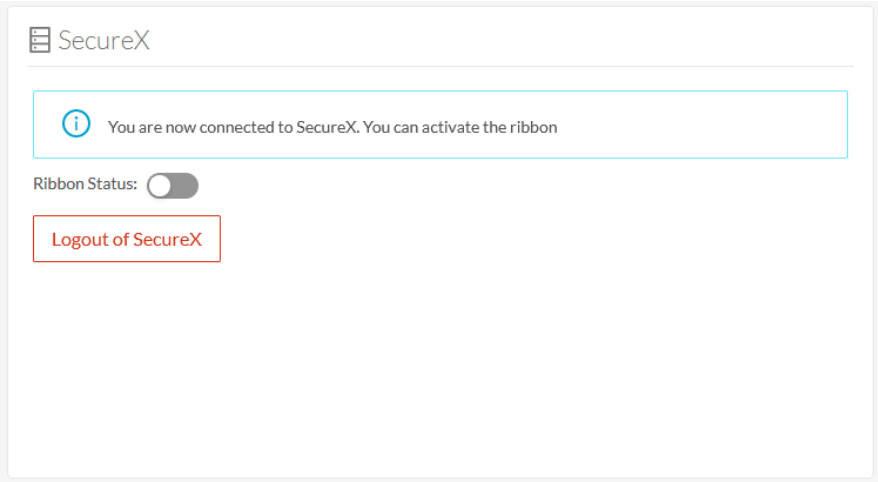
**Step 6** A new page is opened in the browser with a **Grant Application Access** to SecureX, click on **Authorize Cyber Vision**



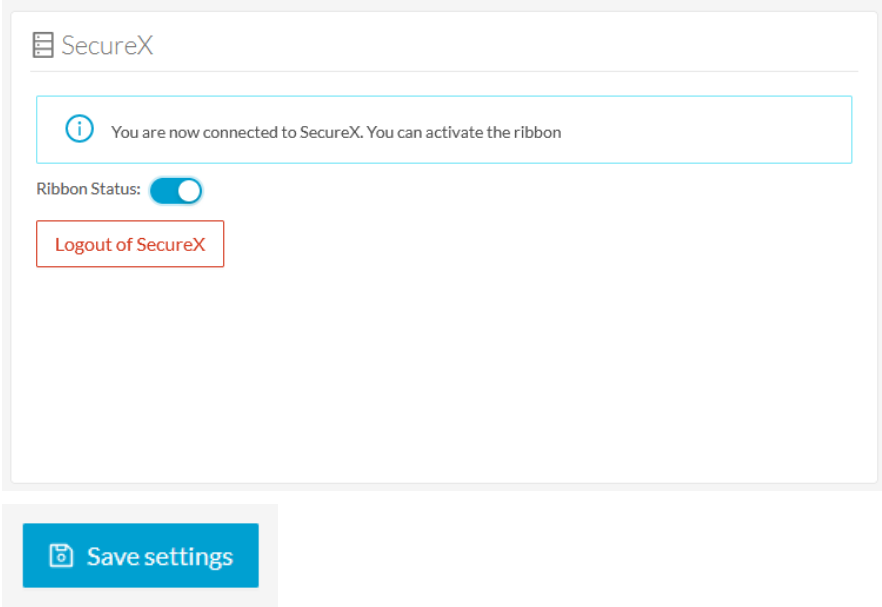
**Step 7** A positive answer from the system will display the following pop-up:



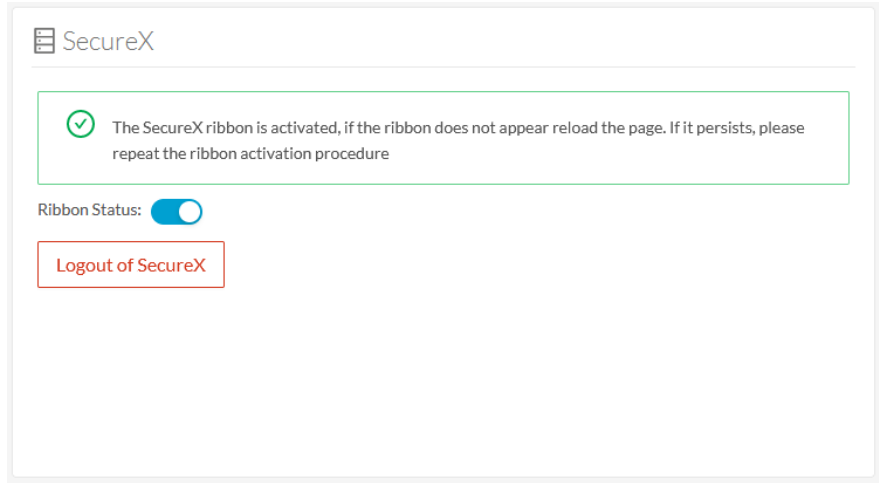
**Step 8** Go back in Cyber Vision user interface, the **SecureX** area of the **My Settings** menu presents now a **Logout of SecureX** button and a slide button to activate the Ribbon:



**Step 9** To activate the ribbon, click on the **Ribbon Status** slide and click on the button **Save Settings**



**Step 10** Once done, the **SecureX** menu should be like:

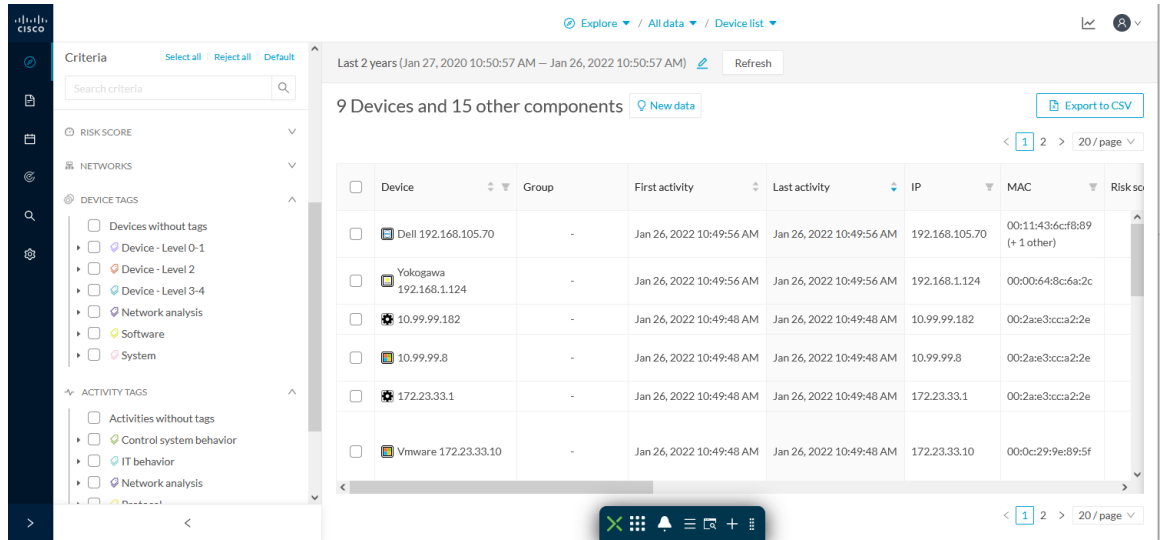


**What to do next**

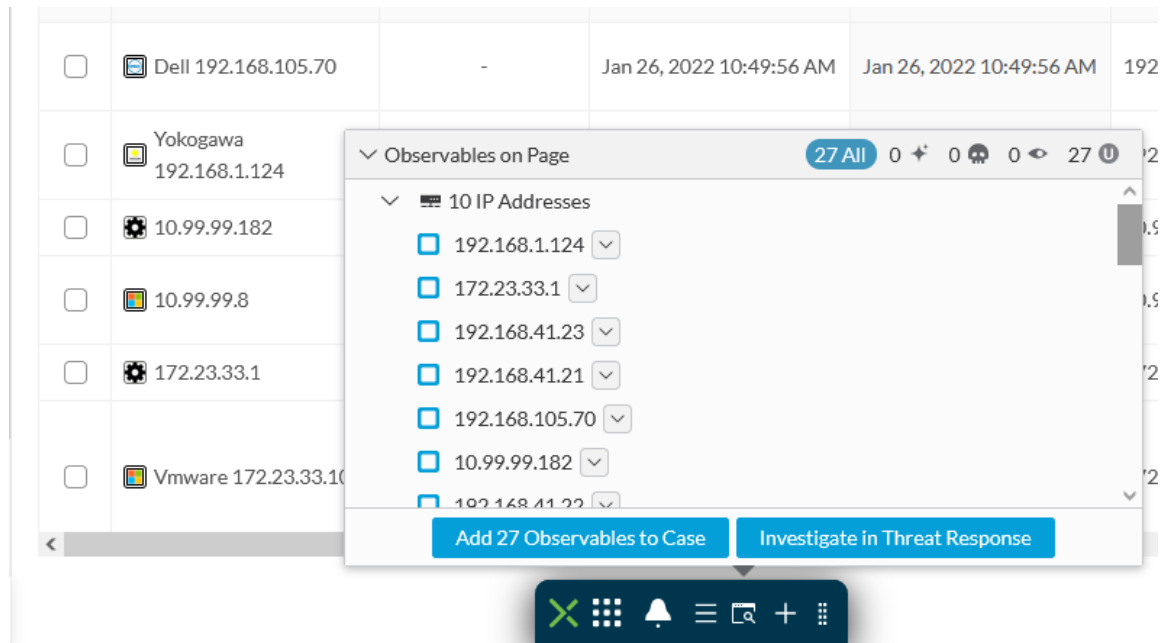
The 3 SecureX features are now enabled and could be used.

**SecureX Ribbon in Cyber Vision**

Once configured and activated, the SecureX Ribbon will appear on the bottom of the Cisco Cyber Vision user interface in the Explore menu, for example in the Device List:



The SecureX Ribbon usage is explained in the [Cisco SecureX Getting Started Guide](#) For example to find observables and investigate them in SecureX threat Response, click the **Find Observables** icon like below:



### SecureX event integration

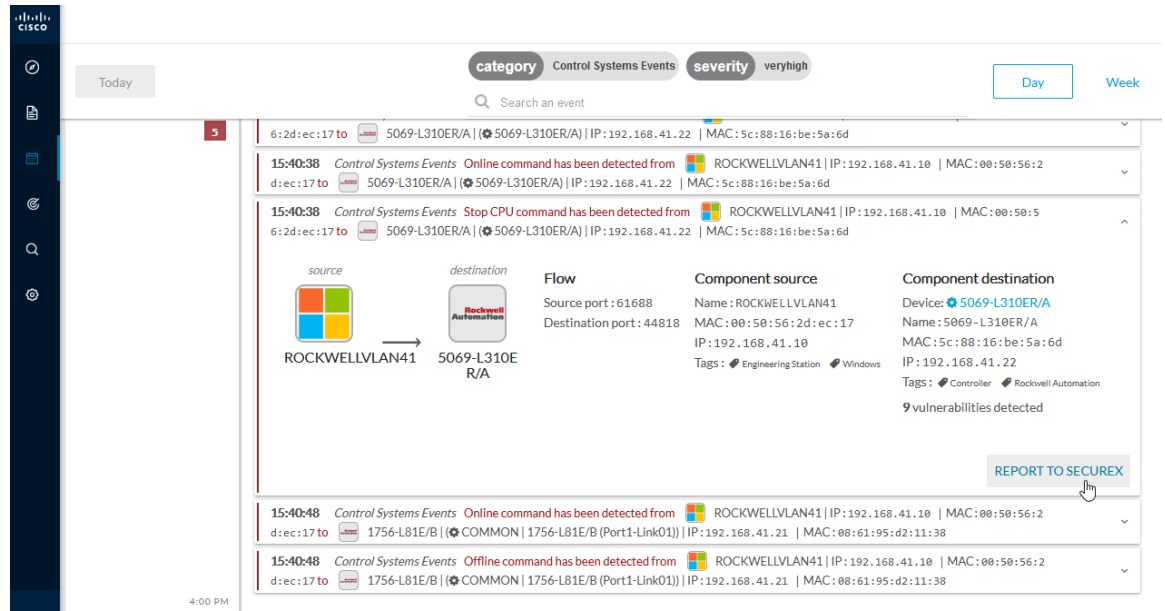
When the configuration of SecureX is made in Cisco Cyber Vision a button will appear in some events of the [The Calendar](#), this button will push the event to SecureX and create incident.

The SecureX button will appear on 3 categories of event:

- Anomaly Detection
- Control Systems Events
- Signature Based Detection

For example:

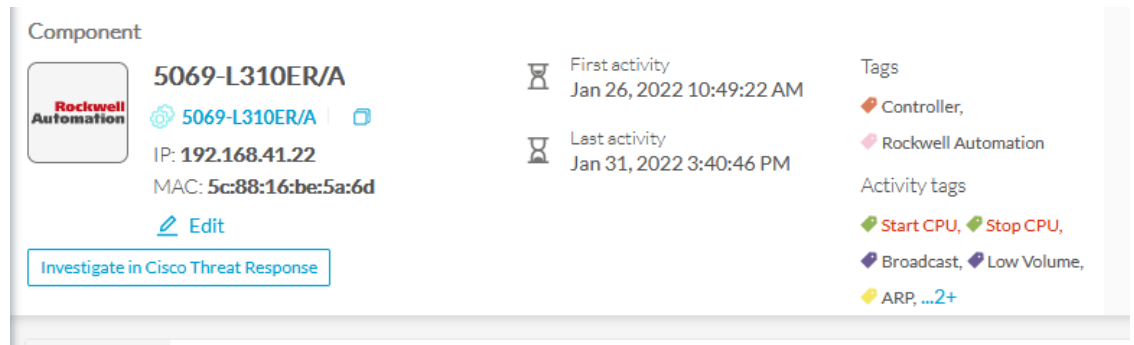




### SecureX component button

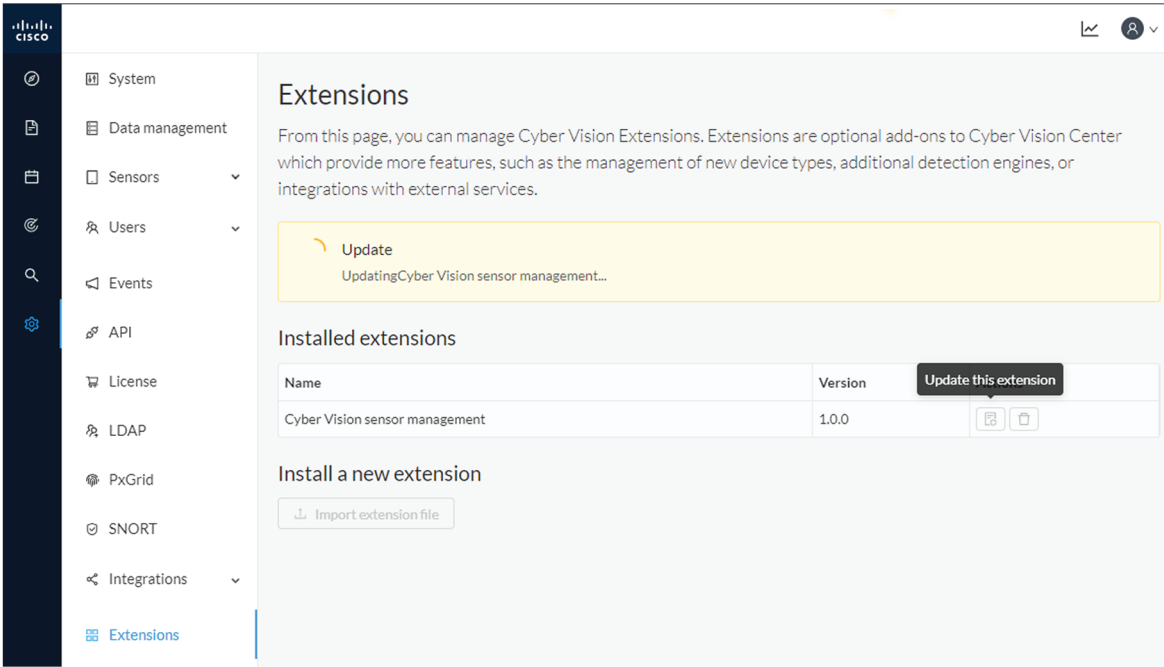
When the SecureX configuration is done, a button will be available in the component technical sheet to investigate in SecureX Threat response the IP and MAC address of the component.

For example:



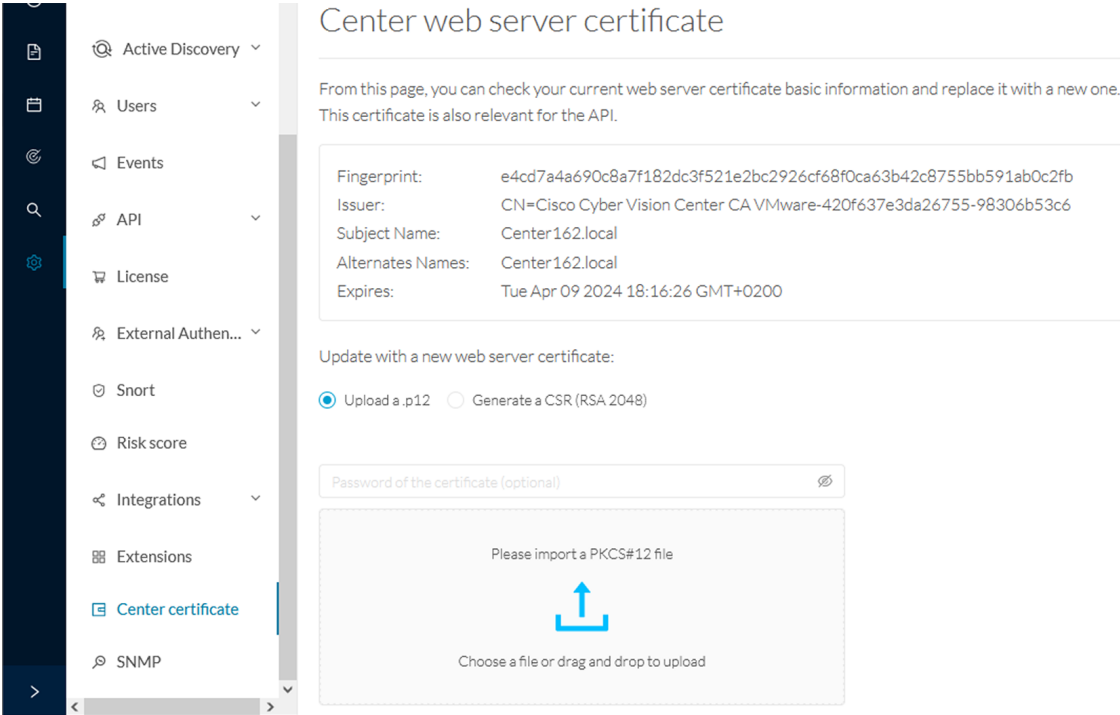
## Extensions

From this page, you can manage Cyber Vision Extensions. Extensions are optional add-ons to Cyber Vision Center which provide more features, such as the management of new device types, additional detection engines, or integrations with external services.



# Center certificate

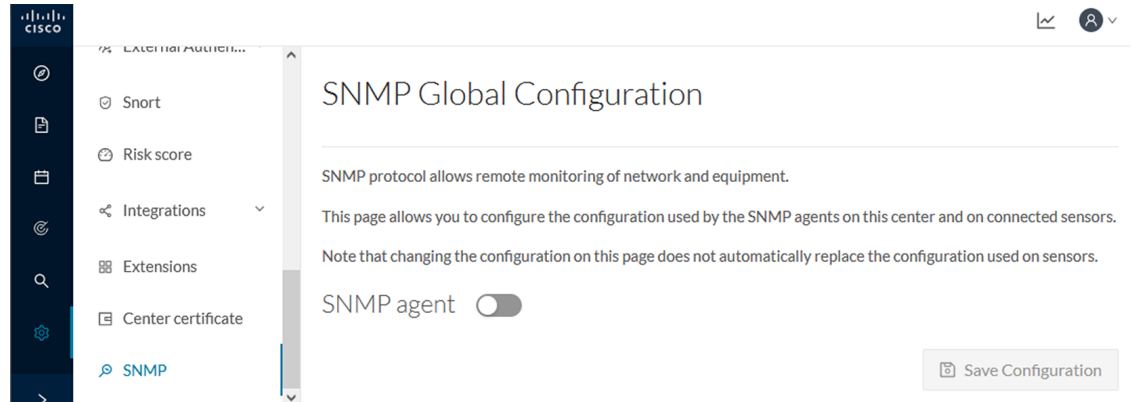
The Center web server certificate page is to configure Cisco Cyber Vision user interface security with an enterprise certificate. You will have the option to upload a .p12 or to generate a CSR.



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

## SNMP

SNMP Protocol in CyberVision is used for remote monitoring purposes.



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** In Cisco Cyber Vision, navigate to Admin > SNMP.

**Step 2** Toggle the SNMP agent button.

A configuration menu appears.

## SNMP Global Configuration

SNMP protocol allows remote monitoring of network and equipment.

This page allows you to configure the configuration used by the SNMP agents on this center and on connected sensors.

Note that changing the configuration on this page does not automatically replace the configuration used on sensors.

SNMP agent

### Configuration

Monitoring hosts (IPv4):

Version:  3  2c

Security type:  ▾

Username:

**Step 3** In the Monitoring hosts (IPv4) field, fill in the IP address of the Monitoring host.

**Step 4** Select a version:

- Version 3
- Version 2c

Version:  3  2c

Security type:  ▾

Username:

**Note** For security reasons, it is recommended to use SNMP version 3.

a) **Version 3**

Select a security type:

- NoAuth: Only a username is required. No authentication password required.

Security type:

Username:

Add the username that will be used for the SNMP authentication. "ics" is used by default.

- Auth with NoPriv : A username and an encrypted password are required.

Security type:

Username:

Authentication:

Add the username that will be used for the SNMP authentication. "ics" is used by default.

Add the Hash algorithm needed and its password. It must be at least 8 characters long.

- Auth with Priv: Only the AES encryption is available. A username, an encrypted password, and an AES encryption are required.

Security type:

Username:

Authentication:

Privacy:

Add the username that will be used for the SNMP authentication. "ics" is used by default.


Add the Hash algorithm needed and its password. It must be at least 8 characters long.

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.

Version:  3  2c

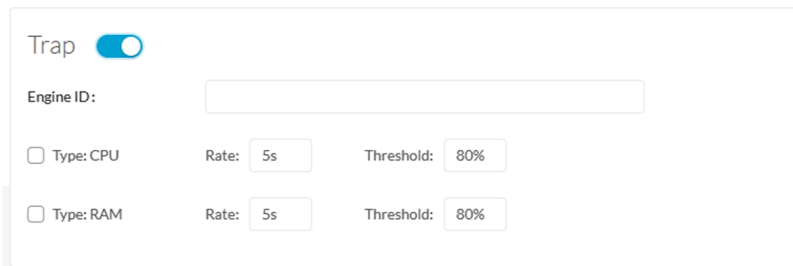
 For security reasons, we recommend using version 3 of the SNMP protocol

Community:

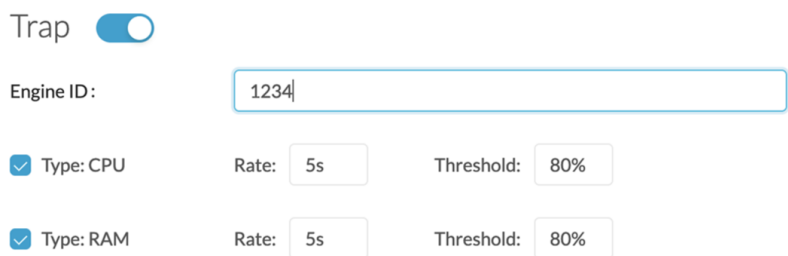
**Step 5** Toggle the Trap button.



The following configuration menu appears:



**Step 6** Setup traps to be delivered.



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

**Step 7** Click Save Configuration.

## SNMP MIB

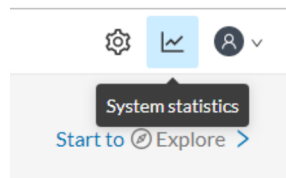
**Table 1:**

MIB	OID prefix	Description
*MIB-2*	.1.3.6.1.2.1.1	System
*IF-MIB*	.1.3.6.1.2.1.2.2.1.1	All physical interfaces
*IF-MIB*	.1.3.6.1.2.1.31.1.1	All physical interfaces
*HOST-RESOURCES-MIB*	.1.3.6.1.2.1.25.1	System
*HOST-RESOURCES-MIB*	.1.3.6.1.2.1.25.2.3	Storage
*HOST-RESOURCES-MIB*	.1.3.6.1.2.1.25.3.3	CPU
*HOST-RESOURCES-MIB*	.1.3.6.1.2.1.25.3.6	Disk

MIB	OID prefix	Description
*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

## System statistics

To access system statistics click the System statistics button on the top right corner of Cisco Cyber Vision.

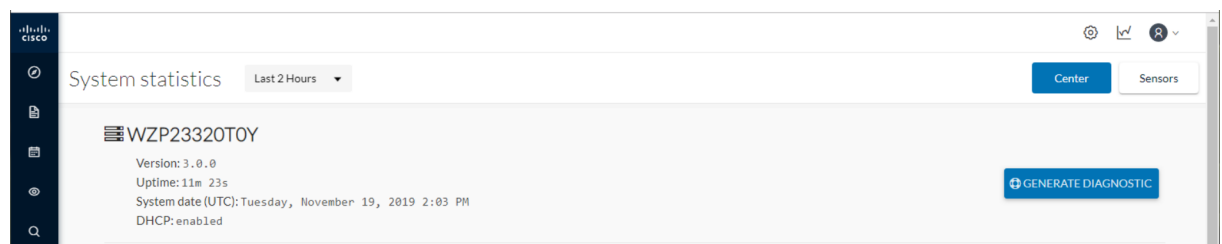


## Center

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



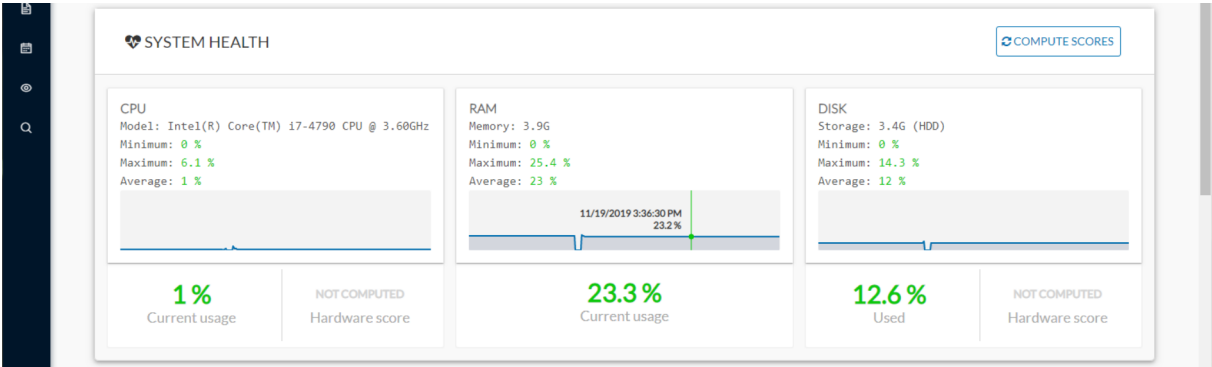
**Note** Most data presented below evolve as you select a different period of time.



At the top of the page, you will find 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).

The button on the right generates a diagnostic file about the Center that is sometimes requested by the Cisco product support in case of trouble.

System health:



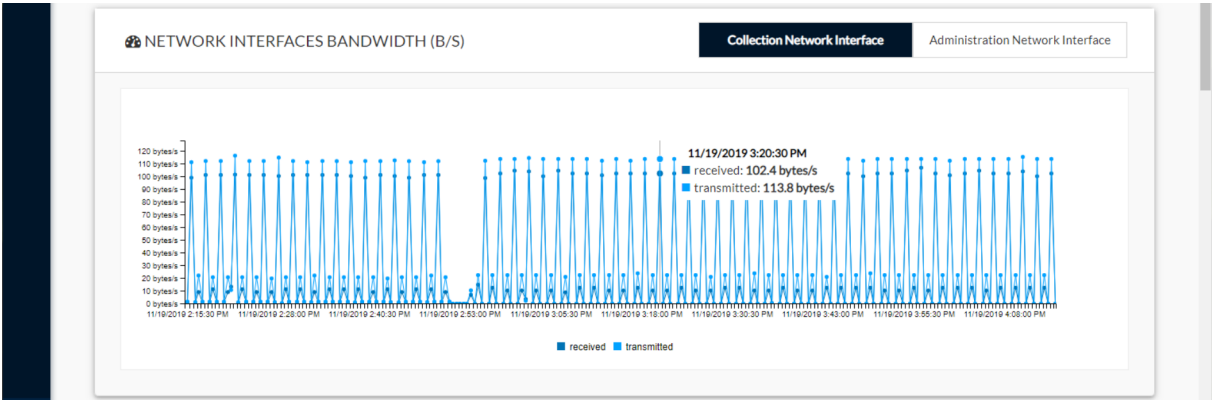
The system health gives you the state of the Center CPU, RAM and disk usage.

Usages (i.e. minimum, maximum and average) are indicated for each of these system resources while the absolute value is shown in a tooltip if you mouse over the line chart.

Below, you have the percentage of the system's current usage. Also, there is an indicative hardware score which is useful to Cisco product support.

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

Network interfaces bandwidth:

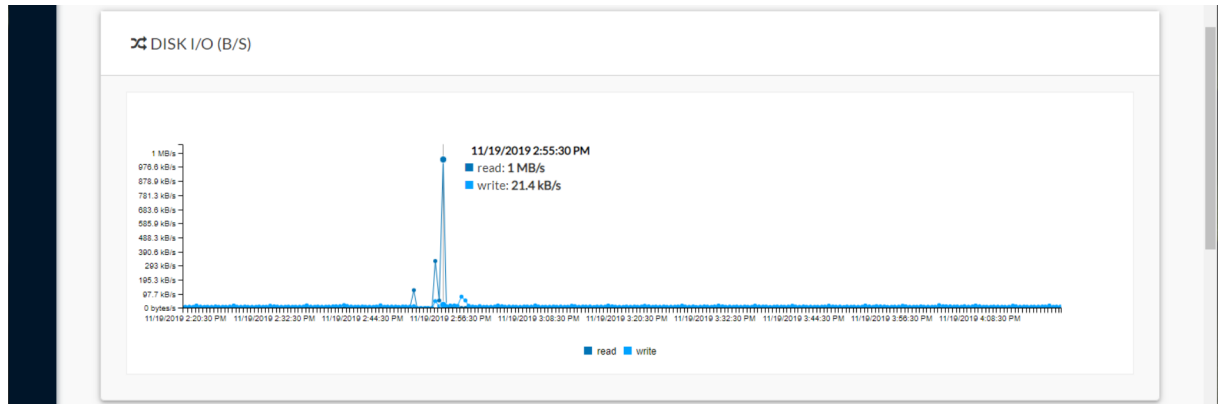


The line charts represent the Administration and Collection network interfaces bandwidth with the number of bytes received and sent by the Center per second.

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

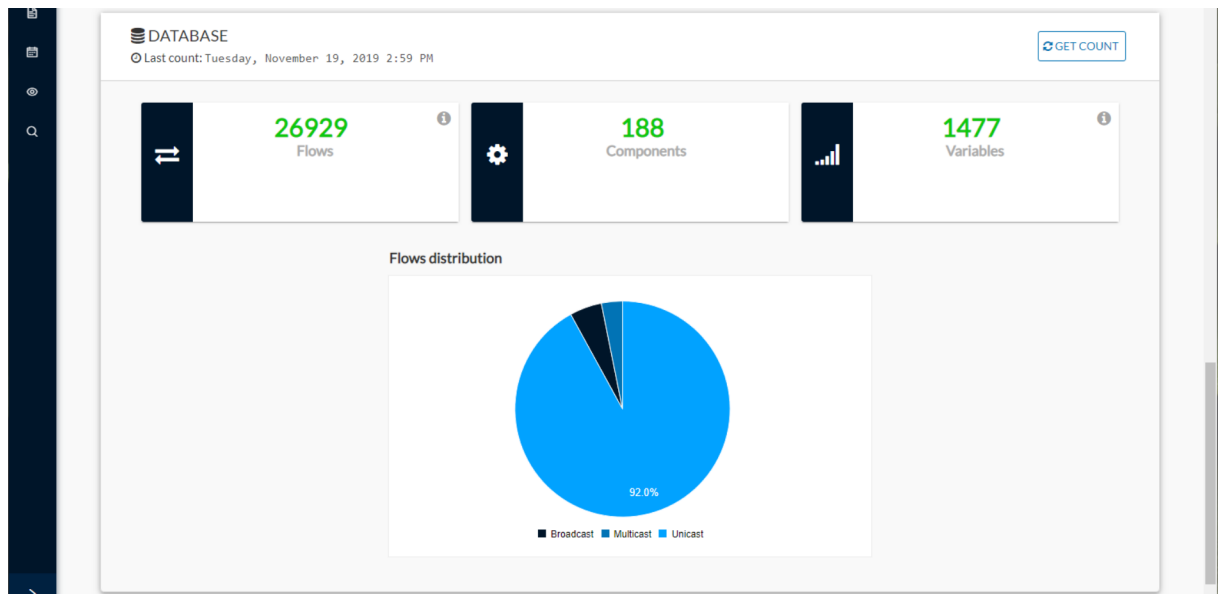
Disk I/O:





The line chart represents the Center hard disk usage with the number of bytes read and written per 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.

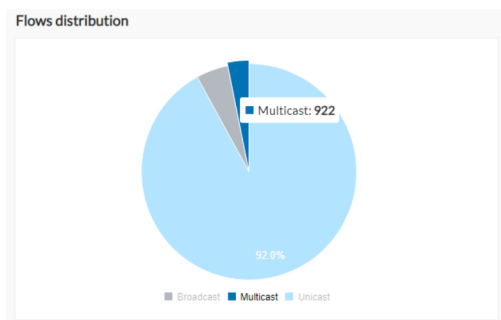


The flows card indicates the total number of flows (i.e. broadcast, multicast and unicast which are stored in the database) detected by Cisco Cyber Vision. If you mouse over the card, you will get the number of activities and the flows evolution tendency. This information enables you to anticipate how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



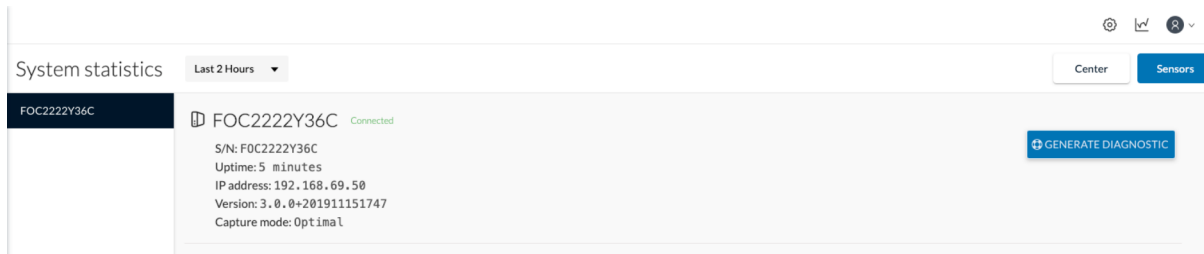
The flows distribution pie chart indicates the distribution of broadcast, multicast and unicast flows stored in the database. Mouse over the chart to see the absolute number of flows per flow type.

## 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** Most data presented below evolve as you select a different period of time.



On the left you have a list of the sensors (only one sensor is represented here). Click on a sensor name to access its statistics.

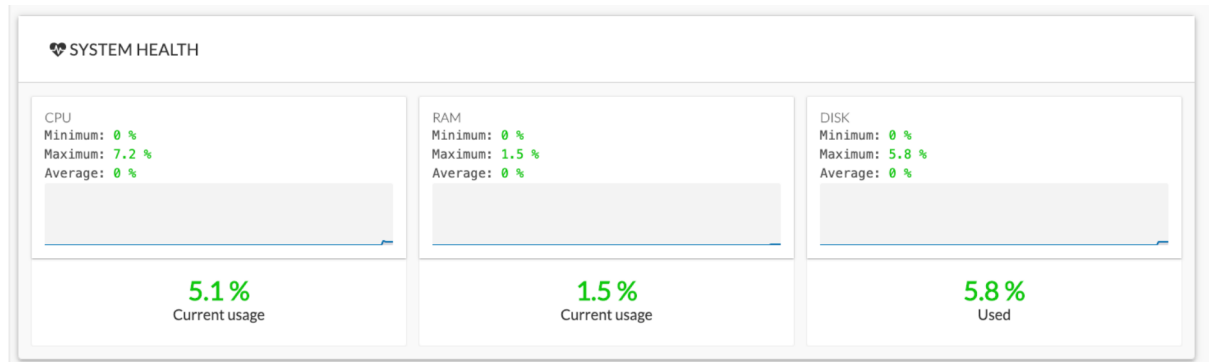
On top of the sensors statistics view you will find general information about the sensor: its status (i.e. Connected), its serial number, its IP and MAC addresses, its firmware version, the capture mode set and the time it has been operating (i.e. uptime).

The button on the right generates a diagnostic file about the sensor that is sometimes requested by the Cisco product support in case of trouble.

**System health:**

The system health gives you the state of the sensor CPU, RAM and disk usage.

Usages (i.e. minimum, maximum and average) are indicated for each of these system resources while the absolute value is shown in a tooltip if you mouse over the line chart.



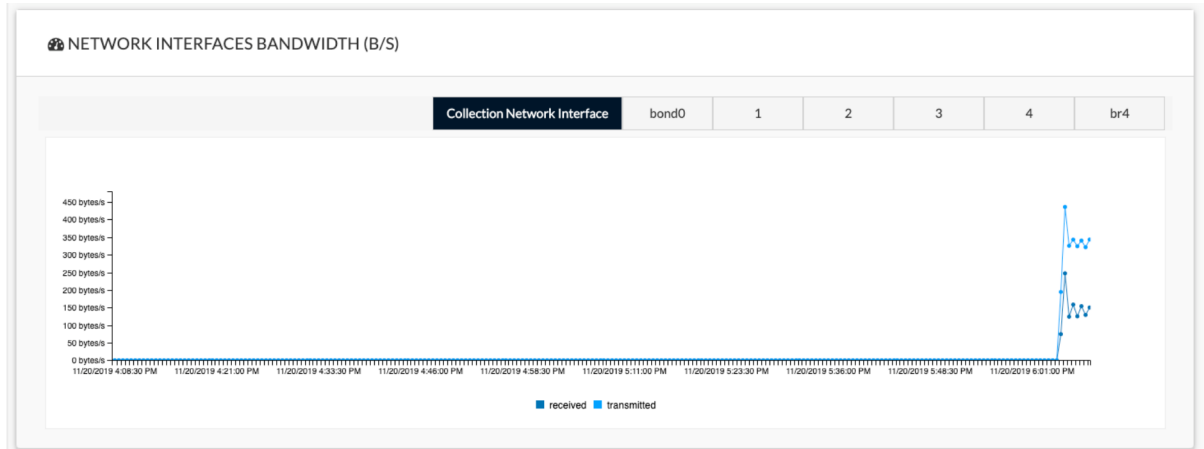
Below, you have the percentage of the system current usage. There is also an indicative hardware score which is useful to Cisco product support.

**Packets captured:**



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

**Network interfaces bandwidth:**

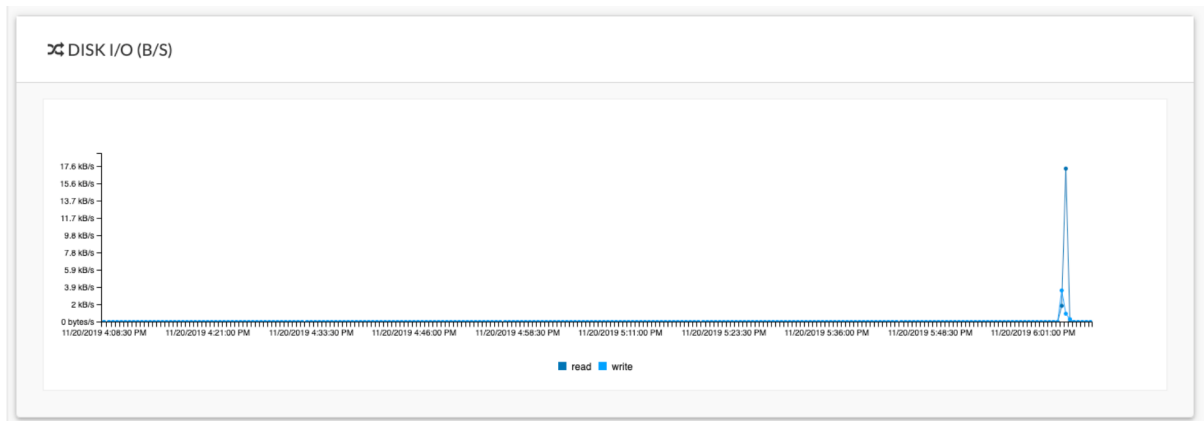


The line charts represent the Collection and the Industrial network interfaces bandwidth with the number of bytes received and sent by the Center per second.

- The Collection Network interface activity chart lets you see the amount of data exchanged between the Center and the sensors.
- The Industrial ones lets you see the amount of data captured by the sensor on the industrial network through each ports couple.

Data sent to the industrial network is also represented but value should stand to zero. If the transmitted line shows activity then the sensor is not passive anymore. If this situation happens, please contact Cisco support immediately.

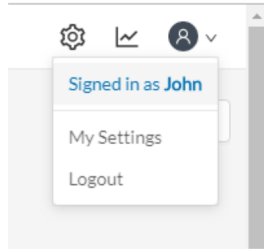
Disk I/O:



The line chart represents the sensor hard disk usage with the number of bytes read and written per second.

## My settings

You can set up your personal account by clicking Settings in the user menu on the top right corner of Cisco Cyber Vision.



From this page, you can:

- Modify your first and last name.
- Change the interface language. Cisco Cyber Vision is available in English, French, German, Japanese, Spanish and Turkish.
- Change 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** Passwords should be changed regularly to ensure the platform and the industrial network security.



**Note** Your email will be requested for login access.

- Restore interface notifications.
- Clear application cookies.

