Cisco Cyber Vision GUI User Guide, Release 5.0.0

First Published: 2021-01-01

Last Modified: 2024-07-12

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

© 2022–2024 Cisco Systems, Inc. All rights reserved.

CONTENTS

About this documentation

Document purpose

This user guide presents the Understanding concepts of Cisco Cyber Vision and how to Navigating through Cisco Cyber Vision within the application by explaining available features.

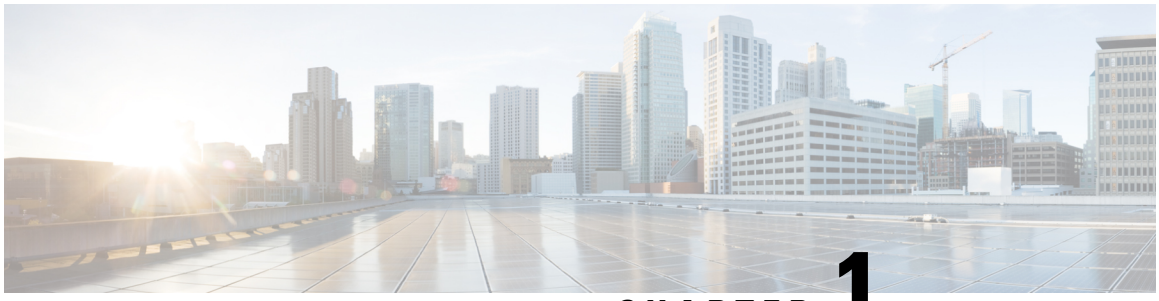
It shows the GUI with the highest license level (Advantage) and all available user roles (from full rights to read-only).

This manual is applicable to **system version 5.0.0**.

Warnings and notices

To ensure your personal safety and to prevent damage to property, observe the following: Warnings and notices and Safety Alert symbols. 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. Take precautions.
Important	Indicates risks that could involve property or Cisco equipment damage and minor personal injury. Take precautions.
Note	Indicates important information on the product described in the documentation.



CHAPTER 1

Introduction

Cisco Cyber Vision Installation

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

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

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

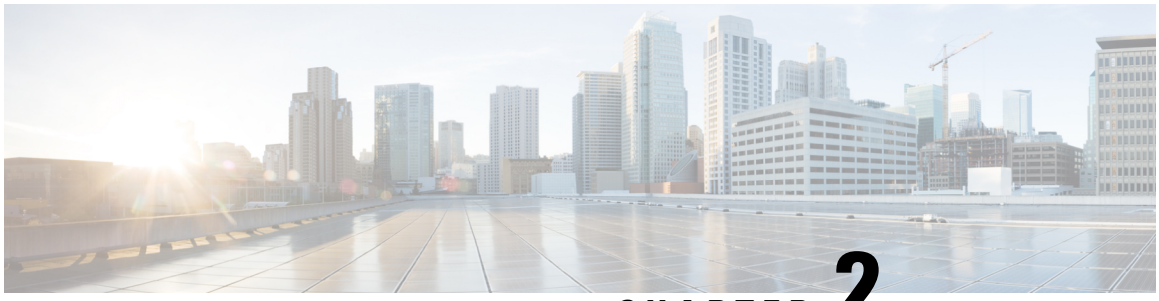
At least one sensor has to be enrolled so that you can see it in the GUI. To do so, refer to Managing the sensors section in the corresponding documentation.

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.

PART I

Understanding concepts



CHAPTER 2

Preset

Preset

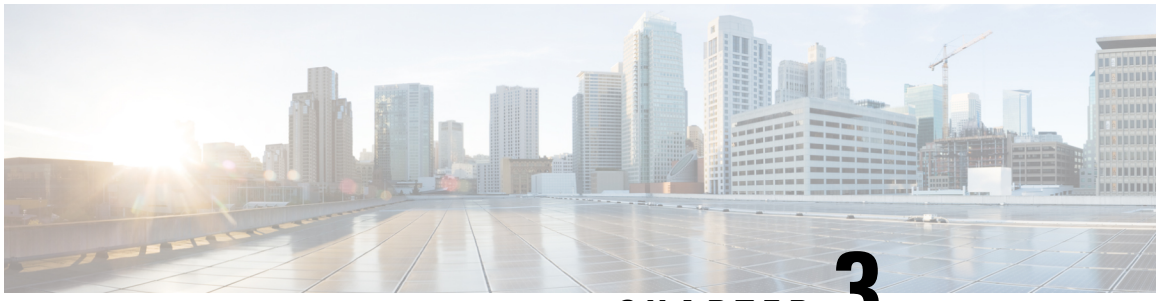
A preset is a set of criteria. Think of a preset as a "magnifying glass" in which you can see details of a big network by choosing the metadata processed by Cisco Cyber Vision that meets your business requirements. We created presets to help you navigate through the data. For example, if you are interested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

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

- Basics: To see all data, or filter data to IT or OT components.
- Asset management: To identify and inventory all assets associated with OT systems, OT process facilities, and IT components.
- Control Systems Management: To check the state of industrial processes.
- IT Communication Management: To see flows according to their nature (OT, IT, IT infrastructure, IPV6 communications, and Microsoft flows).
- Security: To control remote accesses and insecure activities.
- Network Management: To see network detection issues.

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

Note Customized presets are persistent and impact other users.



CHAPTER 3

Filter

Filters

Create presets using the following filters:

Criteria

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

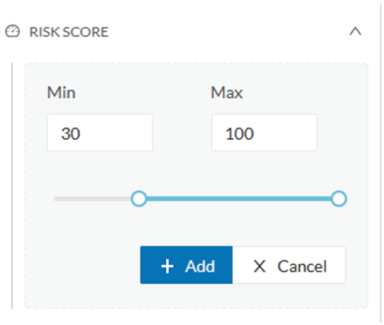
- Risk score: device individual risk
- Networks: device IPs
- Device tags: devices
- Activity tags: activities
- Groups: devices
- Sensors: device “location”

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

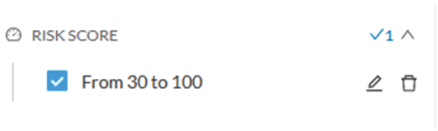
Risk Score

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

Risk score, filter definition

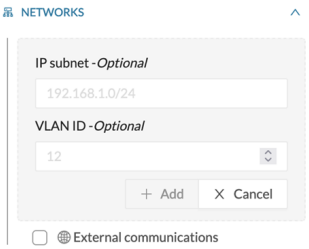


Risk score – inclusive filter



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

Networks

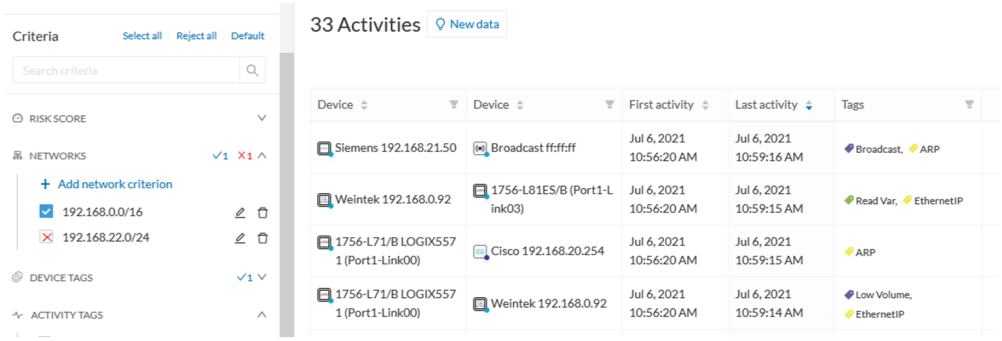


Define a filter based on two network settings: IP range or VLAN ID. This filter will have an impact on the Activity List. The result will be “all activities with one end belonging to this network.” Activities with at least one device in the corresponding network are selected.

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

For instance, use exclusion and combination for this result:

Network filter – negative filter



Multiple negative selections are not supported on 4.0.0.

Filter combination

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

Device tag filters

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

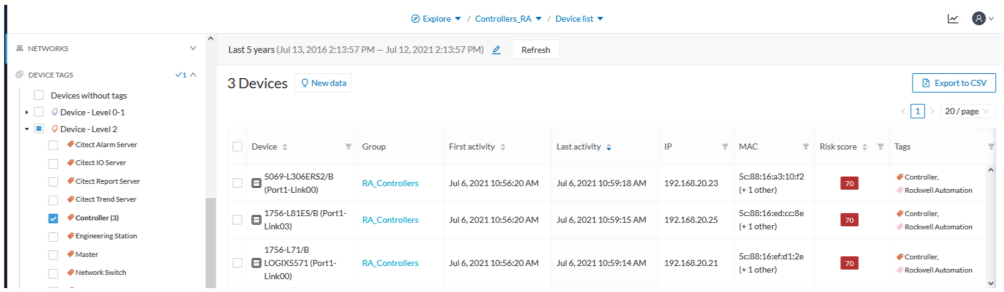
Device tag filters

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

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

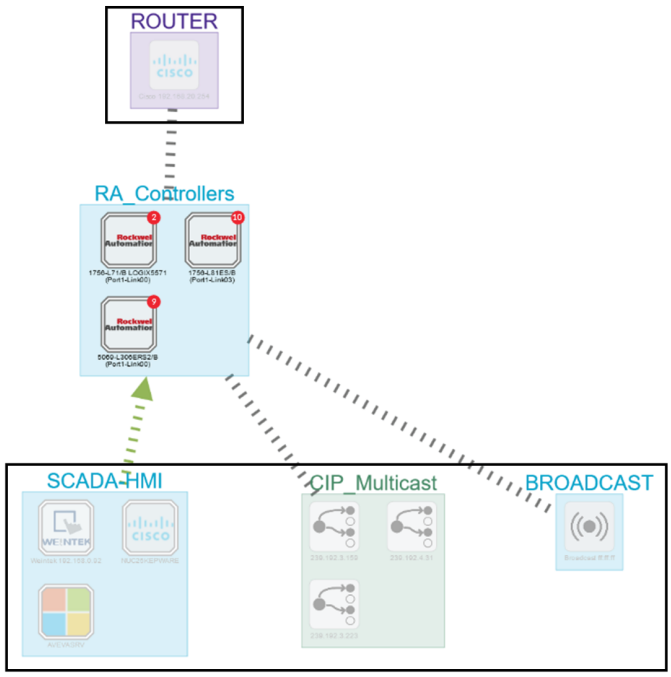
It will give the following results:

Device tag filter, example of Controllers – list of devices



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

Device tag filter, example of Controllers - map

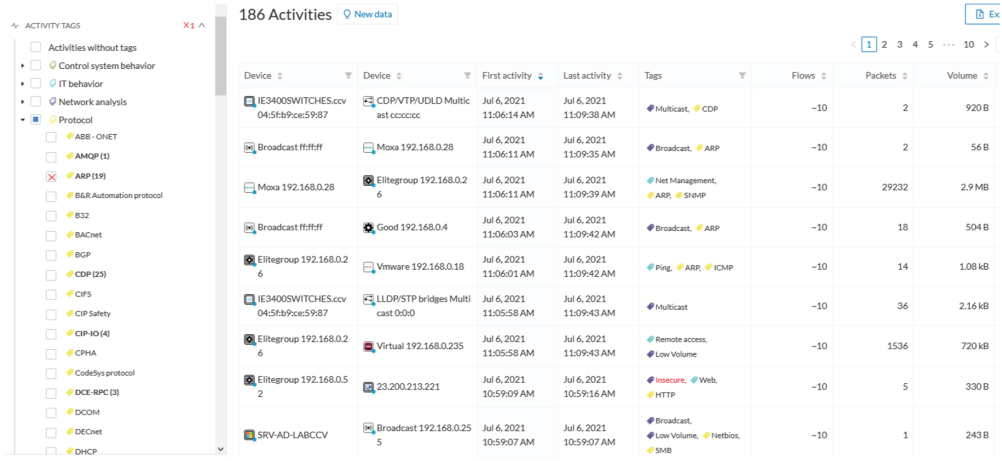


Activity Tags

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

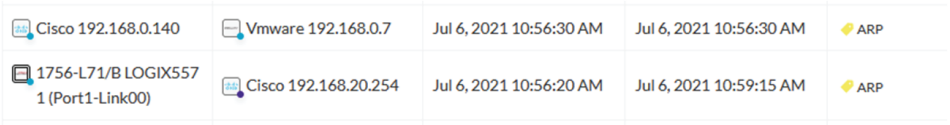
For example, if an activity has two tags, both tags need to be excluded to hide the activity.

Activity filter – negative filter 1



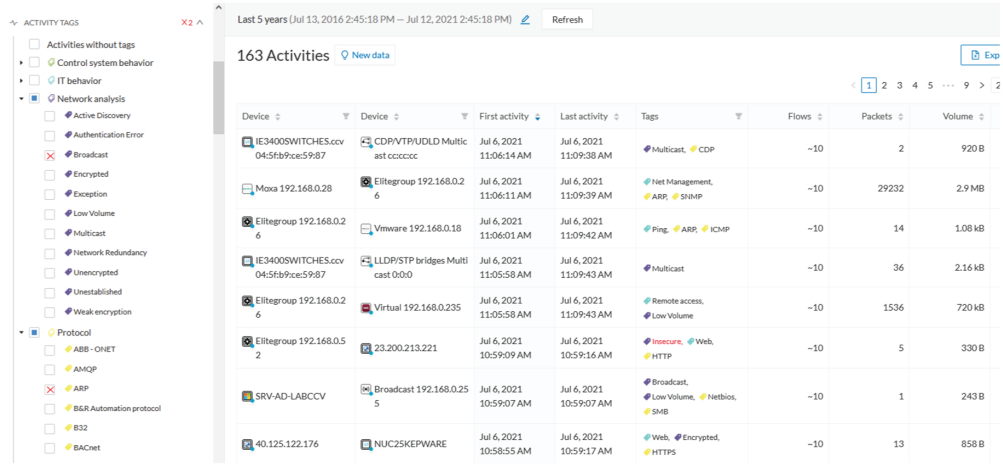
In the example above, several activities show because the ARP tag is present, as well as other **Activity tags**. There is no exact match. The activity below is hidden.

filter 2



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

Activity filter – negative filter 3



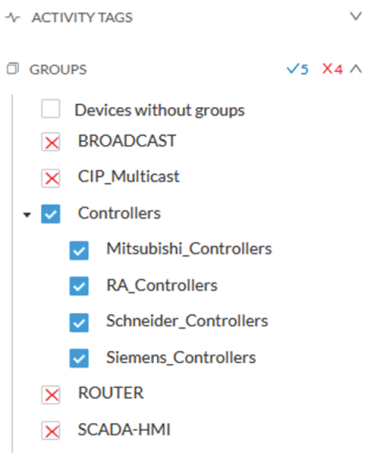
For very specific use cases, combine inclusive and exclusive tags. The above rules, for positive and negative selection, are combined, resulting in the following logic:

- Activities are selected as soon as at least one tag is in the set of included tags
- From this selection, activities which all tags are in the set of included AND excluded tags are hidden

Groups

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

Group filter



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

Sensors

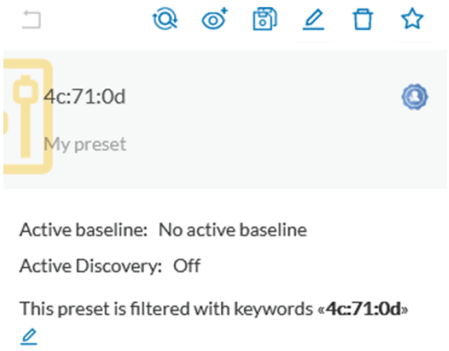
Filter Activities based on the sensor that analyzed the associated packets. For tags, use inclusive and exclusive filters. Usually, either option is used but not both. Inclusive: selects data coming from a set of sensors. Exclusive: Ignore the data from a set of sensors.

Sensor filter

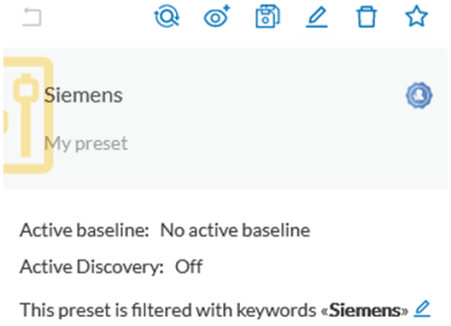
Keyword

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

Keyword = 4c:71:0d

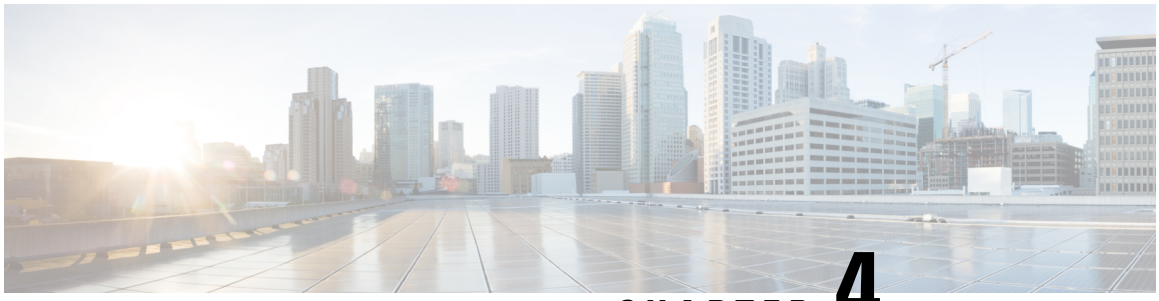


Keyword =siemens



Filter combination

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



CHAPTER 4

Component

Component

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

Some examples of icons:

Manufacturers' icons		
SIEMENS 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.

Multicast		

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

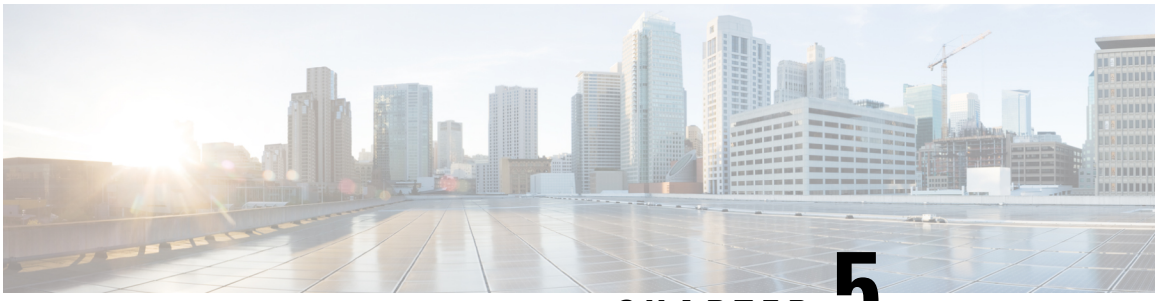
For more information, refer to the Device section.

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

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

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

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



CHAPTER 5

Device

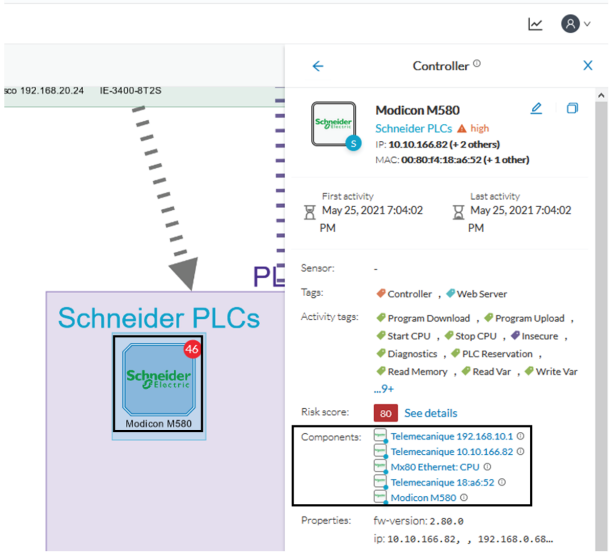
Device

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

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

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

Click on a Schneider controller. A right side panel opens showing its components.



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

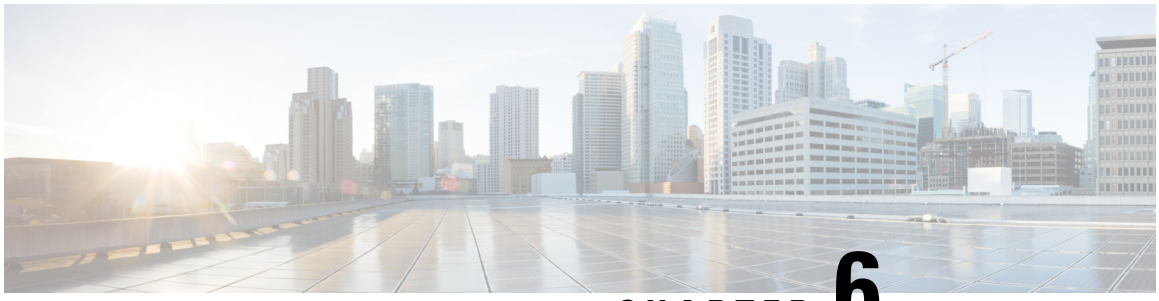
The list of a Rockwell Controller device's components (technical sheet > Basics > Components):

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.

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



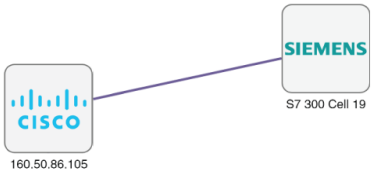
CHAPTER 6

Activity

Activity

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

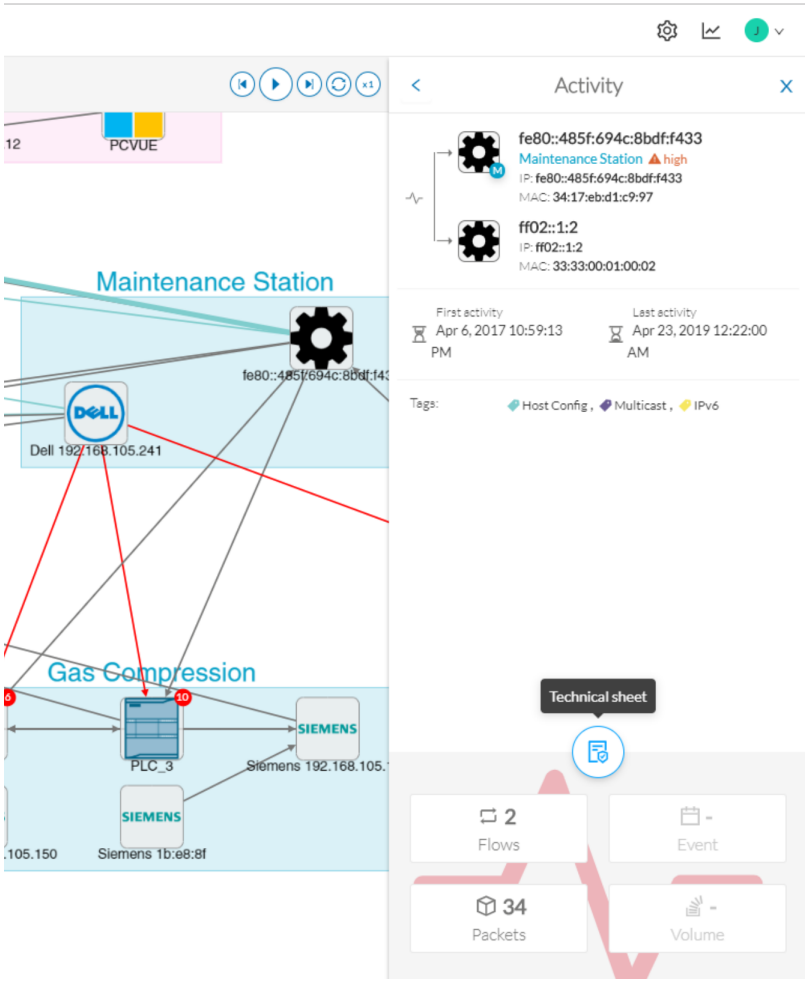
To access the map: Click **Explore > Control Systems Management > OT Activities >** > click a component on the map. The map appears.



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

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

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

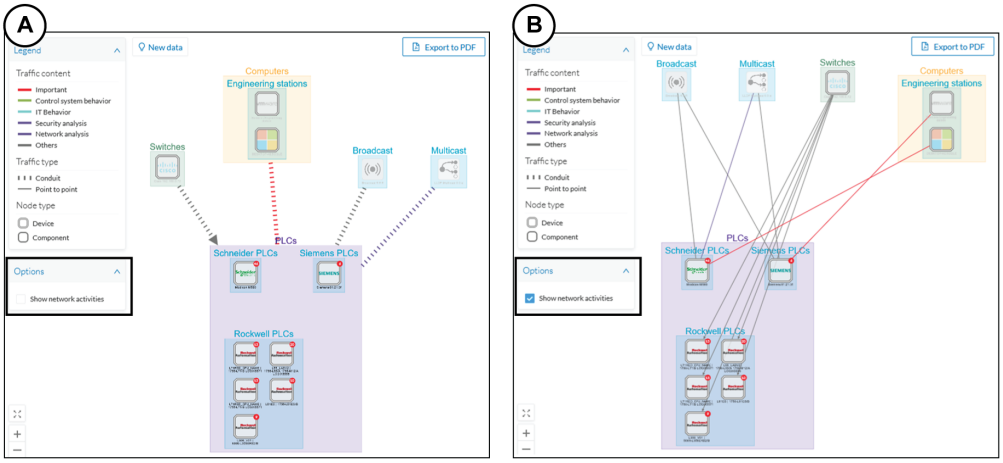


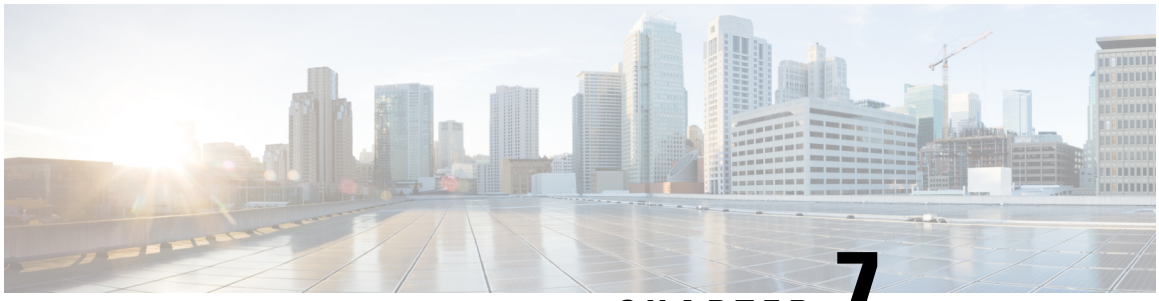
Devices or components with no activity does not mean that they did not have any interaction. In fact, a component can only be detected if it has been involved in a network activity (communication emission/reception). Lack of activity can mean that the other linked component is not part of the preset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

Aggregated activities or conduits

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

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


A
Legend
New data
Export to PDF
Traffic content
Important
Control system behavior
IT Behavior
Security analysis
Network analysis
Others
Traffic type
Conduit
Point to point
Node type
Device
Component
Options
Show network activities
Computers
Engineering stations
Switches
Broadcast
Multicast
PLCs
Schneider PLCs
Siemens PLCs
Rockwell PLCs
B
Legend
New data
Export to PDF
Traffic content
Important
Control system behavior
IT Behavior
Security analysis
Network analysis
Others
Traffic type
Conduit
Point to point
Node type
Device
Component
Options
Show network activities
Broadcast
Multicast
Switches
Computers
Engineering stations
PLCs
Schneider PLCs
Siemens PLCs
Rockwell PLCs



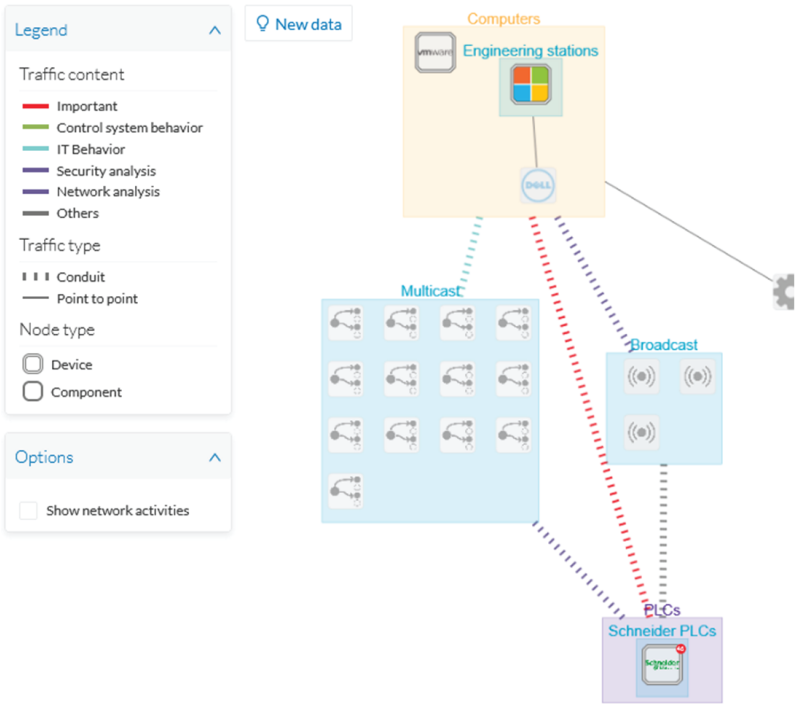
CHAPTER 7

Conduit

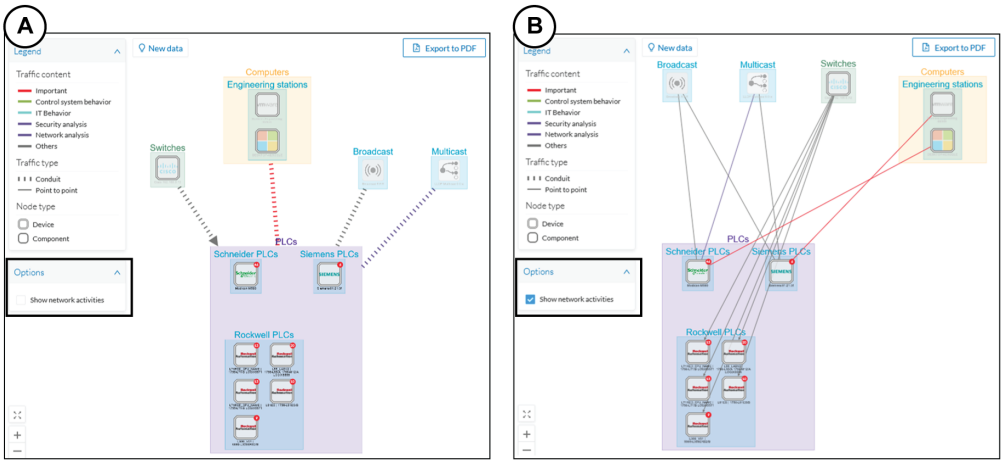
Conduit

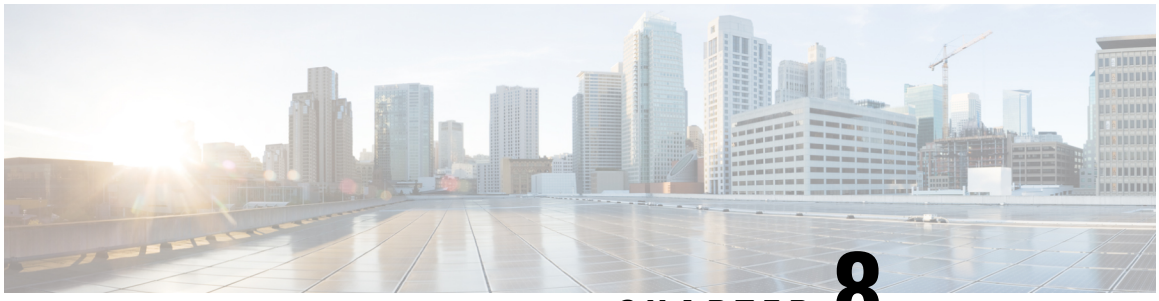
A conduit is the representation of the communications exchanged between two Component. It is an aggregation of Activity to facilitate visibility when devices and components are inside groups. The representation of conduits in Cisco Cyber Vision fit the 62443 standard which specifies policies and requirements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

On the map, a conduit displays as a thick, hyphenated line that links one group to another. If the source and destination groups are known, an arrow appears



Conduits view mode is enabled by default. Disable it by using the **Show network activities** checkbox at the lower left side of the map.





CHAPTER 8

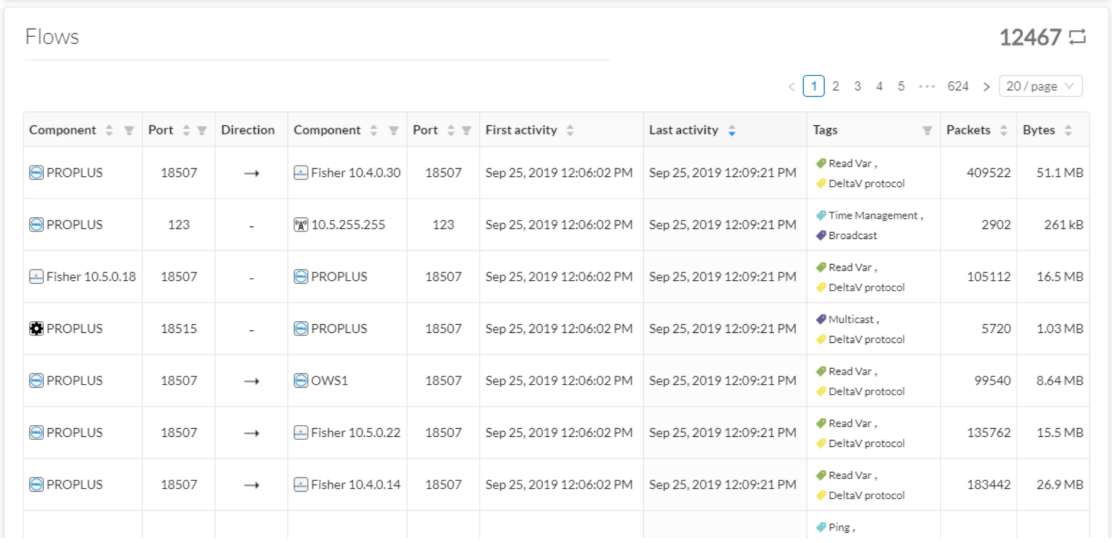
Flow

Flow

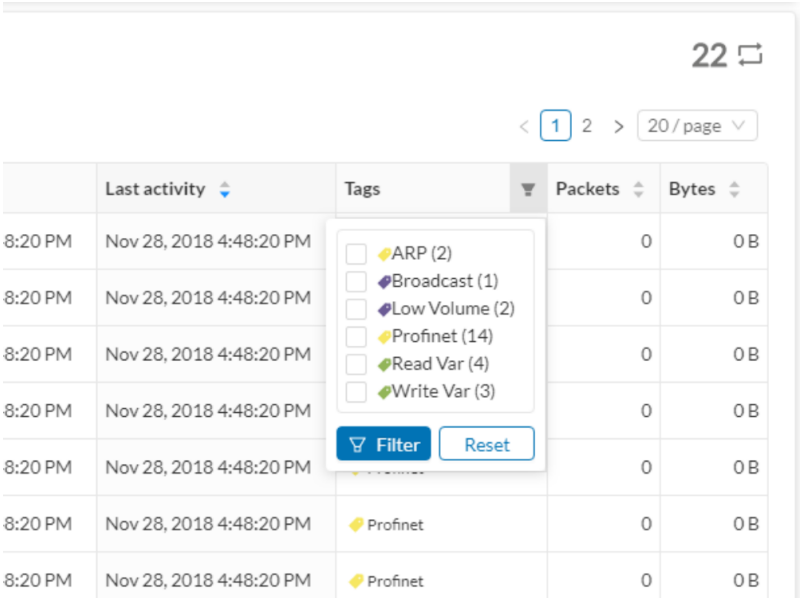
A flow is a single communication exchanged between two components. A group of flows forms an Activity, which is identifiable on the Map by a line that links one component to another.

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

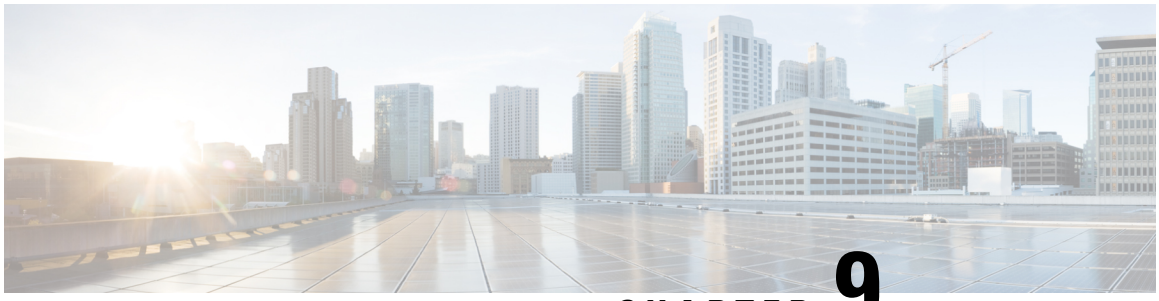
The Activity tab contains a list of flows which gives you detailed information about each single flow: number of flows in the activity, source and destination components (if known), ports used, first and last activity, and tags which characterize each flow.



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



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



CHAPTER 9

External communication

External communication

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

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

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

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

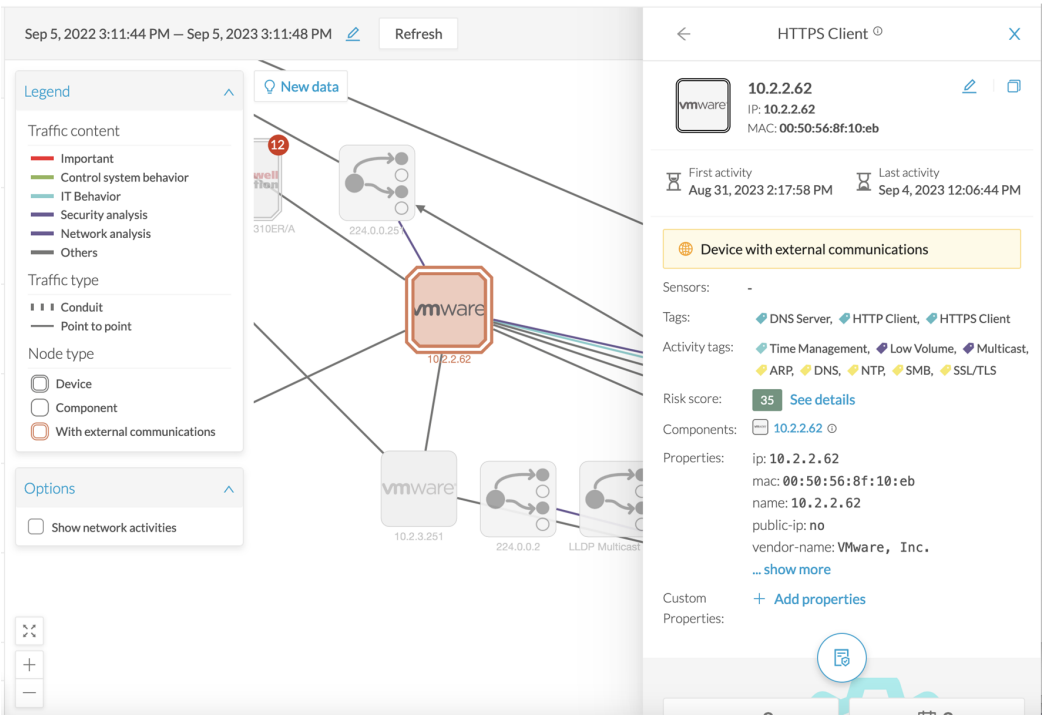
However, because sometimes public IP addresses are used in a private network of an industrial site, it is possible to manually define communications by declaring IP ranges as internal or external through the Network Organization administration page. For more information, refer to Cisco Cyber Vision GUI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

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

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

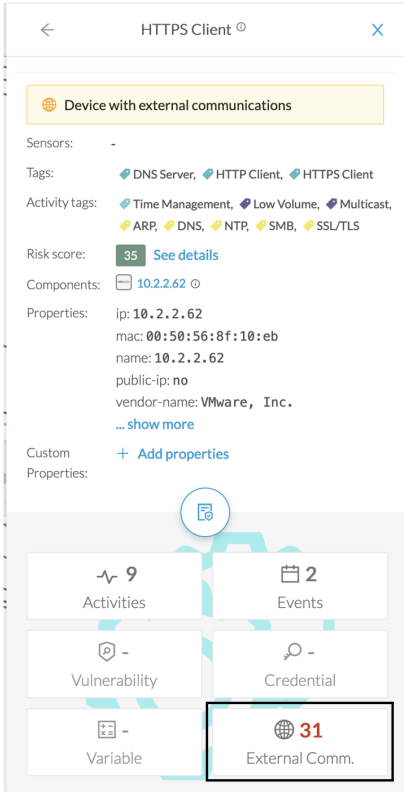
In the GUI, a component with external communications is shown as an icon bordered in orange, or a double orange border for a device.

A device with external communications in the Map:

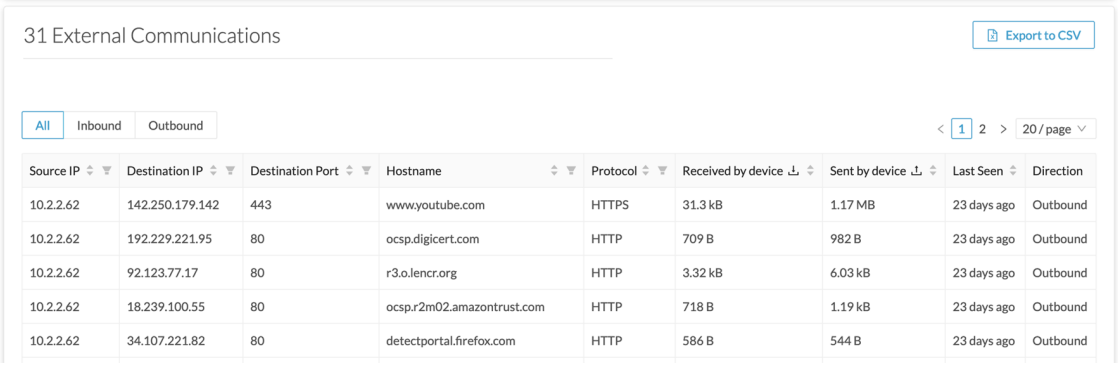


If you click on this component, its right side panel will appear. The **External Communications** button with the number of external communications will open the component's technical sheet directly on the external communications list.

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



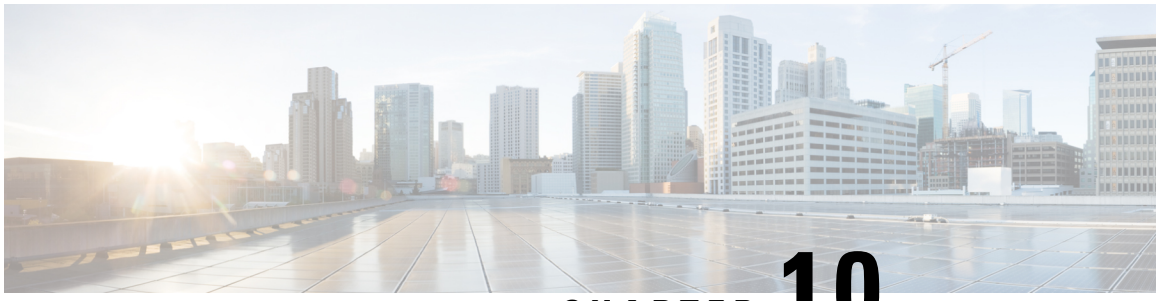
The external communications list in the device's technical sheet:



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

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

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

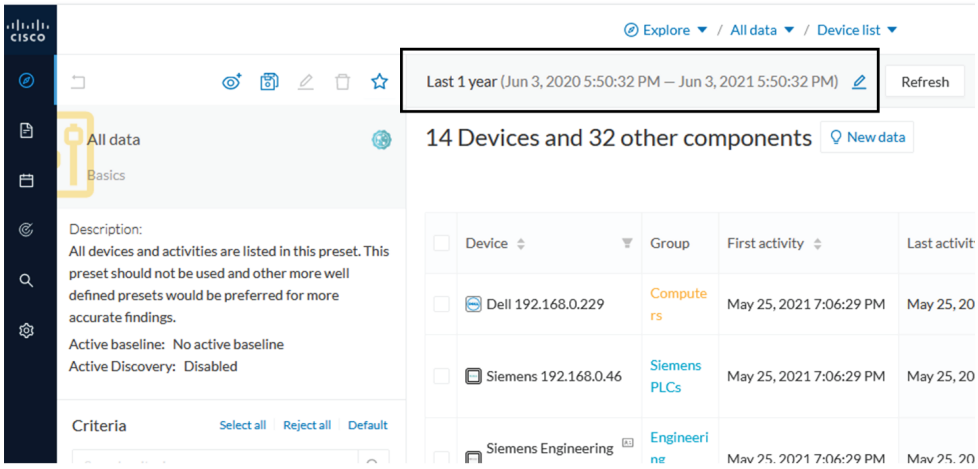


CHAPTER 10

Time span

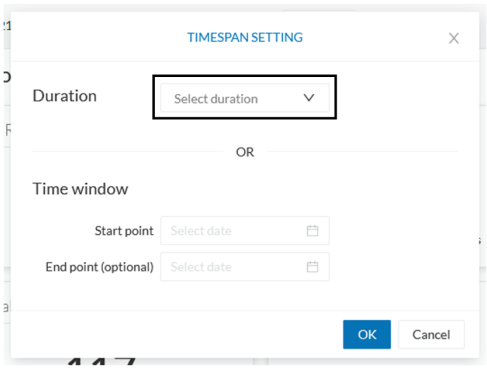
Time span

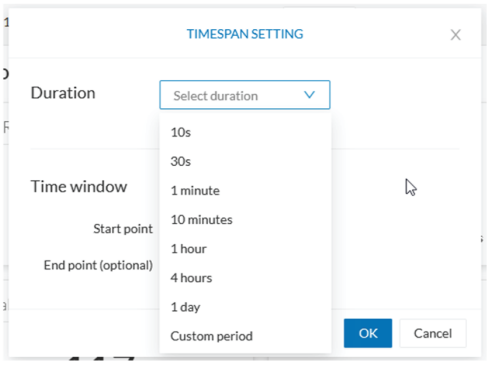
Cisco Cyber Vision is a real-time monitoring solution. The views are continuously updated with network data. You can view the network activity during a defined period of time by selecting a **time span**. Use **time span** to filter data, based on the time you select. This feature is available on each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



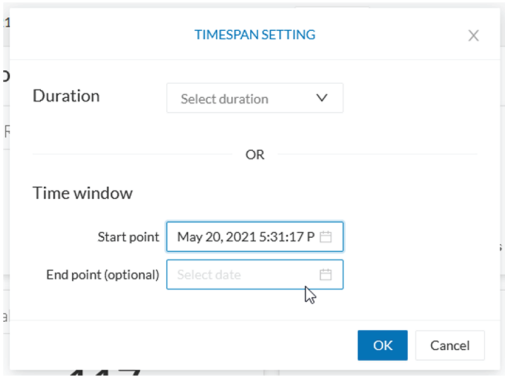
To set a time span: Click the pencil icon.

- To set a duration, select time (from 10 seconds to 1 day) or a custom period up to the present.



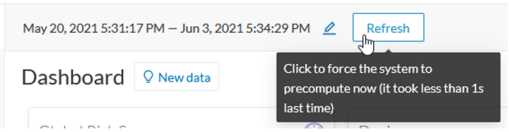


- To set a time window, select a start date and (optionally) an end date. If you don't select an end date, the end date will set to now.



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

Click **Refresh** to compute network data.



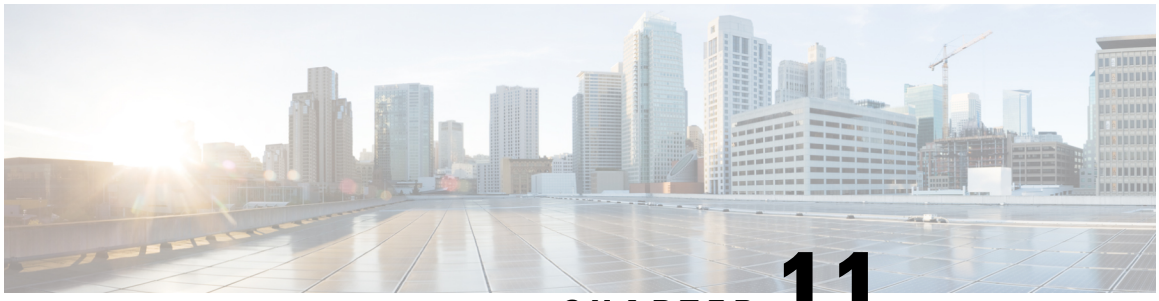
Note No data display is often due to a time span set on an empty period. Remember to first set a long period of time (such as 12 months) before troubleshooting.

Recommendations:

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

Adjust the time frame for the following:

- Set a period of a few minutes to have more visibility on what is *currently* happening on the network.
- Set a period of a few hours to have a view of the daily activity or set a time to see what has happened during the night, the weekend, etc.
- Set limits to view what happened during the night/weekend.
- Set limits to focus on a time frame close to a specific event.

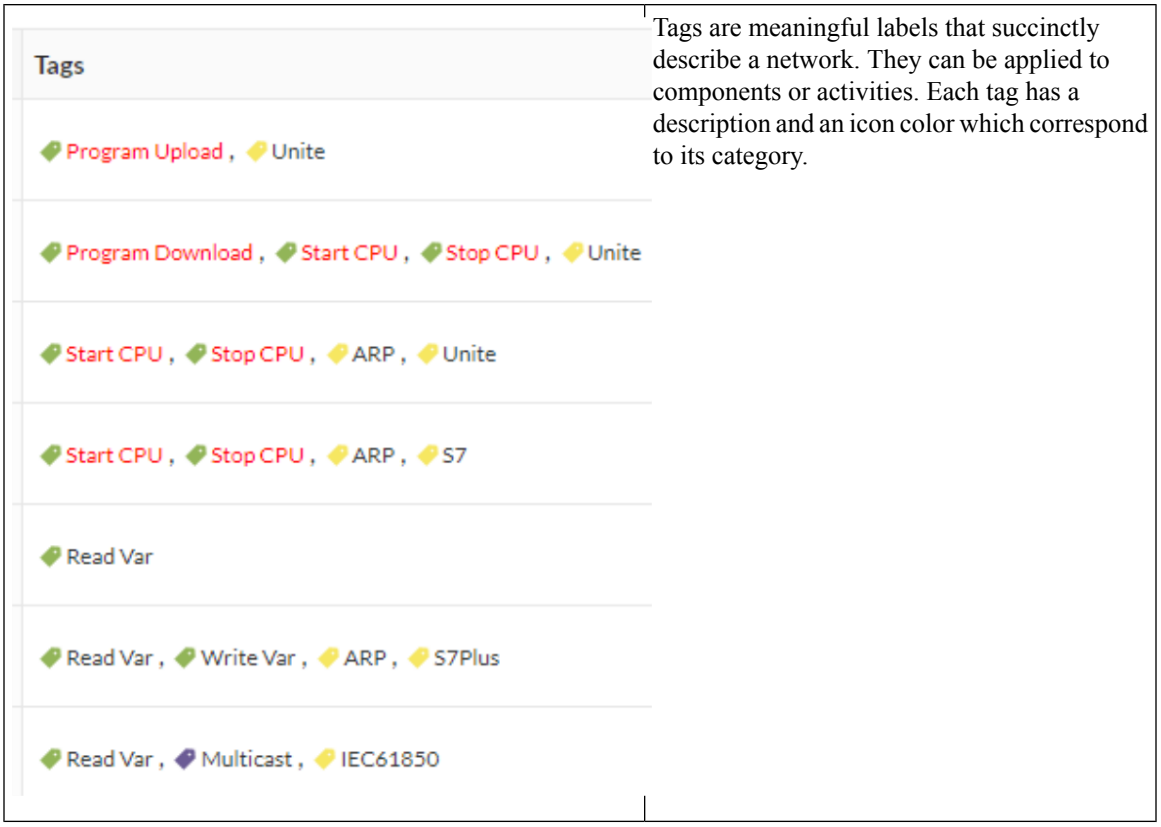


CHAPTER 11

Tag

Tags

Definition of Tags

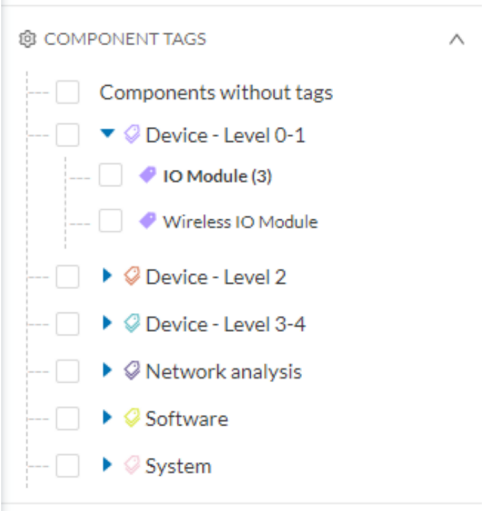


Tags are metadata on Device and Activity. Tags are generated according to the Properties of components. There are two types of tags:

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

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

The device tags categories (Device - Level 0-1, Device - Level 2, etc.) and some tags (IO Module, Wireless IO Module) in the filtering area:



Note Device levels are based on the definitions from the ISA-95 international standard.

Tag Use

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

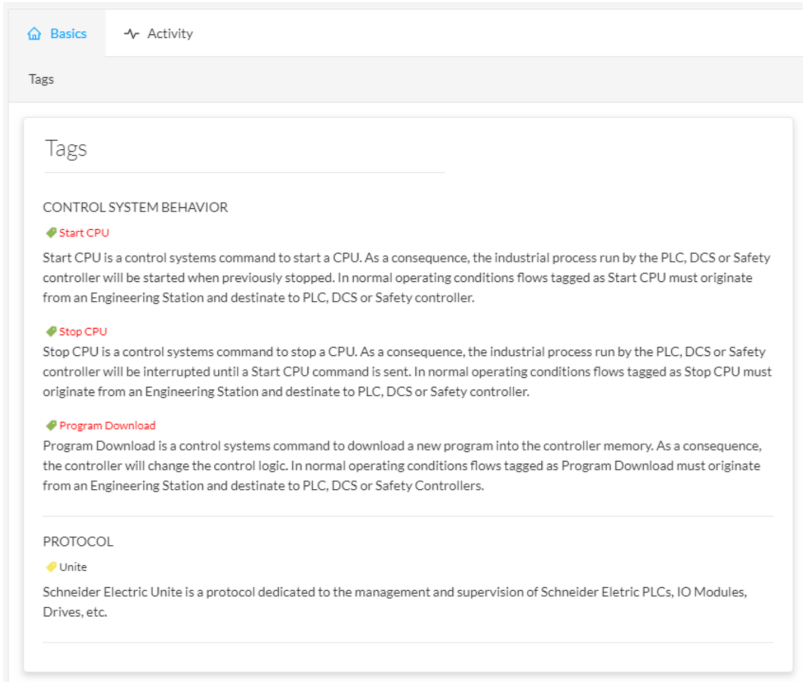
Use tags to define behaviors (i.e., in the Monitor mode) inside an industrial network when combined with information like source and destination ports and flow properties.

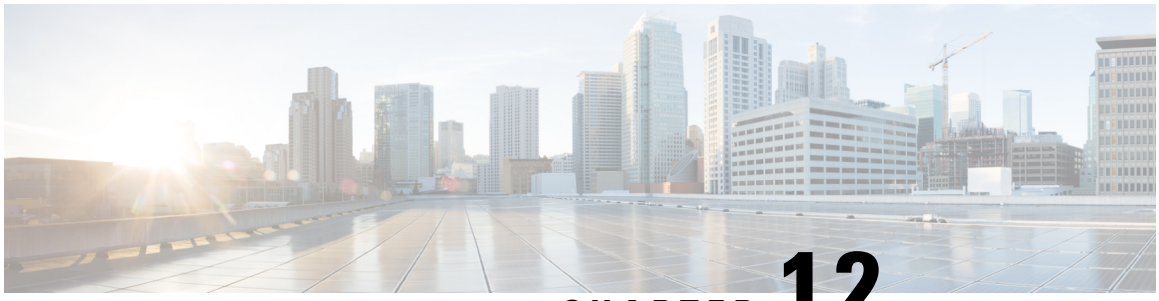
Tag Location

Find tags almost everywhere in Cisco Cyber Vision, from criteria, which are based on tags to filter network data, to the different views available. Views filter and use tags differently. For example, the dashboard shows the preset's results, showing tags over other correlated data. The device list highlights devices, over data like tags. For more information, see the different types of view in Navigating through Cisco Cyber Vision, on page 69.

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

Below is an example of tag definitions.


Basics
Activity
Tags
Tags
CONTROL SYSTEM BEHAVIOR
Start CPU
Start CPU is a control systems command to start a CPU. As a consequence, the industrial process run by the PLC, DCS or Safety controller will be started when previously stopped. In normal operating conditions flows tagged as Start CPU must originate from an Engineering Station and destinate to PLC, DCS or Safety controller.
Stop CPU
Stop CPU is a control systems command to stop a CPU. As a consequence, the industrial process run by the PLC, DCS or Safety controller will be interrupted until a Start CPU command is sent. In normal operating conditions flows tagged as Stop CPU must originate from an Engineering Station and destinate to PLC, DCS or Safety controller.
Program Download
Program Download is a control systems command to download a new program into the controller memory. As a consequence, the controller will change the control logic. In normal operating conditions flows tagged as Program Download must originate from an Engineering Station and destinate to PLC, DCS or Safety Controllers.
PROTOCOL
Unite
Schneider Electric Unite is a protocol dedicated to the management and supervision of Schneider Eletric PLCs, IO Modules, Drives, etc.



CHAPTER 12

Property

Properties

Property Definition

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

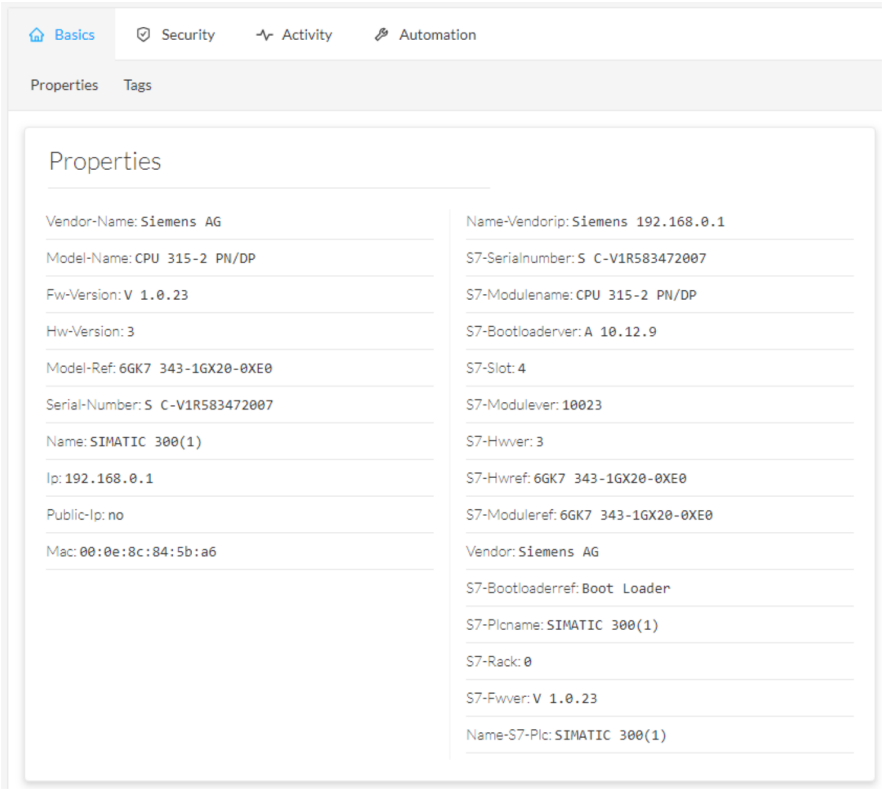
Property Use

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

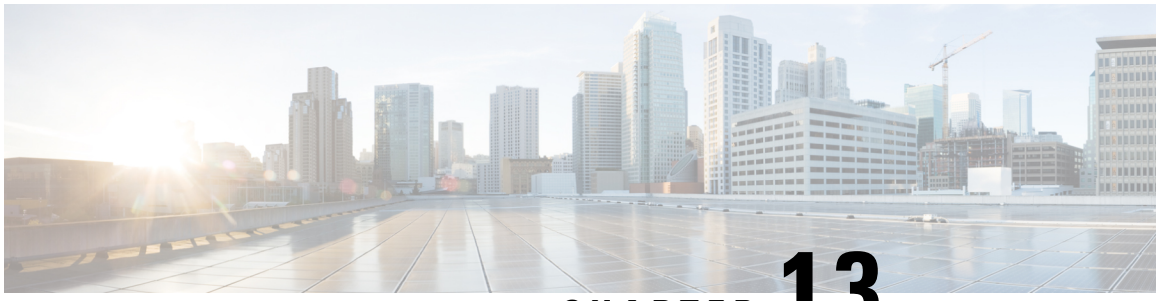
Property Location

View Properties from devices and components Detail panel and Technical sheets under the **Basics** tab.

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



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



CHAPTER 13

Risk score

Risk score

Risk Score Definition

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

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

Risk scores apply to the following:

- Filter criteria
- Device list
- Device technical sheet
- Device risk score widget (Home page)
- Preset highlight widget (Home page)

Risk Score Use

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

Proposed solutions are:

- Patch a device to reduce the surface of attack

- Remove vulnerabilities
- Update firmware
- Remove unsafe protocols whenever possible (e.g., FTP, TFTP, Telnet),
- Install a firewall
- Limit communications with the outside by removing external IPs

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

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

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

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

Risk Score Computation

Risk score is computed as follows:

Risk = Impact x Likelihood

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

- Device tags: Some device types are more critical. Each device type (or device tag) or device tag category is assigned an industrial impact score by Cisco Cyber Vision. For example, the device is a simple IO device that controls a limited portion of the system or it is a Scada that controls the entire factory. These will not have the same impact if they are compromised.
- You effect the device impact by moving it into a group and setting the group's industrial impact (from very low to very high).

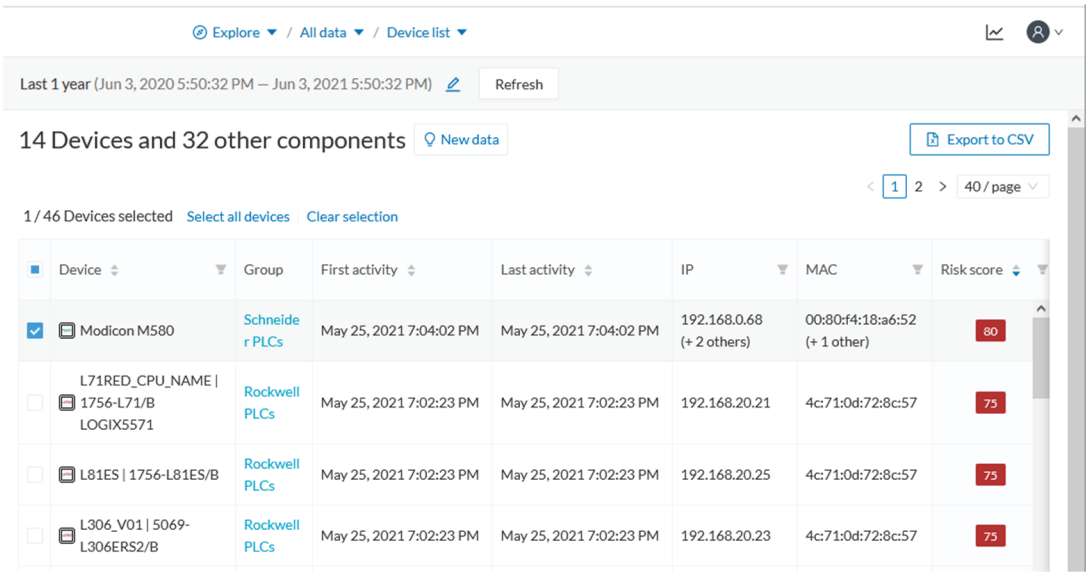
Likelihood is the probability of this device being compromised Likelihood of risk depends on the following:

- Device activies and the activity tags. Some protocols are less secure than others. For example, Telnet is less secure than ssh.
- The exposure of the device communicating with an external subnet.
- Device vulnerabilities, taking into account their CVSS scoring.

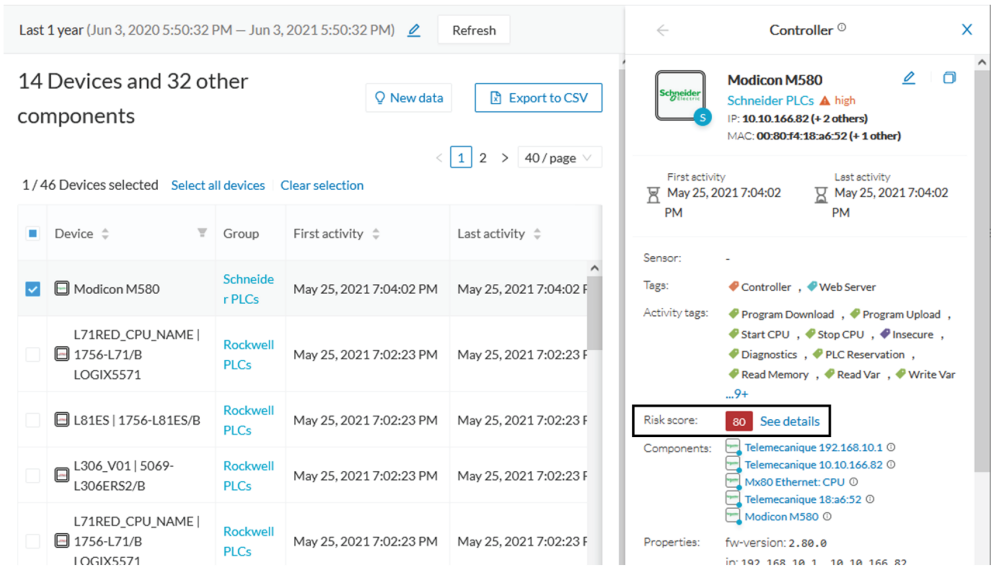
For detailed information about a risk, see **Details** tab inside the technical sheet.

How to take action:

1. In the top menu banner, click **Explore > All data > Dashboard > Device List**.



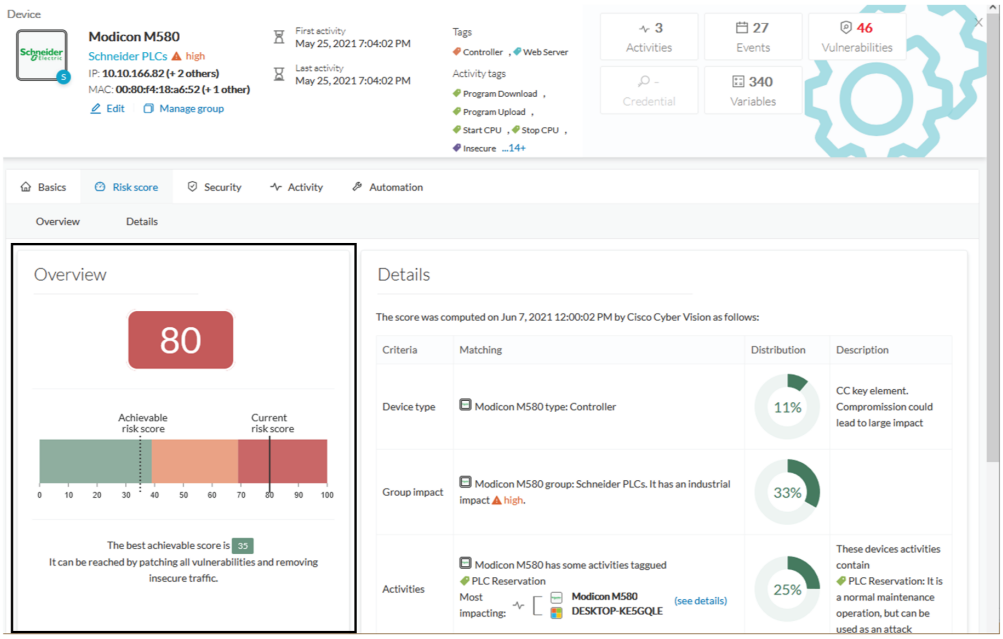
2. In the **Device List**, **Risk score** column, click the **Sort arrow** to get the highest risk scores.
3. Click a device in the list. Its right side panel opens.
4. In **Risk score**, click the **See details** link.



The technical sheet opens.

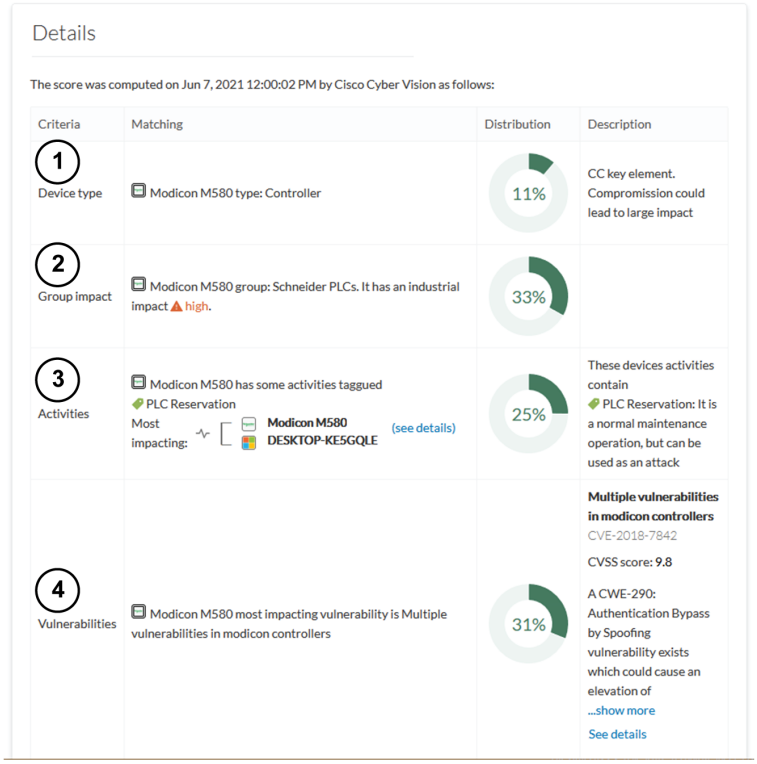
In the **Overview** tab, the **Current** risk score and the **Achievable** risk score display.

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



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

Device type and **Group impact** affect the risk impact variable. **Activities** and **Vulnerabilities** affect the risk likelihood.



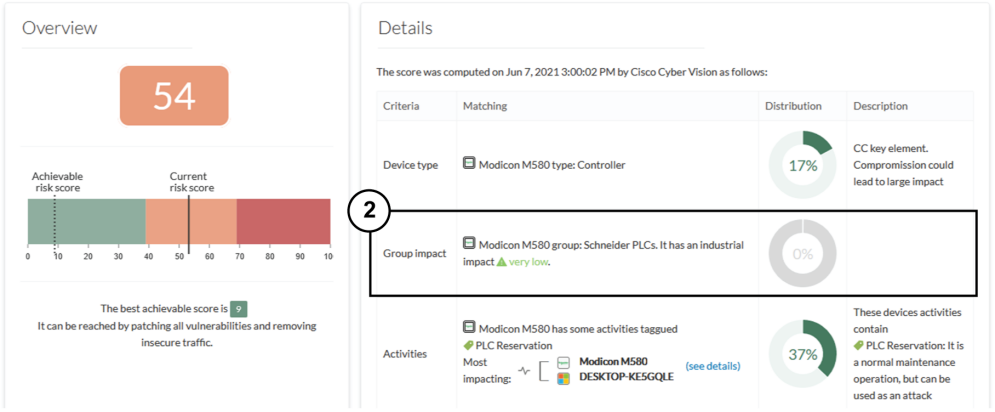
This page shows the last time the risk score was computed by Cisco Cyber Vision. Risk score computation occurs once an hour. To force immediate computation, use the following command on the Center shell prompt:

```
sbs-device-engine
```

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

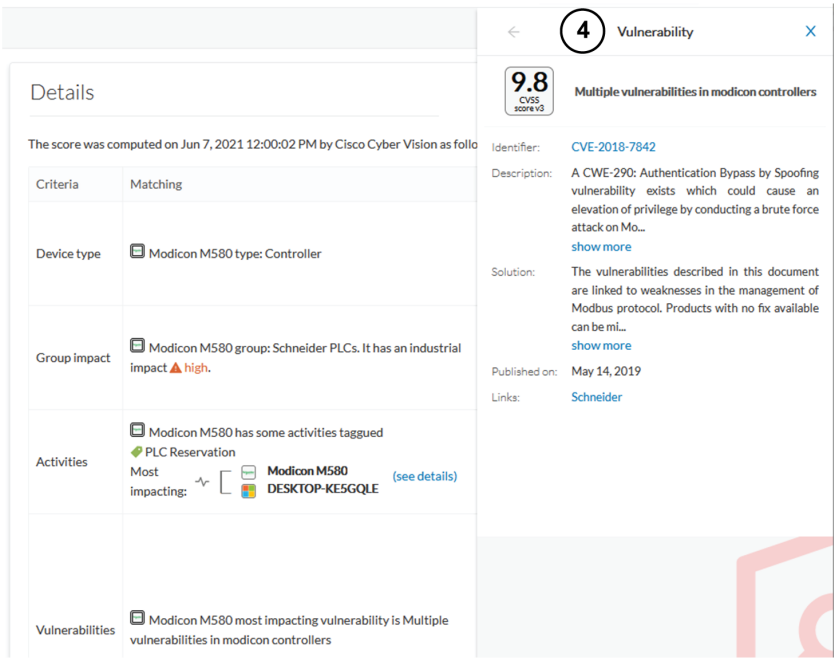
- **Device type**: Each device type corresponds to a Tags detected by Cisco Cyber Vision. No action is required at the device type level because each device tag is assigned a risk score by default.
- **Group impact**: Action is possible if the device belongs to a group. Decrease the impact by lowering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

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

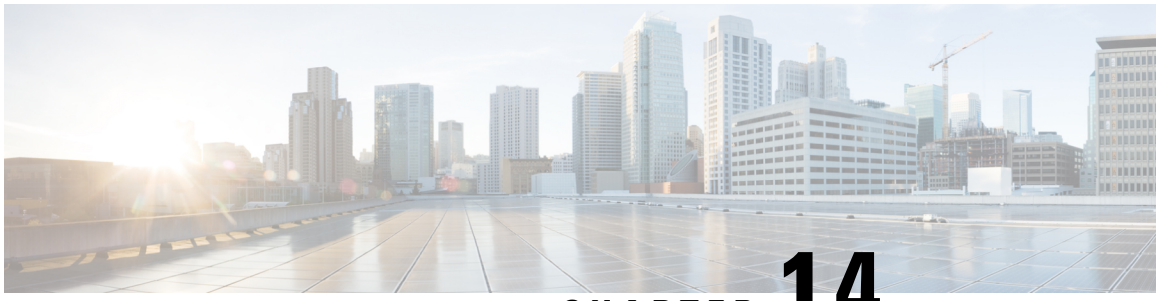


Note The new industrial impact will factor into the next risk score computation (once an hour).

- **Activities**: The most impactful activity tag displays. To lower the risk, remove all potential insecure network activities.
- **Vulnerabilities**: Click the **See details** link for more information about how to patch the vulnerabilities and so reduce the device risk score.



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



CHAPTER 14

Vulnerability

Vulnerability

Definition of Vulnerabilities

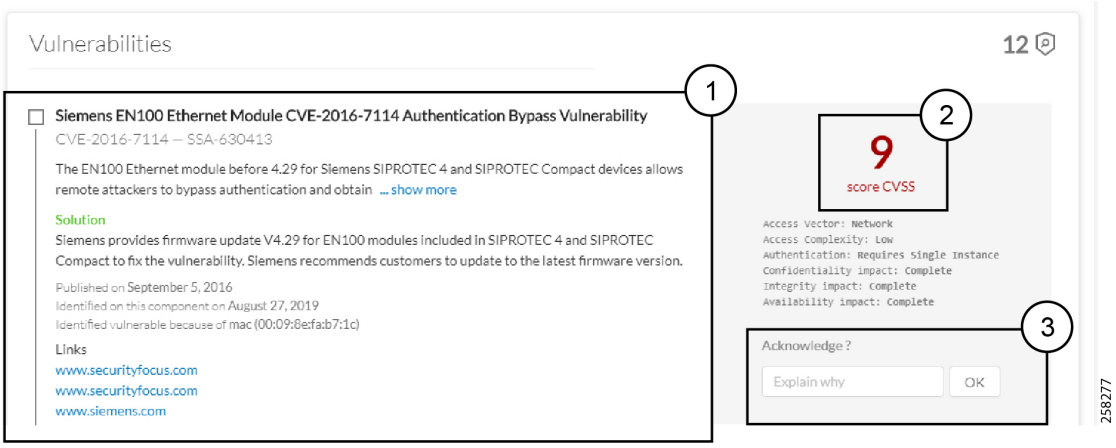
Vulnerabilities are weaknesses detected on devices that can be exploited by a potential attacker to perform malevolent actions on the network.

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

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

Vulnerability Use

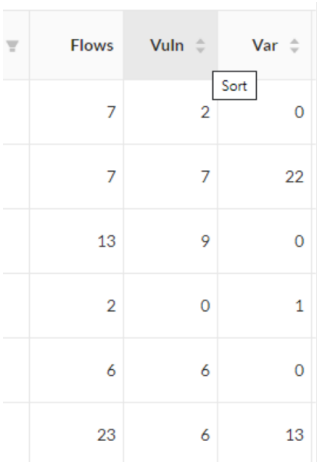
Below is an example of a Siemens component's vulnerability. See the technical sheet, Security tab.



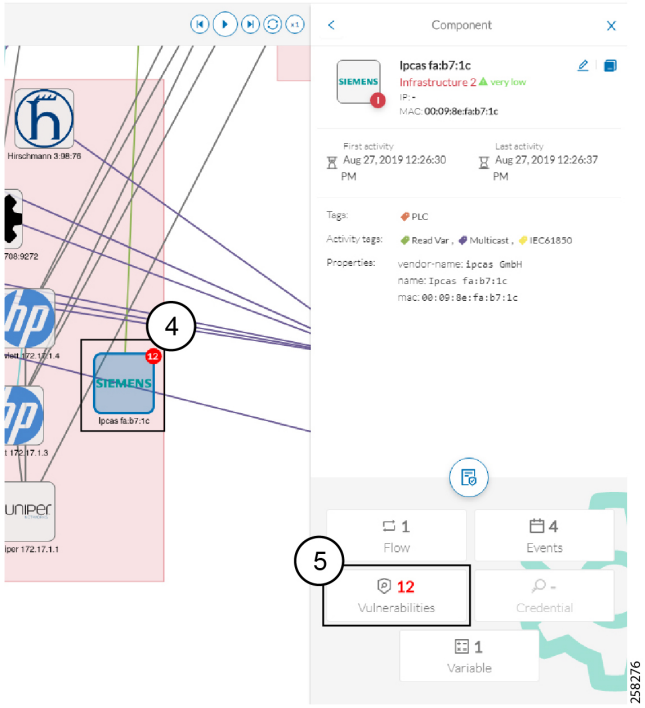
1. **Information** displayed about vulnerabilities includes the following: vulnerability type and reference, possible consequences, and solutions or actions to take on the network. Often, upgrading the device firmware alleviates a vulnerability. Links to the manufacturer website are also available.
2. A **score** reports the severity of the vulnerability. The score is calculated upon criteria from the Common Vulnerability Scoring System (CVSS). Criteria examples are: the ease of attack, its impacts, the importance of the component on the network, and whether actions can be taken remotely or not. Scores range from 0 to 10, with 10 being the most critical score.
3. **Acknowledge** a vulnerability if you don't want to be notified about it anymore. For example: a PLC is detected as vulnerable but a firewall or a security module is placed ahead. The vulnerability is mitigated. Cancel an **Acknowledgment** at any time. Only the Admin, Product, and Operator users can access **Vulnerabilities Acknowledgment/Cancelation**.

Vulnerability Location

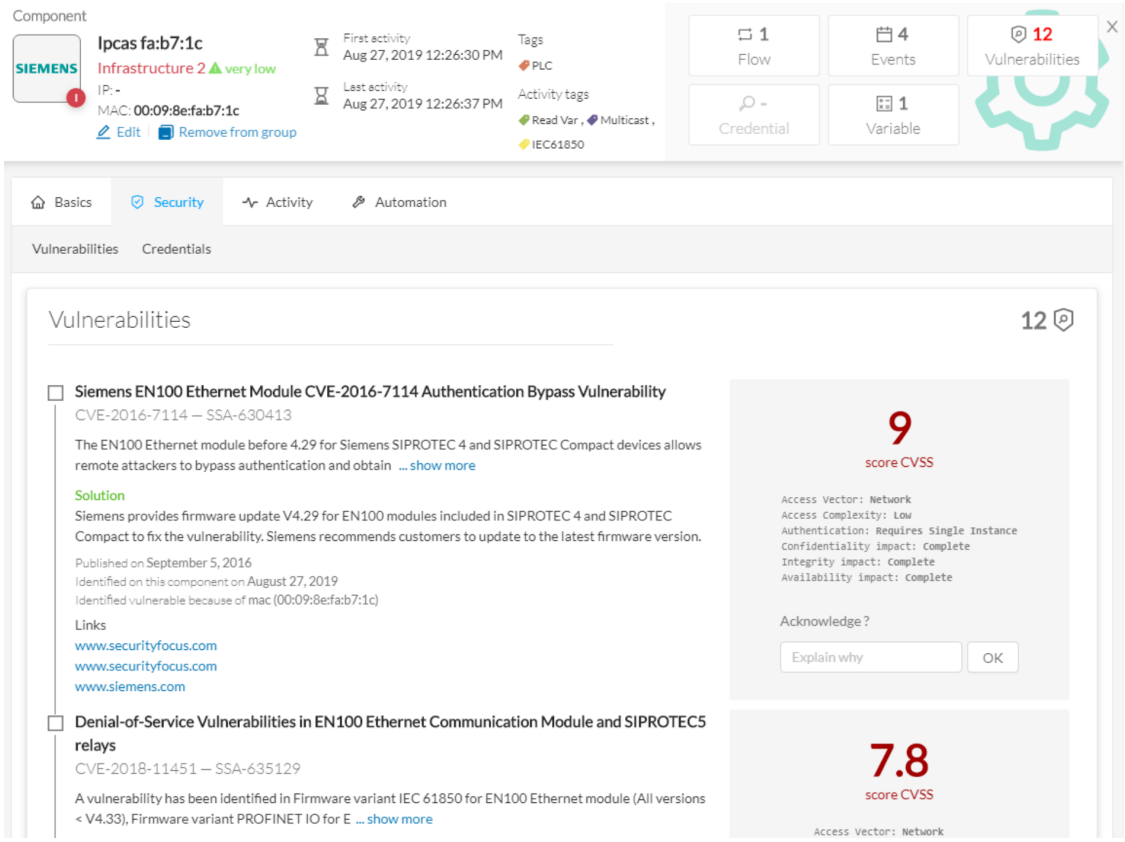
Access Vulnerabilities in any of the following ways: click **Explore > All Data > Vulnerabilities**, use Vulnerabilities of a preset, or through the **Device list**. Use the **Sort arrows** to view the vulnerability column.



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

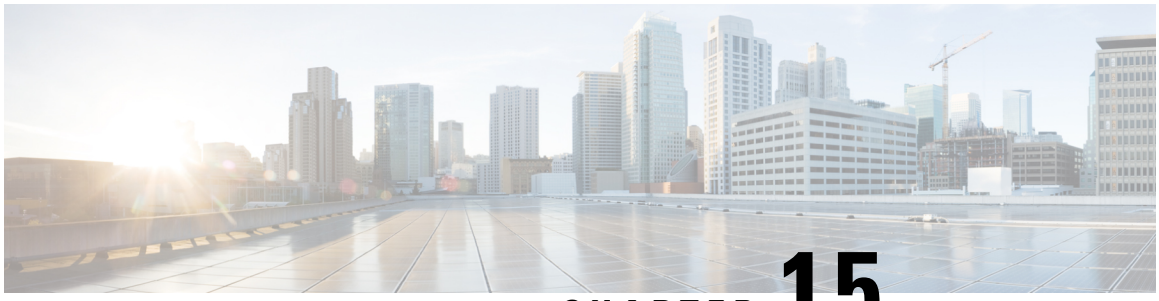


Click the **Vulnerabilities** in red **(5)** and the device or component's technical sheet opens.



Events

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



CHAPTER 15

Events

Events

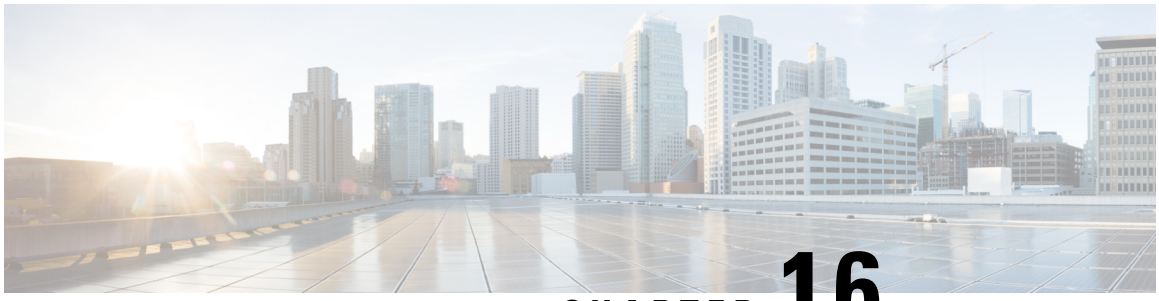
Use **Events** to identify and track significant activities on the network. Events can be an activity, a property, or a change--whether it is software or hardware parts.

The following are event examples:

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

View **Events** 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). The severity level (Critical, High, Medium and Low) of an Event is customizable through the the Events administration page. For more information, refer to the Cisco Cyber Vision Administration Guide.



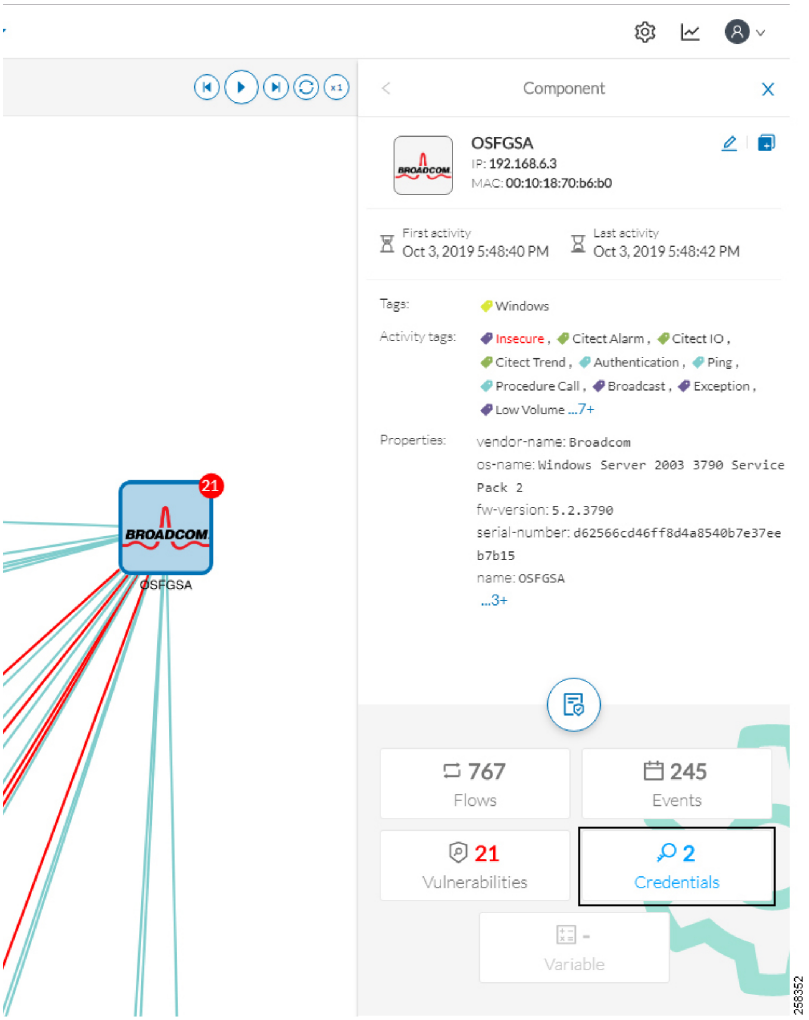
CHAPTER 16

Credential

Credentials

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

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

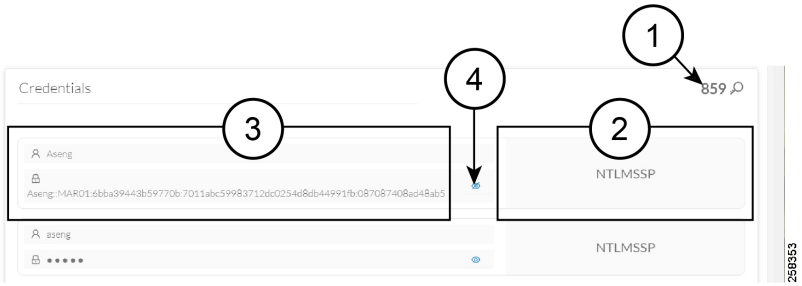


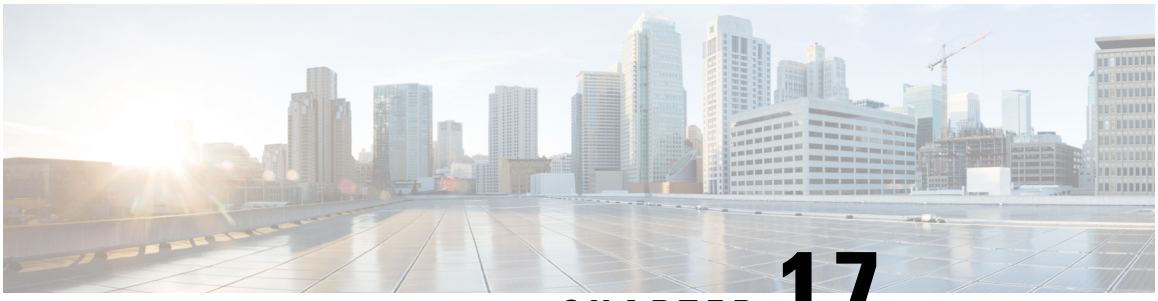
Credential frames are extracted from the network in Deep Packet Inspection. Use the technical sheet of a compoent to access **Credentials**. Click the **Security** tab.

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

An unsafe password:

A hashed password:





CHAPTER 17

Variable access

Variable accesses

Variable Definition

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

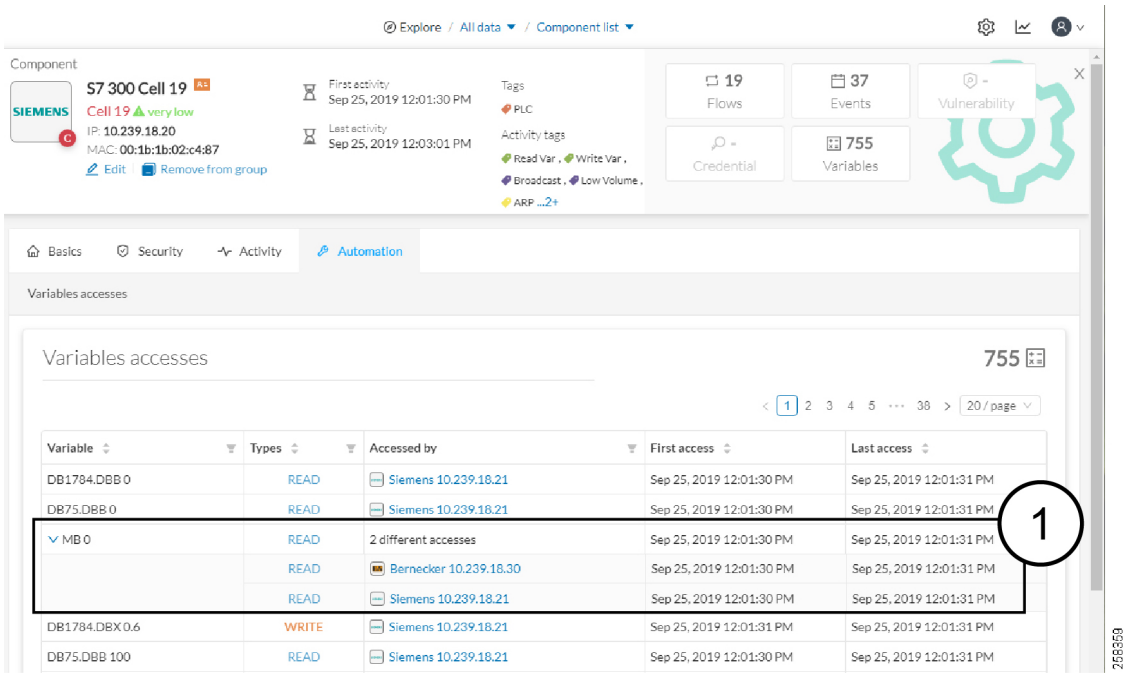
For example, a variable can be the ongoing temperature of an industrial oven. This value is stored in the oven's PLC and can be controlled by another PLC or accessed and supervised by a SCADA system. The same value can be read by another PLC which controls the heating system.

Variable Use

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

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

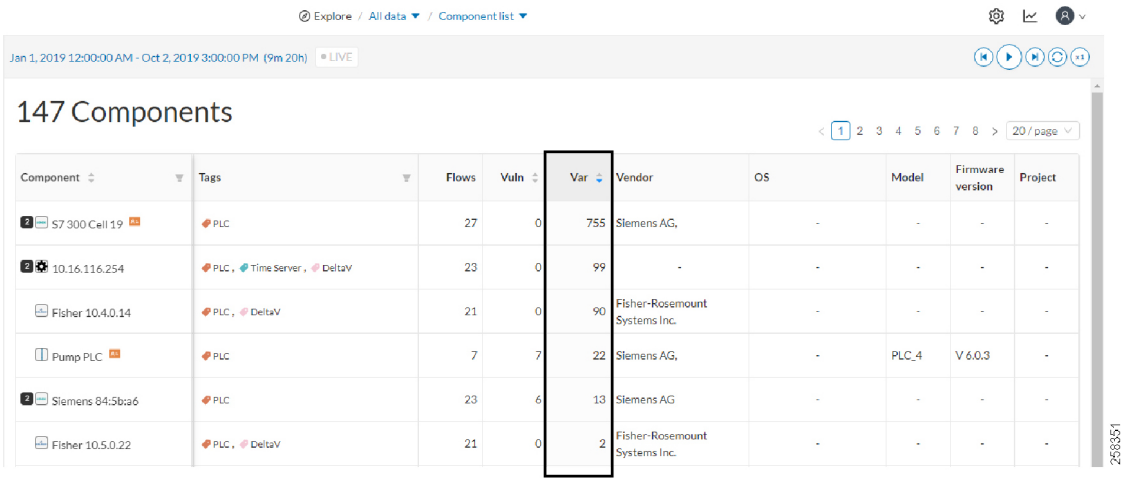
- The name of the variable
- Its type (READ or WRITE) but not the value itself
- Which component accessed the variable
- The first and last time the component accessed the variable



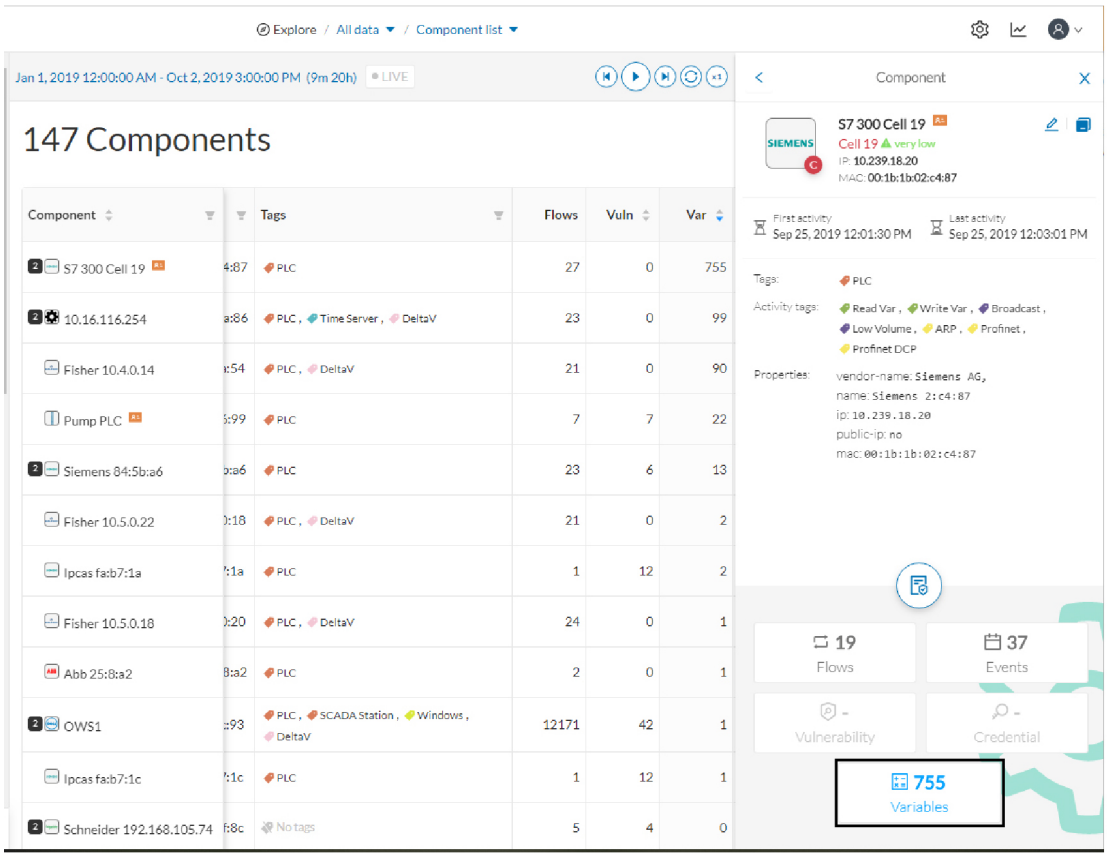
The entry "2 different accesses" **(1)** indicates that two components have read the variable.

Variable Location

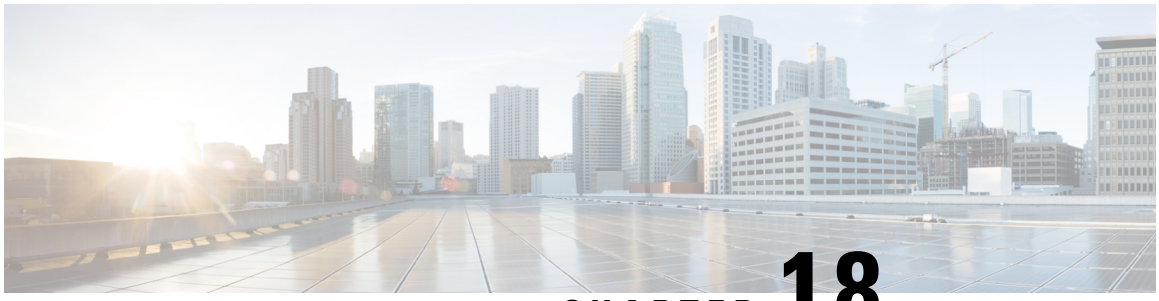
View the number of variable accesses per component on the component list view. Sort the var column by ascending or descending number.



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



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

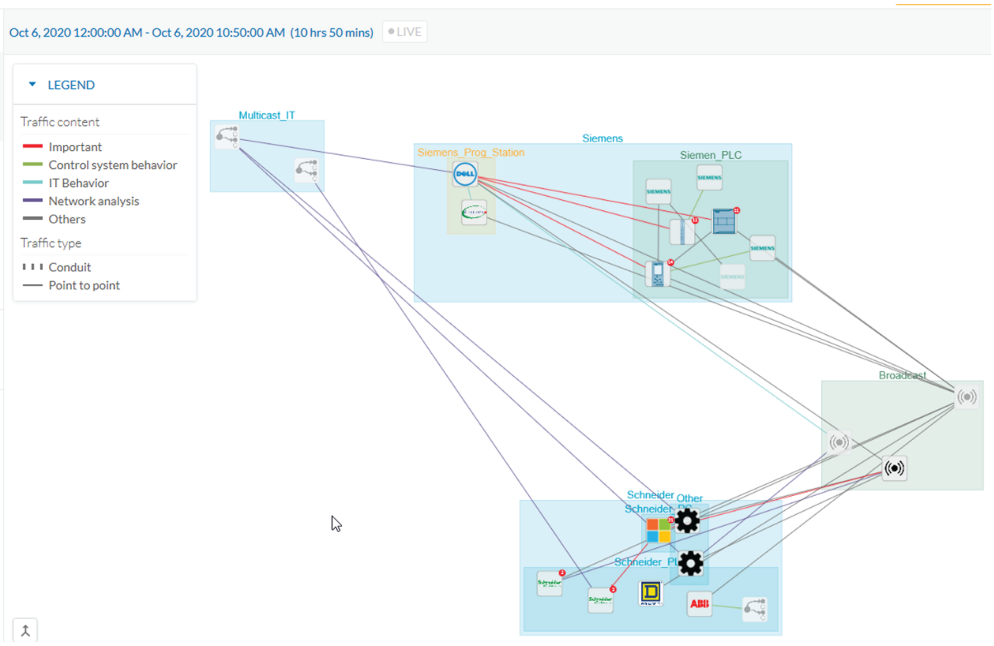


CHAPTER 18

Group

Creating and customizing groups

Accessibility: Admin, Product and Operator users



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

To access this feature, click **Explore > All Data > Device list (or Map)**.

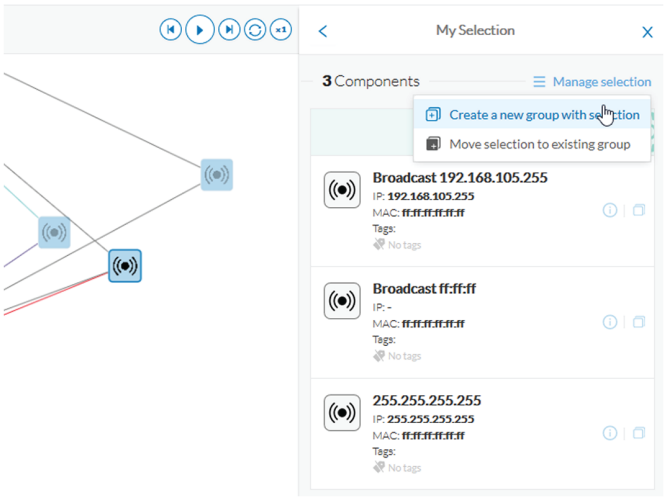
To create a group:

Procedure

Step 1 Select device(s) or components from the **Map** or the **Device list** interface.

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

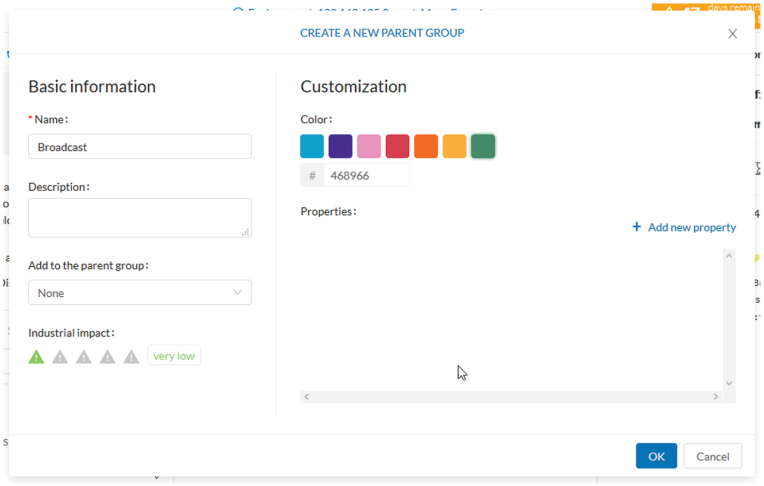
A **My Selection** panel opens on the right.



Step 2 Click **Manage selection**.

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

A Create a new parent group window appears.



Step 4 Name the new parent group. Customize the group by giving it a description, define its industrial impact (e.g., a PLC that controls a robotic arm is highly critical), change its color and add properties.

Step 5 Add the group to a parent group, if already created.

To create a parent group:

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

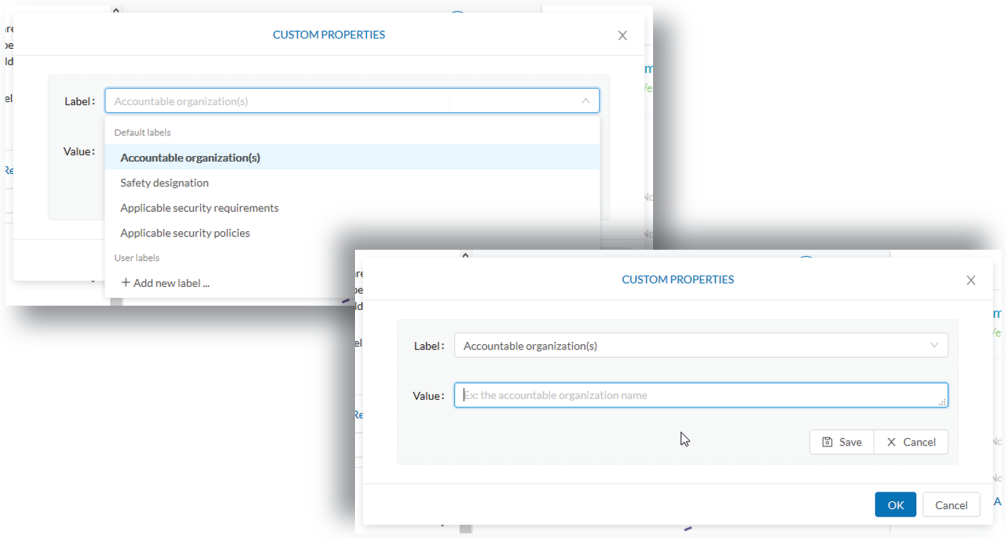
- Select two groups and create a group, as indicated above.
- Select a device or a component and move it into a group. Use the **Move selection to existing group** button.
- Select a group and move it to another group. Use **Move selection to existing group**.

Add group properties

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

To add properties to a group:

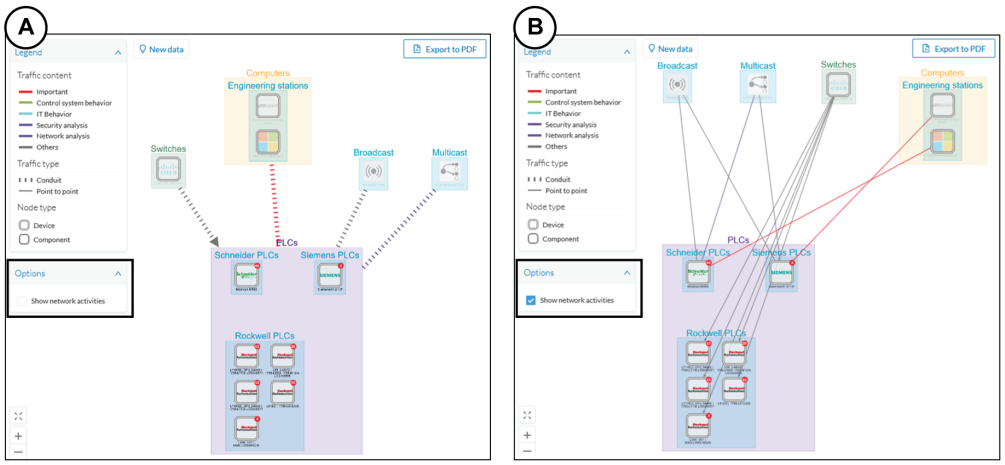
- Select a group in the map and click **Edit** or **Add properties**.
- Choose/define a label and add a value.



Aggregated activities are conduits

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

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



Group Lock/Unlock

Locking a group:

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

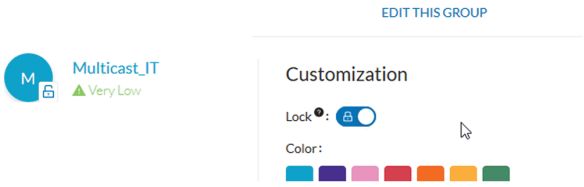
To switch on/off the **Lock** icon:

Step 6 Click a group. The **Group** details panel opens.

Step 7 Click the **Lock** icon on the Group's icon.

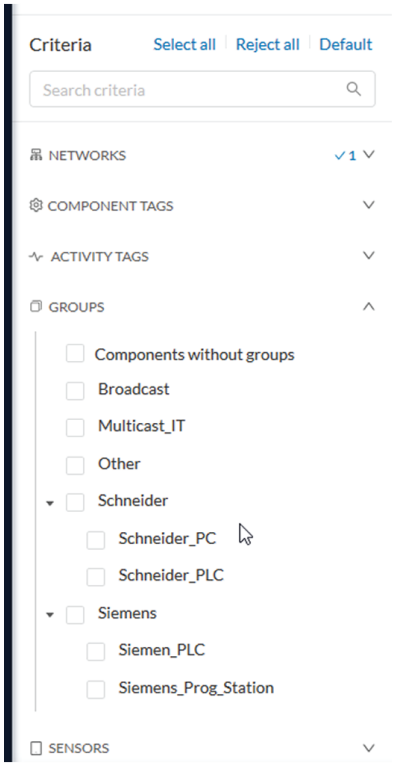
or

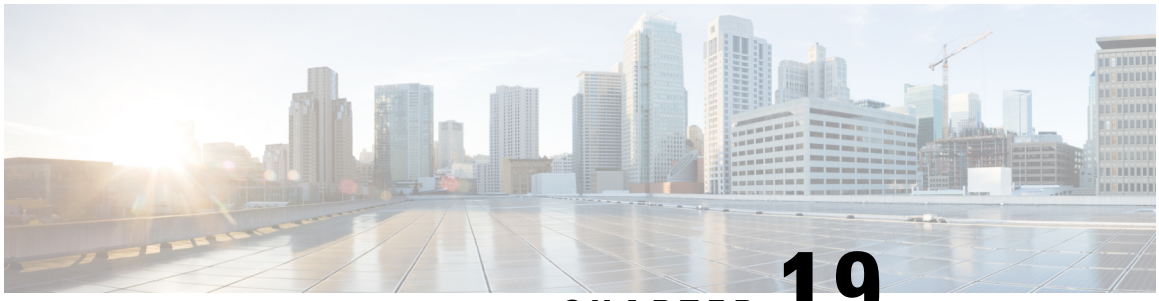
Click the **Edit** icon on the **Group** details panel and toggle on/off the **Lock** icon.



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

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


Criteria
Select all
Reject all
Default
Search criteria
NETWORKS
1
COMPONENT TAGS
ACTIVITY TAGS
GROUPS
Components without groups
Broadcast
Multicast_IT
Other
Schneider
Schneider_PC
Schneider_PLC
Siemens
Siemen_PLC
Siemens_Prog_Station
SENSORS



CHAPTER 19

Active Discovery

Active Discovery

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

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

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

Active Discovery is available on the following devices:

- Cisco Catalyst IE3300 10G Rugged Series Switch
- Cisco Catalyst IE3400 Rugged Series Switch
- Cisco Catalyst IE9300 Rugged Series Switch
- Cisco Catalyst 9300 Series Switch
- Cisco Catalyst 9400 Series Switch
- Cisco IC3000 Industrial Compute Gateway

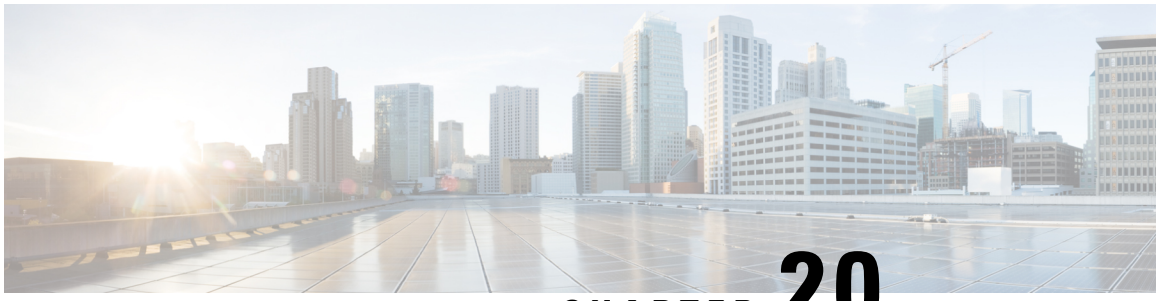
- Cisco IR8340 Integrated Services Router Rugged

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

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

PART II

Navigating through Cisco Cyber Vision



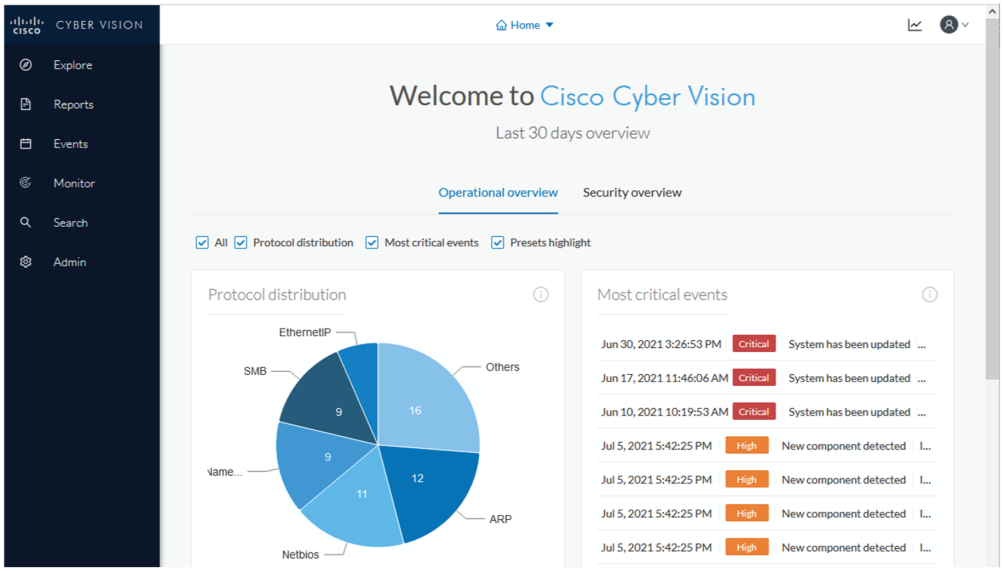
CHAPTER 20

Home

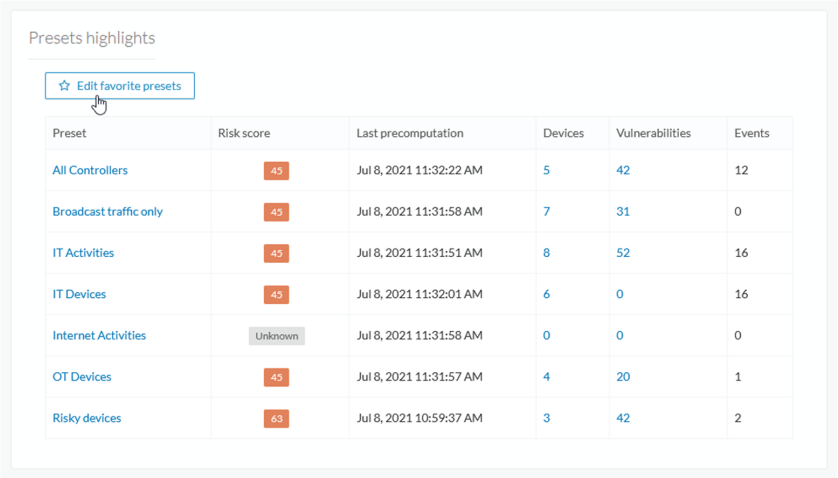
Home

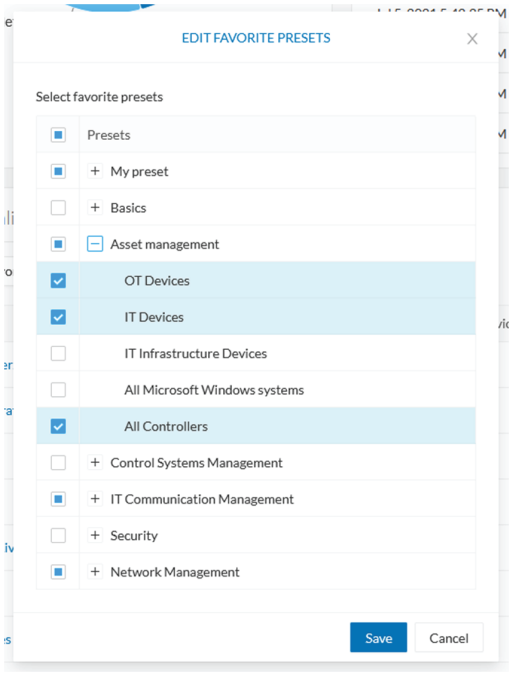
The home page of Cisco Cyber Vision displays two tabs: an **Operational Overview** and a **Security Overview** of the industrial network over the last month.

Use the checkboxes to edit the display. The **Operational Overview** shows the **Protocol distribution** pie chart and a list of the **Most critical events**.

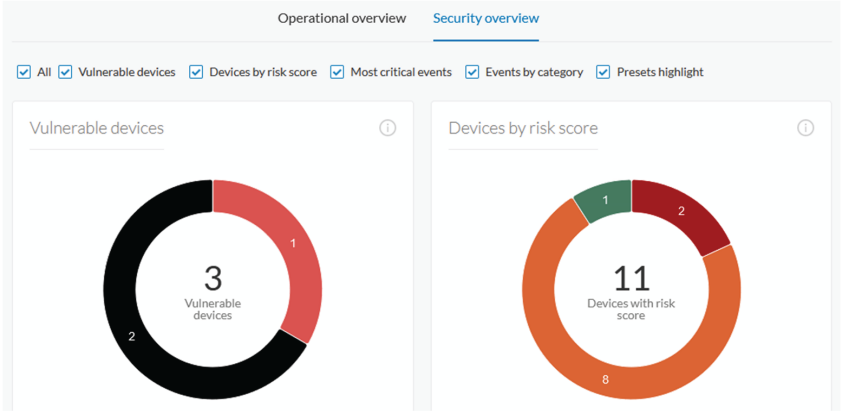


It also shows a **Preset highlights**. Click **Edit favorite presets** to change what displays.

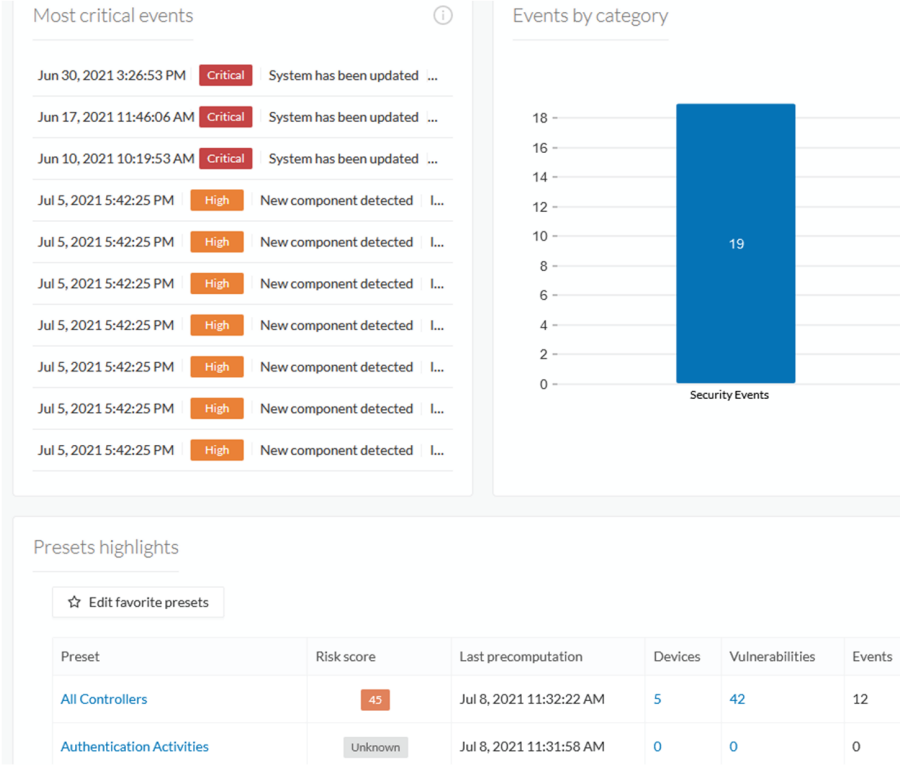




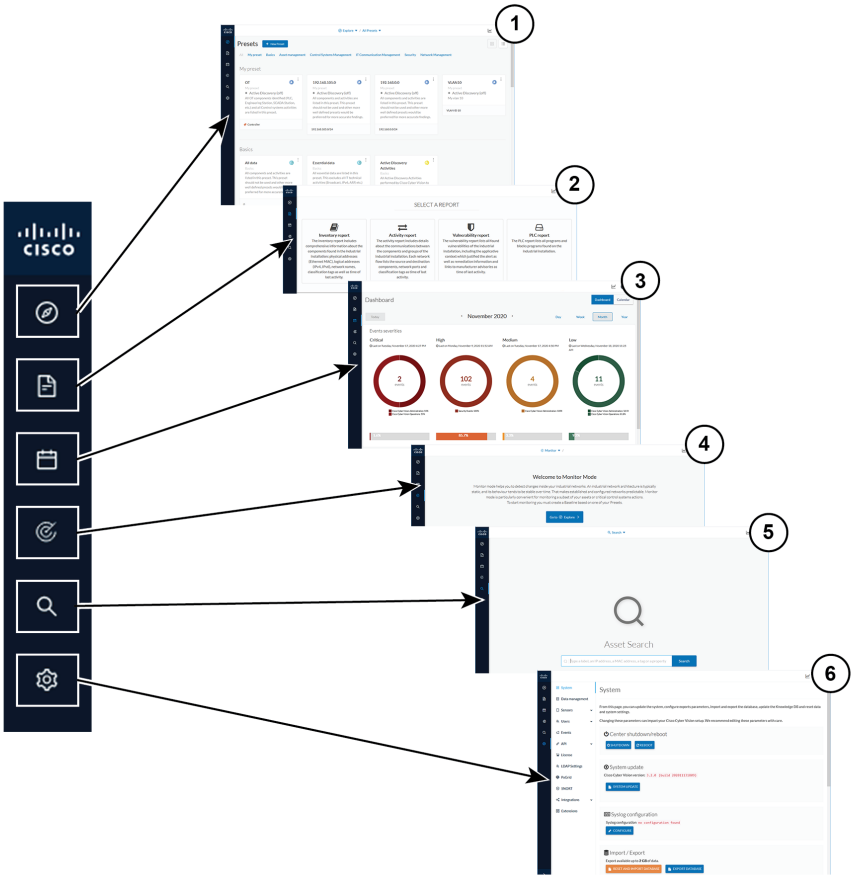
Security Overview shows the **Vulnerable devices per severities** ring chart and the **Devices by risk score** ring chart.



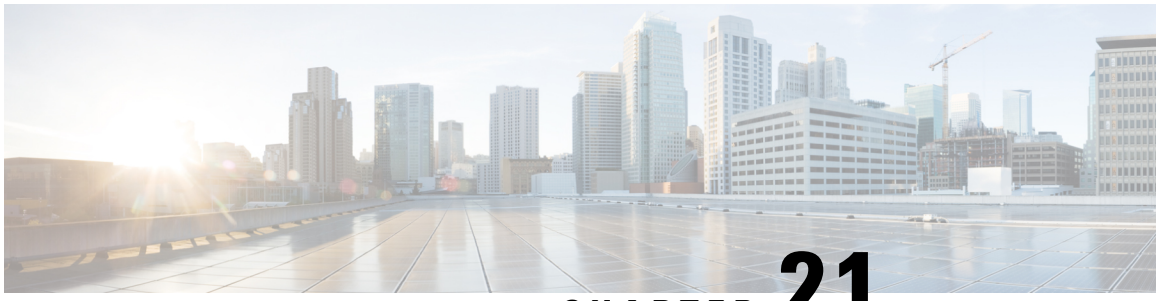
It also shows a list of the **Most critical events**, **Events by category**, and the **Preset highlights** that you can edit.



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



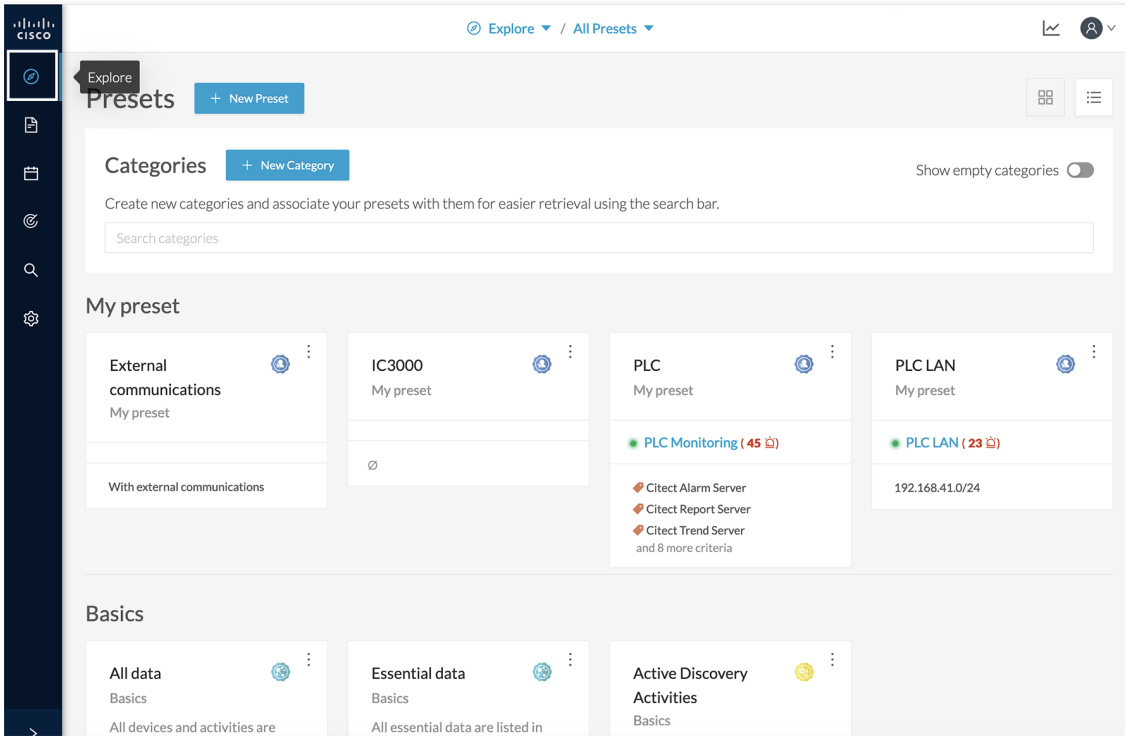
- 1. **Explore**: Shows the overview of Explore, by defaults or configured.
2. **Reports**: Shows the Reports to export valuable information about the industrial network.
3. **Events**: Shows the Events which contains graphics and a calendar of all events generated by Cisco Cyber Vision.
4. **Monitor**: Shows the Monitor to perform and automatize data comparisons of the industrial network.
5. **Search**: Shows the Search to look for precise data in the industrial network.
6. **Admin**: Shows how to update the system, configure exports parameters, import and export the database, update the Knowledge DB and reset data and system settings.



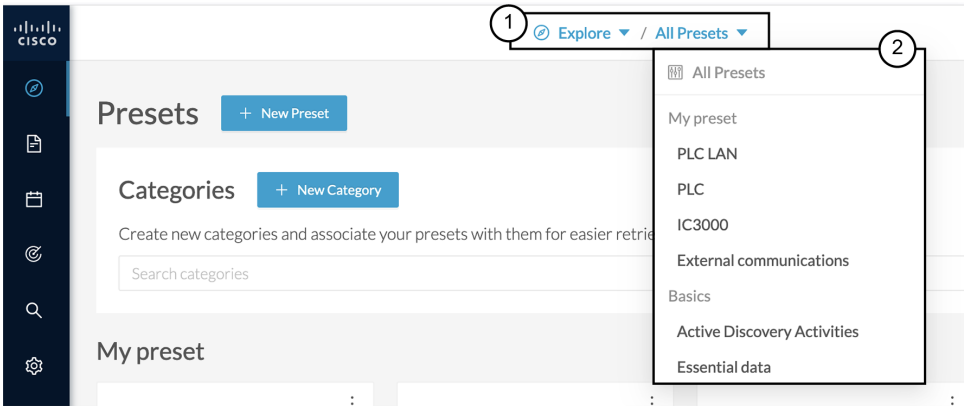
CHAPTER 21

Explore

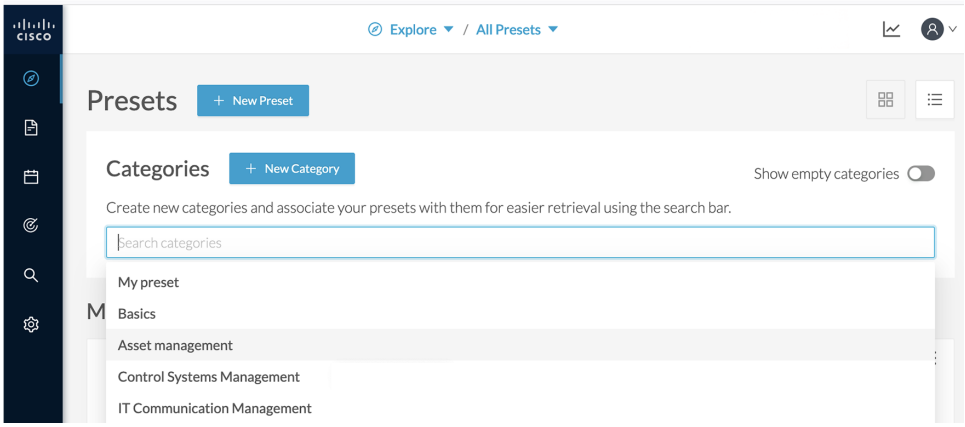
Explore shows an overview of all the Presets in Cisco Cyber Vision, both defaults and custom presets. Click **Explore** on the left navigation bar.



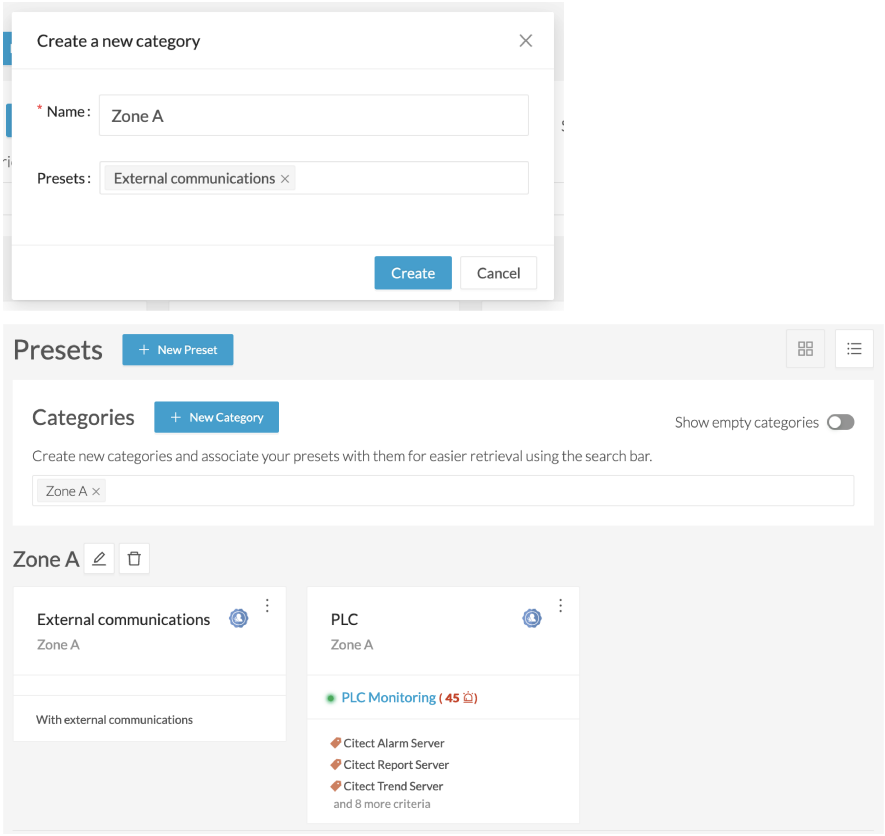
Use the top navigation bar **(1)** to access the different presets **(2)** and Preset views.



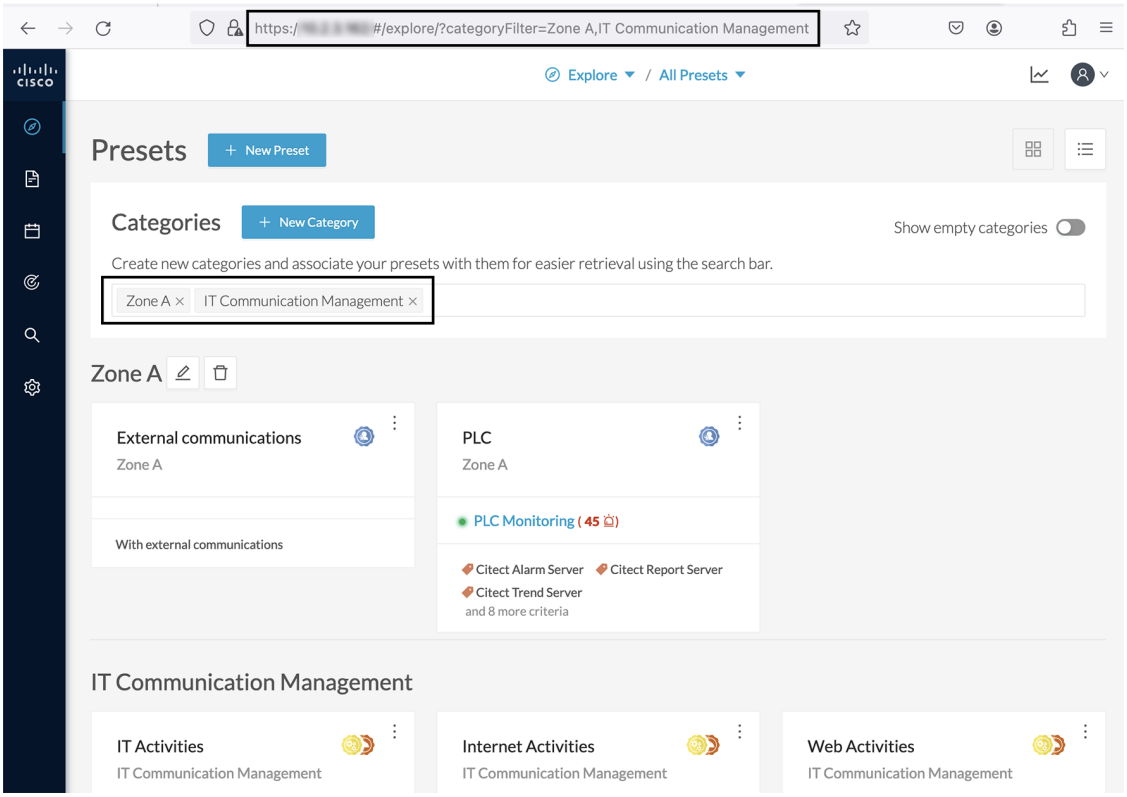
You can also filter presets by categories.



Create new categories to order and search your custom presets.



Filters included in Cisco Cyber Vision Explore page's url allow you to save the selection in your browser's favorites.



- Preset views, on page 78
- Detail panel, on page 89

Preset views

There are several types of views which relate to different perspectives. Using the top navigation bar to access the views, click **Explore > All Data**. The **Dashboard** menu adds.

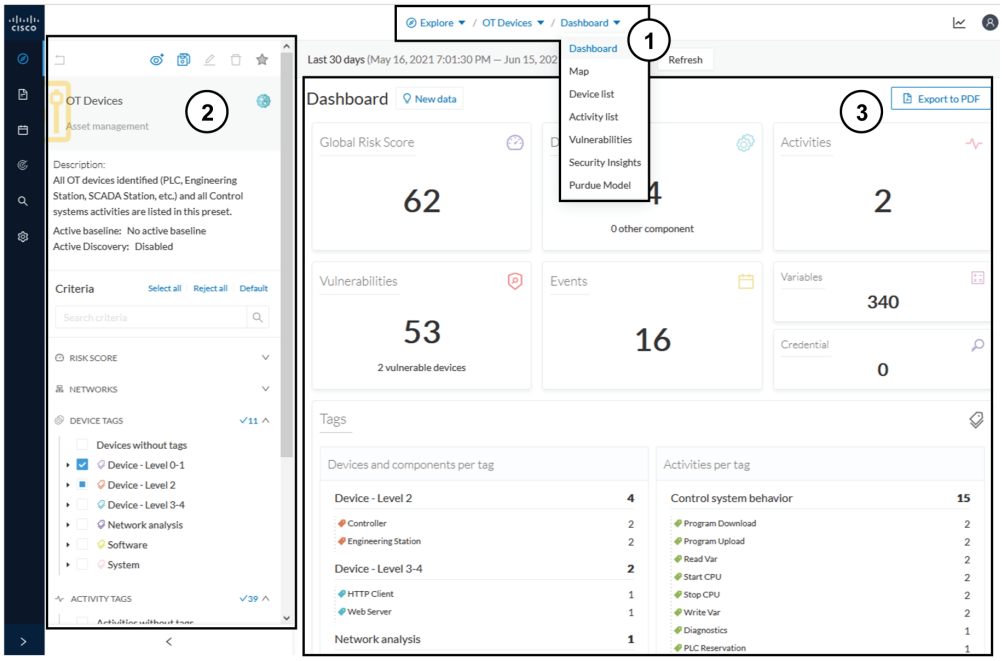
- **Dashboard** view is the default which gives the preset data overview. It is a tag-oriented view showing general insight of the network, without going into deep and technical details.
- **Map** is visual data of the industrial network that gives you a broad insight of how components are connected to each other.
- **Lists**, **Device list** or **Activity list**, show classic but powerful data filtering to match what you are looking for. For more information, refer to the Device and activity lists.
- **Purdue Model** shows how the components of a preset are distributed among the layers of the Purdue Model architecture.

Views are always structured as shown below:

- Use the top navigation bar **(1)** pull-down menus to easily switch between the different views.
- Use the left panel **(2)** to filter, modify, and manage the preset data by adapting criteria and registering changes.

- The center panel **(3)** dynamically changes as you save criteria.

Below is an example of the OT Devices preset on the Dashboard view.

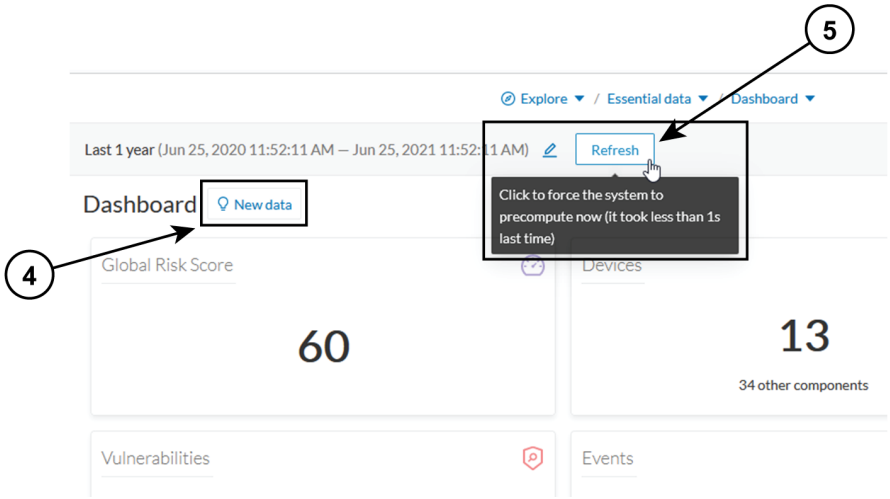


The preset view is optimized to avoid lags, to solve performance issues, and to prevent the application from crashing, especially in case of large data flow. Since Cisco Cyber Vision version 4.0.0, data elements such as components, tags and activities are stored, instead of being directly displayed in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

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

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

- The **New data** button **(4)** appears each time a new computation is done. Click it to update the view. *The new view may not show new data*.
- The **Refresh** button **(5)** forces data computation and refreshes the preset view. This task requires more resources. Use **Refresh** for the following cases:
  - If you suspect that new data was found during the most recent computation (e.g., a new device plugged into the network).
  - If custom data such as groups or names has been changed (e.g., if adding a device into a group).



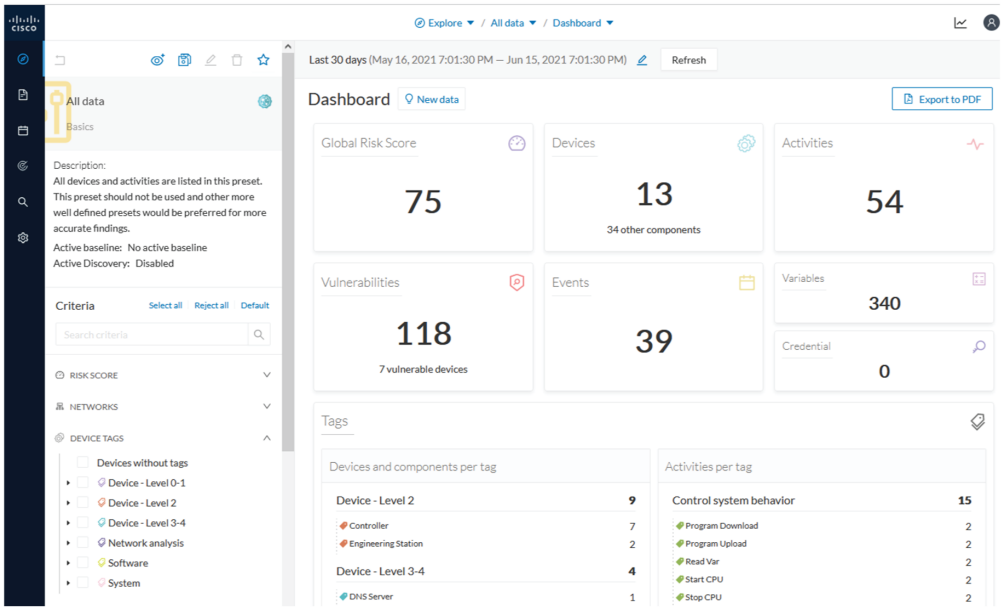
In many cases, computation is forced and the view refreshes as you navigate in the application. For example, refresh happens when you access another preset or move from one view to another.

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

Dashboard

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

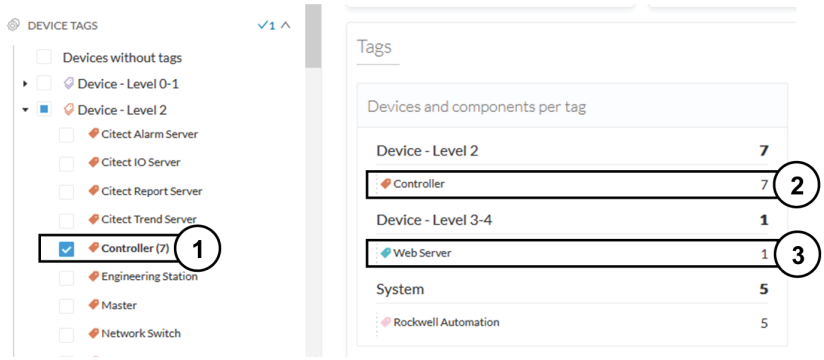
Dashboard also shows **Tags**. The **Tag** pane shows all tags found, including tags set as criteria and shows the number of devices and activities found per tag.



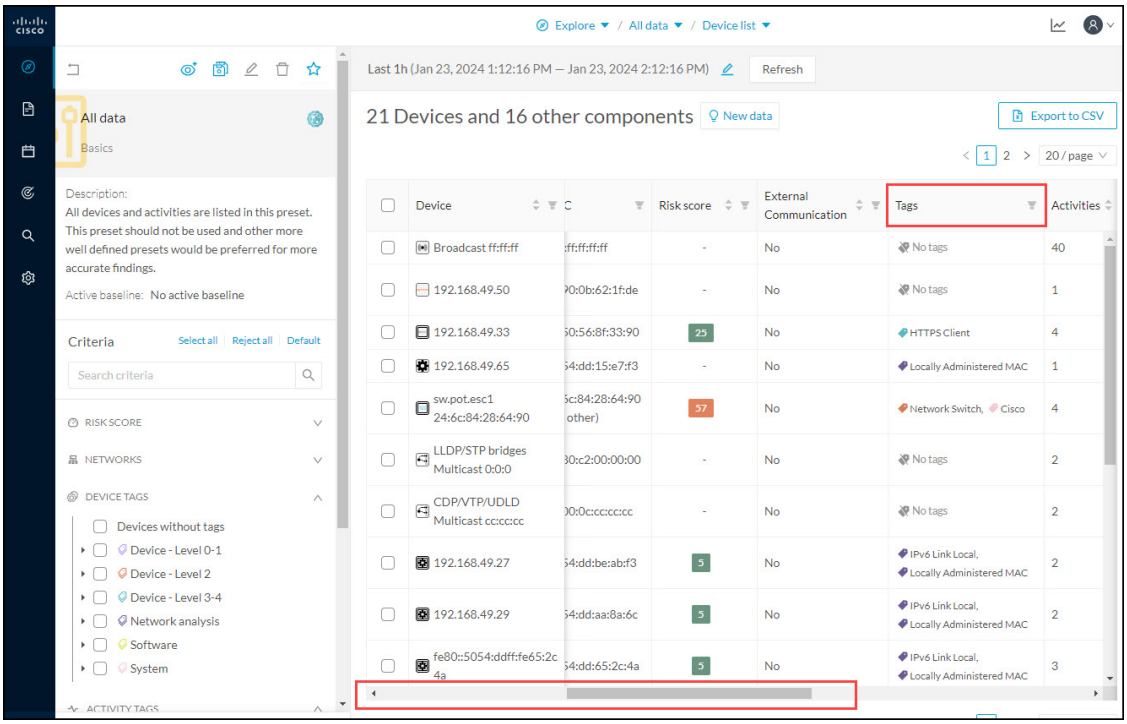
For example:

1. Click **Explore > All Data > Dashboard** from the top navigator menu.
2. Click **Device Tags** from the left panel.
3. Select the **Controller** tag as criteria (under Device - Level 2), and save the selection as "Example: Controller tag."

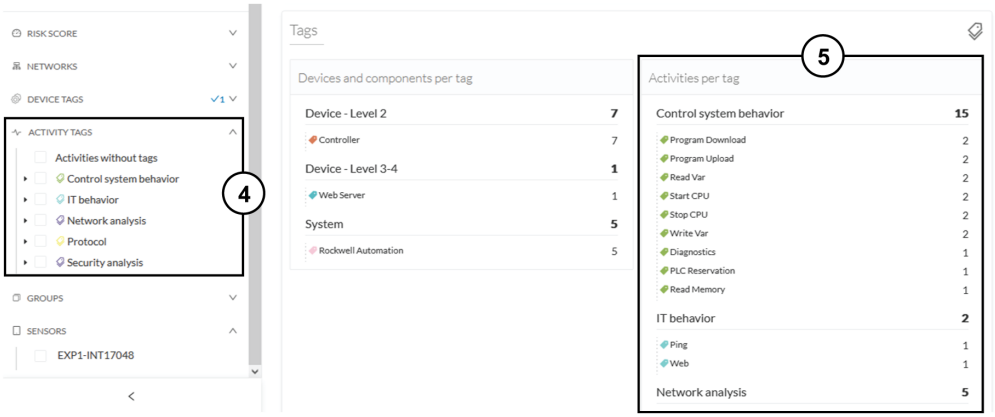
Devices per tag: The number in brackets indicates there are 7 devices tagged as **Controller (1)**. On the **Dashboard**, you see this result **(2)**. One device is tagged as Web Server **(3)**. This means that one of the **Controllers** is a Web Server. Following this logic, we can say that five of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



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



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

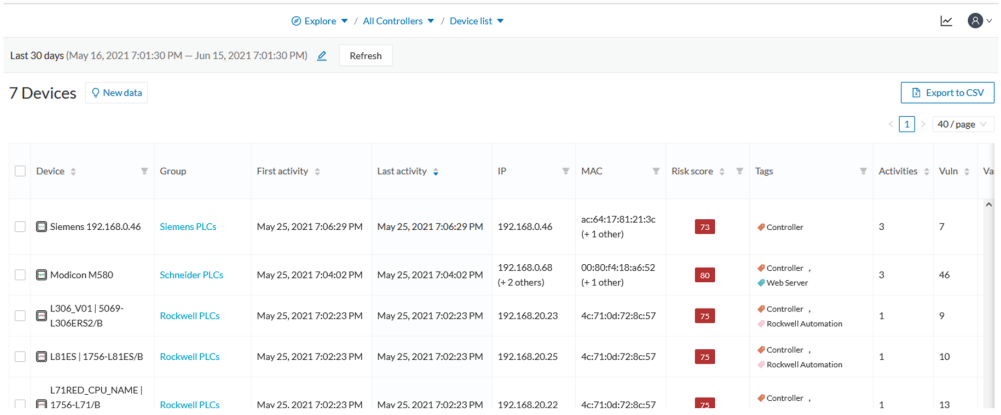


For details on these activities, switch to the Device and activity lists and access them using the filter available in the Tags column.

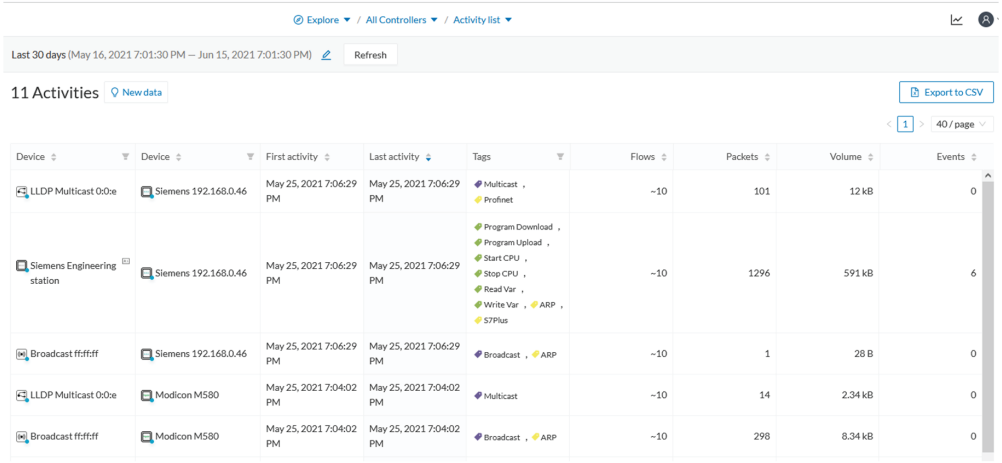
Device and activity lists

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

Below is an example of the Controllers preset in the Device list view.

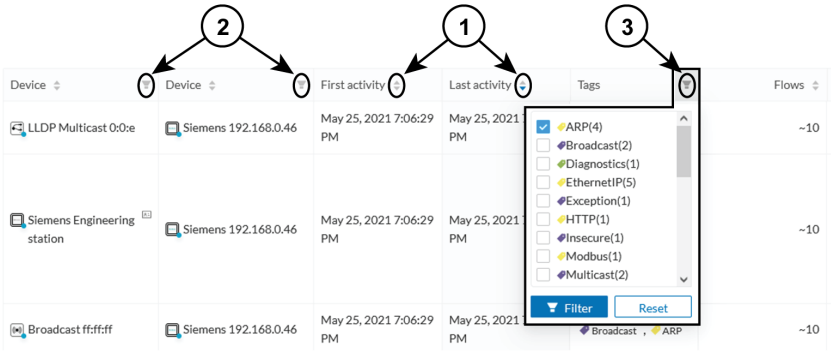


Below is an example of the Controllers preset in the Activity list view.



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

- The **Sort arrows (1)** list data by alphabetical order or by ascending/descending order. Click again to cancel the **Sort**.
- The **Filter** icon **(2)** opens a field to type specific data in or a multiple-choice menu **(3)** to filter **Tags**.

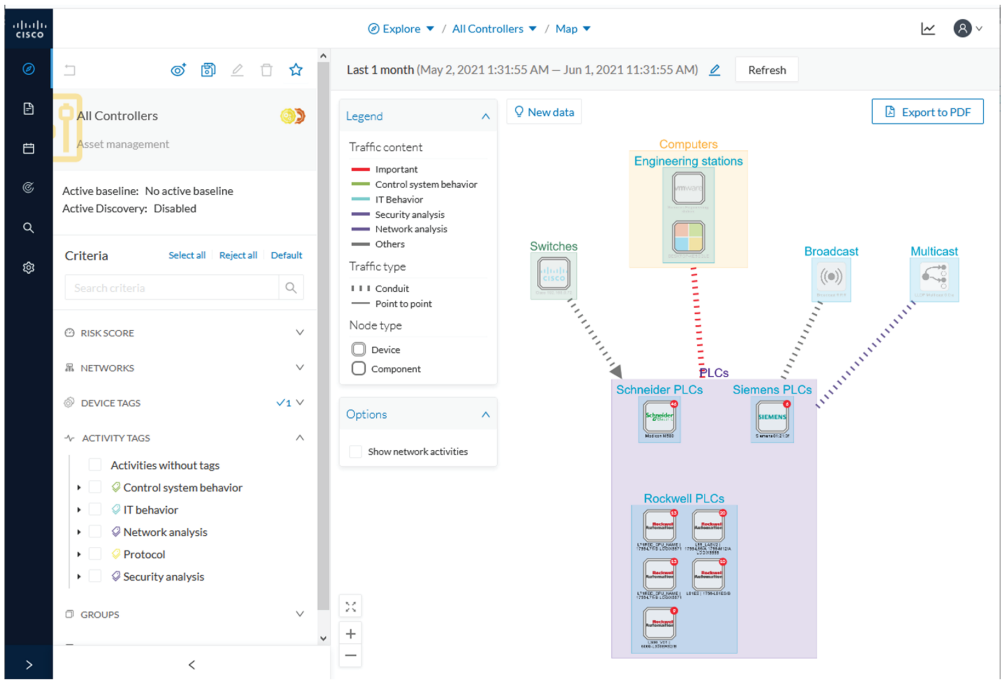


Clicking an element in the lists opens its Detail panel which displays more data.

Map

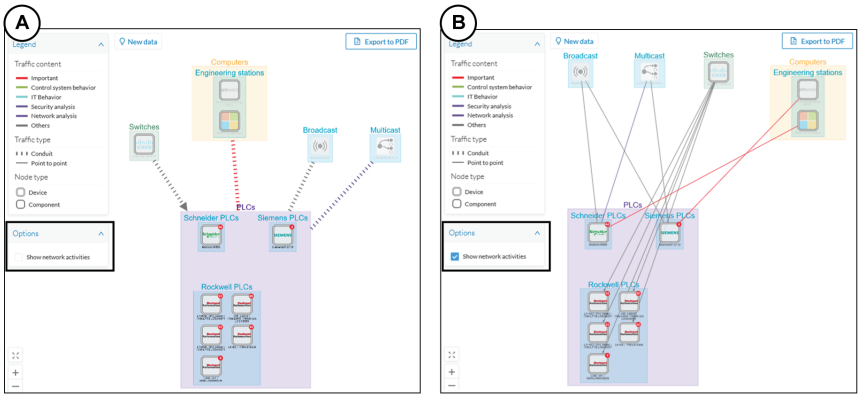
The **Map** view is a visual representation of data of the industrial network that gives you the broadstrokes on how devices and components are interconnected. It shows how the network is structured. **Map** helps you organize components in a way that makes sense to you by creating groups.

Maps displays devices, components, and activities according to criteria set in a preset. **Grayed out devices and components** are displayed because, even if they don't correspond to the preset's criteria, they are necessary to represent the activities of the preset.



Note The **Map** view is ***self-organizing***, that is, elements are redistributed as devices, components, conduits and activities appear or disappear, and as groups are created or deleted. The **Map** automatically adapts over time and when you change a preset. This guarantees that the **Map** is always well organized and components never overlap.

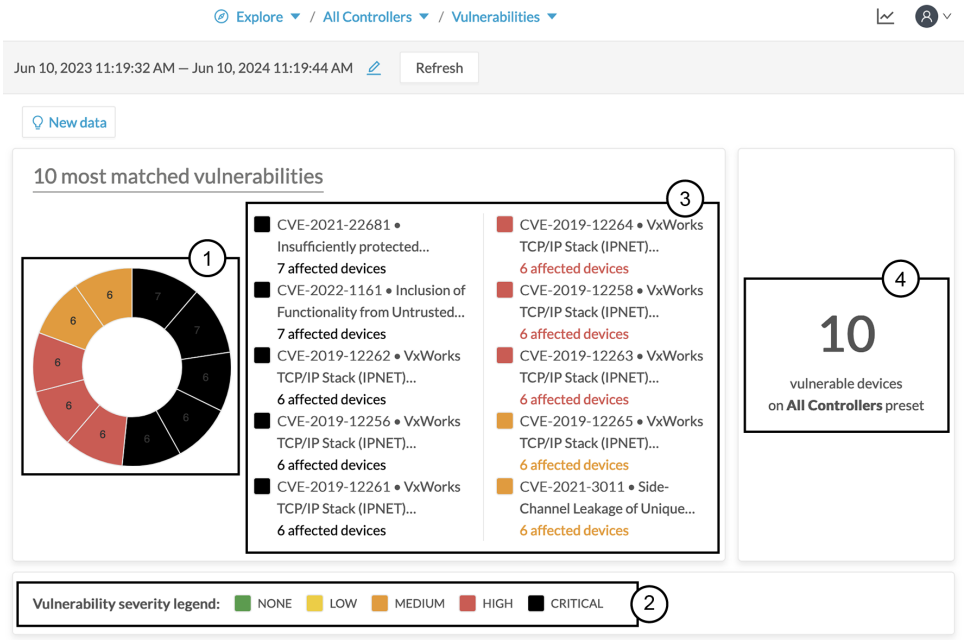
By default, activities between groups are merged and displayed as Conduit **(A)**. Select **Show network activities** for a more detailed view **(B)**. To enhance visibility, elements here are also automatically reorganized on the **Map** .



Vulnerabilities

Click **Explore** > **All Data** > **Vulnerabilities** to see a visual representation and a list of the Vulnerability detected within a preset.

Important If you receive a notification about a new version, update the Knowledge DB in Cisco Cyber Vision as soon as possible. This protects your network against vulnerabilities. Refer to the corresponding documentation.

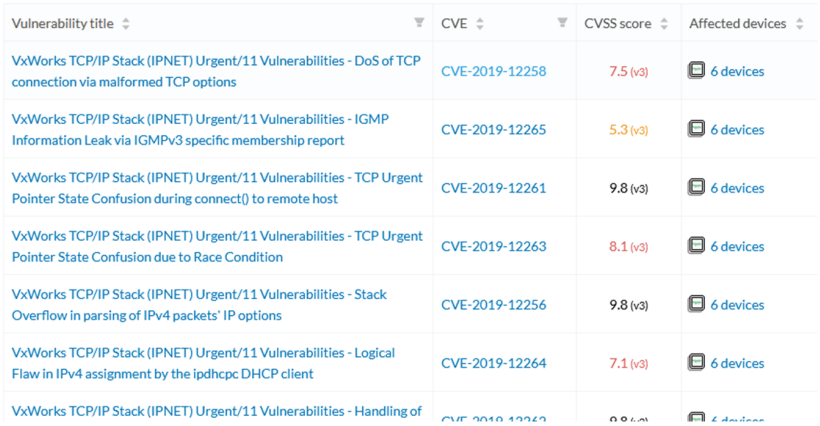


The pie chart shows the 10 most-matched vulnerabilities within the preset and the affected devices **(1)**. The legend below gives you the color code of severity **(2)**. The center panel shows a list of the ten most vulnerabilities **(3)**. Click the hyperlink for an affected device to see the details panel. The right panel shows the total number of devices that are vulnerable in the preset selected **(4)**.

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

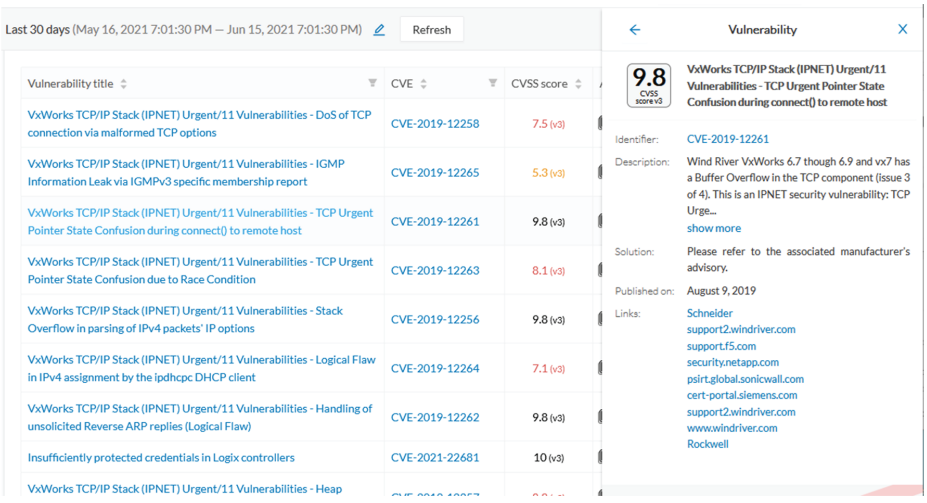
For each vulnerability, the following data is displayed in columns:

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



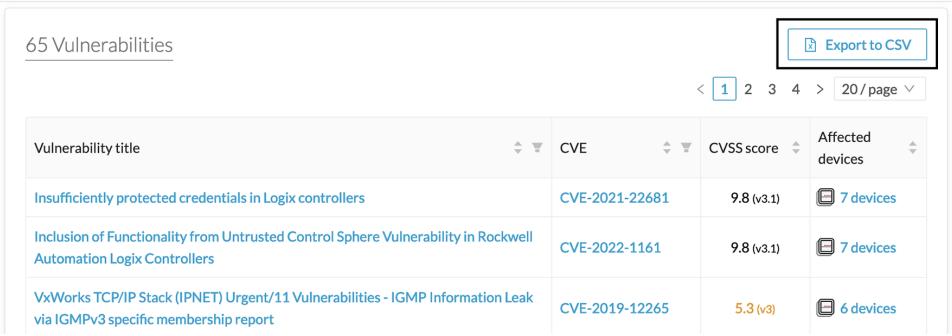
Vulnerability title	CVE	CVSS score	Affected devices
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - DoS of TCP connection via malformed TCP options	CVE-2019-12258	7.5 (v3)	6 devices
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - IGMP Information Leak via IGMPv3 specific membership 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			

Click an element in the list to open the Detail panel, which includes a link to the National Vulnerability Database.



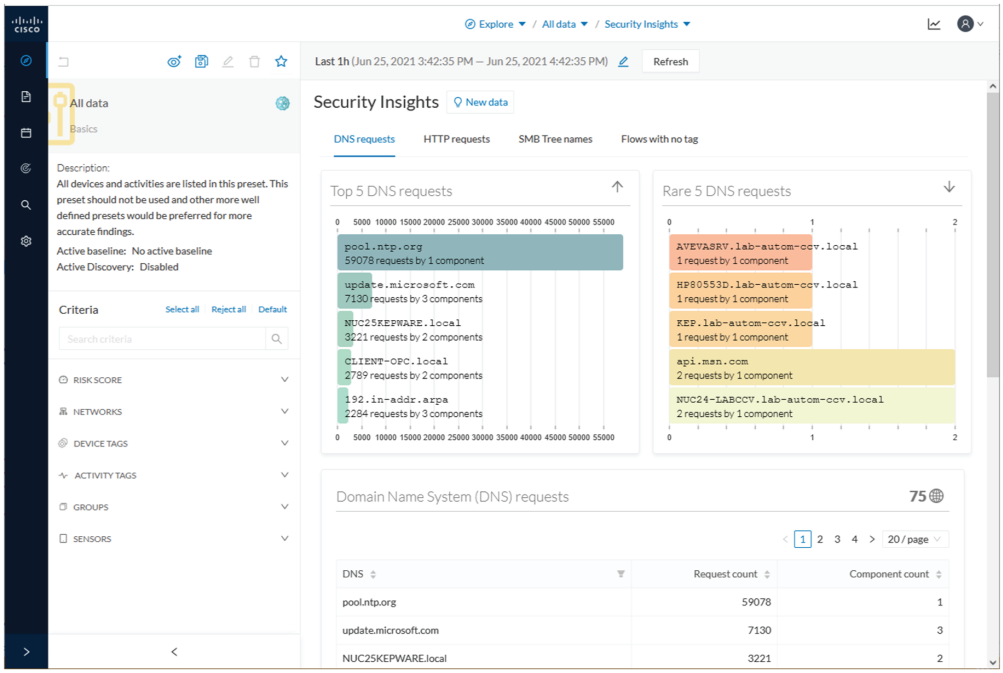
Vulnerability title	CVE	CVSS score
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - DoS of TCP connection via malformed TCP options	CVE-2019-12258	7.5 (v3)
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - IGMP Information Leak via IGMPv3 specific membership report	CVE-2019-12265	5.3 (v3)
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		

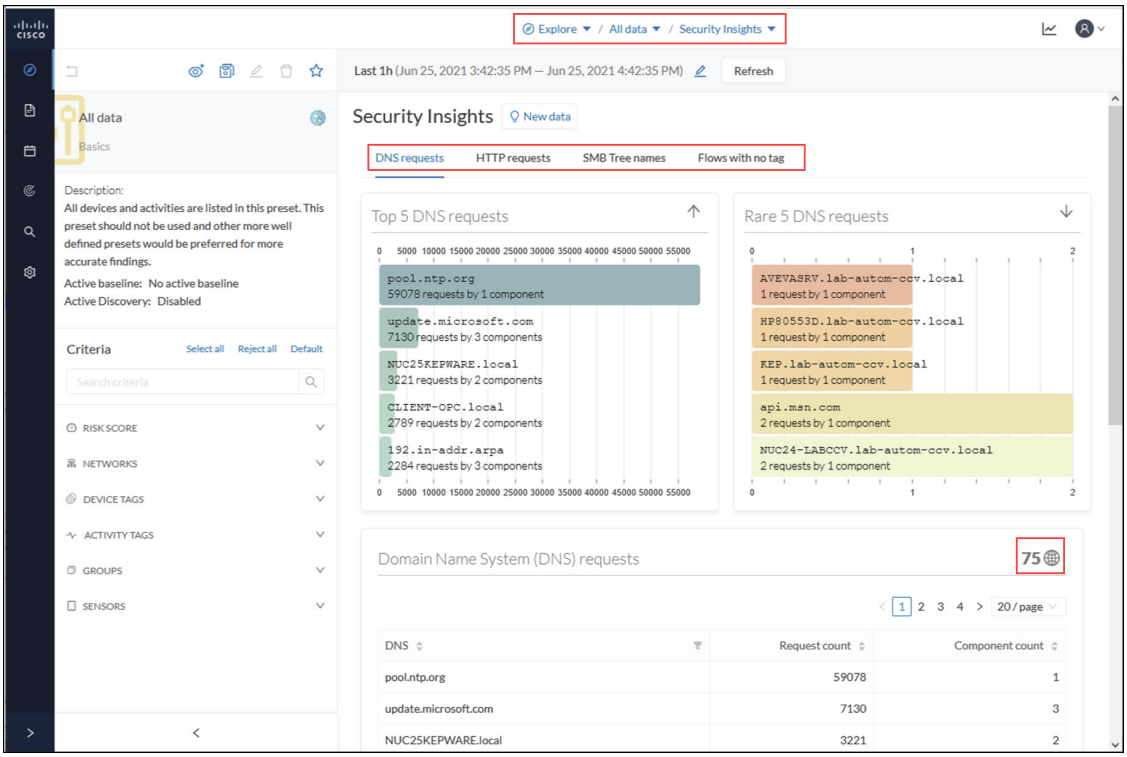
You can **Export to CSV** using the corresponding button on top of the vulnerability list. A report will be generated for the time period defined.



Security Insights

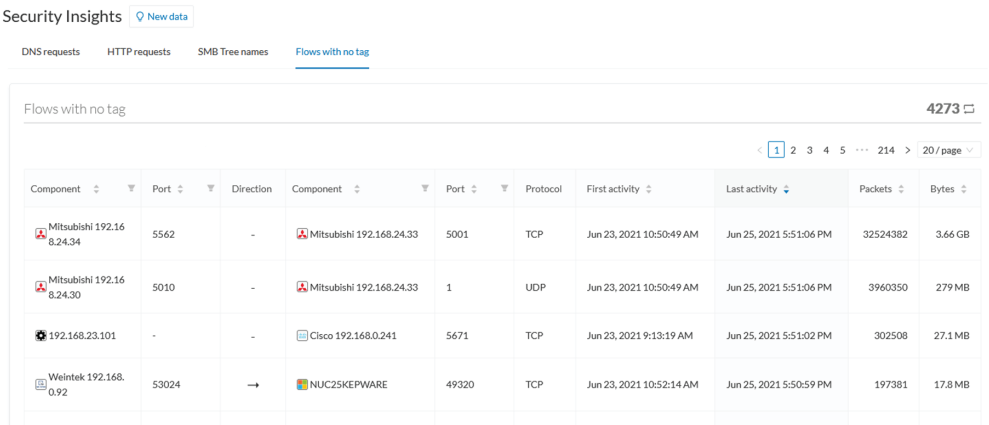
To access **Security Insights**, click **Explore > All data > Dashboard > Security Insights**. **Security Insights** provides statistics for **DNS requests, HTTP requests, SMB Tree names** and **Flows with no tag**.





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

Flows with no tag



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

Next steps:

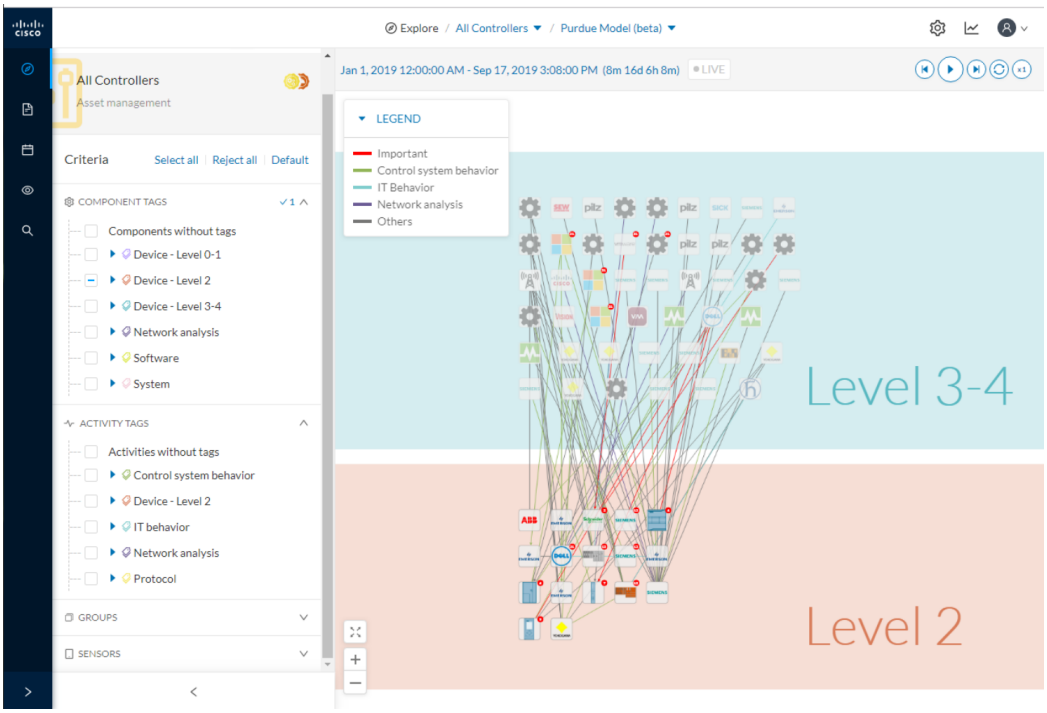
1. Make sure the content is supposed to be on the network.
2. Troubleshoot why it cannot be inspected.

3. Check flows with higher number of packets.

Purdue Model

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

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

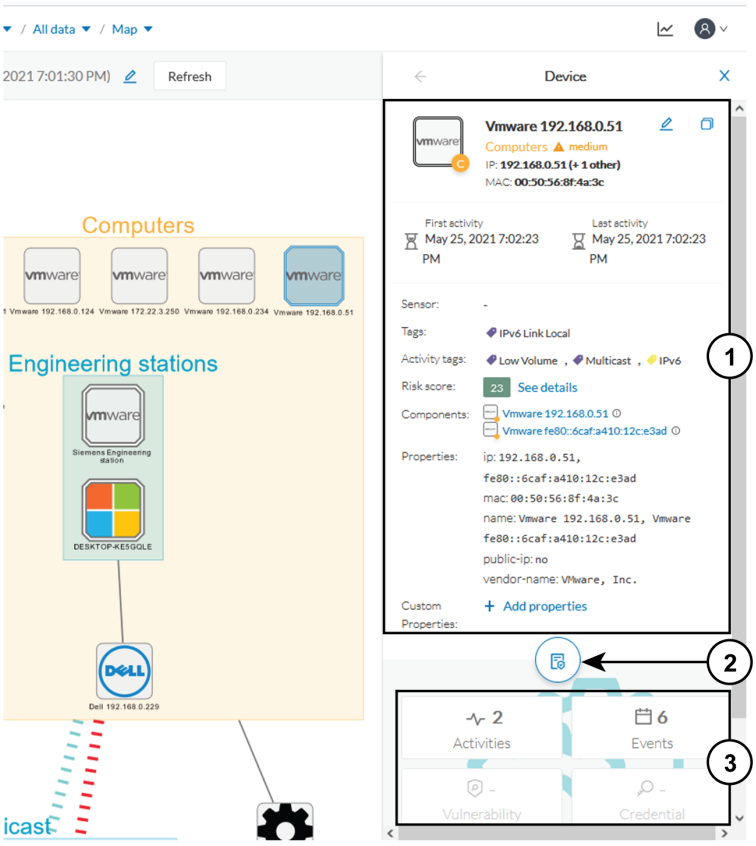


Components are distributed according to the following different layers of the Purdue model:

- Level 0-1: Process and basic control (IO Modules).
- Level 2: Area supervisory control (PLCs, SCADA stations).
- Level 3-4: Manufacturing zone and DMZ (all others).

Detail panel

A Detail panel is a condensed view about a device, a component, a group of components or an activity's information without changing the background device list or a map. To access a detail panel, click a device, a component or an activity on the map or a list.



The detail panel differs depending on the type of element you select. The upper portion **(1)** gives you general information about the element. If you select a device or a component, you can edit its name an add/remove it to/from a group.

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

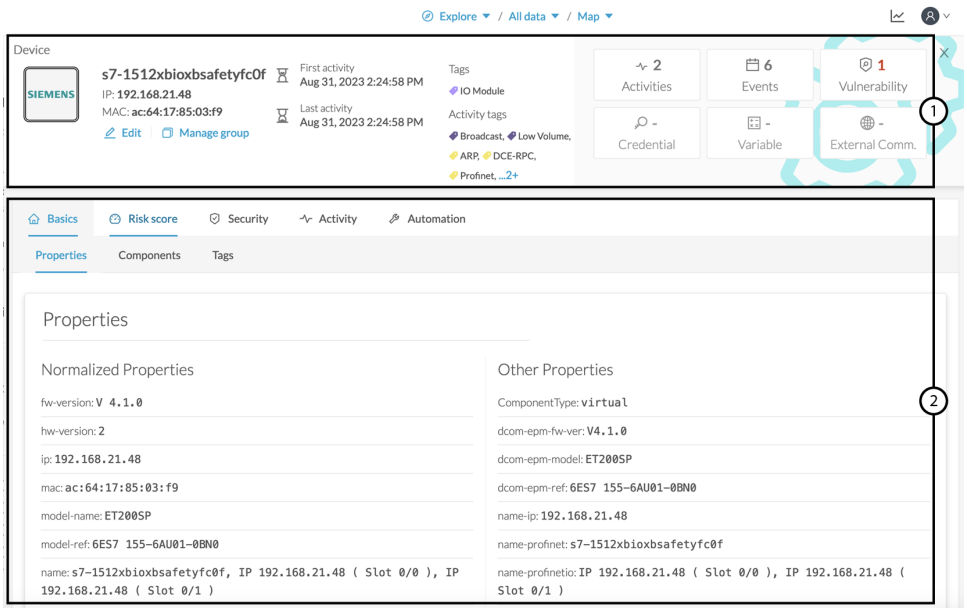
The rectangular buttons below **(3)** redirect to the corresponding information inside the technical sheet.

Technical sheets

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

To access the **technical sheet** of a device, component or an activity's Detail panel, click **Explore > All data > Dashboard > Map**. Click the element about which you want more details. The Details panel appears. Click the **Technical sheet** icon.

A technical sheet of a device



The top box of the technical sheet **(1)** recaps the information found in the **Detail** panel. The rectangular buttons on the right redirect to the corresponding information inside the technical sheet. In a device or a component's technical sheet, you can also edit the element's name, add/remove it to/from a group, and add custom properties.

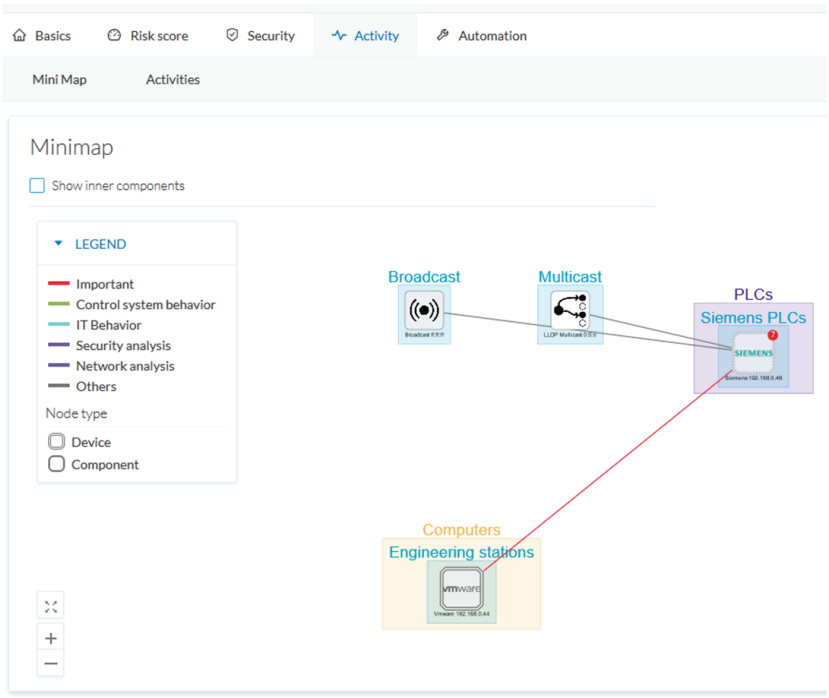
The middle portion **(2)** contains many tabs, depending on the selected element. In the above example, A **Device** detail contains the following tabs:

- **Basics** shows an element's properties and tags that are categorized with their definition. The components of the device also appear, if applicable.
- **Risk score** shows an overview and a more detailed and focused views.
- **Security** shows a component's vulnerabilities and credentials.
- **Activity** shows an activity's flows and contains a Mini map, a view that is restricted to a device or a component and its activities. If applicable, a list of External communication with related information appears under the corresponding tab.
- **Automation** contains variable accesses.

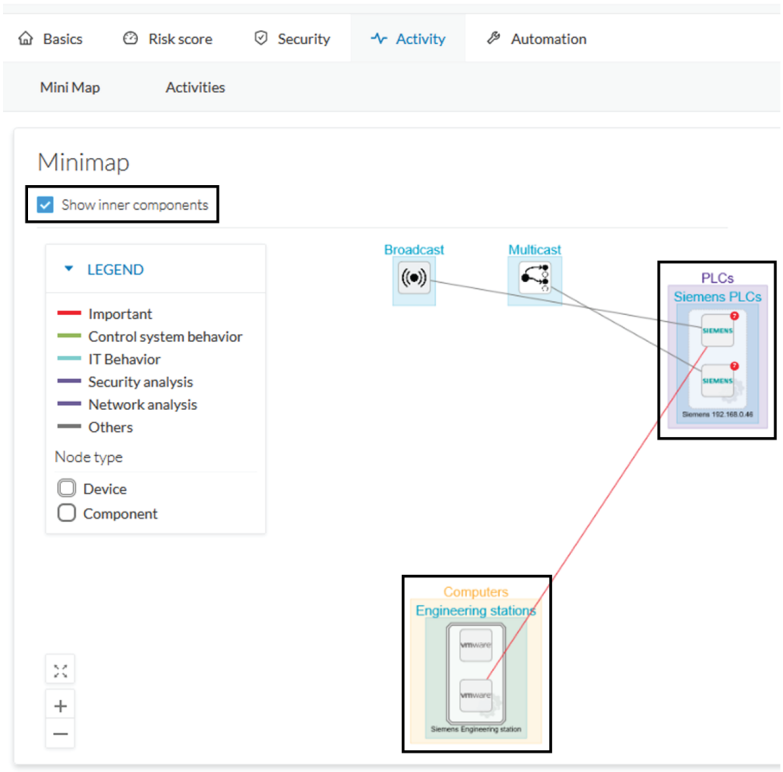
- More information about Properties.
- More information about Tags.
- More information about the Risk score.
- More information about Vulnerability.
- More information about Credentials.
- More information about Flow.
- More information about the Mini map.
- More information about External communication.
- More information about Variable accesses.

Mini map

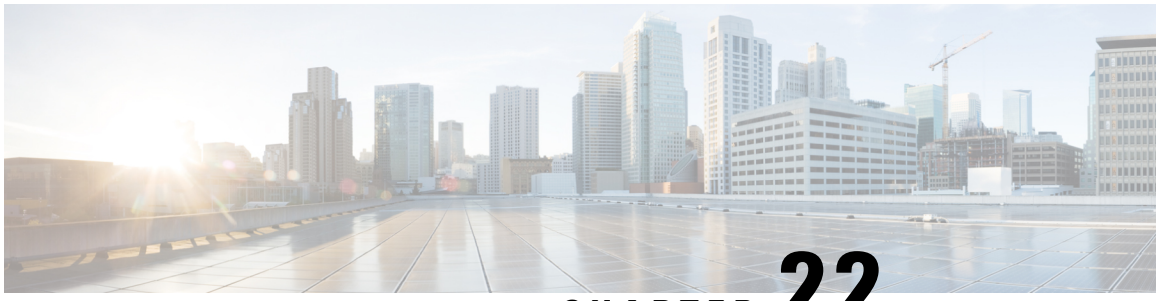
The **Mini Map** is a visual representation restricted to a specific device or component and its activities. To access **Mini Map**: click **Explore > All data > Dashboard > Map >** select a device from the map > click **Technical sheet** from the **Details** panel. Click the **Activity** tab.



Click **Show inner components** for an exploded view of the devices.



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



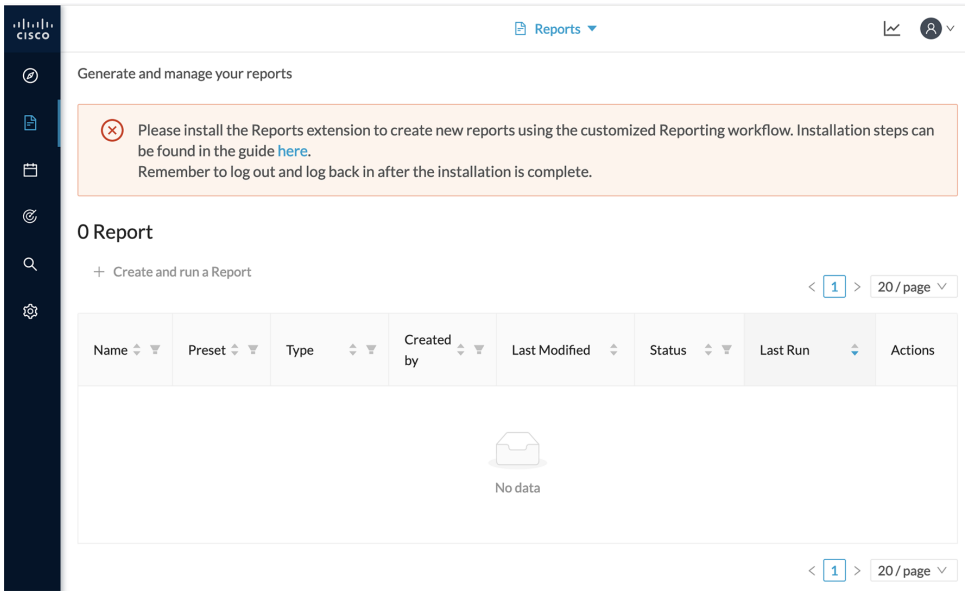
CHAPTER 22

Reports

Reports

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

You must install the **Reports extension** to use this page. Click **Admin > Extension > Import a new extension file**. The extension file is available on cisco.com.



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

Reports extensions include .docx and .pdf formats.

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

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

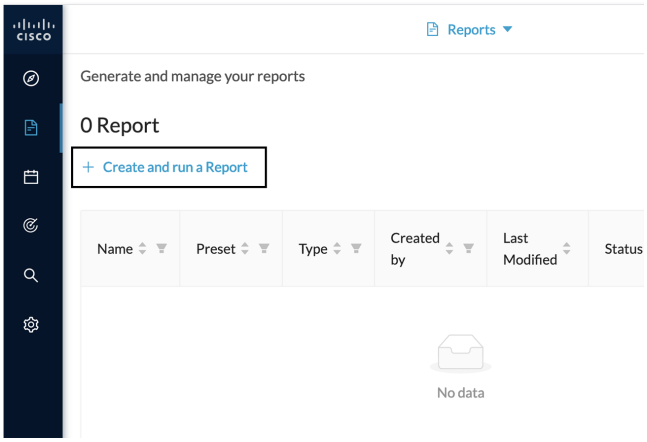
Create a report

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

Procedure

Step 1 From left pane, click **Reports**.

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

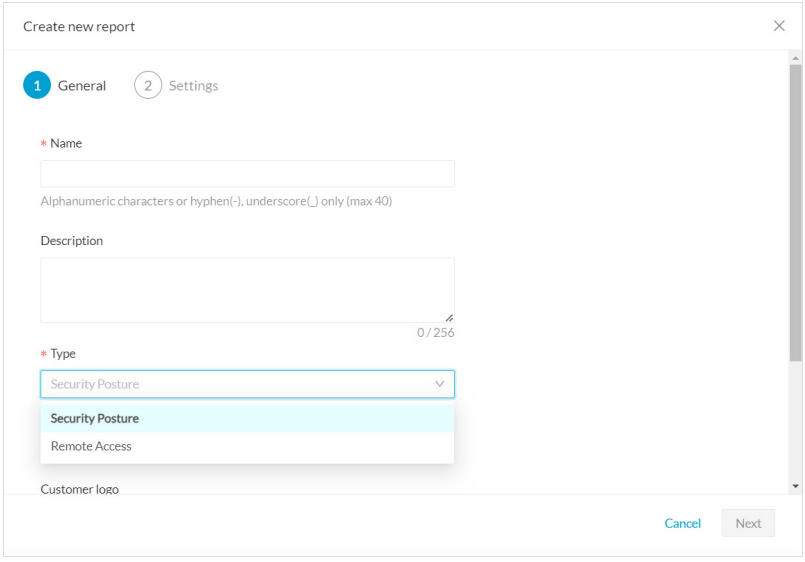


Step 3 Type a **Name**. Optionally, add a **Description**.

Step 4 Select the report type from the dropdown list. Report types are as follows:

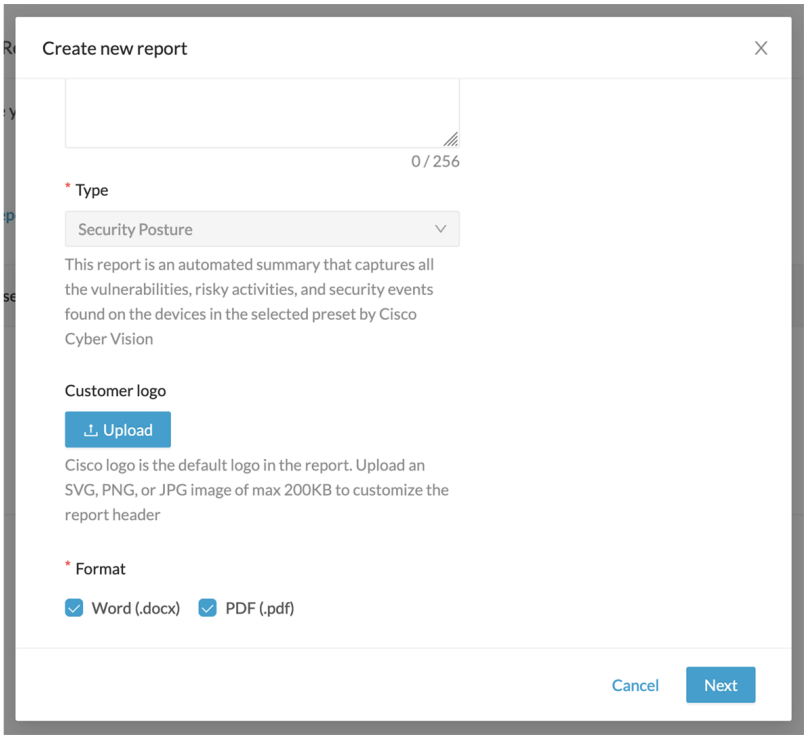
- **Security Posture:**This report is an automated summary that captures all the vulnerabilities, risky acivities, and security events found on the devices in the selected preset by Cisco Cyber Vision.
- **Remote Access:**This report is an automated summary that captures a list of all Remote Access Gateways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

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



Step 5 Optionally, add a **Customer logo**. It will appear on the report.

Step 6 Select the **Format**(s) you want.

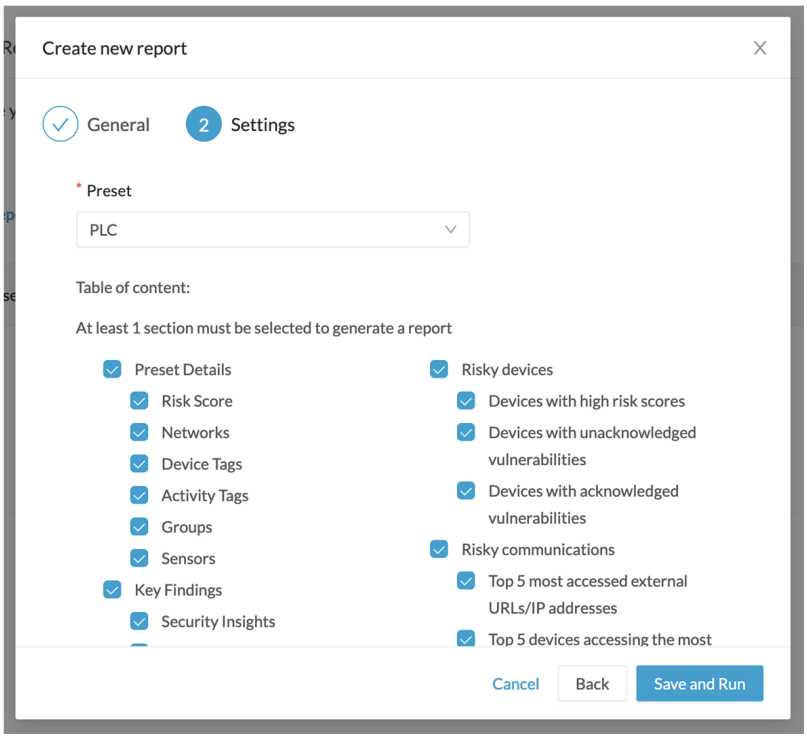


Step 7 Click **Next**.

Step 8 Select a **Preset** from the drop-down menu.

Step 9 In **Table of content**, select the content (sections and sub-sections) you want to appear in the report.

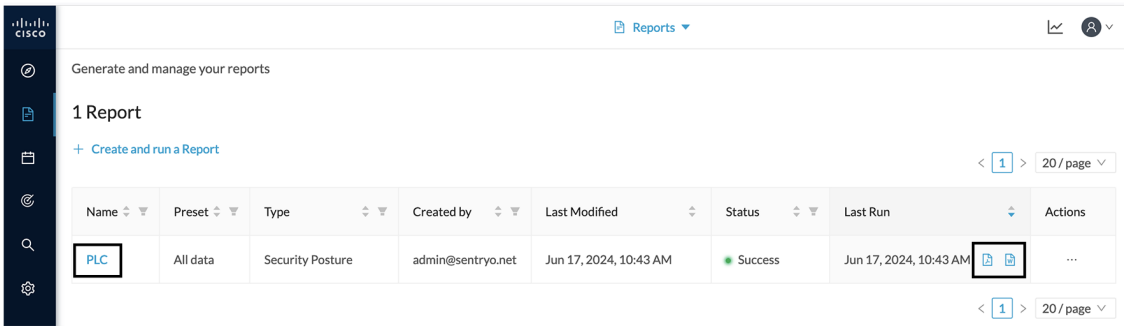
Note Content (sections and sub-sections) will vary depending on the type of report selected.



Step 10 Click **Save and Run**.

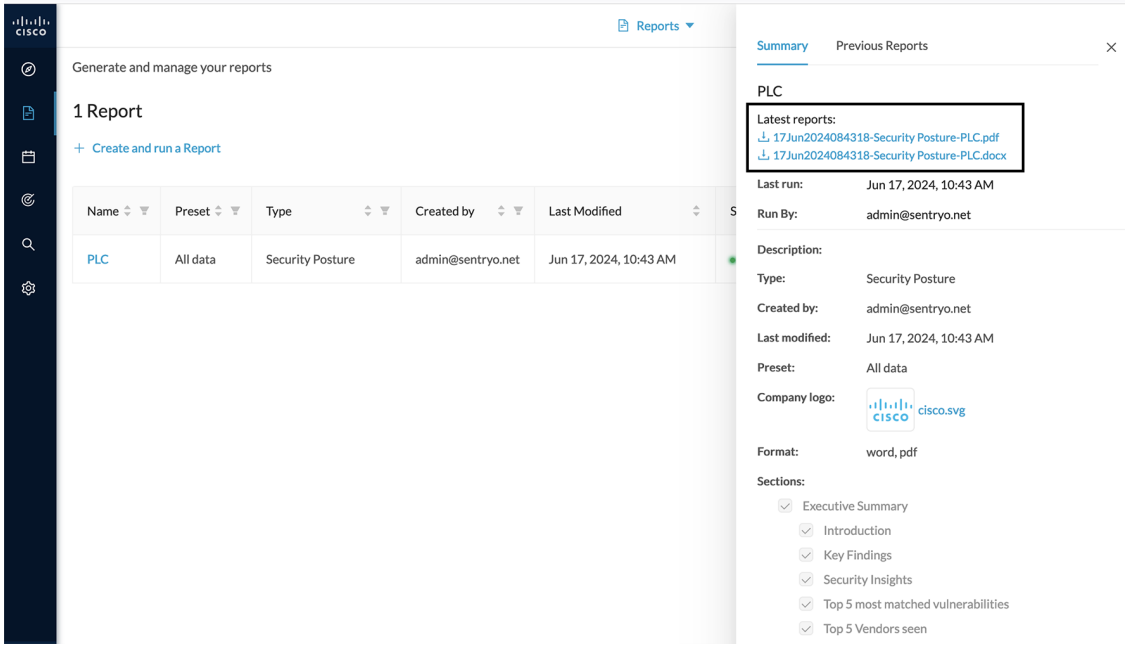
The new report appears in the list with the **Status: Processing**. When done, **Success** appears.

Step 11 To download the report, click the name of the report in the list to open its **Detail** panel. Or, use the format icon(s) in the **Last Run** column.

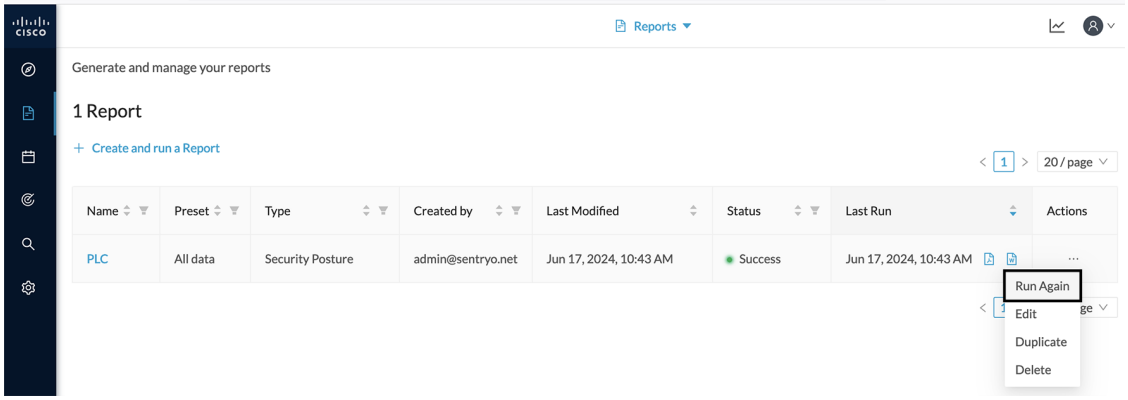


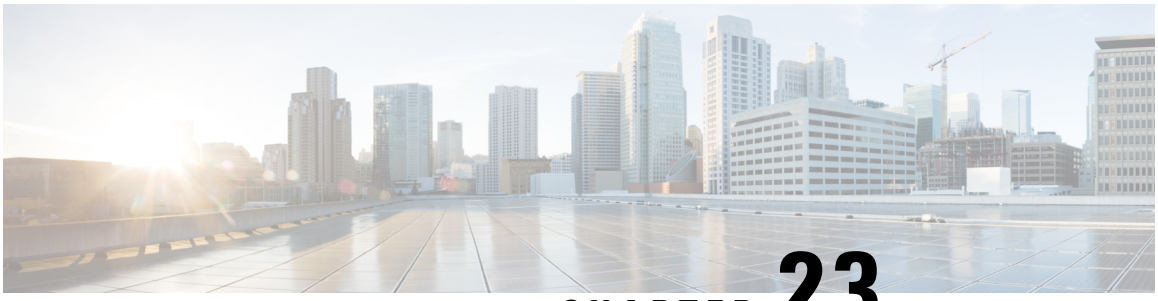
Step 12 In the **Details** panel, click the links to download the latest reports.

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



Step 13 To generate a new report, click **Run Again** under **Actions**.





CHAPTER 23

Events

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

Go to **Admin > Events** to see all available **Events**. See the Cisco Cyber Vision *Administration Guide*.

The **Events** interface provides high visibility on events with the following two views:

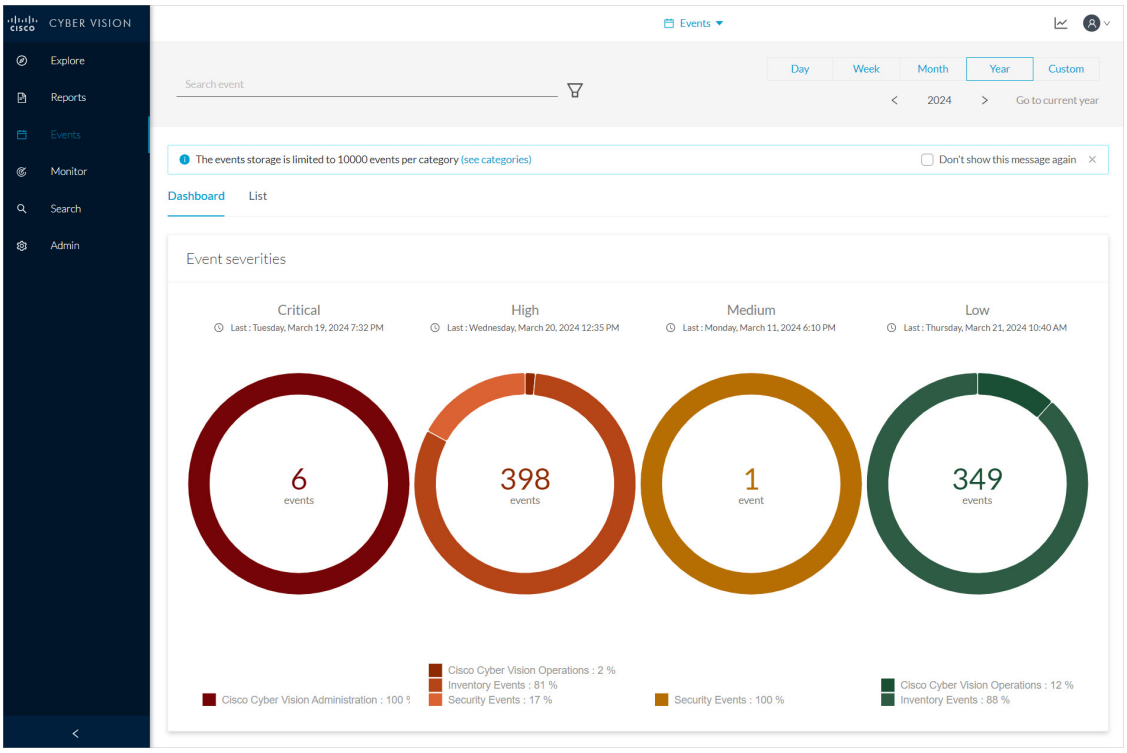
- The Dashboard: Shows a visual and continuously-updated view of the current state of the installation, based on the number of events (by severity and over time).
- The List: Shows a chronological and continuously-updated view of the events within which you can search events.

- The Dashboard, on page 101
- The List, on page 103

The Dashboard

The **Dashboard** shows Event doughnut and line charts. Doughnut charts show color-coded, event severity categories and percentages. You can filter the Events on **Day, Week, Month** or **Year**. Use the arrows for exact dates.

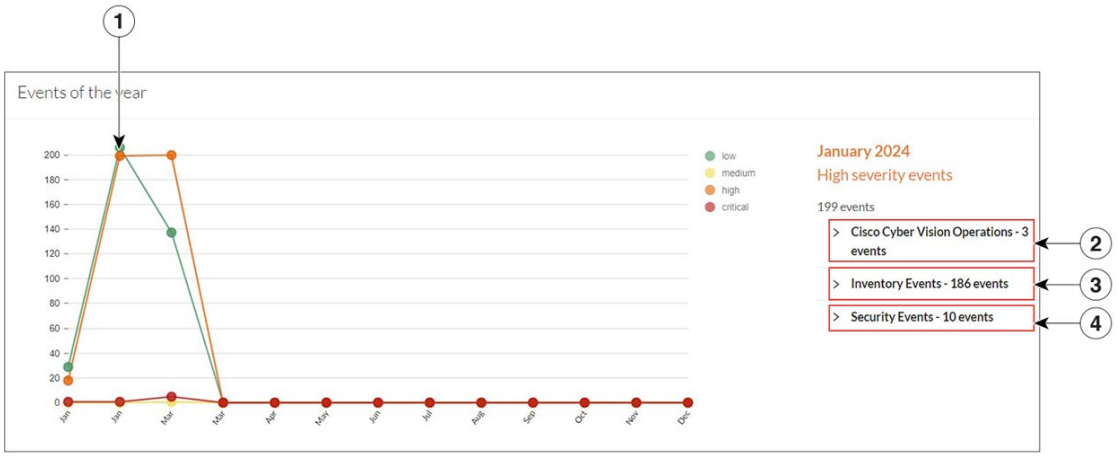
Doughnut charts present events numbers and percentages per categories and severities.



Click a doughnut. The screen toggles to a detailed The List view list filtered with the corresponding category and severity so you can quickly access more events details.

To see the list of Events per categories, click **Admin** > **Events**. See the Cisco Cyber Vision *Administration Guide*.

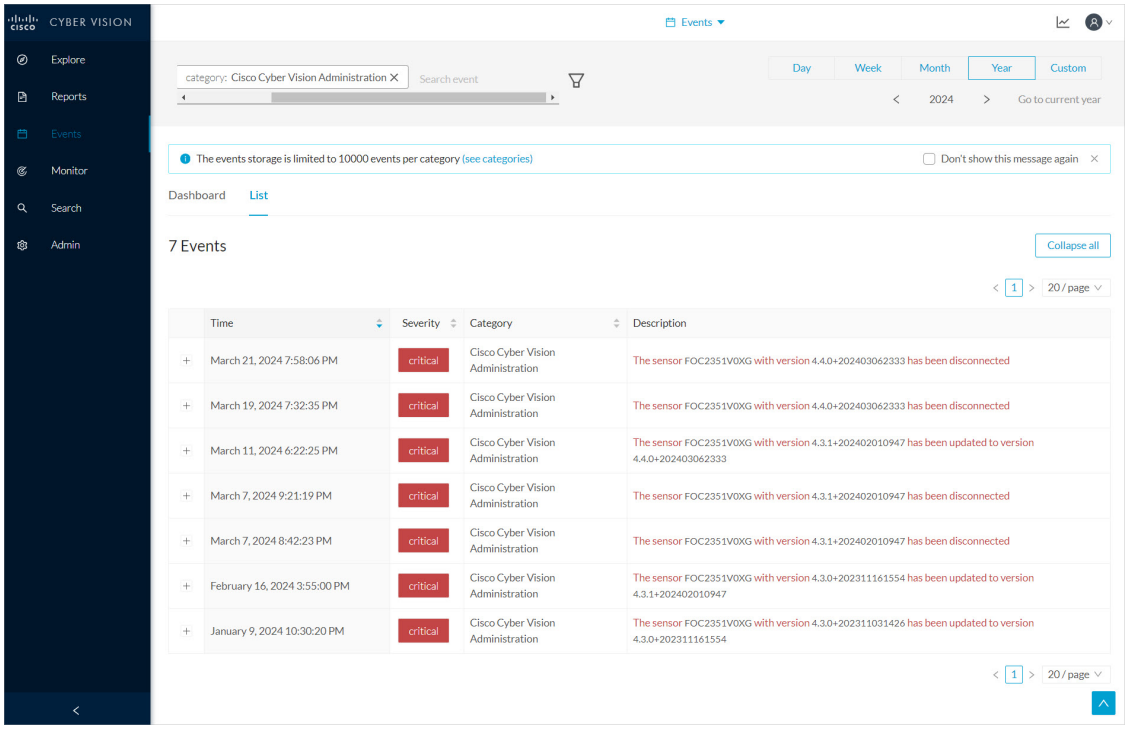
The line chart shows the number of events per severity over time. Click the event marker **circle** to see the number of events per category at a specific time.



Click event markers **(1)** on the line to see the number of events per category according to a specific date. Click tab **(2)** for **Cisco Cyber Vision Operations** events details, tab **(3)** for **Inventory Events** details and tab **(4)** for **Security Events** details.

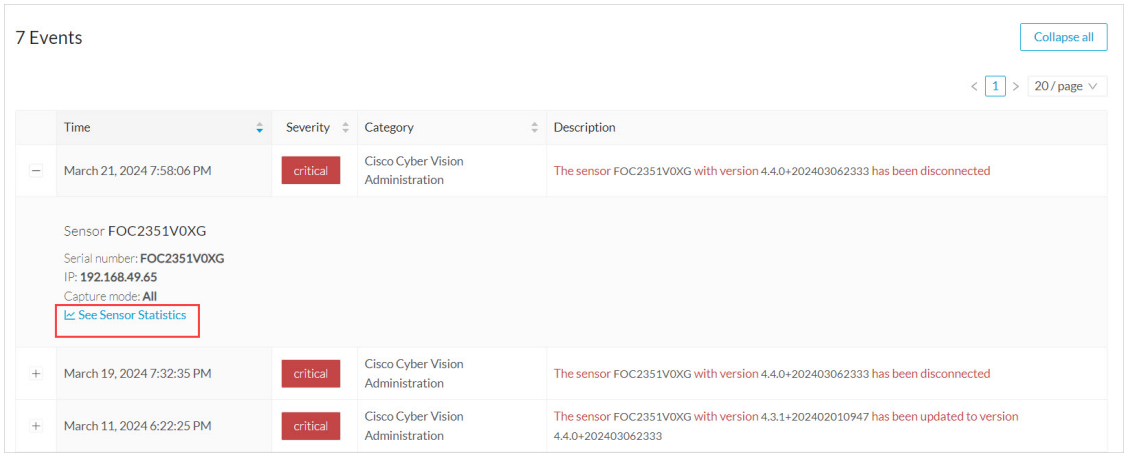
The List

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

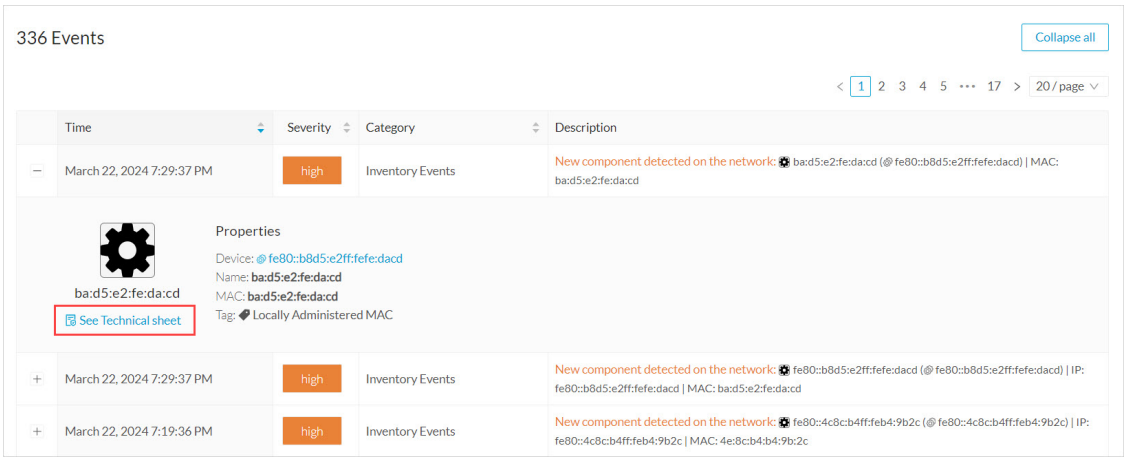


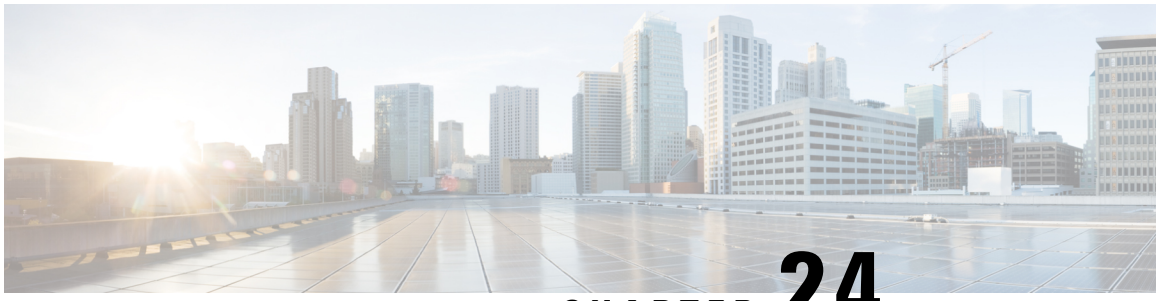
Click an event result for more details about the event.

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



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


336 Events
Collapse all
1 2 3 4 5 ••• 17 20 / page
Time
Severity
Category
Description
March 22, 2024 7:29:37 PM
high
Inventory Events
New component detected on the network: ba:d5:e2:fe:da:cd (@ fe80::b8d5:e2ff:fefe:dacd) | MAC: ba:d5:e2:fe:da:cd
Properties
Device: @ fe80::b8d5:e2ff:fefe:dacd
Name: ba:d5:e2:fe:da:cd
MAC: ba:d5:e2:fe:da:cd
Tag: Locally Administered MAC
ba:d5:e2:fe:da:cd
See Technical sheet
March 22, 2024 7:29:37 PM
high
Inventory Events
New component detected on the network: fe80::b8d5:e2ff:fefe:dacd (@ fe80::b8d5:e2ff:fefe:dacd) | IP: fe80::b8d5:e2ff:fefe:dacd | MAC: ba:d5:e2:fe:da:cd
March 22, 2024 7:19:36 PM
high
Inventory Events
New component detected on the network: fe80::4c8c:b4ff:feb4:9b2c (@ fe80::4c8c:b4ff:feb4:9b2c) | IP: fe80::4c8c:b4ff:feb4:9b2c | MAC: 4e:8c:b4:b4:9b:2c



CHAPTER 24

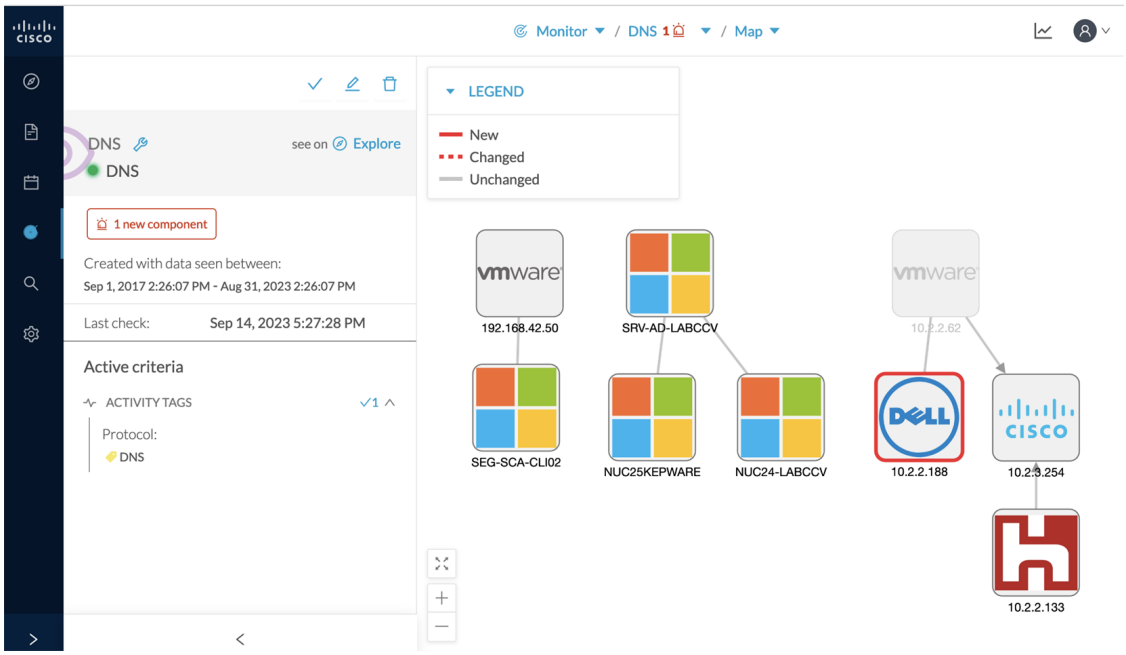
Monitor

For more information about the Monitor mode, refer to the Cisco Cyber Vision GUI Monitor Mode User Guide.

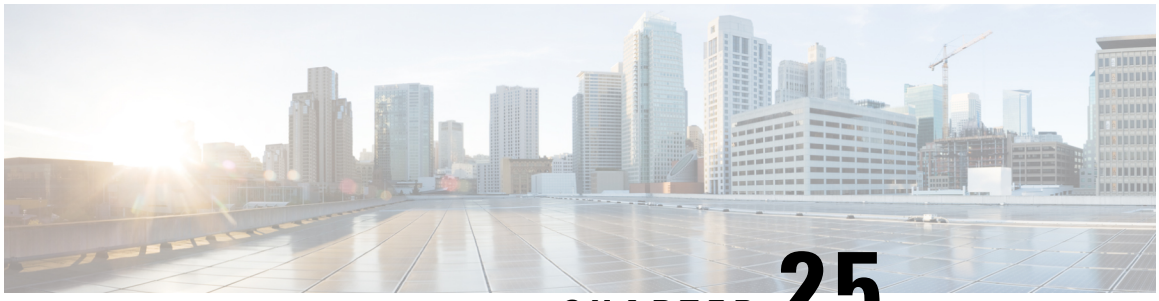
- Monitor, on page 105

Monitor

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



For more information, refer to the Cisco Cyber Vision GUI Monitor Mode User Guide available on cisco.com.



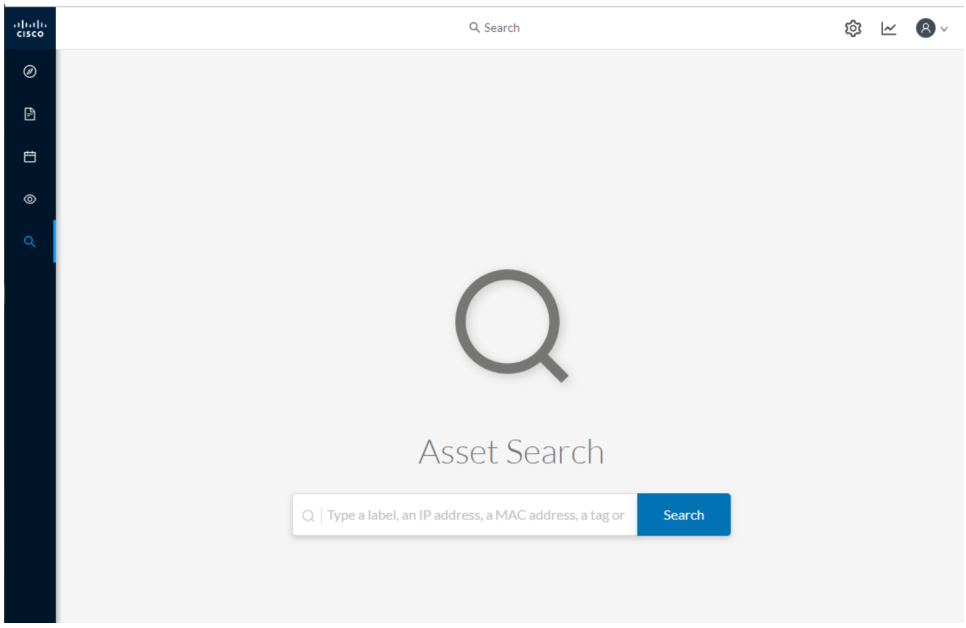
CHAPTER 25

Search

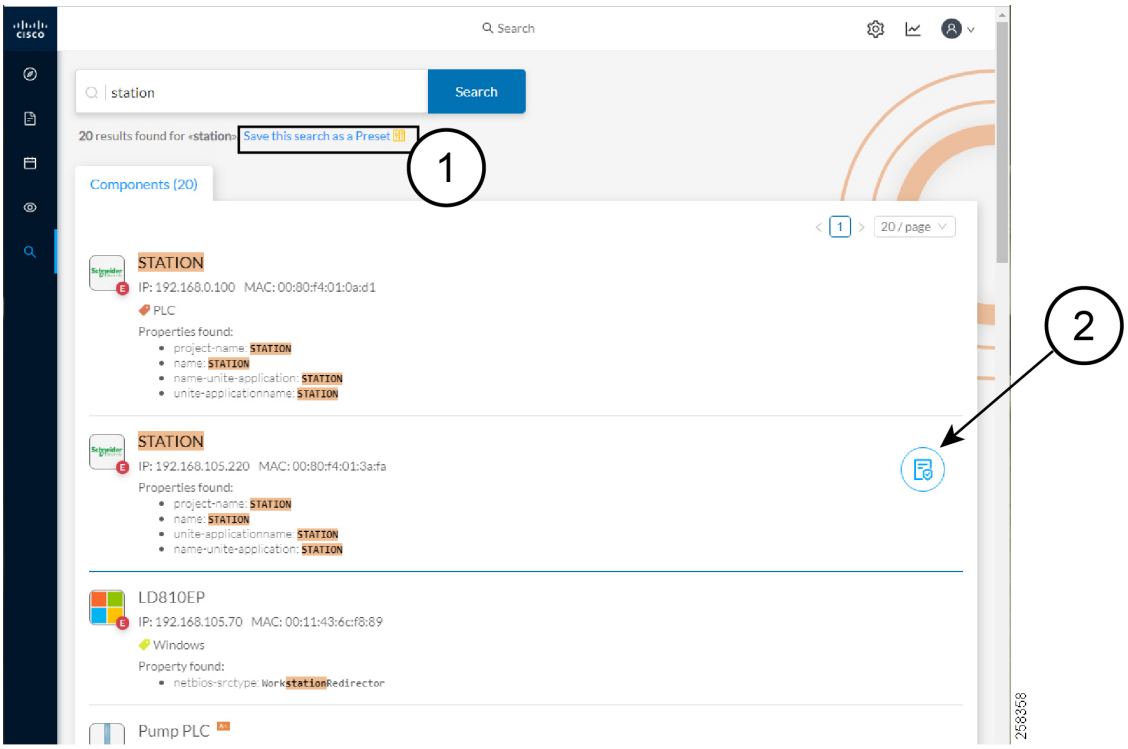
Search

Use **Search** to find components among unstructured data. Search components by name, custom name, IP, MAC, tag and property value.

Note Devices are not available in this page yet.



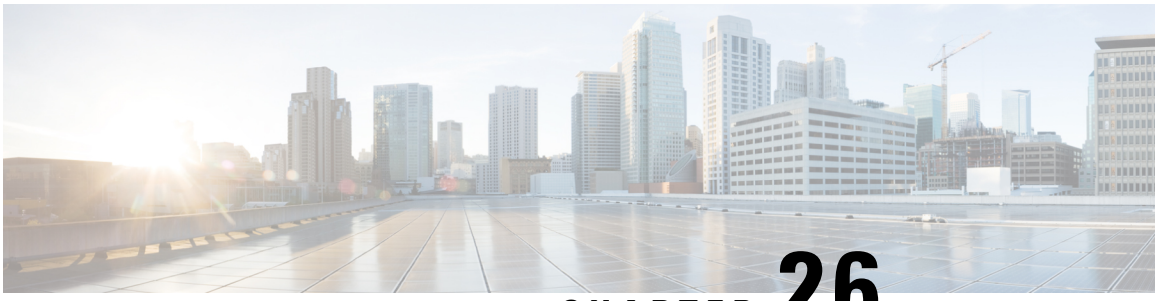
*Results out of a **Station** search*



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

Create a preset from your search results **(1)**. Presets created out of results will automatically update as new data are detected on the network.

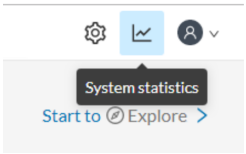
For more information about a component, hover over it. The Technical sheets **(2)** icon appears. The technical sheet gives you access to advanced data about the component.



CHAPTER 26

System statistics

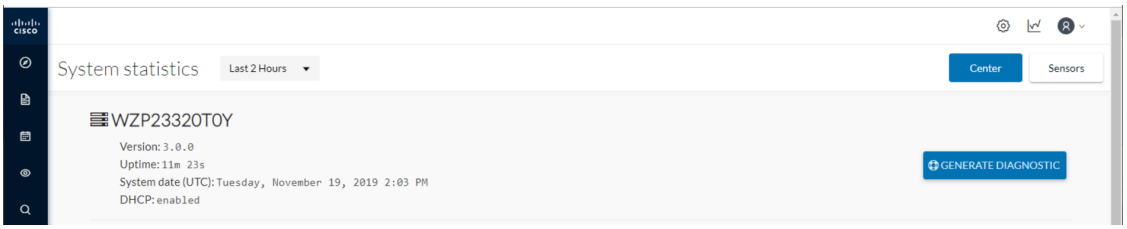
To access system statistics, click the **System statistics** icon in the top right corner of Cisco Cyber Vision interface.



Center

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

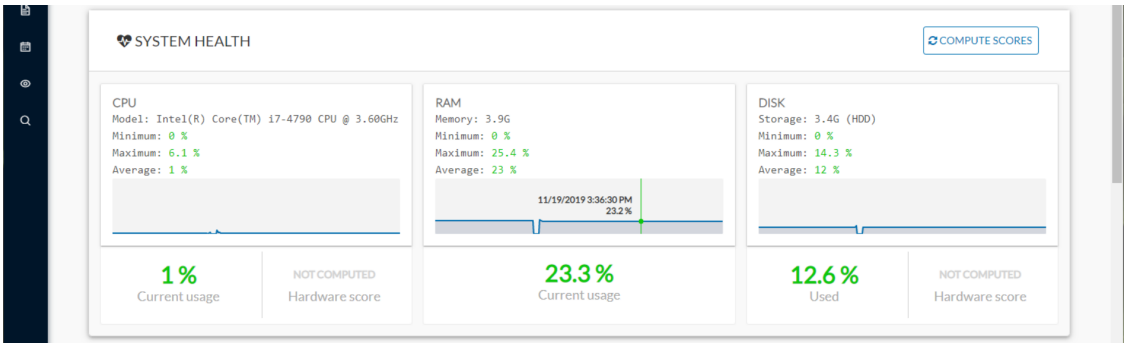
Note Use the drop-down arrow to change the time period.



The **Center** interface shows general information about the Center (the software version, the length of time that it has been operating (i.e., uptime), the Center system date and whether DHCP is enabled or not.

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

System Health



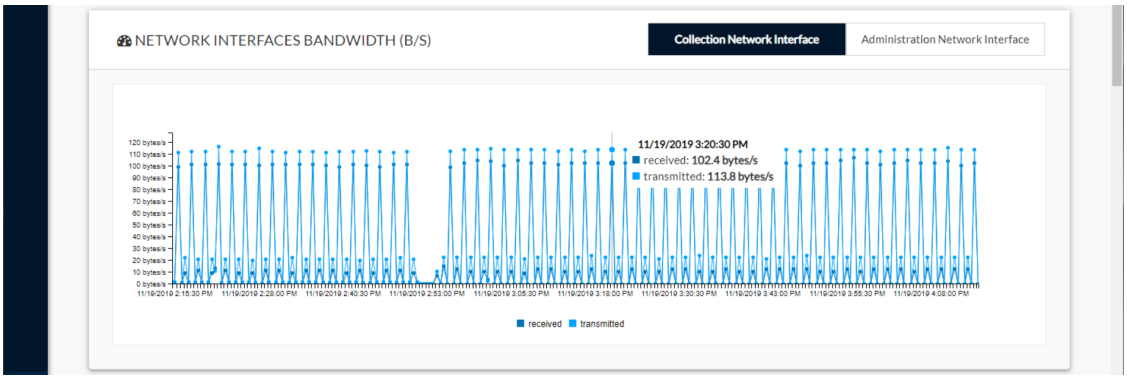
System health shows the status of the Center CPU, RAM and disk usage.

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

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

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

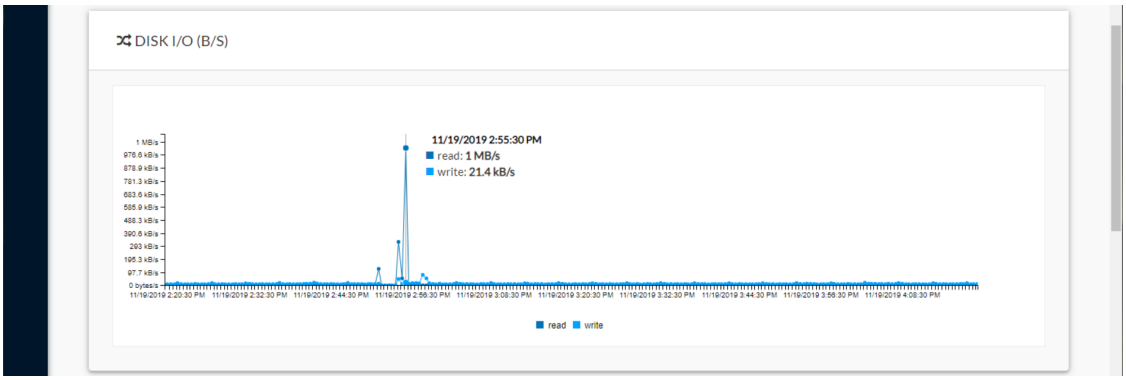
Network Interfaces Bandwidth



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

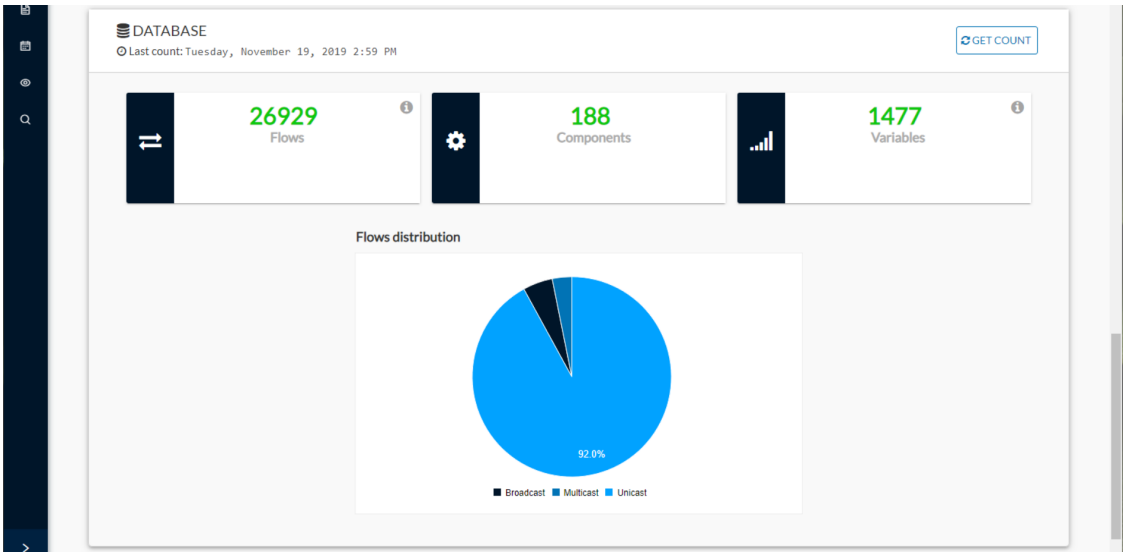
For example, the Collection Network interface activity lets you see the amount of data exchanged between the Center and the sensors.

Disk I/O



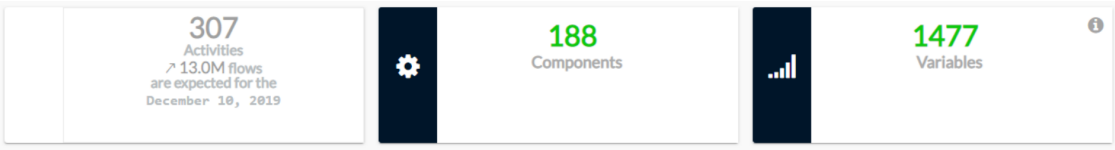
The line chart represents the Center hard disk usage in bytes/second.

Database

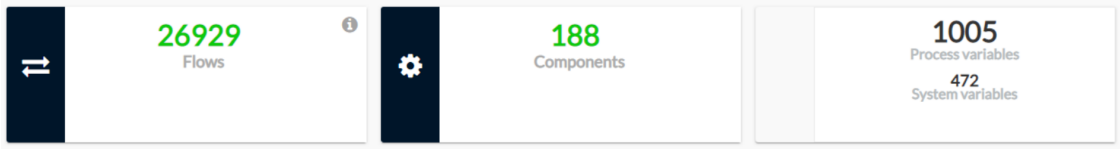


This section describes the database state by showing cards with the number of flows, components and variables that have been detected by Cisco Cyber Vision. Flows distribution is shown in a pie chart.

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

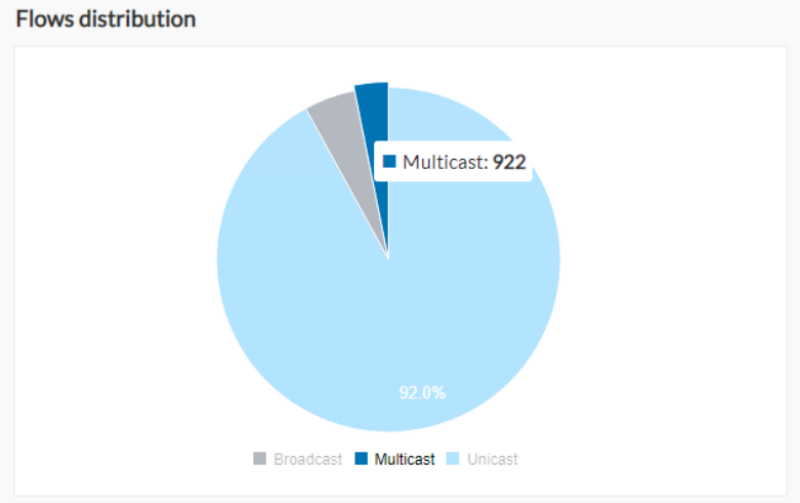


The flows card indicates the total number of flows (i.e. broadcast, multicast and unicast which are stored in the database) detected by Cisco Cyber Vision. If you mouse over the card, you will get the number of activities and the flows evolution tendency. This information enables you to anticipate how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

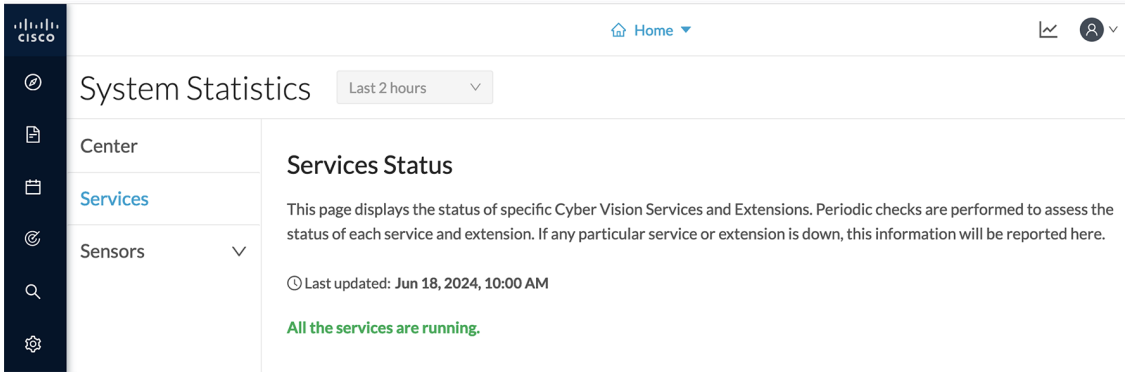
- Process variables are the number of variables used by PLCs' software. Process variables are visible in the Monitor mode of the Cisco Cyber Vision GUI.
- System variables are the number of variables necessary to PLCs' proper operation. System variables are stored in the Cisco Cyber Vision database.



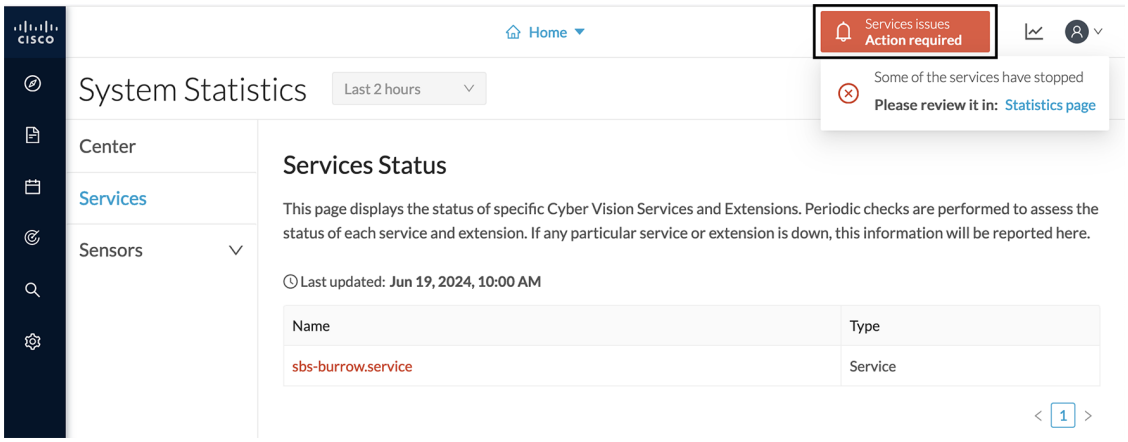
The flows distribution pie chart indicates the distribution of broadcast, multicast and unicast flows stored in the database. Mouse over the chart to see the absolute number of flows per flow type.

Services statistics

The service status page indicates whether all Cisco Cyber Vision background processes like services and extensions are up and running correctly. Checks are performed regularly.



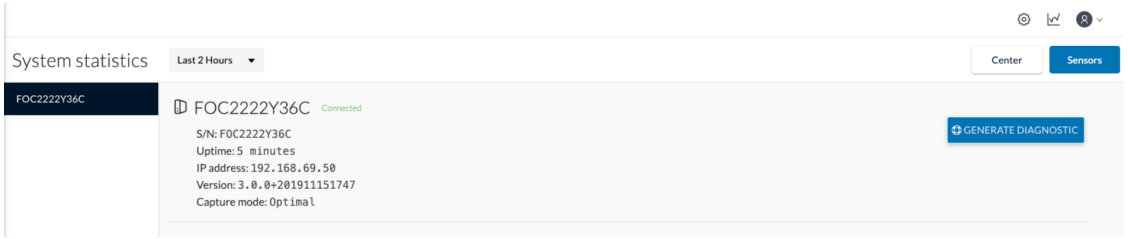
A warning banner appears at the top of the application whenever a service or extension is down with a link to this page. The failing service or extension will appear in red.



Sensors

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

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



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

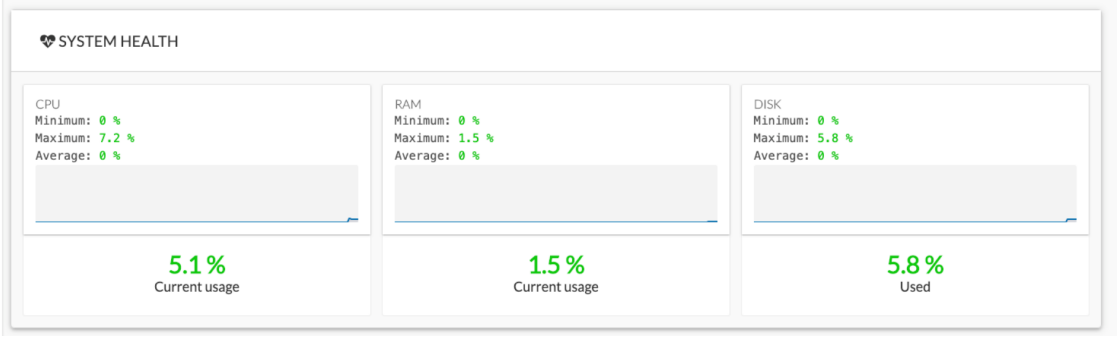
The **Sensors** statistics view shows general information about the sensor: the status (i.e., Connected), serial number, IP and MAC addresses, firmware version, the capture mode set, and the time it has been operating (i.e., uptime).

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

System Health

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

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

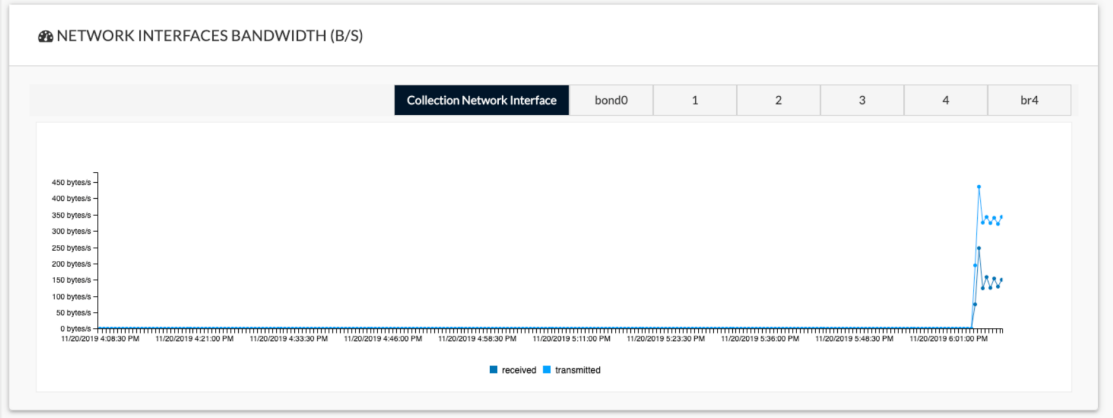


The chart also shows the percentage of the system's Current usage and Hardware score, useful to Cisco product support.

Captured Packets

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

Network Interfaces Bandwidth



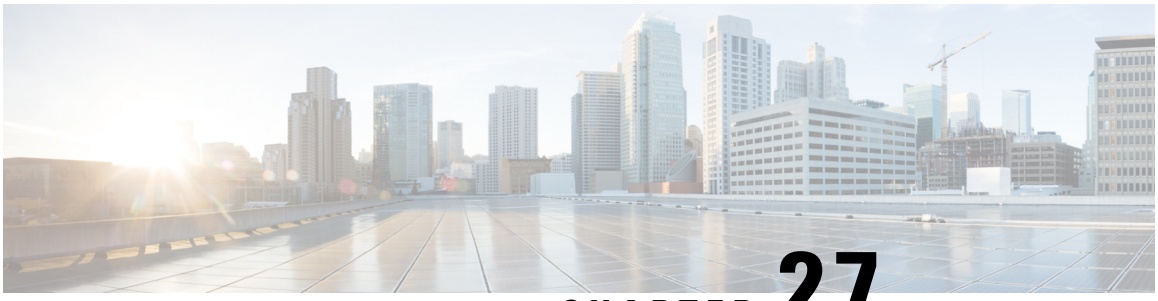
The line charts represent the Collection and Industrial network interfaces bandwidth with the number of bytes received and sent by the Center per second.

- The Collection Network interface activity chart shows the amount of data exchanged between the Center and the sensors.
- The Industrial cahrt shows the amount of data captured by the sensor on the industrial network through each port's couple.

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

Disk I/O

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

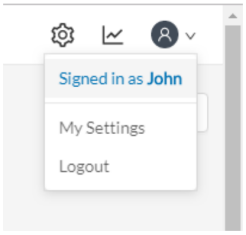


CHAPTER 27

My settings

My settings

Create your personal account by clicking **My Settings** in the user menu on the top right corner of Cisco Cyber Vision.



Insert or update the following:

- Your first and last name.
- The interface language. Cisco Cyber Vision is available in English, German, Spanish, French, Japanese, Korean, and Turkish.
- Your password.

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

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

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

Note Your email will be requested for login access.

- Restore interface notifications.
- Clear application cookies.