Introduction to Cyber Vision

Cisco Cyber Vision Installation

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

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

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

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

Overview

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

Interactive Help

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

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

Access Interactive Help

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

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

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

Procedure

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

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

Presets

Presets are sets of selection criteria that

- enable focused filtering of network metadata processed by Cyber Vision,
- provide rapid access to views matching specific business needs, and
- offer multiple perspectives for efficient navigation of network data.

Presets are designed to simplify navigation and enhance business-oriented visibility into network activity and status, based on recommendations from Cyber Vision playbooks.

Preset views

A preset view is a display mode that

- stores data elements, such as components, tags, and activities,
- refreshes only when necessary or upon explicit user request to reduce system load, and
- optimizes system performance to prevent lags and application crashes, especially when managing large data flows.

Preset views help prevent system overload by showing previously computed data and relying on user actions for updates. This benefits users who interact with preset views frequently or occasionally.

Behavior of preset views

- The elements visible in preset views are based on the last completed computation.
- Data displayed in the user interface and database are asynchronous, lowering workload on the GUI.
- Computation frequency adapts to preset usage. Presets that are viewed frequently are recomputed often. Presets that are not used are skipped.
- An automated background process computes data when a preset is active, but does not auto-refresh the display.
- Two update buttons are available in preset views:
  - New data button: Appears when new computation is available, but the updated view may not show all new data.
  - Refresh button: Forces data computation and a full view refresh, which consumes more system resources. Use this when you expect changes, such as a new device or custom data updates.

Types of preset views

You can access different preset views for various perspectives. To do this, open the main menu, select **Explore**, and use the top navigation bar to choose a preset.

Table 1: Views

Name	Description
Dashboard	The dashboard view appears by default and gives you a preset data overview. This tag-oriented view lets you quickly review the network at a high level.
Map	Use the map view to see how devices and components in your industrial network are connected. You can organize them into groups and explore the network structure. The map view then shows devices, components, and activity based on your selected criteria. It also shows grayed-out items if they are needed to represent preset activities, even if they don't match the criteria.
Device list and Activity list	Use these views to filter and find specific data. You can see both general and technical details for each element in the preset.
Vulnerabilities	This view displays and lists all vulnerabilities detected in a preset.

Name	Description
Security Insights	Each tab displays the most frequent requests, the least frequent requests, and a list of all requests for you to review. **Flows with no tag**: This section lists traffic that Cyber Vision Center cannot analyze, often due to the use of unsupported protocols. To resolve this, first verify that the content should be on the network. Next, determine why analysis is not possible. Finally, check flows with a high number of packets.
Purdue Model	Use the Purdue model view to see how assets in your preset are distributed across the layers of the Purdue model architecture based on tags. This view organizes assets into those layers: • 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)

Communication display options in map preset view

Cyber Vision Center offers three options for presenting communications in the preset map view.

Table 2: Map view options

Option	Description
Show all activities	You can view all activities between groups or individual devices.
Aggregate activities by group	The system increases map readability by grouping and displaying communications between device groups.

Option	Description
Show only zones and conduits	To optimize performance with large data sets or to get a broad overview, show only top-level groups (zones) and summarized communications (conduits) between them. Devices not assigned to any zone appear in a separate group called **Ungrouped**. If group hierarchies segment the control system, the map displays zones and conduits that meet ISA/IEC 62443 standards. A conduit appears as a thick, dashed line and shows communication between two groups. If both the source and destination groups are known, an arrow indicates the direction of communication. By default, Conduits View mode is enabled. To disable it, select **Aggregate activities by group**.

Default preset categories

Generic presets are available by default in Cyber Vision, based on recommended practices and operational categories.

Table 3: Default categories

Preset category	Presets available
Basics	View all data or filter to information technology (IT) or operational technology (OT) components. • All data • Essential data • Active Discovery activities
Asset management	Identify and inventory assets associated with OT systems, facilities, and IT components. • OT devices • IT devices • IT infrastructure devices • All Microsoft Windows systems • All controllers

Preset category	Presets available
Control Systems Management	Check the state of industrial processes. • OT activities • Control system activities • Process control activities
IT Communication management	Flows categorized as OT, IT, infrastructure, IPv6 communications, and Microsoft flows • IT activities • Web activities • Email activities • File activities • Microsoft activities
Security	Remote access control and insecure activity monitoring • DNS activities • Remote procedure call activities • Remote access • Insecure activities • Encrypted activities • Authentication activities
Network Management	Network detection issue identification and resolution • IT infrastructure activities • IT technical activities • IPv6 communications • Multicast traffic only • Broadcast traffic only

Create a new category

Create a category to organize and locate your custom presets easily.

Use categories to order and search custom presets. You can bookmark entries saved on the **Explore** page with URL filters in your browser for quick access.

Procedure

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

Step 2 Click **New Category**.

Step 3 Enter the name and preset details.

Step 4 Click **Create**.

The new category appears on the **Explore** > **All Presets** page.

What to do next

- You can edit the category name and preset details or delete the category from **Explore** > **All Presets**.
- You can search for categories on the **Explore** page to view associated presets.

Create a new preset from an existing data set

Create a customized preset by selecting criteria from an existing data set tailored to your business logic

Customized presets help you tailor views to your operational needs. Presets that you create are available to other users.

Procedure

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

Step 2 Select a predefined data preset from the **All Presets** list.

Step 3 Select the required criteria from **RISK SCORE**, **NETWORKS**, **DEVICE TAGS**, **ACTIVITY TAGS**, **GROUPS**, and **SENSORS**.

Step 4 Click **Save as**.

Step 5 Enter a new **Name** and select a **Category**.

Step 6 Click **OK**.

Your new preset uses the filter criteria you selected and appears in the category you chose.

What to do next

- Search for the selected category on the **Explore** page to view the newly created preset with your filter criteria.
- You can edit or delete presets from the **Explore** page.

Understanding Concepts

Filters

To access the filters, follow these steps:

1. From the main menu choose **Explore**.
2. Click the drop-down arrow in the top navigation bar and click **All Data** under **Basics**.
3. Click the drop-down arrow in the third filter of the top navigation bar and click **Dashboard**.

Create presets using the following filters:

Criteria

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

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

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

Risk Score

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

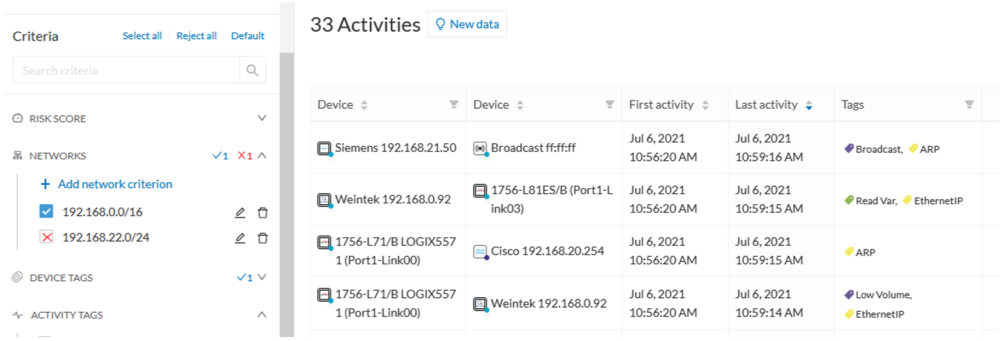
Networks

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

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

For instance, use exclusion and combination for this result:

Network filter – negative filter



Multiple negative selections are not supported on 4.0.0.

Filter combination

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

Device tag filters

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

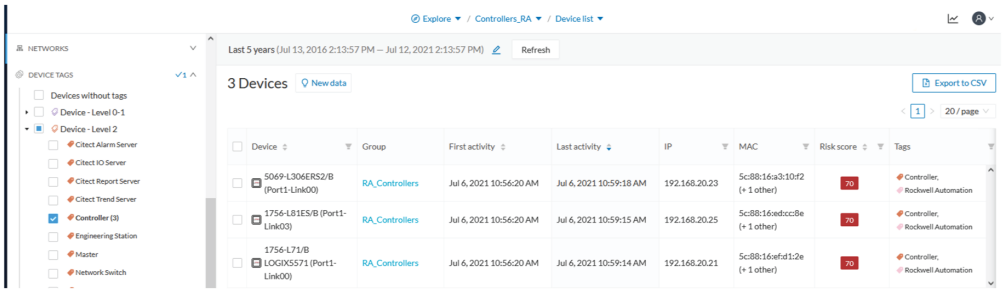
Device tag filters

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

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

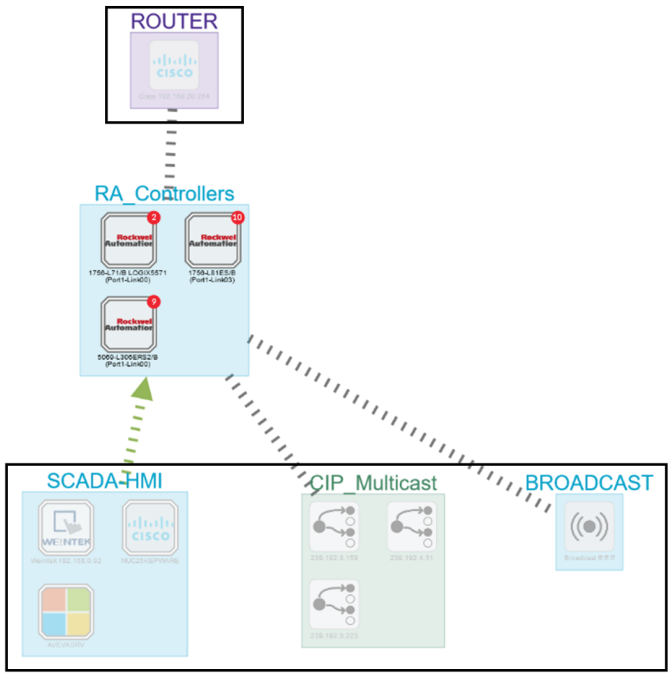
It will give the following results:

Device tag filter, example of Controllers – list of devices



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

Device tag filter, example of Controllers - map

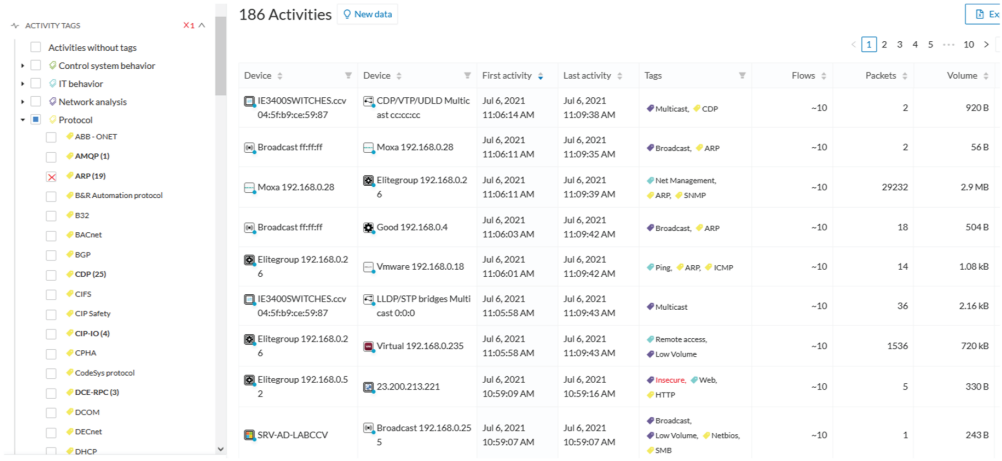


Activity Tags

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

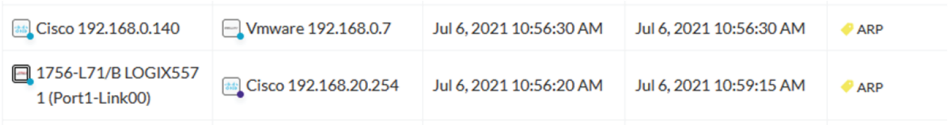
For example, if an activity has two tags, both tags need to be excluded to hide the activity.

Activity filter – negative filter 1



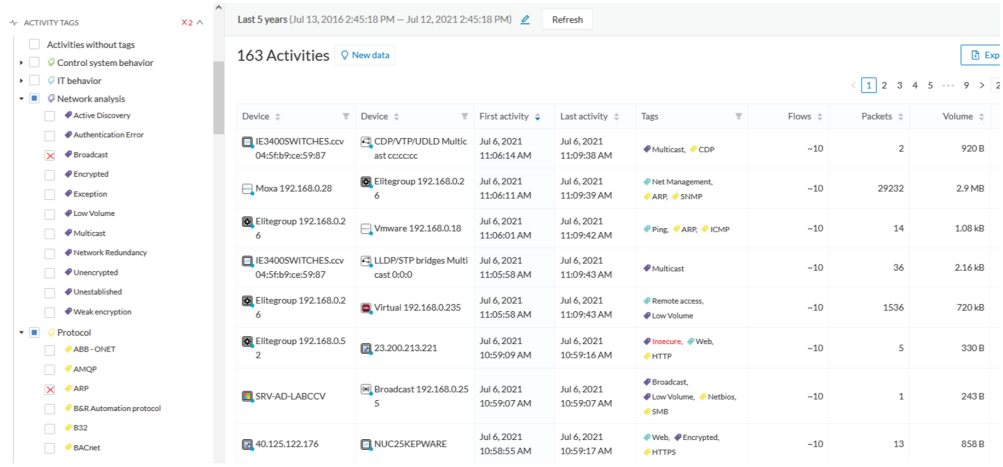
In the example above, several activities show because the ARP tag is present, as well as other **Activity tags**. There is no exact match. The activity below is hidden.

filter 2



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

Activity filter – negative filter 3



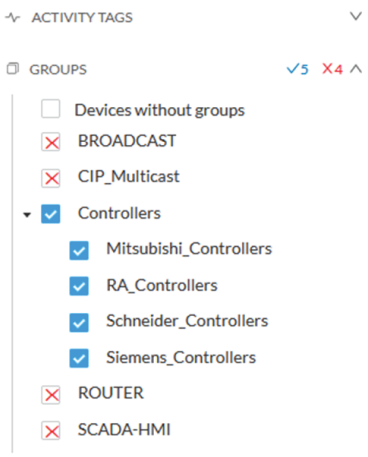
For very specific use cases, combine inclusive and exclusive tags. The above rules, for positive and negative selection, are combined, resulting in the following logic:

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

Groups

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

Group filter



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

Sensors

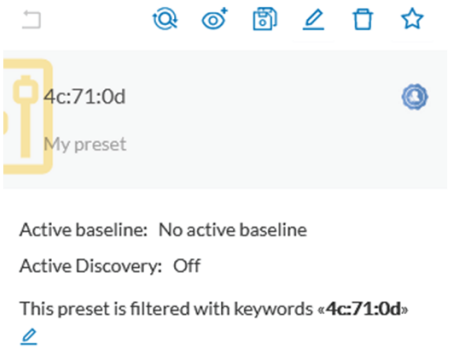
Filter Activities based on the sensor that analyzed the associated packets. For tags, use inclusive and exclusive filters. Usually, either option is used but not both. Inclusive: selects data coming from a set of sensors. Exclusive: Ignore the data from a set of sensors.

Sensor filter

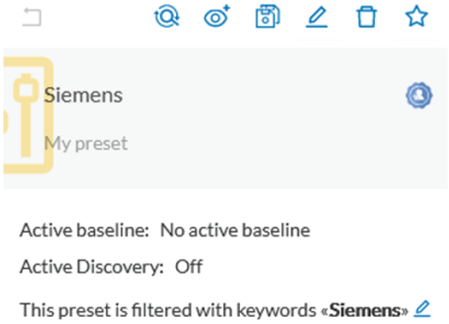
Keyword

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

Keyword = 4c:71:0d



Keyword =siemens



Filter combination

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

Component

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

Some examples of icons:

Manufacturers' icons	SIEMENS	EMERSON	CISCO	

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

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

For more information, refer to the Device section.

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

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

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

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

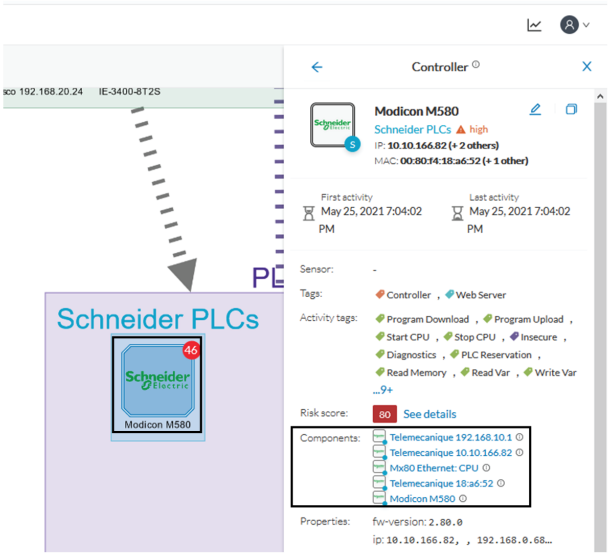
Device

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

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

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

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



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

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

5 Components

Component	First activity	Last activity	IP	MAC	Tags	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.

Activity

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

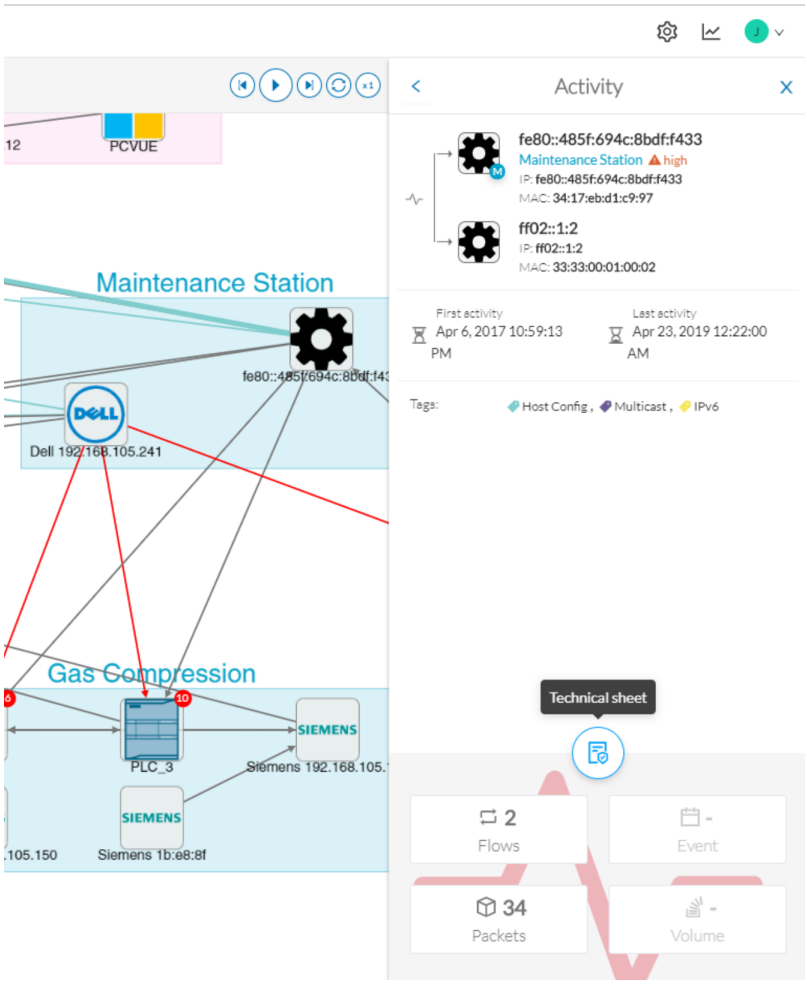
To access the map, choose **Explore** > **Control Systems Management** > **OT Activities** from the main menu. Click a component on the map to view its details.

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

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

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

- The number of packets.
- The volume of data exchanged.
- The number of events.
- A button to access the technical sheet that shows more details about tags and flows.

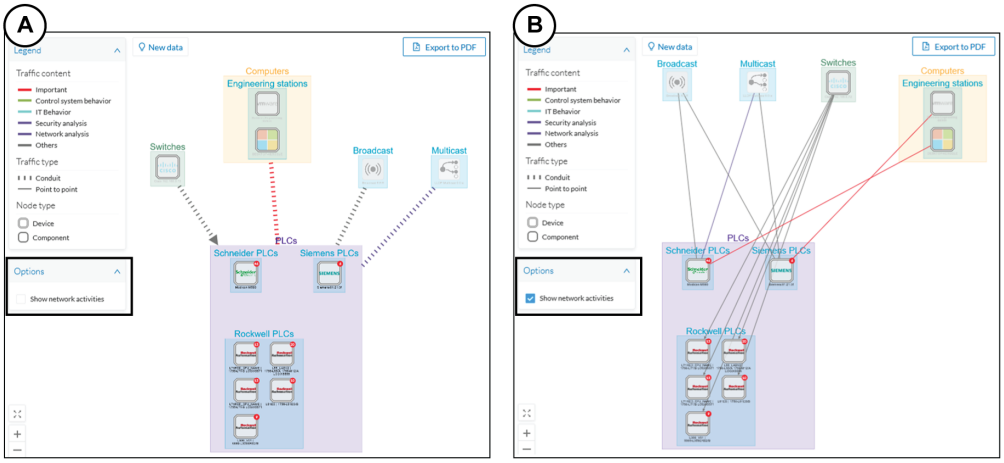


Devices or components with no activity does not mean that they did not have any interaction. In fact, a component can only be detected if it has been involved in a network activity (communication emission/reception). Lack of activity can mean that the other linked component is not part of the preset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

Aggregated activities or conduits

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

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



Flow

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

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

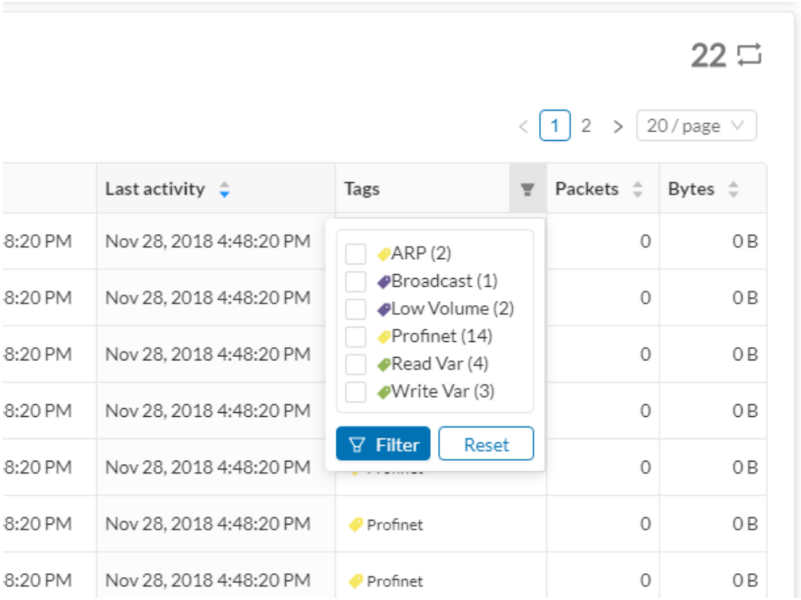
The Activity tab contains a list of flows which gives you detailed information about each single flow: number of flows in the activity, source and destination components (if known), ports used, first and last activity, and tags which characterize each flow.

Flows 12467

< 1 2 3 4 5 ··· 624 > 20 / page

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

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



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

External Communication

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

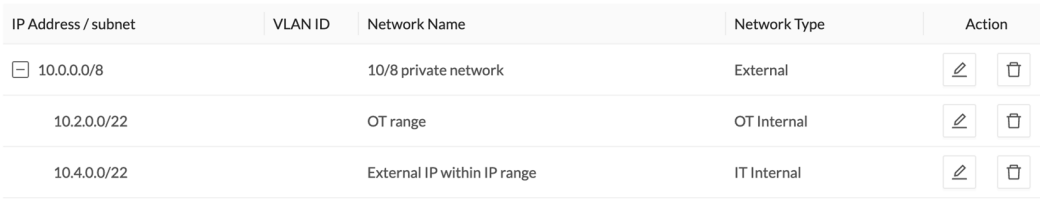
External communications are stored and listed in Cisco Cyber Vision, but not the external components/devices, nor their flows, to not obstruct the system. As a result, Cisco Cyber Vision's performances are increased, the GUI is cleared from unecessary data, and the license device count and risk scores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

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

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

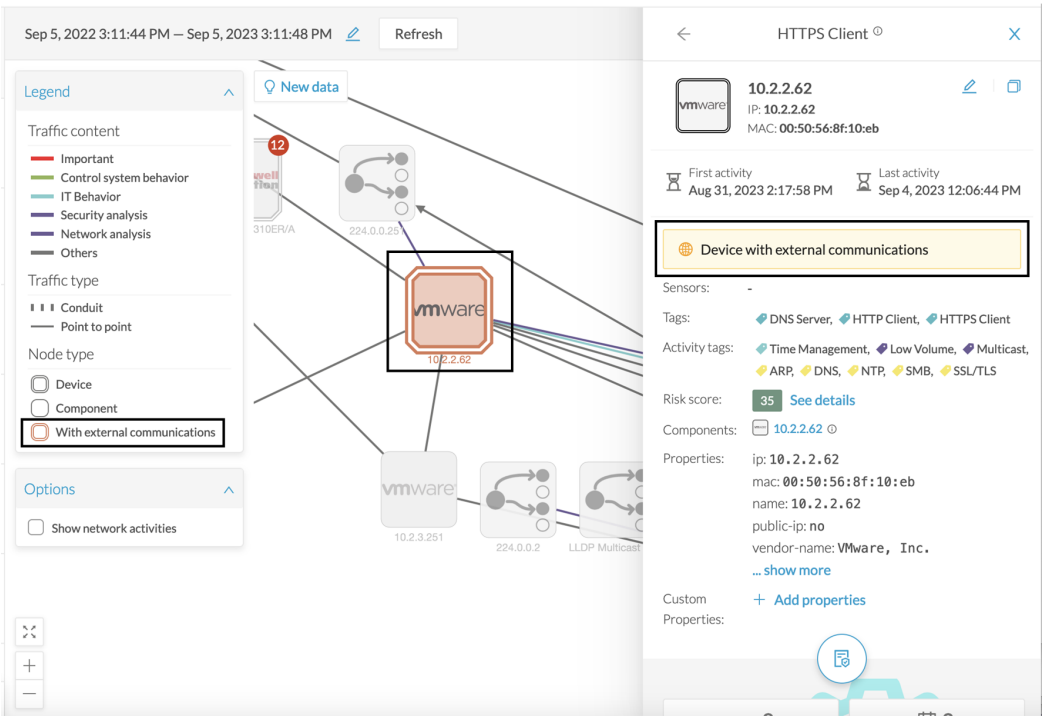
However, because sometimes public IP addresses are used in a private network of an industrial site, it is possible to manually define communications by declaring IP ranges as internal or external through the Network Organization administration page. For more information, refer to Cisco Cyber Vision GUI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

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



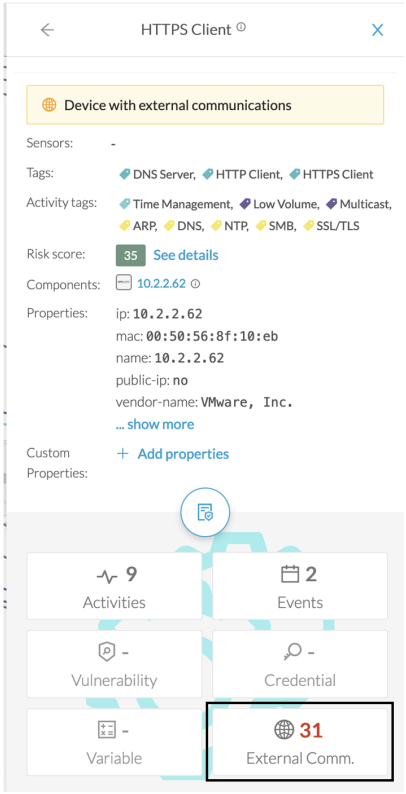
In the GUI, a component with external communications is shown as an icon bordered in orange, or a double orange border for a device.

A device with external communications in the Map:

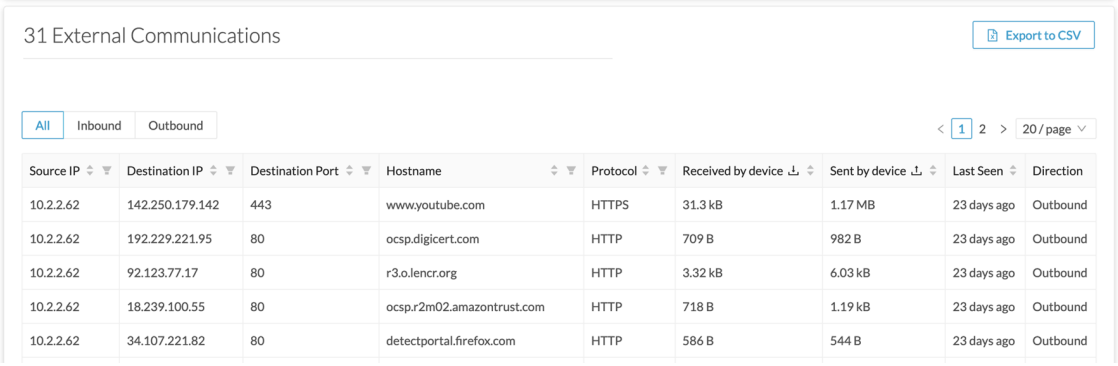


If you click on this component, its right side panel will appear. The **External Communications** button with the number of external communications will open the component's technical sheet directly on the external communications list.

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



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



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

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

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

Time Span

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

To access the timespan settings, follow these steps:

- From the main menu, choose **Explore** > **All data**.
- Click the dropdwn arrow at the top center of the page.
- Select **Device list** from the drop-down list.
- To set a time span, click the pencil icon.

  The **TIMESPAN SETTING** window appears.
- To set a **Duration**, click the drop-down arrow and select duration time (from 10 seconds to 1 day) or a custom period up to the present.
- To set a **Time window**, select a start date and (optionally) an end date.

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

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

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

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

Recommendations:

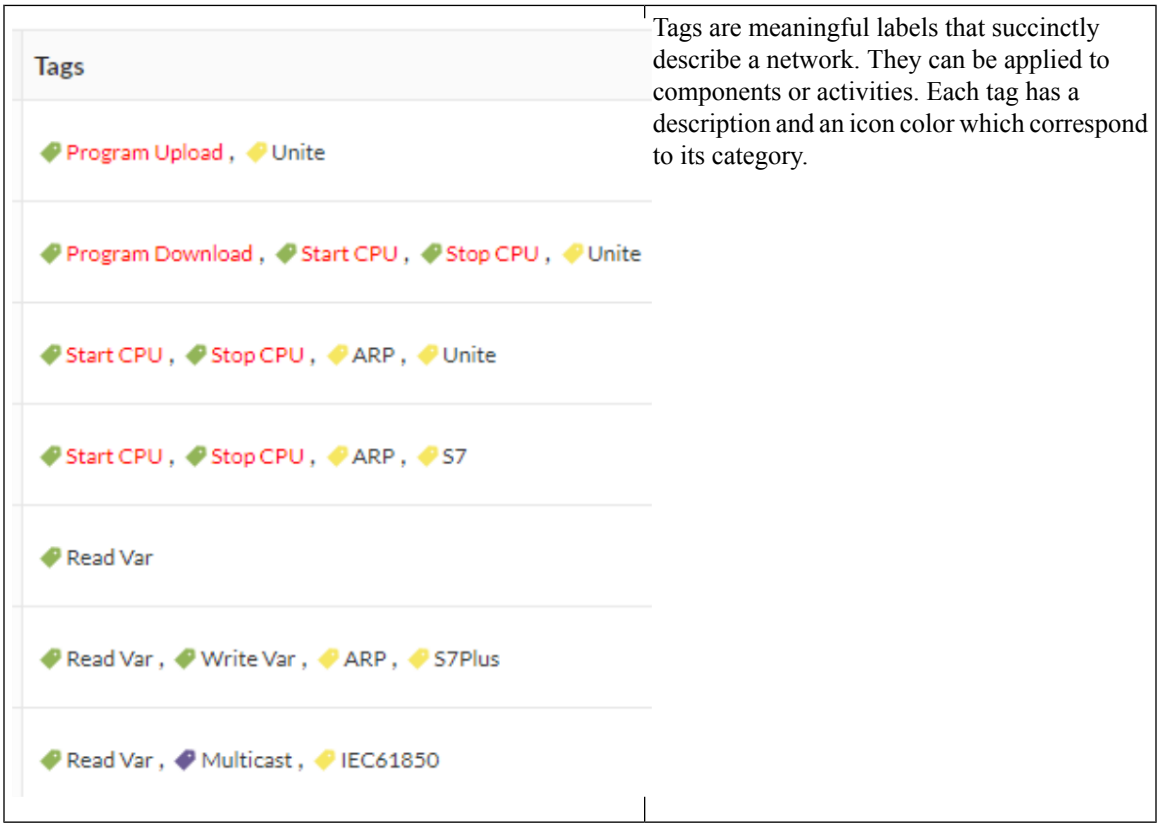
Generally, you can set the time period to 1 or 2 days. This setting is convenient to have an overall view of most supervised standard network activities. This includes daily activities such as maintenance checks and backups.

Adjust the time frame for the following:

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

Tags

Definition of Tags



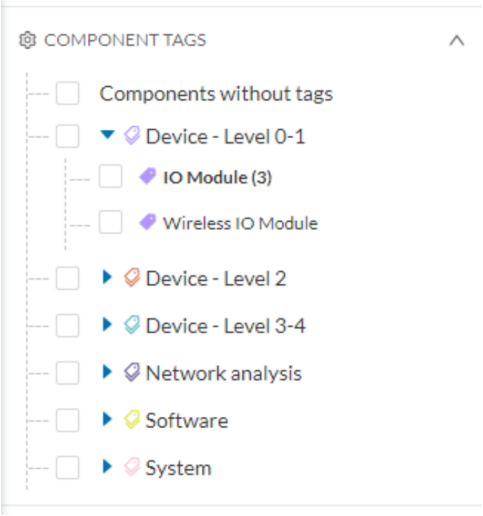
Tags are meaningful labels that succinctly describe a network. They can be applied to components or activities. Each tag has a description and an icon color which correspond to its category.

Tags are metadata on devices and activities. Tags are generated according to the properties of components. There are two types of tags:

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

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

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



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

Tag Use

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

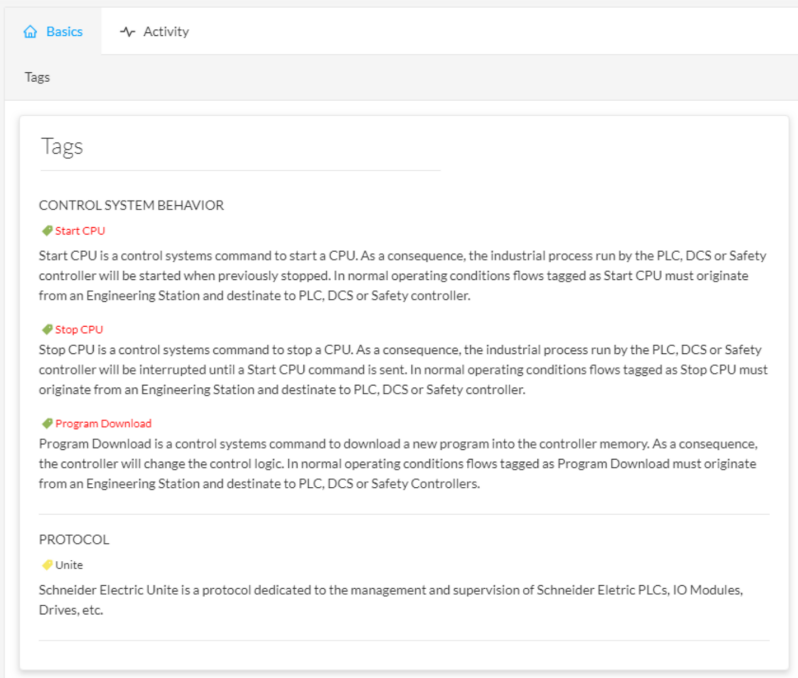
Use tags to define behaviors (i.e., in the Monitor mode) inside an industrial network when combined with information like source and destination ports and flow properties.

Tag Location

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

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

Below is an example of tag definitions.



Properties

Property Definition

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

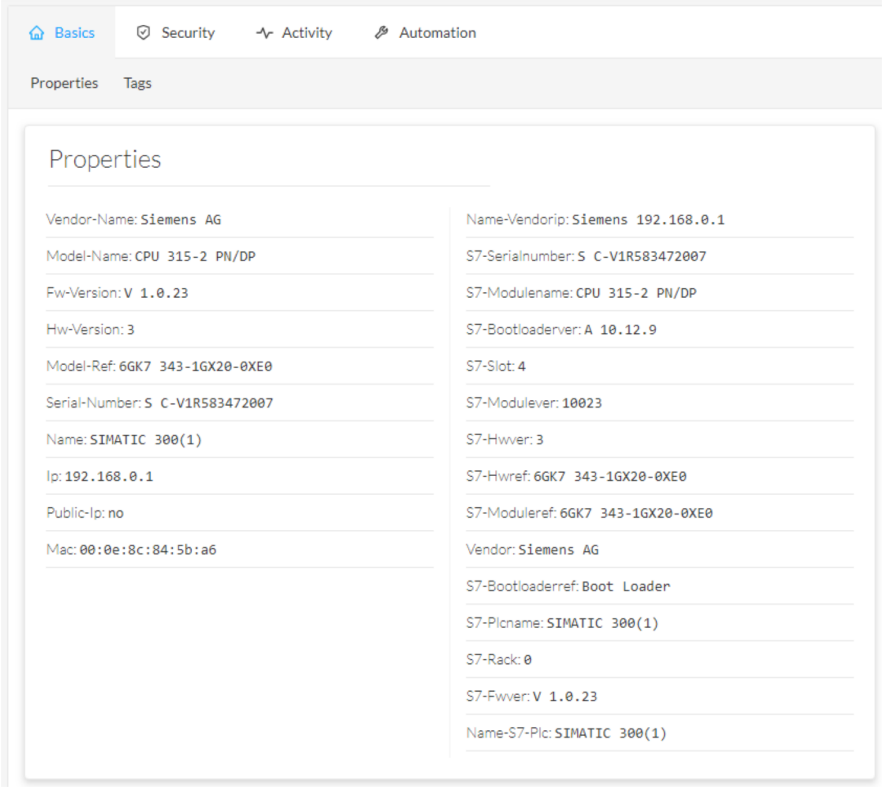
Property Use

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

Property Location

View Properties from devices and components right side panels and technical sheets under the **Basics** tab.

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



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

Vulnerability

Definition of Vulnerabilities

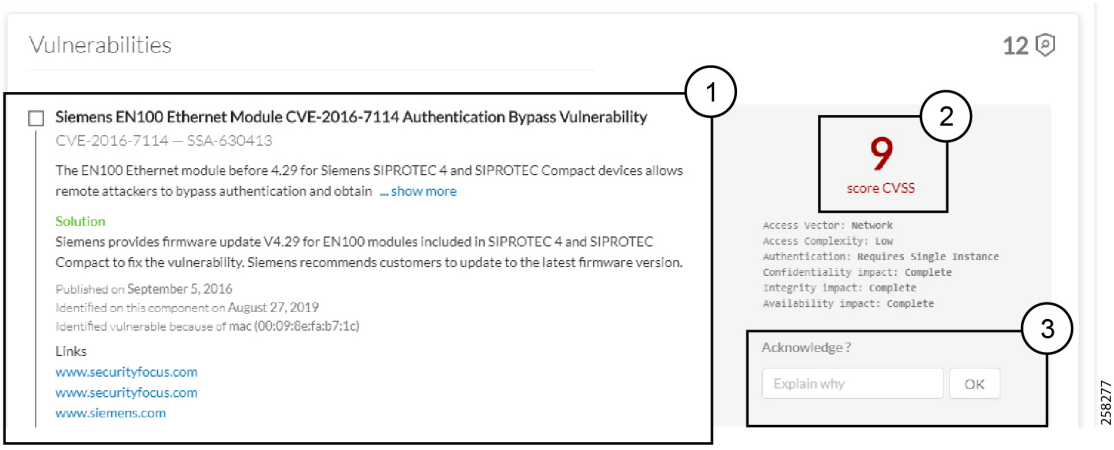
Vulnerabilities are weaknesses detected on devices that can be exploited by a potential attacker to perform malevolent actions on the network.

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

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

Vulnerability Use

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



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

Vulnerability Location

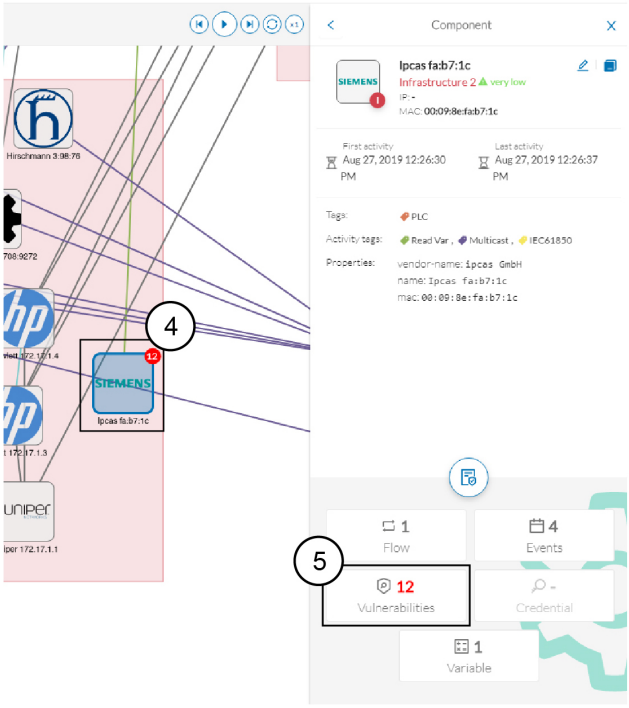
Access Vulnerabilities in any of the following ways: click **Explore > All Data > Vulnerabilities**, use **Vulnerabilities** preset view, or through the **Device list**. Use the **Sort arrows** to view the vulnerability column.

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

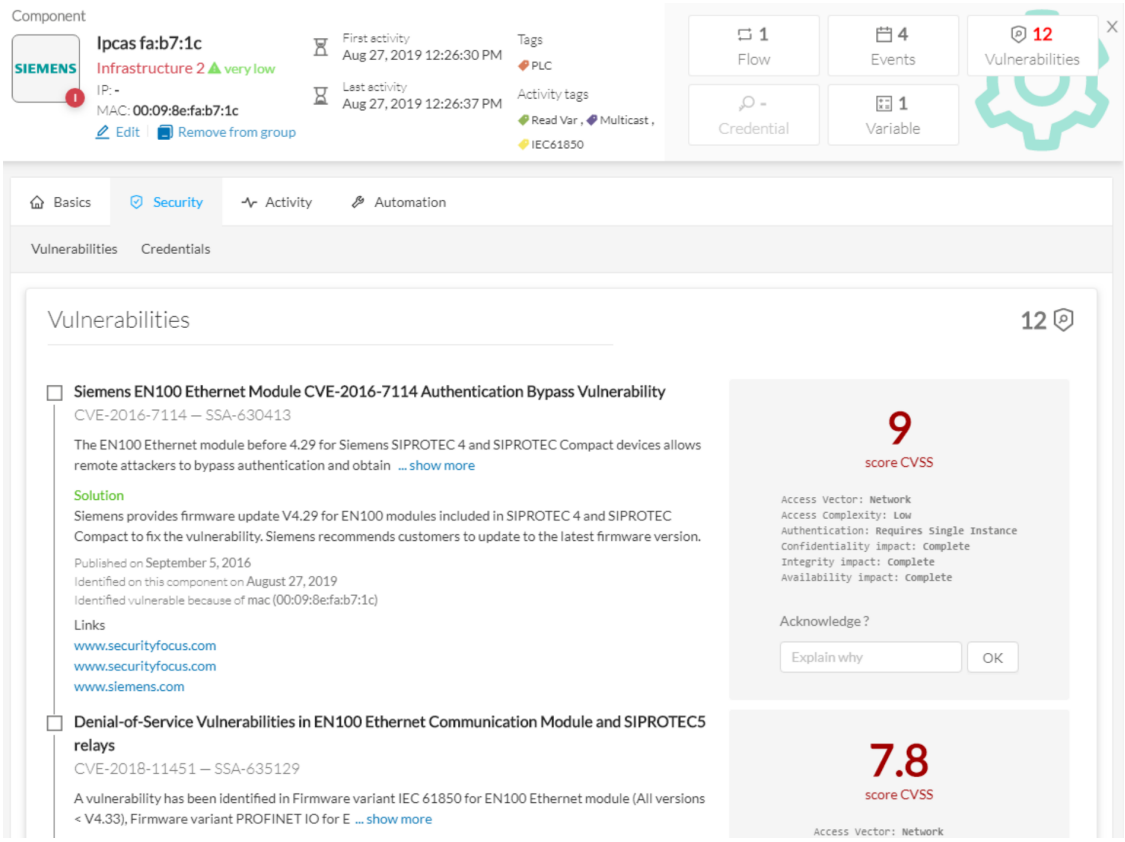
Sort

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

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



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



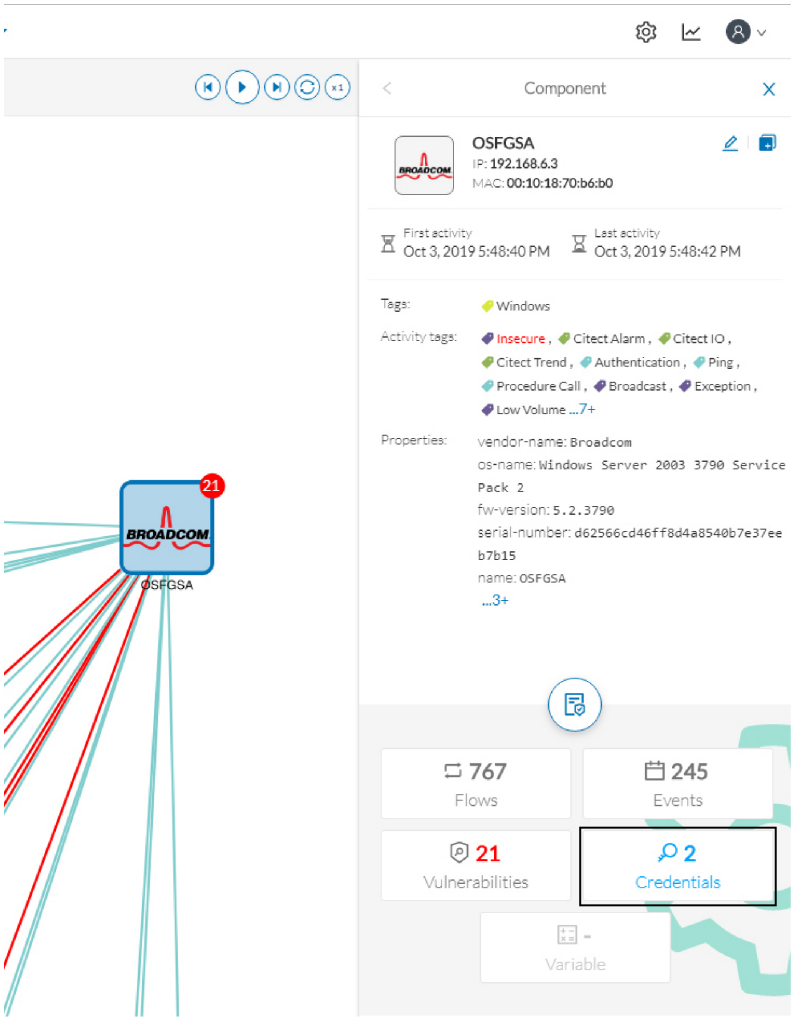
Events

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

Credentials

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

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



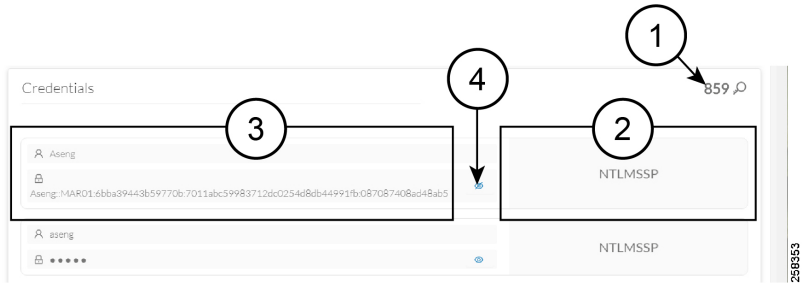
Credential frames are extracted from the network in Deep Packet Inspection. Use the technical sheet of a compoent to access **Credentials**. Click the **Security** tab.

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

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

An unsafe password:

A hashed password:



Variable accesses

Variable accesses are process control monitoring records that

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

Table 4: Feature History Table

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

Significance of variable accesses

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

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

Examples:

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

Variable accesses details

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

Table 5: Fields in the variable accesses table

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

To locate variable access information

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

Enable variable processing in a sensor template

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

Before you begin

Enable **Variable Storage**.

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

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

Procedure

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

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

Note
You can also create a new template.

Step 3 Locate the protocols with variable inspection capability.

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

Step 5 Save changes.

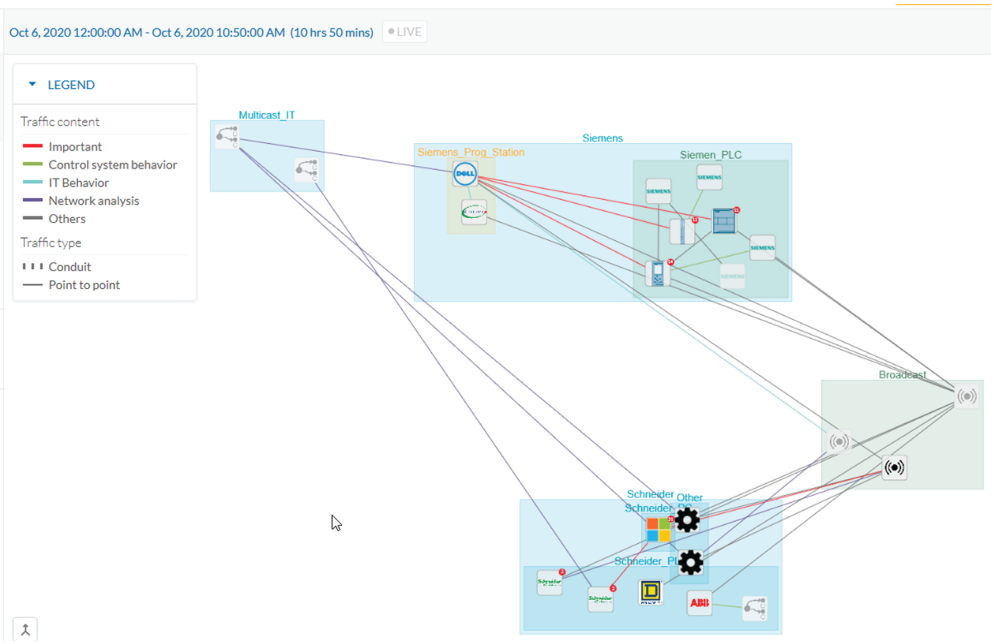
After you complete the configuration, the center sends information to the sensors. The sensors process and identify the variables. You can view detected variables in the center.

What to do next

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

Creating and Customizing Groups

Accessibility: Admin, Product and Operator users



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

To create a group:

Procedure

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

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

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

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

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

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

Step 5 Click **Manage selection**.

The drop-down list appears.

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

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

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

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

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

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

Step 10 Enter **Properties**.

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

To create a parent group:

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

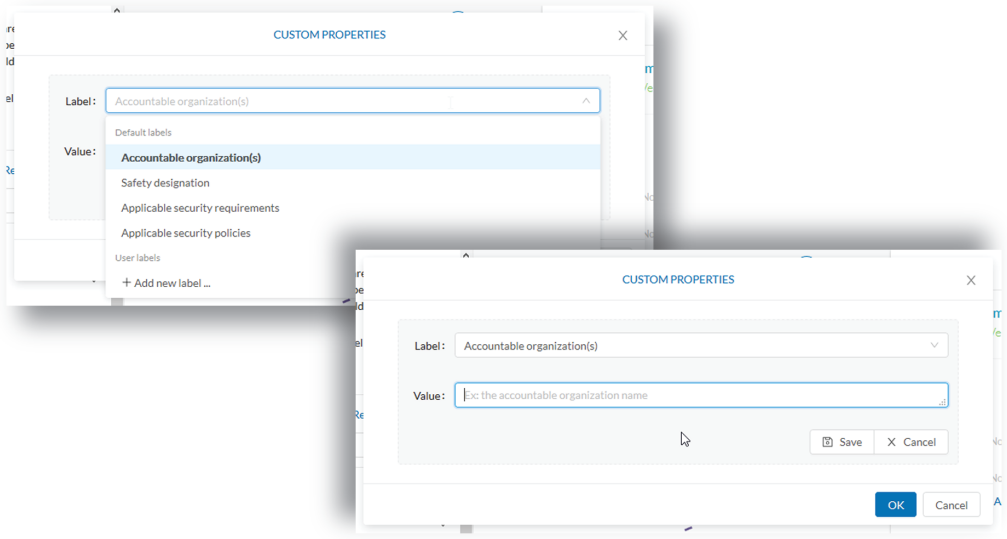
- Select two groups and create a group, as indicated above.
- Select a device or a component and move it into a group. Use the **Move selection to existing group** button.
- Select a group and move it to another group. Use **Move selection to existing group**.

Add group properties

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

To add properties to a group:

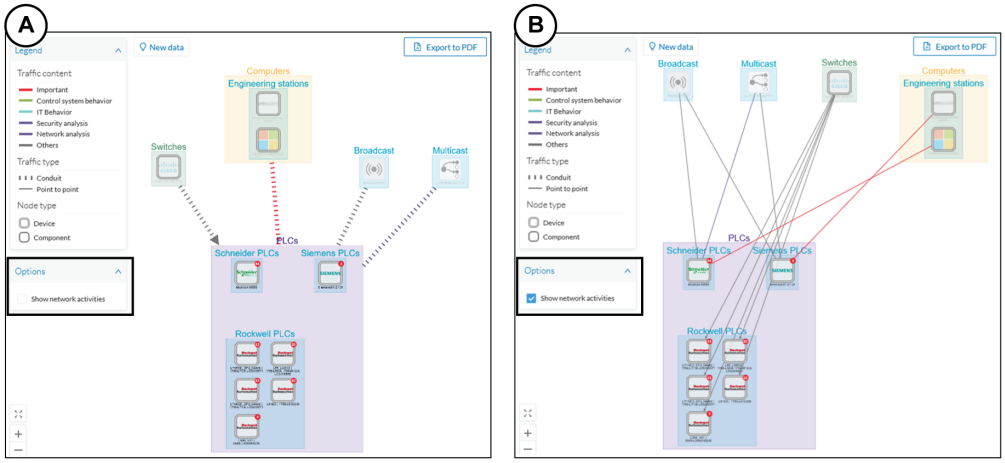
- Select a group in the map and click **Edit** or **Add properties**.
- Choose/define a label and add a value.



Aggregated activities are conduits

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

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



Group Lock/Unlock

Locking a group:

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

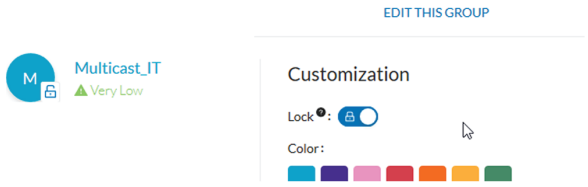
To switch on/off the **Lock** icon:

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

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

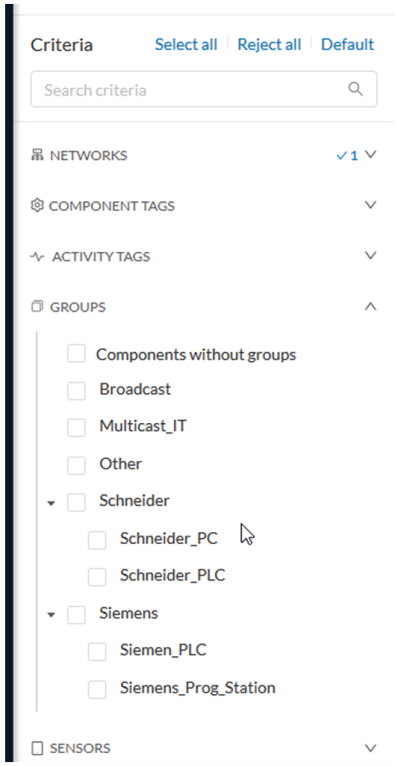
or

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



Step 14 **Groups used as criteria to filter data in Cisco Cyber Vision:**

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



Active Discovery

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

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

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

Active Discovery is available on the following devices:

- Cisco Catalyst IE3300 10G Rugged Series Switch
- Cisco Catalyst IE3400 Rugged Series Switch
- Cisco Catalyst IE9300 Rugged Series Switch
- Cisco Catalyst 9300 Series Switch
- Cisco Catalyst 9400 Series Switch
- Cisco IC3000 Industrial Compute Gateway
- Cisco IR8340 Integrated Services Router Rugged

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

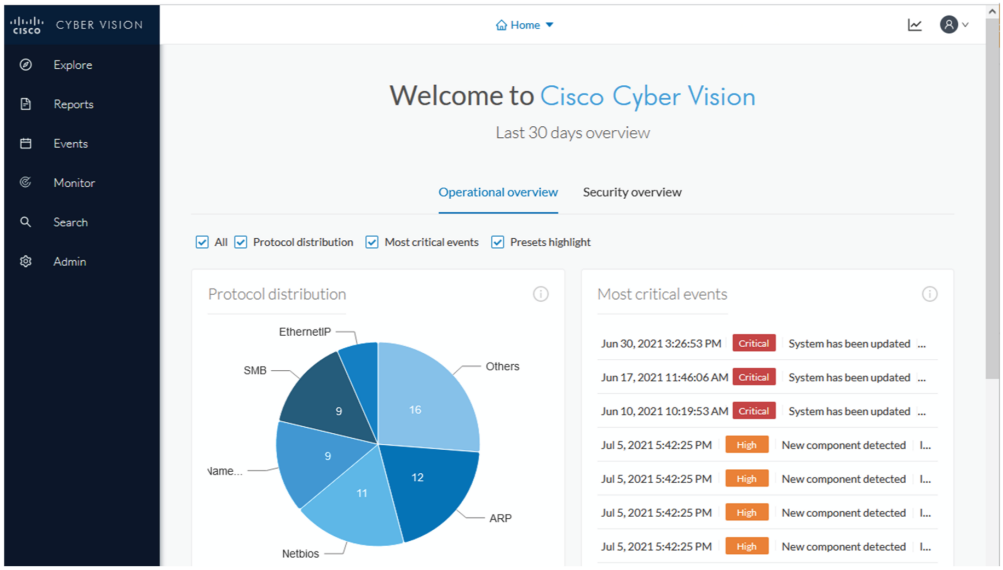
For more information and instructions on how to configure **Active Discovery** in Cisco Cyber Vision, refer to the Active Discovery Configuration Guide.

Navigating Through Cisco Cyber Vision

Home

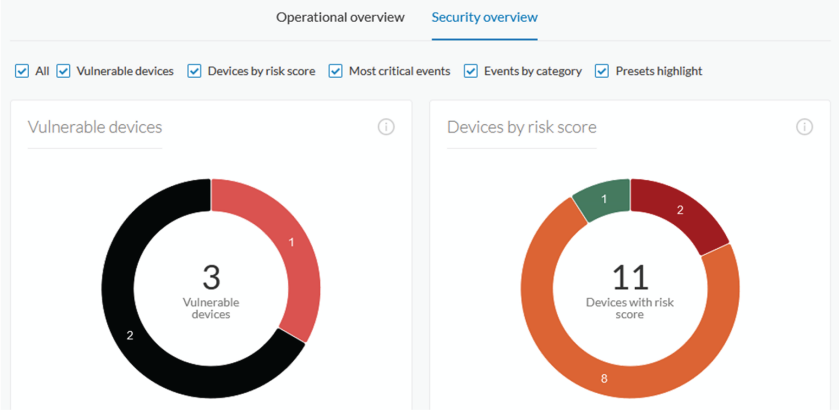
The Cisco Cyber Vision Center's home page displays two tabs: **Operational Overview** and **Security Overview** of the industrial network over the last month.

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



It also shows **Preset highlights**. Click **Edit favorite presets** to change what displays. Select the checkboxes of the presets and click **Save**.

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



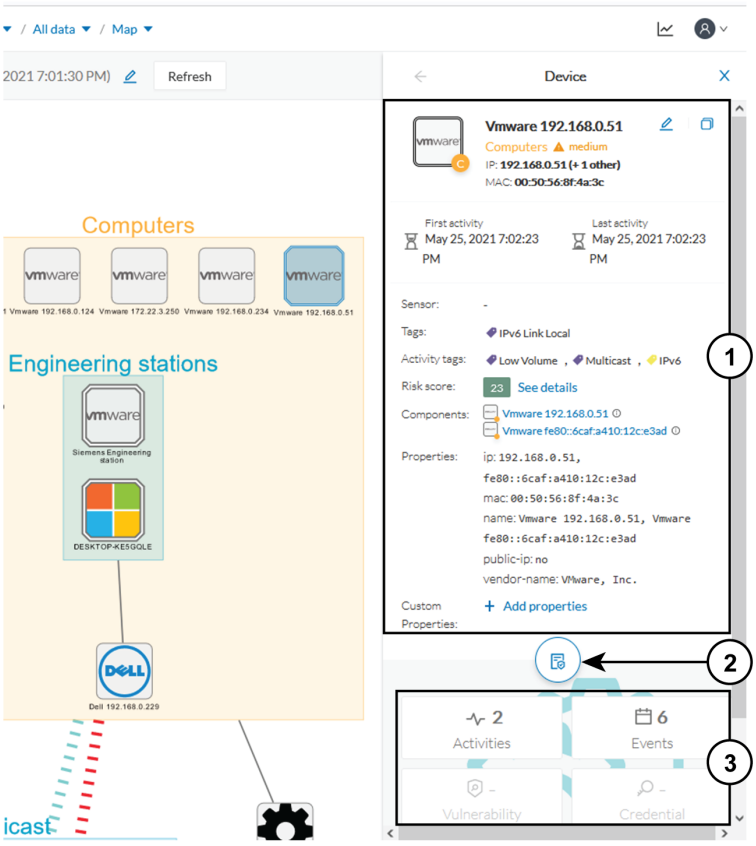
It also shows a list of the **Most critical events**, **Events by category**, and the **Preset highlights** that you can edit.

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

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

Detail Panel

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



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

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

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

Technical Sheets

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

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

1. From the main menu, choose **Explore**.
2. From the top navigation bar, click the drop-down arrow of **All Presets** and select **All Data** from the drop-down list.
3. From the top navigation bar, click the drop-down arrow of the third filter and select **Map** from the drop-down list.
4. Click the **Technical sheet** icon.

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

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

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

- More information about properties.
- More information about tags.
- More information about the risk score.
- More information about vulnerabilities.
- More information about credentials.
- More information about flows.
- More information about the Mini Map.
- More information about external communications.
- More information about variables accesses.

Mini Map

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

1. From the main menu, choose **Explore**.
2. From the top navigation bar, click the drop-down arrow of **All Presets** and select **All Data** from the drop-down list.
3. From the top navigation bar, click the drop-down arrow of the third filter and select **Map** from the drop-down list.
4. Select a device from the map.
5. Click **Technical sheet** from the **Details** panel.
6. Click the **Activity** tab.
7. To view an exploded view of the devices, check the checkbox of **Show inner components**.
8. Click any element in the Mini Map to open its Detail panel for access to more information.

Reports

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

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

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

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

Add a logo, such as your company's logo, to customize the report. The report displays Cisco's logo by default. Use the table of contents menu to set which content appears in the report.

Create a Report

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

Note Only users with 'Reports write' permission can create reports. Users with 'Reports read' permission can download reports.

Procedure

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

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

Step 3 Enter **Name**.

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

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

Report types are as follows:

- **Security Posture:**This report is an automated summary that captures all the vulnerabilities, risky acivities, and security events found on the devices in the selected preset by Cisco Cyber Vision.
- **Remote Access:**This report is an automated summary that captures a list of all Remote Access Gateways and the Remote Access related activities found on the devices in the selected preset by Cisco Cyber Vision.
- **Device Inventory**: This report provides an automated summary of devices, risk profiles, licensing requirements, and inventory distribution within the report's scope.

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

It will appear on the report.

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

Step 7 Choose the **Format**.

Step 8 Click **Next**.

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

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

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

Step 11 Click **Save and Run**.

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

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

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

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

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

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

Events

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

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

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

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

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

The following are examples of events:

- A wrong password entered on the GUI
- A new component connected to the network
- An anomaly detected in the Monitor Mode
- A component detected as vulnerable

The Dashboard of Events

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

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

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

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

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

The List of Events

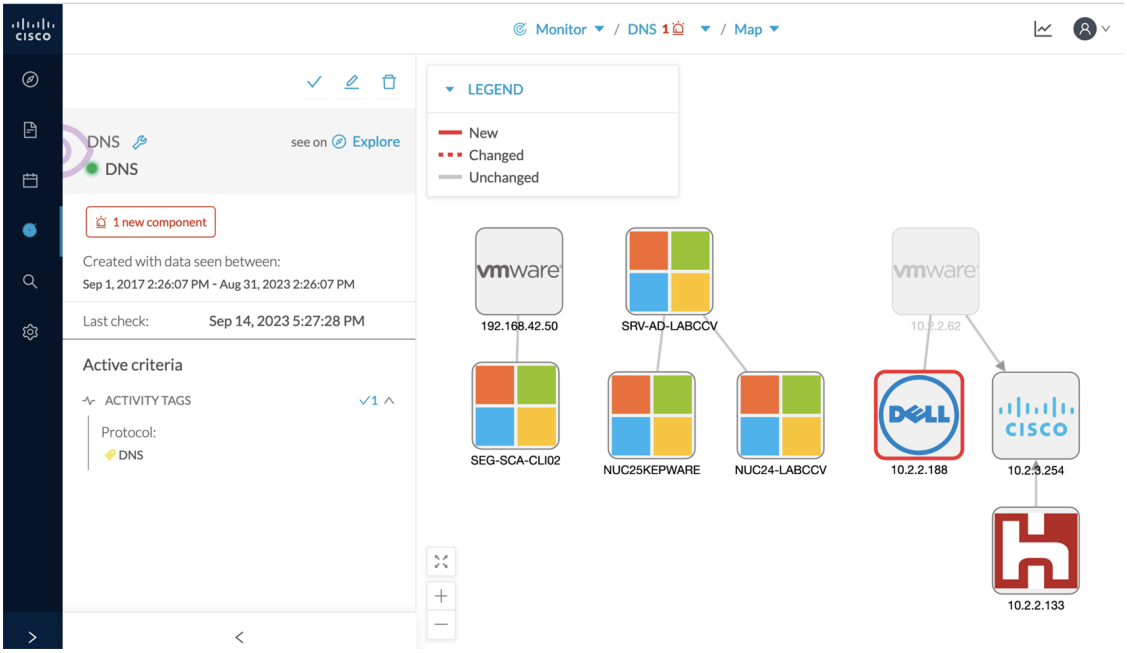
List is a chronological view in which you can see and search events. Use the search bar to find events by MAC and IP addresses, component name, destination and source flow, severity and category. You can search the Events on **Day, Week, Month** or **Year**. Use the arrows for exact dates.

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

1. From the main menu, choose **Events** > **List**.
2. Click an event result for more details about the event.
   a. When an event is related to sensors, click **See Sensor Statistics** for more details.
   b. When an event is related to component or an activity, click **see Technical Sheet** for more details.

Monitor

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



Search

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

Note Devices are not available in this page yet.

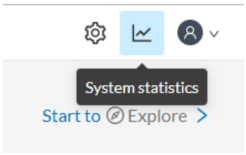
To search, enter the content in the search field and click **Search**.

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

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

System Statistics

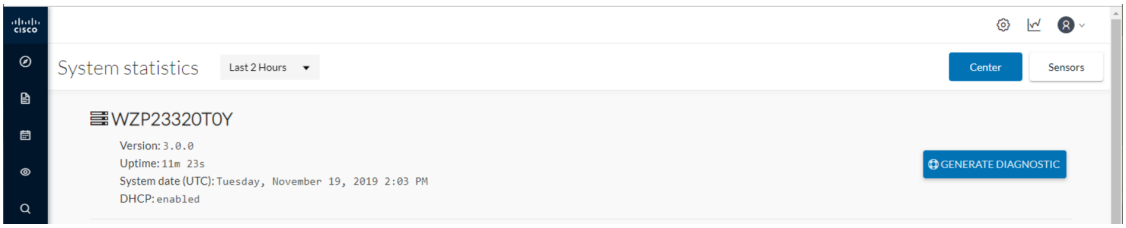
To access system statistics, click the **System statistics** icon in the top right corner of Cisco Cyber Vision interface.



Center

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

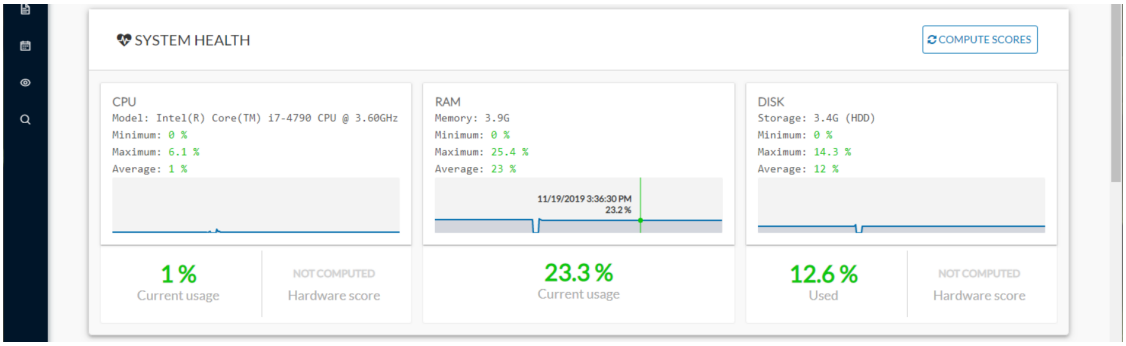
Note Use the drop-down arrow to change the time period.



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

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

System Health



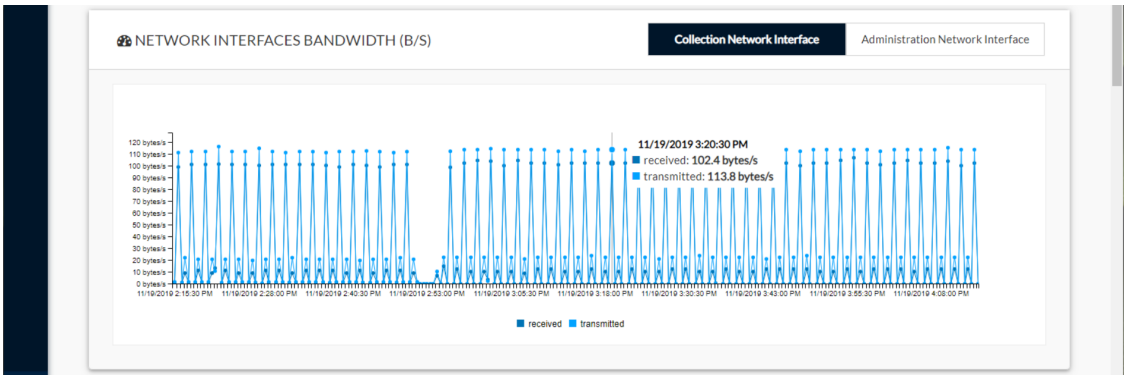
System health shows the status of the Center CPU, RAM and disk usage.

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

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

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

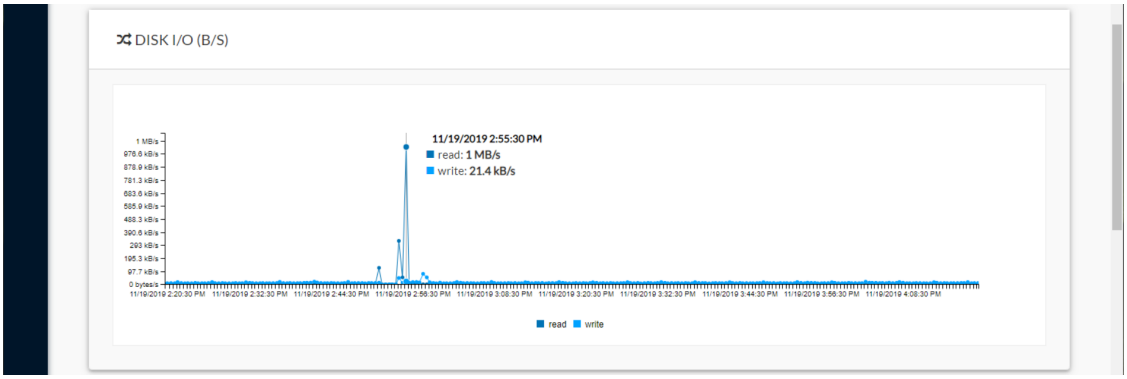
Network Interfaces Bandwidth



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

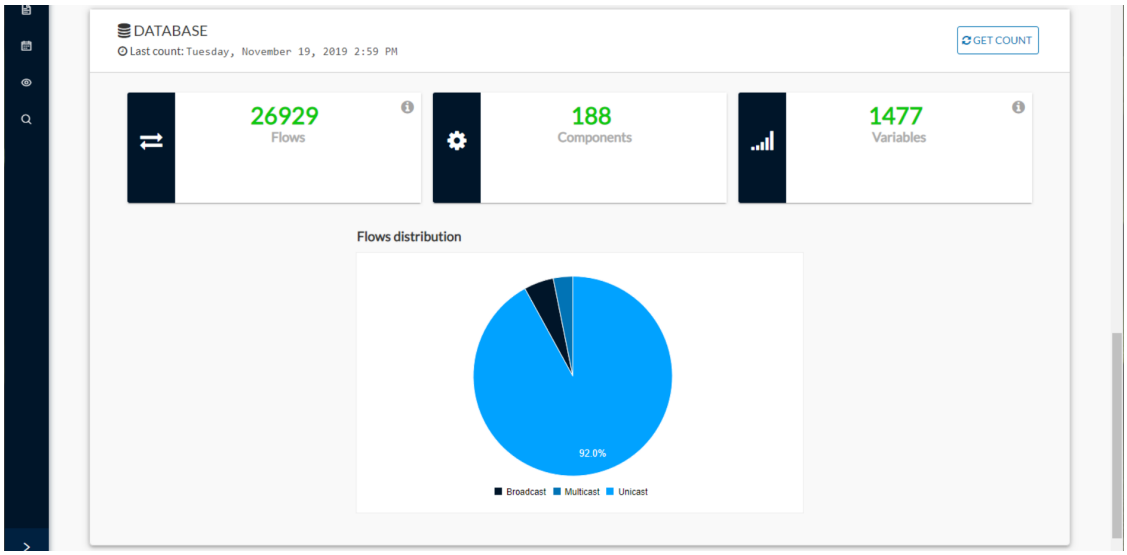
For example, the Collection Network interface activity lets you see the amount of data exchanged between the Center and the sensors.

Disk I/O



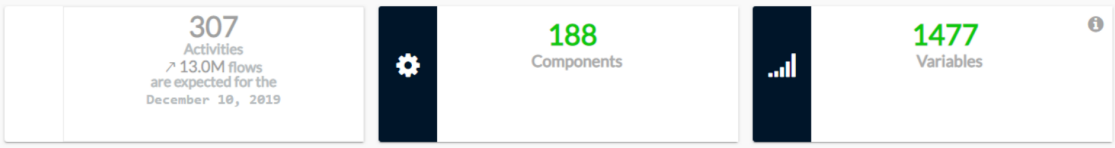
The line chart represents the Center hard disk usage in bytes/second.

Database

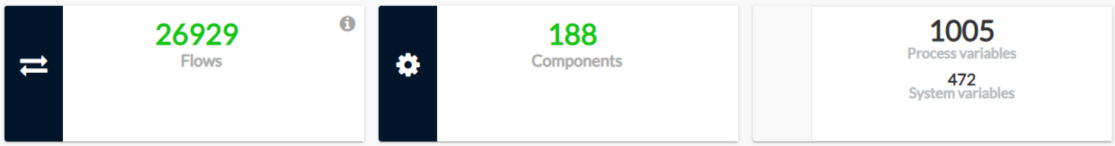


This section describes the database state by showing cards with the number of flows, components and variables that have been detected by Cisco Cyber Vision. Flows distribution is shown in a pie chart.

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

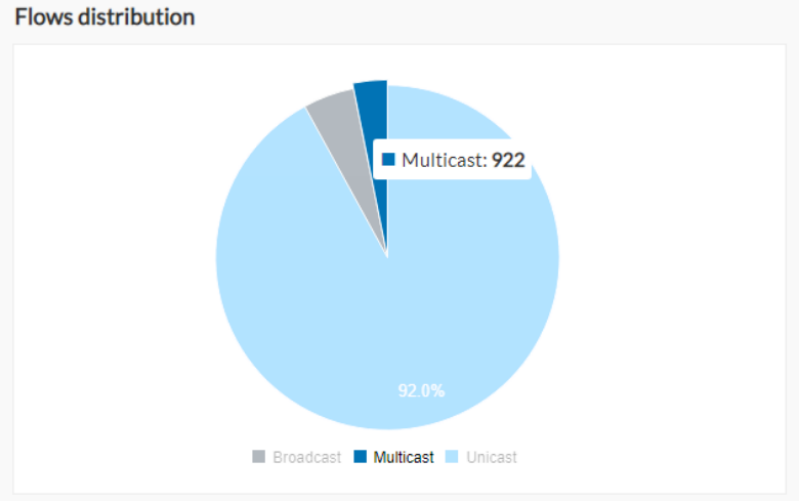


The flows card indicates the total number of flows (i.e. broadcast, multicast and unicast which are stored in the database) detected by . If you mouse over the card, you will get the number of activities and the flows evolution tendency. This information enables you to anticipate how the system load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



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

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



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

Services Statistics

The service status page indicates whether:

- all Cisco Cyber Vision background processes, such as services and extensions, are running correctly.
- all Cisco Cyber Vision background queues used to ingest data from sensors are not congested.

Checks are performed regularly.

Service Status:

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

- An **Update** button is available to refresh the services status; use it to ensure you have the latest information.
- A warning banner appears if a service is down, linking to this page, where the failing service is highlighted in red.

Queue Status:

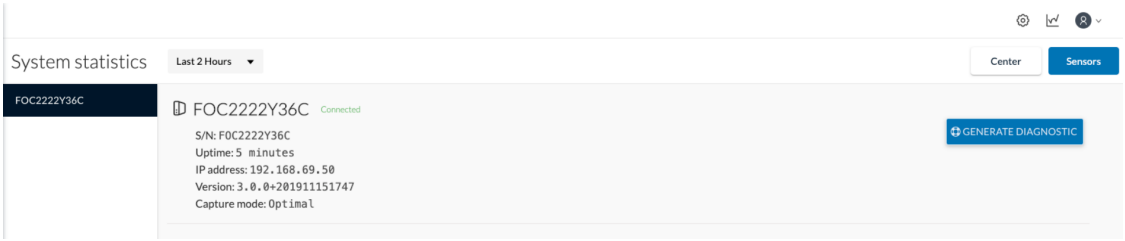
This section shows the status of the queues. If the monitored queues drop messages, this section reports it. Only sensor queues are monitored.

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

Sensors

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

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



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

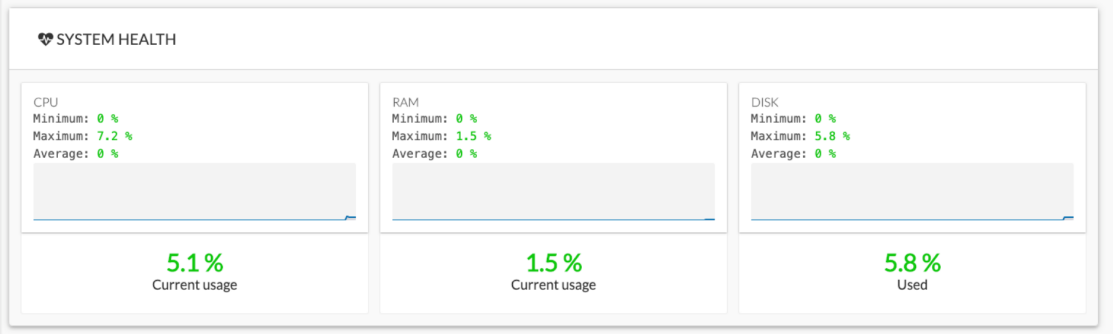
The **Sensors** statistics view shows general information about the sensor: the status (i.e., Connected), serial number, IP and MAC addresses, firmware version, the capture mode set, and the time it has been operating (i.e., uptime).

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

System Health

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

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

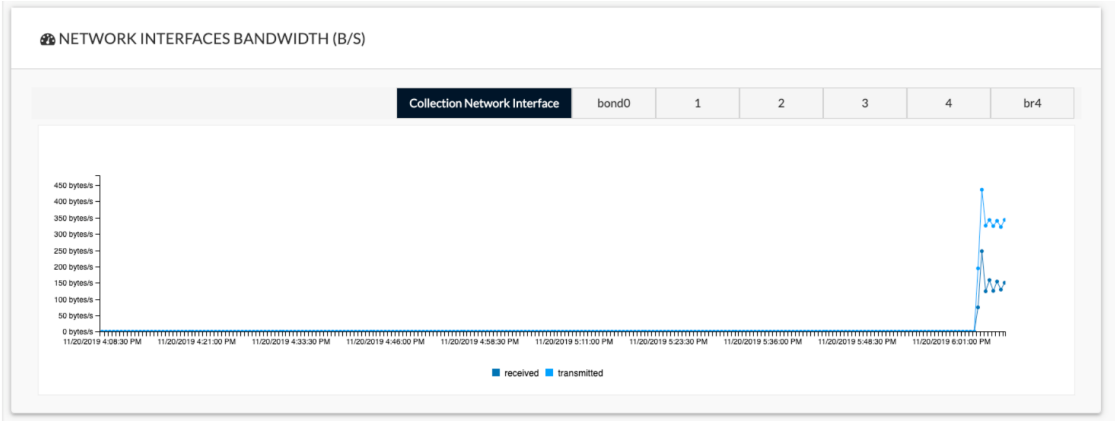


The chart also shows the percentage of the system's Current usage and Hardware score, useful to Cisco Cyber Vision product support.

Captured Packets

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

Network Interfaces Bandwidth



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

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

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

Disk I/O

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

My Settings

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

1. Go to the user menu at the top right corner and click the drop-down arrow.
2. Click **My Settings** from the drop-down list.

   The **My Settings** page appears.
3. Enter **Firstname** and **Lastname** under the **General** fileld.
4. Click the radio button of the preferred interface language under the **Language** filed.
5. Enter your password.

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

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

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

Note Your email will be requested for login access.

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

7. Clear application cookies.

Risk Score

Risk Score Definition

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

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

Risk scores apply to the following:

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

Risk Score Use

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

Proposed solutions are:

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

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

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

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

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

Risk Score Computation

Risk score is computed as follows:

Risk = Impact x Likelihood

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

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

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

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

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

How to take action:

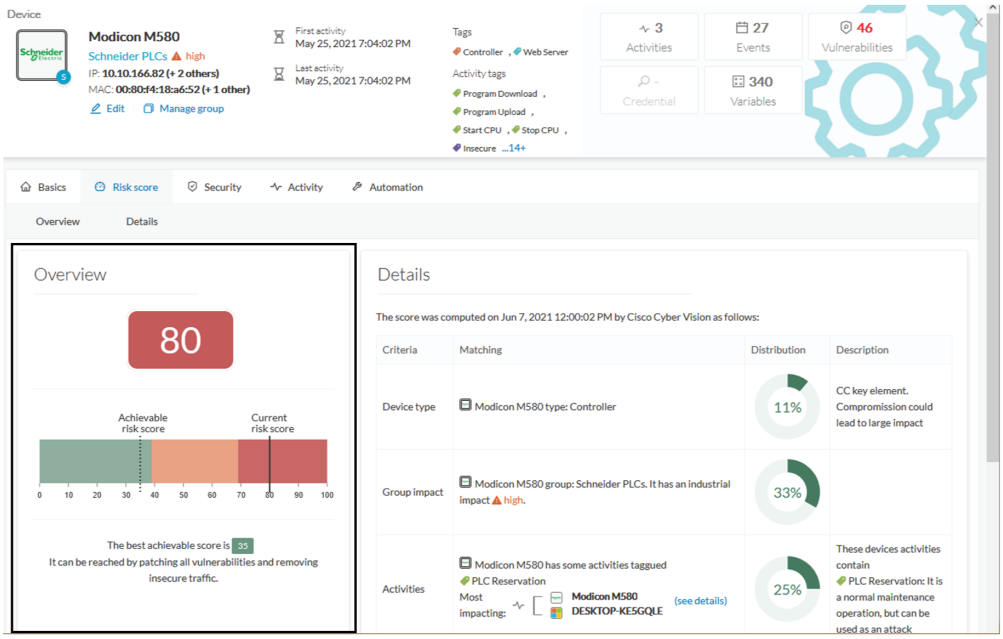
1. From the main menu, choose **Explore**.
2. Click the drop-down arrow in the top navigation bar and select **All Data** under **Basics**.
3. Click the drop-down arrow in the third filter of the top navigation bar and select **Device List**.
4. In the **Risk score** column, click the sort arrow to display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

   The right-side panel appears.
6. In the **Risk score**, click **See details**.

   The technical sheet appears.

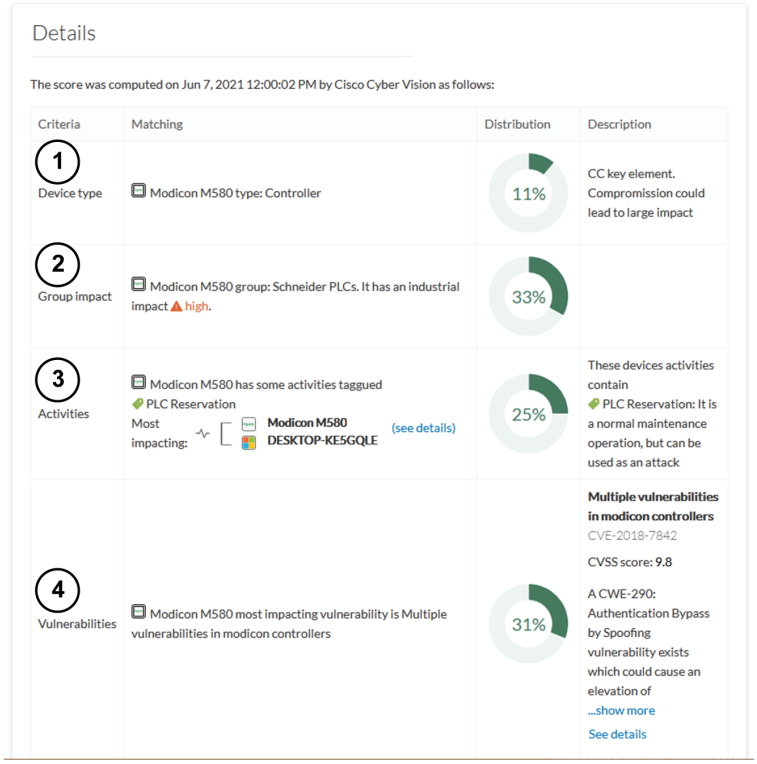
   In the **Overview** tab, the **Current** risk score and the **Achievable** risk are displayed.

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



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

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



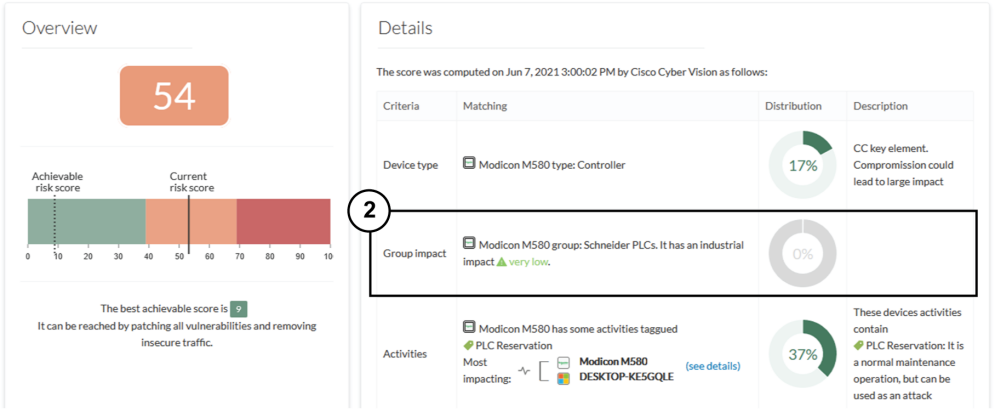
This page shows the last time the risk score was computed by Cisco Cyber Vision. Risk score computation occurs once an hour. To force immediate computation, use the following command on the Center shell prompt:

```
sbs-device-engine
```

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

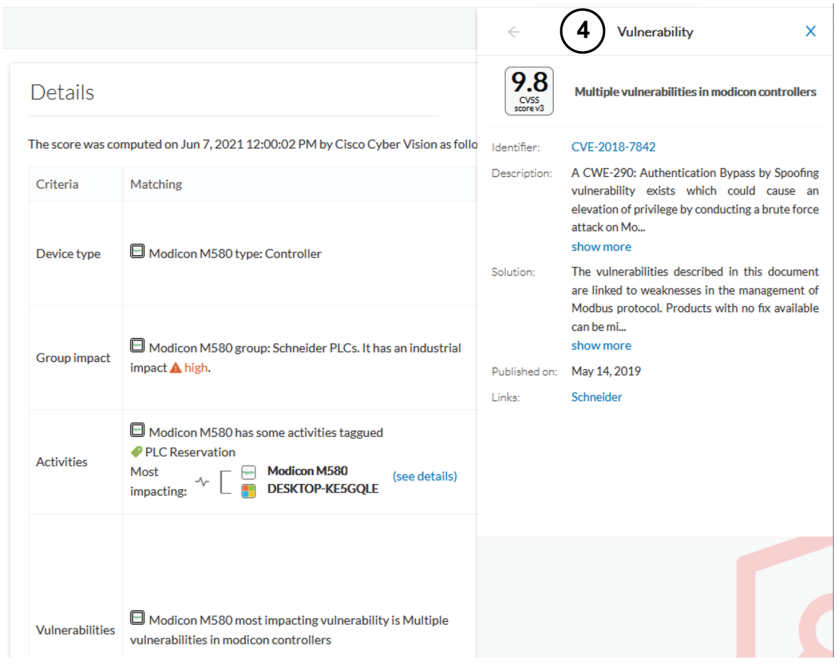
- **Device type**: Each device type corresponds to a device tag detected by Cisco Cyber Vision. No action is required at the device type level because each device tag is assigned a risk score by default.
- **Group impact**: Action is possible if the device belongs to a group. Decrease the impact by lowering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

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



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

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



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