Cisco Cyber Vision GUI User Guide, Release 4.3.0

First Published: 2021-01-01

Last Modified: 2023-12-13

C O N T E N T S

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 4.3.0**.

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 if proper precautions are not taken.

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

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

Warnings and notices

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, on page 5

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 avilable:

- 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.

Preset

C H A P T E R **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

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).
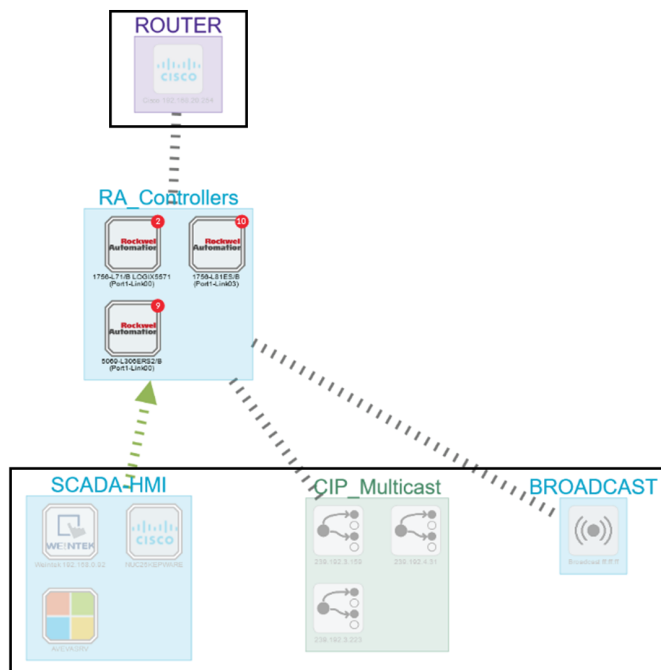
It will give the following results:

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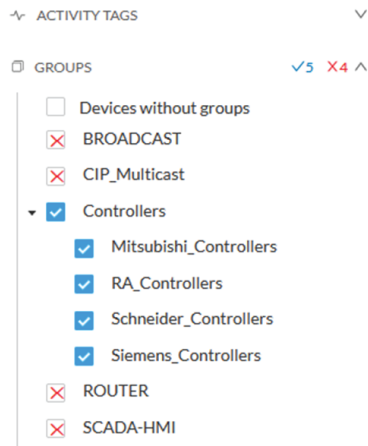
In the example above, only the devices belonging to the selected groups will be selected. Activities always involve two end points and are selected if either end point is part of a selected group, and none are part of an excluded group.

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
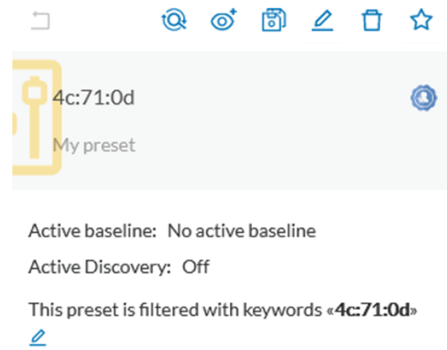
Keyword =siemens
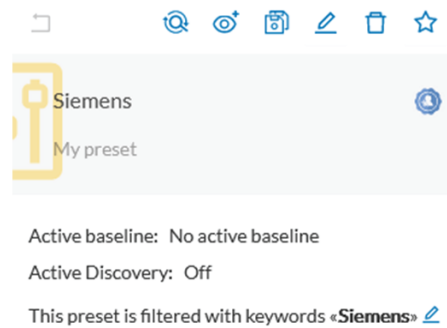
Filter combination

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.

Filters

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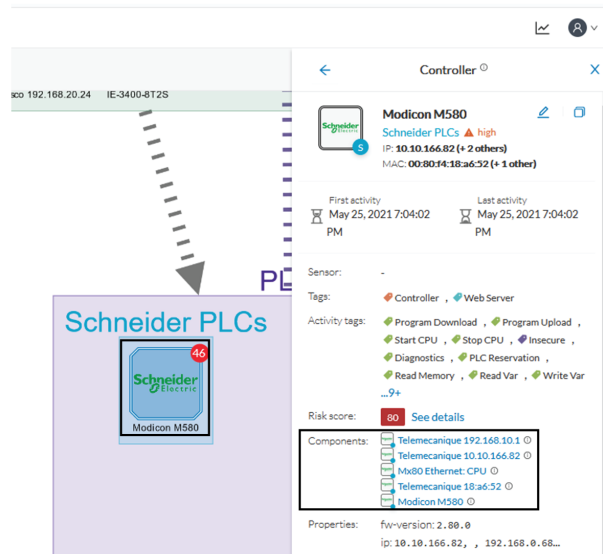
Devices can have a red counter badge. This is the number of vulnerabilities detected. For more information, refer to Vulnerability.

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

5 Components

Component	First activity	Last activity	IP	MAC	Tags	Vulnera...
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.

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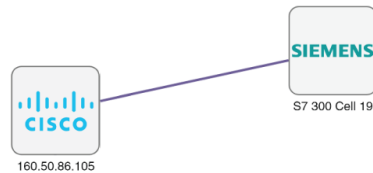
An activity between two components is actually a simplified view of the Flow exchanged. You can have many types of flows going in both directions inside an activity, represented in the map.

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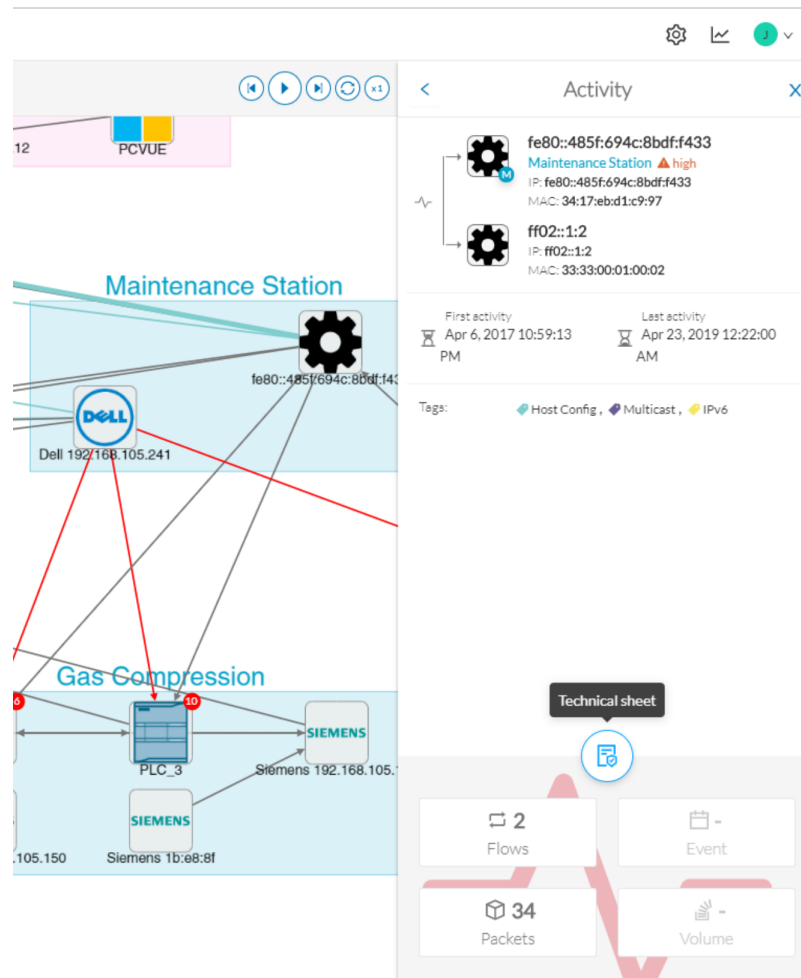
Devices or components with no activity does not mean that they did not have any interaction. In fact, a component can only be detected if it has been involved in a network activity (communication emission/reception). Lack of activity can mean that the other linked component is not part of the preset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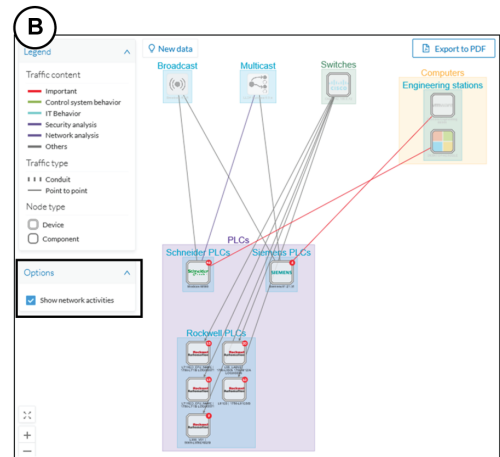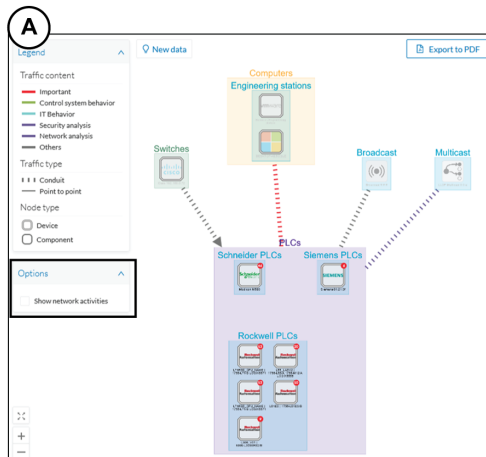
Activity

C H A P T E R 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
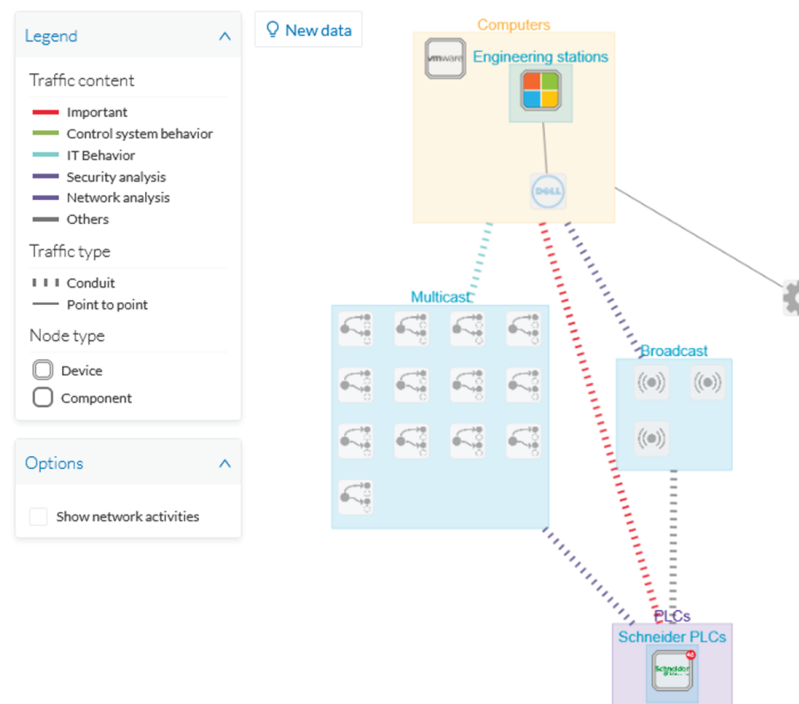
Conduits view mode is enabled by default. Disable it by using the **Show network activities** checkbox at the lower left side of the map.
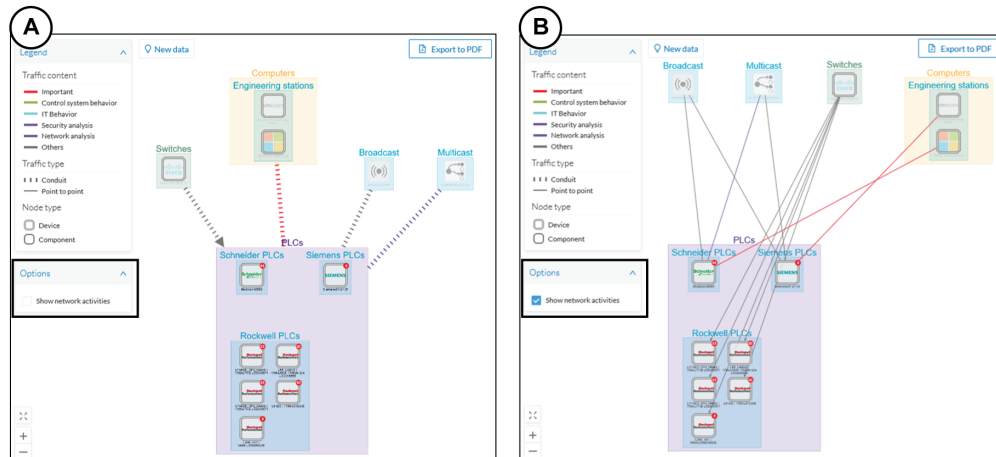
CHAPTER **8**

Flow

- Flow, on page 25

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 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.

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:

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, on page 31

Time span

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

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

• To set a duration, selecting a period of time (from 10 seconds to 1 day) or a custom period up to now.
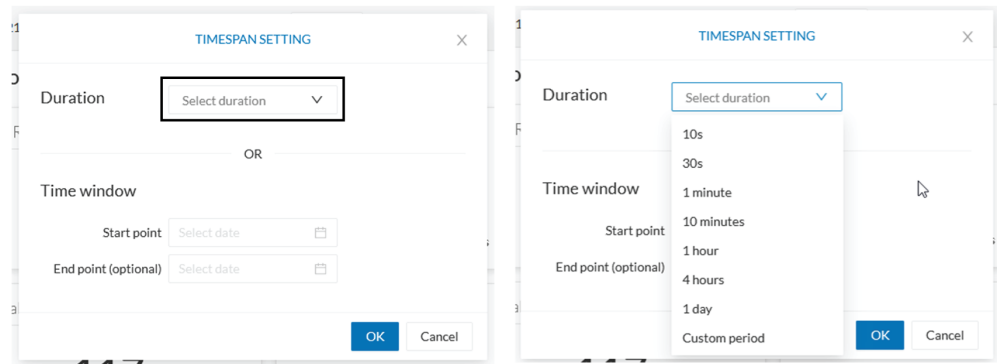
- To set a time window, selecting a start date and optionally an end date. If you don't select one the end date will be set to now.
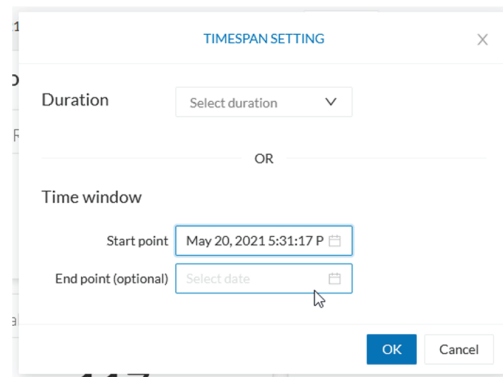
You can set a time window to see everything that has happened during the selected period of time such as historical data or to check the network activity in case of on-site intrusion or accident.

Once the time span set, click the Refresh button to compute network data.

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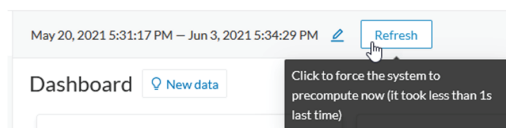
Note   No data display is often due to a time span set on an empty period. Remember to first set a long period of time (such as 12mo) before considering a troubleshooting.

Recommendations:

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

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

- Set a period of a few minutes to have more visibility on what is *currently* happening on the network.

- Set a period of a few hours to have a view of the daily activity or set a time to see what has happened during the night, the week-end, etc.

- Set limits to visualize what happened during the night/week-end.

- Set limits to focus on a time frame close to a specific event.

Time span

Tag

- Tags, on page 35

Tags

What are 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.

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

- Device tags **(1)** which describe the functions of the device or component and are correlated to its properties. A device tag is generated at the component level and synthesized at the device level (which is an aggregation of components).

- Activity tags **(2)** which describe the protocols used and are correlated to its properties. An activity tag is generated at the flow level and synthesized at the activity level (which is a group of flows between two components).

Each tag is classified under categories, which you can find in the filtering area, and applies to a device or an activity.

The device tags categories (Device - Level 0-1, Device - Level 2, etc.) and some tags (IO Module, Wireless IO Module) in the filtering area:
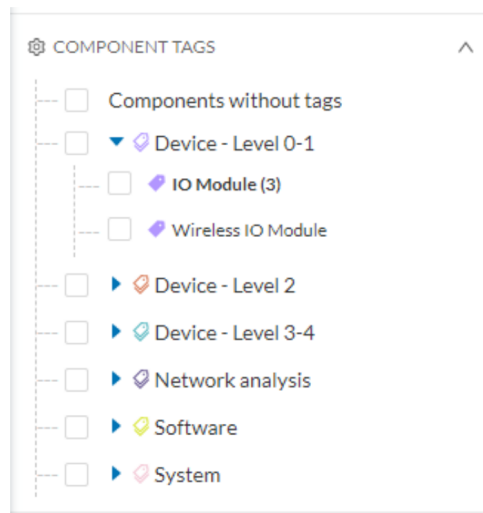
Note   Device levels are based on the definitions presented in the ISA-95 international standard.

What are tags used for?

Exploration of the network and Cisco Cyber Vision is mainly lead by tags. Criteria set on presets are significantly based on tags to Filters the different views.
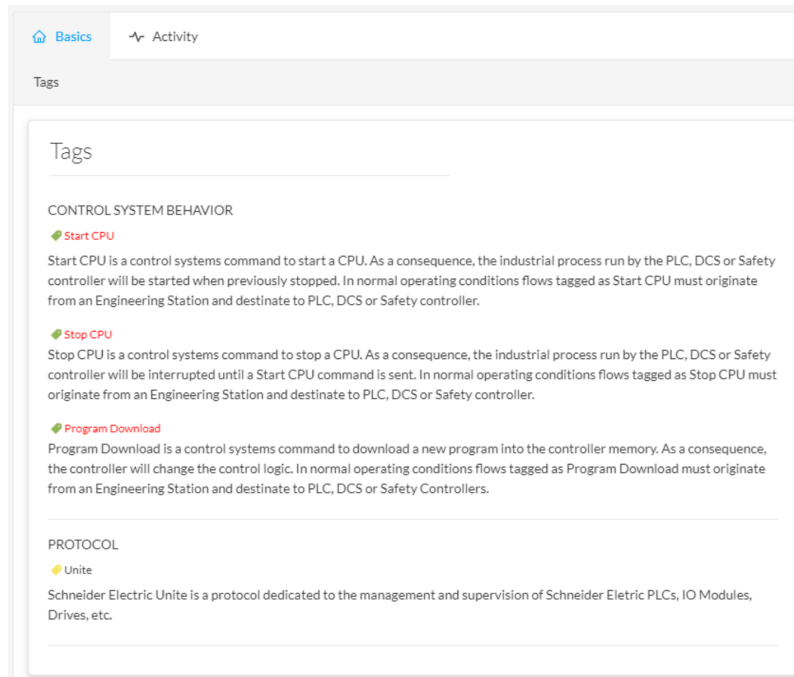
Also, tags are used to define behaviors (i.e. in the Monitor mode) inside an industrial network when combined with information like source and destination ports and flows properties.

Where to find tags?

You will find tags almost everywhere in Cisco Cyber Vision. From criteria, which are based on tags to filter network data, to the different views available. Views take different perspectives and have different approaches concerning tags. For example, the dashboard shows the preset's results bringing out tags over other correlated data, while the device list highlights devices over data like tags. Refer to the Navigating through Cisco Cyber Vision to know more about them.

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

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

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, on page 39

Properties

What are properties?

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

What are properties used for?

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

Where to find properties?

Properties are visible from devices and components Right side panel and Technical sheets under the tab Basics.

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

Properties

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

Risk score

- Risk score, on page 41

Risk score

What is a risk score?

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

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

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

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

What is a risk score used for?

The risk score is meant to help the user easily identifying which devices are the most critical within the overall network. It provides limited and simple information on the cybersecurity of the monitored system. It is intended as a first step in security management to take actions by showing the causes of high scores and providing solutions to reduce them. The goal is to minimize and keep risk scores as low as possible.

The solutions proposed can be:

- to patch a device to reduce the surface of attack,

- to remove vulnerabilities,

- to update firmware,

- to remove unsafe protocols whenever possible (e.g. FTP, TFTP, Telnet),

- to install a firewall,

- to limit communications with the outside, by removing external IPs.

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

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

For example, removing unsafe protocols will affect the likelihood of the risk, but patching a device will act on the impact of the risk.

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

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

How is the risk score computed?

The risk score is computed as follows:

Risk = Impact x Likelihood

Impact:

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

- The device tags, because some device types are more critical. Each device type (or device tag) or device tag category has been assigned an industrial impact score by Cisco Cyber Vision. For example, is the device a simple IO device that controls a limited portion of the system, or is it a Scada that controls the entire factory? These will obviously not have the same impact if they are compromised.

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

Likelihood:

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

- Device activies, more precisely on the activity tags. Because some protocols are less secure than others. For example, Telnet is less secure than ssh.

- The exposure of the device communicating with an external subnet.

- Device vulnerabilities, taking into account their CVSS scoring.

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

How to take action:

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

2. Click a device in the list. Its right side panel opens.

3. Click the risk score's "see details" button.

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

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

The achievable risk score is the best score you can reach if you patch all vulnerabilities on the device and remove all potential insecure network activities. The score cannot be zero because devices have intrinsic risks coming from their device type and, if applicable, their group industrial impact.
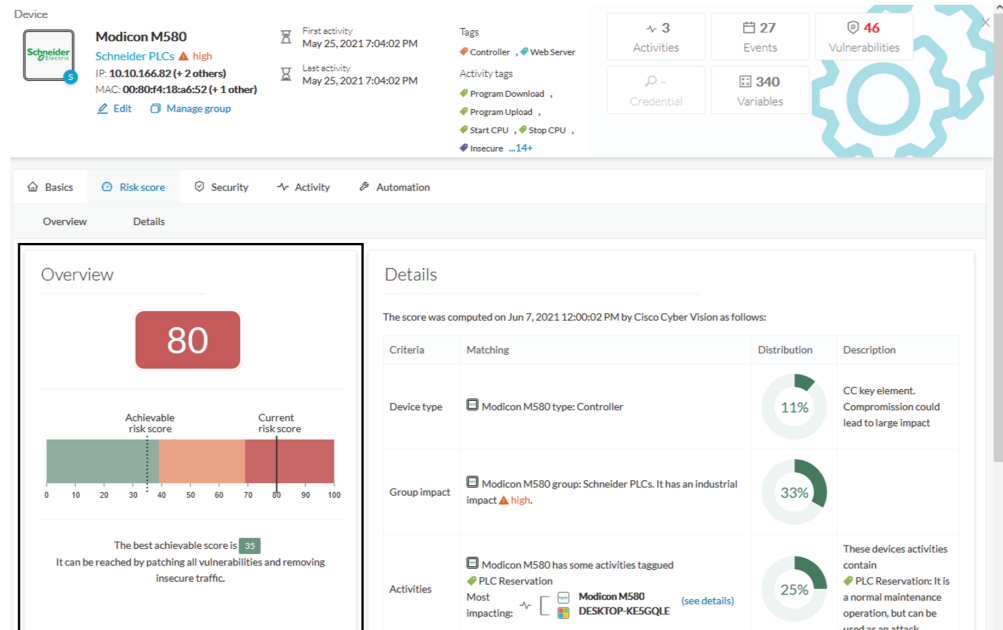
Under Details, you have further information about the different risks impacting the device, the percentage of the risk they represent within a total risk score, and the solutions to reduce or even eliminate them.

Device type **(1)** and group impact **(2)** affect the risk impact variable, meanwhile activities **(3)** and vulnerabilities **(4)** affect the risk likelihood.

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

```
sbs-device-engine
```

Below, appears the information retrieved during the last computation.

- Device type (**1**): Each device type corresponds to a Tags detected by Cisco Cyber Vision. There is no action to be done at the device type level, because each device tag is assigned with a risk score by default in Cisco Cyber Vision.

- The group impact (**2**): Action is possible if the device belongs to a group. You can decrease the impact by lowering the industrial impact of the group that the device belongs to.

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

![pencil note icon]
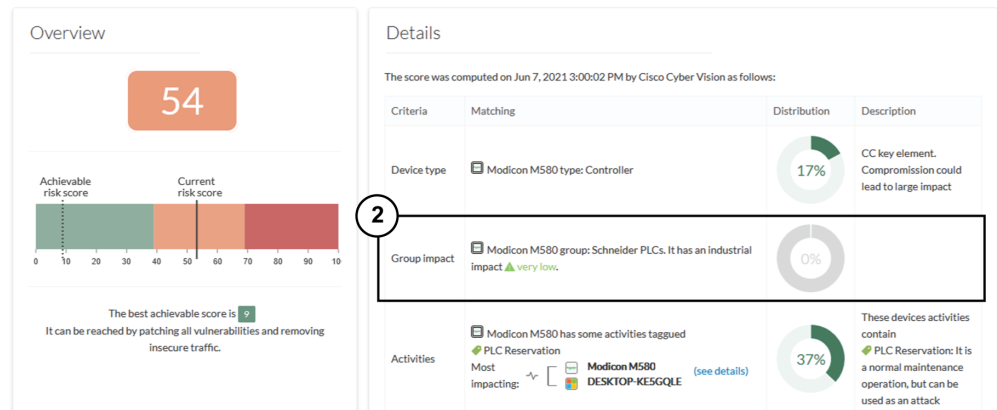
Note The new industrial impact will be taken into account at the next risk score computation (once an hour).

- Activities (**3**): The most impactful activity tag is displayed. The risk can be lowered if all potential insecure network activities are removed.

- Vulnerabilities (**4**): Click the "see details" button for more information about how to patch the vulnerabilities and so reduce the device risk score.

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

C H A P T E R 14

Vulnerability

Vulnerability

What are vulnerabilities?

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

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

☞

Important   It is important to update the Knowledge DB in Cisco Cyber Vision as soon as possible after notification of a new version to be protected against vulnerabilities. To do so, refer to the corresponding documentation.

What are vulnerabilities used for?

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

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

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

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

Where to find vulnerabilities?

Vulnerabilities are accessible through the Vulnerabilities of a preset.

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

Flows	Vuln	Var		Flows	Vuln	Var
7	2	0		12171	42	1
7	7	22		29	13	0
13	9	0		26	13	0
2	0	1		1	12	2
6	6	0		1	12	1
23	6	13		13	9	0

Moreover, vulnerabilities are pointed out in the map by a device or a component with a red counter badge (**4**). If you click it, its side panel opens on the right with the number of vulnerabilities evidenced in red (**5**).
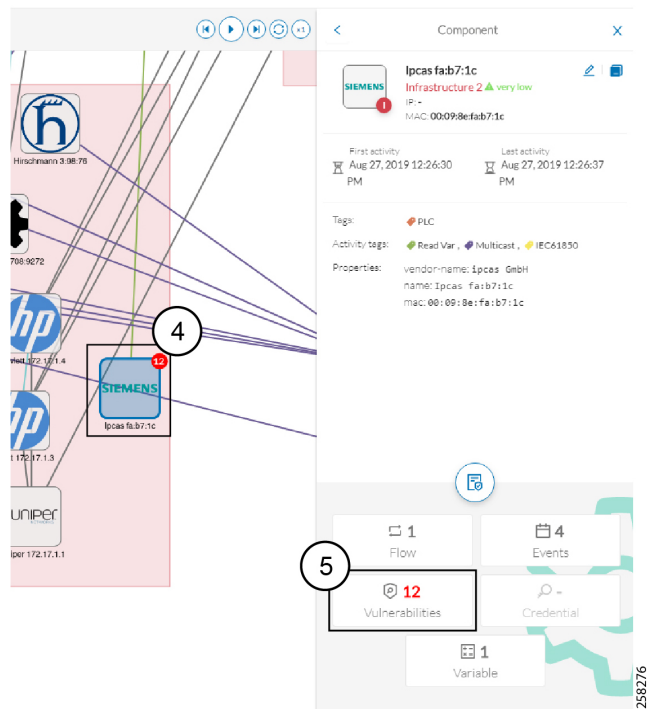
Clicking the vulnerabilities displayed in red **(5)** (in the figure above) opens the device or component's technical sheet with further details about all its vulnerabilities:

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

Events

Events

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

For instance, an event can be:

• A wrong password entered on Cisco Cyber Vision's GUI.

• A new component which has been connected to the network.

• An anomaly detected on the Monitor Mode.

• A component detected as vulnerable.

Events are visible in the Events.

New events may be generated when the database is updated (in real-time or each time an offline capture is uploaded to Cisco Cyber Vision) with a severity level (Critical, High, Medium and Low) customizable through the Events 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; and if credentials are visible on Cisco Cyber Vision, then they're potentially visible to anyone on the network. Credentials visibility on Cisco Cyber Vision should trigger awareness towards actions to be taken to properly secure the protocols used on a network.

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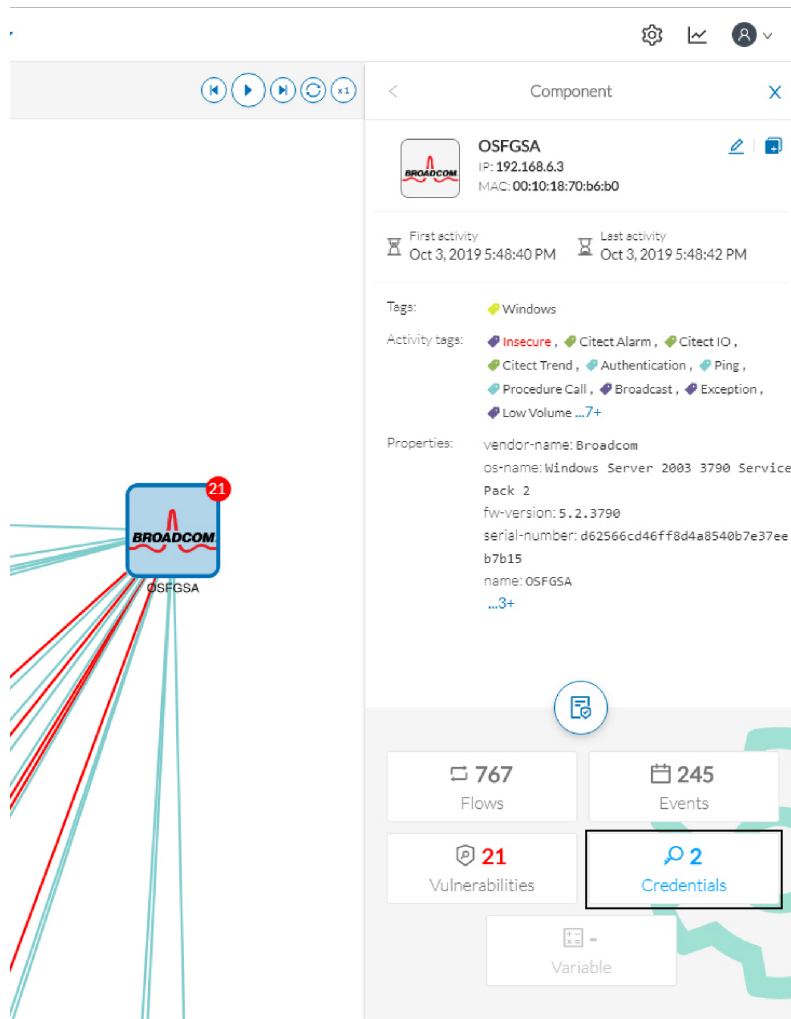
Credential frames are extracted from the network thanks to Deep Packet Inspection. Credentials are then accessible from a component's technical sheet under the security tab. You will find the number of credentials found **(1)**, the protocol used **(2)**, and the user name and password **(3)** with a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

An unsafe password:

A hashed password:

Credentials

Aseng	NTLMSSP
Aseng::MAR01:6bba39443b59770b:7011abc59983712dc0254d8db44991fb:087087408ad48ab5	
aseng	NTLMSSP
•••••	

859

258353
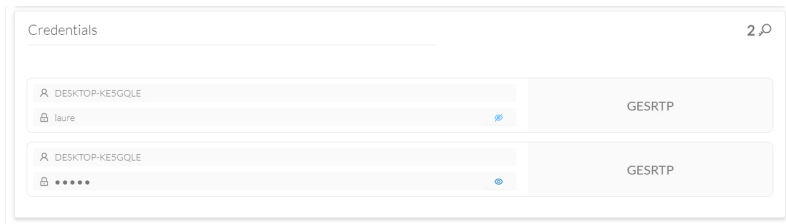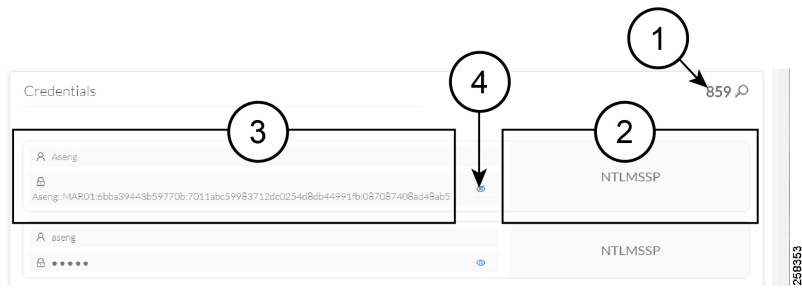
CHAPTER 17

Variable access

Variable accesses

What are variable accesses?

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

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

What are variable accesses used for?

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

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

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

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

Where to find variable accesses?

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

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

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

Group

• Creating and customizing groups, on page 61

Creating and customizing groups

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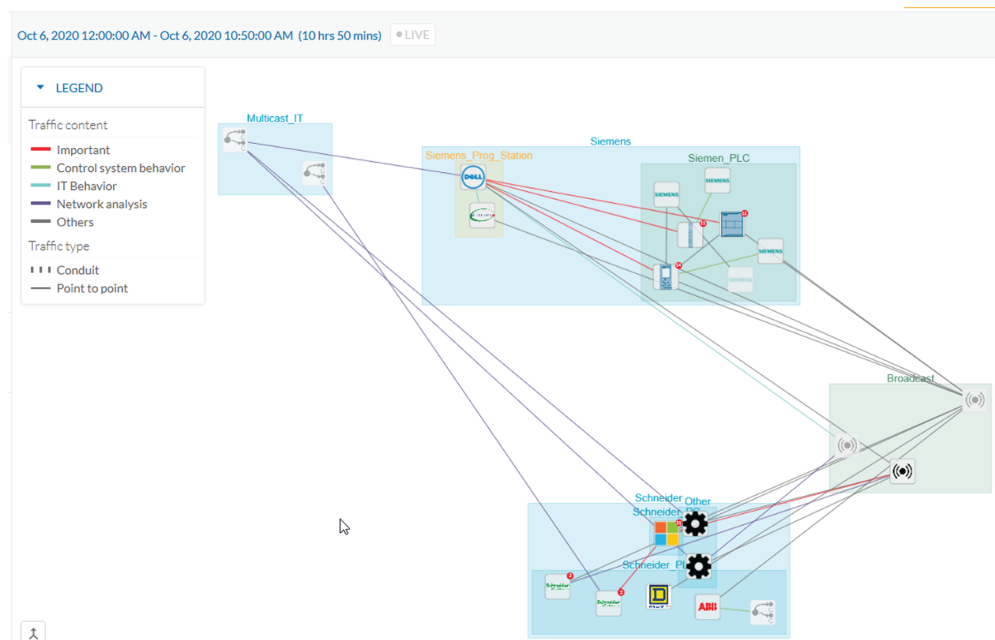
You can organize devices and components into groups as you wish to add meaning to your network representation. For example, this can be done according to the devices' location, process, severity, type, etc. You can also create nested groups inside a parents group, that is, add a group into another group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

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

To create a group:

Procedure

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

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

A My Selection panel opens on the right.
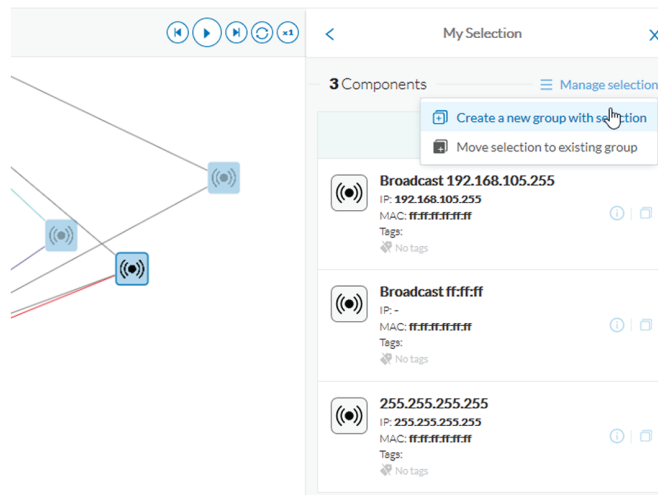
Step 2 Click Manage selection.

Step 3 Click Create a new parent group.

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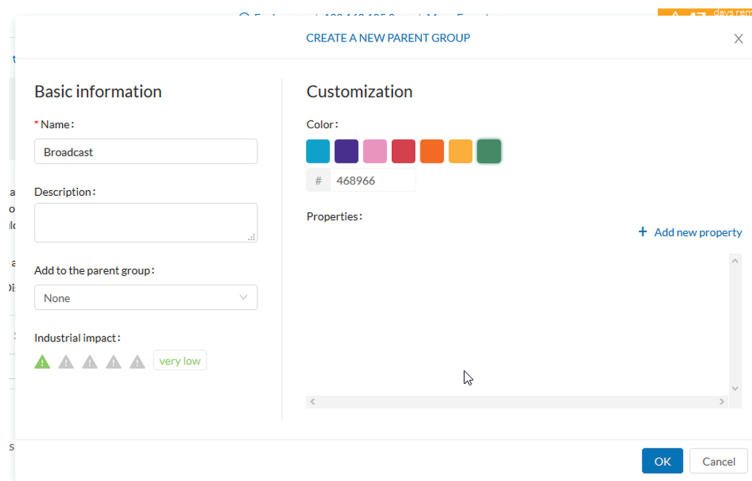
Step 4 Customize the group by giving it a description, defining its industrial impact (e.g. as opposed to a print server, a PLC that controls a robotic arm is highly critical), changing its color and adding properties.

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

To create a parent group:

There are several ways to create a hierarchy among groups:

- Select two groups and create a group as indicated before.

- Select a device or a component and move it into a group clicking the Move selection to existing group button.

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

Add group properties:

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

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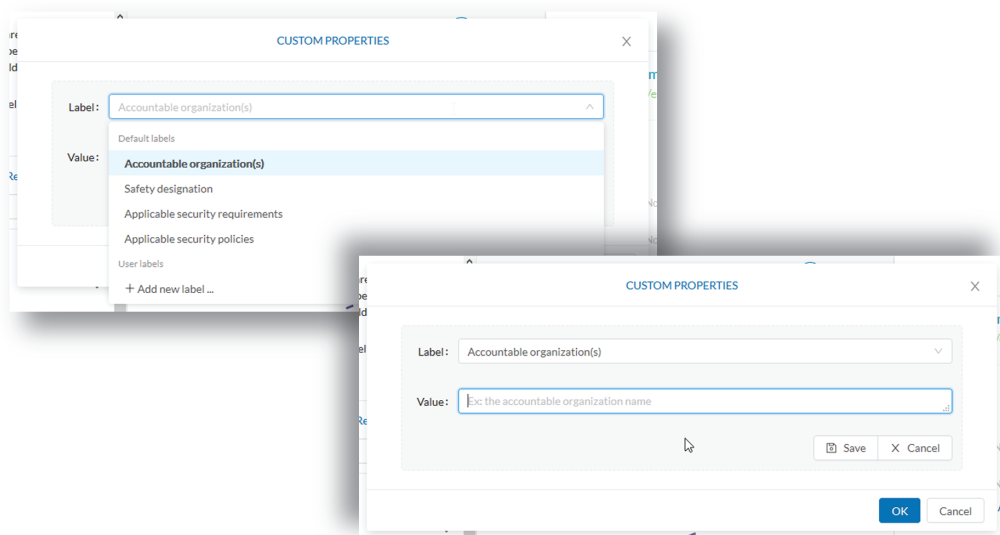
Aggregated activities or conduits:

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

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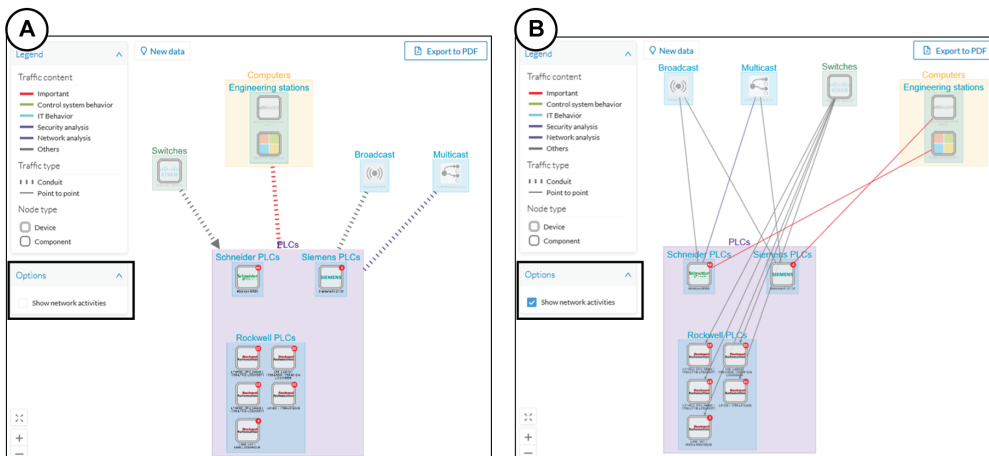
Lock/unlock a group:

Locking a group:

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

- prevents a group to be deleted.

To switch on/off the Lock toggle button,

Step 6	Click a group.
Step 7	Click the Lock button on the group's icon.
	or
	Click the Edit button on the group's right side panel and toggle on/off the Lock button.
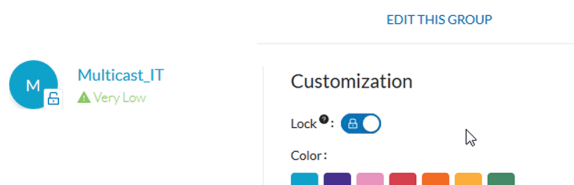
Step 8	**Groups used as criteria to filter data in Cisco Cyber Vision:**
	Any groups created will be added into the Filters to help you refine the dataset and compose presets.

Active Discovery

-

Active Discovery

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

With Active Discovery enabled broadcast and/or unicast messages will be sent to the targeted subnetworks or devices through sensors to speed up network discovery. Then, returned responses will be analyzed and tagged as Active Discovery. Thus, components and activities will be clarified with additional and more reliable information than what is usually found through passive DPI.

The following protocols are supported:

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

Home

• Home, on page 71

Home

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

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

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

In the operational overview, you will find a pie chart with the protocol distribution and a list of the most critical events.
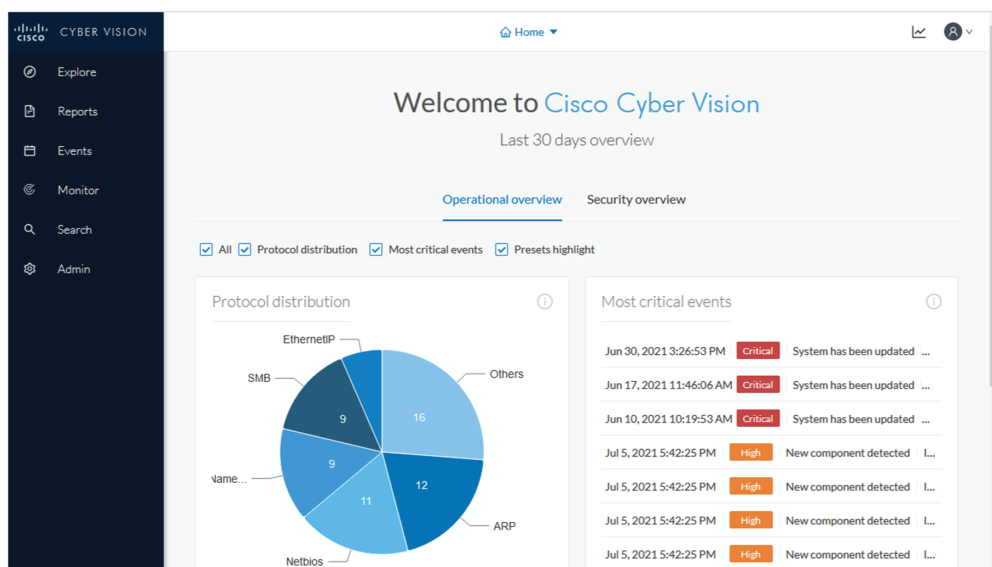
Below, a preset highlight you can edit to display your favorite presets.

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

Below, a list of the most critical events, and events classified per category, as well as a preset highlight that you can edit.
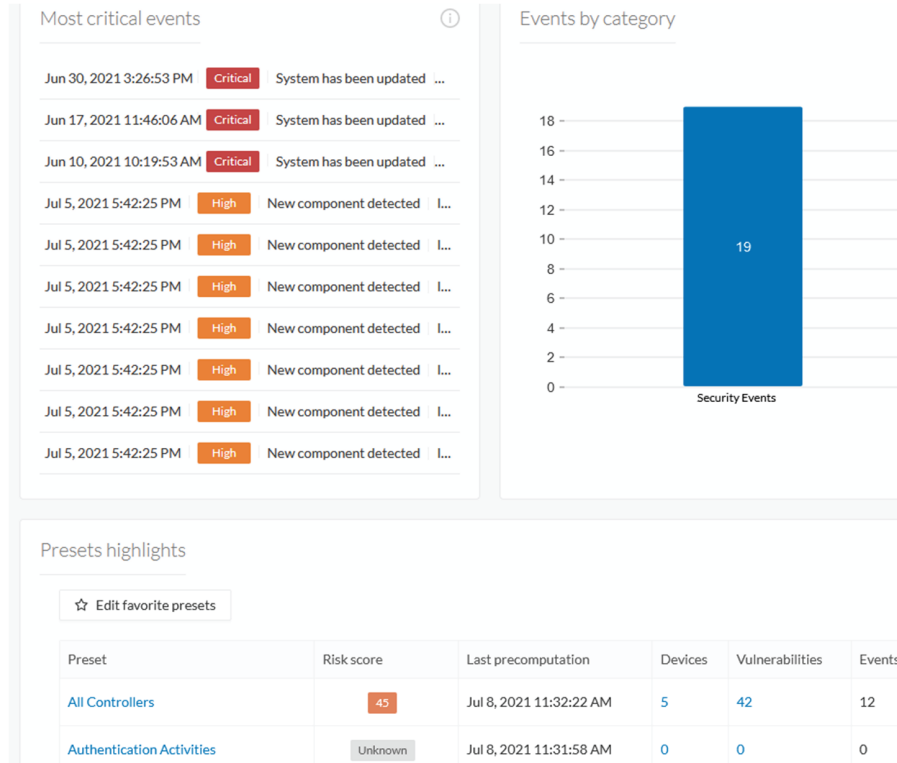
The navigation bar on the left gives access to all other main pages of Cisco Cyber Vision:
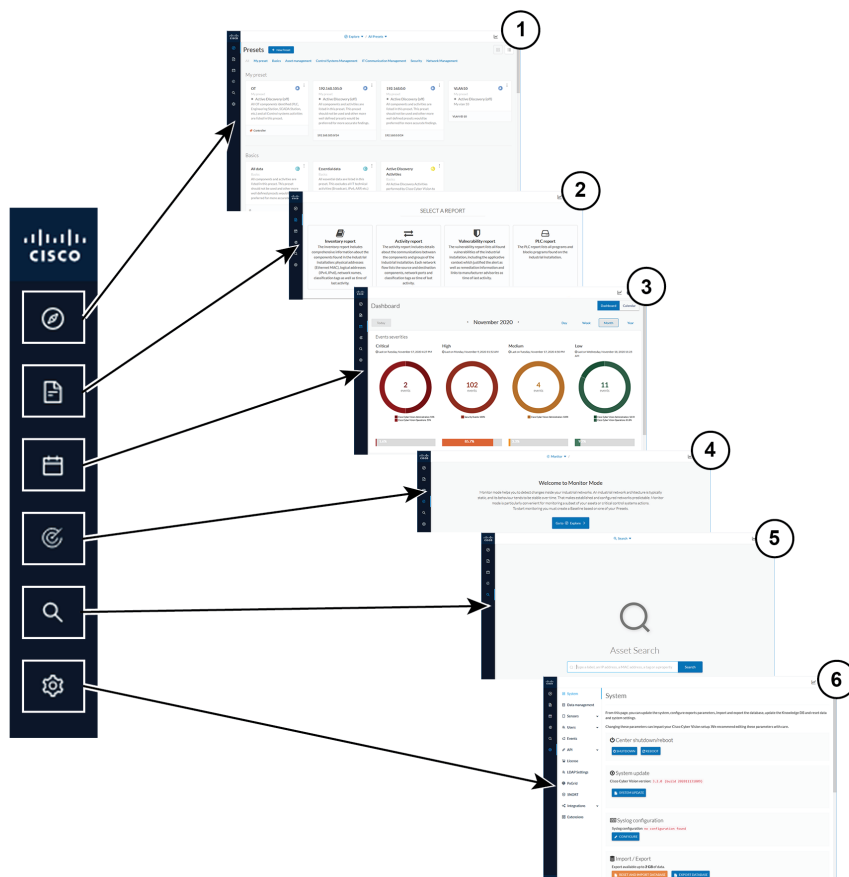
- Explore **(1)**: This button leads to the overview of Explore by defaults or configured.

- Reports **(2)**: This button leads to the Legacy Reports to export valuable information about the industrial network.

- Events **(3)**: This button leads to the Events which contains graphics and a calendar of all events generated by Cisco Cyber Vision.

- Monitor **(4)**: This button leads to the Monitor to perform and automatize data comparisons of the industrial network.

- Search **(5)**: This button leads to the Search to look for precise data in the industrial network.

Explore

Presets is a page containing an overview of all presets existing in Cisco Cyber Vision whether they are present by default or part of users' customizations. You can access this page by clicking the Explore button on the left navigation bar.
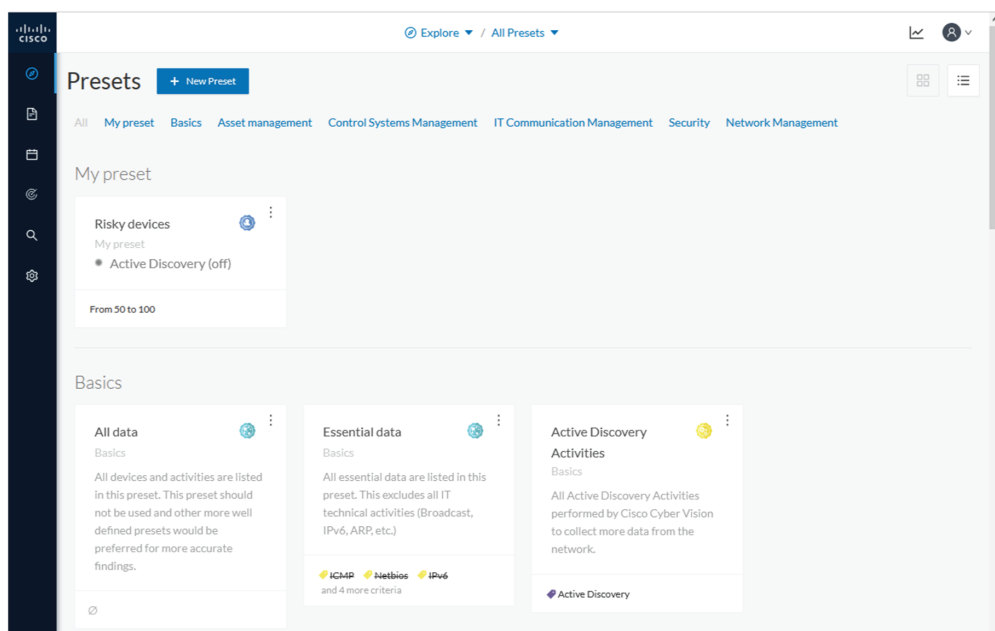
The top navigation bar **(1)** allows you to access the different presets **(2)** and then reach their different Preset views.

Preset views

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

- The dashboard:

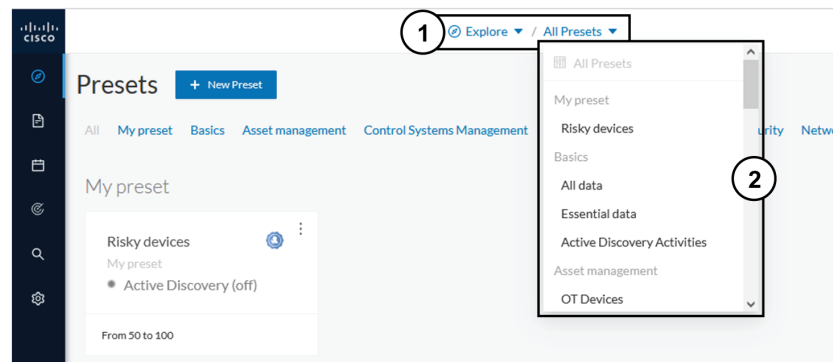 The Dashboard is a unique view which is displayed by default when accessing a preset. It offers an overview of data found by the preset. The fact that it's a tag-oriented view allows you to have a general insight of the network without going into deep and technical details.

- The map:

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

- Lists:

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

- The Purdue Model:

  In this map, the components of a preset are distributed among the layers of the Purdue Model architecture.

Views are always structured as shown below:

- The top navigation bar **(1)**, which allows you to easily switch between the different views thanks to its menu.

- The filtering area on the left **(2)**, which allows you to modify and manage the preset by adapting criteria and registering changes.

- The view you're on **(3)**, which dynamically evolves as you change and save criteria.

Example of the OT Devices preset on the dashboard view:
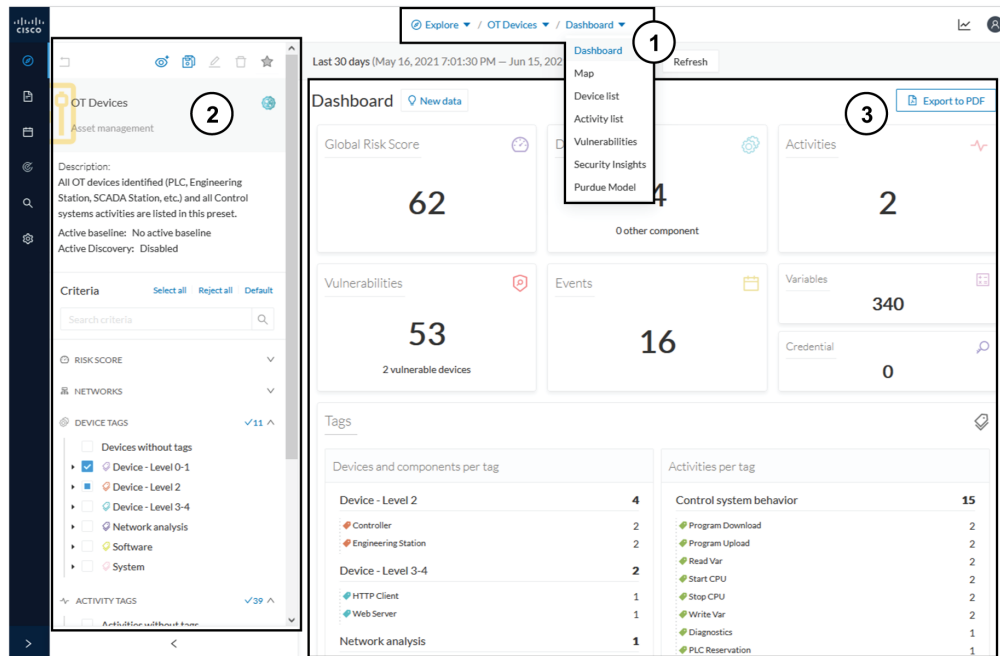
Display of preset views has been optimized to avoid lags, solve performance issues and prevent the application from crashing, especially in case of large data flow.

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

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

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

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

- The New data button (**4**) appears each time a new computation is done and refresh the view as you click on it. The view will be updated to the last computation done in the system, which means that using this button won't necessarily show new data.

- The Refresh button (**5**) forces data computation and refresh the preset view. This task requires more resources and should be used in the following cases:

  - If you expect that new data has been found during the most recent computation (e.g. a new device plugged into the network).

  - If custom data such as groups or names have been changed (e.g. if adding a device into a group).
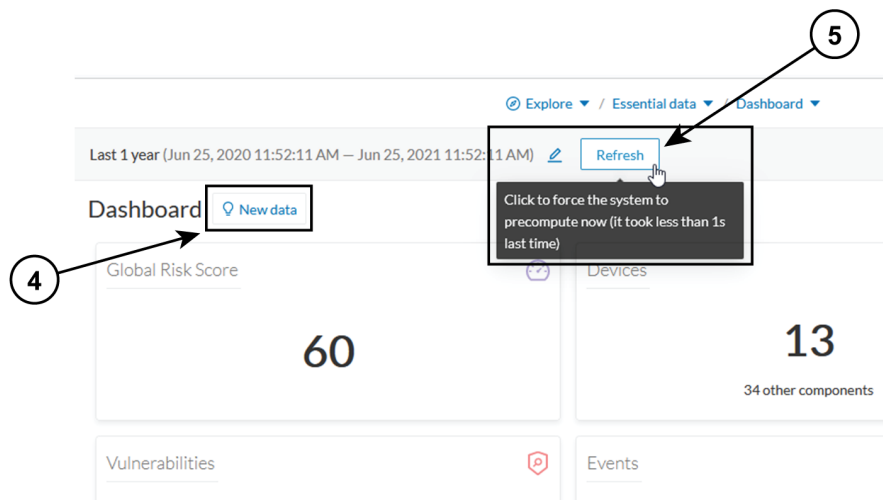
In any cases, the computation is forced and the view is refreshed as you navigate in the application. For example, when accessing another preset or when moving from one view to another.

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

Dashboard

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

The dashboard is also a tag-oriented view. It's an overview of all tags found -independently of the ones set as criteria- with the number of devices and activities found per tag.
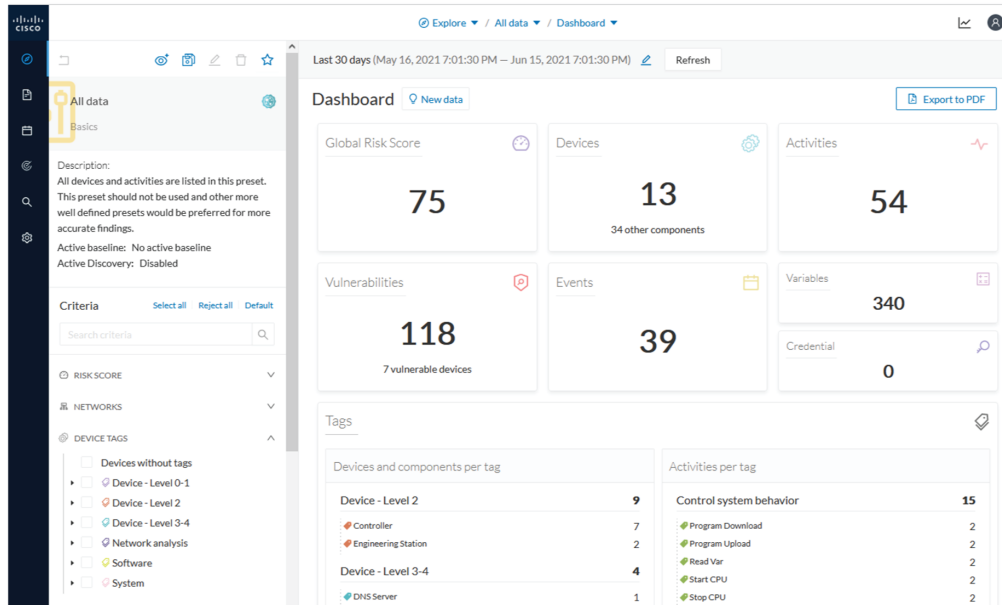
Example: For the purpose of the whole example given below, we access the All data preset, select the Controller tag as criteria (under Device - Level 2), and save the selection as "Example: Controller tag".

Devices per tag: The number in brackets indicates there are 7 devices tagged as Controller **(1)**. On the dashboard, you see this result accordingly **(2)**. One device is tagged as Web Server **(3)**. This means that one of the Controller is a Web Server. Following this logic, we can say that five of the Controllers are Rockwell Automation devices.
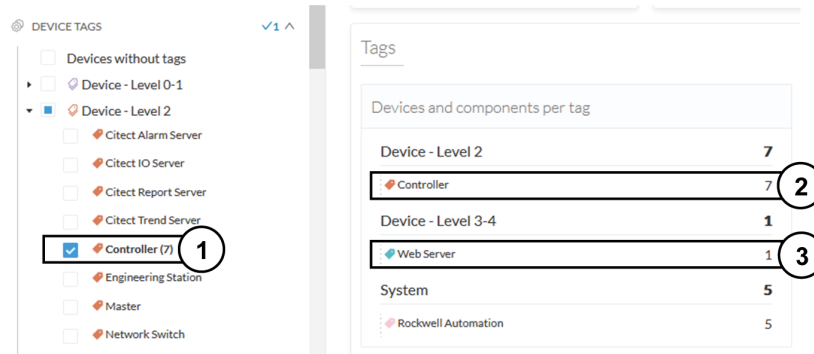
If you want to know more about one of these devices, switch to the Device and activity lists and reach them using the filter available in the tags column.

Activities per tag: As for activities, there is no activity tags set as criteria in the example below **(4)**. Yet, you can see that many activities have been found **(5)**. This is because the dashboard view collects all activities involved with the Controller devices found.
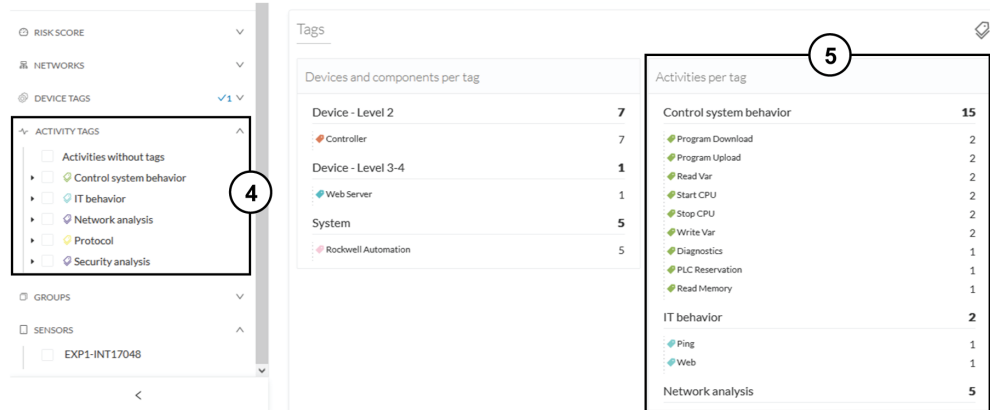
If you want to know more about one of these activities, switch to the Device and activity lists and reach them using the filter available in the tags column.

Device and activity lists

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

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

The All Controllers preset in the device list view:

The All Controllers preset in the activity list view:

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

- The sort icon **(1)** is to sort data by alphabetical order or by ascending/descending order.

- The filter icon **(2)** opens a field to type a specific data in, or a multiple choice menu **(3)** to filter tags.

Clicking an element in the lists opens its Right side panel which leads to more advanced data.

Map

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

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

Map

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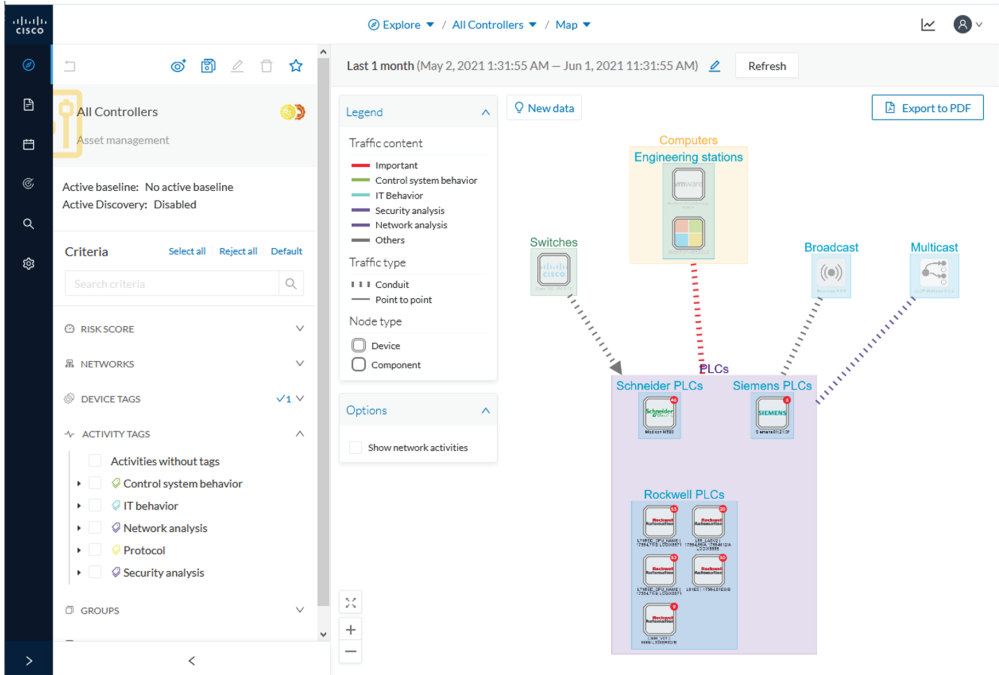
Note	The map is **self-organizing**, that is, elements are redistributed as devices, components, conduits and activities appear or disappear, and as groups are created or deleted. Moreover, the map automatically adapts over time and when changing preset. This way, it is guaranteed that the map is always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

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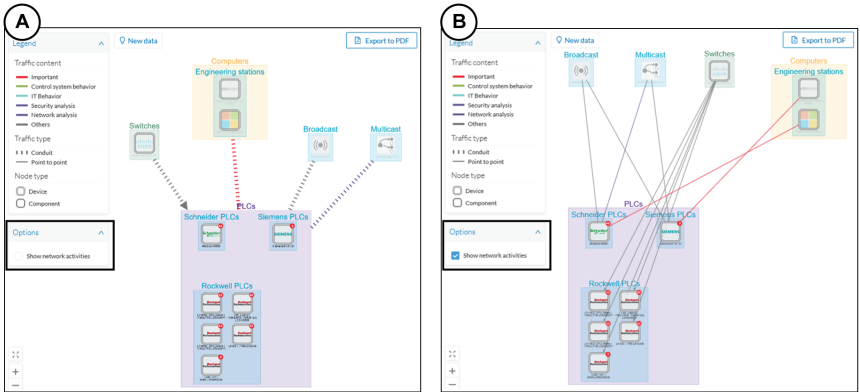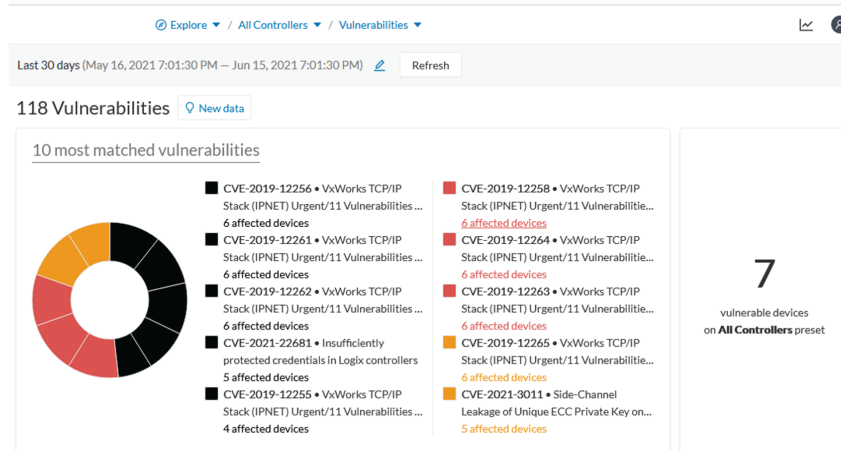
Vulnerabilities

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

☞		
Important	It is important to update the Knowledge DB in Cisco Cyber Vision as soon as possible after notification of a new version to be protected against vulnerabilities. To do so, refer to the corresponding documentation.	

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

On the right, you'll see a summary of the total number of devices that are vulnerable in the preset selected.

Below, you have a list of all the vulnerabilities found in the preset with sort icons to sort data by alphabetical order or by ascending/descending order, and filter icons which opens a field to type a specific data.

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

- The vulnerability name

- Its CVE ID (world unique identifier for a Common Vulnerability Exposure)

- Its CVSS score (Common Vulnerability Scoring System)

- The devices affected by the vulnerability

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

Security Insights

Security Insights is a view that provides statistics for DNS requests, HTTP requests, SMB Tree names and flows with no tag.
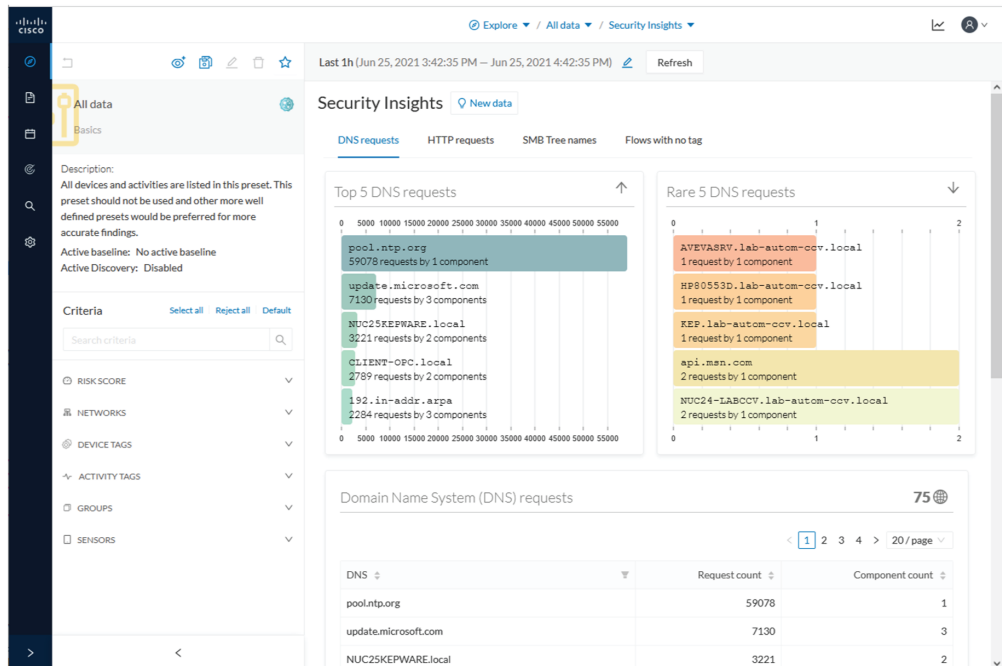
For each category, you will find the most frequent and rarest requests, and the list of all these requests.

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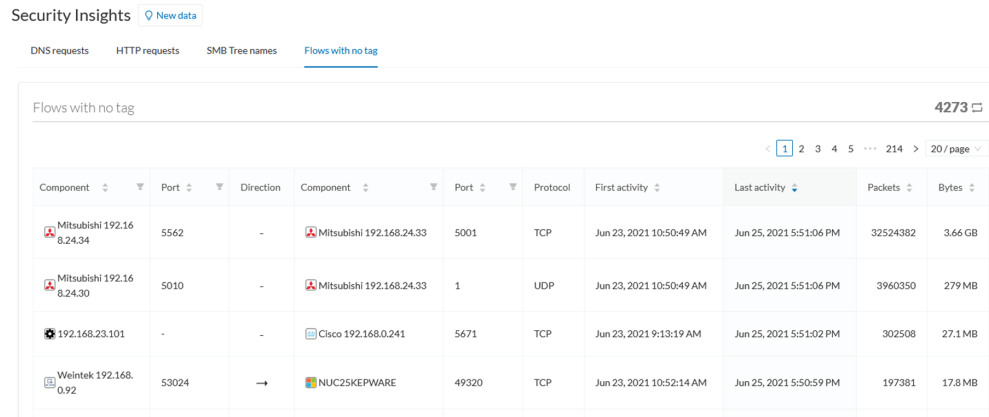
In this category, you will find a list of all flows with no tags, that is, traffic that Cisco Cyber Vision wasn't able to analyze. The reason can be that the protocol is not supported by Cisco Cyber Vision yet. However, this list is interesting from a security standpoint to make sure if such content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

Purdue Model

This map displays the assets of a preset according to the Purdue model architecture. Components are distributed among the layers by considering their tags. The Purdue Model view doesn't undergo any aggregation and is self-organizing.

Assets of the preset All Controllers distributed among the layers of the Purdue model:
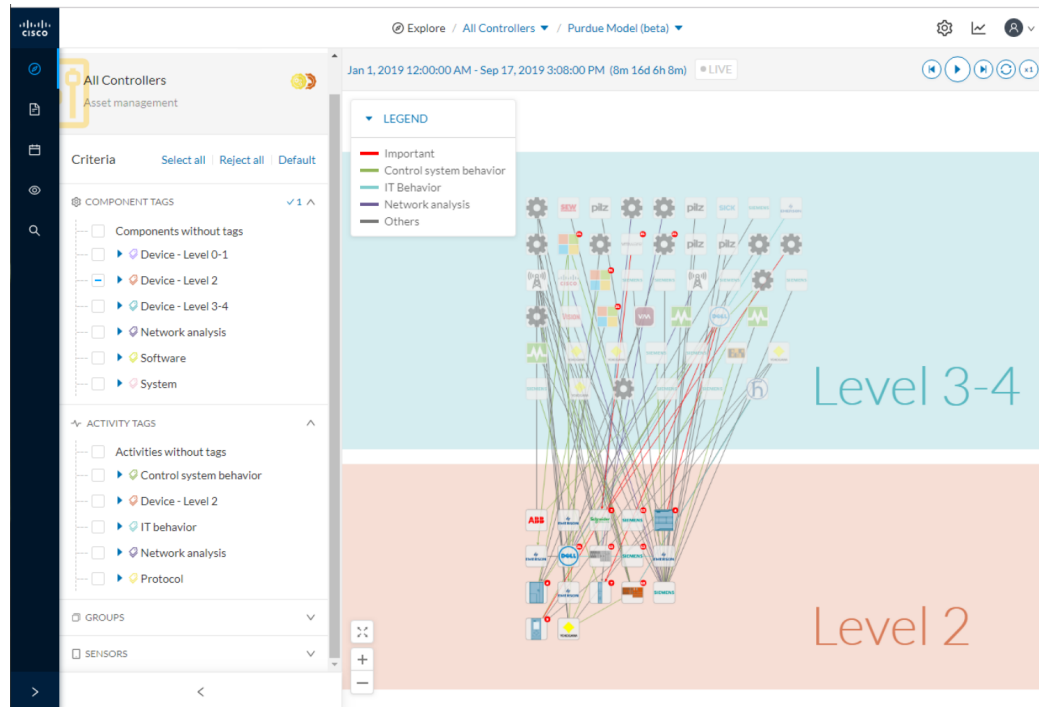
Components are distributed according to the different layers of the Purdue model:

- Level 0-1: Process and basic control (IO Modules).

- Level 2: Area supervisory control (PLCs, SCADA stations).

- Level 3-4: Manufacturing zone and DMZ (all others).

Right side panel

A right side panel is a condensed view about a device, a component, a group of components or an activity's information. This view allows you to quickly scan general information about an element meanwhile you're keeping an eye on a broader view such as a device list or a map.
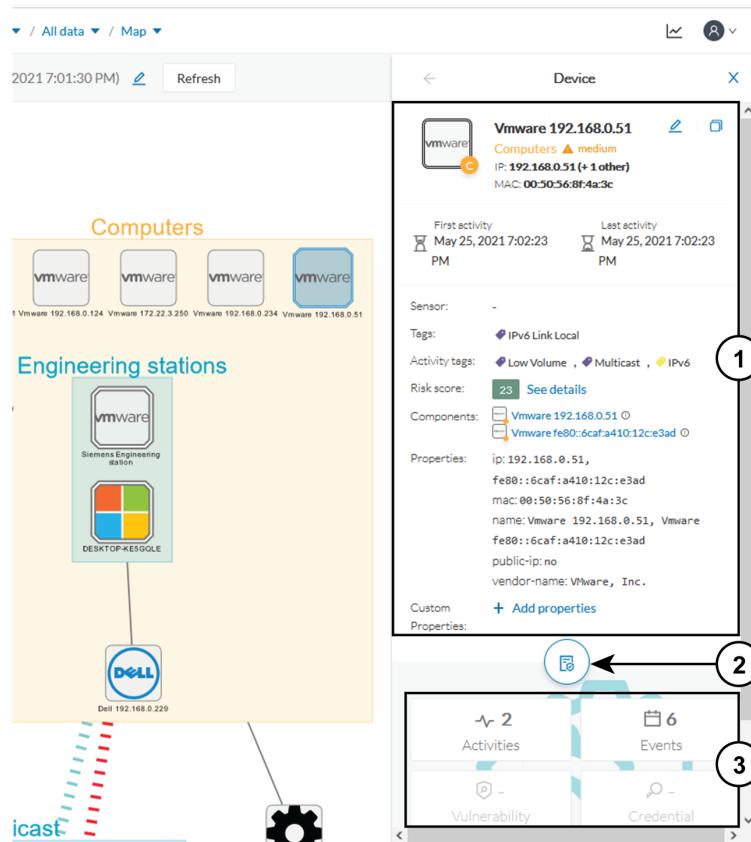
Right side panels differ depending on the type of element consulted. The higher part **(1)** of the right side panel gives you general information about the element. If consulting a device or a component, you can edit its name an add/remove it to/from a group.

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.

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

Technical sheets

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

A device's technical sheet:

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

The lower part **(2)** contains detailed information classified under tabs, displaying or not according to the element you're on:

- Basics contains an element's properties and tags that are categorized with their definition. Device's components also appear if applicable.

- Risk score with an overview and a more detailed and focused views.

- Security contains a component's vulnerabilities you can acknowledge and credentials.

- Activity is about an activity's flows and contains a Mini map which is a view that is restricted to a device or a component and its activities. If applicable, a list of External communication with related information appears under the corresponding tab.

- Automation contains variable accesses.

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

- More information about Properties.

- More information about Tags.

- More information about the Risk score.

- More information about Vulnerability.

- More information about Credentials.

- More information about Flow.

- More information about the Mini map.

      • More information about 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.

This view is accessible through the Activity tab of a Component's Technical sheets.
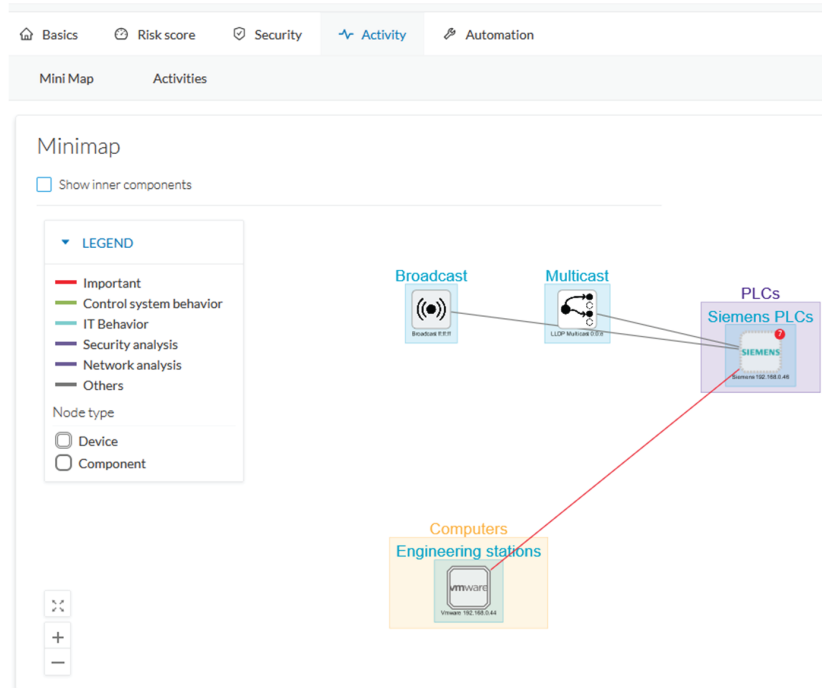
The option "Show inner components" enables an exploded view of the devices.
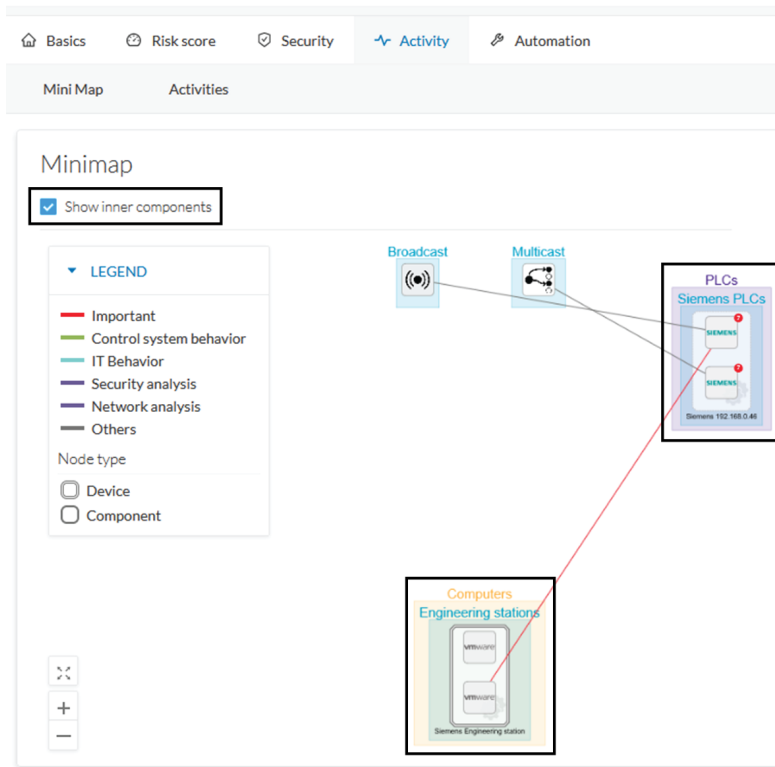
Clicking any element in the Mini Map will open its Right side panel so you can have access to further information.

C H A P T E R 22

Reports

Reports

Security posture reports allow you to export industrial network data from the traffic captured and processed by Cisco Cyber Vision.

That way, you can show off striking information like sensitive entrance points, acknowledged vulnerabilities for status reports, etc.

You must install the reports extension to be able to use this page. You can do so by importing the reports extension file through the Admin Extension page in Cisco Cyber Vision. The extension file is available on cisco.com.

Security posture reports allow you to create reports from a Preset, that is a a set of data, present by default in Cisco Cyber Vision, or a custom one.

Reports are exportable in docx and pdf formats.

You can costumize the report by adding a logo, such as the company's one. By default, the report will be generated with Cisco's logo.

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

Create a report

Procedure

Step 1   Click **Create and run a report**.
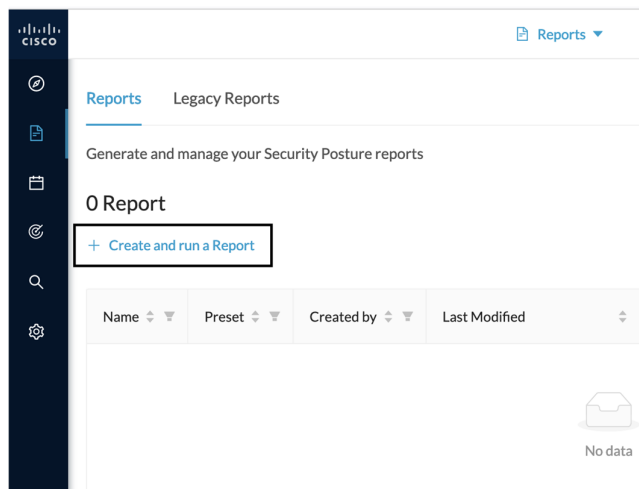
Step 2   Give the report a name and optionally add a description.

Step 3   Optionally, add a logo. It will appear on the report.

Step 4   Select the format(s) you want the report to be generated to.

Step 5   Click **Next**.

Step 6   Select a preset from the dropdown menu.

Step 7   Under table of content, select the content you want to appear in the report.
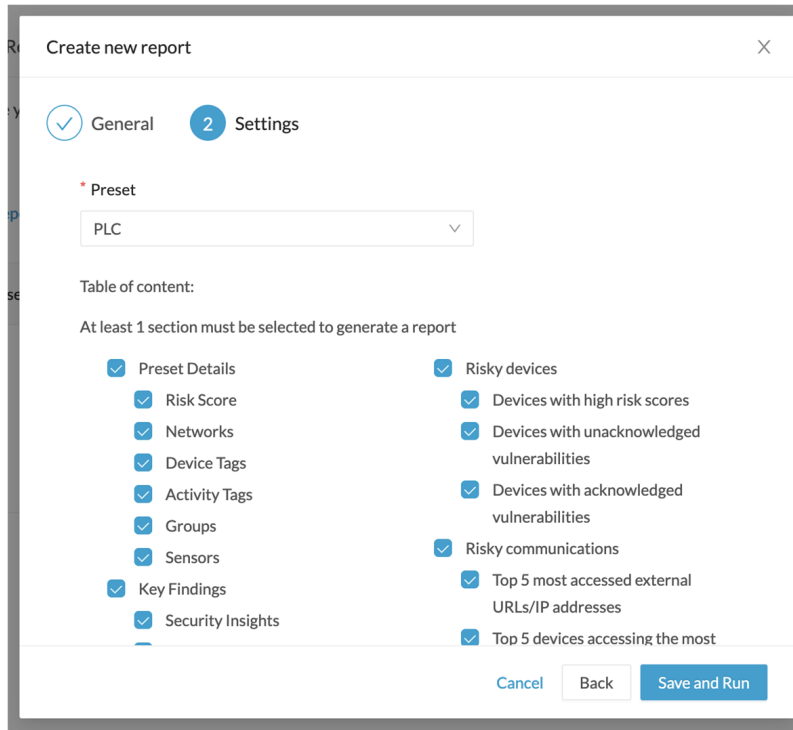
Step 8   Click **Save and run**.

The new report appears in the list with the status Processing. It should eventually turn to Success after a few moment once the report is generated.
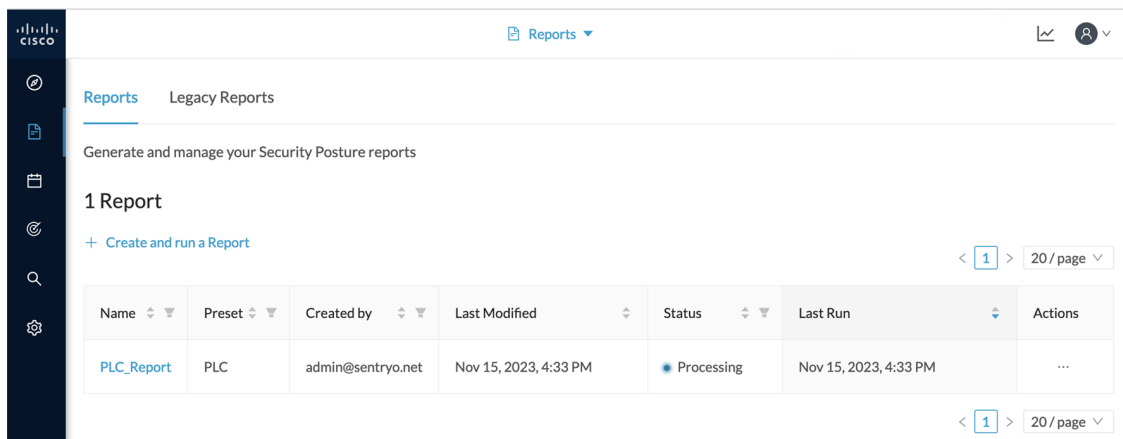
Step 9   To download the report, click the name of the report in the list to open its right side panel or the format button(s).
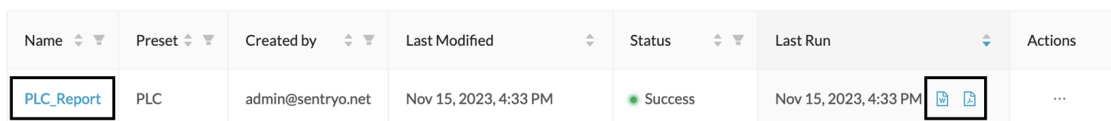
Step 10   On the right side panel, click the links to download the latest reports.

You will find older ones under the Previous Reports menu.
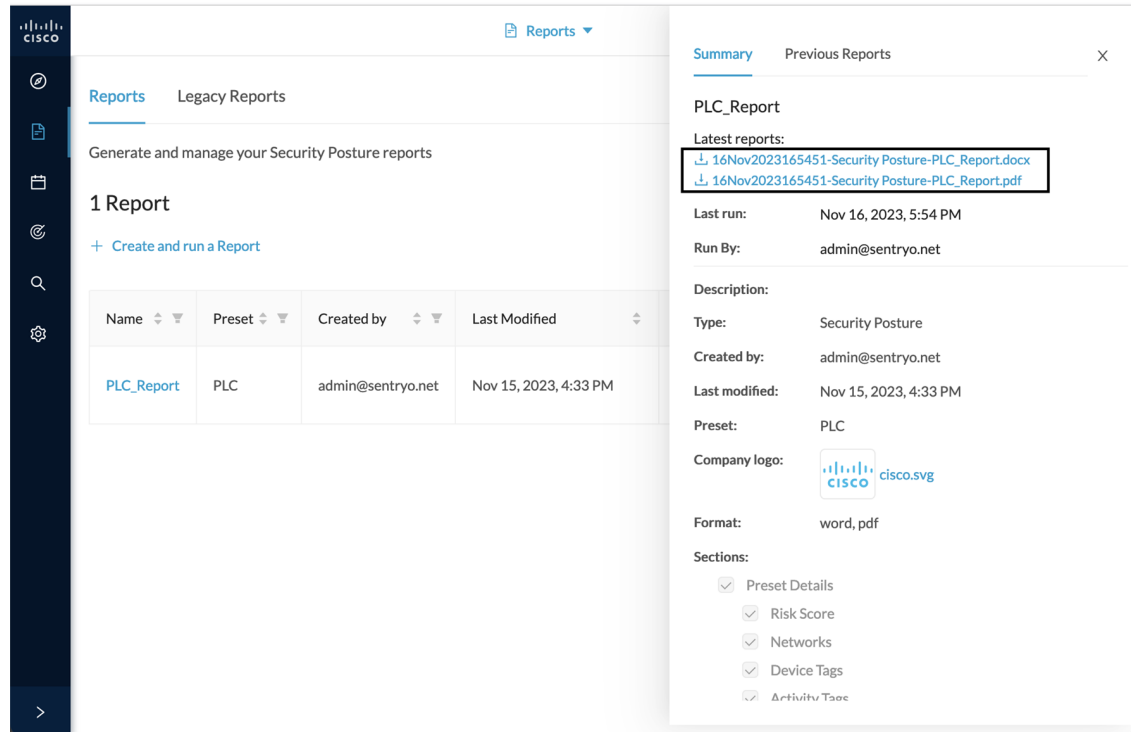
Step 11   To generate a new report click **Run Again** under Actions.
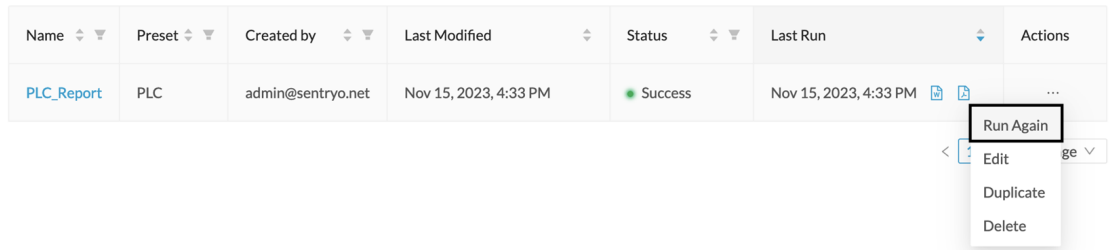
Legacy Reports

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

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

- The **inventory report** lists and details all components of your industrial network. They are sorted by group. For each component different information is given like the component name, when it was active for the first and the last time and tags that qualify its activity. If available, you will also find technical details such as its MAC and IP addresses, hardware and firmware versions, the serial number and extra properties.

- The **activity report** lists and details all communications exchanged between the components of your industrial network. They are sorted by group and by direction (inner, incoming and outgoing communications regarding a group). Information provided includes the protocol, which source and destination ports have been used and tags that qualify its activity.

- The **vulnerability report** lists all components detected as vulnerable and gives further details about vulnerabilities. Vulnerabilities are based on the Knowledge DB provided by Cisco. So, the more you keep the Knowledge DB up to date, the better you will be notified about new known vulnerabilities. The report contains information about the vulnerability, its impact level, its CVSS (Common Vulnerability Scoring System) and solutions. A vulnerability is often about outdated software parts. It is strongly recommended to fix outdated states as soon as possible. Links to manufacturers' websites are provided for this purpose.

- The **PLC report** lists all PLCs in your industrial network. For each PLC, the report lists and details properties, events, programs, program blocks and variable accesses, if there are any.

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

C H A P T E R **23**

Events

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

Refer to the events administration page on the GUI to see all events available. To do so, refer to the Cisco Cyber Vision Administration Guide.

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

- The The Dashboard: a visual and continuously-updated view of the current state of the installation based on the number of events (by severity and over time).

- The The Calendar: a chronological and continuously-updated view of the events within which you can search events.

The Dashboard

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

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

You can see the list of events per categories in the events administration page. To do so, refer to the Cisco Cyber Vision Administration Guide.

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

Below, the line chart puts an emphasis on the number of events per severity over time.
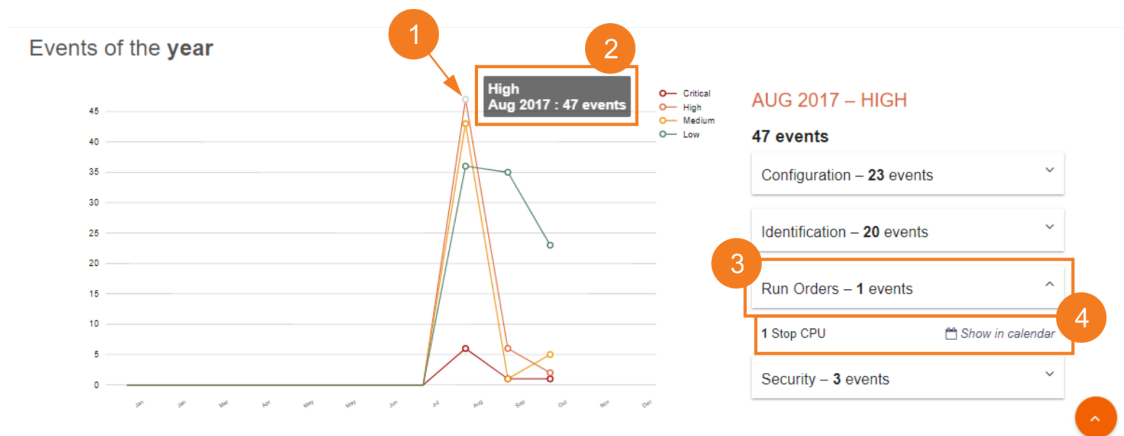
Clicking event markers **(1)** on the line chart lets you see the number of events per category according to a specific time **(2)**.

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

The Calendar

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

You can also see events that have happened during the day, week, month and year.
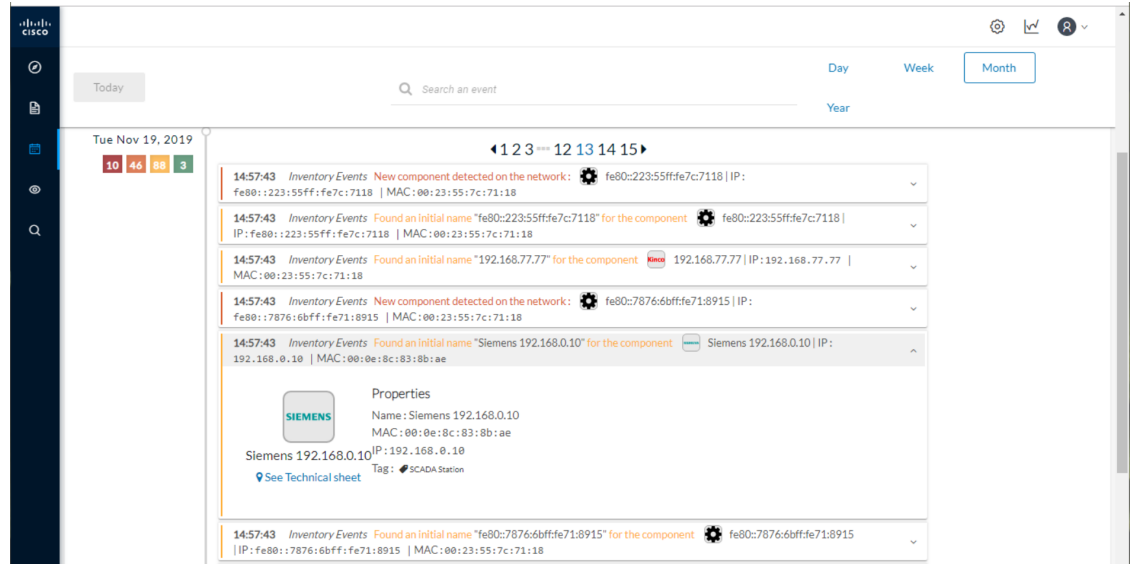
Clicking on a result event will show you details about the event.

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

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

C H A P T E R 24

Monitor

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

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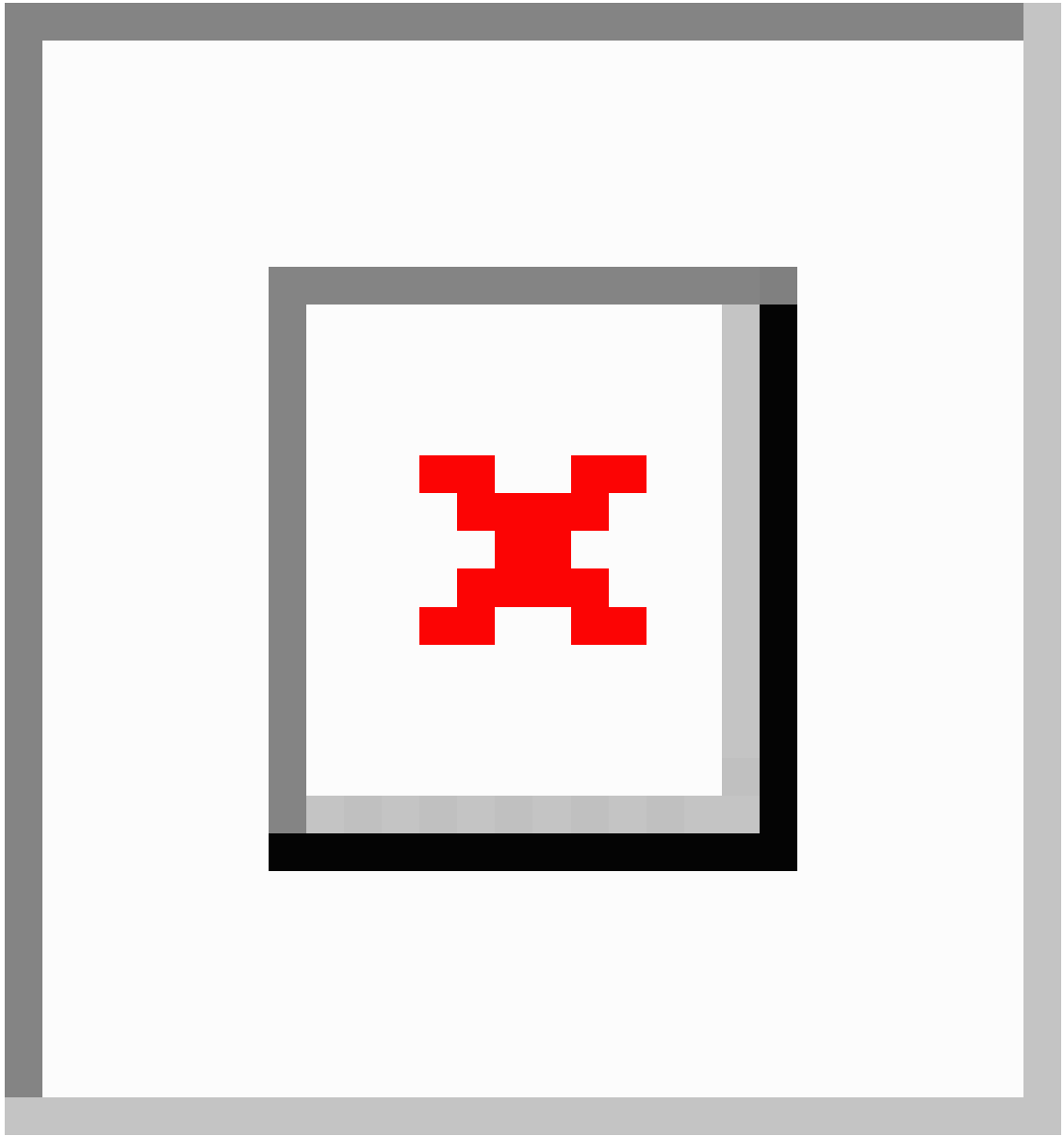
For more information, refer to the Cisco Cyber Vision GUI Monitor Mode User Guide available on cisco.com.

Search

• Search, on page 103

Search

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

✎

Note   Devices are not available in this page yet.
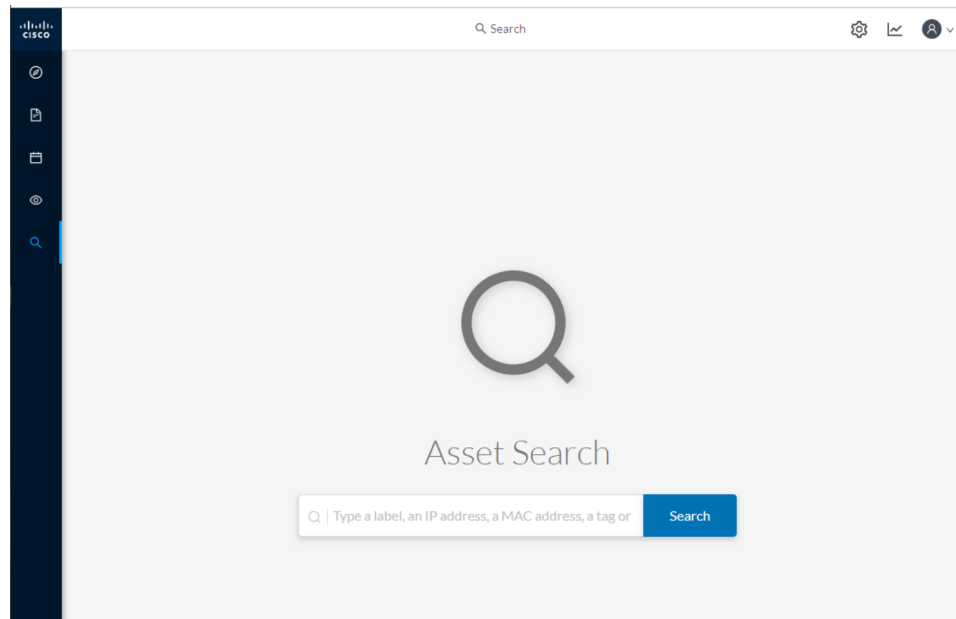
Results out of a Station research:
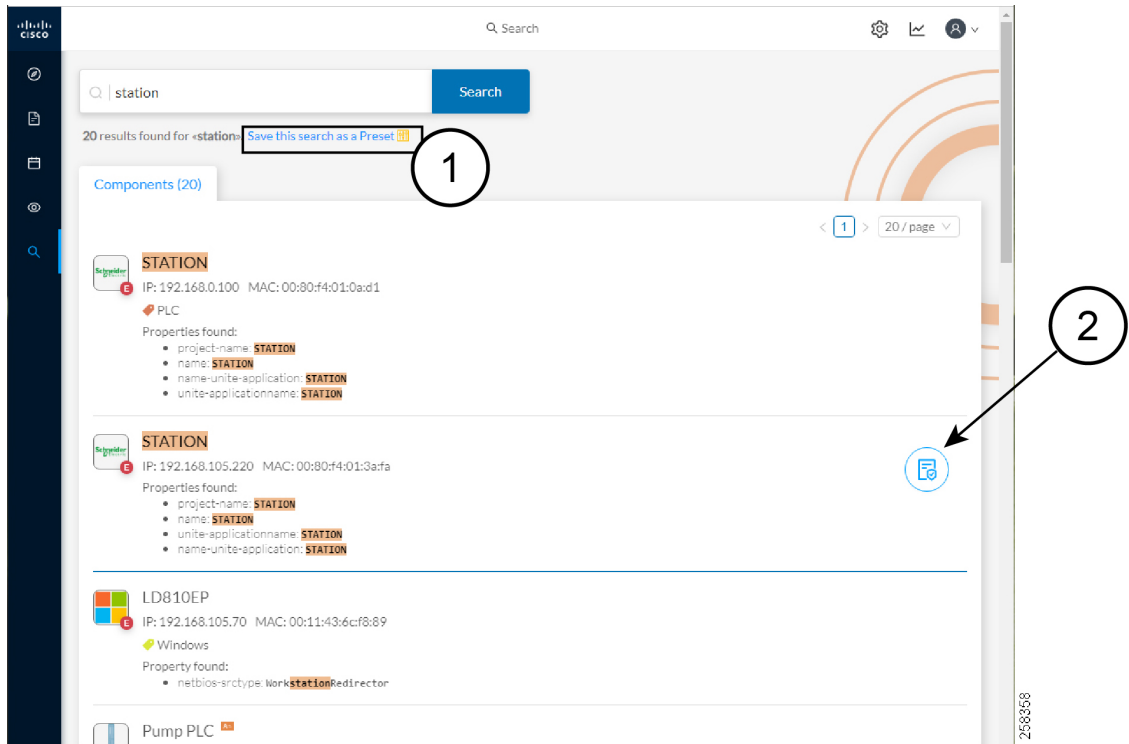
In the example above, 20 components have been found with the mention "station" in their name, property values and tags.

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

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

C H A P T E R **26**

System statistics

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

- Center, on page 105
- Sensors, on page 108

Center

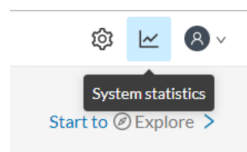The Center statistics view provides data about the state of the Center CPU, RAM, disk, network interfaces bandwidth and database.

Note   Most data presented below evolve as you select a different period of time.
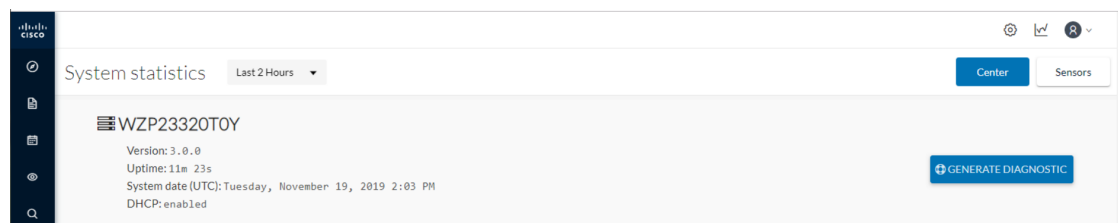
At the top of the page, you will find general information about the Center (the software version, the length of time that it has been operating (i.e. uptime), the Center system date and whether DHCP is enabled or not).

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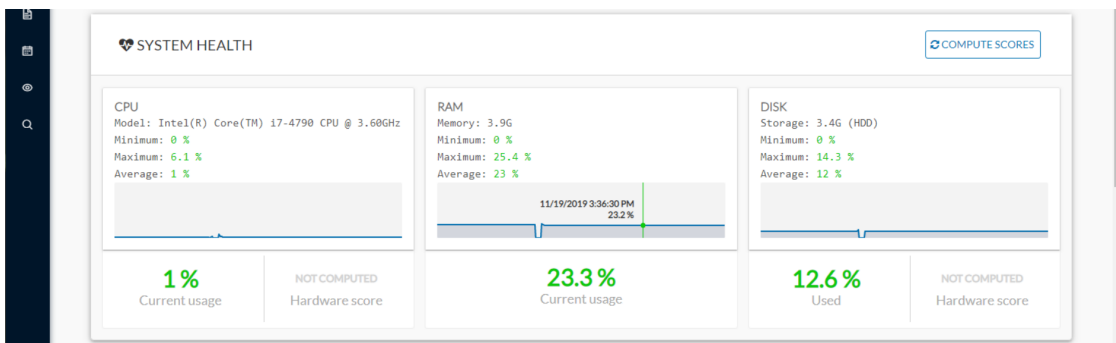
System health:

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

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

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

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

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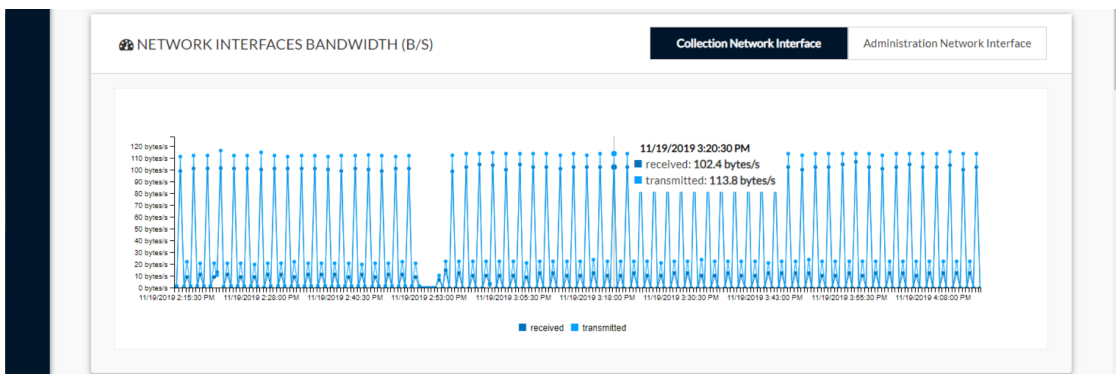
The line charts represent the Administration and Collection network interfaces bandwidth with the number of bytes received and sent by the Center per second.

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

Disk I/O:

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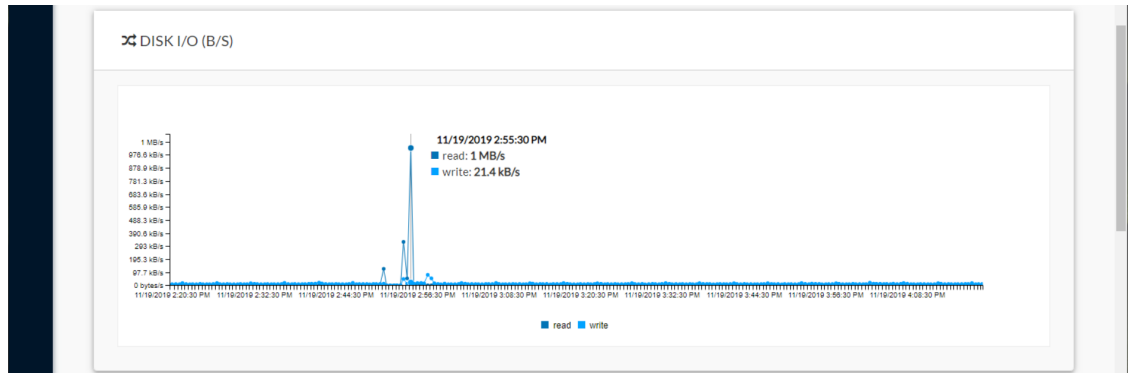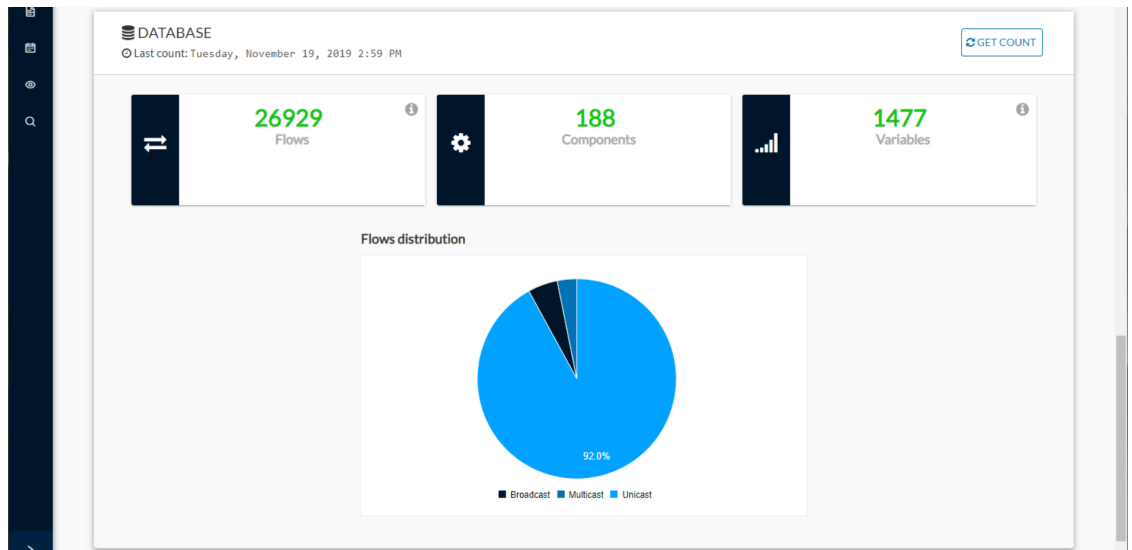
Database:

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

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

The flows card indicates the total number of flows (i.e. broadcast, multicast and unicast which are stored in the database) detected by Cisco Cyber Vision. If you mouse over the card, you will get the number of activities and the flows evolution tendency. This information enables you to anticipate how the system load might be affected by flows in the future.
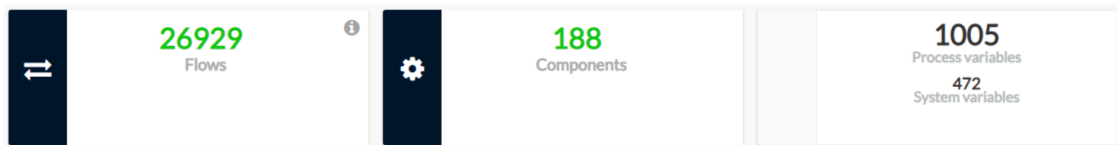
The variables card indicates the total number of variables detected by Cisco Cyber Vision. This indicator is important because an overload of variables could impact the Cisco Cyber Vision performances. If you mouse over the card you will get the number of process variables and the number of system variables.

- Process variables are the number of variables used by PLCs' software. Process variables are visible in the Monitor mode of the Cisco Cyber Vision GUI.

- System variables are the number of variables necessary to PLCs' proper operation. System variables are stored in the Cisco Cyber Vision database.
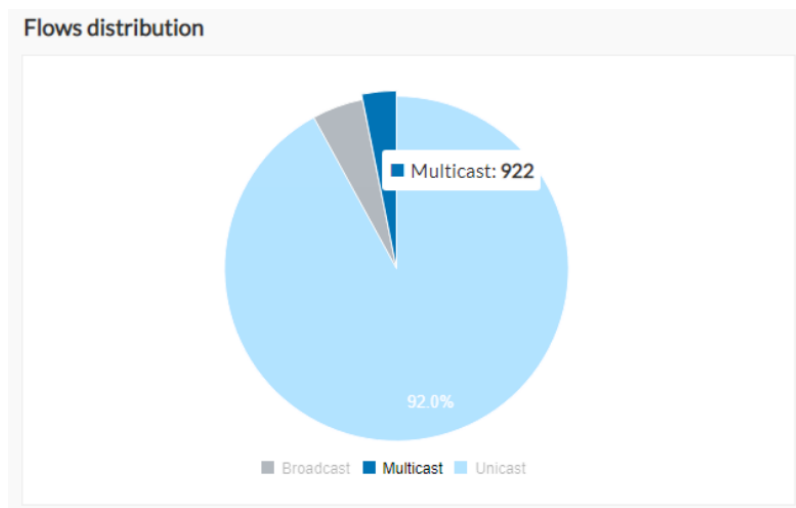
The flows distribution pie chart indicates the distribution of broadcast, multicast and unicast flows stored in the database. Mouse over the chart to see the absolute number of flows per flow type.

Sensors

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

Note   Most data presented below evolve as you select a different period of time.
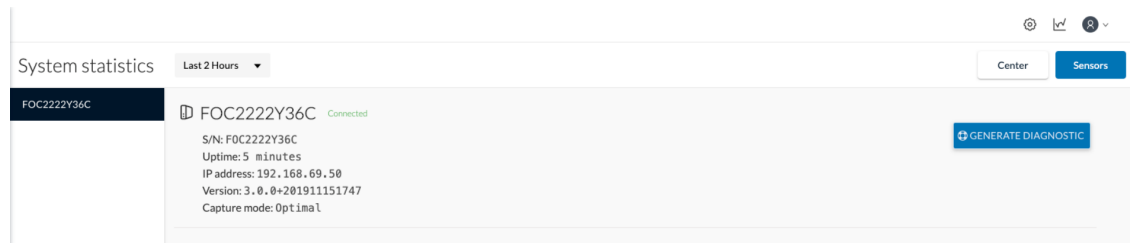
On the left you have a list of the sensors (only one sensor is represented here). Click on a sensor name to access its statistics.

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

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

System health:

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

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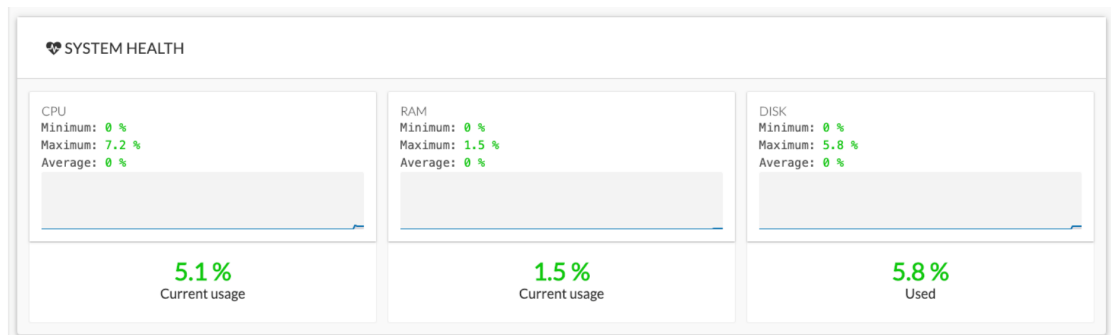

Below, you have the percentage of the system current usage. There is also an indicative hardware score which is useful to Cisco product support.

Packets captured:

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

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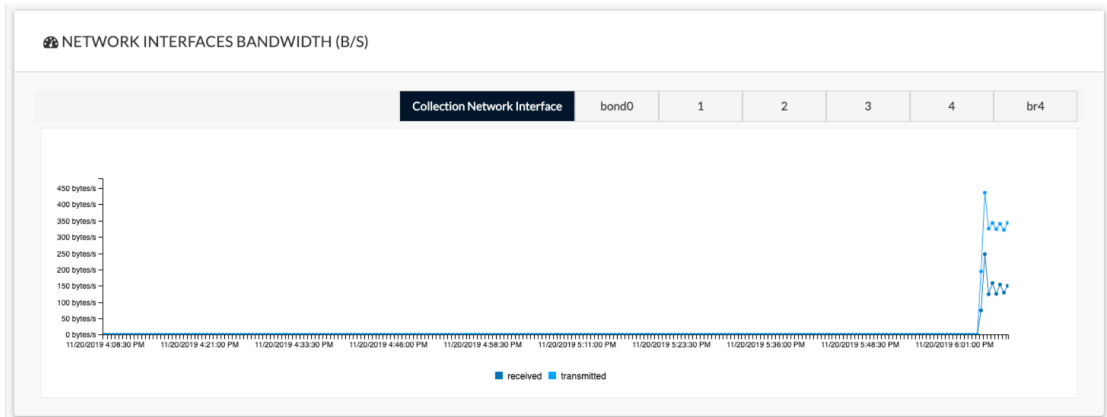
The line charts represent the Collection and the Industrial network interfaces bandwidth with the number of bytes received and sent by the Center per second.

- The Collection Network interface activity chart lets you see the amount of data exchanged between the Center and the sensors.

- The Industrial ones lets you see the amount of data captured by the sensor on the industrial network through each ports couple.

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

Disk I/O:
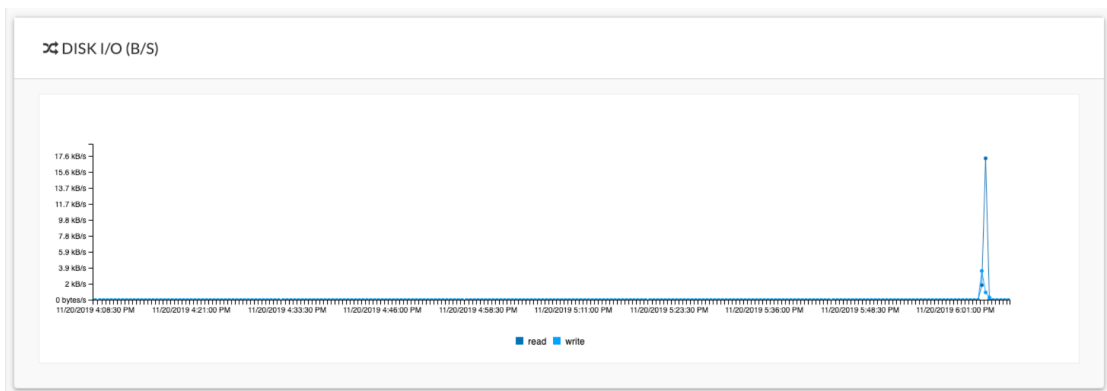
The line chart represents the sensor hard disk usage with the number of bytes read and written per second.
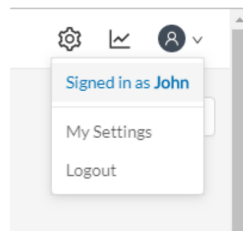
My settings

My settings

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

From this page, you can:

- Modify your first and last name.

- Change the interface language. Cisco Cyber Vision is available in English, French, German, Japanese, Spanish and Turkish.

- Change your password.

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

  - Must contain a lower case character: a-z.

  - Must contain an upper case character: A-Z.

  - Must contain a numeric character: 0-9.

  - Cannot contain the user id.

  - Must contain a special character: ~!"#$%&'()*+,-./:;<=>?@[]^_{|}.

👉

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

Note Your email will be requested for login access.

- Restore interface notifications.

- Clear application cookies.