Cisco Cyber Vision GUI User Guide, Release 4.2.0

First Published: 2021-01-01

Last Modified: 2023-04-28

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

About this documentation

Document purpose

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

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

This manual is applicable to **system version 4.2.0**.

Warnings and notices

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

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

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

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

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

CHAPTER 1

Introduction

Cisco Cyber Vision Installation

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

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

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

If everything is ready to start using the GUI, note that at least one sensor has to be enrolled so that you can enjoy your first experience with the GUI. To do so, 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

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

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

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

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

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

CHAPTER 3

Filter

- Filters, on page 7

Filters

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

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

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

Each category allows to define a subset of the components, or activities for the Activity filter.

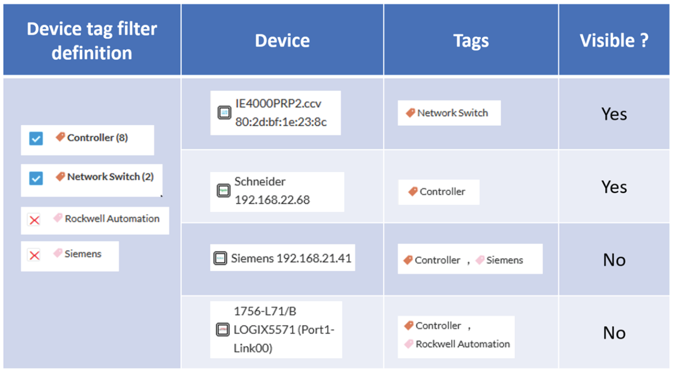
If filters are defined by several categories, the resulting dataset is the intersect of the selections for each category.

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

Device tags

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

Device tag filters



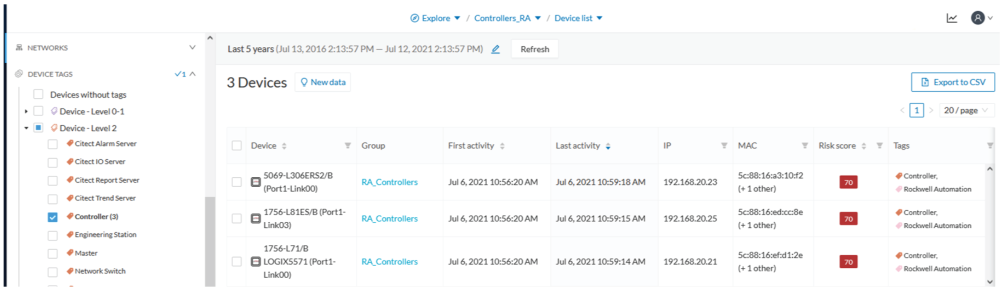
Device tag filter definition	Device	Tags	Visible ?
☑ Controller (8) ☑ Network Switch (2) ☒ Rockwell Automation ☒ Siemens	IE4000PRP2.ccv 80:2d:bf:1e:23:8c	Network Switch	Yes
	Schneider 192.168.22.68	Controller	Yes
	Siemens 192.168.21.41	Controller , Siemens	No
	1756-L71/B LOGIX5571 (Port1-Link00)	Controller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

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

For the other displays like activity list or map, the devices which are communicating with the selected devices will be displayed too (all engineering stations or HMI in our example).

It will give the following results:

Device tag filter, example of Controllers – list of devices



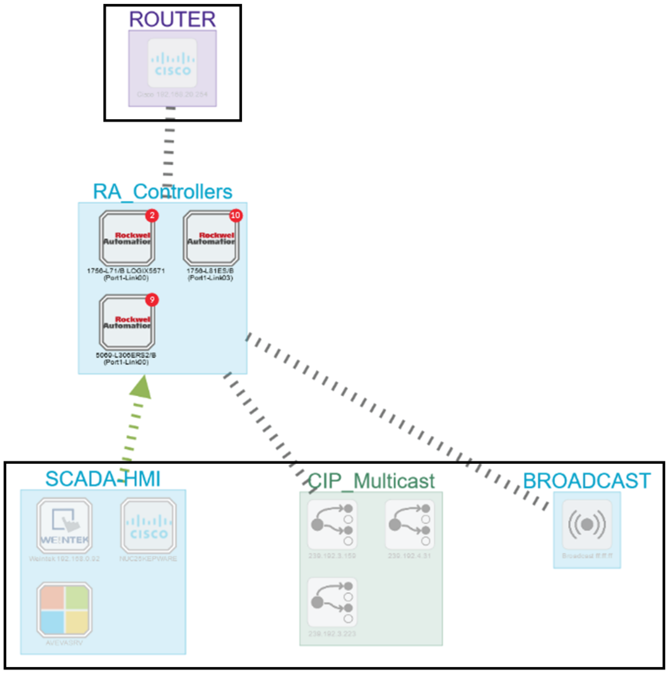
Last 5 years (Jul 13, 2016 2:13:57 PM – Jul 12, 2021 2:13:57 PM)

3 Devices

Device	Group	First activity	Last activity	IP	MAC	Risk score	Tags
5069-L306ERS2/B (Port1-Link00)	RA_Controllers	Jul 6, 2021 10:56:20 AM	Jul 6, 2021 10:59:18 AM	192.168.20.23	5c:88:16:a3:10:f2 (+ 1 other)	70	Controller, Rockwell Automation
1756-L81ES/B (Port1-Link03)	RA_Controllers	Jul 6, 2021 10:56:20 AM	Jul 6, 2021 10:59:15 AM	192.168.20.25	5c:88:16:ed:cc:8e (+ 1 other)	70	Controller, Rockwell Automation
1756-L71/B LOGIX5571 (Port1-Link00)	RA_Controllers	Jul 6, 2021 10:56:20 AM	Jul 6, 2021 10:59:14 AM	192.168.20.21	5c:88:16:ef:d1:2e (+ 1 other)	70	Controller, Rockwell Automation

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

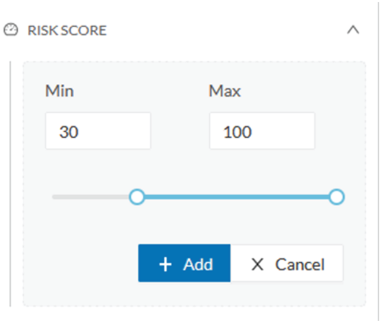
Device tag filter, example of Controllers - map


ROUTER
RA_Controllers
1756-L71/B LOGIX5571 (Port1-Link00)
1756-L81ES/B (Port1-Link03)
5069-L306ERS2/B (Port1-Link00)
SCADA-HMI
CIP_Multicast
BROADCAST

Risk score

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

Risk score, filter definition

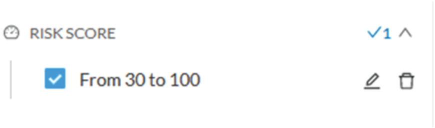


RISK SCORE

Min: 30

Max: 100

Risk score – inclusive filter



RISK SCORE ✓1

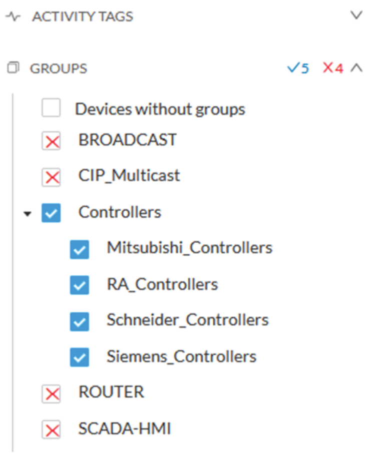
☑ From 30 to 100

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

Groups

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

Group filter



- □ Devices without groups
- ☒ BROADCAST
- ☒ CIP_Multicast
- ☑ Controllers
  - ☑ Mitsubishi_Controllers
  - ☑ RA_Controllers
  - ☑ Schneider_Controllers
  - ☑ Siemens_Controllers
- ☒ ROUTER
- ☒ SCADA-HMI

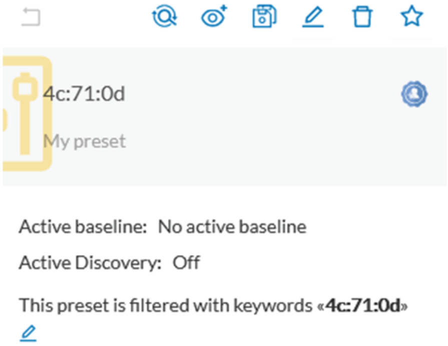
In the example above, only the devices belonging to the selected groups will be selected.

Activities always involve two end points and are selected if either end point is part of a selected group, and none are part of an excluded group.

Keyword

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

Keyword = 4c:71:0d



4c:71:0d

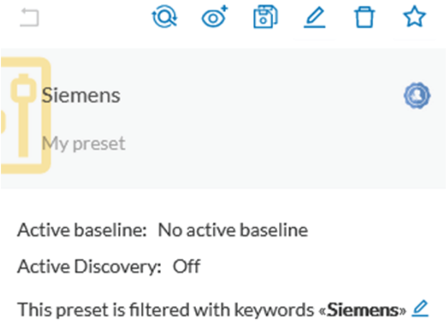
My preset

Active baseline: No active baseline

Active Discovery: Off

This preset is filtered with keywords «**4c:71:0d**»

Keyword =siemens



Siemens

My preset

Active baseline: No active baseline

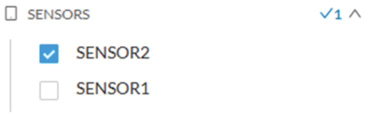
Active Discovery: Off

This preset is filtered with keywords «**Siemens**»

Sensors

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

Sensor filter



□ SENSORS ✓1

☑ SENSOR2

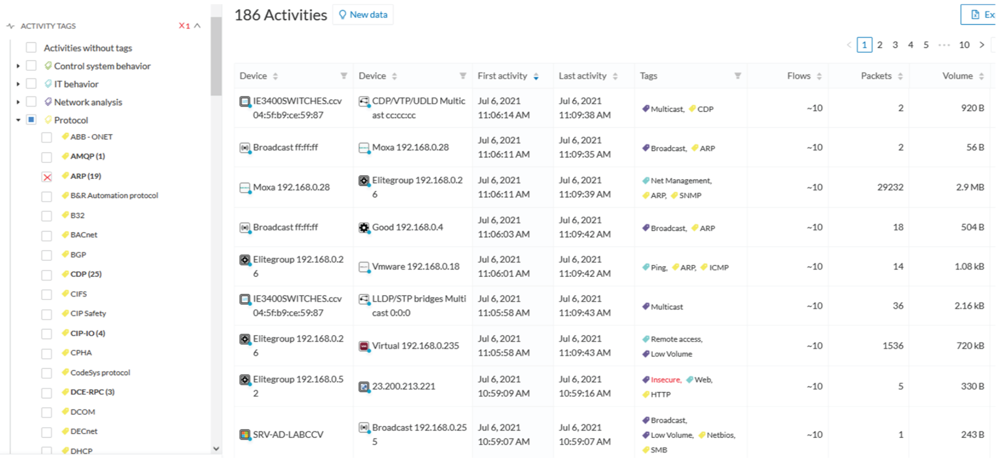
□ SENSOR1

Activity tags

Filtering on activity tag will not have the same behavior than a filter based on devices. Inclusive activity tag filters will be the same, but exclusive will remove activities only when all activity tags are included in the set of excluded tags.

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

Activity filter – negative filter 1



ACTIVITY TAGS ✕1

- □ Activities without tags
- □ Control system behavior
- □ IT behavior
- □ Network analysis
- ■ Protocol
  - □ ABB - ONET
  - □ AMQP (1)
  - ☒ ARP (19)
  - □ B&R Automation protocol
  - □ B32
  - □ BACnet
  - □ BGP
  - □ CDP (25)
  - □ CIFS
  - □ CIP Safety
  - □ CIP-IO (4)
  - □ CPHA
  - □ CodeSys protocol
  - □ DCE-RPC (3)
  - □ DCOM
  - □ DECnet
  - □ DHCP

186 Activities New data

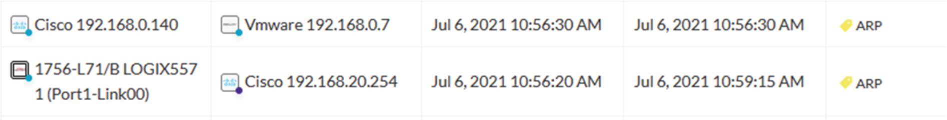
Ex

< 1 2 3 4 5 ··· 10 >

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

In the example above, several activities are kept because the ARP tag is present as well as other activity tags. There is no exact match. But the activity below is hidden:

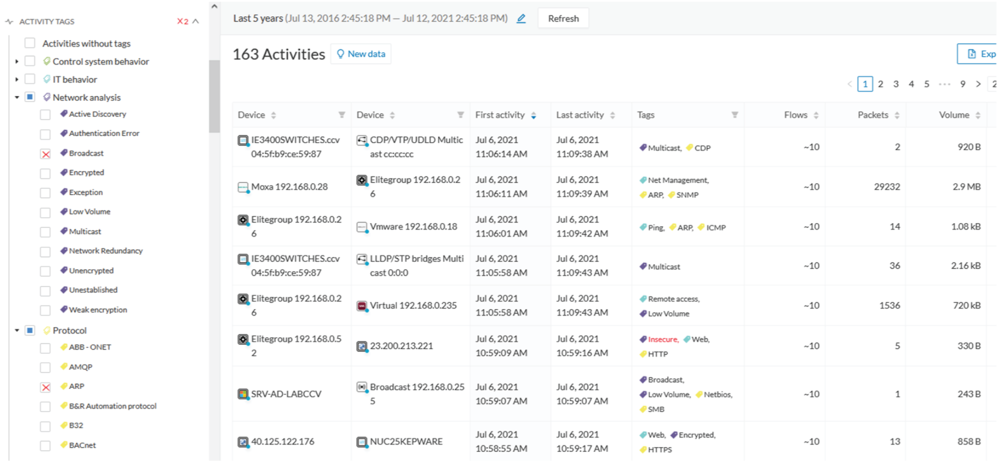
filter 2



Cisco 192.168.0.140	Vmware 192.168.0.7	Jul 6, 2021 10:56:30 AM	Jul 6, 2021 10:56:30 AM	ARP
1756-L71/B LOGIX557 1 (Port1-Link00)	Cisco 192.168.20.254	Jul 6, 2021 10:56:20 AM	Jul 6, 2021 10:59:15 AM	ARP

To remove broadcast and ARP activities, both activity tags need to be selected like below:

Activity filter – negative filter 3



ACTIVITY TAGS ✕2

- □ Activities without tags
- □ Control system behavior
- □ IT behavior
- ■ Network analysis
  - □ Active Discovery
  - □ Authentication Error
  - ☒ Broadcast
  - □ Encrypted
  - □ Exception
  - □ Low Volume
  - □ Multicast
  - □ Network Redundancy
  - □ Unencrypted
  - □ Unestablished
  - □ Weak encryption
- ■ Protocol
  - □ ABB - ONET
  - □ AMQP
  - ☒ ARP
  - □ B&R Automation protocol
  - □ B32
  - □ BACnet

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

163 Activities New data

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

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

Above rules, for positive and negative selection, are combined, resulting in the following logic:

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

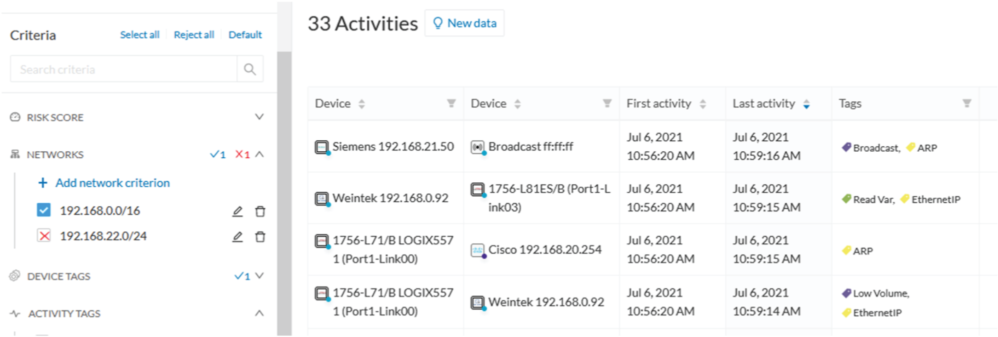
Networks

A filter can be defined based on network settings: IP range or VLAN ID can be used. This filter will have an impact on the activity list, the result will be "all activities with one end belonging to this network". Activities with at least one device in the corresponding network will be selected.

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

Exclusion and combination also can be used, for instance:

Network filter – negative filter

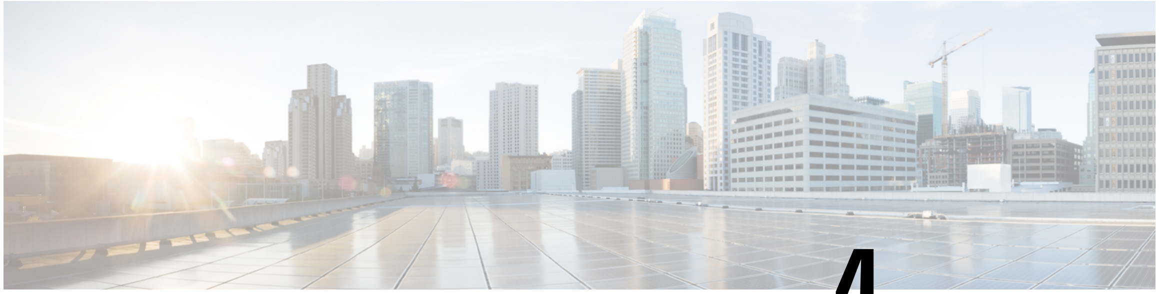


Device	Device	First activity	Last activity	Tags
Siemens 192.168.21.50	Broadcast ff:ff:ff	Jul 6, 2021 10:56:20 AM	Jul 6, 2021 10:59:16 AM	Broadcast, ARP
Weintek 192.168.0.92	1756-L81ES/B (Port1-Link03)	Jul 6, 2021 10:56:20 AM	Jul 6, 2021 10:59:15 AM	Read Var, EthernetIP
1756-L71/B LOGIX5571 (Port1-Link00)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

Multiple negative selections are not supported on 4.0.0.

Filter combination

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



CHAPTER 4

Component

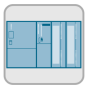
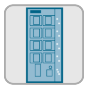
Component

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

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

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

Some examples of icons:

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

Broadcast	((●))	Broadcast destination component.
Multicast		

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

For more information, refer to the Device section.

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

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

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

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

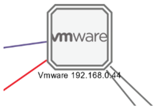
CHAPTER 5

Device

Device

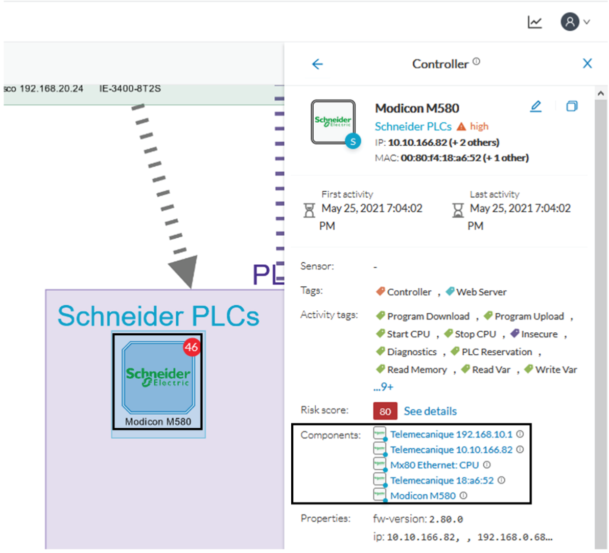
The concept of device has been developed to show the network from a physical point of view (in Cisco Cyber Vision versions older than 4.0.0 only components and aggregated components were used). A device represents in Cisco Cyber Vision a physical machine of the industrial network such as a switch, an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

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



Technically, a device is an aggregation of Component that have been brought together because they have similar properties. In fact, components can share same characteristics such as same IP address, same MAC address, same Netbios name, etc. In addition, tags and properties which are found in protocols are associated to define the type of device. Aggregation of components into a device and definition of the device type are based on a large set of rules with priorities that can be more or less complex.

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



Controller

Modicon M580
Schneider PLCs high
IP: 10.10.166.82 (+ 2 others)
MAC: 00:80:f4:18:a6:52 (+ 1 other)

First activity May 25, 2021 7:04:02 PM

Last activity May 25, 2021 7:04:02 PM

Sensor: -

Tags: Controller , Web Server

Activity tags: Program Download , Program Upload , Start CPU , Stop CPU , Insecure , Diagnostics , PLC Reservation , Read Memory , Read Var , Write Var ...9+

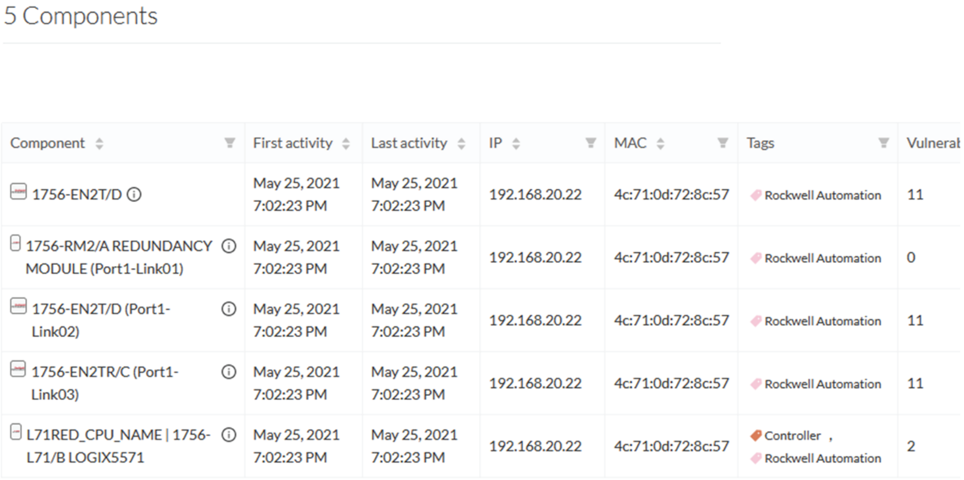
Risk score: 80 See details

Components: Telemecanique 192.168.10.1
Telemecanique 10.10.166.82
Mx80 Ethernet: CPU
Telemecanique 18:a6:52
Modicon M580

Properties: fw-version: 2.80.0
ip: 10.10.166.82, , 192.168.0.68...

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

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



5 Components

Component	First activity	Last activity	IP	MAC	Tags	Vulnerat
1756-EN2T/D ⓘ	May 25, 2021 7:02:23 PM	May 25, 2021 7:02:23 PM	192.168.20.22	4c:71:0d:72:8c:57	Rockwell Automation	11
1756-RM2/A REDUNDANCY MODULE (Port1-Link01) ⓘ	May 25, 2021 7:02:23 PM	May 25, 2021 7:02:23 PM	192.168.20.22	4c:71:0d:72:8c:57	Rockwell Automation	0
1756-EN2T/D (Port1-Link02) ⓘ	May 25, 2021 7:02:23 PM	May 25, 2021 7:02:23 PM	192.168.20.22	4c:71:0d:72:8c:57	Rockwell Automation	11
1756-EN2TR/C (Port1-Link03) ⓘ	May 25, 2021 7:02:23 PM	May 25, 2021 7:02:23 PM	192.168.20.22	4c:71:0d:72:8c:57	Rockwell Automation	11
L71RED_CPU_NAME | 1756-L71/B LOGIX5571 ⓘ	May 25, 2021 7:02:23 PM	May 25, 2021 7:02:23 PM	192.168.20.22	4c:71:0d:72:8c:57	Controller , Rockwell Automation	2

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

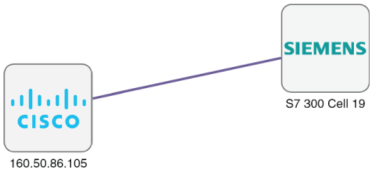
To know which types of device Cisco Cyber Vision is capable of detecting, take a look at the device Tags classified per level in the Cisco Cyber Vision application.

CHAPTER 6

Activity

Activity

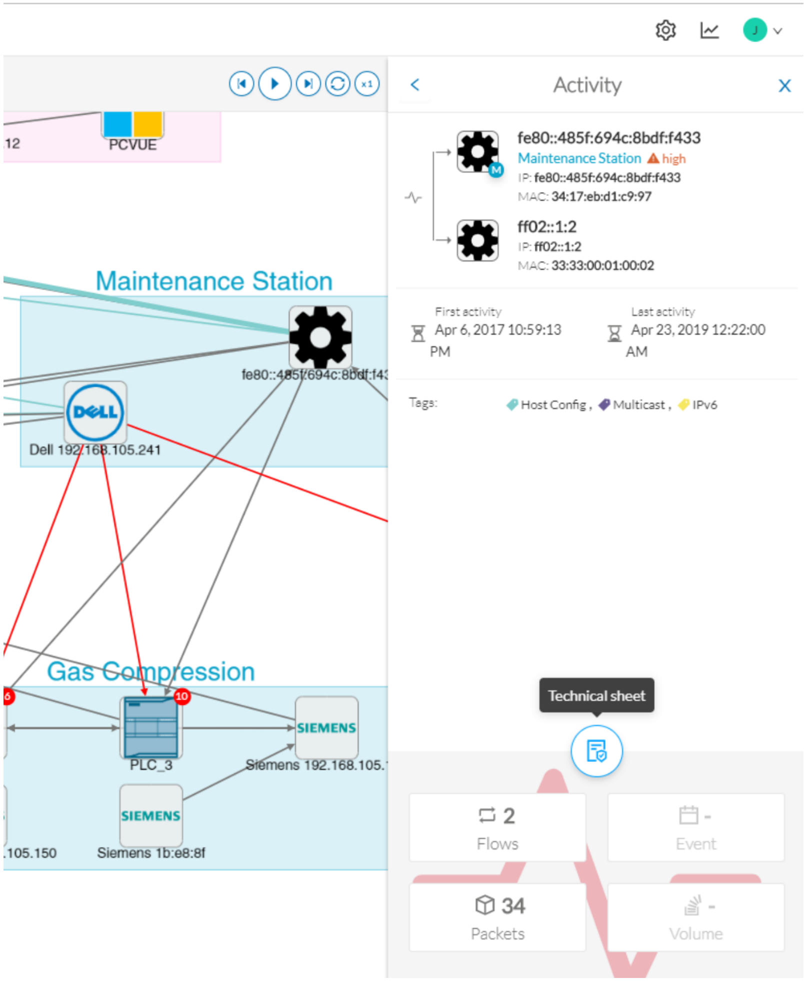
An activity is the representation of the communications exchanged between Device or Component. It is recognizable on the map by a line (or an arrow if the source and destination components are known) which links one component to another:



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

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

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



Activity

fe80::485f:694c:8bdf:f433
Maintenance Station high
IP: fe80::485f:694c:8bdf:f433
MAC: 34:17:eb:d1:c9:97

ff02::1:2
IP: ff02::1:2
MAC: 33:33:00:01:00:02

First activity
Apr 6, 2017 10:59:13 PM

Last activity
Apr 23, 2019 12:22:00 AM

Tags: Host Config , Multicast , IPv6

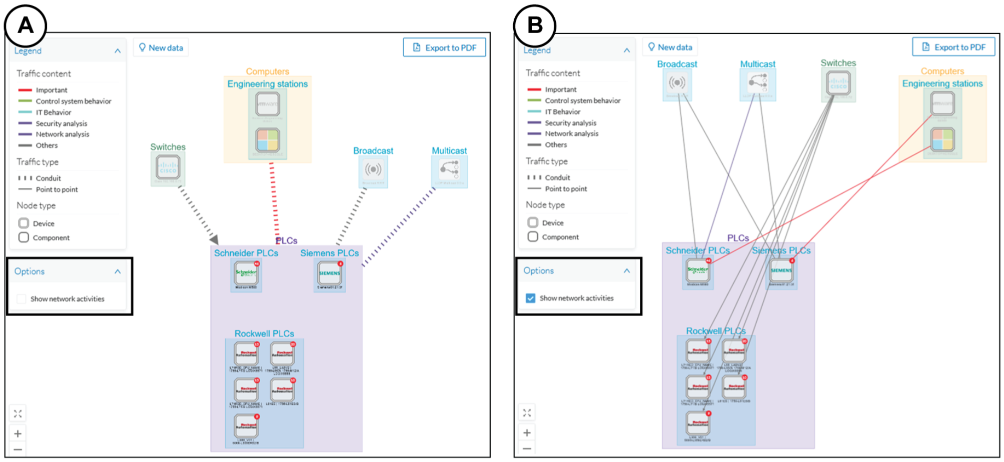
2 Flows
- Event
34 Packets
- Volume

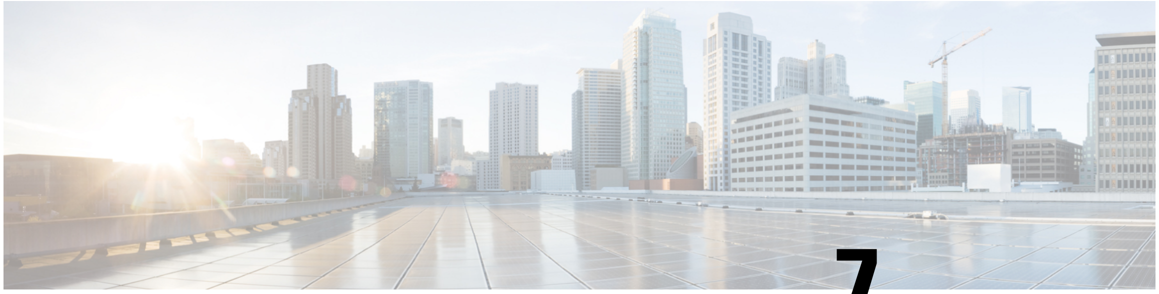
Devices or components with no activity does not mean that it did not have any interaction. In fact, a component can only be detected if at some point it has been involved in a network activity (communication emission/reception). Lack of activity can mean that the other linked component is not part of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

Aggregated activities or conduits:

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

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


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



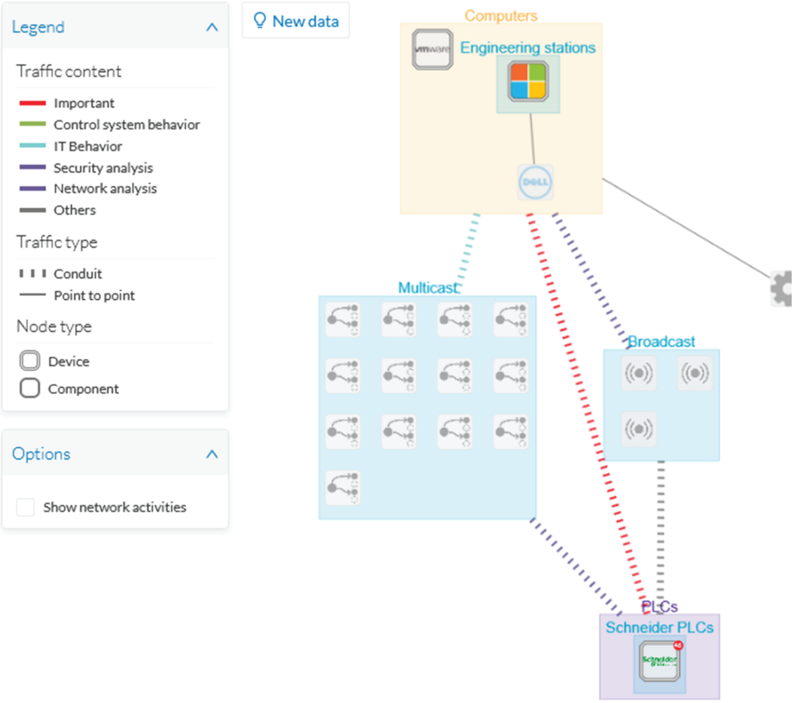
CHAPTER 7

Conduit

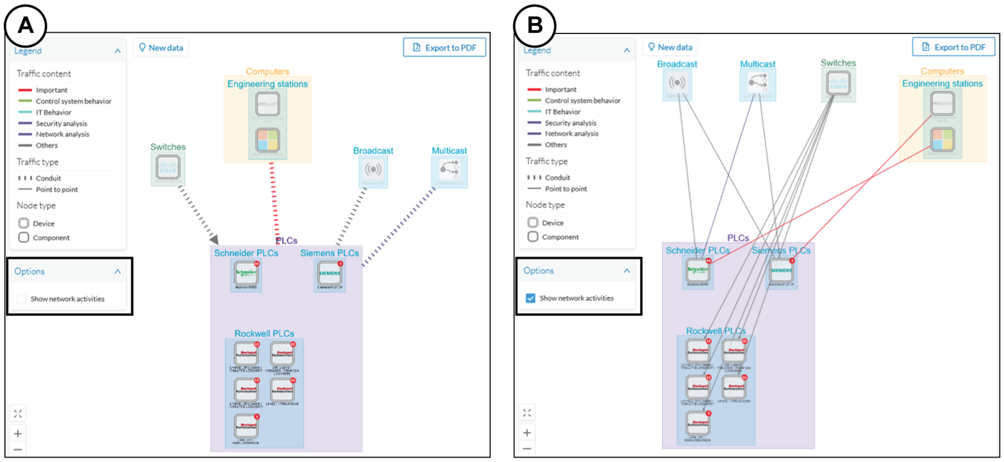
Conduit

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

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



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



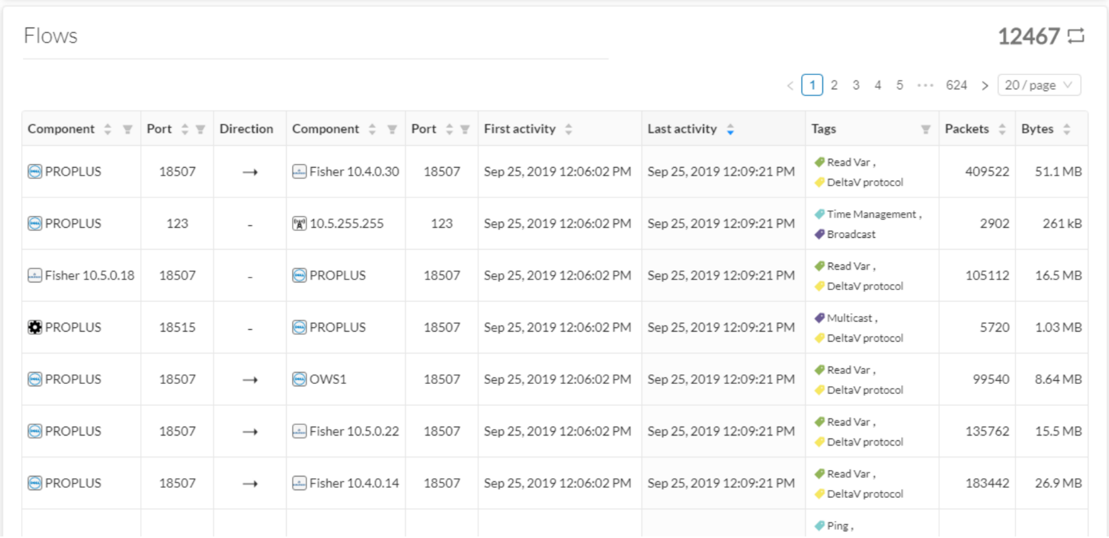
CHAPTER 8

Flow

Flow

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

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



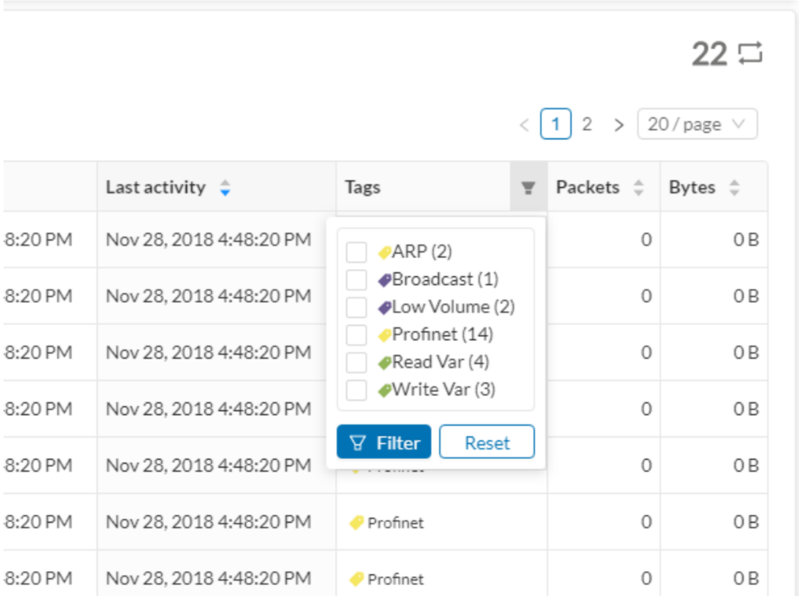
Flows

12467

< 1 2 3 4 5 ••• 624 > 20 / page

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

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



22

	Last activity	Tags	Packets	Bytes
8:20 PM	Nov 28, 2018 4:48:20 PM		0	0 B
8:20 PM	Nov 28, 2018 4:48:20 PM		0	0 B
8:20 PM	Nov 28, 2018 4:48:20 PM		0	0 B
8:20 PM	Nov 28, 2018 4:48:20 PM		0	0 B
8:20 PM	Nov 28, 2018 4:48:20 PM		0	0 B
8:20 PM	Nov 28, 2018 4:48:20 PM	Profinet	0	0 B
8:20 PM	Nov 28, 2018 4:48:20 PM	Profinet	0	0 B

- □ ARP (2)
- □ Broadcast (1)
- □ Low Volume (2)
- □ Profinet (14)
- □ Read Var (4)
- □ Write Var (3)

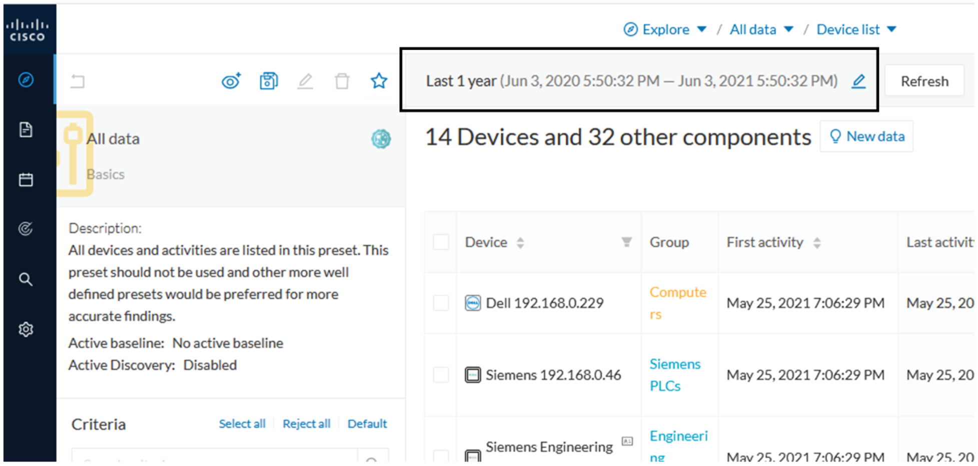
You can click on each flow in the list to have access to the flow's technical sheet for further information about the flow's properties and tags.

CHAPTER 9

Time span

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.



Last 1 year (Jun 3, 2020 5:50:32 PM — Jun 3, 2021 5:50:32 PM)

14 Devices and 32 other components

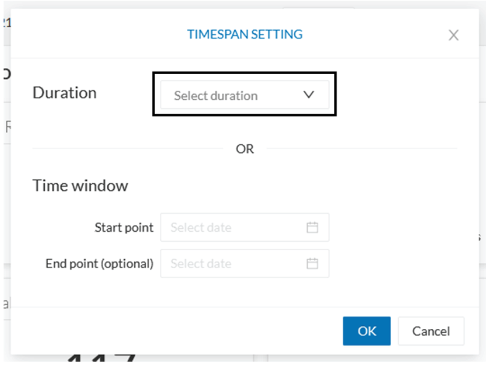
Description:
All devices and activities are listed in this preset. This preset should not be used and other more well defined presets would be preferred for more accurate findings.

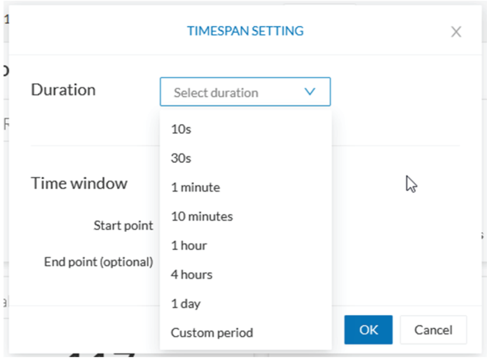
Active baseline: No active baseline
Active Discovery: Disabled

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

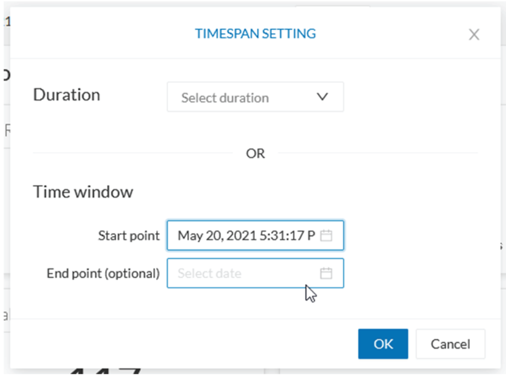
To set a time span, click the pencil button. A window pops up and gives you two options:

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





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

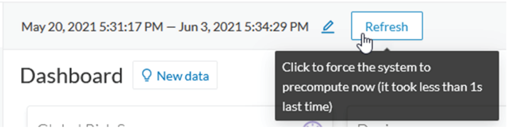


Start point May 20, 2021 5:31:17 P

End point (optional)

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.



May 20, 2021 5:31:17 PM — Jun 3, 2021 5:34:29 PM

Click to force the system to precompute now (it took less than 1s last time)

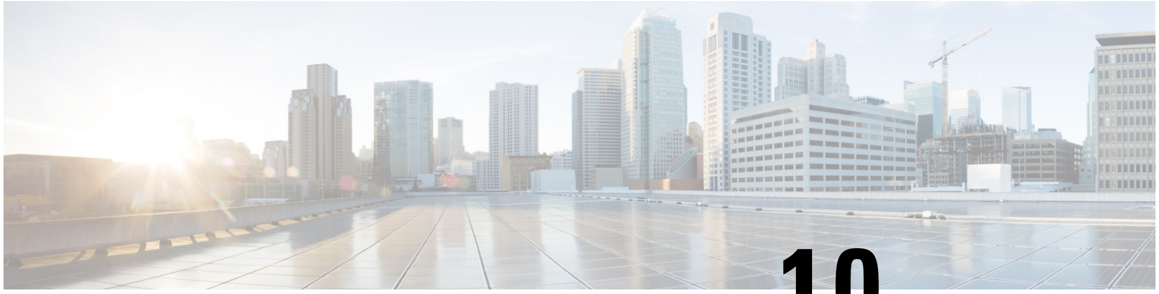
Note No data display is often due to a time span set on an empty period. Remember to first set a long period of time (such as 12mo) before considering a troubleshooting.

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.

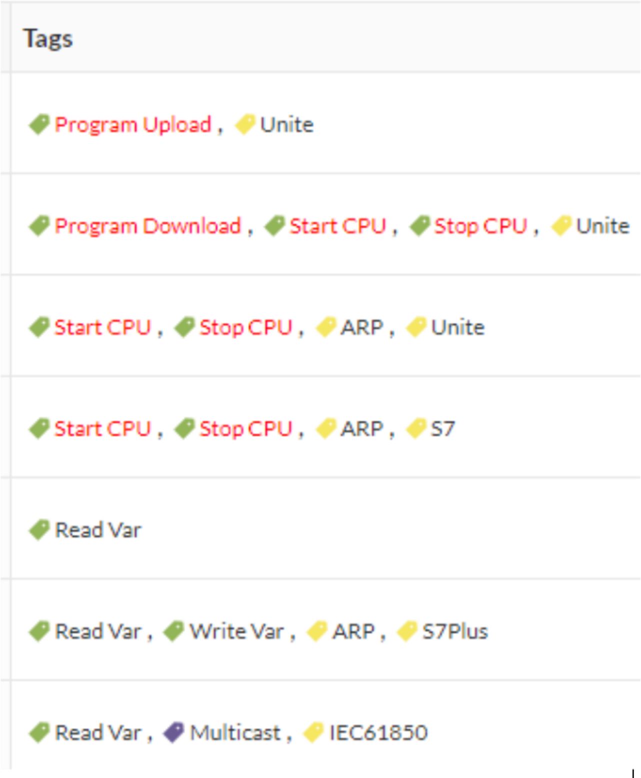


CHAPTER 10

Tag

Tags

What are tags?



Tags
Program Upload , Unite
Program Download , Start CPU , Stop CPU , Unite
Start CPU , Stop CPU , ARP , Unite
Start CPU , Stop CPU , ARP , S7
Read Var
Read Var , Write Var , ARP , S7Plus
Read Var , Multicast , IEC61850

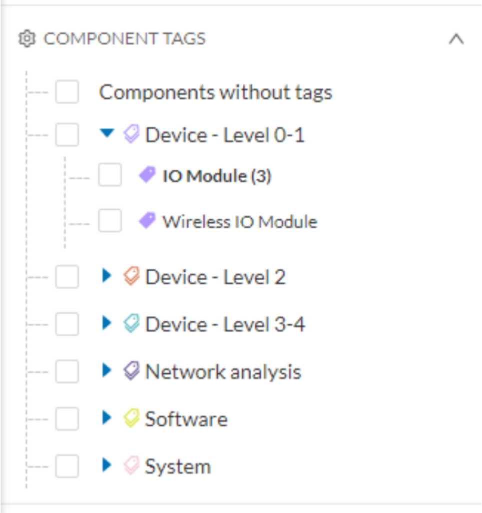
Tags are meaningful labels that succinctly describe a network. They can be applied to components or activities. Each tag has a description and an icon color which correspond to its category.

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:



COMPONENT TAGS

- □ Components without tags
- □ ▼ Device - Level 0-1
  - □ IO Module (3)
  - □ Wireless IO Module
- □ ▶ Device - Level 2
- □ ▶ Device - Level 3-4
- □ ▶ Network analysis
- □ ▶ Software
- □ ▶ System

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.

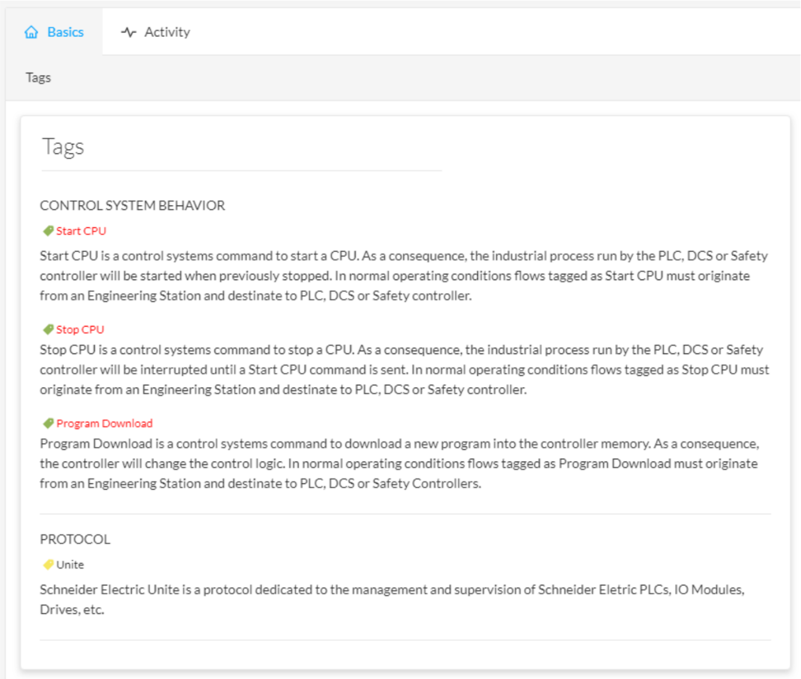
Also, tags are used to define behaviors (i.e. in the Monitor mode) inside an industrial network when combined with information like source and destination ports and flows properties.

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:



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.

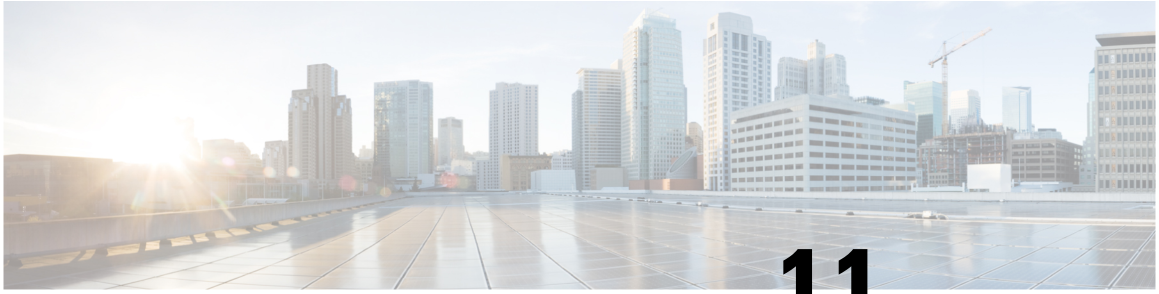
Program Download

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 11

Property

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.

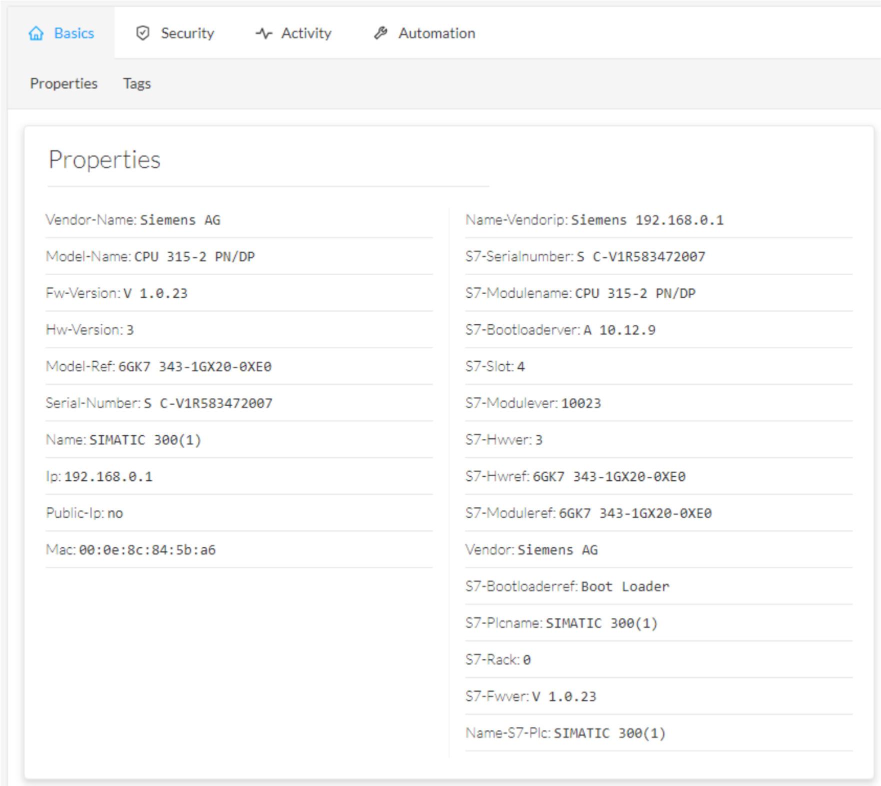
What are properties used for?

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

Vendor-Name: Siemens AG

Model-Name: CPU 315-2 PN/DP

Fw-Version: V 1.0.23

Hw-Version: 3

Model-Ref: 6GK7 343-1GX20-0XE0

Serial-Number: S C-V1R583472007

Name: SIMATIC 300(1)

Ip: 192.168.0.1

Public-Ip: no

Mac: 00:0e:8c:84:5b:a6

Name-Vendorip: Siemens 192.168.0.1

S7-Serialnumber: S C-V1R583472007

S7-Modulename: CPU 315-2 PN/DP

S7-Bootloaderver: A 10.12.9

S7-Slot: 4

S7-Modulever: 10023

S7-Hwver: 3

S7-Hwref: 6GK7 343-1GX20-0XE0

S7-Moduleref: 6GK7 343-1GX20-0XE0

Vendor: Siemens AG

S7-Bootloaderref: Boot Loader

S7-Plcname: SIMATIC 300(1)

S7-Rack: 0

S7-Fwver: V 1.0.23

Name-S7-Plc: SIMATIC 300(1)

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

CHAPTER 12

Risk score

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:

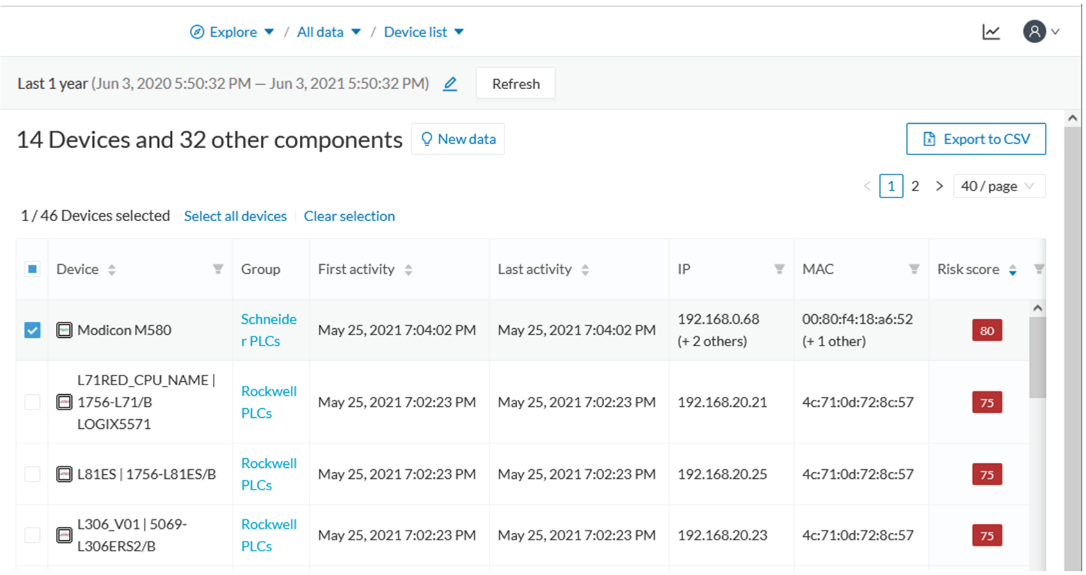
The likelihood answers the question: What is the likelihood of this device being compromised? It depends on:

- 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.



Explore / All data / Device list

Last 1 year (Jun 3, 2020 5:50:32 PM — Jun 3, 2021 5:50:32 PM) Refresh

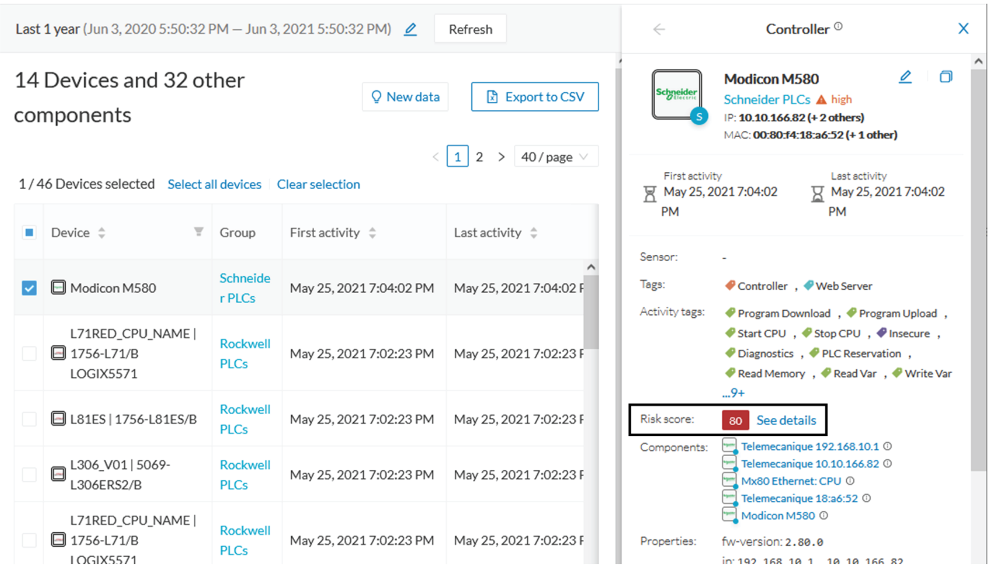
14 Devices and 32 other components New data Export to CSV

1 2 40 / page

1 / 46 Devices selected Select all devices Clear selection

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

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



Last 1 year (Jun 3, 2020 5:50:32 PM — Jun 3, 2021 5:50:32 PM) Refresh

14 Devices and 32 other components New data Export to CSV

1 2 40 / page

1 / 46 Devices selected Select all devices Clear selection

	Device	Group	First activity	Last activity
☑	Modicon M580	Schneider PLCs	May 25, 2021 7:04:02 PM	May 25, 2021 7:04:02 F
□	L71RED_CPU_NAME | 1756-L71/B LOGIX5571	Rockwell PLCs	May 25, 2021 7:02:23 PM	May 25, 2021 7:02:23 F
□	L81ES | 1756-L81ES/B	Rockwell PLCs	May 25, 2021 7:02:23 PM	May 25, 2021 7:02:23 F
□	L306_V01 | 5069-L306ERS2/B	Rockwell PLCs	May 25, 2021 7:02:23 PM	May 25, 2021 7:02:23 F
□	L71RED_CPU_NAME | 1756-L71/B LOGIX5571	Rockwell PLCs	May 25, 2021 7:02:23 PM	May 25, 2021 7:02:23 F

Controller

Modicon M580
Schneider PLCs high
IP: 10.10.166.82 (+ 2 others)
MAC: 00:80:f4:18:a6:52 (+ 1 other)

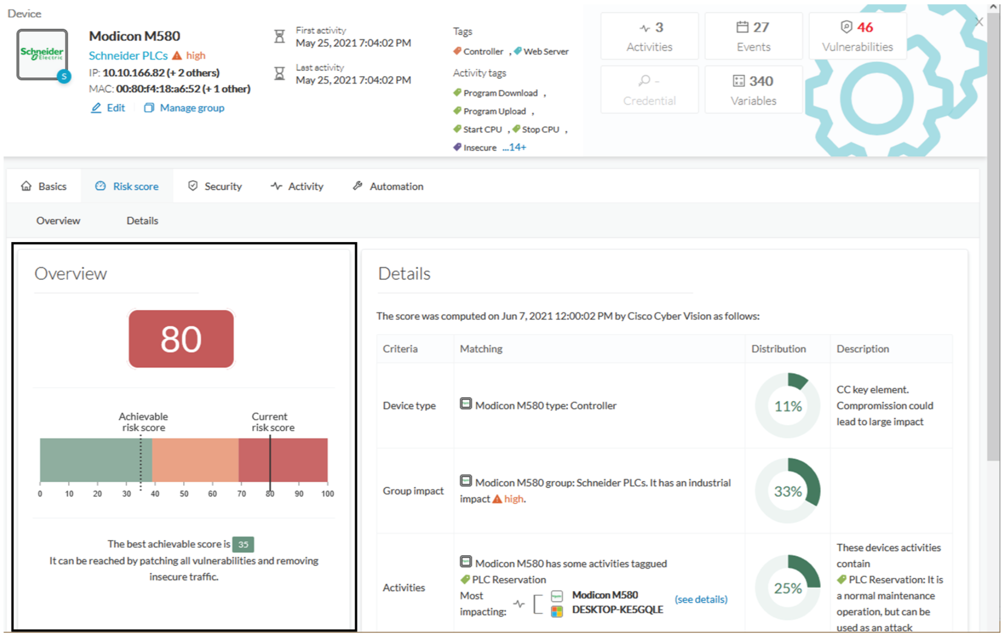
First activity May 25, 2021 7:04:02 PM
Last activity May 25, 2021 7:04:02 PM

Sensor: -
Tags: Controller , Web Server
Activity tags: Program Download , Program Upload , Start CPU , Stop CPU , Insecure , Diagnostics , PLC Reservation , Read Memory , Read Var , Write Var ...9+
Risk score: 80 See details
Components: Telemecanique 192.168.10.1, Telemecanique 10.10.166.82, Mx80 Ethernet: CPU, Telemecanique 18:a6:52, Modicon M580
Properties: fw-version: 2.80.0
ip: 192.168.10.1, 10.10.166.82

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.



Device

Modicon M580
Schneider PLCs ⚠ high
IP: 10.10.166.82 (+ 2 others)
MAC: 00:80:f4:18:a6:52 (+ 1 other)
Edit | Manage group

First activity
May 25, 2021 7:04:02 PM

Last activity
May 25, 2021 7:04:02 PM

Tags
Controller , Web Server

Activity tags
Program Download , Program Upload , Start CPU , Stop CPU , Insecure ...14+

3 Activities | 27 Events | 46 Vulnerabilities | - Credential | 340 Variables

Basics | Risk score | Security | Activity | Automation

Overview | Details

Overview

80

The best achievable score is 35
It can be reached by patching all vulnerabilities and removing insecure traffic.

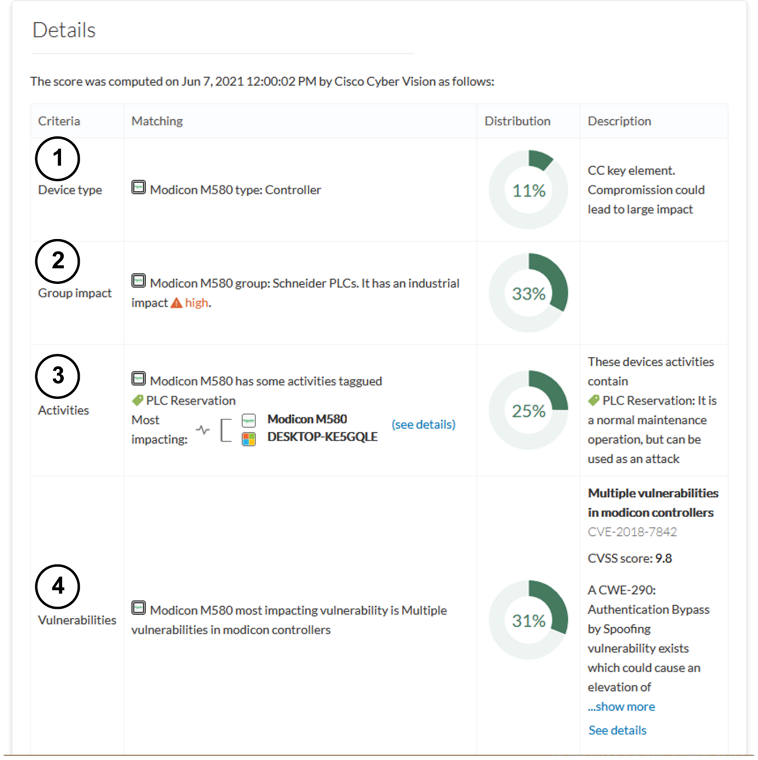
Details

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

Criteria	Matching	Distribution	Description
Device type	Modicon M580 type: Controller	11%	CC key element. Compromission could lead to large impact
Group impact	Modicon M580 group: Schneider PLCs. It has an industrial impact ⚠ high.	33%	
Activities	Modicon M580 has some activities taggued PLC Reservation Most impacting: Modicon M580 DESKTOP-KE5GQLE (see details)	25%	These devices activities contain PLC Reservation: It is a normal maintenance operation, but can be used as an attack

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.



Details

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

Criteria	Matching	Distribution	Description
1 Device type	Modicon M580 type: Controller	11%	CC key element. Compromission could lead to large impact
2 Group impact	Modicon M580 group: Schneider PLCs. It has an industrial impact ▲ high.	33%	
3 Activities	Modicon M580 has some activities taggued PLC Reservation Most impacting: Modicon M580 DESKTOP-KE5GQLE (see details)	25%	These devices activities contain PLC Reservation: It is a normal maintenance operation, but can be used as an attack
4 Vulnerabilities	Modicon M580 most impacting vulnerability is Multiple vulnerabilities in modicon controllers	31%	**Multiple vulnerabilities in modicon controllers** CVE-2018-7842 CVSS score: **9.8** A CWE-290: Authentication Bypass by Spoofing vulnerability exists which could cause an elevation of ...show more See details

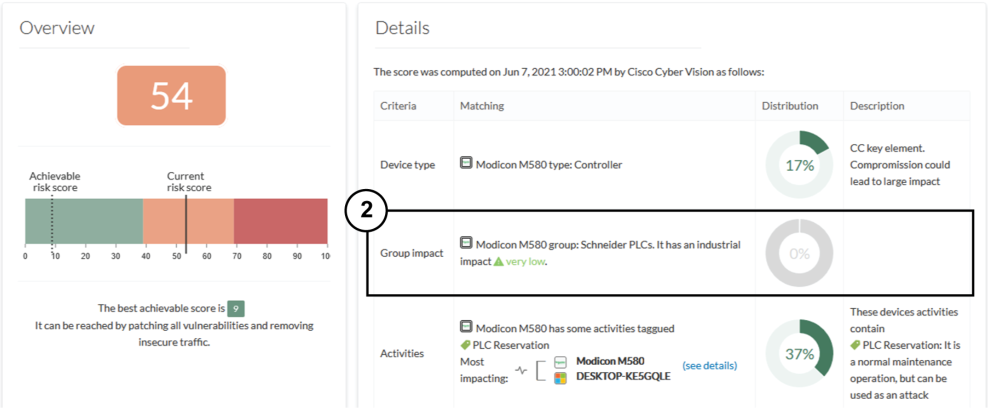
As first information, you have the last time the risk score was computed by Cisco Cyber Vision. Risk score computation occurs once an hour. However, you can force computation by using the following command on the Center shell prompt:

```
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:



Overview

54

The best achievable score is 9
It can be reached by patching all vulnerabilities and removing insecure traffic.

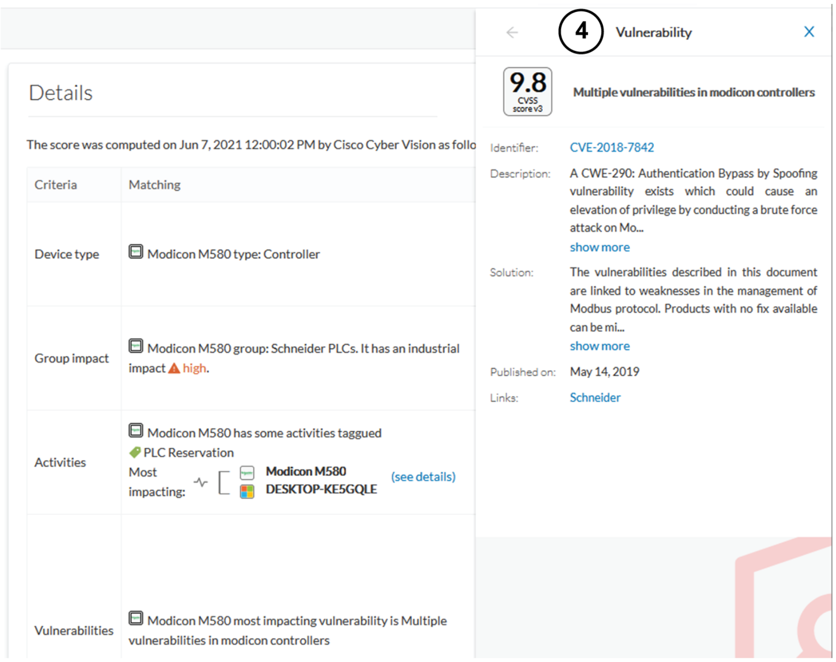
Details

The score was computed on Jun 7, 2021 3:00:02 PM by Cisco Cyber Vision as follows:

Criteria	Matching	Distribution	Description
Device type	Modicon M580 type: Controller	17%	CC key element. Compromission could lead to large impact
Group impact	Modicon M580 group: Schneider PLCs. It has an industrial impact ⚠ very low.	0%	
Activities	Modicon M580 has some activities taggued PLC Reservation Most impacting: Modicon M580 DESKTOP-KE5GQLE (see details)	37%	These devices activities contain PLC Reservation: It is a normal maintenance operation, but can be used as an attack

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.



Details

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

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

Vulnerability

9.8
CVSS score v3

Multiple vulnerabilities in modicon controllers

Identifier: CVE-2018-7842

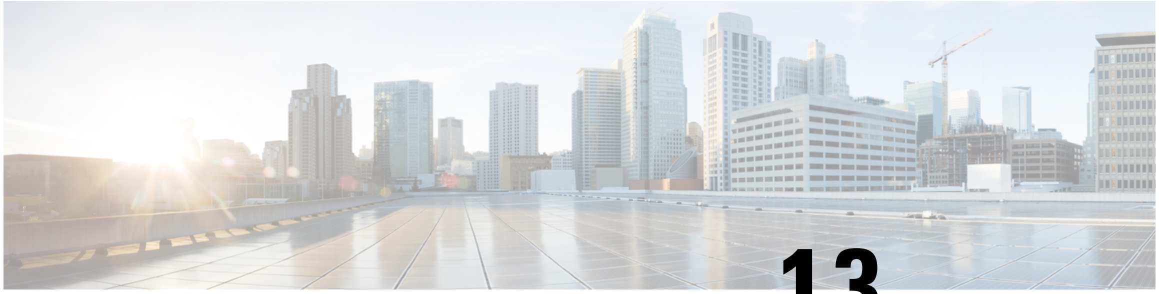
Description: A CWE-290: Authentication Bypass by Spoofing vulnerability exists which could cause an elevation of privilege by conducting a brute force attack on Mo...
show more

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

Published on: May 14, 2019

Links: Schneider

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



CHAPTER 13

Vulnerability

Vulnerability

What are vulnerabilities?

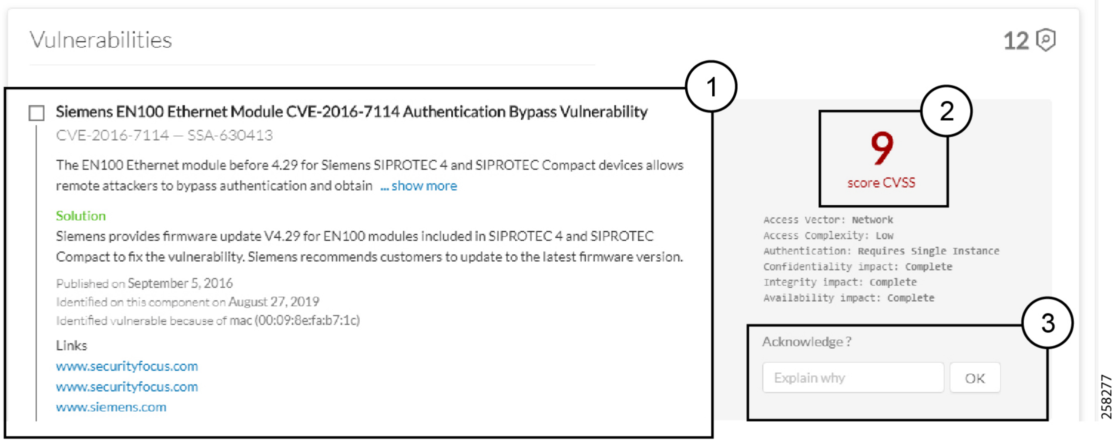
Vulnerabilities are weaknesses detected on devices that can be exploited by a potential attacker to perform malevolent actions on the network.

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:



□ Siemens EN100 Ethernet Module CVE-2016-7114 Authentication Bypass Vulnerability

CVE-2016-7114 — SSA-630413

The EN100 Ethernet module before 4.29 for Siemens SIPROTEC 4 and SIPROTEC Compact devices allows remote attackers to bypass authentication and obtain ... show more

Solution

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

Published on September 5, 2016
Identified on this component on August 27, 2019
Identified vulnerable because of mac (00:09:8e:fa:b7:1c)

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

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

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

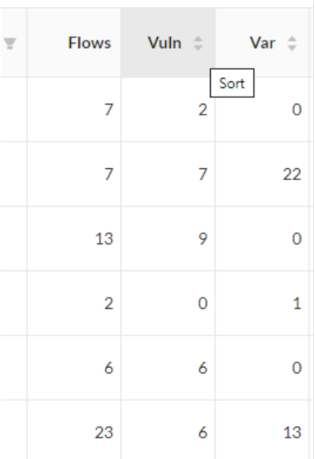
A score reports the severity of the vulnerability **(2)**. This score is calculated upon criteria from the Common Vulnerability Scoring System or CVSS. Criteria are for example the ease of attack, its impacts, the importance of the component on the network, and whether actions can be taken remotely or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

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

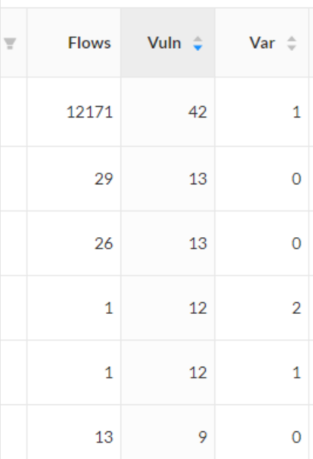
Where to find vulnerabilities?

Vulnerabilities are accessible through the Vulnerabilities of a preset.

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

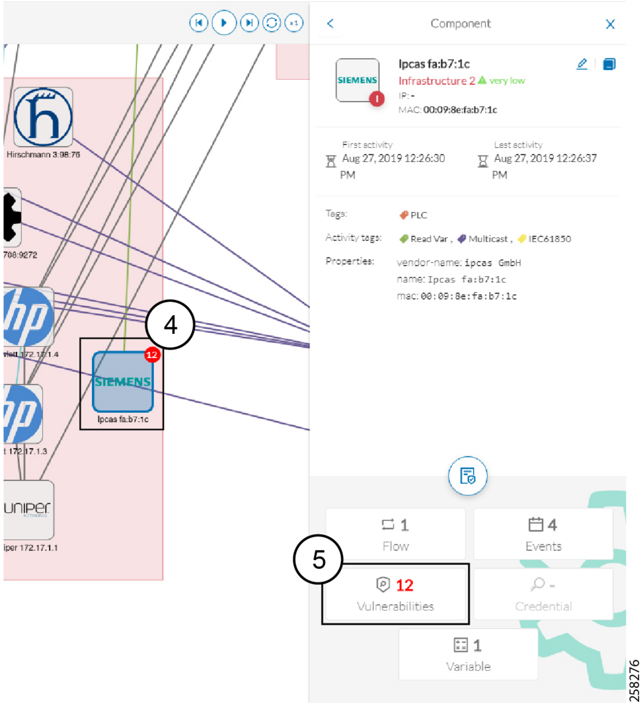


Flows	Vuln	Var
7	2	0
7	7	22
13	9	0
2	0	1
6	6	0
23	6	13



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

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



Component

Ipcas fa:b7:1c
Infrastructure 2 very low
IP: -
MAC: 00:09:8e:fa:b7:1c

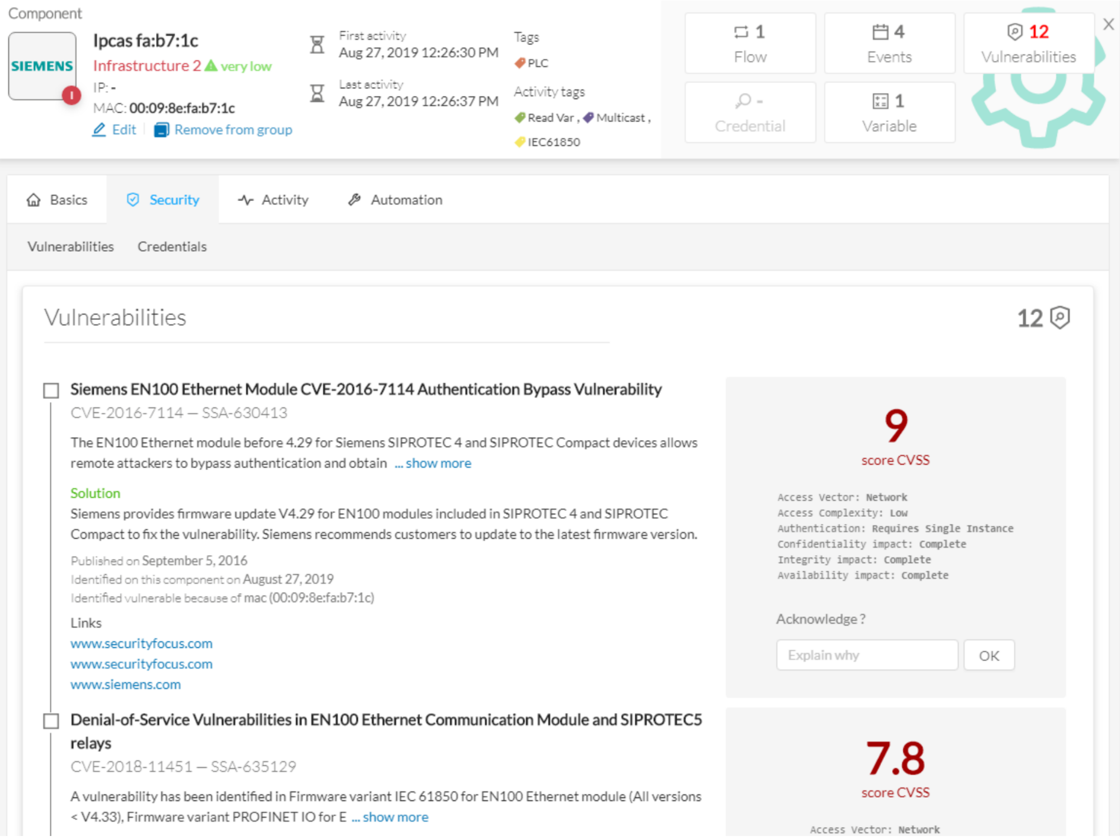
First activity
Aug 27, 2019 12:26:30 PM

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

Tags: PLC
Activity tags: Read Var , Multicast , IEC61850
Properties: vendor-name: `ipcas GmbH`
name: `Ipcas fa:b7:1c`
mac: `00:09:8e:fa:b7:1c`

1 Flow
4 Events
12 Vulnerabilities
- Credential
1 Variable

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:



Ipcas fa:b7:1c
Infrastructure 2 very low
IP: -
MAC: 00:09:8e:fa:b7:1c

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

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

Vulnerabilities 12

□ Siemens EN100 Ethernet Module CVE-2016-7114 Authentication Bypass Vulnerability

CVE-2016-7114 — SSA-630413

The EN100 Ethernet module before 4.29 for Siemens SIPROTEC 4 and SIPROTEC Compact devices allows remote attackers to bypass authentication and obtain ... show more

Solution

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

Published on September 5, 2016
Identified on this component on August 27, 2019
Identified vulnerable because of mac (00:09:8e:fa:b7:1c)

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

9
score CVSS

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

Acknowledge ?

□ Denial-of-Service Vulnerabilities in EN100 Ethernet Communication Module and SIPROTEC5 relays

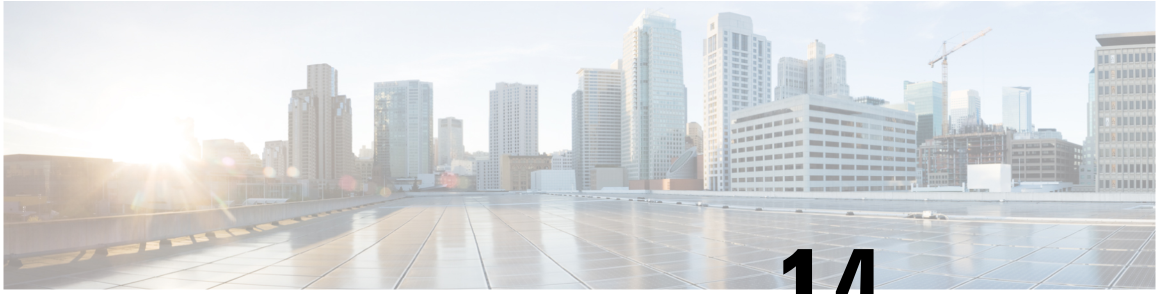
CVE-2018-11451 — SSA-635129

A vulnerability has been identified in Firmware variant IEC 61850 for EN100 Ethernet module (All versions < V4.33), Firmware variant PROFINET IO for E ... show more

7.8
score CVSS

```
Access Vector: Network
```

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



CHAPTER 14

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.

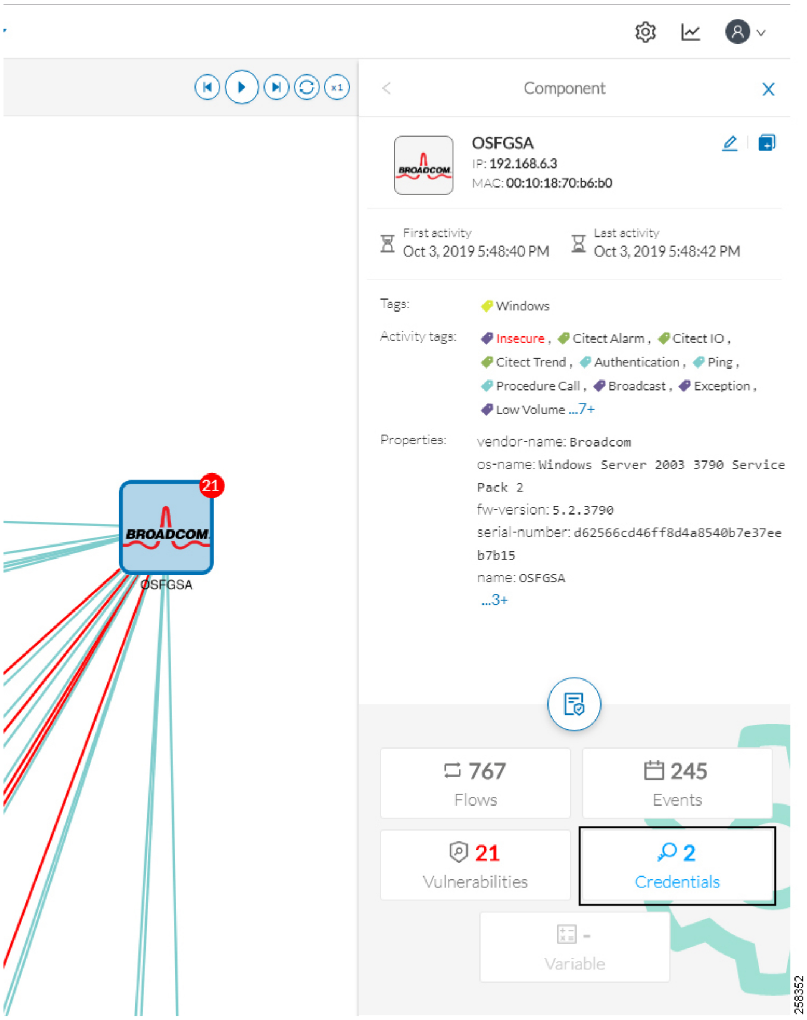
CHAPTER 15

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:



Component

OSFGSA
IP: 192.168.6.3
MAC: 00:10:18:70:b6:b0

First activity Oct 3, 2019 5:48:40 PM
Last activity Oct 3, 2019 5:48:42 PM

Tags: Windows

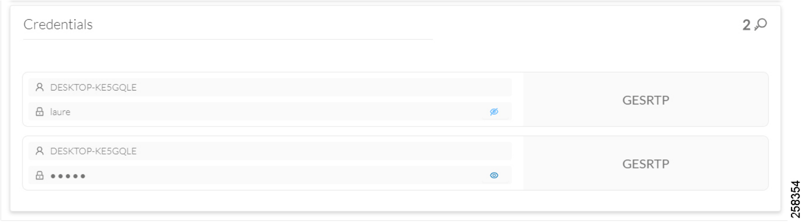
Activity tags: Insecure , Citect Alarm , Citect IO , Citect Trend , Authentication , Ping , Procedure Call , Broadcast , Exception , Low Volume ...7+

Properties: vendor-name: Broadcom
os-name: Windows Server 2003 3790 Service Pack 2
fw-version: 5.2.3790
serial-number: d62566cd46ff8d4a8540b7e37eeb7b15
name: OSFGSA
...3+

767 Flows
245 Events
21 Vulnerabilities
2 Credentials
- Variable

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.

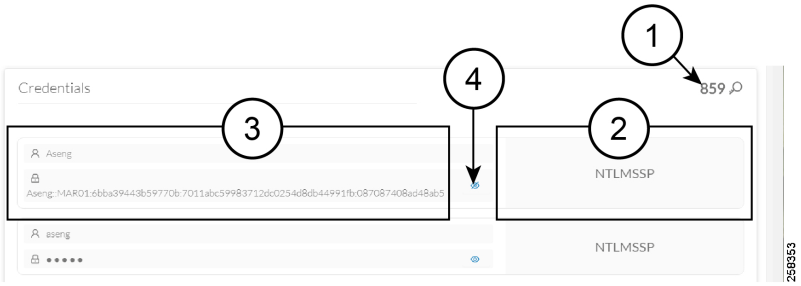
An unsafe password:



Credentials 2

DESKTOP-KE5GQLE laure	GESRTP
DESKTOP-KE5GQLE •••••	GESRTP

A hashed password:



Aseng

Aseng::MAR01:6bba39443b59770b:7011abc59983712dc0254d8db44991fb:087087408ad48ab5

aseng

●●●●●

CHAPTER 16

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.

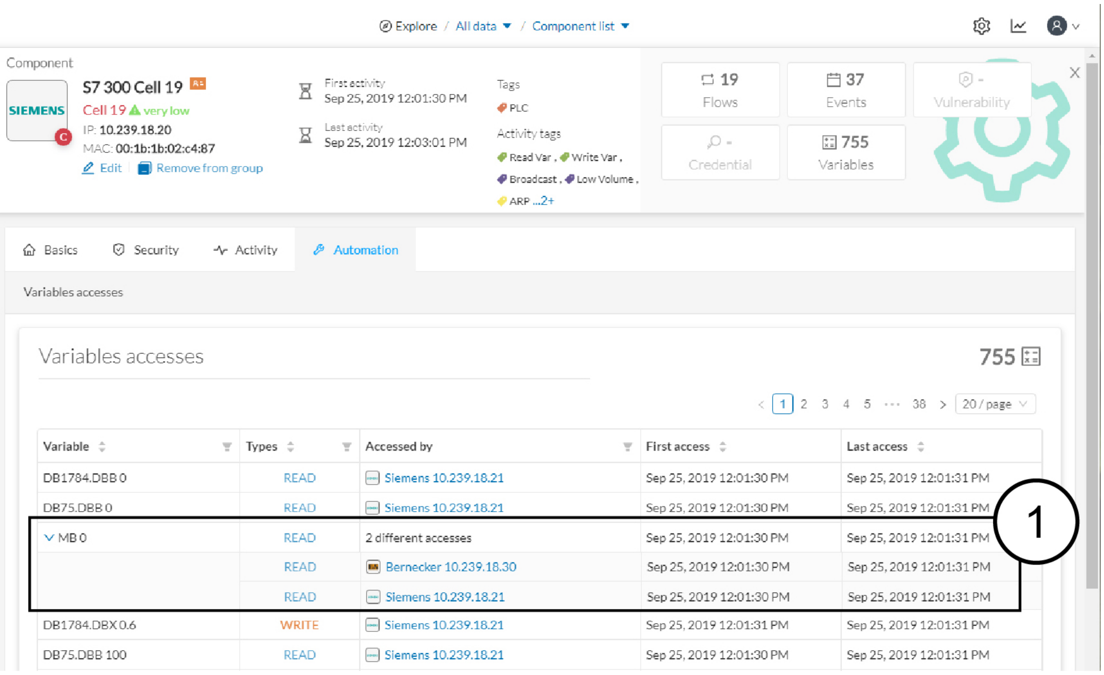
A variable can be for example the ongoing temperature on an industrial oven. This value is stored in the oven's PLC and can be controlled by another PLC or accessed by a SCADA system for supervisory purpose. The same value can be read by another PLC which controls the heating system.

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.



Component

S7 300 Cell 19

Cell 19 very low

IP: 10.239.18.20

MAC: 00:1b:1b:02:c4:87

Edit | Remove from group

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

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

Tags: PLC

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

19 Flows | 37 Events | - Vulnerability | - Credential | 755 Variables

Variables accesses

Variables accesses 755

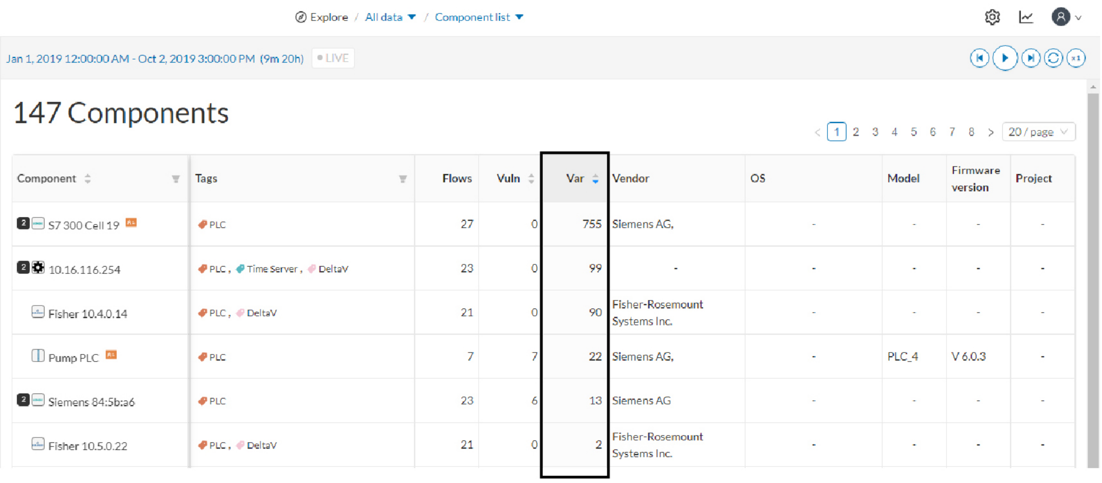
< 1 2 3 4 5 ··· 38 > 20 / page

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

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

Where to find variable accesses?

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



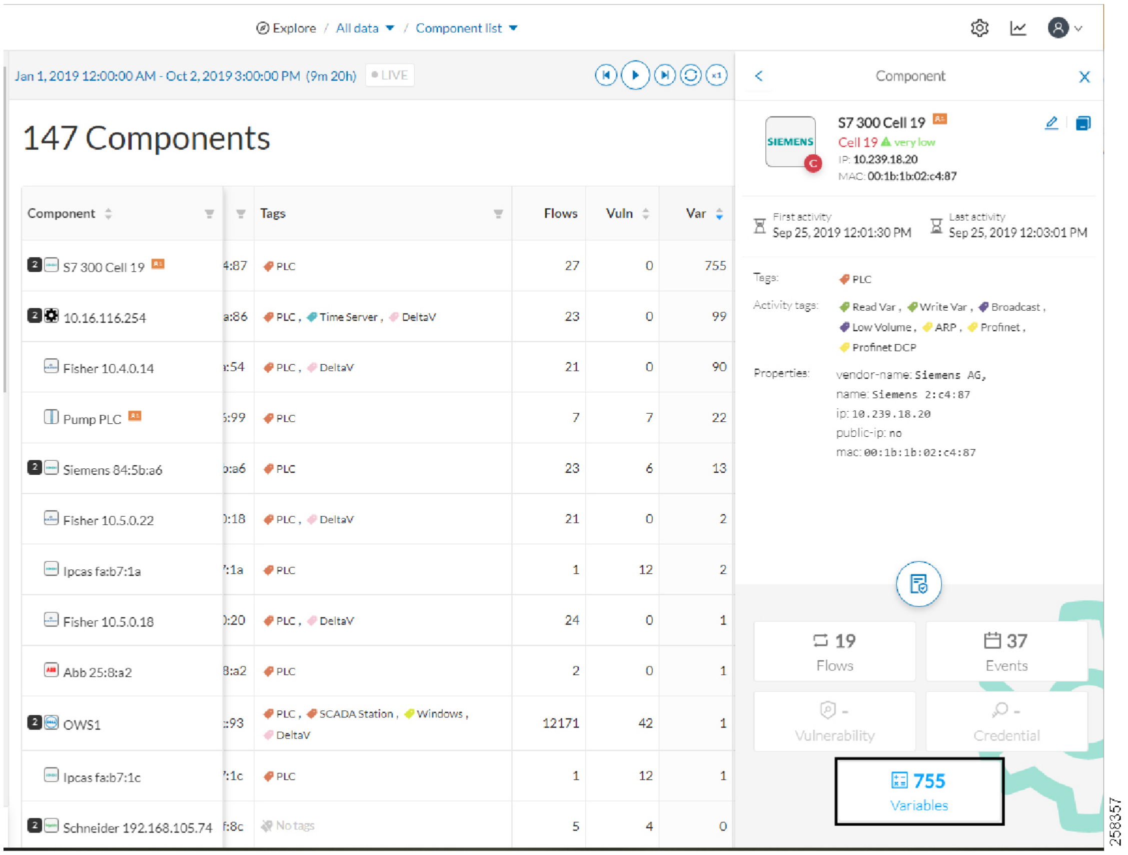
Jan 1, 2019 12:00:00 AM - Oct 2, 2019 3:00:00 PM (9m 20h)

147 Components

< 1 2 3 4 5 6 7 8 > 20 / page

Component	Tags	Flows	Vuln	Var	Vendor	OS	Model	Firmware version	Project
2 S7 300 Cell 19	PLC	27	0	755	Siemens AG,	-	-	-	-
2 10.16.116.254	PLC , Time Server , DeltaV	23	0	99	-	-	-	-	-
Fisher 10.4.0.14	PLC , DeltaV	21	0	90	Fisher-Rosemount Systems Inc.	-	-	-	-
Pump PLC	PLC	7	7	22	Siemens AG,	-	PLC_4	V 6.0.3	-
2 Siemens 84:5b:a6	PLC	23	6	13	Siemens AG	-	-	-	-
Fisher 10.5.0.22	PLC , DeltaV	21	0	2	Fisher-Rosemount Systems Inc.	-	-	-	-

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



Explore / All data / Component list
Jan 1, 2019 12:00:00 AM - Oct 2, 2019 3:00:00 PM (9m 20h)
LIVE
x1
258357

147 Components

Component		Tags	Flows	Vuln	Var
2 S7 300 Cell 19	4:87	PLC	27	0	755
2 10.16.116.254	a:86	PLC , Time Server , DeltaV	23	0	99
Fisher 10.4.0.14	:54	PLC , DeltaV	21	0	90
Pump PLC	5:99	PLC	7	7	22
2 Siemens 84:5b:a6	b:a6	PLC	23	6	13
Fisher 10.5.0.22	):18	PLC , DeltaV	21	0	2
Ipcas fa:b7:1a	':1a	PLC	1	12	2
Fisher 10.5.0.18	):20	PLC , DeltaV	24	0	1
Abb 25:8:a2	8:a2	PLC	2	0	1
2 OWS1	:93	PLC , SCADA Station , Windows , DeltaV	12171	42	1
Ipcas fa:b7:1c	':1c	PLC	1	12	1
2 Schneider 192.168.105.74	f:8c	No tags	5	4	0

Component

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

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

Tags: PLC

Activity tags: Read Var , Write Var , Broadcast , Low Volume , ARP , Profinet , Profinet DCP

Properties:
vendor-name: Siemens AG,
name: Siemens 2:c4:87
ip: 10.239.18.20
public-ip: no
mac: 00:1b:1b:02:c4:87

19 Flows

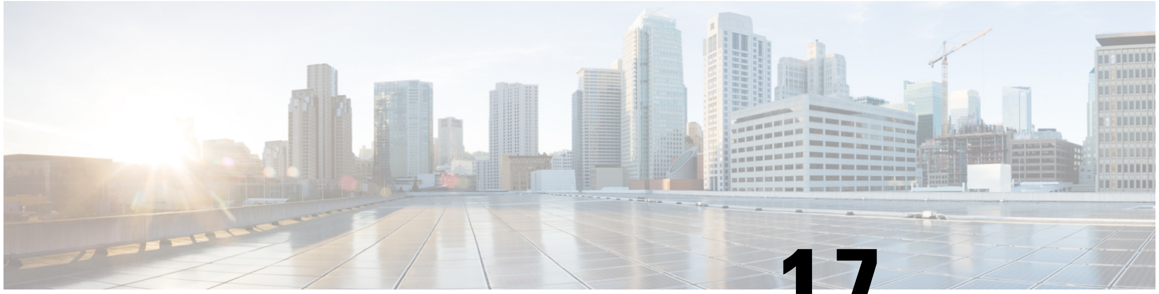
37 Events

- Vulnerability

- Credential

755 Variables

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

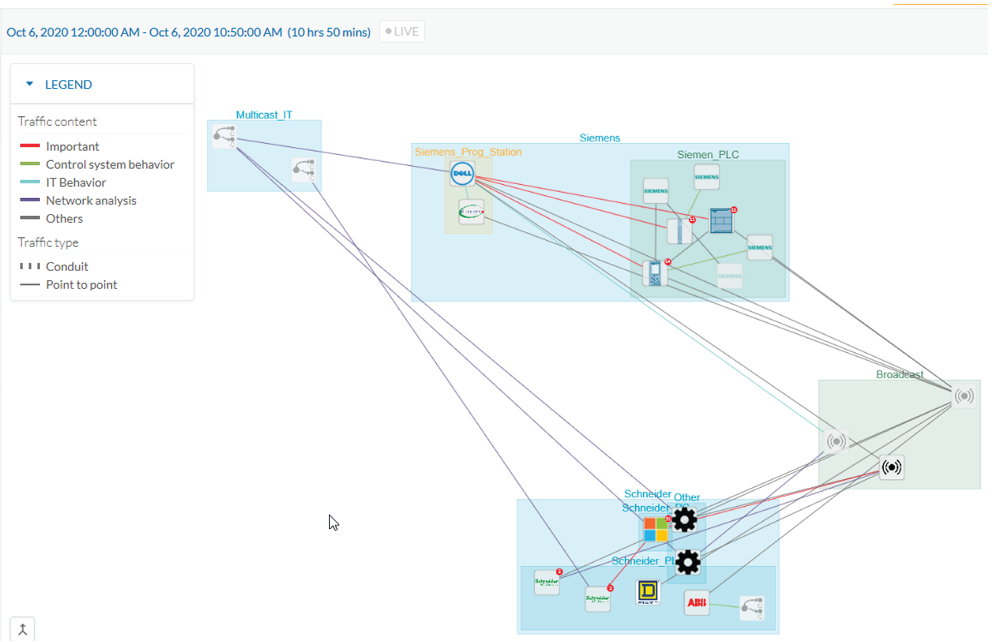


CHAPTER 17

Group

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.

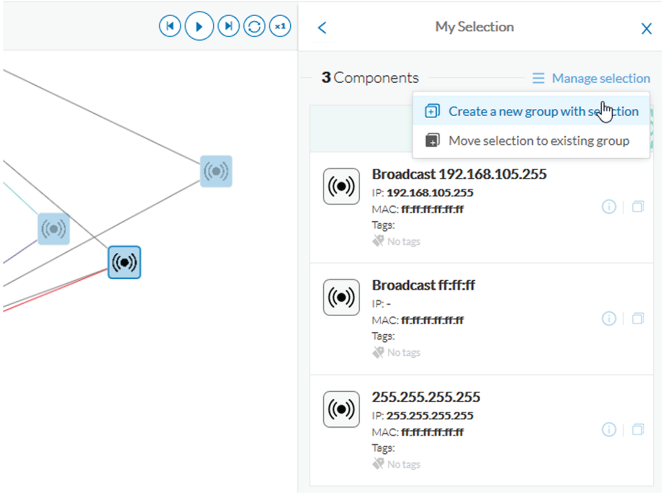
To create a group:

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.


My Selection
Manage selection
Create a new group with selection
Move selection to existing group

3 Components

Broadcast 192.168.105.255
IP: 192.168.105.255
MAC: ff:ff:ff:ff:ff:ff
Tags:
No tags

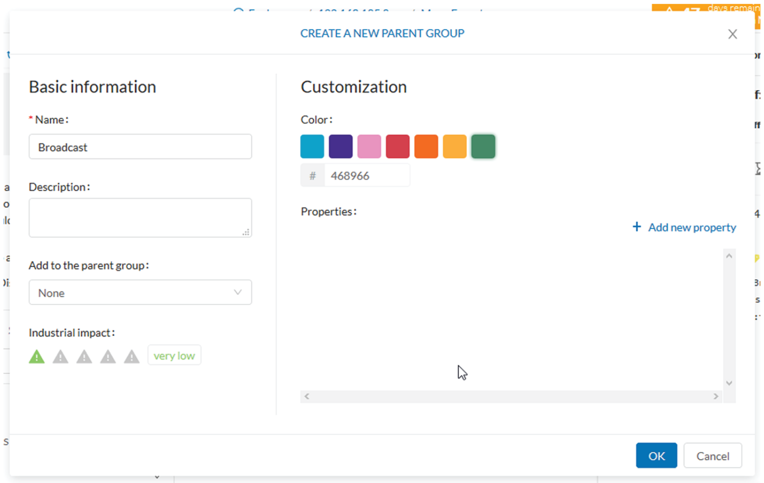
Broadcast ff:ff:ff
IP: -
MAC: ff:ff:ff:ff:ff:ff
Tags:
No tags

255.255.255.255
IP: 255.255.255.255
MAC: ff:ff:ff:ff:ff:ff
Tags:
No tags

Step 2 Click Manage selection.

Step 3 Click Create a new parent group.

A Create a new parent group window pops up:



Basic information

* Name: Broadcast

Description:

Add to the parent group: None

Industrial impact: very low

Customization

Color:

# 468966

Properties:

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:

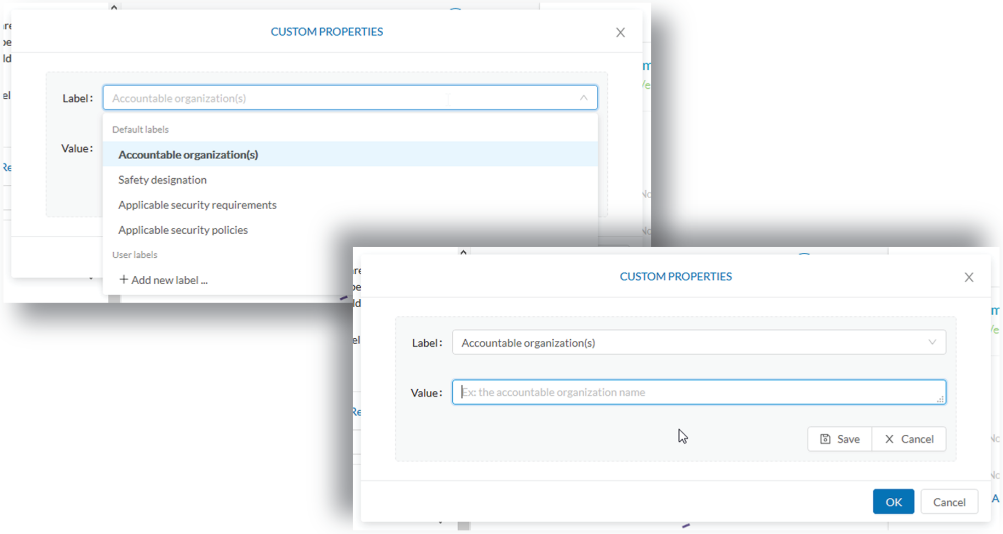
There are several ways to create a hierarchy among groups:

- 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.



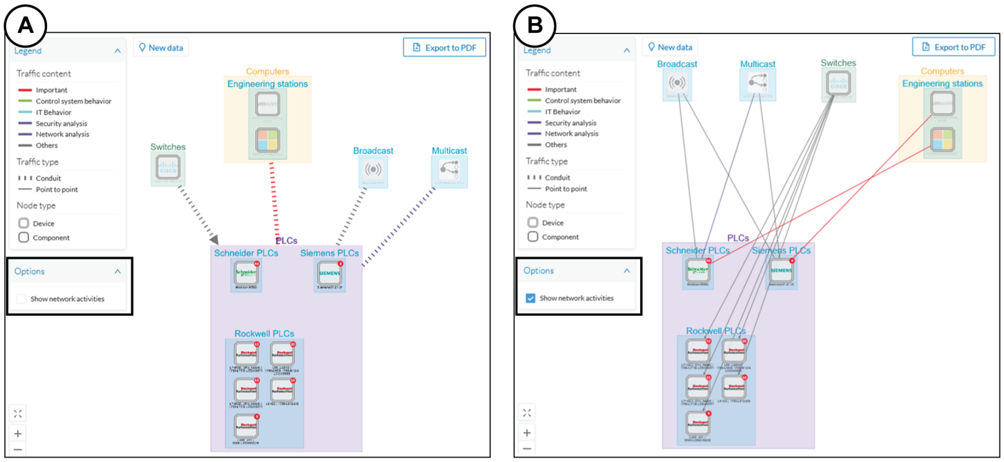
Label: Accountable organization(s)

Value: Ex: the accountable organization name

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.

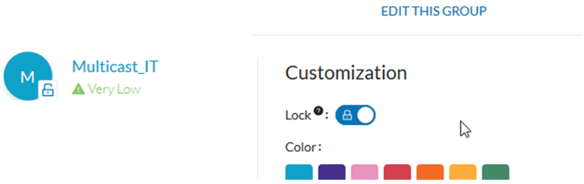
To switch on/off the Lock toggle button,

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.



EDIT THIS GROUP

M Multicast_IT
Very Low

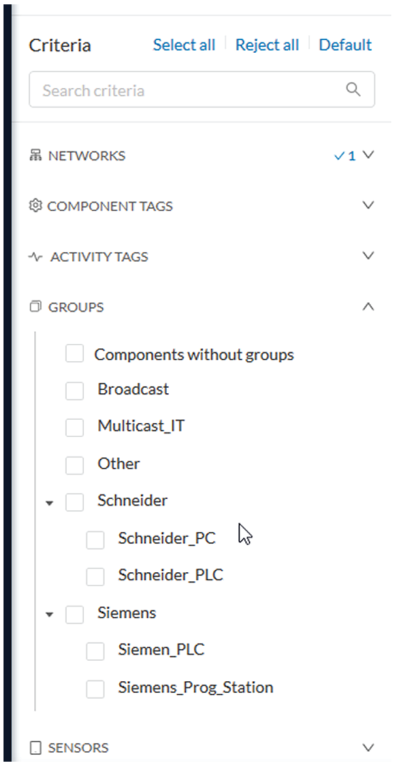
Customization

Lock: 🔒 ●

Color:

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.



Criteria Select all Reject all Default

Search criteria

NETWORKS ✓1

COMPONENT TAGS

ACTIVITY TAGS

GROUPS

- □ Components without groups
- □ Broadcast
- □ Multicast_IT
- □ Other
- □ Schneider
  - □ Schneider_PC
  - □ Schneider_PLC
- □ Siemens
  - □ Siemen_PLC
  - □ Siemens_Prog_Station

SENSORS

CHAPTER 18

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

CHAPTER 19

Home

- Home, on page 67

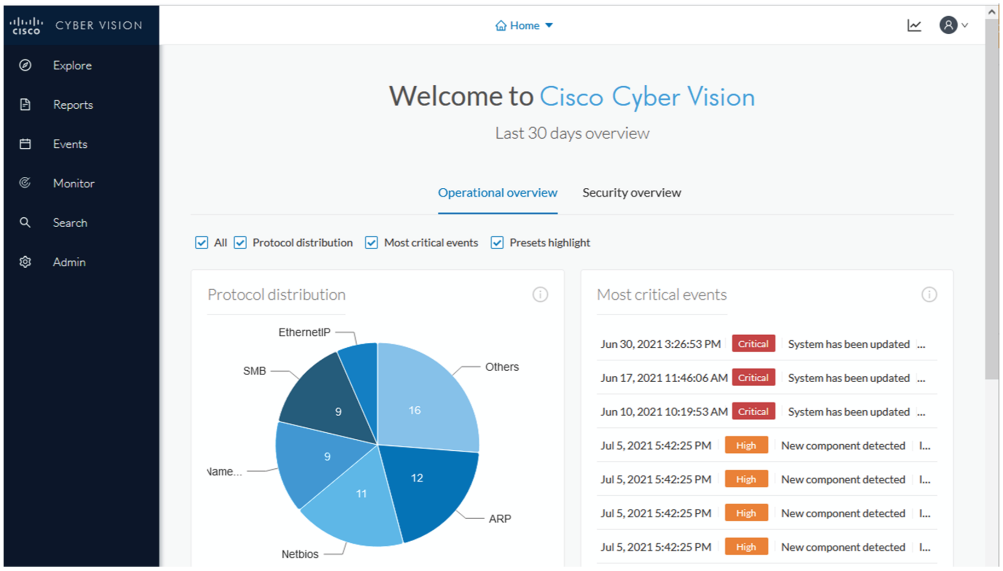
Home

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.

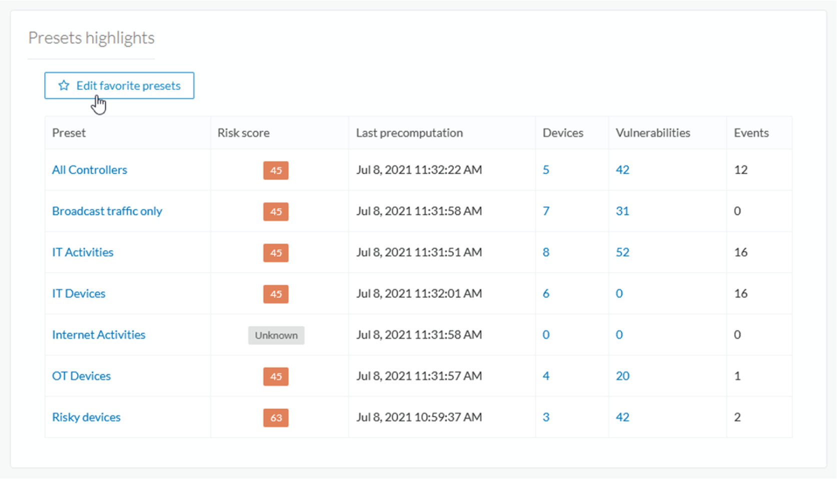
In the operational overview, you will find a pie chart with the protocol distribution and a list of the most critical events.



☑ All ☑ Protocol distribution ☑ Most critical events ☑ Presets highlight

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

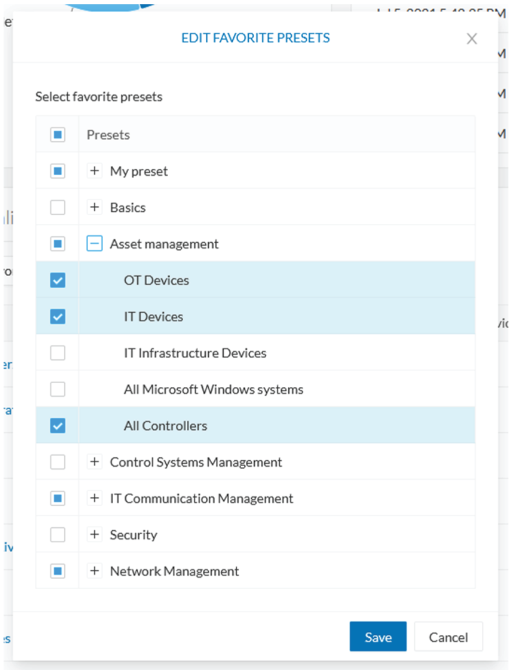
Below, a preset highlight you can edit to display your favorite presets.



Presets highlights

☆ Edit favorite presets

Preset	Risk score	Last precomputation	Devices	Vulnerabilities	Events
All Controllers	45	Jul 8, 2021 11:32:22 AM	5	42	12
Broadcast traffic only	45	Jul 8, 2021 11:31:58 AM	7	31	0
IT Activities	45	Jul 8, 2021 11:31:51 AM	8	52	16
IT Devices	45	Jul 8, 2021 11:32:01 AM	6	0	16
Internet Activities	Unknown	Jul 8, 2021 11:31:58 AM	0	0	0
OT Devices	45	Jul 8, 2021 11:31:57 AM	4	20	1
Risky devices	63	Jul 8, 2021 10:59:37 AM	3	42	2



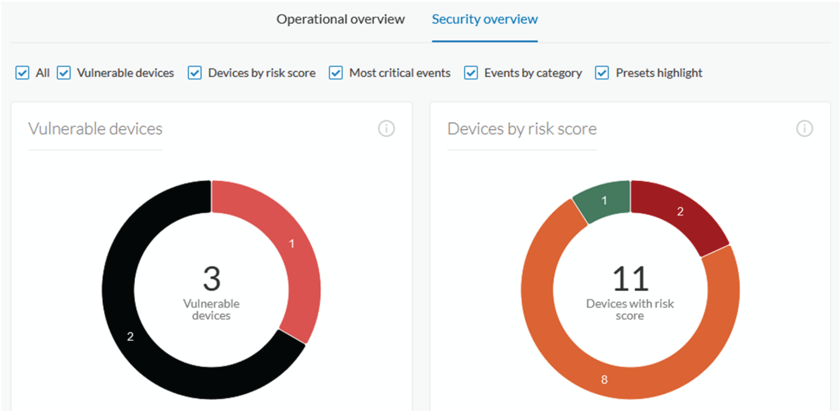
EDIT FAVORITE PRESETS ×

Select favorite presets

- ▣ Presets
- ▣ + My preset
- □ + Basics
- ▣ − Asset management
  - ☑ OT Devices
  - ☑ IT Devices
  - □ IT Infrastructure Devices
  - □ All Microsoft Windows systems
  - ☑ All Controllers
- □ + Control Systems Management
- ▣ + IT Communication Management
- □ + Security
- ▣ + Network Management

Save Cancel

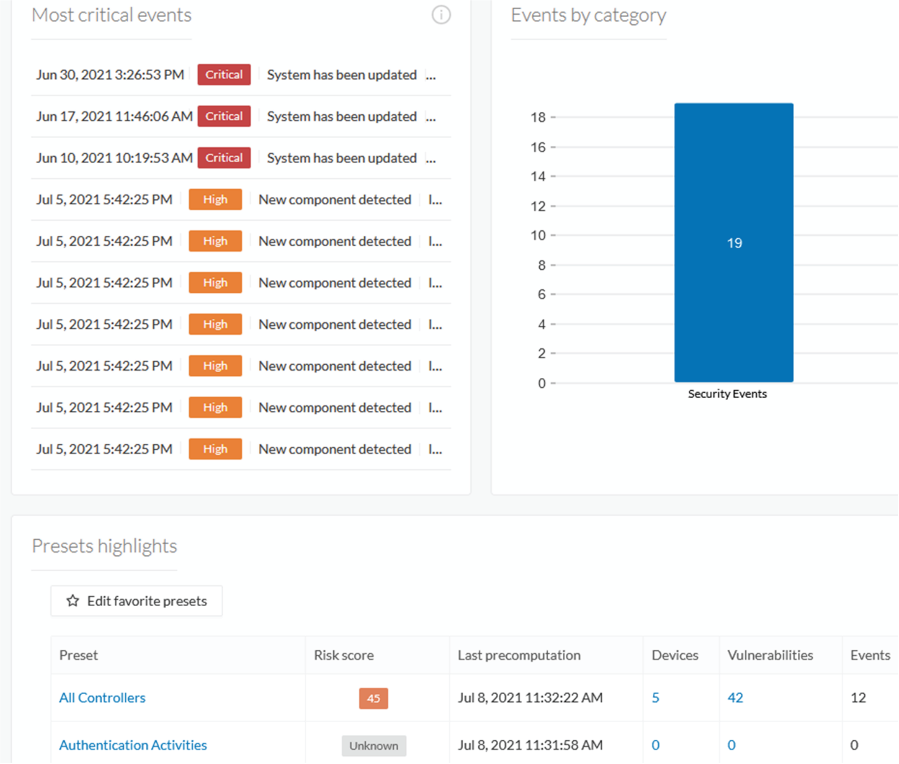
In the security overview, you will find a pie chart representing the vulnerable devices per severities, and a pie chart representing the devices per risk score.



Operational overview | Security overview

☑ All ☑ Vulnerable devices ☑ Devices by risk score ☑ Most critical events ☑ Events by category ☑ Presets highlight

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



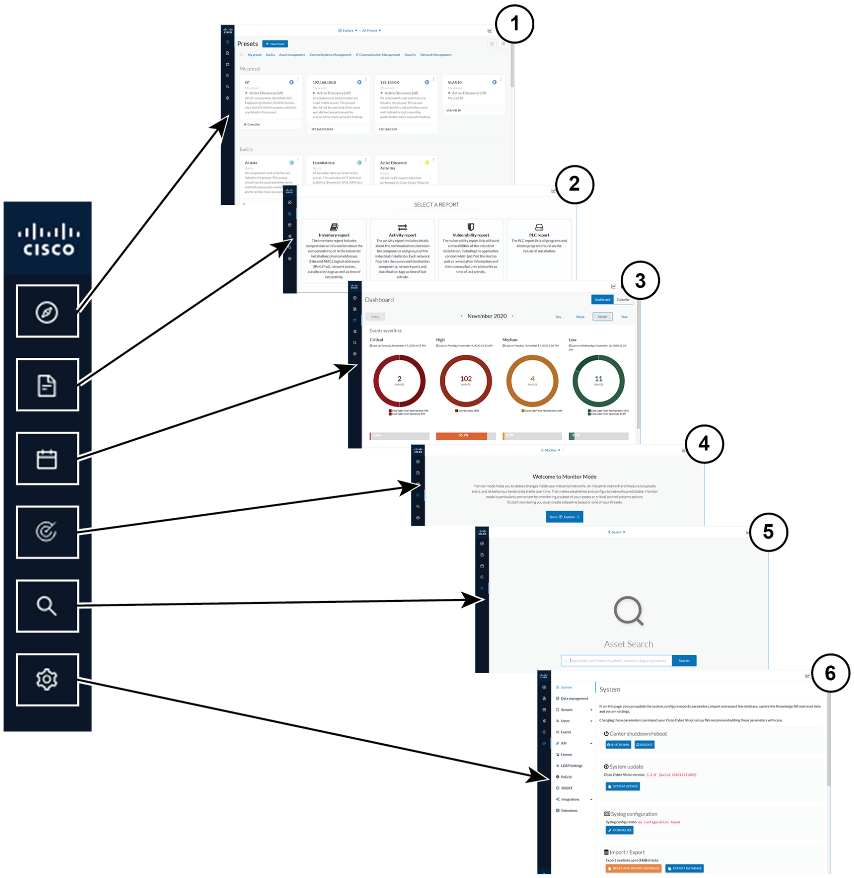
Most critical events

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

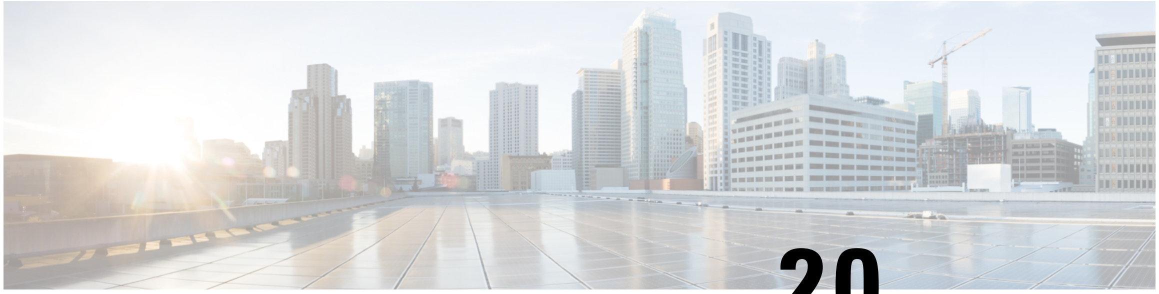
Presets highlights

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

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



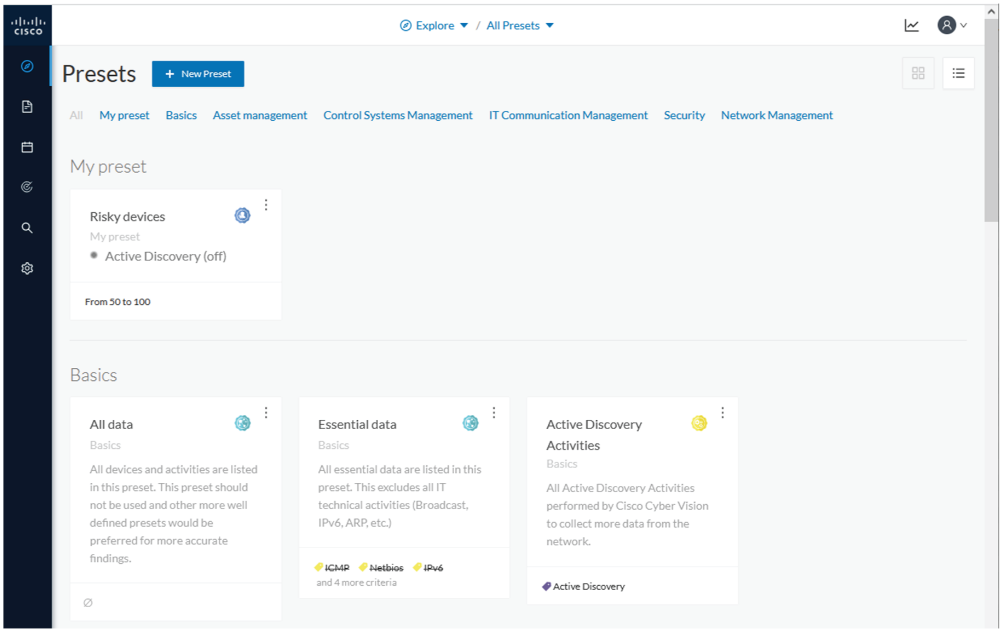
- Explore **(1)**: This button leads to the overview of Explore by defaults or configured.
- Reports **(2)**: This button leads to the Reports to export valuable information about the industrial network.
- Events **(3)**: This button leads to the Events which contains graphics and a calendar of all events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



CHAPTER 20

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.



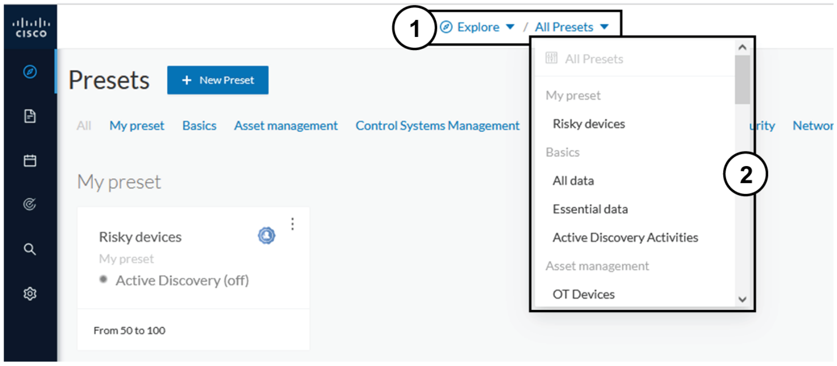
Risky devices
My preset
Active Discovery (off)
From 50 to 100

All data
Basics
All devices and activities are listed in this preset. This preset should not be used and other more well defined presets would be preferred for more accurate findings.

Essential data
Basics
All essential data are listed in this preset. This excludes all IT technical activities (Broadcast, IPv6, ARP, etc.)
and 4 more criteria

Active Discovery Activities
Basics
All Active Discovery Activities performed by Cisco Cyber Vision to collect more data from the network.

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



- Preset views, on page 72
- Right side panel, on page 82

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.

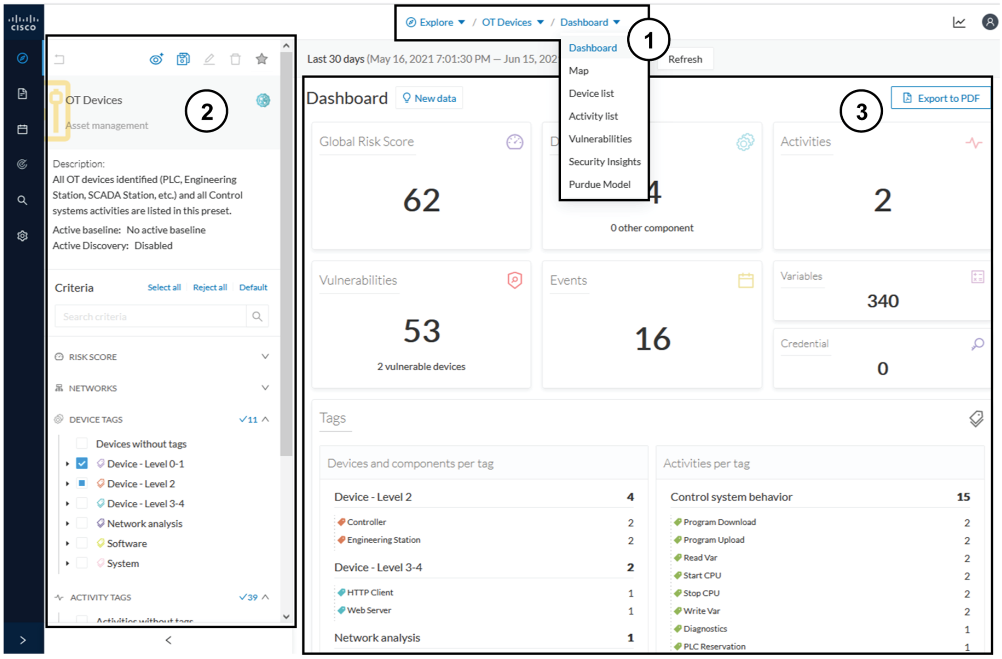
- The Purdue Model:

  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.

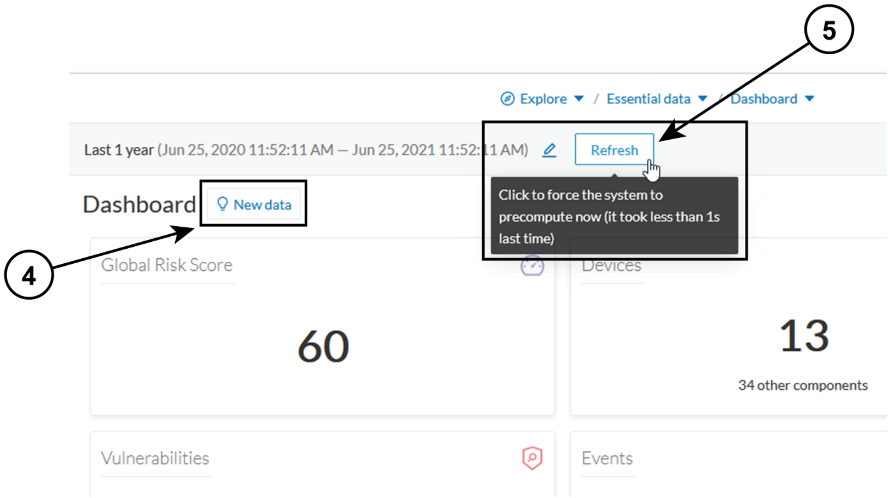
The entire database used to be checked over and over. Elements such as components, tags and activities were counted repeatedly and displayed simultaneously in the preset views, which were continuously refreshed.

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).



Click to force the system to precompute now (it took less than 1s last time)

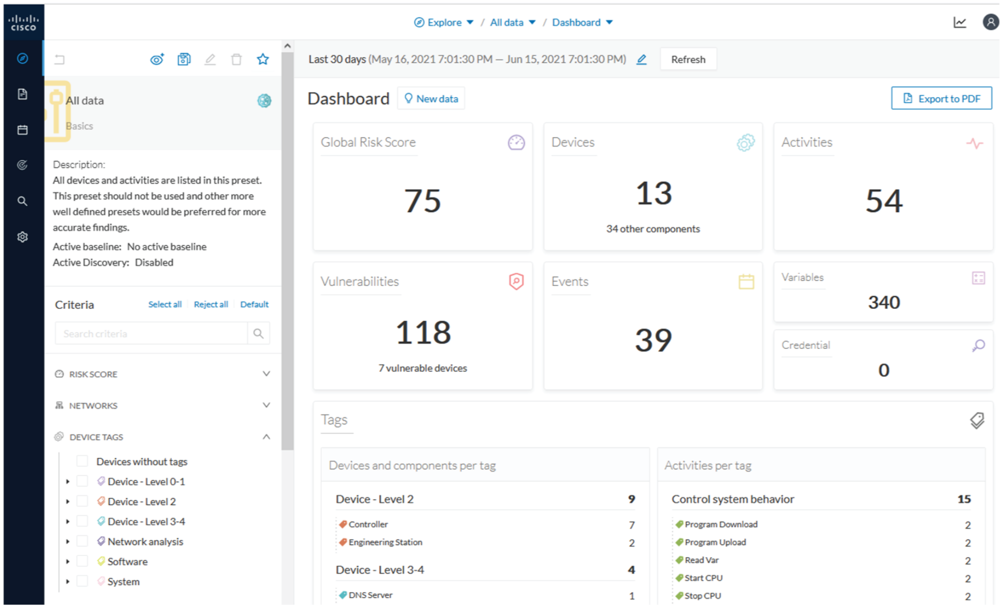
In any cases, the computation is forced and the view is refreshed as you navigate in the application. For example, when accessing another preset or when moving from one view to another.

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.



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

All data
Basics

Description:
All devices and activities are listed in this preset. This preset should not be used and other more well defined presets would be preferred for more accurate findings.
Active baseline: No active baseline
Active Discovery: Disabled

Criteria

- □ Devices without tags
- □ Device - Level 0-1
- □ Device - Level 2
- □ Device - Level 3-4
- □ Network analysis
- □ Software
- □ System

Dashboard

Global Risk Score	Devices	Activities
75	13 34 other components	54

Vulnerabilities	Events	Variables	Credential
118 7 vulnerable devices	39	340	0

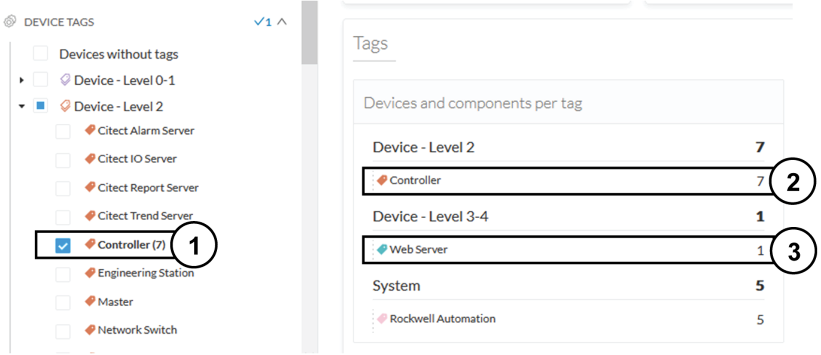
Tags

Devices and components per tag	
Device - Level 2	9
Controller	7
Engineering Station	2
Device - Level 3-4	4
DNS Server	1

Activities per tag	
Control system behavior	15
Program Download	2
Program Upload	2
Read Var	2
Start CPU	2
Stop CPU	2

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.



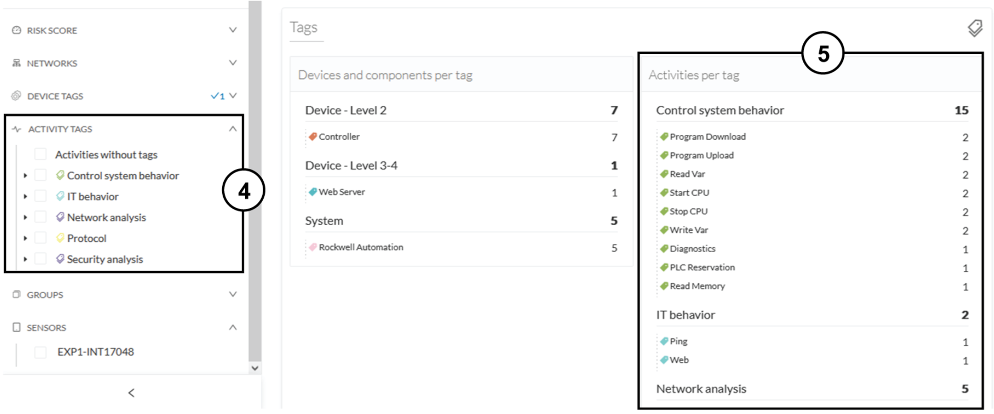
- □ Devices without tags
- □ Device - Level 0-1
- ■ Device - Level 2
  - □ Citect Alarm Server
  - □ Citect IO Server
  - □ Citect Report Server
  - □ Citect Trend Server
  - ☑ Controller (7)
  - □ Engineering Station
  - □ Master
  - □ Network Switch

Tags

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

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.



Devices and components per tag

Tag	Count
Device - Level 2	7
Controller	7
Device - Level 3-4	1
Web Server	1
System	5
Rockwell Automation	5

Activities per tag

Tag	Count
Control system behavior	15
Program Download	2
Program Upload	2
Read Var	2
Start CPU	2
Stop CPU	2
Write Var	2
Diagnostics	1
PLC Reservation	1
Read Memory	1
IT behavior	2
Ping	1
Web	1
Network analysis	5

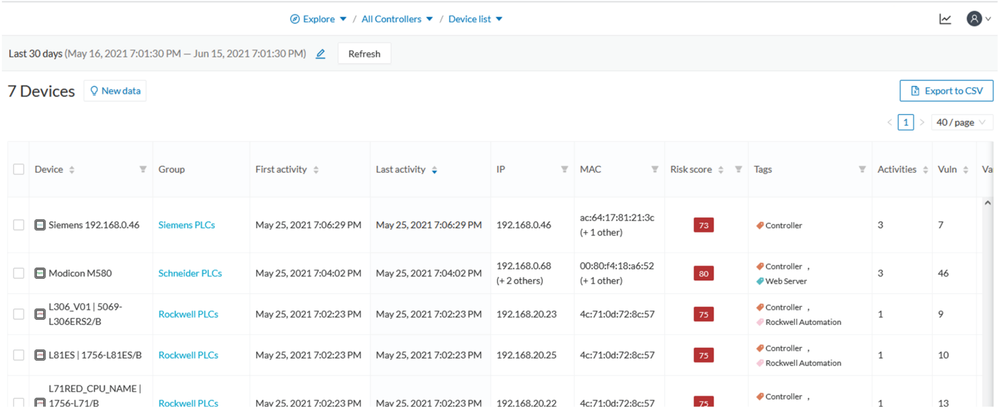
If you want to know more about one of these activities, switch to the Device and activity lists and reach them using the filter available in the tags column.

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:

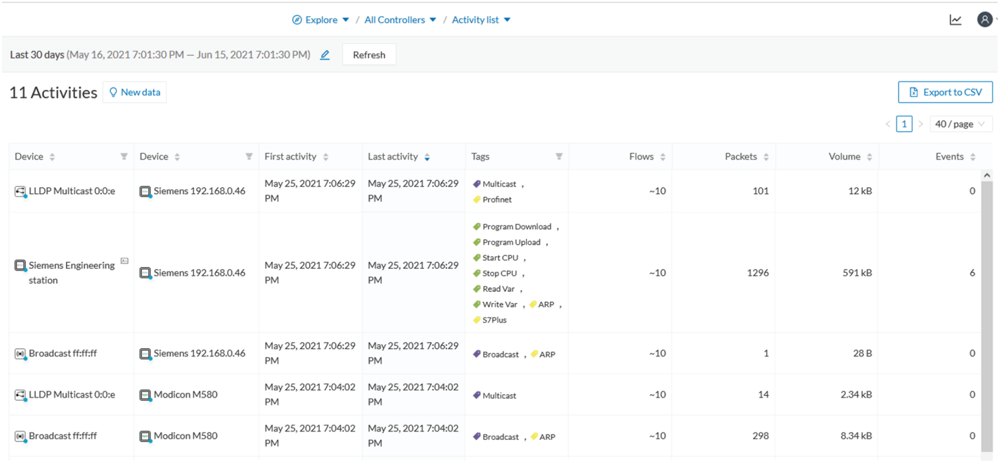


Last 30 days (May 16, 2021 7:01:30 PM — Jun 15, 2021 7:01:30 PM)

7 Devices

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

The All Controllers preset in the activity list view:



Explore / All Controllers / Activity list

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

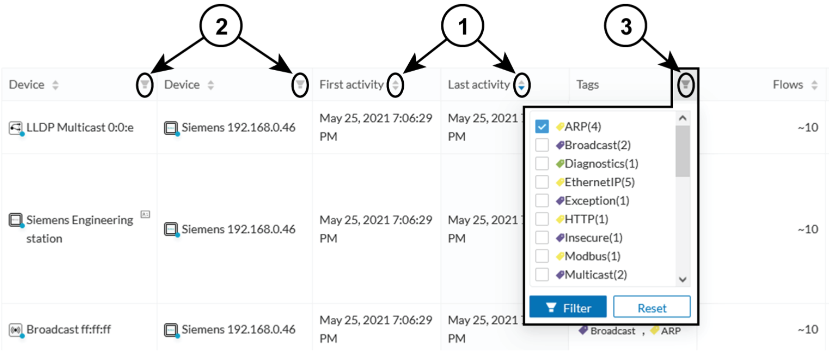
11 Activities New data Export to CSV

1 40 / page

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

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

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



Device	Device	First activity	Last activity	Tags	Flows
LLDP Multicast 0:0:e	Siemens 192.168.0.46	May 25, 2021 7:06:29 PM	May 25, 2021 PM		~10
Siemens Engineering station	Siemens 192.168.0.46	May 25, 2021 7:06:29 PM	May 25, 2021 PM		~10
Broadcast ff:ff:ff	Siemens 192.168.0.46	May 25, 2021 7:06:29 PM	May 25, 2021 PM	Broadcast , ARP	~10

☑ ARP(4)
☐ Broadcast(2)
☐ Diagnostics(1)
☐ EthernetIP(5)
☐ Exception(1)
☐ HTTP(1)
☐ Insecure(1)
☐ Modbus(1)
☐ Multicast(2)

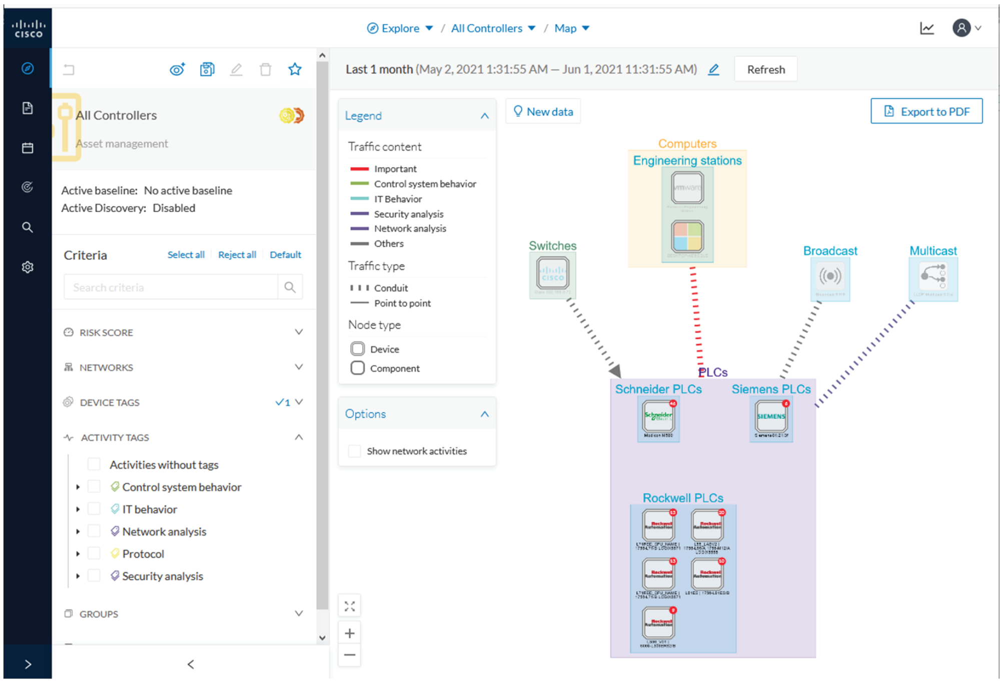
Filter Reset

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

Map

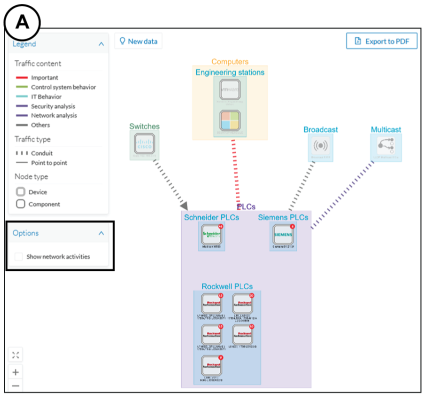
The Map is a visual representation of data of the industrial network that gives you a broad insight on how devices and components are interconnected. It's a good input to get to know how the network is structured. You can start organizing components in a way that makes sense to you by creating groups.

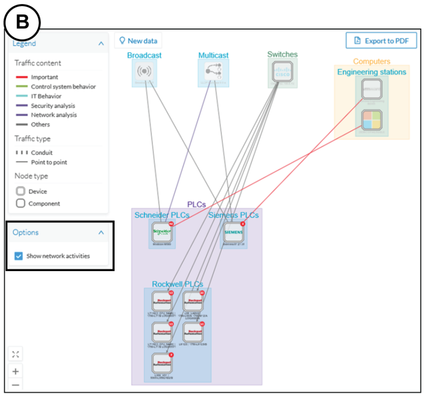
Maps display devices, components and activities according to criteria set in a preset. **Grayed out devices and components** are displayed because, even if they don't correspond to the preset's criteria, they are necessary to represent the activities of the preset.



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

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

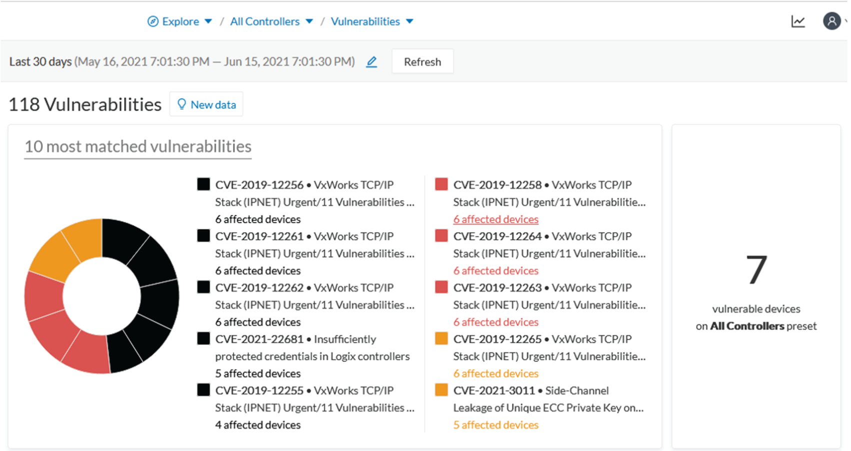




Vulnerabilities

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

Important It is important to 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.



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

118 Vulnerabilities

10 most matched vulnerabilities

■ CVE-2019-12256 • VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities ... 6 affected devices

■ CVE-2019-12261 • VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities ... 6 affected devices

■ CVE-2019-12262 • VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities ... 6 affected devices

■ CVE-2021-22681 • Insufficiently protected credentials in Logix controllers 5 affected devices

■ CVE-2019-12255 • VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities ... 4 affected devices

🟥 CVE-2019-12258 • VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilitie... 6 affected devices

🟥 CVE-2019-12264 • VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilitie... 6 affected devices

🟥 CVE-2019-12263 • VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilitie... 6 affected devices

🟧 CVE-2019-12265 • VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilitie... 6 affected devices

🟧 CVE-2021-3011 • Side-Channel Leakage of Unique ECC Private Key on... 5 affected devices

7 vulnerable devices on **All Controllers** preset

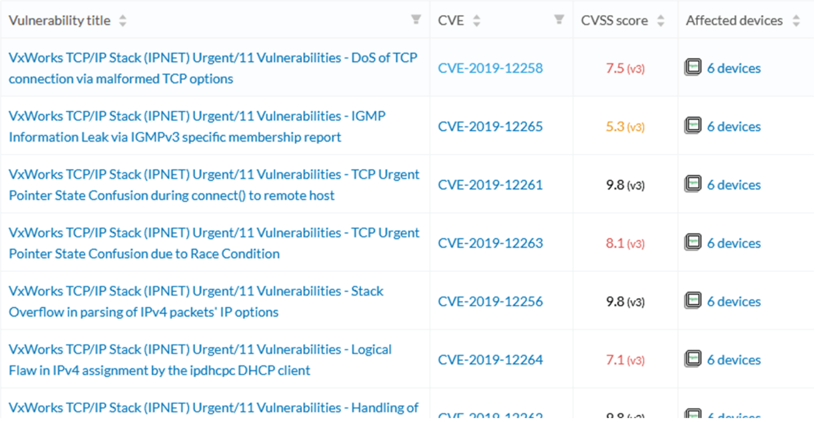
The pie chart presents the 10 most matched vulnerabilities within the preset, that is, the vulnerabilities that have affected more devices. You can click the number of devices detected to see the devices affected.

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

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

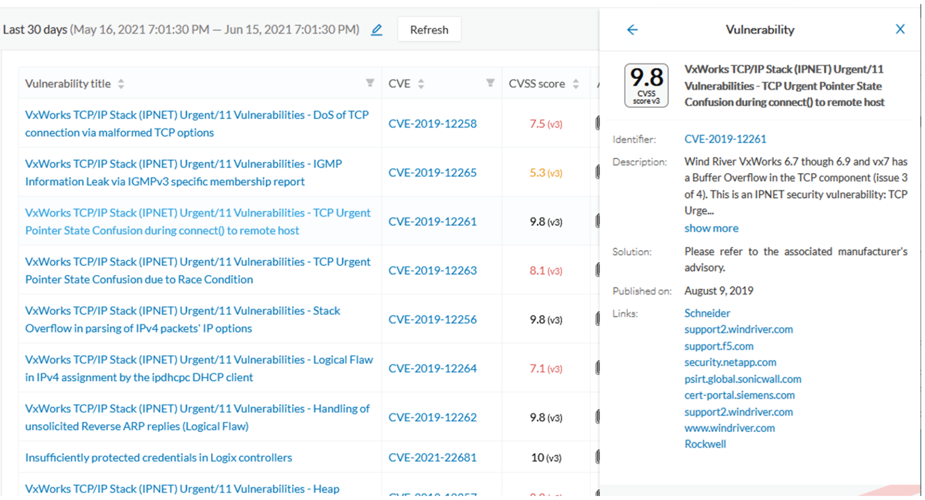
For each vulnerability, the following data are displayed in columns:

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



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

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



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

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

Vulnerability

9.8 CVSS score v3

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

Identifier: CVE-2019-12261

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

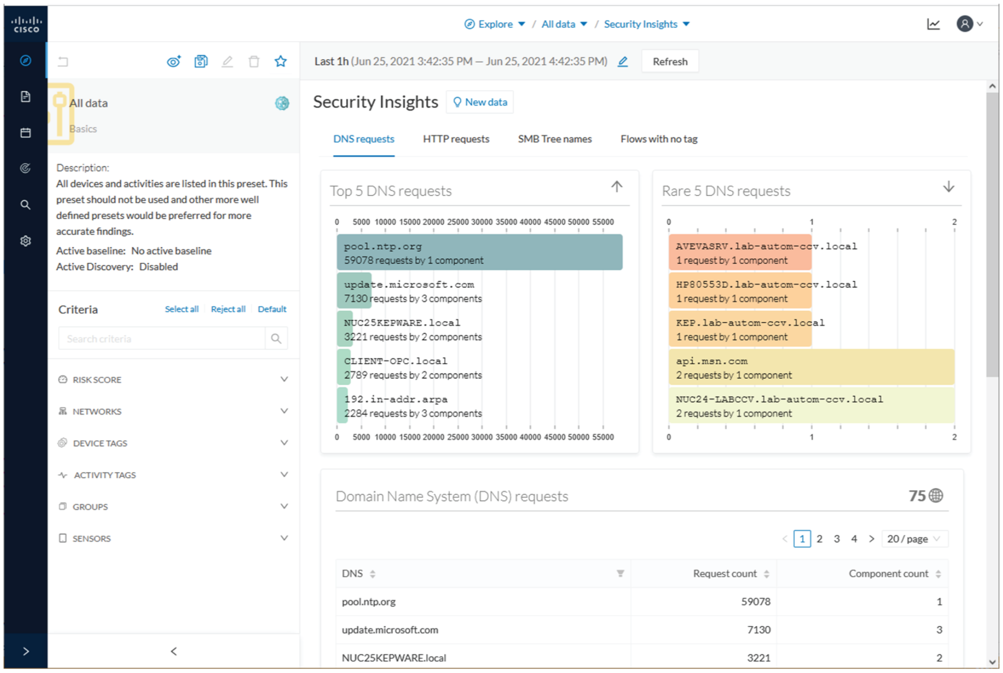
Solution: Please refer to the associated manufacturer's advisory.

Published on: August 9, 2019

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

Security Insights

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



Last 1h (Jun 25, 2021 3:42:35 PM — Jun 25, 2021 4:42:35 PM)

Description:
All devices and activities are listed in this preset. This preset should not be used and other more well defined presets would be preferred for more accurate findings.

Active baseline: No active baseline
Active Discovery: Disabled

Security Insights

Top 5 DNS requests

- pool.ntp.org 59078 requests by 1 component
- update.microsoft.com 7130 requests by 3 components
- NUC25KEPWARE.local 3221 requests by 2 components
- CLIENT-OPC.local 2789 requests by 2 components
- 192.in-addr.arpa 2284 requests by 3 components

Rare 5 DNS requests

- AVEVASRV.lab-autom-ccv.local 1 request by 1 component
- HP80553D.lab-autom-ccv.local 1 request by 1 component
- KEP.lab-autom-ccv.local 1 request by 1 component
- api.msn.com 2 requests by 1 component
- NUC24-LABCCV.lab-autom-ccv.local 2 requests by 1 component

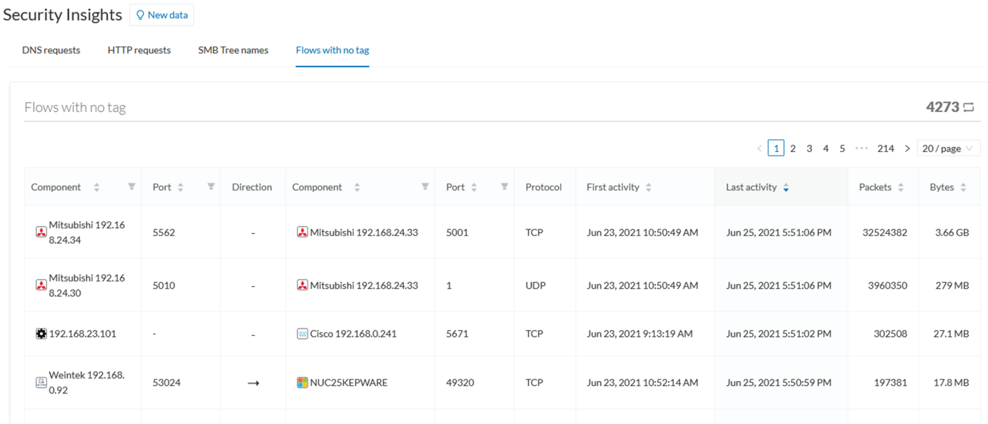
Domain Name System (DNS) requests 75

< 1 2 3 4 > 20 / page

DNS	Request count	Component count
pool.ntp.org	59078	1
update.microsoft.com	7130	3
NUC25KEPWARE.local	3221	2

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

Flows with no tag:



Flows with no tag 4273

< 1 2 3 4 5 ··· 214 > 20 / page

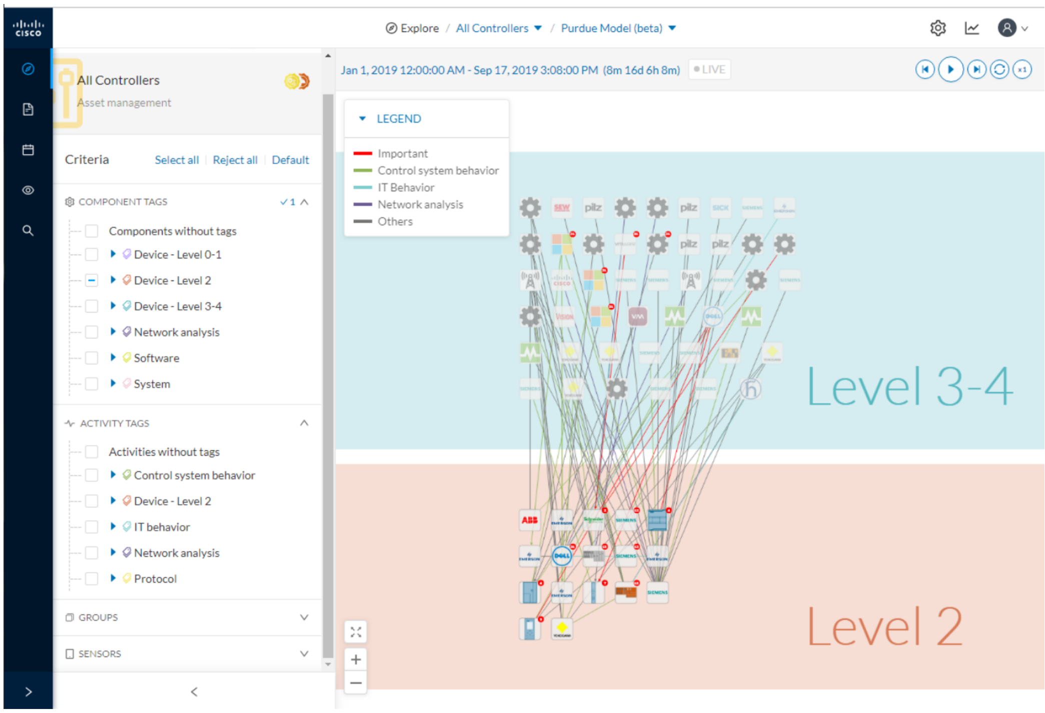
Component	Port	Direction	Component	Port	Protocol	First activity	Last activity	Packets	Bytes
Mitsubishi 192.168.24.34	5562	-	Mitsubishi 192.168.24.33	5001	TCP	Jun 23, 2021 10:50:49 AM	Jun 25, 2021 5:51:06 PM	32524382	3.66 GB
Mitsubishi 192.168.24.30	5010	-	Mitsubishi 192.168.24.33	1	UDP	Jun 23, 2021 10:50:49 AM	Jun 25, 2021 5:51:06 PM	3960350	279 MB
192.168.23.101	-	-	Cisco 192.168.0.241	5671	TCP	Jun 23, 2021 9:13:19 AM	Jun 25, 2021 5:51:02 PM	302508	27.1 MB
Weintek 192.168.0.92	53024	→	NUC25KEPWARE	49320	TCP	Jun 23, 2021 10:52:14 AM	Jun 25, 2021 5:50:59 PM	197381	17.8 MB

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:

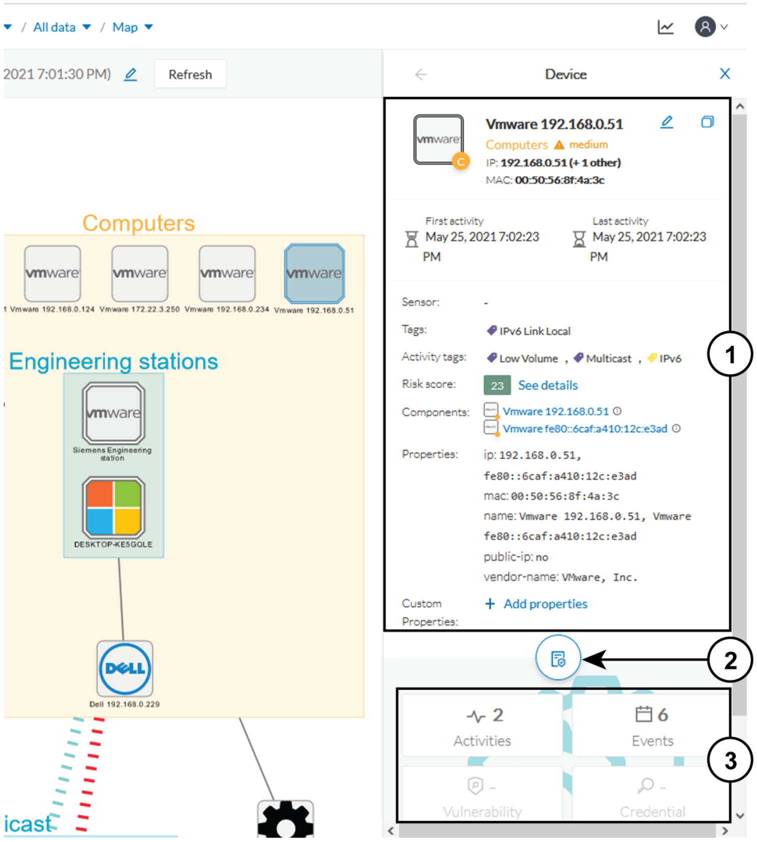


Components are distributed according to the different layers of the Purdue model:

- 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.



Device

Vmware 192.168.0.51
Computers medium
IP: 192.168.0.51 (+ 1 other)
MAC: 00:50:56:8f:4a:3c

First activity May 25, 2021 7:02:23 PM
Last activity May 25, 2021 7:02:23 PM

Sensor: -
Tags: IPv6 Link Local
Activity tags: Low Volume , Multicast , IPv6
Risk score: 23 See details
Components: Vmware 192.168.0.51
Vmware fe80::6caf:a410:12c:e3ad
Properties: ip: 192.168.0.51, fe80::6caf:a410:12c:e3ad
mac: 00:50:56:8f:4a:3c
name: Vmware 192.168.0.51, Vmware fe80::6caf:a410:12c:e3ad
public-ip: no
vendor-name: VMware, Inc.
Custom Properties: + Add properties

2 Activities
6 Events
- Vulnerability
- Credential

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).

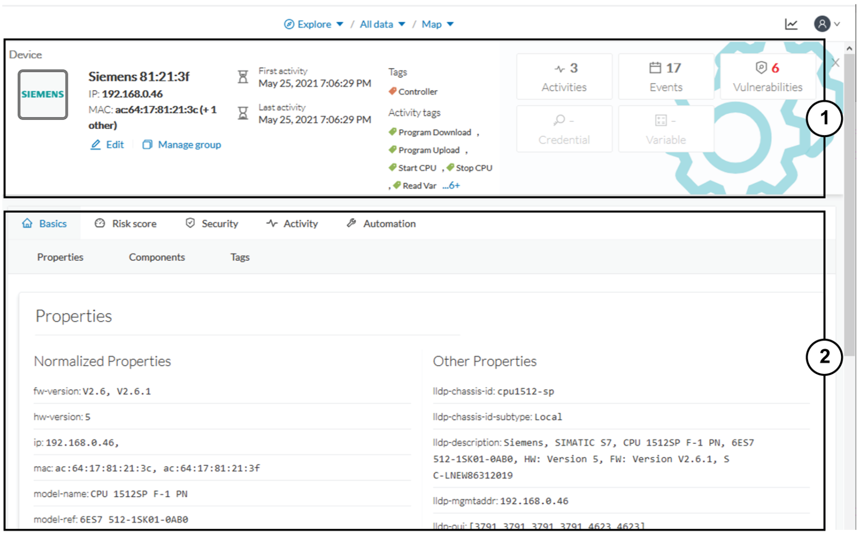
The rectangular buttons below **(3)** redirect to the corresponding information inside the technical sheet.

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:



Siemens 81:21:3f
IP: 192.168.0.46
MAC: ac:64:17:81:21:3c (+ 1 other)

First activity
May 25, 2021 7:06:29 PM

Last activity
May 25, 2021 7:06:29 PM

Tags
Controller

Activity tags
Program Download , Program Upload , Start CPU , Stop CPU , Read Var ...6+

Properties

Normalized Properties

fw-version: V2.6, V2.6.1
hw-version: 5
ip: 192.168.0.46,
mac: ac:64:17:81:21:3c, ac:64:17:81:21:3f
model-name: CPU 1512SP F-1 PN
model-ref: 6ES7 512-1SK01-0AB0

Other Properties

lldp-chassis-id: cpu1512-sp
lldp-chassis-id-subtype: Local
lldp-description: Siemens, SIMATIC S7, CPU 1512SP F-1 PN, 6ES7 512-1SK01-0AB0, HW: Version 5, FW: Version V2.6.1, S C-LNEW86312019
lldp-mgmtaddr: 192.168.0.46
lldp-oui: [3791 3791 3791 3791 4623 4623]

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

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

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

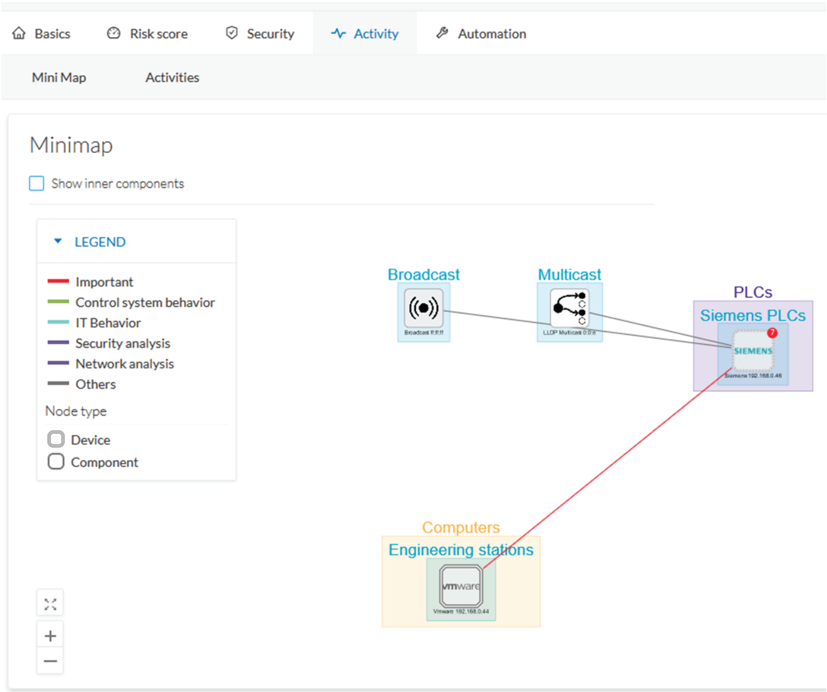
You can access technical sheets through a device, component or an activity's Right side panel, clicking the technical sheet button. A flow's technical sheet is visible when clicking on a particular flow.

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

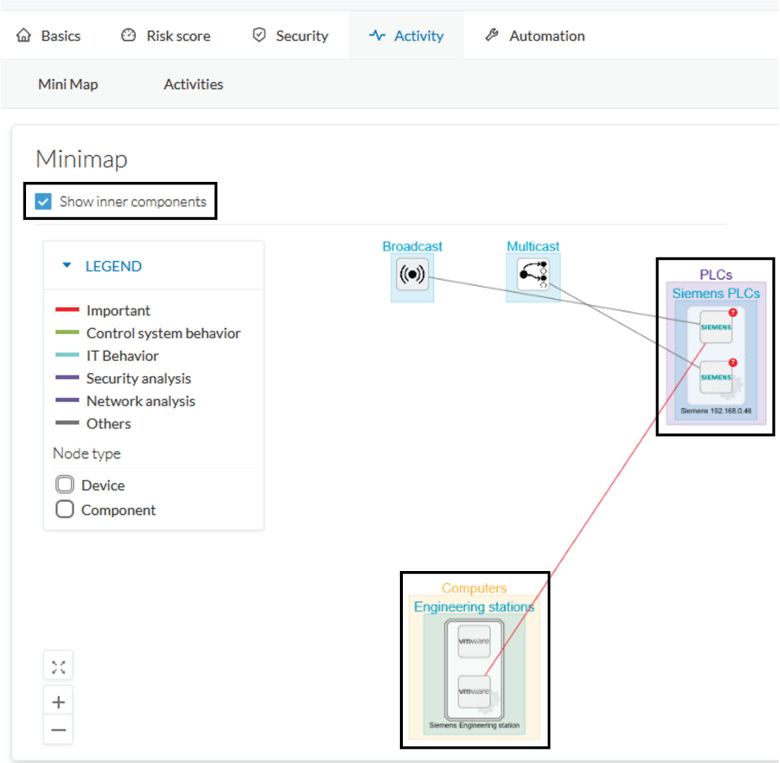
Mini map

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

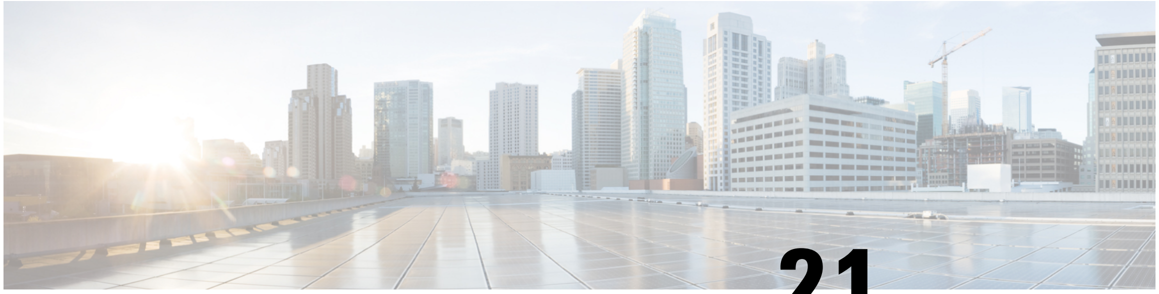
This view is accessible through the Activity tab of a Component's Technical sheets.



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



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

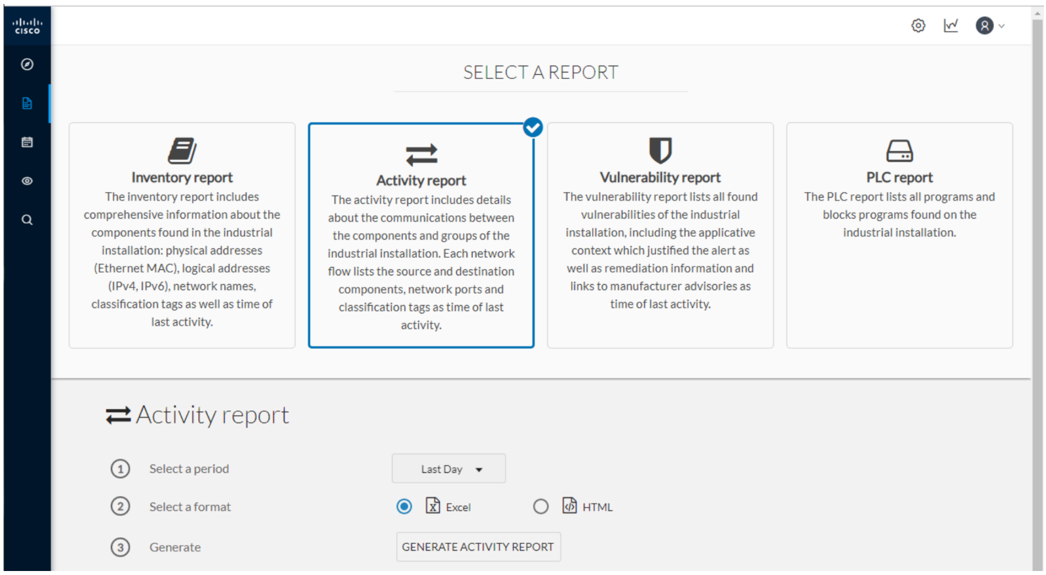


CHAPTER 21

Reports

Reports

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



SELECT A REPORT

Inventory report
The inventory report includes comprehensive information about the components found in the industrial installation: physical addresses (Ethernet MAC), logical addresses (IPv4, IPv6), network names, classification tags as well as time of last activity.

Activity report
The activity report includes details about the communications between the components and groups of the industrial installation. Each network flow lists the source and destination components, network ports and classification tags as time of last activity.

Vulnerability report
The vulnerability report lists all found vulnerabilities of the industrial installation, including the applicative context which justified the alert as well as remediation information and links to manufacturer advisories as time of last activity.

PLC report
The PLC report lists all programs and blocks programs found on the industrial installation.

Activity report

1. Select a period: Last Day
2. Select a format: ● Excel ○ HTML
3. Generate: GENERATE ACTIVITY REPORT

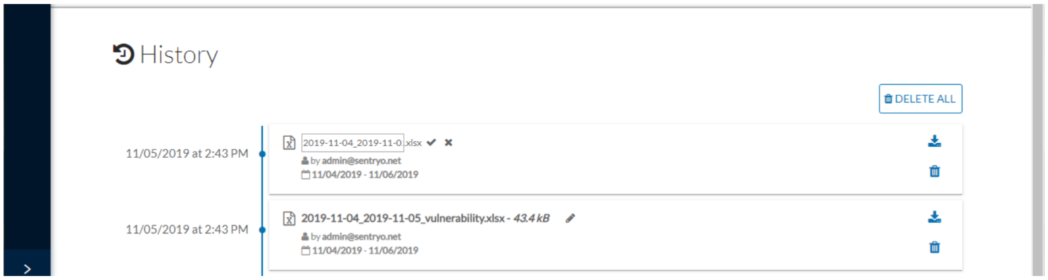
Below is the description of the four types of reports available:

- 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.



History

DELETE ALL

11/05/2019 at 2:43 PM
2019-11-04_2019-11-0.xlsx ✓ ✕
by admin@sentryo.net
11/04/2019 - 11/06/2019

11/05/2019 at 2:43 PM
2019-11-04_2019-11-05_vulnerability.xlsx - *43.4 kB*
by admin@sentryo.net
11/04/2019 - 11/06/2019

CHAPTER 22

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.

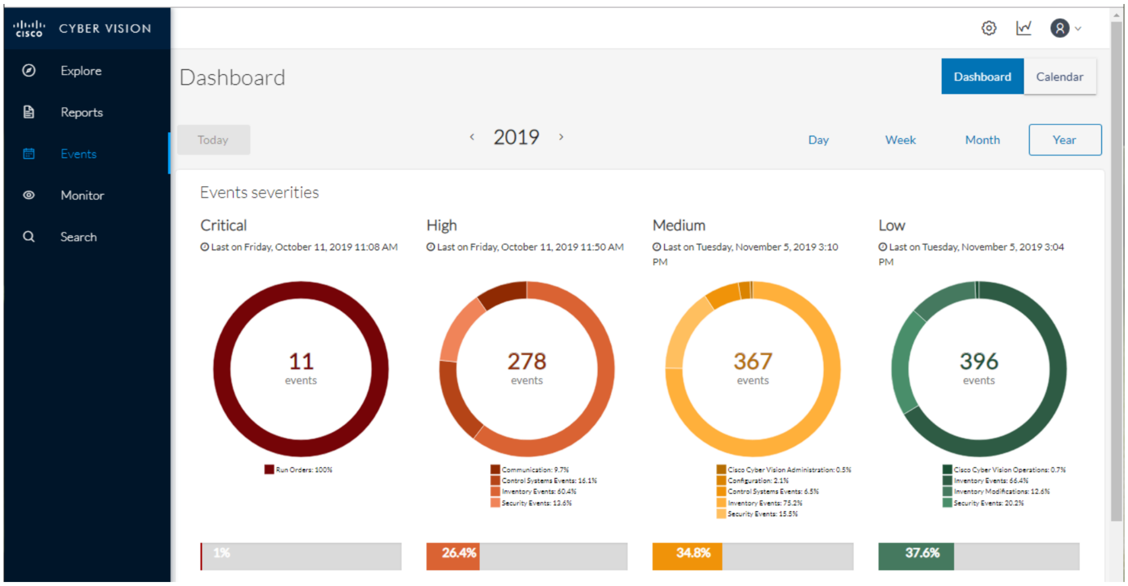
The Events page provides two views to give high visibility on these events:

- 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.

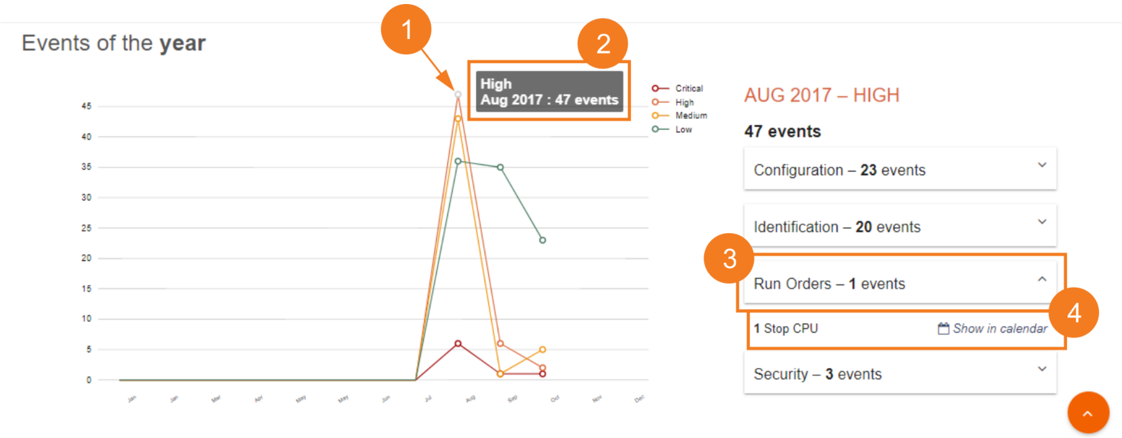
Doughnut charts present events numbers and percentages per categories and severities.



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.



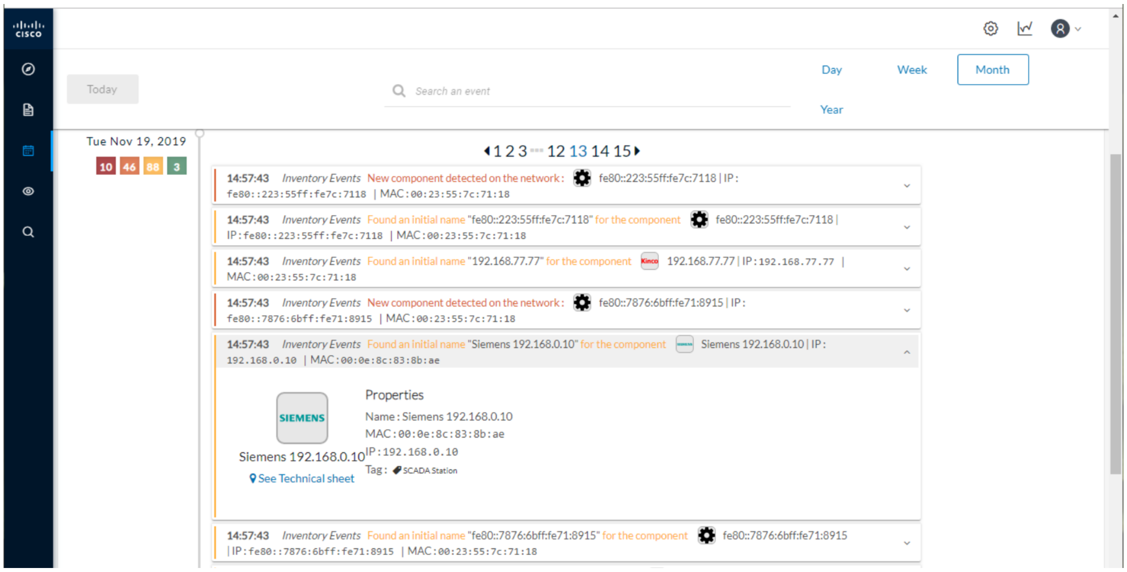
Clicking event markers **(1)** on the line chart lets you see the number of events per category according to a specific time **(2)**.

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.



14:57:43 Inventory Events New component detected on the network : fe80::223:55ff:fe7c:7118 | IP : fe80::223:55ff:fe7c:7118 | MAC : 00:23:55:7c:71:18

14:57:43 Inventory Events Found an initial name "fe80::223:55ff:fe7c:7118" for the component fe80::223:55ff:fe7c:7118 | IP : fe80::223:55ff:fe7c:7118 | MAC : 00:23:55:7c:71:18

14:57:43 Inventory Events Found an initial name "192.168.77.77" for the component 192.168.77.77 | IP : 192.168.77.77 | MAC : 00:23:55:7c:71:18

14:57:43 Inventory Events New component detected on the network : fe80::7876:6bff:fe71:8915 | IP : fe80::7876:6bff:fe71:8915 | MAC : 00:23:55:7c:71:18

14:57:43 Inventory Events Found an initial name "Siemens 192.168.0.10" for the component Siemens 192.168.0.10 | IP : 192.168.0.10 | MAC : 00:0e:8c:83:8b:ae

Siemens 192.168.0.10

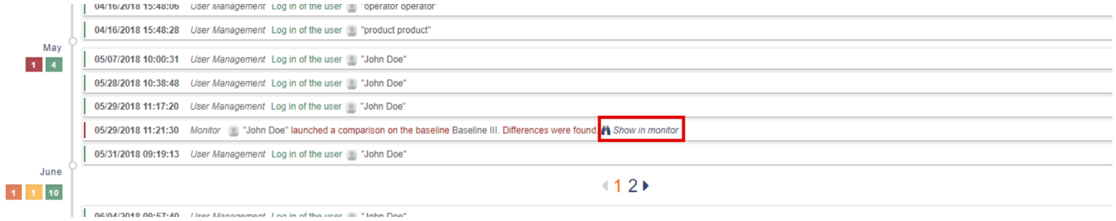
Name : Siemens 192.168.0.10
MAC : 00:0e:8c:83:8b:ae
IP : 192.168.0.10
Tag : SCADA Station

14:57:43 Inventory Events Found an initial name "fe80::7876:6bff:fe71:8915" for the component fe80::7876:6bff:fe71:8915 | IP : fe80::7876:6bff:fe71:8915 | MAC : 00:23:55:7c:71:18

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.



```
04/16/2018 15:48:06  User Management  Log in of the user  "operator operator"
04/16/2018 15:48:28  User Management  Log in of the user  "product product"
05/07/2018 10:00:31  User Management  Log in of the user  "John Doe"
05/28/2018 10:38:48  User Management  Log in of the user  "John Doe"
05/29/2018 11:17:20  User Management  Log in of the user  "John Doe"
05/29/2018 11:21:30  Monitor  "John Doe" launched a comparison on the baseline Baseline III. Differences were found. Show in monitor
05/31/2018 09:19:13  User Management  Log in of the user  "John Doe"
06/04/2018 09:57:40  User Management  Log in of the user  "John Doe"
```

CHAPTER 23

Monitor

Monitor mode

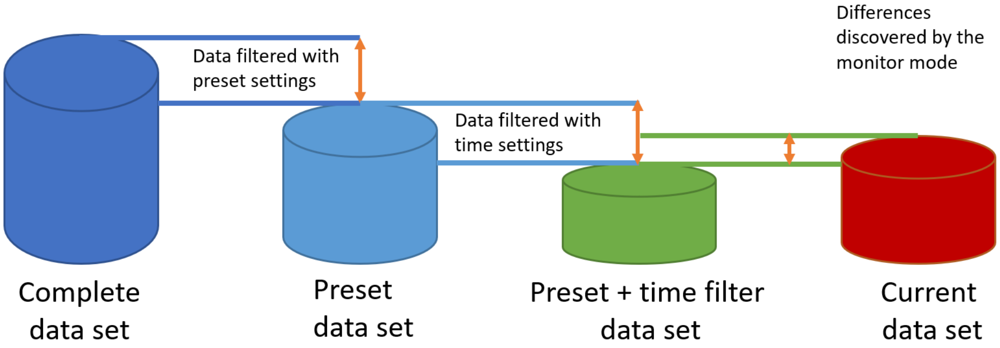
Cisco Cyber Vision provides a monitoring tool called the Monitor mode to detect changes inside industrial networks. Because a network architecture (PLC, switch, SCADA) is constant and its behaviors tend to be stable over time, an established and configured network is predictable. However, some behaviors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

Baselines as Preset's normal states

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

Review and assignment of differences

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


Differences discovered by the monitor mode
Data filtered with preset settings
Data filtered with time settings
Complete data set
Preset data set
Preset + time filter data set
Current data set

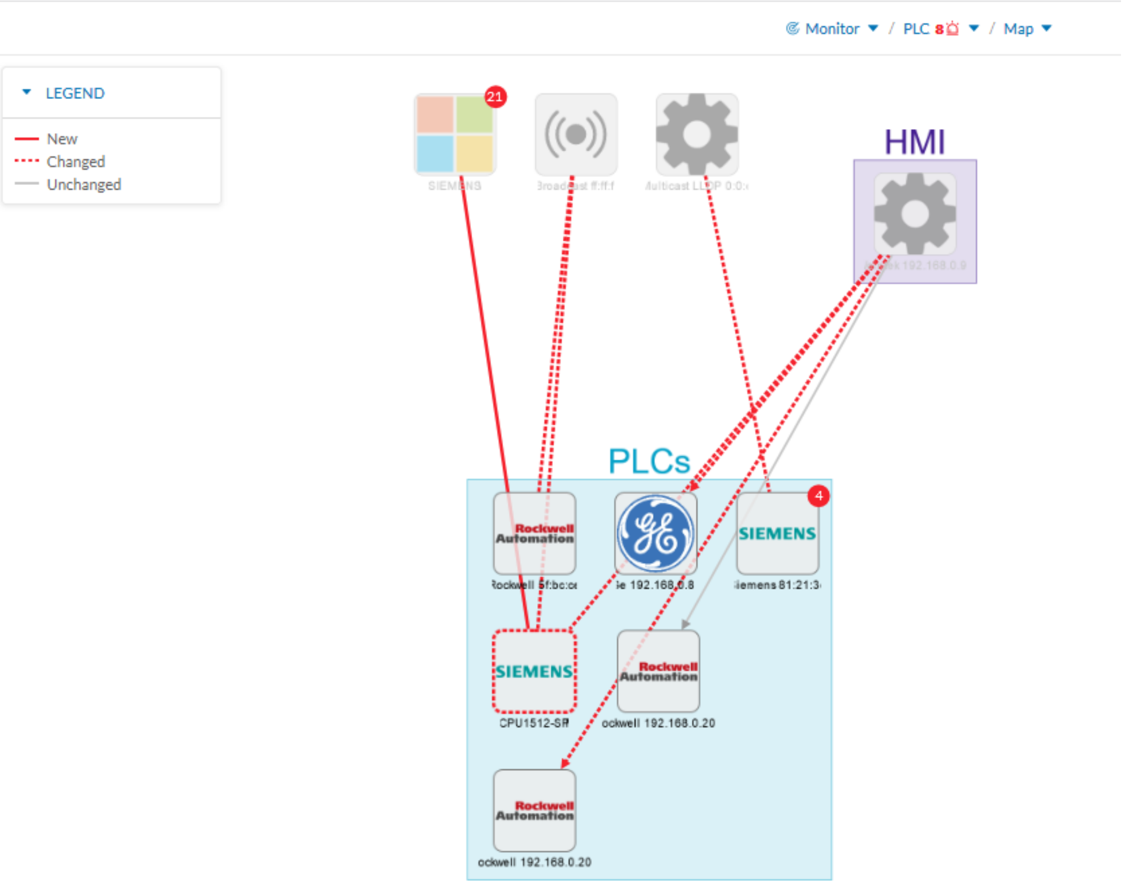
Monitor mode's views

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

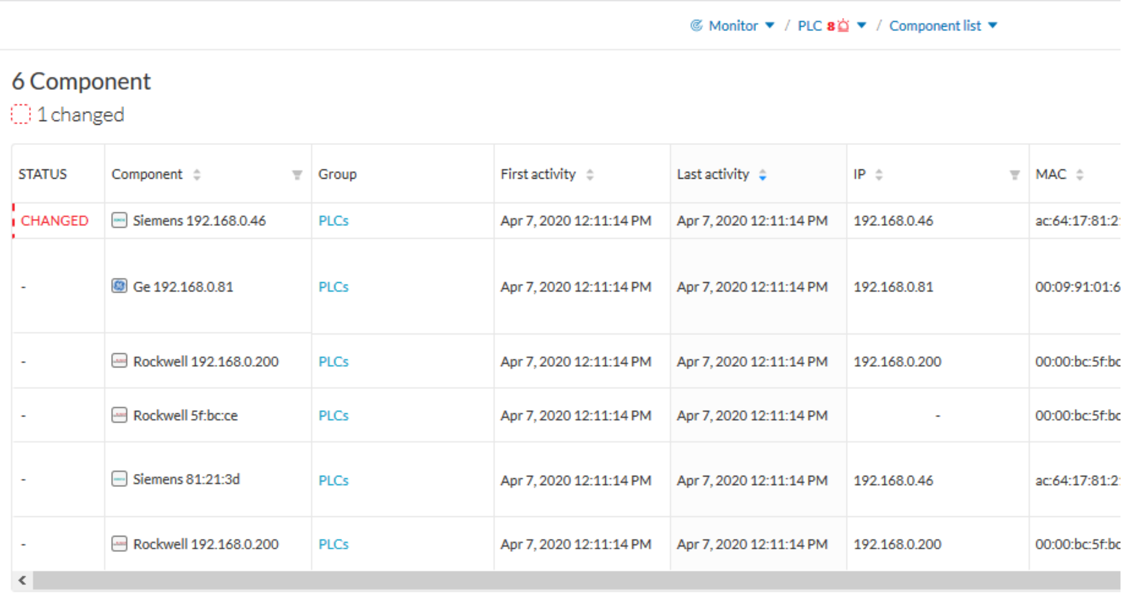
For more information about the views listed below, refer to the Explore chapter.

The map view:

non-aggregated components



The component list view:

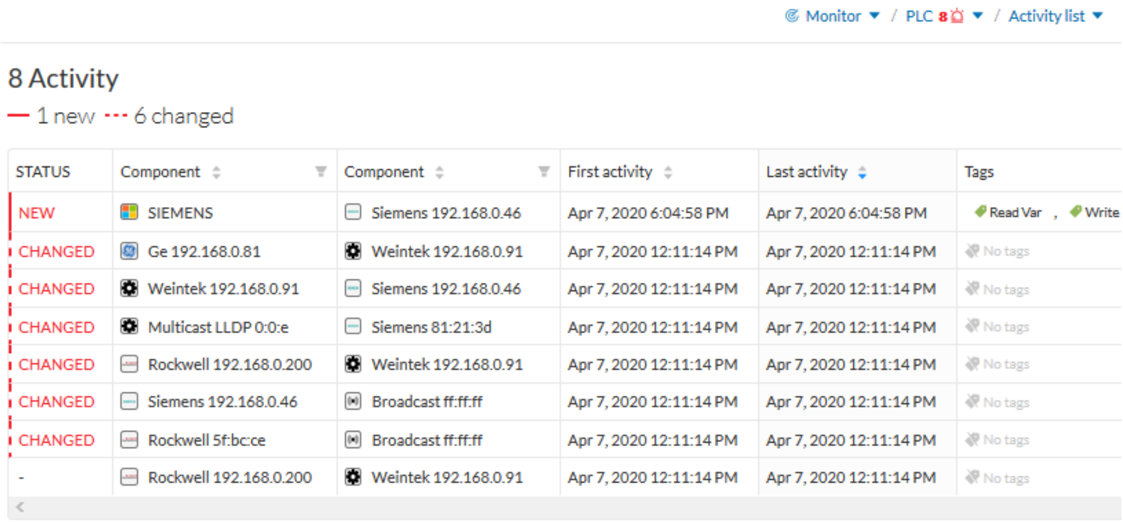


6 Component

⬚ 1 changed

STATUS	Component	Group	First activity	Last activity	IP	MAC
CHANGED	Siemens 192.168.0.46	PLCs	Apr 7, 2020 12:11:14 PM	Apr 7, 2020 12:11:14 PM	192.168.0.46	ac:64:17:81:2
-	Ge 192.168.0.81	PLCs	Apr 7, 2020 12:11:14 PM	Apr 7, 2020 12:11:14 PM	192.168.0.81	00:09:91:01:6
-	Rockwell 192.168.0.200	PLCs	Apr 7, 2020 12:11:14 PM	Apr 7, 2020 12:11:14 PM	192.168.0.200	00:00:bc:5f:bc
-	Rockwell 5f:bc:ce	PLCs	Apr 7, 2020 12:11:14 PM	Apr 7, 2020 12:11:14 PM	-	00:00:bc:5f:bc
-	Siemens 81:21:3d	PLCs	Apr 7, 2020 12:11:14 PM	Apr 7, 2020 12:11:14 PM	192.168.0.46	ac:64:17:81:2
-	Rockwell 192.168.0.200	PLCs	Apr 7, 2020 12:11:14 PM	Apr 7, 2020 12:11:14 PM	192.168.0.200	00:00:bc:5f:bc

The activity list view:



8 Activity

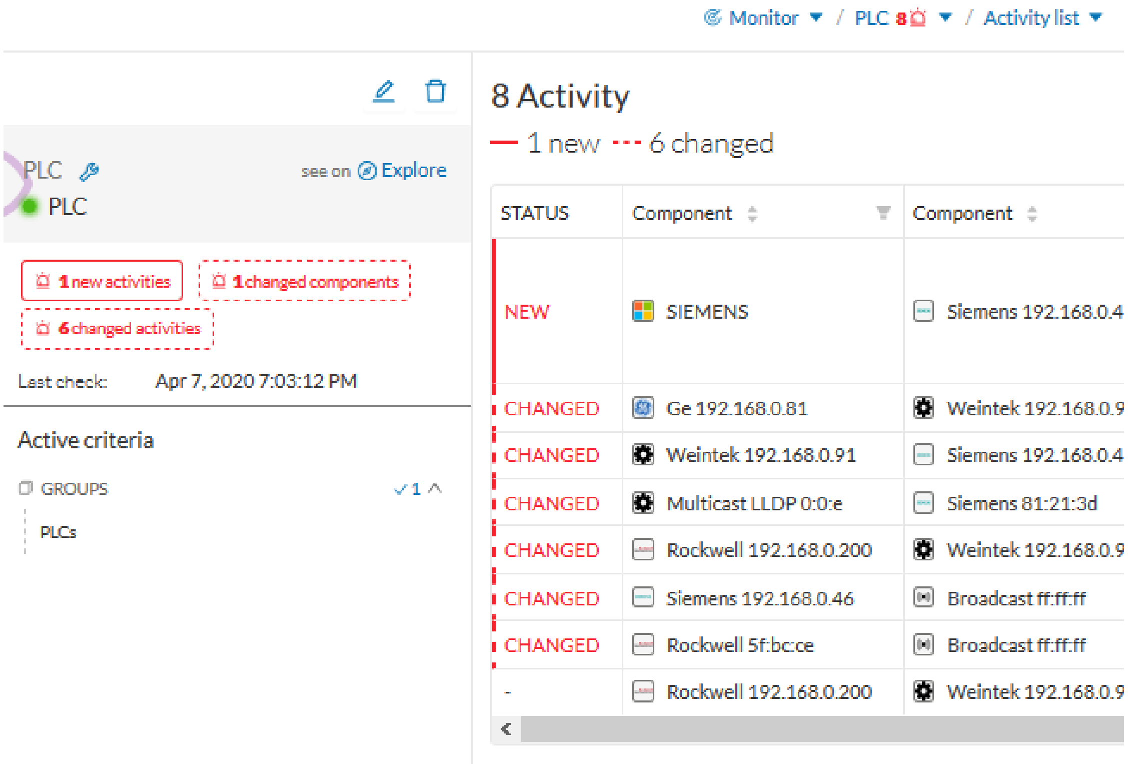
— 1 new --- 6 changed

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

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

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

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



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

Active criteria

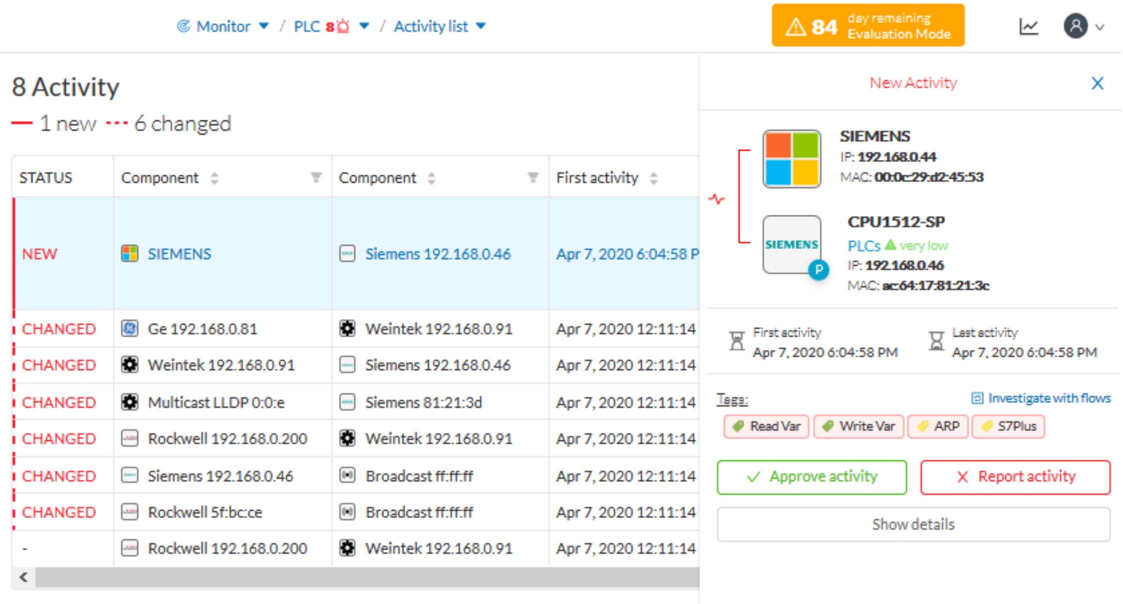
8 Activity

1 new 6 changed

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

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

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


Monitor / PLC 8 / Activity list
84 day remaining Evaluation Mode

8 Activity

— 1 new ··· 6 changed

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

New Activity

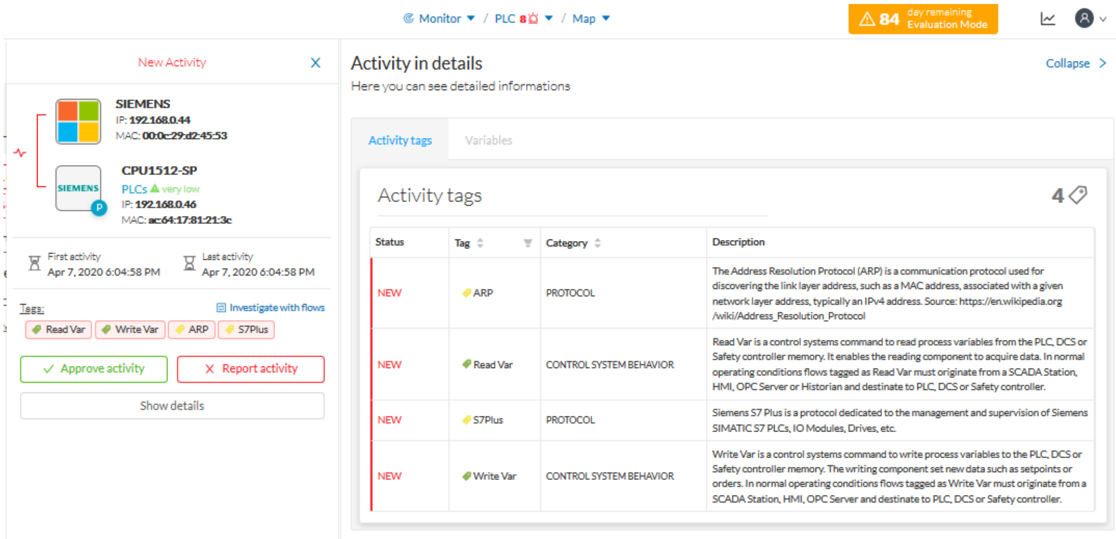
SIEMENS
IP: 192.168.0.44
MAC: 00:0c:29:d2:45:53

CPU1512-SP
PLCs very low
IP: 192.168.0.46
MAC: ac:64:17:81:21:3c

First activity Apr 7, 2020 6:04:58 PM
Last activity Apr 7, 2020 6:04:58 PM

Tags: Read Var, Write Var, ARP, S7Plus

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



New Activity

SIEMENS
IP: 192.168.0.44
MAC: 00:0c:29:d2:45:53

CPU1512-SP
PLCs very low
IP: 192.168.0.46
MAC: ac:64:17:81:21:3c

First activity Apr 7, 2020 6:04:58 PM
Last activity Apr 7, 2020 6:04:58 PM

Tags: Read Var, Write Var, ARP, S7Plus

Activity in details

Here you can see detailed informations

Activity tags 4

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

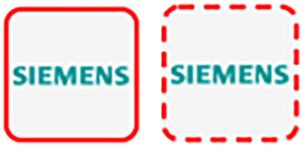
Click the collapse button to come back to the initial view.

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

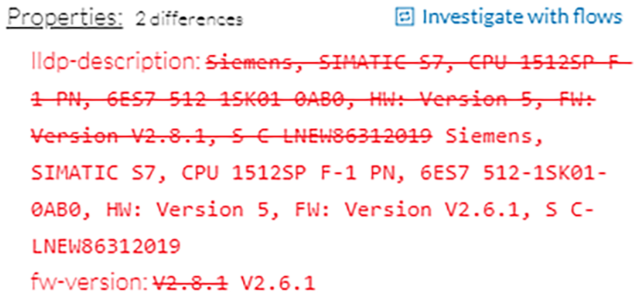
New and changed differences

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

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



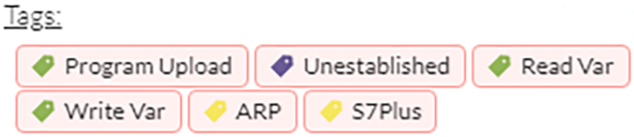
Changed component's properties, with the former crossed out property:


Properties: 2 differences Investigate with flows

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

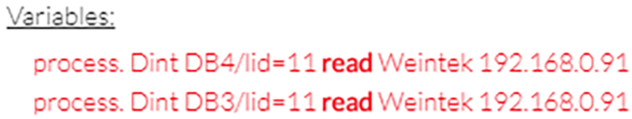
fw-version: ~~V2.8.1~~ V2.6.1

New and changed component and activity tags:


Tags:

Program Upload | Unestablished | Read Var | Write Var | ARP | S7Plus

New and changed activity's variable access:


Variables:

process. Dint DB4/lid=11 **read** Weintek 192.168.0.91

process. Dint DB3/lid=11 **read** Weintek 192.168.0.91

Each difference must be reviewed to identify a potential threat and refine the baseline. Refer to the section Review differences.

Review differences

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

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

Acknowledge differences

Acknowledge in the Monitor mode

"Acknowledge" is an action to be used to indicate that determined behaviors -or differences- are safe and normal. In fact, by doing this action, the difference will be included in the baseline. You can acknowledge differences on any element of the Monitor mode: tags, properties, variable accesses, components, activities and baselines.

Acknowledge a component or an activity

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

- **Acknowledge & Include**

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

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

- **Acknowledge & Keep Warning**

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

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

Report differences

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

Remove and keep warning

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

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

Individual acknowledgment

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

- **Component properties**

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

- **Component and activity tags**

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

- **Activity variable accesses**

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

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

Investigate with flows

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

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

Create a baseline from a default preset

1. Access the Explore page.
2. In Basics, click the preset Essential data.
3. Click the button Add a new baseline from preset.

4. A pop-up appears to invite you to check your new baseline. Click Go check it out.
5. All elements displays. Some components and activities may already appear in red as new or changed.

Create a baseline from a group

To create groups:

Procedure

Step 1 Access the All data preset.

Step 2 Create two groups of components.

Step 3 Click the Autolayout button.

Example:

We create a group HMI and a group PLC.

To create presets from groups:

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

Example:

We select the HMI group in the filter.

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

Step 5 Create a preset from this view.

Step 6 Click Save as and name the preset HMI.

Step 7 Repeat the previous steps for the PLC group.

Step 8 Go to All Presets. You will see your two new presets.

To create a baseline from presets:

Step 9 Access the HMI preset.

Step 10 Click the button "Add a new baseline from preset".

Step 11 Name it HMI.

Step 12 Repeat the previous steps for the PLC preset.

Step 13 Access the Monitor mode. You will see your two new baselines.

Create a weekend baseline

Create another baseline to monitor the network during weekends.

1. Access the All data preset.
2. Set the period for the weekend. For example, from Friday 5 p.m. to Monday 4 a.m.

3. Click the button "Add a new baseline from preset".
4. Name the baseline "All data weekend" and add the description "Must be active from Friday 5pm till Monday 4am".

Enable a baseline monitoring

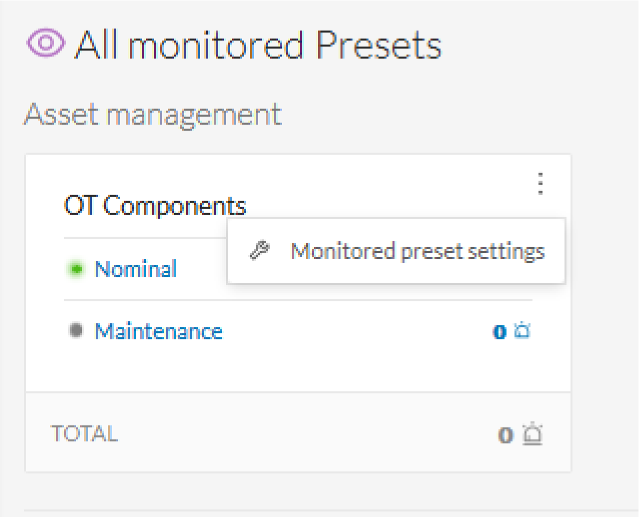
To make the most of the Monitor mode, it is sometimes insightful to create several baselines per preset. However, only one baseline can be active at a time per preset. This is because a baseline is to be used to monitor a well-defined network process during a specific period of time (e.g. baselines Normal operating mode, Maintenance, Week-end, Night). Two baselines cannot happen at the same time on a preset, and you need to enable the proper baseline as the network enters a new operating phase. Consequently, when you enable a baseline on a preset, the active one is automatically disabled.

To enable a baseline:

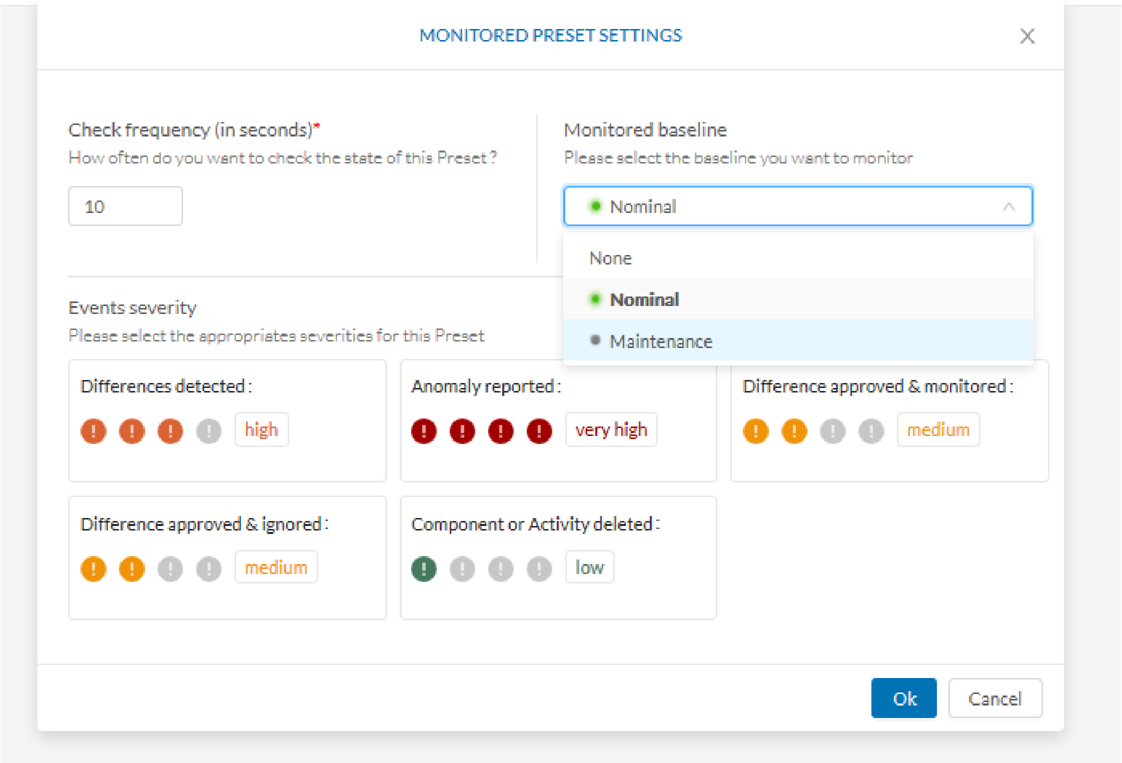
Procedure

Step 1 Access the Monitor page.

Step 2 Click the monitored preset settings menu on the preset you want to monitor.



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



MONITORED PRESET SETTINGS

Check frequency (in seconds)*
How often do you want to check the state of this Preset ?
10

Monitored baseline
Please select the baseline you want to monitor
● Nominal
None
● Nominal
● Maintenance

Events severity
Please select the appropriates severities for this Preset

Differences detected : ● ● ● ○ high

Anomaly reported : ● ● ● ● very high

Difference approved & monitored : ● ● ○ ○ medium

Difference approved & ignored : ● ● ○ ○ medium

Component or Activity deleted : ● ○ ○ ○ low

Ok Cancel

Step 4 Click Ok.

The baseline selected turns to green and is enabled.

Use cases

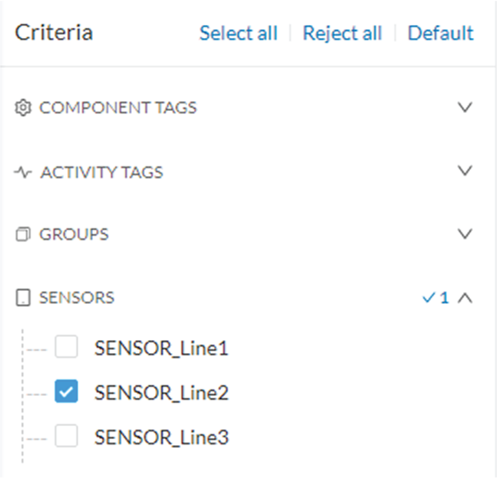
Detection of assets newly connected to the network

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

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

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

Since a sensor is placed on each production chain, we use the sensor filter to display each production chain. In our example, the industrial network we're monitoring has 3 production lines on which we have positioned a sensor. We want to see and monitor what is happening on production line 2. To do so, we access the Preset All data in the Explore mode and we select the filter SENSOR_Line2 (it is possible to rename sensors to identify which area of the network they're monitoring) so only traffic captured on Production Line 2 appears.


Criteria

Select all | Reject all | Default

COMPONENT TAGS

ACTIVITY TAGS

GROUPS

SENSORS ✓1

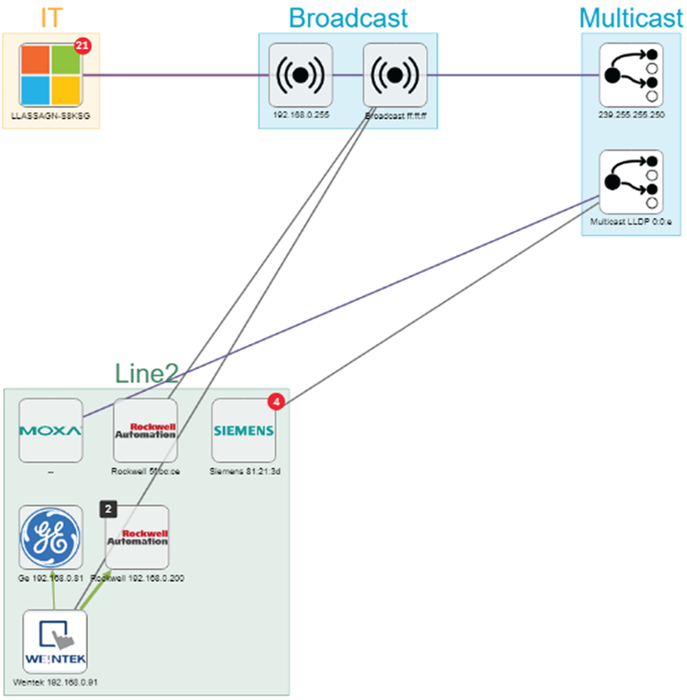
□ SENSOR_Line1

☑ SENSOR_Line2

□ SENSOR_Line3

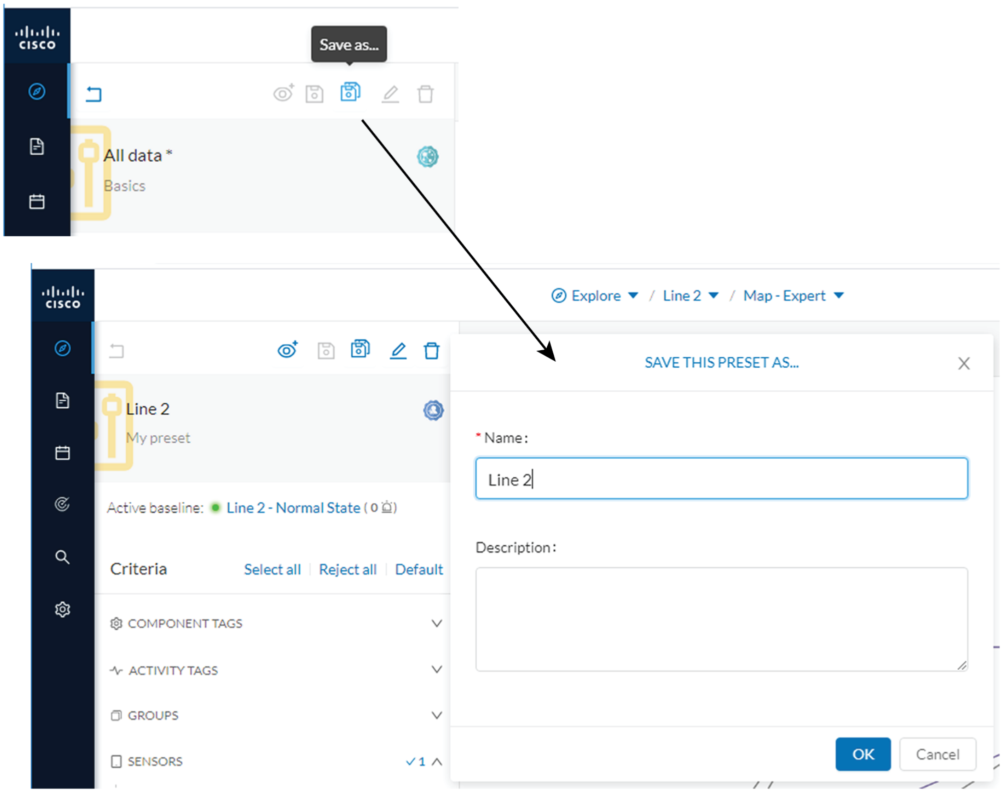
What we need to do then, is to organize the components into groups, per function:

- PLCs in Line 2
- IT
- Broadcast
- Multicast



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

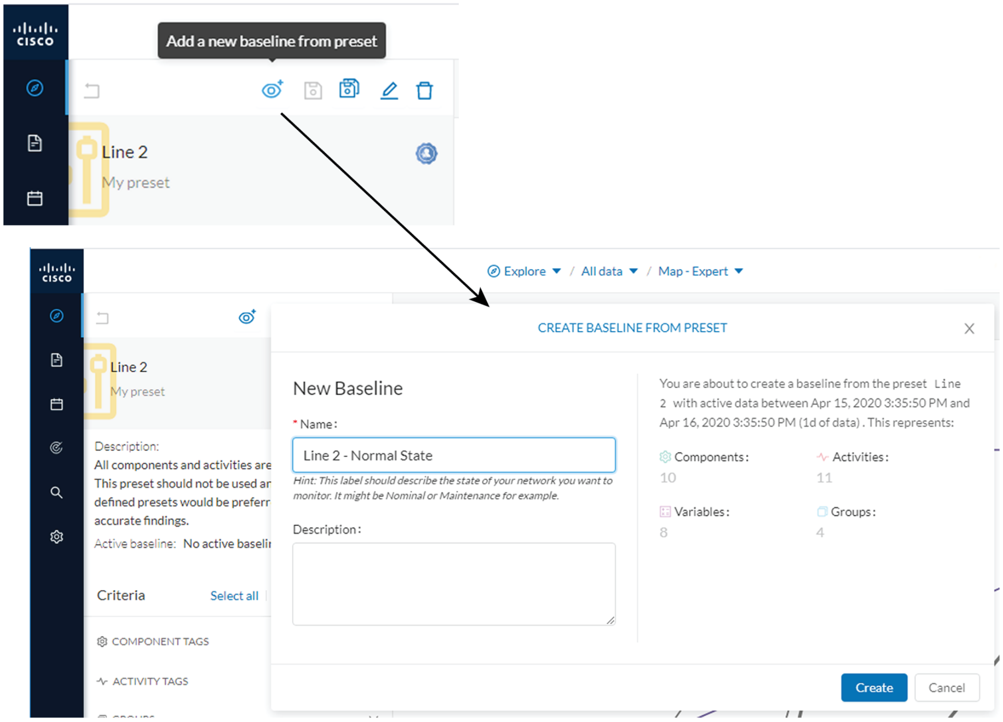
Now that the network data is filtered and grouped, we save the selection as a new preset that we name Line 2.



* Name: Line 2

Description:

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



CREATE BASELINE FROM PRESET

New Baseline

* Name: Line 2 - Normal State

Hint: This label should describe the state of your network you want to monitor. It might be Nominal or Maintenance for example.

Description:

You are about to create a baseline from the preset Line 2 with active data between Apr 15, 2020 3:35:50 PM and Apr 16, 2020 3:35:50 PM (1d of data). This represents:

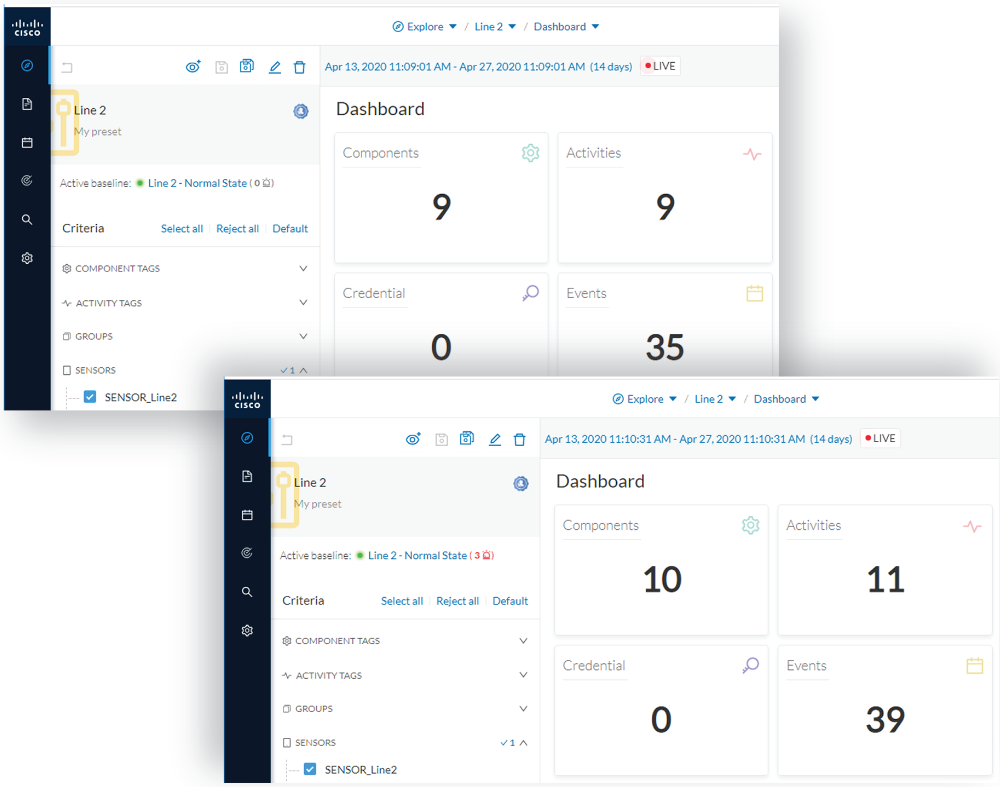
Components: 10	Activities: 11
Variables: 8	Groups: 4

Create Cancel

Description:
All components and activities are
This preset should not be used ar
defined presets would be preferr
accurate findings.

Active baseline: No active baseli

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

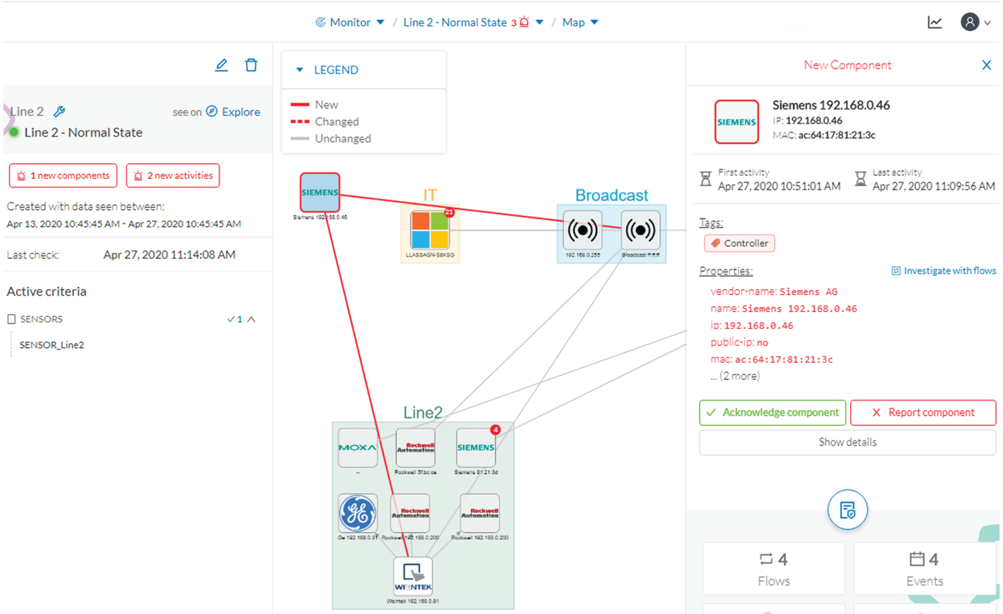


To understand what had happened exactly, we access the baseline in the Monitor mode.

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

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

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



Line 2
Line 2 - Normal State
see on Explore

1 new components
2 new activities

Created with data seen between:
Apr 13, 2020 10:45:45 AM - Apr 27, 2020 10:45:45 AM

Last check: Apr 27, 2020 11:14:08 AM

Active criteria

SENSORS ✓1
SENSOR_Line2

Siemens 192.168.0.46
IP: 192.168.0.46
MAC: ac:64:17:81:21:3c

First activity
Apr 27, 2020 10:51:01 AM

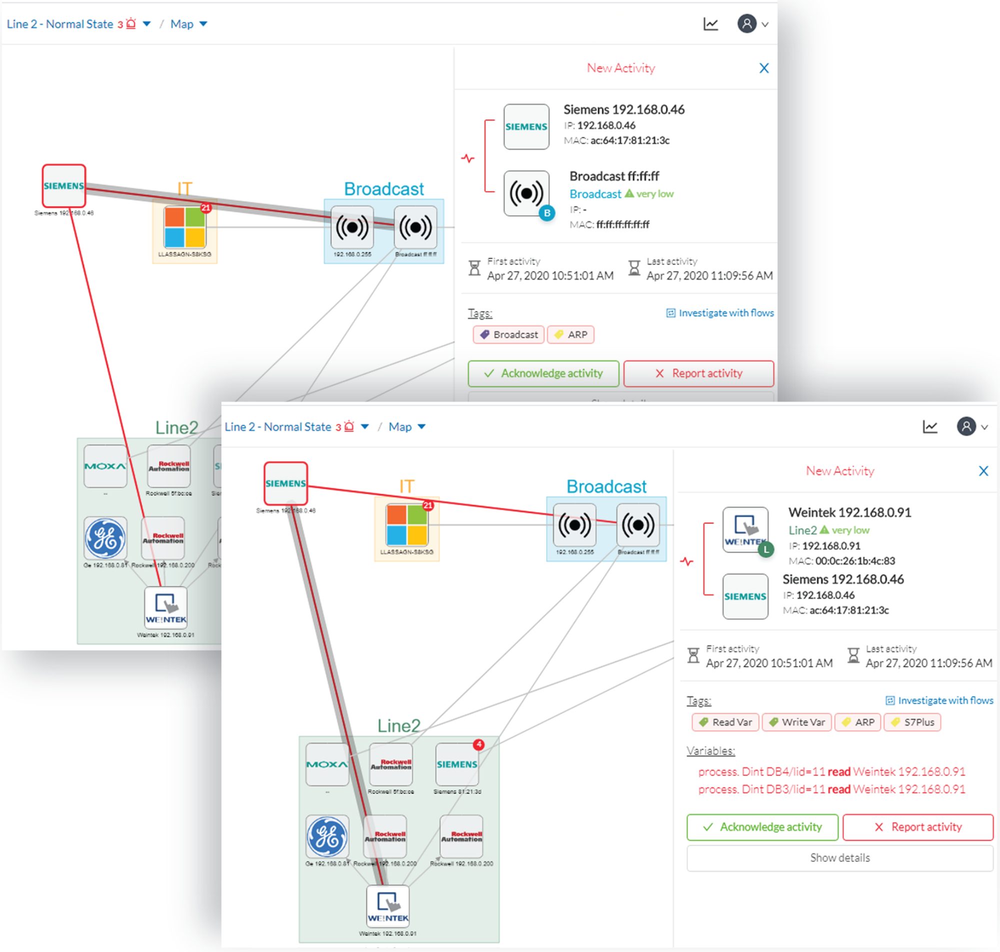
Last activity
Apr 27, 2020 11:09:56 AM

Tags:
Controller

Properties: Investigate with flows

```
vendor-name: Siemens AG
name: Siemens 192.168.0.46
ip: 192.168.0.46
public-ip: no
mac: ac:64:17:81:21:3c
... (2 more)
```

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



New Activity

Siemens 192.168.0.46
IP: 192.168.0.46
MAC: ac:64:17:81:21:3c

Broadcast ff:ff:ff
Broadcast very low
IP: -
MAC: ff:ff:ff:ff:ff:ff

First activity
Apr 27, 2020 10:51:01 AM

Last activity
Apr 27, 2020 11:09:56 AM

Tags: Broadcast, ARP

Investigate with flows

✓ Acknowledge activity
X Report activity

New Activity

Weintek 192.168.0.91
Line2 very low
IP: 192.168.0.91
MAC: 00:0c:26:1b:4c:83

Siemens 192.168.0.46
IP: 192.168.0.46
MAC: ac:64:17:81:21:3c

First activity
Apr 27, 2020 10:51:01 AM

Last activity
Apr 27, 2020 11:09:56 AM

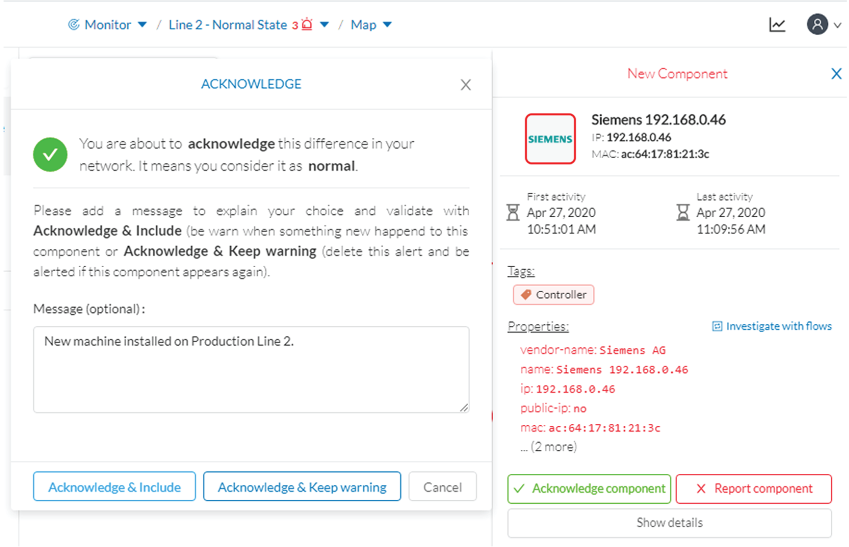
Tags: Read Var, Write Var, ARP, S7Plus

Investigate with flows

Variables:
process. Dint DB4/lid=11 **read** Weintek 192.168.0.91
process. Dint DB3/lid=11 **read** Weintek 192.168.0.91

✓ Acknowledge activity
X Report activity
Show details

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



You are about to **acknowledge** this difference in your network. It means you consider it as **normal**.

Please add a message to explain your choice and validate with **Acknowledge & Include** (be warn when something new happend to this component or **Acknowledge & Keep warning** (delete this alert and be alerted if this component appears again).

Message (optional) :

New machine installed on Production Line 2.

Siemens 192.168.0.46
IP: 192.168.0.46
MAC: ac:64:17:81:21:3c

First activity Apr 27, 2020 10:51:01 AM

Last activity Apr 27, 2020 11:09:56 AM

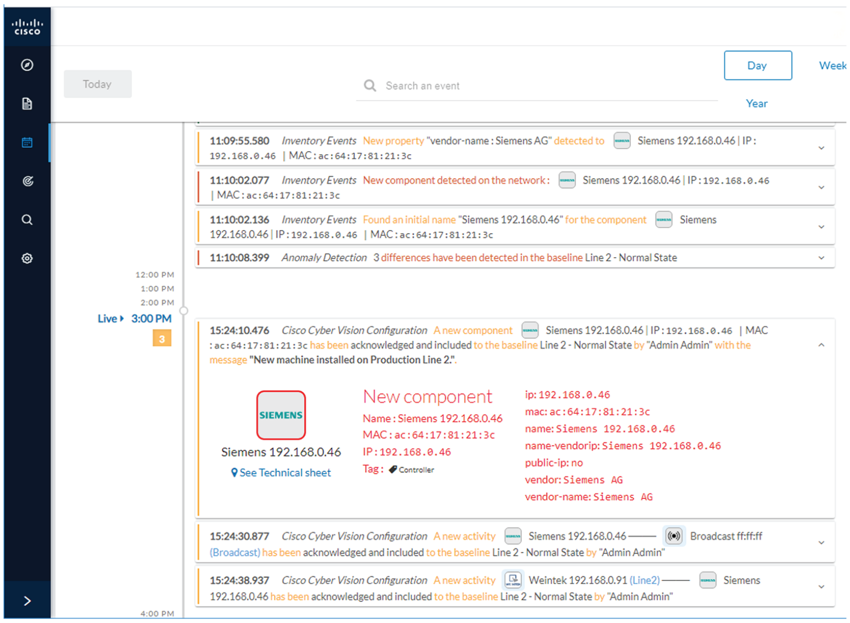
Tags: Controller

Properties:

vendor-name: Siemens AG
name: Siemens 192.168.0.46
ip: 192.168.0.46
public-ip: no
mac: ac:64:17:81:21:3c
... (2 more)

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

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



11:09:55.580 *Inventory Events* New property "vendor-name : Siemens AG" detected to Siemens 192.168.0.46 | IP : 192.168.0.46 | MAC : ac:64:17:81:21:3c

11:10:02.077 *Inventory Events* New component detected on the network : Siemens 192.168.0.46 | IP : 192.168.0.46 | MAC : ac:64:17:81:21:3c

11:10:02.136 *Inventory Events* Found an initial name "Siemens 192.168.0.46" for the component Siemens 192.168.0.46 | IP : 192.168.0.46 | MAC : ac:64:17:81:21:3c

11:10:08.399 *Anomaly Detection* 3 differences have been detected in the baseline Line 2 - Normal State

15:24:10.476 *Cisco Cyber Vision Configuration* A new component Siemens 192.168.0.46 | IP : 192.168.0.46 | MAC : ac:64:17:81:21:3c has been acknowledged and included to the baseline Line 2 - Normal State by "Admin Admin" with the message "New machine installed on Production Line 2.".

Siemens 192.168.0.46
See Technical sheet

New component
Name : Siemens 192.168.0.46
MAC : ac:64:17:81:21:3c
IP : 192.168.0.46
Tag : Controller

ip: 192.168.0.46
mac: ac:64:17:81:21:3c
name: Siemens 192.168.0.46
name-vendorip: Siemens 192.168.0.46
public-ip: no
vendor: Siemens AG
vendor-name: Siemens AG

15:24:30.877 *Cisco Cyber Vision Configuration* A new activity Siemens 192.168.0.46 —— Broadcast ff:ff:ff (Broadcast) has been acknowledged and included to the baseline Line 2 - Normal State by "Admin Admin"

15:24:38.937 *Cisco Cyber Vision Configuration* A new activity Weintek 192.168.0.91 (Line2) —— Siemens 192.168.0.46 has been acknowledged and included to the baseline Line 2 - Normal State by "Admin Admin"

Tracking sensitive assets properties

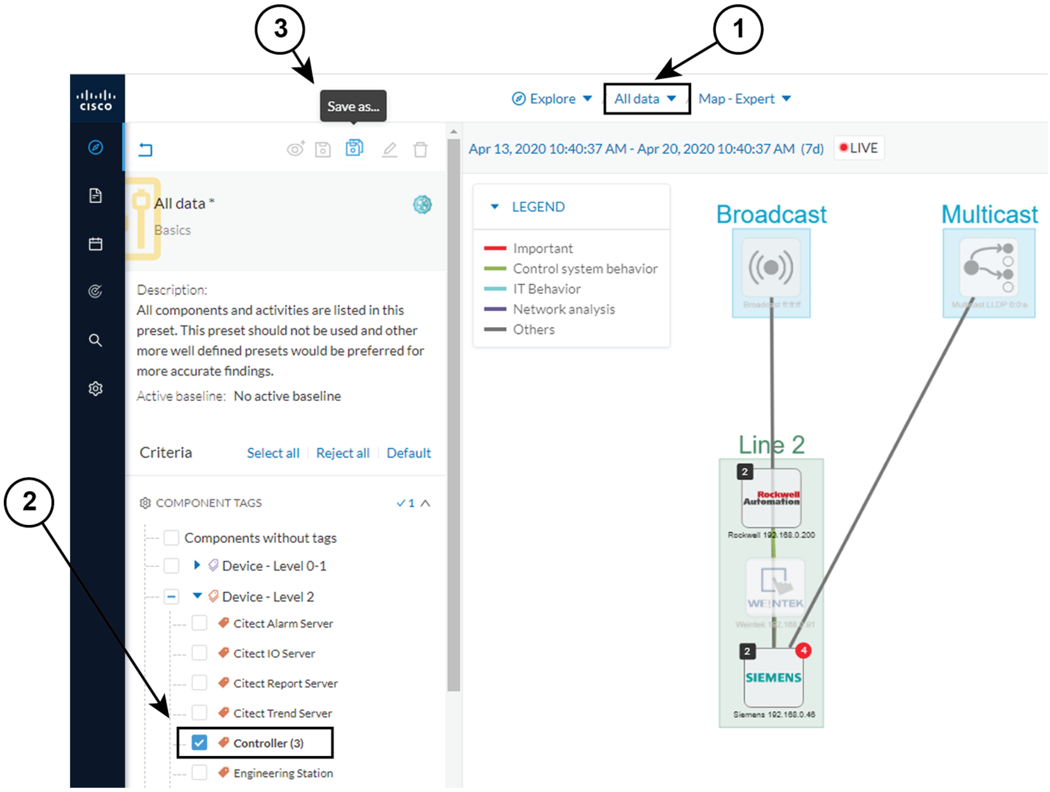
To ensure a network's security, its critical assets need to be monitored closely. Usually, critical assets are controllers which ensure the plant's operation. To monitor them, we're going to check its properties. The properties to keep an eye on are programs and firmware versions changes that might cause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

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

Key Differences: New properties or changed properties on components

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

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

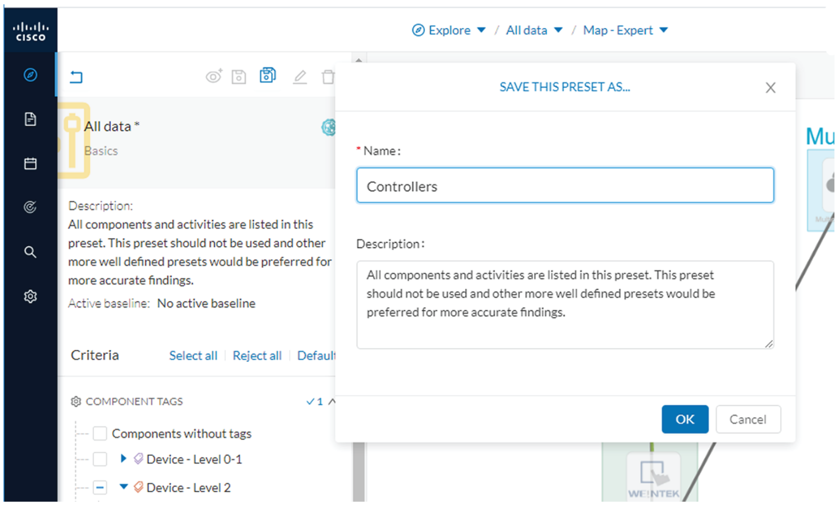


Apr 13, 2020 10:40:37 AM - Apr 20, 2020 10:40:37 AM (7d) ● LIVE

Description:
All components and activities are listed in this preset. This preset should not be used and other more well defined presets would be preferred for more accurate findings.

Active baseline: No active baseline

- □ Components without tags
- □ Device - Level 0-1
- − Device - Level 2
  - □ Citect Alarm Server
  - □ Citect IO Server
  - □ Citect Report Server
  - □ Citect Trend Server
  - ☑ Controller (3)
  - □ Engineering Station



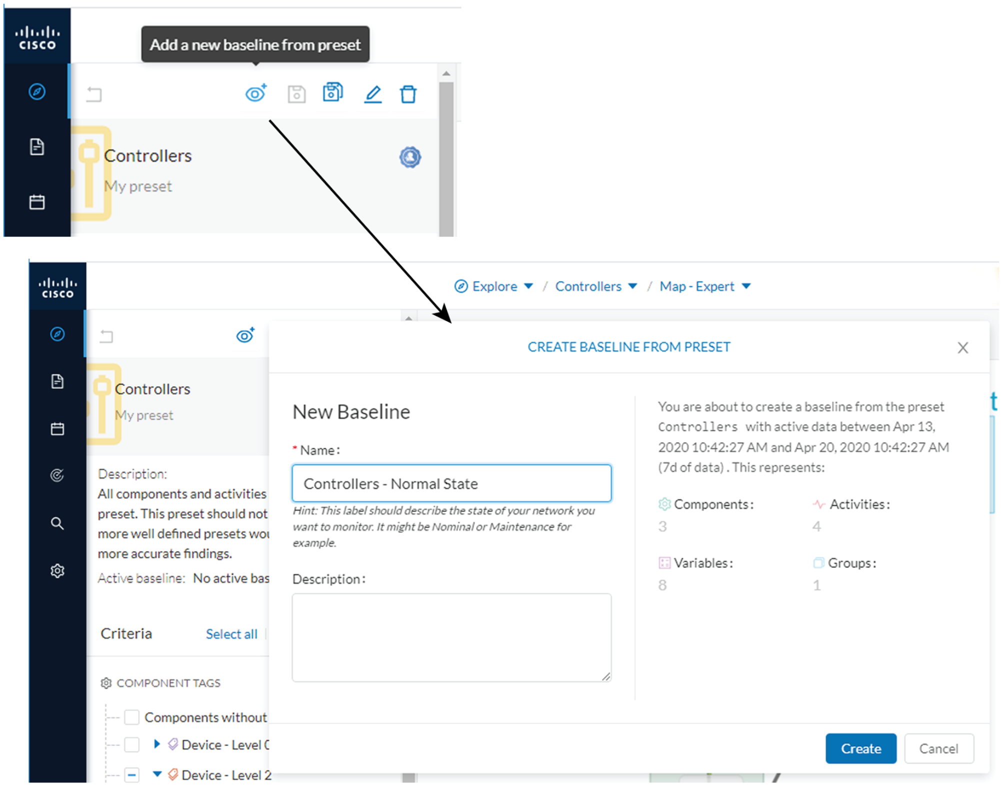
SAVE THIS PRESET AS...

* Name: Controllers

Description: All components and activities are listed in this preset. This preset should not be used and other more well defined presets would be preferred for more accurate findings.

Active baseline: No active baseline

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



CREATE BASELINE FROM PRESET

New Baseline

* Name: Controllers - Normal State

Hint: This label should describe the state of your network you want to monitor. It might be Nominal or Maintenance for example.

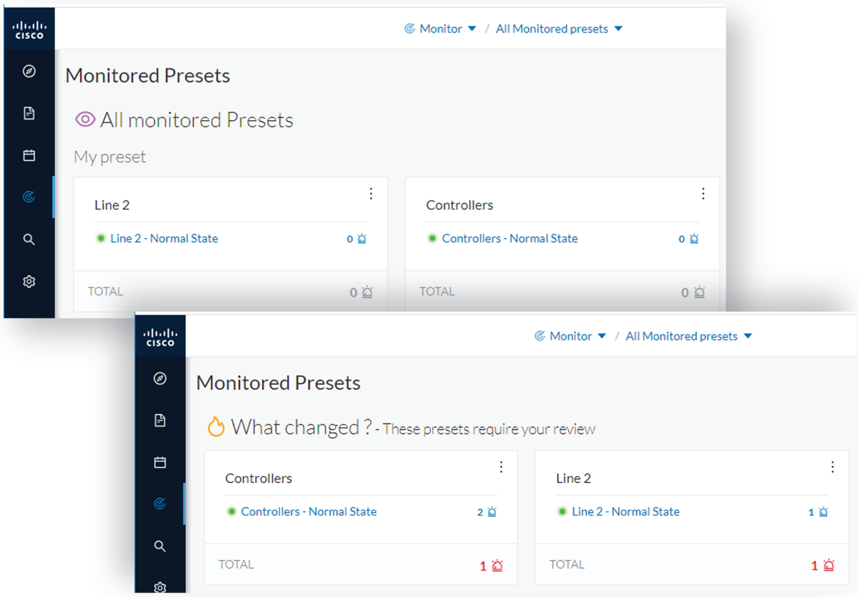
Description:

You are about to create a baseline from the preset `Controllers` with active data between Apr 13, 2020 10:42:27 AM and Apr 20, 2020 10:42:27 AM (7d of data) . This represents:

Components: 3	Activities: 4
Variables: 8	Groups: 1

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

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



Monitor / All Monitored presets

Monitored Presets

All monitored Presets

My preset

Line 2		
Line 2 - Normal State	0	
TOTAL	0	
Controllers		
Controllers - Normal State	0	
TOTAL	0	

Monitor / All Monitored presets

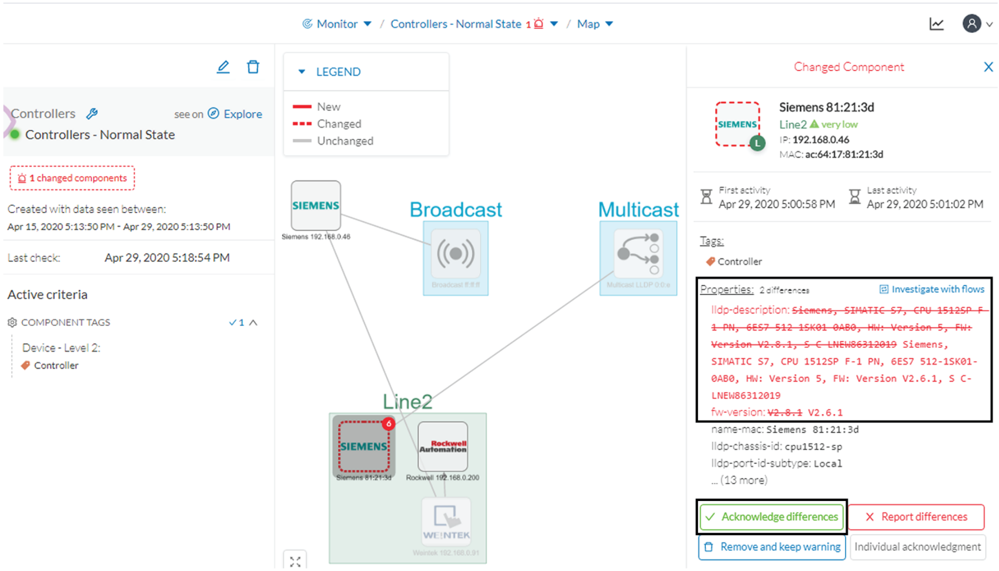
Monitored Presets

What changed ? - These presets require your review

Controllers		
Controllers - Normal State	2	
TOTAL	1	
Line 2		
Line 2 - Normal State	1	
TOTAL	1	

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

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



Monitor / Controllers - Normal State 1 / Map

Controllers see on Explore
Controllers - Normal State

1 changed components

Created with data seen between:
Apr 15, 2020 5:13:50 PM - Apr 29, 2020 5:13:50 PM

Last check: Apr 29, 2020 5:18:54 PM

Active criteria

COMPONENT TAGS ✓1

Device - Level 2:
Controller

Changed Component

Siemens 81:21:3d
Line2 very low
IP: 192.168.0.46
MAC: ac:64:17:81:21:3d

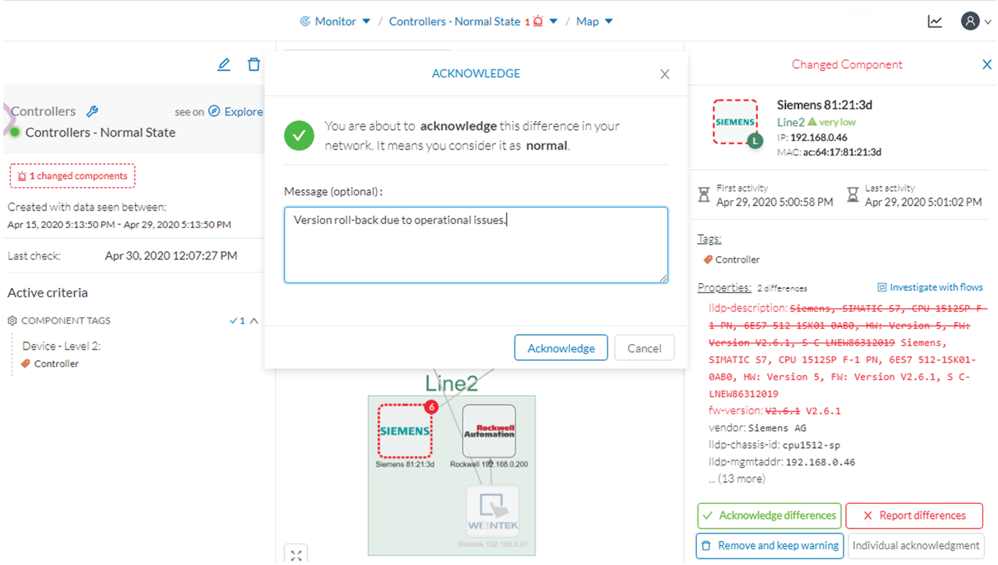
First activity Apr 29, 2020 5:00:58 PM
Last activity Apr 29, 2020 5:01:02 PM

Tags:
Controller

Properties: 2 differences — Investigate with flows

lldp-description: ~~Siemens, SIMATIC S7, CPU 1512SP F-1 PN, 6ES7 512-1SK01-0AB0, HW: Version 5, FW: Version V2.8.1, S C-LNEW86312019~~ Siemens, SIMATIC S7, CPU 1512SP F-1 PN, 6ES7 512-1SK01-0AB0, HW: Version 5, FW: Version V2.6.1, S C-LNEW86312019
fw-version: ~~V2.8.1~~ V2.6.1
name-mac: Siemens 81:21:3d
lldp-chassis-id: cpu1512-sp
lldp-port-id-subtype: Local
... (13 more)

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



Created with data seen between:
Apr 15, 2020 5:13:50 PM - Apr 29, 2020 5:13:50 PM

Last check: Apr 30, 2020 12:07:27 PM

You are about to **acknowledge** this difference in your network. It means you consider it as **normal**.

Message (optional):

Version roll-back due to operational issues.

Siemens 81:21:3d
Line2 very low
IP: 192.168.0.46
MAC: ac:64:17:81:21:3d

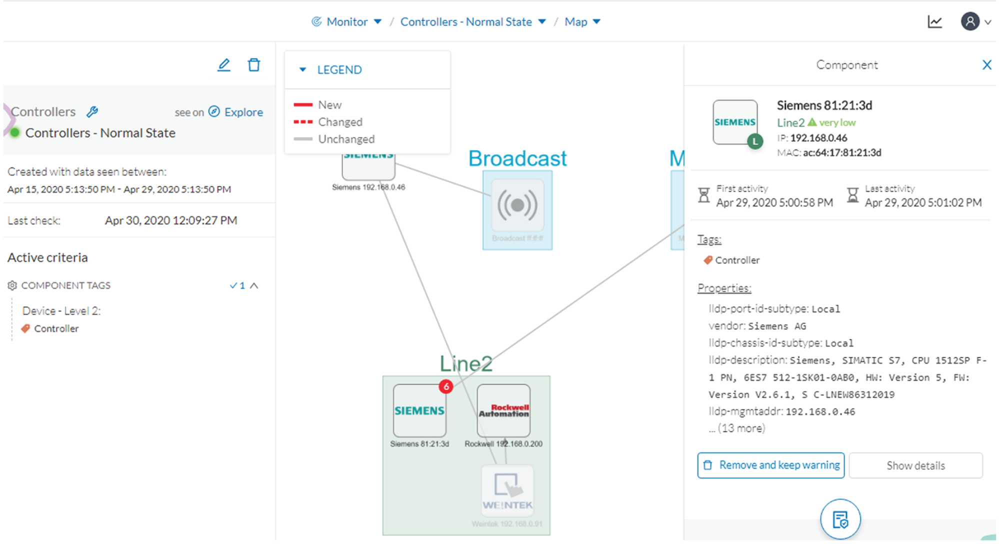
First activity Apr 29, 2020 5:00:58 PM
Last activity Apr 29, 2020 5:01:02 PM

Tags:
Controller

Properties: 2 differences

lldp-description: ~~Siemens, SIMATIC S7, CPU 1512SP F-1 PN, 6ES7 512 1SK01 0AB0, HW: Version 5, FW: Version V2.6.1, S C LNEW86312019~~ Siemens, SIMATIC S7, CPU 1512SP F-1 PN, 6ES7 512-1SK01-0AB0, HW: Version 5, FW: Version V2.6.1, S C-LNEW86312019
fw-version: ~~V2.6.1~~ V2.6.1
vendor: Siemens AG
lldp-chassis-id: cpu1512-sp
lldp-mgmtaddr: 192.168.0.46
... (13 more)

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



Created with data seen between:
Apr 15, 2020 5:13:50 PM - Apr 29, 2020 5:13:50 PM

Last check: Apr 30, 2020 12:09:27 PM

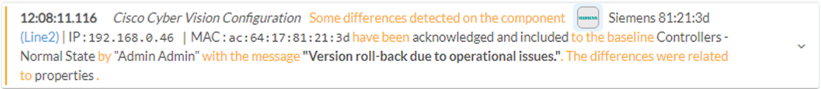
Siemens 81:21:3d
Line2 very low
IP: 192.168.0.46
MAC: ac:64:17:81:21:3d

First activity Apr 29, 2020 5:00:58 PM
Last activity Apr 29, 2020 5:01:02 PM

Tags:
Controller

Properties:
lldp-port-id-subtype: Local
vendor: Siemens AG
lldp-chassis-id-subtype: Local
lldp-description: Siemens, SIMATIC S7, CPU 1512SP F-1 PN, 6ES7 512-1SK01-0AB0, HW: Version 5, FW: Version V2.6.1, S C-LNEW86312019
lldp-mgmtaddr: 192.168.0.46
... (13 more)

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



12:08:11.116 *Cisco Cyber Vision Configuration* Some differences detected on the component Siemens 81:21:3d (Line2) | IP:192.168.0.46 | MAC:ac:64:17:81:21:3d have been acknowledged and included to the baseline Controllers - Normal State by "Admin Admin" with the message **"Version roll-back due to operational issues."**. The differences were related to properties .

Detect changes that impact availability and integrity

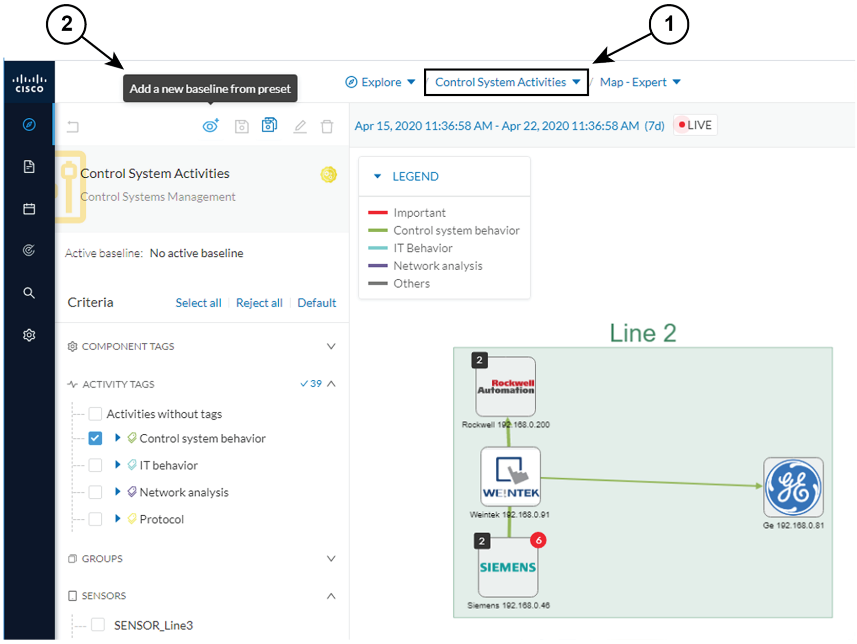
First evidence that someone might have hacked your industrial control system and is trying to disrupt your industrial processes are Stop CPU orders or new programs sent into a Controller's memory. A station that starts to send such content inside a network must be detected as soon as possible. It is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

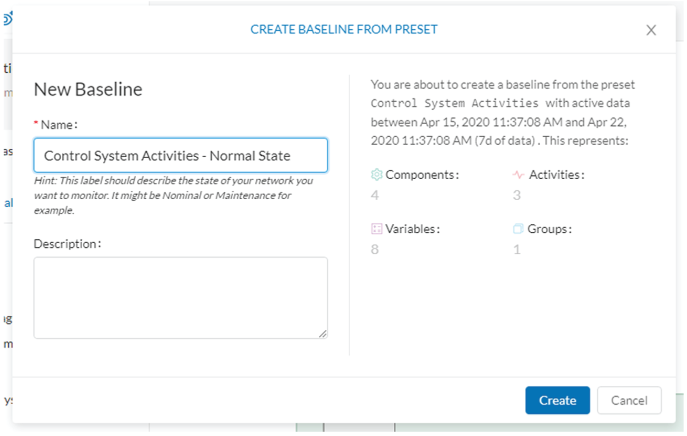
This can be done in Cisco Cyber Vision by using the Control System Activities preset, which is a default preset and will check all activity tags categorized as Control System Behavior and consequently all related components. Key differences in such use case are new or changed activities. Moreover, components'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

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

Key Differences: New or changed activities

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





CREATE BASELINE FROM PRESET

New Baseline

* Name: Control System Activities - Normal State

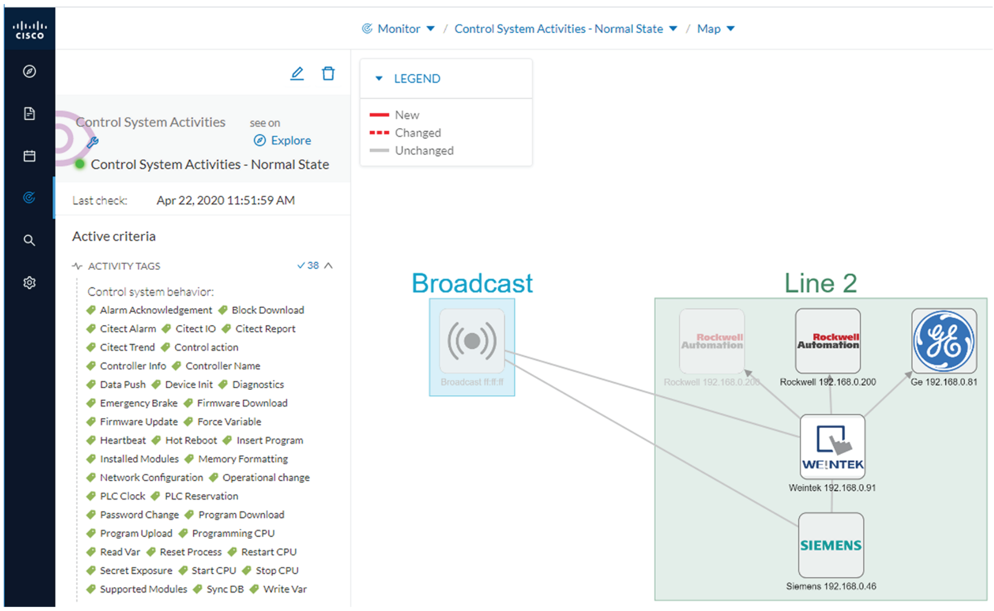
Hint: This label should describe the state of your network you want to monitor. It might be Nominal or Maintenance for example.

Description:

You are about to create a baseline from the preset `Control System Activities` with active data between Apr 15, 2020 11:37:08 AM and Apr 22, 2020 11:37:08 AM (7d of data). This represents:

Components: 4
Activities: 3
Variables: 8
Groups: 1

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



Monitor / Control System Activities - Normal State / Map

Control System Activities — see on Explore

Control System Activities - Normal State

Last check: Apr 22, 2020 11:51:59 AM

Active criteria

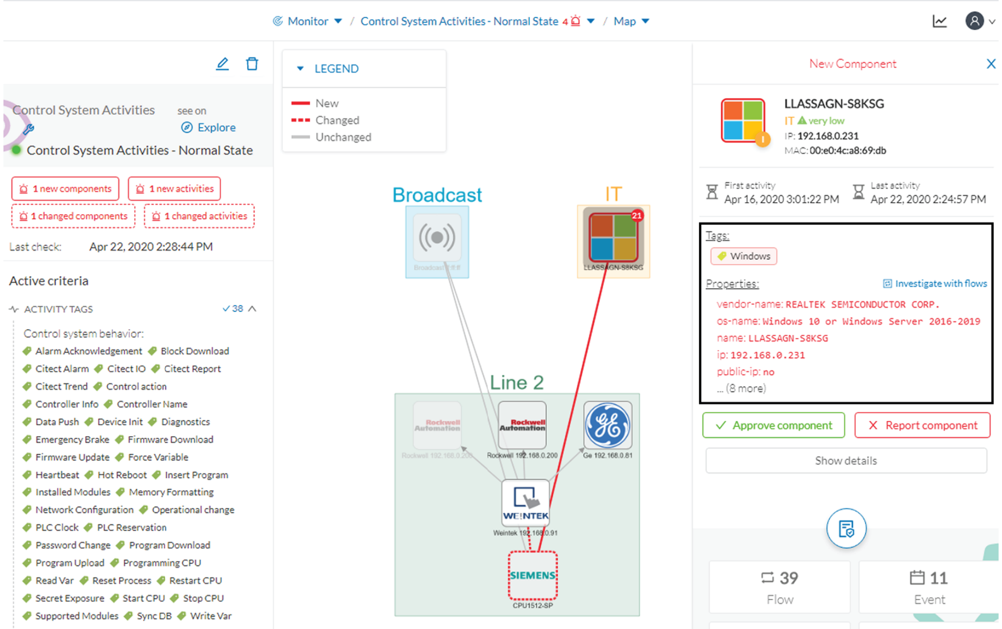
ACTIVITY TAGS ✓38

Control system behavior:
Alarm Acknowledgement, Block Download, Citect Alarm, Citect IO, Citect Report, Citect Trend, Control action, Controller Info, Controller Name, Data Push, Device Init, Diagnostics, Emergency Brake, Firmware Download, Firmware Update, Force Variable, Heartbeat, Hot Reboot, Insert Program, Installed Modules, Memory Formatting, Network Configuration, Operational change, PLC Clock, PLC Reservation, Password Change, Program Download, Program Upload, Programming CPU, Read Var, Reset Process, Restart CPU, Secret Exposure, Start CPU, Stop CPU, Supported Modules, Sync DB, Write Var

LEGEND
- New
- Changed
- Unchanged

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

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



Last check: Apr 22, 2020 2:28:44 PM

New Component

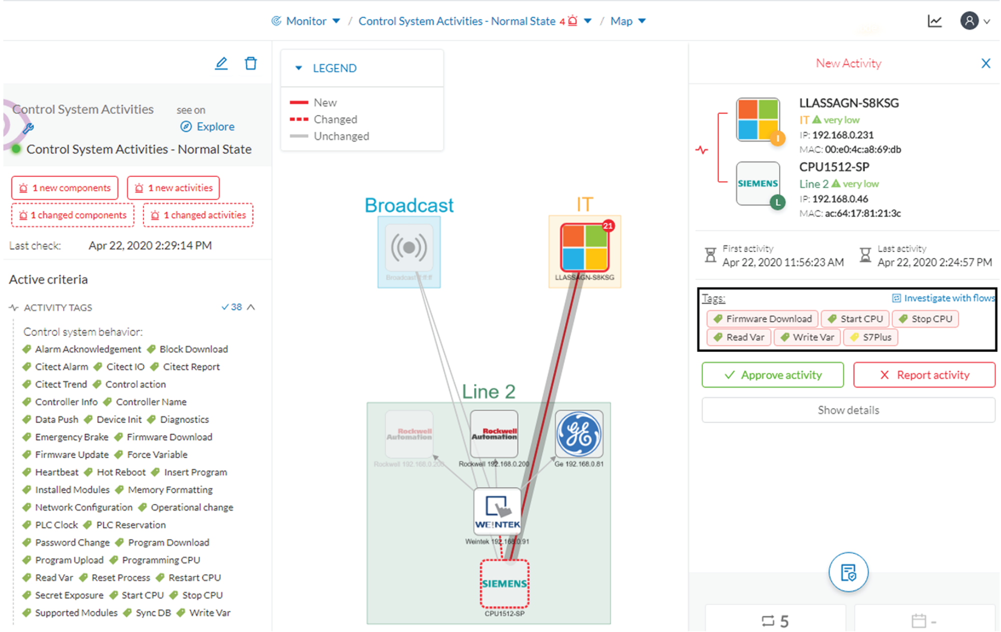
LLASSAGN-S8KSG
IT very low
IP: 192.168.0.231
MAC: 00:e0:4c:a8:69:db

First activity Apr 16, 2020 3:01:22 PM
Last activity Apr 22, 2020 2:24:57 PM

Tags:
Windows

Properties:
vendor-name: REALTEK SEMICONDUCTOR CORP.
os-name: Windows 10 or Windows Server 2016-2019
name: LLASSAGN-S8KSG
ip: 192.168.0.231
public-ip: no
... (8 more)

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



Last check: Apr 22, 2020 2:29:14 PM

New Activity

LLASSAGN-S8KSG
IT very low
IP: 192.168.0.231
MAC: 00:e0:4c:a8:69:db

CPU1512-SP
Line 2 very low
IP: 192.168.0.46
MAC: ac:64:17:81:21:3c

First activity Apr 22, 2020 11:56:23 AM
Last activity Apr 22, 2020 2:24:57 PM

Tags:
Firmware Download
Start CPU
Stop CPU
Read Var
Write Var
S7Plus

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

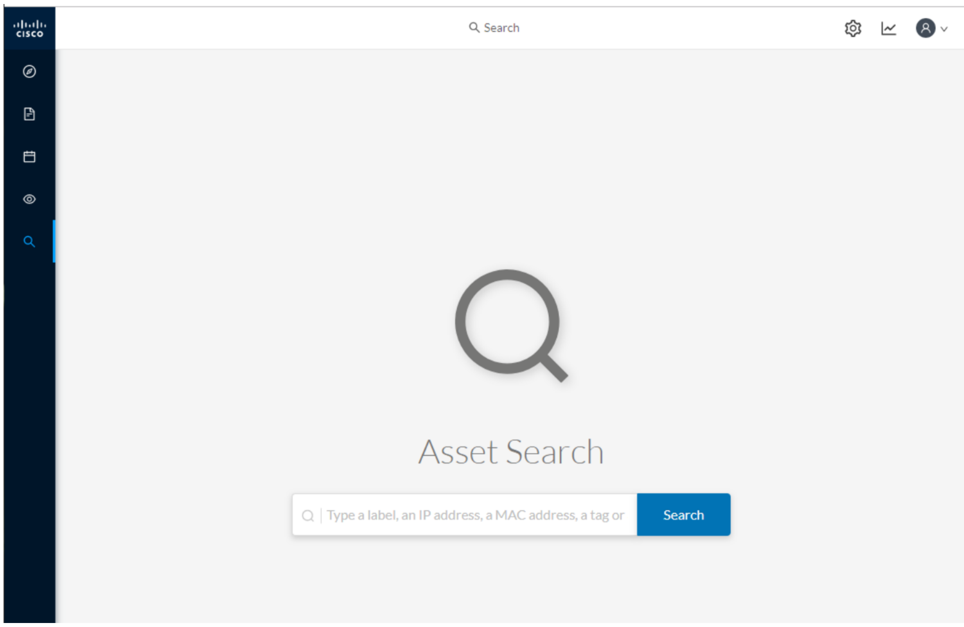
CHAPTER 24

Search

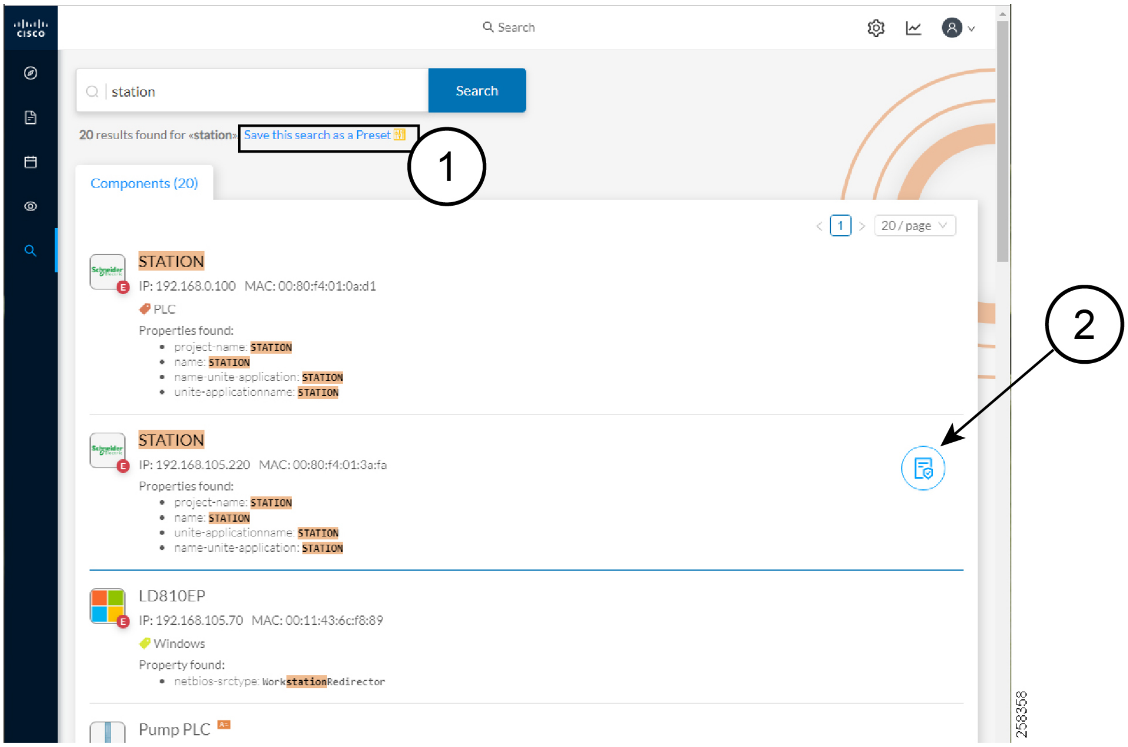
Search

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:



Search

station | Search

20 results found for «station» Save this search as a Preset

Components (20)

1 | 20 / page

STATION
IP: 192.168.0.100 MAC: 00:80:f4:01:0a:d1
PLC
Properties found:
- project-name: STATION
- name: STATION
- name-unite-application: STATION
- unite-applicationname: STATION

STATION
IP: 192.168.105.220 MAC: 00:80:f4:01:3a:fa
Properties found:
- project-name: STATION
- name: STATION
- unite-applicationname: STATION
- name-unite-application: STATION

LD810EP
IP: 192.168.105.70 MAC: 00:11:43:6c:f8:89
Windows
Property found:
- netbios-srctype: WorkstationRedirector

Pump PLC

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

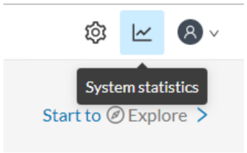
It is possible to create a preset out of your research results **(1)**. Presets created out of results will automatically update as new data are detected on the network.

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.

CHAPTER 25

System statistics

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

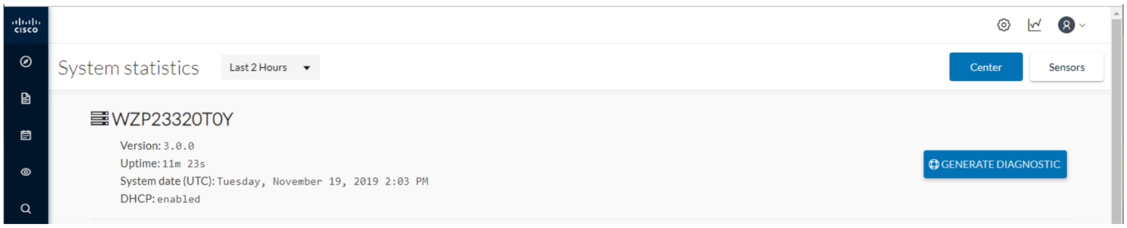


- Center, on page 123
- Sensors, on page 126

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.



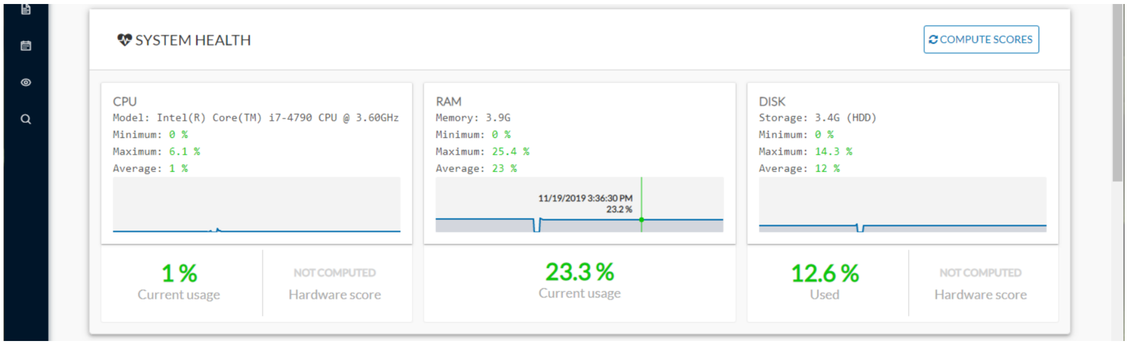
WZP23320T0Y

Version: 3.0.0
Uptime: 11m 23s
System date (UTC): Tuesday, November 19, 2019 2:03 PM
DHCP: enabled

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:


SYSTEM HEALTH

COMPUTE SCORES

CPU
Model: Intel(R) Core(TM) i7-4790 CPU @ 3.60GHz
Minimum: 0 %
Maximum: 6.1 %
Average: 1 %

1 % Current usage

NOT COMPUTED Hardware score

RAM
Memory: 3.9G
Minimum: 0 %
Maximum: 25.4 %
Average: 23 %

11/19/2019 3:36:30 PM
23.2 %

23.3 % Current usage

DISK
Storage: 3.4G (HDD)
Minimum: 0 %
Maximum: 14.3 %
Average: 12 %

12.6 % Used

NOT COMPUTED Hardware score

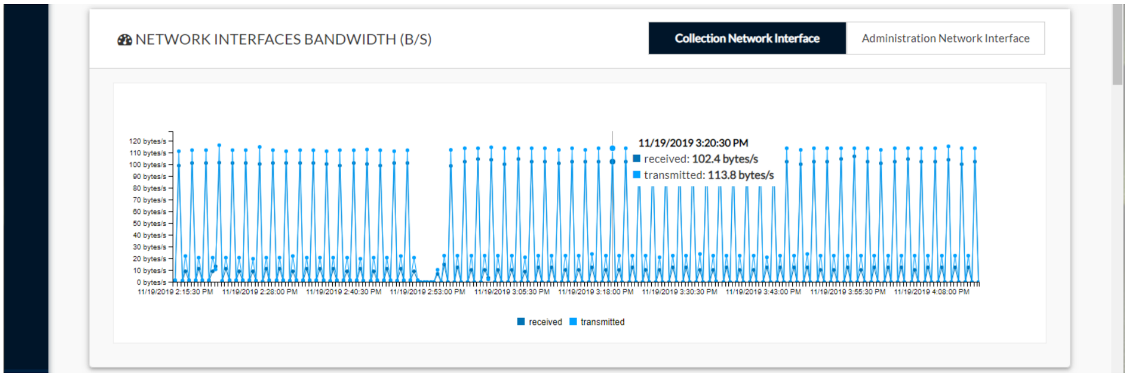
The system health gives you the state of the Center CPU, RAM and disk usage.

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:


NETWORK INTERFACES BANDWIDTH (B/S)

Collection Network Interface

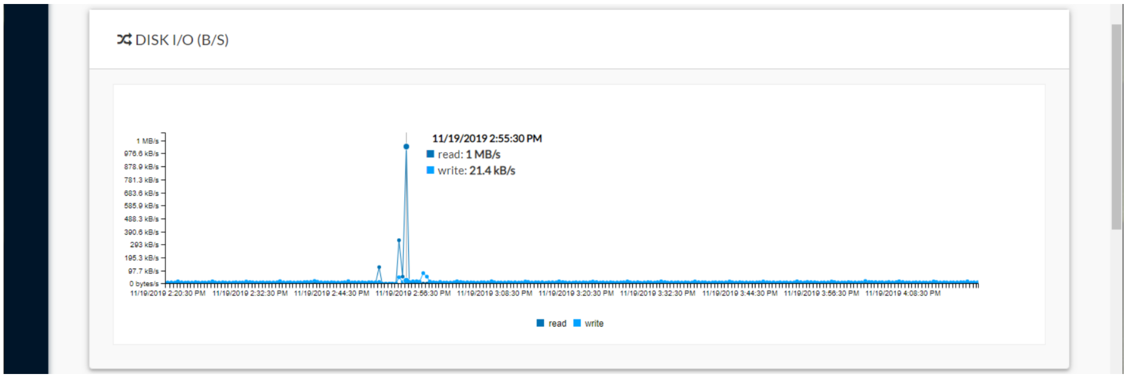
Administration Network Interface

11/19/2019 3:20:30 PM
received: 102.4 bytes/s
transmitted: 113.8 bytes/s

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

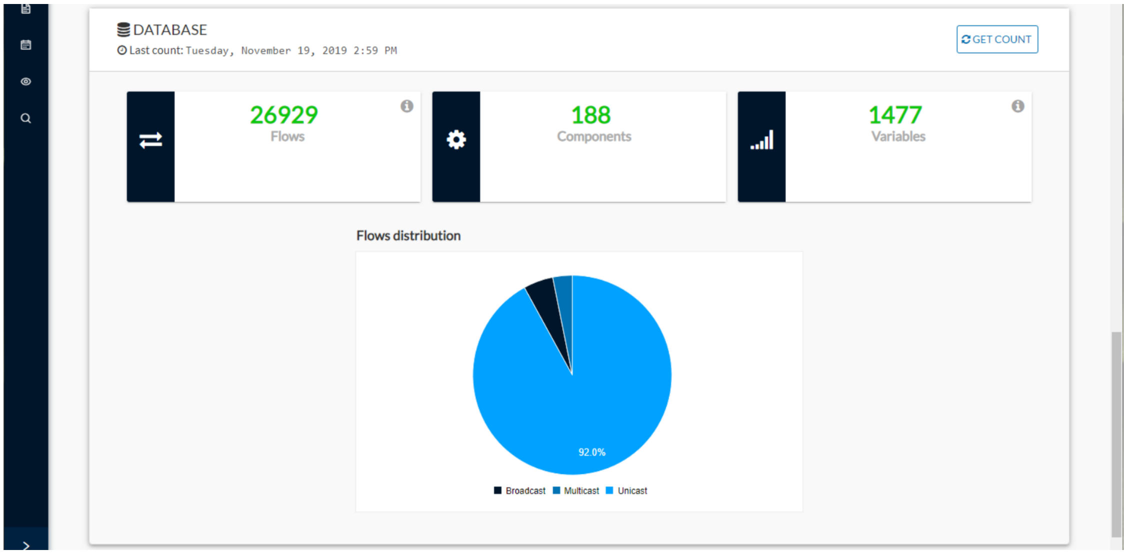
For example, the Collection network interface activity lets you see the amount of data exchanged between the Center and the sensors.

Disk I/O:



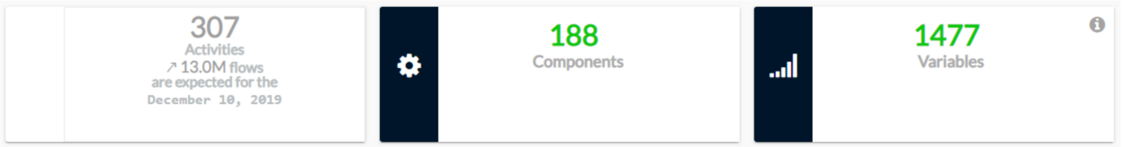
The line chart represents the Center hard disk usage with the number of bytes read and written per second.

Database:

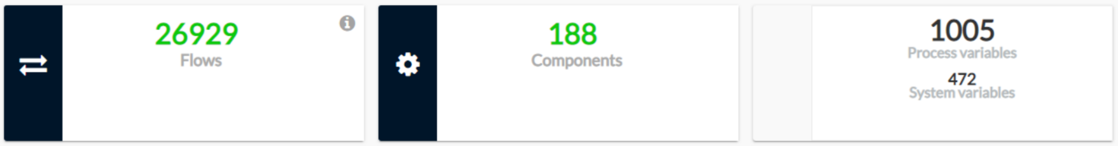


This section describes the database state by showing cards with the number of flows, components and variables that have been detected by Cisco Cyber Vision. Flows distribution is shown in a pie chart.

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.

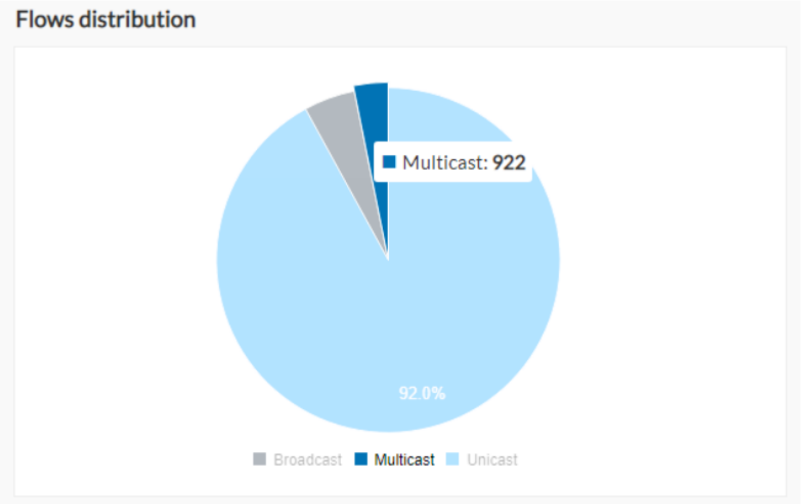


The flows card indicates the total number of flows (i.e. broadcast, multicast and unicast which are stored in the database) detected by Cisco Cyber Vision. If you mouse over the card, you will get the number of activities and the flows evolution tendency. This information enables you to anticipate how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

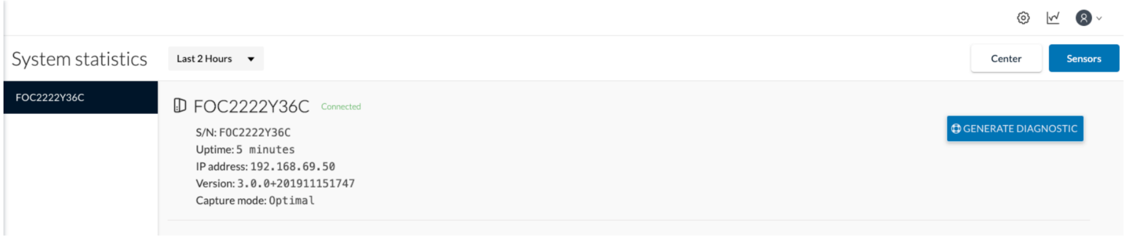


The flows distribution pie chart indicates the distribution of broadcast, multicast and unicast flows stored in the database. Mouse over the chart to see the absolute number of flows per flow type.

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.



FOC2222Y36C Connected

S/N: FOC2222Y36C
Uptime: 5 minutes
IP address: 192.168.69.50
Version: 3.0.0+201911151747
Capture mode: Optimal

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.

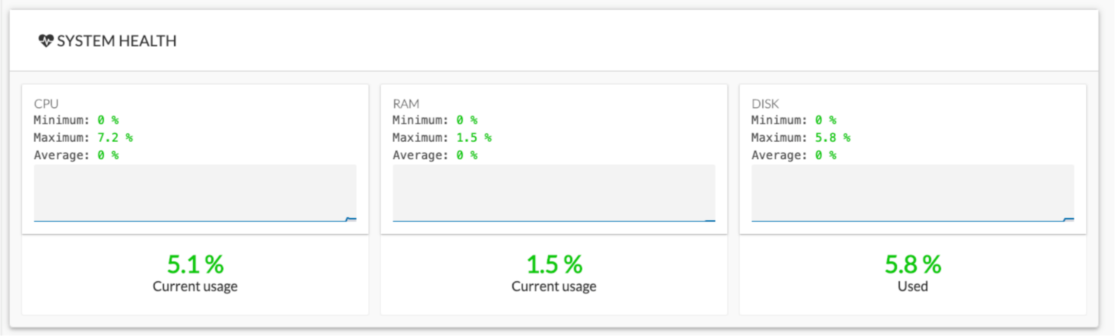
On top of the sensors statistics view you will find general information about the sensor: its status (i.e. Connected), its serial number, its IP and MAC addresses, its firmware version, the capture mode set and the time it has been operating (i.e. uptime).

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.



CPU
Minimum: 0 %
Maximum: 7.2 %
Average: 0 %

5.1 %
Current usage

RAM
Minimum: 0 %
Maximum: 1.5 %
Average: 0 %

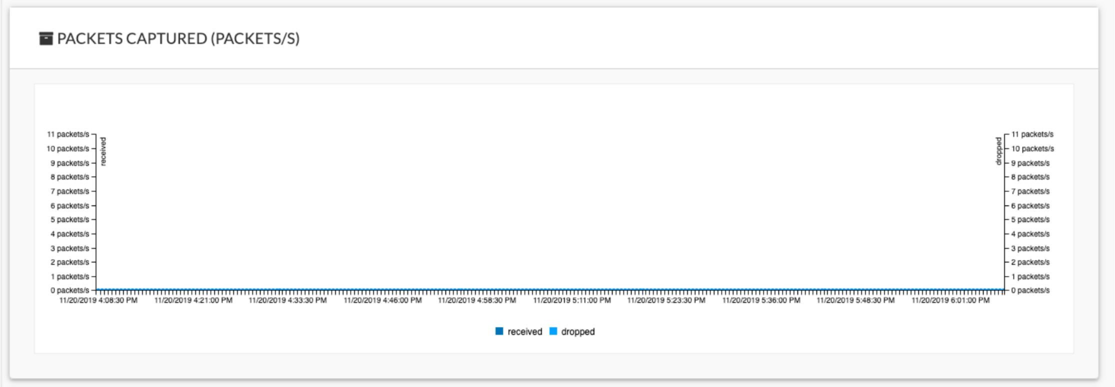
1.5 %
Current usage

DISK
Minimum: 0 %
Maximum: 5.8 %
Average: 0 %

5.8 %
Used

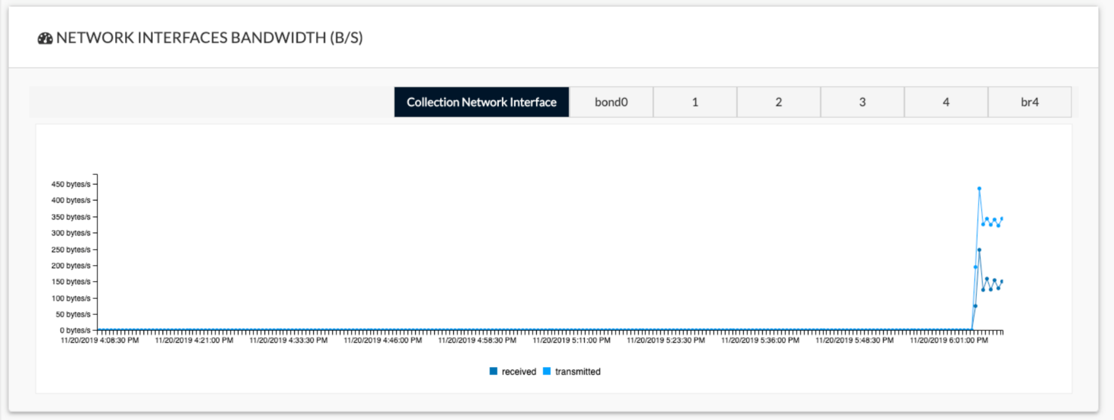
Below, you have the percentage of the system current usage. There is also an indicative hardware score which is useful to Cisco product support.

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:

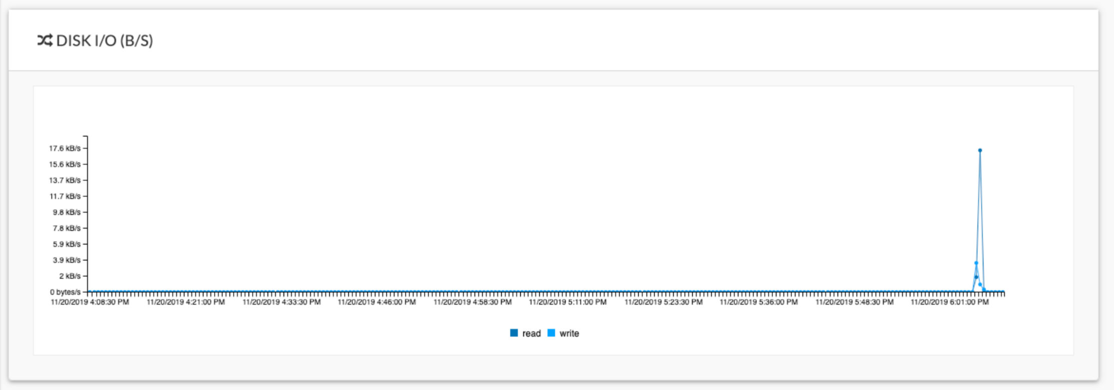


The line charts represent the Collection and the Industrial network interfaces bandwidth with the number of bytes received and sent by the Center per second.

- 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:



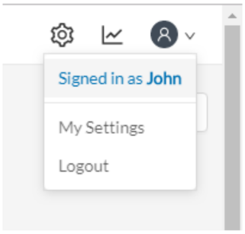
The line chart represents the sensor hard disk usage with the number of bytes read and written per second.

CHAPTER 26

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.