Filter

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.

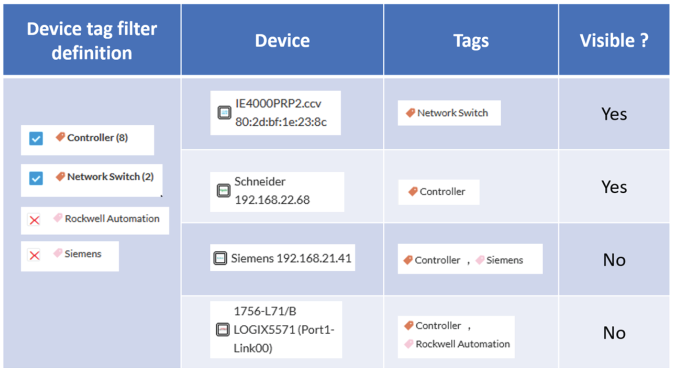
If filters are defined by several categories, the resulting dataset is the intersect of the selections for each category.

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



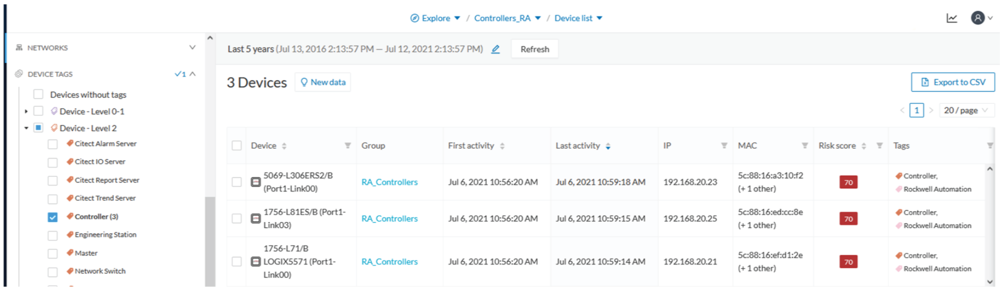
Device tag filter definition	Device	Tags	Visible ?
☑ Controller (8) ☑ Network Switch (2) ☒ Rockwell Automation ☒ Siemens	IE4000PRP2.ccv 80:2d:bf:1e:23:8c	Network Switch	Yes
	Schneider 192.168.22.68	Controller	Yes
	Siemens 192.168.21.41	Controller , Siemens	No
	1756-L71/B LOGIX5571 (Port1-Link00)	Controller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



□ Devices 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
□ Master
□ Network Switch

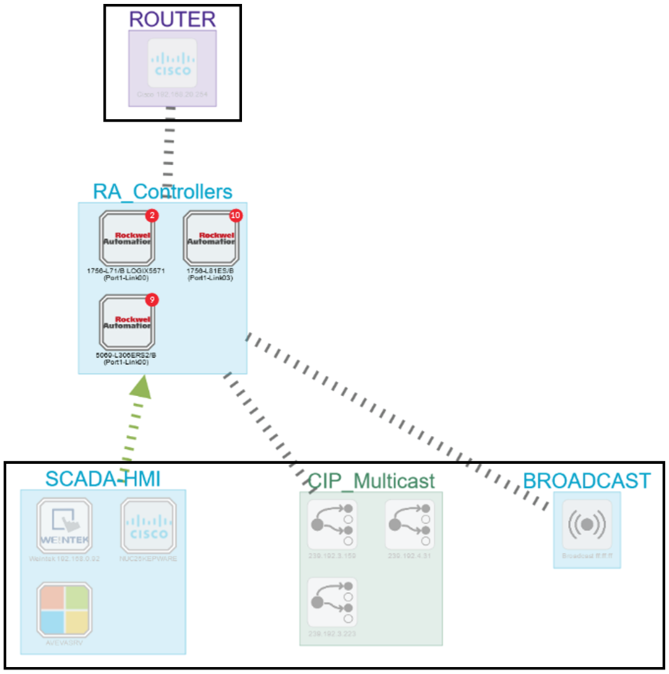
Last 5 years (Jul 13, 2016 2:13:57 PM — Jul 12, 2021 2:13:57 PM)

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:

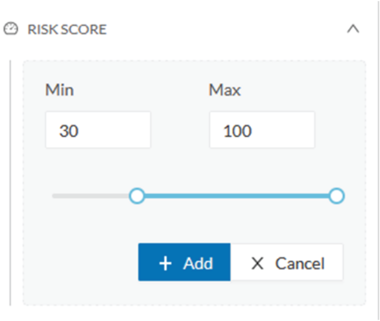
Device tag filter, example of Controllers - map


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

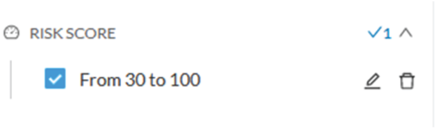


RISK SCORE

Min: 30

Max: 100

Risk score – inclusive filter



RISK SCORE ✓1

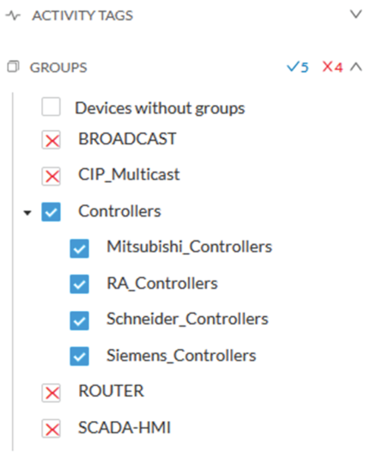
☑ From 30 to 100

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



ACTIVITY TAGS

GROUPS ✓5 ✗4

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

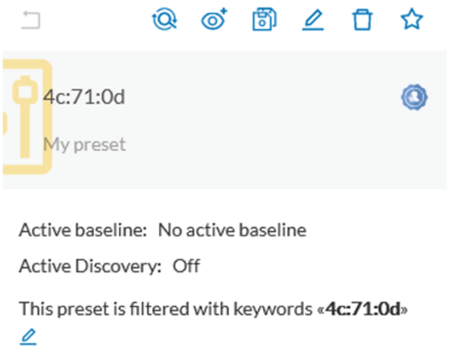
In the example above, only the devices belonging to the selected groups will be selected.

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

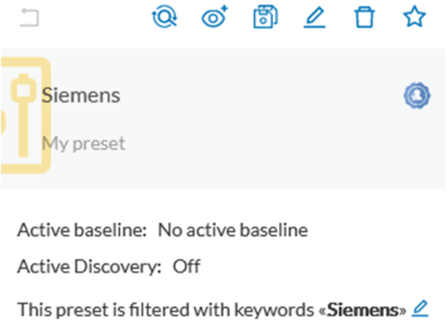
My preset

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

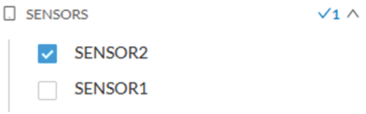
Active Discovery: Off

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

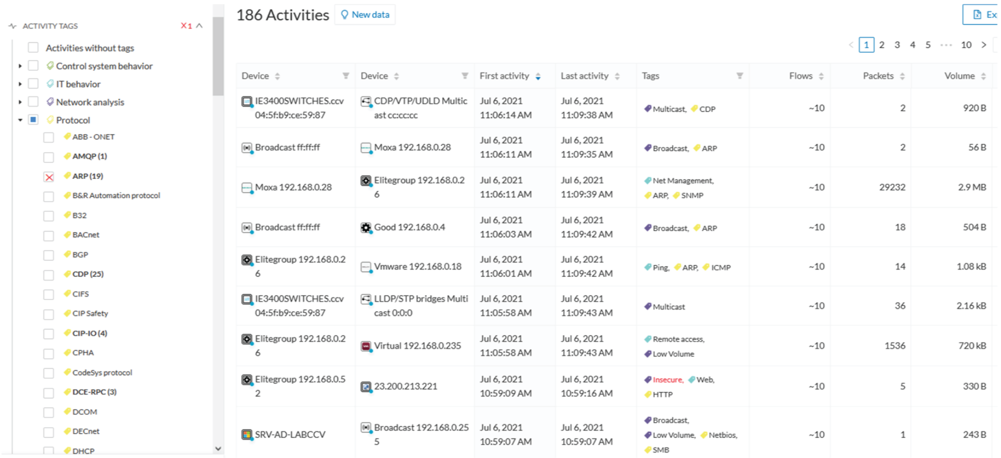
- ☑ SENSOR2
- □ SENSOR1

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

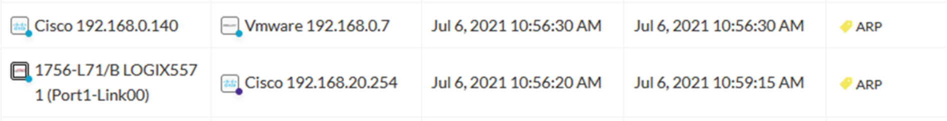
- □ Activities without tags
- □ Control system behavior
- □ IT behavior
- □ Network analysis
- ■ Protocol
  - □ ABB - ONET
  - □ AMQP (1)
  - ☒ ARP (19)
  - □ B&R Automation protocol
  - □ B32
  - □ BACnet
  - □ BGP
  - □ CDP (25)
  - □ CIFS
  - □ CIP Safety
  - □ CIP-IO (4)
  - □ CPHA
  - □ CodeSys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

186 Activities New data

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:

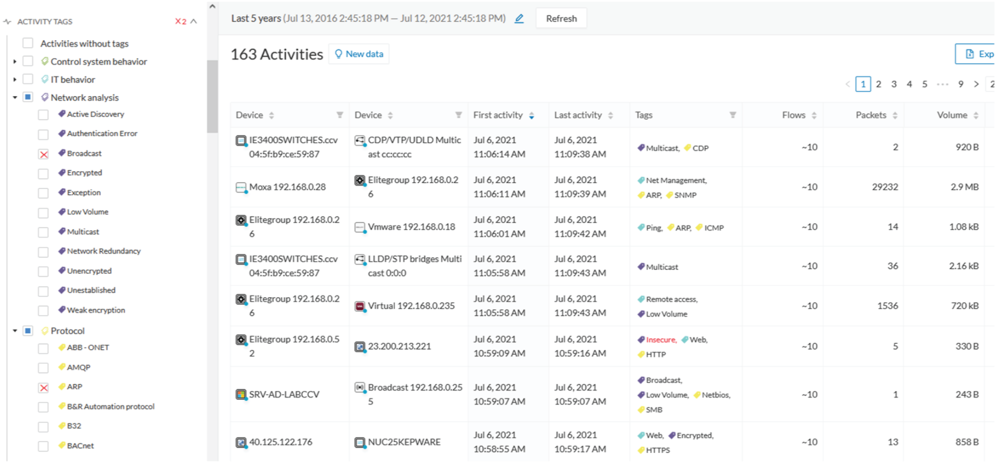
filter 2



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 Exp

< 1 2 3 4 5 ··· 9 > 2

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

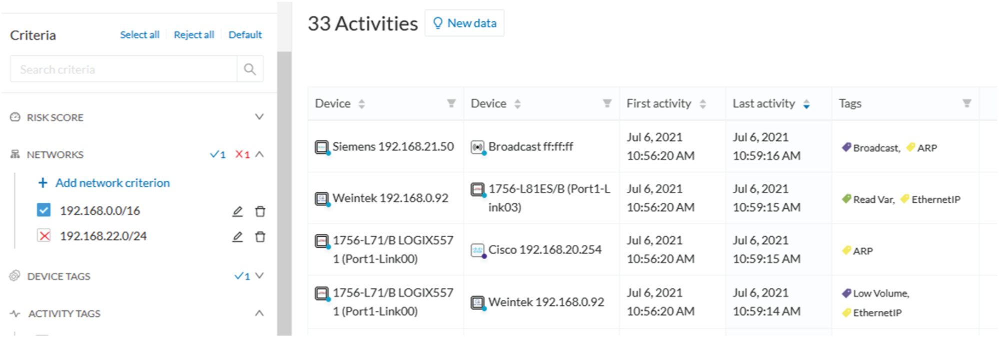
Networks

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



☑ 192.168.0.0/16

☒ 192.168.22.0/24

33 Activities

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.