Release Notes for Cisco Cyber Vision Release 4.0.0

For users upgrading to 4.0.0 from previous versions, please carefully read the Cisco Cyber Vision 4.0.0 update procedure.

Compatible device list

Center	Description
VMware ESXi OVA center	VMware ESXi 6.x or later
Windows Server Hyper-V VHDX center	Microsoft Windows Server Hyper-V version 2016 or later
Cisco UCS C220 M5 CV-CNTR-M5S5	Cyber Vision Center hardware appliance (Cisco UCS® C220 M5 Rack Server) - 16 core CPU, 64 GB RAM, 800GB drives
Cisco UCS C220 M5 CV-CNTR-M5S3	Cyber Vision Center hardware appliance (Cisco UCS® C220 M5 Rack Server) - 12 core CPU, 32 GB RAM, 480GB drives
Sentryo CENTER10	Sentryo CENTER10 hardware appliance
Sentryo CENTER30	Sentryo CENTER30 hardware appliance

Sensor	Description
Cisco IC3000	Cyber Vision Sensor hardware appliance
Cisco Catalyst IE3400	Cyber Vision Sensor IOx application hosted in Cisco Catalyst IE3400 Industrial Ethernet switches
Cisco Catalyst IE3300 10G	Cyber Vision Sensor IOx application hosted in Cisco Catalyst IE3300 Industrial Ethernet switches with 10G ports
Cisco IR1101	Cyber Vision Sensor IOx application hosted in Cisco IR1101 Series Industrial Integrated Services Routers
Cisco Catalyst 9300, 9400	Cyber Vision Sensor IOx application hosted in Catalyst 9300, 9400 Series switches
Sentryo SENSOR3	Sentryo SENSOR3 hardware appliance
Sentryo SENSOR5	Sentryo SENSOR5 hardware appliance
Sentryo SENSOR7	Sentryo SENSOR7 hardware appliance

Links

Software Download

The files below can be find following this link: https://software.cisco.com/download/home/286325414/type

Center	Description
CiscoCyberVision-center-4.0.0.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-with-DPI-4.0.0.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-center-4.0.0.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-sensor-management-4.0.0.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-4.0.0.tar	IE3400, IR1101 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64--4.0.0.tar	IE3400, IR1101 active Discovery sensor installation and update file
CiscoCyberVision-IOx-IC3K-4.0.0.tar	IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.0.0.tar	Catalyst 9x00 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.0.0.tar	Catalyst 9x00 active Discovery sensor installation and update file
Updates	**Description**
CiscoCyberVision-Embedded-KDB-4.0.0.dat	KnowledgeDB embedded in Cisco Cyber Vision 4.0.0
CiscoCyberVision-update-center-4.0.0.dat	Center update file for upgrade from release 3.2.x to release 4.0.0
CiscoCyberVision-update-sensor-4.0.0.dat	Cisco IC3000 Sensor and Sentryo Sensor3, 5, 7 update file for upgrade from release 3.2.x to release 4.0.0
CiscoCyberVision-update-combined-4.0.0.dat	Center, IC3000 Sensor and Legacy Sensor update file from GUI for upgrade from release 3.2.x to release 4.0.0

Cisco Cyber Vision Center 4.0.0 can also be deployed on AWS (Amazon Web Services). The Cyber Vision Center AMI (Amazon Machine Image) can be found on the AWS Marketplace:

https://aws.amazon.com/marketplace/seller-profile?id=e201de70-32a9-47fe-8746-09fa08dd334f

Related Documentation

Cisco Cyber Vision documentation: https://www.cisco.com/c/en/us/support/security/cyber-vision/series.html

- Cisco Cyber Vision GUI User Guide:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_GUI_User_Guide_4_0_0.pdf

- Cisco Cyber Vision Network Sensor Installation Guide for Cisco IE3300 10G, IE3400 and Catalyst 9300:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Installation_Guide_for_Cisco_IE3300_10G_Cisco_IE3400_and_Cisco_Catalyst_9300_4_0_0.pdf

- Cisco Cyber Vision Network Sensor Installation Guide for Cisco IR1101:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_Network_Sensor_Installation_Guide_for_Cisco_IR1101_4_0_0.pdf

- Cisco Cyber Vision Network Sensor Installation Guide for Cisco IC3000:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_Network_Sensor_Installation_Guide_for_Cisco_IC3000_4_0_0.pdf

- Cisco Cyber Vision IC3000 Troubleshooting Guide:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_IC3000_Troubleshooting_Guide_Release_3_0_2.pdf

- Cisco Cyber Vision Center Appliance Installation Guide:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_Center_Appliance_Installation_Guide_4_0_0.pdf

- Cisco Cyber Vision Center VM Installation Guide:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_Center_VM_Installation_Guide_4_0_0.pdf

- Cisco Cyber Vision Integration Guide, Integrating Cisco Cyber Vision with Cisco Identify Services Engine (ISE) via pxGrid:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Integrating-Cisco-Cyber-Vision-with-Cisco-Identify-Services-Engine-via-pxGrid.pdf

- Cisco Cyber Vision REST API User Guide, Release 3.1.0:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_REST-API_User_Guide_Release_3_1_0.pdf

- Cisco Cyber Vision Smart Licensing User Guide, Release 3.2.2

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_Smart_Licensing_User_Guide_3_2_2.pdf

Cisco Cyber Vision 4.0.0 update procedure

Cisco Cyber Vision 4.0.0 update procedure will depend on the architecture deployed and the tool used to deploy it.

If you are currently running a version earlier than Cyber Vision 3.2.3, you must first upgrade to 3.2.3 prior to upgrading to Cyber Vision 4.0. Upgrades directly to Cyber Vision 4.0 are not supported on versions before 3.2.3.

Prerequisites

- The configuration files from previous releases must be removed or modified before upgrading from 3.2.x to 4.0.0.
- The file stowd.conf must be removed.

Data purge

Cisco Cyber Vision update procedure will not purge data automatically. The Center 3.2.x database will be migrated to the new 4.0.0 schema. All components, activities, flows, events, etc. will be migrated.

The migration process could take hours (from 1 to 24 hours). To avoid a long migration process, a data purge should be performed prior to upgrading to 4.0.0.

This purge can be launched from the User Interface (UI) or from the Command Line Interface (CLI). In the UI, the user must navigate to Admin > Data Management > Clear Data where several options are available. From the CLI, the command ‘`sbs-db --help`’ will give to the user the different options available.

Once migrated, the database content will be managed with the new data retention policies of the 4.0.0. Some expiration settings will be applied, and the system will purge by default:

- Events after 6 months.
- Flows after 6 months.
- Variables after 2 years.

After an upgrade, configured expiration settings will apply after 3 days so users can modify default settings.

Center updates

Architecture with Global Center

In the case of a distributed architecture, the following steps need to be followed:

1. Update the Global Center:
    a. Using the graphical user interface:
        - File= CiscoCyberVision-update-combined-4.0.0.dat
        - Navigate to Admin > System and use the System Update button, and browse to select the update file.

    b. Using the command line interface (CLI):
        - File= CiscoCyberVision-update-center-4.0.0.dat
        - Launch the update with the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-center-4.0.0.dat
```

2. Update the Centers connected to the Global Center with the same procedure used for the Global Center (user interface or CLI)
3. Update the sensors, from their corresponding Center (not from the Global Center):
    a. Hardware sensors:
        i. If you used the combined file to update the Center which owned the sensor, the hardware sensors (IC3000 and Sentryo SENSOR's) were updated at the same time.
        ii. If not, the update needs to be done from the Command Line (CLI):
            - File= CiscoCyberVision-update-sensor-4.0.0.dat
            - Launch the update with the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-sensor-4.0.0.dat
```

Note: Cisco Cyber Vision Sensor application should not be updated from the IC3000 Local manager because the configuration will be lost. In case this is done, the sensor enrollment package needs to be deployed again.

b. IOx sensors:

    i. If you have installed the sensor with the sensor management extension, the upgrade of the extension will also update all sensors reachable from the Center.

        - File = CiscoCyberVision-sensor-management-4.0.0.ext
        - Navigate to Admin > Extensions. In the Actions column, use the update button and browse to select the update file.

    ii. If a sensor was not updated by the extension update, access the sensor administration page and use the UPDATE CISCO DEVICES button to update the remaining IOx sensors connected to the Center.

    iii. If you have not installed the sensor with the sensor management extension, the upgrade of the sensor can be performed with the sensor package from the platform Local Manager or from the platform Command Line. This procedure is described in the corresponding sensors installation guides.

        - IE3x00 and IR11101 files = CiscoCyberVision-IOx-aarch64-4.0.0.tar or CiscoCyberVision-IOx-Active-Discovery-aarch64--4.0.0.tar
        - Catalyst 9300 and 94000 files = CiscoCyberVision-IOx-x86-64-4.0.0.tar or CiscoCyberVision-IOx-Active-Discovery-x86-64-4.0.0.tar.

Architecture with one Center

In the case of a single Center, the following steps need to be followed:

1. Update the Center:
    a. Using the graphical user interface:
        - File= CiscoCyberVision-update-combined-4.0.0.dat
        - Navigate to Admin > System, use the System Update button, and browse to select the update file.

    b. Using the command line interface (CLI):
        - File= CiscoCyberVision-update-center-4.0.0.dat
        - Launch the update with the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-center-4.0.0.dat
```

2. Update the sensors:
    a. Hardware sensors:
        i. If you used the combined file to update the Center, the hardware sensors (IC3000 and Sentryo SENSOR's) were updated at the same time.
        ii. If not, the update needs to be done from the command line interface (CLI):
            - File= CiscoCyberVision-update-sensor-4.0.0.dat
            - Launch the update with the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-sensor-4.0.0.dat
```

    b. IOx sensors:
        i. If you have installed the sensor with the sensor management extension, the upgrade of the extension will also update all reachable sensors.
            - File = CiscoCyberVision-sensor-management-4.0.0.ext
            - Navigate to Admin > Extensions. In the Actions column, use the update button and browse to select the update file.
        ii. If you have not installed the sensor with the sensor management extension, the upgrade of the sensor can be performed with the sensor package from the platform Local Manager or from the platform Command Line. This procedure is described in the corresponding sensors installation guides.
            - IE3x00 and IR11101 files = CiscoCyberVision-IOx-aarch64-4.0.0.tar or CiscoCyberVision-IOx-Active-Discovery-aarch64--4.0.0.tar
            - Catalyst 9300 and 94000 files = CiscoCyberVision-IOx-x86-64-4.0.0.tar or CiscoCyberVision-IOx-Active-Discovery-x86-64-4.0.0.tar.

Cisco Cyber Vision 4.0.0 important changes

Communication port and protocol changes

Port

There is no port change in Cisco Cyber Vision 4.0.0. All TCP or UDP ports already used are kept, and no new port number is needed.

Protocol

A modification was done on the product to adopt new secure code best practices to enhance the security posture and resiliency. One of the consequences is that the SFTP subsystem of OpenSSH is now disabled. SFTP can no longer be used to transfer files from or to the Center or sensor, only scp is supported.

API

A HTTP header authentication mechanism has been added to both API v1 and v3.
Token authentication through the URL is not supported with API v3.
Token authentication through the URL is no more supported with API v1.

SYSLOG

Syslog messages header was changed between release 3.2.x and release 4.0.0. The following changes were made, just after the timestamp:

- The text of the 3.2.x version was

  “rsyslogd cybervision[1]: CEF:0|sentryo|cybervision|1.0”
- And is replaced in 4.0.0 with

  “center162.mycorp.com cybervision[1]: CEF:0|Cisco|Cyber Vision|1.0|:”

“center162.mycorp.com” in the 4.0.0 release is the FQDN of the Center. The rest of this first part of the message doesn’t change.

The other fields of the syslog message were not changed.

For example, the following message in 3.2.x:

```
<158>2020-11-18T15:45:15.402498+00:00 rsyslogd cybervision[1]:
CEF:0|sentryo|cybervision|1.0|component_new|New component detected|2|cat=Inventory
Events msg=New component detected on the network: IP 1.2.3.4, MAC aa:bb:cc:dd:ee:ff
SCVEventType=new_component SCVComponentId=bcae40b8-3a98-4bb2-8528-d870e143dbaf
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
```

in 4.0.0:

```
<158>2021-06-04T08:02:06.027021+00:00 center162.mycorp.com cybervision[1]:
CEF:0|Cisco|Cyber Vision|1.0|component_new|New component detected|2|cat=Inventory Events
msg=New component detected on the network: IP 1.2.3.4, MAC aa:bb:cc:dd:ee:ff
SCVEventType=new_component SCVComponentId=1282014e-1563-4e7a-99e6-3d5f79bc56a9
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
```

Few additional messages were created:

Title	Description
data_expired	Data expiration
extension_alert	Extension-related alert
extension_info	Extension-related info
force_mode	Force mode change event
offline	Offline event
weak_encryption	Weak encryption event

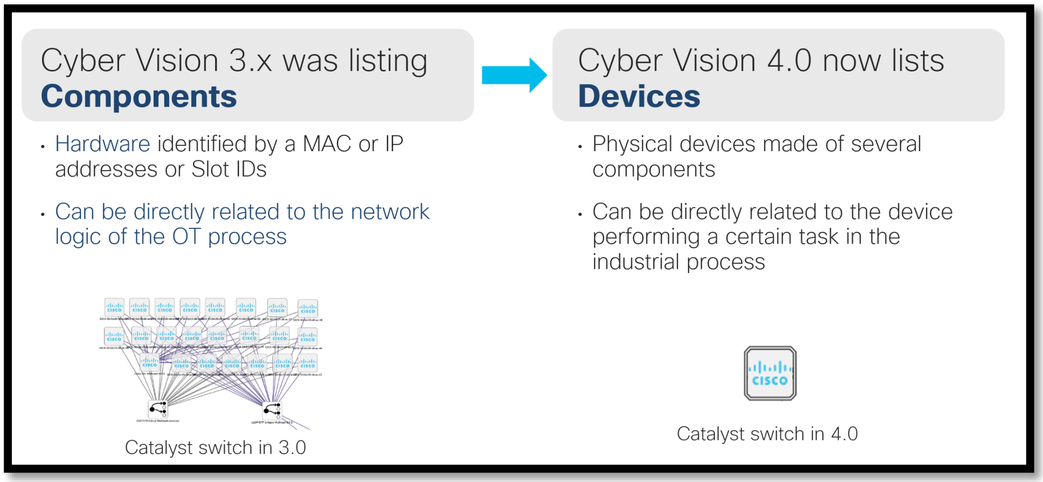
Cisco Cyber Vision new features and improvements

Enhanced device aggregation

Cisco Cyber Vision 4.0.0 now consolidates components into devices:

- Devices match the customer's industrial processes.
- More natural for non-technical users.
- Reduced complexity when looking at large inventories/maps.

Cisco Cyber Vision Enhanced device aggregation



Cyber Vision 3.x was listing **Components**

- Hardware identified by a MAC or IP addresses or Slot IDs
- Can be directly related to the network logic of the OT process

Catalyst switch in 3.0

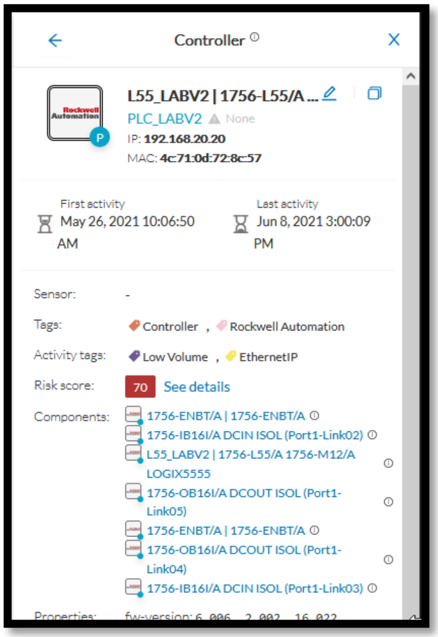
Cyber Vision 4.0 now lists **Devices**

- Physical devices made of several components
- Can be directly related to the device performing a certain task in the industrial process

Catalyst switch in 4.0

A new double-border icon indicates a device.

The user can easily see the list of a device's components clicking on a device icon to view more details:



L55_LABV2 | 1756-L55/A ...

PLC_LABV2 None

IP: 192.168.20.20

MAC: 4c:71:0d:72:8c:57

First activity May 26, 2021 10:06:50 AM

Last activity Jun 8, 2021 3:00:09 PM

Sensor: -

Tags: Controller , Rockwell Automation

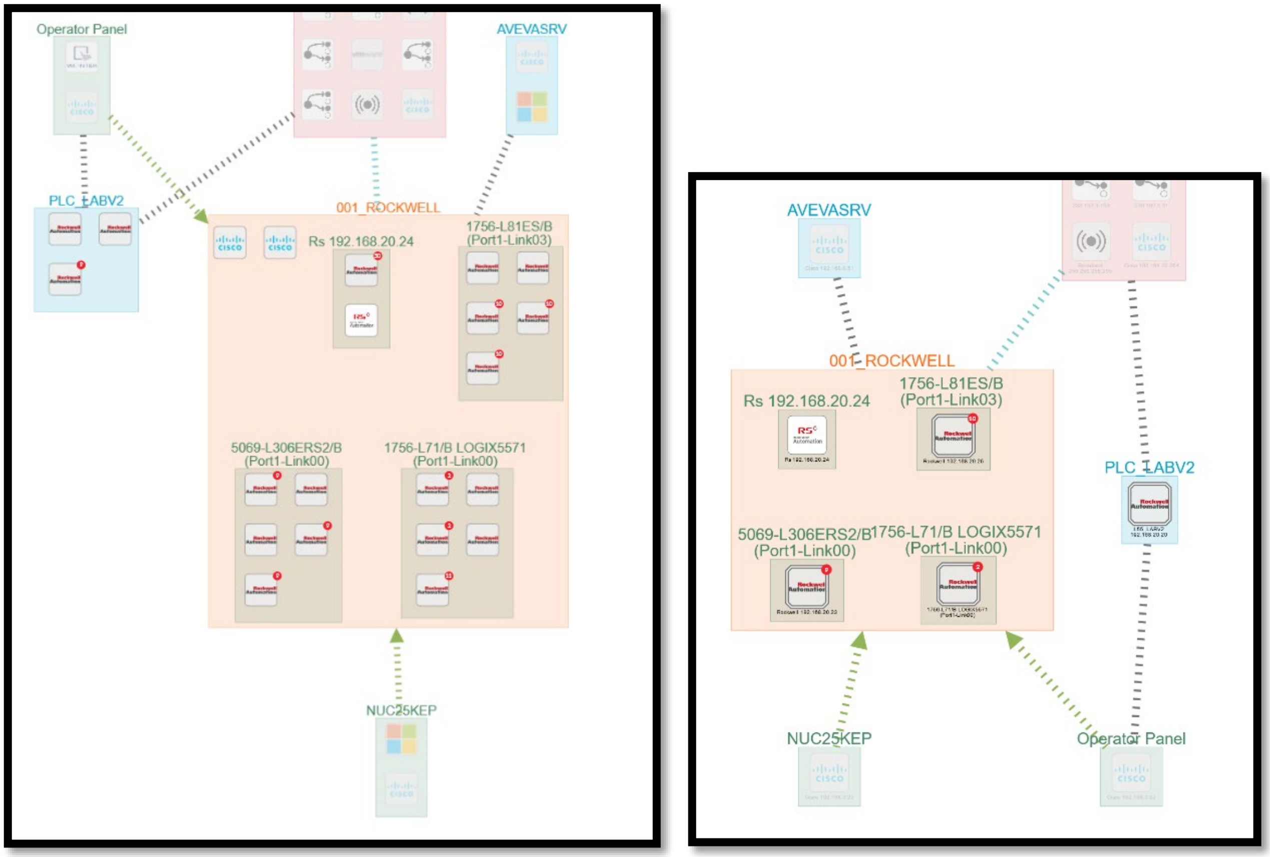
Activity tags: Low Volume , EthernetIP

Risk score: 70 See details

Components:
1756-ENBT/A | 1756-ENBT/A
1756-IB16I/A DCIN ISOL (Port1-Link02)
L55_LABV2 | 1756-L55/A 1756-M12/A LOGIX5555
1756-OB16I/A DCOUT ISOL (Port1-Link05)
1756-ENBT/A | 1756-ENBT/A
1756-OB16I/A DCOUT ISOL (Port1-Link04)
1756-IB16I/A DCIN ISOL (Port1-Link03)

Properties: fw-version: 6.006 2.002 16.022

Cisco Cyber Vision Enhanced device aggregation



Changes to Licensing

Cisco Cyber Vision Licensing is now more aligned with how users leverage the solution, as the new device feature consolidates components. Starting in Cisco Cyber Vision 4.0.0, licensing is based on the number of discovered devices in internal networks.

In addition, users can define in version 4.0.0 their internal network ranges, which by default leverages standardized RFC1918 private networks. This feature will let the user define IT, OT and external networks. Only devices belonging to internal networks will be considered for license calculation.

Performance optimizations

Cisco Cyber Vision 4.0.0 continues to lay the foundation for large scale deployments.

Faster data ingestion

The Cisco Cyber Vision data ingestion pipeline was completely redesigned to improve its scalability both in terms of connected sensors and in the number of data items that can be inserted or updated in the database. As a result, Cisco Cyber Vision Center running on dedicated hardware (such as the official Cisco CV-CNTR-M5S5 product) scales by an order of magnitude better than the 3.2.x release running on the same hardware.

The new sizing recommendations for Cisco Cyber Vision 4.0.0 are therefore:

Items	CV-CNTR-M5S5	CV-CNTR-M5S3
Max number of components on a single Center	50,000	25,000
Max number of components synced to a Global Center	150,000	75,000
Max number of flows stored	8,000,000	4,000,000
Max number of sensors managed	150	75
Max number of Centers synchronized to a Global Center	20	20

Speedy UI even with large datasets

To avoid any large request on the database during navigation, preset data is now pre-computed. Cisco Cyber Vision automatically updates data in the background when changes occur. When the user navigates to a preset visualization (map, device list, activity list, etc.) the data comes from a specific repository made by preset and avoid any delay due to data computation.

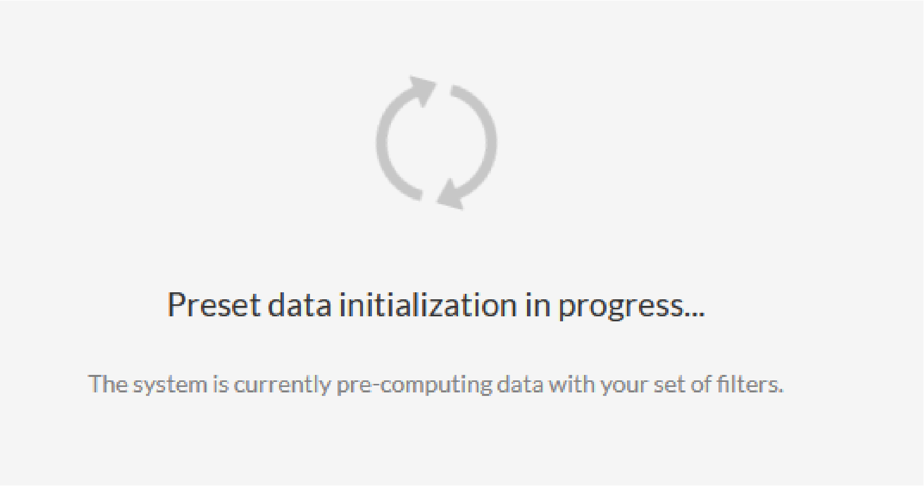
This precomputation has a lot of effects on the UI. It will first speed up the navigation on systems with a large dataset. It will also change the process for a user to create a new preset. When a user filters the data, the process will be:

1. User defines and saves the new filter definition as a preset.
2. The system calculates the different views needed.
3. Once calculated the data will become available on the UI.

As new data is ingested, the same calculations will be needed prior to new data being visible in the UI. While the computation is performed on a periodic basis, a Refresh button is now available, in the preset page, to force the calculation to occur. Once computed, the new data will then be displayed.

Just after the migration of the database all presets need to be pre-computed to prepare visualization data. Until the precomputations are finished the following message will be displayed on all presets:

Cisco Cyber Vision Preset Data Initialization



Preset data initialization in progress...

The system is currently pre-computing data with your set of filters.

This message will also be displayed on a new preset before the end of the first pre-computation.

Preset Data filtering changes

Cisco Cyber Vision 4.0.0 brings several changes related to the Preset data filters.

In version 4.0.0 Cisco Cyber Vision data can now be filtered per preset using the following details:

1. Device tags: devices
2. Risk score: device individual risk
3. Groups: devices
4. Activity tags: activities
5. Sensors: device “location”
6. Networks: device IPs
7. Keyword: device properties including IP, MAC, names, vendors, 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:

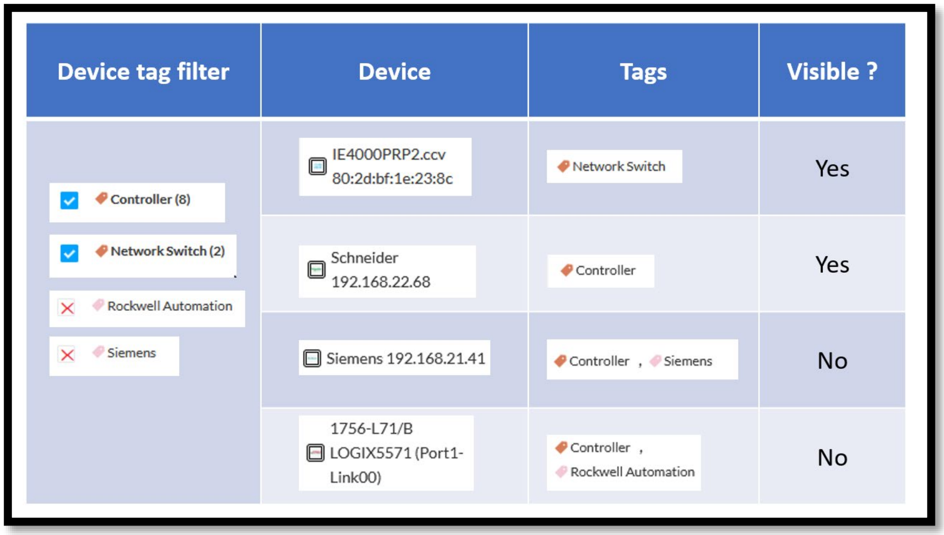
- Each category allows to define a subset of the components, or activities for the Activity filter.
- If filters are defined by several categories, the resulting dataset is the intersect of the selections for each category.

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 show all 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



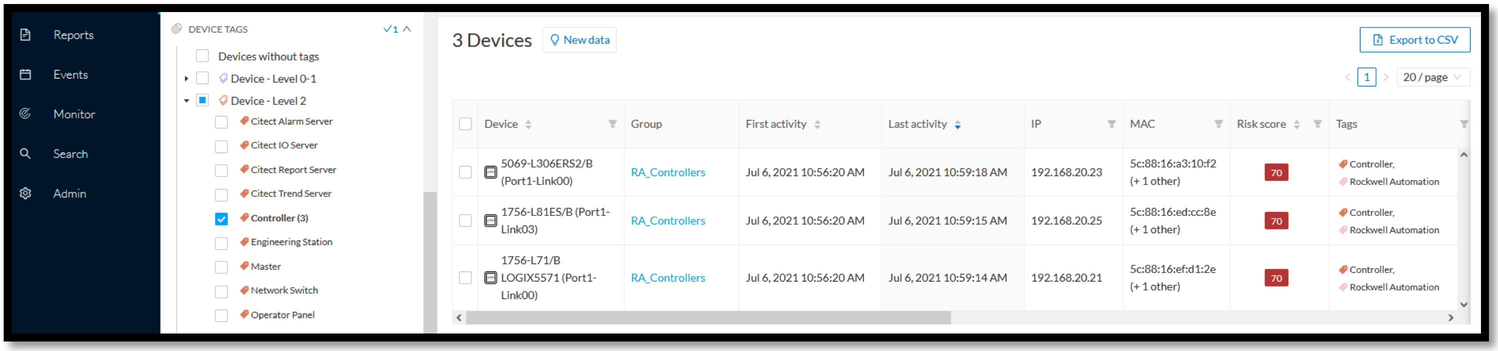
Device tag filter	Device	Tags	Visible ?
☑ Controller (8) ☑ Network Switch (2) ☒ Rockwell Automation ☒ Siemens	IE4000PRP2.ccv 80:2d:bf:1e:23:8c	Network Switch	Yes
	Schneider 192.168.22.68	Controller	Yes
	Siemens 192.168.21.41	Controller , Siemens	No
	1756-L71/B LOGIX5571 (Port1-Link00)	Controller , Rockwell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

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

For other views like the activity list or the 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

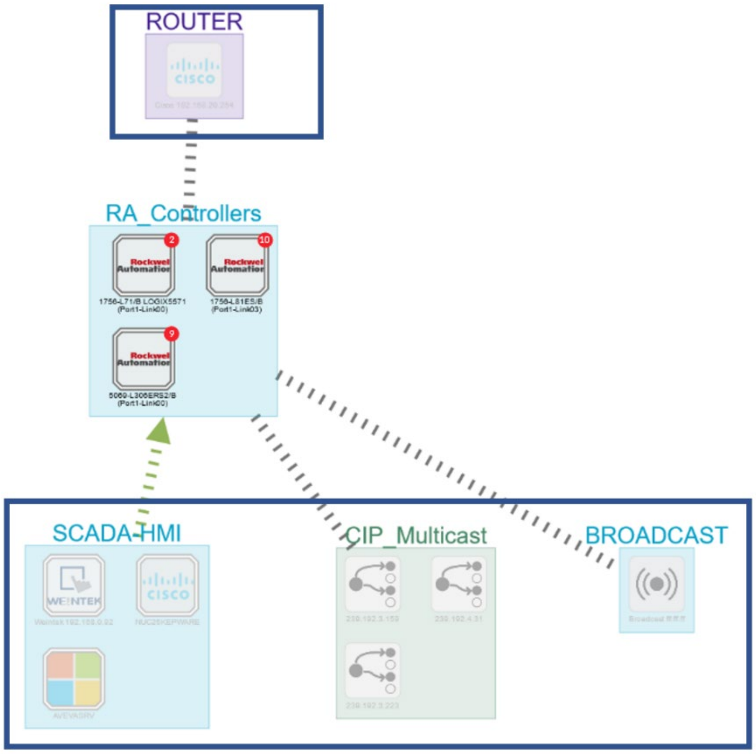


3 Devices

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 components are greyed out.

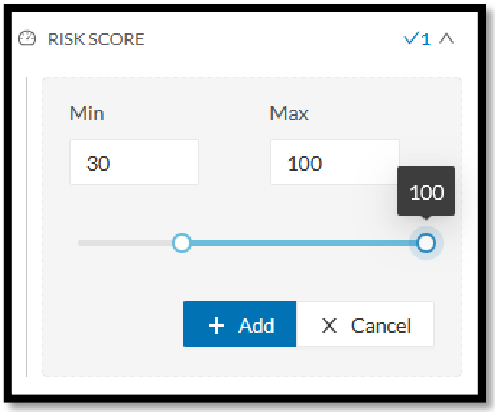
Device tag filter, example of Controllers - map


ROUTER
RA_Controllers
2
1756-L71/B LOGIX5571 (Port1-Link00)
10
1756-L81ES/B (Port1-Link03)
9
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.

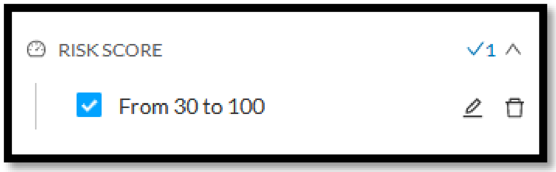
Risk score, filter definition


RISK SCORE ✓1

Min: 30

Max: 100

Risk score – inclusive filter


RISK SCORE ✓1

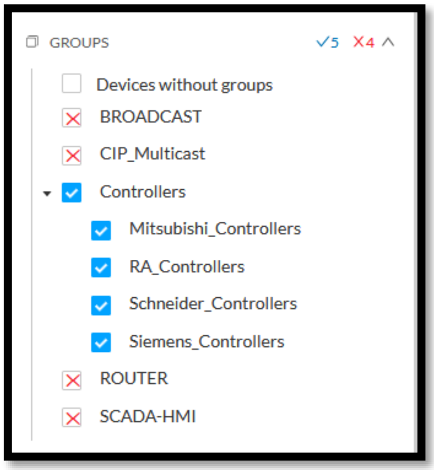
☑ From 30 to 100

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

Groups

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

Group filter



GROUPS ✓5 ✗4

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

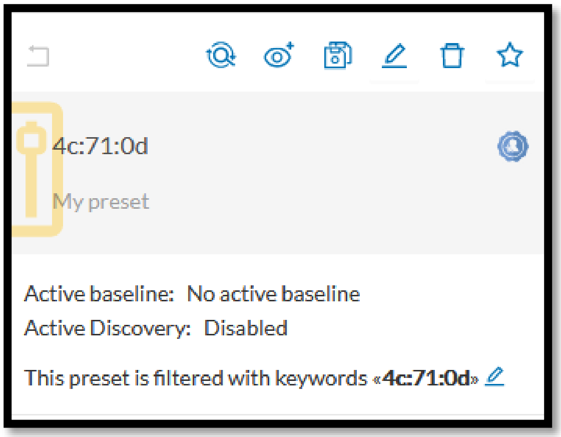
In the example above, only the devices belonging to the selected groups are selected.

Activities always involve two end points and are shown 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 page in 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

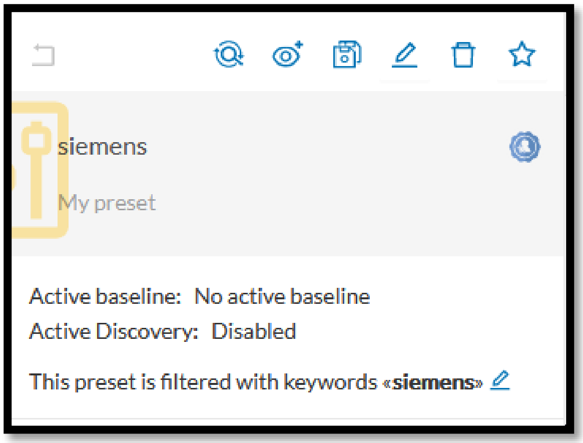
My preset

Active baseline: No active baseline

Active Discovery: Disabled

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

Keyword =siemens



siemens

My preset

Active baseline: No active baseline

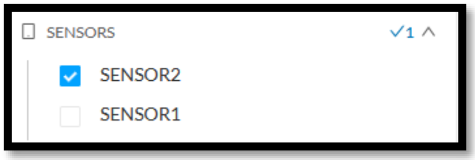
Active Discovery: Disabled

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

Sensors

Activities can 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

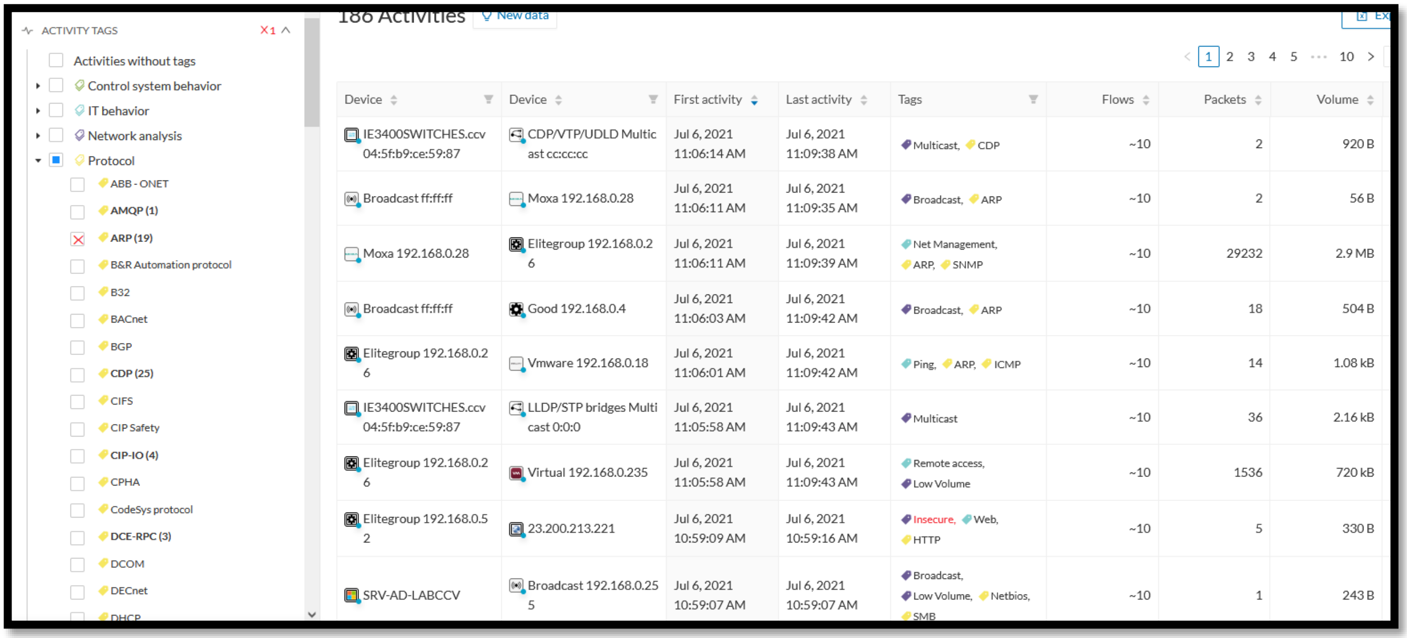
□ SENSOR1

Activity tags

Filtering on activity tag will not have the same behavior as 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

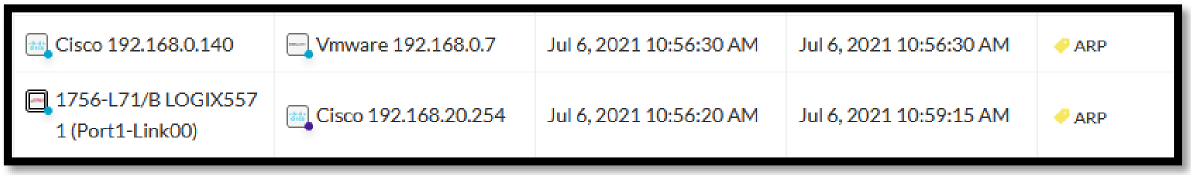
- □ Activities without tags
- □ Control system behavior
- □ IT behavior
- □ Network analysis
- ■ Protocol
  - □ ABB - ONET
  - □ AMQP (1)
  - ☒ ARP (19)
  - □ B&R Automation protocol
  - □ B32
  - □ BACnet
  - □ BGP
  - □ CDP (25)
  - □ CIFS
  - □ CIP Safety
  - □ CIP-IO (4)
  - □ CPHA
  - □ CodeSys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

186 Activities

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 activities below are hidden:

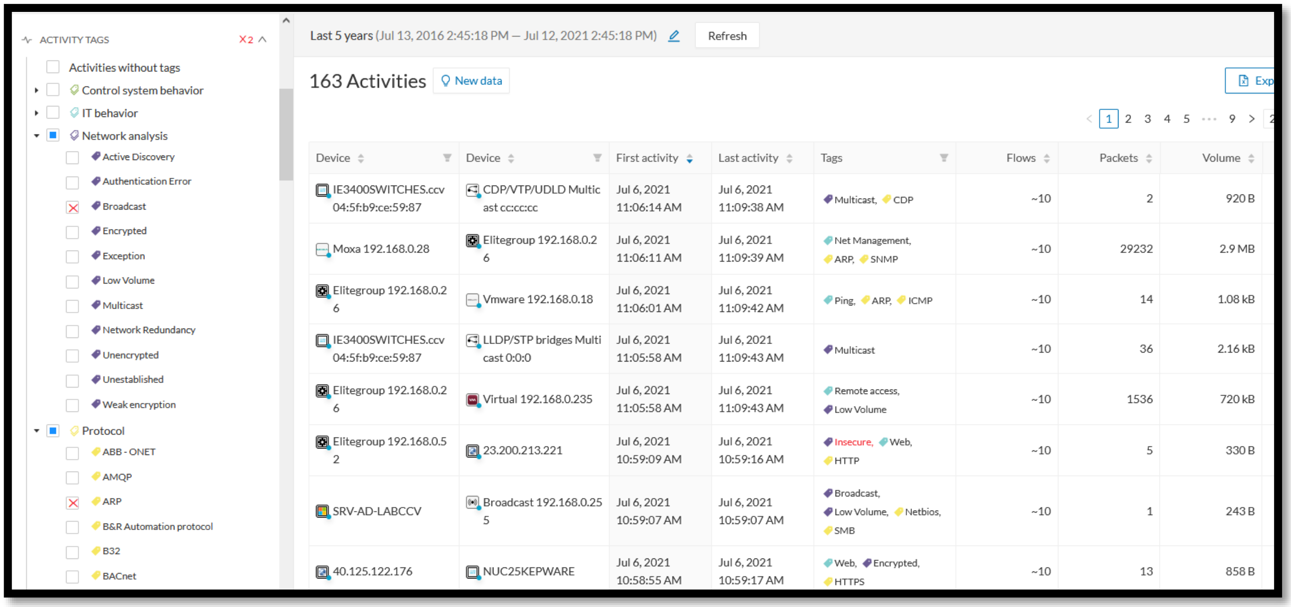
Activity filter – negative filter 2



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 LOGIX5571 (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)

163 Activities

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 rarely used, but for very specific use cases.

These 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.

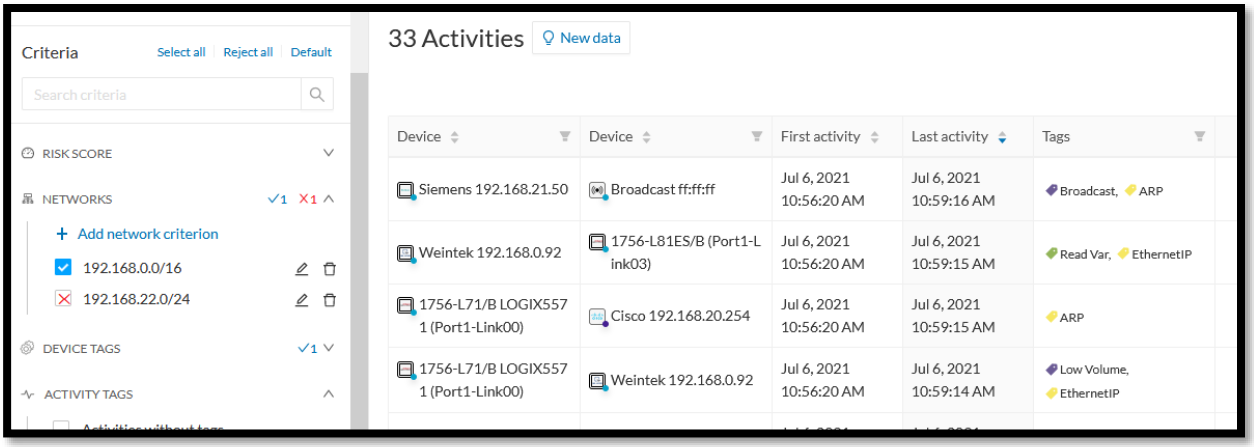
Networks

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 shown.

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

Exclusion and combination can also be used, for example:

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 in version 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.

Smarter data retention to avoid disk saturation

Cisco Cyber Vision 4.0.0 brings some new data retention policies. Some expiration settings will be applied to the data. The default values are:

- Events after 6 months
- Flows after 6 months
- Variables after 2 years.

At startup (new Center) or after a migration from 3.2.x to 4.0.0, there will be a three-day delay before the expiration process will be first run, to allow the user to adjust expiration settings. After 3 days the system will use those settings to purge data. The adjustment of the expiration settings can be done in Admin > Data Management.

Enhanced security insights

Risk scoring

Risk scores guide non expert end users to the most “important” devices. It is intended as a first step in security management to help non expert users sort out information and take first decisions. It provides limited but simple information on the cybersecurity of the monitored system.

Cisco Cyber Vision 4.0.0 brings some risk scores at a device level. Risk score computation will use the standard method: “Risk = Likelihood x Impact” with

- Impact – What is the component “criticality”?
- Likelihood – Is it more likely to be compromised?

In Cisco Cyber Vision 4.0.0, the impact is made of:

- Device “type”, i.e. tags
    - Assign a risk score per device tags or device tag category.
    - Average risk score over all device tags.
- Group Industrial impact, i.e. “Business Impact”
    - Assign a risk score per Industrial Impact which is defined per group.

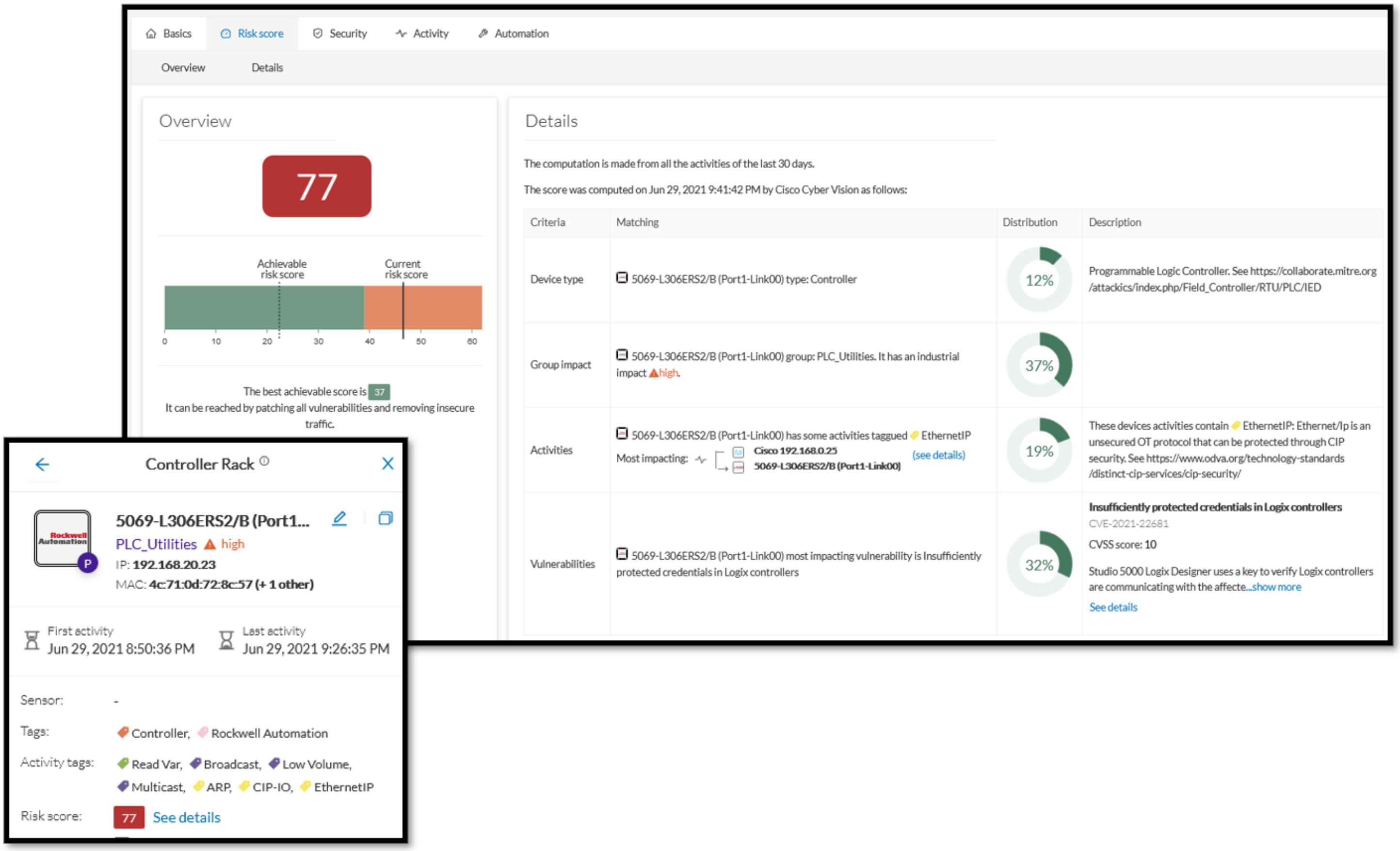
In Cisco Cyber Vision 4.0.0, the likelihood is made of:

- Activities Tags
    - Assign a risk score per activity tag or activity tag category.
    - Max risk score over all activity’s tags.
- Exposure
    - Device communicating with external subnet.
- Vulnerabilities
    - Use the CVSS v3 scoring of vulnerabilities.
    - Take the highest score (no average).

Activity tags and exposure are computed on a time basis. The user cannot choose a time window for it in the admin part of Cisco Cyber Vision.

Once the computation done, the risk score is set for each device and appears on each view displaying devices.

Risk score



The best achievable score is 37
It can be reached by patching all vulnerabilities and removing insecure traffic.

Details

The computation is made from all the activities of the last 30 days.

The score was computed on Jun 29, 2021 9:41:42 PM by Cisco Cyber Vision as follows:

Criteria	Matching	Distribution	Description
Device type	5069-L306ERS2/B (Port1-Link00) type: Controller	12%	Programmable Logic Controller. See https://collaborate.mitre.org/attackics/index.php/Field_Controller/RTU/PLC/IED
Group impact	5069-L306ERS2/B (Port1-Link00) group: PLC_Utilities. It has an industrial impact ⚠high.	37%	
Activities	5069-L306ERS2/B (Port1-Link00) has some activities taggued EthernetIP Most impacting: Cisco 192.168.0.25 → 5069-L306ERS2/B (Port1-Link00) (see details)	19%	These devices activities contain EthernetIP: Ethernet/Ip is an unsecured OT protocol that can be protected through CIP security. See https://www.odva.org/technology-standards/distinct-cip-services/cip-security/
Vulnerabilities	5069-L306ERS2/B (Port1-Link00) most impacting vulnerability is Insufficiently protected credentials in Logix controllers	32%	**Insufficiently protected credentials in Logix controllers** CVE-2021-22681 CVSS score: 10 Studio 5000 Logix Designer uses a key to verify Logix controllers are communicating with the affecte...show more See details

Controller Rack

5069-L306ERS2/B (Port1...
PLC_Utilities ⚠ high
IP: **192.168.20.23**
MAC: **4c:71:0d:72:8c:57 (+ 1 other)**

First activity
Jun 29, 2021 8:50:36 PM

Last activity
Jun 29, 2021 9:26:35 PM

Sensor: -

Tags: Controller, Rockwell Automation

Activity tags: Read Var, Broadcast, Low Volume, Multicast, ARP, CIP-IO, EthernetIP

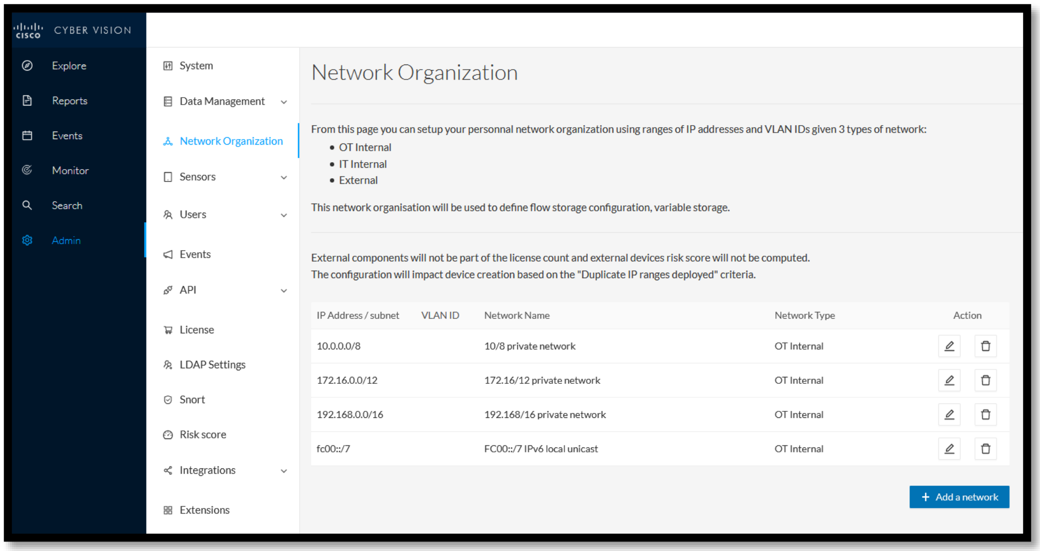
Risk score: 77 See details

Define network boundaries

A new administration page is available to define network boundaries. It will help the user to define IT, OT and External networks. It will help users to:

- Specify if public IP addresses are used in your private network.
- Make risk scoring more accurate.
- Have an accurate view of which devices are internal/external.

Network organization



Network Organization

From this page you can setup your personnal network organization using ranges of IP addresses and VLAN IDs given 3 types of network:

- OT Internal
- IT Internal
- External

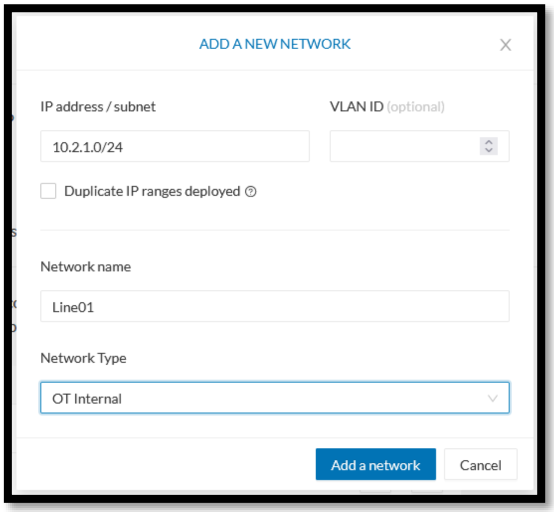
This network organisation will be used to define flow storage configuration, variable storage.

External components will not be part of the license count and external devices risk score will not be computed.
The configuration will impact device creation based on the "Duplicate IP ranges deployed" criteria.

IP Address / subnet	VLAN ID	Network Name	Network Type	Action
10.0.0.0/8		10/8 private network	OT Internal	
172.16.0.0/12		172.16/12 private network	OT Internal	
192.168.0.0/16		192.168/16 private network	OT Internal	
fc00::/7		FC00::/7 IPv6 local unicast	OT Internal	

New networks can be created from this page like below:

Network definition



ADD A NEW NETWORK

IP address / subnet: 10.2.1.0/24

VLAN ID (optional):

□ Duplicate IP ranges deployed

Network name: Line01

Network Type: OT Internal

Note that the default “Ingestion” (see above chapter) configuration is to record detailed flow information only for selected internal networks (see "Define network boundaries" chapter).

There are cases where the detailed multicast flow properties are needed:

- In the case where multicast OT protocols are used and properties need to be browsable.
- If investigation needs to be performed on multicast or general broadcast communications.

There are two options to collect and record these flows details:

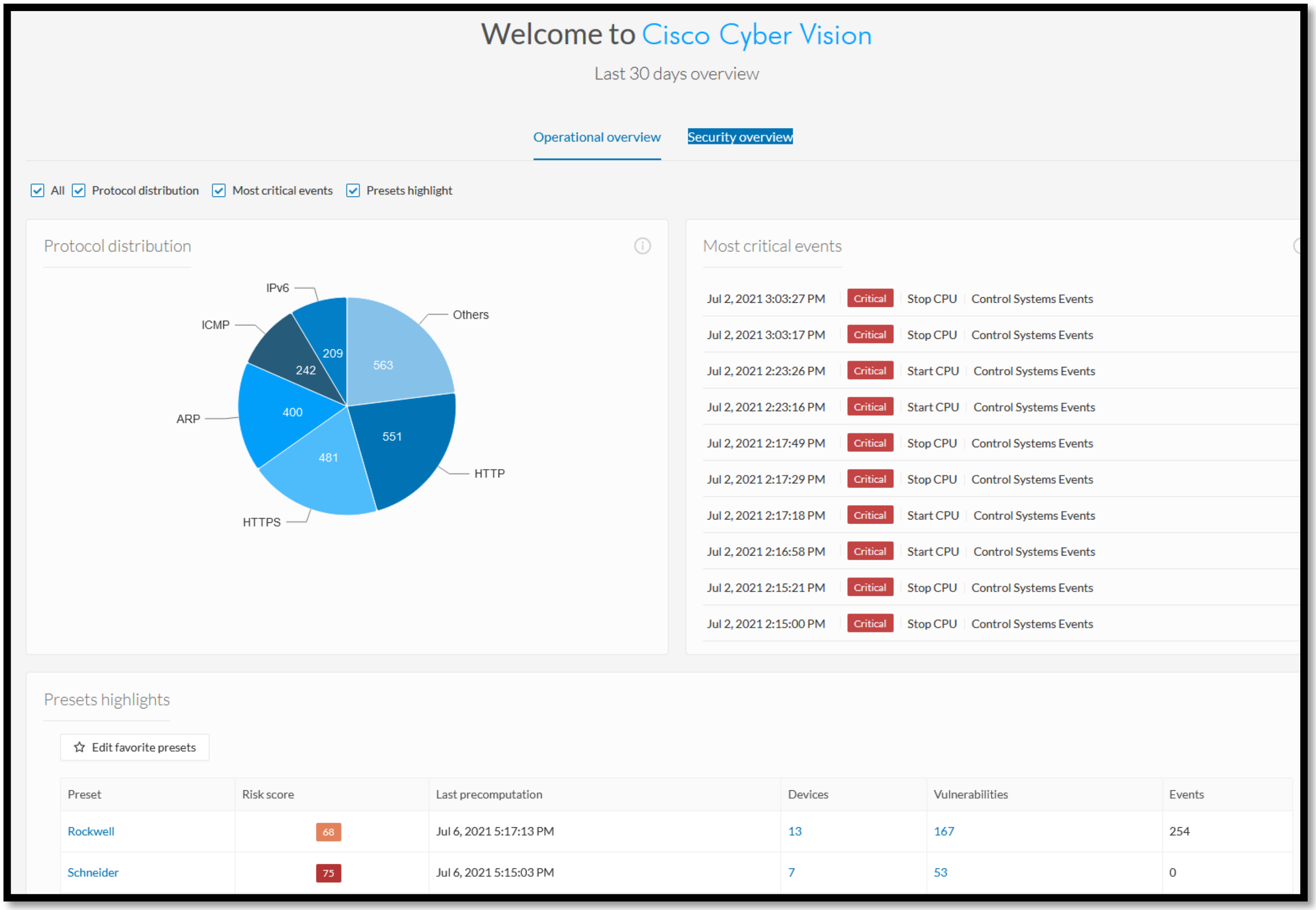
1. on the Data ingestion page, select all flows – this should be performed during a limited time to avoid flooding of the database.
2. add internal network ranges for multicast and general broadcast. As a reminder, the standard address ranges are the following ones. A subnet may be used for instance to record an OT multicast protocol but not all LLMNR communications:
    - IPv4 multicast: 224/4
    - IPv6 multicast: ff02::0/16
    - Global broadcast: 255.255.255.255/32 (may be used DNS)

New dashboards

Cisco Cyber Vision release 4.0.0 brings several new home dashboards to help drive action. New dashboards are made of several widgets which give different types of information. Widgets are grouped in 2 different views:

- Operational overview
- Security overview

Center Dashboard – operational overview



Welcome to Cisco Cyber Vision

Last 30 days overview

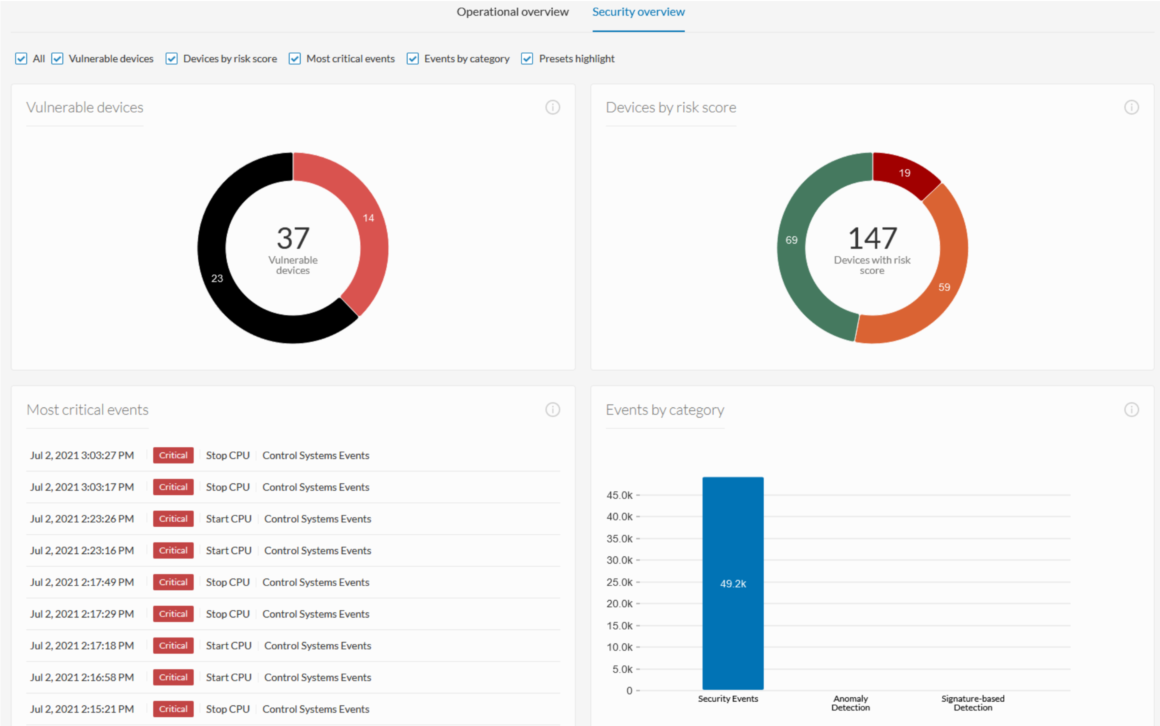
Most critical events

Jul 2, 2021 3:03:27 PM	Critical	Stop CPU	Control Systems Events
Jul 2, 2021 3:03:17 PM	Critical	Stop CPU	Control Systems Events
Jul 2, 2021 2:23:26 PM	Critical	Start CPU	Control Systems Events
Jul 2, 2021 2:23:16 PM	Critical	Start CPU	Control Systems Events
Jul 2, 2021 2:17:49 PM	Critical	Stop CPU	Control Systems Events
Jul 2, 2021 2:17:29 PM	Critical	Stop CPU	Control Systems Events
Jul 2, 2021 2:17:18 PM	Critical	Start CPU	Control Systems Events
Jul 2, 2021 2:16:58 PM	Critical	Start CPU	Control Systems Events
Jul 2, 2021 2:15:21 PM	Critical	Stop CPU	Control Systems Events
Jul 2, 2021 2:15:00 PM	Critical	Stop CPU	Control Systems Events

Presets highlights

Preset	Risk score	Last precomputation	Devices	Vulnerabilities	Events
Rockwell	68	Jul 6, 2021 5:17:13 PM	13	167	254
Schneider	75	Jul 6, 2021 5:15:03 PM	7	53	0

Center Dashboard – Security



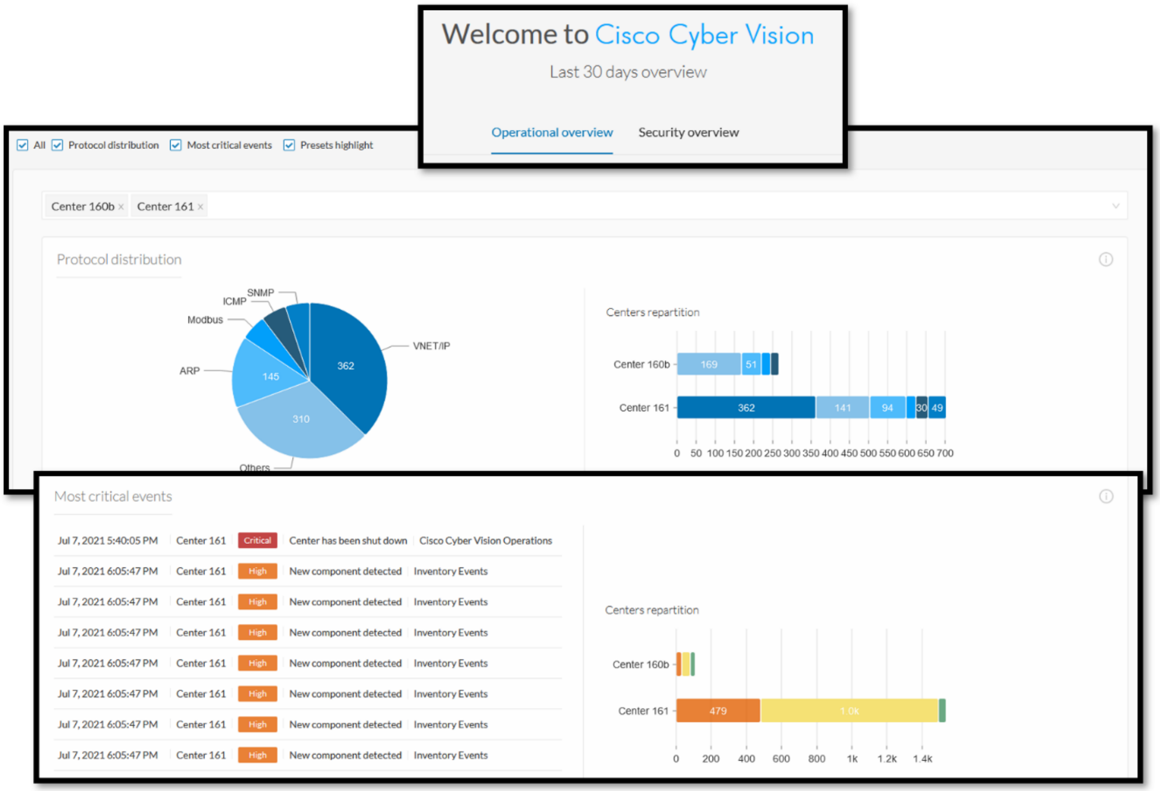
Operational overview | Security overview

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

Most critical events

Jul 2, 2021 3:03:27 PM	Critical	Stop CPU	Control Systems Events
Jul 2, 2021 3:03:17 PM	Critical	Stop CPU	Control Systems Events
Jul 2, 2021 2:23:26 PM	Critical	Start CPU	Control Systems Events
Jul 2, 2021 2:23:16 PM	Critical	Start CPU	Control Systems Events
Jul 2, 2021 2:17:49 PM	Critical	Stop CPU	Control Systems Events
Jul 2, 2021 2:17:29 PM	Critical	Stop CPU	Control Systems Events
Jul 2, 2021 2:17:18 PM	Critical	Start CPU	Control Systems Events
Jul 2, 2021 2:16:58 PM	Critical	Start CPU	Control Systems Events
Jul 2, 2021 2:15:21 PM	Critical	Stop CPU	Control Systems Events

Global Center Dashboard – Operational Overview



Welcome to Cisco Cyber Vision

Last 30 days overview

Operational overview | Security overview

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

Center 160b × Center 161 ×

Most critical events

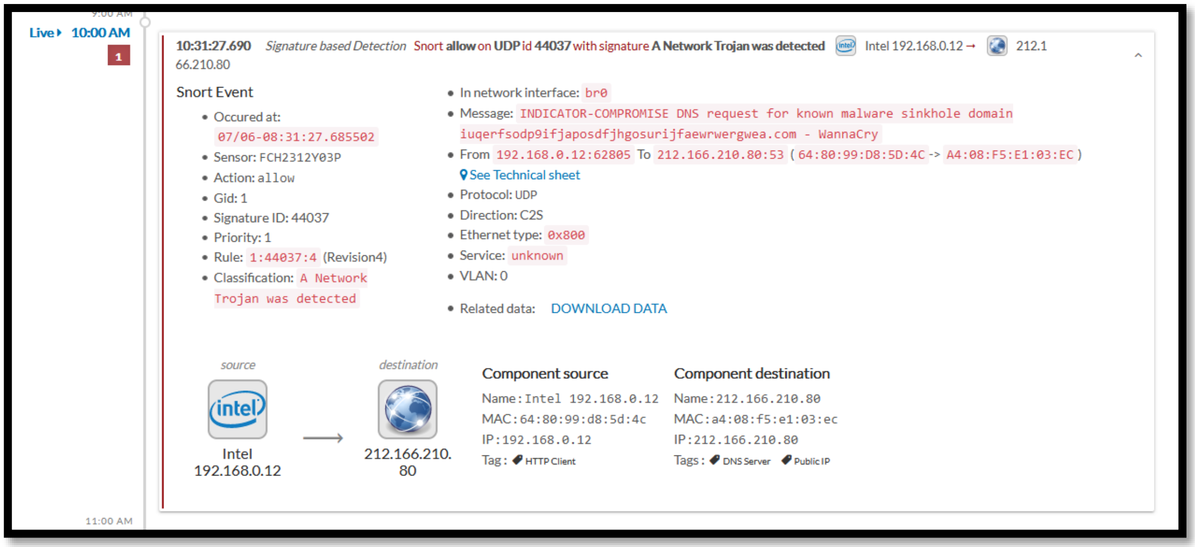
Jul 7, 2021 5:40:05 PM	Center 161	Critical	Center has been shut down	Cisco Cyber Vision Operations
Jul 7, 2021 6:05:47 PM	Center 161	High	New component detected	Inventory Events
Jul 7, 2021 6:05:47 PM	Center 161	High	New component detected	Inventory Events
Jul 7, 2021 6:05:47 PM	Center 161	High	New component detected	Inventory Events
Jul 7, 2021 6:05:47 PM	Center 161	High	New component detected	Inventory Events
Jul 7, 2021 6:05:47 PM	Center 161	High	New component detected	Inventory Events
Jul 7, 2021 6:05:47 PM	Center 161	High	New component detected	Inventory Events
Jul 7, 2021 6:05:47 PM	Center 161	High	New component detected	Inventory Events

Snort enhancements:

A new snort event is now available in Cisco Cyber Vision 4.0.0. This event will help users to correlate Cisco Cyber Vision activity or component and snort event.

It will help the user to find the involved components and the related activity.

Snort event



10:31:27.690 *Signature based Detection* Snort **allow** on **UDP** id **44037** with signature **A Network Trojan was detected** Intel 192.168.0.12 → 212.166.210.80

Snort Event

- Occured at: `07/06-08:31:27.685502`
- Sensor: `FCH2312Y03P`
- Action: `allow`
- Gid: 1
- Signature ID: 44037
- Priority: 1
- Rule: `1:44037:4` (Revision4)
- Classification: `A Network Trojan was detected`

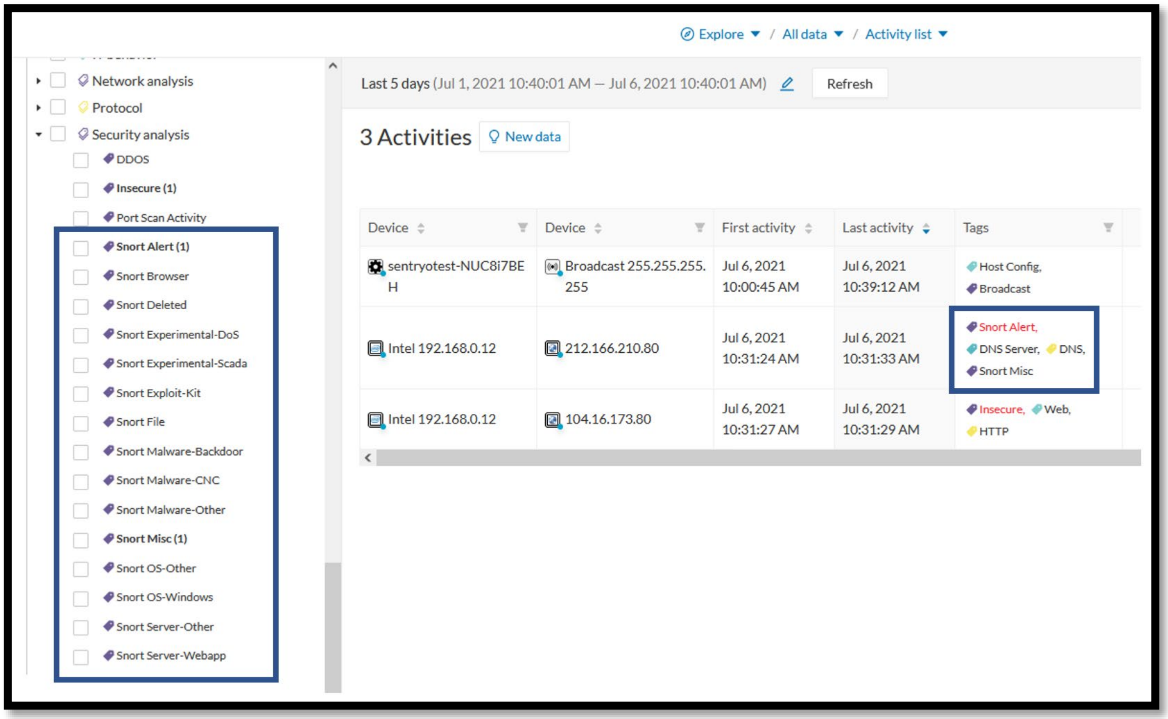
- In network interface: `br0`
- Message: `INDICATOR-COMPROMISE DNS request for known malware sinkhole domain iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com - WannaCry`
- From `192.168.0.12:62805` To `212.166.210.80:53` (`64:80:99:D8:5D:4C` -> `A4:08:F5:E1:03:EC`)
  See Technical sheet
- Protocol: UDP
- Direction: C2S
- Ethernet type: `0x800`
- Service: `unknown`
- VLAN: 0
- Related data: DOWNLOAD DATA

Component source
Name: Intel 192.168.0.12
MAC: 64:80:99:d8:5d:4c
IP: 192.168.0.12
Tag : HTTP Client

Component destination
Name: 212.166.210.80
MAC: a4:08:f5:e1:03:ec
IP: 212.166.210.80
Tags : DNS Server Public IP

In addition to the event, some new snort tags are added to the activity which is related to a snort event:

Snort activity tags



- □ Network analysis
- □ Protocol
- □ Security analysis
  - □ DDOS
  - □ **Insecure (1)**
  - □ Port Scan Activity
  - □ **Snort Alert (1)**
  - □ Snort Browser
  - □ Snort Deleted
  - □ Snort Experimental-DoS
  - □ Snort Experimental-Scada
  - □ Snort Exploit-Kit
  - □ Snort File
  - □ Snort Malware-Backdoor
  - □ Snort Malware-CNC
  - □ Snort Malware-Other
  - □ **Snort Misc (1)**
  - □ Snort OS-Other
  - □ Snort OS-Windows
  - □ Snort Server-Other
  - □ Snort Server-Webapp

Last 5 days (Jul 1, 2021 10:40:01 AM — Jul 6, 2021 10:40:01 AM)

3 Activities

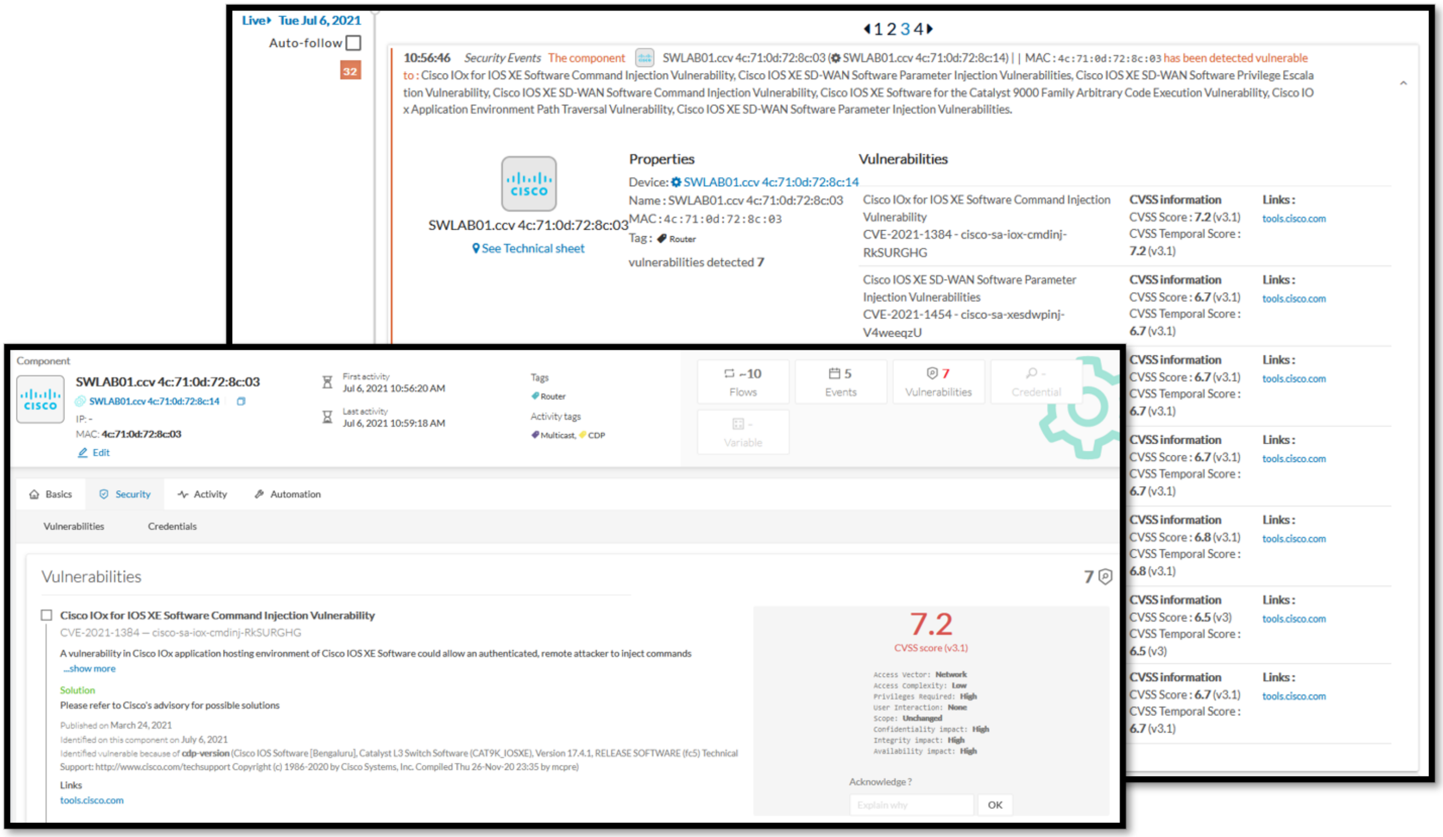
Device	Device	First activity	Last activity	Tags
sentryotest-NUC8i7BEH	Broadcast 255.255.255.255	Jul 6, 2021 10:00:45 AM	Jul 6, 2021 10:39:12 AM	Host Config, Broadcast
Intel 192.168.0.12	212.166.210.80	Jul 6, 2021 10:31:24 AM	Jul 6, 2021 10:31:33 AM	Snort Alert, DNS Server, DNS, Snort Misc
Intel 192.168.0.12	104.16.173.80	Jul 6, 2021 10:31:27 AM	Jul 6, 2021 10:31:29 AM	Insecure, Web, HTTP

New vulnerability detection

Cisco Cyber Vision 4.0.0 is now also detecting vulnerabilities on network equipment. Cisco Cyber Vision 4.0.0 detects vulnerabilities on switches, routers and firewalls from:

- Hirschmann
- Moxa
- Siemens
- Cisco

New vulnerability detection



10:56:46 *Security Events* The component SWLAB01.ccv 4c:71:0d:72:8c:03 (SWLAB01.ccv 4c:71:0d:72:8c:14) | | MAC : 4c:71:0d:72:8c:03 has been detected vulnerable to : Cisco IOx for IOS XE Software Command Injection Vulnerability, Cisco IOS XE SD-WAN Software Parameter Injection Vulnerabilities, Cisco IOS XE SD-WAN Software Privilege Escalation Vulnerability, Cisco IOS XE SD-WAN Software Command Injection Vulnerability, Cisco IOS XE Software for the Catalyst 9000 Family Arbitrary Code Execution Vulnerability, Cisco IOx Application Environment Path Traversal Vulnerability, Cisco IOS XE SD-WAN Software Parameter Injection Vulnerabilities.

SWLAB01.ccv 4c:71:0d:72:8c:03
See Technical sheet

Properties

Device: SWLAB01.ccv 4c:71:0d:72:8c:14
Name : SWLAB01.ccv 4c:71:0d:72:8c:03
MAC : 4c:71:0d:72:8c:03
Tag : Router
vulnerabilities detected **7**

Vulnerabilities

Cisco IOx for IOS XE Software Command Injection Vulnerability CVE-2021-1384 - cisco-sa-iox-cmdinj-RkSURGHG	**CVSS information** CVSS Score : **7.2** (v3.1) CVSS Temporal Score : **7.2** (v3.1)	**Links :** tools.cisco.com
Cisco IOS XE SD-WAN Software Parameter Injection Vulnerabilities CVE-2021-1454 - cisco-sa-xesdwpinj-V4weeqzU	**CVSS information** CVSS Score : **6.7** (v3.1) CVSS Temporal Score : **6.7** (v3.1)	**Links :** tools.cisco.com
	CVSS information CVSS Score : **6.7** (v3.1) CVSS Temporal Score : **6.7** (v3.1)	**Links :** tools.cisco.com
	CVSS information CVSS Score : **6.7** (v3.1) CVSS Temporal Score : **6.7** (v3.1)	**Links :** tools.cisco.com
	CVSS information CVSS Score : **6.8** (v3.1) CVSS Temporal Score : **6.8** (v3.1)	**Links :** tools.cisco.com
	CVSS information CVSS Score : **6.5** (v3) CVSS Temporal Score : **6.5** (v3)	**Links :** tools.cisco.com
	CVSS information CVSS Score : **6.7** (v3.1) CVSS Temporal Score : **6.7** (v3.1)	**Links :** tools.cisco.com

Component

SWLAB01.ccv 4c:71:0d:72:8c:03
SWLAB01.ccv 4c:71:0d:72:8c:14
IP: -
MAC: **4c:71:0d:72:8c:03**
Edit

First activity
Jul 6, 2021 10:56:20 AM
Last activity
Jul 6, 2021 10:59:18 AM

Tags
Router
Activity tags
Multicast, CDP

~10 Flows | 5 Events | 7 Vulnerabilities | - Credential | - Variable

Vulnerabilities 7

□ **Cisco IOx for IOS XE Software Command Injection Vulnerability**
CVE-2021-1384 — cisco-sa-iox-cmdinj-RkSURGHG
A vulnerability in Cisco IOx application hosting environment of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands
...show more

Solution
Please refer to Cisco's advisory for possible solutions

Published on March 24, 2021
Identified on this component on July 6, 2021
Identified vulnerable because of **cdp-version** (Cisco IOS Software [Bengaluru], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.4.1, RELEASE SOFTWARE (fc5) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2020 by Cisco Systems, Inc. Compiled Thu 26-Nov-20 23:35 by mcpre)

Links
tools.cisco.com

7.2
CVSS score (v3.1)

```
Access Vector: Network
Access Complexity: Low
Privileges Required: High
User Interaction: None
Scope: Unchanged
Confidentiality impact: High
Integrity impact: High
Availability impact: High
```

Acknowledge ?
Explain why

New protocol support

The Deep Packet Inspection (DPI) of the Cisco Cyber Vision sensor 4.0.0 was, as for each release, updated. Some protocols were added or updated. Cisco Cyber Vision 4.0.0 decodes now the NTCIP protocol (North America Roadways). Some improvements to the existing protocol support were made:

- Emerson ROC+ (Utilities)
- Yokogawa DCS (Chemicals and Oil&Gas)
- Ethernet/IP (Manufacturing)

Several additions or improvements were also made on the DPI service regarding:

- bittorent
- emule
- SNMP V3
- TLS with security improvement

In addition, Cisco Cyber Vision 4.0.0 Sensor Active Discovery can now send queries using ICMPv6.

Splunk integration

A new Cisco Cyber Vision add-on for Splunk is available. Cisco Cyber Vision add-on makes it easy to feed data into Splunk:

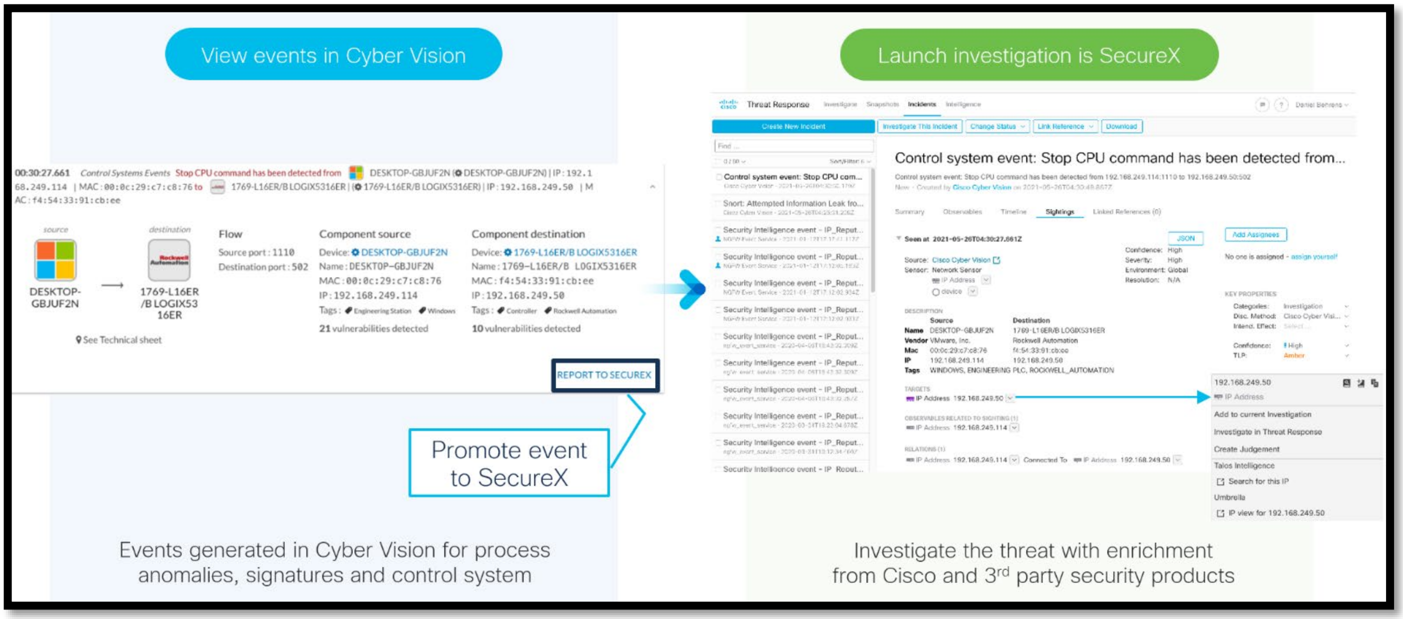
- Feeds the Splunk OT Security module.
- Adds Splunk dashboards specific to Cisco Cyber Vision.

Cisco Cyber Vision add-on is available on Splunk marketplace. Cisco Cyber Vision syslog configuration is needed to send the event to Splunk.

SecureX incidents

Cisco Cyber Vision 4.0.0 now offers to simplify IT/OT threat hunting with Cisco SecureX. Cisco Cyber Vision with SecureX enables a converged IT/OT threat management strategy. It makes things easier for OT teams to share relevant threat intel with IT/Security analysts. Cisco Cyber Vision 4.0.0 release brings a ‘One-click’ promotion of Cisco Cyber Vision security events for further investigation on SecureX. A button is available in the Cisco Cyber Vision event list to promote the event in SecureX. This promotion is available for the following categories:

- Signature-based detection events.
- Control systems events.
- Anomaly detection events.



View events in Cyber Vision

Launch investigation is SecureX

00:30:27.661 *Control Systems Events* Stop CPU command has been detected from DESKTOP-GBJUF2N (DESKTOP-GBJUF2N) | IP : 192.168.249.114 | MAC : 00:0c:29:c7:c8:76 to 1769-L16ER/B LOGIX5316ER | (1769-L16ER/B LOGIX5316ER) | IP : 192.168.249.50 | MAC : f4:54:33:91:cb:ee

Flow
Source port : 1110
Destination port : 502

Component source
Device: DESKTOP-GBJUF2N
Name : DESKTOP-GBJUF2N
MAC : 00:0c:29:c7:c8:76
IP : 192.168.249.114
Tags : Engineering Station Windows
21 vulnerabilities detected

Component destination
Device: 1769-L16ER/B LOGIX5316ER
Name : 1769-L16ER/B LOGIX5316ER
MAC : f4:54:33:91:cb:ee
IP : 192.168.249.50
Tags : Controller Rockwell Automation
10 vulnerabilities detected

Control system event: Stop CPU com...
Snort: Attempted Information Leak fro...
Security Intelligence event - IP_Reput...
Security Intelligence event - IP_Reput...
Security Intelligence event - IP_Reput...
Security Intelligence event - IP_Reput...
Security Intelligence event - IP_Reput...
Security Intelligence event - IP_Reput...
Security Intelligence event - IP_Reput...
Security Intelligence event - IP_Reput...
Security Intelligence event - IP_Reput...
Security Intelligence event - IP_Reput...

Control system event: Stop CPU command has been detected from...

Control system event: Stop CPU command has been detected from 192.168.249.114:1110 to 192.168.249.50:502
New · Created by Cisco Cyber Vision on 2021-05-26T04:30:48.867Z

Seen at 2021-05-26T04:30:27.861Z

Source: Cisco Cyber Vision
Sensor: Network Sensor

Confidence: High
Severity: High
Environment: Global
Resolution: N/A

No one is assigned - assign yourself

KEY PROPERTIES
Categories: Investigation
Disc. Method: Cisco Cyber Visi...
Intend. Effect: Select...
Confidence: High
TLP: Amber

DESCRIPTION

	Source	Destination
Name	DESKTOP-GBJUF2N	1769-L16ER/B LOGIX5316ER
Vendor	VMware, Inc.	Rockwell Automation
Mac	00:0c:29:c7:c8:76	f4:54:33:91:cb:ee
IP	192.168.249.114	192.168.249.50
Tags	WINDOWS, ENGINEERING PLC, ROCKWELL_AUTOMATION	

TARGETS
IP Address 192.168.249.50

OBSERVABLES RELATED TO SIGHTING (1)
IP Address 192.168.249.114

RELATIONS (1)
IP Address 192.168.249.114 Connected To IP Address 192.168.249.50

192.168.249.50
IP Address
Add to current Investigation
Investigate in Threat Response
Create Judgement
Talos Intelligence
Search for this IP
Umbrella
IP view for 192.168.249.50

Promote event to SecureX

Events generated in Cyber Vision for process anomalies, signatures and control system

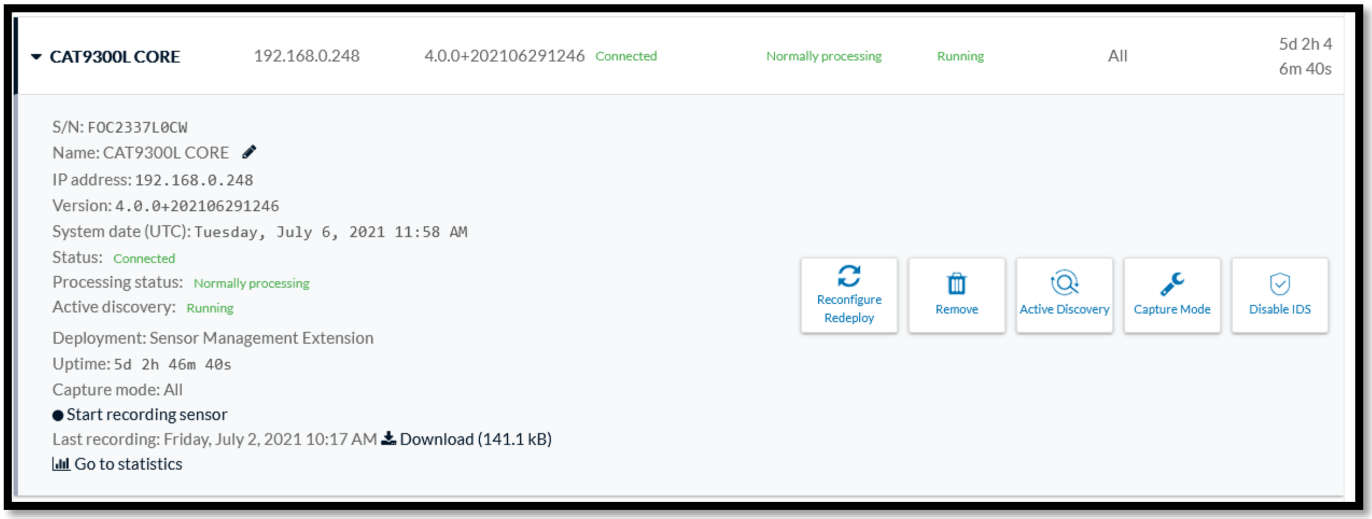
Investigate the threat with enrichment from Cisco and 3rd party security products

Simplified deployments

Catalyst 9000 Sensor now with IDS

Snort is now available on Catalyst 9300 running Cisco Cyber Vision Sensor application. It brings to the solution a new device capable to run the IDS:

IDS Snort on Sensor embedded in Catalyst 9300



CAT9300L CORE 192.168.0.248 4.0.0+202106291246 Connected Normally processing Running All 5d 2h 46m 40s

S/N: FOC2337L0CW
Name: CAT9300L CORE
IP address: 192.168.0.248
Version: 4.0.0+202106291246
System date (UTC): Tuesday, July 6, 2021 11:58 AM
Status: Connected
Processing status: Normally processing
Active discovery: Running
Deployment: Sensor Management Extension
Uptime: 5d 2h 46m 40s
Capture mode: All
● Start recording sensor
Last recording: Friday, July 2, 2021 10:17 AM Download (141.1 kB)
Go to statistics

Note:

When enabling IDS with subscriber rules on a Cat9K device an issue in Cyber Vision licensing module is causing an "out of compliance" answer from the Cisco Smart Software Manager.

This behavior will be changed in a future release. In the meantime if you are facing this issue, please contact support or your sales team to ask for an update of your license.

MSLA licenses

General remarks about licensing

Before performing any actions to license Cisco Cyber Vision products, users are invited to check their Smart account portal and verify that the relevant Smart Licenses are available (type and quantities).

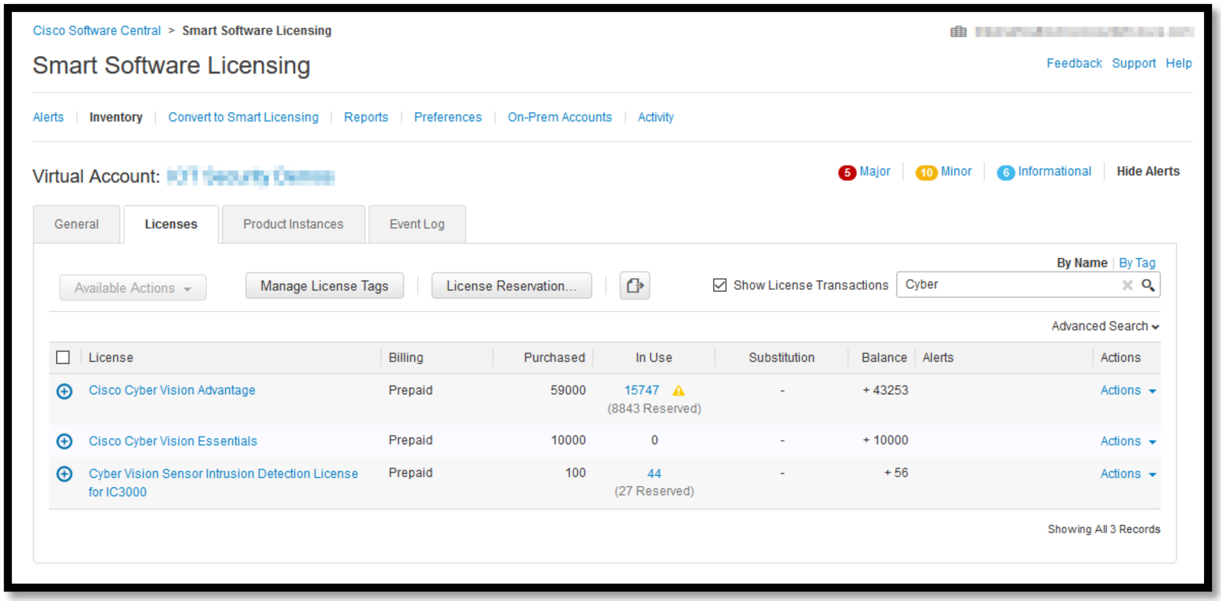
Smart Account: Central repository to view, store, and manage licenses across an entire organization. Software licenses, hardware, and subscriptions are accessible through a Smart Account. Smart Accounts are required to access and manage Smart License-enabled products.

Smart Licensing: Flexible software licensing capability that simplifies activating and managing licenses across an organization. The Smart Licensing capability makes it easier to procure, deploy, and manage Cisco on-prem software licenses. To use Smart Licensing, a Smart Account must first be set up.

For more information, navigate to: Cisco® Smart Licensing.

To check your Cisco Cyber Vision Licenses, access your Smart Account and navigate to Smart Software Licensing > Inventory > Licenses. Cisco Cyber Vision licenses must be available and appear in the Smart Software Licensing license list before proceeding with the registration of the product.

Cisco Cyber Vision Licenses



Cisco Software Central > Smart Software Licensing [redacted]

Smart Software Licensing

Feedback Support Help
Alerts | Inventory | Convert to Smart Licensing | Reports | Preferences | On-Prem Accounts | Activity

Virtual Account: [redacted]

5 Major | 10 Minor | 6 Informational | Hide Alerts
General | Licenses | Product Instances | Event Log
By Name | By Tag
Available Actions | Manage License Tags | License Reservation...
☑ Show License Transactions
Advanced Search

Search: Cyber

□ License	Billing	Purchased	In Use	Substitution	Balance	Alerts	Actions
Cisco Cyber Vision Advantage	Prepaid	59000	15747 ⚠ (8843 Reserved)	-	+ 43253		Actions
Cisco Cyber Vision Essentials	Prepaid	10000	0	-	+ 10000		Actions
Cyber Vision Sensor Intrusion Detection License for IC3000	Prepaid	100	44 (27 Reserved)	-	+ 56		Actions

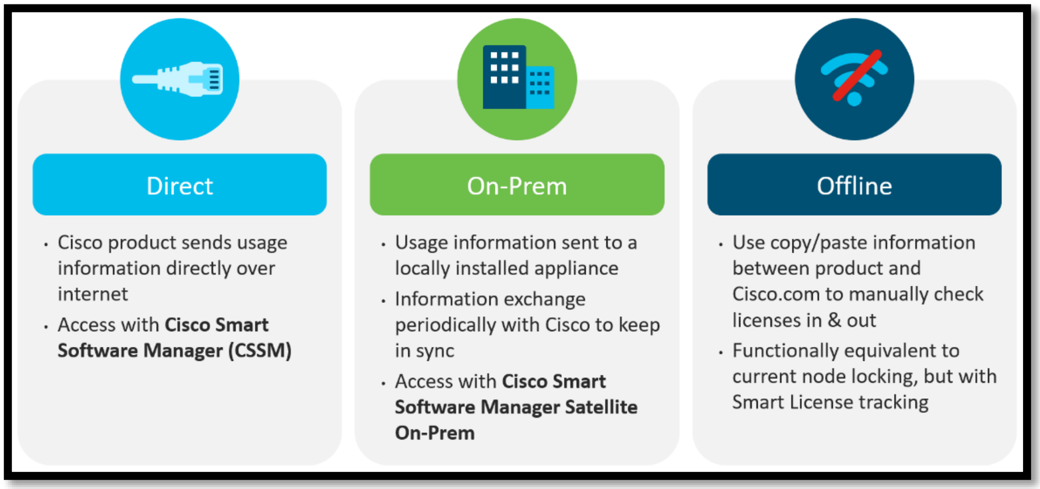
Showing All 3 Records

If you plan to use an offline license, you need to check that your Smart Account can perform a “License Reservation” (check from the License menu that the License reservation button is enabled). If your account doesn’t have the rights to do so, please open a case and provide a business justification.

Compatibility with Smart Software Manager Satellite

Cisco Cyber Vision Release 4.0.0 now supports the Smart Software Manager Satellite as license provider, and its different deployment options.

Cisco Cyber Vision deployment options



Direct

- Cisco product sends usage information directly over internet
- Access with **Cisco Smart Software Manager (CSSM)**

On-Prem

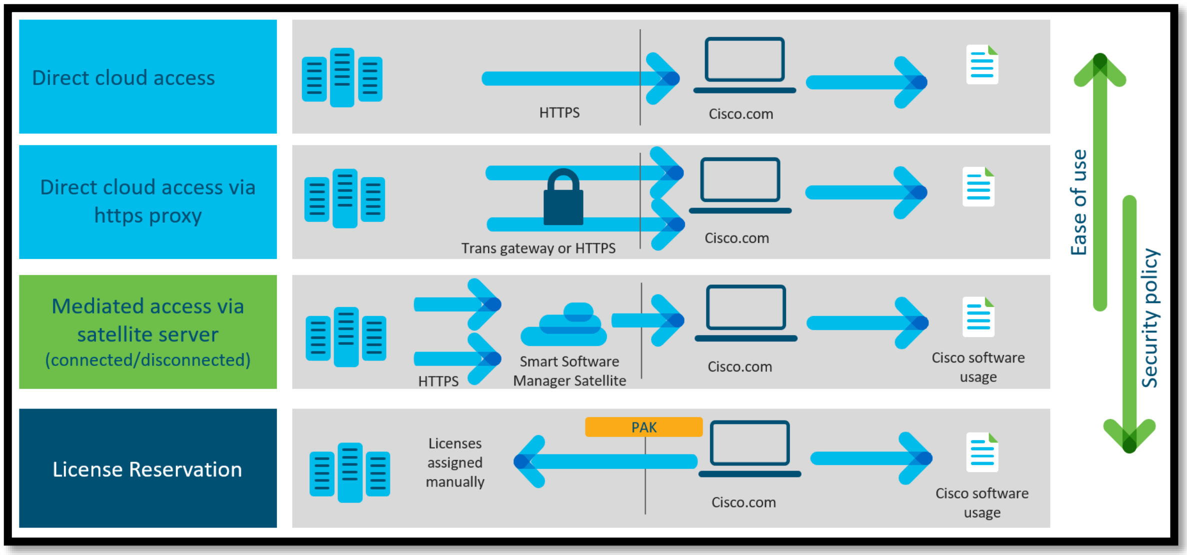
- Usage information sent to a locally installed appliance
- Information exchange periodically with Cisco to keep in sync
- Access with **Cisco Smart Software Manager Satellite On-Prem**

Offline

- Use copy/paste information between product and Cisco.com to manually check licenses in & out
- Functionally equivalent to current node locking, but with Smart License tracking

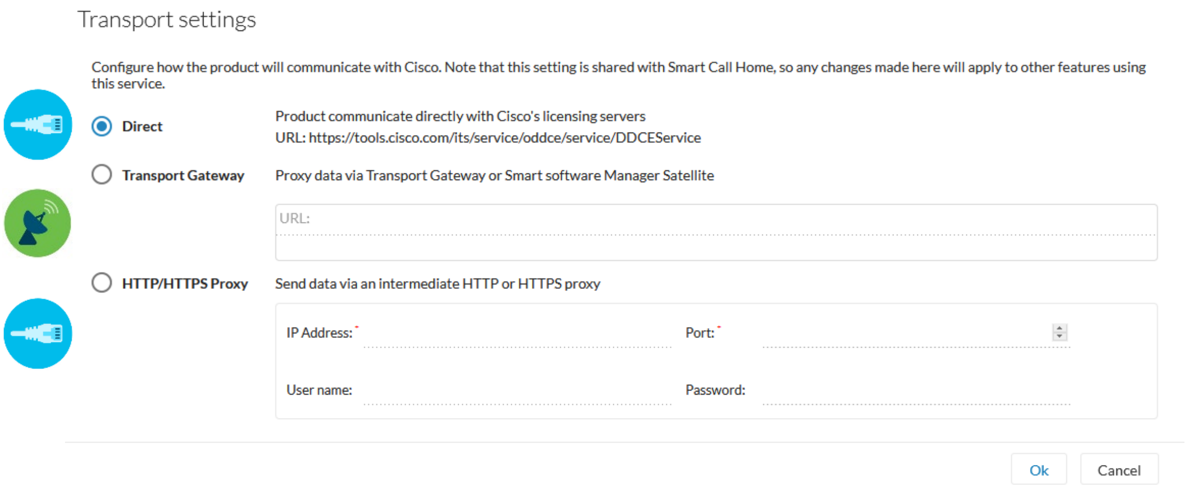
To register Cisco Cyber Vision licensed products, Smart Licensing has different modes depending on the level of security desired:

Cisco Cyber Vision Smart Licensing deployment modes



Cisco Cyber Vision release 4.0.0 can now use all deployment options and transport modes. In Cisco Cyber Vision, navigate to Administration > License > “edit the Smart Call Home Transport Settings” to configure transport settings.

Cisco Cyber Vision Licensing transport settings



Transport settings

Configure how the product will communicate with Cisco. Note that this setting is shared with Smart Call Home, so any changes made here will apply to other features using this service.

● Direct — Product communicate directly with Cisco's licensing servers
URL: https://tools.cisco.com/its/service/oddce/service/DDCEService

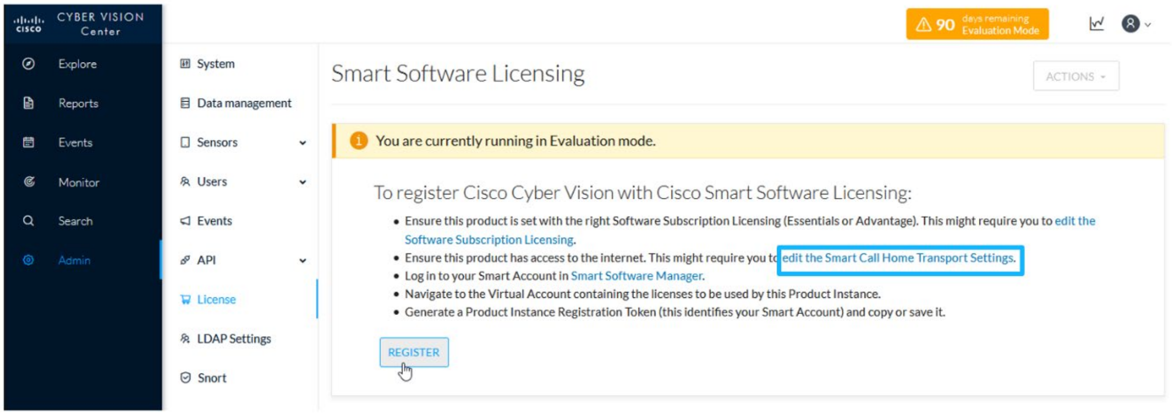
○ Transport Gateway — Proxy data via Transport Gateway or Smart software Manager Satellite
URL:

○ HTTP/HTTPS Proxy — Send data via an intermediate HTTP or HTTPS proxy
IP Address:*
Port:*
User name:
Password:

- Direct: a direct access to the cloud is enabled. A Product Instance Registration Token needs to be collected from the Smart Software Manager to complete registration.
- Transport gateway: an access to the Smart software Manager Satellite is enabled. A Product Instance Registration Token needs to be collected from the Smart Software Manager Satellite to complete registration.
- HTTP/HTTPS Proxy: a direct access to the cloud through a Proxy is enabled. A Product Instance Registration Token needs to be collected from the Smart Software Manager to complete registration.

Once the transport settings are filled, use the Register button to register the product in the Smart Software Manager. The Register button is available in the License Administration page of Cisco Cyber Vision.

Cisco Cyber Vision License Menu with the link to edit the transport settings and the Register button



Smart Software Licensing

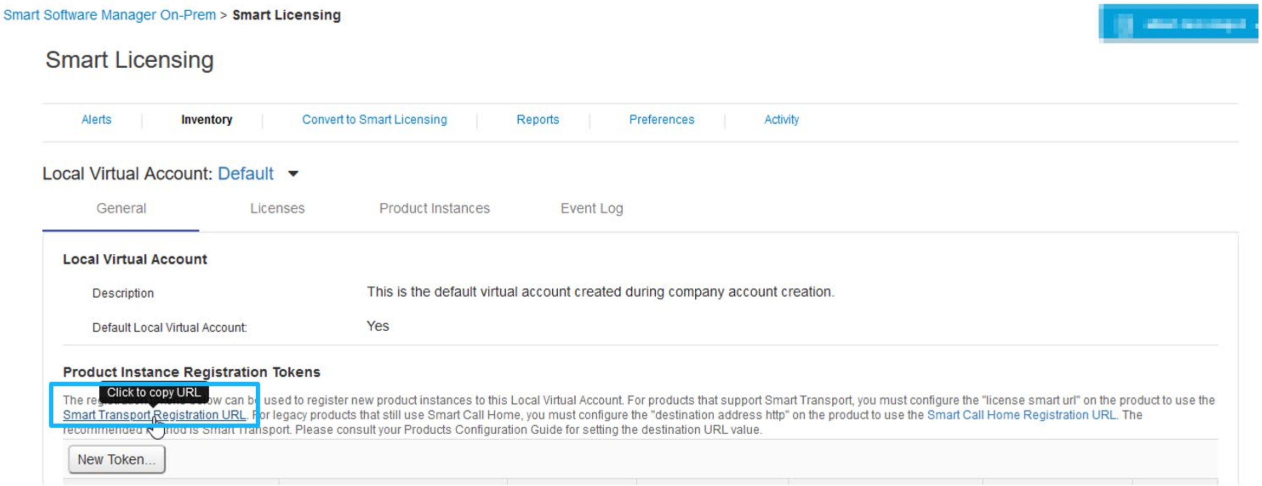
You are currently running in Evaluation mode.

To register Cisco Cyber Vision with Cisco Smart Software Licensing:

- Ensure this product is set with the right Software Subscription Licensing (Essentials or Advantage). This might require you to edit the Software Subscription Licensing.
- Ensure this product has access to the internet. This might require you to edit the Smart Call Home Transport Settings.
- Log in to your Smart Account in Smart Software Manager.
- Navigate to the Virtual Account containing the licenses to be used by this Product Instance.
- Generate a Product Instance Registration Token (this identifies your Smart Account) and copy or save it.

You will find the Smart software Manager Satellite URL in the On-Prem Smart Software Manager.

Smart software Manager Menu to copy the URL



Smart Software Manager On-Prem > **Smart Licensing**

Smart Licensing

Local Virtual Account: Default

Local Virtual Account

Description: This is the default virtual account created during company account creation.

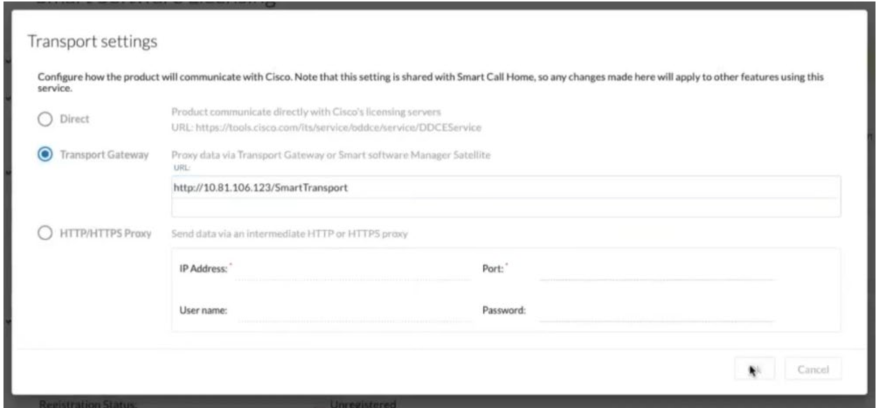
Default Local Virtual Account: Yes

Product Instance Registration Tokens

The re[illegible]w can b[illegible] used to register new product instances to this Local Virtual Account. For products that support Smart Transport, you must configure the "license smart url" on the product to use the Smart Transport Registration URL. For legacy products that still use Smart Call Home, you must configure the "destination address http" on the product to use the Smart Call Home Registration URL. The recommended [illegible] is Smart Transport. Please consult your Products Configuration Guide for setting the destination URL value.

In Cisco Cyber Vision, paste the URL in Transport Settings:

Smart software Manager Menu to copy the URL



Transport settings

Configure how the product will communicate with Cisco. Note that this setting is shared with Smart Call Home, so any changes made here will apply to other features using this service.

○ Direct — Product communicate directly with Cisco's licensing servers
URL: https://tools.cisco.com/its/service/oddce/service/DDCEService

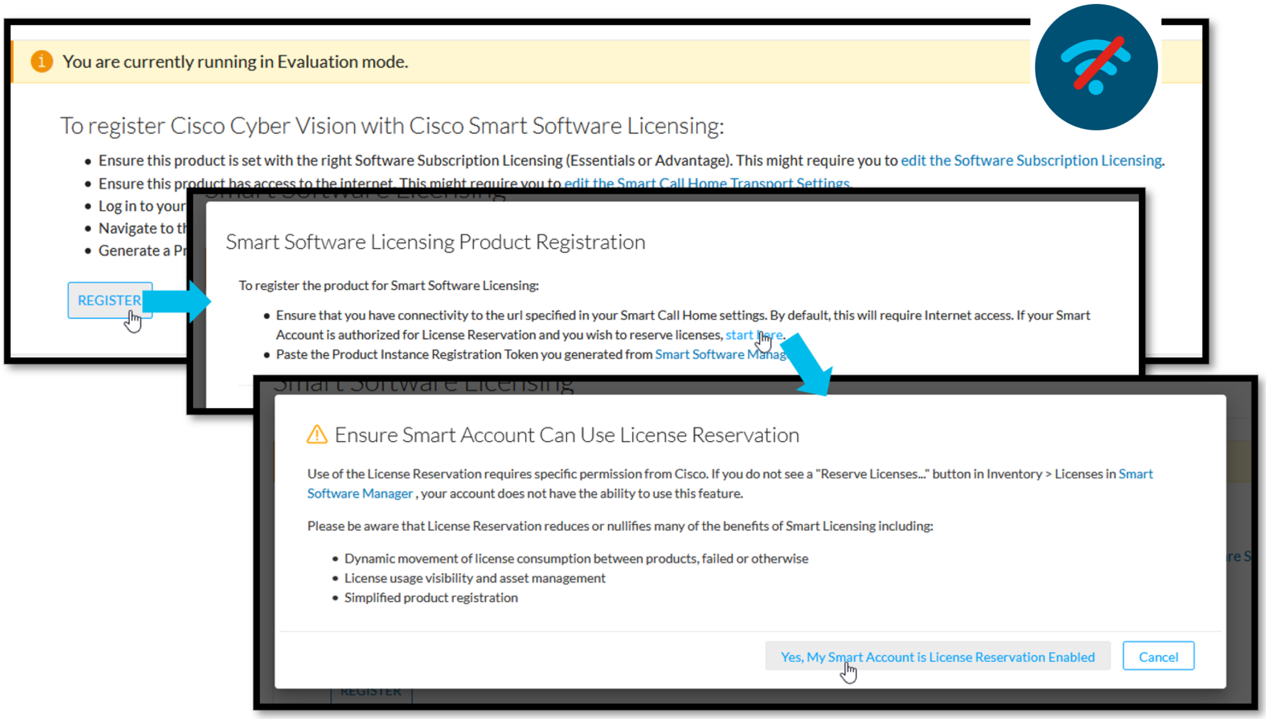
● Transport Gateway — Proxy data via Transport Gateway or Smart software Manager Satellite
URL: http://10.81.106.123/SmartTransport

○ HTTP/HTTPS Proxy — Send data via an intermediate HTTP or HTTPS proxy
IP Address: * Port: *
User name: Password:

A Token needs to be generated from the Smart software Manager Satellite to register Cisco Cyber Vision.

The License Reservation is accessible through the Register button, with the following procedure:

Cisco Cyber Vision Reservation settings



You are currently running in Evaluation mode.

To register Cisco Cyber Vision with Cisco Smart Software Licensing:

- Ensure this product is set with the right Software Subscription Licensing (Essentials or Advantage). This might require you to edit the Software Subscription Licensing.
- Ensure this product has access to the internet. This might require you to edit the Smart Call Home Transport Settings.
- Log in to your
- Navigate to th
- Generate a Pr

Smart Software Licensing Product Registration

To register the product for Smart Software Licensing:

- Ensure that you have connectivity to the url specified in your Smart Call Home settings. By default, this will require Internet access. If your Smart Account is authorized for License Reservation and you wish to reserve licenses, start here.
- Paste the Product Instance Registration Token you generated from Smart Software Manag

⚠ Ensure Smart Account Can Use License Reservation

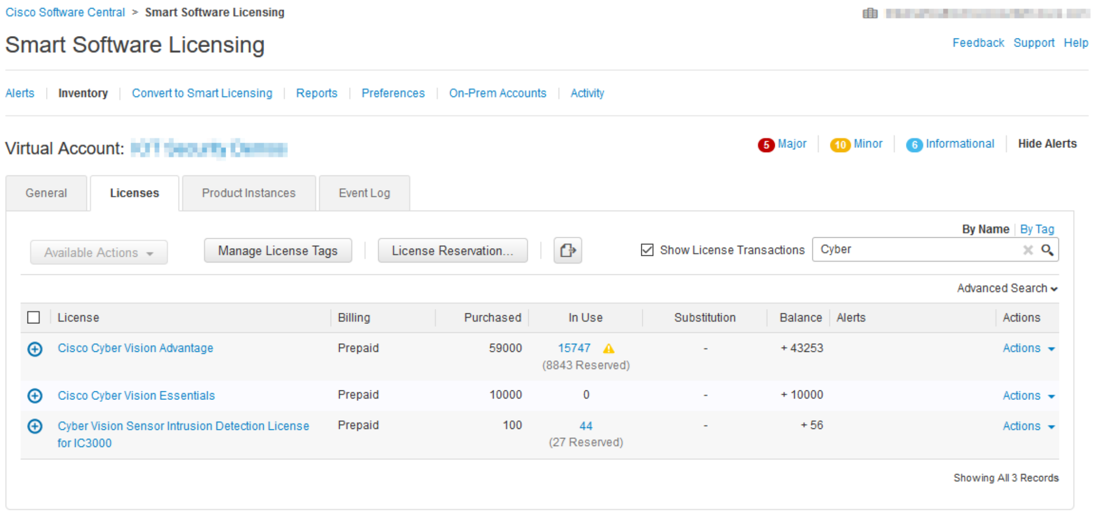
Use of the License Reservation requires specific permission from Cisco. If you do not see a "Reserve Licenses..." button in Inventory > Licenses in Smart Software Manager , your account does not have the ability to use this feature.

Please be aware that License Reservation reduces or nullifies many of the benefits of Smart Licensing including:

- Dynamic movement of license consumption between products, failed or otherwise
- License usage visibility and asset management
- Simplified product registration

If you plan to use an offline license, you need to check that your Smart Account can perform a "License Reservation" (check from the License menu that the License reservation button is enabled). If your account doesn't have the rights to do so, please open a case and provide a business justification.

Cisco Cyber Vision Licenses with "License Reservation…" button enabled



Cisco Software Central > Smart Software Licensing [redacted]

Smart Software Licensing

Feedback Support Help
Alerts | Inventory | Convert to Smart Licensing | Reports | Preferences | On-Prem Accounts | Activity

Virtual Account: [redacted]

5 Major | 10 Minor | 6 Informational | Hide Alerts
General
Licenses
Product Instances
Event Log
By Name | By Tag
Available Actions
Manage License Tags
License Reservation...
Advanced Search

☑ Show License Transactions

Cyber

☐ License	Billing	Purchased	In Use	Substitution	Balance	Alerts	Actions
Cisco Cyber Vision Advantage	Prepaid	59000	15747 ⚠ (8843 Reserved)	-	+ 43253		Actions
Cisco Cyber Vision Essentials	Prepaid	10000	0	-	+ 10000		Actions
Cyber Vision Sensor Intrusion Detection License for IC3000	Prepaid	100	44 (27 Reserved)	-	+ 56		Actions

Showing All 3 Records

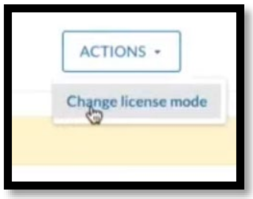
MSLA - Managed Service License Agreement

Managed Service License Agreement is a buying program under which managed service providers receive the right to use Cisco software and/or cloud services (including support).

Note: Smart Software Manager Satellite instance is required to use MSLA.

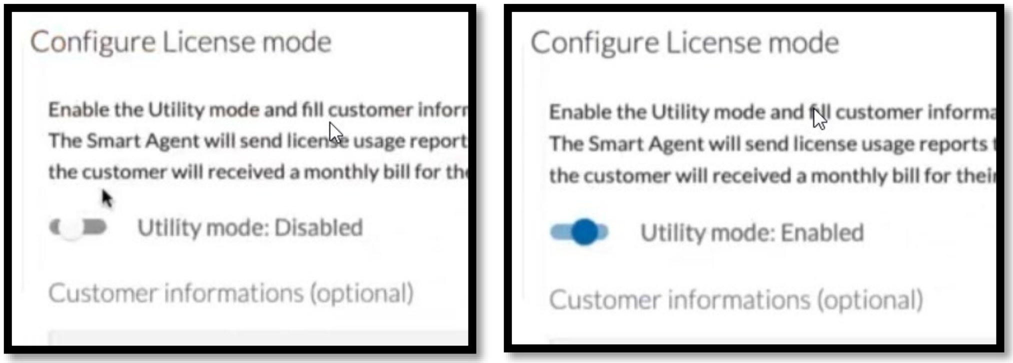
Once Cisco Cyber Vision License transport settings are configured to use a Smart Software Manager Satellite, the License mode can be changed. Click the Actions button on the top right corner of the License page to enable the License mode:

Cisco Cyber Vision Change License Mode action



Enable the Utility mode:

Cisco Cyber Vision Licensing Utility Mode button.


Configure License mode

Enable the Utility mode and fill customer inforr
The Smart Agent will send license usage report
the customer will received a monthly bill for th

Utility mode: Disabled

Customer informations (optional)

Configure License mode

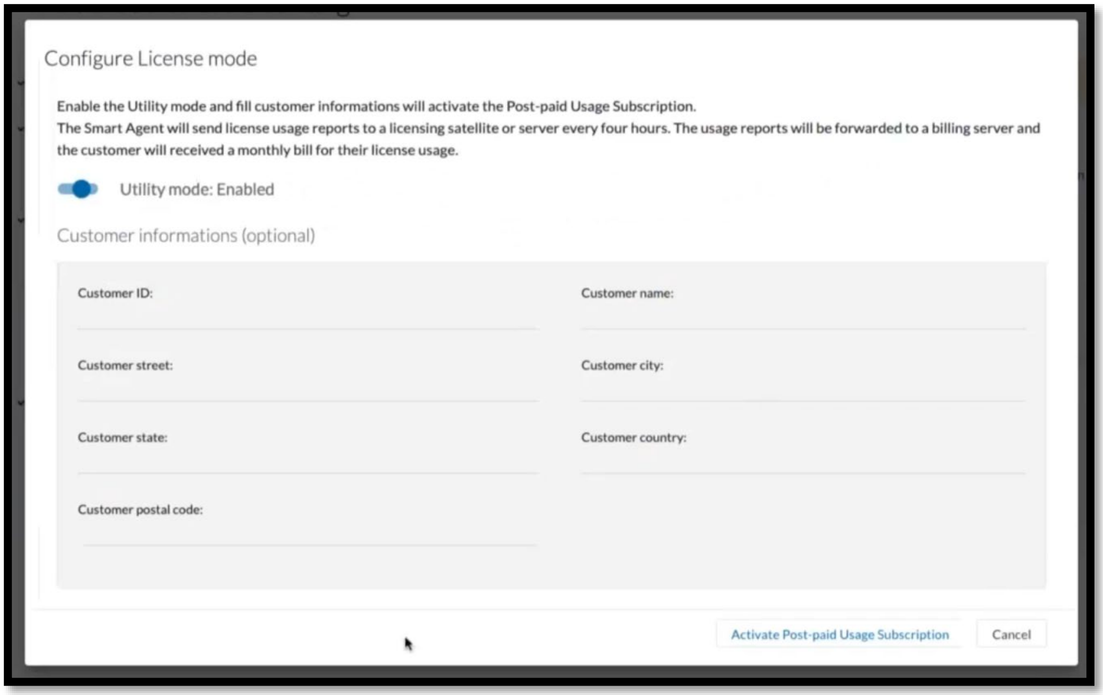
Enable the Utility mode and fill customer informa
The Smart Agent will send license usage reports t
the customer will received a monthly bill for thei

Utility mode: Enabled

Customer informations (optional)

Click the “Activate Post-paid Subscription” button.

Cisco Cyber Vision Licensing Activate



Configure License mode

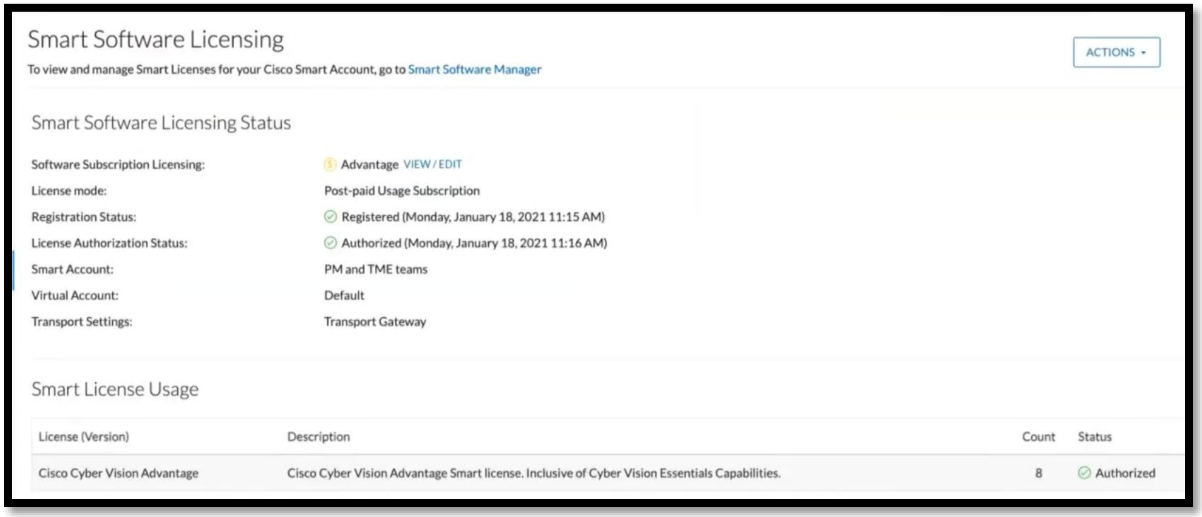
Enable the Utility mode and fill customer informations will activate the Post-paid Usage Subscription.
The Smart Agent will send license usage reports to a licensing satellite or server every four hours. The usage reports will be forwarded to a billing server and the customer will received a monthly bill for their license usage.

Utility mode: Enabled

Customer informations (optional)

Customer ID:	Customer name:
Customer street:	Customer city:
Customer state:	Customer country:
Customer postal code:	

The license is enabled, and the license mode is displayed as “Post-paid Usage Subscription”.



Smart Software Licensing

To view and manage Smart Licenses for your Cisco Smart Account, go to Smart Software Manager

Smart Software Licensing Status

Software Subscription Licensing:	Advantage VIEW / EDIT
License mode:	Post-paid Usage Subscription
Registration Status:	Registered (Monday, January 18, 2021 11:15 AM)
License Authorization Status:	Authorized (Monday, January 18, 2021 11:16 AM)
Smart Account:	PM and TME teams
Virtual Account:	Default
Transport Settings:	Transport Gateway

Smart License Usage

License (Version)	Description	Count	Status
Cisco Cyber Vision Advantage	Cisco Cyber Vision Advantage Smart license. Inclusive of Cyber Vision Essentials Capabilities.	8	Authorized

New license type

Cisco Cyber Vision Release 4.0.0 supports a new license type:

- Cisco Cyber Vision Sensor Intrusion Detection License for Center

DPI licensing is based on the number of active DPI interfaces.

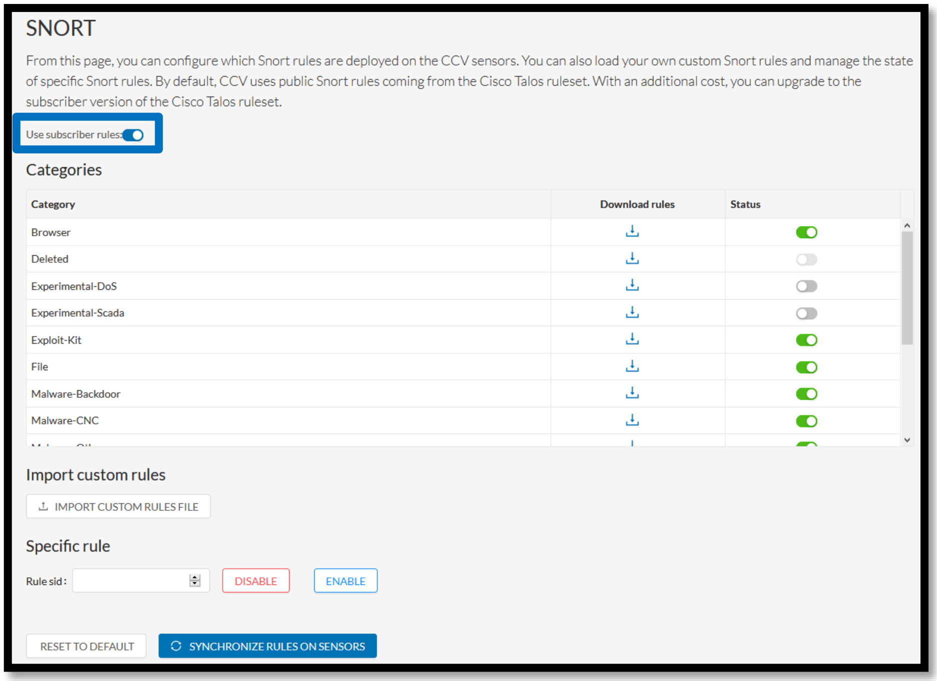
Cisco Cyber Vision Licenses:

- Cisco Cyber Vision Advantage
- Cisco Cyber Vision Essentials
- Cisco Cyber Vision Sensor Intrusion Detection License for IC3000
- Cisco Cyber Vision Sensor Intrusion Detection License for Center

IDS and Snort community rule sets are included in the Advantage license level, with the support for custom Snort rules.

An Intrusion Detection License is required to use the Snort subscriber rule set. A new option is available in the SNORT administration page to select if the solution will use subscriber rules.

Cisco Cyber Vision Activate Subscriber rules



SNORT

From this page, you can configure which Snort rules are deployed on the CCV sensors. You can also load your own custom Snort rules and manage the state of specific Snort rules. By default, CCV uses public Snort rules coming from the Cisco Talos ruleset. With an additional cost, you can upgrade to the subscriber version of the Cisco Talos ruleset.

Use subscriber rules: ●

Categories

Category	Download rules	Status
Browser	⤓	●
Deleted	⤓	○
Experimental-DoS	⤓	○
Experimental-Scada	⤓	○
Exploit-Kit	⤓	●
File	⤓	●
Malware-Backdoor	⤓	●
Malware-CNC	⤓	●

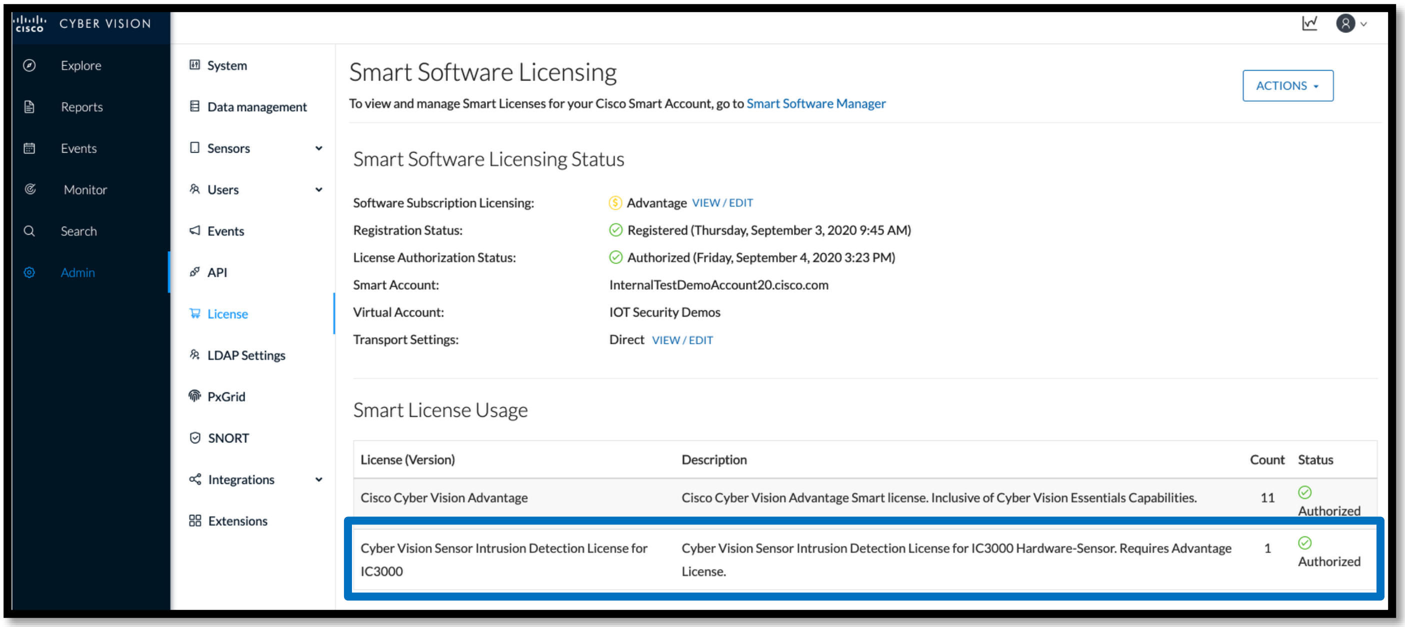
Import custom rules

Specific rule

Rule sid :

Once Subscriber Rules are activated, Intrusion Detection Licenses are required.

Cisco Cyber Vision IDS License



Smart Software Licensing

To view and manage Smart Licenses for your Cisco Smart Account, go to Smart Software Manager

Smart Software Licensing Status

Software Subscription Licensing:	Advantage VIEW / EDIT
Registration Status:	✓ Registered (Thursday, September 3, 2020 9:45 AM)
License Authorization Status:	✓ Authorized (Friday, September 4, 2020 3:23 PM)
Smart Account:	InternalTestDemoAccount20.cisco.com
Virtual Account:	IOT Security Demos
Transport Settings:	Direct VIEW / EDIT

Smart License Usage

License (Version)	Description	Count	Status
Cisco Cyber Vision Advantage	Cisco Cyber Vision Advantage Smart license. Inclusive of Cyber Vision Essentials Capabilities.	11	✓ Authorized
Cyber Vision Sensor Intrusion Detection License for IC3000	Cyber Vision Sensor Intrusion Detection License for IC3000 Hardware-Sensor. Requires Advantage License.	1	✓ Authorized

Support for Center in AWS

Cisco Cyber Vision Center is available in the AWS marketplace for customers to deploy their own instance in the Cloud. Amazon VirtualPrivate Cloud (Amazon VPC) enables you to launch Amazon WebServices (AWS) resources into a virtual network that you define. This virtual network closely resembles a traditional network that might operate in your own data Center, with the benefits of using the scalable infrastructure of AWS. Cisco Cyber Vision Virtual center can be now deployed on AWS.

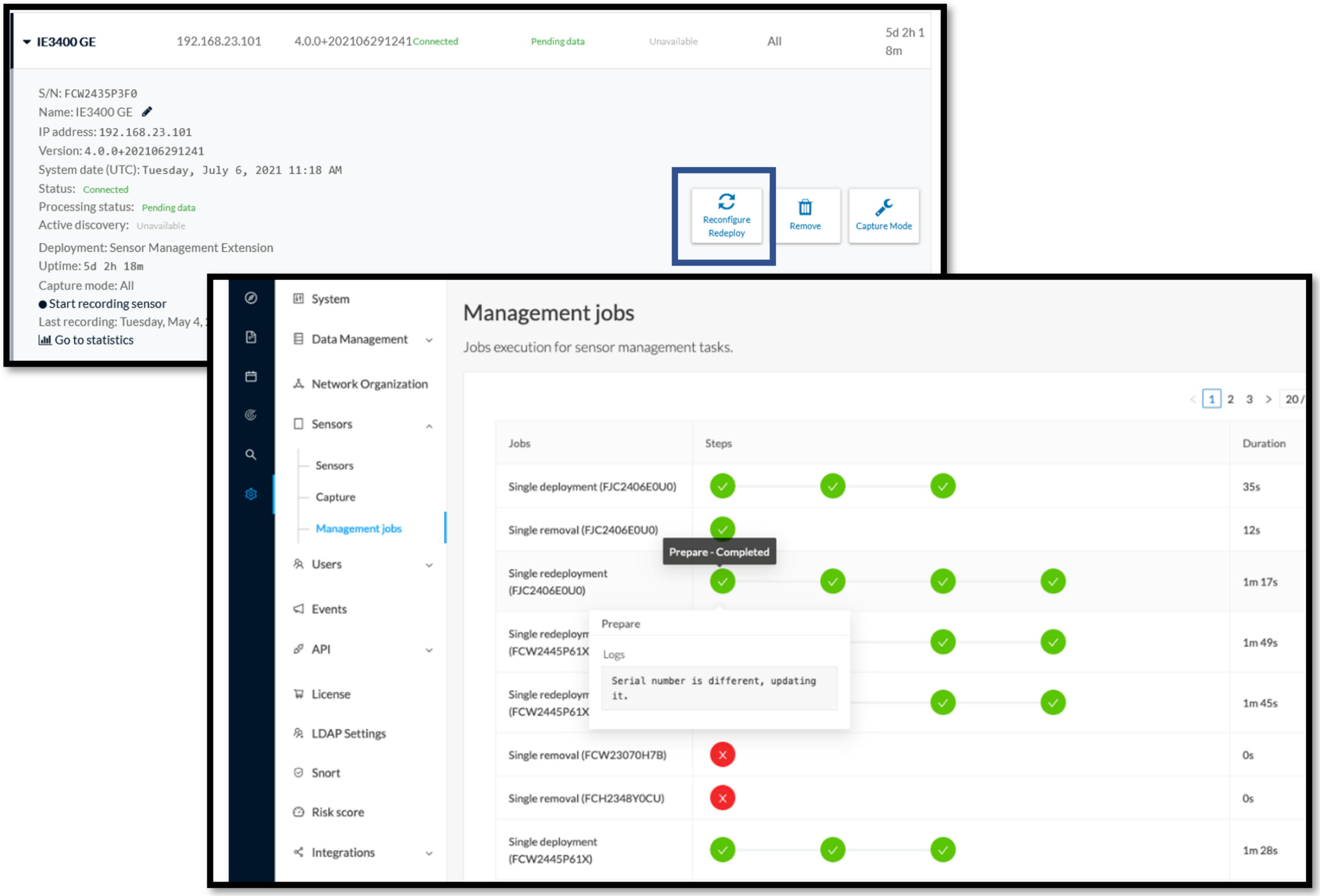
Simplifying sensor deployments

Cisco Cyber Vision Release 4.0.0 brings a new feature to manage IOx sensors. This feature will help to deploy a single sensor and handle several maintenance cases like:

- Switch replacement (e.g. IE3400 to another IE3400)
- Switch upgrade (e.g. IE3400 to a Catalyst 9300)
- Sensor application change (e.g. with or without active discovery)

The different tasks will be monitored in a new “Jobs execution for sensor management tasks” page which shows job status:

Sensor Management Jobs



IE3400 GE 192.168.23.101 4.0.0+202106291241 Connected Pending data Unavailable All 5d 2h 18m

S/N: FCW2435P3F0
Name: IE3400 GE
IP address: 192.168.23.101
Version: 4.0.0+202106291241
System date (UTC): Tuesday, July 6, 2021 11:18 AM
Status: Connected
Processing status: Pending data
Active discovery: Unavailable
Deployment: Sensor Management Extension
Uptime: 5d 2h 18m
Capture mode: All
● Start recording sensor
Last recording: Tuesday, May 4,
Go to statistics

Management jobs

Jobs execution for sensor management tasks.

Jobs	Steps	Duration
Single deployment (FJC2406E0U0)	✓ ✓ ✓	35s
Single removal (FJC2406E0U0)	✓	12s
Single redeployment (FJC2406E0U0)	✓ ✓ ✓ ✓	1m 17s
Single redeploym (FCW2445P61X	✓ ✓	1m 49s
Single redeploym (FCW2445P61X	✓ ✓	1m 45s
Single removal (FCW23070H7B)	✗	0s
Single removal (FCH2348Y0CU)	✗	0s
Single deployment (FCW2445P61X)	✓ ✓ ✓	1m 28s

Prepare - Completed

Prepare

Logs

```
Serial number is different, updating
it.
```

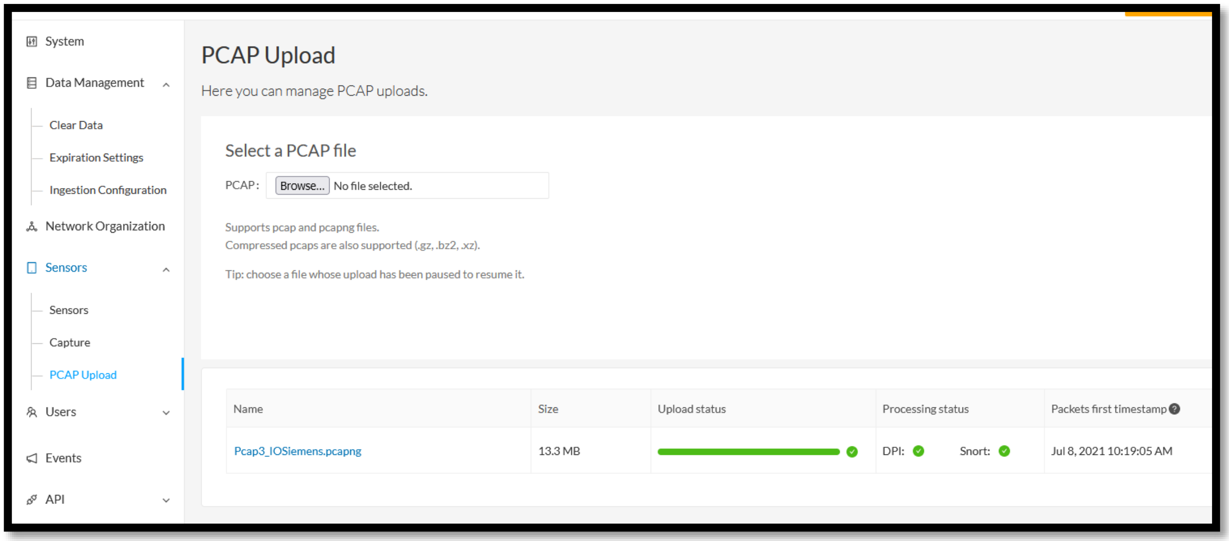
Mass scale deployments via Ansible scripts

Cisco Cyber Vision 4.0.0 API was changed to enable sensor deployment through the API. It enables simplified workflow for mass deployment via the Cisco Cyber Vision API. Some Ansible scripts are available to use it and deploy all types of sensors.

PCAP import

A new page is available in the Cisco Cyber vision Admin menu to import pcap files in the Center. This new feature will simplify demonstration done with the product. It allows users to add data without using any command line.

PCAP upload



PCAP Upload

Here you can manage PCAP uploads.

Select a PCAP file

PCAP: Browse... No file selected.

Supports pcap and pcapng files.
Compressed pcaps are also supported (.gz, .bz2, .xz).

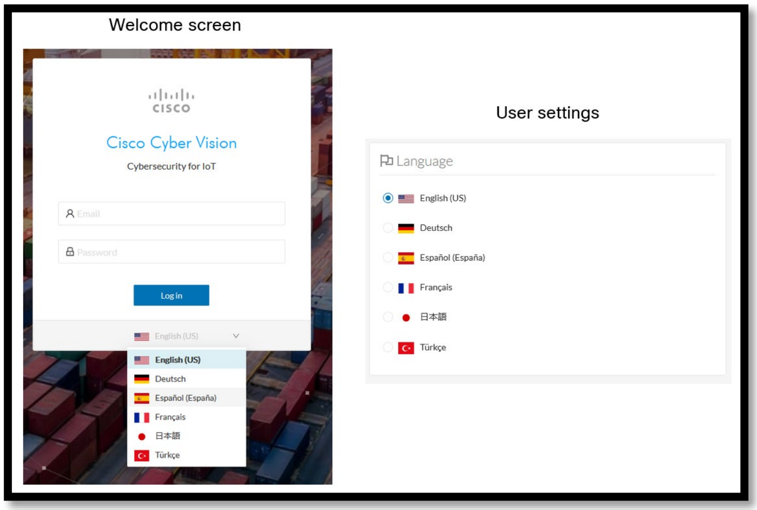
Tip: choose a file whose upload has been paused to resume it.

Name	Size	Upload status	Processing status	Packets first timestamp
Pcap3_IOSiemens.pcapng	13.3 MB	✓	DPI: ✓ Snort: ✓	Jul 8, 2021 10:19:05 AM

New UI languages

Cisco Cyber Vision is now available in 6 different languages:

Languages



Language

● English (US)
○ Deutsch
○ Español (España)
○ Français
○ 日本語
○ Türkçe

Cisco Cyber Vision Bug fixed

Issues ID / CDETS	Description
#6889 / CSCvx20904	Sensor Management Extension - Unable to change password after application deployed
#7863 / CSCvy44848	Flow panic with CIP protocol
#7645 / CSCvy14777	Syslog over TLS is not working
#8052 / CSCvz02532	API GET /components/{id} doesn't retrieve the ‘userProperties’ as documentation said
#- / CSCvy90252	Time management tag is not in the right position
#8174 / CSCvy83222	Migration of component IDs exhaust memory when there are too many flows
#8005 / CSCvy54003	Cisco Cyber Vision 4.0 Beta - Incorrect Device Generation
#7974 / CSCvy53149	Sensor performance degradation over time
#7861 / CSCvy44622	OOM error on IC3000 sensor
#7950 / CSCvy44621	Bogus filter syntax when a manual enrollment package is regenerated
#7949 / CSCvy44609	ssh connection failure not detected when updating the capture mode on hardware sensors
#7730 / CSCvy27818	Sensor cannot be deployed if extension has seen an older version
#7708 / CSCvy22752	Decode Error on Ethernet Type 34968
#7719 / CSCvy21319	Several flow properties are relative to a communication and should not be attached to components
#7795 / CSCvx80604	Cisco Cyber Vision Center displays Sensor is disconnected though sensor is reachable from CVC

Issues ID / CDETS	Description
#7794 / CSCvx64116	Sensor deployment with extension does not work in certain conditions
#7793 / CSCvx07418	Incorrect Component Count for Licensing
#4826 / CSCvu80810	Sensor app upgrade via cli fails and sensor cannot be activated again

Cisco Cyber open CDETS and known issues

Issues ID / CDETS	Component	Description
#8158 /	Global Center	Cisco Cyber Vision Global Center Data Management menu gives to the user the ability to purge data, but it will affect the synchronization with all synchronized CENTERS. Purge options will be disabled in next release.
#7808 / CSCvy30877	Centers	RPC-DCOM flows often not tagged: cannot selectively delete and appear in security insights
#8192 / CSCvy83325	Catalyst	The extension installs to a Catalyst 9300 in Stackwise-480 with 2 SSDs fails.
#8309 / CSCvz02406	Catalyst	IDS on Cat9k caused out of compliance license.
#8333 /	Centers	Double DNS_Server tags. Some DNS_Server components tags are badly added to activities (linked mDNS protocol).
#8302 /	Centers	Too many Cyber Vision event and syslog message when some Gateways detected by the product