



Release Notes for Cisco Cyber Vision

Release 4.3.0

WARNING:

For users upgrading to 4.3.0 from previous versions:

- Please read the Cisco Cyber Vision 4.3.0 update procedure carefully.
- Please check the networking configurations before and after the upgrade, see Upgrade to 4.3.0 considerations.
- For IC3000 users, please read with attention: IC3000 considerations

SUMMARY

Compatible device list	4
Unsupported device list	5
Cisco Cyber Vision 4.3.0 update procedure	6
Warnings	6
Upgrade Path	6
Compatibility Guidelines	7
Data purge	7
Upgrade to 4.3.0 considerations	8
IC3000 considerations	10
Limitations	10
Upgrade with the extension	11
Installation with the extension	13
Manual Installation:	13
Center updates	14
Architecture with Global Center	14
Architecture with one Center	17
AWS and Azure Centers	18
Cisco Cyber Vision 4.3.0 important changes	19
Communication port and protocol changes	19
Port	19
Protocol	19
API	19
SYSLOG	19
Cisco Cyber Vision new features and improvements	22
External communication	22
Introduction	22
Internal vs External	23
External communication impact in the UI	23
Subnetting for network organization	25
Network Organization configuration	25
Network Organization API	27
Network Organization impact on Cyber Vision	27
Sensor templates	28
New report feature	31
Report extension setup:	31
To create and run a report:	32
IC3000 sensor application migration	33
Monitor mode changes	34
Active Discovery changes	36

UI diagnostic enhancement	37
Cisco Cyber Vision 4.3.0 enhancements	38
Cisco Cyber Vision 4.3.0 Resolved Caveats	39
Cisco Cyber Vision Open Caveats	40
Links	41
Software Download	41
Related Documentation	43

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
AWS – Center AMI	Amazon Web Services center image
Azure – Center plan	Microsoft Azure center plan

Platform	Minimum Version	Description
Cisco IC3000	1.5.1	Cyber Vision Sensor hardware appliance
Cisco Catalyst IE3400	17.3.x	Cyber Vision Sensor IOx application hosted in Cisco Catalyst IE3400 Industrial Ethernet switches
Cisco Catalyst IE3300 10G	17.6.x	Cyber Vision Sensor IOx application hosted in Cisco Catalyst IE3300 Industrial Ethernet switches with 10G ports
Cisco Catalyst IE3300 *	17.11.x	Cyber Vision Sensor IOx application hosted in Cisco Catalyst IE3300 Industrial Ethernet switches
Cisco Catalyst IE9300	17.12.x	Cyber Vision Sensor IOx application hosted in Cisco Catalyst IE9300 Rugged Series switches (IOS 17.12 mini)
Cisco IR1101	17.3.x	Cyber Vision Sensor IOx application hosted in Cisco IR1101 Series Industrial Integrated Services Routers
Cisco Catalyst IR8300	17.9.x	Cyber Vision Sensor IOx application hosted in Cisco Catalyst IR8300 Rugged Series Routers
Cisco Catalyst 9300, 9400	17.3.x	Cyber Vision Sensor IOx application hosted in Catalyst 9300, 9300X, 9400 Series switches

* IE3300 support Cyber Vision application hosting when the platform has 4GB DRAM.

All 4G units start with Version ID (VID) from -06. A CLI command could be used to identify whether its 2G vs 4G, looking at the Max DRAM size of `show platform resources`.

IE switches recommended firmware are: 17.12.1, 17.9.5, 17.6.6.

Unsupported device list

As of version 4.2.0, [Sentryo hardware is no longer supported](#).

Center	Description
Sentryo CENTER10	Sentryo CENTER10 hardware appliance
Sentryo CENTER30	Sentryo CENTER30 hardware appliance
Sensor	
Sentryo SENSOR3	Sentryo SENSOR3 hardware appliance
Sentryo SENSOR5	Sentryo SENSOR5 hardware appliance
Sentryo SENSOR7	Sentryo SENSOR7 hardware appliance

Cisco Cyber Vision 4.3.0 update procedure

Cisco Cyber Vision 4.3.0 update procedure depends on the architecture deployed and the tool used to deploy it.

Warnings

Cisco Cyber Vision version 4.3.0 brings 2 new features which impact the upgrade procedure:

1. IC3000 application change
2. External communications-

For IC3000 application change: [click here](#). For external communications: check the Cyber Vision [network configuration](#) before and after the product upgrade. Network configuration may have an impact on the product database. **Some data stored may be purged** based on it. Find explanations to prepare the product and review the configuration applied.

Upgrade Path

Upgrade Path to Cisco Cyber Vision 4.3.0

Current Software Release	Upgrade Path to Release 4.3.0
If version prior to 3.2.4	Upgrade first to 3.2.4, then to 4.0.0, then to 4.1.4, then to 4.3.0
Version 3.2.4	Upgrade first to 4.0.0, then to 4.1.4, then to 4.3.0
Version 4.0.0 to 4.0.3	Upgrade first to 4.1.4, then to 4.3.0
Version 4.1.0 to 4.1.4	Upgrade directly to 4.3.0
Version 4.2.0 to 4.2.6	Upgrade directly to 4.3.0

Compatibility Guidelines

There is downward compatibility of one version between the Global Center and the Center with sync and sensors.

- Global Center (Version N): Compatible with Centers with sync with versions N and N-1 (e.g., Global Center version 4.2.0 can manage local Centers with versions 4.2.0 and 4.1.4).
- Center with sync (Version N): Compatible with sensors with versions N and N-1 (e.g., Center with sync version 4.2.0 can manage sensors with versions 4.2.0 and 4.1.4).

Data purge

The Center database is regularly maintained to contain the volume of data stored.

The data retention policies are, by default, in version 4.3.0.

- Flows: 7 days
- Events: limited to 10 000 per category
- Variables after 2 years
- External communications: 30 days (limit 1 million)

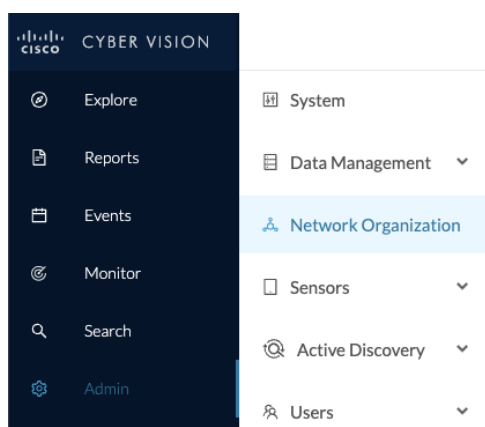
Upgrade to 4.3.0 considerations

All users must check their networking configurations before and after the upgrade. In release 4.3.0, all communications to components considered as External will not be stored anymore as an activity. The details of the external component are not stored as a standard component. A component is considered External based on the configuration done in the Network Organization page (see example below).

For each external communication:

- some details of the external communications are attached to the internal component.
- an activity is not created.
- the external component is not stored, as a standard component.

During the upgrade of an existing database to the latest version, some purges will occur based on product configuration. Before the upgrade, perform network configuration from the User Interface, in the Admin / Network Organization menu.











Review and modify the network organization before the upgrade, as in version 4.3.0 all external communications are stored in a different manner and external components are removed from the database. All subnets not listed are considered as external. Belonging components are deleted.

For example, if the OT network user is not using private IP address ranges, he has to create the ones he is using before the upgrade. Otherwise, all components in those ranges will be purged.











Before the upgrade, the ranges defined by the Internet Assigned Numbers Authority (IANA) for private usages are added and configured as internal to avoid any data deletion by mistake:

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

For example, if the organization is before the upgrade:

IP Address / subnet	VLAN ID	Network Name	Network Type	Action
10.0.0.0/20		IT Range	IT Internal	 
10.0.16.0/20		OT Range	OT Internal	 
10.128.0.0/9		Ext	External	 
169.254.0.0/16		IPv4 link local	OT Internal	 

The subnet 10.0.0./8 is added during the upgrade process:

IP Address / subnet	VLAN ID	Network Name	Network Type	Action
10.0.0.0/8		10/8 private network	OT Internal	 
10.0.0.0/20		IT Range	IT Internal	 
10.0.16.0/20		OT Range	OT Internal	 
10.128.0.0/9		Ext	External	 
169.254.0.0/16		IPv4 link local	OT Internal	 

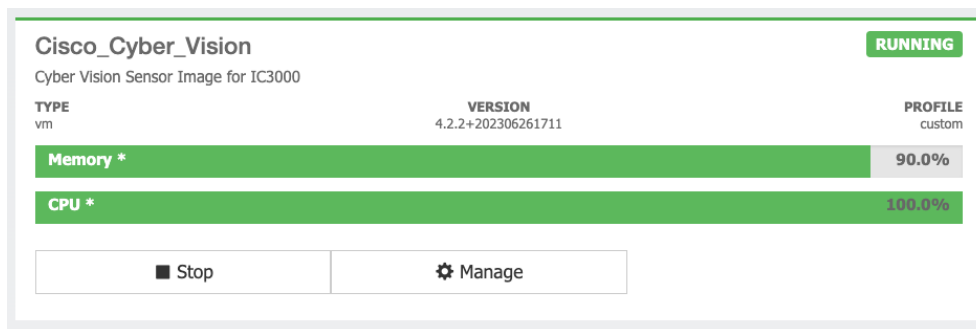
Check the configuration after the upgrade to adjust the configuration and fix the type of the 3 ranges added during the upgrade.

IC3000 considerations

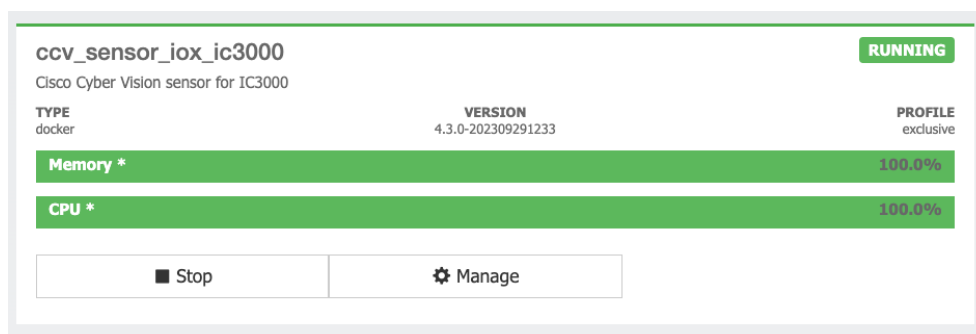
Cisco Cyber Vision sensor application for IC3000 format will change from Virtual Machine to Docker in version 4.3.0. The upgrade from a previous version will consist of a redeployment of a new application. This upgrade can be performed in 2 ways:

1. For IC3000 sensors deployed with the Sensor Management extension, the extension will manage it for the user (details here: [Installation with the extension](#))
2. For IC3000 sensors deployed manually, perform the upgrade manually. Delete and reinstall the sensor (details here: [Manual Installation:](#)).

IC3000 Cyber Vision application before 4.3.0:



IC3000 Cyber Vision application after 4.3.0:



Limitations

The active discovery feature requires an IC3000 with a firmware version 1.5.1.

Even if you do not use active discovery, we recommend using the latest IC3000 firmware to run the Cyber Vision sensor.

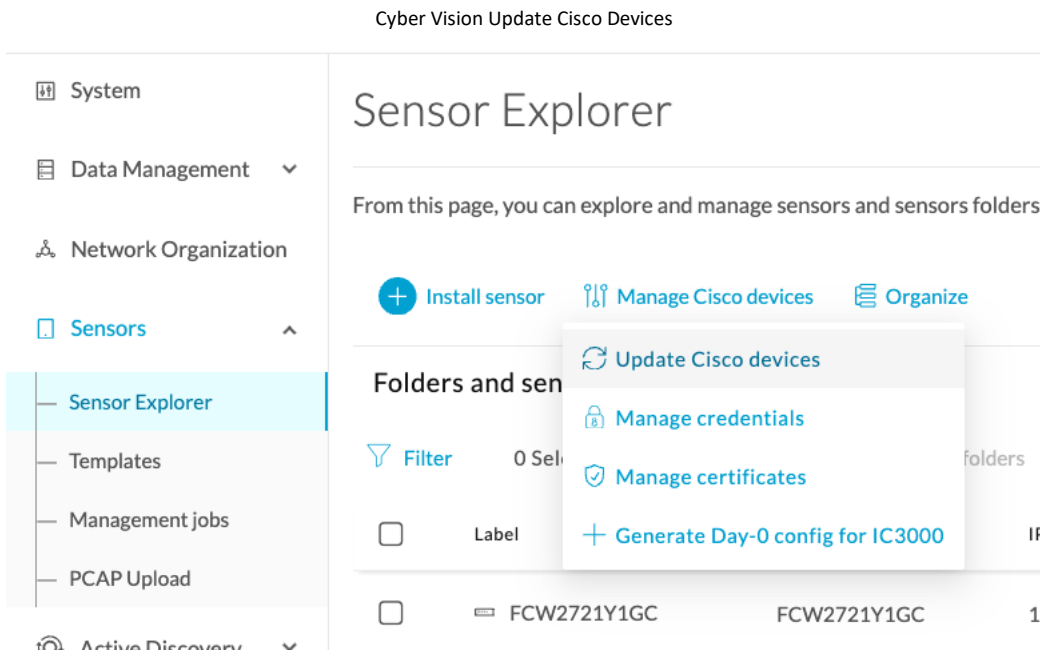
Note:

The ssh access to the sensor application is no longer possible. The IC3000 local manager provides a console connection to the application.

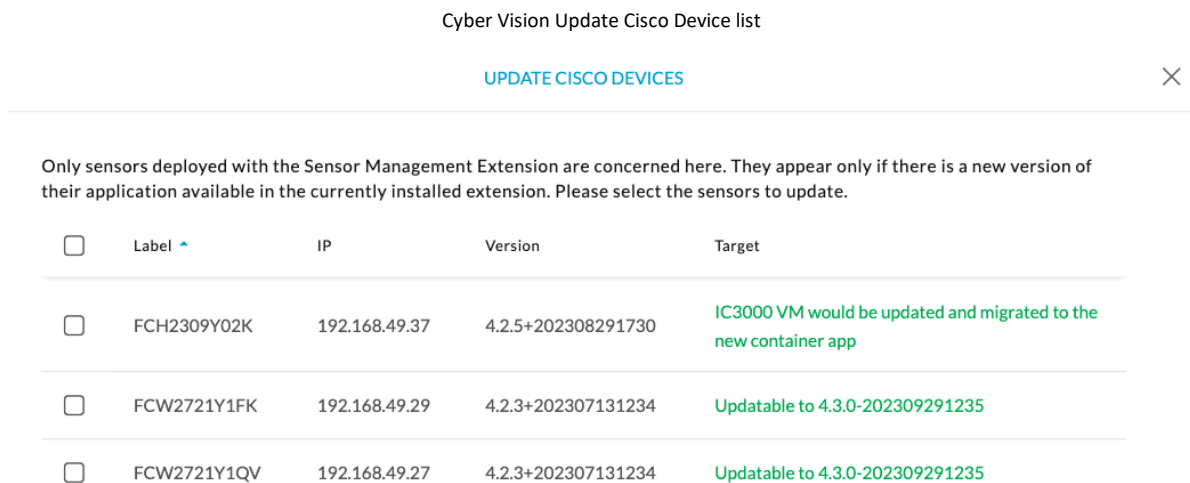
Access using the appconsole user is crashing the sensor application. This is a known issue of the IC3000 firmware version 1.5.1.

Upgrade with the extension

Follow the standard process to use the 'Update Cisco Devices' functionality (Sensors > Sensor Explore > Manage Cisco devices > Update Cisco devices).



The system lists the upgradable sensors.



If the IC3000 firmware version is not at least 1.5.1 and if the sensor application is using the active discovery, the Sensor Management Extension will not perform the upgrade. Upgrade the IC3000 firmware first.

Cyber Vision Update Cisco Device list – IC3000 firmware issue

UPDATE CISCO DEVICES ✕

Only sensors deployed with the Sensor Management Extension are concerned here. They appear only if there is a new version of their application available in the currently installed extension. Please select the sensors to update.

<input type="checkbox"/>	Label ▲	IP	Version	Target
<input type="checkbox"/>	IC3000-16-SENSOR-17-EXT	192.168.51.17	4.2.6+202309071750	Cannot migrate IC3000 VM to container: the sensor has Active Discovery enabled but does not support it anymore: << Platform requires at least version 1.5.1 to support Cyber Vision Active Discovery. Only a passive deployment is possible with the installed version. >>
<input type="checkbox"/>	IE3400-14-SENSOR-15-EXT	192.168.51.15	4.2.6+202309071552	Updatable to 4.3.0-202309291254

1 - 2

Don't stop the update if the deployment fails on some sensors

Cancel

Update

Installation with the extension

The installation of the IC3000 sensor application with the extension will have some limitations if the IC3000 firmware is below 1.5.1.

Cyber Vision sensor application installation – IC3000 firmware issue

Install via extension

Configure Cyber Vision IOx sensor app

The device requires additional parameters. Some parameters have been pre-filled. Please complete the remaining fields.

Cisco device: IC3000-2C2F-K9

! Platform requires at least version 1.5.1 to support Cyber Vision Active Discovery. Only a passive deployment is possible with the installed version.

Collection IP address*	Collection prefix length*
<input type="text"/>	<input type="text"/>
	Like 24, 16 or 8
Collection gateway	
<input type="text"/>	

Manual Installation:

The IC3000 Cyber Vision Sensor Installation Guide will help you manually deploy or redeploy your sensors.

Guide available here: <https://www.cisco.com/c/en/us/support/security/cyber-vision/products-installation-guides-list.html>.

Center updates

Architecture with Global Center

Preliminary checks: We highly recommend that you check the health of all Centers connected to the Global Center and of the Global Center itself before updating.

Use an SSH connection to the Center and type the following command:

```
systemctl --failed
```

The number of listed sbs-* units should be 0. If not, fix the failures before updating.

Cisco Cyber Vision system check – 0 failure

```
root@Center21:~# systemctl --failed
0 loaded units listed.
root@Center21:~#
```

All sbs services should be in a normal state before performing an update. If not, fix the failures before upgrading.

Cisco Cyber Vision system check – example of failure

```
root@Center21:~# systemctl --failed
UNIT                                LOAD    ACTIVE SUB    DESCRIPTION
● sbs-marmotd.service loaded failed failed marmotd persistence service

LOAD    = Reflects whether the unit definition was properly loaded.
ACTIVE  = The high-level unit activation state, i.e. generalization of SUB.
SUB     = The low-level unit activation state, values depend on unit type.

1 loaded units listed.
root@Center21:~#
```

Perform a system reboot to solve the issue. For help, please contact support.

For a distributed architecture, use the following steps:

1. Update the Global Center with a or b methods below.
 - a. Use the Graphical User Interface:
 - File= CiscoCyberVision-update-combined--<LAST-VERSION>.dat
 - Navigate to Admin > System, use the System Update button and browse and select the update file.
 - b. Use the Command Line Interface (CLI):
 - File= CiscoCyberVision-update-center--<LAST-VERSION>.dat
 - Launch the update with the following command:
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. If you installed the sensors with the sensor management extension:
 - i. first upgrade the extension and then update the sensors.
 - File = CiscoCyberVision-sensor-management--<LAST-VERSION>.ext
 - Navigate to Admin > Extensions. In the Actions column, use the update button and browse to select the update file.
 - The Cisco Cyber Vision sensor management extension can also be updated from the CLI with the command:

```
sbs-extension upgrade /data/tmp/CiscoCyberVision-sensor-management--<LAST-VERSION>.ext
```

- ii. Update all sensors with the extension.

Access the sensor administration page, > “Manage Cisco devices” / “Update Cisco devices” or use the redeploy button in the sensor’s right-side panel. For a complete procedure add hyperlink “Cisco Cyber Vision new features and improvements” or use any sensor installation guide from version 4.2.0.

- b. If you did not install the sensor with the sensor management extension, upgrade the sensor with the sensor package from the platform Local Manager or from the platform Command Line. Use one of the corresponding sensor installation guides.
 - IE3x00, IE93x0 and IR1101 files = CiscoCyberVision-IOx-aarch64--<LAST-VERSION>.tar or CiscoCyberVision-IOx-Active-Discovery-aarch64---<LAST-VERSION>.tar
 - Catalyst 9300 and 9400 and IR8340 files = CiscoCyberVision-IOx-x86-64-<LAST-VERSION>.tar or CiscoCyberVision-IOx-Active-Discovery-x86-64-<LAST-VERSION>.tar.
 - IC3000 files = CiscoCyberVision-IOx-IC3000-<LAST-VERSION>.tar or CiscoCyberVision-IOx-Active-Discovery-IC3000-<LAST-VERSION>.tar

Important remark regarding CiscoCyberVision-IOx-x86-64 sensor application update:

IMPORTANT: Because of rspan compatibility, you cannot update the Cisco CyberVision –IOx-x86-64 sensor application through the Local Manager of a Catalyst 9300, 9400, or IR8340 files from release 4.1.2 (or lower) to release 4.1.3 (or higher). Instead, redeploy the sensor application and upload the enrollment package again. Once you perform the update to a release greater than 4.1.2 with the redeploy, use the standard update procedure for the other releases (for example: 4.2.0 to 4.3.0).

Guidelines here:

[Cisco Cyber Vision Sensor Application for Cisco Switches Installation Guide, Release 4.2.0](#)

- **[procedure with the local manager for the redeploy](#)**
- **[Upgrade procedures for standard updates](#)**

[Cisco Cyber Vision Sensor Application for Cisco IR8340 Installation Guide, Release 4.2.0](#)

- **[procedure with the local manager for the redeploy](#)**
- **[Upgrade procedures for standard updates](#)**

Architecture with one Center

For a single Center, use the following steps:

1. Update the Center with a or b methods below.
 - a. Use the Graphical User Interface:
 - File= CiscoCyberVision-update-combined-<LAST-VERSION>.dat
 - Navigate to Admin > System, use the System Update button, and browse and select the update file.
 - b. Use the Command Line Interface (CLI):
 - File= CiscoCyberVision-update-center-<LAST-VERSION>.dat
 - Launch the update with the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-center-<LAST-VERSION>.dat
```

2. Update the sensors.
 - a. If you installed the sensors with the sensor management extension:
 - i. first upgrade the extension and then update the sensors.
 - File = CiscoCyberVision-sensor-management--<LAST-VERSION>.ext
 - Navigate to Admin > Extensions. In the Actions column, use the update button and browse to select the update file.
 - The Cisco Cyber Vision sensor management extension can also be updated from the CLI with the command:

```
sbs-extension upgrade /data/tmp/CiscoCyberVision-sensor-management--<LAST-VERSION>.ext
```

- ii. Then update all sensors with the extension.

Access the sensor administration page, > “Manage Cisco devices” / “Update Cisco devices” or use the redeploy button in the sensor’s right-side panel. For a complete procedure add hyperlink “Cisco Cyber Vision new features and improvements” or use any sensor installation guide from version 4.2.0.

- b. If you did not install the sensor with the sensor management extension, upgrade the sensor with the sensor package from the platform Local Manager or from the platform Command Line. Use one of the corresponding sensor installation guides.
 - IE3x00, IE93x0 and IR1101 files = CiscoCyberVision-IOx-aarch64--<LAST-VERSION>.tar or CiscoCyberVision-IOx-Active-Discovery-aarch64---<LAST-VERSION>.tar
 - Catalyst 9300 and 9400 and IR8340 files = CiscoCyberVision-IOx-x86-64-<LAST-VERSION>.tar or CiscoCyberVision-IOx-Active-Discovery-x86-64-<LAST-VERSION>.tar.
 - IC3000 files = CiscoCyberVision-IOx-IC3000-<LAST-VERSION>.tar or CiscoCyberVision-IOx-Active-Discovery-IC3000-<LAST-VERSION>.tar

Important remark regarding CiscoCyberVision-IOx-x86-64 sensor application update:

IMPORTANT: Because of rspan compatibility, you cannot update the Cisco CyberVision –IOx-x86-64 sensor application through the Local Manager of a Catalyst 9300, 9400, or IR8340 files from release 4.1.2 (or lower) to release 4.1.3 (or higher). Instead, redeploy the sensor application and upload the enrollment package again. Once you perform the update to a release greater than 4.1.2 with the redeploy, use the standard update procedure for the other releases (for example: 4.2.0 to 4.3.0).

Guidelines here:

[Cisco Cyber Vision Sensor Application for Cisco Switches Installation Guide, Release 4.2.0](#)

- **[procedure with the local manager for the redeploy](#)**
- **[Upgrade procedures for standard updates](#)**

[Cisco Cyber Vision Sensor Application for Cisco IR8340 Installation Guide, Release 4.2.0](#)

- **[procedure with the local manager for the redeploy](#)**
- **[Upgrade procedures for standard updates](#)**

AWS and Azure Centers

For a Center deployed in AWS or Azure, follow the procedure described in Architecture with one Center.

Cisco Cyber Vision 4.3.0 important changes

Communication port and protocol changes

Port

No modification in 4.3.0.

Protocol

No modification in 4.3.0.

API

Some changes were made in release 4.3.0. Several API routes changed, and few new were added.

New endpoints

- reports
 - /reports2/reports-metadata - GET
 - /reports2/reports-metadata - POST
 - /reports2/reports-metadata/reports/{reports-id}/download
 - /reports2/reports-metadata/{id} - PUT
 - /reports2/reports-metadata/{id} - DELETE
 - /reports2/reports-metadata/{id}/reports - GET
 - /reports2/reports-metadata/{id}/reports - POST
 - /reports2/reports-metadata/{id}/reports/{reportsId} - DELETE
 - /reports2/reports-type - GET
- custom networks
 - GET (/networks/)
 - POST (/networks/)
 - OPTIONS (/networks/)
 - HEAD (/networks/)
 - PATCH (/networks/check)
- external communications
 - {type}/{id}/externalCommunications - GET

New attributes

- monitor mode, new attributes on GET/PUT preset settings:
"differenceActivityNew": true,
"differenceActivityTagNew": true,
"differenceComponentNew": true,
"differenceComponentPropertyModified": true,
"differenceComponentPropertyNew": true,
"differenceComponentTagNew": true,
"differenceComponentVariableAccessNew": true,
- vulnerability details on GET devices or components:
/devices/{device_id}/vulnerabilities/{vulnerability_id}
/components/{component_id}/vulnerabilities/{vulnerability_id}
- on all GET components or devices route, a new parameter has been added:
externalCommunicationsCount
- new payload option on any POST /presets/* route:
"hasExternalCommunications": {
 "operator": "string",
 "value": {
 "id": "string" }}
- on all GET /presets/* route situation has been replaced with:
"hasExternalCommunications": "string"

Removed endpoint

- activeDiscovery/sensors

Changed endpoints

- GET /devices/{device_id}/vulnerabilities or /components/{component_id}/vulnerabilities

Due to defect: **CSCwi74303 API route /devices/:id/vulnerabilities response has changed in 4.3.0**, these routes vulnerabilities are having less details. A fix is available in release 4.3.2.

- on the GET components and devices endpoints, vulnerabilities:
cvss updated to CVSS
version updated to CVSSVersion

SYSLOG

No modification in 4.3.0.

Cisco Cyber Vision new features and improvements

External communication

Introduction

For Release 4.3.0, we added External Communication. This feature enhances the way components are currently created based on the DPI and the information we are able to gather.

If the communication includes a device / IP that is not defined by an internal network in the network organization (or is explicitly defined as External), then only the minimal data is stored for the internal component, without creating the external component. This data includes:

- Internal Device (IP, MAC)
- Source port (TCP/UDP)
- External Device (IP)
- Destination port (TCP/UDP)

This eliminates the impact of creating and storing components that are not providing value.

Use the Network Organization to define Internal and External subnets.

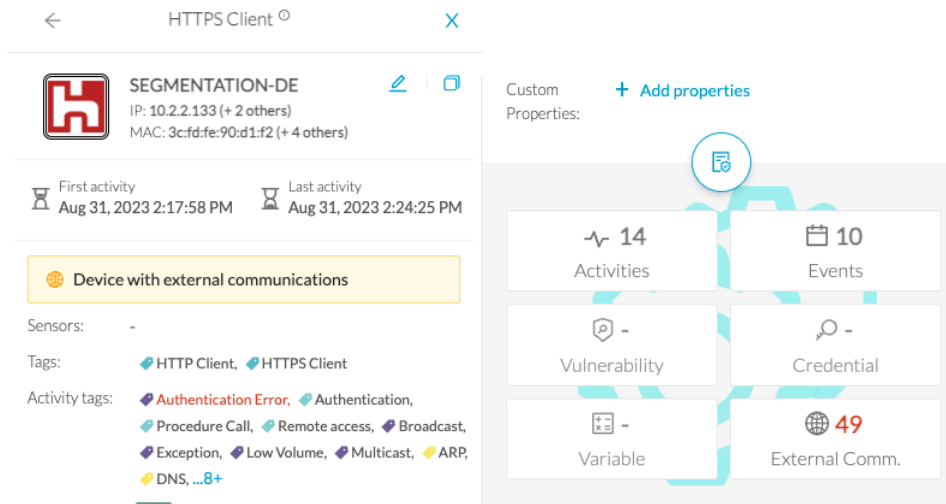
Cisco Cyber Vision Network Organization

6 Networks

IP Address / subnet	VLAN ID	Network Name	Network Type	Action
10.0.0.0/8		10/8 private network	External	
10.0.0.0/20		IT Range	IT Internal	
10.0.16.0/20		OT Range	OT Internal	
169.254.0.0/16		IPv4 link local	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	
192.168.11.0/24	11	LGV-Network	OT Internal	
192.168.12.0/24	12	AGV-Network	OT Internal	
fc00::7		FC00::7 IPv6 local unicast	OT Internal	
fe80::10		IPv6 link local	OT Internal	

On the left side panel, an orange rectangle indicates that the device had some external communications. A new panel indicates the number of external communications.

Cisco Cyber Vision device with external communications left panel



A new activity tab lists the external communications.

Cisco Cyber Vision external communication details

49 External Communications Export to CSV

< 1 2 3 > 20 / page

Source IP	Destination IP	Destination Port	Hostname	Protocol	Received by device	Sent by device	Last Seen	Direction
10.2.2.133	92.123.77.35	80	r3.o.lencr.org	HTTP	3 kB	5.22 kB	4 days ago	Outbound
10.2.2.133	172.217.168.195	80	ocsp.pki.goog	HTTP	732 B	947 B	4 days ago	Outbound
10.2.2.133	23.55.161.211	80	ciscobinary.openh264.org	HTTP	9.69 kB	512 kB	4 days ago	Outbound
10.2.2.133	52.12.130.210	443	location.services.mozilla.com	HTTPS	1.49 kB	4.45 kB	4 days ago	Outbound
10.2.2.133	172.217.132.137	443	r4---sn-5hne6nzk.gvt1.com	HTTPS	122 kB	8.81 MB	4 days ago	Outbound
10.2.2.133	142.250.179.163	80	ocsp.pki.goog	HTTP	4.63 kB	6.29 kB	4 days ago	Outbound
10.2.2.133	192.229.221.95	80	ocsp.digicert.com	HTTP	1.34 kB	1.9 kB	4 days ago	Outbound
10.2.2.133	18.239.100.55	80	ocsp.r2m02.amazontrust.com	HTTP	849 B	1.32 kB	4 days ago	Outbound

A new Security Insights tab lists all devices / components which have external communications.

Cisco Cyber Vision external communication Security Insights tab

Security Insights

Devices with external communication DNS requests HTTP requests SMB Tree names Flows with no tag

<input type="checkbox"/>	Device	Risk Score	IP	MAC	Count	Last Activity	Data Volume
<input type="checkbox"/>	ROCKWELLSRV	10	10.2.2.123 (+ 4 others)	00:50:56:8f:6a:59 (+ 2 others)	4	Sep 4, 2023 12:10:38 PM	1.27 MB
<input type="checkbox"/>	10.2.2.62	10	10.2.2.62	00:50:56:8f:10:eb	31	Sep 4, 2023 12:06:44 PM	1.55 MB
<input type="checkbox"/>	SEGMENTATION-DE	10	10.2.2.133 (+ 2 others)	3c:fd:fe:90:d1:f2 (+ 4 others)	49	Aug 31, 2023 2:18:23 PM	13.9 MB

Subnetting for network organization

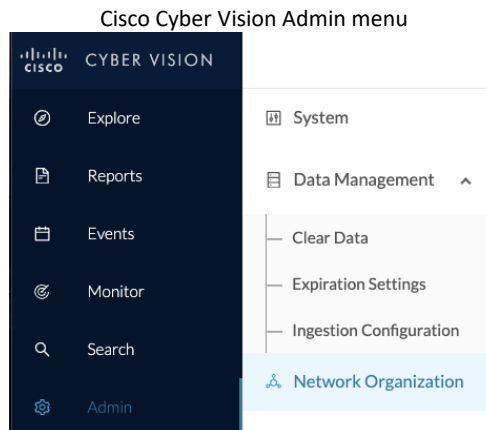
Network Organization configuration

When deploying Cyber Vision, the Network Organization is a critical setting that can impact the effectiveness of Cyber Visions device discovery. In previous Cyber Vision releases, the Network Organization settings did not allow overlapping networks to be defined. For customers who leverage a large network for all their IT networks, and smaller subnets out of that to define their OT networks, this requires a lot of network definition.

This feature allows a subnetting approach.

To define subnets:

1. Click Admin > Network Organization.



The configuration now supports subnets.

Cisco Cyber Vision Network Organization

6 Networks

IP Address / subnet	VLAN ID	Network Name	Network Type	Action
10.0.0.0/8		10/8 private network	External	
10.0.0.0/20		IT Range	IT Internal	
10.0.16.0/20		OT Range	OT Internal	
169.254.0.0/16		IPv4 link local	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	
192.168.11.0/24	11	LGV-Network	OT Internal	
192.168.12.0/24	12	AGV-Network	OT Internal	
fc00::/7		FC00::/7 IPv6 local unicast	OT Internal	
fe80::/10		IPv6 link local	OT Internal	

Network Organization API

We created some new API routes to manage the Network Organization with some scripts. We updated the API documentation to describe the new Network Organization routes.

Cisco Cyber Vision Network Organization API routes

CustomNetwork

GET	/networks/
PUT	/networks/
POST	/networks/
DELETE	/networks/
POST	/networks/check

Network Organization impact on Cyber Vision

Network Organization impacts the external communications detailed above. It also impacts the ingestion configuration. For all defined ranges, you can enable or disable the flow storage.

Cisco Cyber Vision Ingestion Configuration - Flow retention

Flows Configuration

Flows Storage

If disabled, flows won't be stored in the database, you can enable storage and adjust settings in your network configuration.

Select All OT

Network Name	IP Address / subnet	VLAN ID	Network Type
<input type="checkbox"/> 10/8 private network	10.0.0.0/8		External
<input checked="" type="checkbox"/> IT Range	10.0.0.0/20		IT Internal
<input checked="" type="checkbox"/> OT Range	10.0.16.0/20		OT Internal
<input checked="" type="checkbox"/> IPv4 link local	169.254.0.0/16		OT Internal
<input checked="" type="checkbox"/> 192.168/16 private network	192.168.0.0/16		OT Internal
<input checked="" type="checkbox"/> LGV-Network	192.168.11.0/24	11	OT Internal
<input checked="" type="checkbox"/> AGV-Network	192.168.12.0/24	12	OT Internal
<input checked="" type="checkbox"/> FC00::/7 IPv6 local unicast	fc00::/7		OT Internal
<input checked="" type="checkbox"/> IPv6 link local	fe80::/10		OT Internal
<input type="checkbox"/> Others			External

L2 Flow Storage

L2 flows are defined by communication between endpoints without IP addresses.

Sensor templates

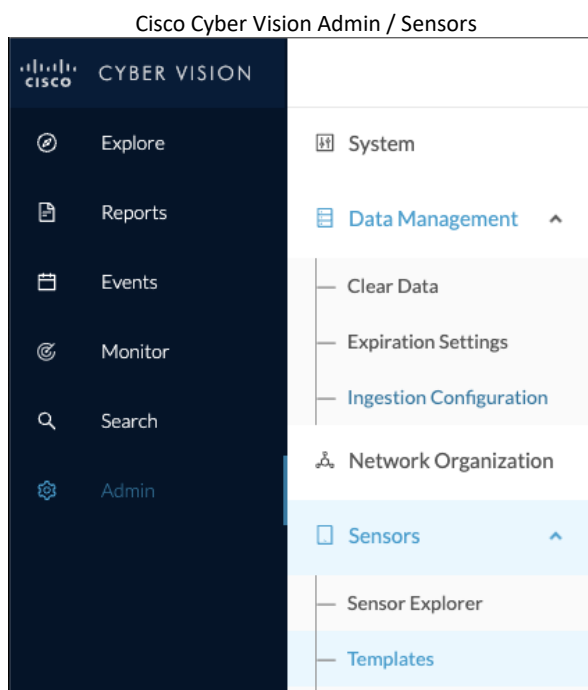
In previous Cyber Vision versions, any settings on the sensor, including custom protocol ports, and which protocols are enabled, require you to modify a configuration file hosted on the sensor. It required a manual connection to each sensor to modify the configuration.

Cyber Vision version 4.3.0 provides a feature with a centralized method for managing the configuration of multiple sensors. The Sensor Template feature lets you configure sensor settings from the user interface. You create some templates and assign those templates to the sensors. In Cyber Vision 4.3.0, a template can manage 2 types of settings which help you:

1. Enable or disable protocol DPI
2. Customize the protocol ports

To access Sensor Templates:

Click Admin > Sensors > Templates.



You can create, edit and delete templates. A default template is assigned to all new sensors. You can also create a new sensor template with the button “Add sensor template.”

Cisco Cyber Vision Configuration Template menu

Configuration Template

Sensor configuration templates allow you to enable and personalize protocol settings, and deploy them to a large number of sensors.

[Add sensor template](#) As of: November 8, 2023 at 3:34:44 PM

Name	Sensor Count	Deployment progress	Last update	Actions
Default	2	<div style="width: 100%; height: 10px; background-color: green; border: 1px solid green;"></div>	-	...

To create a template:

1. Click **Admin > Sensors > Templates > Add sensor template.**
2. In **Basic information:** Add a **Name** and **Description** (optional).
3. In **Protocol configuration:** Enable / disable protocols and change port settings.
4. Select sensors: Select sensors affected to the template.
5. Summary: Check and validate the template configuration.

Cisco Cyber Vision Create sensor template

[CREATE SENSOR TEMPLATE](#) X

1 Basic information — 2 Protocol configuration — 3 Select sensors — 4 Summary

* Name

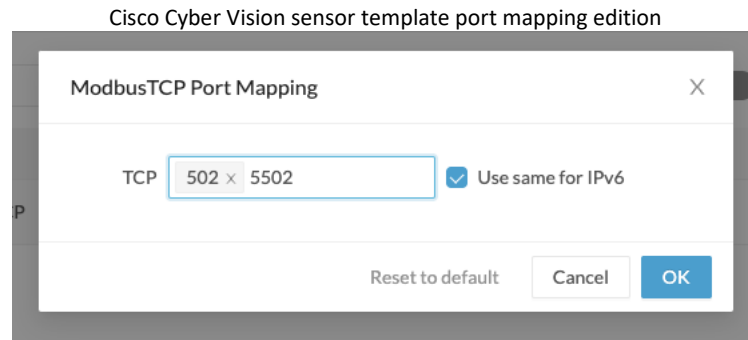
Please enter a name

Description

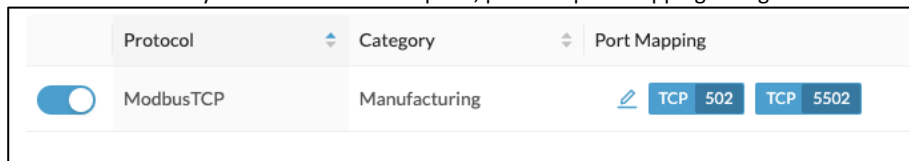
To enable or disable the DPI of a protocol, use the selector.



To change the Port Mapping, a text box is available to add / delete ports.



Cisco Cyber Vision sensor template, protocol port mapping changed



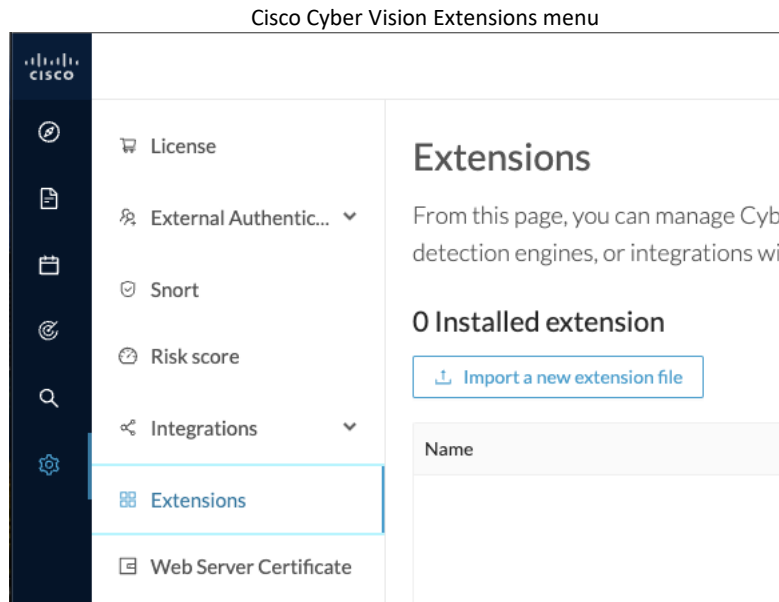
New report feature

For Cisco Cyber Vision version 4.3.0, we added a new report for **Security Posture**. To see the report, you must install a report management extension.

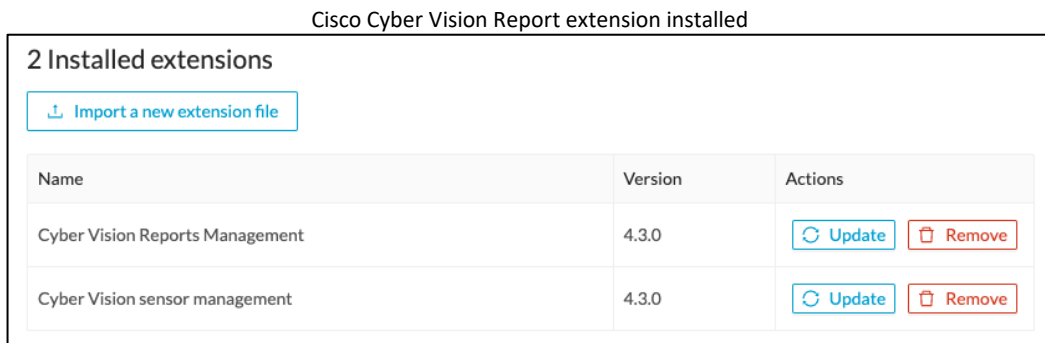
Report extension setup:

Click **Admin > Extensions > Import a new extension file**.

Select **CiscoCyberVision-reports-management-4.3.0.ext**.

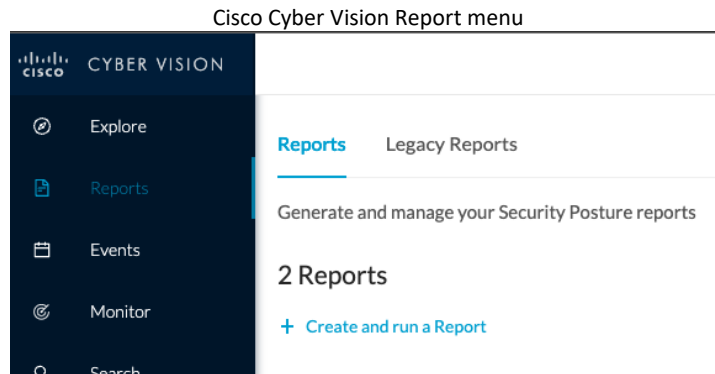


Install the Cyber Vision report management extension.



To create and run a report:

1. Click **Create and run a report**.



2. Type in a Name, Description, and Type (Security Posture).
3. For Logo, you can import a company logo.
4. For Format: Word (doc) or Adobe (.pdf).
5. For Presets: reports are based on preset datasets. Select the preset for the report.
6. For Table of Content: choose the content for the report.
7. Click Save

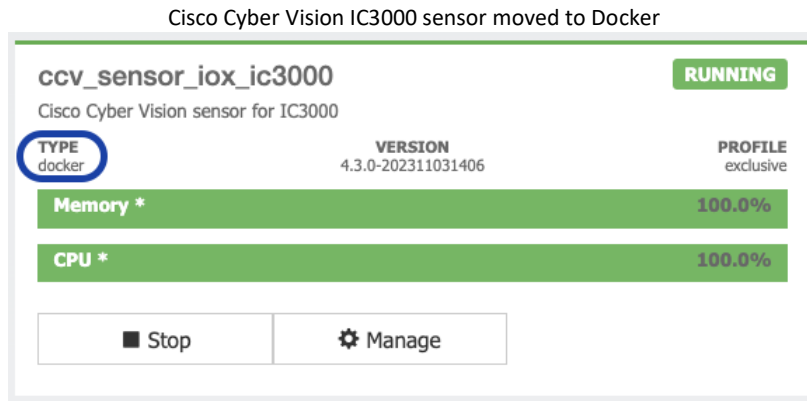
Cisco Cyber Vision Report list

Name	Preset	Created by	Last Modified	Status	Last Run	Actions
PLC	All Controllers	admin@sentryo.net	Nov 10, 2023, 11:26 AM	Processing	Nov 10, 2023, 11:25 AM	...
ALLNetwork	All data	admin@sentryo.net	Nov 10, 2023, 11:24 AM	Success	Nov 9, 2023, 6:45 PM	...
Rockwell	Rockwell	admin@sentryo.net	Nov 10, 2023, 11:24 AM	Success	Nov 9, 2023, 6:43 PM	...

In this table, you can see the Status of the reports. You can download the generated reports and can edit, delete or duplicate an existing configuration.

IC3000 sensor application migration

We enhanced the Cyber Vision IC3000 sensor application type in version 4.3.0. Now you can configure Active Discovery on multiple vlans on a single interface (with 802.1Q trunking encapsulation).

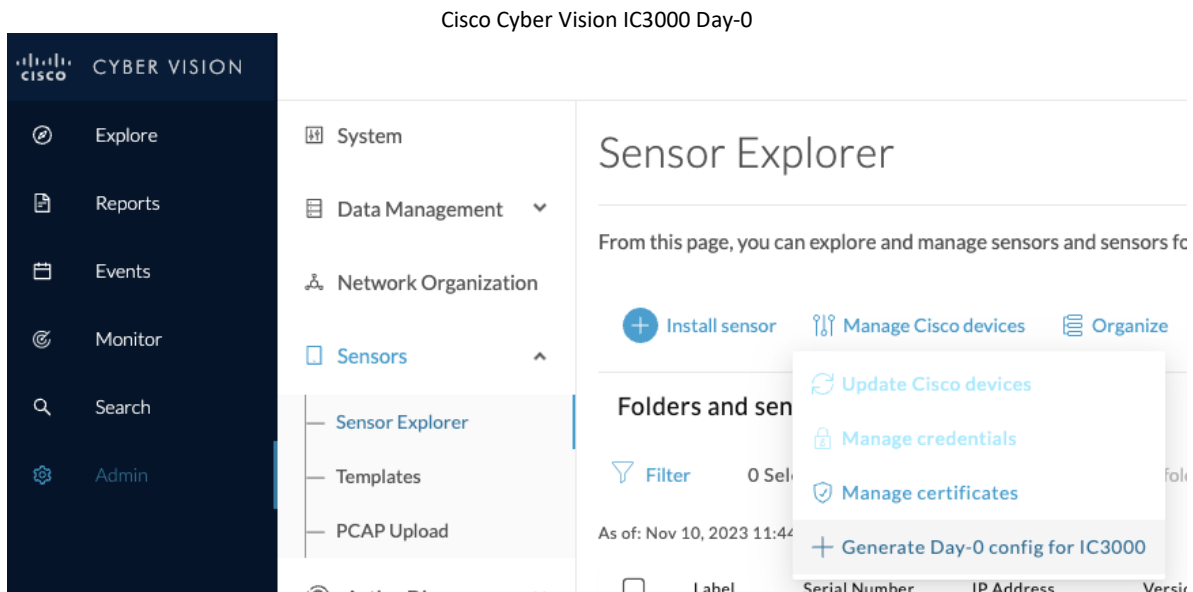


The impact on upgrades and installations are detailed here: [IC3000 considerations](#).

Other impacts are:

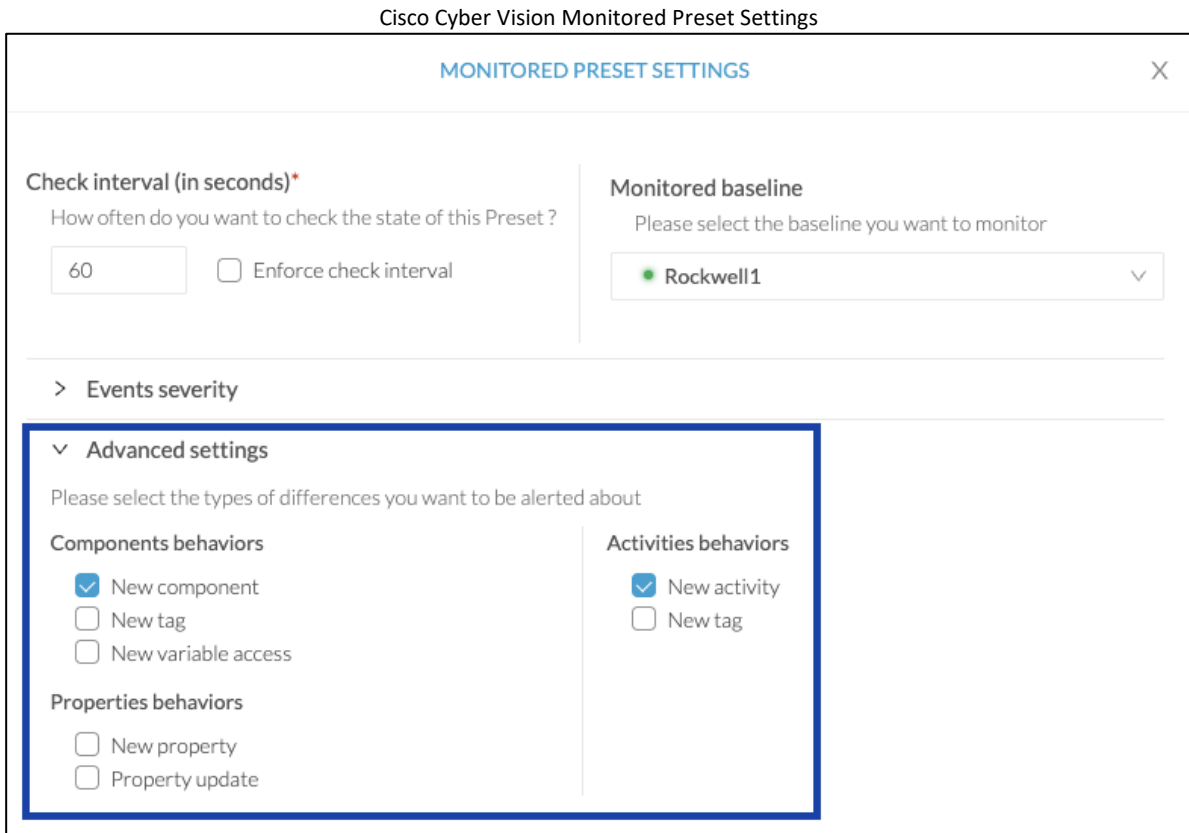
1. The sensor offline feature is no longer available.
2. Direct ssh connection to the sensor is no longer possible. Use the IC3000 local manager console connection.
3. Active Discovery requires an IC3000 firmware 1.5.1 minimum.

In addition, IC3000 Day-0 feature is still available, but this is now a separate feature available. To access it: Click **Admin > Sensors > Sensor Explorer > Manage Cisco devices > Generate Day-0 config for IC3000**.



Monitor mode changes

To configure Cyber Vision baselines, some advanced settings are now available. Click Explore > Monitor > Monitored preset settings > expand Advanced settings > check New component and New activity.

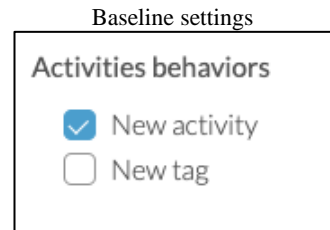
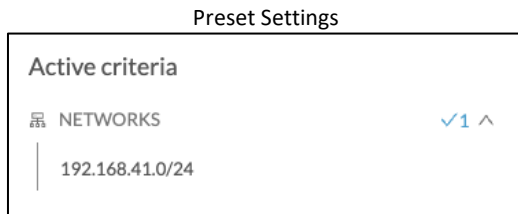


The new settings help you decrease the number of alerts generated by the system. The setting capabilities allow the system to filter to generate differences only on some behaviors and not all of them, as before.

For example, apply the system for the following use cases:

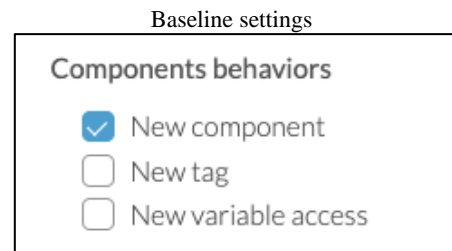
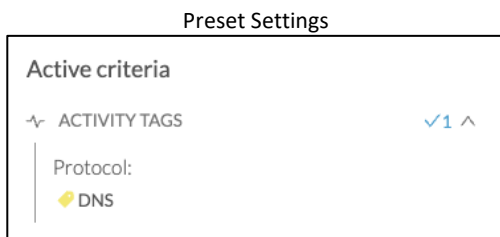
- **Detection of a new activity on a set of critical equipment**

Since production lines are the most central and critical part of an industrial network, monitor the set of PLCs which manage these production lines to ensure you are notified in case a new activity happens on the network.



- **Tracking components that are doing specific protocols**

Tracking components that send DNS requests on a network allows you to be notified in case a component of the monitored network is doing this type of request. You will have information such as the component's IP address.



Active Discovery changes

Cyber Vision version 4.3.0 is now able to actively discover devices on new protocols. Several new protocols are now available:

- Bacnet – Building management protocol
- DNP3 – power grid
- Melsoft - Mitsubishi
- Modbus, UMAS
- Omron

UI diagnostic enhancement

The diagnostic generation from the user interface is now done in the background. It lets the user navigate during the diagnostic generation and download the package once it's ready.

Cisco Cyber Vision statistics page – Diagnostic generation

Diagnostic

Last diagnostic generated: **Nov 9, 2023 6:47 PM**

 Download diagnostic

 Generate diagnostic

Cisco Cyber Vision 4.3.0 enhancements

CDETS	Description
CSCwe16301	Add a LLMNR inspector and dissector
CSCwe16281	Yokogawa - add the Controller tag when Controller Info/Controller Name/ Supported Module tags are set
CSCwe16266	Add event when Triton detected
CSCwe16236	Use MODBUS query (function code 43) for Active Discovery - unicast
CSCwe16234	Clear Data - review code and optimize it to speed up operation
CSCwe16206	Allow for simple tuning of the monitor mode
CSCwe16204	Melssoft: The properties observed in the flows are not used in the component
CSCwf43032	Add heap and profile to sensor diagnostic
CSCwf78646	Sensor explorer: improve user experience
CSCwh37562	Add scp client to sensor iox app
CSCwh51681	sbs-diag add type and name on diag file name
CSCwh55833	Diagnostic File: Add sensor status in the sbs_sensor_list output

Cisco Cyber Vision 4.3.0 Resolved Caveats

CDETS	Description
CSCWe16283	MMS : Wrong model names and fw version
CSCWe16262	Reset-data: Cancel button should be disabled once clear data is started
CSCWe16209	Wrong device icons seen on the Device view
CSCWe16208	reset all data "failing" in case of too much data
-	Fins Omron : The tags between the PLC and the engineering station are reversed - 11764
CSCWe16171	Device engine uncomplete assetization - Rockwell example
CSCWe16166	mdns decoded name: remove .local extension
CSCwf03873	Device technical sheet - Vulnerability widget - typo in 'Acknowledged' word in vulnerability filter
CSCwh37567	UI - Fix Sort - Remove the sort parameter from the URL when switching the tabs
CSCwh19219	[FIPS] kdb import fails for subscriber rules
CSCwh20627	rsyslog-sensors max tcp connection can be exceeded
CSCwh37566	Explore - option to select custom period
CSCwh32778	No warning when deploying sensor with extension on cat9k without ssd
CSCwh37561	Deadlock in sbs-worker on sensor-info table
CSCwh59619	NAD Event - Limit content of large events
CSCwh72942	Flow-Flow properties purge - Improve the batch size limit management
CSCwf68110	Display clear error message in the UI when center update process fails
CSCwf68109	Issue when updating center with many IC3000
CSCwh65365	make sensor export flow properties every 120s by default
CSCwi00089	sql error persisting some opcua variables
CSCwi00088	"Failed to retrieve vulnerabilities" on some devices
CSCwh37564	Admin - additional pop-up for CPU intensive processes
CSCwh65364	Click here to fill should be updated with message and a button
CSCwi00089	sql error persisting on some opcua variables

Cisco Cyber Vision Open Caveats

Issues ID / CDETS	Component	Description
CSCwi33573	Center	Edit Network settings - Device engine options clarify VLAN Usage
CSCwi33574	Center	Edit Network settings - Unclear Device engine options
CSCwi33572	Center	Edit Network settings - Device engine options interlock
CSCwi32082	Center + extensions	Extension issues when center is not stopped properly
CSCwi28690	Center	External communications without direction are not listed
CSCwb12630	Center + ISE	All components are not synchronized with ISE
CSCwd39017	Center	Missing information in the Smart License Usage
CSCwi74303	Center API	API route /devices/:id/vulnerabilities response has changed in 4.3.0

CSCwi32082: Extension issues when center is not stopped properly.

When report management and sensor management extensions are installed, if the center is not stopped properly, it may happen that the extensions didn't start properly. A workaround is available, from the sensor command line type:

```
sudo podman rm -f reports-management
sudo systemctl restart sbs-extension
```

CSCwi33572 / CSCwi33574 / CSCwi33574: Edit Network settings - Device engine options.

Clarifications needed regarding those options:

1. The 2 check boxes must not be used at the same time.
2. "This IP range is deployed several time, the device engine will not use IP to group components into device."

IP will not be used for the whole range to group components into devices.

3. "Do not group component seen by different sensors. For this IP range, the device engine will only use components from one sensor to create devices."

IP will be used to group components into devices for all components seen by one sensor.

4. Vlan considerations:
 - a. Option 1 needs VLAN ID to work
 - b. Option 2 must not have VLAN ID to work.

CSCwi74303 API route /devices/:id/vulnerabilities response has changed in 4.3.0

API route devices changed; vulnerabilities are having less details.

Links

Software Download

The files below can be found at the following link:

<https://software.cisco.com/download/home/286325414/type>

Remarks:

- VMWare OVA files are available in 2 different configurations: A standard configuration and a specific configuration with an extra interface made to receive OT network traffic and do the DPI. The DPI center will do the DPI of that traffic directly like remote sensors are doing it.
- IOX sensors are available in 2 versions: one with the active discovery capability, another one without that capability. The version without that capability prevents any active behavior on the OT network.

Center	Description
CiscoCyberVision-center-4.3.0.ova	VMware OVA file, for Center setup
CiscoCyberVision-center-with-DPI-4.3.0.ova	VMware OVA file, for Center with DPI setup
CiscoCyberVision-center-4.3.0.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-reports-management-4.3.0.ext	Reports management extension installation file
CiscoCyberVision-sensor-management-4.3.0.ext	Sensor management extension installation file
Sensor	Description
CiscoCyberVision-IOx-aarch64-4.3.0.tar	Cisco IE3400, Cisco IE3300 10G, Cisco IE9300, Cisco IR1101 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64--4.3.0.tar	Cisco IE3400, Cisco IE3300 10G, Cisco IE9300 Cisco IR1101 Active Discovery sensor installation and update file
CiscoCyberVision-IOx-IC3000-4.3.0.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-IC3000-4.3.0.tar	Cisco IC3000 Active Discovery sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.3.0.tar	Cisco Catalyst 9x00 and Cisco Catalyst IR8340 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.3.0.tar	Cisco Catalyst 9x00 and Cisco Catalyst IR8340 Active Discovery sensor installation and update file
Updates	Description
CiscoCyberVision-Embedded-KDB-4.3.0.dat	KnowledgeDB embedded in Cisco Cyber Vision 4.3.0
CiscoCyberVision-update-center-4.3.0.dat	Center update file for upgrade from release 4.1.x or 4.2.x to release 4.3.0
CiscoCyberVision-update-sensor-4.3.0.dat	Cisco IC3000 Sensor update file for upgrade from release 4.0.x or 4.1.x to release 4.3.0
CiscoCyberVision-update-combined-4.3.0.dat	Center and IC3000 Sensor update file from GUI for upgrade from release 4.0.x or 4.1.x to release 4.3.0

Cisco Cyber Vision Center 4.3.0 can also be deployed on AWS (Amazon Web Services) and Microsoft Azure.

The Cisco Cyber Vision Center AMI (Amazon Machine Image) can be found on the AWS Marketplace:

<https://aws.amazon.com/marketplace/pp/prodview-tql4ows5l5cle>

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

<https://aws.amazon.com/marketplace/search/results?searchTerms=Cisco+Cyber+vision>

The Cisco Cyber Vision Center Plan can be found on the Microsoft Azure marketplace:

<https://azuremarketplace.microsoft.com/en-us/marketplace/apps/cisco.cisco-cyber-vision?tab=Overview>

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:
[Cisco Cyber Vision GUI User Guide](#)
- Cisco Cyber Vision GUI Administration User Guide:
[Cisco Cyber Vision GUI Administration Guide](#)
- Cisco Cyber Vision Monitor Mode Guide
[Cisco Cyber Vision Monitor Mode Guide](#)
- Cisco Cyber Vision Architecture Guide
[Cisco Cyber Vision Architecture Guide](#)
- Cisco Cyber Vision Active Discovery Configuration Guide
[Cisco Cyber Vision Active Discovery Configuration Guide](#)
- Cisco Cyber Vision Sensor Application for Cisco Switches Installation Guide:
[Cisco Cyber Vision Sensor Application for Cisco Switches Installation Guide](#)
- Cisco Cyber Vision Network Sensor Installation Guide for Cisco IR1101:
[Cisco Cyber Vision Network Sensor Installation Guide for Cisco IR1101](#)
- Cisco Cyber Vision Network Sensor Installation Guide for Cisco IC3000:
[Cisco Cyber Vision Network Sensor Installation Guide for Cisco IC3000](#)
- Cisco Cyber Vision Network Sensor Installation Guide for Cisco IR8340:
[Cisco Cyber Vision Network Sensor Installation Guide for Cisco IR8340](#)
- Cisco Cyber Vision Center Appliance Installation Guide:
[Cisco Cyber Vision Center Appliance Installation Guide](#)
- Cisco Cyber Vision Center VM Installation Guide:
[Cisco Cyber Vision Center VM Installation Guide](#)
- Cisco Cyber Vision Center AWS Installation Guide:
[Cisco Cyber Vision for AWS Cloud Installation Guide](#)
- Cisco Cyber Vision Center Azure Installation Guide:
[Cisco Cyber Vision for Azure Cloud Installation Guide](#)
- Cisco Cyber Vision Integration Guide, Integrating Cisco Cyber Vision with Cisco Identity Services Engine (ISE) via pxGrid:
[Integrating-Cisco-Cyber-Vision-with-Cisco-Identity-Services-Engine-via-pxGrid_3_1_1.pdf](#)
- Cisco Cyber Vision Smart Licensing User Guide
[Cisco Cyber Vision Smart Licensing User Guide](#)