

Release Notes for Cisco Cyber Vision

Release 5.0.0

July 2024

Contents

Compatible device list	3
Unsupported device list.....	4
Cisco Cyber Vision 5.0.0 update procedure	5
Upgrade to 5.0.0 considerations – To read before updating	5
Upgrade path	7
Compatibility Guidelines	7
Data purge	8
System updates - Preliminary checks	9
System updates – Cyber Vision system from 4.4.x to 5.0.x	10
System updates – Cyber Vision system from 4.3.x to 5.0.x	16
AWS and Azure Centers	19
Cisco Cyber Vision 5.0.0 important changes	20
Communication port and protocol changes	20
API	20
SYSLOG	20
Cisco Cyber Vision new features and improvements	21
Custom preset categories	21
Vulnerability csv export	23
Report enhancements	24
Deployment tokens	25
Cisco Cyber Vision Center service status	27
New user interface	28
DPI changes	28
Active Discovery	28
Cisco Cyber Vision 5.0.0 Resolved Caveats.....	29
Cisco Cyber Vision Open Caveats	30
Cisco Cyber Vision deprecated features.....	30
Links	31
Software Download	31
Related Documentation	33

Compatible device list

Table 1. Centers

Center	Description
VMware ESXi OVA center	VMware ESXi 6.x or later
Windows Server Hyper-V VHD Center	Microsoft Windows Server Hyper-V version 2016 or later
CV-CNTR-M6N Cisco UCS C225 M6N	Cyber Vision Center hardware appliance (Cisco UCS® C225 M6 Rack Server) - 24 core CPU, 128 GB RAM, Two or Four 1.6 TB NVMe drives
CV-CNTR-M5S5 Cisco UCS C220 M5	Cyber Vision Center hardware appliance (Cisco UCS® C220 M5 Rack Server) - 16 core CPU, 64 GB RAM, 800GB drives
CV-CNTR-M5S3 Cisco UCS C220 M5	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

Table 2. Sensors

Platform	Minimum Version	Recommended Version	Description
Cisco IC3000	1.5.1	1.5.1	Cyber Vision Sensor IOx application hosted in Cisco IC3000
Cisco Catalyst IE3400	17.3.x	17.6.7 / 17.9.5 / 17.12.2	Cyber Vision Sensor IOx application hosted in Cisco Catalyst IE3400 Industrial Ethernet switches
Cisco Catalyst IE3300 10G	17.6.x	17.6.7 / 17.9.5 / 17.12.2	Cyber Vision Sensor IOx application hosted in Cisco Catalyst IE3300 Industrial Ethernet switches with 10G ports
Cisco Catalyst IE3300 *	17.11.x	17.12.2	Cyber Vision Sensor IOx application hosted in Cisco Catalyst IE3300 Industrial Ethernet switches
Cisco Catalyst IE9300	17.12.x	17.12.2	Cyber Vision Sensor IOx application hosted in Cisco Catalyst IE9300 Rugged Series switches (IOS 17.12 mini)
Cisco IR1101	17.3.x	17.6.7 / 17.9.5 / 17.12.2	Cyber Vision Sensor IOx application hosted in Cisco IR1101 Series Industrial Integrated Services Routers
Cisco IR1800**	17.15.1	17.15.1	Cyber Vision Sensor IOx application hosted in Cisco IR1800 Rugged Series Routers
Cisco Catalyst IR8300	17.9.x	17.9.5 / 17.12.2	Cyber Vision Sensor IOx application hosted in Cisco Catalyst IR8300 Rugged Series Routers
Cisco Catalyst 9300, 9400***	17.3.3	17.6.7 / 17.9.5 / 17.12.2	Cyber Vision Sensor IOx application hosted in Catalyst 9300, 9300L, 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`.

** Cisco IR1835 with IOS 17.15 supports up to 3GB of memory allocated to IOX.

*** Cisco Catalyst 9400 requires IOS XE 17.5.1 minimum to deploy an IOX application without SSD

Unsupported device list

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

Table 3. Sentryo centers (end of life)

Center	Description
Sentryo CENTER10	Sentryo CENTER10 hardware appliance
Sentryo CENTER30	Sentryo CENTER30 hardware appliance

Table 4. Sentryo sensors (end of life)

Center	Description
Sentryo SENSOR3	Sentryo SENSOR3 hardware appliance
Sentryo SENSOR5	Sentryo SENSOR5 hardware appliance
Sentryo SENSOR7	Sentryo SENSOR7 hardware appliance

Cisco Cyber Vision 5.0.0 update procedure

Cisco Cyber Vision 5.0.0 update procedure depends on the architecture deployed and the tool used to deploy it.

Upgrade to 5.0.0 considerations – To read before updating

Four important considerations need to be understood before upgrading a system to 5.0.0.

Consideration 1

Upgrading to 4.3.0 is mandatory before upgrading to 5.0.0 if the targeted Center is still in a version below 4.3.0.

Consideration 2

Cisco Cyber Vision Center system partition size needs to be checked if the Center was originally installed with a Cisco Cyber Vision version below 3.2.0.

Cisco Cyber Vision Center system has two partitions, one for the system, the other for data. Before version 3.2.0 the system partition had a size of 512MB, which is now too limited for version 5.0.0.

During the Center upgrade to 5.0.0, a check will be done, and the upgrade will be stopped if the system partition size is below 1GB. A message will be then displayed:

“This Center is installed on a partition which is less than 1GB. Upgrading to 4.4.0 or greater is not possible on this kind of installation. Please contact TAC”.

The following command can also be used to check the Center partition size:

```
lsblk
```

The command answer will be something like:

```
sda      8:0    0   500G  0 disk
├--sda1  8:1    0    511M  0 part  /system
└--sda2  8:2    0  499.5G  0 part
   └--data_crypt 251:0    0  499.5G  0 crypt /data
```

Figure 1.

Cisco Cyber Vision system check – partition size

If the partition sda1 is having a size below 1GB, the upgrade will not be completed, and the TAC support needs to be contacted.

Consideration 3

Cisco Cyber Vision hardware sensors are no longer supported. All Centers with a database containing IC3000 sensors with a version below 4.3.0 or some Sentryo's sensors are not upgradable to version 4.4.x and 5.0.x.

To upgrade to version 5.0.0, all old Sentryo's sensors must be removed and the IC3000 sensors must be upgraded to version 4.3.0 or later.

A warning message will prevent users and the upgrade will be stopped:

“Some sensors attached to this Center are not supported anymore. 4.3.x is their last supported version. IC3000 sensor is still supported but needs to be updated to IOX version 4.3.0 or above. Other sensors must be removed to update this Center.”

Consideration 4

Cisco Cyber Vision upgrade process changed and during the first boot the Center may be long to start. During this phase the Center Database is updated to a new schema and maintained, it could take time and will depend on the system performance and the amount of data stored. During this step the following message will appear in place of the user interface:

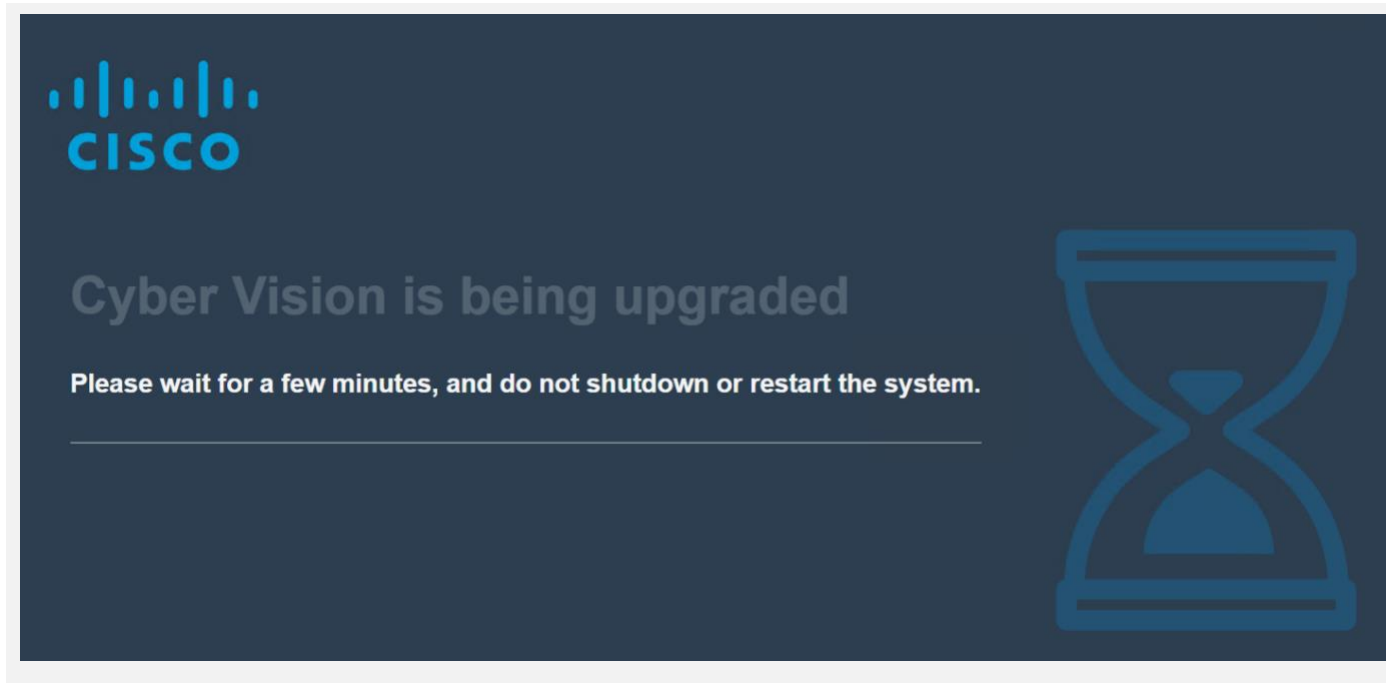


Figure 2.
Cisco Cyber Vision upgrade considerations – upgrade warning

Upgrade path

Table 5. Upgrade Path to Cisco Cyber Vision 5.0.0

Current Software Release	Upgrade Path to Release 4.4.2
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, then to 5.0.0
Version 3.2.4	Upgrade first to 4.0.0, then to 4.1.4, then to 4.3.0, then to 5.0.0
Version 4.0.0 to 4.0.3	Upgrade first to 4.1.4, then to 4.3.0, then to 5.0.0
Version 4.1.0 to 4.1.4	Upgrade first to 4.3.0, then to 5.0.0
Version 4.2.0 to 4.2.6	Upgrade first to 4.3.0 and then to 5.0.0
Version 4.3.0 to 4.3.3	Upgrade directly to 5.0.0
Version 4.4.0 to 4.4.3	Upgrade directly to 5.0.0

For the upgrade to any previous release (i.e. 4.3.0), please read carefully the Release Notes of the corresponding release available here: [Cyber Vision release notes](#).

Compatibility Guidelines

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

- Global Center (Version N): Compatible with Centers with synchronization 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 synchronization (Version N): Compatible with sensors with versions N and N-1 (e.g., Center with synchronization 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 5.0.0:

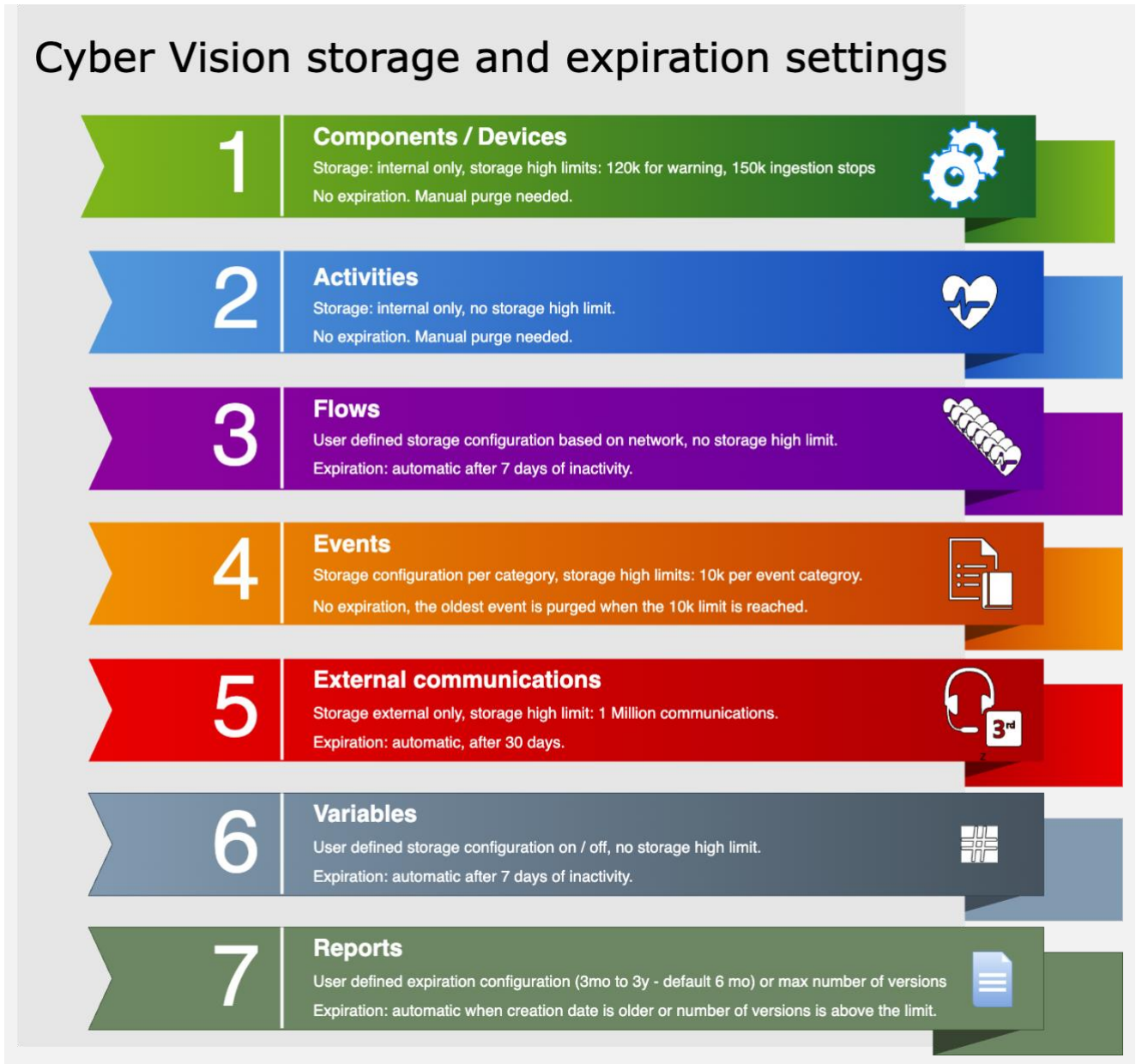


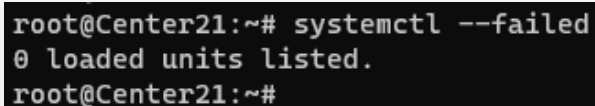
Figure 3.
Cisco Cyber Vision data retention policies

System updates - Preliminary checks

1. We highly recommend that you check the health of all Centers connected to the Global Center and of the Global Center itself before updating.
2. 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.

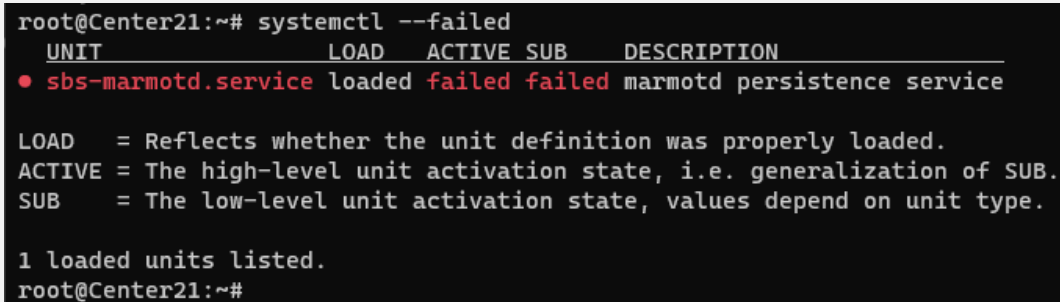


```
root@Center21:~# systemctl --failed
0 loaded units listed.
root@Center21:~#
```

Figure 4.

Cisco Cyber Vision system check – 0 failure

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



```
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:~#
```

Figure 5.

Cisco Cyber Vision system check – example of failure

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

System updates – Cyber Vision system from 4.4.x to 5.0.x

Architecture with Global Center

1. Update the Global Center with a or b methods below.
 - a. Use the Graphical User Interface:
 - File= CiscoCyberVision-update-center-<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 Centers connected to the Global Center with the same procedure used for the Global Center (User Interface or CLI).
3. Update the different extensions installed:
 - a. If you installed the sensor management extension, upgrade the extension:
 - File = CiscoCyberVision-sensor-management-<LAST-VERSION>.ext
 - Navigate to **Admin > Extensions**. In the **Actions** column on the far right, 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 --run /data/tmp/CiscoCyberVision-sensor-management-<LAST-VERSION>.ext
```

- b. If you installed the report management extension, upgrade the extension:
 - File = CiscoCyberVision-report-management-<LAST-VERSION>.ext
 - Navigate to **Admin > Extensions**. In the **Actions** column on the far right, use the **Update** button and browse to select the update file.
 - The Cisco Cyber Vision report management extension can also be updated from the CLI with the command:

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

4. Update the sensors from their corresponding Center (not from the Global Center).

Update all sensors with the sensor self-update feature. Cisco Cyber Vision now allows sensor updates regardless of the install method (i.e., without the extension). Release 4.4.0 provides the necessary foundation for sensor self-updates. Starting with Cisco Cyber Vision release 4.4.1, you can update all sensors automatically. The required steps are:

- Select sensors to update.
- The Center adds a new job to the sensor queue.
- The sensor automatically collects and validates the update file.
- The sensor restarts with the new version.

To do so: navigate to **Admin > Sensors > Sensor Explorer** and select the different sensors you would like to update, or all sensor with the top left check box:

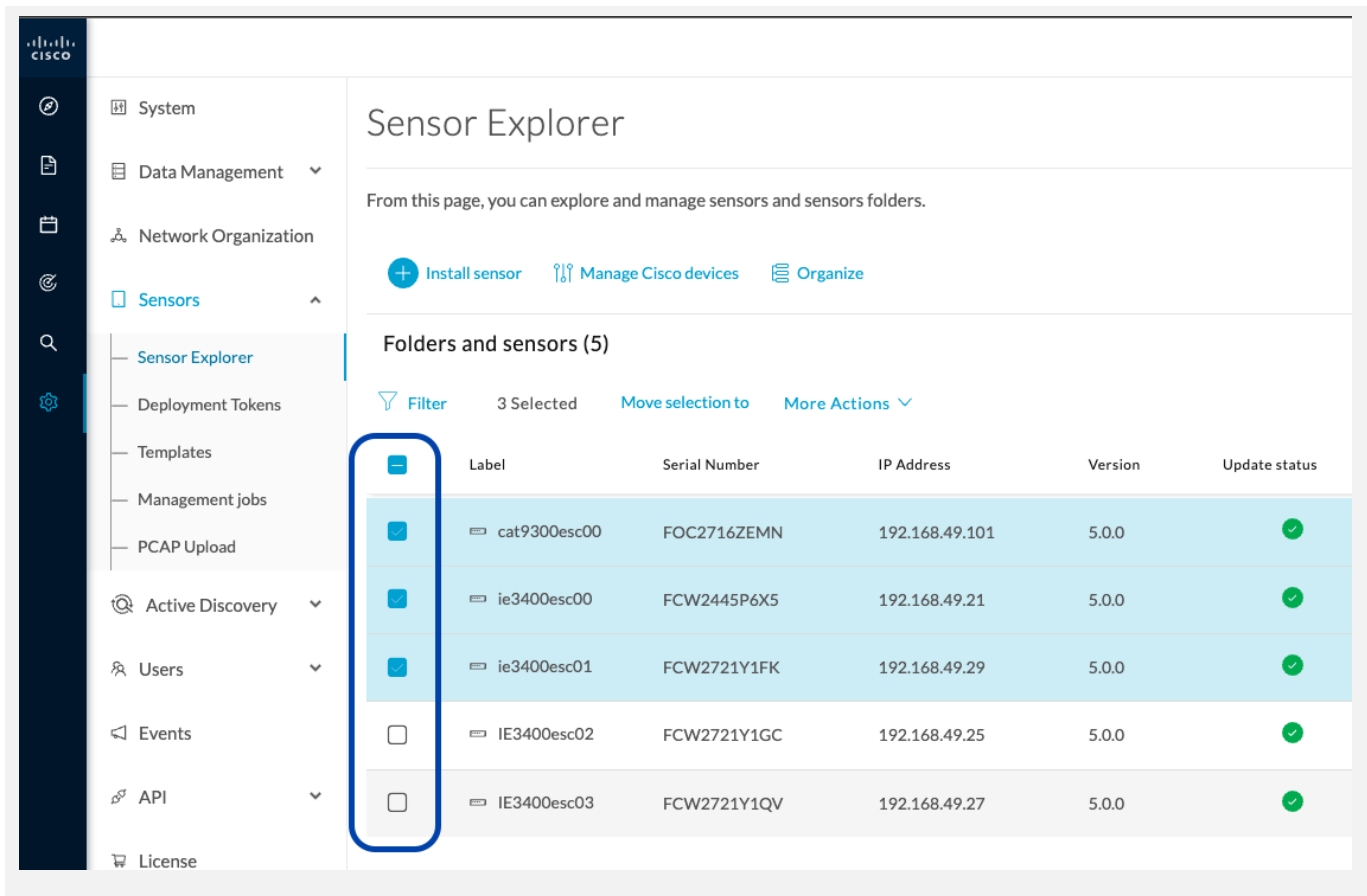


Figure 6.
Cisco Cyber Vision sensor to update selection

Then use the menu, **More Actions > Update sensors** it will open a menu to proceed to the update:

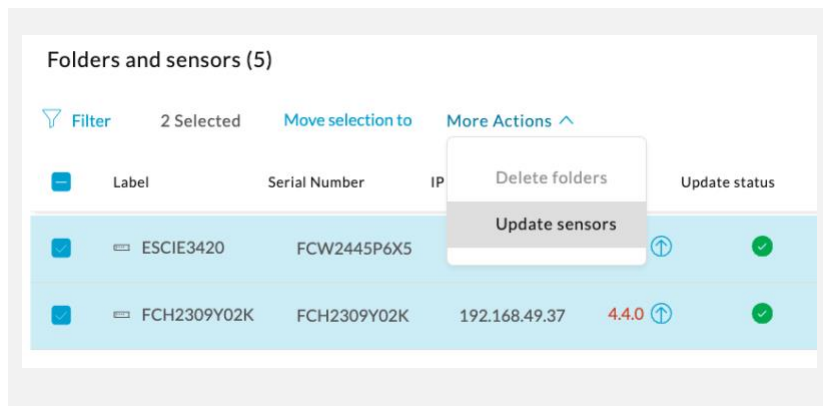


Figure 7.
Cisco Cyber Vision Update sensors menu

For a complete procedure, use any sensor installation guide from version 5.0.0 or later.

Guideline links:

- [Cisco Cyber Vision Sensor Application for Cisco Switches Installation Guide, Release 4.4.0](#)
- [Cisco Cyber Vision Network Sensor Installation Guide for Cisco IR8340, Release 4.4.0](#)
- [Cisco Cyber Vision Network Sensor Installation Guide for Cisco IC3000, Release 4.3.0](#)
- [Cisco Cyber Vision Network Sensor Installation Guide for Cisco IR1101, Release 4.4.0](#)

Architecture with one Center

1. Update the Center with a or b methods below.

a. Use the Graphical User Interface:

- File= CiscoCyberVision-update-center-<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 different extensions installed:

a. If you installed the sensor management extension, upgrade the extension:

- File = CiscoCyberVision-sensor-management-<LAST-VERSION>.ext
- Navigate to **Admin > Extensions**. In the **Actions** column on the far right, 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 --run /data/tmp/CiscoCyberVision-sensor-management-<LAST-VERSION>.ext
```

b. If you installed the report management extension, upgrade the extension:

- File = CiscoCyberVision-report-management-<LAST-VERSION>.ext
- Navigate to **Admin > Extensions**. In the **Actions** column on the far right, use the **Update** button and browse to select the update file.
- The Cisco Cyber Vision report management extension can also be updated from the CLI with the command:

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

3. Update sensors

Update all sensors with the sensor self-update feature. Cisco Cyber Vision now allows sensor updates regardless of the install method (i.e., without the extension). Release 4.4.0 provides the necessary foundation for sensor self-updates. Starting with Cisco Cyber Vision release 4.4.1, you can update all sensors automatically. The required steps are:

- Select sensors to update.
- The Center adds a new job to the sensor queue.
- The sensor automatically collects and validates the update file.
- The sensor restarts with the new version.

To do so: navigate to **Admin > Sensors > Sensor Explorer** and select the different sensors you would like to update, or all sensor with the top left check box:

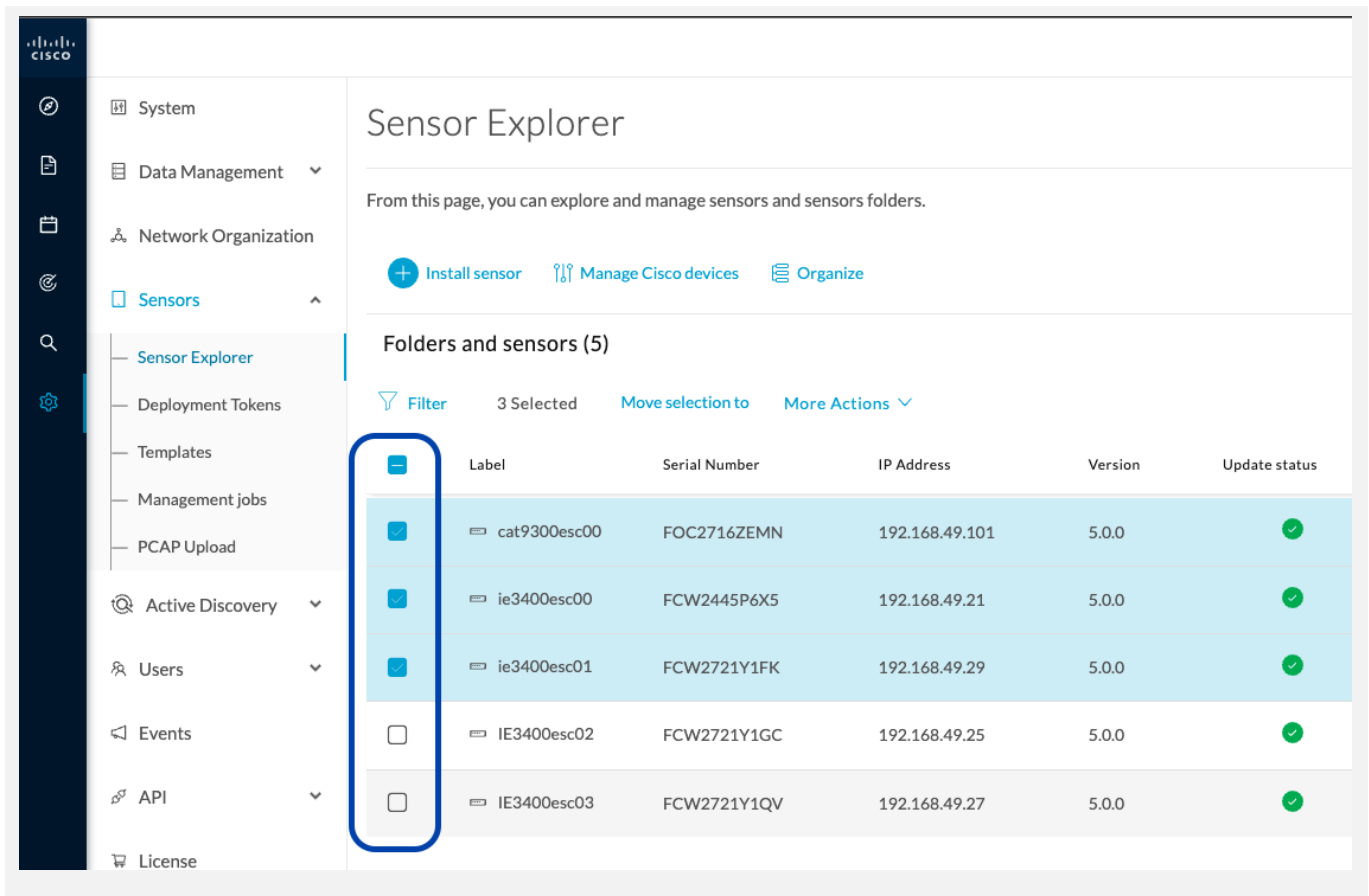


Figure 8.
Cisco Cyber Vision sensor to update selection

Then use the menu, **More Actions > Update sensors** it will open a menu to proceed to the update:

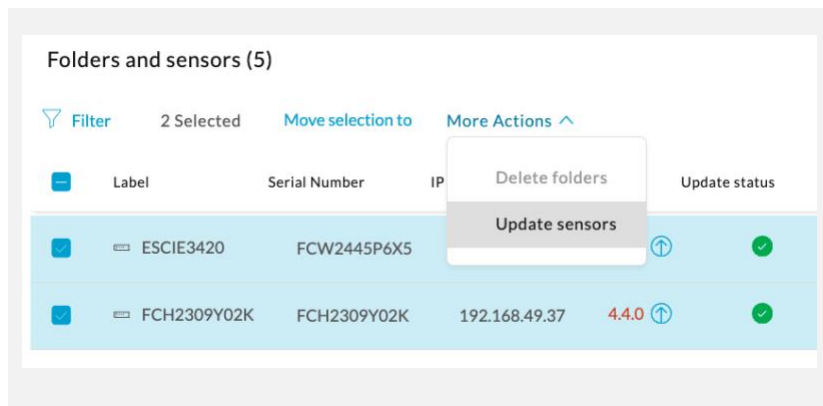


Figure 9.
Cisco Cyber Vision Update sensors menu

For a complete procedure, use any sensor installation guide from version 5.0.0 or later.

Guideline links:

- [Cisco Cyber Vision Sensor Application for Cisco Switches Installation Guide, Release 4.4.0](#)
- [Cisco Cyber Vision Network Sensor Installation Guide for Cisco IR8340, Release 4.4.0](#)
- [Cisco Cyber Vision Network Sensor Installation Guide for Cisco IC3000, Release 4.3.0](#)
- [Cisco Cyber Vision Network Sensor Installation Guide for Cisco IR1101, Release 4.4.0](#)

System updates – Cyber Vision system from 4.3.x to 5.0.x

Architecture with Global Center

1. Update the Global Center with a or b methods below.
 - a. Use the Graphical User Interface:
 - File= CiscoCyberVision-update-center-<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 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 on the far right, 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 --run /data/tmp/CiscoCyberVision-sensor-management-<LAST-VERSION>.ext
```

- ii. Update all sensors with the extension.

Click **Admin > Sensors > Sensor Explorer > Manage Cisco devices > Update Cisco devices** or use the redeploy button in the sensor's right-side panel. For a complete procedure, use any sensor installation guide from version 4.2.0 or later.

- 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.
 - o IE3x00, IE93x0 and IR1101 files = CiscoCyberVision-IOx-aarch64--<LAST-VERSION>.tar or CiscoCyberVision-IOx-Active-Discovery-aarch64---<LAST-VERSION>.tar
 - o Catalyst 9300 and 9400 and IR8340 files = CiscoCyberVision-IOx-x86-64-<LAST-VERSION>.tar or CiscoCyberVision-IOx-Active-Discovery-x86-64-<LAST-VERSION>.tar.
 - o IC3000 files = CiscoCyberVision-IOx-IC3000-<LAST-VERSION>.tar or CiscoCyberVision-IOx-Active-Discovery-IC3000-<LAST-VERSION>.tar

Guideline links:

[Cisco Cyber Vision Sensor Application for Cisco Switches Installation Guide, Release 4.4.0](#)

[Cisco Cyber Vision Network Sensor Installation Guide for Cisco IR8340, Release 4.4.0](#)

[Cisco Cyber Vision Network Sensor Installation Guide for Cisco IC3000, Release 4.3.0](#)

[Cisco Cyber Vision Network Sensor Installation Guide for Cisco IR1101, Release 4.4.0](#)

Architecture with one Center

4. Update the Center with a or b methods below.

a. Use the Graphical User Interface:

- File= CiscoCyberVision-update-center-<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
```

5. 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 on the far right, 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 --run /data/tmp/CiscoCyberVision-sensor-management-<LAST-VERSION>.ext
```

ii. Update all sensors with the extension.

Click **Admin > Sensors > Sensor Explorer > Manage Cisco devices > Update Cisco devices** or use the redeploy button in the sensor's right-side panel. For a complete procedure, use any sensor installation guide from version 4.2.0 or later.

- 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.
 - o IE3x00, IE93x0 and IR1101 files = CiscoCyberVision-IOx-aarch64--<LAST-VERSION>.tar or CiscoCyberVision-IOx-Active-Discovery-aarch64---<LAST-VERSION>.tar
 - o Catalyst 9300 and 9400 and IR8340 files = CiscoCyberVision-IOx-x86-64-<LAST-VERSION>.tar or CiscoCyberVision-IOx-Active-Discovery-x86-64-<LAST-VERSION>.tar.
 - o IC3000 files = CiscoCyberVision-IOx-IC3000-<LAST-VERSION>.tar or CiscoCyberVision-IOx-Active-Discovery-IC3000-<LAST-VERSION>.tar

Guideline links:

[Cisco Cyber Vision Sensor Application for Cisco Switches Installation Guide, Release 4.4.0](#)

[Cisco Cyber Vision Network Sensor Installation Guide for Cisco IR8340, Release 4.4.0](#)

[Cisco Cyber Vision Network Sensor Installation Guide for Cisco IC3000, Release 4.3.0](#)

[Cisco Cyber Vision Network Sensor Installation Guide for Cisco IR1101, Release 4.4.0](#)

AWS and Azure Centers

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

Cisco Cyber Vision 5.0.0 important changes

Communication port and protocol changes

Port

No modification in 5.0.0.

Protocol

No modification in 5.0.0.

API

Some changes were made in release 5.0.0. Several API routes changed:

New endpoints - No modification in 5.0.0.

New attributes - No modification in 5.0.0.

Removed endpoint - No modification in 5.0.0.

Changed endpoints - No modification in 5.0.0.

SYSLOG

No modification in 5.0.0.

Cisco Cyber Vision new features and improvements

Custom preset categories

Cyber Vision 5.0.0 includes the concept of preset categories. It will help the user to organize and filter all custom presets created. This new feature is available from the main Explore menu:

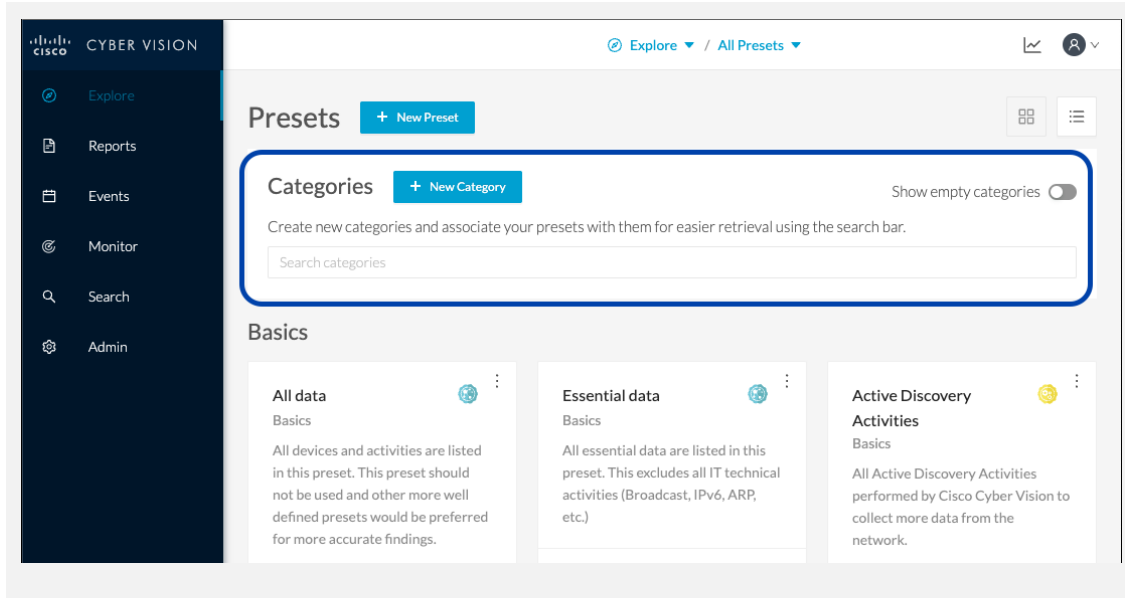


Figure 10.
Cisco Cyber Vision Explore menu with the new custom preset categories

When a custom preset is created it can be associated to a category. All existing custom presets can also be associated to categories. It will help the user to easily and quickly retrieve an existing preset.

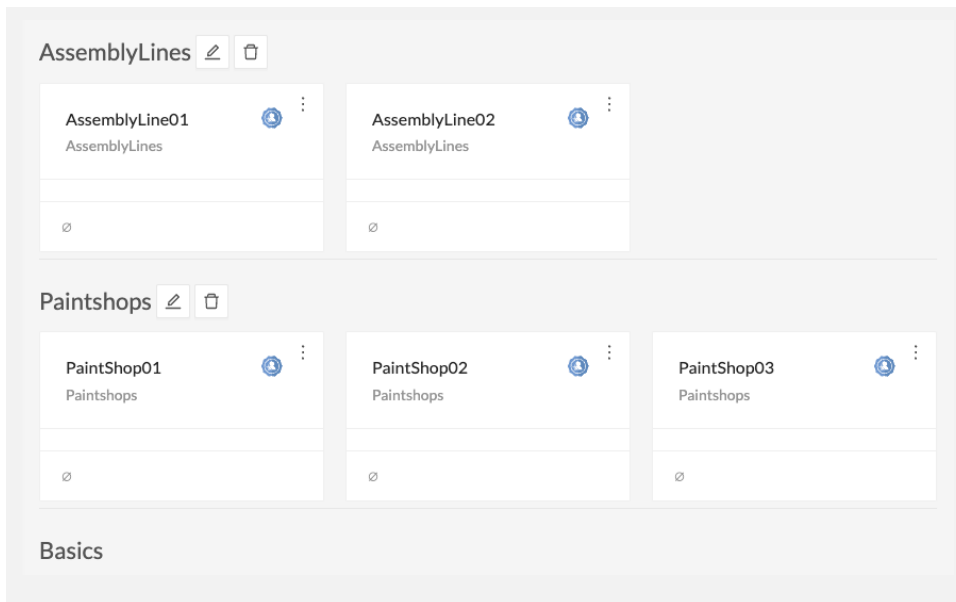


Figure 11.
Cisco Cyber Vision Explore menu with defined custom preset categories

Users can filter presets based on their category. For example, only the presets from the “Paintshops” category are shown here below:

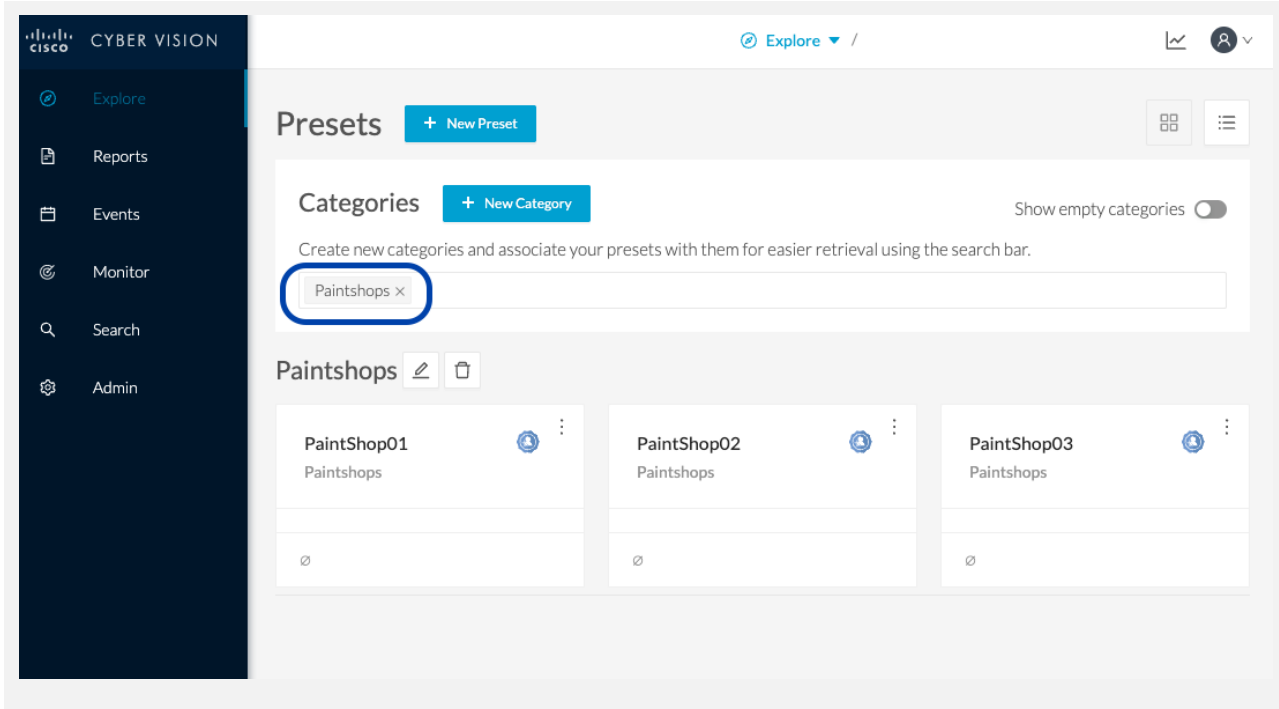


Figure 12.
Cisco Cyber Vision Explore preset filtered

This filter is also available in the Cisco Cyber Vision Center’s URL and can be bookmarked.

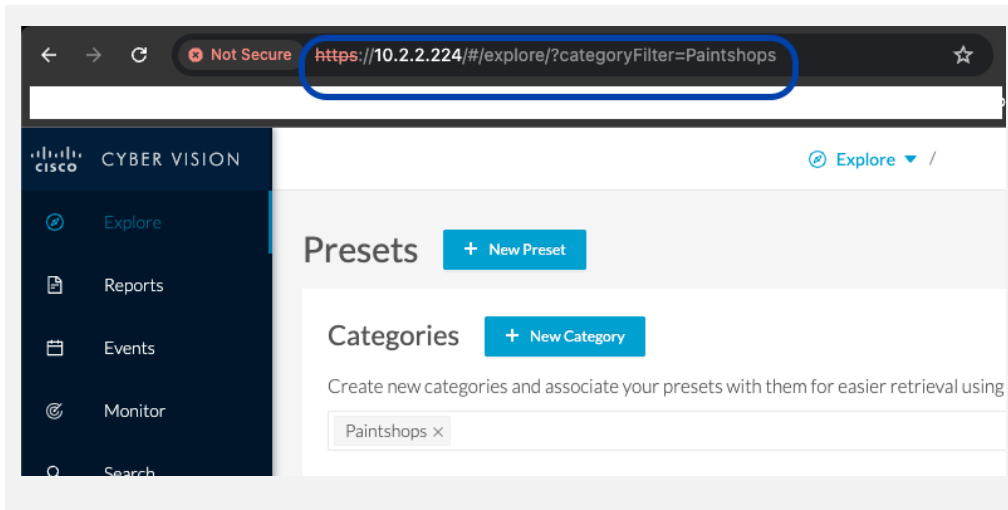


Figure 13.
Cisco Cyber Vision URL with category filters

Vulnerability csv export

In Cisco Cyber Vision release 5.0.0 a new vulnerability CSV export button is available on the vulnerability page of each preset. For example:

The screenshot shows the Cisco Cyber Vision interface for the 'Vulnerabilities' section. At the top, there's a navigation bar with 'Explore' and 'All data' menus, and a 'Vulnerabilities' dropdown menu. Below this, a time range filter shows 'Last 1h (Jul 5, 2024 4:53:02 PM – Jul 5, 2024 5:53:02 PM)' and a 'Refresh' button. The main content area is divided into several sections:

- 10 most matched vulnerabilities:** A donut chart on the left shows the distribution of vulnerabilities by severity. To the right, a list of 10 vulnerabilities is shown, each with its CVE ID, title, and the number of affected devices.

CVE ID	Title	Affected devices
CVE-2023-20198	Cisco IOS XE Software Web UI Privilege Escalatio...	4 affected devices
CVE-2017-11780	Windows SMB Remote Code Execution Vulnerability	1 affected device
CVE-2017-0143	Windows SMB Remote Code Execution Vulnerability	1 affected device
CVE-2017-0146	Windows SMB Remote Code Execution...	1 affected device
CVE-2022-20919	Cisco IOS and IOS XE Software Common...	1 affected device
CVE-2017-0147	Windows SMB Information Disclosure...	1 affected device
CVE-2017-0279	Windows SMB Remote Code Execution Vulnerability	1 affected device
CVE-2017-0275	Windows SMB Information Disclosure...	1 affected device
CVE-2017-0280	Windows SMB Denial of Service Vulnerability	1 affected device
CVE-2023-20076	Cisco IOx Application Hosting Environment...	1 affected device
- 5 vulnerable devices on All data preset:** A summary card on the right indicates that 5 devices are vulnerable across the entire data preset.
- Vulnerability severity legend:** A legend below the chart shows color-coded boxes for NONE (green), LOW (yellow), MEDIUM (orange), HIGH (red), and CRITICAL (black).
- 29 Vulnerabilities:** A table below the legend lists all 29 vulnerabilities. The first row is highlighted:

Vulnerability title	CVE	CVSS score	Affected devices
Cisco IOS XE Software Web UI Privilege Escalation Vulnerability	CVE-2023-20198	10 (v3.1)	4 devices
Cisco IOS and IOS XE Software Common Industrial Protocol...			
- Export to CSV:** A blue button with a download icon and the text 'Export to CSV' is located at the top right of the vulnerability list table.

A tooltip message states: 'Only devices with unacknowledged vulnerabilities will be listed in the CSV export'.

Figure 14.
Cisco Cyber Vision Vulnerability CSV export

This feature replaces the vulnerability legacy report.

Report enhancements

Cisco Cyber Vision version 5.0.0 brings several enhancements on the security report:

- About key findings, a new dynamic global Risk information line is available with:
 - If 70-100 then shows “Investigating network activities to restrict communications and resolving vulnerabilities or applying compensating controls should be a priority “
 - If 40-69 then shows “Resolving vulnerabilities is recommended, especially as individual devices might have very high scores”
 - If 0-39 then shows “Addressing vulnerabilities is still recommended although very few devices might need attention”
- A new sub section under risky communication is available to list all active DNS servers
- About external accesses: a total number of devices accessing external domains/IP addresses was added

Deployment tokens

Zero Touch Provisioning allows you to automate Cisco Cyber Vision deployment on sensor batches. It is to be used with third-party tools like Cisco Catalyst WAN Manager. Refer to its documentation on [cisco.com](https://www.cisco.com) to complete sensor deployment.

From this page, you can create, edit, and delete deployment tokens for Zero Touch Provisioning.

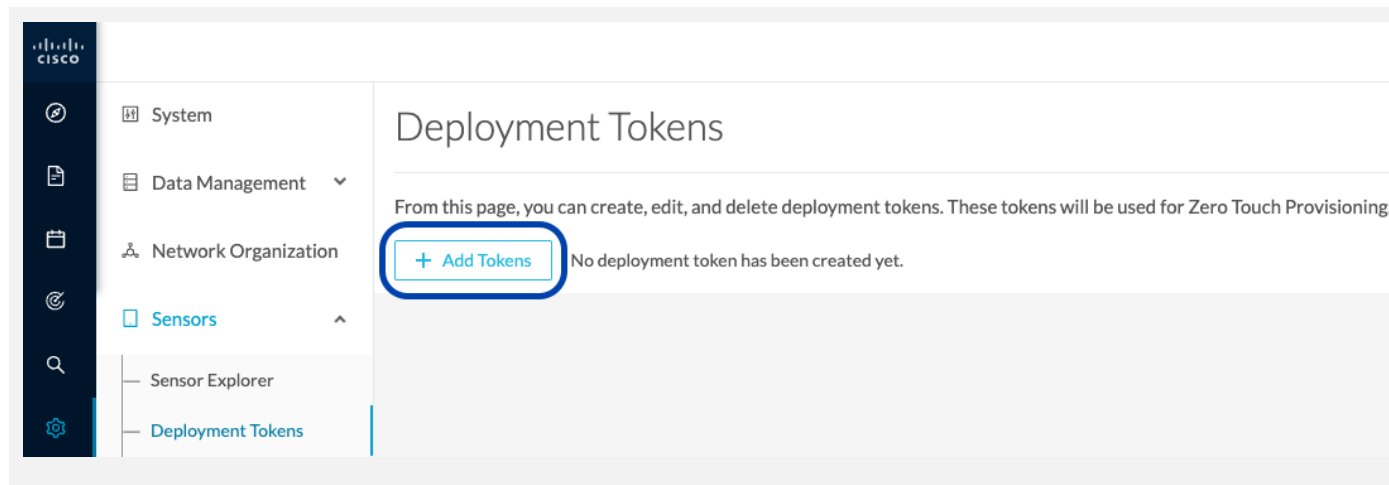


Figure 15.
Cisco Cyber Vision Deployment tokens – Add tokens

During token creation, the application will request a token per application type. A token contains the application name and a PSK (pre-shared key).

Once proper configuration is done on Cisco Catalyst WAN Manager, it will deploy the sensors and apply parameters which will allow the sensor to on-board itself on the Center.

Communication between the sensors and the Center will start after sensors have presented the PSK to the Center and the Center has delivered all necessary information for enrolment.

In the Add new deployment tokens:

- Add a name to the deployment phase.
- Add a number of uses for the number of devices to be deployed.
- Set the tokens expiration time.
- You can enable the token to continue the deployment process.

The screenshot shows a dialog box titled "Add new deployment tokens" with a close button (X) in the top right corner. The form contains the following fields:

- Name:** A text input field containing "Phase1".
- Number of uses:** A numeric input field with a spinner, containing the value "50".
- Expiration time:** A date picker field showing "2024-11-30".
- Enabled:** A toggle switch that is currently turned on (blue).

At the bottom of the dialog, there are two buttons: "Cancel" and "Create".

Figure 16.
Cisco Cyber Vision Deployment tokens – new token

The deployment phase with tokens per device type will be presented as a table in the new Deployment Tokens menu:

Name	Tokens	Status	Creation Date	Expiration Date	Usages	
Phase1	Image	Token	Enabled	Jul 5, 2024	Nov 30, 2024	0/50
	cviox-aarch64.tar	Show				
	cviox-active-discovery-aarch64.tar	Show				
	cviox-active-discovery-ic3000-x86-64.tar	Show				
	cviox-active-discovery-x86-64.tar	Show				
	cviox-ic3000-x86-64.tar	Show				
	cviox-x86-64.tar	Show				

Figure 17.
Cisco Cyber Vision Deployment tokens –token list

Cisco Cyber Vision Center service status

The service status page indicates whether all Cisco Cyber Vision background processes like services and extensions are up and running correctly. Checks are performed regularly.

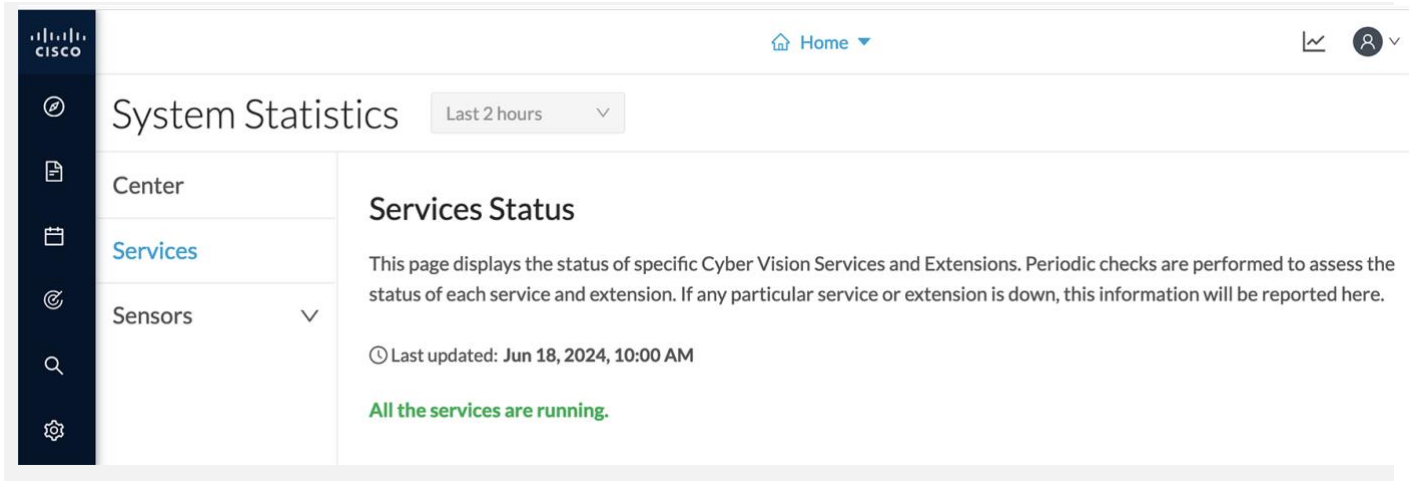


Figure 18.
Cisco Cyber Vision service status – All services running

A warning banner appears at the top of the application whenever a service or extension is down with a link to the Statistics page. The failing service or extension will appear in red.

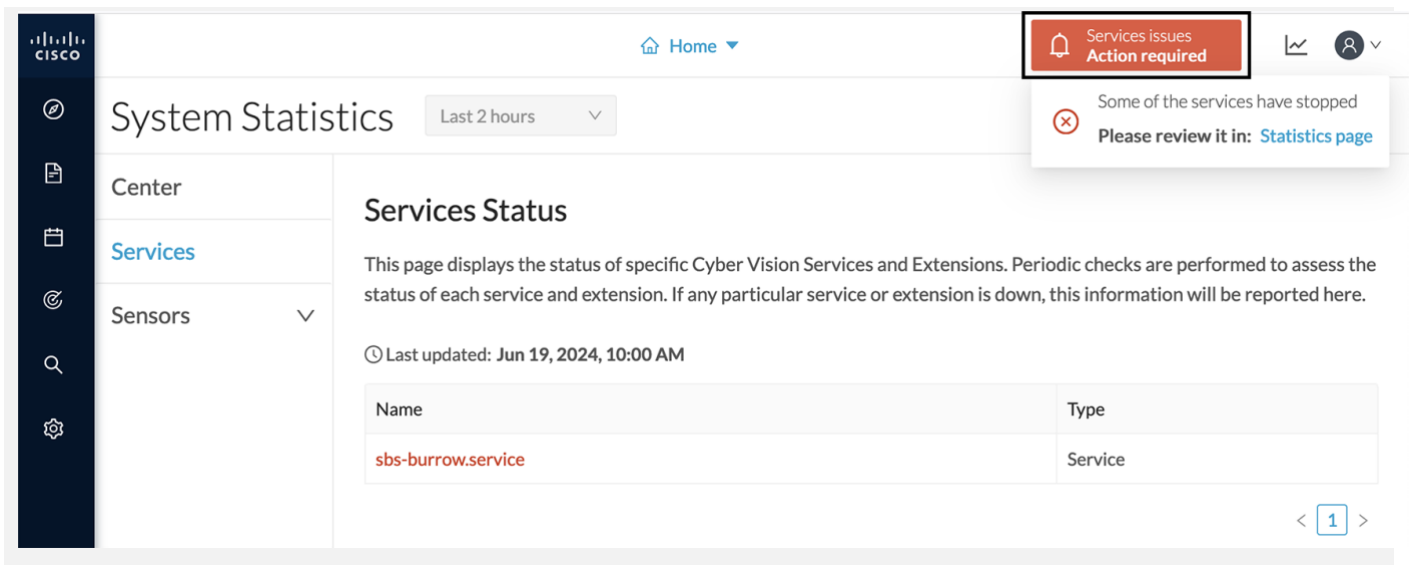


Figure 19.
Cisco Cyber Vision service status – one service is failing

New user interface

Cisco Cyber Vision 5.0.0 version includes a brand-new user interface that is only available in beta mode. Contact your Cisco representative for a demo session.

DPI changes

Protocol enhancements

List of the protocol enhancements:

- dce-rpc traffic not spotted when authentication of type "SPNEGO and level Packet integrity"
- DPI improvements - LLDP For Rockwell Automation PLC

Active Discovery

Global enhancements

The active discovery engine was updated to handle parallel scanning

Cisco Cyber Vision 5.0.0 Resolved Caveats

Table 6. Cisco Cyber Vision resolved caveats

CDETS	Description
CSCwd39017	Missing information in the Smart License Usage 12672
CSCwj40907	Error when trying to clear data on a center 15387
	Sensor self-update - Improve update for folder 15555
CSCwj93198	XDR: Correction in error message 15631
CSCwj93197	XDR: Option always shows "In progress" 15632
	Sticky filter on activity and device views on preset change 15644
	Clarify error message when sensor self-update ends up doing a rollback 15648
CSCwj79899	Collection interface used for active discovery is always shown as VLAN 1 15661
	HTTP Active discovery fails on some particular redirection 15669
CSCwj93196	FMC script is abnormally long during the synchronization 15744
	VRRP unicast activities are wrongly tagged "Multicast" 15748
	Services are trying to connect to pxGrid on Global Center 15755
	Sensors sometimes loose secure storage enrollment data 15759
CSCwk14838	CV Unable to retrieve users from "Nested" Group on Windows LDAP 15870
CSCwk04882	Rabbitmq queues ttl may not be applied on all queues 15871
CSCwk04881	Additional NIC card on UCS M6 can shift port numbering 15876
	Backup and restore – restoring a dual interface center on a center configured as single interface is not working 15877
CSCwk19981	Selected device counter is lost 15937
CSCwk19980	No redirection with LDAP users and expired license 15941
	Services monitoring issues 15958
CSCwk24950	Bogus MAC addresses created when erspan is fragmented 5971
CSCwk50604	sbs-refresh-viewsd crash when a preset(s) is deleted before getting refreshed 15975
	Sensor self update - Improve update for folder 15994
	API - Request Preset RiskScore via API return 0 16062
	Certificate: wrong warning message seen on the center 16101
CSCwk50603	Remote Access Report is empty - No Data Found 16122
CSCwk50606	Disabled telemetry service warning when DNS is unresponsive 16152
CSCwk50605	Service status issue on GC 16154
	XDR investigation redirection leads to SecureX page 16155
CSCwk53768	IC3000 drops L2 packets 16159
CSCwk62289	Evaluation of cybervision for OpenSSH regreSSHion vulnerability
CSCwh80822	Handle snmp sysDesc on IE switch where Profinet is enabled 14092
CSCwj52714	Flow panic in protocolReassembly with CIP 15448
	Flow panic on DCE-RPC 15345
CSCwk24950	Bogus mac addresses created when erspan is fragmented 15971
	wrong OPC-UA application name 14995
CSCwh80822	Handle snmp sysDesc on IE switch where Profinet is enabled 14092
	Model-ref and model-name swap for Melsoft/Fins/Bacnet/DNP3 15404
CSCwi44112	API Active discovery endpoints issue 15602
	Beckhoff and Bacnet Active Discovery does not show broadcast queries 15498
CSCwd39017	Missing information in the Smart License Usage 12672
CSCwj40907	Error when trying to clear data on a center 15387
CSCwk62289	Evaluation of Cyber Vision for OpenSSH regreSSHion vulnerability

Cisco Cyber Vision Open Caveats

Table 7. Cisco Cyber Vision open caveats

CDETS	Component	Description
CSCwk42900	Center	Sensors still count for license when snort is disabled by CLI
CSCwk39764	Center	License expired redirection prevents from disabling snort

Cisco Cyber Vision deprecated features

Cisco Cyber Vision integrations with FMC and FTD will be deprecated. It is now displayed in the product shown below:

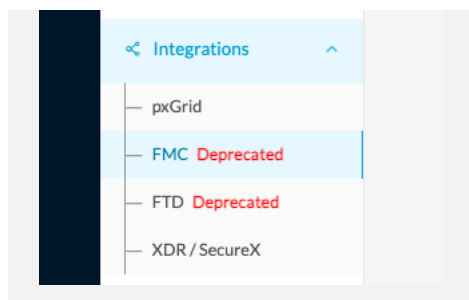


Figure 20. Cisco Cyber Vision integrations

The 2 features will be removed from the product in release 5.1.0 (end of calendar year 2024).

FMC integration will be replaced by a new connector available in the FMC Cisco Secure Dynamic Attributes Connector (CSDAC). CSDAC Cyber Vision documentation is available here:

[Cisco Secure Dynamics Attributes Connector Guides](#)

For example: [Cisco Secure Dynamic Attributes Connector Configuration Guide 3.0](#)

For FTD, there is no plan for replacement. The integration could still be done through the APIs of the 2 platforms.

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.

Table 8. Cisco Cyber Vision 5.0.0 center files

Center	Description
CiscoCyberVision-center-5.0.0.ova	VMware OVA file, for Center setup
CiscoCyberVision-center-with-DPI-5.0.0.ova	VMware OVA file, for Center with DPI setup
CiscoCyberVision-center-5.0.0.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-reports-management-5.0.0.ext	Reports management extension installation file
CiscoCyberVision-sensor-management-5.0.0.ext	Sensor management extension installation file

Table 9. Cisco Cyber Vision 5.0.0 sensor files

Sensor	Description
CiscoCyberVision-IOx-aarch64-5.0.0.tar	Cisco IE3400, Cisco IE3300 10G, Cisco IE9300, Cisco IR1101, Cisco IR1800 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64--5.0.0.tar	Cisco IE3400, Cisco IE3300 10G, Cisco IE9300, Cisco IR1101, Cisco IR1800 Active Discovery sensor installation and update file
CiscoCyberVision-IOx-IC3000-5.0.0.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-IC3000-5.0.0.tar	Cisco IC3000 Active Discovery sensor installation and update file
CiscoCyberVision-IOx-x86-64-5.0.0.tar	Cisco Catalyst 9x00 and Cisco Catalyst IR8340 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-x86-64-5.0.0.tar	Cisco Catalyst 9x00 and Cisco Catalyst IR8340 Active Discovery sensor installation and update file

Table 10. Cisco Cyber Vision 5.0.0 update files

Updates	Description
CiscoCyberVision-Embedded-KDB-5.0.0.dat	KnowledgeDB embedded in Cisco Cyber Vision 5.0.0
CiscoCyberVision-update-center-5.0.0.dat	Center update file for upgrade from release 4.3.x to release 5.0.0 (UI and CLI)

Release Notes for Cisco Cyber Vision Release 5.0.0

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

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

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

The Cisco Cyber Vision Center Plan is 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>

Center Deployment guides:

[Cisco Cyber Vision Center Appliance Installation Guide](#)

[Cisco Cyber Vision Center VM Installation Guide](#)

[Cisco Cyber Vision for Azure Cloud Installation Guide](#)

[Cisco Cyber Vision for the AWS Cloud Installation Guide](#)

Sensor deployment guides:

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

[Cisco Cyber Vision Network Sensor Installation Guide for Cisco IR8340](#)

[Cisco Cyber Vision Network Sensor Installation Guide for Cisco IC3000](#)

[Cisco Cyber Vision Network Sensor Installation Guide for Cisco IR1101](#)

System end-user guides:

[Cisco Cyber Vision GUI User Guide](#)

[Cisco Cyber Vision GUI Administration Guide](#)

[Cisco Cyber Vision GUI Monitor Mode User Guide](#)

[Cisco Cyber Vision Active Discovery Configuration Guide](#)

[Cisco Cyber Vision syslog notification format Configuration Guide](#)

[Cisco Cyber Vision Architecture Guide](#)

[Cisco Cyber Vision Integration Guide, Integrating Cisco Cyber Vision with Cisco Identity Services Engine \(ISE\) via pxGrid](#)

[Cisco Cyber Vision Smart Licensing User Guide](#)

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at <https://www.cisco.com/go/offices>.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)