



Release Notes for Cisco Cyber Vision

Release 4.2.1 - 4.2.2

For users upgrading to 4.2.2 from previous versions, please read the Cisco Cyber Vision 4.2.2 update procedure carefully.

Preamble, 4.2.1 vs 4.2.2	3
Compatible device list	4
Unsupported device list	4
Cisco Cyber Vision 4.2.2 update procedure	5
Upgrade Path	5
Compatibility Guidelines	5
Data purge	5
Center updates	6
Architecture with Global Center	6
Architecture with one Center	9
AWS and Azure Centers	10
Cisco Cyber Vision 4.2.1 important changes	11
Command line access	11
Communication port and protocol changes	11
Port	11
Protocol	11
API	11
SYSLOG	11
Cisco Cyber Vision new features and improvements	12
Certificate renewal	12
Centers	13
Sensors	16
Data ingestion control	21
Components	21
Flows	23
Sensor memory consumption	24
DPI enhancement for potential scan detection	25
Cisco Cyber Vision 4.2.1 Resolved Caveats	26
Cisco Cyber Vision 4.2.2 Resolved Caveats	27

Cisco Cyber Vision Open Caveats	27
Links	28
Software Download	28
Related Documentation	30

Preamble, 4.2.1 vs 4.2.2

An important defect has been discovered in Cisco Cyber Vision 4.2.1 (defect CSCwf75759). This defect affects the performance of the preset data computation. A user may wait several hours before seeing the preset data on the user interface. This defect doesn't affect the rest of the product.

Release 4.2.2 contains a fix for that defect. All customers must upgrade the release 4.2.1 to release 4.2.2.

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	1.4.1	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 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, 9400 Series switches

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 4.2.2 update procedure

Cisco Cyber Vision 4.2.2 update procedure will depend on the architecture deployed and the tool used to deploy it.

Upgrade Path

Upgrade Path to Cisco Cyber Vision 4.2.2

Current Software Release	Upgrade Path to Release 4.1.4
If version prior to 3.2.4	Upgrade first to 3.2.4, then to 4.0.0, then to 4.1.4 and to 4.2.2
Version 3.2.4	Upgrade first to 4.0.0, then to 4.1.4, then to 4.2.2
Version 4.0.0 to 4.0.3	Upgrade first to 4.1.4, then to 4.2.2
Version 4.1.0 to 4.1.4	Upgrade directly to 4.2.2
Version 4.2.0 to 4.2.1	Upgrade directly to 4.2.2

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 in 4.0.0, 4.0.1, 4.0.2 or 4.0.3 will be migrated to the new 4.1.x and 4.2.0 schemas. All components, activities, flows, events, etc. will be migrated.

The new data retention policies introduced in 4.0.0 are still valid in 4.1.x for event and variables:

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

The flow expiration has been adjusted in 4.2.2 to 7 days maximum.

- Flows after 7 days.

Once migrated, the following expiration settings will be applied, and the system will run the purge process.

Center updates

Architecture with Global Center

Preliminary checks: it is highly recommended that you check the health of all Centers connected to the Global Center and of the Global Center itself before proceeding to the update.

To do so, it is recommended to use an SSH connection to the Center and to type the following command:

```
systemctl --failed
```

The number of listed sbs-* units should be 0, otherwise the failure needs to be fixed before the update.

Cisco Cyber Vision system check – 0 failure

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

All sbs services need to be running in a normal state before performing an update. If any is listed as failed it must be fixed prior 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:~#
```

Rebooting of the Center most often solves the issue. If not, please contact the support.

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

1. Update the Global Center:
 - a. Either using the Graphical User Interface:
 - File= CiscoCyberVision-update-combined-4.2.2.dat
 - Navigate to Admin > System, use the System Update button and browse and select the update file.
 - b. Or using the Command Line Interface (CLI):
 - File= CiscoCyberVision-update-center-4.2.2.dat
 - Launch the update with the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-center-4.2.2.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 owns the sensor, and the SSH connection from the Center to the allowed sensor, the hardware sensors (IC3000 and Sentryo SENSOR's) were updated at the same time.
 - ii. If the Cisco IC3000 sensor was deployed using the Sensor management extension, it can be upgraded by deploying it again.
 - iii. If not, the update needs to be done from the Command Line Interface (CLI):
 - File= CiscoCyberVision-update-sensor-4.2.2.dat
 - Launch the update with the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-sensor-4.2.2.dat
```

You can check the sensor version on the Administration / Sensor Explorer page, to make sure that the version is 4.2.2.

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 sensors with the sensor management extension, first upgrade the extension and then update the sensors.
 - File = CiscoCyberVision-sensor-management-4.2.2.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-4.2.2.ext
```
 - ii. Then all sensors need to be updated with the extension, to do so, access the sensor administration page, and use the menu “Manage Cisco devices” / “Update Cisco devices” or use the redeploy button in the sensor’s right side panel. A complete procedure is available in the document (part “Cisco Cyber Vision new features and improvements”) or in all sensor installation guides from version 4.2.0.
 - 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 IR1101 files = CiscoCyberVision-IOx-aarch64-4.2.2.tar or CiscoCyberVision-IOx-Active-Discovery-aarch64--4.2.2.tar
 - Catalyst 9300 and 9400 and IR8340 files = CiscoCyberVision-IOx-x86-64-4.2.2.tar or CiscoCyberVision-IOx-Active-Discovery-x86-64-4.2.2.tar.

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

The sensor update through the Local Manager of a Catalyst 9300, 9400 or IR8340 files is not possible from a release 4.1.2 (or lower) to a release 4.1.3 (or higher) due to the addition of the rspan compatibility. The sensor application needs to be redeployed and the enrollment package uploaded again. Once the update to a release greater than 4.1.2 is done with the redeploy, the standard update procedure could be used for other releases for example 4.2.0 to 4.2.2.

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

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

- Update the Center:
 - Either using 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.
 - Or using 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
```

- Update the sensors:
 - Hardware sensors:
 - i. If you used the combined file to update the Center which owned the sensor and the SSH connection from the Center to the allowed sensor, the hardware sensors (Cisco IC3000 and Sentryo SENSOR's) were updated at the same time.
 - ii. If the Cisco IC3000 sensor was deployed using the sensor management extension, it can be upgraded by deploying it again.
 - iii. If not, the update needs to be done from the Command Line Interface (CLI):
 - File= CiscoCyberVision-update-sensor-<LAST-VERSION>.dat
 - Launch the update with the following command:

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

- IOx sensors:
 - i. If you have installed the sensors with the sensor management extension, first upgrade the extension itself and then all sensors will have to be updated.
 - 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. All sensors need to be updated with the extension. To do so, access the sensor administration page, and use the menu “Manage Cisco devices” / “Update Cisco devices” or use the redeploy button in the sensor’s right side panel. A complete procedure is available in the document (part “Cisco Cyber Vision new features and improvements”) or in all sensor installation guides from version 4.2.0.
- 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 Local Manager platform or from the Command Line Interface. This procedure is described in the corresponding sensors installation guides.
 - IE3x00 and IR1101 files = CiscoCyberVision-IOx-aarch64-4.2.2.tar or CiscoCyberVision-IOx-Active-Discovery-aarch64-4.2.2.tar
 - Catalyst 9300 and 9400 and IR8340 files = CiscoCyberVision-IOx-x86-64-4.2.2.tar or CiscoCyberVision-IOx-Active-Discovery-x86-64-4.2.2.tar.

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

Sensor update through the Local Manager of a Catalyst 9300, 9400 or IR8340 files is not possible from a release 4.1.2 (or lower) to a release 4.1.3 (or higher) due to the addition of the rspan compatibility. The sensor application needs to be deployed again and the enrollment package uploaded again. Once the update to a release greater than 4.1.2 is done with the redeploy, the standard update procedure could be used for other releases for example 4.2.0 to 4.2.2.

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

In case of a Center deployed in AWS or Azure, follow the procedure described in Architecture with one Center hereabove.

Cisco Cyber Vision 4.2.1 important changes

Command line access

In 4.1.0, a major change regarding the Center Command Line Interface (CLI) access through serial console or SSH was made. The user root is no longer usable to establish the connection. A new user called 'cv-admin' must be used. This user has limited rights and many CLI commands will require permission elevation:

- prefix the command with "sudo".
- or open a root shell using "sudo -i" and enter a command.

Communication port and protocol changes

Port

No modification in 4.2.1.

Protocol

No modification in 4.2.1.

API

No modification in 4.2.1.

SYSLOG

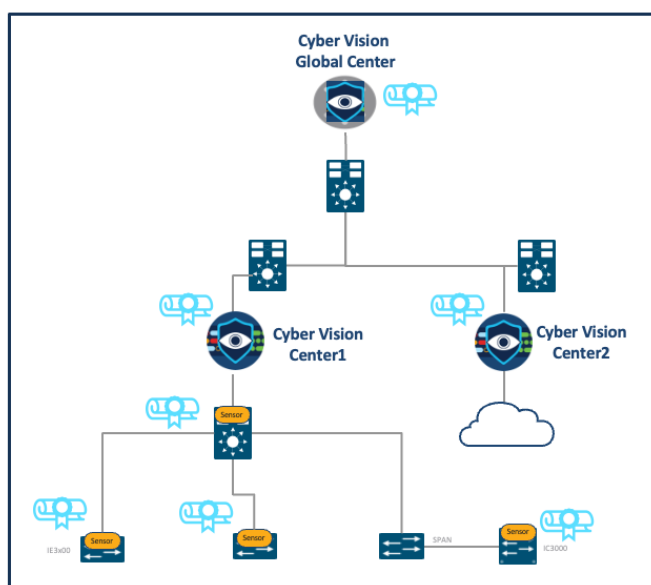
No modification in 4.2.1.

Cisco Cyber Vision new features and improvements

Certificate renewal

A Cisco Cyber Vision system uses several certificates. Each component has its own certificate to manage its secure communications.

Cisco Cyber Vision system certificates



Cyber Vision certificates

- Global center certificate
 - GUI https communication
 - Local center communication
- Center
 - GUI https communication
 - Global center communication
- Sensors
 - Center communication

Each certificate has its own expiration date. Installation date + 2 years.

The certificates generated by Cisco Cyber Vision have a validity of two years. In versions prior to 4.2.1 certificate renewals needed to be done manually from the Command Line (CLI). In version 4.2.1 there are two new features assist the user:

1. An automatic certificate renewal for Centers.
2. Cisco Cyber Vision user interface offers several ways to generate certificates when automatic certificate renewal is not possible.

Centers

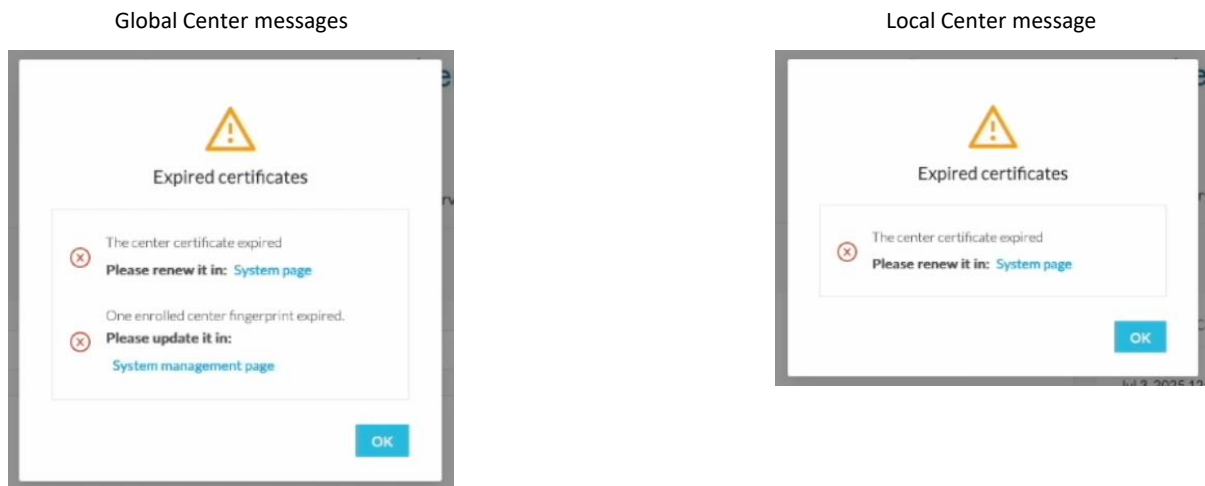
Autorenewal:

In a standard situation, a Center (connected to a Global Center or not, or a Global Center) will renew its certificate automatically. No user action is required.

User warnings

In case of problem during the renewal process, errors will be displayed on the Cisco Cyber Vision User Interface and the user will have some actions to do manually.

Error messages will appear on the Cisco Cyber Vision UI as the user access the system. Links to renew the certificate will also be displayed.



At the same time:

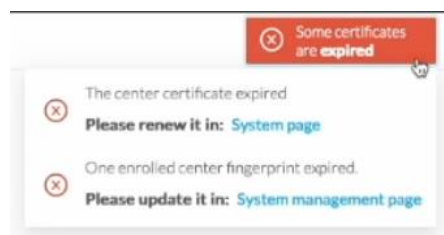
A banner will appear at the top right corner of the UI, to warn the user:

Certificate expiration banner



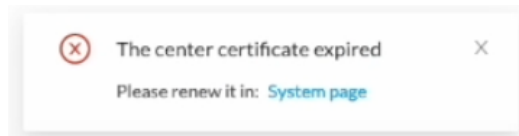
A single click on the banner will give access to further action details:

Certificate expiration banner details



A toast will appear at the bottom left of the UI, to warn the user of a certificate expiration and propose a link to renew it:

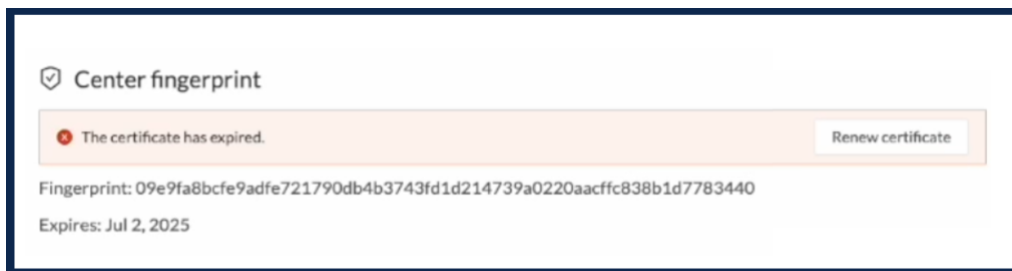
Certificate expiration warning



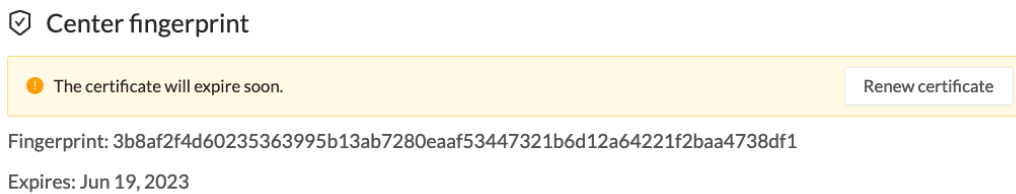
Manual renewal

To manually renew the Center certificate (Center, Center connected to a Global Center or a Global center) navigate in Cisco Cyber Vision > Admin > System. A message will appear for renewal of the certificate:

Center Certificate renewal - expired



Center Certificate renewal – will expire




If the certificate used is not an external certificate, the web page needs to be reloaded to consider the new certificate.

Once done, if the system is made of Centers connected to a Global Center the different fingerprints will have to be updated. Messages will indicate that fingerprints need to be updated, like below:

1. Case of a certificate update on a Center connected to a Global Center:

- a message clearly states what the user needs to do on the connected Center:

 **Enroll to a Global Center**

 Center enrolled but disconnected, due to the update of the certificate of this center. Certificate fingerprint must be updated in the Global Center System Management page.

- On the Global Center a button is available to update the fingerprint.

System management

From this page you can manage centers and sensors.



Center Name	IP	Version	Enrollment status
LC1	10.2.2.184	SBS: 5.0.0+202305032335 KDB: 20230503	

The fingerprint of the Center connected to a Global Center is available in the admin menu, on the system page.

2. Case of a certificate update on a Global Center:




- a message indicates on the Global Center that the Global Center fingerprint is outdated in a particular connector Center:

System management

From this page you can manage centers and sensors.



Fingerprint: fed598fe5c46487429f642b945f7f95ff3074ccbe34ec04c8a4da091e58fbl

	Center Name	IP	Version	Enrollment status	Up time	Connectivity Status
	Local center 206	10.2.2.206	SBS: 5.0.0+202305040948 KDB: 20230504	Outdated global center fingerprint 	1 hr 16 mins 31 secs	

- a message clearly states what the user needs to do on the connected Center:

 **Enroll to a Global Center**

 Center enrolled but disconnected, due to the update of the certificate of the Global Center.



The fingerprint of the Global Center is available in the Cisco Cyber Vision UI > Admin > System.

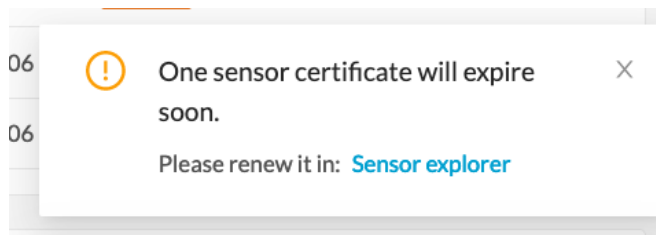
Sensors

For the sensor certificates, the user must renew the certificates from the UI. No auto renewal is available in version 4.2.1.

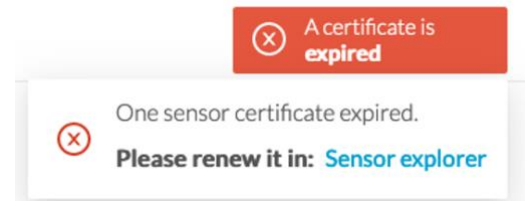
User warnings

The system will warn the user when it's time to renew the sensors' certificates.

The following toast and banners will appear in Cisco Cyber Vision's User Interface:



This banner will display more information as the user click on it:



A warning will be displayed in the Sensor Explorer page:

Sensor Explorer

From this page, you can explore and manage sensors and sensors folders. Sensors can be remotely and securely rebooted, shut down, and erased. When a sensor connects for the first time, you must authorize it so the Center can receive its data.

⚠ 1 sensor certificate will expire soon
[Manage certificates](#) ×

[+ Install sensor](#)
[🔍 Manage Cisco devices](#)
[📁 Organize](#)

Folders and sensors (1)

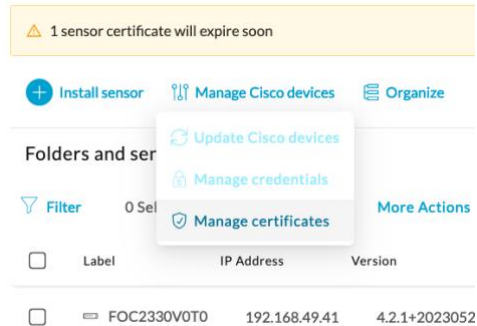
🔍 Filter
0 Selected
Move selection to
[More Actions](#) ▾
As of: Jun 6, 2023 5:24 PM
🔄

<input type="checkbox"/>	Label	IP Address	Version	Location	Health status ▾	Processing status	Ac
<input type="checkbox"/>	FOC2330V0T0	192.168.49.41	4.2.1+202305251420		Connected	Normally processing	

Sensor certificate renewal

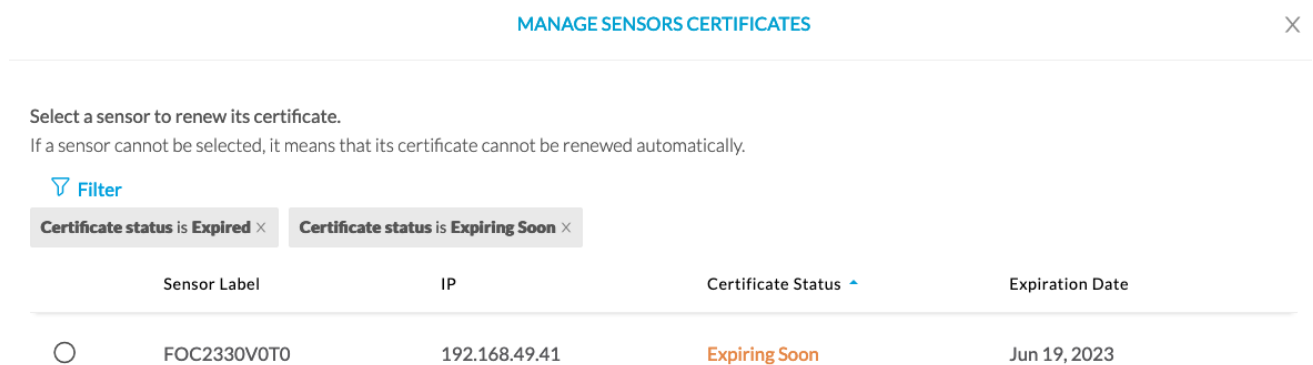
To renew the sensor certificates a menu is now available in the Sensor Explorer page, under the Manage Cisco devices dropdown menu.

Sensor Certificate renewal – Manage certificates.



A new menu is available to check sensor certificates and renew them.

Sensor Certificate renewal – Manage sensor certificates.



Once the sensor is selected in the list, the user must click the Renew Certificate button. The certificate will be renewed and automatically sent to the sensor if the sensor communication is still up.

Sensor Certificate renewal – Renew certificate.

MANAGE SENSORS CERTIFICATES ×

Select a sensor to renew its certificate.
If a sensor cannot be selected, it means that its certificate cannot be renewed automatically.

[Filter](#)

Certificate status is Expired × **Certificate status is Expiring Soon** ×

Sensor Label	IP	Certificate Status	Expiration Date
<input checked="" type="radio"/> FOC2330V0T0	192.168.49.41	Expiring Soon	Jun 19, 2023

The new expiration date will be displayed on the table:

Sensor Certificate renewal – New expiration date.

Sensor Label	IP	Certificate Status	Expiration Date
<input type="radio"/> FOC2330V0T0	192.168.49.41	Valid	Aug 2, 2025

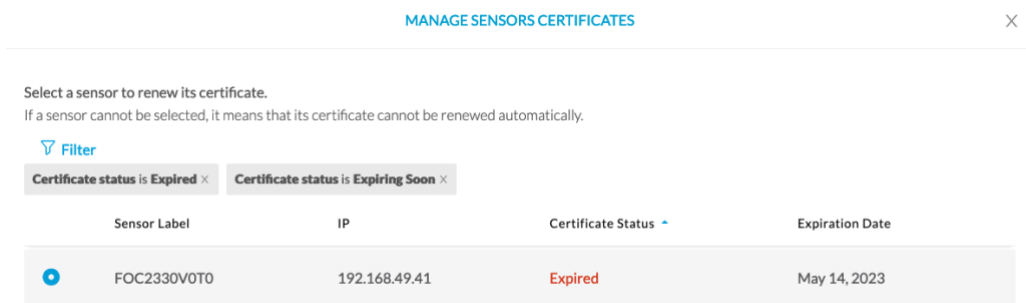
Sensor certificate renewal after expiration

In case of certificate expiration, communication with the sensor is no longer possible if the sensor was deployed manually (without the sensor management extension). In this case, the certificate could still be renewed but it must be sent to the sensor manually. The certificate is part of the enrollment package.

The user just needs to generate a new enrollment package and send it to the sensor application.

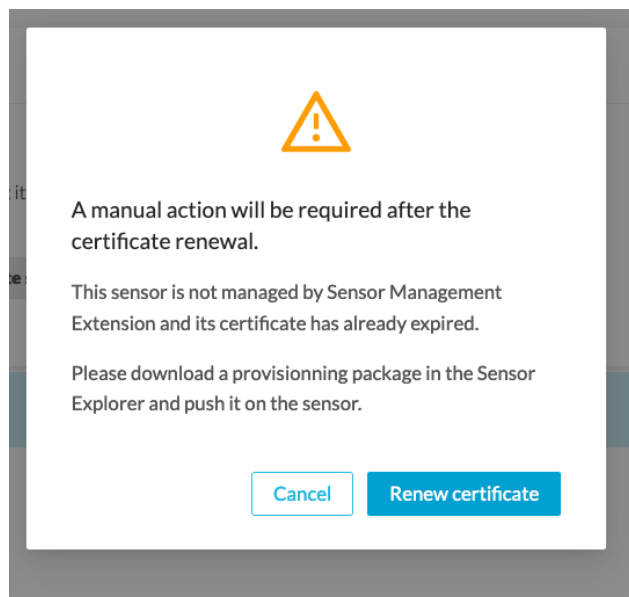
For example:

Sensor Certificate renewal – expired certificate.



The certificate must first be renewed with the process explained above. When the user will click on the Renew Certificate button a specific popup will appear which indicates that the provisioning package must be sent to the sensor:

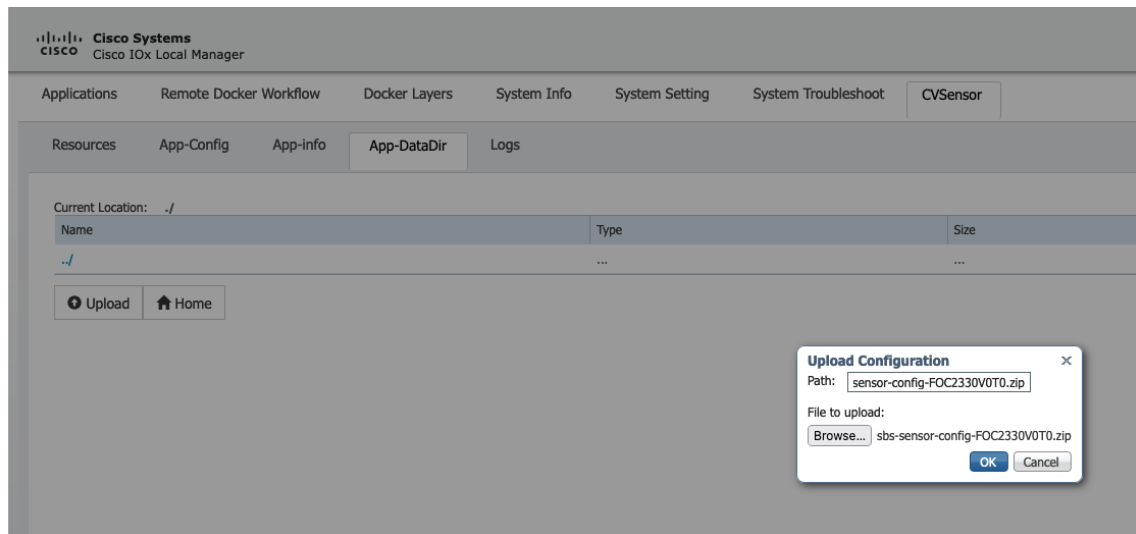
Sensor Certificate renewal – provisioning package manual push requested.



The provisioning package can be sent to the sensor application through the Cisco IOX Local Manager. The different steps are explained in the different sensor installation guides.

Sensor Certificate renewal – provisioning package uploaded in IOX.

Configuration > Services > IOx



Data ingestion control

Cisco Cyber Vision version 4.2.1 contains two new controls in the Center and the Center with Global Center's data ingestion chain.

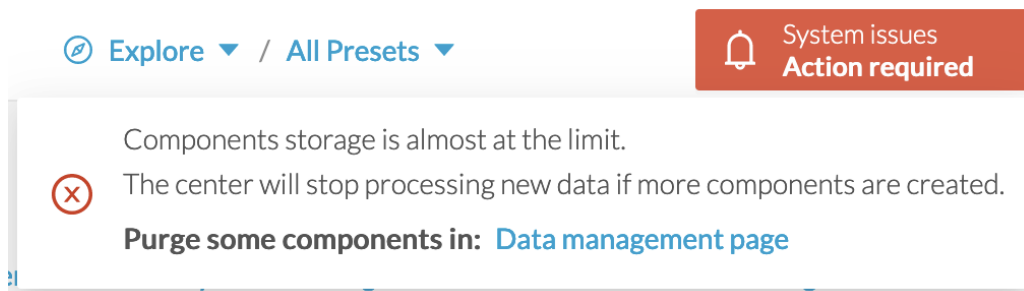
1. A limit has been added to the system to control the number of components in the database.
2. New default settings have been added for flow ingestion:
 - a. By default, flow storage is disabled in new Centers.
 - b. If flow storage is enabled, flows will be purged after 7 days of inactivity.

Components

In Cisco Cyber Vision, a component represents an object of the industrial network from a network point of view. It can be the network interface of a PLC, a PC, a SCADA station, etc., or a broadcast or multicast address. To protect the system the number of components stored in the database is now limited.

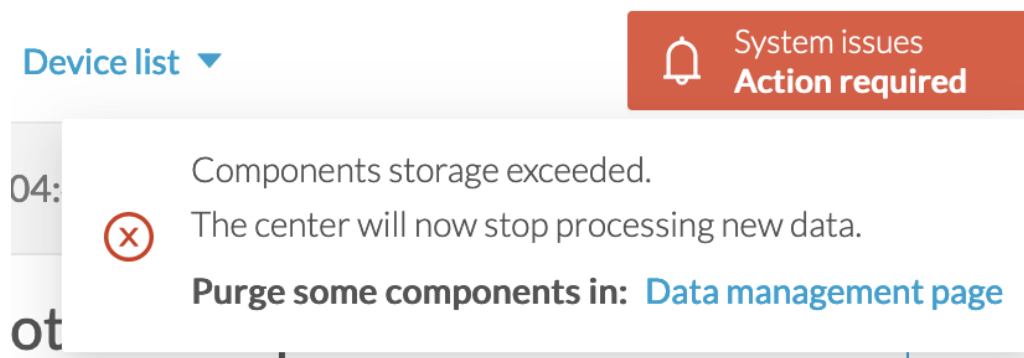
When the system contains more than 120 000 components a warning is displayed to inform the user that a purge must be performed. A new purge menu is now available in the Admin page to purge components based on several criteria.

Component limit – storage is almost at the limit.



If the system reaches 150 000 components the ingestion will stop. Incoming sensor data will not be treated nor stored and be directly deleted. A warning will be displayed on the user interface to inform the user.

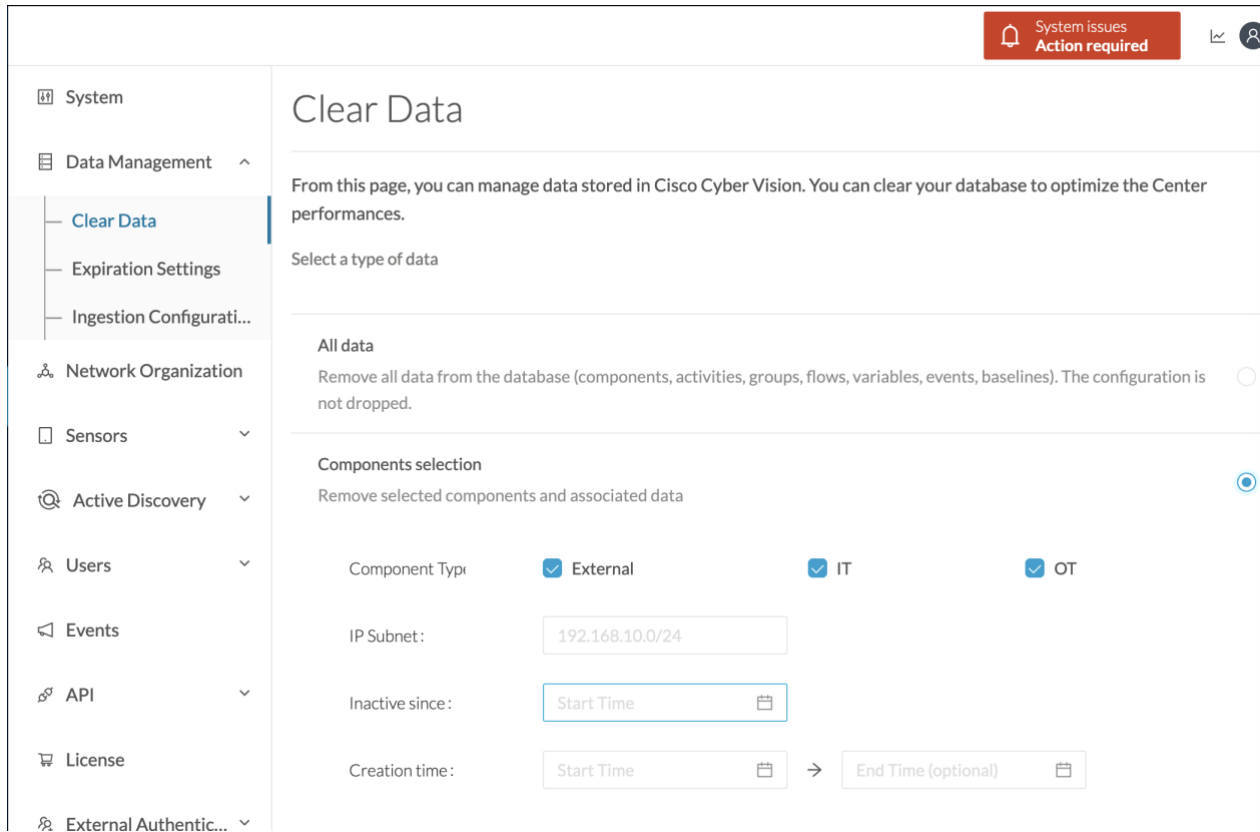
Component limit – storage exceeded.



Cisco Cyber Vision version 4.2.1 allows the user to select which components can be deleted in the data purge menu based on:

- the component type (External, IT or OT),
- their IP subnet,
- their inactivity,
- their creation time.

Component limit – component purge



Flows

Cisco Cyber Vision version 4.2.1 brings several changes regarding flow storage:

- Flow storage is disabled by default.
- Flow purge expiration period is now set to 7 days.

Flow storage will be disabled in recently deployed Centers. Default settings will be:

Flow storage - default configuration

Ingestion Configuration

From this page you can customize traffic ingestion.

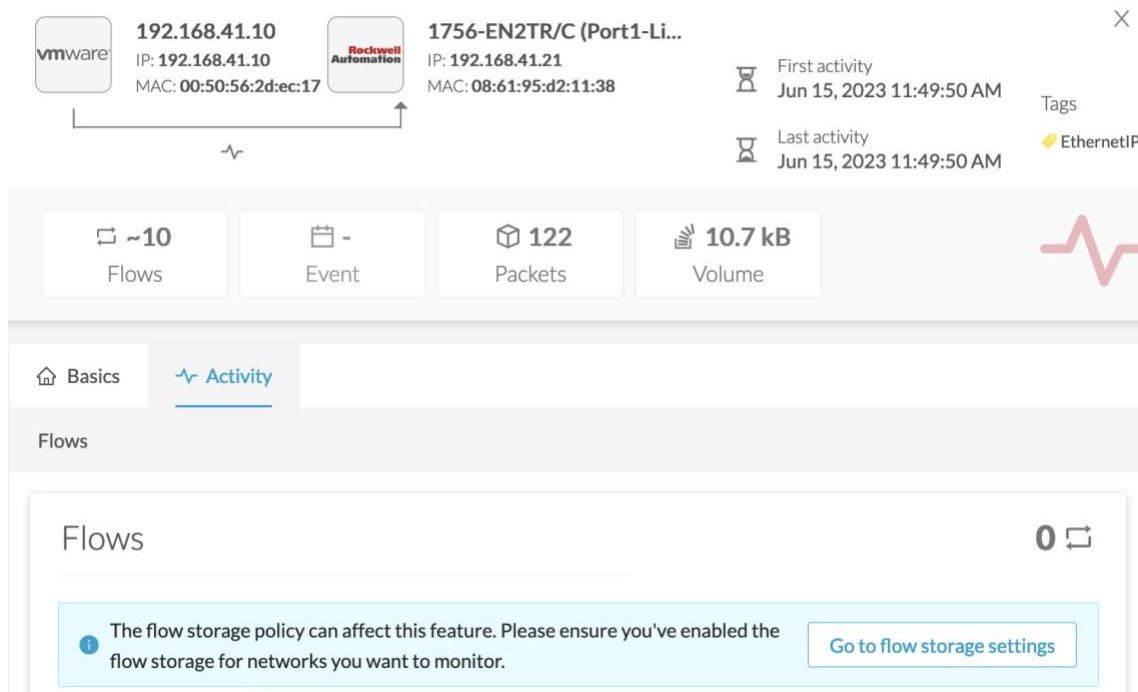
Flows Configuration

Flows Storage

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

In the User Interface several messages were added to indicate to the user that features may be limited due to absence of flows in the database. For example, in the activity technical sheet, a warning is now visible at the top of the flows table to explain why the table is empty.

Flow storage – user interface warning



If flow storage is enabled, an automatic purge will occur on flows when a period of inactivity exceeds 7 days. Version 4.2.0 allowed the user to set the inactivity period. Version 4.2.1 has now a fixed period of inactivity to prevent any performance issue.

Sensor memory consumption

Several issues were reported regarding sensor application reboots due to over memory consumption. Many customer issues were addressed protocol per protocol over time. To be more resilient and avoid sensor issues, sensors' memory consumption is limited to their available memory in version 4.2.1. Ways to limit all non-fixed RAM buffers based on the available memory were added.

DPI is a resource-intensive activity which may use a lot of CPUs and RAM. Usage depends on the number of packets received per second, protocol complexity, request/response matching and quality of captured traffic. Traffic with lost packets or segments will require effort to reconstitute a complete exchange (reassembly, defragmentation).

CPU usage will be highly linked to:

- The amount of traffic (packets per second).
- The complexity of the DPI:
 - i. In-depth protocol analysis.
 - ii. Number of extracted properties.

RAM usage is more complex:

- Some fixed-sized buffers are used, for example per interface to receive packets. These are allocated at startup and will result in high memory usage even without traffic (e.g. immediately after sensor startup).
- Some common dynamic buffers are used for all packets:
 - i. TCP reassembly
 - ii. IP defragmentation
- Some other dynamic buffers are used by protocol:
 - i. Management of requests and responses to understand the whole context.
 - ii. Caching flows to produce more meaningful information.
 - iii. Application reassembly.
 - iv. Extraction of OT variables from flows before sending them to the Center.

All non-fixed RAM buffers are managed dynamically to analyze a maximum of flows. Some controls are implemented to avoid any overconsumption and balance the resource needs of all these functions. This part was drastically improved in version 4.2.1.

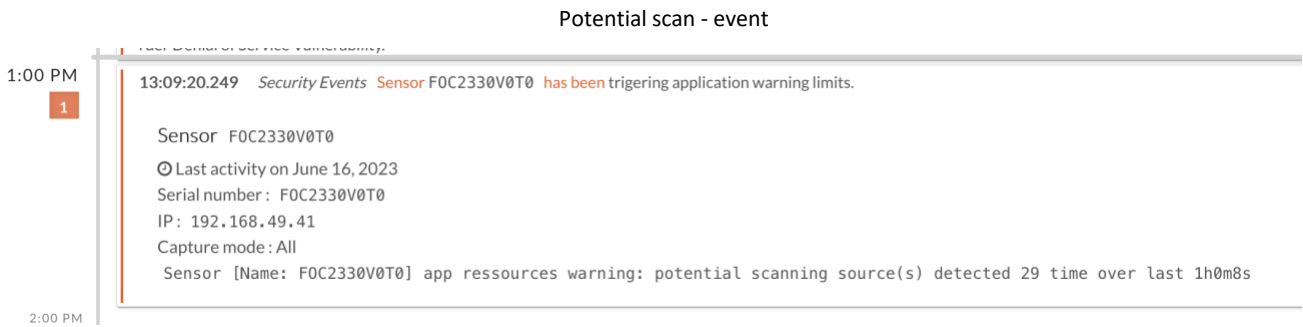
Important remarks linked to the usage of Snort in the sensor:

- Snort will use RAM and CPU for the same reasons.
- It will increase consumption when it's launched on the sensor.

DPI enhancement for potential scan detection

Cisco Cyber Vision’s philosophy is to detect as many components as possible. However, in case of network scanning (whether it is legitimate or illegitimate), extremely important numbers of components will be created due to the many requests and responses generated, which is a threat for the Center reliability. Version 4.2.1 includes significant changes in Deep packet inspection (DPI) process when encountering this situation which goals are to keep the Center safe, and users alerted:

- As soon as the sensor detects a scan of the network, it will stop sending flows to the Center which will block components creation.
- The sensor will alert the Center that a scan has been detected and a “potential scanning source(s) detected” security event will be generated on the Event page to alert the user:



Cisco Cyber Vision 4.2.1 Resolved Caveats

CDETS	Description
CSCwa59246	Risk Score are missing from Device list export (csv)
CSCwe57538	Change sensor memory consumption
CSCwe47641	Active Discovery 4.2.0 UI - Add Sensor name
CSCwe47639	Active Discovery 4.2.0 UI - Mix of local and UTC time in the same screen.
CSCwe47637	Active Discovery 4.2.0 - WMI properties are not used as standardised properties.
CSCwe52757	sbs-authd-enroll error when Ansible deploys more than 3 sensors
CSCwe63444	Typos and language errors on the GUI
CSCwe63438	Bizarre mDNS names - stop using for component name
CSCwe68289	Add a way to delete a certain category of event on a certain day
CSCwe69071	Security Insight - Filtering Components table doesn't work
CSCwe80495	Stats mismatch between the Activity on the list and on the sidebar
-	OOM when sensor app is running with 1GB (12477)
CSCwe88635	Packets with SGT tag (trustsec) fail the DPI engine for all protocols
CSCwe88634	Activities can be "first_seen" after "last_seen"
CSCwf01100	CV to ISE Group name Issue
CSCwf00620	AWS - Proposed a complete setup center if metadata are not available
CSCwe30142	There is no "Controller" tag for the FANUC component
CSCwe52758	Link between GICS-PC1 is not there.
	MMS Variable cannot be fully disabled at DPI level, handling of bitfield split is missing (12152)
CSCwe68290	Improve delete component command to delete component without any remaining activity
CSCwe87311	enip-configcomment is not a model-name
CSCwe16235	Siemens S7plus get 3 Digits firmware version
CSCwe99465	sbs-aspic is using 100% cpu despite all ad profiles being paused/not scheduled
CSCwf21131	CCV data exports via "Export to CSV" and/or "Reports" do not include a "VLAN ID" column -
CSCwf23069	Allow duplicate sensor IPs (with warning)
CSCwf24509	Avoid to create too many components in 4.2.x
CSCwf30143	decode failure with ethertype 0x8033
CSCwf31543	Redis database can be corrupted
CSCwf31542	cli access on center impossible because passwd.lock and shadow.lock files are still present at boot
	Remove VXLAN encapsulation of traffic for SDA Fabric deployment (7130)
CSCwe63448	erspan2: be robust when L2 is missing after un-encapsulation
CSCwf01887	S7+ protocol: the property of the flow is not correct
CSCwf34356	CV Onprem - Limit component number

Cisco Cyber Vision 4.2.2 Resolved Caveats

CDETS	Description
CSCwe57536	Device technical sheet - Components table - filtering by tag doesn't work from scratch
CSCwe63437	Lack of consistency on GUI for time range – month mo or mth
CSCwe96157	Global score of some presets are not computed
CSCwe57346	Snort - sync to sensor feedback
CSCwf01888	AWS Instance - Setup failed if IMDSv2 is forced
CSCwf30142	Using in sensor name can mess up the output of sbs-sensor list
CSCwf31541	Device name can be edited in a GC with double click
CSCwf31540	GC preset selection of centers and sensors inconsistent
CSCwf35784	performance issue with S7Plus variables
CSCwf53173	Certificate renewal issue when updating LC/GC with almost expired certificates
CSCwf53172	panic in flow runner with mqtt traffic
CSCwf60530	Activity filter popup not anchored
CSCwf72281	Certificate fingerprint displayed in admin page it wrong if web certificate has been updated
CSCwf75759	Mat views Computation issue in 4.2.1

Cisco Cyber Vision Open Caveats

Issues ID / CDETS	Component	Description
CSCwb12630	Center + ISE	All components are not synchronized with ISE
CSCwd39017	Center	Missing information in the Smart License Usage
CSCwe16323	IC3000	USB enrolment is not working

Links

Software Download

The files below can be found at the following link:

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

Center	Description
CiscoCyberVision-center-4.2.2.ova	VMware OVA file, for Center setup
CiscoCyberVision-center-with-DPI-4.2.2.ova	VMware OVA file, for Center with DPI setup
CiscoCyberVision-center-4.2.2.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-sensor-management-4.2.2.ext	Sensor management extension installation file
Sensor	Description
CiscoCyberVision-IOx-aarch64-4.2.2.tar	Cisco IE3400, Cisco IE3300 10G, Cisco IE9300, Cisco IR1101 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64--4.2.2.tar	Cisco IE3400, Cisco IE3300 10G, Cisco IE9300 Cisco IR1101 Active Discovery sensor installation and update file
CiscoCyberVision-IOx-IC3K-4.2.2.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.2.2.tar	Cisco Catalyst 9x00 and Cisco Catalyst IR8340 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.2.2.tar	Cisco Catalyst 9x00 and Cisco Catalyst IR8340 Active Discovery sensor installation and update file
Updates	Description
CiscoCyberVision-Embedded-KDB-4.2.2.dat	KnowledgeDB embedded in Cisco Cyber Vision 4.2.2
CiscoCyberVision-update-center-4.2.2.dat	Center update file for upgrade from release 4.0.x or 4.1.x to release 4.2.2
CiscoCyberVision-update-sensor-4.2.2.dat	Cisco IC3000 Sensor and Sentryo Sensor3, 5, 7 update file for upgrade from release 4.0.x or 4.1.x to release 4.2.2
CiscoCyberVision-update-combined-4.2.2.dat	Center, IC3000 Sensor and Legacy Sensor update file from GUI for upgrade from release 4.0.x or 4.1.x to release 4.2.2

Cisco Cyber Vision Center 4.2.2 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 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](#)