Release Notes for Cisco Cyber Vision Release 4.3.1

Warning:

For users upgrading to 4.3.1 from versions < 4.3.0:

- **First update the center to 4.3.0 and then to 4.3.1. Read the 4.3.0 Release notes carefully.**
- **For** IC3000 users, please read IC3000 considerations

SUMMARY

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
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

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 IR830(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: 17.6.6a, 17.9.5 and 17.12.2.

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 4.3.1 update procedure

Cisco Cyber Vision 4.3.1 update procedure depends on the architecture deployed and the tool used to deploy it.

Warnings

First upgrade to 4.3.0 before upgrading to 4.3.1.

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

1. IC3000 application change
2. External communications

For IC3000 application change: click here.

For external communications: Please review the 4.3.0 release notes.

Upgrade Path

Upgrade Path to Cisco Cyber Vision 4.3.1

Current Software Release	Upgrade Path to Release 4.3.1
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 *
Version 4.3.0	Upgrade directly to 4.3.1 *

* To limit the number of upgrades, if center and sensors are upgraded simultaneously, sensors could be directly updated to 4.3.1. Only the center must be updated first to 4.3.0.

Compatibility Guidelines

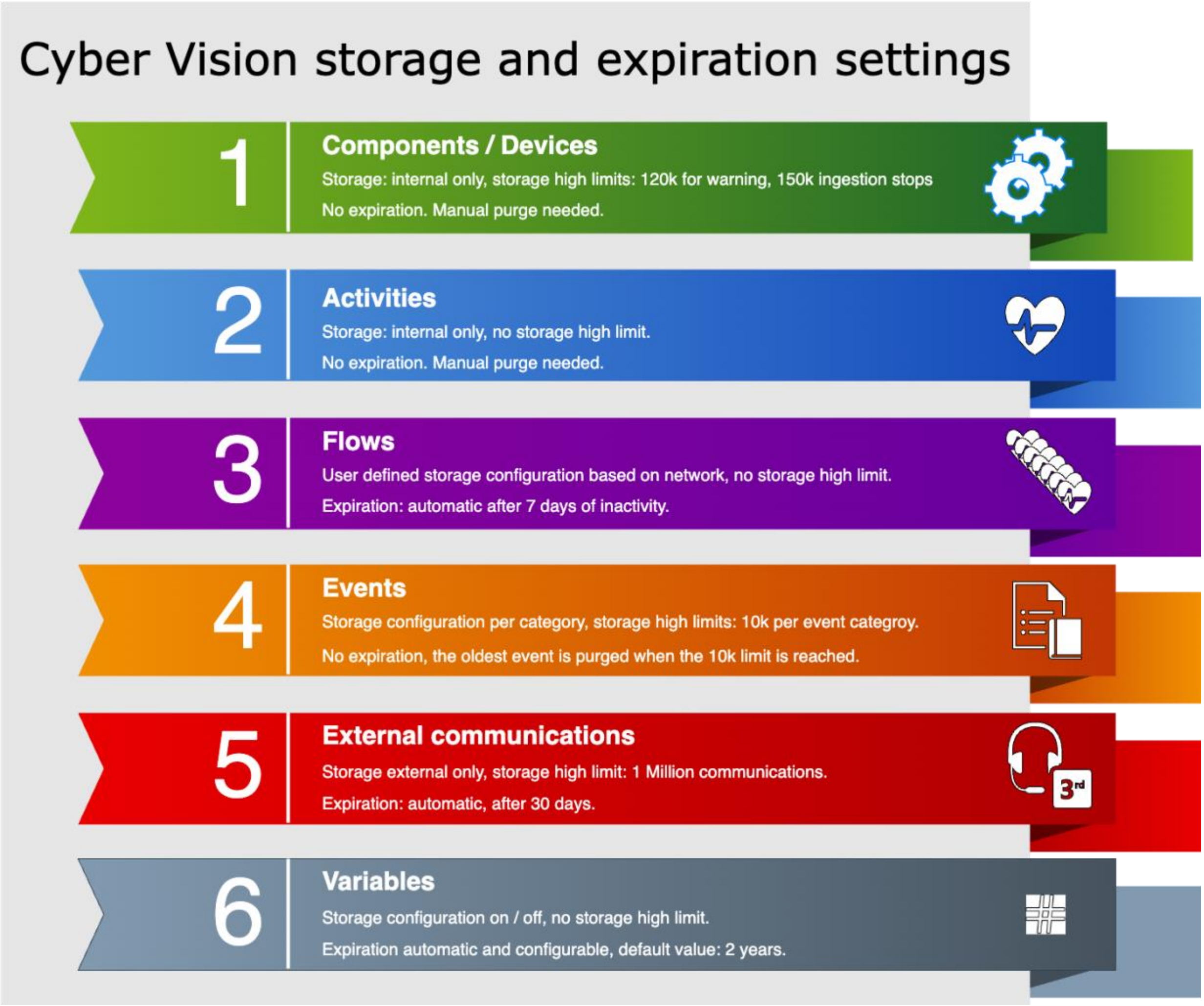
There is downward compatibility of one version between the Global Center and the Center with synchronization and sensors.

- 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 4.3.1.



Cyber Vision storage and expiration settings

1 **Components / Devices**
Storage: internal only, storage high limits: 120k for warning, 150k ingestion stops
No expiration. Manual purge needed.

2 **Activities**
Storage: internal only, no storage high limit.
No expiration. Manual purge needed.

3 **Flows**
User defined storage configuration based on network, no storage high limit.
Expiration: automatic after 7 days of inactivity.

4 **Events**
Storage configuration per category, storage high limits: 10k per event categroy.
No expiration, the oldest event is purged when the 10k limit is reached.

5 **External communications**
Storage external only, storage high limit: 1 Million communications.
Expiration: automatic, after 30 days.

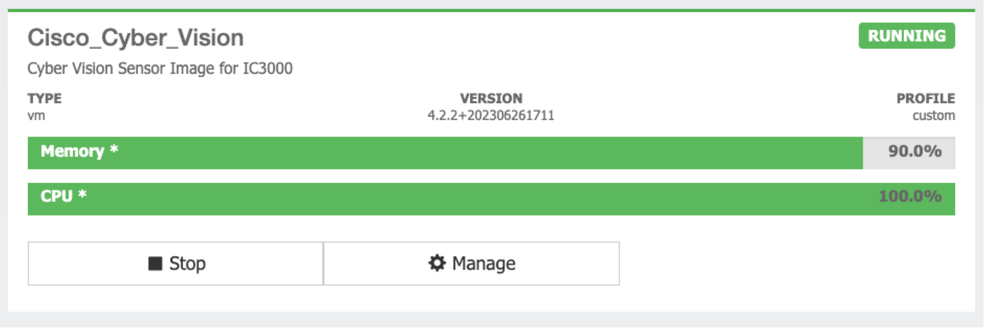
6 **Variables**
Storage configuration on / off, no storage high limit.
Expiration automatic and configurable, default value: 2 years.

IC3000 considerations

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



Cisco_Cyber_Vision

Cyber Vision Sensor Image for IC3000

TYPE: vm

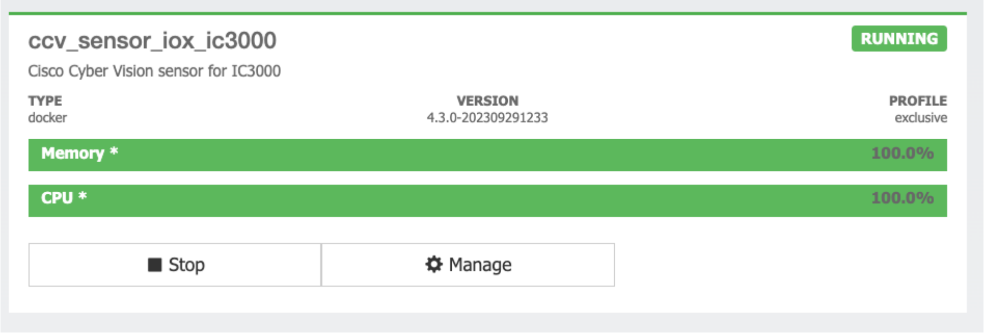
VERSION: 4.2.2+202306261711

PROFILE: custom

Memory *: 90.0%

CPU *: 100.0%

IC3000 Cyber Vision application **after** 4.3.0:



ccv_sensor_iox_ic3000

Cisco Cyber Vision sensor for IC3000

TYPE: docker

VERSION: 4.3.0-202309291233

PROFILE: exclusive

Memory *: 100.0%

CPU *: 100.0%

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:

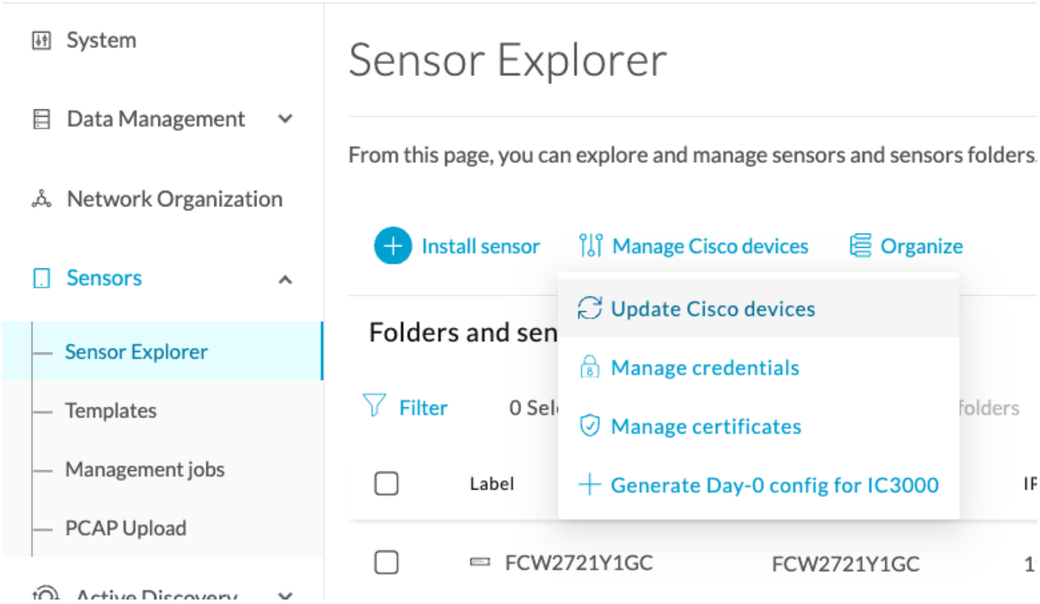
The ssh access to the sensor application is no longer possible. The IC3000 local manager provides a console connection to the application.

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

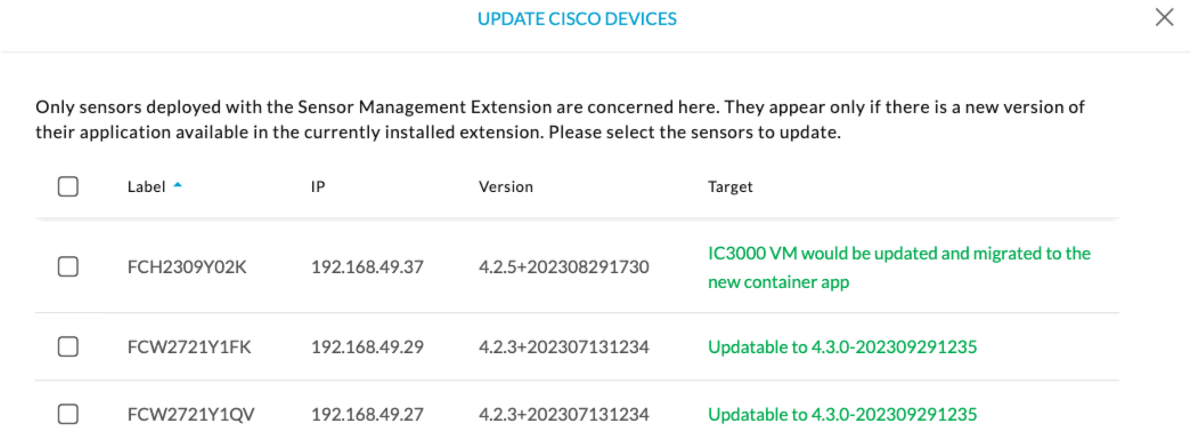
Follow the standard process to use the **Update Cisco devices** functionality. Click **Admin > Sensors > Sensor Explorer > Manage Cisco devices > Update Cisco devices**).

Cyber Vision Update Cisco Devices



The system lists the upgradable sensors.

Cyber Vision Update Cisco Device list

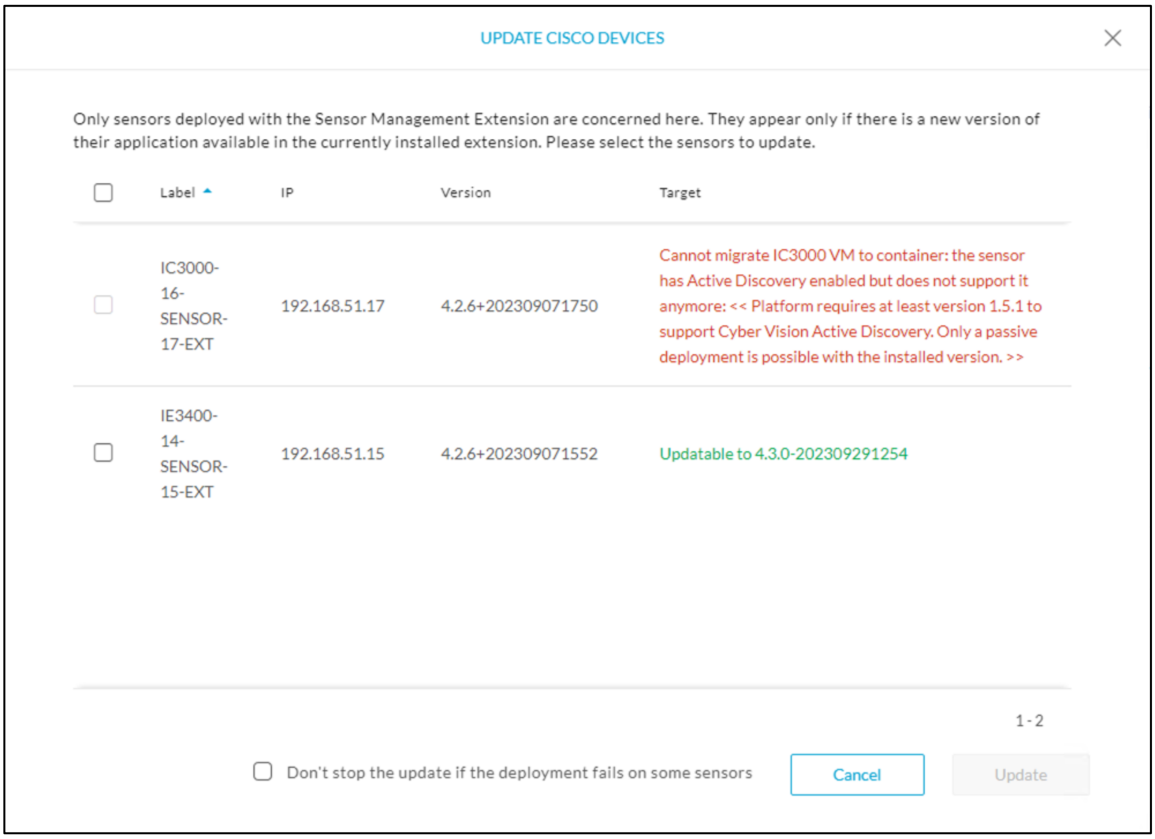


Only sensors deployed with the Sensor Management Extension are concerned here. They appear only if there is a new version of their application available in the currently installed extension. Please select the sensors to update.

□	Label ▲	IP	Version	Target
□	FCH2309Y02K	192.168.49.37	4.2.5+202308291730	IC3000 VM would be updated and migrated to the new container app
□	FCW2721Y1FK	192.168.49.29	4.2.3+202307131234	Updatable to 4.3.0-202309291235
□	FCW2721Y1QV	192.168.49.27	4.2.3+202307131234	Updatable to 4.3.0-202309291235

IMPORTANT: 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.

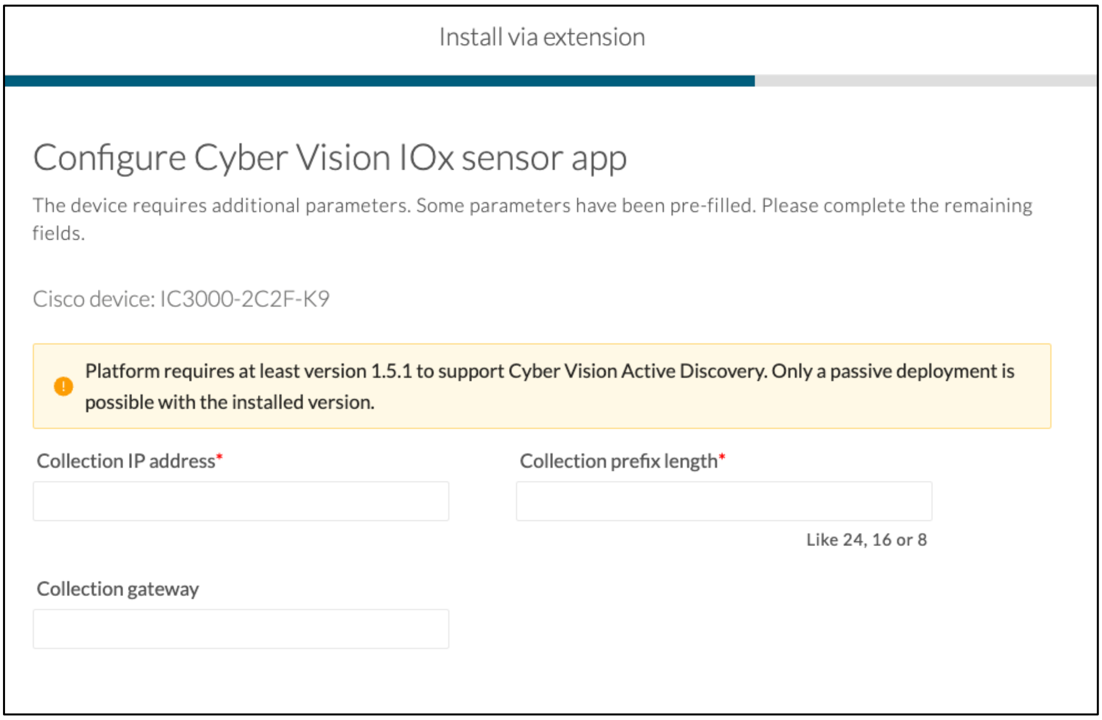
□	Label	IP	Version	Target
□	IC3000-16-SENSOR-17-EXT	192.168.51.17	4.2.6+202309071750	Cannot migrate IC3000 VM to container: the sensor has Active Discovery enabled but does not support it anymore: << Platform requires at least version 1.5.1 to support Cyber Vision Active Discovery. Only a passive deployment is possible with the installed version. >>
□	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 IC3000 sensor application installed with the extension will be some limited to passive only 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*

Like 24, 16 or 8

Collection gateway

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

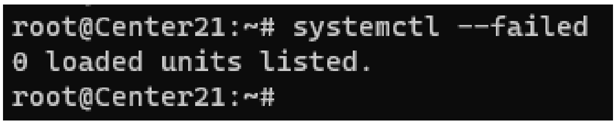
Preliminary checks

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.

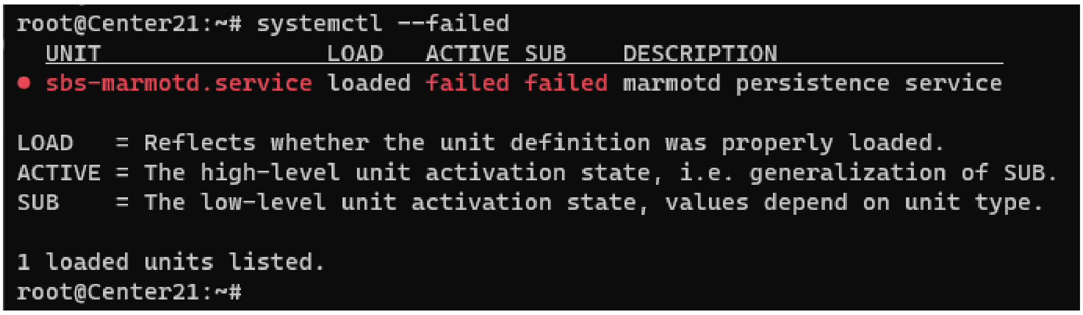
Cisco Cyber Vision system check – 0 failure



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

3. 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.

Architecture with Global Center

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:

```
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 /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.

  - 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: 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
      - Click **Admin > System > System update** button 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
- Click **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 /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 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: 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 4.3.1 Important changes

Communication port and protocol changes

Port

No modification in 4.3.1.

Protocol

No modification in 4.3.1.

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,
```

- vulnerabilitiy 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, t**hese 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 4.3.1.

Cisco Cyber Vision 4.3.1 Enhancements

CDETS	Description
-	Collecting report extension logs for diagnostics
CSCwi28690	External communications list, add in the UI the ones without direction
CSCwe16266	HAProxy - increase the number of concurrent connections
-	Extend our OUI database for mac matching
CSCwi35078	Add an option to store Broadcast and multicast flows
-	Disable enip 0x6b variables processing by default
-	Monitor mode - 'new component' and 'new activity' advanced settings always checked
-	sbs-diag: add counts for some tables

Cisco Cyber Vision 4.3.1 Resolved Caveats

CDETS	Description
	Improve snort errors
	Sensor management extension: can't install on slow machines
CSCwi26036	UI Issue - Sensor certificate expiration date sorting is not working well.
CSCwi26035	Mode Monitor - Bulk Ack differences for filtered list is not working
	Snort sync, warning on sensor pcap
CSCwi27447	Text overlapping in sensor wizard
	s7 program download in wrong direction
CSCwi32082	4.3.0 - Extension issues when center is not stopped properly
CSCwi35076	Azure - change network limits.
CSCwi37749	Limit burrow maximum memory usage
CSCwi37748	Optimize device api route to improve performance
CSCwi36607	Sensor-inputd reliability issue causes message accumulation
CSCwi39458	Journal folder is sometimes missing
CSCwi46934	Vlan missing with some specific span configuration
CSCwi52532	Extension install/update should be shown completed only after it has fully started
CSCwi28691	Monitor mode: Number of components not the same depending on the advanced settings
CSCwi29604	Disable Flow exceptions generated by burrow's analyzers
	TLS communications server side not set on handshakes
	setup-center: NTP error about DNS

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
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

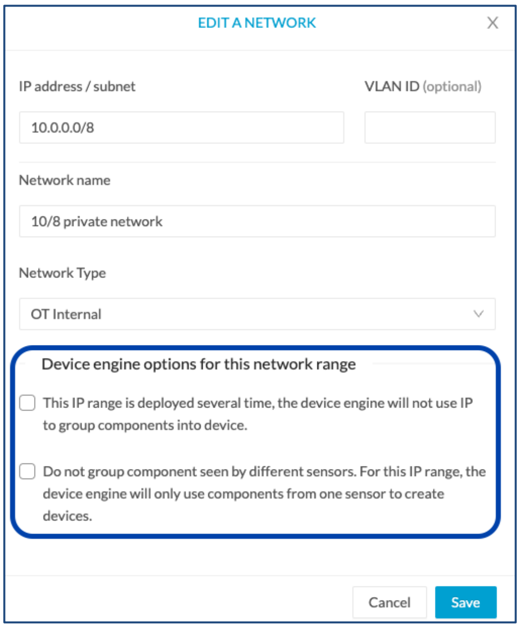
CSCwi33572 / CSCwi33574 / CSCwi33574: Edit Network settings - Device engine options.

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 times, 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 components 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.



IP address / subnet: 10.0.0.0/8

VLAN ID (optional):

Network name: 10/8 private network

Network Type: OT Internal

Device engine options for this network range

□ This IP range is deployed several time, the device engine will not use IP to group components into device.

□ 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.

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-4.3.1.ova	VMware OVA file, for Center setup
CiscoCyberVision-center-with-DPI-4.3.1.ova	VMware OVA file, for Center with DPI setup
CiscoCyberVision-center-4.3.1.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-reports-management-4.3.1.ext	Reports management extension installation file
CiscoCyberVision-sensor-management-4.3.1.ext	Sensor management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-4.3.1.tar	Cisco IE3400, Cisco IE3300 10G, Cisco IE9300, Cisco IR1101 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64--4.3.1.tar	Cisco IE3400, Cisco IE3300 10G, Cisco IE9300 Cisco IR1101 Active Discovery sensor installation and update file
CiscoCyberVision-IOx-IC3000-4.3.1.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-IC3000-4.3.1.tar	Cisco IC3000 Active Discovery sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.3.1.tar	Cisco Catalyst 9x00 and Cisco Catalyst IR8340 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.3.1.tar	Cisco Catalyst 9x00 and Cisco Catalyst IR8340 Active Discovery sensor installation and update file
Updates	**Description**
CiscoCyberVision-Embedded-KDB-4.3.1.dat	KnowledgeDB embedded in Cisco Cyber Vision 4.3.1
CiscoCyberVision-update-center-4.3.1.dat	Center update file for upgrade from release 4.3.0 to release 4.3.1 (UI and CLI)

Cisco Cyber Vision Center 4.3.1 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

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 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

- 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