Release Notes for Cisco Cyber Vision Release 4.2.6

For users upgrading to 4.2.6 from previous versions, please read the Cisco Cyber Vision 4.2.6 update procedure carefully.

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 IE3300 *	17.11.x	Cyber Vision Sensor IOx application hosted in Cisco Catalyst IE3300 Industrial Ethernet switches
Cisco Catalyst IE9300	17.12.x	Cyber Vision Sensor IOx application hosted in Cisco Catalyst IE9300 Rugged Series switches (IOS 17.12 mini)
Cisco IR1101	17.3.x	Cyber Vision Sensor IOx application hosted in Cisco IR1101 Series Industrial Integrated Services Routers
Cisco Catalyst IR8300	17.9.x	Cyber Vision Sensor IOx application hosted in Cisco Catalyst IR8300 Rugged Series Routers
Cisco Catalyst 9300, 9400	17.3.x	Cyber Vision Sensor IOx application hosted in Catalyst 9300, 9300X, 9400 Series switches

* IE3300 support Cyber Vision application hosting when the platform has 4GB DRAM.
All 4G units start with Version ID (VID) from -06. A CLI command could be used to identify whether its 2G vs 4G, looking at the Max DRAM size of `show platform resources`.

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 4.2.6 update procedure

Cisco Cyber Vision 4.2.6 update procedure will depend on the architecture deployed and the tool used to deploy it.

Upgrade Path

Upgrade Path to Cisco Cyber Vision 4.2.6

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 4.2.6
Version 3.2.4	Upgrade first to 4.0.0, then to 4.1.4, then to 4.2.6
Version 4.0.0 to 4.0.3	Upgrade first to 4.1.4, then to 4.2.6
Version 4.1.0 to 4.1.4	Upgrade directly to 4.2.6
Version 4.2.0 to 4.2.4	Upgrade directly to 4.2.6

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 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 above expiration settings will be applied, and the system will run the purge process.

Since 4.2.4, event retention is limited per event categories.

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--<LAST-VERSION>.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--<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. 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--<LAST-VERSION>.dat
            - Launch the update with the following command:

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

You can check the sensor version on the Administration / Sensor Explorer page

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--<LAST-VERSION>.ext
- Navigate to Admin > Extensions. In the Actions column, use the update button and browse to select the update file.
- The Cisco Cyber Vision sensor management extension can also be updated from the CLI with the command:

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

ii. Then 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--<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.

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 4.2.4.

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--<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.

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 4.2.4.

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 4.2.6 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 4.2.6.

Protocol

No modification in 4.2.6.

API

No modification in 4.2.6.

SYSLOG

No modification in 4.2.6.

Cisco Cyber Vision new features and improvements

Sensor stats API

A new API route is available to get sensor statistics data. This route is documented in the application swagger.

Route : /api/3.0/sensors/sensor ID/stats
This route has 2 parameters:

- the sensor id
- the time period to collect (2h to 360d)

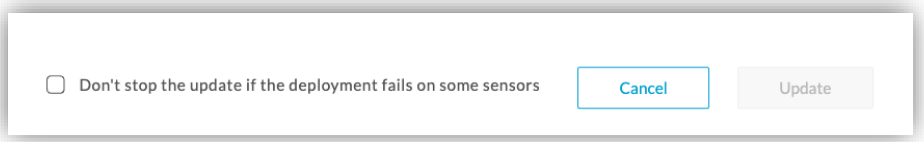
The answer model is available in the swagger and will have the following form:

Support C9300X

Cyber Vision Sensor IOx application could be hosted in Catalyst 9300 Series switches including the new Catalyst 9300X models.

Sensor update, all at a time

A new check box is available in the Cyber Vision sensor update overlay:



When the system has to update several sensors with the sensor management extension, it will build some batches of 10 sensors maximum. By default, if one sensor update fails during a batch all the other batches not already executed will be cancelled.
This new check box permits to the system to execute all batches, even if some failures are observed.

Cisco Cyber Vision 4.2.6 Resolved Caveats

CDETS	Description
CSCwe16199	Fix snort segfault
CSCwf53174	Center name on Global center may be too long
CSCwf54948	rabbitmq-center.pass is no more saved on /data/tmp/
CSCwf73636	Invalid swagger documentation with ExtraFields
CSCwf84618	Remove docker layers and sensor update
CSCwf84617	Management jobs - Date time of canceled jobs is moving
CSCwf81232	Certificate error in log with center-dpi
CSCwf84621	API routes `devices` parameters `from` and `to` are not working
CSCwf87301	Journal size is not limited
	Support C9300X - 13293
CSCwh00328	Vulnerability evaluation is not done after a KDB update on a LC
CSCwh01748	Clean sensor log files when they have more than 6 Months
CSCwh01746	sbs-diag change du-largest-files
CSCwh01745	Sensor management extension - All versions of the different sensor app packages are kept
CSCwh01744	Sensor update with extension: add an option "no matter what"
CSCwh08960	Sensor deployed with extension are sending dhcp requests
CSCwh16526	Panic in flow with mqtt traffic
CSCwh37565	Diagnostic file: Add CPU details of the setup in the diag
CSCwh01749	Highlight more the Click here to fill... message during sensor redeploy
	Improve Log rotation - 13376
CSCwh05538	Custom snort rules are not checked and can cause sensor to reboot in a loop
CSCwh14986	Role Management: character return error when modifying if mapped to an AD group
CSCwh20628	Certificate error in log for sensors in GC
CSCwh22022	Port scan tags are not sent to the GC
	Expose sensor statistics data through the API.
CSCwh26117	Pcap upload fails silently because it generates a message too big
	sbs-diag: add expiration logs

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

Remarks:

- VMWare OVA file 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.
- 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-4.2.6.ova	VMware OVA file, for Center setup
CiscoCyberVision-center-with-DPI-4.2.6.ova	VMware OVA file, for Center with DPI setup
CiscoCyberVision-center-4.2.6.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-sensor-management-4.2.6.ext	Sensor management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-4.2.6.tar	Cisco IE3400, Cisco IE3300 10G, Cisco IE9300, Cisco IR1101 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64--4.2.6.tar	Cisco IE3400, Cisco IE3300 10G, Cisco IE9300 Cisco IR1101 Active Discovery sensor installation and update file
CiscoCyberVision-IOx-IC3K-4.2.6.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.2.6.tar	Cisco Catalyst 9x00 and Cisco Catalyst IR8340 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.2.6.tar	Cisco Catalyst 9x00 and Cisco Catalyst IR8340 Active Discovery sensor installation and update file
Updates	**Description**
CiscoCyberVision-Embedded-KDB-4.2.6.dat	KnowledgeDB embedded in Cisco Cyber Vision 4.2.6
CiscoCyberVision-update-center-4.2.6.dat	Center update file for upgrade from release 4.1.x or 4.2.x to release 4.2.6
CiscoCyberVision-update-sensor-4.2.6.dat	Cisco IC3000 Sensor update file for upgrade from release 4.0.x or 4.1.x to release 4.2.6
CiscoCyberVision-update-combined-4.2.6.dat	Center and IC3000 Sensor update file from GUI for upgrade from release 4.0.x or 4.1.x to release 4.2.6

Cisco Cyber Vision Center 4.2.6 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