



Release Notes for Cisco Cyber Vision

Release 4.1.3

For users upgrading to 4.1.3 from previous versions, please carefully read the [Cisco Cyber Vision 4.1.3 update procedure](#).

For users upgrading IOx-x86-64 or Ox-Active-Discovery-x86-64 sensors (Catalyst 9300,9400 or IR8340), please carefully read the [Additional remarks](#).

Compatible device list	3
Cisco Cyber Vision 4.1.3 update procedure	4
Upgrade Path	4
Compatibility Guidelines	4
Data purge	4
Center updates	5
Architecture with Global Center	5
Architecture with one Center	8
Additional remarks	9
AWS and Azure Centers	10
Cisco Cyber Vision 4.1.3 important changes	10
Command line access	10
Communication port and protocol changes	10
Port	10
Protocol	10
API	10
SYSLOG	10
Cisco Cyber Vision new features and improvements	11
Sensor IOx update procedure with the sensor management extension	11
Sensor IOx in Catalyst 9300 and 9400, RSPAN	15
Cisco Cyber Vision Center Diagnostic from the User Interface	16

Cisco Cyber Vision changes	17
Cisco Cyber Vision Resolved Caveats	18
Cisco Cyber Vision Open Caveats	19
Links	20
Software Download	20
Related Documentation	22

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
Sentryo CENTER10	Sentryo CENTER10 hardware appliance
Sentryo CENTER30	Sentryo CENTER30 hardware appliance
Sensor	Description
Cisco IC3000	Cyber Vision Sensor hardware appliance
Cisco Catalyst IE3400	Cyber Vision Sensor IOx application hosted in Cisco Catalyst IE3400 Industrial Ethernet switches
Cisco Catalyst IE3300 10G	Cyber Vision Sensor IOx application hosted in Cisco Catalyst IE3300 Industrial Ethernet switches with 10G ports
Cisco IR1101	Cyber Vision Sensor IOx application hosted in Cisco IR1101 Series Industrial Integrated Services Routers
Cisco Catalyst IR8300	Cyber Vision Sensor IOx application hosted in Cisco Catalyst IR8300 Rugged Series Routers
Cisco Catalyst 9300, 9400	Cyber Vision Sensor IOx application hosted in Catalyst 9300, 9400 Series switches
Sentryo SENSOR3	Sentryo SENSOR3 hardware appliance
Sentryo SENSOR5	Sentryo SENSOR5 hardware appliance
Sentryo SENSOR7	Sentryo SENSOR7 hardware appliance

Cisco Cyber Vision 4.1.3 update procedure

Cisco Cyber Vision 4.1.3 update procedure will depend on the architecture deployed and the tool used to deploy it.

Upgrade Path

Upgrade Path to Cisco Cyber Vision 4.1.3

Current Software Release	Upgrade Path to Release 4.1.1
If version prior to 3.2.4	Upgrade first to 3.2.4, then to 4.0.0, and to 4.1.3
Version 3.2.4	Upgrade first to 4.0.0, then to 4.1.3
Version 4.0.0 to 4.1.2	Upgrade directly to Release 4.1.3

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 4.1.0 can manage local Centers with versions 4.1.0 and 4.0.3.
- Center with sync (Version N): Compatible with sensors with versions N and N-1.
e.g. Center with sync version 4.1.0 can manage sensors with versions 4.1.0 and 4.0.3.

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 schema. 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. Once migrated, the following expiration settings will be applied, and the system will run the purge process unless the configuration is modified within 2 days:

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

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 this check, 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-4.1.3.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-4.1.3.dat
 - Launch the update with the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-center-4.1.3.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-4.1.3.dat
 - Launch the update with the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-sensor-4.1.3.dat
```

You can check the sensor version on the Administration / Sensor Explorer page, to make sure that the version is 4.1.3.

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-4.1.3.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 --run /data/tmp/CiscoCyberVision-sensor-management-4.1.3.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. A complete procedure is available in the document (part “Cisco Cyber Vision new features and improvements”) or in all sensor deployment guides version 4.1.3 minimum.
- 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-aarch64-4.1.3.tar or CiscoCyberVision-IOx-Active-Discovery-aarch64--4.1.3.tar
 - Catalyst 9300 and 9400 and IR8340 files = CiscoCyberVision-IOx-x86-64-4.1.3.tar or CiscoCyberVision-IOx-Active-Discovery-x86-64-4.1.3.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.

Architecture with one Center

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

1. Update the Center:

a. Either using the Graphical User Interface:

- File= CiscoCyberVision-update-combined-4.1.3.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-4.1.3.dat
- Launch the update with the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-center-4.1.3.dat
```

2. Update the sensors:

a. 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-4.1.3.dat
 - Launch the update with the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-sensor-4.1.3.dat
```

b. 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-4.1.3.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 --run /data/tmp/CiscoCyberVision-sensor-management-4.1.3.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. A complete procedure is available in the document (part “Cisco Cyber Vision new features and improvements”) or in all sensor deployment guides version 4.1.3 minimum.
- 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-aarch64-4.1.3.tar or CiscoCyberVision-IOx-Active-Discovery-aarch64--4.1.3.tar
 - Catalyst 9300 and 9400 and IR8340 files = CiscoCyberVision-IOx-x86-64-4.1.3.tar or CiscoCyberVision-IOx-Active-Discovery-x86-64-4.1.3.tar.

Additional remarks

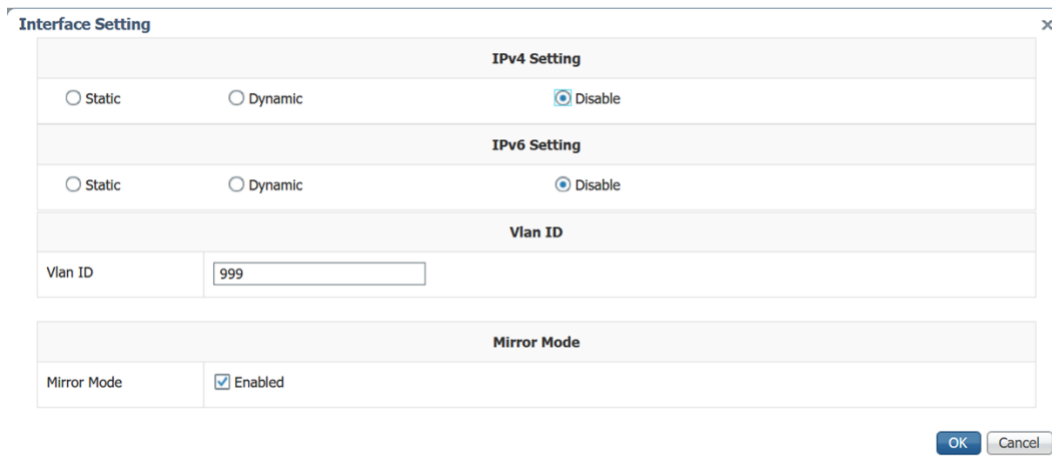
Important remark regarding CiscoCyberVision-IOx-x86-64 sensor application update:

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 enrolment package uploaded again.

Guidelines here: [Cisco Cyber Vision Sensor Application for Cisco Switches Installation Guide, Release 4.1.3](#)

A new RSPAN option (vs ERSPAN) is available in Cyber vision when the user deploys a **CiscoCyberVision-IOx-x86-64** sensor which lets the user choosing the right mode.

A new “Mirroring” check box is available in the IOX local manager on the interface eth1 which must be checked.



An Additional remark for IR8340, eth1 and eth3 needs to be swapped. Eth1 needs to be associated with mgmt-bridge300 and eth3 with VPG0.

AWS and Azure Centers

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

Cisco Cyber Vision 4.1.3 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 more 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 the command.

Communication port and protocol changes

Port

No modification in 4.1.3.

Protocol

No modification in 4.1.3.

API

No modification in 4.1.3.

SYSLOG

No modification in 4.1.3.

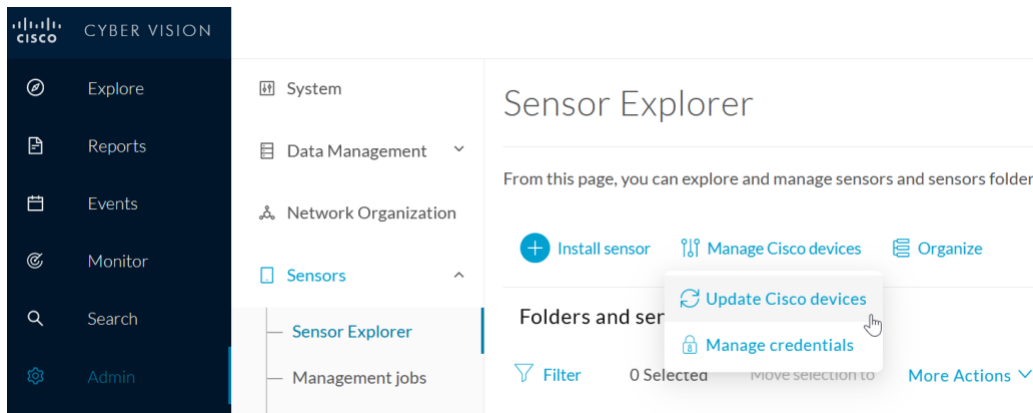
Cisco Cyber Vision new features and improvements

Sensor IOx update procedure with the sensor management extension

Sensor update behavior changes in release 4.1.3. Before this release, the update of all sensors occurred automatically after the extension update. Starting with release 4.1.3 the automatic update is not launched, and the user can select which sensors to update.

Once the sensor management extension is updated, the user can navigate to the Sensor Explorer menu, click “Manage Cisco devices” and “Update Cisco Devices”:

Cisco Cyber Vision, Sensor Explorer “Update Cisco devices »



A list of sensors to update will be built by the system, with their ability to be updated:

Cisco Cyber Vision, Update Cisco devices list

UPDATE CISCO DEVICES				
Only sensors deployed with the Sensor Management Extension (except IC3000) are concerned here. They appear only if there is a new version of their application available in the currently installed extension. Please select the sensors to update.				
<input type="checkbox"/>	Label ^	IP	Version	Target
<input type="checkbox"/>	IE3300 Mitsu PLC	192.168.0.145	4.1.3+202209061752	Available disk space is too low, 300M free are required.
<input type="checkbox"/>	IE3300 SCHN IO	192.168.0.141	4.1.3+202209061752	Available disk space is too low, 300M free are required.
<input type="checkbox"/>	IE3300 SIEM IO	192.168.0.143	4.1.3+202210041830	Updatable to 4.1.3+202210112248
<input type="checkbox"/>	IE3400 GE	192.168.0.137	4.1.3+202210041830	Updatable to 4.1.3+202210112248
<input type="checkbox"/>	IE3400 HSRP	192.168.31.16	4.1.3+202210041830	Updatable to 4.1.3+202210112248

This list presents the different sensor applications to update and the system capacity to update them. If the sensor is updatable, a green message is displayed, and the sensor is selectable. If the sensor needs to be updated but the system detects an issue to run the update, the reason is displayed in red, and the sensor is not selectable.

Possible issues include invalid platform credentials, connection failure, and available disk space.

For example, in case of connection failure:

Cisco Cyber Vision, Update Cisco devices list with connection failures

UPDATE CISCO DEVICES				
Only sensors deployed with the Sensor Management Extension (except IC3000) are concerned here. They appear only if there is a new version of their application available in the currently installed extension. Please select the sensors to update.				
<input type="checkbox"/>	Label ^	IP	Version	Target
<input type="checkbox"/>	FCW2521P24U	192.168.69.140	4.1.3+202209061745	Contact with this device has been lost. Check connection.
<input type="checkbox"/>	FOC2417V07Z	192.168.69.138	4.1.3+202209061745	Contact with this device has been lost. Check connection.

The user must select which sensors to launch the update. The check box of individual lines can be ticked, or all sensors can be selected with the top left check box:

Cisco Cyber Vision, Update Cisco devices list with connection failures

UPDATE CISCO DEVICES				
Only sensors deployed with the Sensor Management Extension (except IC3000) are concerned here. They appear only if there is a new version of their application available in the currently installed extension. Please select the sensors to update.				
<input type="checkbox"/>	Label ^	IP	Version	Target
<input type="checkbox"/>	IE3300 Mitsu PLC	192.168.0.145	4.1.3+202209061752	Available disk space is too low, 300M free are required.
<input type="checkbox"/>	IE3300 SCHN IO	192.168.0.141	4.1.3+202209061752	Available disk space is too low, 300M free are required.
<input type="checkbox"/>	IE3300 SIEM IO	192.168.0.143	4.1.3+202210041830	Updatable to 4.1.3+202210112248
<input checked="" type="checkbox"/>	IE3400 GE	192.168.0.137	4.1.3+202210041830	Updatable to 4.1.3+202210112248
<input checked="" type="checkbox"/>	IE3400 HSRP	192.168.31.16	4.1.3+202210041830	Updatable to 4.1.3+202210112248
<input type="checkbox"/>	IE3400 Mitsu IO	192.168.0.139	4.1.3+202210041830	Updatable to 4.1.3+202210112248

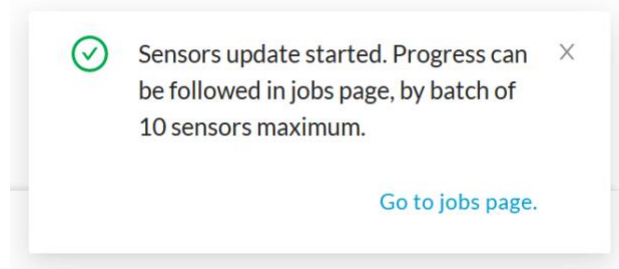
1 - 19

Once the different sensors are selected, the user must click the “Update” button. Some jobs are created to update sensors in batches. Four types of batches will be created, one per application type:

- CiscoCyberVision-IOx-aarch64-4.1.1.tar
- CiscoCyberVision-IOx-Active-Discovery-aarch64--4.1.1.tar
- CiscoCyberVision-IOx-x86-64-4.1.1.tar
- CiscoCyberVision-IOx-Active-Discovery-x86-64-4.1.1.tar

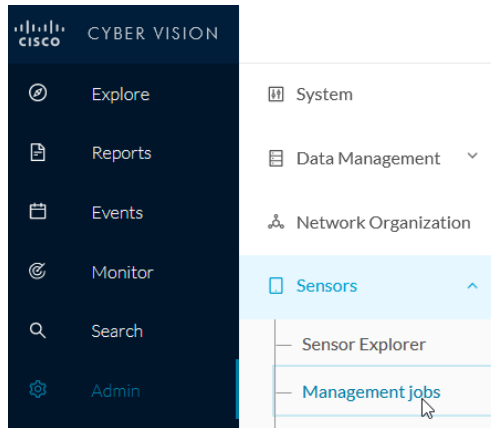
Each batch can contain up to 10 sensors. If more than 10 sensors need to be updated, several batches are created.

Cisco Cyber Vision, Update Cisco devices list with connection failures


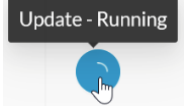





Batch update advancements can be followed on the “Management jobs” page:

Cisco Cyber Vision, Management Jobs



Advancements will be shown as below:

Cisco Cyber Vision, Management Jobs, update status	
Green icon indicating the update completed successfully.	
Blue icon indicating the update is in progress.	
Grey clock icon indicating the sensor is waiting for the update.	
Grey icon indicating the update has been cancelled.	
Red icon indicating an error occurred.	

In case of error, click the red icon to view status per sensor like below:

Cisco Cyber Vision, Management Jobs, update failure

Batch update (FOC2401V07N, FOC2412V0DL, FOC2431V08E, FOC2330V0TJ, FOC2334V00D, FOC2431V0A0, FOC2413V0X3) ✖

Update

Error

Fatal error: at least one device failed

Logs

```

X FOC2413V0X3: failed: job with status
FAILED has error: Error while changing
app state:Cannot start while in DEPLOYED
state. Allowed operations are
['activate', 'upgrade', 'undeploy',
'download_data']
✓ FOC2401V07N: succeeded to update
X FOC2412V0DL: failed: job with status
FAILED has error: Error while changing
app state:Cannot start while in DEPLOYED
state. Allowed operations are
['undeploy', 'upgrade', 'download_data',
'activate']
✓ FOC2431V08E: succeeded to update
✓ FOC2330V0TJ: succeeded to update
X FOC2334V00D: failed: job with status
FAILED has error: Error while changing
app state:Cannot start while in DEPLOYED
state. Allowed operations are
['undeploy', 'upgrade', 'download_data',
'activate']
✓ FOC2431V0A0: succeeded to update
                    
```

In case of recurrent errors on a particular sensor, a redeploy may help to solve the issue and to upgrade the application.

Sensor IOx in Catalyst 9300 and 9400, RSPAN

In releases prior to 4.1.3, using Cisco Cyber Vision Sensor on Catalyst 9300 and Catalyst 9400 required leveraging ERSPAN on the platform, which requires enabling routing.

When routing is not possible, RSPAN, which is an alternative to send raw packets to the sensor, can be used.

RSPAN usage has the following known issues:

- Multicast traffic is not sent from the switch backplane using RSPAN (it is with ERSPAN).
- With RSPAN, the Cisco Cyber Vision sensor receives raw packets without the source VLAN header. If there are assets with the same IP address, but on different VLANs, with an RSPAN deployment they will be seen as the same asset by Cisco Cyber Vision.

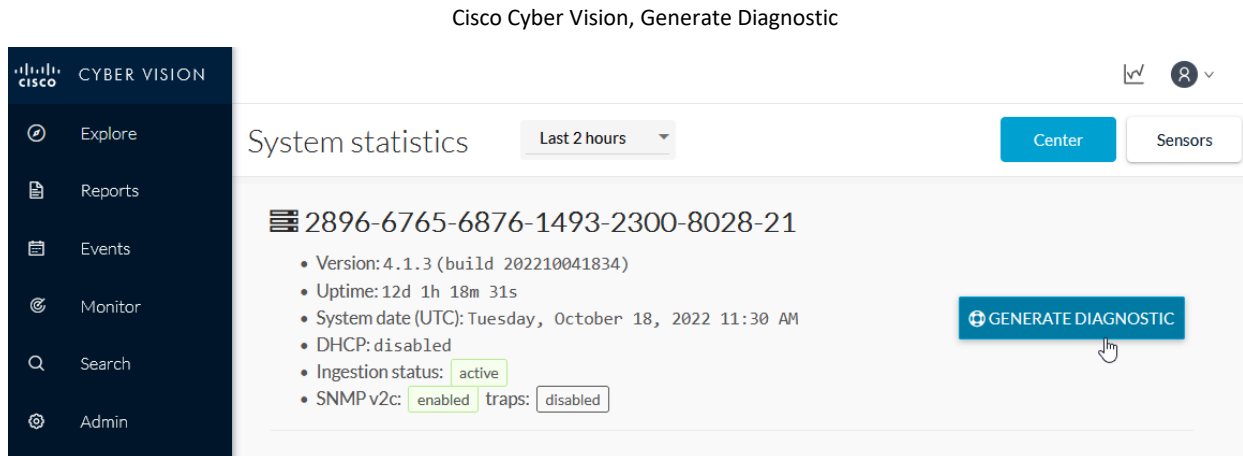
The deployment of the Cisco Cyber Vision sensor with the RSPAN option is possible with the Sensor Management extension and with the Local Manager platform.

The update to release 4.1.3 is not possible via the Local Manager. The Cisco Cyber Vision sensor needs to be removed and then deployed again to change the version from a release 4.1.2 or lower to a release 4.1.3 or higher. This limitation is valid for all platforms using the CiscoCyberVision-IOx-x86-64 sensor application including the Catalyst 9300, Catalyst 9400 and IR8340.

Cisco Cyber Vision Center Diagnostic from the User Interface

Starting with release 4.1.3 the diagnostic file generated via the UI is now a lighter weight version. This version will be faster to generate and smaller to download. If a complete diagnostic file is needed, it can be retrieved from the Center command line.

The button is available on the Center Statistics page:



Cisco Cyber Vision changes

CDETS	Description
	127.0.0.1 is no more considered as a public IP (3993.)
	Bacnet, extract more models and firmwares (5612)
	A column date was added in the Sensor Management Jobs page (8757)
	SSDP: Flow aggregation and tag added (10085)
CSCwb21265 CSCwd33782	Sbs-diag - Develop a version for the UI (10413)
	Add a sensor Constrained RAM mode (10211)
	Device-engine add Tag AMQP in lookup table (10413)
	Sbs-diag - Add certificates expiry date (10790)
	00:00:00:00:00:00 MAC no more assigned as Xerox (10802)
CSCwd21727	Sensor management extension: sensor updates were completely changed to fulfill customer requests (10851)
	Sbs-diag - add Global Center and Center enrolled configuration and status (11015)
	Change pxGrid integration to not send MAC addresses associated with more than 10 IPs (11092)
	Sbs-diag - add redis journal (11139)
	Avoid to create unused preset materialized views to limit DB size (10641)
	IOx Sensor: Support RSPAN on CAT9k (10849,11011)
	sbs-diag:: add missing conf (11228)
	Switch default in setup-center to single-intf (11272)

Cisco Cyber Vision Resolved Caveats

CDETS	Description
	User Interface resize pop-up message box hiding group configuration edit button (9390)
	RBAC: change read-only permission for Center Certificate (9779)
	Sensor management extension improve feedbacks when application installation failed (10128)
	Rabbitmq can still fail after a reboot (10215)
	Sorting flows by protocol type doesn't work (10311)
	Exported CSV shows port with empty values as 0 (10312)
	Active Discovery can miss some ip to scan (10449)
	Export to csv doesn't work for activities in device technical sheet (10460)
	On device technical sheet in components filtering by tags user gets input field instead of dropdown (10469)
	Device technical sheet > components table > sorting doesn't work correctly (10531)
CSCwc48048	LDAP role mapping is not done correctly (10532)
	Network filtering - Filtering with direct IP address doesn't work after preset saving (10554)
	Global Risk Score takes into consideration ghost devices (10582)
	Global Center - Hide the edit buttons on components and devices (10606)
	Fix Melfsoft directions (10645)
CSCwc80817	DPI sensor memory issue due to HSRP - VRRP (10758)
	sbs-diag - order by duration materialized view statistics (10640)
CSCwc84522	SecureX Ribbon is not configurable with a Cyber Vision LDAP user (10846)
	Obsolete caption in some messages (10852)
	Improve single IP searching (9085)
	Rabbitmq queues created with pcap upload are not deleted (10439)
	10 most matched vulnerabilities: affected device tab is empty (10596)
	SecureX connection can consume all postgres connection slots (11021)
CSCwd33798	All Cisco Cyber Vision sensors appear as disconnected (11022)
	LC/GC enrollement timeouts: display a clear error message (11016)
	make burrow analyzer do not crash burrow process (11104)
	sbs-db purge-components --network does not work with a single ip ('/32') (11149)

Cisco Cyber Vision Open Caveats

Issues ID / CDETS	Component	Description
CSCwb12630	Center + ISE	All components are not synchronized with ISE
CSCvy57108	Center	Linux computer incorrectly tagged as Windows
CSCwd39017	Center	Missing information in the Smart License Usage

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-4.1.3.ova	VMware OVA file, for Center setup
CiscoCyberVision-center-with-DPI-4.1.3.ova	VMware OVA file, for Center with DPI setup
CiscoCyberVision-center-4.1.3.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-sensor-management-4.1.3.ext	Sensor management extension installation file
Sensor	Description
CiscoCyberVision-IOx-aarch64-4.1.3.tar	Cisco IE3400, Cisco IR1101 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64--4.1.3.tar	Cisco IE3400, Cisco IR1101 Active Discovery sensor installation and update file
CiscoCyberVision-IOx-IC3K-4.1.3.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.1.3.tar	Cisco Catalyst 9x00 and Cisco Catalyst IR8340 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.1.3.tar	Cisco Catalyst 9x00 and Cisco Catalyst IR8340 Active Discovery sensor installation and update file
Updates	Description
CiscoCyberVision-Embedded-KDB-4.1.3.dat	KnowledgeDB embedded in Cisco Cyber Vision 4.1.3
CiscoCyberVision-update-center-4.1.3.dat	Center update file for upgrade from release 4.0.x or 4.1.x to release 4.1.3
CiscoCyberVision-update-sensor-4.1.3.dat	Cisco IC3000 Sensor and Sentryo Sensor3, 5, 7 update file for upgrade from release 4.0.x or 4.1.x to release 4.1.3
CiscoCyberVision-update-combined-4.1.3.dat	Center, IC3000 Sensor and Legacy Sensor update file from GUI for upgrade from release 4.0.x or 4.1.x to release 4.1.3

Cisco Cyber Vision Center 4.1.3 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/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.html](#)
- Cisco Cyber Vision GUI Administration User Guide:
[Cisco Cyber Vision GUI Administration Guide.html](#)
- 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 4 0 0.pdf](#)
- 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](#)