Release Notes for Cisco Cyber Vision

Release 4.4.3

July 2024

Contents

Cyber Vision release 4.4.2 and 4.4.3

Cyber Vision 4.4.2 fixes a regression in capture quality on the IC3000 platform from the 4.4.0 release and addresses two cosmetic issues found in version 4.4.1.

Cyber Vision 4.4.3 is fixing OpenSSH CVE-2024-6387 (CSCwk62289).

The defect list is:

Table 1. 4.4.1 defects fixed in 4.4.2 and 4.4.3

CDETS ID	Description
CSCwk50605	Global Center Service status is not accurate
CSCwk50606	Telemetry service is failing in some conditions
CSCwk53768	IC3000 traffic drops
CSCwk62289	Evaluation of cybervision for OpenSSH regreSSHion vulnerability

Compatible device list

Table 2. Centers

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

Table 3. Sensors

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

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

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

Unsupported device list

As of version 4.2.0, Sentryo hardware is no longer supported.

Table 4. Sentryo centers (end of life)

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

Table 5. Sentryo sensors (end of life)

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

Cisco Cyber Vision 4.4.3 update procedure

Cisco Cyber Vision 4.4.3 update procedure depends on the architecture deployed and the tool used to deploy it.

Upgrade to 4.4.3 considerations – To read before updating

Four important considerations need to be understood before upgrading a system to 4.4.x.

Consideration 1

Upgrading to 4.3.0 is mandatory before upgrading to 4.4.x if the targeted Center is still in a version below 4.3.0.

Consideration 2

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

Cisco Cyber Vision Center system has two partitions, one for the system, the other for data. Before version 3.2.0 the system partition had a size of 512MB, which is now too limited for version 4.4.3.

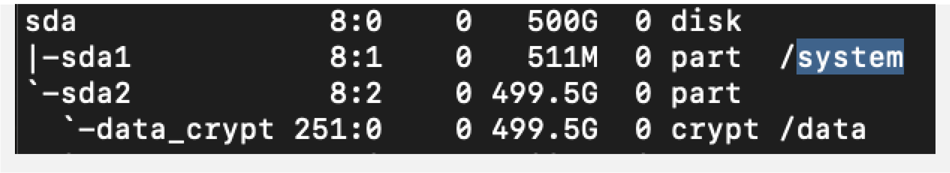
During the Center upgrade to 4.4.3, a check will be done, and the upgrade will be stopped if the system partition size is below 1GB. A message will be then displayed:

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

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

```
lsblk
```

The command answer will be something like:



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

Figure 1.
Cisco Cyber Vision system check – partition size

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

Consideration 3

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

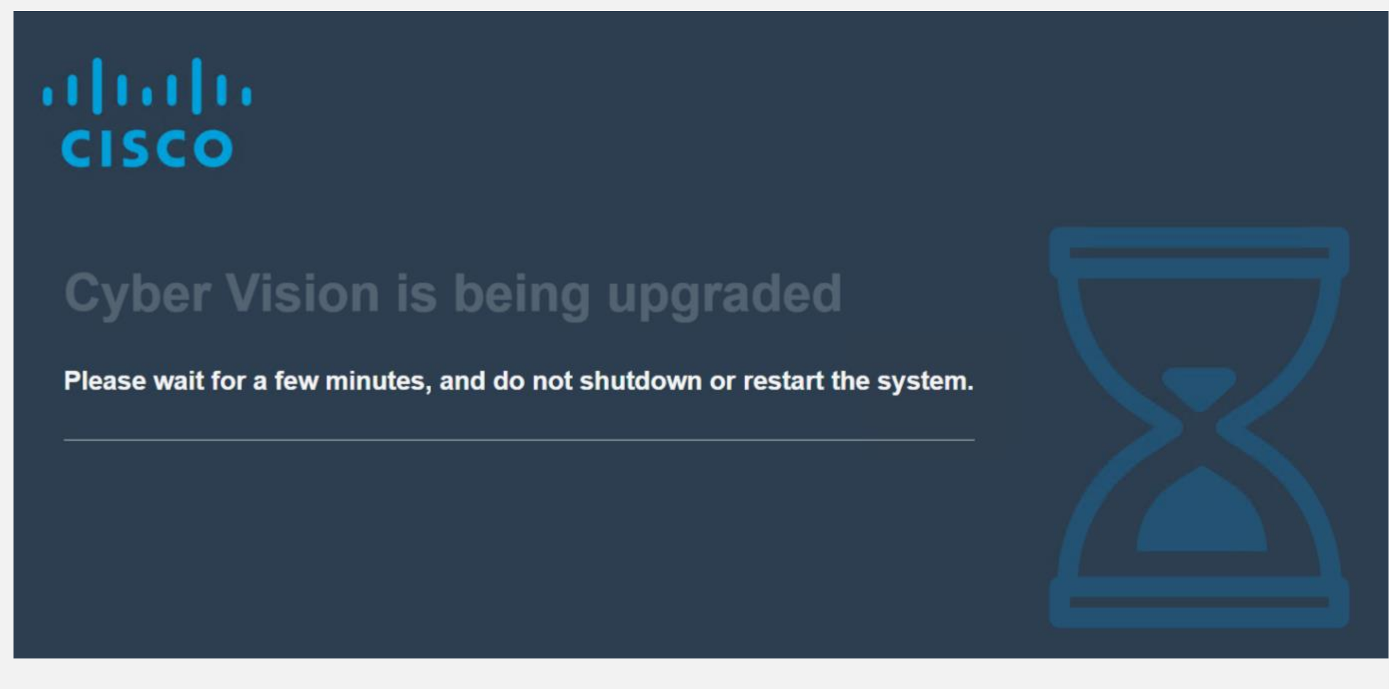
To upgrade to version 4.4.3, all old Sentryo's sensors must be removed and the IC3000 sensors must be upgraded to version 4.3.0 or later.

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

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

Consideration 4

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



Cyber Vision is being upgraded

Please wait for a few minutes, and do not shutdown or restart the system.

Figure 2.
Cisco Cyber Vision upgrade considerations – upgrade warning

Upgrade path

Table 6. Upgrade Path to Cisco Cyber Vision 4.4.3

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

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).

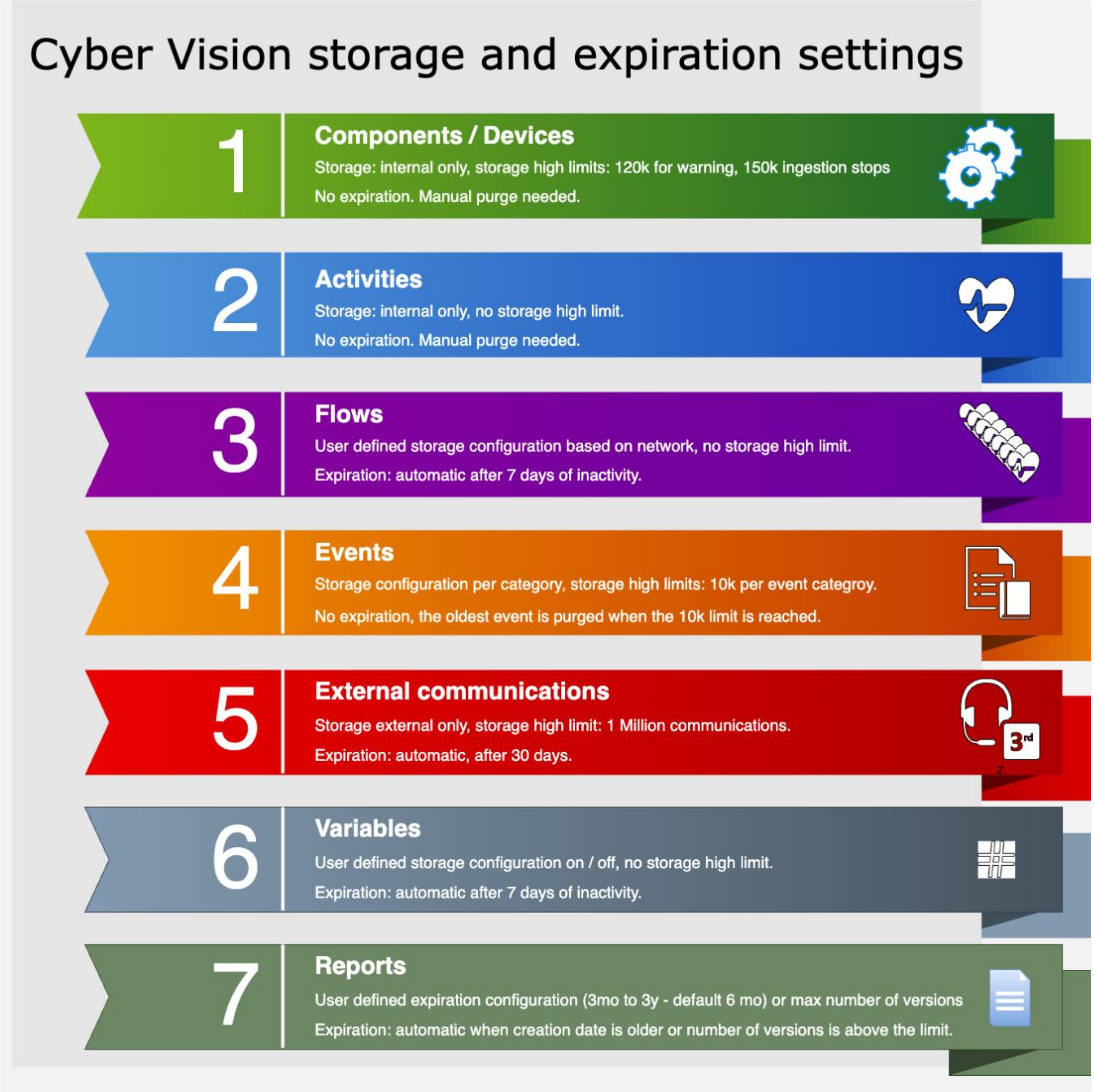
- Center with synchronization (Version N): Compatible with sensors with versions N and N-1

  (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 4.4.3:



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**
User defined storage configuration on / off, no storage high limit.
Expiration: automatic after 7 days of inactivity.

7 **Reports**
User defined expiration configuration (3mo to 3y - default 6 mo) or max number of versions
Expiration: automatic when creation date is older or number of versions is above the limit.

Figure 3.
Cisco Cyber Vision data retention policies

System updates

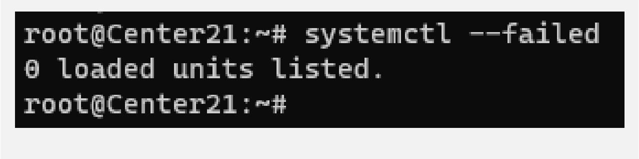
Preliminary checks

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

2. Use an SSH connection to the Center and type the following command:

   ```
   systemctl --failed
   ```

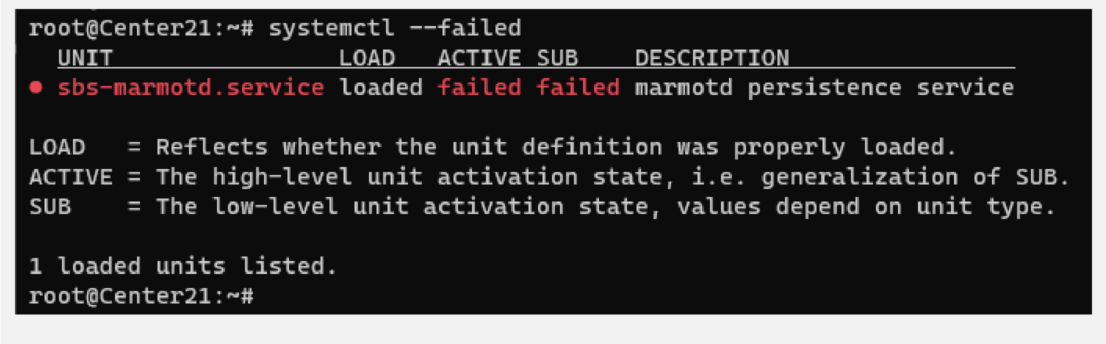
The number of listed sbs-* units should be 0. If not, fix the failures before updating.



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

Figure 4.
Cisco Cyber Vision system check – 0 failure

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



```
root@Center21:~# systemctl --failed
  UNIT                 LOAD   ACTIVE SUB    DESCRIPTION
● sbs-marmotd.service loaded failed failed marmotd persistence service

LOAD   = Reflects whether the unit definition was properly loaded.
ACTIVE = The high-level unit activation state, i.e. generalization of SUB.
SUB    = The low-level unit activation state, values depend on unit type.

1 loaded units listed.
root@Center21:~#
```

Figure 5.
Cisco Cyber Vision system check – example of failure

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

Architecture with Global Center

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

    a. Use the Graphical User Interface:

    - File= CiscoCyberVision-update-center-<LAST-VERSION>.dat
    - Navigate to **Admin > System**, use the **System update** button and browse and select the update file.

    b. Use the Command Line Interface (CLI):

    - File= CiscoCyberVision-update-center-<LAST-VERSION>.dat
    - Launch the update with the following command:

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

2. Update the Centers connected to the Global Center with the same procedure used for the Global Center (User Interface or CLI).

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

    a. If you installed the sensors with the sensor management extension:

    i. First upgrade the extension and then update the sensors

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

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

    ii. Update all sensors with the extension.

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

b. If you did not install the sensor with the sensor management extension, upgrade the sensor with the sensor package from the platform Local Manager or from the platform Command Line. Use one of the corresponding sensor installation guides.

   - 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

Guideline links:

Cisco Cyber Vision Sensor Application for Cisco Switches Installation Guide, Release 4.4.0
Cisco Cyber Vision Network Sensor Installation Guide for Cisco IR8340, Release 4.4.0
Cisco Cyber Vision Network Sensor Installation Guide for Cisco IC3000, Release 4.3.0
Cisco Cyber Vision Network Sensor Installation Guide for Cisco IR1101, Release 4.4.0

Architecture with one Center

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

   a. Use the Graphical User Interface:

   - File= CiscoCyberVision-update-center-<LAST-VERSION>.dat
   - Navigate to **Admin > System**, use the **System update** button and browse and select the update file.

   b. Use the Command Line Interface (CLI):

   - File= CiscoCyberVision-update-center-<LAST-VERSION>.dat
   - Launch the update with the following command:

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

2. Update the sensors.

   a. If you installed the sensors with the sensor management extension:

      i. First upgrade the extension and then update the sensors

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

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

      ii. Update all sensors with the extension.

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

b. If you did not install the sensor with the sensor management extension, upgrade the sensor with the sensor package from the platform Local Manager or from the platform Command Line. Use one of the corresponding sensor installation guides.

  - 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

Guideline links:

Cisco Cyber Vision Sensor Application for Cisco Switches Installation Guide, Release 4.4.0
Cisco Cyber Vision Network Sensor Installation Guide for Cisco IR8340, Release 4.4.0
Cisco Cyber Vision Network Sensor Installation Guide for Cisco IC3000, Release 4.3.0
Cisco Cyber Vision Network Sensor Installation Guide for Cisco IR1101, Release 4.4.0

AWS and Azure Centers

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

Cisco Cyber Vision 4.4.3 important changes

Communication port and protocol changes

Port

No modification in 4.4.3.

Protocol

No modification in 4.4.3.

API

Some changes were made in release 4.4.3. Several API routes changed:

New endpoints - No modification in 4.4.3.

New attributes - No modification in 4.4.3.

Removed endpoint - No modification in 4.4.3.

Changed endpoints - No modification in 4.4.3.

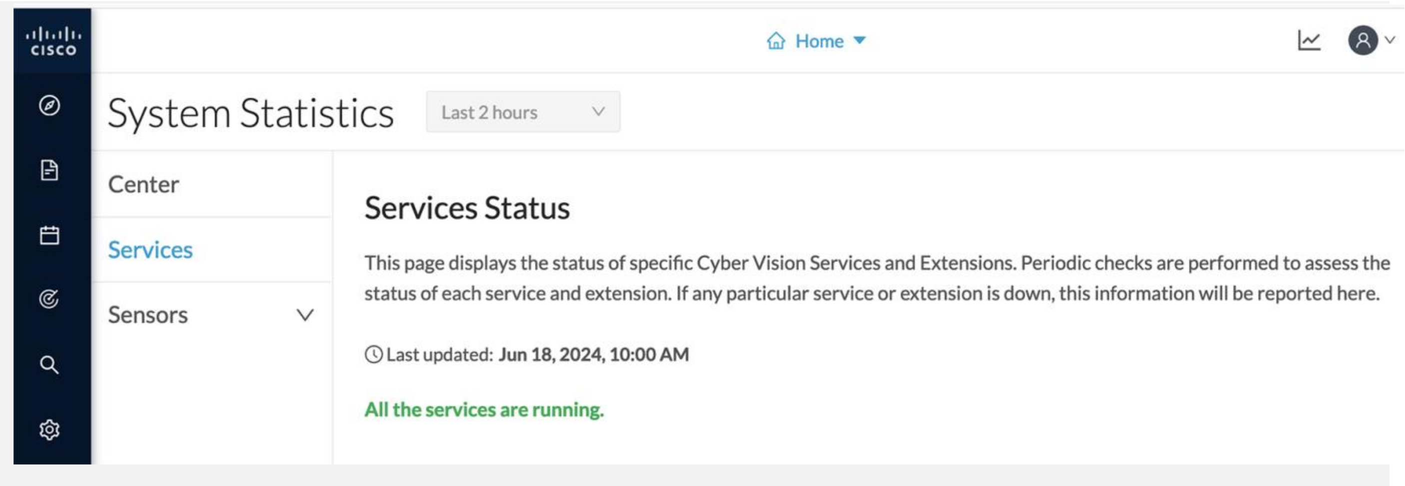
SYSLOG

No modification in 4.4.3.

Cisco Cyber Vision new features and improvements

Cyber vision center service status

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



Services Status

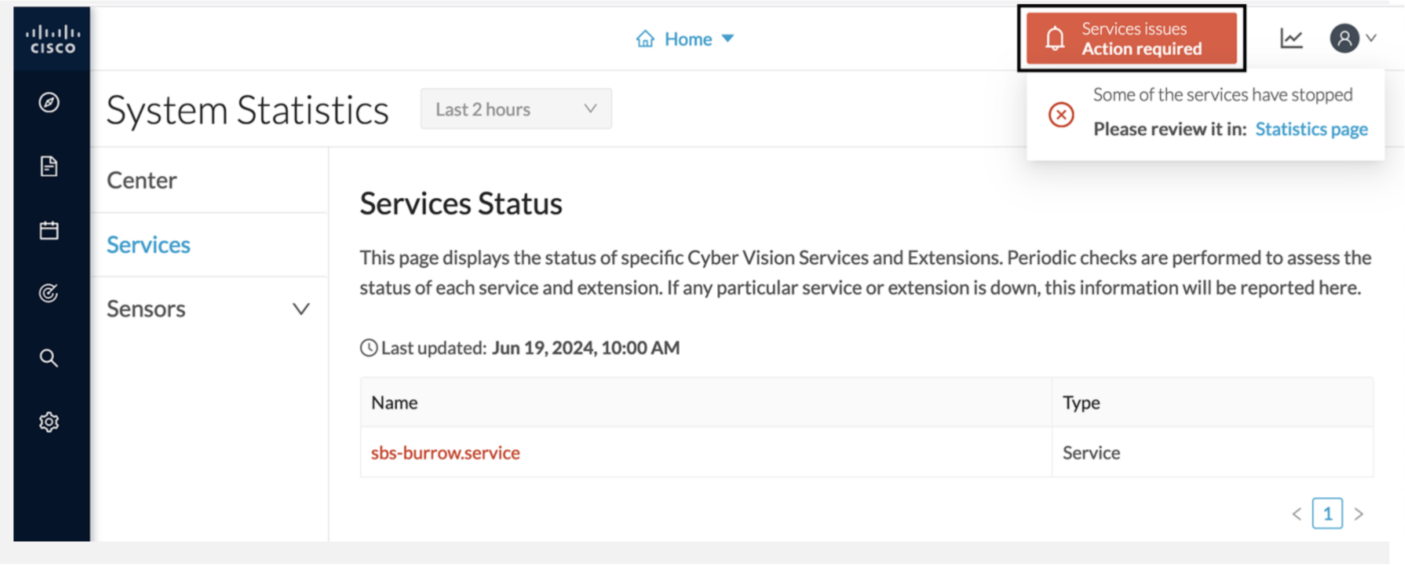
This page displays the status of specific Cyber Vision Services and Extensions. Periodic checks are performed to assess the status of each service and extension. If any particular service or extension is down, this information will be reported here.

Last updated: **Jun 18, 2024, 10:00 AM**

All the services are running.

Figure 6.
Cisco Cyber Vision service status – All services running

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



Some of the services have stopped
Please review it in: Statistics page

Services Status

This page displays the status of specific Cyber Vision Services and Extensions. Periodic checks are performed to assess the status of each service and extension. If any particular service or extension is down, this information will be reported here.

Last updated: **Jun 19, 2024, 10:00 AM**

Name	Type
sbs-burrow.service	Service

Figure 7.
Cisco Cyber Vision service status – one service is failing

Cisco Cyber Vision 4.4.3 Resolved Caveats

Table 7. Cisco Cyber Vision resolved caveats

CDETS	Description
-	DPI - Wrong OPC-UA application name
-	Report generation hanging
-	Beckhoff and Bacnet Active Discovery does not show broadcast queries
-	LDAP Settings - UI issues
-	Trying to run an active discovery scan while one is in progress show a wrong error
CSCwj93198	XDR: Correction in error message
-	Ambiguous UI when selecting components to delete
-	Sticky filter on activity and device View on preset change
-	Clarify error message when sensor self-update ends up doing a rollback
CSCwj79899	Collection interface used for active discovery is always shown as vlan 1
-	Sensor self-update - Properties drawer not updated when triggering update
-	Sensor self-update button display wrong mouse-over
-	sync-apps fails for 2 sensor apps
-	Services monitoring issues
CSCwk24950	Random MAC addresses created when erspan is fragmented
-	API Request Preset RiskScore via API return 0
CSCwj93196	FMC script is abnormally long during the synchronization
CSCwj69323	XDR ribbon, Cyber Vision incidents cannot be found on the XDR site
CSCwk04880	Backup and Restore – restoring a dual interface center on a center configured as single interface is not working
CSCwk04879	Backup and Restore – restoring a center backup may fail due to number of interfaces count.
CSCwd39017	Missing information in the Smart License Usage
CSCwk50605	Global Center Service status is not accurate
CSCwk50606	Telemetry service is failing in some conditions
CSCwk53768	IC3000 traffic drops
CSCwk62289	Evaluation of cybervision for OpenSSH regreSSHion vulnerability

Cisco Cyber Vision Open Caveats

Table 8. Cisco Cyber Vision enhancements

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

Cisco Cyber Vision deprecated features

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

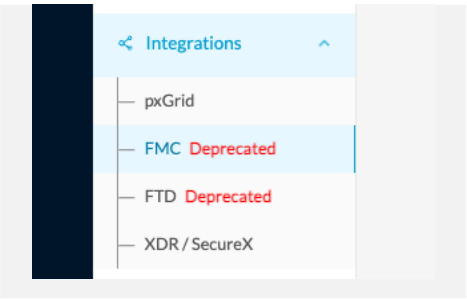


Figure 8.
Cisco Cyber Vision integrations

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

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

Cisco Secure Dynamics Attributes Connector Guides

For example: Cisco Secure Dynamic Attributes Connector Configuration Guide 3.0

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

Links

Software Download

The files below can be found at the following link: https://software.cisco.com/download/home/286325414/type

Remarks:

- VMWare OVA files are available in 2 different configurations: A standard configuration and a specific configuration with an extra interface made to receive OT network traffic and do the DPI. The DPI center will do the DPI of that traffic directly like remote sensors are doing it.
- IOX sensors are available in 2 versions: one with the active discovery capability, another one without that capability. The version without that capability prevents any active behavior on the OT network.

Table 9. Cisco Cyber Vision 4.4.3 center files

Center	Description
CiscoCyberVision-center-4.4.3.ova	VMware OVA file, for Center setup
CiscoCyberVision-center-with-DPI-4.4.3.ova	VMware OVA file, for Center with DPI setup
CiscoCyberVision-center-4.4.3.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-reports-management-4.4.3.ext	Reports management extension installation file
CiscoCyberVision-sensor-management-4.4.3.ext	Sensor management extension installation file

Table 10. Cisco Cyber Vision 4.4.3 sensor files

Sensor	Description
CiscoCyberVision-IOx-aarch64-4.4.3.tar	Cisco IE3400, Cisco IE3300 10G, Cisco IE9300, Cisco IR1101 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64--4.4.3.tar	Cisco IE3400, Cisco IE3300 10G, Cisco IE9300 Cisco IR1101 Active Discovery sensor installation and update file
CiscoCyberVision-IOx-IC3000-4.4.3.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-IC3000-4.4.3.tar	Cisco IC3000 Active Discovery sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.4.3.tar	Cisco Catalyst 9x00 and Cisco Catalyst IR8340 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.4.3.tar	Cisco Catalyst 9x00 and Cisco Catalyst IR8340 Active Discovery sensor installation and update file

Table 11. Cisco Cyber Vision 4.4.3 update files

Updates	Description
CiscoCyberVision-Embedded-KDB-4.4.3.dat	KnowledgeDB embedded in Cisco Cyber Vision 4.4.3
CiscoCyberVision-update-center-4.4.3.dat	Center update file for upgrade from release 4.3.x to release 4.4.3 (UI and CLI)

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

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

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

The Cisco Cyber Vision Center Plan is on the Microsoft Azure marketplace:

https://azuremarketplace.microsoft.com/en-us/marketplace/apps/cisco.cisco-cyber-vision?tab=Overview

Related Documentation

Cisco Cyber Vision documentation:

https://www.cisco.com/c/en/us/support/security/cyber-vision/series.html

Center Deployment guides:

Cisco Cyber Vision Center Appliance Installation Guide
Cisco Cyber Vision Center VM Installation Guide
Cisco Cyber Vision for Azure Cloud Installation Guide
Cisco Cyber Vision for the AWS Cloud Installation Guide,

Sensor deployment guides:

Cisco Cyber Vision Sensor Application for Cisco Switches Installation Guide
Cisco Cyber Vision Network Sensor Installation Guide for Cisco IR8340
Cisco Cyber Vision Network Sensor Installation Guide for Cisco IC3000
Cisco Cyber Vision Network Sensor Installation Guide for Cisco IR1101

System end-user guides:

Cisco Cyber Vision GUI User Guide
Cisco Cyber Vision GUI Administration Guide
Cisco Cyber Vision GUI Monitor Mode User Guide
Cisco Cyber Vision Active Discovery Configuration Guide
Cisco Cyber Vision syslog notification format Configuration Guide
Cisco Cyber Vision Architecture Guide
Cisco Cyber Vision Integration Guide, Integrating Cisco Cyber Vision with Cisco Identity Services Engine (ISE) via pxGrid
Cisco Cyber Vision Smart Licensing User Guide

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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