Release Notes for Cisco Cyber Vision Release 4.0.3

For users upgrading to 4.0.3 from previous versions, please carefully read the Cisco Cyber Vision 4.0.3 update procedure.

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
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 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 4.0.3 update procedure

Cisco Cyber Vision 4.0.3 update procedure will depend on the architecture deployed and the tool used to deploy it.

If you are currently running a version earlier than Cisco Cyber Vision 4.0.0, you must first upgrade to 4.0.0 prior to upgrading to Cyber Vision 4.0.32. Versions 4.0.0, 4.0.1 and 4.0.2 can be updated to 4.0.3.

Upgrade Path to Cisco Cyber Vision 4.0.3

Current Software Release	Upgrade Path to Release 4.0.2
If version prior to 3.2.4	Upgrade first to 3.2.4 then to 4.0.0 and finally to 4.0.3
Version 3.2.4	Upgrade first to 4.0.0 then to 4.0.3
Version 4.0.0 and 4.0.1	You can upgrade directly to Release 4.0.3

Data purge

Cisco Cyber Vision update procedure will not purge data automatically. The Center database in 4.0.0, 4.0.1 and 4.0.2 will be migrated to the new 4.0.3 schema. All components, activities, flows, events, etc. will be migrated.

The new data retention policies introduced in 4.0.0 are still valid in 4.0.3. Once migrated, the following expiration settings will be applied, and the system will purge unless the configuration is modified:

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

Center updates

Architecture with Global Center

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-4.0.3.dat
        - Navigate to Admin > System and use the System Update button and browse and select the update file.
    b. Or using the command line interface (CLI):
        - File= CiscoCyberVision-update-center-4.0.3.dat
        - Launch the update with the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-center-4.0.3.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 owned the sensor, the hardware sensors (IC3000 and Sentryo SENSOR's) were updated at the same time.
        ii. If not, the update needs to be done from the Command Line (CLI):
            - File= CiscoCyberVision-update-sensor-4.0.3.dat
            - Launch the update with the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-sensor-4.0.3.dat
```

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 sensor with the sensor management extension, the upgrade of the extension will also update all sensors reachable from the Center.
      - File = CiscoCyberVision-sensor-management-4.0.3.ext
      - Navigate to Admin > Extensions. In the Actions column, use the update button and browse to select the update file.
      - Cyber Vision sensor management extension could also be updated from the CLI with the command:

```
sbs-extension upgrade /data/tmp/CiscoCyberVision-sensor-management-4.0.3.ext
```

   ii. If a sensor was not updated by the extension update, access the sensor administration page, and use the UPDATE CISCO DEVICES button to update the remaining IOx sensors connected to the Center.

   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 IR11101 files = CiscoCyberVision-IOx-aarch64-4.0.3.tar or CiscoCyberVision-IOx-Active-Discovery-aarch64--4.0.3.tar
      - Catalyst 9300 and 94000 files = CiscoCyberVision-IOx-x86-64-4.0.3.tar or CiscoCyberVision-IOx-Active-Discovery-x86-64-4.0.3.tar.

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-4.0.3.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-4.0.3.dat
        - Launch the update with the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-center-4.0.3.dat
```

2. Update the sensors:
    a. Hardware sensors:
        i. If you used the combined file to update the Center, the hardware sensors (IC3000 and Sentryo SENSOR's) were updated at the same time if the SSH connection to the sensors is allowed.
        ii. If not, the update needs to be done from the command line interface (CLI):
            - File= CiscoCyberVision-update-sensor-4.0.3.dat
            - Launch the update with the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-sensor-4.0.3.dat
```

    b. IOx sensors:
        i. If you have installed the sensor with the sensor management extension, the upgrade of the extension will also update all reachable sensors.
            - File = CiscoCyberVision-sensor-management-4.0.3.ext
            - Navigate to Admin > Extensions. In the Actions column, use the update button and browse to select the update file.

              Cyber Vision sensor management extension could also be updated from the CLI with the command:

```
sbs-extension upgrade /data/tmp/CiscoCyberVision-sensor-management-4.0.3.ext
```

        ii. 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-aarch64-4.0.3.tar or CiscoCyberVision-IOx-Active-Discovery-aarch64--4.0.3.tar
            - Catalyst 9300 and 9400 files = CiscoCyberVision-IOx-x86-64-4.0.3.tar or CiscoCyberVision-IOx-Active-Discovery-x86-64-4.0.3.tar.

AWS Center

In the case of a center deployed in AWS, the procedure below has to be followed. But the build used need to bas asked to Cisco support. The standard update packages are not working on an AWS center.

Cisco Cyber Vision 4.0.3 important changes

Communication port and protocol changes

Port

There is no port change in Cisco Cyber Vision 4.0.3. All TCP or UDP ports already used are kept, and no new port number is needed.

Protocol

No modification in 4.0.3.

API

No modification in 4.0.3.

SYSLOG

No modification in 4.0.3.

Cyber Vision Sensor Management Extension impacted by Log4J

The vulnerabilities are located into the Cisco Cyber Vision Sensor Management Extension.

Cisco Cyber Vision Sensor Management Extension release 4.0.3 fixes those vulnerabilities.

Cisco information on log4j:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd

Cisco Cyber Vision Resolved Caveats

CDETS	Description
CSCvy30877	RPC-DCOM flows often not tagged - 7808
CSCwa14472	Revert fix that was blocking LDAP login - 8648
CSCvz68350	Fix vulnerabilities listed in the corresponding CDETS - 9268
CSCvz68532	Fix vulnerabilities listed in the corresponding CDETS - 9268
CSCwa14488	NTP service fails on ic3k if center is not reachable at boot - 9153
CSCwa49482	Cyber Vision Sensor Management Extension impacted by Log4J (CVE-2021-44228)
	sbs-passwd missing in hardware sensors - 9368
	Fix enip DPI which gives less properties than before - 9312
	Fix oom error on multiple sensors - 9272
	Ciscossl updated - 9134
	Haproxy updated - 8980
	Redis updated - 8979
	CIP DPI - Sensor performance issues - 9151
	Fix log errors on dump restore via UI - 8103
	Sentryo SENSOR7 wrongly reports faulty status - 8601
	Sensors sometimes stop sending log - 8489
	Once a baseline was set on a preset, it can't be changed, even after deleting the baseline - 8289
	Device list interaction slow on big table - 7505

Cisco Cyber Vision Open Caveats

Issues ID / CDETS	Component	Description
CSCwa15184	Centers	Online license registration fails when using a proxy
CSCwa14510	Centers	Cyber Vision Device engine 4.0.2 sometime breaks Rockwell chassis into several devices
CSCvz88557	Centers	CV sensor does not survive stack failover
-	AWS Center	Standard Center update packages don’t work on an AWS center.

Links

Software Download

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

Center	Description
CiscoCyberVision-center-4.0.3.ova	VMware OVA file, for Center setup
CiscoCyberVision-center-with-DPI-4.0.3.ova	VMware OVA file, for Center with DPI setup
CiscoCyberVision-center-4.0.3.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-sensor-management-4.0.3.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-4.0.3.tar	IE3400, IR1101 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64--4.0.3.tar	IE3400, IR1101 Active Discovery sensor installation and update file
CiscoCyberVision-IOx-IC3K-4.0.3.tar	IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.0.3.tar	Catalyst 9x00 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.0.3.tar	Catalyst 9x00 Active Discovery sensor installation and update file
Updates	**Description**
CiscoCyberVision-Embedded-KDB-4.0.3.dat	KnowledgeDB embedded in Cisco Cyber Vision 4.0.3
CiscoCyberVision-update-center-4.0.3.dat	Center update file for upgrade from release 4.0.0 or 4.0.1 to release 4.0.3
CiscoCyberVision-update-sensor-4.0.3.dat	Cisco IC3000 Sensor and Sentryo Sensor3, 5, 7 update file for upgrade from release 4.0.0, 4.0.1 or 4.0.2 to release 4.0.3
CiscoCyberVision-update-combined-4.0.3.dat	Center, IC3000 Sensor and Legacy Sensor update file from GUI for upgrade from release 4.0.0, 4.0.1 or 4.0.2 to release 4.0.3

Cisco Cyber Vision Center 4.0.3 can also be deployed on AWS (Amazon Web Services). The 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

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_4_0_0.pdf
- Cisco Cyber Vision Network Sensor Installation Guide for Cisco IE3300 10G, IE3400 and Catalyst 9300:

  Installation_Guide_for_Cisco_IE3300_10G_Cisco_IE3400_and_Cisco_Catalyst_9300_4_0_0.pdf
- 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_4_0_0.pdf
- Cisco Cyber Vision IC3000 Troubleshooting Guide:

  Cisco_Cyber_Vision_IC3000_Troubleshooting_Guide_Release_3_0_2.pdf
- Cisco Cyber Vision Center Appliance Installation Guide:

  Cisco_Cyber_Vision_Center_Appliance_Installation_Guide_4_0_0.pdf
- Cisco Cyber Vision Center VM Installation Guide:

  Cisco_Cyber_Vision_Center_VM_Installation_Guide_4_0_0.pdf
- Cisco Cyber Vision Center AWS Installation Guide:

  Cisco Cyber Vision for AWS Cloud Installation Guide
- Cisco Cyber Vision SecureX Integration Guide:

  Cisco Cyber Vision SecureX Integration Guide Release 4_0_0.pdf
- Cisco Cyber Vision Integration Guide, Integrating Cisco Cyber Vision with Cisco Identify Services Engine (ISE) via pxGrid:

  Integrating-Cisco-Cyber-Vision-with-Cisco-Identify-Services-Engine-via-pxGrid.pdf
- Cisco Cyber Vision Smart Licensing User Guide, Release 3.2.2

  Cisco_Cyber_Vision_Smart_Licensing_User_Guide_3_2_2.pdf