Release Notes for Cisco Cyber Vision Release 4.1.1

For users upgrading to 4.1.1 from previous versions, please carefully read the Cisco Cyber Vision 4.1.1 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 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 4.1.1 update procedure

Cisco Cyber Vision 4.1.1 update procedure will depend on the architecture deployed and the tool used to deploy it.

Upgrade Path

If you are currently running a version earlier than Cisco Cyber Vision 4.0.0, you must first upgrade to 4.0.0 prior upgrading to Cyber Vision 4.1.1. Versions 4.0.0, 4.0.1, 4.0.2, 4.0.3 and 4.1.0 can be updated to 4.1.1.

Upgrade Path to Cisco Cyber Vision 4.1.1

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 finally to 4.1.1
Version 3.2.4	Upgrade first to 4.0.0 then to 4.1.1
Version 4.0.0 to 4.1.0	You can upgrade directly to Release 4.1.1

Compatibility Guidelines

There is downward compatibility of one version between Global Center → Local Center and Sensors.

- Global Center (Version N): Compatible with local centers with versions N and N-1.

  For ex., Global center version 4.1.0 can manage local centers with versions 4.1.0 and 4.0.3.
- Local Center (Version N): Compatible with sensors with versions N and N-1.

  For ex., Local center 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:~#
```

Rational: all sbs services need to run in a normal state before the update. If one of them is listed as failed it has to be fixed before the upgrade.

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 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-4.1.1.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-4.1.1.dat
        - Launch the update with the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-center-4.1.1.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 Sensor is allowed, the hardware sensors (IC3000 and Sentryo SENSOR's) were updated at the same time.
        ii. If IC3000 sensor was deployed using the "Sensor management extension", it can be upgraded by "redeploying it"
        iii. If not, the update needs to be done from the Command Line (CLI):
            - File= CiscoCyberVision-update-sensor-4.1.1.dat
            - Launch the update with the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-sensor-4.1.1.dat
```

You may check the sensor version on the Administration / Sensor page, to make sure that the version is 4.1.

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-4.1.1.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-4.1.1.ext
```

ii. If a sensor was not updated by the extension update, access the sensor administration page, and use the UPDATE CISCO DEVICES button or the redeploy 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 IR1101 files = CiscoCyberVision-IOx-aarch64-4.1.1.tar or CiscoCyberVision-IOx-Active-Discovery-aarch64--4.1.1.tar
- Catalyst 9300 and 9400 files = CiscoCyberVision-IOx-x86-64-4.1.1.tar or CiscoCyberVision-IOx-Active-Discovery-x86-64-4.1.1.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-4.1.1.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-4.1.1.dat
- Launch the update with the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-center-4.1.1.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 Sensor is allowed, the hardware sensors (IC3000 and Sentryo SENSOR's) were updated at the same time.
        ii. If IC3000 sensor was deployed using the "Sensor management extension", it can be upgraded by "redeploying it"
        iii. If not, the update needs to be done from the command line interface (CLI):
            - File= CiscoCyberVision-update-sensor-4.1.1.dat
            - Launch the update with the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-sensor-4.1.1.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-4.1.1.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-4.1.1.ext
```

        ii. If a sensor was not updated by the extension update, access the sensor administration page, and use the UPDATE CISCO DEVICES button or the redeploy 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 IR1101 files = CiscoCyberVision-IOx-aarch64-4.1.1.tar or CiscoCyberVision-IOx-Active-Discovery-aarch64--4.1.1.tar
            - Catalyst 9300 and 9400 files = CiscoCyberVision-IOx-x86-64-4.1.1.tar or CiscoCyberVision-IOx-Active-Discovery-x86-64-4.1.1.tar.

AWS Center

In case of a center deployed in AWS, the same procedure as "One center" above has to be followed.

Cisco Cyber Vision 4.1.1 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 4.1.1.

Protocol

No modification in 4.1.1.

API

No modification in 4.1.1.

SYSLOG

No modification in 4.1.1.

Cisco Cyber Vision Resolved Caveats

CDETS	Description
CSCwb21270	Cisco Cyber Vision Sensor Management extension can keep traces of old sensors which prevent sensor deployment (9931)
CSCwb30722	Cisco Cyber Vision Sensor Management extension cannot deploy sensor application on IR8340 with no SSD (10034)
CSCwb45210	Center SNMP traps (CPU / RAM) do not use the same logic (10093)
	S7Plus DPI improvements: incomplete decoding (5642)
	Mix of ISL and HSR layers leads to Unknown ethertype 0x4c logs (5775)
	Handling TCP gaps in S7Plus reassembly (6158)
	IR1101 disk usage trend not relevant (7831)
	EthernetIP unknown command code 0x372f, 0x100, 0x2030 (8054)
	Searching for an event in the calendar page led to error if there are too many events (8460)
	Tag "Important" flag not up to date (9393)
	Active Discovery - Add a warning in case of failure due to sensor time discrepancy (9807)
	Active Discovery - Add a warning if the preset does not have any IPV4 component in case of unicast scan (9808)
	Sensor Explorer: Impossible to import offline file on Windows PC (9818)
	RBAC: link from event widgets is dead when there are no event-read privilege (9824)
	SNMP agent configuration interface is confusing (9835)
	LDAP integration: Role Mapping Summary needs to be responsive to display the role names in a single line (9876)
	Wrong direction and wrong names for "New remote access" events (9894)
	Sensor logs empty in center (9914)

CDETS	Description
	Update scand process (10018)
	Device engine fix issue with serial 00000000 (10023)
	RBAC - Global Center Main Dashboard Error (10026)
	Purdue Model - All Devices are in Level 3-4 (10031)
	Regression on the date format in the event page (calendar view) (10032)
	Feedbacks from SecureX team (10043)
	Misleading help text for setup-center-cli command (10047)
	Several French translation issues (10054)
	sbs db command in Admin System does not have the right format (10055)
	sbs-db purge add date format in the command line help (10056)
	Optimization of FTP stream analysis (10057)
	Sensor Explorer, version column, remove build number (10074)
	LDAP role mapping - force the user to map a default or a custom role (10086)
	Sensor management extension: Broken job is created if the deploy pre-checks fails (10131)
	Diagnostic generation takes long time (10158)
	BacNet flow tables causes panic out of bounds in bacnet analyzer (10024)

Cisco Cyber Vision Open Caveats

Issues ID / CDETS	Component	Description
	Center	Sensor explorer "Update Cisco Device" does not find upgradable devices (9917) Workaround: use the redeploy option
CSCwb25431	Center	Active Discovery ENIP Unicast in Backplane – some components could be created for non-existent modules
CSCwb12630	Center + ISE	All components are not synchronized with ISE
CSCwb21265	Center	Cyber Vision user not able to generate diagnostic files from the UI. Workaround: diagnostic generation remains possible form the CLI.
CSCvy57108	Center	Linux computer incorrectly tagged as Windows

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-4.1.1.ova	VMware OVA file, for Center setup
CiscoCyberVision-center-with-DPI-4.1.1.ova	VMware OVA file, for Center with DPI setup
CiscoCyberVision-center-4.1.1.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-sensor-management-4.1.1.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-4.1.1.tar	Cisco IE3400, Cisco IR1101 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64--4.1.1.tar	Cisco IE3400, Cisco IR1101 Active Discovery sensor installation and update file
CiscoCyberVision-IOx-IC3K-4.1.1.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.1.1.tar	Cisco Catalyst 9x00 and Cisco Catalyst IR8340 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.1.1.tar	Cisco Catalyst 9x00 and Cisco Catalyst IR8340 Active Discovery sensor installation and update file
Updates	**Description**
CiscoCyberVision-Embedded-KDB-4.1.1.dat	KnowledgeDB embedded in Cisco Cyber Vision 4.1.1
CiscoCyberVision-update-center-4.1.1.dat	Center update file for upgrade from release 4.0.x or 4.1.0 to release 4.1.1
CiscoCyberVision-update-sensor-4.1.1.dat	Cisco IC3000 Sensor and Sentryo Sensor3, 5, 7 update file for upgrade from release 4.0.x or 4.1.0 to release 4.1.1
CiscoCyberVision-update-combined-4.1.1.dat	Center, IC3000 Sensor and Legacy Sensor update file from GUI for upgrade from release 4.0.x or 4.1.0 to release 4.1.1

Cisco Cyber Vision Center 4.1.1 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.html
- 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
- 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 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 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