Release Notes for Cisco Cyber Vision Release 3.2.3

Users upgrading to 3.2.x from previous versions should read the upgrade procedures 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, Scale: 20K components
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 and 9400 Series switches
Sentryo SENSOR3	Sentryo SENSOR3 hardware appliance
Sentryo SENSOR5	Sentryo SENSOR5 hardware appliance
Sentryo SENSOR7	Sentryo SENSOR7 hardware appliance

Links

Software Download

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

Center	Description
CiscoCyberVision-center-3.2.3.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-with-DPI-3.2.3.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-center-3.2.3.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-sensor-management-3.2.3.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-3.2.3.tar	IE3x00, IR1101 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-3.2.3.tar	IE3x00 sensor installation and update file with the active discovery
CiscoCyberVision-IOx-IC3K-3.2.3.tar	IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-3.2.3.tar	Catalyst 9x00 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-86-64-3.2.3.tar	Catalyst 9x00 sensor installation and update file with Active Discovery
Updates	**Description**
CiscoCyberVision-sysupgrade-3.2.3	Center and Sensor update file for upgrade from release < 3.2 to release 3.2.x
CiscoCyberVision-sysupgrade-sensor-3.2.3	Sensor update file for embedded senor in IC3000 and Sentryo SENSOR3, 5 and 7 for upgrade from release < 3.2 to release 3.2.x
CiscoCyberVision-Embedded-KDB-3.2.3.dat	KnowledgeDB embedded in Cisco Cyber Vision 3.2.2
CiscoCyberVision-update-center-3.2.3.dat	Center update file for upgrade from release 3.2.0, 3.2.1 or 3.2.2 to release 3.2.3
CiscoCyberVision-update-sensor-3.2.3.dat	Sentryo Sensor3, 5, 7 update file for upgrade from release 3.2.0, 3.2.1 or 3.2.2 to release 3.2.3
CiscoCyberVision-update-combined-3.2.3.dat	Center and Legacy Sensor update file from GUI for upgrade from release 3.2.0, 3.2.1 or 3.2.2 to release 3.2.3

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:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_GUI_User_Guide_3_2_0.pdf

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

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_Network_Sensor_Installation_Guide_for_Cisco_IE3300_10G_Cisco_IE3400_and_Cisco_Catalyst_9300_3_2_0.pdf

- Cisco Cyber Vision Network Sensor Installation Guide for Cisco IR1101:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_Network_Sensor_Installation_Guide_for_Cisco_IR1101_3_1_1.pdf

- Cisco Cyber Vision Network Sensor Installation Guide for Cisco IC3000:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_Network_Sensor_Installation_Guide_for_Cisco_IC3000_3_2_0.pdf

- Cisco Cyber Vision IC3000 Troubleshooting Guide:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_IC3000_Troubleshooting_Guide_Release_3_0_2.pdf

- Cisco Cyber Vision Center Appliance Installation Guide:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_Center_Appliance_Installation_Guide_3_2_0.pdf

- Cisco Cyber Vision Center VM Installation Guide:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_Center_VM_Installation_Guide_3_2_0.pdf

- Cisco Cyber Vision Integration Guide, Integrating Cisco Cyber Vision with Cisco Identify Services Engine (ISE) via pxGrid:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Integrating-Cisco-Cyber-Vision-with-Cisco-Identify-Services-Engine-via-pxGrid.pdf

- Cisco Cyber Vision REST API User Guide, Release 3.1.0:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_REST-API_User_Guide_Release_3_1_0.pdf

Cisco Cyber Vision 3.2.0, 3.2.1, 3.2.2 and 3.2.3 update procedure

Cisco Cyber Vision 3.2.x includes many enhancements and improvements which require changes to the underlying architecture when upgrading from release 3.1.x to release 3.2.3. These changes will affect both Centers and sensors, excluding IOx sensors (which are embedded in Catalyst 9300, 9400, IE3400, IE3300 10G, and IR1101).

These partition changes require specific update packages called “CiscoCyberVision-sysupgrade”, which will replace the usual update packages and procedures.

Center updates

All 3.1.x versions can be directly upgraded in release 3.2.x with the usage of the right upgrade package called “CiscoCyberVision-sysupgrade-3.2.3”.

Older versions (3.0.x) need to be upgraded first to release 3.1.2, then to 3.2.3.

The upgrade from 3.1.x to 3.2.3 needs to be launched from the Center Command Line Interface (CLI):

1. Send the package to the `/data/tmp` folder of the Center by using the ‘`scp`’ command.
2. Launch the update with the following command:

```
bash /data/tmp/CiscoCyberVision-sysupgrade-3.2.3
```

Sensor updates – IC3000 Sensor and Sentryo SENSOR3/5/7 cases

All 3.1.x versions can be directly upgraded in release 3.2.x with the usage of the right upgrade package called “CiscoCyberVision-sysupgrade-sensor-3.2.3”, previous versions need to be first updated to 3.1.2.

The upgrade needs to be launched from the sensor Command Line Interface (CLI):

1. Send the package to the `/data/tmp` folder of the sensor by using the ‘`scp`’ command.
2. Launch the update with the following command:

```
bash /data/tmp/CiscoCyberVision-sysupgrade-sensor-3.2.3
```

Sensor updates – Cisco IOx sensor cases

Cisco IOx sensors can be updated with the standard methods described in the relevant user manuals:

1. Cisco Cyber Vision Sensor Extension update
2. Local Manager update
3. CLI update

Cisco Cyber Vision 3.2.0, 3.2.1, 3.2.2 and 3.2.3 important changes

Communication port change

An important change was made on the communication between the sensors and the Center. In previous versions, all sensor communications were multiplexed on port TCP/443. Starting with version 3.2.0, sensors will also use port TCP/5671, in addition to port TCP/443.
In case of network architecture with firewalls between the sensors and the Center, rules will have to be updated to authorize this new port alongside port TCP/443.

API authentication

A HTTP header authentication mechanism has been added to both API v1 and v3.
Token authentication through the URL is not supported with API v3.
Token authentication through the URL is now deprecated with API v1 and will be removed in future releases.

Cisco Cyber Vision 3.2.1 important change

Center DPI Change

The update from Cisco Cyber Vision release 3.2.0 to 3.2.1 will delete all center DPI already configured. Some configuration files were changed to ensure compatibility with future releases which prevents forward compatibility for this minor release. The Center DPI needs to be recreated in the release 3.2.1.

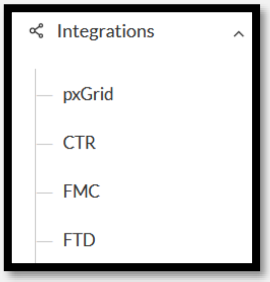
Cisco Cyber Vision 3.2.2 important change

Cisco Smart Agent Certificates Update

All Cisco Cyber Vision releases inferior to 3.2.2 contain a version of the Cisco Smart Agent with some certificates which will be revoked. Release 3.2.2 and 3.0.6 bring a new version of the Cisco Smart Agent with new certificates.

If the upgrade to release 3.2.2, 3.2.3 or 3.0.6 is not done, users may experience slowness related to licensing requests.

Cisco Cyber Vision enhancements

Issues ID / CDETS	Description
#6388 /	Cisco Cyber Vision operating system journal is now persisted after a reboot.
#6803 /	pxGrid menu was moved to the Administration / Integrations Menu 
#6862 /	Active Discovery settings are hidden in a Cisco Cyber Vision Global Center
#6883 /	Center Type and Center id are now added in the diagnostic
#6889 / CSCvx20904	Cisco Cyber Vision Sensor Management Extension now permits to change platform user and password. In release 3.2.3 this function is only available through CLI with the command 'sbs-iox-password'. This tool can update the device's password stored in the sensor management extension. If the password is modified on the device after the deployment, the Cisco Cyber Vision sensor application should still work fine but users won't be able to update or delete it. A lot of bad login events will be shown on the device. It's because the extension is trying to connect back to the device with the old password. Usage: sbs-iox-password <Local manager IP address>
#6900 /	Decode failure and exception events are now not stored in the database nor sent to syslog
#6928 /	For performance improvements activity_flow table was changed
#7113 /	Low volume and unestablished activity tags evaluation could now be disabled by configuration flags
#7114 /	Port scan detection could now be disabled by configuration flags
#7236 /	Service sbs-marmotd logs are now present in the center diagnostics
#7368 /	PostGreSQL upgraded to version12.6
#6951 /	Syslog configuration of a Global Center was updated to remove unnecessary properties
#7154 /	PostGreSQL checkpoint timeout value updated for better performance
#7421 /	sbs-db command changes to purge events, flows and variables: • 'purge-since DATE' will remove flows, events and variables since date • 'purge-until DATE' will remove flows, events and variables until date
#7567 /	DNP3 add decoding for useful device attribute objects

Cisco Cyber Vision bug fixed

Issues ID / CDETS	Description
#5242 / CSCvt81656	Arbitrary, unsigned files are copied to /system/cfg via a USB drive during boot
#6192 /	Iox sensor manual enrollment fails if serial number is entered in lowercase
#6220 /	Extensions-apid does not emit syslog events
#6244 /	Active Discovery - Wrong message on IE3x00 Configuration display
#6264 /	Hardware sensors upgraded from 3.1 to 3.2 have a wrong rsyslog configuration
#6708 /	Mismatch of total vulnerabilities numbers between dashboard and vulnerabilities page
#6875 /	Cisco Cyber Vision Center NTP service does not start if eth0 is in dhcp
#6886 /	Center DPI - Reload flow when Data Management action is not done
#6895 /	Backend panic when deleting API token with incorrect token id
#6910 /	IR1101 with firmware 17.5 generate warning
#6936 /	Profinet-io-cm information are affected to the wrong component
#7063 /	sysinfod-Sensor-handler can eat all postgresql connections
#7078 /	Cisco Cyber Vision Center ntp: invalid configuration
#7208 /	Flow vlan information are missing on data analyzed by non-iox Sensor
#7247 /	IC3000 Sensor issues with reboots due to RAM and disk full due to wrong settings
#7364 /	DeltaV too many variables are created
#7380 /	Bacnet property are limited to UTF8
#7384 / CSCvx82697	Update CiscoSSL to 7.2.225
#7407 /	Some capture filters can crash flowsf on iox sensors
#6868 /	stowd failed to handle frame from RMQ
#6882 /	sensorsyncd could fill sensor disk

Issues ID / CDETS	Description
#6636 /	When licensing process is incomplete GUI becomes very slow
#7477 /	Center DPI sbs-netconf: empty filter setting gives an “Optimal Filter” instead of a “All filter”
#7515 /	Impossible to play PCAP with flowctl on a hardware sensor without filter
#6856 /	Knowledge Base version could create trouble on LC enrolment
#7186 /	Selection badge is not visible after preset creation with network filter
#7201 /	Can't find filtered results because of the leading and trailing spaces of a string (all filters)
#7561 /	Cannot update Knowledge Base on an unenrolled center
#7400 /	Unhandled layer over HSR or Vlan802.1Q gives a decode errors
#7516 /	DeltaV variable values, a new parameter was added to flow configuration to enable unmapped variable export

Cisco Cyber open CDETS and known issues

Issues ID / CDETS	Component	Description
#5695 / CSCvv49682	IC3000	Cisco Cyber Vision Sensor installation with extension fails with IC3000 release 1.3.1. Local Manager installation or USB installation should be used.
# - / CSCvv48350	IC3000	Multicast packets are dropped by the platform before Cisco Cyber Vision Application.