Release Notes for Cisco Cyber Vision Release 4.0.2

For users upgrading to 4.0.2 from previous versions, please carefully read the Cisco Cyber Vision 4.0.2 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 4.0.2 update procedure

Cisco Cyber Vision 4.0.2 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 4.0.2. Versions 4.0.0 and 4.0.1 can be updated to 4.0.2.

Upgrade Path to Cisco Cyber Vision 4.0.2

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 4.0.2
Version 3.2.4	Upgrade first to 4.0.0 then to 4.0.2
Version 4.0.0 and 4.0.1	You can upgrade directly to Release 4.0.2

Data purge

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

The new data retention policies introduced in 4.0.0 are still valid in 4.0.2. 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-4.0.2.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-4.0.2.dat
        - Launch the update with the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-center-4.0.2.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-4.0.2.dat
            - Launch the update with the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-sensor-4.0.2.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-4.0.2.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-4.0.2.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-aarch64-4.0.2.tar or CiscoCyberVision-IOx-Active-Discovery-aarch64--4.0.2.tar
      - Catalyst 9300 and 94000 files = CiscoCyberVision-IOx-x86-64-4.0.2.tar or CiscoCyberVision-IOx-Active-Discovery-x86-64-4.0.2.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-4.0.2.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-4.0.2.dat
        - Launch the update with the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-center-4.0.2.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-4.0.2.dat
            - Launch the update with the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-sensor-4.0.2.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-4.0.2.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-4.0.2.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-aarch64-4.0.2.tar or CiscoCyberVision-IOx-Active-Discovery-aarch64--4.0.2.tar
            - Catalyst 9300 and 9400 files = CiscoCyberVision-IOx-x86-64-4.0.2.tar or CiscoCyberVision-IOx-Active-Discovery-x86-64-4.0.2.tar.

Cisco Cyber Vision 4.0.2 important change

Communication port and protocol changes

Port

There is no port change in Cisco Cyber Vision 4.0.2. All TCP or UDP ports already used are kept, and no new port number is needed.

Protocol

No modification in 4.0.2.

API

No modification in 4.0.2.

SYSLOG

No modification in 4.0.2.

Cisco Cyber Vision new features and improvements

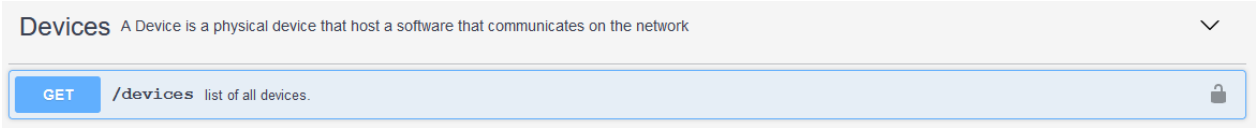
Device engine improvements

Cisco Cyber Vision 4.0.2 uses Siemens hardware serial numbers and Ethernet/IP property “enip-serial” to consolidate devices.

API – add Devices route in API 3.0 to find all devices

In Cisco Cyber Vision 4.0.2, an API call to do a bulk retrieval of all devices independently of the presets was added.

Cisco Cyber Vision API 3.0 swagger – Devices route

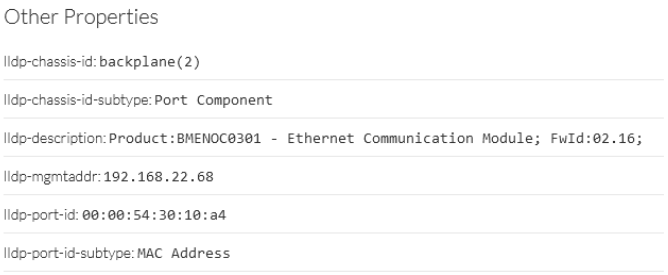


Improvements of devices/components properties

Schneider LLDP properties added to normalized properties

Cisco Cyber Vision 4.0.2 uses Schneider LLDP properties to enrich components.

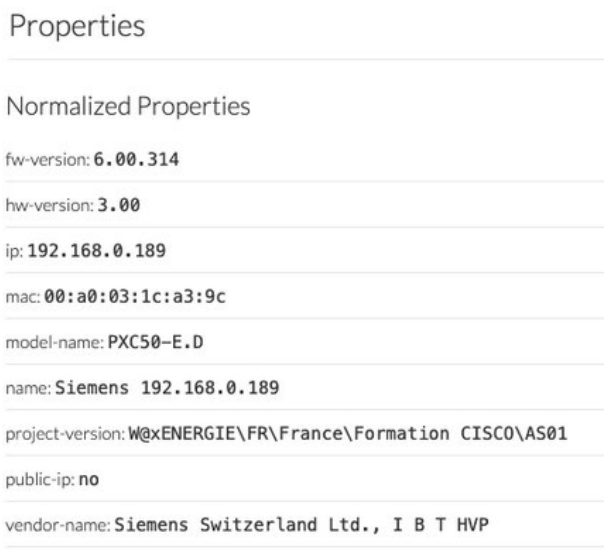
Cisco Cyber Vision Schneider LLDP properties



Siemens BACnet normalized properties enhancements for vulnerability matching

Cisco Cyber Vision 4.0.2 improves handling of Siemens BACnet properties to let the system match vulnerabilities.

Cisco Cyber Vision Siemens BACnet properties



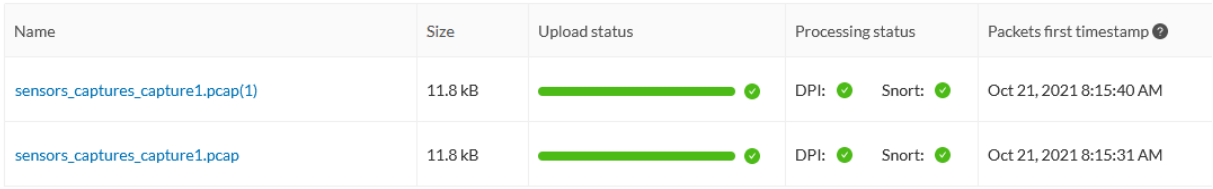
Limit Monitor Baseline maps to be opened when they have too many components

In Cisco Cyber Vision 4.0.2, the system enforces a size limit for maps displayed in the Monitor menu.

PCAP upload enhancements

In Cisco Cyber Vision 4.0.2, the same PCAP file can be uploaded several times, and the PCAP list will be cleaned when the user purges all data of the Center.

Cisco Cyber Vision PCAP upload menu



Center diagnostic files enhancements

In Cisco Cyber Vision 4.0.2, the Center DPI logs, and the authorized network configuration are added in the diagnostic file. Authorized networks are configured during the Center initial configuration and define which subnet are authorized to reach the center Access/Admin interface and defaults to all networks.

RabbitMQ updated

RabbitMQ has been updated to version 3.8.23.

Cisco Cyber Vision Resolved Caveats

Issues ID / CDETS	Description
#5119 /	Some password fields have now the autocomplete disabled
#8192 / CSCvy83325	Sensor deployments with sensor management extension fixed on redundant catalysts
#8298 /	Remove disk type from the Statistics page
#8407 /	Setup-center.py does not restart systemd-network which creates error when DHCP is used
#8599 / CSCvz38511	Cyber Vision ISE integration - Center now sends pxgrid updates for Device group changes
#8648 /	Change login error messages to improve security
#8666 /	Change text on some Sensor deployment pages, add “Center collection IP”
#8677 / CSCvz50904	Smart agent fault with SLR licenses fixed
#8827 /	Burrow failed to insert because of maximum value of “pending_modification_id_seq”
#8846 /	Cyber Vision ISE integration - ISE Pxgrid connection issues. A pxgrid json limit of 4025 bytes was sometime reached. Cyber Vision center now limits the json file to 4025 bytes.
#8864 /	Cyber Vision user interface flow content statistic “tls-extensions” field is now added on 2 lines
#8936 /	Cyber Vision Global Center sometime stops handling data from some Local Centers
#6203 /	License page did not show details when in SLR mode, snort subscriber rules license is missing with Center DPI activated
#7869 /	Licensing: in SLR mode, the system doesn’t have to count sensor or center DPI with snort, if subscriber rules are not enabled
#8302 /	Internet gateways are now no more "rediscovered" and no new event are sent every hour
#2510 /	User Product Role rights need were adjusted
#6128 /	Siemens S7: false positive detection of a "Program upload" tag
#7449 /	Cyber Vision Global Center vulnerabilities acknowledge/Unacknowledge should not be available
#7829 /	Center sensor statistics page, the graph for packets captured misleading
#7887 /	Flow DPI; handle the case of SMB Session Setup AndX Request (0x73) with word count = 13

Issues ID / CDETS	Description
#7938 /	Check minor version during system restore
#7940 /	Improve Flow memory usage
#7980 /	Activity tech sheet can't be opened from Calendar, 500 error on GET flows
#8064 /	Errors in Cyber Vision local center administration page with user role "Product"
#8088 /	ISE integration - The first pxgrid synchronization does not occur after a pxgrid-agent restart
#8110 /	Sensor capture files cannot be retrieved if file is too large on iox devices
#8157 /	Global center - Don't show Risk Score in the administration menu
#8161 /	Risk Score table display issue (too large)
#8176 /	Center folder size per folder or partition displays incoherent data
#8177 /	User interface Map - Nothing is displayed if hard limit is equal of number of edges or nodes
#8188 /	Multiple calls on Preset Dashboard visualization
#8274 /	Device CSV exports have a bad title on column 2
#8279 /	User interface Explore menu - Number of tags not refreshed in the preset filters
#8328 /	Setup center network is sometime blocked at boot when upgrading to 4.0.0
#8333 /	mDNS flows use wrong tag and wrong analyzer
#8405 /	Removing unenrolled IOx sensors must be done twice
#8411 /	Event page – Sometime an error appears on event filtering
#8432 /	Cisco Cyber Vision Center - adjust oom killer
#8435 /	Center reboots are now safer during upgrades
#8662 /	SecureX feedbacks on incident formats
#8709 /	Preset materialized views initialization fails after a new center deployment

Issues ID / CDETS	Description
#8712 /	SNMPv3 process failed on Sensors
#8714 /	Center - Marmotd stops and does not restart
#8844 /	API route “/api/3.0/flowContent” always returns a 404 error
#8901 /	Center - rabbitmq queues for flowtables are now more lazy
#8907 / **CSCvz79589**	Snort MODBUS preprocessor issue fix
#8965 /	Variables make marmotd consume a lot of RAM, even when variables are not stored

Cisco Cyber Vision Open Caveats

Issues ID / CDETS	Component	Description
CSCwa14510	Centers	Cyber Vision Device engine 4.0.2 breaks Rockwell chassis into several devices
CSCwa14472	Centers	Cyber Vision User Interface LDAP login is no more possible with 4.0.2.
CSCvy30877	Centers	RPC-DCOM flows often not tagged: cannot selectively delete and appear in security insights
CSCwa14488	Centers	Cyber Vision sensor in IC3000 - NTP service sometime fails

Links

Software Download

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

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

Cisco Cyber Vision Center 4.0.2 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