Release Notes for

Cisco Cyber Vision

Release 5.0.1

September 2024

Contents

Compatible device list 3
Unsupported device list 4
Cisco Cyber Vision 5.0.1 update procedure 5
Upgrade to 5.0.1 considerations – To read before updating 5
Upgrade path 7
Compatibility Guidelines 7
Data purge 8
System updates - Preliminary checks 9
System updates – Cyber Vision system from 4.4.x to 5.0.x 10
System updates – Cyber Vision system from 4.3.x to 5.0.x 16
AWS and Azure Centers 19
Cisco Cyber Vision 5.0.1 important changes 20
Communication port and protocol changes 20
API 20
SYSLOG 20
Cisco Cyber Vision new features and improvements 21
Zone and conduits 21
DPI changes 22
Cisco Cyber Vision 5.0.1 other enhancements 22
Cisco Cyber Vision 5.0.1 Resolved Caveats 23
Cisco Cyber Vision Open Caveats 23
Links 24
Software Download 24
Related Documentation 26

Compatible device list

Table 1. 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 2. 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 IR1800**	17.15.1	17.15.1	Cyber Vision Sensor IOx application hosted in Cisco IR1800 Rugged Series 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, 9300L, 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 IR1835 with IOS 17.15 supports up to 3GB of memory allocated to IOX.
*** 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 3. Sentryo centers (end of life)

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

Table 4. 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 5.0.1 update procedure

Cisco Cyber Vision 5.0.1 update procedure depends on the architecture deployed and the tool used to deploy it.

Upgrade to 5.0.1 considerations – To read before updating

Four important considerations need to be understood before upgrading a system to 5.0.1.

Consideration 1

Upgrading to 4.3.0 is mandatory before upgrading to 5.0.1 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 5.0.1.

During the Center upgrade to 5.0.1, 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 and 5.0.x.

To upgrade to version 5.0.1, 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:

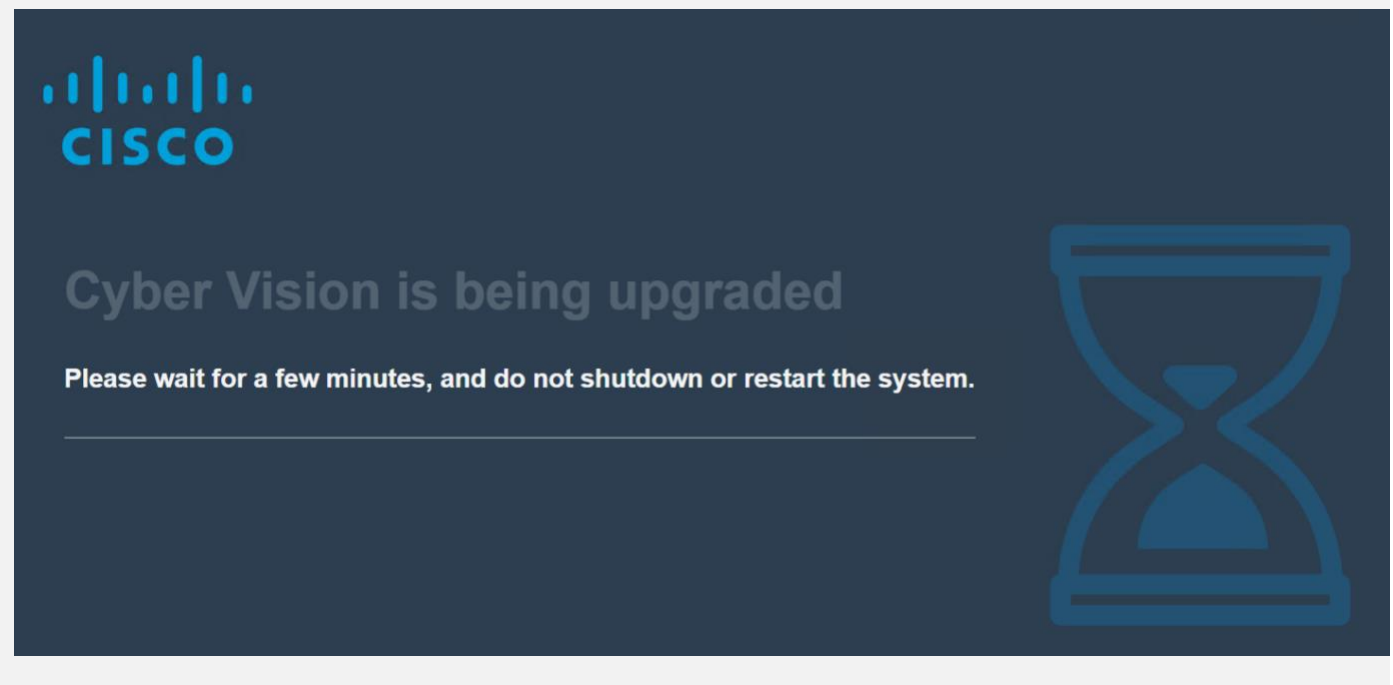

Figure 2.
Cisco Cyber Vision upgrade considerations – upgrade warning

Upgrade path

Table 5. Upgrade Path to Cisco Cyber Vision 5.0.1

Current Software Release	Upgrade Path to Release 5.0.1
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 5.0.1
Version 3.2.4	Upgrade first to 4.0.0, then to 4.1.4, then to 4.3.0, then to 5.0.1
Version 4.0.0 to 4.0.3	Upgrade first to 4.1.4, then to 4.3.0, then to 5.0.1
Version 4.1.0 to 4.1.4	Upgrade first to 4.3.0, then to 5.0.1
Version 4.2.0 to 4.2.6	Upgrade first to 4.3.0 and then to 5.0.1
Version 4.3.0 to 4.3.3	Upgrade directly to 5.0.1
Version 4.4.0 to 4.4.3	Upgrade directly to 5.0.1
Version 5.0.0	Upgrade directly to 5.0.1

For the upgrade to any previous release (i.e. 4.3.0), please read carefully the Release Notes of the corresponding release available here: Cyber Vision release notes.

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 5.0.0 can manage local Centers with versions 5.0.0 and 4.4.x).
- Center with synchronization (Version N): Compatible with sensors with versions N and N-1

  (e.g., Center with synchronization version 5.0.0 can manage sensors with versions 5.0.0 and 4.4.x).

Data purge

The Center database is regularly maintained to contain the volume of data stored.

The data retention policies are, by default, in version 5.0.1:

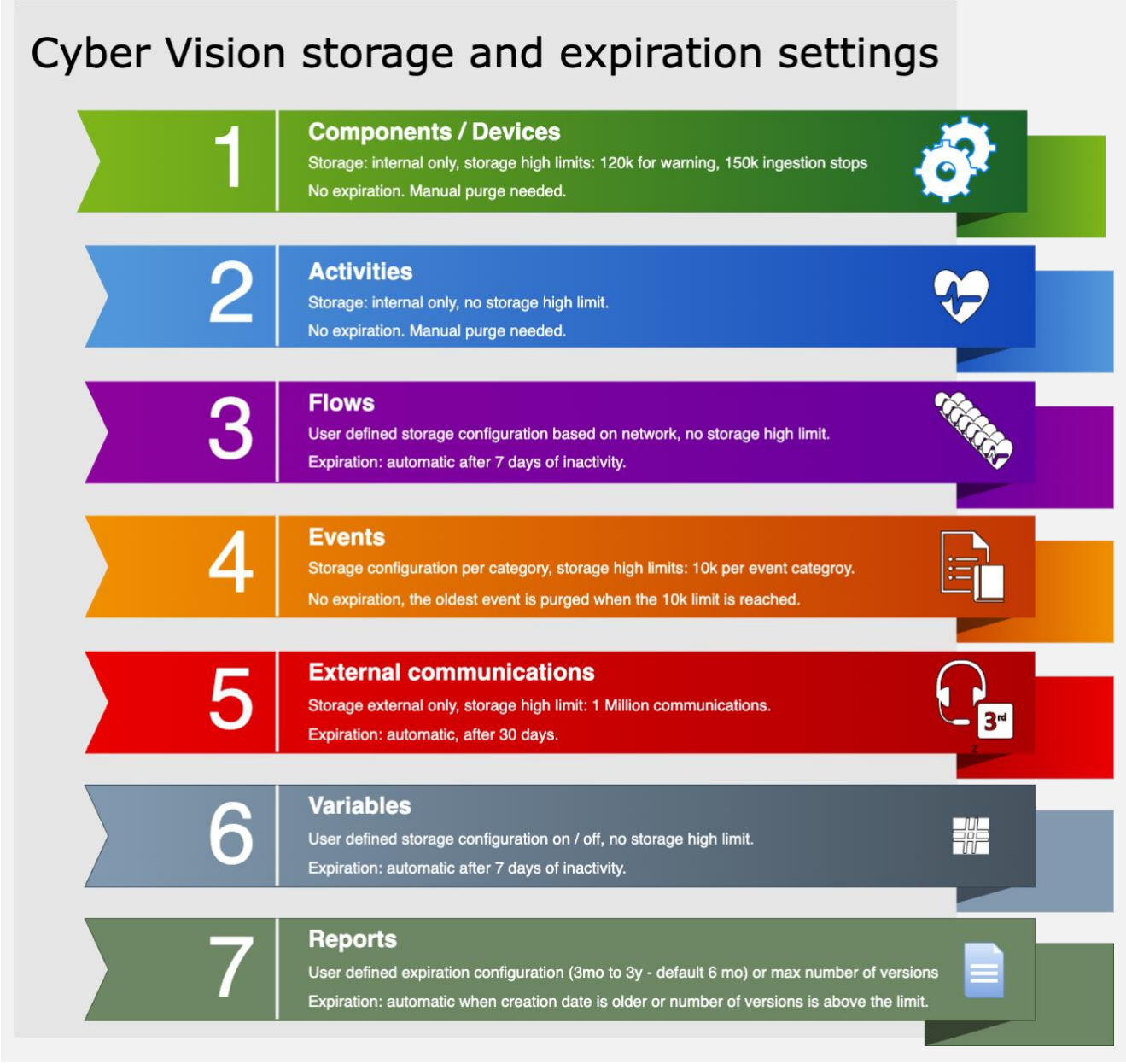

Figure 3.
Cisco Cyber Vision data retention policies

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.

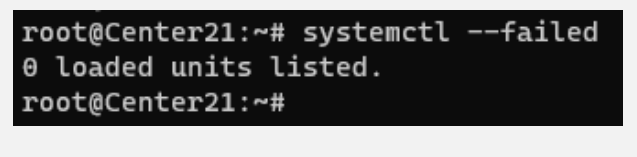

Figure 4.
Cisco Cyber Vision system check – 0 failure

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

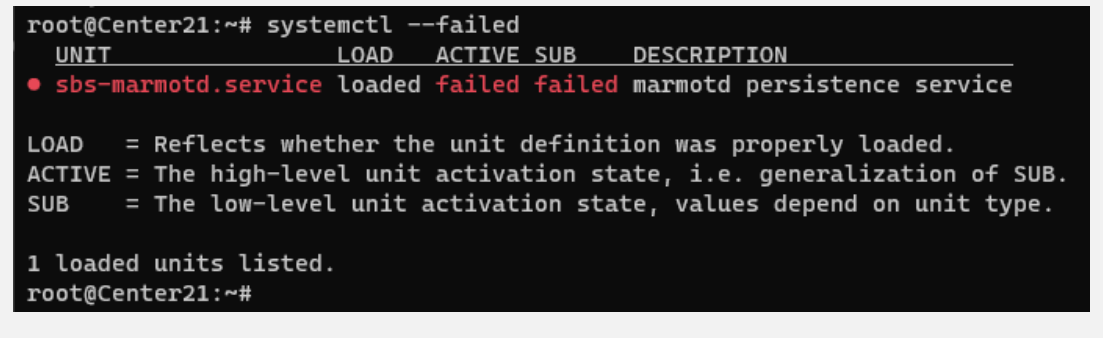

Figure 5.
Cisco Cyber Vision system check – example of failure

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

System updates – Cyber Vision system from 4.4.x to 5.0.x

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 different extensions installed:
    a. If you installed the sensor management extension, upgrade the extension:
        - 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
```

    b. If you installed the report management extension, upgrade the extension:
        - File = CiscoCyberVision-report-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 report management extension can also be updated from the CLI with the command:

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

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

Update all sensors with the sensor self-update feature. Cisco Cyber Vision now allows sensor updates regardless of the install method (i.e., without the extension). Release 4.4.0 provides the necessary foundation for sensor self-updates. Starting with Cisco Cyber Vision release 4.4.1, you can update all sensors automatically. The required steps are:

- Select sensors to update.
- The Center adds a new job to the sensor queue.
- The sensor automatically collects and validates the update file.
- The sensor restarts with the new version.

To do so: navigate to **Admin > Sensors > Sensor Explorer** and select the different sensors you would like to update, or all sensor with the top left check box:

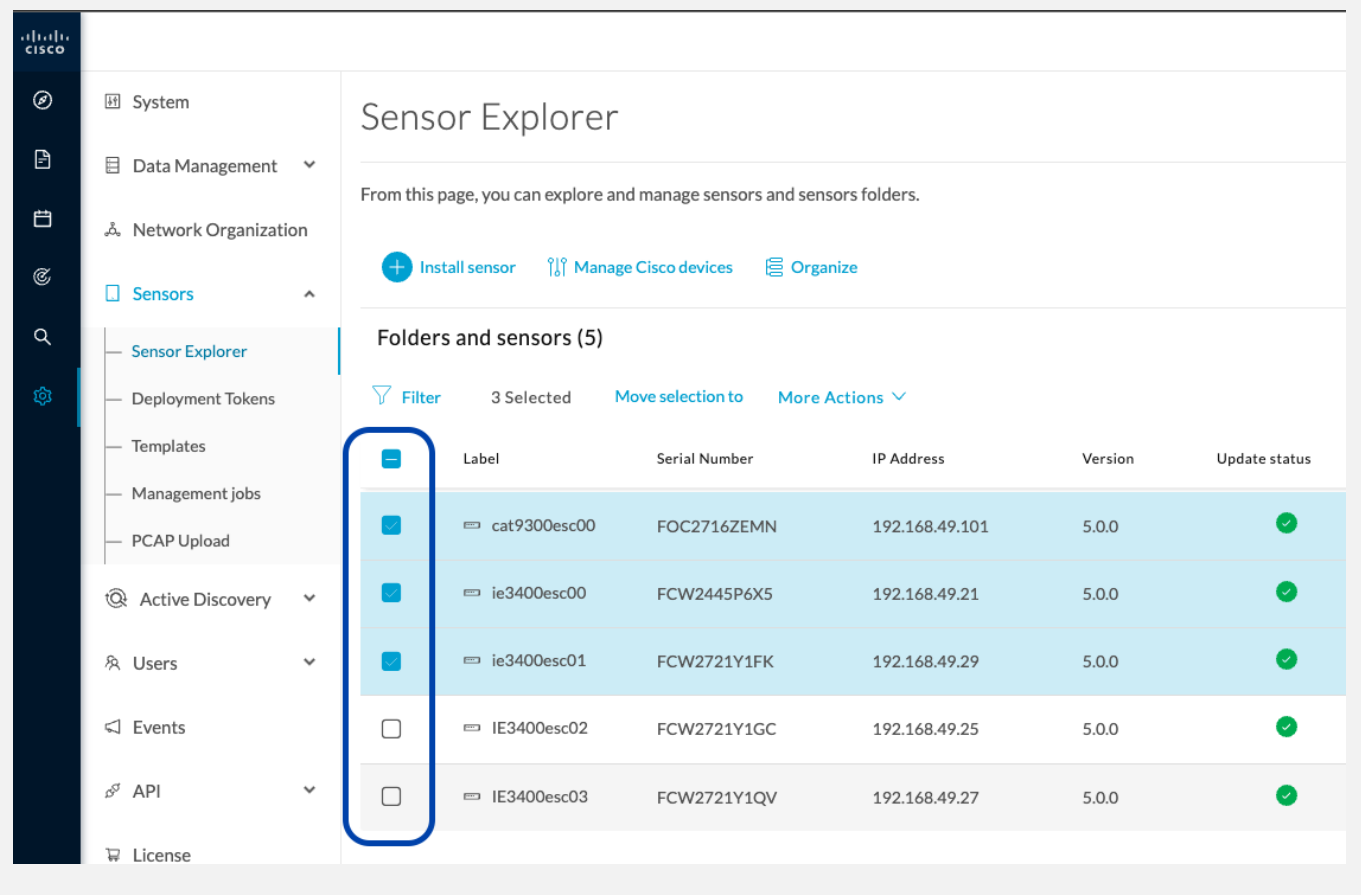

Figure 6.
Cisco Cyber Vision sensor to update selection

Then use the menu, **More Actions > Update sensors** it will open a menu to proceed to the update:

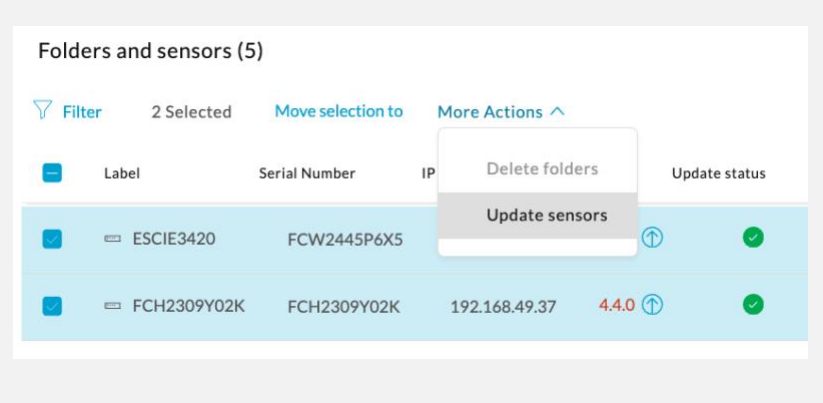

Figure 7.
Cisco Cyber Vision Update sensors menu

For a complete procedure, use any sensor installation guide from version 5.0.0 or later.

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

5. Update the Cyber Vision Knowledge Data Base (KDB) from the Global Center.

Once the global center and the local centers are deployed, the Cyber Vision Knowledge Data Base (KDB) must be updated to refresh the data used by the product. Centers use KDB content to calculate vulnerabilities, to communicate snort rules to IDS sensors, and to display tags in the user interface. Maintaining the KDB up to date will fix some defects, add update rules and properties which will enrich the data presented. It is highly recommended to keep the KDB up to date.
The KDB update is available on the Global Center. The latest KDB is downloaded from Cisco Cyber Vision software download page and the import is made from the Admin menu and click on the button 'Import a Knowledge DB'.

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 different extensions installed:
    a. If you installed the sensor management extension, upgrade the extension:
        - 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
```

    b. If you installed the report management extension, upgrade the extension:
        - File = CiscoCyberVision-report-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 report management extension can also be updated from the CLI with the command:

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

3. Update sensors

Update all sensors with the sensor self-update feature. Cisco Cyber Vision now allows sensor updates regardless of the install method (i.e., without the extension). Release 4.4.0 provides the necessary foundation for sensor self-updates. Starting with Cisco Cyber Vision release 4.4.1, you can update all sensors automatically. The required steps are:

- Select sensors to update.
- The Center adds a new job to the sensor queue.
- The sensor automatically collects and validates the update file.
- The sensor restarts with the new version.

To do so: navigate to **Admin > Sensors > Sensor Explorer** and select the different sensors you would like to update, or all sensor with the top left check box:

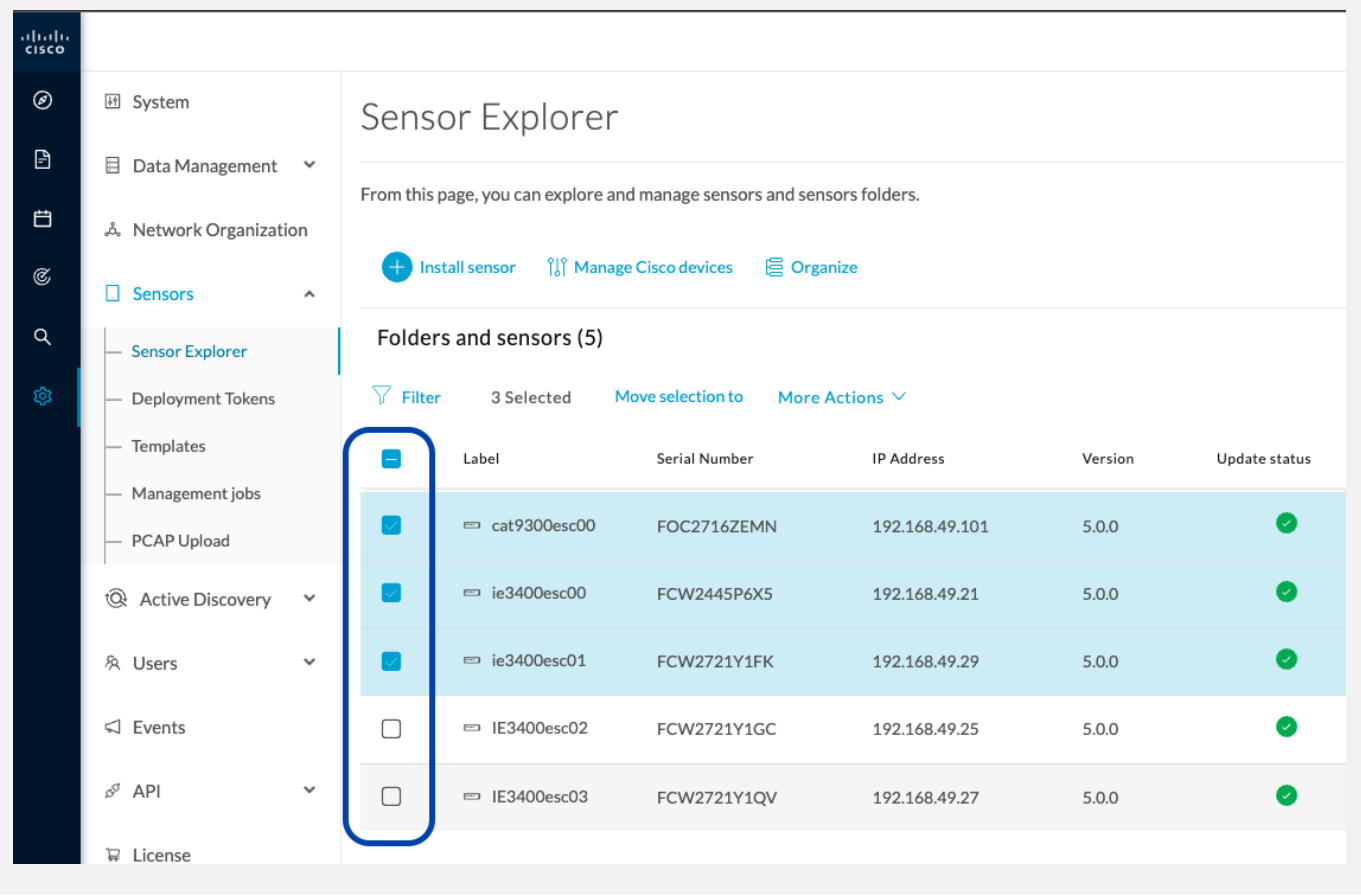

Figure 8.
Cisco Cyber Vision sensor to update selection

Then use the menu, **More Actions > Update sensors** it will open a menu to proceed to the update:

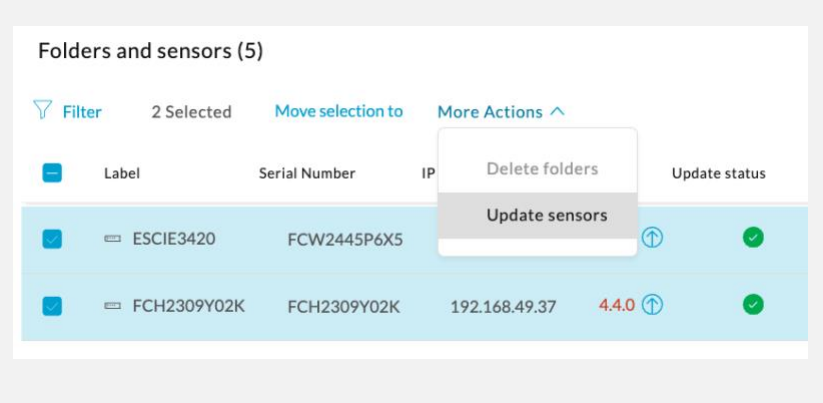

Figure 9.
Cisco Cyber Vision Update sensors menu

For a complete procedure, use any sensor installation guide from version 5.0.0 or later.

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

4. Update the Cyber Vision Knowledge Data Base (KDB) from the Global Center.

Once the center is deployed, the Cyber Vision Knowledge Data Base (KDB) must be updated to refresh the data used by the product. Centers use KDB content to calculate vulnerabilities, to communicate snort rules to IDS sensors, and to display tags in the user interface. Maintaining the KDB up to date will fix some defects, add update rules and properties which will enrich the data presented. It is highly recommended to keep the KDB up to date.
The latest KDB is available on Cisco Cyber Vision software download page and the import is made from the Admin menu and click on the button ‘Import a Knowledge DB’.

System updates – Cyber Vision system from 4.3.x to 5.0.x

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

5. 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
```

6. 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 5.0.1 important changes

Communication port and protocol changes

Port

No modification in 5.0.1.

Protocol

No modification in 5.0.1.

API

Some changes were made in release 5.0.1. Several API routes changed:

New endpoints - No modification in 5.0.1.

New attributes - No modification in 5.0.1.

Removed endpoint - No modification in 5.0.1.

Changed endpoints – one modification in 5.0.1.

/api/3.0/presets/{preset_id}/visualisations/graph/{format} was changed.

- Before 5.0.1, value answer was having nodes and edges directly at the top-level of the json.
- 5.0.1 due to the new feature “zone and conduits” is having a sub-object which includes nodes and edges.

Before 5.0.1:

```
{
    "nodes": [{}, {}],
    "edges": [{}, {}, {}, {}]
}
```

After 5.0.1:

```
{
    "graph": {
        "nodes": [{}, {}],
        "edges": [{}, {},{}, {}]
    }
```

SYSLOG

No modification in 5.0.1.

Cisco Cyber Vision new features and improvements

Zone and conduits

Cyber Vision preset maps are having limitations in terms of number of objects which can be displayed at the same time. It's done for performance purposes, for example to avoid freezing web browsers.

For large datasets and for users who don't need to have all details, a new option is now available to display only groups. It will show only the top-level groups of the group hierarchy (zones) and a summary of activities between top-level groups (conduits).

With a group hierarchy defined to segment control system the new map option could display zones and conduits as it is described in ISA/IEC 62443 series of standards.

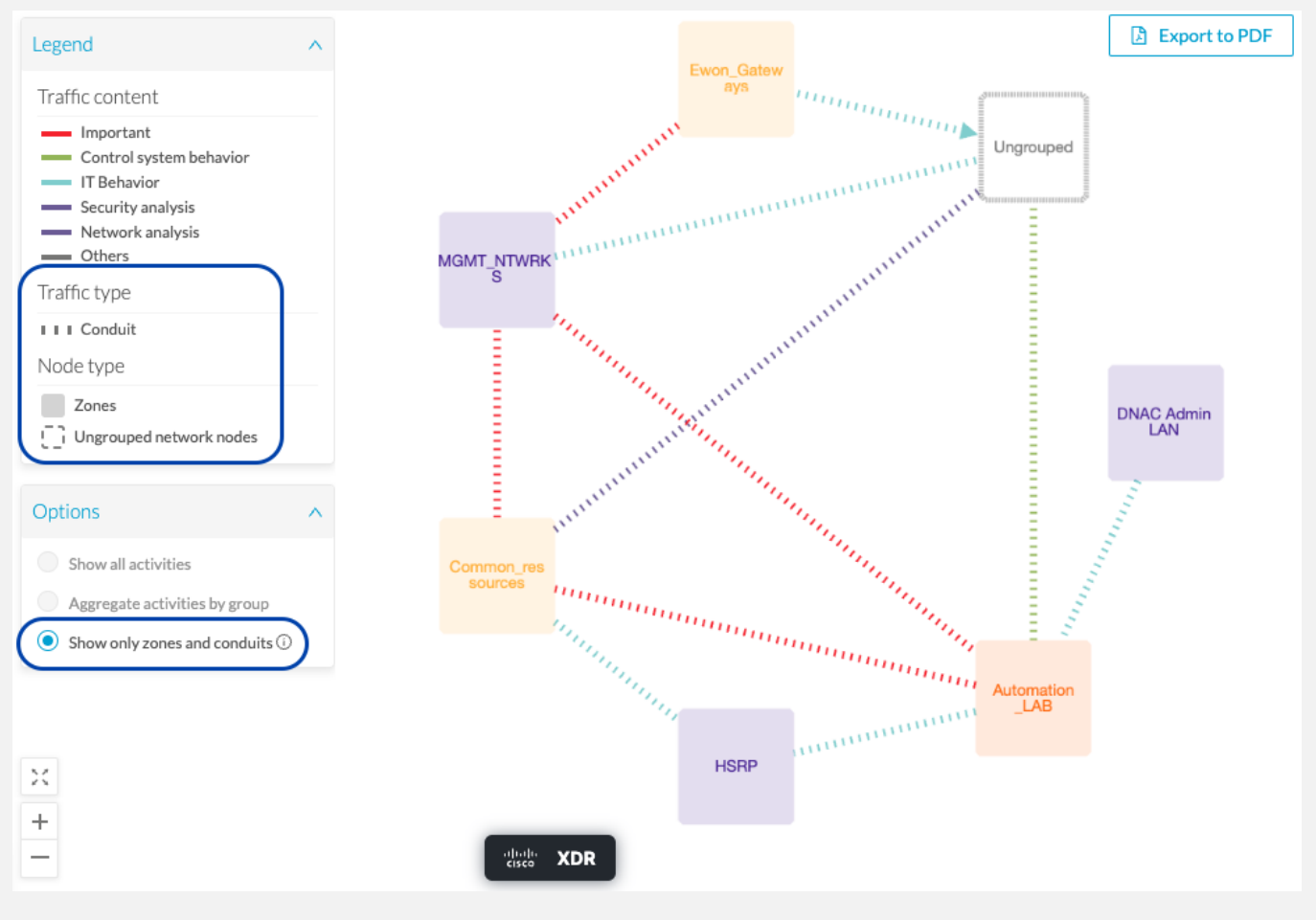

Figure 10.
New zones and conduits map option

DPI changes

New Protocols

Added new Rodaways protocol (disabled by default):

- Traffic Signals: Dotab3418e
- Message Signs： DotSignView, DotSignLink
- Ramp Metering: DotRmsRev8, DotRmsURMS, DotRmsTOS, DotRmsOCRMS
- Highway Advisory Radio: HarDCC
- Misc Data collection: PeekADR, Iteris and IterisVelocity

Protocol enhancements

- add onvif detection over http
- let http traffic discovery use dynamic discovery including on low ports (<1024)
- handle also Wavetronix SS105 data format for Radars
- new SNMP engine with property matching autoupdate from KDB
- Fully rework OMRON (obsoleted design)

Cisco Cyber Vision 5.0.1 other enhancements

Table 6. Cisco Cyber Vision other enhancements

CDETS	Description
-	Avoid displaying public icon on release greater than 5.0.1 16138
-	MAC OUI update 16370
-	Setup center: rework dns 16150

Cisco Cyber Vision 5.0.1 Resolved Caveats

Table 7. Cisco Cyber Vision resolved caveats

CDETS	Description
	GC update does not push embedded KDB to LCs 15872
CSCwk47711	API route networknode-list is having an empty "otherproperties" field
CSCwk47710	sbs-backup is not working with sensor management disabled
	HTTP-backend panic on logs after UndeployApp failure 16156
	[API] Deployments endpoints minor issues 16199
CSCwk58619	IC3000 sensor self-update fails because of Secure storage timeout
CSCwk58618	IC3000 sensor self-update fails because of process not terminated
CSCwk58617	Sensor logs overlap
	Internal error on sensor deletion after Center upgrade 16255
	Time boundaries get stuck in explore mode 16269
CSCwk85244	IC3000 sensor reassembly issue - 100% drop
	Select All Sensor doesn't consider sensors with duplicate names 16290
CSCwk85243	sysinfo can fail to be collected in sensors
CSCwk81878	Disk filled by postres pgsql_tmp files when integration with ISE is used
CSCwk90020	Vulnerabilities still displayed after device FW update
CSCwm01243	Single quote in sensor name break update to 5.0.0
	Active discovery: Missing interface field for IC3K 16552
CSCwm26218	dns_requests purge jobs can take all available slots
	Fix certificate revoke on single interface 16582
	Improve purge performances of dns_requests table 16577
CSCwk90020	Vulnerabilities still displayed after device fw update
	Too many Secure X logs 16251

Cisco Cyber Vision Open Caveats

Table 8. Cisco Cyber Vision open caveats

CDETS	Component	Description
CSCwk39764	Center	License expired redirection prevents from disabling snort

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 5.0.1 center files

Center	Description
CiscoCyberVision-center-5.0.1.ova	VMware OVA file, for Center setup
CiscoCyberVision-center-with-DPI-5.0.1.ova	VMware OVA file, for Center with DPI setup
CiscoCyberVision-center-5.0.1.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-reports-management-5.0.1.ext	Reports management extension installation file
CiscoCyberVision-sensor-management-5.0.1.ext	Sensor management extension installation file

Table 10. Cisco Cyber Vision 5.0.1 sensor files

Sensor	Description
CiscoCyberVision-IOx-aarch64-5.0.1.tar	Cisco IE3400, Cisco IE3300 10G, Cisco IE9300, Cisco IR1101, Cisco IR1800 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64--5.0.1.tar	Cisco IE3400, Cisco IE3300 10G, Cisco IE9300, Cisco IR1101, Cisco IR1800 Active Discovery sensor installation and update file
CiscoCyberVision-IOx-IC3000-5.0.1.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-IC3000-5.0.1.tar	Cisco IC3000 Active Discovery sensor installation and update file
CiscoCyberVision-IOx-x86-64-5.0.1.tar	Cisco Catalyst 9x00 and Cisco Catalyst IR8340 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-x86-64-5.0.1.tar	Cisco Catalyst 9x00 and Cisco Catalyst IR8340 Active Discovery sensor installation and update file

Table 11. Cisco Cyber Vision 5.0.1 update files

Updates	Description
CiscoCyberVision-Embedded-KDB-5.0.1.dat	KnowledgeDB embedded in Cisco Cyber Vision 5.0.1
CiscoCyberVision-update-center-5.0.1.dat	Center update file for upgrade from release 4.3.x to release 5.0.1 (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**.