Release Notes for

Cisco Cyber Vision

Release 4.4.0

May 2024

Contents

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 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, 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 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 4.4.0 update procedure

Cisco Cyber Vision 4.4.0 update procedure depends on the architecture deployed and the tool used to deploy it.

Upgrade to 4.4.0 considerations – To read before updating

Four important considerations need to be understood before upgrading a system to 4.4.0.

Consideration 1

Upgrading to 4.3.0 is mandatory before upgrading to 4.4.0 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 4.4.0.

During the Center upgrade to 4.4.0, 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:

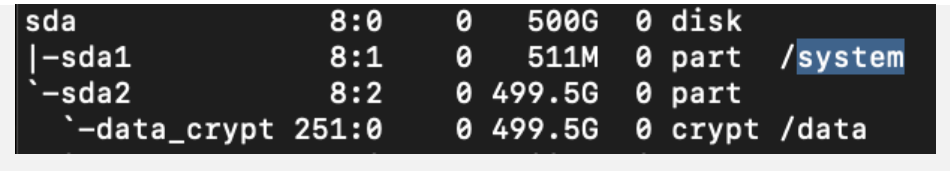

Figure 1.
Cisco Cyber Vision system check – partition size

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 4.4.0.

To upgrade to version 4.4.0, 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:

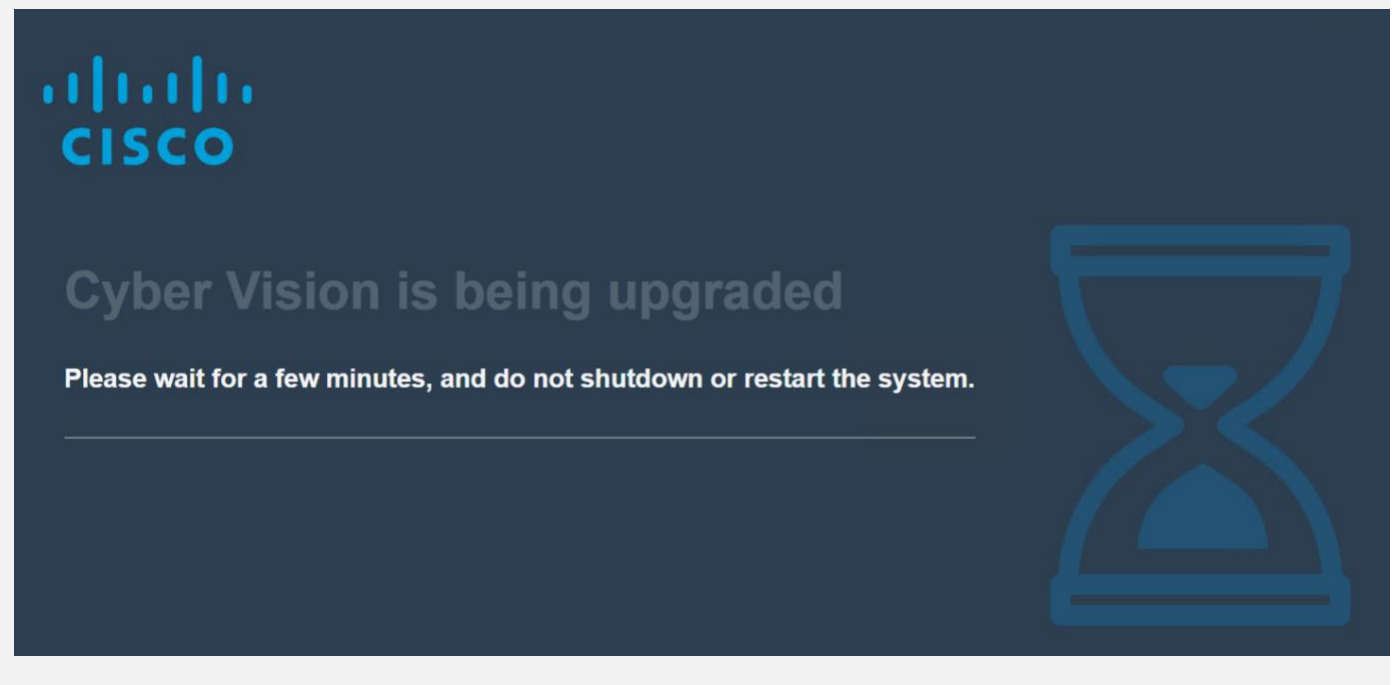

Figure 2.
Cisco Cyber Vision upgrade considerations – upgrade warning

Upgrade path

Table 5. Upgrade Path to Cisco Cyber Vision 4.4.0

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

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 4.2.0 can manage local Centers with versions 4.2.0 and 4.1.4).
- Center with synchronization (Version N): Compatible with sensors with versions N and N-1

  (e.g., Center with synchronization version 4.2.0 can manage sensors with versions 4.2.0 and 4.1.4).

Data purge

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

The data retention policies are, by default, in version 4.4.0:

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.

```
root@Center21:~# systemctl --failed
0 loaded units listed.
root@Center21:~#
```

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.

```
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:~#
```

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

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

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 4.3.0
Cisco Cyber Vision Network Sensor Installation Guide for Cisco IR8340, Release 4.3.0
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 4.3.0

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 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 4.3.0
Cisco Cyber Vision Network Sensor Installation Guide for Cisco IR8340, Release 4.3.0
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 4.3.0

AWS and Azure Centers

For a Center deployed in AWS or Azure, follow the procedure described in Architecture with one Center.

Cisco Cyber Vision 4.4.0 important changes

Communication port and protocol changes

Port

No modification in 4.4.0.

Protocol

No modification in 4.4.0.

API

Some changes were made in release 4.4.0. Several API routes changed:

New endpoints - No modification in 4.4.0.

New attributes - No modification in 4.4.0.

Removed endpoint - No modification in 4.4.0.

Changed endpoints

- Presets: The following key-value pair is removed from 4.4.0: "storageStatus": "string"
- Sensor Explorer: Response Body is changed in 4.4

```
"updateStatus": {
  "failed": 0,
  "na": 0,
  "pending": 0,
  "updating": 0,
  "uploading": 0
}
```

- Reports: reports-metadata – POST, payload changed:

```
{
"description": "string",
"filter_id": "string",
"filter_type": "string",
"logo_id": "string",
"name": "string",
"output_type": [
"string"
],
"sections": [
{
"section_id": "string",
"sub_section_ids": [
"string"
]
}
],
"type": "string"
}
```

SYSLOG

No modification in 4.4.0.

Cisco Cyber Vision new features and improvements

ISE integration enhancement

The link between Cisco Cyber Vision and ISE is aimed to create endpoints in ISE based on Cisco Cyber Vision's components. pxGrid is used to publish discovered components as endpoints in ISE.

Cisco Cyber Vision components are created and maintained in ISE with the following rules:

- Component selection based on subnets selected in Cisco Cyber Vision.
- Component aggregation based on MAC addresses.
- 2 IP addresses maximum per MAC address. MAC address with more than 2 IP addresses will not be sent.
- Refresh of Cisco Cyber Vision components' properties as they are updated.
- A list of properties is sent from Cisco Cyber Vision to ISE. Some are predefined properties in ISE, others need to be created manually.

The synchronization is done thanks to two mechanisms:

- Pull: Cisco Cyber Vision sends all changes on the fly (new component, new property, property change).
- Push: Cisco ISE requests all relevant components and their properties regularly to adapt the whole database.

Version 4.4.0 brings several changes:

- Configuration page enhancement
- Stability enhancement
- Subnet selection

ISE – pxGrid integration setting page enhanced

The Cisco Cyber Vision pxGrid integration page was enhanced for a better user experience.

New clear statuses are now available for pull and push services:

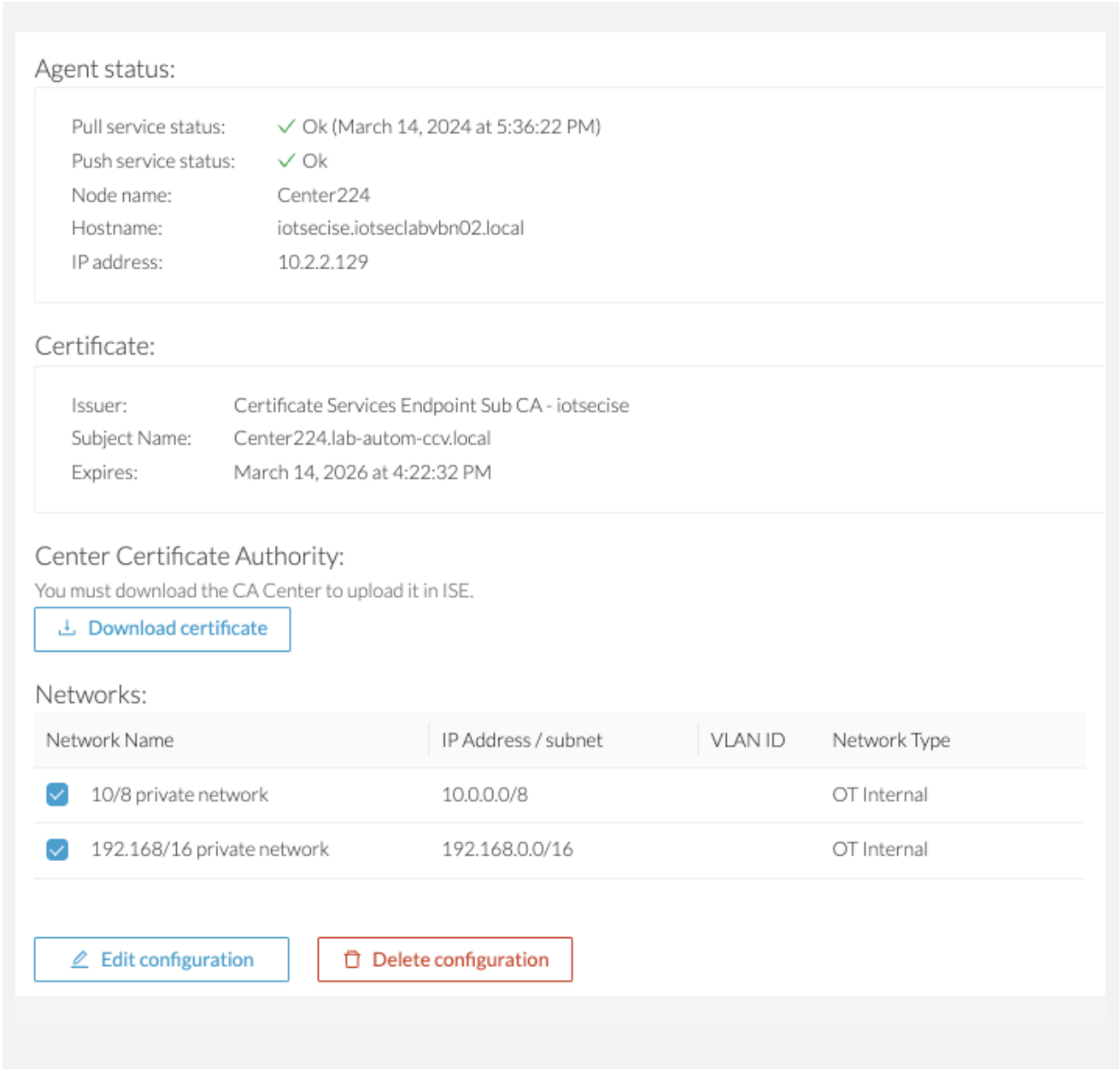

Figure 6.
Cisco Cyber Vision ISE integration – new integration page

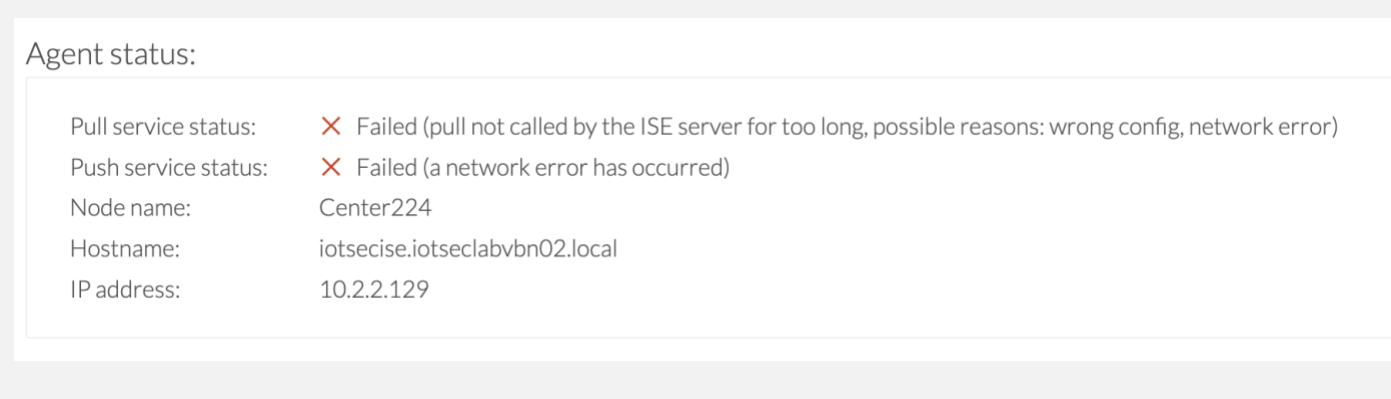

Figure 7.
Cisco Cyber Vision ISE integration – error

ISE integration – subnet selection

Cisco Cyber Vision Center integration with Cisco ISE now offers a way to filter the components sent to ISE. The user can select the different subnets they would like to synchronize with ISE:

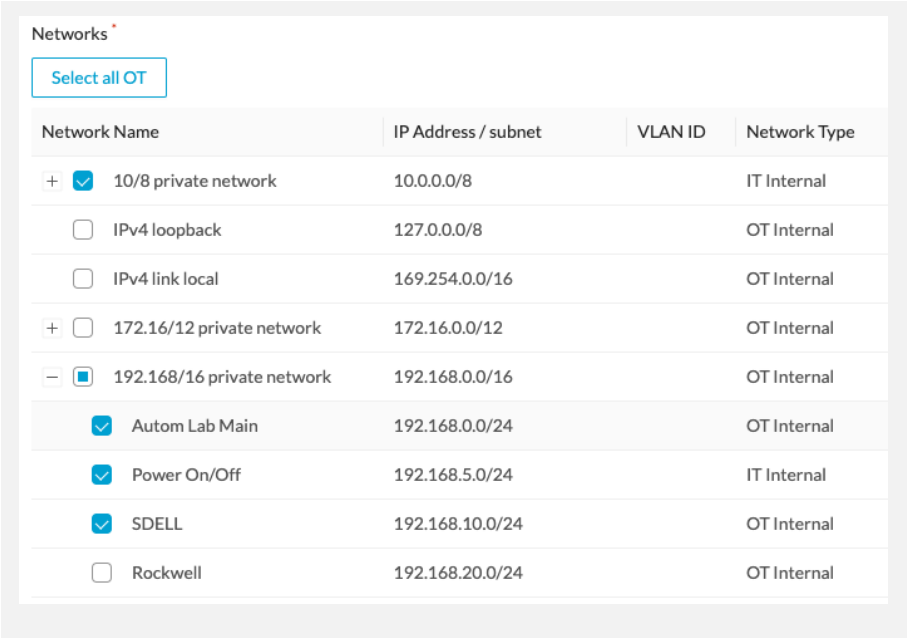

Figure 8.
Cisco Cyber Vision ISE integration – subnet selection

Event page enhancements: new look and customer filters

New look

The Cisco Cyber Vision event page was completely rebuilt to match the look and feel of the rest of the application. There are two tabs available to analyze the events:

- Dashboard
- List

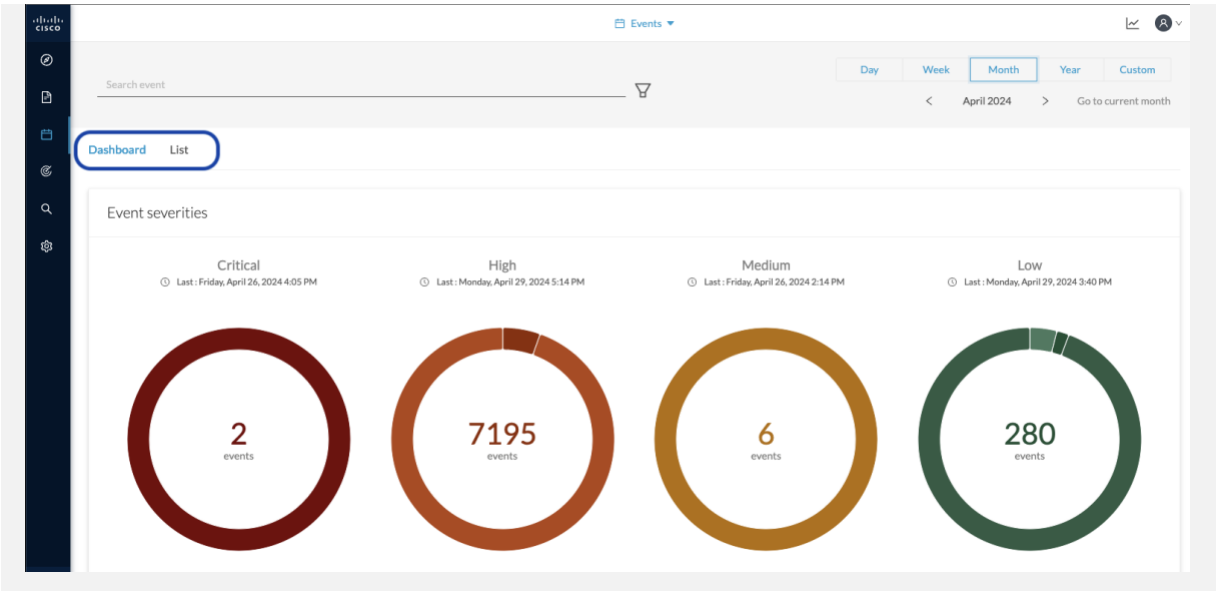

Figure 9.
Cisco Cyber Vision Event page – Dashboard

The dashboard gives highlights of the events.

The list provides all events displayed as a list ordered by time.

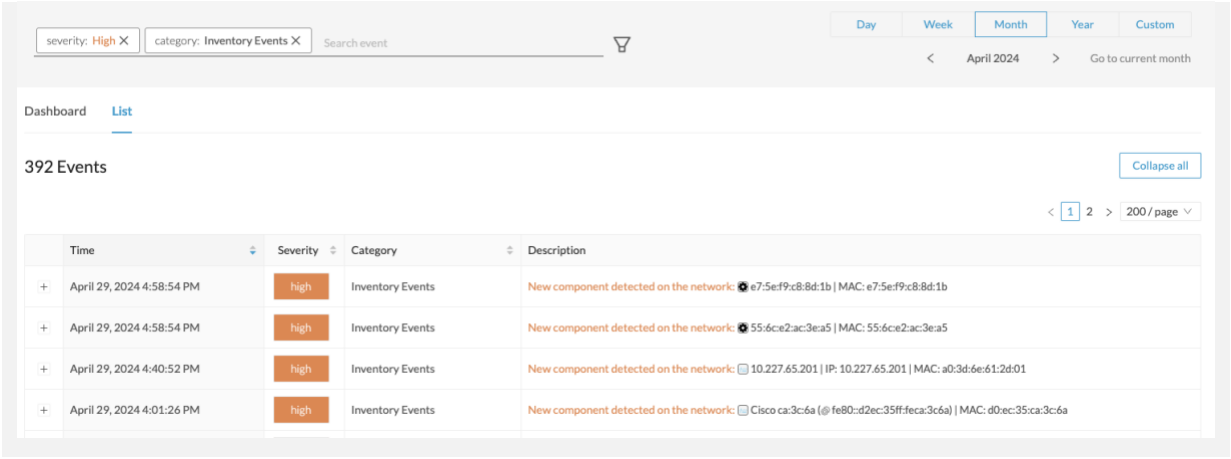

Figure 10.
Cisco Cyber Vision Event page – List

Custom filters

The two event tabs (Dashboard and List) share a common filter which have more functionalities than in the previous version.

You can now customize filters by editing them:

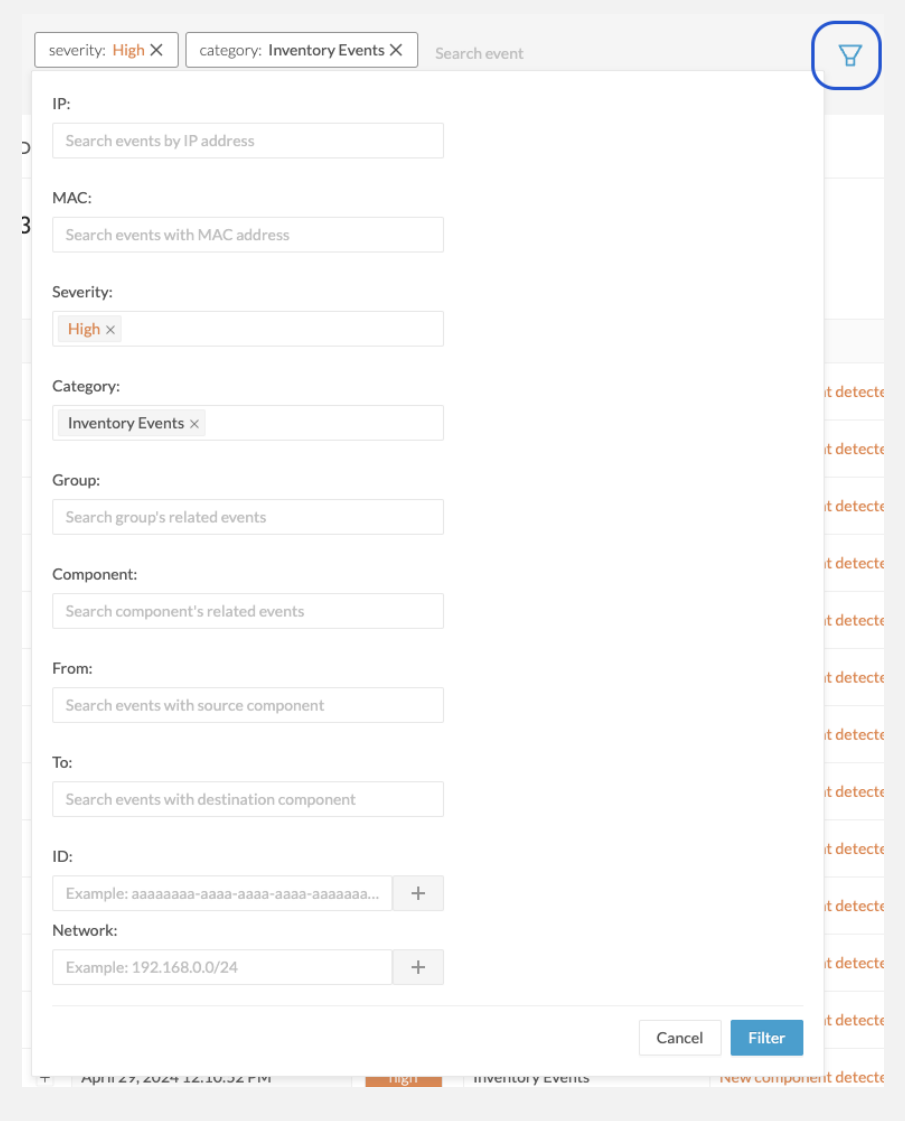

Figure 11.
Cisco Cyber Vision Event page – filters

The two pages can be filtered based on time thanks to predefined filters or the custom time filter:

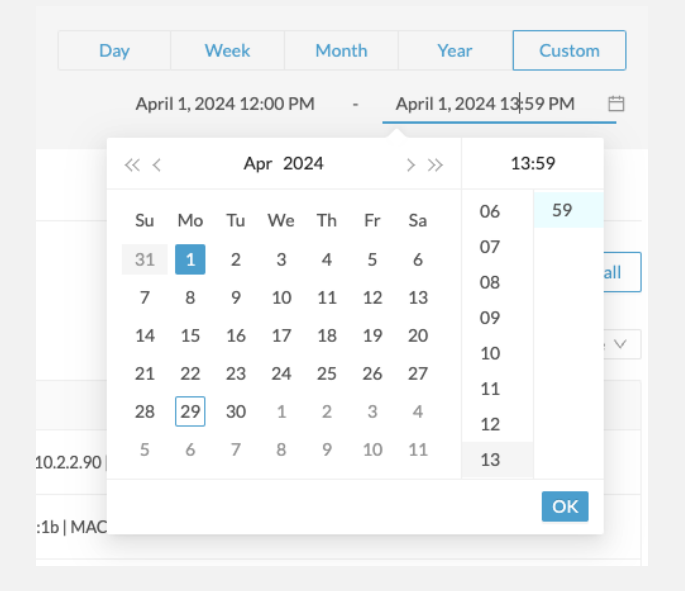

Figure 12.
Cisco Cyber Vision Event page – time filter

Remote Access Gateway Detection

OT gateways are commonly used in industrial environment. Many vendors in the market (like Ewon) provide external access solutions to OT assets for remote support/maintenance. Cisco Cyber Vision can now detect and tag Ewon remote access gateways:

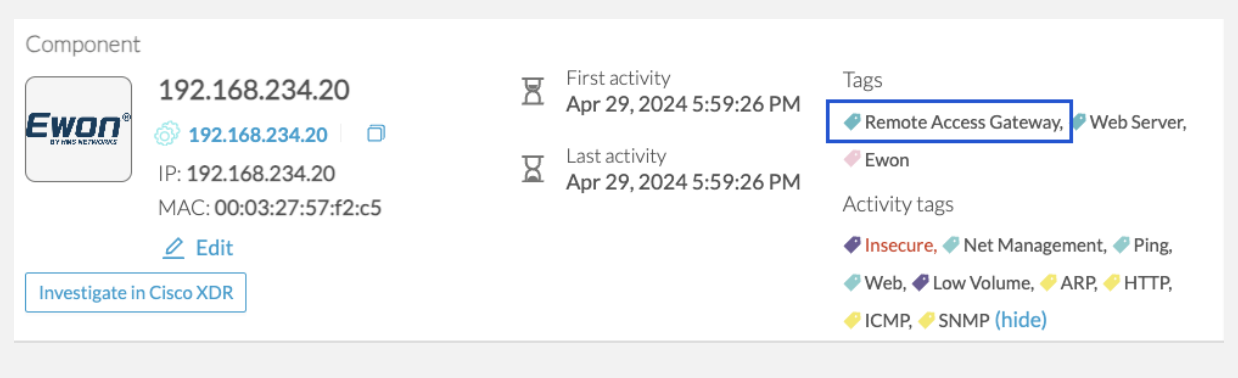

Figure 13.
Cisco Cyber Vision Remote Gateways – Ewon

Cisco Cyber Vision 4.4.0 can detect Ewon remote gateways thanks:

- to passive deep packet inspection (DPI) of http or snmp protocols

  and/or

- to Active Discovery done on http or snmp protocols.

Future releases of Cisco Cyber Vision will be able to detect more remote gateway vendors.

Remote Access Report

A new report is available to list remote access details seen by the system. This new report will list:

- discovered remote gateways
- remote access communication with
    - DNS Queries for Remote Access Domain Names
    - Attempted Remote Access Communications

This new report is available as a new type during report creation:

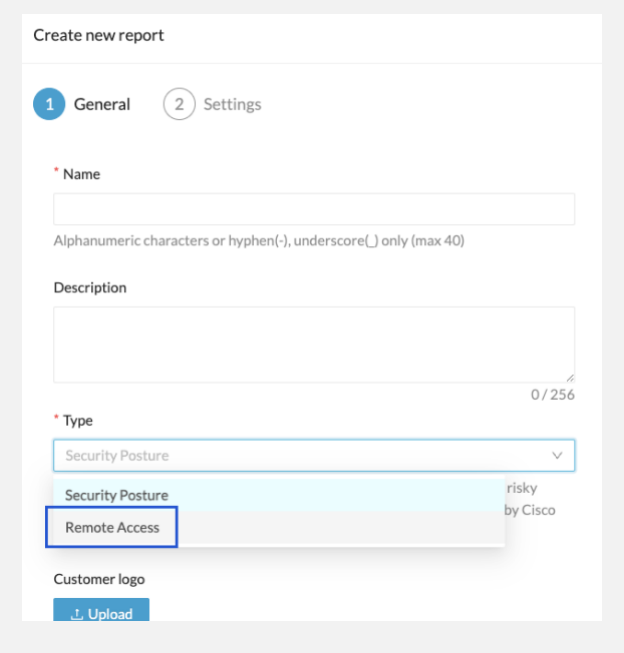

Figure 14.
Cisco Cyber Vision reports – Remote access

Reports: Enhancements

Several enhancements were done on the existing report type called “Security Posture” with additional content and cosmetic changes. In addition, the reports now have their expiration settings. Reports will now be removed from the system after a certain duration or when the number of versions of the same report reach a certain limit.

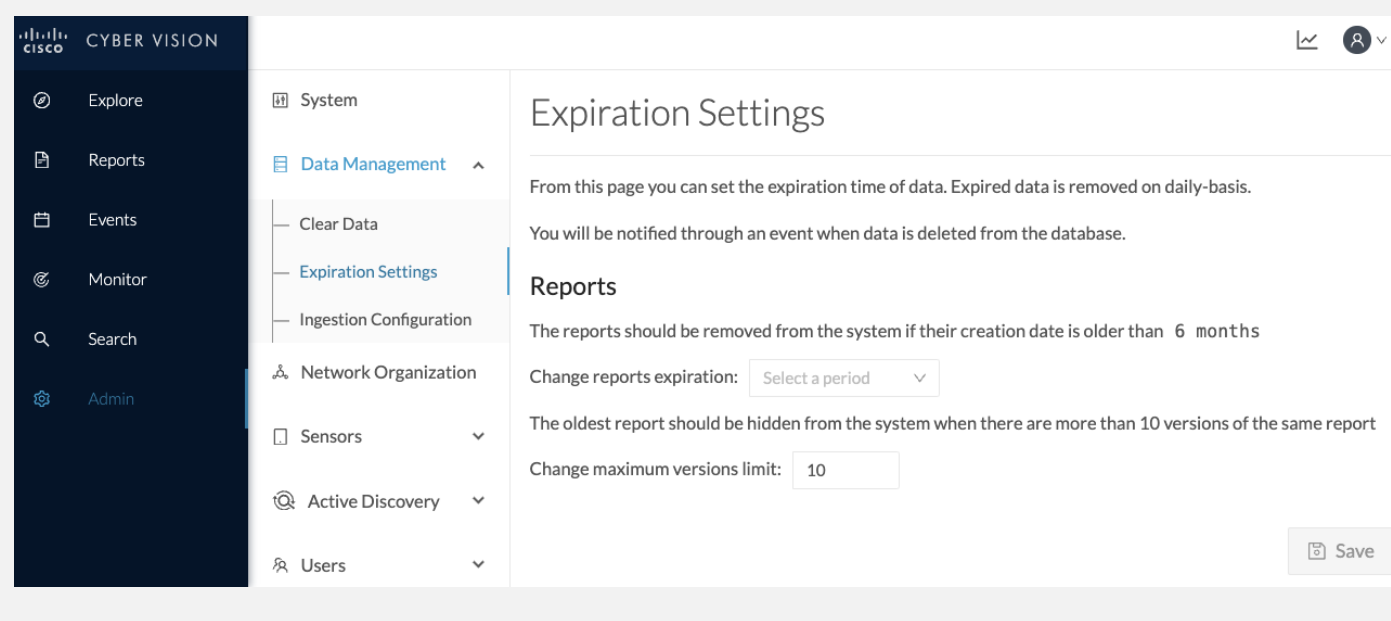

Figure 15.
Cisco Cyber Vision reports – Expiration Settings

Sensor self-update

Cisco Cyber Vision will allow for updating of sensors regardless of install method (i.e., without the extension). Release 4.4.0 brings all the necessary foundations to enable sensor self-update. Though the foundation is present in the 4.4.0 release, the self-update feature can only be exercised in subsequent releases (once there is a new release to upgrade to).

In Cisco Cyber Vision future releases, a new procedure will be available to update all sensors automatically. Required steps will be:

1. Select which sensors to update,
2. The Center adds a new job to the sensor queue,
3. The Sensor automatically collects/validates update file,
4. The Sensor re-starts with the new version.

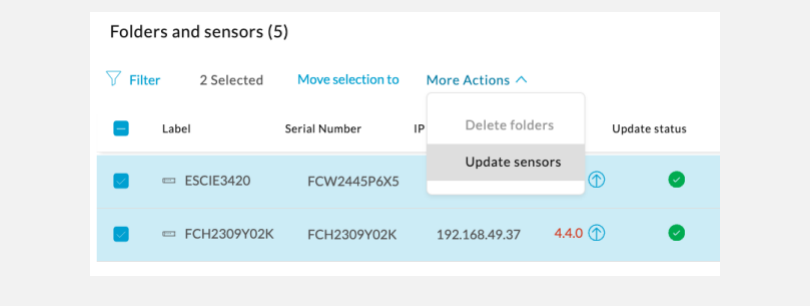

Figure 16.
Cisco Cyber Vision Sensor self-update – New update sensors menu

Some new icons are available on the sensor explorer menu for this new feature. They will give the status of the sensor update:

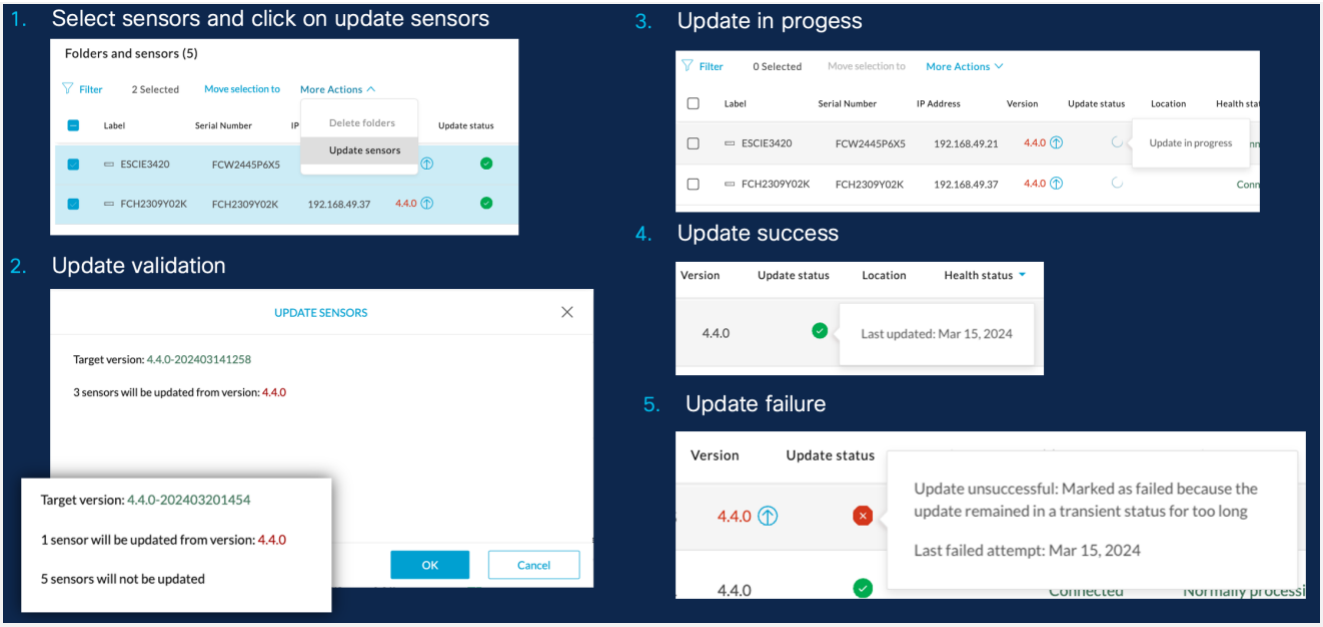

Figure 17.
Cisco Cyber Vision Sensor self-update – New icon and menus

XDR integration

Cisco XDR is an online platform that centralizes security events from various Cisco software equipment's through an API. For instance, events such as those from Cisco Cyber Vision or firewall activities can be transmitted to Cisco XDR and correlated, then presented across diverse dashboards. XDR will replace SecureX, which will reach its end of life on July 31, 2024. However, it is still possible to use SecureX until then by adjusting the desired integration here.

The XDR integration will bring several features. Once activated, users will be able to authenticate and benefit from XDR integration's features:

- Create incidents from the events page for these categories of events:
    - Anomaly Detection
    - Control Systems Events
    - Signature based Detection
- Activate XDR Ribbon and benefit from the associated features

Moreover, without requiring XDR authentication, users will have access to the 'Investigate' button on the Cyber Vision technical sheet for components, which will direct them to Cisco Threat Response (CTR).

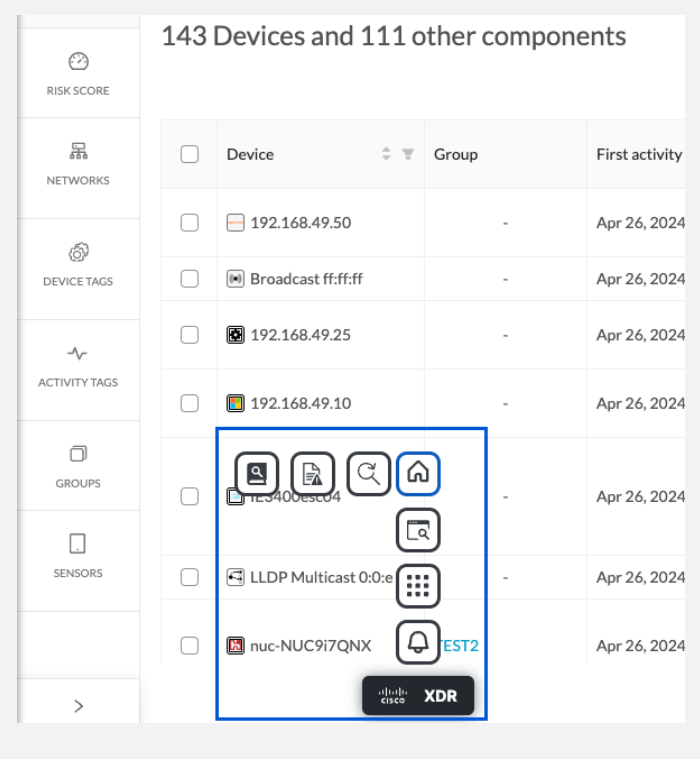

Figure 18.
Cisco Cyber Vision XDR integration – New XDR ribbon

Addition of Snort “Shared Object” Rules

Cisco Cyber Vision 4.4.0 adds a new type of Snort subscriber rules: the “Shared Object” rules.

Snort.org definition:

- Commonly referred to as “Shared Object rules”, “SO rules”, “pre-compiled rules”, or “Shared Objects” are detection that is written in the Shared Object rule language, which is, essentially, “C”. This allows for primarily two things for the Snort platform:
    - Detection that is not possible under the regular Snort rules language. Since Shared Object rules are “C” based, they can essentially be coded to detect a much greater set of conditions than regular Snort rules can. One of the common misconceptions about Shared Object rules are that they are closed source, and while under certain conditions that may be true, they are not inherently closed source. You can, in fact write your own shared object rules.
    - It allows for obfuscation of exact detection in the rule language. Under certain conditions (Agreements with vendors, use of Shared Object rules in ‘classified’ environments, Sourcefire 0-day detection, etc.) it may be necessary to obfuscate how detection is performed with a particular rule.

Backup and restore

A new CLI command is available to manage Cisco Cyber Vision Center full backup. This command will save the complete Center configuration and all the data collected. The backup will permit the creation of a new Center which will be exactly like the previous one (same IP addresses, same name, same sensor connected, same data organization, …).

Procedure:

1. On existing Center, use "**`sbs-backup export`**" command.
2. A backup file is created. Optionally, copy it to the new Center.
3. On new Center (or same Center), import using "**`sbs-backup import`**" command.

Constraints of the new backup restore command:

- The new appliance requires an equal number of network interfaces as the Center is backed up.
- Set up the new appliance with Cisco Cyber Vision configuration.
    1. Achieve the Center setup and select the right deployment mode (single or dual interface)
    2. Add an IP address to eth0 to transfer the Center archive.
- The new Center interface configuration (single or dual) needs to match the backed-up Center.
- As the new Center adopts all old Center settings like the IP address, the old appliance needs to be powered off.
- The Cisco Cyber Vision license cannot be copied.
    1. Return the license to the smart account server.
    2. After restoring, the new Center needs to be licensed.
- Install the report extension on the restored Center.

    Report configuration and old report versions are copied.

Catalyst 9300 support without SSD

Cisco Cyber Vision sensor release 4.4.0 can be installed on Catalyst 9300 without requiring SSD. It requires a Catalyst 9300 with IOS version greater or equal to 17.3.3 and 4G or greater available memory on flash (as IOS-XE and IOx applications will co-exist on the same filesystem).

Sensor storage capability will be reduced, there is no “Store & Forward” capability, and no PCAP recording capability.

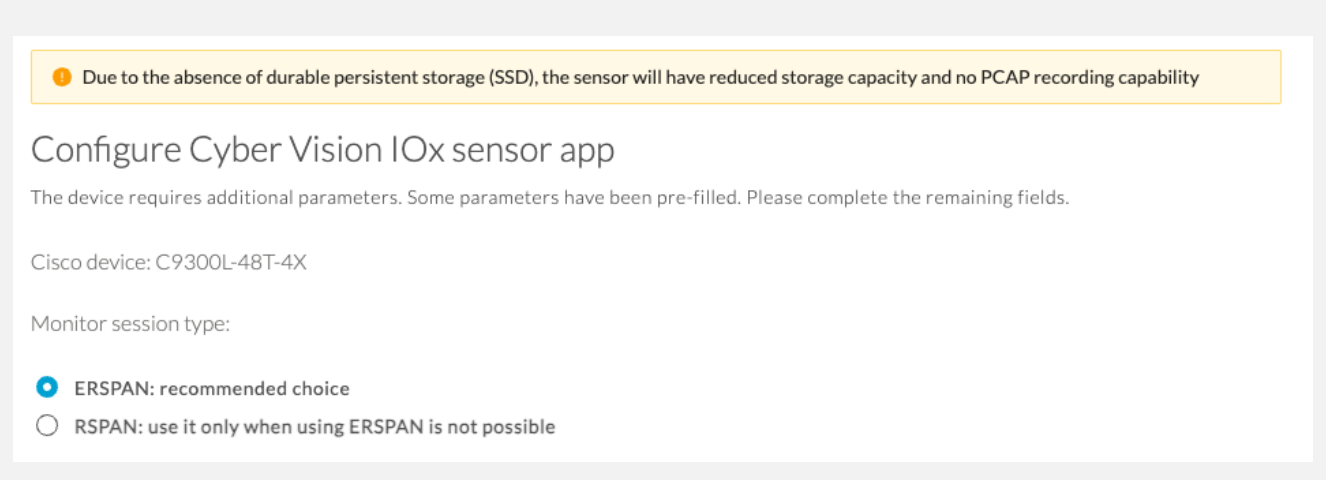

Figure 19.
Cisco Cyber Vision Catalyst 9300 – no persistent storage warning message

IE3x00 IOS 17.14 – IOX NAT

In industrial networking environments, efficient communication between internal applications and external servers is essential for seamless operations. However, the requirement for each application to have a routable IP address, in addition to the IP address for switch management, poses challenges for network administrators. IOS version 17.14 introduces a new feature called “L3NAT for IOx Applications” to avoid creating a dedicated IP address for a Cisco Cyber Vision sensor embedded in an IE3x00 switch. Two solutions are available to deploy a Cisco Cyber Vision sensor:

- The usage of a dedicated IP address for the Cisco Cyber Vision sensor
- The new feature in IOS 17.14, "L3NAT for IOx Applications" allows you to use the switch's management IP as a proxy for all network applications.

The Layer3 Network Address Translation (L3NAT) for IOx applications is supported starting with IOS-XE release 17.14.1. This feature uses the management IP of the switch as a proxy for all applications within the routed network. The complexity and overhead associated with managing multiple public IP addresses are reduced. The IE3x00 platform supports the L3NAT feature with the Cisco Cyber Vision (CCV) IOx application. However, it cannot be used to NAT other Ethernet traffic from hosts connected to its physical Ethernet ports.

Because of this traffic limit on eth0 to the Cisco Cyber Vision link (sensor to Center), active discovery cannot be used on this port.

Cisco Cyber Vision is compatible with this new IOS feature “Layer3 Network Address Translation (L3NAT) for IOx applications”. An architecture like the following could be used to onboard a new sensor hosted on an IE3x00 platform release 17.14.1:

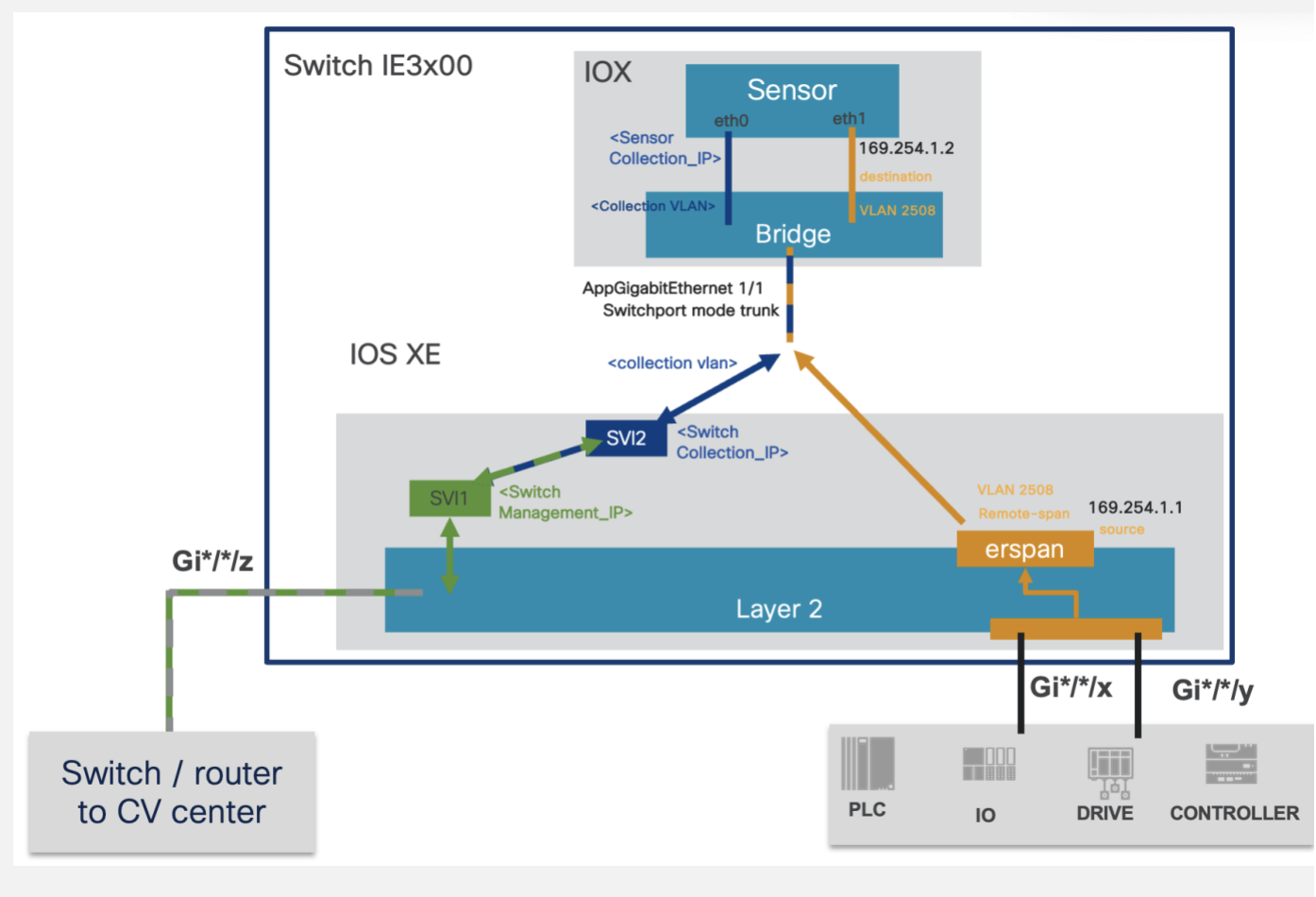

Figure 20.
Cisco Cyber Vision Sensor – IE3x00 L3NAT for IOx application

DPI changes

New protocols

List of the new protocol features:

- B&R PLC (X20 series)
- AMS protocol for Beckhoff devices
- New MAC OUI ranges for vendor naming
- LLDP flow tagging
- Mitsubishi compact PLC of type FX5U

Protocol enhancements

List of the protocol enhancements:

- Ethernet/IP backplane scanning when using DeviceNet mode
- EWON remote access detection via HTTP passive DPI
- Emerson system tag added when detecting DeltaV SCADA protocols
- Support of CC-LINK-IE TraSysNodeInfoDetailGet message
- TLS communication server side is set on handshake even if SYN/ACK are missing
- Support for Mitsubishi compact PLC of type FX5U

Active Discovery

New protocols

List of the new protocol features:

- GE PLC over GE-SRTP
- HTTP/HTTPS simple scanner
- Beckhoff AMS scanner for broadcast/unicast

Protocol enhancements

List of the protocol enhancements:

- Retrieve CPU name/description when target ENIP device is PLC
- Enhance SNMP to detect and query eWON remote access gateways

Telemetry

Telemetry monitors your system to provide anonymous diagnostics and usage data, helps us to understand and enhance product usage. Cisco Cyber Vision telemetry data communication occurs as HTTPS traffic through Port 443 with https://connectdna.cisco.com/.

Telemetry is enabled by default. To disable this feature, navigate to Admin > System and turn off the toggle under the Telemetry Collection section of the page.

UI user password reset CLI command

A new CLI command is available to reset a User Interface account password. This command is:

```
sbs-db reset-password
```

The command has only one argument: the email used as username.

```
root@Center224:~# sbs-db reset-password -h

Usage: sbs-db reset-password EMAIL

reset one user password

Arguments:
  EMAIL        the user email
```

Figure 21.
Cisco Cyber Vision reset user

The command will return a temporary password which must be changed after the first login on the User Interface:

```
root@Center224:~# sbs-db reset-password eric@cisco.com
User password successfully reset. You can now set a new password by login to the GUI using this
temporary password: wf1hTTeR1dWU7Mhy7kGOOS2D5a0
```

Figure 22.
Cisco Cyber Vision reset user

Cisco Cyber Vision 4.4.0 enhancements

Table 6. Cisco Cyber Vision enhancements

CDETS	Description
CSCwe16233	Database maintenance during center updates
CSCwj13393	Disable splash screen for remote connection users
CSCwj32447	Add a way to reset UI user password form CLI

Cisco Cyber Vision 4.3.0 Resolved Caveats

Table 7. Cisco Cyber Vision resolved caveats

CDETS	Description
CSCwe16275	Events counter not updated at event deletion
CSCwe88633	Active Discovery: Retry in Unicast not used in multiple protocols
CSCwb12630	Some attributes sent via pxGrid are missing in ISE
CSCwf59282	Active discovery: wrong number of discovered devices reported for profinet broadcast
CSCwh37564	Add additional pop-ups for CPU intensive processes
CSCwi27446	Center with SLR license temporary shown as demo mode
CSCwi40737	Marmotd: Panic error causing service to stop
CSCwi59858	Last Logon date and time is wrong for LDAP users
CSCwi60005	Security posture report - Filter MAC vendors
CSCwi63442	sbs-netconf is forcing to set a gateway
CSCwj68386	Unable to delete user due to error
CSCwj24441	Improve information on unknown sensors by revoking their certificates
CSCwj23000	Change default variable expiration period to 7 days
CSCwj00403	Add a new automatic expiration for credentials
CSCwj00402	IC3000 IDS license is no more working in 4.3.0
CSCwj18913	Increase the network name column width in the Network table used in Ingestion config or ISE integration
CSCwj18912	Component list in the device overlay - do not list all sensors
CSCwj18911	Scroll bars disappear in several menus after opening device or component overlay in the search menu
CSCwj28616	LDAP integration - Error on first tab is not shown on second tab
CSCwj32446	Newly generated report file is empty due to Special character
CSCwj75034	License - smart agent avoid displaying the error code 'Payment required'
CSCwj48982	LC-GC re-enrollment error because of events not purged
CSCwj50836	IE9x00 SD card document Partition instead of format
CSCwj52714	flow panic in protocolReassembly with CIP
	Fix opcua reassembly which result in wrong variables name
	Bacnet protocol, fix wrong server-side assignment when whois was detected
	Yokohama protocol, fix decode error due to wrong udp decoder decision
	All protocols: fix properties count to keep it right regardless of flowtable export interval
	Fix missing variables so that it does not depends on export-interval value
	Fix CIP/ENIP Module detection when path through chassis is used. New DisabledLinkAddress config parameter
	Fix direction for S7 program download in some cases
	Missing DCE-RPC tag on WMI flow and missing ROCPLUS tag on Emerson flow
CSCwi46934	Vlan missing with some specific span configurations
	Fix Memory leak with tcp reassembly
	Bacnet NAME assigned to wrong side

Cisco Cyber Vision Open Caveats

Table 8. Cisco Cyber Vision enhancements

CDETS	Component	Description
CSCwj93196		FMC script is abnormally long during the synchronization
CSCwj69323		XDR ribbon, Cyber Vision incidents cannot be found on the XDR site.
CSCwk04880	Center	Backup and Restore – restoring a dual interface center on a center configured as single interface is not working
CSCwk04879	Center	Backup and Restore – restoring a center backup may fail due to number of interfaces count.
CSCwd39017	Center	Missing information in the Smart License Usage

Cisco Cyber Vision deprecated features

Cisco Cyber Vision integrations with FMC and FTD will be deprecated. It is now displayed in the product shown below:

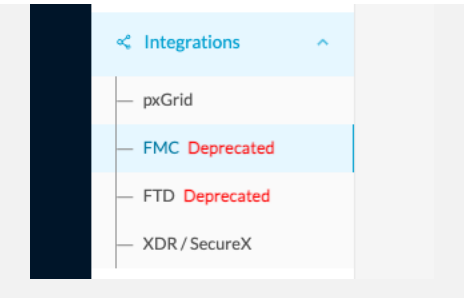

Figure 23.
Cisco Cyber Vision integrations

The 2 features will be removed from the product in release 5.1.0 (end of calendar year 2024).

FMC integration will be replaced by a new connector available in the FMC Cisco Secure Dynamic Attributes Connector (CSDAC). CSDAC Cyber Vision documentation is available here:

Cisco Secure Dynamics Attributes Connector Guides

For example: Cisco Secure Dynamic Attributes Connector Configuration Guide 3.0

For FTD, there is no plan for replacement. The integration could still be done through the APIs of the 2 platforms.

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 4.4.0 center files

Center	Description
CiscoCyberVision-center-4.4.0.ova	VMware OVA file, for Center setup
CiscoCyberVision-center-with-DPI-4.4.0.ova	VMware OVA file, for Center with DPI setup
CiscoCyberVision-center-4.4.0.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-reports-management-4.4.0.ext	Reports management extension installation file
CiscoCyberVision-sensor-management-4.4.0.ext	Sensor management extension installation file

Table 10. Cisco Cyber Vision 4.4.0 sensor files

Sensor	Description
CiscoCyberVision-IOx-aarch64-4.4.0.tar	Cisco IE3400, Cisco IE3300 10G, Cisco IE9300, Cisco IR1101 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64--4.4.0.tar	Cisco IE3400, Cisco IE3300 10G, Cisco IE9300 Cisco IR1101 Active Discovery sensor installation and update file
CiscoCyberVision-IOx-IC3000-4.4.0.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-IC3000-4.4.0.tar	Cisco IC3000 Active Discovery sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.4.0.tar	Cisco Catalyst 9x00 and Cisco Catalyst IR8340 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.4.0.tar	Cisco Catalyst 9x00 and Cisco Catalyst IR8340 Active Discovery sensor installation and update file

Table 11. Cisco Cyber Vision 4.4.0 update files

Updates	Description
CiscoCyberVision-Embedded-KDB-4.4.0.dat	KnowledgeDB embedded in Cisco Cyber Vision 4.4.0
CiscoCyberVision-update-center-4.4.0.dat	Center update file for upgrade from release 4.3.x to release 4.4.0 (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**.