Release Notes for Cisco Cyber Vision Release 4.2.0

For users upgrading to 4.2.0 from previous versions, please read the Cisco Cyber Vision 4.2.0 update procedure 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
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
AWS – Center AMI	Amazon Web Services center image
Azure – Center plan	Microsoft Azure center plan
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 Catalyst IE9300	Cyber Vision Sensor IOx application hosted in Cisco Catalyst IE9300 Rugged Series switches
Cisco IR1101	Cyber Vision Sensor IOx application hosted in Cisco IR1101 Series Industrial Integrated Services Routers
Cisco Catalyst IR8300	Cyber Vision Sensor IOx application hosted in Cisco Catalyst IR8300 Rugged Series Routers
Cisco Catalyst 9300, 9400	Cyber Vision Sensor IOx application hosted in Catalyst 9300, 9400 Series switches

Unsupported device list

As of version 4.2.0, Sentryo hardware is no longer supported.

Center	Description
Sentryo CENTER10	**Sentryo CENTER10 hardware appliance**
Sentryo CENTER30	**Sentryo CENTER30 hardware appliance**
Sensor	
Sentryo SENSOR3	**Sentryo SENSOR3 hardware appliance**
Sentryo SENSOR5	**Sentryo SENSOR5 hardware appliance**
Sentryo SENSOR7	**Sentryo SENSOR7 hardware appliance**

Cisco Cyber Vision 4.2.0 update procedure

Cisco Cyber Vision 4.2.0 update procedure will depend on the architecture deployed and the tool used to deploy it.

Upgrade Path

Upgrade Path to Cisco Cyber Vision 4.2.0

Current Software Release	Upgrade Path to Release 4.1.4
If version prior to 3.2.4	Upgrade first to 3.2.4, then to 4.0.0, then to 4.1.4 and to 4.2.0
Version 3.2.4	Upgrade first to 4.0.0, then to 4.1.4, then to 4.2.0
Version 4.0.0 to 4.0.3	Upgrade first to 4.1.4, then to 4.2.0
Version 4.1.0 to 4.1.4	Upgrade directly to 4.2.0

Compatibility Guidelines

There is downward compatibility of one version between the Global Center and the Center with sync and sensors.

- Global Center (Version N): Compatible with Centers with sync 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 sync (Version N): Compatible with sensors with versions N and N-1.

  e.g. Center with sync version 4.2.0 can manage sensors with versions 4.2.0 and 4.1.4.

Data purge

The Center database in 4.0.0, 4.0.1, 4.0.2 or 4.0.3 will be migrated to the new 4.1.x and 4.2.0 schemas. All components, activities, flows, events, etc. will be migrated.

The new data retention policies introduced in 4.0.0 are still valid in 4.1.x. Once migrated, the following expiration settings will be applied, and the system will run the purge process unless the configuration is modified within 2 days:

- Events after 6 months.
- Flows after 6 months.
- Variables after 2 years.

Center updates

Architecture with Global Center

Preliminary checks: it is highly recommended that you check the health of all Centers connected to the Global Center and of the Global Center itself before proceeding to the update.

To do so, it is recommended to use an SSH connection to the Center and to type the following command:

systemctl --failed

The number of listed sbs-* units should be 0, otherwise the failure needs to be fixed before the update.

Cisco Cyber Vision system check – 0 failure

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

All sbs services need to be running in a normal state before performing an update. If any is listed as failed it must be fixed prior upgrading.

Cisco Cyber Vision system check – example of failure

```
root@Center21:~# systemctl --failed
  UNIT                 LOAD   ACTIVE SUB    DESCRIPTION
● sbs-marmotd.service loaded failed failed marmotd persistence service

LOAD   = Reflects whether the unit definition was properly loaded.
ACTIVE = The high-level unit activation state, i.e. generalization of SUB.
SUB    = The low-level unit activation state, values depend on unit type.

1 loaded units listed.
root@Center21:~#
```

Rebooting of the Center most often solves the issue. If not, please contact the support.

In the case of a distributed architecture, the following steps need to be followed:

1. Update the Global Center:
    a. Either using the Graphical User Interface:
        - File= CiscoCyberVision-update-combined-4.2.0.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-4.2.0.dat
        - Launch the update with the following command:

    sbs-update install /data/tmp/CiscoCyberVision-update-center-4.2.0.dat
2. Update the Centers connected to the Global Center with the same procedure used for the Global Center (User Interface or CLI).
3. Update the sensors from their corresponding Center (not from the Global Center):
    a. Hardware sensors:
        i. If you used the combined file to update the Center which owns the sensor, and the SSH connection from the Center to the allowed sensor, the hardware sensors (IC3000 and Sentryo SENSOR's) were updated at the same time.
        ii. If the Cisco IC3000 sensor was deployed using the Sensor management extension, it can be upgraded by deploying it again.
        iii. If not, the update needs to be done from the Command Line Interface (CLI):
            - File= CiscoCyberVision-update-sensor-4.2.0.dat
            - Launch the update with the following command:

    sbs-update install /data/tmp/CiscoCyberVision-update-sensor-4.2.0.dat

You can check the sensor version on the Administration / Sensor Explorer page, to make sure that the version is 4.2.0.

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 sensors with the sensor management extension, first upgrade the extension and then update the sensors.

- File = CiscoCyberVision-sensor-management-4.2.0.ext
- Navigate to Admin > Extensions. In the Actions column, 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 /data/tmp/CiscoCyberVision-sensor-management-4.2.0.ext
```

ii. Then all sensors need to be updated with the extension, to do so, access the sensor administration page, and use the menu “Manage Cisco devices” / “Update Cisco devices” or use the redeploy. A complete procedure is available in the document (part “Cisco Cyber Vision new features and improvements”) or in all sensor deployment guides version 4.2.0 minimum.

iii. If you have not installed the sensor with the sensor management extension, the upgrade of the sensor can be performed with the sensor package from the platform Local Manager or from the platform Command Line. This procedure is described in the corresponding sensors installation guides.

- IE3x00 and IR1101 files = CiscoCyberVision-IOx-aarch64-4.2.0.tar or CiscoCyberVision-IOx-Active-Discovery-aarch64--4.2.0.tar
- Catalyst 9300 and 9400 and IR8340 files = CiscoCyberVision-IOx-x86-64-4.2.0.tar or CiscoCyberVision-IOx-Active-Discovery-x86-64-4.2.0.tar.

Important remark regarding CiscoCyberVision-IOx-x86-64 sensor application update:

The sensor update through the Local Manager of a Catalyst 9300, 9400 or IR8340 files is not possible from a release 4.1.2 (or lower) to a release 4.1.3 (or higher) due to the addition of the rspan compatibility. The sensor application needs to be redeployed and the enrollment package uploaded again.

Guidelines here: **Cisco Cyber Vision Sensor Application for Cisco Switches Installation Guide, Release 4.1.3**

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-4.2.0.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-4.2.0.dat
        - Launch the update with the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-center-4.2.0.dat
```

2. Update the sensors:
    a. Hardware sensors:
        i. If you used the combined file to update the Center which owned the sensor and the SSH connection from the Center to the allowed sensor, the hardware sensors (Cisco IC3000 and Sentryo SENSOR's) were updated at the same time.
        ii. If the Cisco IC3000 sensor was deployed using the sensor management extension, it can be upgraded by deploying it again.
        iii. If not, the update needs to be done from the Command Line Interface (CLI):
            - File= CiscoCyberVision-update-sensor-4.2.0.dat
            - Launch the update with the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-sensor-4.2.0.dat
```

    b. IOx sensors:
        i. If you have installed the sensors with the sensor management extension, first upgrade the extension itself and then all sensors will have to be updated.
            - File = CiscoCyberVision-sensor-management-4.2.0.ext
            - Navigate to Admin > Extensions. In the Actions column, 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 /data/tmp/CiscoCyberVision-sensor-management-4.2.0.ext
```

ii. All sensors need to be updated with the extension. To do so, access the sensor administration page, and use the menu “Manage Cisco devices” / “Update Cisco devices” or use the redeploy button. A complete procedure is available in the document (part “Cisco Cyber Vision new features and improvements”) or in all sensor deployment guides version 4.2.0 minimum.

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 Local Manager platform or from the Command Line Interface. This procedure is described in the corresponding sensors installation guides.

- IE3x00 and IR1101 files = CiscoCyberVision-IOx-aarch64-4.2.0.tar or CiscoCyberVision-IOx-Active-Discovery-aarch64--4.2.0.tar
- Catalyst 9300 and 9400 and IR8340 files = CiscoCyberVision-IOx-x86-64-4.2.0.tar or CiscoCyberVision-IOx-Active-Discovery-x86-64-4.2.0.tar.

Important remark regarding CiscoCyberVision-IOx-x86-64 sensor application update:

The sensor update through the Local Manager of a Catalyst 9300, 9400 or IR8340 files is not possible from a release 4.1.2 (or lower) to a release 4.1.3 (or higher) due to the addition of the rspan compatibility. The sensor application needs to be redeployed and the enrolment package uploaded again.

Guidelines here: **Cisco Cyber Vision Sensor Application for Cisco Switches Installation Guide, Release 4.1.3**

AWS and Azure Centers

In case of a Center deployed in AWS or Azure, follow the same procedure described with one Center hereabove.

Cisco Cyber Vision 4.2.0 important changes

Command line access

In 4.1.0, a major change regarding the Center Command Line Interface (CLI) access through serial console or SSH was made. The user root is no longer usable to establish the connection. A new user called ‘cv-admin’ must be used. This user has limited rights and many CLI commands will require permission elevation:

- prefix the command with "sudo".
- or open a root shell using "sudo -i" and enter a command.

Communication port and protocol changes

Port

No modification in 4.2.0.

Protocol

No modification in 4.2.0.

API

No modification in 4.2.0.

SYSLOG

No modification in 4.2.0.

Cisco Cyber Vision new features and improvements

Active Discovery improvements

Several improvements were made related to the Active Discovery feature in release 4.2.0.

- Target IPs for Unicast discovery are now set in profiles.
- Two new Unicast protocols are supported:
    - S7: Siemens host discovery
    - WMI: Windows host discovery

To configure Active Discovery, two steps must be completed:

1- Policy definition: A policy is a set of protocols and a few settings.

2- Profile definition: A profile defines...

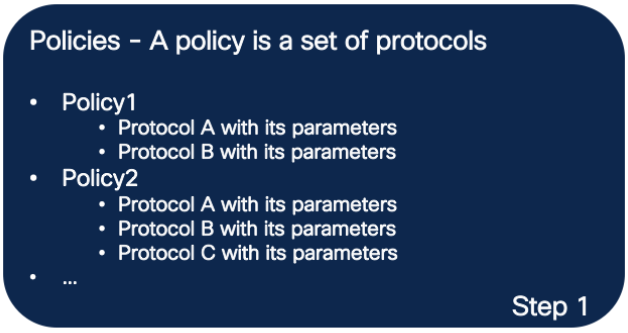
a. what is to be discovered:

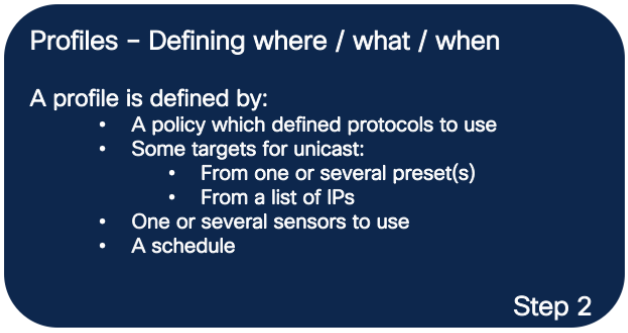
i. protocols through a policy

ii. targets in case Unicast protocols are selected

b. where to look for I.e., which sensors will be queried.

c. when (run once or scheduled for frequency).





Consequently, profiles will replace former discovery settings you could find in presets in the Explore page. Active Discovery configuration is entirely done in the Admin page.

Active Discovery profile definition

Profile parameters:

1- **Name**: name of the profile

2- **Discovery policy**: policy to use

3- **Target**: Targets can be a mix made of preset(s), IP(s) and IP range(s). It is not required to fill in this field if the selected policy doesn't contain Unicast configuration. Parameters are:

   a. **IPs from Presets**: IPs listed in the Devices/Components list will be used.

   b. **IPs targets**: example:

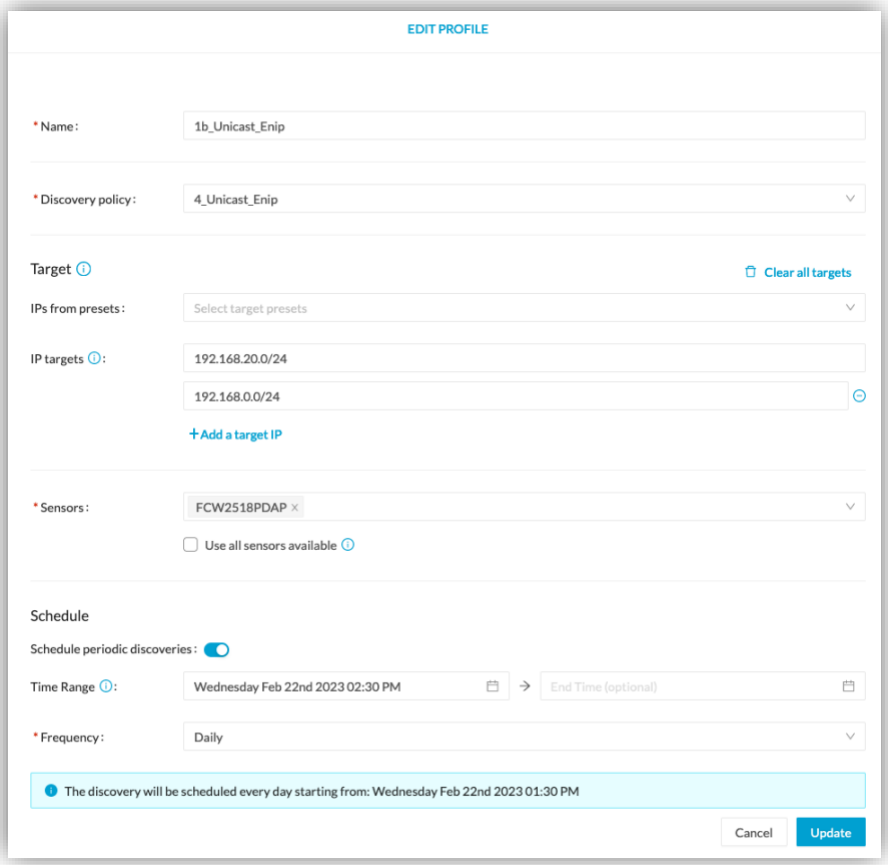
      i. IP: 192.68.1.1

      ii. Range: 192.68.1.1-192.68.1.9

      iii. Subnet: 192.68.1.0/24

4- **Sensors**: list of sensors to be used.

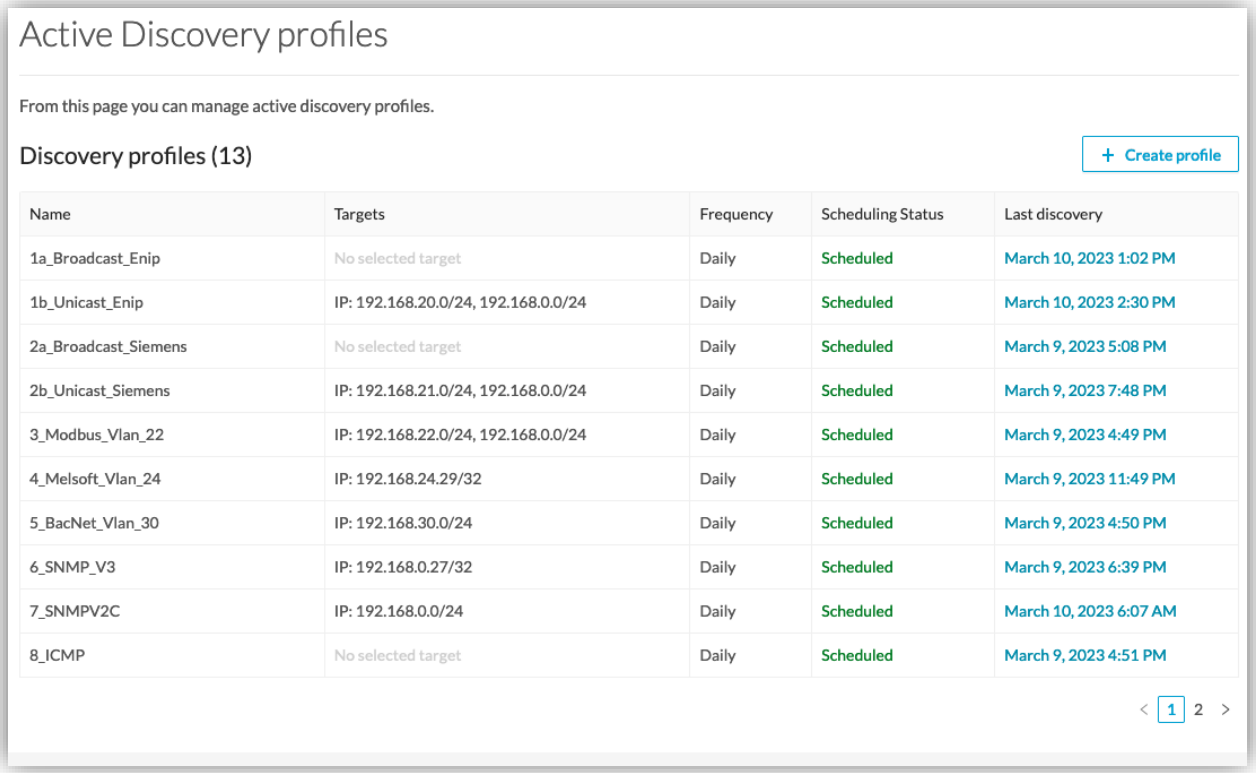
5- **Schedule**: the profile can be set to launch the discovery as 'run once' or can be scheduled. Scheduling contains a frequency (Hourly, Daily, Weekly, Monthly) and a start and end time.



Active Discovery profile status

Profile list

A list of all defined profiles is visible in the Admin menu:



This list gives details about the profiles and allows the user to access:

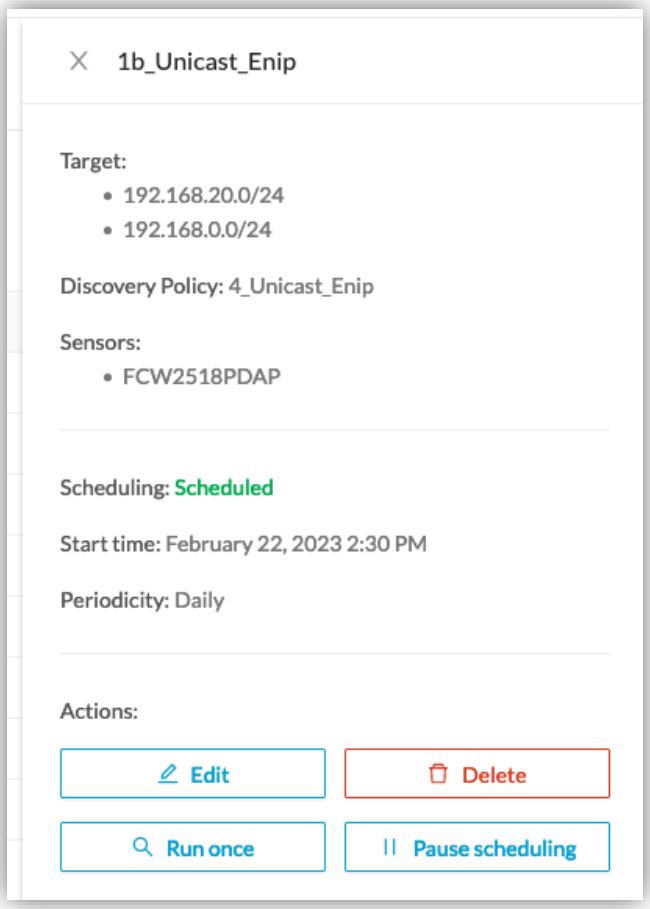
1- Actions and properties in an overlay, clicking any item in any column, except for Last discovery.

2- Last discovery results, clicking any time in the Last discovery column.

Profile side panel

The overlay gives details on the profile and allows the user to:

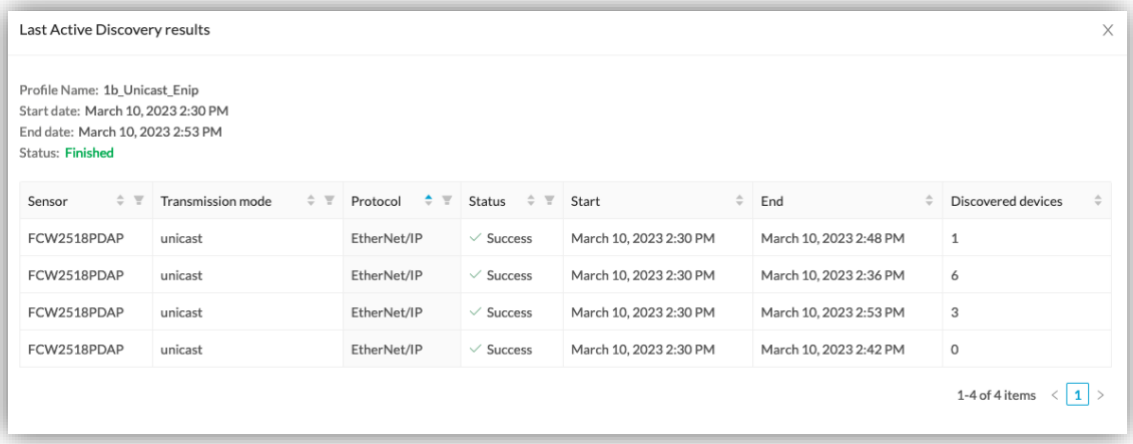
- Edit the profile through the edit profile page.
- Delete the profile.
- Run it once.
- Pause or resume the scheduling.



Discovery results

The results of a profile appear:

- Above the table (start, end, status)
- And with one line per range of 127 IPs maximum.



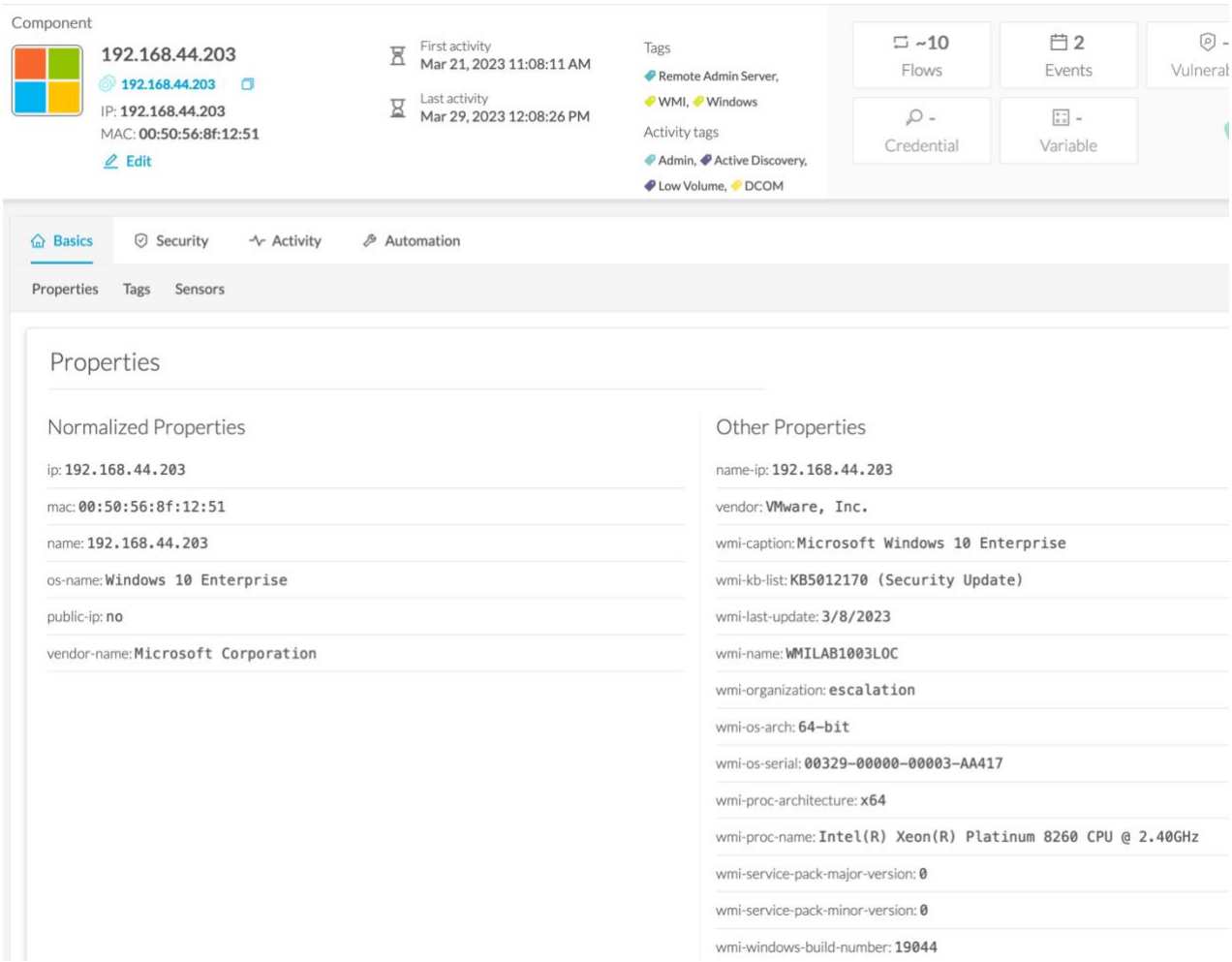
Once discovered, the device can be seen in the Explore menu. The preset Active Discovery Activities will give you further information.

WMI discovery

Windows host discovery is now available in Cisco Cyber Vision 4.2.0 allowing you to see some Windows host properties like:

Property	Description
wmi-caption	Operating system name and version
wmi-kb-list	List of installed KB
wmi-last-update	Last update date
wmi-name	Host name
wmi-organization	Organization name

For example:



WMI Active Discovery requires a Windows user account with the necessary rights to access the host and collect the WMI properties.

S7 discovery

The S7 Unicast discovery will collect some properties of compatible Siemens devices.

For example:

s7-bootloaderref: **Boot Loader**

s7-bootloaderver: **V 2.2.1**

s7-fwver: **V 2.9.4**

s7-hwref: **6ES7 515-2RM00-0AB0**

s7-hwver: **1**

s7-modulename: **PLC_1**

s7-moduleref: **6ES7 515-2RM00-0AB0**

s7-modulever: **1**

s7-plcname: **PLC_1**

s7-rack: **0**

s7-serialnumber: **S C-M6DA37302020**

Sensor management extension disablement

When users leverage the Cisco Cyber Vision Sensor Management Extension to deploy sensors, the extension will continue to log into the device periodically to check the device's status. This cannot be modified by the user. If the extension fails to connect (no response or invalid credentials) it will attempt to connect every 5 minutes which will cause authentication failures to fill up logs.

Cisco Cyber Vision release 4.2.0 is now providing a way to disable the Sensor Management Extension. The extension needs to be activated again to install or update a sensor.

A new command is available from the CLI (Command Line Interface) to disable or enable the Sensor Management Extension.

sbs-extension cmd sensor-management disable

```
root@center:/data/home/cv-admin# sbs-extension cmd sensor-management disable
Disabling, do not interrupt...
sensor-management-main
sensor-management-postgres
sensor-management-influxdb
Extension has been disabled
```

sbs-extension cmd sensor-management enable

```
root@center:/data/home/cv-admin# sbs-extension cmd sensor-management enable
Enabling, do not interrupt...
run script wrote to stdout:
sensor-management-postgres
sensor-management-influxdb
sensor-management-main
Extension has been enabled
```

The status of the extension will be displayed in the user interface.

Some errors will be displayed if the user tries to uninstall or update the Sensor Management Extension when it's disabled:


```
root@center:/data/home/cv-admin# sbs-extension upgrade --no-version-check /data/tmp/CiscoCyberVision-sensor-
management-4.2.0-BETA3.ext
pre-upgrade script wrote to stderr:
ERROR: Extension is disabled, for safety reasons the upgrade is not possible

pre-upgrade script returned with error code 1, canceling
```

Collection network interface - DHCP server option removed

The DHCP server option is no longer available on the Collection network interface. Consequently, the corresponding step no longer applies in the Center's Basic Configuration of Cisco Cyber Vision 4.2.0.

Cisco Cyber Vision Resolved Caveats

CDETS	Description
	Event page - search failure due to some characters
CSCwe16299	Some enip variables are not seen by the product
CSCvy57108	Some Ubuntu device are tagged as Windows or VMWare
CSCwe16268	Subnet filter: support of IPv6
CSCwe16257	Decode error can flood center journal when center dpi is used
	SNMP: Use SNMP properties as normalized properties for devices (9889)
	Preset filter based on sensor is not working on a particular center (10601)
	Foxboro dissection - TCP direction sometimes wrong (10636)
	Center certificate expiry management (10674)
CSCwe16240	User Admin Read Rights allow to modify roles and security settings
	Changing Admin user role shouldn't be possible
	Successive LC KDB upgrades from GC after LC/GC disconnection
CSCwe16237	CDP version inconsistent behavior when value changed
CSCwe16235	Siemens S7: the returned firmware for the normalized properties is wrong
	Preset not created after PCAP upload for some filenames
CSCwe16222	Switch to the presets List View does not work
	Sensor most of the time in "abnormal" "Pending data" status (11419)
	Improve "Refresh" and "New data" user experience (11421)
CSCwe16220	Snort event direction wrong for some IoCs
CSCwe16215	Rabbitmq queues are not limited in size
CSCwe16213	Component Sensor ID displayed is not consistent
CSCwe16212	Preset Dashboard "Vulnerabilities" device value is counting components
CSCwe16211	OMRON - FINS protocol: improve DPI and tag activities
CSCwe16210	Bad WMI tagging of activities
CSCwe16351	KDB rules are not evaluated after a center upgrade
CSCwe16349	Device list: column are misaligned
CSCwe16348	Need caption or help on date format for sbs db purge-components
CSCwe16347	Improve user experience when a sub-group is selected in a preset
CSCwe16346	“No SSH" notification for sensors should be removed from global center sensor explorer
CSCwe16205	Profinet Protocol: PN_IO CM create Engineering Station tag on PLC
CSCwe16200	All vulnerabilities matched on a given component are assigned the same matching reasons
CSCwe16196	snort segfault: workaround for ic3k

CDETS	Description
CSCwe16193	Backup Sensor Management data before upgrading it.
CSCwe16337	Increase materialized views refresh period to resolve user experience issues
CSCwe16336	Update materialized views when API route visualisations networknode-list is used
CSCwe16192	Icons not aligned in the selection panel header
CSCwe16335	4.1.4: name-vendor-is now name-ip and creates difference in baselines
CSCwe16334	List of filters (ex: Activity -> Protocol) sorted but case-sensitive
CSCwe16183	4.1.4 - Error during KDB import
CSCwe16182	IEEE OUI DB add the latest DB in 4.2.0 release.
CSCwe16319	API Calls must refresh materialized views (creat mat views and update last_access field)
CSCwe16179	Mismatch in the vulnerability count in 'All Data' preset
CSCwe16316	LC-GC synchronization issues after upgrading an existing Global Center
CSCwe16303	syslog on global center does not always use the right format
CSCwe16178	syslog events send by a GC do not mention the LC generating the event
CSCwe16169	IPv6 networks filter configuration issue
CSCwe16167	Extension: when choosing the extension, only .ext files should be listed
CSCwe16165	Purge Flows - Remove event checks and fix event UI
CSCwe16164	sbs-diag sensor minor changes
CSCwe10575	Expiration - purge flow_properties_statistics based on flow period
CSCwe16161	Missing broadcast and multicast flows from the Insight "untagged flows" view
CSCwe18206	Sensor Management Extension - Periodic Connection to device unable to be modified
CSCwe30144	burrow taking all RAM with big DB

Cisco Cyber Vision Open Caveats

Issues ID / CDETS	Component	Description
CSCwb12630	Center + ISE	All components are not synchronized with ISE
CSCwd39017	Center	Missing information in the Smart License Usage
CSCwd82713	IE9300	The switch platform may sometime completely stop the traffic on the appGigabit interface. Restarting IOX is the needed to recover it.
CSCwe50724	IE3x00 and IE9300	Active Discovery Profinet DCP (Multicast Ethernet) is not working
CSCwe16323	IC3000	USB enrolment is not working

Links

Software Download

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

Center	Description
CiscoCyberVision-center-4.2.0.ova	VMware OVA file, for Center setup
CiscoCyberVision-center-with-DPI-4.2.0.ova	VMware OVA file, for Center with DPI setup
CiscoCyberVision-center-4.2.0.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-sensor-management-4.2.0.ext	Sensor management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-4.2.0.tar	Cisco IE3400, Cisco IE3300 10G, Cisco IE9300, Cisco IR1101 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64--4.2.0.tar	Cisco IE3400, Cisco IE3300 10G, Cisco IE9300 Cisco IR1101 Active Discovery sensor installation and update file
CiscoCyberVision-IOx-IC3K-4.2.0.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.2.0.tar	Cisco Catalyst 9x00 and Cisco Catalyst IR8340 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.2.0.tar	Cisco Catalyst 9x00 and Cisco Catalyst IR8340 Active Discovery sensor installation and update file
Updates	**Description**
CiscoCyberVision-Embedded-KDB-4.2.0.dat	KnowledgeDB embedded in Cisco Cyber Vision 4.2.0
CiscoCyberVision-update-center-4.2.0.dat	Center update file for upgrade from release 4.0.x or 4.1.x to release 4.2.0
CiscoCyberVision-update-sensor-4.2.0.dat	Cisco IC3000 Sensor and Sentryo Sensor3, 5, 7 update file for upgrade from release 4.0.x or 4.1.x to release 4.2.0
CiscoCyberVision-update-combined-4.2.0.dat	Center, IC3000 Sensor and Legacy Sensor update file from GUI for upgrade from release 4.0.x or 4.1.x to release 4.2.0

Cisco Cyber Vision Center 4.2.0 can also be deployed on AWS (Amazon Web Services) and Microsoft Azure.

The Cisco 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

The Cisco Cyber Vision Center Plan can be found 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

- Cisco Cyber Vision GUI User Guide:

  Cisco_Cyber_Vision_GUI_User_Guide.html
- Cisco Cyber Vision GUI Administration User Guide:

  Cisco_Cyber_Vision_GUI_Administration_Guide.html
- Cisco Cyber Vision Architecture Guide

  Cisco Cyber Vision Architecture Guide
- Cisco Cyber Vision Active Discovery Configuration Guide

  Cisco Cyber Vision Active Discovery Configuration Guide
- Cisco Cyber Vision Sensor Application for Cisco Switches Installation Guide:

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

  Cisco_Cyber_Vision_Network_Sensor_Installation_Guide_for_Cisco_IR1101_4_0_0.pdf
- Cisco Cyber Vision Network Sensor Installation Guide for Cisco IC3000:

  Cisco_Cyber_Vision_Network_Sensor_Installation_Guide_for_Cisco_IC3000
- Cisco Cyber Vision Network Sensor Installation Guide for Cisco IR8340:

  Cisco_Cyber_Vision_Network_Sensor_Installation_Guide_for_Cisco_IR8340
- Cisco Cyber Vision Center Appliance Installation Guide:

  Cisco_Cyber_Vision_Center_Appliance_Installation_Guide
- Cisco Cyber Vision Center VM Installation Guide:

  Cisco_Cyber_Vision_Center_VM_Installation_Guide
- Cisco Cyber Vision Center AWS Installation Guide:

  Cisco Cyber Vision for AWS Cloud Installation Guide
- Cisco Cyber Vision Center Azure Installation Guide:

  Cisco Cyber Vision for Azure Cloud Installation Guide
- Cisco Cyber Vision Integration Guide, Integrating Cisco Cyber Vision with Cisco Identity Services Engine (ISE) via pxGrid:

  Integrating-Cisco-Cyber-Vision-with-Cisco-Identity-Services-Engine-via-pxGrid_3_1_1.pdf
- Cisco Cyber Vision Smart Licensing User Guide

  Cisco_Cyber_Vision_Smart_Licensing_User_Guide