



# Release Notes for Cisco Cyber Vision Release 4.1.0

For users upgrading to 4.1.0 from previous versions, please carefully read the Cisco Cyber Vision 4.1.0 update procedure.

Compatible device list	3
Cisco Cyber Vision 4.1.0 update procedure	4
Data purge	4
Center updates	5
Architecture with Global Center	5
Architecture with one Center	7
AWS Center	8
Cisco Cyber Vision 4.1.0 important changes	9
Command line access	9
Communication port and protocol changes	9
Port	9
Protocol	10
API	10
SYSLOG	10
Cisco Cyber Vision new features and improvements	11
Sensor explorer	11
Custom User Roles	14
External Authentication - Secure LDAP	15
Center web server certificate	16
Brownfield Global Center migration	17
Cyber Vision Center SNMP monitoring	18
Cyber Vision Unicast Active Discovering	19
Introduction	19
Policies	20
Preset settings	21

SNMP Policies	22
Ethernet/IP unicast policies	23
Cyber Vision SecureX Ribbon integration	23
Cisco Cyber Vision new Center and sensor's options	25
Microsoft Azure	25
Cisco Catalyst IR8300	25
Cisco Cyber Vision Resolved Caveats	26
Cisco Cyber Vision Open Caveats	27
Links	28
Software Download	28
Related Documentation	29

## Compatible device list

Center	Description
<b>VMware ESXi OVA center</b>	VMware ESXi 6.x or later
<b>Windows Server Hyper-V VHDX Center</b>	Microsoft Windows Server Hyper-V version 2016 or later
<b>Cisco UCS C220 M5 CV-CNTR-M5S5</b>	Cyber Vision Center hardware appliance (Cisco UCS® C220 M5 Rack Server) - 16 core CPU, 64 GB RAM, 800GB drives
<b>Cisco UCS C220 M5 CV-CNTR-M5S3</b>	Cyber Vision Center hardware appliance (Cisco UCS® C220 M5 Rack Server) - 12 core CPU, 32 GB RAM, 480GB drives
<b>Sentryo CENTER10</b>	Sentryo CENTER10 hardware appliance
<b>Sentryo CENTER30</b>	Sentryo CENTER30 hardware appliance
Sensor	Description
<b>Cisco IC3000</b>	Cyber Vision Sensor hardware appliance
<b>Cisco Catalyst IE3400</b>	Cyber Vision Sensor IOx application hosted in Cisco Catalyst IE3400 Industrial Ethernet switches
<b>Cisco Catalyst IE3300 10G</b>	Cyber Vision Sensor IOx application hosted in Cisco Catalyst IE3300 Industrial Ethernet switches with 10G ports
<b>Cisco IR1101</b>	Cyber Vision Sensor IOx application hosted in Cisco IR1101 Series Industrial Integrated Services Routers
<b>Cisco Catalyst IR8300</b>	Cyber Vision Sensor IOx application hosted in Cisco Catalyst IR8300 Rugged Series Routers
<b>Cisco Catalyst 9300, 9400</b>	Cyber Vision Sensor IOx application hosted in Catalyst 9300, 9400 Series switches
<b>Sentryo SENSOR3</b>	Sentryo SENSOR3 hardware appliance
<b>Sentryo SENSOR5</b>	Sentryo SENSOR5 hardware appliance
<b>Sentryo SENSOR7</b>	Sentryo SENSOR7 hardware appliance

## Cisco Cyber Vision 4.1.0 update procedure

Cisco Cyber Vision 4.1.0 update procedure will depend on the architecture deployed and the tool used to deploy it.

**If you are currently running a version earlier than Cisco Cyber Vision 4.0.0, you must first upgrade to 4.0.0 prior upgrading to Cyber Vision 4.1.0. Versions 4.0.0, 4.0.1 and 4.0.2 and 4.0.3 can be updated to 4.1.0.**

Upgrade Path to Cisco Cyber Vision 4.1.0

Current Software Release	Upgrade Path to Release 4.1.0
If version prior to 3.2.4	Upgrade first to 3.2.4 then to 4.0.0 and finally to 4.1.0
Version 3.2.4	Upgrade first to 4.0.0 then to 4.1.0
Version 4.0.0 to 4.0.3	You can upgrade directly to Release 4.1.0

### 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 4.1.0 schema. All components, activities, flows, events, etc. will be migrated.

The new data retention policies introduced in 4.0.0 are still valid in 4.1.0. 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 to check the health of all Centers connected to the Global Center and of the Global Center itself before proceeding to the update.

To do this check, 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:~#
```

Rational: all sbs services need to run in a normal state before the update. If one of them is listed as failed it has to be fixed before the upgrade.

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-4.1.0.dat
- Navigate to Admin > System and use the System Update button and browse and select the update file.

b. Or using the command line interface (CLI):

- File= CiscoCyberVision-update-center-4.1.0.dat
- Launch the update with the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-center-4.1.0.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 Sensor is allowed, the hardware sensors (IC3000 and Sentryo SENSOR's) were updated at the same time.
- ii. If IC3000 sensor was deployed using the "Sensor management extension", it can be upgraded by "redeploying it"
- iii. If not, the update needs to be done from the Command Line (CLI):
  - File= CiscoCyberVision-update-sensor-4.1.0.dat
  - Launch the update with the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-sensor-4.1.0.dat
```

You may check the sensor version on the Administration / Sensor page, to make sure that the version is 4.1.

Note: Cisco Cyber Vision Sensor application should not be updated from the IC3000 Local manager because the configuration will be lost. In case this is done, the sensor enrollment package needs to be deployed again.

b. IOx sensors:

- i. If you have installed the sensor with the sensor management extension, the upgrade of the extension will also update all sensors reachable from the Center.
  - File = CiscoCyberVision-sensor-management-4.1.0.ext
  - Navigate to Admin > Extensions. In the Actions column, use the update button and browse to select the update file.
  - Cyber Vision sensor management extension could also be updated from the CLI with the command:

```
sbs-extension upgrade /data/tmp/CiscoCyberVision-sensor-management-4.1.0.ext
```

- ii. If a sensor was not updated by the extension update, access the sensor administration page, and use the UPDATE CISCO DEVICES button or the redeploy button to update the remaining IOx sensors connected to the Center.
- iii. If you have not installed the sensor with the sensor management extension, the upgrade of the sensor can be performed with the sensor package from the platform Local Manager or from the platform Command Line. This procedure is described in the corresponding sensors installation guides.
  - IE3x00 and IR11101 files = CiscoCyberVision-IOx-aarch64-4.1.0.tar or CiscoCyberVision-IOx-Active-Discovery-aarch64--4.1.0.tar
  - Catalyst 9300 and 9400 files = CiscoCyberVision-IOx-x86-64-4.1.0.tar or CiscoCyberVision-IOx-Active-Discovery-x86-64-4.1.0.tar.

## Architecture with one Center

In the case of a single Center, the following steps need to be followed:

1. Update the Center:

- a. Either using the graphical user interface:
  - File= CiscoCyberVision-update-combined-4.1.0.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-4.1.0.dat
  - Launch the update with the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-center-4.1.0.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 Sensor is allowed, the hardware sensors (IC3000 and Sentryo SENSOR's) were updated at the same time.
- ii. If IC3000 sensor was deployed using the "Sensor management extension", it can be upgraded by "redeploying it"
- iii. If not, the update needs to be done from the command line interface (CLI):
  - File= CiscoCyberVision-update-sensor-4.1.0.dat
  - Launch the update with the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-sensor-4.1.0.dat
```

b. IOx sensors:

- i. If you have installed the sensor with the sensor management extension, the upgrade of the extension will also update all reachable sensors.
  - File = CiscoCyberVision-sensor-management-4.1.0.ext
  - Navigate to Admin > Extensions. In the Actions column, use the update button and browse to select the update file.

Cyber Vision sensor management extension could also be updated from the CLI with the command:

```
sbs-extension upgrade /data/tmp/CiscoCyberVision-sensor-management-4.1.0.ext
```

- ii. If a sensor was not updated by the extension update, access the sensor administration page, and use the UPDATE CISCO DEVICES button or the redeploy button to update the remaining IOx sensors connected to the Center.
- iii. If you have not installed the sensor with the sensor management extension, the upgrade of the sensor can be performed with the sensor package from the platform Local Manager or from the platform Command Line. This procedure is described in the corresponding sensors installation guides.
  - IE3x00 and IR1101 files = CiscoCyberVision-IOx-aarch64-4.1.0.tar or CiscoCyberVision-IOx-Active-Discovery-aarch64--4.1.0.tar
  - Catalyst 9300 and 9400 files = CiscoCyberVision-IOx-x86-64-4.1.0.tar or CiscoCyberVision-IOx-Active-Discovery-x86-64-4.1.0.tar.

## AWS Center

In case of a center deployed in AWS, the same procedure as "One center" above has to be followed.



## Cisco Cyber Vision 4.1.0 important changes

### Command line access

A major change regarding the Center command line (CLI) access through serial console or SSH was made. The user root is no more 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 the command.

### Communication port and protocol changes

#### Port

A new port is used if the LDAP external authentication is configured over TLS/SSL. In this case the port TCP 636 is used instead of the port 389, from the Center admin interface to the Active Directory server.

#### SecureX

Cyber Vision 4.1 is now integrated with SecureX. For that integration to work, it is required to allow the connection between both the Client (web browser) and the Center admin interface to <https://securex.<region>.security.cisco.com>. <region> may either be empty for North America or "eu" for Europe or "apjc" for Asia.

#### SNMP agent

It is possible to activate an SNMP agent on Cyber Vision centers. Access to UDP port 161 from the client to the center admin interface is required to allow access to the SNMP agent and retrieve indicators.

#### Active discovery

4.1 allows to configure unicast active discovery for SNMP and Rockwell CIP protocols. Connections are established from sensors where dedicated IP addresses are set in each of the subnets where devices are polled. As connections are direct (same LAN) no additional route or firewall rule is needed, but connections from the sensor to devices using TCP port 44818 (Rockwell) and UDP or TCP port 161 (SNMP) will be made.

#### Hardware sensor management (IC3000)

SSH is no more required for normal operation. Still used for sensor software upgrade, but upgrades can also be performed by redeploying the sensor.

**Protocol**

No modification in 4.1.0.

**API**

No modification in 4.1.0.

**SYSLOG**

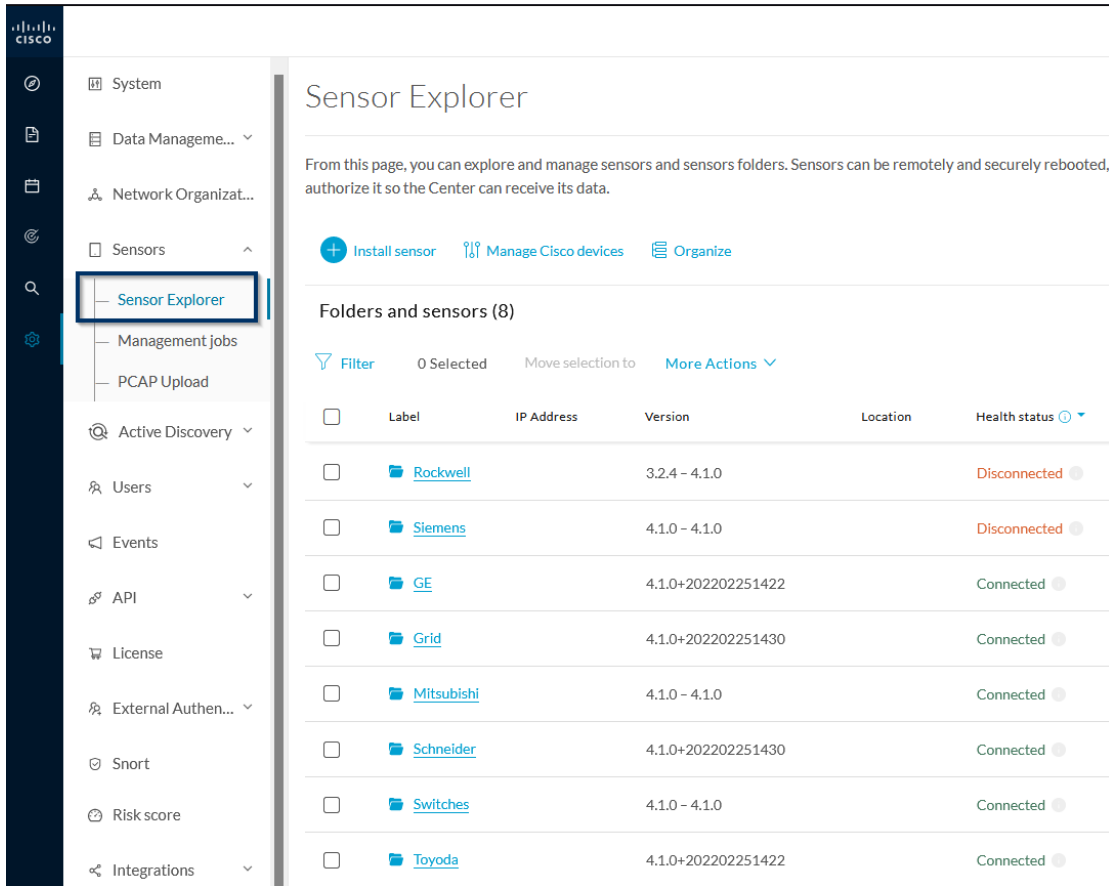
No modification in 4.1.0.

## Cisco Cyber Vision new features and improvements

### Sensor explorer

The old Cisco Cyber Vision Sensors page was redesigned and improved. A new Sensor Explorer page is now available in the administration menu of Cisco Cyber Vision:

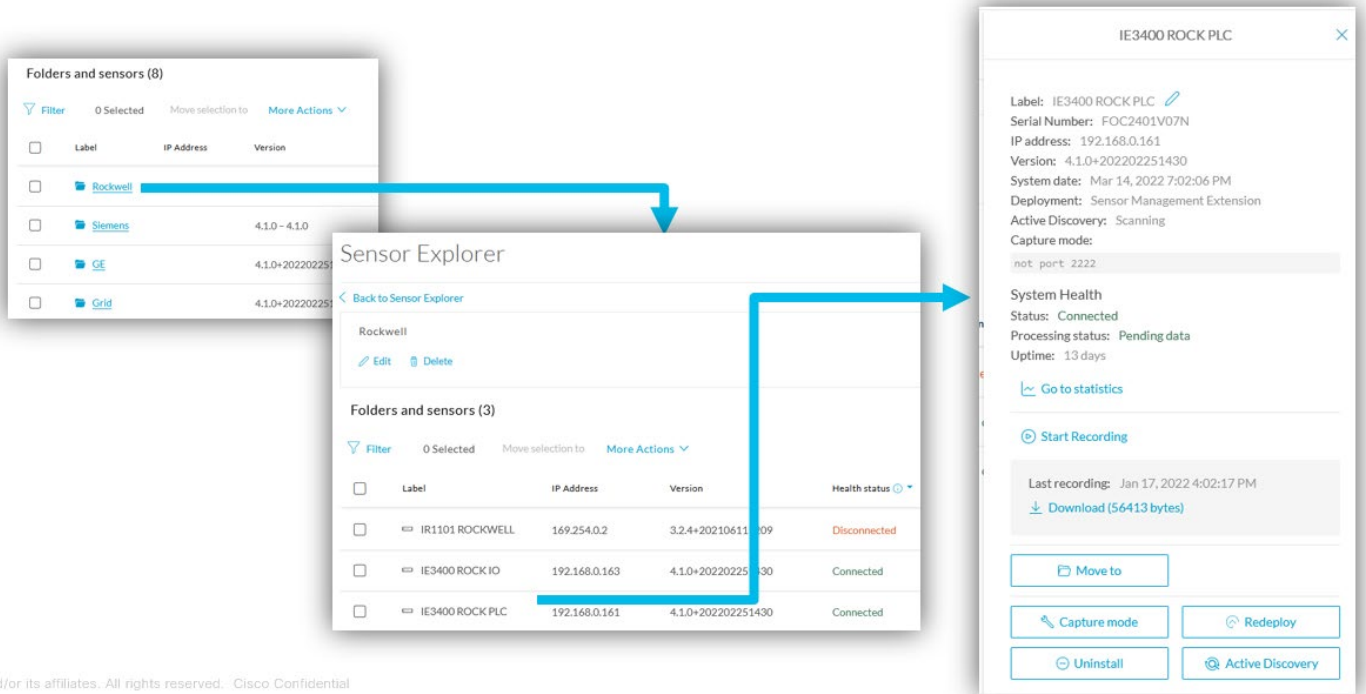
Cisco Cyber Vision new Sensor Explorer menu



This new design will improve sensor management, especially when there are many. The new folder feature will allow you to organize sets of sensors and make navigation between groups and bulk actions easier. Sensor's health is also easier to check.

Sensor action buttons and related information were moved to an overlay window which appears on the right side of the screen as you click a sensor in the list:

Cisco Cyber Vision new Sensor Explorer menu – sensor details



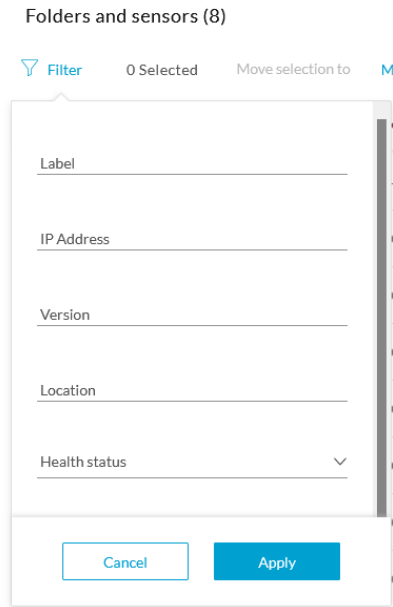
and/or its affiliates. All rights reserved. Cisco Confidential

You can perform several bulk actions on the sensors, such as:

- Filter sensors on the sensors list
- Move sensors into folders
- Delete folders
- Reboot/Shutdown sensors on a selected folder

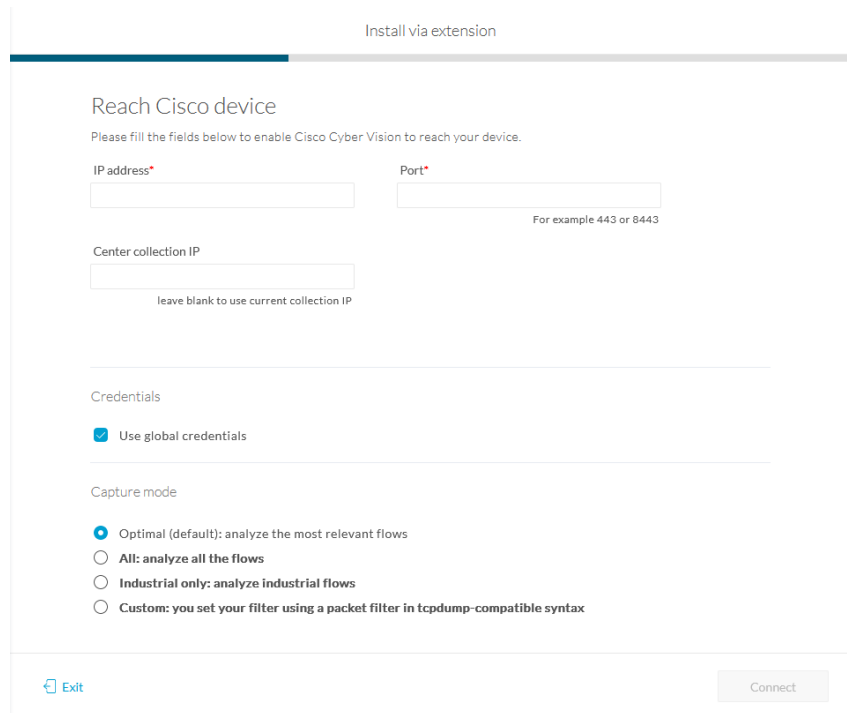
For example, a new menu will allow you to filter folders and sensors:

Cisco Cyber Vision new Sensor Explorer menu – filters



The user interface to install or redeploy a sensor was redesigned to guide you through the sequence of steps:

Cisco Cyber Vision new Sensor Explorer menu – New setup screens



## Custom User Roles

In addition to the four historical predefined roles (Admin, Auditor, Operator and Product), this new feature will allow you to easily create custom user roles.

These can be managed in the new Role Management administration page. You just need to create a new role by duplicating and modifying existing roles and setting read/write accesses to distinct parts of Cisco Cyber Vision. Roles can then be assigned to a Cisco Cyber Vision user.

**Note:** The minimum default access is read-only for the Explore page.

Cisco Cyber Vision Custom User Roles

The screenshot displays the 'Role management' page in Cisco Cyber Vision. A sidebar on the left contains navigation options: System, Data Management, Network Organization, Sensors, Active Discovery, Users (selected), Events, API, License, External Authentication, Snort, Risk score, and Integrations. The 'Users' section is expanded to show 'Management', 'Role Management', and 'Security settings'. The main content area is titled 'Role management' and includes a sub-header: 'From this page, you can create Cisco Cyber Vision user roles, edit and delete them.' Below this, there are tabs for 'ADMIN\_ESCALATION', 'NEWCCVGROUP' (active), 'ADMIN', 'AUDITOR', 'OPERATOR', and 'PRODUCT'. The 'NEWCCVGROUP' role is selected, showing a 'demo' user. A table lists 'Administrative Rights' for various system components, with 'read' and 'write' access permissions indicated by checkboxes.

Administrative Rights	read	write		read	write
Active Discovery	<input type="checkbox"/>	<input type="checkbox"/>	API	<input type="checkbox"/>	<input type="checkbox"/>
Center Certificate	<input type="checkbox"/>	<input type="checkbox"/>	Data Management	<input type="checkbox"/>	<input type="checkbox"/>
Events	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Events Settings	<input type="checkbox"/>	<input type="checkbox"/>
Explore	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Extensions	<input type="checkbox"/>	<input type="checkbox"/>
External Authentication	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Integrations	<input type="checkbox"/>	<input type="checkbox"/>
License	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Monitor	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Network Organization	<input type="checkbox"/>	<input type="checkbox"/>	Reports	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Risk Score	<input type="checkbox"/>	<input type="checkbox"/>	Secure X	<input type="checkbox"/>	<input type="checkbox"/>
Security Settings	<input type="checkbox"/>	<input type="checkbox"/>	Sensors	<input type="checkbox"/>	<input type="checkbox"/>
SNMP	<input type="checkbox"/>	<input type="checkbox"/>	Snort	<input type="checkbox"/>	<input type="checkbox"/>
System	<input type="checkbox"/>	<input type="checkbox"/>	User Admin	<input type="checkbox"/>	<input type="checkbox"/>
Vulnerability Management	<input type="checkbox"/>	<input type="checkbox"/>			

A 'Save' button is located at the bottom right of the interface.

## External Authentication - Secure LDAP

The existing LDAP feature to use an external user directory was improved. It is now possible to secure the connection with an LDAP server using TLS certificates.

Four different versions of Active Directory are supported: Windows Server 2012, 2016, 2019 and 2022.

Redundant LDAP servers are also supported by Cisco Cyber Vision.

In addition, custom and default roles can be mapped to groups in Active Directory.

Cisco Cyber Vision LDAP connection

[EDIT LDAP SETTINGS](#) ✕

---

SettingsRole Mapping

---

LDAP over TLS/SSL

Use self signed certificate

\* Primary Server Address

\* Primary Server Port


Secondary Server Address

Secondary Server Port

\* Base DN ⓘ

\* Server Response Time ⓘ

\* CA Trust Chain

  
Choose a file or drag and drop to upload  
Accepted files: .pem

## Center web server certificate

In addition to the historical auto-signed certificate, Cyber Vision Center web server now gives the possibility to use an enterprise certificate. A new Center certificate page is available in Cisco Cyber Vision’s administration menu from where you can upload a .p12 file or generate a CSR to generate and import a complete PEM bundle (concatenated CA, subCA, certificate).

Cisco Cyber Vision LDAP connection

- System
- Data Management
- Network Organization
- Sensors
- Active Discovery
- Users
- Events
- API
- License
- External Authentic...
- Snort
- Risk score
- Integrations
- Extensions
- Center certificate**

### Center web server certificate

From this page, you can check your current web server certificate basic information and replace it with a new one. This certificate is also relevant for the API.


Fingerprint:	65ebcf80c2c3973e4c9d34b68e5cdb1f0a184119bc4f9bf5efd32c44708e57db
Issuer:	CN=Cisco Cyber Vision Center CA CENTERVM-INT17023
Subject Name:	Center102
Alternates Names:	Center102
Expires:	Mon Apr 29 2024 19:02:01 GMT+0200

Update with a new web server certificate:

Upload a .p12     Generate a CSR (RSA 2048)

Password of the certificate (optional)

Please import a PKCS#12 file



Choose a file or drag and drop to upload



## Brownfield Global Center migration

The synchronization between Centers and a Global Center was completely redesigned in Cisco Cyber Vision 4.1.0. The new software architecture significantly improves:

- Data synchronization
- Connection of a synchronized Center to a Global Center without data loss
- Center enrollment/unenrollment
- Performances and robustness

Cisco Cyber Vision Global Center System management

	Center Name	IP	Version	Enrollment status	Up time	Connectivity Status	Action
+	Center 159	10.2.3.159	SBS: 4.1.0+202202021811 KDB: 20220202	Synchronization delay: 1 sec	24 days 9 hrs 15 mins 3 secs	Connected	Unenroll
+	Center 160b	10.2.3.160	SBS: 4.1.0+202202021811 KDB: 20220202	Synchronization delay: 1 sec	24 days 9 hrs 14 mins 55 secs	Connected	Unenroll
+	Center 161	10.2.3.161	SBS: 4.1.0+202202021811 KDB: 20220202	Enrolled	24 days 7 hrs 43 mins 29 secs	Connected	Unenroll

## Cyber Vision Center SNMP monitoring

SNMP can now be used for remote monitoring of Cisco Cyber Vision Centers.

Cisco Cyber Vision version 4.1.0 supports:

- SNMP v2c with a community for authentication
- SNMP V3 with a username for authentication (NoAuthNoPriv)
- SNMP V3 with a username and password for authentication (AuthNoPriv)
- SNMP V3 with a username and password for authentication and encryption (AuthPriv).

A new SNMP page in the admin menu will allow you to enable monitoring and add required settings:

Cisco Cyber Vision center SNMP settings

SNMP Global Configuration

SNMP protocol allows remote monitoring of network and equipment.

This page allows you to configure the configuration used by the SNMP agents on this center and on connected sensors.

Note that changing the configuration on this page does not automatically replace the configuration used on sensors.

SNMP agent

Configuration

Monitoring hosts (IPv4):

Version:  3  2c

Security type:

Username:

Authentication:

Privacy:

Trap

In addition to SNMP monitoring, enabling traps will let Cisco Cyber Vision send unrequested messages to the SNMP manager. Traps can be activated for CPU or Memory consumptions and rates and thresholds can be customized.

Cisco Cyber Vision center SNMP trap settings

Trap

Engine ID:

Type: CPU      Rate:       Threshold:

Type: RAM      Rate:       Threshold:

## Cyber Vision Unicast Active Discovering

### Introduction

Cisco Cyber Vision Sensors can now send unicast messages to devices. Available unicast discovery protocols are SNMP and Ethernet/IP (ENIP). This feature will offer better visibility when broadcast discovery is limited by network architecture or sensor placement, it enables advanced discovery inquiries such as backplane configurations.

Unicast Active Discovery packets will only work on LAN and cannot be routed: for each subnet to be “discovered” a dedicated IP must be provisioned and will be activated on a sensor with Active Discovery feature enabled.

The unicast Active Discovery configuration is more complex than the Broadcast one. It consists of the following steps:

1. Configure the sensor
  - a. Add the necessary interfaces to join the network
  - b. Deploy the Active Discovery sensor application

2. Define Active Discovery Policies

A policy is used by a preset to define the list of broadcast and unicast protocols used by selected sensors. Policies also list different protocol parameters.

3. Associate a policy to a preset

Active Discovery will use preset definition to run. The sensors selected in the preset filters will be used as scanner. The list of components with an IPv4 will be used by the scanner as the list of devices to scan.

In the preset settings, the scanning schedule will also be defined.

## Policies

New Active Discovery Policies will give you full control of how Active Discovery is performed:

- Protocol to use for broadcast and unicast discovery
- Protocol parameters

A new Policies page is available in the Cisco Cyber Vision administration menu to manage and configure Active Discovery policies.

Cisco Cyber Vision Policies Management

The screenshot displays the 'Active Discovery policies' management page. On the left is a navigation sidebar with the 'Policies' option selected under the 'Active Discovery' section. The main content area features a table listing various policies and their associated preset counts. Below the table is a pagination control showing '1' of 1 items and a '+ Create policy' button.

Name	Number of associated presets
All Broadcast + snmp	4
CAT9300	0
IC3000 Siemens old	0
ROCKWELL_ActivDisc	1
Rockwell	0
SIEMENS_ActivDisc	0
Siemens	1
rockwell_Sensors	1

## Preset settings

Additional parameters were added in the Active Discovery preset settings:

- Policies need to be associated to Cyber Vision Presets. Active Discovery cannot run by error: users must select a policy.
- Ability to run once or schedule regular discovery to keep inventory up to date.

**Cisco Cyber Vision Active Discovery Preset Settings**

ACTIVE DISCOVERY SETTINGS X

---

Active Discovery policies

Use Active Discovery

Name	Enabled broadcast protocols	Configured unicast protocols
<input type="radio"/> All Broadcast + snmp	EtherNet/IP, SiemensS7, Profinet	SNMPv2c
<input type="radio"/> CAT9300	EtherNet/IP, SiemensS7, Profinet, ICMPv6	None
<input type="radio"/> IC3000 Siemens old	SiemensS7, Profinet	None
<input checked="" type="radio"/> ROCKWELL_ActivDisc	EtherNet/IP	EtherNet/IP
<input type="radio"/> Rockwell	EtherNet/IP, SiemensS7, Profinet	None
<input type="radio"/> SIEMENS_ActiveDisc	SiemensS7, Profinet	None
<input type="radio"/> Siemens	EtherNet/IP, SiemensS7, Profinet	None
<input type="radio"/> rockwell_Sensors	EtherNet/IP, ICMPv6	None

< 1 >

Schedule broadcast mode       Schedule unicast mode

Days

M T W T F S S

Time

0:05

Days

M T W T F S **S**

Time

11:00

### SNMP Policies

SNMP settings available for Active Discovery give the user the ability to choose the version of SNMP to use and the level of authentication and encryption.

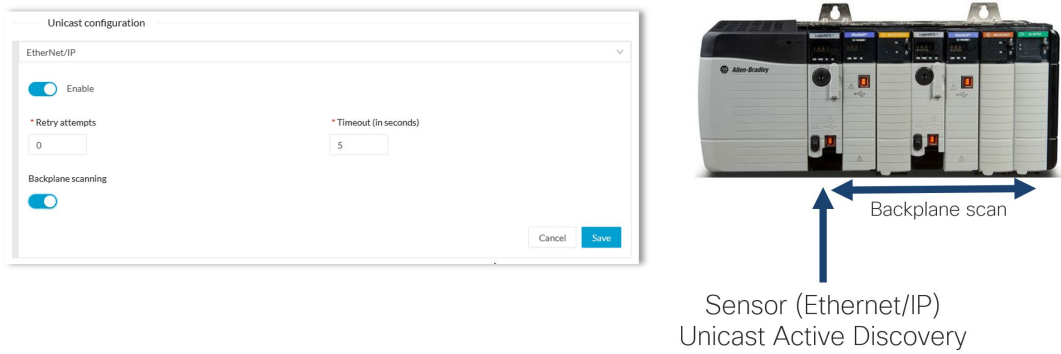
Version	Level	Authentication	Encryption
SNMPv1 optional (Fallback when v2c failed)	noAuthNoPriv	Community String	
SNMPv2c	noAuthNoPriv	Community String	
SNMPv3	noAuthNoPriv	Username	
SNMPv3	AuthNoPriv	MD5 or SHA	
SNMPv3	AuthPriv	MD5 or SHA	AES or DES

Cisco Cyber Vision Active Discovery SNMP Settings

### Ethernet/IP unicast policies

Ethernet/IP settings let the user choose whether the backplane is monitored or not. If this option is selected, the scanner will scan all chassis slots:

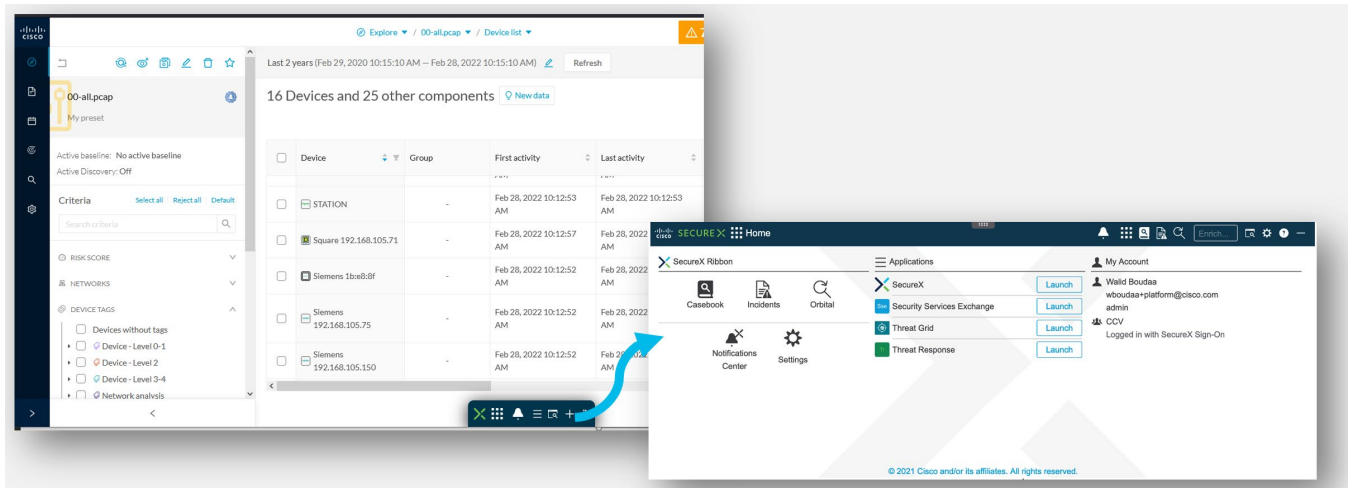
Cisco Cyber Vision Active Discovery Ethernet/IP Settings



### Cyber Vision SecureX Ribbon integration

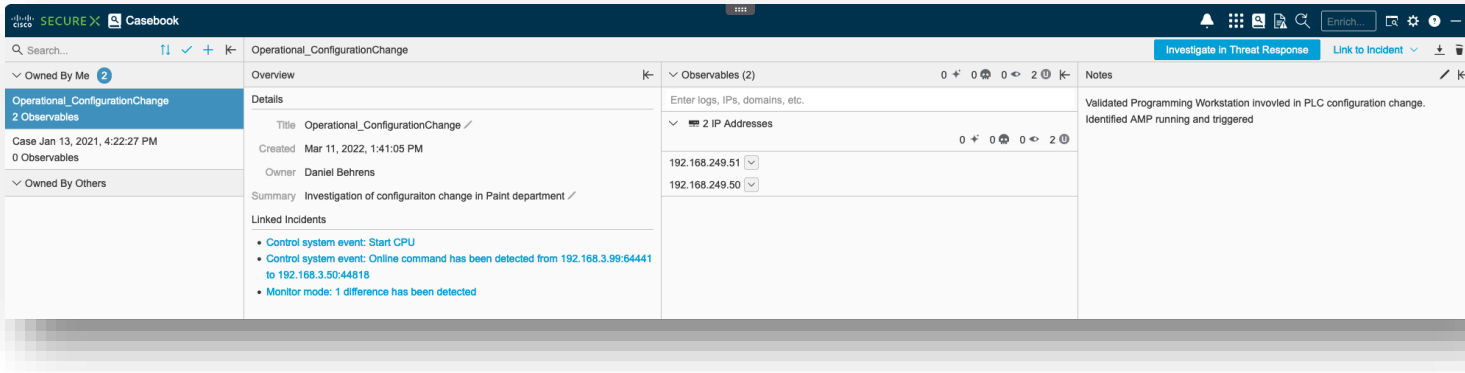
Cisco SecureX Ribbon is now available in Cisco Cyber Vision. It gives a unified visibility and accelerates incident response using Cisco Cyber Vision observables.

Cisco Cyber Vision SecureX Ribbon



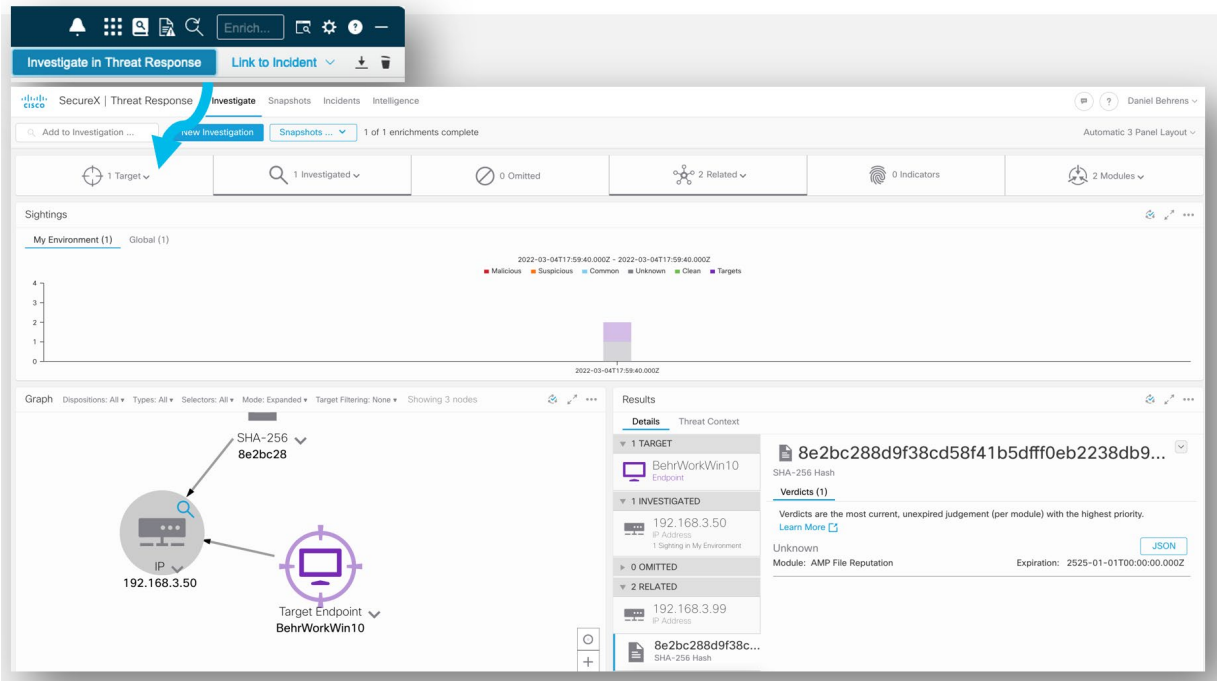
SecureX Ribbon gives access to the Casebook to simplify and streamline your investigative processes for security incidents.

Cisco Cyber Vision SecureX Casebook



SecureX Threat Investigation is also accessible from the ribbon to investigate in Cisco SecureX Threat Response leveraging information from Cisco Cyber Vision. It gives a holistic view across the entire organization.

Cisco Cyber Vision SecureX Casebook





## Cisco Cyber Vision new Center and sensor's options

### Microsoft Azure

In addition to AWS, a Center can now be installed in Microsoft Azure. Center deployment is easy thanks to the Azure virtual machine customization.

Cisco Cyber Vision Center deployment in Azure

Basics Virtual Machine Settings **Cyber Vision Settings** Review + create

Configure Cyber Vision \*

**Cyber Vision configuration**

Keyboard layout \*

Center type \*

FQDN name \*

Webapp TLS certificate \*  Generate an autosigned certificate with the FQDN  
 Use a custom certificate

**DNS servers**

**i** If no servers are provided, the default provider is OpenDNS: 208.67.222.222, 208.67.220.220

**NTP servers**

**Authorized networks**

**i** If no networks are provided, the default value is to authorize evrything (0.0.0.0/0)

Json templates can be used to automatize deployments.

### Cisco Catalyst IR8300

Cisco Cyber Vision network-sensor runs on Catalyst IR8300 (FW 17.8.x). The IDS option is available (PID: CV-IDS-IR8300).

Cisco Cyber Vision Senor deployment in Catalyst IR8300



## Cisco Cyber Vision Resolved Caveats

CDETS	Description
CSCwa15184	Online licence registration fails when using a proxy
CSCwa14510	Cyber Vision Device engine sometime breaks Rockwell chassis into several devices
CSCwb18555	Fix Security issue
CSCvt81726	Fix Security issue
CSCvt81722	Fix Security issue
	Add event on Start/Stop recording on sensors (789)
	password number of days until password expiration is wrong (3797)
	ENIP Rockwell: Wrong program name on Download Program (5508)
	IEC61850 tag is missing (6865)
	Network interfaces bandwidth section has fewer tabs than expected (7170)

## Cisco Cyber Vision Open Caveats

Issues ID / CETS	Component	Description
	Center	Sensor explorer "Update Cisco Device" does not find upgradable devices (9917)
<b>CSCwb21270</b>	Center	Sensor Management extension: Sensor not able to be installed due to "duplicate" entry – Could only happen after issue during sensor deletion
<b>CSCwb12630</b>	Center + ISE	All components are not synchronized with ISE
<b>CSCwb08691</b>	Sensor DPI	T101-T104 protocol translation write command not visible in center

## Links

### Software Download

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

Center	Description
<b>CiscoCyberVision-center-4.1.0.ova</b>	VMware OVA file, for Center setup
<b>CiscoCyberVision-center-with-DPI-4.1.0.ova</b>	VMware OVA file, for Center with DPI setup
<b>CiscoCyberVision-center-4.1.0.vhdx</b>	Hyper-V VHDX file, for Center setup
<b>CiscoCyberVision-sensor-management-4.1.0.ext</b>	Sensor Management extension installation file
Sensor	Description
<b>CiscoCyberVision-IOx-aarch64-4.1.0.tar</b>	Cisco IE3400, Cisco IR1101 sensor installation and update file
<b>CiscoCyberVision-IOx-Active-Discovery-aarch64--4.1.0.tar</b>	Cisco IE3400, Cisco IR1101 Active Discovery sensor installation and update file
<b>CiscoCyberVision-IOx-IC3K-4.1.0.tar</b>	Cisco IC3000 sensor installation and update file
<b>CiscoCyberVision-IOx-x86-64-4.1.0.tar</b>	Cisco Catalyst 9x00 sensor installation and update file
<b>CiscoCyberVision-IOx-Active-Discovery-x86-64-4.1.0.tar</b>	Cisco Catalyst 9x00 Active Discovery sensor installation and update file
Updates	Description
<b>CiscoCyberVision-Embedded-KDB-4.1.0.dat</b>	KnowledgeDB embedded in Cisco Cyber Vision 4.1.0
<b>CiscoCyberVision-update-center-4.1.0.dat</b>	Center update file for upgrade from release 4.0.0 or 4.0.1 to release 4.1.0
<b>CiscoCyberVision-update-sensor-4.1.0.dat</b>	Cisco IC3000 Sensor and Sentryo Sensor3, 5, 7 update file for upgrade from release 4.0.0, 4.0.1 or 4.0.2 to release 4.1.0
<b>CiscoCyberVision-update-combined-4.1.0.dat</b>	Center, IC3000 Sensor and Legacy Sensor update file from GUI for upgrade from release 4.0.0, 4.0.1 or 4.0.2 to release 4.1.0

Cisco Cyber Vision Center 4.1.0 can also be deployed on AWS (Amazon Web Services). The Cyber Vision Center AMI (Amazon Machine Image) can be found on the AWS Marketplace:

<https://aws.amazon.com/marketplace/seller-profile?id=e201de70-32a9-47fe-8746-09fa08dd334f>

<https://aws.amazon.com/marketplace/search/results?searchTerms=Cisco+Cyber+vision>

## Related Documentation

**Cisco Cyber Vision documentation:** <https://www.cisco.com/c/en/us/support/security/cyber-vision/series.html>

- Cisco Cyber Vision GUI User Guide:  
[Cisco Cyber Vision GUI User Guide.html](#)
- Cisco Cyber Vision Network Sensor Installation Guide for Cisco IE3300 10G, IE3400 and Catalyst 9300:  
[Installation Guide for Cisco IE3300 10G Cisco IE3400 and Cisco Catalyst 9300](#)
- 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 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 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](#)