Cisco Cyber Vision Release Notes, Release 5.2.x

April 2025

Introduction to Cisco Cyber Vision

Cisco Cyber Vision helps industrial organizations improve operational resilience by providing continuous visibility into operational technology (OT) security posture. Cisco Cyber Vision equips you with the required insights to build secure industrial networks, reduce downtime, and enforce cybersecurity policies through seamless integration with the IT security operations center. Cisco Cyber Vision enables easy deployment within an industrial network.

Cisco Cyber Vision offers the following capabilities:

- Unmatched visibility on all assets connected to the industrial network, including their detailed profiles and communication patterns.
- Enhanced view of the OT security posture, including asset vulnerabilities, risk scores, intrusions, malicious activities, and abnormal behaviors.
- Automated network segmentation by grouping assets into zones and sharing this information with Cisco Secure Firewall or Cisco ISE for enforcement.
- Reporting to help stakeholders implement security best practices and drive compliance with industry standards and regulations.
- Extends IT security operations to OT by integrating with security, network management, or any custom tool. Cisco Cyber Vision helps provide rich context on OT assets and communication activities to help gain a unified view of both IT and OT domains.

What's new

Release 5.2.1

New and changed diagnostic files

Newly added diagnostic files:

- A CSV list of sensors
- Logs for LDAP settings

The systemctl diagnostic file is enhanced to show all stopped Cyber Vision services.

Sensor-specific diagnostic logs

A diagnostic log file is generated for each sensor, with the file name containing the name of the sensor and the Center that it is associated with.

Monitor mode enhancement

The scope of Cyber Vision Center Service Status is enhanced to cover all Cyber Vision services. For any failing service, a warning is displayed in the Center for your action.

Release 5.2.0

Active Discovery as an active probe on a Center interface

Configure Active Discovery on a center interface to transform it into an active probe. Using the probe, you can send packets based on user-configured protocols and frequencies and discovers network devices that sensors might not detect.

It is especially useful for identifying silent devices like certain PLCs, by prompting them to respond to the Center. The responses include device details like model and vendor references, helping you identify more vulnerabilities.

New Active Discovery protocol support

The Hirschman broadcast HiDiscovery protocol is now supported.

Reporting device license requirements

You can view license requirements for the devices in your network in the following reports:

1. From the **Explore > *<choose a preset>* > Device List** page, you can download a CSV file containing device details. This CSV file now includes a **License Req** column, which indicates whether the device consumes a license with a **Yes** or **No**.

2. Device inventory reports on the **Reports** page now include a summary of the number of devices in your network that require a license.

Diagnostic logs enhancements

The following logs are now available:

1. Hourly compilation of RabbitMQ queues, and the message count for each queue. These logs contain the data for the last seven days.

2. Hourly compilation of data regarding components, devices, activities, flow properties and statistics, variables, internal communications, events, and sensors. These logs contain the data for the last 30 days.

DPI

New protocol

Siemens LOGO! compact PLC protocols are now supported.

Enhanced protocols

The following protocols are enhanced:

1. Moxa Remote Gateway detection
2. Codesys TCP/UDP V3 improvements
3. Siemens S7plus—turns backplane scan into rack and slot

There are performance improvements for all protocols to decrease flowtable sizes by removing unused/expensive properties

FIPS release

A FIPS-compliant Cisco Cyber Vision Center package is now available. The Federal Information Processing Standard (FIPS) 140-3 is a U.S. government standard for specific security requirements for cryptographic modules. This standard applies to all federal agencies that use cryptography-based security systems to protect sensitive information in computer and telecommunication systems.

If you do not require FIPS compliance for your organization, download the standard release of Cisco Cyber Vision.

FIPS build limitations

- Sensors running the FIPS build of the sensor application can only be enrolled to Center instances running the FIPS build of CV Center.
- By design, it is not possible to cross-update or downgrade from a non-FIPS Center to a FIPS Center, or the other way around.
- IC3000 sensors are not supported as IC3000 doesn't have a FIPS version of the platform firmware and the resulting deployment cannot be considered FIPS-compliant.
- The Cyber Vision sensor management extension is not supported. Sensor deployment must be done manually or using other automation tools such as Cisco Catalyst SD-WAN or Ansible playbooks.
- The Cyber Vision products published in public cloud marketplaces like AWS Marketplace are not FIPS-compliant. Cyber Vision is not supported on AWS GovCloud and other non-standard cloud environments.

Interactive Help

Cisco Cyber Vision offers contextual help through the Interactive Help feature. The Interactive Help menu offers easy access to a wide range of documentation resources, and to step-by-step walkthroughs of select taskflows.

Interactive Help is enabled by default. To disable the feature in your Cisco Cyber Vision center, go to Admin > System. The Interactive Help plugin area contains a toggle button for the feature.

Cisco may collect some anonymous product usage behavior data in accordance with the Cisco End User License Agreement and the Cisco Privacy Statement for optimal delivery of Interactive Help.

LDS support for user authentication

Cisco Cyber Vision Center now supports user authentication through Lightweight Directory Services (LDS).

Purge multiple VLAN components

The sbs-db-purge-components command is enhanced to allow the removal of multiple components associated with a VLAN.

CEF support for syslog configuration

New syslog configurations in the Cisco Cyber Vision Center require use of the Common Event Format (CEF) standard.

Exising syslog configurations that use non-CEF message formats are not affected in Cisco Cyber Vision Release 5.2.x.

Non-CEF message formats may not be supported in later releases of Cisco Cyber Vision.

Beta UI

Cisco Cyber Vision Center offers a beta UI experience, with informative, easy-to-handle dashboards that present data on assets, vulnerabilities, alerts, and organization hierarchies. You can quickly apply data filters to view necessary information.

This UI experience is a beta feature. To access the beta UI and its features, write to cv-beta@cisco.com. You will receive the command to enable the Cisco Cyber Vision Beta UI in addition to the existing classic UI.

You can also configure functional groups in the beta UI, and assign data sources to organization hierarchies.

To configure network definitions, sensors, and PCAPs, you must continue to use the classic UI. The overall task flows of Cisco Cyber Vision are currently spread across the classic and beta UIs, with the beta UI offering enhanced visualization of the center's data.

Beta UI Enhancements

- User profile: The user profile is now displayed in the top banner of the Beta UI. The profile section displays the email id or username, or both, of a user, based on where user information is stored (Cisco Cyber Vision database or LDAP directory).
- The left menu in the Beta UI is collapsible.
- You can now log out from the Cisco Cyber Vision Center through the Beta UI.
- Session expiry: If a session is inactive for an hour, you must log into the Cisco Cyber Vision Center again.

Communications map enhancements

The communications map displays an overview of all the communication events between connected assets. The following enhancements are now available:

- Apply a time filter to the map to view communications in a specific period.
- Group assets by the subnet or functional group that they belong to to organize your communication map.

- Click an asset for a line graph representation of data flow. You can filter the graph by time and protocol.

Cisco Security Risk Score

Cisco Cyber Vision Center now presents a Cisco Security Risk Score for the vulnerabilities displayed. The risk score is based on Cisco Vulnerability Management's predictive model. In Cisco Cyber Vision, the risk score includes factors of exploitability and dark web activity for topical context about risk severity to help prioritize vulnerability management.

Rack slot information for modular PLCs

The asset summary page for modular PLCs includes information on rack slots. For each slot on a modular PLC, the model name, slot type, firmware version, and serial number are displayed.

Rerun functional group suggestions

You can regenerate functional group suggestions at any time in the Asset Visibility > <choose an asset> > Communications page. You can rerun asset data at multiple levels to receive specific functional group suggestions:

- Data associated with one sensor
- Data associated with one asset
- Data associated with an existing functional group
- All the data in the Cisco Cyber Vision center

When you accept a functional group suggestion, existing functional groups may be modified to ensure an asset is part of any one functional group.

Heat maps for alerts

The Alerts page displays a heat map to help you quickly visualise alert trends. The map spans the last 7 days, broken into two-hour segments.

Hover over a segment to view the alert count.

Enable syslog notification for alert types

You can choose to send syslog notifications to a connected syslog server for an alert type. Syslog notifications are enabled by default for new and existing alert types in your Center. You can choose to disable the notifications in the Alerts page.

Acknowledge vulnerabilities across assets

You can view, acknowledge, or cancel acknowledgment of a vulnerability across multiple assets.

Known limitations

Cyber Vision sensor self-update

- After a Cyber Vision sensor self-update process is complete, if a platform is restarted within 5 minutes of the update the sensor returns to the previous version.
- If a Cyber Vision sensor is first updated to version n using the self-update feature, then to version n+1 with the sensor management extension, the sensor remains at version n.

Address reservation in DPI configuration

The docker reserves the first address of a defined network. You must not assign the first address when you configure the DPI interface in an Encapsulated Remote Switched Port Analyzer (ERSPAN).

Cisco Cyber Vision partition size

Cisco Cyber Vision Center system has two partitions, one for the system and one for data. The system partition size must be at least 1 GB for the upgrade process to complete successfully—a lower partition size results in upgrade failure.

If your Cisco Cyber Vision center runs 3.1.0 or earlier versions, the system partition may be 512MB which is insufficient to upgrade to Cisco Cyber Vision center release 4.4.0 and later. Contact the Cisco TAC team to get support with updating the system partition to 1 GB.

To check the system partition size of your Cisco Cyber Vision center, access the center CLI and use the command:

```
lsblk
```

Compatibility

Compatible Cyber Vision Centers

Table 1. List of Center images available for Cisco Cyber Vision Release 5.2.x.

Center	Description
OVA - Center image	Suitable for VMware ESXi 6.x or later
VHDX - Center image	Suitable for Microsoft Windows Server Hyper-V version 2016 or later

Table 2. List of marketplaces with native Center images (non-FIPS-compliant) for Cisco Cyber Vision Release 5.2.x.

Center	Description
AWS - Center AMI	Amazon Web Services center image. This Center image is the standard version and is not FIPS-compliant.
Azure - Center Plan	Microsoft Azure center plan. This Center image is the standard version and is not FIPS-compliant.

Table 3. List of centers compatible with Cisco Cyber Vision Release 5.2.x.

Center	Description
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, 800 GB 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, 480 GB drives

Compatible Sensors

Table 4. List of sensors compatible with Cisco Cyber Vision Release 5.2.x

Platform	Minimum Version	Recommended Version	Description
Cisco IC3000	1.5.1	1.5.1	Cyber Vision Sensor IOx application hosted in Cisco IC3000. This sensor is not compatibile with FIPS-compliant Cisco Cyber Vision Center.

Platform	Minimum Version	Recommended Version	Description
Cisco Catalyst IE3400	17.3.x	17.6.7, 17.9.5, or 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, or 17.12.2	Cyber Vision Sensor IOx application hosted in Cisco Catalyst IE3300 Industrial Ethernet switches with 10GbE ports
Cisco Catalyst IE3300 Cyber Vision application hosting is supported only when the platform has 4GB DRAM. All 4GB units starting with Version ID (VID) from -06. Use the CLI command show platform resources and see the Max DRAM Size field to verify if the device has a 4GB memory.	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 running IOS 17.12 minimum
Cisco IR1101	17.3.x	17.6.7, 17.9.5, or 17.12.2	Cyber Vision Sensor IOx application hosted in Cisco IR1101 Series Industrial Integrated Services Routers
Cisco Catalyst IR1800 Cisco Catalyst IR1835 with IOS 17.15 supports up to 3GB of memory allocated to IOX.	17.15.1	17.15.1	Cyber Vision Sensor IOx application hosted in Cisco IR1800 Rugged Series Routers
Cisco Catalyst IR8300	17.9.x	17.9.5 or 17.12.2	Cyber Vision Sensor IOx application hosted in Cisco Catalyst IR8300 Rugged Series Routers
Cisco Catalyst 9300, 9400 Cisco Catalyst 9400 requires IOS XE 17.5.1 minimum to deploy an IOX application without SSD	17.3.3	17.6.7, 17.9.5, or 17.12.2	Cyber Vision Sensor IOx application hosted in Catalyst 9300, 9300L, 9300X, 9400 Series switches
Docker sensors Docker sensor containers run on x86-64 and ARM64 devices, and require 4GB memory.	Ubuntu 20.04, 22.04, and 24.04 Docker 27.0	Ubuntu 24.04 Docker 27.x	Cyber Vision Sensor Docker application. See the hardware requirements for Docker sensor installation.

Centers and sensors compatibility

There is downward compatibility of one release between the global center and synchronized centers, and between centers and sensors.

- If the global Center runs release N, it can manage synchronized centers that run releases N or N-1.

  For example, a global center running release 5.0.0 can manage other centers running releases 5.0.0 or 4.4.x.

- If a center runs release N, it is compatible with sensors running releases N or N-1.

  For example, a center running release 5.0.0 can manage sensors running releases 5.0.0 or 4.4.x.

Sentryo hardware and Cisco IC3000 sensors

If you are upgrading to Cisco Cyber Vision release 4.4.0 or later releases:

1. Sentryo hardware are not supported. Remove any connected Sentryo hardware before you start the upgrade process.

2. Cisco IC3000 sensors must run Cyber Vision center release 4.3.0 or later releases. If the Cisco IC3000 sensors connected to your Cisco Cyber Vision center run an earlier Cyber Vision release, upgrade them to 4.3.0 or later releases before you initiate the upgrade process.

Fresh Installs and Upgrades

Install Cisco Cyber Vision

1. In the case of fresh installs, go to Cisco Software Central, and in the **Download and Upgrade** section, click **Access Downloads**.
   a. Use the search button to find Cyber Vision.
   b. Choose Cyber Vision Center or Cyber Vision FIPS Software.
   c. Choose release 5.2.x.
2. From the list of software displayed, download the following:
   a. One center OVA or VHDX file, depending on your network architecture. You can download FIPS or standard version of the center.
   b. Cisco Cyber Vision Sensor Management Extension (not available for FIPS centers)
   c. Cisco Cyber Vision Reports Management Extension

Installation guides

- Cisco Cyber Vision Center VM Installation Guide, Release 4.4.0 and Later
- Cisco Cyber Vision Center Appliance Installation Guide, Release 4.4.0 and Later
- Cisco Cyber Vision for Azure Cloud Installation Guide, Release 4.4.0 and Later
- Cisco Cyber Vision for the AWS Cloud Installation Guide, Release 4.4.0 and Later

Install extensions

Software type	GUI process	CLI process
Sensor Management Extension (not compatible with FIPS-Compliant Center) Install this extension in connected centers, or in the single center in your network.	1. In your Cisco Cyber Center, go to **Admin > Extensions**. 2. For the sensor management extension list item, click **Update**. 3. Upload the extension file that you downloaded from Cisco Software Central.	In the Cisco Cyber Vision center CLI, use the command: `sbs-extension upgrade --run /data/tmp/CiscoCyberVision-sensor-management-<LATEST-VERSION>.ext`
Reports Management Extension	1. In your Cisco Cyber Center, go to **Admin > Extensions**. 2. For the reports management extension list item, click **Update**. 3. Upload the extension file that you downloaded from Cisco Software Central.	In the Cisco Cyber Vision center CLI, use the command: `sbs-extension upgrade --run /data/tmp/CiscoCyberVision-report-management-<LATEST-VERSION>.ext`

Upgrade considerations

If you are upgrading to Cisco Cyber Vision release 5.2.x from an earlier release, see the Cisco Cyber Vision Upgrade Guide.

Upgrade path

Table 5. Upgrade paths to Cisco Cyber Vision Center Release 5.2.x

Current Software Release	Upgrade Path to Release 5.2.x
4.3.x, 4.4.x, 5.x.x	Upgrade directly to 5.2.x
4.2.x	Upgrade first to 4.3.0 then to 5.2.x
4.1.x	Upgrade first to 4.3.0, then to 5.2.x
4.0.x	Upgrade first to 4.1.4, then to 4.3.0, then to 5.2.x
3.2.4	Upgrade first to 4.0.0, then to 4.1.4, then to 4.3.0, then to 5.2.x
3.2.3 or earlier	Upgrade first to 3.2.4, then to 4.0.0, then to 4.1.4, then to 4.3.0, then to 5.2.x

Resolved Caveats

Release 5.2.1

Bug ID	Headline
CSCwo94883	Event counter discrepancy in device inventory report
CSCwp24693	Vulnerability number flapping on a Siemens device
CSCwq00338	KDB properties rule does not apply if property already exists
CSCwo88406	Sensor Management extension on Center tries to reach switch IP address even after sensor deletion
CSCwp11561	LLDP properties are not updated in 5.2.0
CSCwq07086	Active Discovery profiles weekly scheduling: discovery done on Mondays only

Release 5.2.0

Bug ID	Headline
CSCwo12515	Cyber Vision Sensor remains in previous version when a self-update is followed by a sensor management application update
CSCwn98948	Cyber Vision License: User interface issue when user changes the license ,ode
CSCwh39606	Cyber Vision Sensor onboarding, add a new option to define desired sensor name during the sensor integration
CSCwn92541	Cyber Vision extension: Unexpected behavior during extension upgrade
CSCwo44366	Cyber Vision Docker sensor: VLAN field stuck as REQUIRED on ERSPAN setup
CSCwo26730	Cyber Vision User Interface: Locked empty group management issue
CSCwn21137	Cyber Vision User Interface: Incorrect message in baseline difference acknowledgement dialog box
CSCwo42340	Cyber Vision API: Fix Fields option on component route swagger
CSCwo51248	Cyber Vision center: allow choosing webapp CSR key length

Cisco Cyber Vision Documentation

- Cisco Cyber Vision Admin Guide, Release 5.2.x
- Cisco Cyber Vision Upgrade Guide, Release 5.1.x
- Cisco Cyber Vision CLI Guide
- Cisco Cyber Vision Docker Sensor Configuration Guide
- Cisco Cyber Vision Active Discovery Configuration Guide, Release 5.2.x
- Cisco Cyber Vision Network Sensor Installation Guide for Cisco IC3000, Release 5.1.x
- Cisco Cyber Vision Network Sensor Installation Guide for Cisco IR8340, Release 5.1.x
- Cisco Cyber Vision Network Sensor Installation Guide for Cisco IR1101 and IR1800, Release 5.1.x
- Cisco Cyber Vision Sensor Application for Cisco Switches Installation Guide, Release 5.1.x
- Integrate Cisco Cyber Vision with Cisco Identity Services Engine (ISE) through pxGrid, Release 4.4.1 and Later Releases
- Cisco Cyber Vision Center Appliance Installation Guide, Release 4.4.0 and Later
- Cisco Cyber Vision Center VM Installation Guide, Release 4.4.0 and Later
- Cisco Cyber Vision for Azure Cloud Installation Guide, Release 4.4.0 and Later
- Cisco Cyber Vision for the AWS Cloud Installation Guide, Release 4.4.0 and Later
- Cisco Cyber Vision syslog notification format Configuration Guide