Release Notes for Cisco Cyber Vision Center, Release 5.4.x

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Cyber Vision, Release 5.4.x 3
New software features 3
FIPS release 5
Changes in behavior 6
Resolved issues 6
Known issues 7
Compatibility 8
Scalability 10
Supported software packages 10
Related resources 12
Legal information 12

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Cyber Vision, Release 5.4.x

Cisco Cyber Vision Release 5.4.x delivers a range of new features and enhancements for both Center and Sensor components, focused on simplifying deployment, improving user access controls, enhancing communication and vulnerability analysis, and streamlining large-scale sensor onboarding. These updates provide more granular network visibility, better data quality monitoring, and support for IPv6 administration, helping organizations manage industrial networks with greater efficiency, security, and ease of use.

New software features

Center features

This section provides a brief description of the new software features introduced in Cisco Cyber Vision Center in this release.

Table 1. New software features for Cisco Cyber Vision Center, Release 5.4.1

Product Impact	Feature	Description
Upgrade	Enhanced hardware support	Cyber Vision center deployments now support the Cisco UCS C225 M8N Rack Server (CV-CNTR-M8N configuration), providing greater flexibility for your infrastructure.
Greater visibility and control	Advanced DPI capabilities	The DPI engine includes these improvements to increase visibility and security across your industrial network: • GigE Vision: Added support for inspecting GigE Vision protocol traffic. • Palo Alto Networks: Improved identification accuracy for Palo Alto firewalls. • AutomationDirect: Added identification support for AutomationDirect Productivity series PLCs. • SEL-487: Enhanced MMS decoding capabilities for SEL-487 protective relays. • Siemens LOGO: Added identification support for Siemens LOGO PLC devices.

Table 2. New software features for Cisco Cyber Vision Center, Release 5.4.0

Product Impact	Feature	Description
Ease of Setup	Restrict users to a specific preset category	This feature enables precise data access control by assigning preset categories to Cyber Vision user roles, limiting users to the **Explore** menu with read-only permissions. **Note**: Once you restrict a user to a specific preset category, they will not have access to the new UI.

© 2025 Cisco and/or its affiliates. All rights reserved.

Product Impact	Feature	Description
Ease of Use	Group by network functionality in communications	The communication map displays all communications between network groups and simplifies network interaction analysis.
Ease of Use	Synchronize custom properties from Cyber Vision to Cisco ISE assets	This feature enables you to automatically synchronize custom device properties defined in Cyber Vision with your Cisco ISE assets. It ensures that asset information remains consistent and up to date across both platforms.
Ease of Use	Communication maps and their filter enhancements	Easily spot communications between assets, including those outside your active view. Communication maps highlight assets outside your active view filter with dotted lines.
Ease of Use	Network-based organization hierarchy alert configuration	You can configure alerts at the organization hierarchy level with one additional entity type: **Organization Hierarchy (Networks)**. The system changes all existing alert rules with the entity type **Organization Hierarchy** to **Organization Hierarchy (Sensors)** automatically.
Ease of Use	MITRE mapping and additional details	You can view additional information such as MITRE ATT&CK Tactic and Technique Mapping within your vulnerability views, making it easier to investigate, mitigate, and respond to security vulnerabilities of Cyber Vision assets.
Ease of Use	Consistent Groups and Subgroups on the Zones and Conduits Map	Easily visualize network communications to ensure devices remain within their designated boundaries. The system now supports one level of sub-zones within existing zones and conduits. You can quickly identify devices that should not communicate outside their networks.
Ease of Use	Mute or unmute alert instances for prohibited vendor alert type	You can use the mute and unmute feature to control prohibited vendor alerts. Mark alert instances as reviewed and not urgent, so they remain in the system but are not active. Select the duration to mute an alert instance; after that period, the alert becomes active again.
Ease of Use	PCAP capture on the Cyber Vision Center interface	You can capture PCAP data directly from the Cyber Vision Center interface, in addition to sensor-based capture.
Ease of Use	External communications visibility	View all communications between a selected asset and external entities. You can identify unexpected external communications that may expose your organization to attacks.

© 2025 Cisco and/or its affiliates. All rights reserved.

Product Impact	Feature	Description
Upgrade	Basic IPv6 Day-0 Configuration Support	Cyber Vision supports both IPv4 and IPv6 for administration services. You can access the Cyber Vision web UI and integrate with third-party solutions (Syslog, Cisco ISE, LDAP) using either IPv4 or IPv6 on center eth0. **Note**: License activation requires direct transport and does not work through Transport Gateway or HTTP/HTTPS Proxy. Sensor data collection continues on IPv4 only.

Sensor features

This section provides a brief description of the new software features introduced in Cisco Cyber Vision Sensor in this release.

Table 3. New software features for Cisco Cyber Vision Sensor, Release 5.4.x

Product Impact	Feature	Description
Ease of Use	Sensor collected data quality report	Easily monitor the quality of your sensor statistics with the **Status Overview** page. See real-time details for each sensor. Stay informed and ensure your data is always reliable.
Ease of setup	Bulk host onboarding and sensor deployment	Bulk host onboarding and sensor deployment in Cisco Cyber Vision lets you add multiple routers at once and deploy sensor applications to them using a guided, wizard-based workflow. It automates reachability and readiness checks, reduces manual effort, and accelerates large-scale rollouts.
Ease of Use	Send GPS data to Center for sensor geolocation	Sensors can now report GPS coordinates (latitude/longitude) to the Cyber Vision Center for accurate mapping and visualization of the physical location of the platform hosting the Cyber Vision sensor application.

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 that defines 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, please download the standard release of Cisco Cyber Vision.

FIPS build limitations

- Sensors running the FIPS build of the sensor application can only be enrolled in 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 vice versa.
- IC3000 sensors are not supported, as the IC3000 does not have a FIPS version of the platform firmware; therefore, the resulting deployment cannot be considered FIPS-compliant.

© 2025 Cisco and/or its affiliates. All rights reserved.

- The Cyber Vision sensor management extension is not supported. Sensor deployment must be performed manually or by using other automation tools, such as Cisco Catalyst SD-WAN or Ansible playbooks.
- The Cyber Vision sensor self-update is not supported. Sensor updates must be performed manually or by using other automation tools, such as Ansible playbooks.
- The Cyber Vision Docker sensor and Virtual Machine sensor are not supported.
- The Cyber Vision report management extension is not supported.
- Cyber Vision products published in public cloud marketplaces, such as AWS Marketplace, are not FIPS-compliant. Cyber Vision is not supported on AWS GovCloud or other non-standard cloud environments.

Changes in behavior

This section provides a brief description of the behavior changes introduced in this release.

Table 4. Behavior changes for Cyber Vision, Release Cyber Vision 5.4

Description	Behavior changes
Sensor communication changes. The system needs a port change for communication between sensors and center.	• Previously, the system used two ports: Secure syslog (TCP 10514) and AMQP (TCP 5671). • In release 5.4.0, the system uses only one port: AMQP (TCP 5671).
Cyber Vision center version 5.4.0 is no longer an NTP server.	Previously, the center acted as an NTP server for its sensors. In release 5.4.0, the center does not act as an NTP server for sensors.

Resolved issues

This table lists the resolved issues in this specific software release.

Note: This software release may contain bug fixes first introduced in other releases. To see additional information, click the bug ID to access the Cisco Bug Search Tool.

Table 5. Resolved issues for Cyber Vision, Release Cyber Vision 5.4.2

Bug ID	Description
CSCwt81742	Marmotd fails on Global Center when handling custom networks
CSCwt86153	API - Device route optimization

Table 6. Resolved issues for Cyber Vision, Release Cyber Vision 5.4.1

Bug ID	Description
CSCws49678	Flow storage issue for network previously internal, then external
CSCws67669	Security report failure
CSCws78839	XDR ribbon disappears when clicking on "Find observables"
CSCws78838	XDR Observables return an error

© 2025 Cisco and/or its affiliates. All rights reserved.

CSCws90747	Device Inventory report: Device counts by group show mangled group names
CSCws90746	Alert details: Assets have a dropdown that results in blank rows
CSCws97378	OH filter is not applied on the subnet detail map
CSCwt09193	New UI: Asset dropdown results in blank rows
CSCwt14798	Active discovery: Avoid scanning key reserved IPv4 addresses
CSCwt14799	Editing component custom properties does not trigger an ISE push
CSCwt36037	Components are assigned to more than one device
CSCwt64824	License issue in MSLA mode

Table 7. Resolved issues for Cyber Vision, Release Cyber Vision 5.4.0

Bug ID	Description
CSCwo49568	AssetGroup update is sent to Cisco ISE for omitted subnet.
CSCwq26491	Some assets do not have any associated sensor
CSCwr27273	Sensor Deployment: Unable to change the serial number of a replaced switch.
CSCwr29610	Decode error: Unknown EthernetCTP function type 49790.
CSCwr31911	Upgrading the Cyber Vision version has various effects on the KDB version.
CSCwr44097	The setup-center-CLI firewall command flushes everything.
CSCwr60394	Reaching the component limit does not generate an event.
CSCwr67069	Telnet DPI: Do not store all characters.
CSCws05661	The Network Definition page in the new user interface is slow to render.
CSCws05660	Device Inventory report failure.
CSCws25735	License page displays no information when in pending state.
CSCws27064	Cisco ISE pull does not work with a custom webapp certificate.
CSCws30764	Functional Groups: Error when trying to re-run Asset Clustering.
CSCws33762	Deleting multiple sensors can cause haproxy to stop.
CSCws51266	pg_stat_statements remain large after upgrading to 5.4.0.
CSCws69119	Center update event may be lost.
CSCwr76265	Cyber Vision Device list is unable to filter based on VLAN, group, or OS columns
CSCws27063	The Security report's vulnerability list is not accurate
CSCws48961	The SEA agent running in the Cyber Vision IOx application could, under specific circumstances, use CPU cycles even when idling

Known issues

This table lists the limitations for this release. Click the bug ID to access the Cisco Bug Search Tool and see additional information

© 2025 Cisco and/or its affiliates. All rights reserved.

Table 8. Known issues for Cyber Vision, Release Cyber Vision 5.4.x

Bug ID	Description
NA	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.
NA	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).
NA	Platforms such as the Catalyst 9350 and 9300X require trunk configurations on both AppGigabit interfaces. Because IOX connects to either interface unpredictably, you must configure both as trunks.

Compatibility

Center compatibility

Table 9. Compatibility information for Cisco Cyber Vision Center, Release 5.4.x

Product	Supported Release
VMware ESXi	6.x and later
Nutanix AOS (Acropolis OS)	6.10 and later
Microsoft Windows Server Hyper-V	2016 and later
Cyber Vision Center hardware appliance (Cisco UCS® C220 M5 Rack Server)	CV-CNTR-M5S5: 16-core CPU, 64 GB RAM, 800 GB drives CV-CNTR-M5S3: 12-core CPU, 32 GB RAM, 480 GB drives
Cyber Vision Center hardware appliance (Cisco UCS® C225 M6 Rack Server)	CV-CNTR-M6N: 24-core CPU, 128 GB RAM, two or four 1.6 TB NVMe drives

Sensor compatibility

Table 10. Compatibility information for Cisco Cyber Vision sensors, Release 5.4.x

Product	Supported Release
Cisco IC3000	Minimum version: 1.5.2 Recommended versions: 1.5.2
Cisco Catalyst IE3400	Minimum version: 17.6.x Recommended versions: 17.9.6a, 17.12.5, 17.15.3 and above
Cisco Catalyst IE3300 10G	Minimum version: 17.6.x Recommended versions: 17.9.6a, 17.12.5, 17.15.3

© 2025 Cisco and/or its affiliates. All rights reserved.

Product	Supported Release
Cisco Catalyst IE3300 (with 4GB DRAM units starting with Version ID (VID) from -06)	Minimum version: 17.12.x Recommended versions: 17.12.5, 17.15.3
Cisco Catalyst IE3500	Minimum version: 17.18.x Recommended versions: 17.18.x
Cisco Catalyst IE9300	Minimum version: 17.12.x Recommended versions: 17.12.5, 17.15.3
Cisco Catalyst IR1101	Minimum version: 17.6.x Recommended versions: 17.9.6, 17.12.4, 17.15.3
Cisco Catalyst IR1800	Minimum version: 17.6.x Recommended versions: 17.9.6, 17.12.4, 17.15.3
Cisco Catalyst IR1835	Minimum version: 17.15.1 Recommended versions: 17.9.6, 17.12.4, 17.15.3
Cisco Catalyst IR8300 (running IOS-XE 17.15.x with a minimum 3 GB memory allocated to IOx applications)	Minimum version: 17.9.x Recommended versions: 17.9.6, 17.12.4, 17.15.3
Cisco Catalyst 9300	Minimum version: 17.6.x Recommended versions: 17.9.6a, 17.12.5, 17.15.3
Cisco Catalyst 9400	Minimum versions: 17.6.x Recommended versions: 17.9.6a, 17.12.5, 17.15.3
Cisco Catalyst 9350	Minimum versions: 17.18.2 Recommended versions: 17.18.2
Ubuntu LTS	Minimum version: 20 Recommended versions: 24.04
Docker	Minimum version: 27.0 Recommended versions: 27.x
VMware ESXi	Minimum version: 6.x Recommended versions: 8.x
Rockwell Stratix 5800 Switch • 1783-MMS10EA • 1783-MMS10EAR • 1783-MMS10A • 1783-MMS10AR	Minimum version: 17.12.x Recommended versions: 17.12.4, 17.15.4

© 2025 Cisco and/or its affiliates. All rights reserved.

Upgrade compatibility

If you are upgrading to Cisco Cyber Vision release 5.4.x from an earlier release, see the Cisco Cyber Vision Upgrade Guide.

Table 11. Upgrade paths to Cisco Cyber Vision Center Release 5.4.x

Current software release	Upgrade path to Release 5.4.x
4.3.x, 4.4.x, 5.x.x	Upgrade directly to 5.4.x
4.1.x	Upgrade first to 4.3.0, then to 5.4.x

Scalability

Cyber Vision Center hardware appliance performance

Table 12. Cisco Cyber Vision Center (Standalone/Local) hardware appliance scale

Item	CV-CNTR-M6N
Max components	50,000
Max number of sensors	300
Max number of flows stored	16 million

Table 13. Cisco Cyber Vision Global Center scale

Item	CV-CNTR-M6N
Max components synced	150,000
Max number of registered centers	20

See Cisco Cyber Vision Data Sheet.

Supported software packages

This section provides information about the release packages associated with Cisco Cyber Vision, Release 5.4.x.

Center software

Table 14. Software packages for Cisco Cyber Vision Center, Release 5.4.x

Software Package	Description	Release
CiscoCyberVision-Center-5.4.x.ova	Install Cisco Cyber Vision Center on a VMware ESXi virtual machine.	5.4.x

© 2025 Cisco and/or its affiliates. All rights reserved.

Software Package	Description	Release
CiscoCyberVision-center-5.4.x.qcow2	Install Cisco Cyber Vision Center on an Oracle-hosted virtual machine.	5.4.x
CiscoCyberVision-5.4.x.vhdx	Install Cisco Cyber Vision Center on a Hyper-V VHDX virtual machine.	5.4.x
CiscoCyberVision-Center-with-DPI-5.4.x.ova	Install Cisco Cyber Vision Center with DPI capabilities on a VMware ESXi virtual machine.	5.4.x
CiscoCyberVision-reports-management-5.4.x.ext	Install the extension in a Cisco Cyber Vision Center for reports management.	5.4.x
CiscoCyberVision-sensor-management-5.4.x.ext	Install the extension in a Cisco Cyber Vision Center for sensor management. The extension is not compatible with a FIPS-Compliant Center.	5.4.x
CiscoCyberVision-update-center-fips-5.4.x.dat	Manually update a Cisco Cyber Vision Center to a FIPS-compliant Center.	5.4.x
CiscoCyberVision-fips-5.4.x.vhdx	Install FIPS-compliant Cisco Cyber Vision Center on a Hyper-V VHDX virtual machine.	5.4.x
CiscoCyberVision-center-5.4.x.qcow2	Install FIPS-compliant Cisco Cyber Vision Center on an Oracle-hosted virtual machine.	5.4.x
CiscoCyberVision-Center-fips-5.4.x.ova	Install FIPS-compliant Cisco Cyber Vision Center on a VMware ESXi virtual machine.	5.4.x

Sensor software

Table 15. Software packages for Cisco Cyber Vision sensors, Release 5.4.x

Software Package	Description	Release
CiscoCyberVision-IOx-Active-Discovery-IC3000-5.4.x.tar	Not FIPS-compliant. Cisco Cyber Vision Sensor IOx Application 5.4.x with Active Discovery for Cisco IC3000 Industrial Compute Gateway.	5.4.x
CiscoCyberVision-IOx-Active-Discovery-aarch64-5.4.x.tar	Not FIPS-compliant. Cisco Cyber Vision Sensor IOx Application 5.4.x with Active Discovery for Cisco Catalyst IE3300, IE3400, and IE9300 Rugged Series Switch.	5.4.x
CiscoCyberVision-IOx-Active-Discovery-x86-64-5.4.x.tar	Not FIPS-compliant. Cisco Cyber Vision Sensor IOx Application 5.4.x with Active Discovery for Cisco Catalyst 9300, 9400 Series Switch and for Cisco Catalyst IR8340 Rugged Router.	5.4.x
CiscoCyberVision-IOx-IC3000-5.4.x.tar	Not FIPS-compliant. Cisco Cyber Vision Sensor IOx Application 5.4.x for Cisco IC3000 Industrial Compute Gateway.	5.4.x

© 2025 Cisco and/or its affiliates. All rights reserved.

Software Package	Description	Release
CiscoCyberVision-IOx-aarch64-5.4.x.tar	Not FIPS-compliant. Cisco Cyber Vision Sensor IOx Application 5.4.x for Cisco Catalyst IE3300, IE3400, and IE9300 Rugged Series Switch and Cisco IR1101, IR1800 Integrated Services Router Rugged.	5.4.x
CiscoCyberVision-IOx-x86-64-5.4.x.tar	Not FIPS-compliant. Cisco Cyber Vision Sensor IOx Application 5.4.x for Cisco Catalyst 9300, 9400 Series Switch and for Cisco Catalyst IR8340 Rugged Router.	5.4.x
CiscoCyberVision-IOx-Active-Discovery-fips-aarch64-5.4.x.tar	FIPS-compliant. Cisco Cyber Vision Sensor FIPS IOx Application 5.4.x with Active Discovery for Cisco Catalyst IE3400 Rugged Series Switch and Cisco Catalyst IE9300 Rugged Series Switch.	5.4.x
CiscoCyberVision-IOx-Active-Discovery-fips-x86-64-5.4.x.tar	FIPS-compliant. Cisco Cyber Vision Sensor FIPS IOx Application 5.4.x with Active Discovery for Cisco Catalyst 9300, 9400 Series Switch and for Cisco Catalyst IR8340 Rugged Router.	5.4.x
CiscoCyberVision-IOx-fips-aarch64-5.4.x.tar	FIPS-compliant. Cisco Cyber Vision Sensor FIPS IOx Application 5.4.x for Cisco Catalyst IE3300, IE3400, and IE9300 Rugged Series Switch and Cisco IR1101, IR1800 Integrated Services Rugged Router.	5.4.x
CiscoCyberVision-IOx-fips-x86-64-5.4.x.tar	FIPS-compliant. Cisco Cyber Vision Sensor FIPS IOx Application 5.4.x for Cisco Catalyst 9300, 9400 Series Switch and for Cisco Catalyst IR8340 Rugged Router.	5.4.x

Related resources

Collection page: Cisco Cyber Vision User Content

Legal information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2025 Cisco Systems, Inc. All rights reserved.