Release Notes for Cisco Cyber Vision Center, Release 5.5.x

Cisco Cyber Vision, Release 5.5.x

Cisco Cyber Vision Release 5.5.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.

Upgrade information: Center startup time

The Cisco Cyber Vision upgrade performs several database tasks during the first boot. Consequently, the Center takes time to start. During this phase, the system updates the database schema. The time required depends on your system's performance and the amount of data stored.

The user interface displays this message:

" Cyber Vision is being upgraded. Please wait for a few minutes, and do not shutdown or restart the system."

Important: Wait until the upgrade finishes. Do not reboot the Center while this process runs.

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 5.5.x

Product Impact	Feature	Description
Ease of use	Cisco Cyber Vision Site Manager	The Site Manager is a new way to centrally manage your Cyber Vision Local Centers. The Site Manager offers a single-pane view of all your Centers, including their geolocation and health status, as well as the health status of their sensors. A cloud connection enables automatic knowledge database updates and more.
Upgrade	Intrusion detection alert type	This alert type monitors network traffic using the Snort intrusion detection system. It raises an alert when suspicious or malicious network activity is detected on monitored assets, based on Snort rules.
Upgrade	Inactive asset alert type	This alert type detects assets that stop communicating due to failure or misconfiguration. Define custom rules for the inactivity period to reduce manual monitoring.

Product Impact	Feature	Description
Upgrade	Assets with unexpected external communications alert type	This alert type monitors asset communications. It raises an alert if an asset communicates to external IP addresses or domains.
Ease of Use	Custom properties	Cisco Cyber Vision now supports custom properties at both the network and asset levels. You can view, add, and edit these properties, with strict validation rules enforced to maintain data integrity. This enhancement enables the addition of custom metadata to assets, facilitating more efficient emergency response and maintenance operations.
Ease of Use	Bulk vulnerability acknowledgment for assets	You can now acknowledge or unacknowledge multiple vulnerabilities at once from the asset vulnerability table. This change removes manual processing, saving time for asset security.
Ease of Use	Cisco ISE integration through ISE-API	Cisco Cyber Vision integrates with Cisco ISE using the ISE API, enabling direct synchronization of network groups and Security Group Tags (SGTs) from Cyber Vision to ISE.
Ease of Setup	Enhanced system connectivity and security settings	The system offers intuitive user interface-based settings to simplify administrative workflow. Date and time settings allow for precise time synchronization for the center and connected sensors. DNS management streamlines system access. Proxy configurations ensure secure, controlled connectivity in isolated environments.
Ease of Use	Network based auto grouping	The network based auto grouping feature streamlines device management. It automatically organizes devices based on established network definitions. Groups are created and named according to your network names. You can use this feature for easier ISE API integration and device classification.
Ease of Use	External IP country mapping	This feature maps the countries of external IP addresses your device connects with. It identifies geographical locations and helps prioritize which communications to investigate to improve network insight and security.
Ease of Use	ASN and ASN organization insights for external communications	This feature shows ASN (Autonomous System Number) and ASN Organization information for external communications. It helps identify traffic sources and network owners. Enables quick detection of suspicious communications and reduces investigation time.
Hardware Reliability	Enhanced hardware support	Cyber Vision Center deployments support the Cisco UCS C225 M8N Rack Server (CV-CNTR-M8N configuration). This hardware provides greater flexibility for your infrastructure.

Product Impact	Feature	Description
Ease of Use	Asset vulnerability insights in new UI	Cyber Vision Center matches asset properties against the knowledge database to detect vulnerabilities. You can view the matched asset properties in the New UI. This process provides clear, actionable insights into your security posture.
Ease of Use	Enable Cyber Vision Center as an SEA Gateway	The Secure Equipment Access agent can run directly on the Cyber Vision Center. This setup eliminates the need to host the agent within an IOx application. When you enable the Center as an SEA gateway, you provide secure, remote access to the Center and its network resources through the IoT Operations Dashboard. You do not need direct inbound access.
Upgrade	Enhanced asset creator	The asset creator uses properties to aggregate various components into a single asset. This feature improves the accuracy of the asset creator for switches and routers, ensuring more precise device management.
Upgrade	Enhanced asset property selection	This feature improves the selection of asset properties, such as product references and serial numbers. These properties appear directly at the asset level to provide better visibility and management.
Upgrade	Enhanced vulnerability matching	This feature improves vulnerability matching across multiple release trains. It simplifies security management and ensures accurate tracking for diverse software versions.

Sensor features

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

Table 2. New software features for Cisco Cyber Vision Sensor, Release 5.5.x

Product Impact	Feature	Description
Ease of Setup	Bulk host onboarding and sensor deployment on switches	Enables you to onboard multiple switches and deploy sensor applications to them using a guided, wizard-based workflow.
Ease of Use	Enhancement of sensor health monitoring	Monitor sensor health proactively with automated updates and deep insights. The sensor management system tracks each sensor's status and provides actionable updates, helping you resolve issues before they affect your operations. Use Advanced View to analyze performance trends and troubleshoot efficiently.

API features

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

Table 3. New API features for Cisco Cyber Vision Sensor, Release 5.5.x

Product Impact	Feature	Description
Ease of Setup	Bulk organization hierarchy level creation	You can create one or more organization hierarchy levels in a single API request using `POST /oh`. Each level includes a name and parent hierarchy level ID. The response reports successful and failed level creation attempts.
Ease of Setup	Bulk network assignment to organization hierarchy levels	You can assign one or more networks to a hierarchy level using `PUT /oh/{levelId}/networks`. Each request can assign up to 500 networks by network UUID.
Ease of Setup	Custom properties	You can create, list, retrieve, update, and delete custom key-value properties for assets and networks. Asset custom property retrieval includes properties defined directly on the asset and properties inherited from associated networks.

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.
- 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
Enhancements	• The Cyber Vision center receives an incorrect hostname when using DHCP option 12. • The system sends the CyberVision Risk Score as an ISE custom attribute.
Deep Packet Inspection (DPI) new protocols	• GRID: add R-GOOSE protocol • New Camera AXIS P5676-LE support • New Sick Camera hardware support • IO Link Turck Protocol • GigE Vision inspection • AutomationDirect Productivity PLC • New protocol Sick Cola A/B • Rockwell Automation SCADA - FTView SE • SEC/GEMS protocol (disabled by default)
Active discovery new protocols	• GigE Vision scanner • Broadcast scanner for TURCK • Broadcast scanner for Bosch RCP plus • Handle new Siemens LOGO PLC

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 5.5.x

Bug ID	Description
CSCwr22441	Upgrade to FIPS from a regular image should be prohibited
CSCwu06204	Component limit could be bypassed

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

Table 6. Known issues for Cyber Vision, Release Cyber Vision 5.5.x

Bug ID	Description
NA	The Cisco Cyber Vision sensor self-update fails when sensors are installed on Catalyst 9000 series or IR8340 platforms without an SSD. If this occurs, the system rolls back to the previous release. A subsequent self-update attempt completes successfully and updates the sensor to the latest release.
NA	Codesys DPI: The TargetSystemVersion property may contain an incorrect value; this property has been removed until a fix is available.
NA	The CVSM link in the enrolled center redirects incorrectly immediately following enrollment.
NA	Bulk deployment of Cisco Cyber Vision sensors via the new user interface encounters issues when you install the sensor on a Catalyst 9k with an SSD. The new user interface displays error messages during deployment and fails to show the sensor as running. However, the old user interface displays the sensor as running, which indicates a successful deployment and operational status.
NA	The Cisco Cyber Vision integration with the Cisco ISE API fails to synchronize **IP SGT static mapping** when you use the **Force Synchronization** button. You use the **Edit Configuration** button instead.

Compatibility

Center compatibility

Table 7. Compatibility information for Cisco Cyber Vision Center, Release 5.5.x

Product	Supported Release
VMware ESXi	7.x and later
Nutanix AOS (Acropolis OS)	6.10 and later
Microsoft Windows Server Hyper-V	2019 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

Cisco Cyber Vision supports running the Cyber Vision Center on multiple platforms, including public cloud environments. The Cyber Vision Center runs as a cloud appliance on these public cloud platforms:

- Amazon AWS software appliance

- Microsoft Azure software appliance
- Google Cloud Compute software appliance

Sensor compatibility

Table 8. Compatibility information for Cisco Cyber Vision sensors, Release 5.5.x

Product	Supported Release
Cisco IC3000	Minimum version: 1.5.2 Recommended versions: 1.5.2
Cisco Catalyst IE3400	Minimum version: 17.9.x Recommended versions: 17.12.7a, 17.15.4, 17.18.3 and above
Cisco Catalyst IE3300 10G	Minimum version: 17.9.x Recommended versions: 17.12.7a, 17.15.4, 17.18.3 and above
Cisco Catalyst IE3300 (with 4GB DRAM units starting with Version ID (VID) from -06)	Minimum version: 17.12.x Recommended versions: 17.12.7a, 17.15.4, 17.18.3 and above
Cisco Catalyst IE3500	Minimum version: 17.18.x Recommended versions: 17.18.3 and above
Cisco Catalyst IE9300	Minimum version: 17.12.x Recommended versions: 17.12.7a, 17.15.4, 17.18.3 and above
Cisco Catalyst IR1101	Minimum version: 17.9.x Recommended versions: 17.12.7a, 17.15.4, 17.18.3 and above
Cisco Catalyst IR1800	Minimum version: 17.9.x Recommended versions: 17.12.7a, 17.15.4, 17.18.3 and above
Cisco Catalyst IR1835	Minimum version: 17.15.x Recommended versions: 17.15.4, 17.18.3 and above
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: 17.12.7a, 17.15.4, 17.18.3 and above
Cisco Catalyst 9300	Minimum version: 17.9.x Recommended versions: 17.12.7a, 17.15.4, 17.18.3 and above
Cisco Catalyst 9400	Minimum version: 17.9.x Recommended versions: 17.12.7a, 17.15.4, 17.18.3 and above
Cisco Catalyst 9350	Minimum version: 17.18.2 Recommended versions: 17.18.3 and above
Docker sensor	Ubuntu LTS 24.04 / 22.04 with Docker 28.x / 29.x
Sensor VM	VMWare ESXi: 7x or later or HyperV 2019 or later

Product	Supported Release
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, 17.18.1 and above

Upgrade compatibility

If you are upgrading to Cisco Cyber Vision release 5.5.x from an earlier release, see the Cisco Cyber Vision Upgrade Guide.

Table 9. Upgrade paths to Cisco Cyber Vision Center Release 5.5.x

Current software release	Upgrade path to Release 5.5.x
5.1.x, 5.2.x, 5.3.x, 5.4.x	Upgrade directly to 5.5.x
4.3.x, 4.4.x, 5.0.x	Upgrade first to 5.4.2 then to 5.5.x
4.1.x	Upgrade first to 4.3.0, then to 5.4.2, then to 5.5.x

Scalability

Cyber Vision Center hardware appliance performance

Table 10. Cisco Cyber Vision Center (Standalone/Local) hardware appliance scale

Item	CV-CNTR-M6N
Max components	70,000
Max number of sensors	400
Max number of flows stored	21 million

Table 11. 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 5.5.x.

Center software

Table 12. Software packages for Cisco Cyber Vision Center, Release 5.5.x

Software Package	Description	Release
CiscoCyberVision-Center-5.5.x.ova	Install Cisco Cyber Vision Center on a VMware ESXi virtual machine.	5.5.x
CiscoCyberVision-Center-5.5.x.ova	Install Cisco Cyber Vision Center on a VMware ESXi virtual machine.	5.5.x
CiscoCyberVision-center-5.5.x.qcow2	Install Cisco Cyber Vision Center on an Oracle-hosted virtual machine.	5.5.x
CiscoCyberVision-5.5.x.vhdx	Install Cisco Cyber Vision Center on a Hyper-V VHDX virtual machine.	5.5.x
CiscoCyberVision-Center-with-DPI-5.5.x.ova	Install Cisco Cyber Vision Center with DPI capabilities on a VMware ESXi virtual machine.	5.5.x
CiscoCyberVision-reports-management-5.5.x.ext	Install the extension in a Cisco Cyber Vision Center for reports management.	5.5.x
CiscoCyberVision-sensor-management-5.5.x.ext	Install the extension in a Cisco Cyber Vision Center for sensor management. The extension is not compatible with a FIPS-Compliant Center.	5.5.x
CiscoCyberVision-update-center-fips-5.5.x.dat	Manually update a Cisco Cyber Vision Center to a FIPS-compliant Center.	5.5.x
CiscoCyberVision-fips-5.5.x.vhdx	Install FIPS-compliant Cisco Cyber Vision Center on a Hyper-V VHDX virtual machine.	5.5.x
CiscoCyberVision-center-5.5.x.qcow2	Install FIPS-compliant Cisco Cyber Vision Center on an Oracle-hosted virtual machine.	5.5.x
CiscoCyberVision-Center-fips-5.5.x.ova	Install FIPS-compliant Cisco Cyber Vision Center on a VMware ESXi virtual machine.	5.5.x

Sensor software

Table 13. Software packages for Cisco Cyber Vision sensors, Release 5.5.x

Software Package	Description	Release
CiscoCyberVision-IOx-Active-Discovery-IC3000-5.5.x.tar	Not FIPS-compliant. Cisco Cyber Vision Sensor IOx Application 5.5.x with Active Discovery for Cisco IC3000 Industrial Compute Gateway.	5.5.x
CiscoCyberVision-IOx-Active-Discovery-IC3000-5.5.x.tar	Not FIPS-compliant. Cisco Cyber Vision Sensor IOx Application 5.4.x with Active Discovery for Cisco IC3000 Industrial Compute Gateway.	5.5.x

Software Package	Description	Release
CiscoCyberVision-IOx-Active-Discovery-aarch64-5.5.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.	5.5.x
CiscoCyberVision-IOx-Active-Discovery-x86-64-5.5.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.	5.5.x
CiscoCyberVision-IOx-IC3000-5.5.x.tar	Not FIPS-compliant. Cisco Cyber Vision Sensor IOx Application 5.4.x for Cisco IC3000 Industrial Compute Gateway.	5.5.x
CiscoCyberVision-IOx-aarch64-5.5.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.	5.5.x
CiscoCyberVision-IOx-x86-64-5.5.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.	5.5.x
CiscoCyberVision-IOx-Active-Discovery-fips-aarch64-5.5.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.	5.5.x
CiscoCyberVision-IOx-Active-Discovery-fips-x86-64-5.5.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.	5.5.x
CiscoCyberVision-IOx-fips-aarch64-5.5.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.	5.5.x
CiscoCyberVision-IOx-fips-x86-64-5.5.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.	5.5.x

Related resources

Collection page: Cisco Cyber Vision User Content

Legal information