Release Notes for Cisco Cyber Vision, Release 5.6.x

Cisco Cyber Vision, Release 5.6.x

Cisco Cyber Vision Release 5.6.x expands security monitoring, auditability, usability, asset investigation, vulnerability reporting, and network-segmentation workflows. Cyber Vision Secure Remote Access (SRA) adds new storage, naming, and multi-VRF enhancements.

New software features

Cisco Cyber Vision features

This section provides a brief description of the Cisco Cyber Vision Center features included in Release 5.6.x.

Table 1. New software features for Cisco Cyber Vision Center and Site Manager, Release 5.6.0

Product Impact	Feature	Description
Greater Control	Network Scanner alert type	Introduces the Network Scanner alert type to detect network reconnaissance and scanning attempts. Administrators can add trusted scanner IP addresses to an allowed list so that their activity does not generate alerts.
Better Visibility	Network Detection	Automatically detects networks from analyzed traffic at regular intervals and on demand. Administrators can review, accept, update, or discard detected networks and manually define networks with custom properties and organizational hierarchies.
Ease of Process	Assets page enhancement	Provides security, network, and inventory views and a consolidated Summary tab for alerts, vulnerabilities, behaviors, services, and communications. Summary cards and dedicated tabs help users move from an asset overview to detailed information.
Software Reliability	Deep Packet Inspection (DPI) improvements	Adds and enhances DPI support for Niagara Fox on Tridium JACE 9000, Sentinel UDP/1947, AutomationDirect DoMore BRX and Click PLCs, S7plus, Sick Cola2 Netscan, and ABB DCS800 MMS. Also improves DHCP-based Windows profiling, EtherNet/IP device identification, memory use, and protocol-decoding reliability.
Ease of Use	Automatic Purge of Components	Automates the removal of components that meet the configured purge criteria, reducing routine cleanup work.
Ease of Use	Asset Behavior	Introduces behavior-focused information for assets to help users understand observed activity and investigate deviations.
Better Visibility	Snort/IDS enhancements	Enhances Intrusion Detection alerts by displaying the MITRE ATT&CK tactics and techniques mapped to the Snort GID:SID pair that generated the alert. The alert preview shows tactics, and the Summary tab shows the GID:SID pair, tactics, and techniques.
Ease of Use	Segmentation	Introduces Cyber Vision Segmentation and replaces functional groups with asset groups for segmentation workflows. Users can define Security Group Tag identities, model and review rules, review recommendations, and simulate rule impact for supported IE 3x00 switches. Release 5.6.0 does not deploy SGT mappings or Security Group ACL configuration to devices.
Ease of Use	Reworked Asset table view presets	Reworks Asset table presets so users can quickly switch among views for inventory, network, security, and other common tasks.
Ease of Use	View alerts per asset	Shows alerts associated with an asset directly from its Asset Summary page.
Greater Control	Assets with unexpected behaviors alert type	Introduces an alert type that monitors selected assets for specified behaviors within a configurable 1-to-30-day time window. Administrators can select initiator, target, or both roles and assign alert severity. Matching activity raises an alert and can generate Syslog lifecycle events.
Ease of Process	Sensor management extension discontinuation	Discontinues the Sensor Management extension. Sensors previously deployed through the extension are automatically converted and can be managed from the Sensors Management page in the new UI.
Better Visibility	Communications page enhancement	Enhances the New UI Communications map with a left-side control panel for filters, display settings, and legend information; in-place group exploration; contextual details; active-view visibility controls; and right-click quick actions.
Greater Control	Pause or resume individual alert rules	Moves pause and resume actions from the alert-type level to individual alert rules. Administrators can pause or resume one or multiple rules without affecting other rules of the same alert type. Pausing a rule stops new alerts but does not change existing alerts.

Product Impact	Feature	Description
Better Visibility	Audit logs	Records supported user authentication and configuration actions in the audit log. Authorized users can review and export audit records and configure a retention period from 7 through 365 days. The default retention period is 90 days.
Ease of Use	Display themes	Lets users display the Cyber Vision interface using the Light or Dark theme or the theme configured for their system. Users select the display theme from the user menu.
Ease of Use	SRA preserves device settings in cloud console after agent removal	Check the **Preserve device settings in cloud console after agent removal** check box to retain device settings posting removing an agent.

Cyber Vision Secure Remote Access (SRA) features

This section provides a brief description of the Cyber Vision Secure Remote Access (SRA) features included in Release 5.6.x.

Table 2. New software features for Cyber Vision Secure Remote Access (SRA), Release 5.6.0

Product Impact	Feature	Description
Software Reliability	Azure Blob storage support for session recordings	Adds Azure Blob Storage as a storage option for remote-access session recordings.
Ease of Use	Rename the SEA service to Cyber Vision Secure Remote Access - UI updates	Renames Secure Equipment Access (SEA) to Cyber Vision Secure Remote Access (SRA) and applies the related user-interface changes.
Ease of Use	Eliminate need for email for SSO cross-launch from CV Center to Cyber Vision Secure Remote Access (SRA)	Removes the requirement to provide an email address when using single sign-on to cross-launch Cyber Vision Secure Remote Access from Cisco Cyber Vision Center.
Ease of Setup	Multi-VRF support for CLI and SD-WAN (Cyber Vision Secure Remote Access Agent adjustments)	Updates the remote-access agent to support multi-VRF deployments for CLI-based and Cisco Catalyst SD-WAN workflows.

New hardware features

No new hardware features are included in Release 5.6.0.

FIPS release

A FIPS-compliant Cisco Cyber Vision Center package is available for supported deployment options in Release 5.6.0. FIPS 140-3 defines security requirements for cryptographic modules used 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 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

- Pause and resume controls move from alert types to individual alert rules in Release 5.6.0. When you upgrade from Release 5.5.x, Cyber Vision sets every rule associated with a paused alert type to Paused. Resume individual rules as needed after the upgrade.
- After upgrading to Cisco Cyber Vision Release 5.6.x, wait a few days before enabling segmentation. This delay allows Cyber Vision to populate the sensor-to-communication link data required for segmentation.
- Cisco Cyber Vision Release 5.6.x does not support functional groups. Before upgrading, be aware that the upgrade:
  - Deletes all alert rules linked to functional groups.
  - Deletes the complete alert history generated by those rules.
  - Immediately decreases the corresponding alert counters.
  - Stops monitoring and syslog emission for those rules.

Resolved issues

Table 3. Resolved bugs in Cisco Cyber Vision Release 5.6.x

Cisco bug ID	Description
CSCwq35445	Timeout during purge-components: Timeout reached.
CSCwu67727	Allow purge from the UI of components without IP addresses.
CSCwv86561	Excessive memory usage on a sensor with HTTP packets.

Known issues

Table 4. Known issues in Cisco Cyber Vision Release 5.6.x

Cisco bug ID	Description
CSCwu94398	BACnet DPI creates several devices for one physical asset.
CSCwu94397	Asset Creator: More than one BACnet ID for a unique asset.

Compatibility

Center compatibility

Table 5. Compatibility information for Cisco Cyber Vision Center, Release 5.6.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
Cyber Vision Center hardware appliance (Cisco UCS® C225 M8 Rack Server)	CV-CNTR-M8N: 32-core CPU, 192 GB RAM, two or four 1.6 TB NVMe drives

Sensor compatibility

Table 6. Compatibility information for Cisco Cyber Vision sensors, Release 5.6.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: 7.x or later Microsoft Hyper-V: 2019 or later
Rockwell Stratix 5800 Switch 1783-MMS10EA 1783-MMS10EAR	Minimum version: 17.12.x Recommended versions: 17.12.4, 17.15.4, 17.18.1 and above

Product	Supported Release
1783-MMS10A 1783-MMS10AR	

Upgrade compatibility

- If you are upgrading to Cisco Cyber Vision Release 5.6.x from an earlier release, see the Cisco Cyber Vision Upgrade Guide.
- When you upgrade from Release 5.2.x or 5.3.x to Release 5.6.x, Cyber Vision deletes all communications.

Table 7. Upgrade paths to Cisco Cyber Vision Center Release 5.6.x

Current software release	Upgrade path to Release 5.6.x
5.1.x, 5.2.x, 5.3.x, 5.4.x, and 5.5.x	Upgrade directly to 5.6.x
4.3.x, 4.4.x, and 5.0.x	Upgrade first to 5.4.2, then to 5.6.x
4.1.x	Upgrade first to 4.3.0, then to 5.4.2, then to 5.6.x

Scalability

For current performance and scalability limits, see the Cisco Cyber Vision Performance and Scale Guide, Release 5.6.x.

Supported software packages

This section lists the software packages for Cisco Cyber Vision Release 5.6.0.

Center software

Table 8. Software packages for Cisco Cyber Vision Center, Release 5.6.x

Software Package	Description	Release
CiscoCyberVision-Center-5.6.x.ova	Install Cisco Cyber Vision Center on a VMware ESXi virtual machine.	5.6.x
CiscoCyberVision-center-5.6.x.qcow2	Install Cisco Cyber Vision Center on an Oracle-hosted virtual machine.	5.6.x
CiscoCyberVision-5.6.x.vhdx	Install Cisco Cyber Vision Center on a Hyper-V VHDX virtual machine.	5.6.x
CiscoCyberVision-Center-with-DPI-5.6.x.ova	Install Cisco Cyber Vision Center with DPI capabilities on a VMware ESXi virtual machine.	5.6.x
CiscoCyberVision-reports-management-5.6.x.ext	Install the extension in a Cisco Cyber Vision Center for reports management.	5.6.x
CiscoCyberVision-update-center-fips-5.6.x.dat	Manually update an older FIPS-compliant Cisco Cyber Vision Center to a 5.6 FIPS-compliant Center.	5.6.x
CiscoCyberVision-fips-5.6.x.vhdx	Install FIPS-compliant Cisco Cyber Vision Center on a Hyper-V VHDX virtual machine.	5.6.x
CiscoCyberVision-center-fips-5.6.x.qcow2	Install FIPS-compliant Cisco Cyber Vision Center on an Oracle-hosted virtual machine.	5.6.x
CiscoCyberVision-Center-fips-5.6.x.ova	Install FIPS-compliant Cisco Cyber Vision Center on a VMware ESXi virtual machine.	5.6.x

Sensor software

Table 9. Software packages for Cisco Cyber Vision sensors, Release 5.6.x

Software Package	Description	Release
CiscoCyberVision-IOx-Active-Discovery-IC3000-5.6.x.tar	Not FIPS-compliant. Cisco Cyber Vision Sensor IOx Application 5.6.x with Active Discovery for Cisco IC3000 Industrial Compute Gateway.	5.6.x
CiscoCyberVision-IOx-Active-Discovery-aarch64-5.6.x.tar	Not FIPS-compliant. Cisco Cyber Vision Sensor IOx Application 5.6.x with Active Discovery for Cisco Catalyst IE3300, IE3400, IE3500, and IE9300 Rugged Series Switch.	5.6.x
CiscoCyberVision-IOx-Active-Discovery-x86-64-5.6.x.tar	Not FIPS-compliant. Cisco Cyber Vision Sensor IOx Application 5.6.x with Active Discovery for Cisco Catalyst 9300, 9400 Series Switch and for Cisco Catalyst IR8340 Rugged Router.	5.6.x
CiscoCyberVision-IOx-IC3000-5.6.x.tar	Not FIPS-compliant. Cisco Cyber Vision Sensor IOx Application 5.6.x for Cisco IC3000 Industrial Compute Gateway.	5.6.x
CiscoCyberVision-IOx-aarch64-5.6.x.tar	Not FIPS-compliant. Cisco Cyber Vision Sensor IOx Application 5.6.x for Cisco Catalyst IE3300, IE3400, IE3500, and IE9300 Rugged Series Switch and Cisco IR1101, IR1800 Integrated Services Router Rugged.	5.6.x
CiscoCyberVision-IOx-x86-64-5.6.x.tar	Not FIPS-compliant. Cisco Cyber Vision Sensor IOx Application 5.6.x for Cisco Catalyst 9300, 9400 Series Switch and for Cisco Catalyst IR8340 Rugged Router.	5.6.x
CiscoCyberVision-IOx-Active-Discovery-fips-aarch64-5.6.x.tar	FIPS-compliant. Cisco Cyber Vision Sensor FIPS IOx Application 5.6.x with Active Discovery for Cisco Catalyst IE3400, IE3500, and IE9300 Rugged Series Switch.	5.6.x
CiscoCyberVision-IOx-Active-Discovery-fips-x86-64-5.6.x.tar	FIPS-compliant. Cisco Cyber Vision Sensor FIPS IOx Application 5.6.x with Active Discovery for Cisco Catalyst 9300, 9400 Series Switch and for Cisco Catalyst IR8340 Rugged Router.	5.6.x
CiscoCyberVision-IOx-fips-aarch64-5.6.x.tar	FIPS-compliant. Cisco Cyber Vision Sensor FIPS IOx Application 5.6.x for Cisco Catalyst IE3300, IE3400, IE3500, and IE9300 Rugged Series Switch and Cisco IR1101, IR1800 Integrated Services Rugged Router.	5.6.x
CiscoCyberVision-IOx-fips-x86-64-5.6.x.tar	FIPS-compliant. Cisco Cyber Vision Sensor FIPS IOx Application 5.6.x for Cisco Catalyst 9300, 9400 Series Switch and for Cisco Catalyst IR8340 Rugged Router.	5.6.x

Related resources

Collection page: Cisco Cyber Vision User Content

Legal information