Release Notes for Cisco Cyber Vision Center, Release 5.3.0

Cisco Cyber Vision, Release 5.3.0

Cisco Cyber Vision Release 5.3.0 elevates your operational security with a suite of powerful new features. Experience a transformative new user interface, designed for unparalleled ease of use and clarity, offering AI-powered asset clustering and simplified views of your network. Boost your threat detection and response capabilities through seamless integration with Splunk, and gain deeper operational insights by capturing critical variable data from your industrial environments. With streamlined deployment and enhanced security, Cyber Vision 5.3.0 empowers you to manage and protect your industrial networks with greater efficiency and precision.

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 5.3.0

Product Impact	Feature	Description
Ease of Use	New UI	Cisco Cyber Vision Center offers New UI that comprises simplified, structured views of assets, vulnerabilities, and alerts. The New UI includes a new method for automatically grouping assets using AI-based clustering. Click **Go to Cyber Vision New UI** in the top banner of your Center to get started.
Ease of Setup	Integrate Cisco Cyber Vision Center with Splunk	Integrate Cisco Cyber Vision with Splunk to gain real-time views of large datasets, enabling better detection and response to threats and vulnerabilities.
Ease of Setup	Cisco Cyber Vision Center VM on Nutanix	Deploy Cisco Cyber Vision Center VMs on Nutanix.
Ease of Setup	Deploy Cisco Cyber Vision sensor and Cisco SEA agent together	Deploy both the Cisco Cyber Vision sensors and the Cisco Secure Equipment Access (SEA) agent on your network devices, using a single software package.
Ease of Use	(New UI) Receive property-based group suggestions from asset clustering algorithm	Asset clustering algorithms suggest property-based groups (assets that share the same definition, network, or other properties), in addition to communication-based groups (assets that primarily communicate with each other).
Ease of Use	(New UI) Filter Cyber Vision Center data by organization hierarchy	All the data views in New UI can be filtered by organization hierarchy, by sensors or networks that an asset is associated with. At the top of the left menu, in the **Organization** filter, choose the hierarchy level you want to focus on. **Global** is the default choice and covers all assets.

Product Impact	Feature	Description
Ease of Use	(New UI) Filter data in Cyber Vision Center	A product-level banner in New UI allows you to filter data on all its pages, except configuration pages. If you have not applied any filters, the value **No filter applied** is displayed. Click **Edit** to apply one or more filters from functional group, network or sensor, asset type, and vendor categories.
Ease of Use	(New UI) Assign a network to an organization hierarchy	Assign a network to an organization hierarchy level.
Ease of Use	(New UI) See functional-group centric views of communication map	The communications map displays the communication activity between the configured functional groups. The communication links between groups are not actionable. Click a functional group to view the inter-asset communications within a group. Click the communication links between assets to view the details of the activities.
Ease of Use	(New UI) Active and cleared alerts	The **Alerts** page displays two types of alerts: • Active: alerts that are currently active in Cisco Cyber Vision and are yet to be addressed. • Cleared: alerts that are no longer considered active due to actions such as vulnerability acknowledgement or editing alert rules. A cleared alert is displayed in this list for up to 14 days.
Ease of Use	(New UI) Pause alert creations	You can pause an alert type in the **Configure > Alerts** page to pause alert matching for the configured alert rules. You can resume alert creation from the same page at any time.
Ease of Use	(New UI) Change vulnerability scoring system for alerts	The Cisco Security Risk Score is the default scoring system applied to alert configurations. However, you can choose to update an alert configuration to apply the CVSS scoring system instead.
Ease of Use	(New UI) Alert for severe vulnerabilities in monitored entities	Create and edit rules for the **Severe vulnerabilities in monitored entities** alert based on the Cisco Security Risk Score or the CVSS score. You can edit each rule in this alert type for greater control over the alerts you see.
Ease of Use	(New UI) Alert for prohibited vendors	The **Configure > Alerts** page contains a default alert for prohibited vendors. The alert rule is based on an editable list of prohibited vendors. You cannot add any other rules to this alert type.

Product Impact	Feature	Description
Ease of Use	(New UI) Asset vendor names and icons	Cisco Cyber Vision center infers asset type based on the asset's vendor name, enhancing asset identification and grouping processes. In New UI, communication maps now include icons of vendors to help you identify assets more easily.
Ease of Use	(New UI) Search bar	New UI contains a search bar in the global top banner. You can search for an asset by name, IP address, or MAC address.
Ease of Use	Non-CEF syslogs support removed	You can no longer use non-CEF syslog formats with Cisco Cyber Vision Center. Any existing syslog connections that are based on non-CEF formats are automatically updated to CEF formats when you upgrade to Cisco Cyber Vision Center Release 5.3.x.
Ease of Use	SAML 2.0 SSO authentication support	Cisco Cyber Vision Center supports SAML 2.0 SSO authentication.
Ease of Use	Clear multiple components using a VLAN ID	When you clear data, you can enter a VLAN ID to purge all the components associated with it. You can clear data for one VLAN ID at a time.
Ease of Use	Bosch camera CVE added to knowledge database	Bosch camera Common Vulnerabilities and Exposures (CVE) are added to the Cyber Vision knowledge database.
API Experience	New APIs	The Cisco Cyber Vision API includes new APIs: • Deployment: POST /deployments/jwt/detailed • Sensors: ◦ POST /sensors/active-discovery ◦ POST /sensors/rename ◦ POST /sensors/{id}/capture-mode ◦ POST /sensors/{id}/snort/{action} • Sensor Explorer: POST /admin/sensorExplorer/selection/moveTo • Sensor Templates: ◦ GET /admin/sensorTemplates ◦ POST /admin/sensorTemplates/{template_id}/addSensors
Ease of Use	Device list CSV enhancements	The device list CSV that you download from Cisco Cyber Vision Center includes a column to list the sensors that have seen that device.
Ease of Use	ERSPAN support	Cisco Cyber Vision supports ERSPAN monitoring of traffic to Center DPI interfaces.

Product Impact	Feature	Description
Ease of Use	Cisco In Product Support	Use Cisco In Product Support to manage your Cisco support cases and related tasks directly from the Center.
Ease of Use	Enable or disable Snort on a Center DPI interface	You can choose to enable or disable Snort IDS/IPS on a Cisco Cyber Vision Center DPI interface. In earlier releases of Cisco Cyber Vision Center, Snort was enabled by default and could not be modified.

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, Release 5.3.0

Product Impact	Feature	Description
Ease of Setup	Detect and process variable data	Cisco Cyber Vision sensors can capture and relay measurable variables such as pressure or temperature to Cisco Cyber Vision Center. Enable Variables Storage in the **Admin > Data Management > Ingestion Configuration** page of Cisco Cyber Vision Center to allow the center to add the variables to the database for processing.
Upgrade	Change in supported platform versions	The minimum supported version for many Cisco devices is updated from 17.3.x to 17.6.x. Refer to the Compatibility information for Cisco Cyber Vision sensors, Release 5.3.x section for the latest compatibility information.

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 3. Resolved issues for Cisco Cyber Vision, Release 5.3.0

Bug ID	Description
CSCwo75543	CiscoMetadata layer can prevent BPF filter from seeing IPS
CSCwp33271	Syslog message doesn't show IP address for user operations
CSCwq31768	Error not displayed when several AD interfaces added
CSCwo91447	Event filter popup not working for IP, MAC, From, and To fields
CSCwo74017	Event: External remote access missing information
CSCwp95291	Inconsistent software version property leads to vulnerabilities discrepancy

Bug ID	Description
CSCwp09736	Network organization: network deletion " unknown error"
CSCwq49048	SCAND-wrapper service fails when center interface used for AD is down
CSCwp27748	API response difference from swagger documentation on component routes
CSCwi79542	Prevent RRD batch update failure when duplicate message is received

Open issues

This are no open issues in this specific release.

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

To search for a documented Cisco product issue, type in the browser: <bug number> site:cisco.com.

Table 4. Known issues for Cisco Cyber Vision, Release 5.3.0

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	When you upgrade a Cisco Cyber Vision Center, all the configured alert rules are purged.

Compatibility

Center compatibility

Table 5. Compatibility information for Cisco Cyber Vision Center, Release 5.3.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

Product	Supported Release
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 6. Compatibility information for Cisco Cyber Vision sensors, Release 5.3.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
Cisco Catalyst IE3300 10G	Minimum version: 17.6.x Recommended versions: 17.9.6a, 17.12.5, 17.15.3
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 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

Product	Supported Release
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
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

Upgrade compatibility

If you are upgrading to Cisco Cyber Vision release 5.3.0 from an earlier release, see the Cisco Cyber Vision Upgrade Guide.

Table 7. Upgrade paths to Cisco Cyber Vision Center Release 5.3.0

Current software release	Upgrade path to Release 5.3.0
4.3.x, 4.4.x, 5.x.x	Upgrade directly to 5.3.0
4.1.x	Upgrade first to 4.3.0, then to 5.3.0

Supported software packages

This section provides information about the release packages associated with Cisco Cyber Vision, Release 5.3.0.

Center software

Table 8. Software packages for Cisco Cyber Vision Center, Release 5.3.0

Software Package	Description	Release
CiscoCyberVision-Center-5.3.x.ova	Install Cisco Cyber Vision Center on a VMware ESXi virtual machine.	5.3.0
CiscoCyberVision-center-5.3.x.qcow2	Install Cisco Cyber Vision Center on an Oracle-hosted virtual machine.	5.3.0

Software Package	Description	Release
CiscoCyberVision-5.3.x.vhdx	Install Cisco Cyber Vision Center on a Hyper-V VHDX virtual machine.	5.3.0
CiscoCyberVision-Center-with-DPI-5.3.x.ova	Install Cisco Cyber Vision Center with DPI capabilities on a VMware ESXi virtual machine.	5.3.0
CiscoCyberVision-reports-management-5.3.x.ext	Install the extension in a Cisco Cyber Vision Center for reports management.	5.3.0
CiscoCyberVision-sensor-management-5.3.x.ext	Install the extension in a Cisco Cyber Vision Center for sensor management. The extension is not compatible with a FIPS-Compliant Center.	5.3.0
CiscoCyberVision-update-center-fips-5.3.x.dat	Manually update a Cisco Cyber Vision Center to a FIPS-compliant Center.	5.3.0
CiscoCyberVision-fips-5.3.x.vhdx	Install FIPS-compliant Cisco Cyber Vision Center on a Hyper-V VHDX virtual machine.	5.3.0
CiscoCyberVision-center-5.3.x.qcow2	Install FIPS-compliant Cisco Cyber Vision Center on an Oracle-hosted virtual machine.	5.3.0
CiscoCyberVision-Center-fips-5.3.x.ova	Install FIPS-compliant Cisco Cyber Vision Center on a VMware ESXi virtual machine.	5.3.0

Sensor software

Table 9. Software packages for Cisco Cyber Vision sensors, Release 5.3.x

Software Package	Description	Release
CiscoCyberVision-IOx-Active-Discovery-IC3000-5.3.x.tar	Not FIPS-compliant. Cisco Cyber Vision Sensor IOx Application 5.3.x with Active Discovery for Cisco IC3000 Industrial Compute Gateway.	5.3.0
CiscoCyberVision-IOx-Active-Discovery-aarch64-5.3.x.tar	Not FIPS-compliant. Cisco Cyber Vision Sensor IOx Application 5.3.x with Active Discovery for Cisco Catalyst IE3300, IE3400, and IE9300 Rugged Series Switch.	5.3.0
CiscoCyberVision-IOx-Active-Discovery-x86-64-5.3.x.tar	Not FIPS-compliant. Cisco Cyber Vision Sensor IOx Application 5.3.x with Active Discovery for Cisco Catalyst 9300, 9400 Series Switch and for Cisco Catalyst IR8340 Rugged Router.	5.3.0
CiscoCyberVision-IOx-IC3000-5.3.x.tar	Not FIPS-compliant. Cisco Cyber Vision Sensor IOx Application 5.3.x for Cisco IC3000 Industrial Compute Gateway.	5.3.0

Software Package	Description	Release
CiscoCyberVision-IOx-aarch64-5.3.x.tar	Not FIPS-compliant. Cisco Cyber Vision Sensor IOx Application 5.3.x for Cisco Catalyst IE3300, IE3400, and IE9300 Rugged Series Switch and Cisco IR1101, IR1800 Integrated Services Router Rugged.	5.3.0
CiscoCyberVision-IOx-x86-64-5.3.x.tar	Not FIPS-compliant. Cisco Cyber Vision Sensor IOx Application 5.3.x for Cisco Catalyst 9300, 9400 Series Switch and for Cisco Catalyst IR8340 Rugged Router.	5.3.0
CiscoCyberVision-IOx-Active-Discovery-fips-aarch64-5.3.x.tar	FIPS-compliant. Cisco Cyber Vision Sensor FIPS IOx Application 5.3.x with Active Discovery for Cisco Catalyst IE3400 Rugged Series Switch and Cisco Catalyst IE9300 Rugged Series Switch.	5.3.0
CiscoCyberVision-IOx-Active-Discovery-fips-x86-64-5.3.x.tar	FIPS-compliant. Cisco Cyber Vision Sensor FIPS IOx Application 5.3.x with Active Discovery for Cisco Catalyst 9300, 9400 Series Switch and for Cisco Catalyst IR8340 Rugged Router.	5.3.0
CiscoCyberVision-IOx-fips-aarch64-5.3.x.tar	FIPS-compliant. Cisco Cyber Vision Sensor FIPS IOx Application 5.3.x for Cisco Catalyst IE3300, IE3400, and IE9300 Rugged Series Switch and Cisco IR1101, IR1800 Integrated Services Rugged Router.	5.3.0
CiscoCyberVision-IOx-fips-x86-64-5.3.x.tar	FIPS-compliant. Cisco Cyber Vision Sensor FIPS IOx Application 5.3.x for Cisco Catalyst 9300, 9400 Series Switch and for Cisco Catalyst IR8340 Rugged Router.	5.3.0

Related resources

Collection page: Cisco Cyber Vision User Content

Legal information