

New and Changed Information

- New and changed information for release 5.3.x, on page 1

New and changed information for release 5.3.x

Cisco Cyber Vision Release 5.3.x offers these features:

Table 1: New and changed information, release 5.3.x

Feature	Description
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. See Cisco Cyber Vision New UI.
(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). See Asset clustering.
(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. See Filter views in Cyber Vision New UI.

Feature	Description
(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. See Filter views in Cyber Vision New UI.
(New UI) Assign a network to an organization hierarchy	Assign a network to an organization hierarchy level. See Assign a network to an organization hierarchy.
(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. See Assets and functional group communication maps.
(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. See Alerts.
(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. See Alert type management options and permitted alert rule actions.
(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. See Create alert rules.
(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. See Alerts.

Feature	Description
(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. See Alerts.
(New UI) Using asset vendor names and icons	Cisco Cyber Vision center infers device type based on device 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. See Assets and functional group communication maps.
(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. See Asset data management.
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. See Configure syslog.
SAML 2.0 SSO authentication support	Cisco Cyber Vision Center supports SAML 2.0 SSO authentication. See Single sign-on (SSO).
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. See Purge components from the database.
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.
Cisco In Product Support	Use Cisco In Product Support to manage your Cisco support cases and related tasks directly from the Center. See Cisco In Product Support.
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. See Enable IDS on a sensor.

Feature	Description
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. See Enable variable processing in a sensor template.
Integration with Secure Equipment Access	You can integrate Cisco Cyber Vision Center with Cisco Secure Equipment Access for remote access management of your OT assets. See Integrate Cisco Cyber Vision Center with SEA.