New and Changed Information

New and Changed Information

Features of Cisco Cyber Vision Release 5.2.x are as follows:

Feature	Description
Interactive Help	Cisco Cyber Vision offers contextual help through the Interactive Help feature. The Interactive Help menu offers easy access to a wide range of documentation resources, and to step-by-step walkthroughs of select taskflows. Interactive help is enabled by default. To disable the feature in your Cisco Cyber Vision center, go to **Admin** > **System**. The Interactive help plug-in area contains a toggle button for the feature. Cisco may collect some anonymous product usage behavior data in accordance with the Cisco End User License Agreement and the Cisco Privacy Statement for optimal delivery of Interactive Help. See Interactive Help Plugin.
LDS support for user authentication	Cisco Cyber Vision Center now supports user authentication through Lightweight Directory Services (LDS). See LDAP.
Purge multiple VLAN components	The **sbs-db purge-components** command is enhanced to allow the removal of multiple components associated with a VLAN.
CEF support for syslog configuration	New syslog configurations in the Cisco Cyber Vision Center require use of the Common Event Format (CEF) standard.

Feature	Description
	Exising syslog configurations that use non-CEF message formats are not affected in Cisco Cyber Vision Release 5.2.x. Non-CEF message formats may not be supported in later releases of Cisco Cyber Vision.
Beta UI	Cisco Cyber Vision Center offers a beta UI experience, with informative, easy-to-handle dashboards that present data on assets, vulnerabilities, alerts, and organization hierarchies. You can quickly apply data filters to view necessary information. This UI experience is a beta feature. To access the beta UI and its features, write to cv-**beta@cisco.com**. You will receive the command to enable the Cisco Cyber Vision Beta UI in addition to the existing classic UI. You can also configure functional groups in the beta UI, and assign data sources to organization hierarchies. To configure network definitions, sensors, and PCAPs, you must continue to use the classic UI. The overall task flows of Cisco Cyber Vision are currently spread across the classic and beta UIs, with the beta UI offering enhanced visualization of the center's data. **Beta UI Enhancements** See Introduction of the Cisco Cyber Vision Beta Version. **1.** User profile: The user profile is now displayed in the top banner of the Beta UI. The profile section displays the email id or username, or both, of a user, based on where user information is stored (Cisco Cyber Vision database or LDAP directory). **2.** The left menu in the Beta UI is collapsible. **3.** You can now log out from the Cisco Cyber Vision Center through the Beta UI. **4.** Session expiry: If a session is inactive for an hour, you must log into the Cisco Cyber Vision Center again. **Communications map enhancements**: The communications map displays an overview of all the communication events between connected assets. See Explore communication map. The following enhancements are now available:

Feature	Description
	1. Apply a time filter to the map to view communications in a specific time period. 2. Group assets by the subnet or functional group that they belong to to organize your communication map. 3. Click an asset to for a line graph representation of data flow. You can filter the graph by time and protocol. **Cisco Security Risk Score**: Cisco Cyber Vision Center now presents a Cisco Security Risk Score for the vulnerabilities displayed. The risk score is based on Cisco Vulnerability Management's predictive model. In Cisco Cyber Vision, the risk score includes factors of exploitability and dark web activity for topical context about risk severity to help prioritize vulnerability management. See Dashboard for the New UI. **Rack slot information for modular PLCs**: The asset summary page for modular PLCs includes information on rack slots. For each slot on a modular PLC, the model name, slot type, firmware version, and serial number are displayed. **Rerun functional group suggestions**: You can regenerate functional group suggestions at any time in the **Asset Visibility** > <choose an asset> > **Communications** page. You can rerun asset data at multiple levels to receive specific functional group suggestions: 1. Data associated with one sensor 2. Data associated with one asset 3. Data associated with an existing functional group 4. All the data in the Cisco Cyber Vision center When you accept a functional group suggestion, existing functional groups may be modified to ensure an asset is part of any one functional group. . **Heat maps for alerts**: The Alerts page displays a heat map to help you quickly visualise alert trends. The map spans the last 7 days, broken into two-hour segments. Hover over a segment to view the alert count. **Enable syslog notification for alert types**: You can choose to send syslog notifications to a connected

Feature	Description
	syslog server for an alert type. Syslog notifications are enabled by default for new and existing alert types in your Center. You can choose to disable the notifications in the Alerts page. See Syslog notifications for alert types. **Acknowledge vulnerabilities across assets**: You can view, acknowledge, or cancel acknowledgment of a vulnerability across multiple assets. .