Release Notes for Cisco Cyber Vision for Release 3.0.0

Cisco Cyber Vision Software

Notable new features

ICS CyberVision becomes Cisco Cyber Vision

The application has been rebranded and rearchitected to improve navigation and exploration of data over the network. Thus, a new page, Explore, is now the main starting point with new concepts and views aimed at enhancing users' experience and knowledge of the network to monitor. Significant changes have also been made in system administration, security monitoring and general performance.

Explore

Presets to explore the network

Presets have been created to help navigate through vast amounts of collected data and visualize large OT networks, by selecting among metadata added by Cisco Cyber Vision. In a nutshell, a preset is a set of criteria that can be set thanks to a filtering system.

Generic presets are provided by default (e.g. Asset management, Security, Control system integrity, Network Quality...) to guide you looking at the right data. You can also create your own presets according to your own business logic.

Filtering system to set presets' criteria

Filters have been created to help define which criteria in a Preset are to be matched. Filters are mainly based on component and activity tags but can also filter on groups and sensors. There are inclusive, restrictive and negative filters.

Preset views

Several views have been designed to display the data of each Preset. Former Map views (i.e. Net, Industrial and Security views) no longer exist. Instead, maps are now just one of the ways to visualize data. Lists (or tables) are now also provided by the Explore page.

The different views are:

- The Dashboard
- The Map - Expert
- The Map - Simple
- The Component list
- The Activity list
- The Purdue Model

Each one of these views relates to a perspective, whether the view is tag, component or activity oriented. Such data layout offers an overview of the industrial network as well as the possibility to go into deeper technical details which are reachable through Right side panels, Technical sheets and Mini Maps.

Aggregations of components

An aggregation is a cluster of components that have been brought together because they have similar properties, such as a shared IP address, MAC address and NetBIOS name. Aggregations can uncover devices over the network such as PLCs and routers, several Ethernet interfaces with the same NetBIOS name, and broadcast communications. Aggregations are enabled based on the currently selected view.

System administration

Data management

A new system administration page dedicated to data management has been added. Data stored in Cisco Cyber Vision Center can be cleared to optimize Center performance and in case of troubleshooting. Different data deletion options are available (from all data to variables only).

Smart Licensing

Cyber Vision is Cisco Smart Licensing enabled. A new administration page allows the registration of Cyber Vision Center to the Smart Licensing cloud service, and offline license management is also possible.

pxGrid

Cisco Platform Exchange Grid (pxGrid) has been implemented to synchronize detected network assets with Cisco Identity Services Engine (ISE). To secure the communication, the Center certificate can be downloaded and the connection to the ISE Server can be configured from the pxGrid system administration page.

Manual sensor installation

Manual sensor installation now supports the Cyber Vision IOx sensor application running on the Industrial Compute Gateway IC3000.

Security

IDS (Intrusion Detection System)

Snort signature engine has been implemented in sensors. An event will be generated by the Center when an intrusion is detected.

Port scanning detection

Port scanning detection has been implemented. An event will be generated in case a machine is scanning the network.

New features and enhancements

Search page for unstructured data

A new page is available to search for components among unstructured data. You can search

components by name, custom name, IP, MAC, tag and property value.

Sensor status

There are now two categories of sensor status which indicate on one side at which step of the enrolment process the sensor is and on the other one the network connection state between the sensor and the Center.

Sensors' data in the Monitor mode

You can now create baselines from data captured by specific sensors.

Filtering tools in table lists

Any table list available in Cisco Cyber Vision now contain filtering tools to sort out large amount of data (by typing a component, a port, selecting tags, etc.).

Activities and flows

The concept of "flow" has been refined to enhance clarity of the protocol data shown by Cyber Vision. There are now two concepts: Activities and Flows. Each one designates communication between components at two different levels:

- An activity is the representation of a group of communications exchanged between two components, that is, a macro and simplified view of communications.
- A flow is the representation of a single communication between two components, that is, a protocol connection.

A group of flows between two components forms an activity.

Tags

Classification of tags has been improved.

Some tags of components are used to offer a view of the components according to the Purdue model architecture (see Purdue Model view).

Variable accesses

Variable accesses representation has been improved.

For more information about the above features, refer to the Cisco Cyber Vision GUI User Guide.

Protocols

The following protocols are now supported:

- Mitsubishi
- IEEE C37.118
- Honeywell TCP
- IEC 61850
- Foxboro COMEX
- Omron

Hardware

Cisco Cyber Vision Center

Cisco UCS C220 M5 will be used as Center to gather data from all Edge Sensors and act as the monitoring, detection and management platform for the whole solution. It includes a RAID storage array, 3 redundant internal cooling fans and dual hot-swappable power supplies.

The UCS will be used in place of the CENTER10 and CENTER30 which are still supported by version 3 of Cisco Cyber Vision.

For more information, refer to Cisco Cyber Vision Center Appliance Quickstart Guide.

Cisco Cyber Vision Sensor

Cisco Industrial Compute Gateway IC3000 will be used as sensor. The device captures traffic in SPAN mode through 2 RJ45 10/100/1000 BaseT connectors ports and 2 SFP fiber ports. To be enrolled, the IC3000 must be manually installed, through a USB port.

Former SENSOR3, SENSOR5 and SENSOR7 are still supported on the platform.

For more information, refer to Cisco Cyber Vision Sensor Quickstart Guide.

Software Download

https://software.cisco.com/download/home/286325414/type

Related Documentation

Cisco Cyber Vision GUI User Guide:
https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_GUI_User_Guide_Release_3_0_0.pdf

Cisco Cyber Vision Center Appliance Quickstart Guide:
https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_Center_Appliance_Quickstart_Guide_Release_3_0_0.pdf

Cisco Cyber Vision Sensor Quickstart Guide:
https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_Sensor_Quickstart_Guide_Release_3_0_0.pdf