



Release Notes for Cisco Cyber Vision

Release 3.2.0

For users upgrading to 3.2.0 from previous versions, please carefully read the upgrade procedures.

Compatible device list	2
Links	3
Software Download	3
Related Documentation	4
Cisco Cyber Vision 3.2.0 update procedure	5
Center updates	5
Sensor updates – IC3000 Sensor and Sentryo SENSOR3,5,7 cases	5
Sensor updates – Cisco IOx sensor cases	5
Cisco Cyber Vision 3.2.0 important changes	6
Communication port change	6
API authentication	6
Cisco Cyber Vision new features and improvements	7
Global Center	7
Center single interface	9
Center DPI and IDS	10
Active Discovery	12
UI improvements	14
Nested Groups	14
Group Properties	15
Aggregated activities	16
Network filters	17
Vulnerability Dashboard	18
API Documentation	19

Data handling changes	20
Secure Boot	20
DPI improvements	20
IDS licensing updates	21
Knowledge Base improvements	22
Improvements of Cisco Cyber Vision integration with pxGrid and Cisco ISE	22
Cisco Cyber Vision Bug fixed	24
Cisco Cyber open CDETS and known issues	25

Compatible device list

Center	Description
VMware ESXi OVA center	VMware ESXi 6.x or later
Windows Server Hyper-V VHDX center	Microsoft Windows Server Hyper-V version 2016 or later
Cisco UCS C220 M5 CV-CNTR-M5S5	Cyber Vision Center hardware appliance (Cisco UCS® C220 M5 Rack Server) - 16 core CPU, 64 GB RAM, 800GB drives, Scale: 20K components
Cisco UCS C220 M5 CV-CNTR-M5S3 (NEW!)	Cyber Vision Center hardware appliance (Cisco UCS® C220 M5 Rack Server) - 12 core CPU, 32 GB RAM, 480GB drives
Sentryo CENTER10	Sentryo CENTER10 hardware appliance
Sentryo CENTER30	Sentryo CENTER30 hardware appliance
Sensor	Description
Cisco IC3000	Cyber Vision Sensor hardware appliance
Cisco Catalyst IE3400	Cyber Vision Sensor IOx application hosted in Cisco Catalyst IE3400 Industrial Ethernet switches
Cisco Catalyst IE3300 10G (NEW!)	Cyber Vision Sensor IOx application hosted in Cisco Catalyst IE3300 Industrial Ethernet switches with 10G ports
Cisco IR1101	Cyber Vision Sensor IOx application hosted in Cisco IR1101 Series Industrial Integrated Services Routers
Cisco Catalyst 9300, 9400	Cyber Vision Sensor IOx application hosted in Catalyst 9300, 9400 Series switches
Sentryo SENSOR3	Sentryo SENSOR3 hardware appliance
Sentryo SENSOR5	Sentryo SENSOR5 hardware appliance
Sentryo SENSOR7	Sentryo SENSOR7 hardware appliance

Links

Software Download

The files below can be find following this link: <https://software.cisco.com/download/home/286325414/type>

Center	Description
CiscoCyberVision-center-3.2.0.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-with-DPI-3.2.0.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-center-3.2.0.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-sensor-management-3.2.0.ext	Sensor Management extension installation file
Sensor	Description
CiscoCyberVision-IOx-aarch64-3.2.0.tar	IE3400, IR1101 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64--3.2.0.tar	Active Discovery sensor installation and update file
CiscoCyberVision-IOx-IC3K-3.2.0.tar	IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-3.2.0.tar	Catalyst 9x00 sensor installation and update file
Updates	Description
CiscoCyberVision-sysupgrade-3.2.0	Center and Sensor update file
CiscoCyberVision-sysupgrade-sensor-3.2.0	Sensor update file for embedded sensor in IC3000 and Sentryo SENSOR3, 5 and 7
CiscoCyberVision-Embedded-KDB-3.2.0.dat	KnowledgeDB embedded in Cisco Cyber Vision 3.2.0

Related Documentation

Cisco Cyber Vision documentation: <https://www.cisco.com/c/en/us/support/security/cyber-vision/series.html>

- 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_3_2_0.pdf

- Cisco Cyber Vision Network Sensor Installation Guide for Cisco IE3300 10G, IE3400 and Catalyst 9300:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_Network_Sensor_Installation_Guide_for_Cisco_IE3300_10G_Cisco_IE3400_and_Cisco_Catalyst_9300_3_2_0.pdf

- Cisco Cyber Vision Network Sensor Installation Guide for Cisco IR1101:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_Network_Sensor_Installation_Guide_for_Cisco_IR1101_3_1_1.pdf

- Cisco Cyber Vision Network Sensor Installation Guide for Cisco IC3000:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_Network_Sensor_Installation_Guide_for_Cisco_IC3000_3_2_0.pdf

- Cisco Cyber Vision IC3000 Troubleshooting Guide:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_IC3000_Troubleshooting_Guide_Release_3_0_2.pdf

- Cisco Cyber Vision Center Appliance Installation Guide:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_Center_Appliance_Installation_Guide_3_2_0.pdf

- Cisco Cyber Vision Center VM Installation Guide:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_Center_VM_Installation_Guide_3_2_0.pdf

- Cisco Cyber Vision Integration Guide, Integrating Cisco Cyber Vision with Cisco Identify Services Engine (ISE) via pxGrid:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Integrating-Cisco-Cyber-Vision-with-Cisco-Identify-Services-Engine-via-pxGrid.pdf

- Cisco Cyber Vision REST API User Guide, Release 3.1.0:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_REST-API_User_Guide_Release_3_1_0.pdf

Cisco Cyber Vision 3.2.0 update procedure

Cisco Cyber Vision 3.2.0 includes many enhancements and improvements which require changes to the underlying architecture when upgrading from release 3.1.x to release 3.2.0. These changes will affect both Centers and sensors, excluding IOx sensors (which are embedded in Catalyst 9300, 9400, IE3400, IE3300 10G, and IR1101).

These partition changes require specific update packages called “CiscoCyberVision-sysupgrade”, which will replace the usual update packages and procedures.

Center updates

All 3.1.x versions can be directly upgraded in release 3.2.0 with the usage of the right upgrade package called “CiscoCyberVision-sysupgrade-3.2.0”.

Older versions (3.0.x) need to be upgraded first to release 3.1.2, then to 3.2.0.

The upgrade from 3.1.x to 3.2.0 needs to be launched from the Center Command Line Interface (CLI):

1. Send the package to the `/data/tmp` folder of the Center by using the `'scp'` command.
2. Launch the update with the following command:

```
bash /data/tmp/CiscoCyberVision-sysupgrade-3.2.0
```

Sensor updates – IC3000 Sensor and Sentryo SENSOR3,5,7 cases

All 3.x.x versions can be directly upgraded in release 3.2.0 with the usage of the right upgrade package called “CiscoCyberVision-sysupgrade-sensor-3.2.0”.

The upgrade needs to be launch from the sensor Command Line Interface (CLI):

1. Send the package to the `/data/tmp` folder of the sensor by using the `'scp'` command.
2. Launch the update with the following command:

```
bash /data/tmp/CiscoCyberVision-sysupgrade-sensor-3.2.0
```

Sensor updates – Cisco IOx sensor cases

Cisco IOx sensors can be updated with the standard methods described in the relevant user manuals:

1. Cisco Cyber Vision Sensor Extension update
2. Local Manager update
3. CLI update

Cisco Cyber Vision 3.2.0 important changes

Communication port change

An important change was made on the communication between sensors and the Center. In previous versions, all sensor communications were multiplexed on port TCP/443. Starting with version 3.2.0, sensors will also use port TCP/5671, in addition to port TCP/443.

In case of network architecture with firewalls between the sensors and the Center, rules will have to be updated to authorize this new port alongside port TCP/443.

API authentication

A HTTP header authentication mechanism has been added to both API v1 and v3.

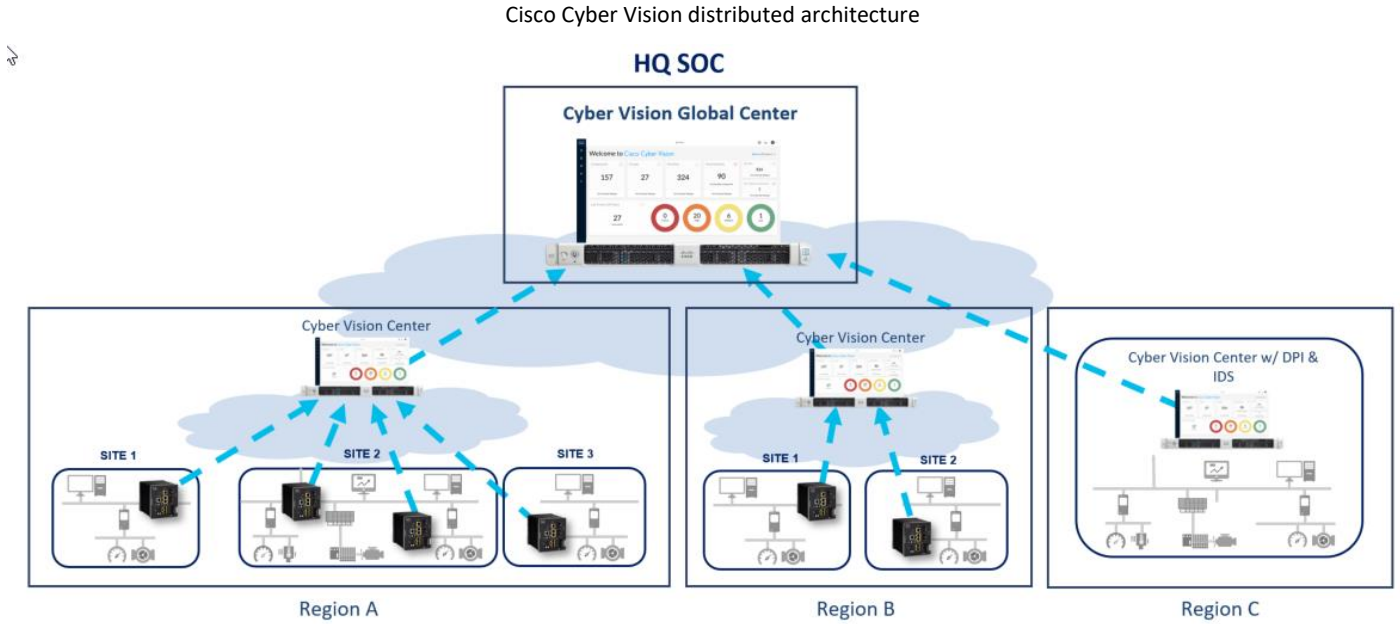
Token authentication through the URL is not supported with API v3.

Token authentication through the URL is now deprecated with API v1 and will be removed in future releases.

Cisco Cyber Vision new features and improvements

Global Center

The Global Center feature gives global visibility on all industrial assets and security events across several sites from a central console.



The global Center gives visibility on:

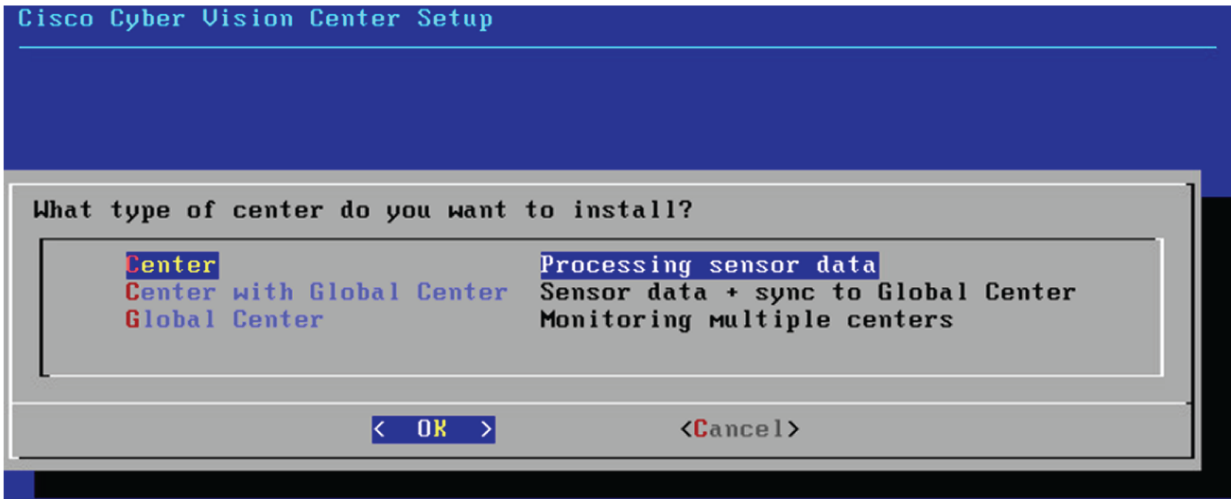
- Asset inventory
- Vulnerabilities
- Activities
- Global Center Presets to view data per site and across sites.

The Global Center provides centralized management of KnowledgeDB updates.

A new step during Center installation allows the user to choose which type of Center to deploy:

- **Center:** processing sensor data, for standalone architecture.
- **Center with Global Center:** processing sensor data and synchronization with a Global Center, for distributed architecture.
- **Global Center:** monitoring multiple centers, for distributed architecture.

Cisco Cyber Vision installation types

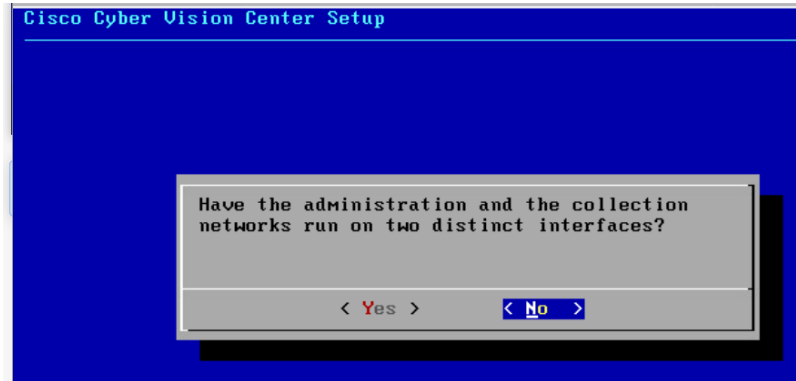


Center single interface

Starting in Cyber Vision 3.2.0, a new deployment option for the Center is now available. Users can deploy the Center leveraging either a single interface for both Administration and Collection, or two independent interfaces, one for Administration and one for Collection.

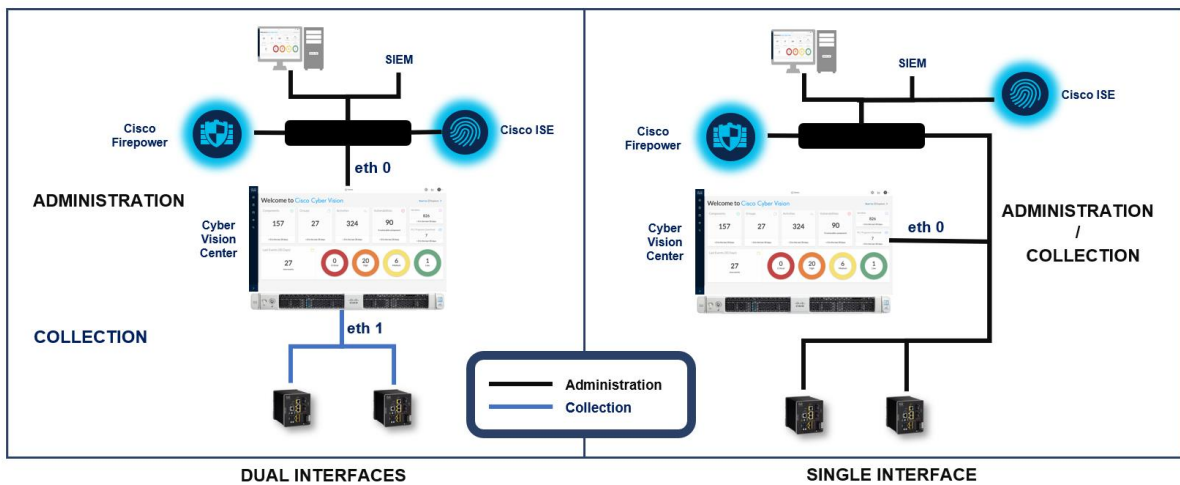
Users can choose whether the Center will use a single or a dual interface during the Center setup (dual interface is recommended for security reasons). Choosing Yes will result in a dual interface deployment, while No will result in a single interface deployment.

Cisco Cyber Vision Administration and Collection segments will run on one or two interfaces



- Single interface: all communications will be done on eth0 (Administration + Collection)
- Dual interface:
 - eth1: sensor communications (Collection segment)
 - eth0: all other communications (Administration segment)

Cisco Cyber Vision dual or single interface



Center DPI and IDS

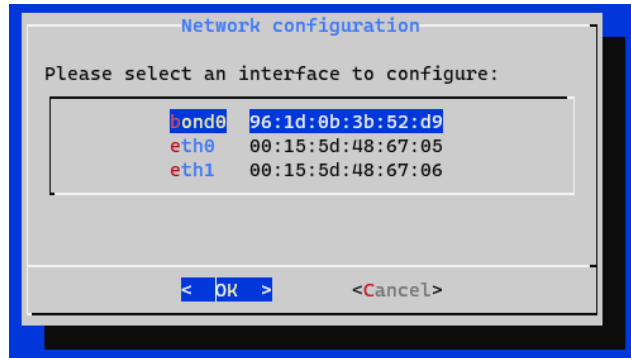
Cyber Vision Center now has built-in DPI and IDS support. Up to 4 interfaces can be configured to receive traffic for DPI and IDS.

This option can be activated on Center Appliances and Virtual Centers which have any additional interfaces available.

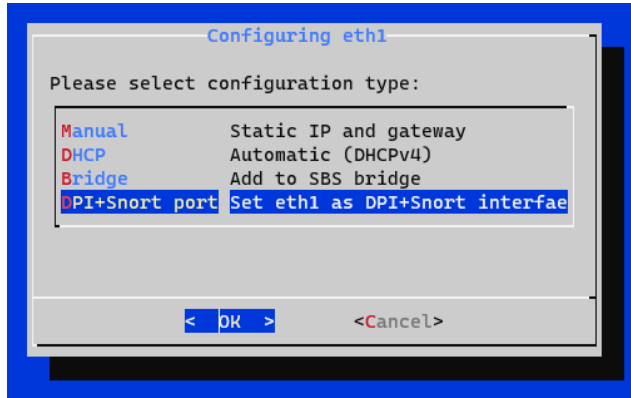
This option needs to be configured from the Center's CLI (Command Line Interface) through the command `sbs-netconf`

A configuration menu will appear, with the following configurations to perform.

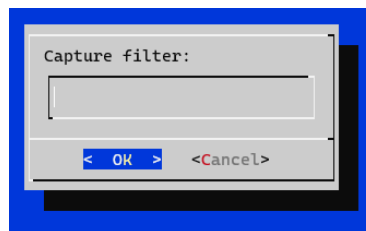
- Select the interface:



- Choose the configuration type DPI+Snort port:



- Add a capture filter if needed:



Once configured, the new sensor capability will be displayed in the sensor list (navigate to Administration > Sensors > Management in Cisco Cyber Vision).

Cisco Cyber Vision Center with DPI + IDS on eth1

- System
- Data management
- Sensors
 - Management
 - Capture
- Users
- Events
- API
- License
- LDAP Settings
- PxGrid
- SNORT
- Integrations

Sensors

From this page, you can manage sensors in online and offline modes and generate provisioning packages to deploy Cisco Cyber Vision on remote sensors. Sensors can also be remotely and securely rebooted, shut down, and erased. When a sensor connects for the first time, you must authorize it so the Center can receive its data.

Name	IP	Version	Status	Processing status	Active Discovery status	Capture Mode [®]	Uptime
<div style="border: 1px solid #ccc; padding: 5px;"> <p>▼ CENTER-ETH1</p> <p>Name: CENTER-ETH1 ✎</p> <p>Status: Running</p> <p>Processing status: Waiting for data</p> <p>Active discovery: Unavailable</p> <p>Deployment: Automatic via DHCP</p> <p>Capture mode: Optimal</p> <p>● Start recording sensor</p> </div>	N/A	N/A	Running	Waiting for data	Unavailable	Optimal	N/A
▶ IE3300-10G	192.168.72.141	3.2.0+202010271236	Connected	Pending data	Unavailable	All	1h 16m 32s

UPDATE CISCO DEVICES

+ DEPLOY CISCO DEVICE

+ INSTALL SENSOR MANUALLY

IMPORT OFFLINE FILE

Active Discovery

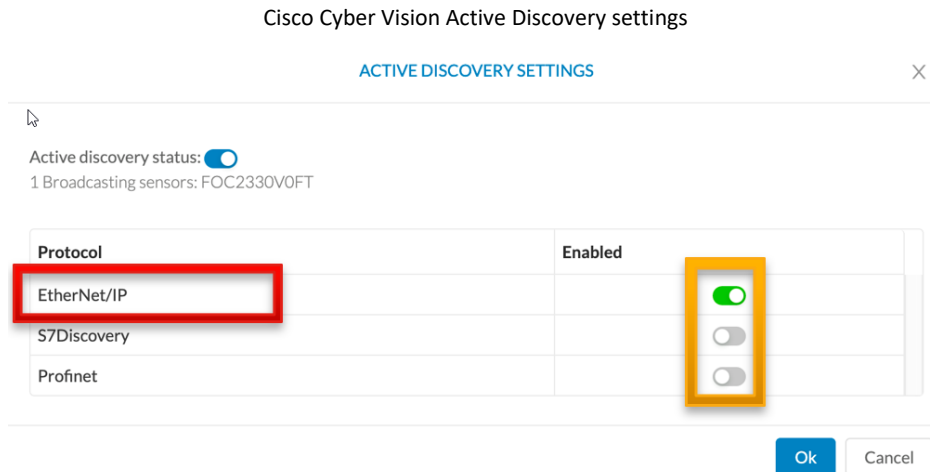
Starting in Cyber Vision 3.2.0, sensors running on the IE3400, IE3300 with 10G, and IC3000 can send requests leveraging industrial protocols to obtain more complete device details. This solution will discover silent devices or add more properties on devices.

The Center can send requests to the sensors to perform Active Discovery on a dedicated protocol based on user's configuration.

Release 3.2.0 brings three protocols supported for Active Discovery:

- Ethernet/IP list identity broadcast message
- S7 discovery broadcast message
- Profinet identification multicast message

Active Discovery settings can be adjusted from the application User Interface. Per preset, Active Discovery needs to be activated and then enabled per protocol.



There are now two sensor builds, one with the Active Discovery feature and the other with passive only. Utilizing a specific version of the Sensor application means no accidental activation of Active Discovery.

During the sensor installation process, new parameters will be requested for the Active Discovery functionality. Users will have to define new interfaces to reach the different networks where they want to discover hardware.

Cisco Cyber Vision Active Discovery settings for IC3000

Application type:
 Passive only
 Passive and Active Discovery

Physical interface:
The port used to send packets
Int2

IP address:
IP address of the interface used to do Active Discovery
192.168.40.22

Prefix length:
Like 24, 16 or 8
24

Cisco Cyber Vision Active Discovery settings for IE3400 and IE3300 10G

Active Discovery configuration

From here you can enable and configure Active Discovery.

IP address:
IP address of the interface used to do Active Discovery
192.168.0.165

Prefix length:
Like 24, 16 or 8
24

VLAN:
VLAN number of the interface. Use 1 by default
1

USE COLLECTION REMOVE

IP address:
IP address of the interface used to do Active Discovery

Prefix length:
Like 24, 16 or 8

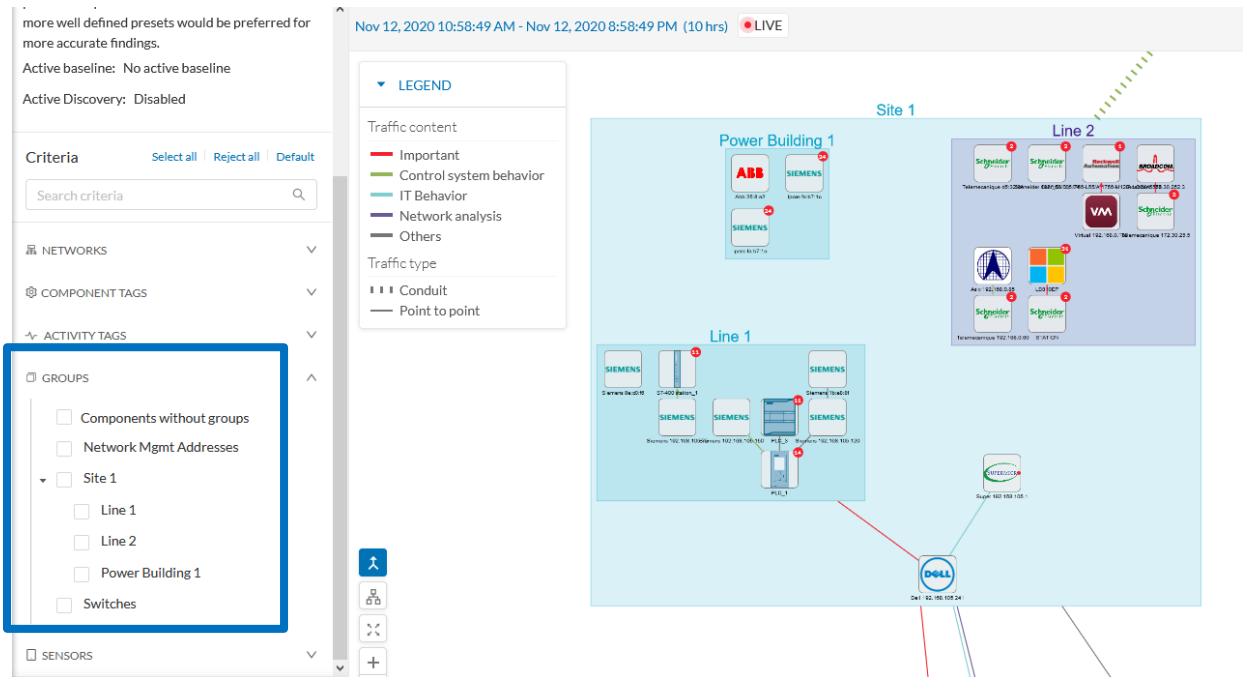
VLAN:
VLAN number of the interface. Use 1 by default

UI improvements

Nested Groups

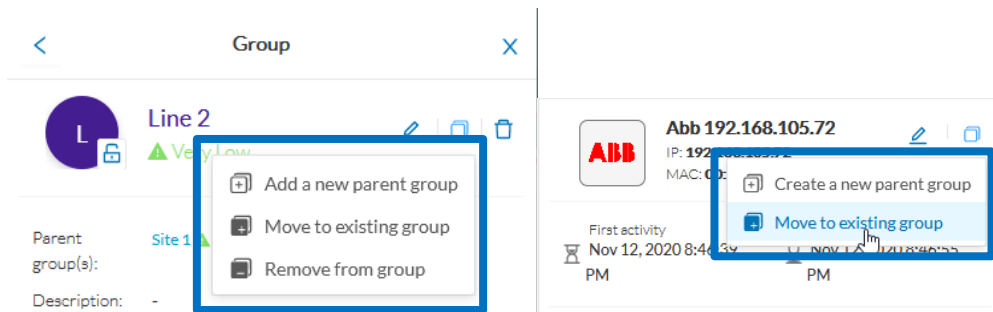
Cisco Cyber Vision release 3.2.0 now provides the ability to create nested groups for a more flexible organization of components to match the business and processes. Nested groups enable multi-faced views and quick drill down in the data set.

Cisco Cyber Vision Nested Groups



New UI functions are present to manage groups and group hierarchy:

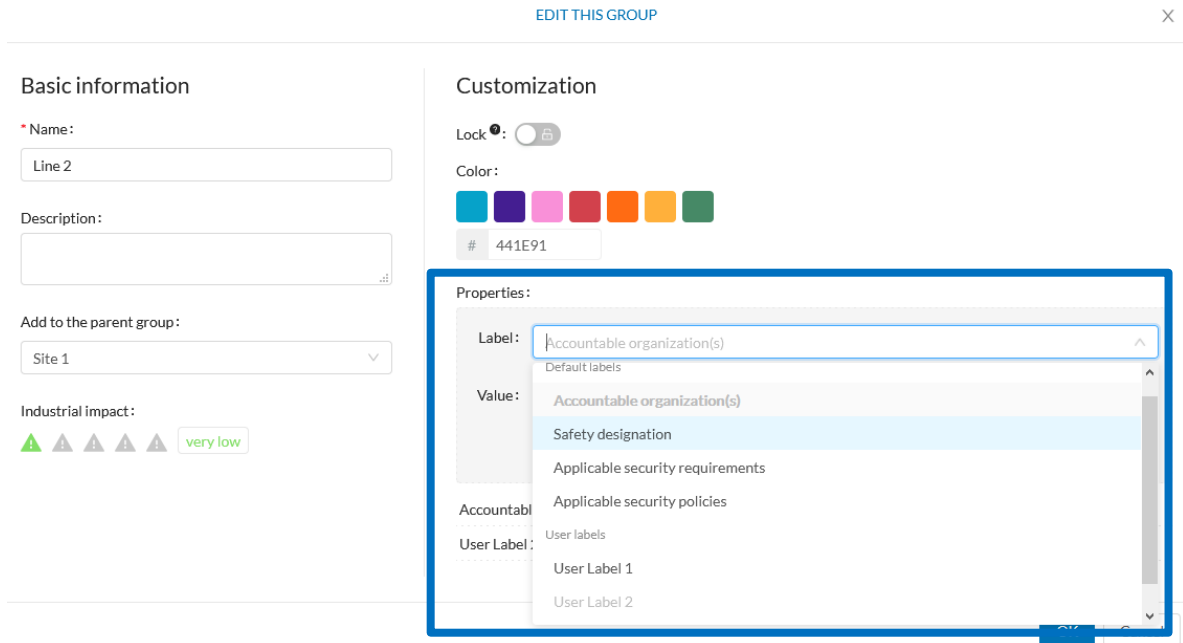
Cisco Cyber Vision Management of Nested Groups



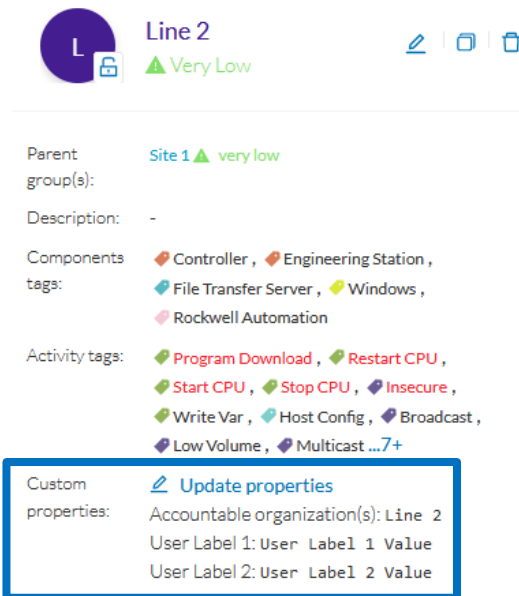
Group Properties

In addition to nested groups, Cisco Cyber Vision now supports group properties with predefined and user properties.

Cisco Cyber Vision Group Properties Edition



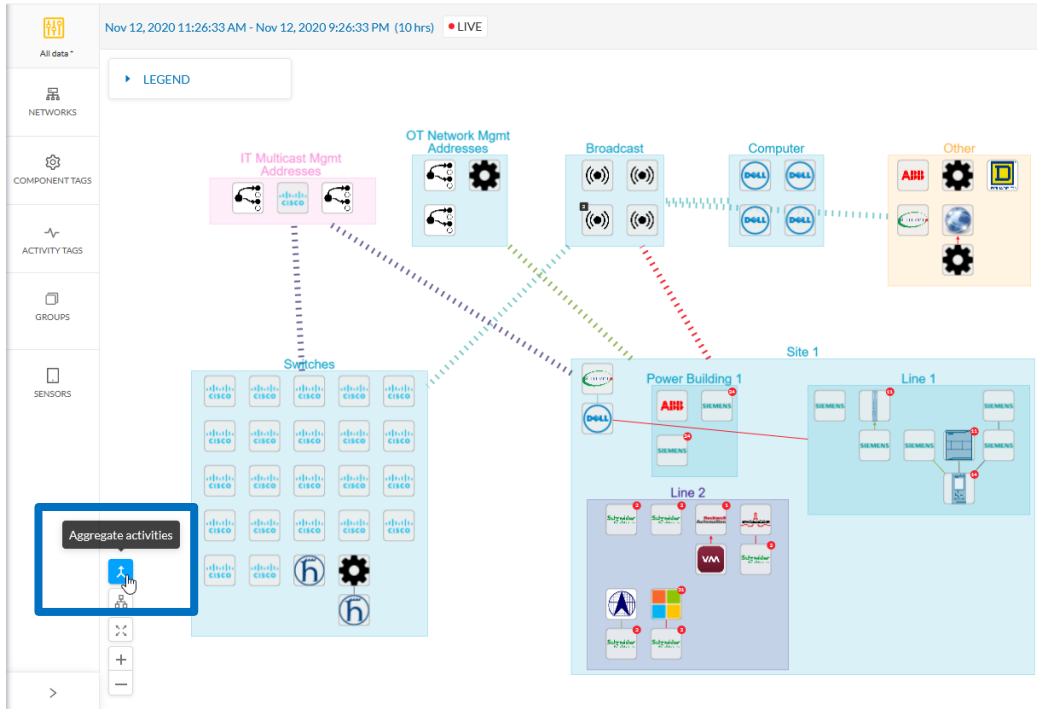
Cisco Cyber Vision Group properties display



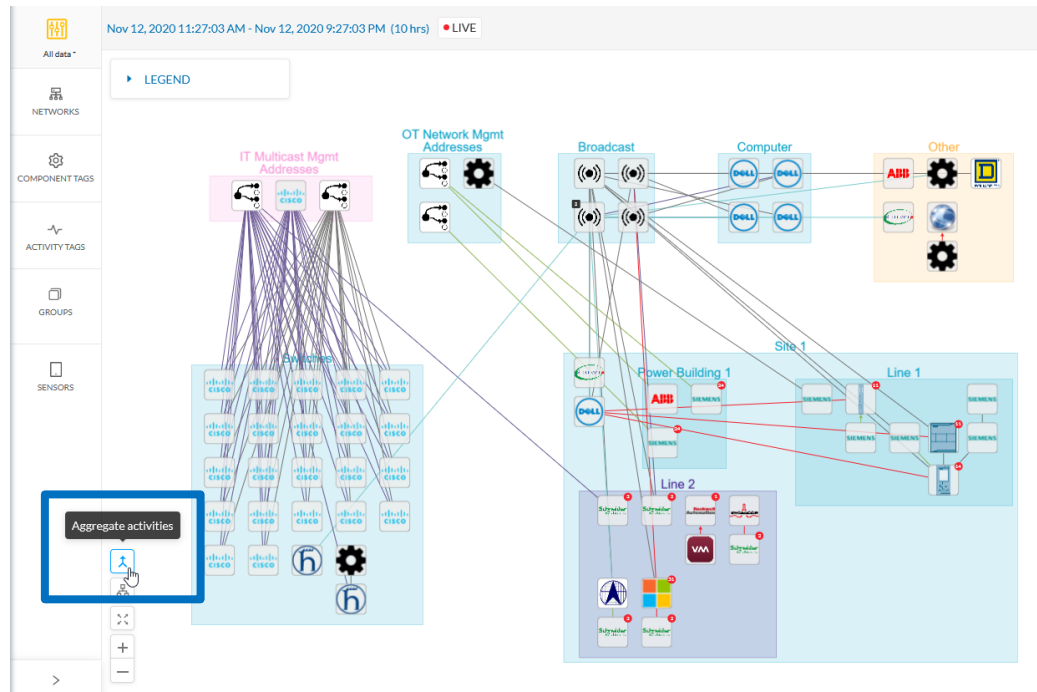
Aggregated activities

Cisco Cyber Vision Maps now have the ability to aggregate activities to simplify the view. Activities with groups or with aggregated objects are now presented in a specific representation, which will replace several flows displayed on the map.

Cisco Cyber Vision Aggregate Activities ON



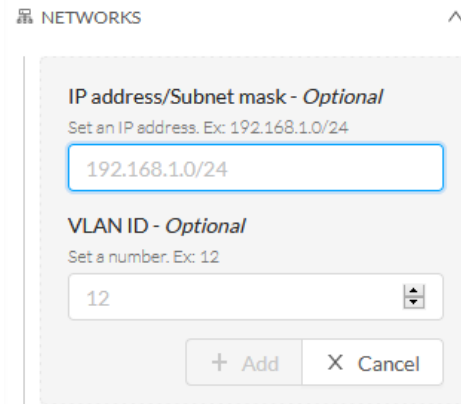
Cisco Cyber Vision Aggregate Activities OFF



Network filters

A new filter category has been added to Cisco Cyber Vision to organize the dataset. Activities and components can be filtered based on subnets or VLAN ID.

Cisco Cyber Vision Network Filters Definition



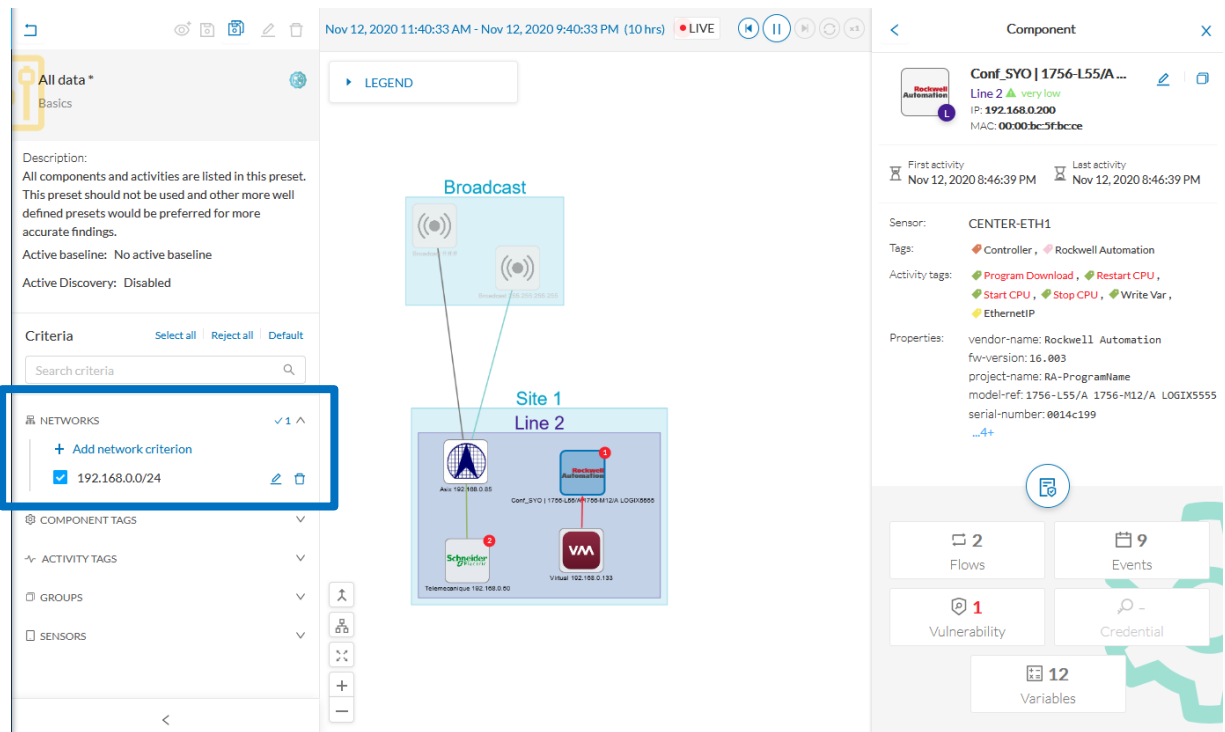
NETWORKS

IP address/Subnet mask - Optional
Set an IP address. Ex: 192.168.1.0/24
192.168.1.0/24

VLAN ID - Optional
Set a number. Ex: 12
12

+ Add X Cancel

Cisco Cyber Vision Network filter based on subnet



Nov 12, 2020 11:40:33 AM - Nov 12, 2020 9:40:33 PM (10 hrs) LIVE

LEGEND

Broadcast

Site 1
Line 2

Component

Conf_SYO | 1756-L55/A...
Line 2 very low
IP: 192.168.0.200
MAC: 00:00:bc:5f:bcce

First activity: Nov 12, 2020 8:46:39 PM
Last activity: Nov 12, 2020 8:46:39 PM

Sensor: CENTER-ETH1
Tags: Controller, Rockwell Automation
Activity tags: Program Download, Restart CPU, Start CPU, Stop CPU, Write Var, EthernetIP
Properties: vendor-name: Rockwell11 Automation, fw-version: 16.003, project-name: RA-ProgramName, model-ref: 1756-L55/A 1756-M12/A LOGIX5555, serial-number: 0014c199, ...4+

2 Flows, 9 Events, 1 Vulnerability, Credential, 12 Variables

Criteria: 192.168.0.0/24

Vulnerability Dashboard

For each preset, a new view is now available in Cisco Cyber Vision release 3.2.0. The Vulnerability Dashboard:

- Gives the top 10 vulnerabilities plus full inventory list
- Is based on presets to drill down data by tags, subnets, VLANs, groups and/or sensors
- Gives links to quickly identify affected components
- Displays additional context for impact and remediation

Cisco Cyber Vision Vulnerability Dashboard

83 Vulnerabilities

10 most matched vulnerabilities

12 Total vulnerable components for All data

Vulnerability severity legend: NONE (Green), LOW (Yellow), MEDIUM (Orange), HIGH (Red), CRITICAL (Black)

Vulnerability title	CVE	CVSS score	Affected components
Schneider Electric Modicon Modbus Protocol Multiple Authentication Bypass Vulnerabilities	CVE-2017-6032	5.3 (v3)	5 components
Schneider Electric Modicon Modbus Protocol - Multiple Authentication Bypass Vulnerabilities	CVE-2017-6034	9.8 (v3)	5 components
Multiple Denial of Service Vulnerabilities on Siemens devices using the PROFINET Discovery and Configuration Protocol	CVE-2017-2680	6.5 (v3)	3 components
Denial-of-Service Vulnerability in Profinet Devices	CVE-2019-10936	7.5 (v3)	3 components
Multiple Siemens Products CVE-2017-12741 Denial of Service Vulnerability	CVE-2017-12741	7.5 (v3)	3 components
Uncontrolled Resource Consumption Vulnerability in Siemens SIMATIC S7	CVE-2019-13940	7.5 (v3)	2 components
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - TCP Urgent Pointer State Confusion due to Race Condition	CVE-2019-12263	8.1 (v3)	2 components
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - Logical Flaw in IPv4 assignment by the ipdhcpc DHCP client	CVE-2019-12264	7.1 (v3)	2 components
Siemens EN100 Ethernet Module CVE-2016-7114 Authentication Bypass Vulnerability	CVE-2016-7114	8.8 (v3)	2 components
Denial-of-Service Vulnerabilities in EN100 Ethernet Communication Module and SIPROTECS relays	CVE-2018-11451	7.5 (v3)	2 components

API Documentation

Cisco Cyber Vision Center now exposes a new API in addition to API V1. API V3 can now be used to interact with the product. This new API is described in a new Administration page (API / Documentation). This page gives details on all available requests and responses as well as the ability to try out the available calls.

Cisco Cyber Vision API Documentation route list

Cisco Cyber Vision API route details

Data handling changes

The internal data handling pipeline of the Cisco Cyber Vision Center has been completely overhauled to increase the overall performance of sensor data intake. On the same hardware, Cisco Cyber Vision 3.2 can handle approximately twice as much incoming data without having to drop flow tables and without delaying database updates. Data processing is now based on the industrial standard RabbitMQ message broker.

These changes are foundational for new and upcoming features of Cisco Cyber Vision, with Global Center data synchronization being the first example.

Secure Boot

Cisco Cyber Vision Center now supports UEFI Secure Boot on Cisco UCS hardware and on compatible VMware vSphere deployments. Center images now use the GRUB2 bootloader, which verifies the integrity of system files at boot time. Additional hardening enhancements have been made to ensure that boot security cannot be bypassed on systems with Secure Boot enabled.

Legacy BIOS boot is still supported on systems which do not provide UEFI Secure Boot, like on Sentryo CENTER10 and CENTER30 hardware. System images can use both boot modes.

Note: boot security is also provided on sensors based on IOx technology as all sensor images are signed and verified at install time by the platform.

DPI improvements

Cisco Cyber Vision Sensors could now do the DPI on new protocols like

- HSR, PRP, MRP, DLR, VRRP
- Fanuc robot protocols

Improvements of some protocols were also added to this version:

- FL-NET
- OPC UA/DA
- Ethernet/IP (CIP)
- S7, Profinet

IDS licensing updates

IDS and Snort community rule set are included in Advantage license, with the support for custom Snort rules.

A License is required for Snort subscriber rule set. A new option is available in the SNORT administration page to select if the solution will use subscriber rules.

Cisco Cyber Vision Activate Subscriber rules

SNORT

From this page, you can configure which Snort rules are deployed on the CCV sensors. You can also load your own custom Snort rules and manage the state of specific Snort rules. By default, CCV uses public Snort rules coming from the Cisco Talos ruleset. With an additional cost, you can upgrade to the subscriber version of the Cisco Talos ruleset.

Use subscriber rules:

Categories

Category	Download rules	Status
Browser	↓	<input checked="" type="checkbox"/>
Deleted	↓	<input type="checkbox"/>
Experimental-DoS	↓	<input type="checkbox"/>
Experimental-Scada	↓	<input type="checkbox"/>
Exploit-Kit	↓	<input checked="" type="checkbox"/>
File	↓	<input checked="" type="checkbox"/>
Malware-Backdoor	↓	<input checked="" type="checkbox"/>
Malware-CNC	↓	<input checked="" type="checkbox"/>

Import custom rules

[↓ IMPORT CUSTOM RULES FILE](#)

Specific rule

Rule sid: [DISABLE](#) [ENABLE](#)

[RESET TO DEFAULT](#) [SYNCHRONIZE RULES ON SENSORS](#)

Cisco Cyber Vision IDS License

Smart Software Licensing

To view and manage Smart Licenses for your Cisco Smart Account, go to [Smart Software Manager](#)

Smart Software Licensing Status

- Software Subscription Licensing: Advantage [VIEW / EDIT](#)
- Registration Status: Registered (Thursday, September 3, 2020 9:45 AM)
- License Authorization Status: Authorized (Friday, September 4, 2020 3:23 PM)
- Smart Account: InternalTestDemoAccount20.cisco.com
- Virtual Account: IOT Security Demos
- Transport Settings: Direct [VIEW / EDIT](#)

Smart License Usage

License (Version)	Description	Count	Status
Cisco Cyber Vision Advantage	Cisco Cyber Vision Advantage Smart license. Inclusive of Cyber Vision Essentials Capabilities.	11	<input checked="" type="checkbox"/> Authorized
Cyber Vision Sensor Intrusion Detection License for IC3000	Cyber Vision Sensor Intrusion Detection License for IC3000 Hardware-Sensor. Requires Advantage License.	1	<input checked="" type="checkbox"/> Authorized

Knowledge Base improvements

In addition to the new subscriber rules, the KnowledgeDB release introduces the support of Phoenix Contact vulnerabilities. All recent Phoenix Contact vulnerabilities have now been added as part of the KnowledgeDB. Cisco Cyber Vision is thus able to match the latest vulnerabilities to Phoenix Contact devices detected on the network.

Improvements of Cisco Cyber Vision integration with pxGrid and Cisco ISE

The list of the attributes exchanged was improved with 2 new attributes (Group path and Custom name):

List of endpoint custom attributes to create in Cisco ISE:

Endpoint Custom Attributes

Attribute Name	Type
<input type="text" value="assetSource"/>	String
<input type="text" value="assetGroup"/>	String
<input type="text" value="assetProjectVersion"/>	String
<input type="text" value="assetOsName"/>	String
<input type="text" value="assetProjectName"/>	String
<input type="text" value="assetModelName"/>	String
<input type="text" value="assetGroupPath"/>	String
<input type="text" value="assetCustomName"/>	String

The list of attributes available is now:

List of properties exchange with Cisco ISE:

CCV properties	Description	ISE properties	ISE Custom Attributes
ID	Cisco Cyber Vision Component ID	assetId	no
Name	Component name	assetName	no
Ip	Component IP address	assetIpAddress	no
Mac	Component MAC address	assetMacAddress	no
Vendor-name	Component manufacturer (IEEE OUI)	assetVendor	no
Model-ref	Manufacturer product ID	assetProductId	no
Serial-number	Manufacturer serial number	assetSerialNumber	no
Tags	All levels component tags are concatenated in one string	assetDeviceType	no
Fw-version	Component firmware version	assetSwRevision	no
Hw-version	Component hardware version	assetHwRevision	no
Protocols	All protocols are concatenated in one string	assetProtocol	no
Model-name	Manufacturer model name	assetModelName	yes
Os-name	Operating system name	assetOsName	yes
Project-name	Project name (inside PLC program)	assetProjectName	yes
Project-version	Project version (inside PLC program)	assetProjectVersion	yes
Group	Component group	assetGroup	yes
Group path	Component group path (nested groups)	assetGroupPath	yes
Custom name	Component custom name	assetCustomName	yes

ISE will update custom attributes when profiling policies in ISE defined to leverage them. Without a profiling policy leveraging them, custom attributes may not be updated in ISE.

Cisco Cyber Vision Bug fixed

Issues ID / CDETS	Description
#5253 / CSCvt81672	Cisco Cyber Vision Center Command Injection Vulnerability. A vulnerability was fixed in the Center's CLI. The vulnerability potentially allowed an authenticated, local attacker to inject arguments into a vulnerable command on an affected device.
#5238 / CSCvt81671	Postgresql version was upgraded, previous version was vulnerable to high severity CVEs.
#5251 / CSCvt81711	Various security issues fixed.
#5265 / CSCvt81666	Various security issues fixed.
#4821 / CSCvu41812	Issue fixed in ISE PxGrid communication. Before, ISE PxGrid communication used to go down after upgrade and needed to be started manually.
#3542 / CSCvt18302	Cisco Cyber Vision Center pxGrid configuration did not come when there was a white space in the node name.
#2629 / CSCvs44234	Cisco Cyber Vision Center is now flagging read/write variables in S7 communication even on router redundancy context.
#3543 / CSCvt34698	Basic Auth Base64 HTTP Credential not detected.

Cisco Cyber open CDETS and known issues

Issues ID / CDETS	Component	Description
#5695 / CSCvv49682	IC3000	Cisco Cyber Vision Sensor installation with extension fails with IC3000 release 1.3.1. Local Manager installation or USB installation should be used.
# - / CSCvv48350	IC3000	Multicast packets are dropped by the platform, before Cisco Cyber Vision Application.
#4049 /	IE3400 Sensor	MTU to the IOx application is limited to 1500 including ERSPAN header which creates issues with large packets where packets are dropped. IE3400 image 17.4.1 solved this issue in addition to the command <code>"ip link set mtu 2000 dev eth1"</code> on the sensor Command line Interface.
#6202 / CSCvv46925	IE3400H, Catalyst9400	Cisco Cyber Vision Extension Sensor management does not support IE-3400H, Catalyst 9400. Manual installation should be used to deploy the sensor.