



Release Notes for Cisco Cyber Vision

Release 3.1.0

Compatible device list	3
Links	4
Software Download	4
Related Documentation	5
Important note to Cisco Cyber Vision version 3.0.x users	6
Cisco Cyber Vision New features	6
Cisco Cyber Vision Network Sensors enhancements in version 3.1.0	6
Network Sensors	6
Network-Sensor Requirements & Caveats	6
Cisco Cyber Vision Sensors enhancements in version 3.1.0	6
Sensor Store and forward	6
Sensor app management	7
Sensor DPI Engine Optimizations	8
New or improved protocol support	8
New “Security insights” dashboards	10
Intrusion detection & investigation improvements	11
Cisco Threat Response	11
SNORT intrusion detection improvements	12
Integrations	13
Cisco Cyber Vision Center to ISE improvements	13
Cisco Cyber Vision Center to FMC	16
Cisco Cyber Vision Center to FTD	16
New monitoring/baseline UX/UI	17
Baselines as Preset's normal states	17
Review and assignment of differences	17
New in 3.1: Creating baselines from presets	18
New in 3.1: View all anomalies across all baselines	19
New in 3.1: View new and changed items	19
New in 3.1: Detailed list of new and modified assets	20
New in 3.1: Detailed list of new and modified activities	20

investigate baseline changes	21
New monitoring/baseline UX/UI	22
New extension capabilities	22
PDF and CSV export across the platform	22
Platform admin enhancements	23
Miscellaneous	23
DNS default server change	23
Cisco Cyber Vision issues fixed	24
Cisco Cyber open CDETS and known issues	27

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 Rack Server	Cyber Vision Center hardware appliance (Cisco UCS® C220 M5 Rack Server)
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 IR1101	Cyber Vision Sensor IOx application hosted in Cisco IR1101 Series Industrial Integrated Services Routers
Cisco Catalyst 9300	Cyber Vision Sensor IOx application hosted in Catalyst 9300 Series switches
Sentryo SENSOR3	Sentryo SENSOR3 hardware appliance
Sentryo SENSOR5	Sentryo SENSOR5 hardware appliance
Sentryo SENSOR7	Sentryo SENSOR7 hardware appliance

Links

Software Download

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

The files below can be find following this link.

Center	Description
CiscoCyberVision-3.1.0.ova	VMWare OVA file, for Center setup
CiscoCyberVision-3.1.0.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-sensor-management-3.1.0.ext	Sensor Management extension installation file
Sensor	Description
CiscoCyberVision-IOx-aarch64-3.1.0.tar	IE3400, IR1101 sensor installation and update file
CiscoCyberVision-IOx-IC3K-3.1.0.tar	IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-3.1.0.tar	Cat9k sensor installation and update file
Updates	Description
CiscoCyberVision-update-center-3.1.0.dat	Center update file
CiscoCyberVision-update-sensor-3.1.0.dat	Sentryo Sensor3, 5, 7 update file
CiscoCyberVision-update-combined-3.1.0.dat	Center and Legacy Sensor update file from GUI
CiscoCyberVision-Embedded-KDB-3.1.0.dat	KnowledgeBase embedded in Cisco Cyber Vision 3.1.0

Related Documentation

New!

- 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_1_0.pdf

- Cisco Cyber Vision IE3400 and CAT9300 Installation Guide:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_IE3400_and_CAT9300_Installation_Guide_Release_3_1_0.pdf

- Cisco Cyber Vision IR1101 Installation Guide:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_IR1101_Installation_Guide_Release_3_1_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

- 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 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 Center VM Installation Guide:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_Center_VM_Installation_Guide_Release_3_0_1.pdf

Important note to Cisco Cyber Vision version 3.0.x users

A version 3.0.3 is released at the same time as version 3.1.0. Upgrade from any version (prior to 3.0.3) to 3.1.0 could fail due to the size of a partition. Version 3.0.3 will increase the partition's size to avoid any issue to occur during the upgrade. Only the Cisco Cyber Vision Center must be upgraded to 3.0.3 before being upgraded to version 3.1.0.

Cisco Cyber Vision New features

Cisco Cyber Vision Network Sensors enhancements in version 3.1.0

Network Sensors

Network Sensors are now available, Cisco Cyber Vision Sensor can now be deployed on the following hardware:

- Cisco IR1101: The next-generation rugged integrated services router.
- Cisco IE3400 and 3400H: Advanced modular switches for the most demanding industrial environments.
- Cisco Catalyst 9000: The foundation of the modern intent-based network (9300, 9400, 9500 models supported as of IOS-XE Release 17.3.1).

Network-Sensor Requirements & Caveats

- IR1101
 - Store & Forward requires Expansion Module with mSATA
 - Cellular interface for WAN connections requires use of VPN tunnel
 - ERSPAN to IOx not supported natively on cellular interface
 - ERSPAN source must be attached to Tunnel interface
- Catalyst 9K
 - Requires DNA Advantage License
 - IOx requires USB SSD (SSD-120G)
 - SPAN to IOx officially supported as of IOS-XE release 17.3.1
- IE3400
 - IOx requires SD-Card (4GB)

Cisco Cyber Vision Sensors enhancements in version 3.1.0

Sensor Store and forward

The Cisco Cyber Vision Sensor will now store DPI data indefinitely on disk when the connection to the Center is lost.

Data is uploaded to the Cisco Cyber Vision Center when the connection is restored.

Sensor app management

Sensor app management is an IOx app install module built into Cisco Cyber Vision Center. With this sensor management extension, the Cisco Cyber Vision Sensor application for IOx can be easily installed, configured, and managed centrally from the Cisco Cyber Vision Center.

A new button “Deploy Cisco Device” is available in the Sensors Management page. This button opens new screens to deploy Sensor application on IOx devices.

Sensors Management New Deploy Button:



New GUIs to configure remote sensor in the Center:

IC3000 Sensor Application command line view:

A screenshot of a web-based configuration form titled 'Deploy IOx App'. The form contains several input fields for network configuration. The fields are arranged in two columns. The first column includes: 'IP address:' (192.168.30.25), 'User:' (admin), 'Capture IP address:' (169.254.1.2), 'Capture VLAN number:' (2508), 'Collection subnet mask:' (24), and 'Collection VLAN number:' (507). The second column includes: 'Port:' (443), 'Password:' (masked with asterisks), 'Capture subnet mask:' (30), 'Collection IP address:' (192.168.69.208), and 'Collection gateway:' (192.168.69.1). At the bottom left, there is a 'Capture mode:' section with four radio button options: 'All: analyze all the flows' (selected), 'Optimal (Default): analyze the most relevant flows', 'Industrial only: analyze industrial flows', and 'Custom: you set your filter using a packet filter in tcpdump-compatible syntax'. At the bottom right, there are two buttons: '+ Deploy' and 'Cancel'. A mouse cursor is pointing at the '+ Deploy' button.

Deep Packet Inspection

Sensor DPI Engine Optimizations

In addition to the developments required to support new network devices, more storage and functionalities, an effort was done to change the DPI engine for more efficiency and agility. These enhancements will increase performances and be useful for future functionalities development.

New or improved protocol support

- Manufacturing protocols
 - PCCC/DF1 (Allen-Bradley/Rockwell)
 - FL-NET / CMP-LINK (Toyoda/Jtekt)

Center GUI – Explore – Toyoda PLC and TOYPUC / FLNet protocols

The screenshot displays the 'Component' details for a Toyoda PLC. The component name is 'Toyoda 192.168.0.97' with IP: 192.168.0.97 and MAC: 00:60:53:24:15:f8. It shows activity logs with a first activity on May 20, 2020 at 3:09:42 PM and a last activity at the same time. The 'Tags' section includes 'Controller' and 'Activity tags' such as 'Program Download', 'Program Upload', 'Reset Process', 'Start CPU', and 'Stop CPU...7+'. A summary box on the right indicates 212 Flows, 40 Events, and 97985 Variables. The 'Properties' section lists vendor information (TOYODA MACHINE WORKS, LTD.), firmware version (V1.30), and specific device details like 'toyoduc-some-version: V10.a' and 'toyoduc-status: Under a stop+Under stop-request continuity+PC3 mode+Alarm(2062)'.

This screenshot shows a network diagram on the left with two Toyoda PLCs (PC3JX and Toyoda 192.168.250.1) connected to a central device (192.168.250.255). On the right, the 'Component' details for 'Toyoda 192.168.250.1' are shown, including IP: 192.168.250.1, MAC: 00:60:53:24:15:f7, and activity logs. The 'Tags' section includes 'Controller', 'Activity tags' like 'Write Var', 'Broadcast', 'Exception', and 'FLnet'. The 'Properties' section lists vendor information and device details. A summary box on the right indicates 2 Flows, 5 Events, and 2 Variables.

- Power Grid protocols
 - IEC 101 over TCP
 - IEC 104 IOA as a variable

Center GUI – Explore – IEC104 protocol variables

The screenshot displays the 'Variables accesses' section in the Center GUI. At the top, there is a component header for '1.1.0.1' with IP '1.1.0.1' and MAC '00:24:9b:1e:66:90'. It shows activity logs for 'First activity' and 'Last activity' on May 20, 2020. There are also tags like 'Controller', 'Slave', and 'Public IP', and activity tags like 'Notify Var', 'Read Var', 'Broadcast', 'Low Volume', and 'ARP...1+'. A sidebar on the right shows '13 Flows', '3 Events', 'Vulnerability', and 'Credential' counts, along with a '544 Variables' indicator. The main table lists variable accesses with columns for Variable, Protocol, Details, Types, Accessed by, First access, and Last access.

Variable	Protocol	Details	Types	Accessed by	First access	Last access
104.SIQ	IEC104	IOA_M_SP_NA_1	READ	1.1.0.2	May 20, 2020 3:24:15 PM	May 20, 2020 3:24:15 PM
104.SIQ	IEC104	IOA_M_SP_TB_1	NOTIFY	1.1.0.2	May 20, 2020 3:44:50 PM	May 20, 2020 3:44:50 PM
105.SIQ	IEC104	IOA_M_SP_NA_1	READ	1.1.0.2	May 20, 2020 3:24:15 PM	May 20, 2020 3:24:15 PM
106.SIQ	IEC104	IOA_M_SP_NA_1	READ	1.1.0.2	May 20, 2020 3:24:15 PM	May 20, 2020 3:24:15 PM
107.SIQ	IEC104	IOA_M_SP_NA_1	READ	1.1.0.2	May 20, 2020 3:24:15 PM	May 20, 2020 3:24:15 PM

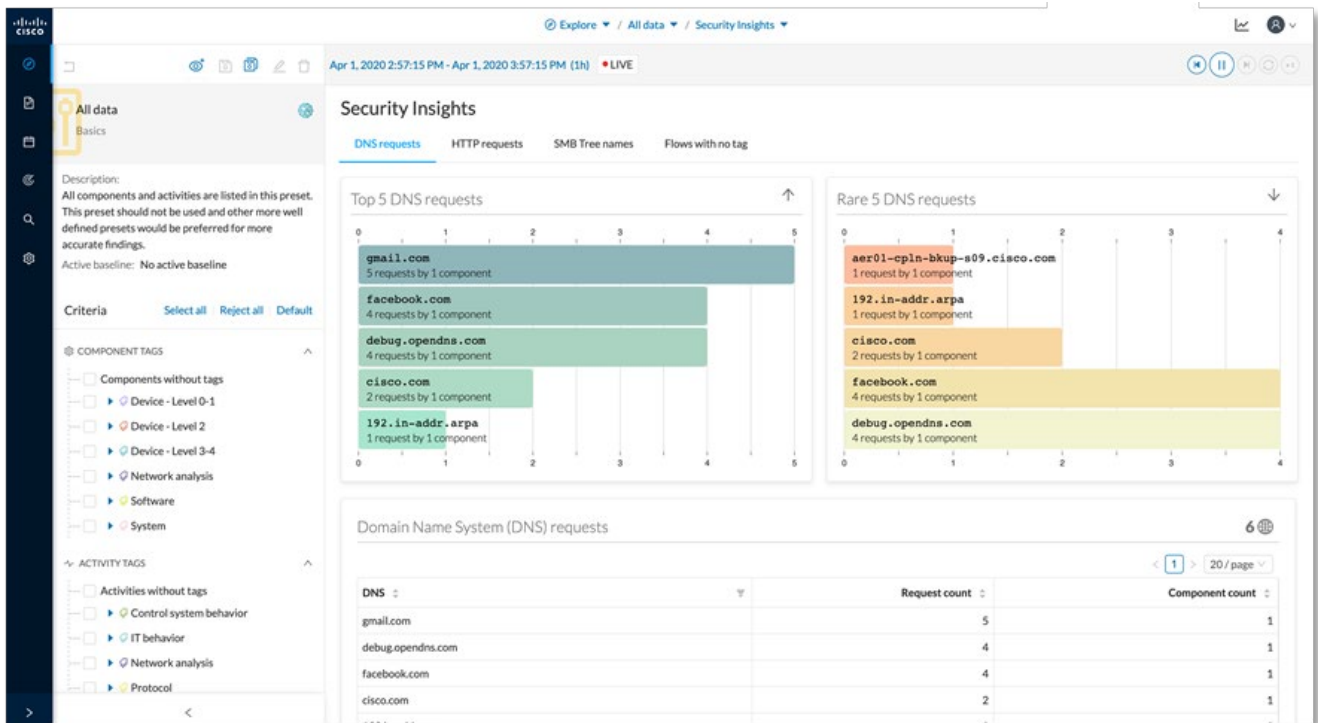
- IEC 61850 Sampled Values
- ICCP (GRID)/TASE.2

New “Security insights” dashboards

The new Security insights page is available to improve the presentation of Sensor DPI. Available dashboards focus on:

- DNS Requests
- HTTP requests
- SMB Tree Names
- Flows with no tag

Center GUI – Explore – Security Insights – DNS requests



Intrusion detection & investigation improvements

Cisco Threat Response

Cisco Cyber Vision is now integrated with Cisco's security investigation platform (i.e. CTR). A new button in the Component page will pivot from Cisco Cyber Vision to CTR to investigate observables. The IP and Mac addresses will be used to display the details pulled from Umbrella, FTD, Talos, AMP, Stealthwatch, etc.

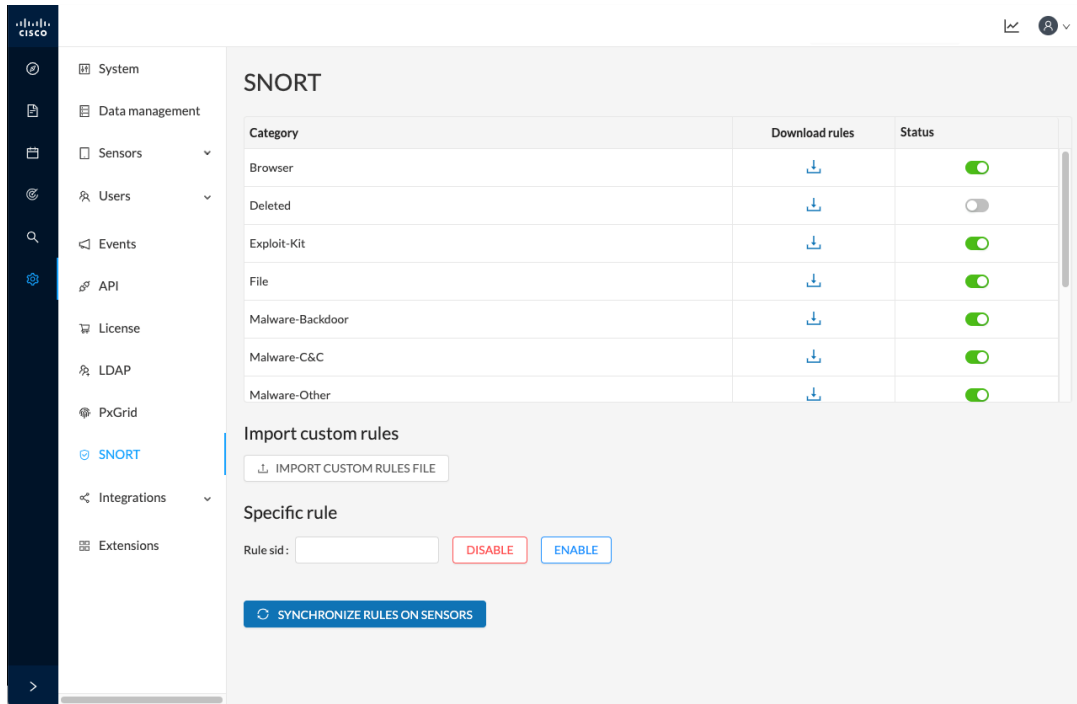
Center GUI – Component details – Investigate in CTR

The screenshot displays the Cisco Cyber Vision interface. On the left, a 'Component' card for 'vmware' shows details for IP: 208.67.222.222 and MAC: 00:50:56:c0:00:08. A button labeled 'Investigate in Cisco Threat Response' is highlighted. A large blue arrow points from this button to the right, where the Threat Response interface is shown. This interface includes a search bar with the IP address 208.67.222.222, a 'Relations Graph', and a detailed view of the IP address with associated actions like 'Copy to Clipboard' and 'Create Judgement'. A table at the bottom right shows a judgement from Umbrella with a disposition of 'Unknown' and a reason of 'Neutral Cisco Umbrella r'.

SNORT intrusion detection improvements

Cisco Cyber Vision Center GUI has a new dashboard to manage sets of rules. Rules can be enabled or disabled by categories, or individually through their sid. Custom rules can also be imported in the system. The new administration panels developed will allow the rules to synchronize on the sensors and you to enable or disable the SNORT engine in sensors.

Center GUI – Administration – SNORT settings



Talos subscriber ruleset is now included in Cisco Cyber Vision.

Integrations

Cisco Cyber Vision Center to ISE improvements

Several developments have been done in Cisco Cyber Vision 3.0.2 and 3.1.0 to improve the way information is pushed to ISE. As a reminder, Cisco Cyber Vision uses pxGrid to publish discovered components as endpoints in ISE. Three main topics were addressed:

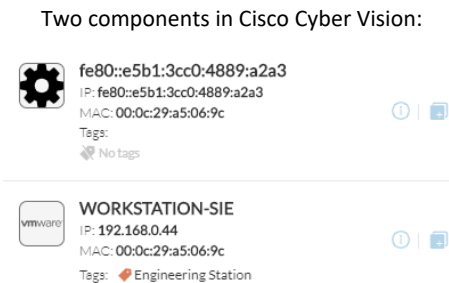
- Components aggregation based on MAC addresses.
- Refresh of Cisco Cyber Vision components' properties.
- Properties clarification and documentation.

Related issues have been closed (refer to [Cisco Cyber Vision Bug fixed](#) here below).

MAC aggregation

When endpoints in ISE are the equivalent of components in Cisco Cyber Vision, they are handled differently. In fact, ISE endpoints have a single MAC address and are listed as such, whereas in Cisco Cyber Vision several components can have a same MAC address and/or a same IP address and are aggregated in one component. Consequently, changes had to be made on the way Cisco Cyber Vision sends this data to ISE to reflect aggregated components.

Example:



These components represent a Virtual Machine with two IP addresses (an IPV4 and an IPV6) on the same MAC address.

In this case, Cisco Cyber Vision sends to ISE an aggregated component based on the MAC address with a summary of the properties of both components. You can see below that the IP addresses are combined into one field to display both IPV4 and IPV6 IP addresses, and other properties like protocols are merged too.

Cisco Cyber Vision components aggregated in a single endpoint in ISE:

assetDeviceType	Engineering Station
assetId	2a90413b-36e8-5ad7-8963-516cf81132f1,e46a6ace-20e4-58b9-8b2f-7f8b3961ab77
assetIpAddress	fe80::e5b1:3cc0:4889:a2a3,192.168.0.44
assetMacAddress	00:0c:29:a5:06:9c
assetName	fe80::e5b1:3cc0:4889:a2a3,WORKSTATION-SIE
assetProtocol	IPv6,ARP, S7Discovery, Profinet, Profinet DCP, Profinet, S7Plus, ARP, Profinet DCP
assetVendor	VMware, Inc.
ip	fe80::e5b1:3cc0:4889:a2a3,192.168.0.44

Endpoints refresh

Cisco Cyber Vision sends components to ISE to create endpoints. In version 3.0.2, when a new property is discovered on a component, this property is sent to ISE and the endpoint is updated accordingly.

Example:

A PLC program project name has been discovered in Cisco Cyber Vision and is pushed to ISE so the corresponding endpoint is updated:

assetProjectVersion	
assetOsName	
assetProjectName	SecDemo_Cell1PLC
assetModelName	

Properties supported

The following table lists and describes all components properties that can be sent to ISE and their corresponding names.

Note: ISE default properties are used as much as possible, but some properties must be created manually in ISE (see in the table “ISE Custom Attributes: Yes”).

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	Component group	assetCCVGrp	yes

All ISE Custom attributes request policies in ISE to be refreshed. Without policy the custom attributes will not be updated in ISE.

Cisco Cyber Vision Center to FMC

A new administration page was developed to connect Cisco Cyber Vision with Firepower Management Center. A list of the new components discovered by Cisco Cyber Vision is sent every 10 seconds with the following properties:

- Name
- Id
- Ip
- Mac

And if they are available:

- hw_version
- model-ref
- serial_number
- fw_version
- tags

Cisco Cyber Vision Center to FTD

Cisco Cyber Vision can now connect with Firepower Threat Defense to automatically kill anomalies detected by the Monitor Mode and Snort events.

Every 10 seconds Cisco Cyber Vision will browse the new Monitor mode and Snort events and send the corresponding actions to the firewall. To enable that functionality, the user needs to add some parameters in the FTD administration page.

Two options are available to kill a session from monitor difference detection events or kill a session from Snort events.

New monitoring/baseline UX/UI

In version 3.1.0 the Monitor mode has been completely redone to match version 3.0.0 of Cisco Cyber Vision's logic and architecture.

Cisco Cyber Vision provides a monitoring tool called the Monitor mode to detect changes inside industrial networks such as unpredicted behaviors that can compromise a network's operation and security. The Monitor mode aims to show the evolution of a network's behaviors based on presets. Changes are noted as differences in the Monitor mode when a behavior happens. Using the Monitor mode is particularly convenient for large networks as a preset shows a network fragment and changes are highlighted and managed separately, in the Monitor mode's views.

Baselines as Preset's normal states

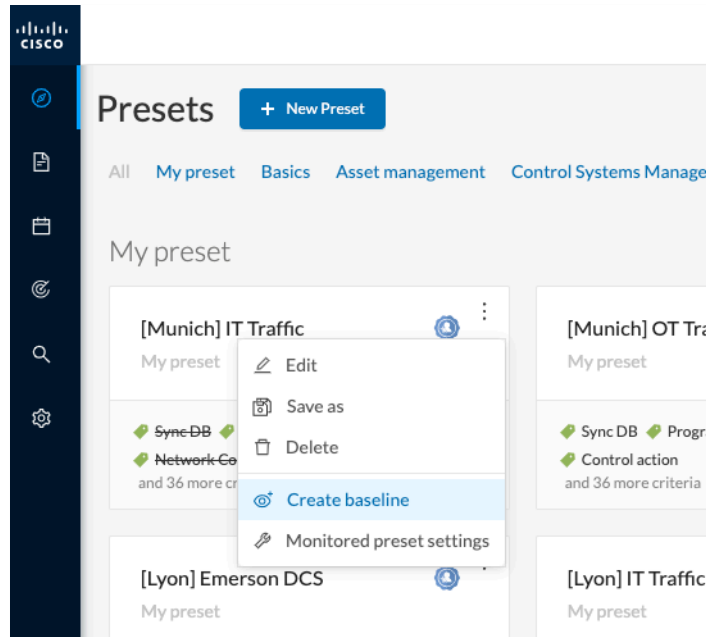
A Preset is a set of criteria which aims to show a detailed fragment of a network. To start monitoring a network, you need to pick up a preset, and to define what would be its normal, stable state, which will be the preset's baseline. This state may rely on a time period, as a network fragment may be subject to several states. Hence, it is possible to create several planned, controlled and time-framed baselines per preset, and to monitor the whole network, with prioritized critical points. For example, a normal state of the network can be a typical weekday operating mode, in which numerous processes are performed iteratively. During weekends, these processes may be slowed down, different, or even stopped. Any network phase can be saved as a baseline by selecting the time span in which it occurs and monitored. Thus, you can set several baselines per Preset, such as a weekly operating state, a regular maintenance period, a degraded mode, a weekend and night mode, and so forth. A baseline is created for a situation considered as part of a normal operating process and will consider all network behaviors (components, activities, properties, tags, variable accesses) to be reviewed.

Review and assignment of differences

Any difference detected is highlighted in the Monitor mode. When reviewing these, they can be acknowledged, reported or removed. It depends on whether you consider them as normal or not, and their level of criticality. That is, you can include these changes into your baseline if it is part of a normal network development process, take action in case of suspicious behavior, or remove a difference because you don't need to see it. By doing so, each baseline will be refined bit by bit over time and become more compliant with your needs.

New in 3.1: Creating baselines from presets

Center GUI – Explore – Presets dashboard



- Fine tune the dataset you want to monitor by creating presets
- Create several baselines for each preset to monitor various states (production/maintenance)
- Set frequency checks and event severity by baseline

What is a Baseline?

It is a snapshot of the production system, letting users define what “normal” is.

Cisco Cyber Vision detects changes to trigger alerts.

New in 3.1: View all anomalies across all baselines

Center GUI – Monitor – All Monitor Presets Dashboard

The screenshot shows the 'Monitor' dashboard with the following data:

Section	Baseline	Monitoring	Normal baseline	Maintenance	Production phase	TOTAL
Monitored Presets	siemens only	72	9	0	13	72
	192.168.0 subnet	9	9	0	0	9
	General Map	13	0	0	13	13
All monitored Presets	General Map	13	0	0	13	13
	siemens only	72	9	0	0	72
	192.168.0 subnet	9	9	0	0	9

Callouts in the image point to:

- Critical anomalies you should investigate:** Points to the '72' anomaly count for 'siemens only' in the 'Monitored Presets' section.
- Anomaly count per baseline:** Points to the '13' anomaly count for 'General Map' in the 'Monitored Presets' section.
- Set several baselines per preset:** Points to the 'Production phase' and 'Maintenance Phase' options for the 'General Map' preset.

New in 3.1: View new and changed items

Center GUI – Monitor – Map

The screenshot shows a network map view with the following details:

- LEGEND:** New (red line), Changed (dashed red line), Unchanged (grey line).
- Active criteria:** 7 new components, 6 new activities.
- ACTIVITY TAGS:** Protocol (ARP, IGMP, IPv6, NetBios, SMB), Network analysis (Broadcast, Insecure, Low-Vol), IT behavior (Host Config, Ping).
- Map View:** Shows various network components like 'Manuf - EngineeringManuf - Scada & IMI', 'Gas Compression', 'Energy Management', 'IT Machines - To Investigate', and 'Emerson Process'.

Callouts in the image point to:

- Anomalies that have been detected:** Points to the '7 new components' and '6 new activities' notification.
- Tags defining the traffic being monitored:** Points to the 'ACTIVITY TAGS' section.
- Map view of new or modified assets:** Points to the network map area.

New in 3.1: Detailed list of new and modified assets

Center GUI – Monitor – Component List

98 Components
7 new

STATUS	Component	Group	First activity	Last activity
NEW	192.168.69.28	-	Apr 14, 2020 9:43:37 PM	Apr 22, 2020 2:13:22 PM
NEW	Cisco 192.168.70.100	-	Apr 15, 2020 5:38:21 AM	Apr 22, 2020 2:13:22 PM
NEW	208.67.222.222	-	Apr 14, 2020 9:43:27 PM	Apr 22, 2020 2:13:22 PM
NEW	192.168.100.2	-	Apr 14, 2020 9:43:37 PM	Apr 22, 2020 2:13:22 PM
NEW	208.67.220.220	-	Apr 14, 2020 9:43:32 PM	Apr 22, 2020 2:13:22 PM
NEW	Vmware 192.168.72.176	-	Apr 14, 2020 9:43:27 PM	Apr 22, 2020 2:13:22 PM
NEW	Vmware 192.168.70.1	-	Apr 15, 2020 5:38:21 AM	Apr 22, 2020 2:13:22 PM
-	FDAIRA-M-VBLV	-	Apr 14, 2020 9:43:37 PM	Apr 16, 2020 8:07:09 PM
-	Profinet DCP Multicast 0.0.0	Siemens IO from my Auto Robot	Oct 11, 2019 9:24:08 AM	Apr 14, 2020 3:29:55 PM
-	Sew 0id:c1	QA	Oct 11, 2019 11:00:12 AM	Apr 14, 2020 3:29:55 PM

New in 3.1: Detailed list of new and modified activities

Center GUI – Monitor – Activity List

170 Activities
6 new

STATUS	Component	Component	First activity	Last activity
NEW	Vmware 192.168.72.176	192.168.69.28	Apr 14, 2020 9:43:37 PM	Apr 22, 2020 2:13:23 PM
NEW	Vmware 192.168.72.176	208.67.220.220	Apr 14, 2020 9:43:32 PM	Apr 22, 2020 2:13:23 PM
NEW	Vmware 192.168.72.176	FDAIRA-M-VBLV	Apr 14, 2020 9:43:52 PM	Apr 22, 2020 2:13:23 PM
NEW	Vmware 192.168.72.176	208.67.222.222	Apr 14, 2020 9:43:27 PM	Apr 22, 2020 2:13:23 PM
NEW	Vmware 192.168.72.176	192.168.100.2	Apr 14, 2020 9:43:37 PM	Apr 22, 2020 2:13:23 PM
NEW	Vmware 192.168.70.1	Cisco 192.168.70.100	Apr 15, 2020 5:38:21 AM	Apr 22, 2020 2:13:23 PM
-	1756-ENBT/A	STATION-ROCKWEL	Oct 11, 2019 11:12:58 AM	Apr 14, 2020 3:29:55 PM
-	Fisher 10.4.0.14	OWS1	Oct 11, 2019 11:03:46 AM	Apr 14, 2020 3:29:55 PM
-	Yokogawa 192.168.1.128	239.192.24.4	Oct 11, 2019 11:06:52 AM	Apr 14, 2020 3:29:55 PM
-	Yokogawa 192.168.1.2	239.192.24.0	Oct 11, 2019 11:06:52 AM	Apr 14, 2020 3:29:55 PM
-	Yokogawa 192.168.1.2	224.0.0.2	Oct 11, 2019 11:07:54 AM	Apr 14, 2020 3:29:55 PM

investigate baseline changes

Center GUI – Monitor – Investigate Changes - Flows

Detailed history of application flows

Understand the new activity thanks to Tags

List of variables being accessed

Include new activity in what is "normal"

Access full technical sheet with all details

Component	Port	Direction	Component	Port	Protocol	First activity	Last activity	Tags	Packets
Siemens 192.168.0.0	-	-	Siemens 192.168.0.1	-	-	Oct 11, 2019 9:24:08 AM	Apr 22, 2020 2:13:22 PM	ARP	4
Siemens 192.168.0.0	1025	→	Siemens 192.168.0.1	102	TCP	Oct 11, 2019 9:24:08 AM	Apr 22, 2020 2:13:22 PM	Read Var., S7	134
SENTRYO-XP-1	137	-	192.168.0.255	137	UDP	Oct 11, 2019 9:24:08 AM	Apr 22, 2020 2:13:22 PM	Broadcast., Netbios	20
SENTRYO-XP-1	138	-	192.168.0.255	138	UDP	Oct 11, 2019 9:24:08 AM	Apr 22, 2020 2:13:22 PM	Insecure., Broadcast., Low Volume., Netbios., SMB	1
Siemens 192.168.0.1	-	-	SENTRYO-XP-1	-	-	Oct 11, 2019 10:03:46 AM	Apr 22, 2020 2:13:22 PM	ARP	1
Siemens 192.168.0.1	-	-	SENTRYO-XP-1	-	ICMPv4	Oct 11, 2019 10:03:46 AM	Apr 22, 2020 2:13:22 PM	Ping	4
SENTRYO-XP-1	1002	→	Siemens 192.168.0.1	102	TCP	Oct 11, 2019 10:03:46 AM	Apr 22, 2020 2:13:22 PM	Read Var., Write Var., S7	614
SENTRYO-XP-1	-	-	255.255.255.255	-	-	Oct 11, 2019 10:03:46 AM	Apr 22, 2020 2:13:22 PM	Broadcast., ARP	4

Center GUI – Monitor – Investigate Changes - Variables

Detailed history of variable access

Understand the new activity thanks to Tags

List of variables being accessed

Include new activity in what is "normal"

Access full technical sheet with all details

Status	Variable	Type	Accessed by	Protocol	Details	First access	Last access
NEW	Q2.0	WRITE	SENTRYO-XP-1	s7	Q0	Aug 30, 1754 10:53:02 PM	Aug 30, 1754 10:53:02 PM
NEW	M2.0	WRITE	SENTRYO-XP-1	s7	M0	Aug 30, 1754 10:53:02 PM	Aug 30, 1754 10:53:02 PM
NEW	Q2.0	READ	SENTRYO-XP-1	s7	Q0	Aug 30, 1754 10:53:02 PM	Aug 30, 1754 10:53:02 PM
NEW	M2.0	READ	SENTRYO-XP-1	s7	M0	Aug 30, 1754 10:53:02 PM	Aug 30, 1754 10:53:02 PM
NEW	Q2.1	WRITE	SENTRYO-XP-1	s7	Q0	Oct 11, 2019 10:03:46 AM	Apr 22, 2020 2:13:23 PM
NEW	Q2.1	READ	SENTRYO-XP-1	s7	Q0	Aug 30, 1754 10:53:02 PM	Aug 30, 1754 10:53:02 PM
NEW	MW6	READ	SENTRYO-XP-1	s7	M0	Oct 11, 2019 10:03:46 AM	Apr 22, 2020 2:13:23 PM
NEW	M8.0	READ	SENTRYO-XP-1	s7	M0	Oct 11, 2019 10:03:46 AM	Apr 22, 2020 2:13:23 PM
NEW	M8.1	READ	SENTRYO-XP-1	s7	M0	Oct 11, 2019 10:03:46 AM	Apr 22, 2020 2:13:23 PM
NEW	M8.2	READ	SENTRYO-XP-1	s7	M0	Oct 11, 2019 10:03:46 AM	Apr 22, 2020 2:13:23 PM
NEW	M8.3	READ	SENTRYO-XP-1	s7	M0	Oct 11, 2019 10:03:46 AM	Apr 22, 2020 2:13:23 PM
NEW	M8.4	READ	SENTRYO-XP-1	s7	M0	Oct 11, 2019 10:03:46 AM	Apr 22, 2020 2:13:23 PM
NEW	M8.5	READ	SENTRYO-XP-1	s7	M0	Oct 11, 2019 10:03:46 AM	Apr 22, 2020 2:13:23 PM

New monitoring/baseline UX/UI

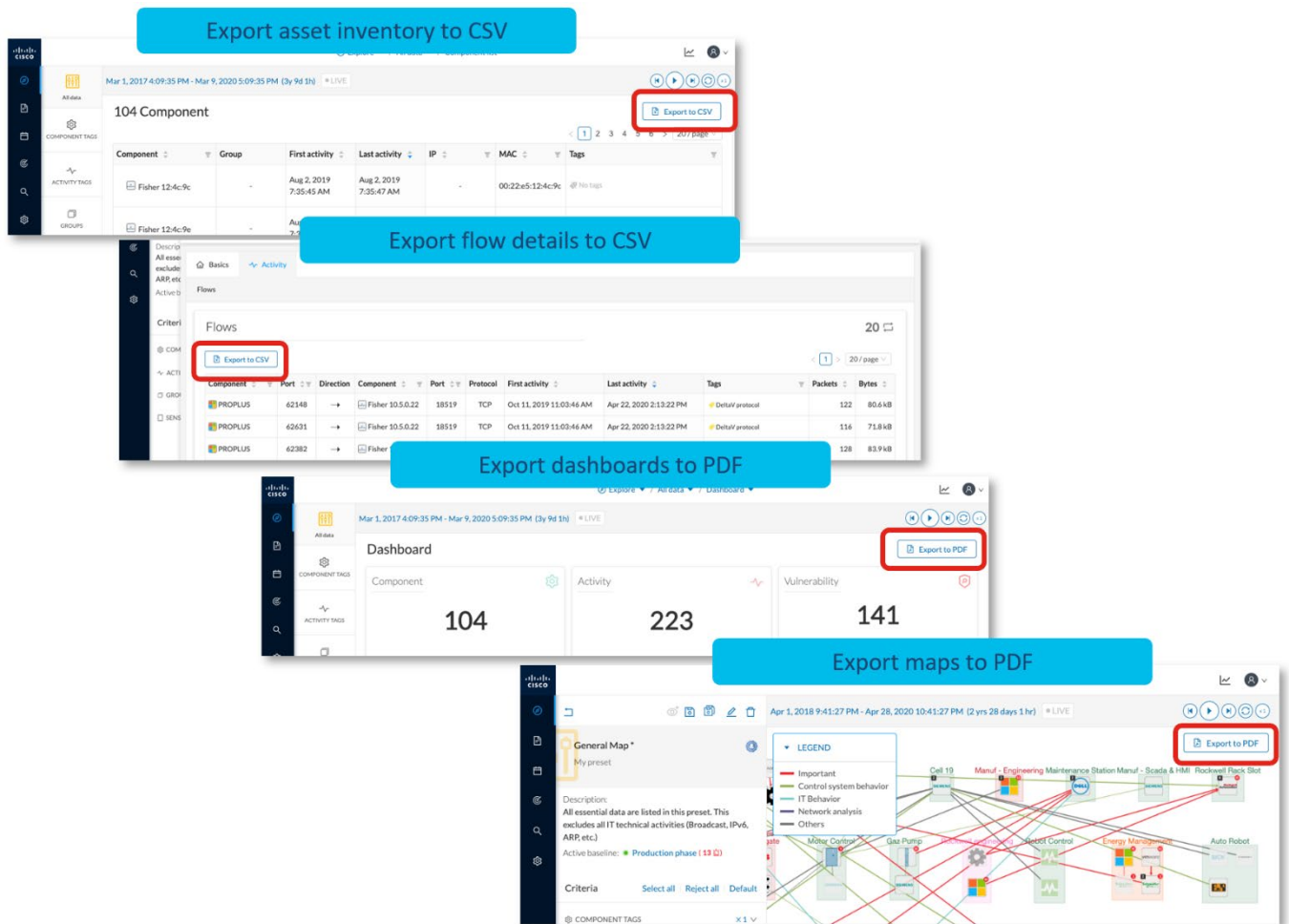
New extension capabilities

Extensions are optional add-ons to Cisco Cyber Vision Center which provide more features, such as the management of new device types, additional detection engines, or integrations with external services. It's an enhanced architecture to easily add new feature packages. Starting with Cisco Cyber Vision 3.1.0, the first extension available is the IOx Sensor management extension, which enables simplified deployment of the Sensor application on supported platforms.

PDF and CSV export across the platform

Several buttons are now available in the GUI to download list or map as csv and pdf files.

Center GUI – Explore – New Export buttons



Platform admin enhancements

Several administration enhancements come with the release 3.1 of Cisco Cyber Vision:

- French & German user interface

In addition to English, the GUI is now available in French and German.

- User security settings


From a new administration page, Cisco Cyber Vision user passwords security settings can be changed: the lifetime, the numbers of authorized failed login attempt and the number of days before a password can be reused.

Miscellaneous

DNS default server change

Before version 3.1.0, Cisco Cyber Vision (Center and sensors) was using the Google DNS servers as default DNS server. Now Cisco Cyber Vision uses Umbrella service as default DNS Server.

Cisco Cyber Vision issues fixed

Issues ID / CDETS	Description
3532 / CSCvs44270	In release 3.0.x, Cisco Cyber Vision monitoring feature is detecting changes globally rather than locally. In version 3.1.0, Baselines are based on Presets to filter the dataset.
1130 /	In version 3.1.0, the size of the capture file generated in the sensor with the command <code>flowctl start-recording</code> is limited to 50 MB.
1428 /	In version 3.1.0, statistics of the offline sensor mode have been enhanced for diagnostics purpose.
1431 /	<p>The name of the sensor is now used in the system statistics page, where before it was the hardware serial number:</p> 
3538 / CSCvs87918 3670 / CSCvu07872	In version 3.1.0, DPI of grid protocols was improved, several issues reported were de facto fixed. For example, in version 3.0.x, no GOOSE flows were tagged as GOOSE and no GOSSE variables could be seen. In version 3.1.0 both issues are now fixed.
3537 / CSCvs70058	In version 3.0.x, Cisco Cyber Vision failed to report flows with content statistics for IEC104 Read operation. DPI of grid protocols has been improved for version 3.1.0, and IEC104 is now decoded correctly.
4022-2647 / CSCvs43173	In release 3.0.x, Cisco Cyber Vision wasn't reporting Unsolicited Reporting operations with DNP3 and T104 systems. This issue is fixed in version 3.1.0.
4022-2801 / CSCvu07855	In release 3.0.x, Cisco Cyber Vision failed to tag and classify Write operations with IEC104 protocol, which is now fixed in the new release.

Issues ID / CDETS	Description
3530 / CSCvs44038	In release 3.0.x, the Center wasn't classifying Rockwell controller with a tag "Controller". In version 3.1.0, new properties coming from the DPI are used to tag the processor as controller.
3544 / CSCvt39890	Grammatical errors on the Monitor mode page are now fixed.
3519 / CSCvt33027	In version Sensor 3.0.x, the sensor was demonstrating poor performances with SQL and CIP-Ethernet/IP traffic was seen. Version 3.1.0 brings several improvements which fixed these issues.
- / CSCvt52568	Keyence Devices showed with Mitsubishi Icon in Cisco Cyber Vision 3.0.x. The latest KnowledgeDB delivered with the version 3.1.0 fixed this issue.
3545 / CSCvt39922	In version 3.0.1, the system statistics page link redirected to the home page dashboard. The root cause has been identified and fixed in version 3.1.0.
3530 / CSCvt80075	Cisco Cyber Vision is not classifying all models of Rockwell PLCs as controllers. In version 3.1.0, new properties coming from the DPI are used to tag processors as controllers.
- / CSCvu22193	Remarks were done during the test phase of version 3.1.0 around sensors provisioning. It is mandatory to use the right provisioning package filename with .zip extension in the path field of the Local Manager for the provisioning of sensors embedded in IR1101, IE3400, and Catalyst 9k. A note was added in the user manual to avoid mistakes.
3155 / CSCvs59015	In version 3.0.1, the IC3000 sensor stopped sending data as 12k pps input threshold was exceeded. This issue is now fixed in version 3.1.0. However, this doesn't mean that all packets above 12k pps will be decoded by the sensor. It means that even if the sensor can't decode everything, it will remain functional and drop extra packets, which is reported in the statistics page of the application.
2861/ CSCvt00131	Fixed: Cisco Cyber Vision was sending multiple components to ISE for the same MAC address.
2862/ CSCvt00490	Fixed: Cisco Cyber Vision Center was not sending custom attributes for OT components using pxGrid to ISE.
2863/ CSCvs72464	Fixed: Cisco Cyber Vision Center was not sending all device attributes information using pxGrid to ISE.

Issues ID / CDETS	Description
1584 /	Fixed: a sensor filter could be set with more than 939 characters.
2486 /	Fixed: Unestablished tag setting was not stable.
2492 /	Fixed: Missing Windows flag on some Windows components.
2925 /	Fixed: events – some vulnerabilities fields were empty.
2928 /	Fixed: GUI - Data management - Clear Data Icon remains now in green when data was cleared.
2994 /	Fixed: some duplication of components could be shown.
3116 /	Fixed: GUI - Live Data Custom period popup - The focus was automatically added on the input text.
3125 /	Fixed: Vulnerabilities Links are not valid on Security tab of a component.
3185 /	Fixed: in the Search Page - Right Component and activity panel could appear when the search page was used.
3497 /	Fixed: Inverted normalized property in the Rockwell 1756 components.
3500 /	Fixed: Problems displaying Bytes in Rockwell Ethernet/IP Flows.
3502 /	Fixed: Missing the "Engineering Station" Tag on some engineering Station components.
3702 /	Fixed: The Cisco Cyber Vision Center displays an improper sensor IP address when enrolling an IR1101 sensor.
3726 /	Fixed: DNS Server tag is set even without DNS answer.

Cisco Cyber open CDETS and known issues

Issues ID / CDETS	Component	Description
CSCvs47260 CSCvs47253	IC3000 Sensor integration	<ul style="list-style-type: none">The password configuration required when generating a provisioning package for the IC3000 is sometimes not considered. Thus, login in IOx Local Manager to install the Sensor Application is refused and the procedure must be redone.Login to IOx Local Manager won't work unless the IC3000 is rebooted once.
#3542 / CSCvt18302	pxGrid-agent	pxGrid configuration fails when using white spaces in the Node Name field because this is not endured in ISE.
CSCvt55787	pxGrid-agent	The Cisco Cyber Vision Center should not send broadcast address to ISE as an endpoint using pxGrid.