Release Notes for Cisco Cyber Vision Release 3.1.2

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, 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-3.1.2.ova	VMWare OVA file, for Center setup
CiscoCyberVision-3.1.2.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-sensor-management-3.1.2.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-3.1.2.tar	IE3400, IR1101 sensor installation and update file
CiscoCyberVision-IOx-IC3K-3.1.2.tar	IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-3.1.2.tar	Catalyst 9x00 sensor installation and update file
Updates	**Description**
CiscoCyberVision-update-center-3.1.2.dat	Center update file
CiscoCyberVision-update-sensor-3.1.2.dat	Sentryo Sensor3, 5, 7 update file
CiscoCyberVision-update-combined-3.1.2.dat	Center and Legacy Sensor update file from GUI
CiscoCyberVision-Embedded-KDB-3.1.2.dat	KnowledgeBase embedded in Cisco Cyber Vision 3.1.2

Related Documentation

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

New!

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 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 Network Sensor Installation Guide for Cisco 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_IE3400_and_Catalyst_9300_3_1_1.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 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

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

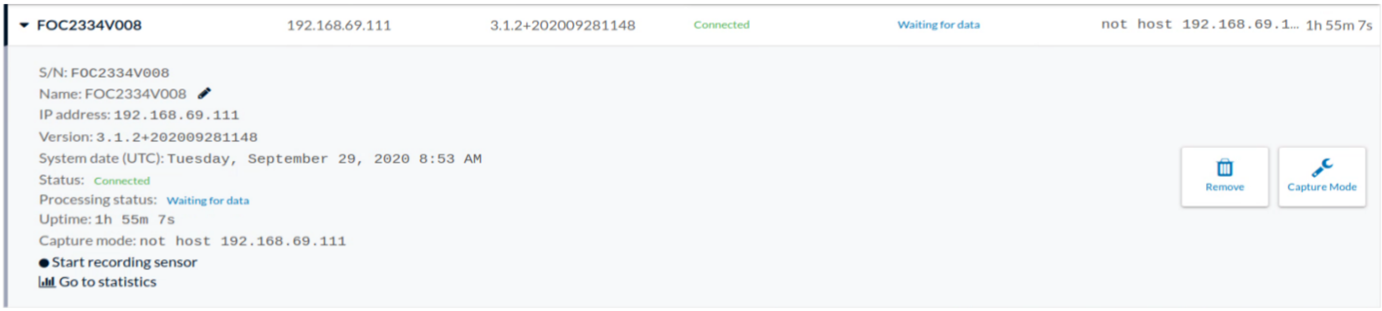
https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Integrating-Cisco-Cyber-Vision-with-Cisco-Identify-Services-Engine-via-pxGrid.pdf

Cisco Cyber Vision new features and improvements

IOx sensors on Catalyst IE3400, on Catalyst 9300, 9400 and on IR1101 improvements

All IOx Cisco Cyber Vision Sensors now support traffic filtering, to focus on relevant traffic and reduce the load on the Center. The Capture Mode button is now enabled for all sensors embedded in Catalyst IE3400, Catalyst 9300, 9400 and IR1101.

Capture Mode Button now enabled for IOx sensors:

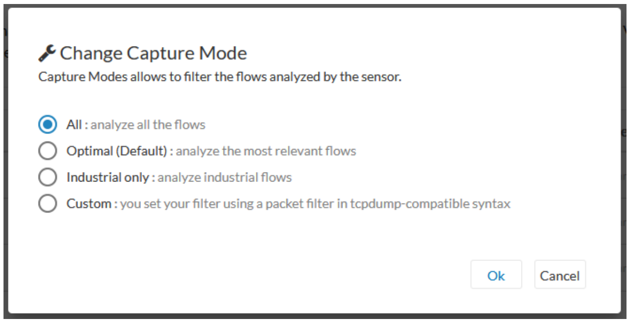


FOC2334V008	192.168.69.111	3.1.2+202009281148	Connected	Waiting for data	not host 192.168.69.1...	1h 55m 7s

S/N: FOC2334V008
Name: FOC2334V008
IP address: 192.168.69.111
Version: 3.1.2+202009281148
System date (UTC): Tuesday, September 29, 2020 8:53 AM
Status: Connected
Processing status: Waiting for data
Uptime: 1h 55m 7s
Capture mode: not host 192.168.69.111
● Start recording sensor
Go to statistics

The Capture Mode button will allow the user to choose how the flows are filtered by the sensor.

List of Capture Modes:



Change Capture Mode

Capture Modes allows to filter the flows analyzed by the sensor.

◉ **All** : analyze all the flows
○ **Optimal (Default)** : analyze the most relevant flows
○ **Industrial only** : analyze industrial flows
○ **Custom** : you set your filter using a packet filter in tcpdump-compatible syntax

Cisco Cyber Vision Sensors will analyze incoming traffic based on the Capture Mode set.

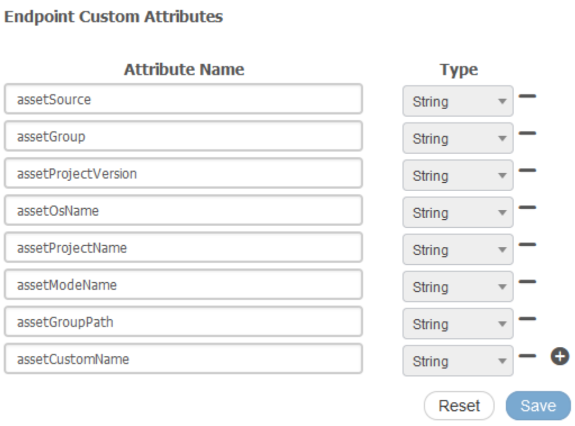
The different Capture Modes are:

- ALL: No filter is applied. The sensor analyzes all incoming flows, and they will be all stored inside the Center database.
- OPTIMAL (Default): The applied filter selects the most relevant flows according to Cisco expertise. Multicast flows are not recorded. This capture mode is recommended for long term capture and monitoring.
- INDUSTRIAL ONLY: The filter selects industrial protocols only like modbus, S7, EtherNet/IP, etc. This means that IT flows of the monitored network won't be analyzed by the sensor and won't appear in the GUI.
- CUSTOM (advanced users): Use this capture mode to fully customize the filter to be applied. To do so, you must use the tcpdump syntax to define the filtering rules. Tcpdump syntax help is available on https://www.tcpdump.org/manpages/pcap-filter.7.html.

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
assetSource	String
assetGroup	String
assetProjectVersion	String
assetOsName	String
assetProjectName	String
assetModeName	String
assetGroupPath	String
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

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

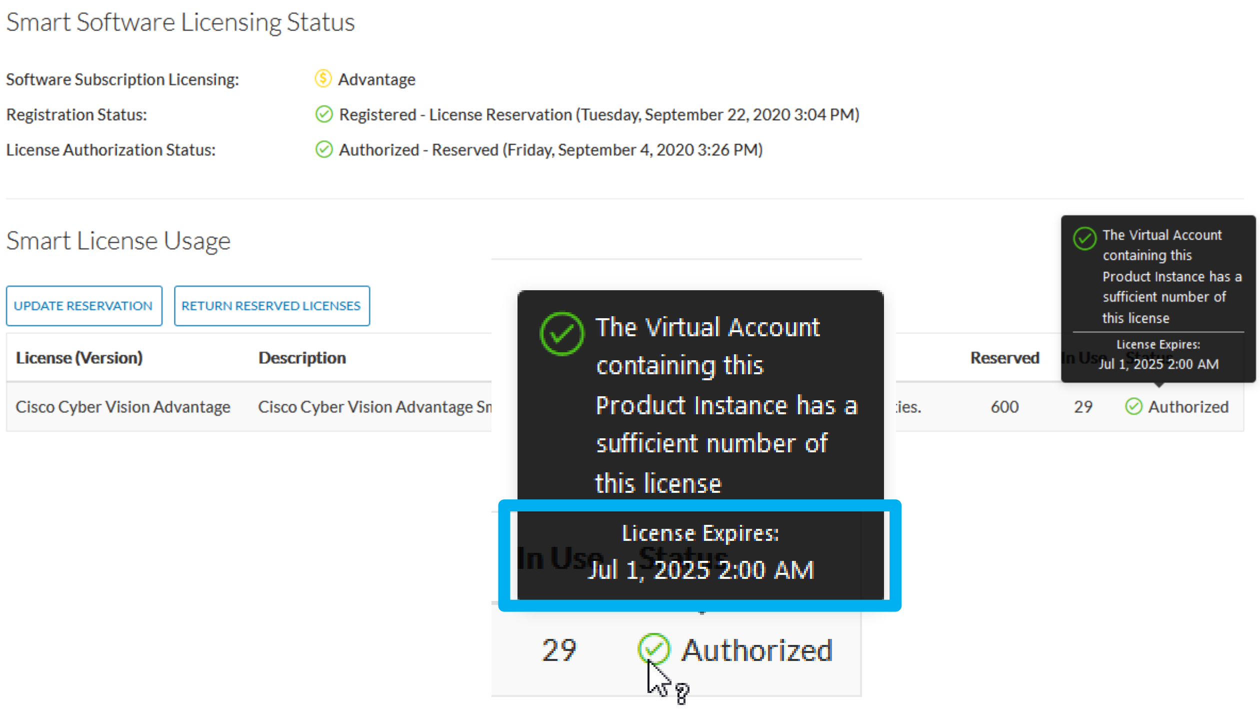
Group path is already added but will be available as of release 3.2, as it will give the folder hierarchy which is a 3.2

new functionality.

Smart licensing – add term end date

When the user clicks on the license status in the dedicated admin page of the Center, the term and date is displayed in the application.

License status



Smart Software Licensing Status

Software Subscription Licensing: Advantage

Registration Status: Registered - License Reservation (Tuesday, September 22, 2020 3:04 PM)

License Authorization Status: Authorized - Reserved (Friday, September 4, 2020 3:26 PM)

Smart License Usage

License (Version)	Description	Reserved	In Use	Status
Cisco Cyber Vision Advantage	Cisco Cyber Vision Advantage Sn ... ies.	600	29	Authorized

The Virtual Account containing this Product Instance has a sufficient number of this license

License Expires: Jul 1, 2025 2:00 AM

Cisco Cyber Vision Center Diagnostic improvements

Center diagnostic was improved, with 2 guidelines:

- A default version which must take less space
- More human readable information

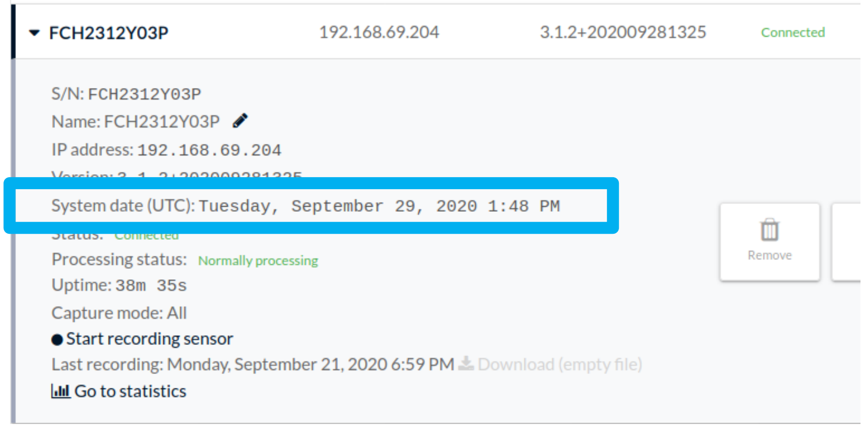
Several changes were done:

- extract human-readable info from the Center and sensor rrd files and move the rrd files to the full diagnostic
- limit the number of files per sensor in the regular diagnostic
- generate tags statistics
- generate events statistics
- limit the scope of large SQL requests to a reasonable period
- remove duplicate requests and improve some SQL requests
- Add sensor extension application logs

Add sensor date and time in sensor admin page and sensor statistics page

Sensor date and time was added in the application on 2 pages (sensor administration page and sensor statistics page). This information will allow the user to avoid time issues regarding flows appearing in the past or in the future.

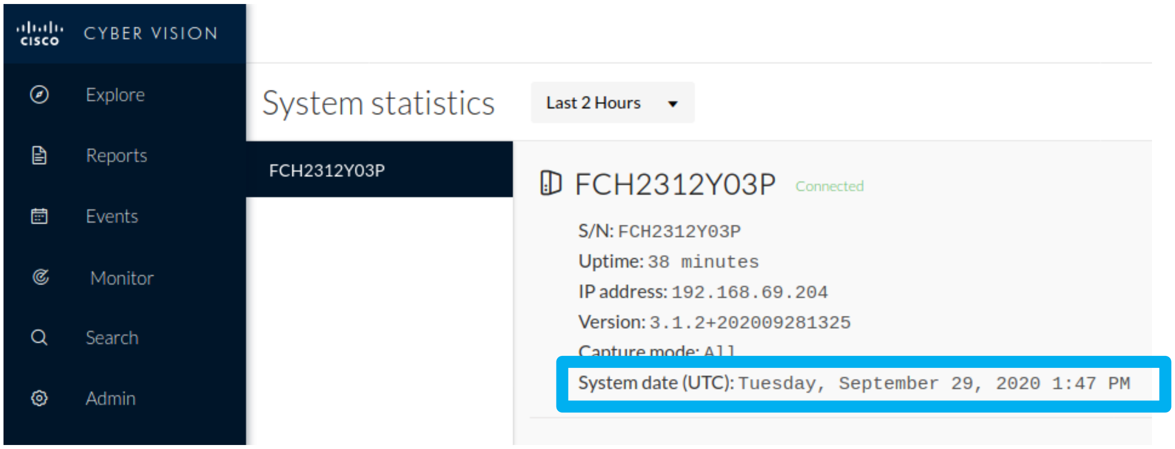
Sensor administration page



FCH2312Y03P 192.168.69.204 3.1.2+202009281325 Connected

S/N: FCH2312Y03P
Name: FCH2312Y03P
IP address: 192.168.69.204
Version: 3.1.2+202009281325
System date (UTC): Tuesday, September 29, 2020 1:48 PM
Status: Connected
Processing status: Normally processing
Uptime: 38m 35s
Capture mode: All
● Start recording sensor
Last recording: Monday, September 21, 2020 6:59 PM Download (empty file)
Go to statistics

Sensor statistics page



System statistics Last 2 Hours

FCH2312Y03P

FCH2312Y03P Connected

S/N: FCH2312Y03P
Uptime: 38 minutes
IP address: 192.168.69.204
Version: 3.1.2+202009281325
Capture mode: All
System date (UTC): Tuesday, September 29, 2020 1:47 PM

Improve some syslog events with the addition of the Sensor ID (phase 2)

Events related to flow like new flow, new component, new properties, etc. are now sent to syslog with a new field called “SCVSensorId”.

Example of a new communication event:

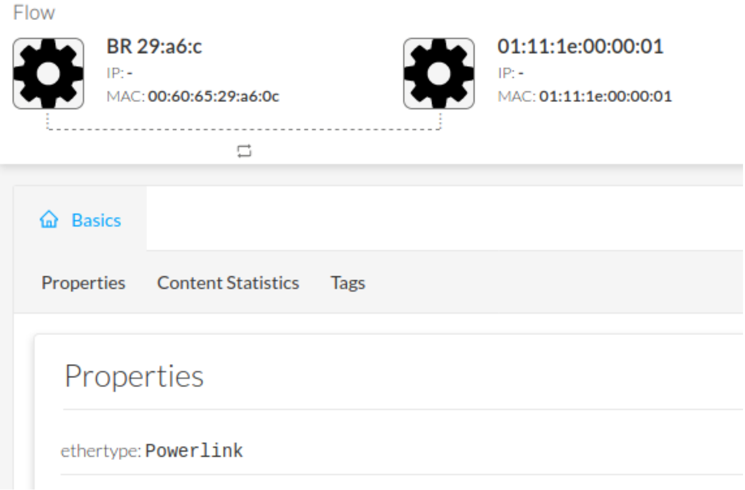
Message: CEF:0|sentryo|cybervision|1.0|communication_new|New communication|0|cat=Security Events msg=New REMOTE_ADMIN communication has been detected between 10.10.20.11:1888 and 10.10.20.8:3389 cmp-a-mac=f8:db:88:5a:c0:b3 cmp-b-mac=f8:db:88:91:43:de cmp-a=10.10.20.11 cmp-b=10.10.20.8 cmp-a-port=1888 cmp-b-port=3389 SCVEventType=flow_new SCVFlowCmpAComponentId=bdf00b4b-1676-525e-8144-f8bce9a6794b SCVFlowCmpAComponentName= SCVFlowCmpBComponentId=75551c22-4a54-5548-96e6-0db38428553b SCVFlowCmpBComponentName= SCVFlowCommunicationType=REMOTE_ADMIN SCVFlowId=3bfb9262-8401-5edd-b552-e2eff21898fc SCVSensorId=40cf0a62-7245-4b12-8256-2215cfac4a94

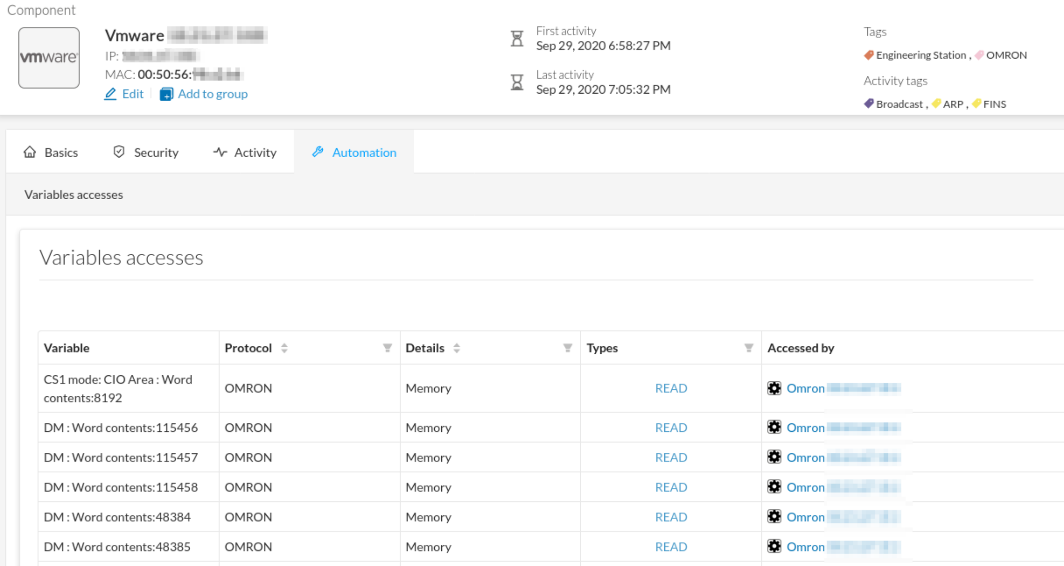
Example of a new tag event:

Message: CEF:0|sentryo|cybervision|1.0|analyzer_tag_assign|Tag assigned on flow or component|0|cat=Inventory Events msg=New tag REMOTE_ADMIN_SERVER automatically assigned to component. cmp-a-mac=f8:db:88:5a:c0:b3 cmp-b-mac=f8:db:88:91:43:de cmp-a=10.10.20.11 cmp-b=10.10.20.8 cmp-a-port=1888 cmp-b-port=3389 SCVEventType=new_tag SCVComponentId=75551c22-4a54-5548-96e6-0db38428553b SCVComponentName=ENG_WORKSTATION SCVFlowCmpAComponentId=bdf00b4b-1676-525e-8144-f8bce9a6794b SCVFlowCmpAComponentName= SCVFlowCmpBComponentId=75551c22-4a54-5548-96e6-0db38428553b SCVFlowCmpBComponentName= SCVFlowId=3bfb9262-8401-5edd-b552-e2eff21898fc SCVSensorId=40cf0a62-7245-4b12-8256-2215cfac4a94 SCVTagName=REMOTE_ADMIN_SERVER SCVTagValue=info

This information cannot be sent for all component-related event. Only activities and flow-related events can have this information on the current release.

Cisco Cyber Vision Bug fixed

Issues ID / CDETS	Description
#4184 /	Fix SNORT on Cyber Vision Sensor running on IC3000 not working unless sensor rebooting.
#5116 /	Fix SQL injection in /scv/3.0/baseline/[baseline_id] /component/[component_id] /activities endpoint.
#4388 /	Fix Powerlink decode failure on Powerlink Ethertype.  Flow Basics Properties Content Statistics Tags Properties BR 29:a6:c IP: - MAC: 00:60:65:29:a6:0c 01:11:1e:00:00:01 IP: - MAC: 01:11:1e:00:00:01 ethertype: Powerlink
#5064 /	sbs-diag – Fix errors with –o option.
#4431 /	sbs-diag – Warn user while using a bad option.
#5144 /	Enforce extensions file permissions.
#5029 /	Enforce bruteforce login mitigation.
#4168 /	Enforce admin.security.passphraseMinLength parameter checking.
#4814 / CSCvu88825	Fix welcome page event statistic (donut) calculation.
#5148 / CSCvv20283	Fix decode failure on Ethernet Type 40093 (Ox9C9D).

<table>
<tr><th>Issues ID / CDETS</th><th>Description</th></tr>
<tr><td><b>#5399 / CSCvv49658</b></td><td>OMRON Fix missing read variable.

Component
Vmware [redacted]
IP: [redacted]
MAC: 00:50:56:[redacted]
Edit | Add to group
First activity Sep 29, 2020 6:58:27 PM
Last activity Sep 29, 2020 7:05:32 PM
Tags: Engineering Station , OMRON
Activity tags: Broadcast , ARP , FINS
Basics | Security | Activity | Automation
Variables accesses
Variables accesses
<table>
<tr><th>Variable</th><th>Protocol</th><th>Details</th><th>Types</th><th>Accessed by</th></tr>
<tr><td>CS1 mode: CIO Area : Word contents:8192</td><td>OMRON</td><td>Memory</td><td>READ</td><td>Omron [redacted]</td></tr>
<tr><td>DM : Word contents:115456</td><td>OMRON</td><td>Memory</td><td>READ</td><td>Omron [redacted]</td></tr>
<tr><td>DM : Word contents:115457</td><td>OMRON</td><td>Memory</td><td>READ</td><td>Omron [redacted]</td></tr>
<tr><td>DM : Word contents:115458</td><td>OMRON</td><td>Memory</td><td>READ</td><td>Omron [redacted]</td></tr>
<tr><td>DM : Word contents:48384</td><td>OMRON</td><td>Memory</td><td>READ</td><td>Omron [redacted]</td></tr>
<tr><td>DM : Word contents:48385</td><td>OMRON</td><td>Memory</td><td>READ</td><td>Omron [redacted]</td></tr>
</table></td></tr>
<tr><td><b>#5043 /</b></td><td>BACNET – Fix incorrect activity tag “Variable Force” added on read variable flow.</td></tr>
<tr><td><b>#5075 / CSCvv12058</b></td><td>Fix sensor extension installation error with IR1101 with Firmware version 17.3.</td></tr>
<tr><td><b>#4399 / CSCvu42090</b></td><td>Fix VLAN ID lost on IOx sensor using ERSPAN. Now the VLAN ID of the original traffic is displayed in the application.</td></tr>
<tr><td><b>#3929 / CSCvt55787</b></td><td>Fix Cisco Cyber Vision Center should not send broadcast address to Cisco ISE as an endpoint using pxGrid.</td></tr>
<tr><td><b>#4397 / CSCvu47880</b></td><td>Fix Cisco Cyber Vision update does not remove Attribute from an endpoint in Cisco ISE through pxGrid (i.e. an empty group is not sent when a component is removed of a group in Cyber Vision).</td></tr>
<tr><td><b>#4822 / CSCvu58108</b></td><td>Cisco Cyber Vision updates not seen in Cisco ISE after PSN (Policy Service Node) reboot breaks pxGrid connection</td></tr>
<tr><td><b>#5401 /</b></td><td>Cisco ISE 2.7 SP2 – Fix Cisco Cyber Vision which didn’t recognized certificate generated from ISE 2.7 SP2.</td></tr>
<tr><td><b>#5108 /</b></td><td>Fix SENSOR3/5 bridge function.</td></tr>
<tr><td><b>#4206 /</b></td><td>Fix Monitor mode – Display refresh button when there are no data.</td></tr>
<tr><td><b>#5181 /</b></td><td>Reduce IOx sensors mandatory minimum size from 2GB to 1GB (1024Mb) to support Polaris 17.5.1 with IE3400 SD card partitioning reducing space for IOx applications.</td></tr>
</table>

#4237 /	Fix packet deduplication when ERSPAN decapsulation is active on IOx sensors.
#1792 /	Fix rich event component icon not displayed.

Issues ID / CDETS	Description
#5361 /	Fix typo on sensor administration page.
#5321 / CSCvt81711	Fix generateSensorP12() vulnerable to limited directory traversal.
#4714 /	Fix statistics page logout crash.
#4853 /	Fix sensor statistics page crash.
#4212 /	Fix Display tag less filters in baseline panel.
#5491 /	DNP3 fix panic in Cisco Cyber Vision Sensor DPI module.
#4787 /	Fix sbs-sensor -list and sbs-sensor -h commands.
#5708 /	Cisco ISE and Cyber Vision integration – Fix certificate permissions on Cyber Vision side.
#3140 /	Fix number of vulnerabilities counter not updated in statistic list.
#4283 /	Fix sbs-db purge command.

Cisco Cyber open CDETS and known issues

Issues ID / CDETS	Component	Description
#3542 / CSCvt18302	pxGrid-agent	Cisco Cyber Vision pxGrid configuration fails when using white spaces in the Node Name field because this is not endured in Cisco ISE.
#4821 / CSCvu41812	pxGrid-agent	Cisco ISE pxGrid communication goes down after upgrade and needs to be started manually.
#4825 / CSCvu80175	pxGrid-agent	Cisco Cyber Vision pxGrid does not publish Stomp Updates unless reboot right after integration.
#4049 /	Sensor Umas DPI	Umas – Firmware version is not always decoded correctly.
#4914 / CSCvu91917	Sensor management extension	Sensor management extension – Improvement of error messages on failed deployment is needed.