Release Notes for Cisco Cyber Vision Release 3.2.1

Users upgrading to 3.2.0 or 3.2.1 from previous versions should read the upgrade procedures carefully.

Compatible device list 3
Links 4
Software Download 4
Related Documentation 5
Cisco Cyber Vision 3.2.0 and 3.2.1 update procedure 6
Center updates 6
Sensor updates – IC3000 Sensor and Sentryo SENSOR3/5/7 cases 6
Sensor updates – Cisco IOx sensor cases 6
Cisco Cyber Vision 3.2.0 and 3.2.1 important changes 7
Communication port change 7
API authentication 7
Cisco Cyber Vision 3.2.1 important change 7
Center DPI Change 7
Cisco Cyber Vision new features and improvements 8
Licensing 8
General remarks about licensing 8
Compatibility with Smart Software Manager Satellite 9
MSLA - Managed Service License Agreement 13
New license type 15
Snort 17
rules 17
snort filters 18
DPI improvements 19

Center DPI interface management 21
Sensor Management Extension: new hardware supported 21
Global center: Synchronize custom presets 22
Global center: A Center can now be deployed and started before enrollment to its Global Center 23
SNMPv3 for sysinfo notifications 23
Center conversion to a Center with data synchronization 25
Cisco Cyber Vision other enhancements 26
Cisco Cyber Vision bug fixed 28
Cisco Cyber open CDETS and known issues 31

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	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	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 and 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-3.2.1.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-with-DPI-3.2.1.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-center-3.2.1.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-sensor-management-3.2.1.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-3.2.1.tar	IE3x00, IR1101 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-3.2.1.tar	IE3x00 sensor installation and update file with the active discovery
CiscoCyberVision-IOx-IC3K-3.2.1.tar	IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-3.2.1.tar	Catalyst 9x00 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-86-64-3.2.1.tar	Catalyst 9x00 sensor installation and update file with Active Discovery
Updates	**Description**
CiscoCyberVision-sysupgrade-3.2.1	Center and Sensor update file for upgrade from release < 3.2 to release 3.2.x
CiscoCyberVision-sysupgrade-sensor-3.2.1	Sensor update file for embedded senor in IC3000 and Sentryo SENSOR3, 5 and 7
CiscoCyberVision-Embedded-KDB-3.2.1.dat	KnowledgeDB embedded in Cisco Cyber Vision 3.2.1
CiscoCyberVision-update-center-3.2.1.dat	Center update file for upgrade from release 3.2.0 to release 3.2.1
CiscoCyberVision-update-sensor-3.2.1.dat	Sentryo Sensor3, 5, 7 update file for upgrade from release 3.2.0 to release 3.2.1
CiscoCyberVision-update-combined-3.2.1.dat	Center and Legacy Sensor update file from GUI for upgrade from release 3.2.0 to release 3.2.1

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 and 3.2.1 update procedure

Cisco Cyber Vision 3.2.x includes many enhancements and improvements which require changes to the underlying architecture when upgrading from release 3.1.x to release 3.2.1. These changes will affect both Centers and sensors, excluding IOx sensors (which are embedded in Catalyst 9300, 9400 or 9500, 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.x with the usage of the right upgrade package called “CiscoCyberVision-sysupgrade-3.2.1”.

Older versions (3.0.x) need to be upgraded first to release 3.1.2, then to 3.2.1.

The upgrade from 3.1.x to 3.2.1 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-3.2.1`

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

All 3.1.x versions can be directly upgraded in release 3.2.x with the usage of the right upgrade package called “CiscoCyberVision-sysupgrade-sensor-3.2.1”, previous versions need to be first updated to 3.1.2.

The upgrade needs to be launched 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-3.2.1`

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 and 3.2.1 important changes

Communication port change

An important change was made on the communication between the 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 3.2.1 important change

Center DPI Change

The update from Cisco Cyber Vision release 3.2.0 to 3.2.1 will delete all center DPI already configured. Some configuration files were changed to ensure compatibility with future releases which prevents forward compatibility for this minor release. The Center DPI needs to be recreated in the release 3.2.1.

Cisco Cyber Vision new features and improvements

Licensing

General remarks about licensing

Before performing any actions to license Cisco Cyber Vision products, users are invited to check their Smart account portal and verify that the relevant Smart Licenses are available (type and quantities).

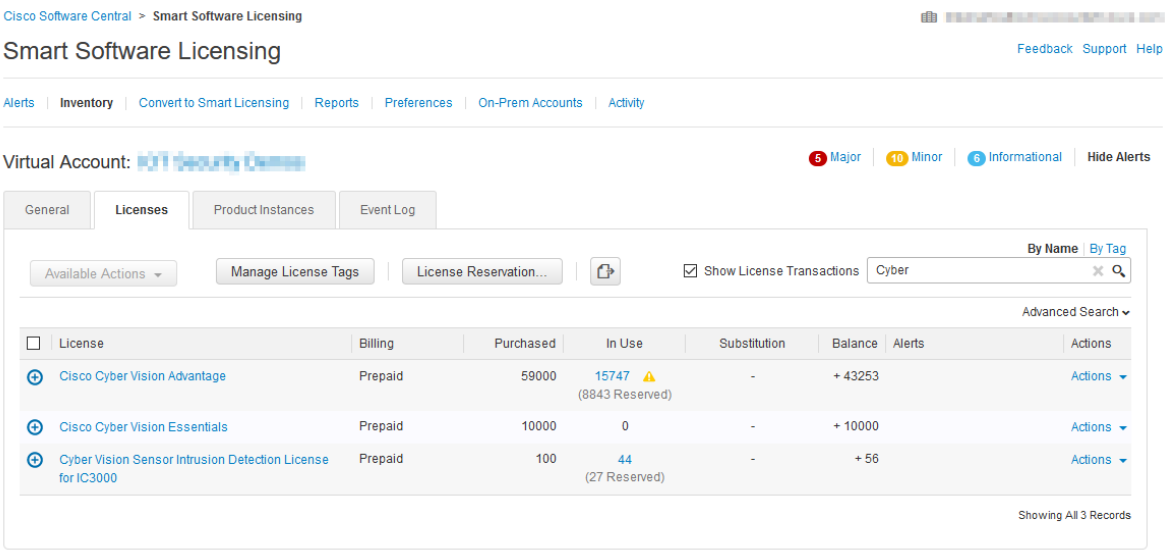
Smart Account: Central repository to view, store, and manage licenses across an entire organization. Software licenses, hardware, and subscriptions are accessible through a Smart Account. Smart Accounts are required to access and manage Smart License-enabled products.

Smart Licensing: Flexible software licensing capability that simplifies activating and managing licenses across an organization. The Smart Licensing capability makes it easier to procure, deploy, and manage Cisco on-prem software licenses. To use Smart Licensing, a Smart Account must first be set up.

For more information, navigate to: Cisco® Smart Licensing.

To check your Cisco Cyber Vision Licenses, access your Smart Account and navigate to Smart Software Licensing > Inventory > Licenses. Cisco Cyber Vision licenses must be available and appear in the Smart Software Licensing license list before proceeding with the registration of the product.

Cisco Cyber Vision Licenses

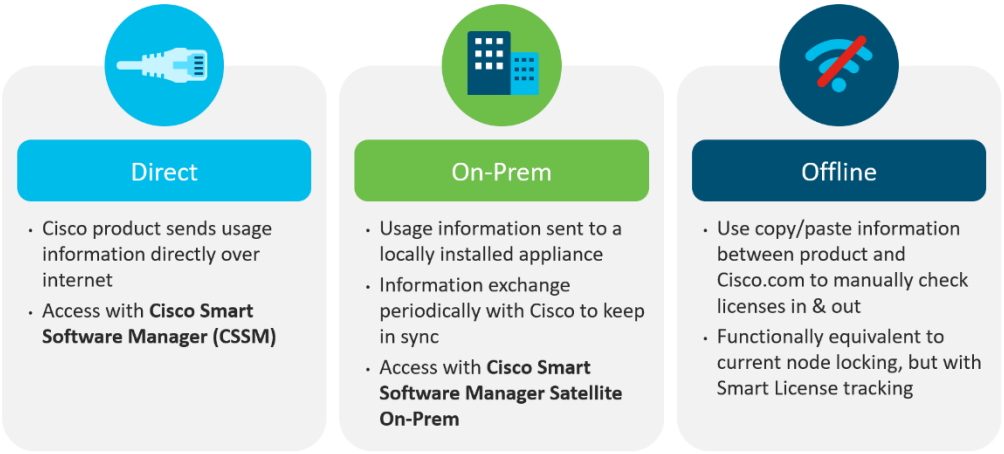


If you plan to use an offline license, you need to check that your Smart Account can perform a “License Reservation” (check from the License menu that the License reservation button is enabled). If your account doesn’t have the rights to do so, please open a case and provide a business justification.

Compatibility with Smart Software Manager Satellite

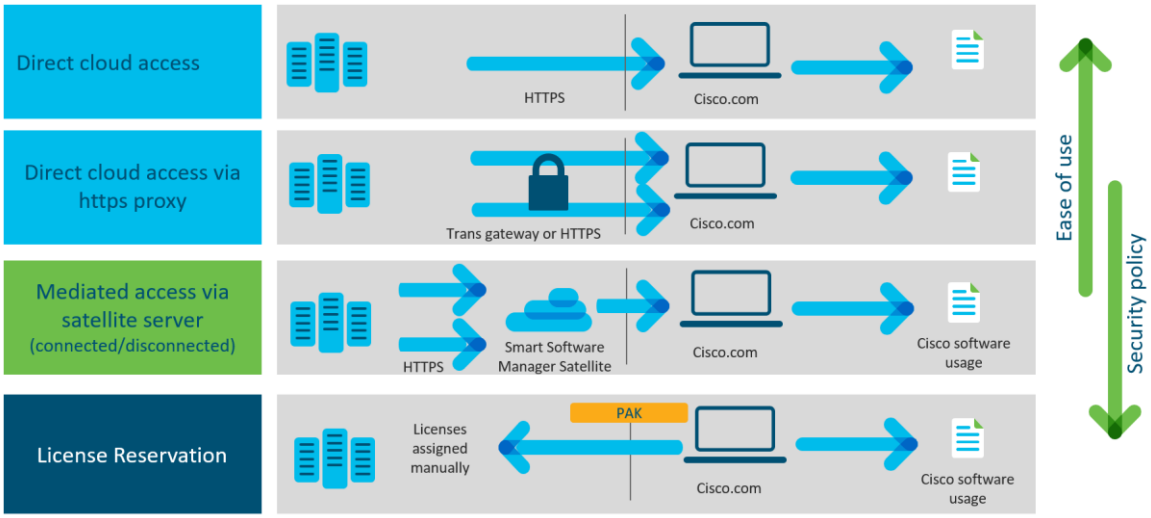
Cisco Cyber Vision Release 3.2.1 now supports the Smart Software Manager Satellite as license provider, and its different deployment options.

Cisco Cyber Vision deployment options



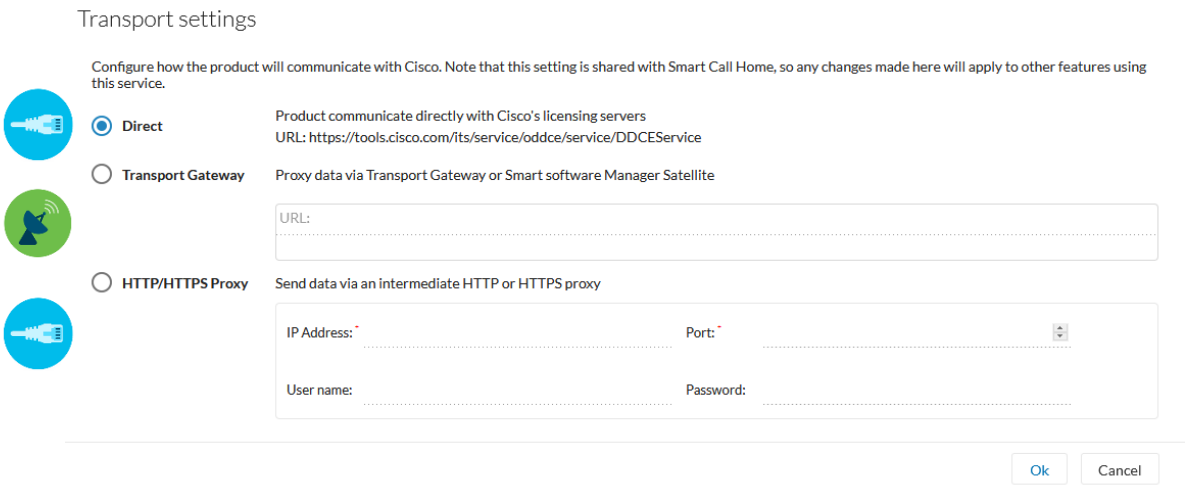
To register Cisco Cyber Vision licensed products, Smart Licensing has different modes depending on the level of security desired:

Cisco Cyber Vision Smart Licensing deployment modes



Cisco Cyber Vision release 3.2.1 can now use all deployment options and transport modes. In Cisco Cyber Vision, navigate to Administration > License > “edit the Smart Call Home Transport Settings” to configure transport settings.

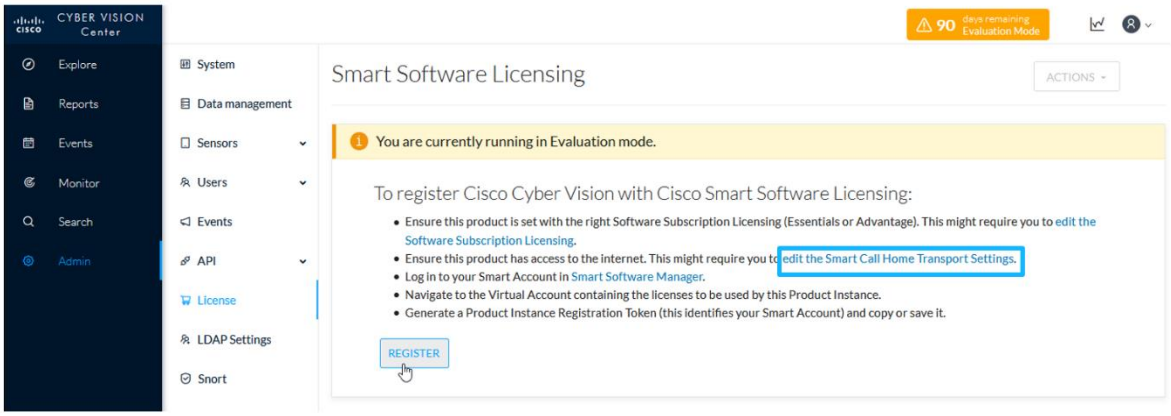
Cisco Cyber Vision Licensing transport settings



- Direct: a direct access to the cloud is enabled. A Product Instance Registration Token needs to be collected from the Smart Software Manager to complete registration.
- Transport gateway: an access to the Smart software Manager Satellite is enabled. A Product Instance Registration Token needs to be collected from the Smart Software Manager Satellite to complete registration.
- HTTP/HTTPS Proxy: a direct access to the cloud through a Proxy is enabled. A Product Instance Registration Token needs to be collected from the Smart Software Manager to complete registration.

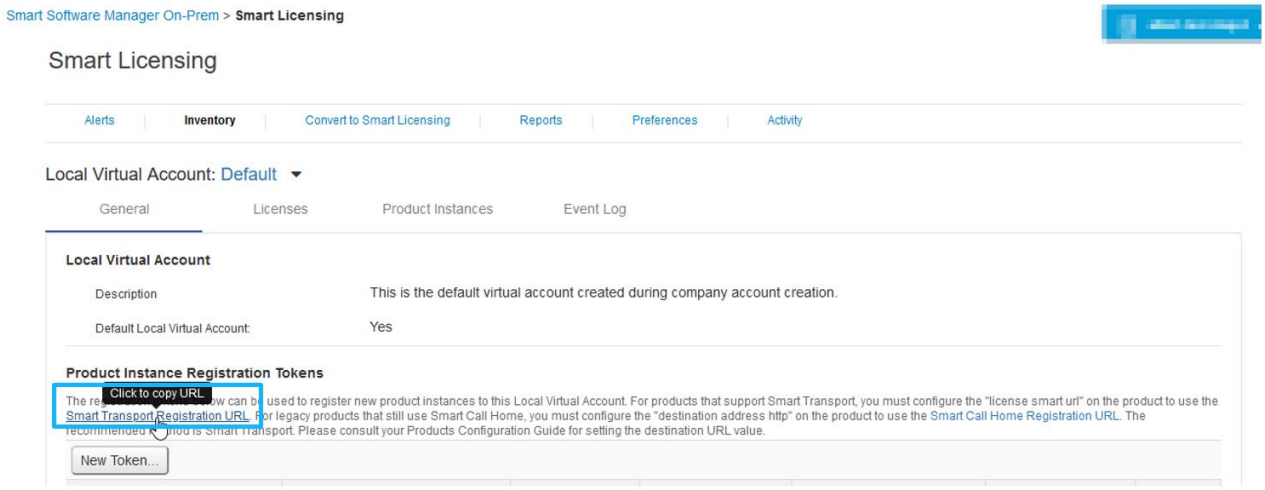
Once the transport settings are filled, use the Register button to register the product in the Smart Software Manager. The Register button is available in the License Administration page of Cisco Cyber Vision.

Cisco Cyber Vision License Menu with the link to edit the transport settings and the Register button



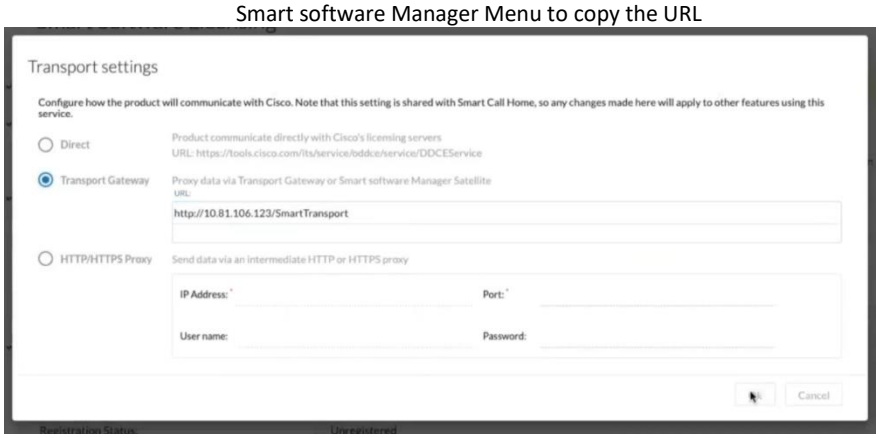
You will find the Smart software Manager Satellite URL in the On-Prem Smart Software Manager.

Smart software Manager Menu to copy the URL



In Cisco Cyber Vision, paste the URL in Transport Settings:

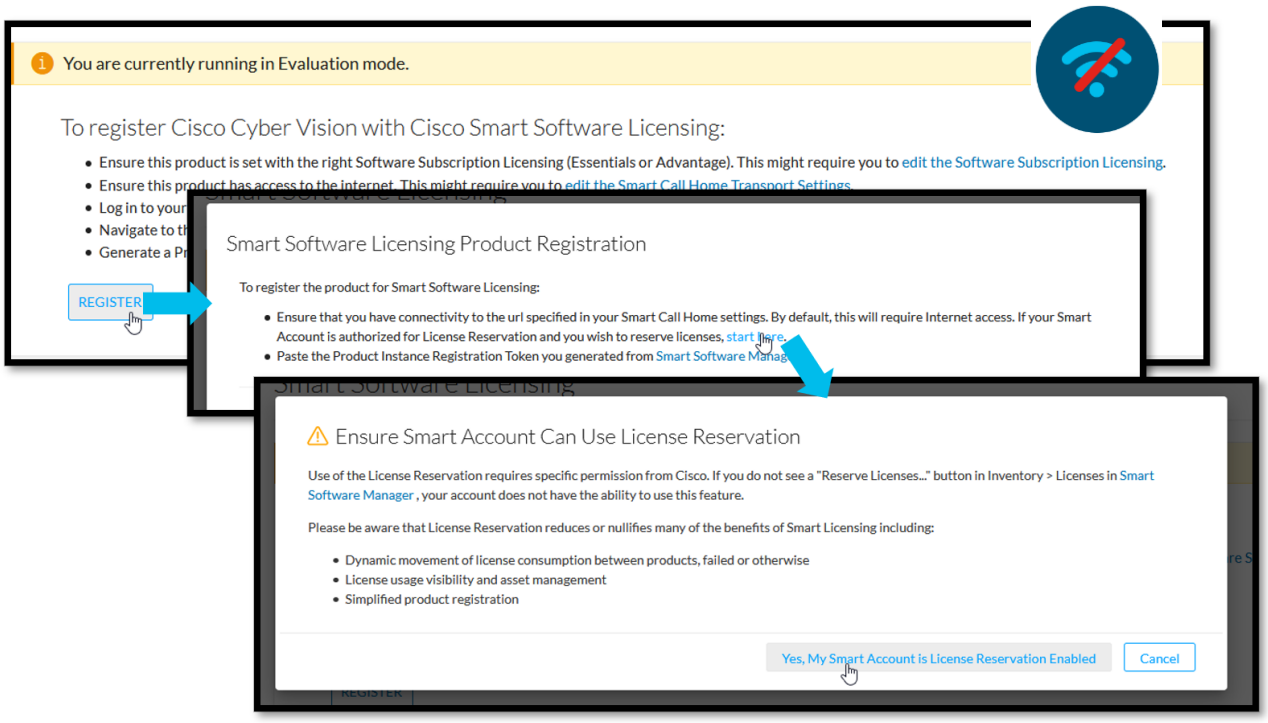
Smart software Manager Menu to copy the URL



A Token needs to be generated from the Smart software Manager Satellite to register Cisco Cyber Vision.

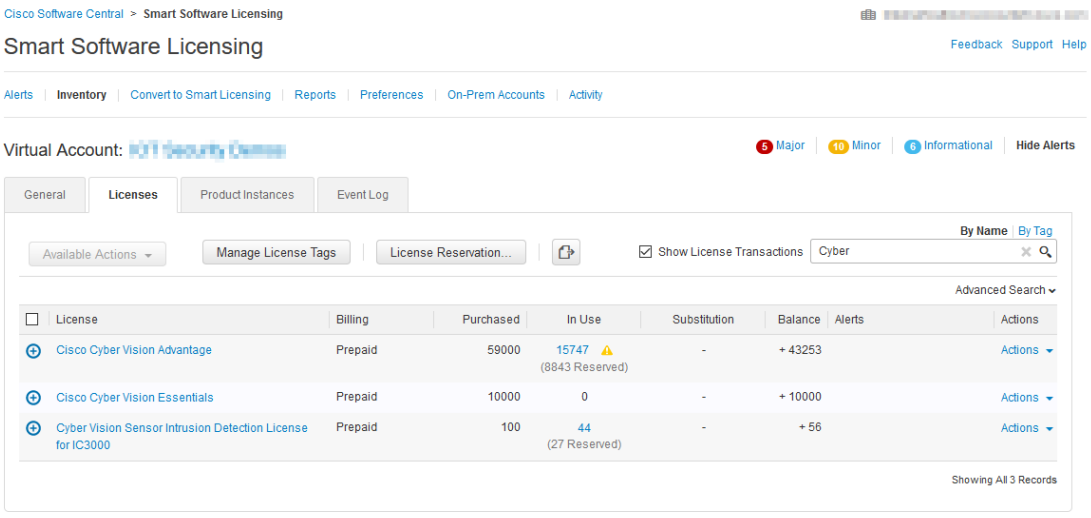
The License Reservation is accessible through the Register button, with the following procedure:

Cisco Cyber Vision Reservation settings



If you plan to use an offline license, you need to check that your Smart Account can perform a “License Reservation” (check from the License menu that the License reservation button is enabled). If your account doesn’t have the rights to do so, please open a case and provide a business justification.

Cisco Cyber Vision Licenses with “License Reservation…” button enabled



MSLA - Managed Service License Agreement

Managed Service License Agreement is a buying program under which managed service providers receive the right to use Cisco software and/or cloud services (including support).

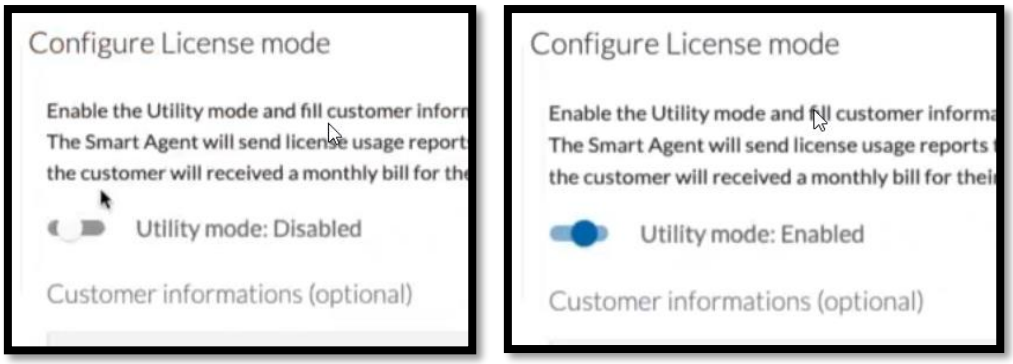
Note: Smart Software Manager Satellite instance is required to use MSLA.

Once Cisco Cyber Vision License transport settings are configured to use a Smart Software Manager Satellite, the License mode can be changed. Click the Actions button on the top right corner of the License page to enable the License mode:

Cisco Cyber Vision Change License Mode action

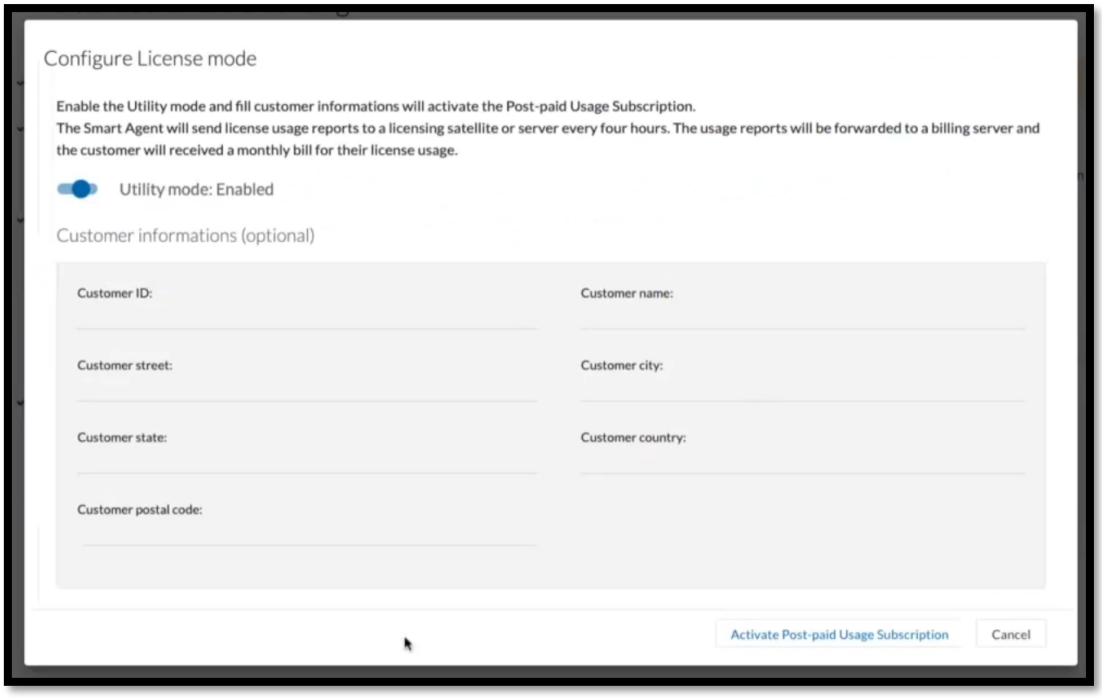
Enable the Utility mode:

Cisco Cyber Vision Licensing Utility Mode button.



Click the “Activate Post-paid Subscription” button.

Cisco Cyber Vision Licensing Activate



The license is enabled, and the license mode is displayed as “Post-paid Usage Subscription”.

New license type

Cisco Cyber Vision Release 3.2.1 supports a new license type:

- Cyber Vision Sensor Intrusion Detection License for Center

DPI licensing is based on the number of active DPI interfaces.

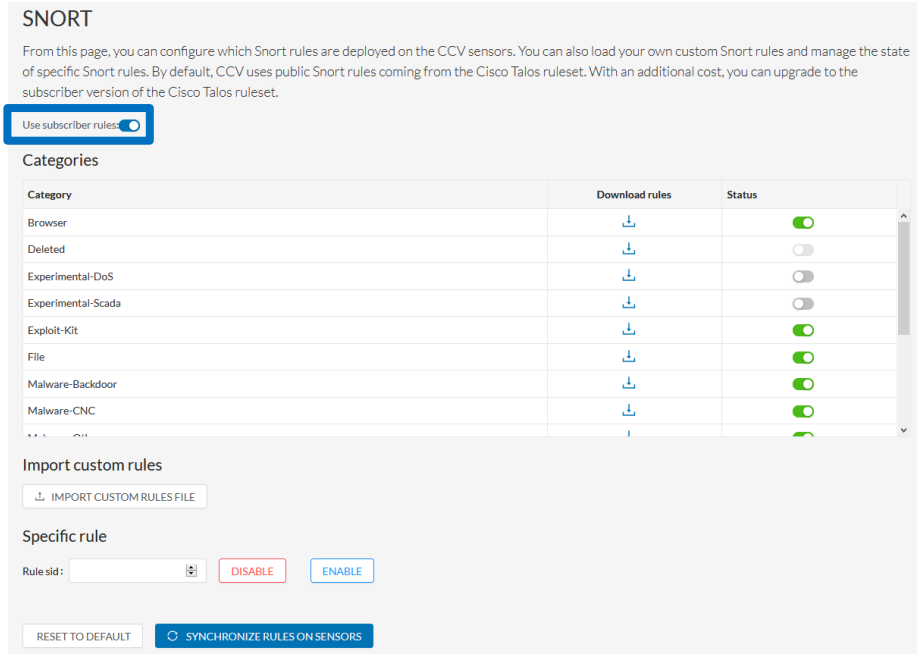
Cisco Cyber Vision Licenses:

- Cisco Cyber Vision Advantage
- Cisco Cyber Vision Essentials
- Cyber Vision Sensor Intrusion Detection License for IC3000
- Cyber Vision Sensor Intrusion Detection License for Center

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

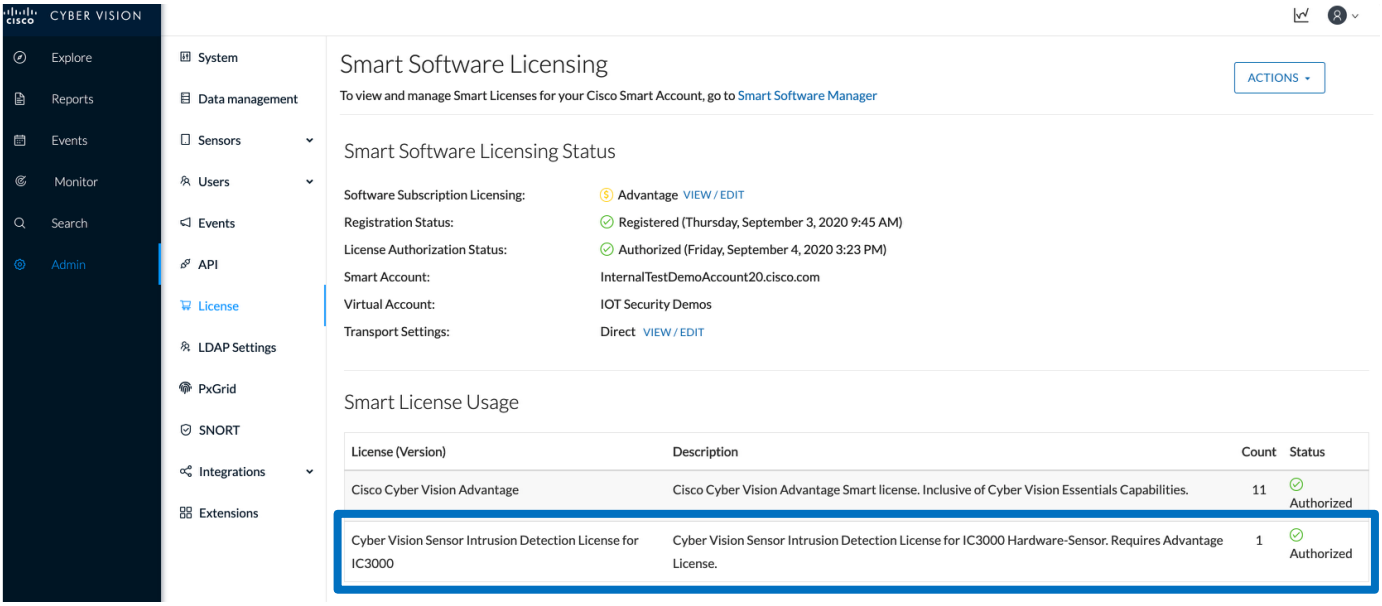
An Intrusion Detection License is required to use the Snort subscriber rule set. A new option is available in the SNORT administration page to select if the solution will use subscriber rules.

Cisco Cyber Vision Activate Subscriber rules



Once Subscriber Rules are activated, Intrusion Detection Licenses are required.

Cisco Cyber Vision IDS License



Snort

rules

Up to now, the Cisco Cyber Vision Knowledge DB included the Snort Registered ruleset and the Snort Subscriber ruleset. Starting from this release, the Cisco Cyber Vision Knowledge DB introduces the Snort Community ruleset instead of the Snort Registered ruleset. As such, the following policy will be applied:

- Users with a paid license will receive the Subscriber ruleset which contains the latest rules made available to Cisco customers as they are released by the Talos Security Intelligence and Research Team.
- Users with a free license will receive the Community ruleset which is a subset of the Subscriber ruleset. The Community ruleset is freely available to all Snort users and contains rules that have been submitted by members of the open-source community or by Snort Integrators.

Unless otherwise specified, all updates reported in the subsequent Knowledge DB release notes will be specific to the Subscriber ruleset.

The Subscriber ruleset is not accessible for users with a Cisco Cyber Vision version prior to 3.2.0. Users running the 3.2.0 version and above can switch between the Community and the Subscriber ruleset through the dedicated Snort page on the Cisco Cyber Vision Center webapp.

Please note that, to keep consistency between the Community and the Subscriber ruleset, Snort rules with the same sid are assigned the same category by taking as a baseline the categories within the Subscriber ruleset.

Please also note that, when exporting Snort rules, users might notice the presence of empty non-triggering rules. These are used internally to cover the missing sids between the community and the subscriber rulesets and should not trigger any alert. If you observe an alert on one of these rules, please notify the Cisco Cyber Vision team.

snort filters

In release 3.2.0, incoming traffic in Snort couldn't be easily filtered. Cisco Cyber Vision release 3.2.1 now applies configured sensor filters to the Snort DAQ engine as well. It means that all filters defined for the DPI side will be used directly in the IDS engine:

Cisco Cyber Vision sensor filter

Cisco Cyber Vision snort filter

```
root@sensor:~# ps ax | grep snort
  519 ?        Ssl    0:00 /opt/sbs/bin/sbs-nidsproxy snort-sensor /data/var/lib/snort/multi-user/alert_json.txt
  574 ?        Ssl    0:00 /opt/sbs/bin/sbs-nidsproxy snort-sensor /data/var/lib/snort/br0/alert_json.txt
  640 ?        Ssl    0:00 /opt/sbs/bin/sbs-nidsproxy snort-sensor /data/var/lib/snort/br1/alert_json.txt
  685 ?        Ssl    0:00 /opt/sbs/bin/sbs-nidsproxy snort-sensor /data/var/lib/snort/br2/alert_json.txt
  709 ?        Ssl    0:00 /opt/sbs/bin/sbs-nidsproxy snort-sensor /data/var/lib/snort/br3/alert_json.txt
 1664 ?        SNs    0:00 /usr/bin/lxc-start -F -n snort
 1669 ?        SNs    0:00 /bin/bash /usr/bin/snort_wrapper /data/var/lib/snort -c /data/etc/snort/snort.lua -A alert_json -g snort
-u snort --daq-dir=/usr/lib/daq -k none --daq afpacket
 1691 ?        SNl   14:33 /usr/bin/snort -c /data/etc/snort/snort.lua -A alert_json -g snort -u snort --daq-dir=/usr/lib/daq -k non
e --daq afpacket -l /data/var/lib/snort/br0 -i br0 --bpf not dst net 224.0.0.0/4 and not ip6 multicast
 1697 ?        SNl   14:14 /usr/bin/snort -c /data/etc/snort/snort.lua -A alert_json -g snort -u snort --daq-dir=/usr/lib/daq -k non
e --daq afpacket -l /data/var/lib/snort/br1 -i br1 --bpf not dst net 224.0.0.0/4 and not ip6 multicast
 1703 ?        SNl   16:23 /usr/bin/snort -c /data/etc/snort/snort.lua -A alert_json -g snort -u snort --daq-dir=/usr/lib/daq -k non
e --daq afpacket -l /data/var/lib/snort/br2 -i br2 --bpf not dst net 224.0.0.0/4 and not ip6 multicast
 1710 ?        SNl   14:10 /usr/bin/snort -c /data/etc/snort/snort.lua -A alert_json -g snort -u snort --daq-dir=/usr/lib/daq -k non
e --daq afpacket -l /data/var/lib/snort/br3 -i br3 --bpf not dst net 224.0.0.0/4 and not ip6 multicast
13909 pts/0    S+     0:00 grep snort
```

Changes are also applied dynamically if the filter is changed from the Center interface.

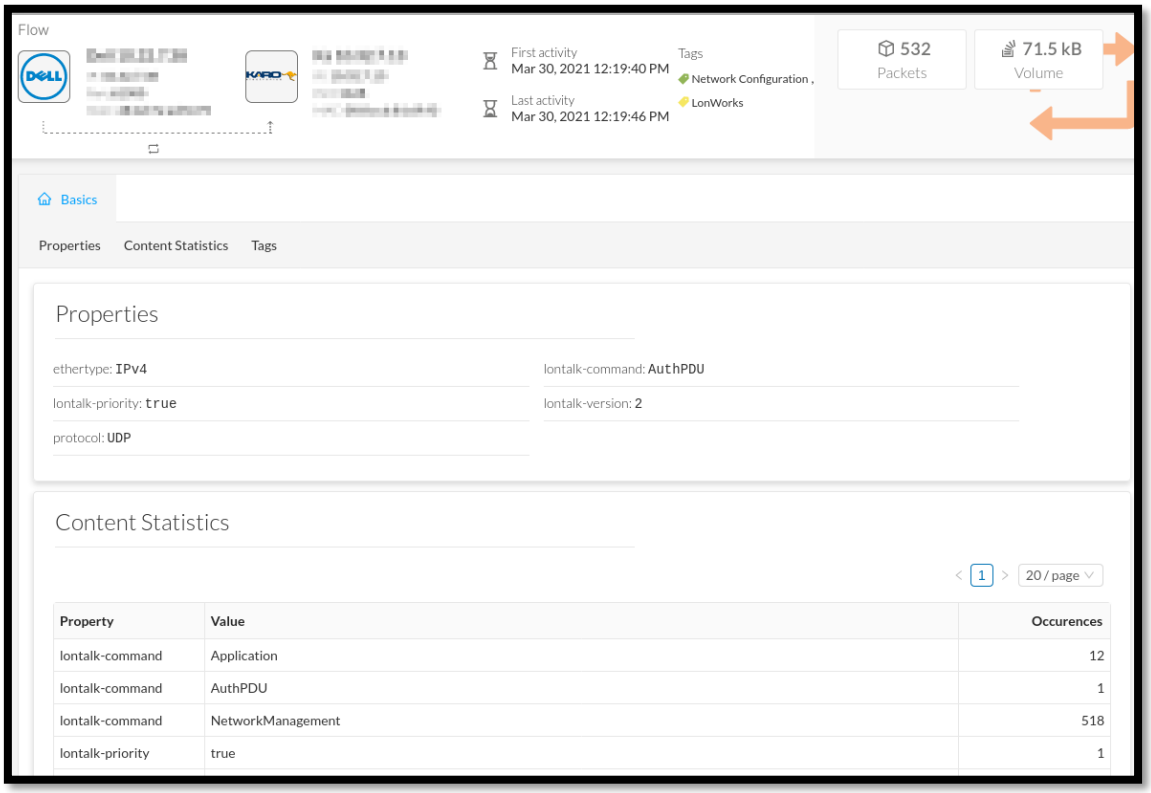
DPI improvements

Several issues related to the DPI engine have been fixed, and some improvements were done. The lists below detail the changes made in Cisco Cyber Vision 3.2.1:

New DPI features:

Issues ID / CDETS	Description
#2934 /	netbios name service is now used
#5677 /	echo Protocol is now tagged
#5678 /	Lontalk protocol is now tagged

Several properties were added related to LonWorks protocol in addition to the protocol tag:



DPI fixes:

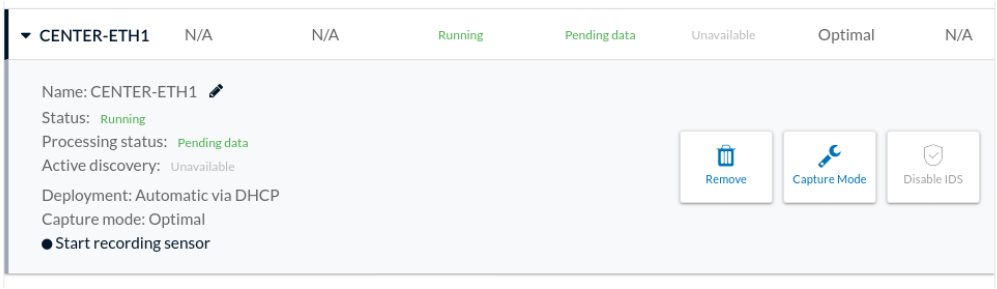
Issues ID / CDETS	Description
#5801 /	enip: broken forward open table
#5865 /	Incomplete handling of TCP data, leading to invalid statistics about layer7 bytes
#6042 /	Modbus: the direction of the flows is not detected in Modbus

Center DPI interface management

Cisco Cyber Vision Center DPI interfaces can now be configured individually, and settings will be available in a separate configuration file for each. It means that if the Center has several DPI interfaces, they can be configured with their own parameters, for example their own traffic filter.

Configuration of all DPI interfaces can be done from the Administration menu on the sensor page:

Cisco Cyber Vision DPI sensor filter



The configuration file is located in "/data/etc/flow/conf.d/ethx". All information is stored in the file called config.yml.

Sensor Management Extension: new hardware supported

In release 3.2.0 a limitation in the Cisco Cyber Vision sensor management extension was preventing sensor configuration in the following equipment:

- Cisco Catalyst IE3400 Heavy Duty Switch
- Cisco Catalyst 9400 Switch

This limitation was documented in CDETS: CSCvw46925.

In release 3.2.1, the list of devices which are supported by the Cisco Cyber Vision Sensor Management Extension is:

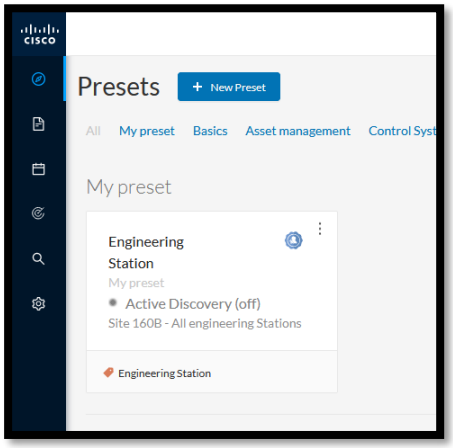
- Cisco IC3000 Industrial Compute Gateway
- Cisco Catalyst IE3400 Rugged Switch
- Cisco Catalyst IE3300 Rugged 10G series
- Cisco Catalyst IE3400 Heavy Duty Switch
- Cisco IR1101 Integrated Services Router Rugged
- Cisco Catalyst 9300 Switch
- Cisco Catalyst 9400 Switch

Global center: Synchronize custom presets

Cisco Cyber Vision 3.2.1 includes a feature related to Center synchronization to a Global Center. Now all user presets are automatically synchronized to the Global Center upon creation or modification.

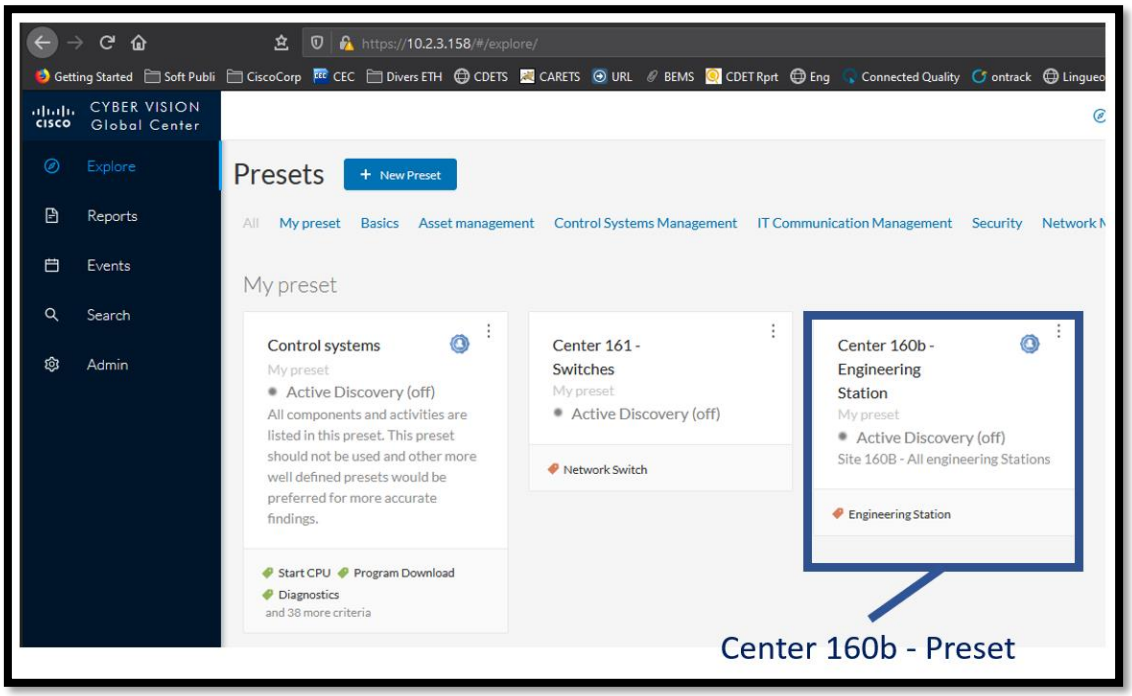
For example, a Center in the site “160b” has a user defined preset called “Engineering Station”:

Cisco Cyber Vision Center Presets



In the Global Center, this preset is shown as “Center 160b – Engineering Station” (center name – preset name). The area “My Preset” in the Explore Menu will present presets from the Global Center and from all attached Centers.

Cisco Cyber Vision Global Center Presets



Global center: A Center can now be deployed and started before enrollment to its Global Center

Cisco Cyber Vision release 3.2.1 includes a new feature that allows users to deploy the Center before deploying the Global Center.

It means that a Center can be deployed on a local site, its sensors can be enrolled, and data collection consumption can begin immediately. When the Global Center is ready, the Center can be enrolled, and all the data collected previously will be synchronized with all customization like groups and custom presets.

SNMPv3 for sysinfo notifications

Cisco Cyber Vision release 3.2.1 Center and sensors can send SNMP traps related to CPU and Memory usage. In previous versions traps used SNMPv2c, with release 3.2.1 the product can use SNMPv3.

SNMPv2c is the version used by default. The desired SNMP version can be set in the configuration file. Cyber Vision Center & sensors have no SNMP agent available, only SNMP traps are used to monitor Center's and Sensor's appliances.

SNMP traps on these products need to be activated with a configuration file to monitor CPU and Memory usage only.

A file called sysinfod.conf needs to be created into the Center or sensor in the path /data/etc/sbs/. This file will activate SNMP traps sent to a SNMP receiver and defines thresholds.

Example of sysinfod.conf:

```
snmp:
 target: 10.2.1.1
 port: 162
 version: 3
 security:
   username: test
   msgFlags: AuthPriv
   authenticationProtocol: SHA
   authenticationPassphrase: test1234
   privacyProtocol: AES
   privacyPassphrase: test1234
   authoritativeEngineID: 800000020109840301
 cpuUsageHigh:
   -
     rate: 5
     threshold: 5
   -
     rate: 30
     threshold: 85
 memUsageHigh:
   -
     rate: 5
     threshold: 50
   -
     rate: 30
     threshold: 85
```

Configuration parameters are:

- **target**: is the SNMP Manager IP Address. If not present, SNMP Notifications are disabled.
- **port**: is the SNMP Manager Port
- **version**: defines SNMP version, could be version 2c (by default) or version 3.
- **community**: (only for SNMPv2c)
  - **public (default)**
  - **custom**
- **security**: (only for SNMPv3)
  - **Username**: account used to the SNMPv3 session
  - **msgFlags**: defines authentication level
    - AuthPriv
    - NoAuthNoPriv (Default)
    - AuthNoPriv
    - AuthPriv
    - Reportable
  - **authenticationProtocol: defines authentication protocol**
    - SHA
    - MD5 (Default with NoAuthNoPriv)
  - **authenticationPassphrase:**
  - **privacyProtocol: defines encryption protocol**
    - AES
    - DES
    - NoPriv (Default)
  - **privacyPassphrase**
  - **authoritativeEngineID: unique identifier of a snmp device**
- **memUsageHigh** and **cpuUsageHigh** are the lists of notifications to be sent to the SNMP Manager
  - **rate** is the time interval in seconds at which a notification will be sent
  - **threshold** is the value that, if reached, will send a notification

The categories of notifications are:

- **memUsageHigh:** RAM usage alert
- **cpuUsageHigh:** CPU usage alert

After the file sysinfod.conf creation in the device, the device or the service responsible must be restarted ("`systemctl restart sysinfod`").

To check the notification status, launch the command: "`systemctl status sysinfod`" just after the service startup.

Cisco Cyber Vision sysinfod status

```
root@center:~# systemctl status sysinfod
● sysinfod.service - Cisco Cyber Vision Sysinfo Daemon
   Loaded: loaded (/lib/systemd/system/sysinfod.service; disabled)
   Active: active (running) since Thu 2021-01-28 15:50:00 UTC; 11s ago
 Main PID: 38500 (sysinfod)
   CGroup: /system.slice/sysinfod.service
           └─38500 /opt/sbs/bin/sysinfod

Jan 28 15:50:00 center sysinfod[38500]: sysinfo Center type: standalone [caller=postgres.go:290]
Jan 28 15:50:01 center sysinfod[38500]: sysinfo Notifications enabled [caller=notification.go:152]
Jan 28 15:50:01 center sysinfod[38500]: sysinfo Init worker to check sensor SSH access using a cycle: 60 secs [c...o:72]
Jan 28 15:50:01 center sysinfod[38500]: sysinfo Init listener for async system command using: /data/tmp/sysinfod...o:75]
Jan 28 15:50:01 center sysinfod[38500]: sysinfo Init sysinfo monitor service using a cycle: 5 secs [caller=main.go:78]
Jan 28 15:50:01 center sysinfod[38500]: sysinfo monitor tick: 5s [caller=monitor.go:17]
Hint: Some lines were ellipsized, use -l to show in full.
root@center:~#
```

Once the notifications are enabled, SNMP traps will be sent as thresholds are reached.

Center conversion to a Center with data synchronization

If you initially installed a Center without data synchronization enabled (i.e. without Global Center), but you want to manage it through a Global Center, the database must be previously converted. To do so, use the following command:

`sbs db-toolbox enable-synchronization`

Warning: This command will delete all data in the database, except sensors, users, and custom presets configurations. Activities, flows, components and events will be deleted.

Cisco Cyber Vision other enhancements

Issues ID / CDETS	Description
#5876 /	A loader is now displayed on KDB import on Global Center
#6157 /	After Cisco Cyber Vision Sensor Management extension removal: it was hard to remove extension-managed iox sensors. User experience is now improved.
#6212 /	skipflowcontent in sbs-burrow support glob matching (i.e.: skipflowcontent: ['slmp-*])
#6219 /	Dynamic Protocols inspection always failed at one time. The following protocols are handled by dynamic inspection (not linked to a port rule): DCERPC, SLMP, IEC101, Toyopuc, ssh, FTP. Inspection is now more robust.
#6221 /	Disable flow and variable insertion is now possible in sbs-stowd
#6230 /	Upgrade to postgresql 12.5 is done.
#6257 /	It's now possible to use some properties in sbs-burrow's analyzers, but not store them in Data Base.
#6259 /	Flow enforce a maximum size for the properties it generates
#6325 /	Synchronize snort rules on kdb import
#6335 /	Fog Director libraries upgrade in Cisco Cyber Vision Sensor Management Extension
#6370 /	Bulk deployment – A public API to create sensor and get provisioning was added in the product. It will authorize the usage of solution like Ansible to deploy sensors.
#6388 /	In Cisco Cyber Vision 3.2.1 now journal persists after reboot
#6433 /	Custom Properties in the API were extended to 512 characters
#6434 /	In flow configuration, old max_variables are supported to avoid production incidents
#6506 /	sbs-diag: add previous boots in the diagnostic created
#6557 /	sbs-syncd performance improvements
#6521 /	API V3: Sensor list route, add sensor status.
#6608 /	On upgrade from 3.2.0 (which has no preset synchronization) to higher version (with preset synchronization) on a running setup with a Global Center configuration, all existing presets will now be synchronized automatically.
#6630 /	Cisco Cyber Vision Sensor Active Discovery is now possible on Catalyst 9300 and Catalyst 9400.
#6658 /	Center DPI now used only one file per interface for flow configuration

Issues ID / CDETS	Description
#6661 /	Bulk deployment – A new API route was created to get center version -. It will authorize the usage of solution like Ansible to deploy sensors.
#6160 /	Remove Press erase button for iox sensor
#6756/	Improve command sbs-db "purge flow from/since date" which was very slow
#6718 /	Flow on center now uses a smaller buffer ratio
#6258 /	Flow_property_statistics table now doesn't use the property value in the composite PK
#6311 /	Sbs-burrow benchmark now doesn't fail at second iteration
#6533 /	Sensor ID was added in 2 new syslog events (New gateway, and vulnerabilities events).
#6534 /	Sbs-db will be rewritten in go and the new version is accessible with the command line sbs-db-toolbox. sbs-db-toolbox is now available in release 3.2.1 to allow the command `sbs-db-toolbox enable-synchronization`. **Sbs-db must still be used for all the other commands**.
#6342 /	Several DPI performance improvements added

Cisco Cyber Vision bug fixed

Issues ID / CDETS	Description
#6343 /	Flow filtering now works on IE3300/Cat9400/IE3400H, it was working in 3.2.0 only on IR1101, IE3400, Cat9300.
#4525 /	Cisco Cyber Vision sensor will by default not "split" unknown structure to limit variable number
#4982 /	Duplicate subscriptions on sensor-inputd are now checked
#5362 /	Tooltip of group parents is no more broken
#5868 /	Snort no more displays error log after activation
#5914 /	Enroll Local Center: user has now some feedbacks on wrong Certificate and IP address
#5978 /	Offline sensor file import in Cisco Cyber Vision Center, a sensor name is now displayed
#6044 /	Read errors from go-diskqueue are now handled.
#6129 /	Monitor Mode: reported property is now marked as new
#6142 / CSCvw50771	Static route is available without center's reboot
#6143 /	Global Center's enrollment form no more disappears
#6144 /	Some inconsistencies on Sensor's management page were removed
#6149 /	Incorrect types for password setting no more cause 400 error
#6150 /	Creation of expired token without date no more causes 500 error
#6153 /	DPI enip: unanswered requests are not kept too long
#6164 /	Global center a good error message is shown while center enrollment presents a wrong fingerprint
#6168 /	egel-filter.conf at the root of a USB key now filters offline traffic
#6170 /	Fix SLMP Decode errors which could generate millions of events in 24h
#6172 /	Variable export interval is now respected to avoid missing exports
#6175 /	'podman stats' command is now working
#6176 /	sbs-ted now can get token
#6178 /	Fix some wrong English labels

Issues ID / CDETS	Description
#6191 /	GUI – Center Statistics Eth0, Eth1 are no more shown instead of the tab name
#6195 /	GUI Map: group doesn't appear anymore as dot when there is some conflict between maps
#6199 /	Errors on group custom properties were fixed
#6205 /	IOx Sensor: configure internal interface MTU if asked by platform
#6224 / CSCvw50763	Export activities to CSV is now possible on an unsaved preset
#6242 /	Sysinfo no more crashes on IC3K with Active Discovery
#6279 / CSCvw58685	icmp no more dropped by center firewall
#6301 / CSCvw52202 CSCvx17844	FMC integration, fix missing component attributes
#6312 /	Fix value for last seen FlowInfo
#6314 /	GUI: Activity count is now filled on group details
#6323 /	GUI: Pagination is no longer reset on column sort
#6329 /	Fix snort on Center DPI sometimes fails when rebooted
#6332 /	Fix Vulnerabilities Dashboard where sorting by CVSS prevents page navigation
#6339 /	Global Center – No License should be asked or seen on a global center
#6346 /	Fix: Button "Manage group" shows a wrong display on Firefox
#6352 /	Fix: Active Discovery flows which were not tagged on Sensor 3
#6353 /	Sbs-burrow now correctly updates the 'last seen logs' status
#6362 /	Fix issue with S7 DPI when blocklist found in ProgramData
#6375 / CSCvw76017	SBS-netconf cancel button is now working when trying to cancel adding a route on an interface
#6380 /	Update incoming traffic filter on IOx sensors is now working
#6424 /	A temporary solution prevents Vlan id changes on Broadcast and multicast components
#6428 /	Component serial number doesn't use smb-server-guid property anymore.

Issues ID / CDETS	Description
#6435 /	Fixed flow panic in Protocol Reassembly
#6437 /	Fix some Flow exception events which reference a sensor ID that does not exist anymore
#6528 /	Fix: Custom presets could not be edited in some conditions
#6556 /	Fix: In single interface mode, haproxy does not set headers corresponding to the presented certificate
#6597 /	Database upsert of flow tags by burrow are now more efficient.
#6263 /	pg_data_files_sorted_by_size_desc file is not empty anymore in sbs-diag
#6341 /	In release 3.2.0 RabbitMQ sometime fails to start, this is now fixed.
#6411 /	Some minor GUI issues are now fixed
#6429 /	Fix: SMB OS name decoding could produce some properties with wrong character encoding
#6662 /	Fix: Error on preset synchronization
#6674 /	Fix: Issue activating double default gateway on SENSOR with active discovery
#6694 /	Snort: Disable interface check for sensor which prevents snort to start
#6719 /	Fix: Some sensor builds were fetching next instead of the right build on dependencies
#6373 /	Fix: S7-slot property of a component change over time
#6709 /	Fix: Decode error: with Toyopuc invalid 0 length
#6731 /	3.2.1 fix an issue where a database import never ends.
#6773 /	Fix: Cannot synchronize nids from GUI
#6774 /	Fix: "toolbox convert-st-to-lc" does not correctly set the list of tables to save
#6775 /	Fix: sbs-diag: getting previous boots takes too much time
#6806 /	Fix: toolbox conversion: the list of tables to dump is empty

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.
# - / CSCvx20904	Sensor Management Extension	Sensor Management Extension - Unable to change password after application deployed.