Release Notes for Cisco Cyber Vision Release 4.0.1

For users upgrading to 4.0.1 from previous versions, please carefully read the Cisco Cyber Vision 4.0.1 update procedure.

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
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, 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-4.0.1.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-with-DPI-4.0.1.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-center-4.0.1.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-sensor-management-4.0.1.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-4.0.1.tar	IE3400, IR1101 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64--4.0.1.tar	IE3400, IR1101 active Discovery sensor installation and update file
CiscoCyberVision-IOx-IC3K-4.0.1.tar	IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.0.1.tar	Catalyst 9x00 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.0.1.tar	Catalyst 9x00 active Discovery sensor installation and update file
Updates	**Description**
CiscoCyberVision-Embedded-KDB-4.0.1.dat	KnowledgeDB embedded in Cisco Cyber Vision 4.0.1
CiscoCyberVision-update-center-4.0.1.dat	Center update file for upgrade from release 4.0.0 to release 4.0.1
CiscoCyberVision-update-sensor-4.0.1.dat	Cisco IC3000 Sensor and Sentryo Sensor3, 5, 7 update file for upgrade from release 4.0.0 to release 4.0.1
CiscoCyberVision-update-combined-4.0.1.dat	Center, IC3000 Sensor and Legacy Sensor update file from GUI for upgrade from release 4.0.0 to release 4.0.1

Cisco Cyber Vision Center 4.0.1 can also be deployed on AWS (Amazon Web Services). The Cyber Vision Center AMI (Amazon Machine Image) can be found on the AWS Marketplace:

https://aws.amazon.com/marketplace/seller-profile?id=e201de70-32a9-47fe-8746-09fa08dd334f

https://aws.amazon.com/marketplace/search/results?searchTerms=Cisco+Cyber+vision

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:

  Cisco_Cyber_Vision_GUI_User_Guide_4_0_0.pdf
- Cisco Cyber Vision Network Sensor Installation Guide for Cisco IE3300 10G, IE3400 and Catalyst 9300:

  Installation_Guide_for_Cisco_IE3300_10G_Cisco_IE3400_and_Cisco_Catalyst_9300_4_0_0.pdf
- Cisco Cyber Vision Network Sensor Installation Guide for Cisco IR1101:

  Cisco_Cyber_Vision_Network_Sensor_Installation_Guide_for_Cisco_IR1101_4_0_0.pdf
- Cisco Cyber Vision Network Sensor Installation Guide for Cisco IC3000:

  Cisco_Cyber_Vision_Network_Sensor_Installation_Guide_for_Cisco_IC3000_4_0_0.pdf
- Cisco Cyber Vision IC3000 Troubleshooting Guide:

  Cisco_Cyber_Vision_IC3000_Troubleshooting_Guide_Release_3_0_2.pdf
- Cisco Cyber Vision Center Appliance Installation Guide:

  Cisco_Cyber_Vision_Center_Appliance_Installation_Guide_4_0_0.pdf
- Cisco Cyber Vision Center VM Installation Guide:

  Cisco_Cyber_Vision_Center_VM_Installation_Guide_4_0_0.pdf
- Cisco Cyber Vision Center AWS Installation Guide:

  Cisco Cyber Vision for AWS Cloud Installation Guide
- Cisco Cyber Vision SecureX Integration Guide:

  Cisco Cyber Vision SecureX Integration Guide Release 4_0_0.pdf
- Cisco Cyber Vision Integration Guide, Integrating Cisco Cyber Vision with Cisco Identify Services Engine (ISE) via pxGrid:

  Integrating-Cisco-Cyber-Vision-with-Cisco-Identify-Services-Engine-via-pxGrid.pdf
- Cisco Cyber Vision Smart Licensing User Guide, Release 3.2.2

  Cisco_Cyber_Vision_Smart_Licensing_User_Guide_3_2_2.pdf

Cisco Cyber Vision 4.0.1 update procedure

Cisco Cyber Vision 4.0.1 update procedure will depend on the architecture deployed and the tool used to deploy it.

If you are currently running a version earlier than Cisco Cyber Vision 4.0.0, you must first upgrade to 4.0.0 prior to upgrading to Cyber Vision 4.0.1.

Data purge

Cisco Cyber Vision update procedure will not purge data automatically. The Center 4.0.0 database will be migrated to the new 4.0.1 schema. All components, activities, flows, events, etc. will be migrated.

The new data retention policies introduced in 4.0.0 are still valid in 4.0.1. Once migrated, the following expiration settings will be applied and the system will purge unless the configuration is modified:

- Events after 6 months.
- Flows after 6 months.
- Variables after 2 years.

Center updates

Architecture with Global Center

In the case of a distributed architecture, the following steps need to be followed:

1. Update the Global Center:
    a. Using the graphical user interface:
        - File= CiscoCyberVision-update-combined-4.0.1.dat
        - Navigate to Admin > System and use the System Update button, and browse and select the update file.
    b. Using the command line interface (CLI):
        - File= CiscoCyberVision-update-center-4.0.1.dat
        - Launch the update with the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-center-4.0.1.dat
```

2. Update the Centers connected to the Global Center with the same procedure used for the Global Center (user interface or CLI)
3. Update the sensors, from their corresponding Center (not from the Global Center):
    a. Hardware sensors:
        i. If you used the combined file to update the Center which owned the sensor, the hardware sensors (IC3000 and Sentryo SENSOR's) were updated at the same time.
        ii. If not, the update needs to be done from the Command Line (CLI):
            - File= CiscoCyberVision-update-sensor-4.0.1.dat
            - Launch the update with the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-sensor-4.0.1.dat
```

Note: Cisco Cyber Vision Sensor application should not be updated from the IC3000 Local manager because the configuration will be lost. In case this is done, the sensor enrollment package needs to be deployed again.

b. IOx sensors:

   i. If you have installed the sensor with the sensor management extension, the upgrade of the extension will also update all sensors reachable from the Center.

      - File = CiscoCyberVision-sensor-management-4.0.1.ext
      - Navigate to Admin > Extensions. In the Actions column, use the update button and browse to select the update file.

   ii. If a sensor was not updated by the extension update, access the sensor administration page, and use the UPDATE CISCO DEVICES button to update the remaining IOx sensors connected to the Center.

   iii. If you have not installed the sensor with the sensor management extension, the upgrade of the sensor can be performed with the sensor package from the platform Local Manager or from the platform Command Line. This procedure is described in the corresponding sensors installation guides.

      - IE3x00 and IR11101 files = CiscoCyberVision-IOx-aarch64-4.0.1.tar or CiscoCyberVision-IOx-Active-Discovery-aarch64--4.0.1.tar
      - Catalyst 9300 and 94000 files = CiscoCyberVision-IOx-x86-64-4.0.1.tar or CiscoCyberVision-IOx-Active-Discovery-x86-64-4.0.1.tar.

Architecture with one Center

In the case of a single Center, the following steps need to be followed:

1. Update the Center:
    a. Using the graphical user interface:
        - File= CiscoCyberVision-update-combined-4.0.1.dat
        - Navigate to Admin > System, use the System Update button, and browse and select the update file.
    b. Using the command line interface (CLI):
        - File= CiscoCyberVision-update-center-4.0.1.dat
        - Launch the update with the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-center-4.0.1.dat
```

2. Update the sensors:
    a. Hardware sensors:
        i. If you used the combined file to update the Center, the hardware sensors (IC3000 and Sentryo SENSOR's) were updated at the same time.
        ii. If not, the update needs to be done from the command line interface (CLI):
            - File= CiscoCyberVision-update-sensor-4.0.1.dat
            - Launch the update with the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-sensor-4.0.1.dat
```

    b. IOx sensors:
        i. If you have installed the sensor with the sensor management extension, the upgrade of the extension will also update all reachable sensors.
            - File = CiscoCyberVision-sensor-management-4.0.1.ext
            - Navigate to Admin > Extensions. In the Actions column, use the update button and browse to select the update file.
        ii. If you have not installed the sensor with the sensor management extension, the upgrade of the sensor can be performed with the sensor package from the platform Local Manager or from the platform Command Line. This procedure is described in the corresponding sensors installation guides.
            - IE3x00 and IR1101 files = CiscoCyberVision-IOx-aarch64-4.0.1.tar or CiscoCyberVision-IOx-Active-Discovery-aarch64--4.0.1.tar
            - Catalyst 9300 and 9400 files = CiscoCyberVision-IOx-x86-64-4.0.1.tar or CiscoCyberVision-IOx-Active-Discovery-x86-64-4.0.1.tar.

Cisco Cyber Vision 4.0.1 important change

Communication port and protocol changes

Port

There is no port change in Cisco Cyber Vision 4.0.1. All TCP or UDP ports already used are kept, and no new port number is needed.

Protocol

No modification in 4.0.1.

API

No modification in 4.0.1.

SYSLOG

No modification in 4.0.1.

Cisco Cyber Vision new features and improvements

IDS license for Catalyst 9300

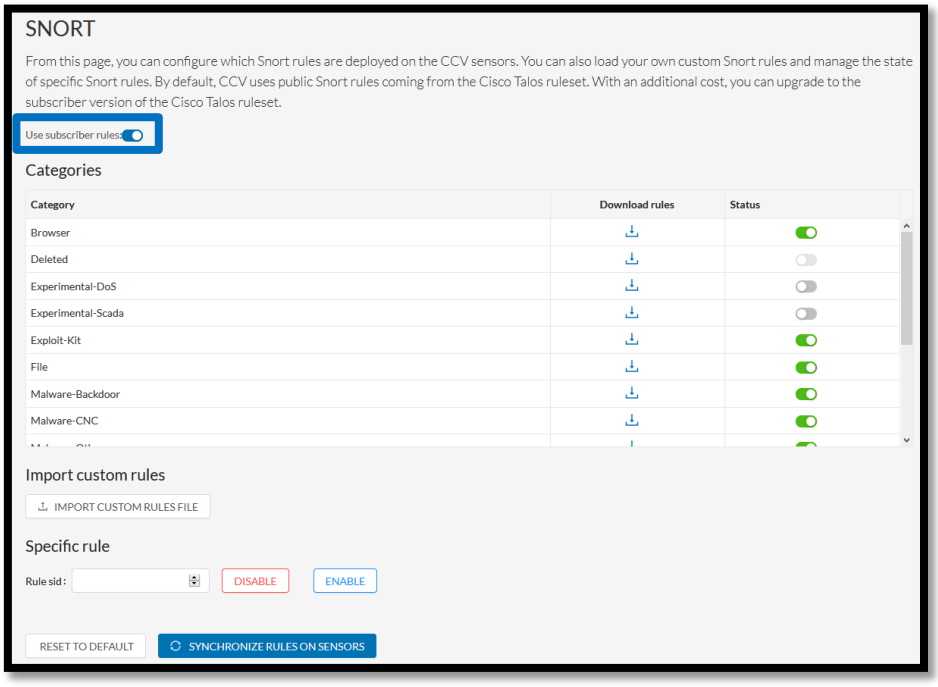
Cisco Cyber Vision 4.0.1 will now request a license for Snort running in a Sensor hosted by a Catalyst 9300. As it was already done for the IC3000 sensor and for the Center DPI interface a license is needed to use the Snort with subscriber rule set.

Cisco Cyber Vision Release 4.0.1 now supports the following Licenses:

- Cisco Cyber Vision Advantage
- Cisco Cyber Vision Essentials
- Cisco Cyber Vision Sensor Intrusion Detection License for IC3000
- Cisco Cyber Vision Center IDS
- Cisco Cyber Vision Cat9k IDS

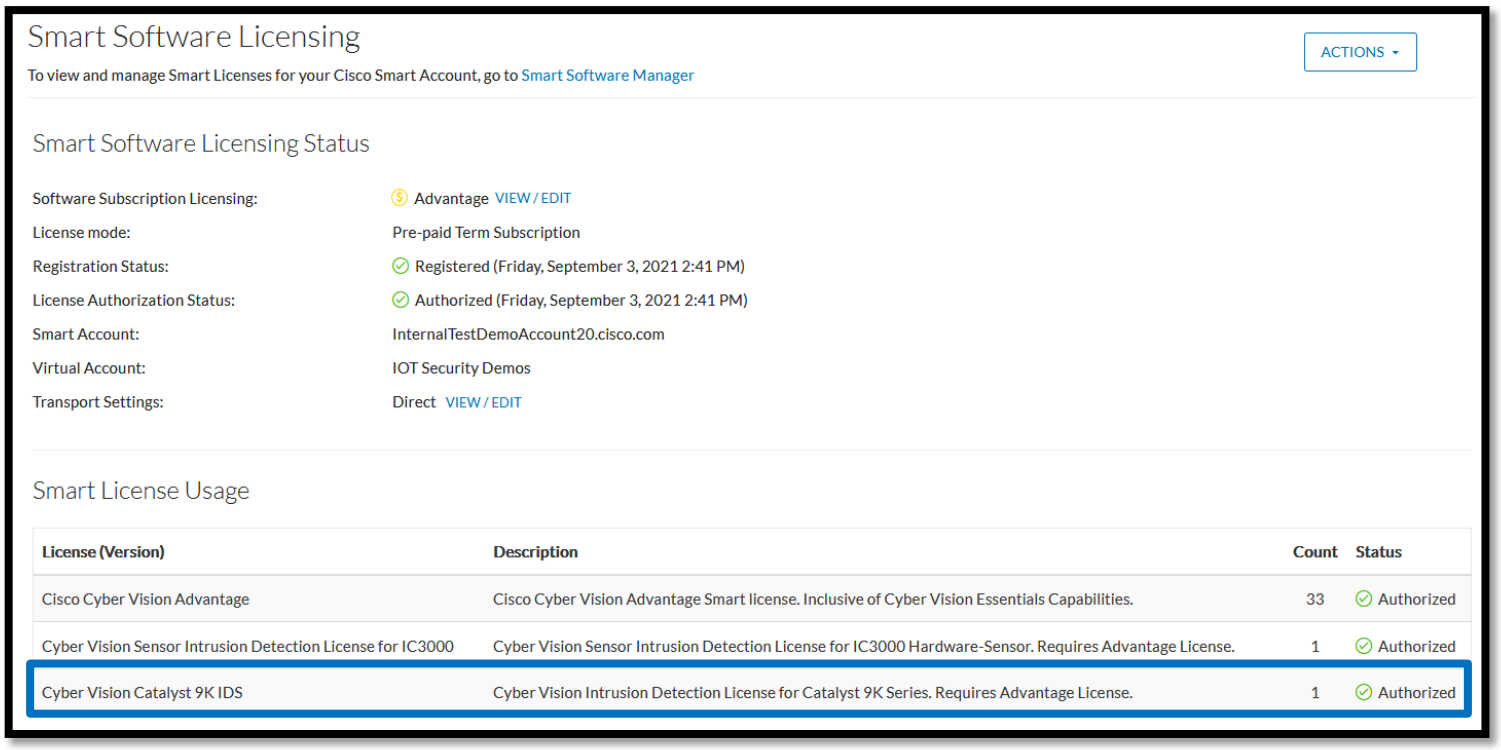
IDS and Snort community rule sets are included in the Advantage license level, with the support for custom Snort rules. An Intrusion Detection License is required to use the Snort subscriber rule set. A new option is available in the SNORT administration page to select if the solution will use subscriber rules.

Cisco Cyber Vision Activate Subscriber rules



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

Cisco Cyber Vision Cat9k IDS License



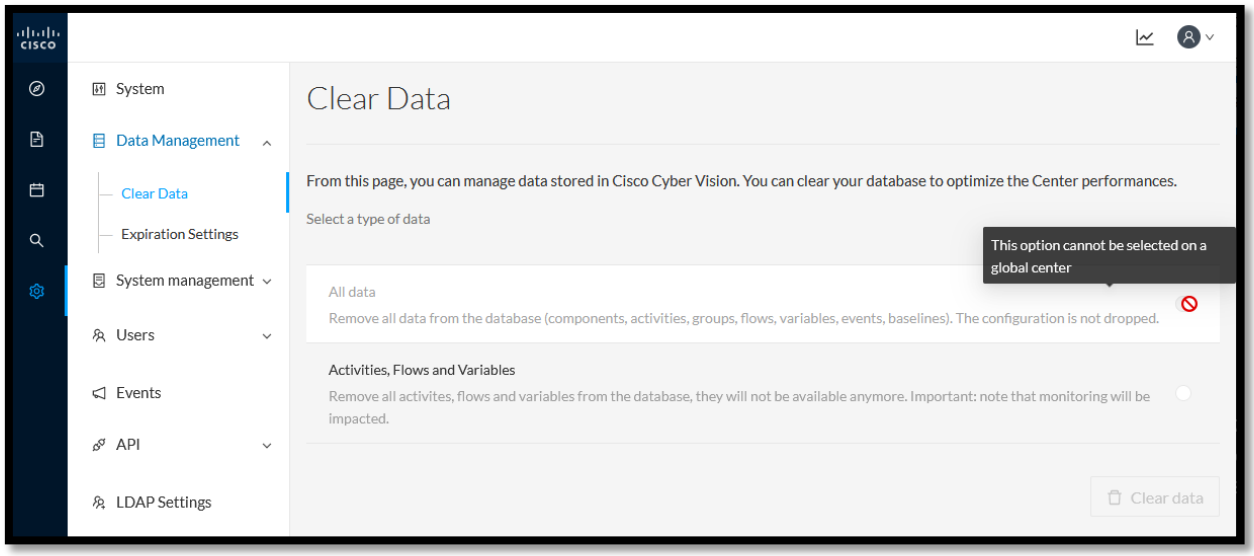
Gitlab ID: 8309

CDETS ID: CSCvz02406

Data management – disable clear data options

Starting in Cyber Vision 4.0.1, the ability to remove all data from the Global Center has been removed and will be displayed as disabled in the administration menu.

Cisco Cyber Vision Global Center Clear Data is now disabled

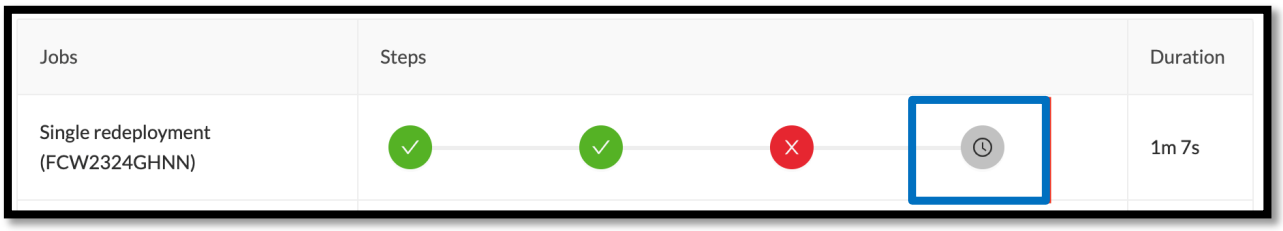


Gitlab ID: 8158

Sensor management job – pending icon change

Cisco Cyber Vision 4.0.1 introduces a new pending icon to the sensor management interface to make each step in the process clear.

Cisco Cyber Vision Sensor management pending step icon

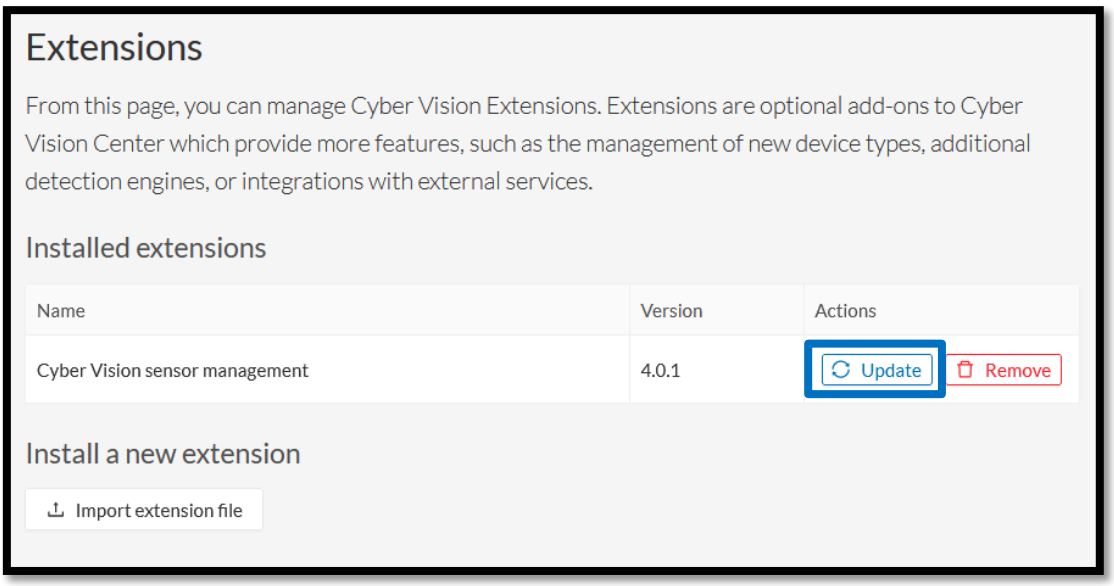


Gitlab ID: 8194

Cisco Cyber Vision Extension update button change

In Cisco Cyber Vision 4.0.1, the Sensor Extension Management icons have been updated to make it clearer which action the users is taking.

Cisco Cyber Vision Sensor management update button



Gitlab ID: 8360

Cisco Cyber Vision Bug fixed

Issues ID / CDETS	Description
#8540 / CSCvz14256	Cisco Cyber Vision Sensor 4.0.0 failed to be deployed on Catalyst 9300 version 17.6.1
#7702 /	DPI better inspects Toyopuc protocols to avoid false positive
#7891 /	Fix TLS decode error
#8095 /	Fix incorrect tagging of a Toyoda PLC with the tag “Engineering Station”
#8144 /	Fix server side of some protocols
#8287 /	Fix incorrect typing when user tries root login on VMWare console
#8388 /	Use latest KDB to update burrow reference
#8406 /	Fix the default expiration setting for variable which cannot be reset
#7998 /	Fix the preset materialized view computation which sometime takes too long time to be created (for example with 400K components)

Cisco Cyber open CDETS and known issues

Issues ID / CDETS	Component	Description
#7808 / CSCvy30877	Centers	RPC-DCOM flows often not tagged: cannot selectively delete and appear in security insights
#8192 / CSCvy83325	Catalyst	The extension installs to a Catalyst 9300 in Stackwise-480 with 2 SSDs fails.
#8333 /	Centers	Double DNS_Server tags. Some DNS_Server components tags are badly added to activities (linked mDNS protocol).
#8677 / CSCvz50904	Centers	Smart agent sometimes crashes when starting on centers using SLR license mode
#8599 / CSCvz38511	Centers	Cisco Cyber Vision is not sending pxgrid update for device group change for all the components belonging to corresponding devices. .