Release Notes for Cisco Cyber Vision Release 4.1.4

For users upgrading to 4.1.4 from previous versions, please carefully read the Cisco Cyber Vision 4.1.4 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
AWS – Center AMI	Amazon Web Services center image
Azure – Center plan	Microsoft Azure center plan
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 Catalyst IE9300	Cyber Vision Sensor IOx application hosted in Cisco Catalyst IE9300 Rugged Series switches
Cisco IR1101	Cyber Vision Sensor IOx application hosted in Cisco IR1101 Series Industrial Integrated Services Routers
Cisco Catalyst IR8300	Cyber Vision Sensor IOx application hosted in Cisco Catalyst IR8300 Rugged Series 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

Cisco Cyber Vision 4.1.4 update procedure

Cisco Cyber Vision 4.1.4 update procedure will depend on the architecture deployed and the tool used to deploy it.

Upgrade Path

Upgrade Path to Cisco Cyber Vision 4.1.4

Current Software Release	Upgrade Path to Release 4.1.4
If version prior to 3.2.4	Upgrade first to 3.2.4, then to 4.0.0, and to 4.1.4
Version 3.2.4	Upgrade first to 4.0.0, then to 4.1.4
Version 4.0.0 to 4.1.3	Upgrade directly to Release 4.1.4

Compatibility Guidelines

There is downward compatibility of one version between the Global Center and the Center with sync and sensors.

- Global Center (Version N): Compatible with Centers with sync with versions N and N-1.

  e.g. Global Center version 4.1.0 can manage local Centers with versions 4.1.0 and 4.0.3.
- Center with sync (Version N): Compatible with sensors with versions N and N-1.

  e.g. Center with sync version 4.1.0 can manage sensors with versions 4.1.0 and 4.0.3.

Data purge

The Center database in 4.0.0, 4.0.1, 4.0.2 or 4.0.3 will be migrated to the new 4.1.x schema. All components, activities, flows, events, etc. will be migrated.

The new data retention policies introduced in 4.0.0 are still valid in 4.1.x. Once migrated, the following expiration settings will be applied, and the system will run the purge process unless the configuration is modified within 2 days:

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

Center updates

Architecture with Global Center

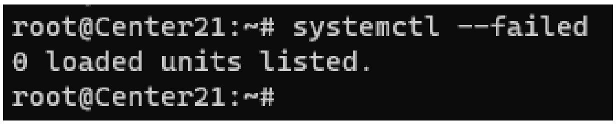
Preliminary checks: it is highly recommended that you check the health of all Centers connected to the Global Center and of the Global Center itself before proceeding to the update.

To do this check, it is recommended to use an SSH connection to the Center and to type the following command:

```
systemctl --failed
```

The number of listed sbs-* units should be 0, otherwise the failure needs to be fixed before the update.

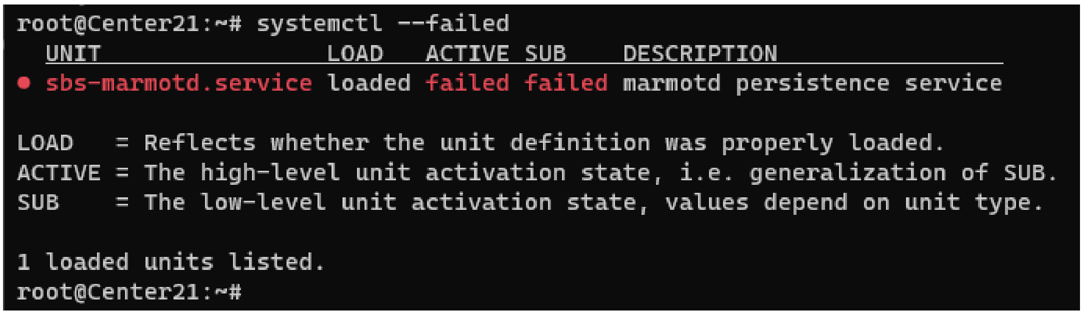
Cisco Cyber Vision system check – 0 failure



```
root@Center21:~# systemctl --failed
0 loaded units listed.
root@Center21:~#
```

All sbs services need to be running in a normal state before performing an update. If any is listed as failed it must be fixed prior upgrading.

Cisco Cyber Vision system check – example of failure



```
root@Center21:~# systemctl --failed
  UNIT                   LOAD   ACTIVE SUB    DESCRIPTION
● sbs-marmotd.service loaded failed failed marmotd persistence service

LOAD   = Reflects whether the unit definition was properly loaded.
ACTIVE = The high-level unit activation state, i.e. generalization of SUB.
SUB    = The low-level unit activation state, values depend on unit type.

1 loaded units listed.
root@Center21:~#
```

Rebooting of the Center most often solves the issue. If not, please contact the support.

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

1. Update the Global Center:
    a. Either using the Graphical User Interface:
        - File= CiscoCyberVision-update-combined-4.1.4.dat
        - Navigate to Admin > System, use the System Update button and browse and select the update file.

    b. Or using the Command Line Interface (CLI):
        - File= CiscoCyberVision-update-center-4.1.4.dat
        - Launch the update with the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-center-4.1.4.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 owns the sensor, and the SSH connection from the Center to the allowed sensor, the hardware sensors (IC3000 and Sentryo SENSOR's) were updated at the same time.
        ii. If the Cisco IC3000 sensor was deployed using the Sensor management extension, it can be upgraded by deploying it again.
        iii. If not, the update needs to be done from the Command Line Interface (CLI):
            - File= CiscoCyberVision-update-sensor-4.1.4.dat
            - Launch the update with the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-sensor-4.1.4.dat
```

You can check the sensor version on the Administration / Sensor Explorer page, to make sure that the version is 4.1.4.

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 sensors with the sensor management extension, first upgrade the extension and then update the sensors.

      - File = CiscoCyberVision-sensor-management-4.1.4.ext
      - Navigate to Admin > Extensions. In the Actions column, use the update button and browse to select the update file.
      - The Cisco Cyber Vision sensor management extension can also be updated from the CLI with the command:

```
sbs-extension upgrade /data/tmp/CiscoCyberVision-sensor-management-4.1.4.ext
```

   ii. Then all sensors need to be updated with the extension, to do so, access the sensor administration page, and use the menu “Manage Cisco devices” / “Update Cisco devices” or use the redeploy. A complete procedure is available in the document (part “Cisco Cyber Vision new features and improvements”) or in all sensor deployment guides version 4.1.4 minimum.

   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 IR1101 files = CiscoCyberVision-IOx-aarch64-4.1.4.tar or CiscoCyberVision-IOx-Active-Discovery-aarch64--4.1.4.tar
      - Catalyst 9300 and 9400 and IR8340 files = CiscoCyberVision-IOx-x86-64-4.1.4.tar or CiscoCyberVision-IOx-Active-Discovery-x86-64-4.1.4.tar.

Important remark regarding CiscoCyberVision-IOx-x86-64 sensor application update:

The sensor update through the Local Manager of a Catalyst 9300, 9400 or IR8340 files is not possible from a release 4.1.2 (or lower) to a release 4.1.3 (or higher) due to the addition of the rspan compatibility. The sensor application needs to be redeployed and the enrollment package uploaded again.

Architecture with one Center

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

1. Update the Center:
    a. Either using the Graphical User Interface:
        - File= CiscoCyberVision-update-combined-4.1.4.dat
        - Navigate to Admin > System, use the System Update button, and browse and select the update file.

    b. Or using the Command Line Interface (CLI):
        - File= CiscoCyberVision-update-center-4.1.4.dat
        - Launch the update with the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-center-4.1.4.dat
```

2. Update the sensors:
    a. Hardware sensors:
        i. If you used the combined file to update the Center which owned the sensor and the SSH connection from the Center to the allowed sensor, the hardware sensors (Cisco IC3000 and Sentryo SENSOR's) were updated at the same time.
        ii. If the Cisco IC3000 sensor was deployed using the sensor management extension, it can be upgraded by deploying it again.
        iii. If not, the update needs to be done from the Command Line Interface (CLI):
            - File= CiscoCyberVision-update-sensor-4.1.4.dat
            - Launch the update with the following command:

```
sbs-update install /data/tmp/CiscoCyberVision-update-sensor-4.1.4.dat
```

    b. IOx sensors:
        i. If you have installed the sensors with the sensor management extension, first upgrade the extension itself and then all sensors will have to be updated.
            - File = CiscoCyberVision-sensor-management-4.1.4.ext
            - Navigate to Admin > Extensions. In the Actions column, use the update button and browse to select the update file.

              The Cisco Cyber Vision sensor management extension can also be updated from the CLI with the command:

```
sbs-extension upgrade /data/tmp/CiscoCyberVision-sensor-management-4.1.4.ext
```

ii. All sensors need to be updated with the extension. To do so, access the sensor administration page, and use the menu “Manage Cisco devices” / “Update Cisco devices” or use the redeploy button. A complete procedure is available in the document (part “Cisco Cyber Vision new features and improvements”) or in all sensor deployment guides version 4.1.4 minimum.

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 Local Manager platform or from the Command Line Interface. This procedure is described in the corresponding sensors installation guides.

- IE3x00 and IR1101 files = CiscoCyberVision-IOx-aarch64-4.1.4.tar or CiscoCyberVision-IOx-Active-Discovery-aarch64--4.1.4.tar
- Catalyst 9300 and 9400 and IR8340 files = CiscoCyberVision-IOx-x86-64-4.1.4.tar or CiscoCyberVision-IOx-Active-Discovery-x86-64-4.1.4.tar.

Important remark regarding CiscoCyberVision-IOx-x86-64 sensor application update:

The sensor update through the Local Manager of a Catalyst 9300, 9400 or IR8340 files is not possible from a release 4.1.2 (or lower) to a release 4.1.3 (or higher) due to the addition of the rspan compatibility. The sensor application needs to be redeployed and the enrolment package uploaded again.

Guidelines here: **Cisco Cyber Vision Sensor Application for Cisco Switches Installation Guide, Release 4.1.3**

AWS and Azure Centers

In case of a Center deployed in AWS or Azure, follow the same procedure described with one Center hereabove.

Cisco Cyber Vision 4.1.4 important changes

Command line access

In 4.1.0, a major change regarding the Center Command Line Interface (CLI) access through serial console or SSH was made. The user root is no more usable to establish the connection. A new user called ‘cv-admin’ must be used. This user has limited rights and many CLI commands will require permission elevation:

- prefix the command with "sudo".
- or open a root shell using "sudo -i" and enter the command.

Communication port and protocol changes

Port

No modification in 4.1.4.

Protocol

No modification in 4.1.4.

API

No modification in 4.1.4.

SYSLOG

No modification in 4.1.4.

Cisco Cyber Vision new features and improvements

DPI improvements for roadways

New protocols added in the solution:

- HP, MikroTik discovery
- Wavetronix Z1
- RTSP
- Kistler KiTraffic (inspection only)
- 2070 OS/9 telnet login prompts
- MQTT
- SCATTS
- Q-Free/Intelight Maxtime/Maxview traffic intersection control system (from HTTP)
- Connected vehicule (V2X) traffic between Cohda RSU and TMC over DSRC link: SPaT and MAP messages
- RTP video streams
- Axis camera HTTP traffic

Improved protocols:

- CDP
- LLDP
- SNMP
- NTCIP

Several tags related to transportation protocols were added.

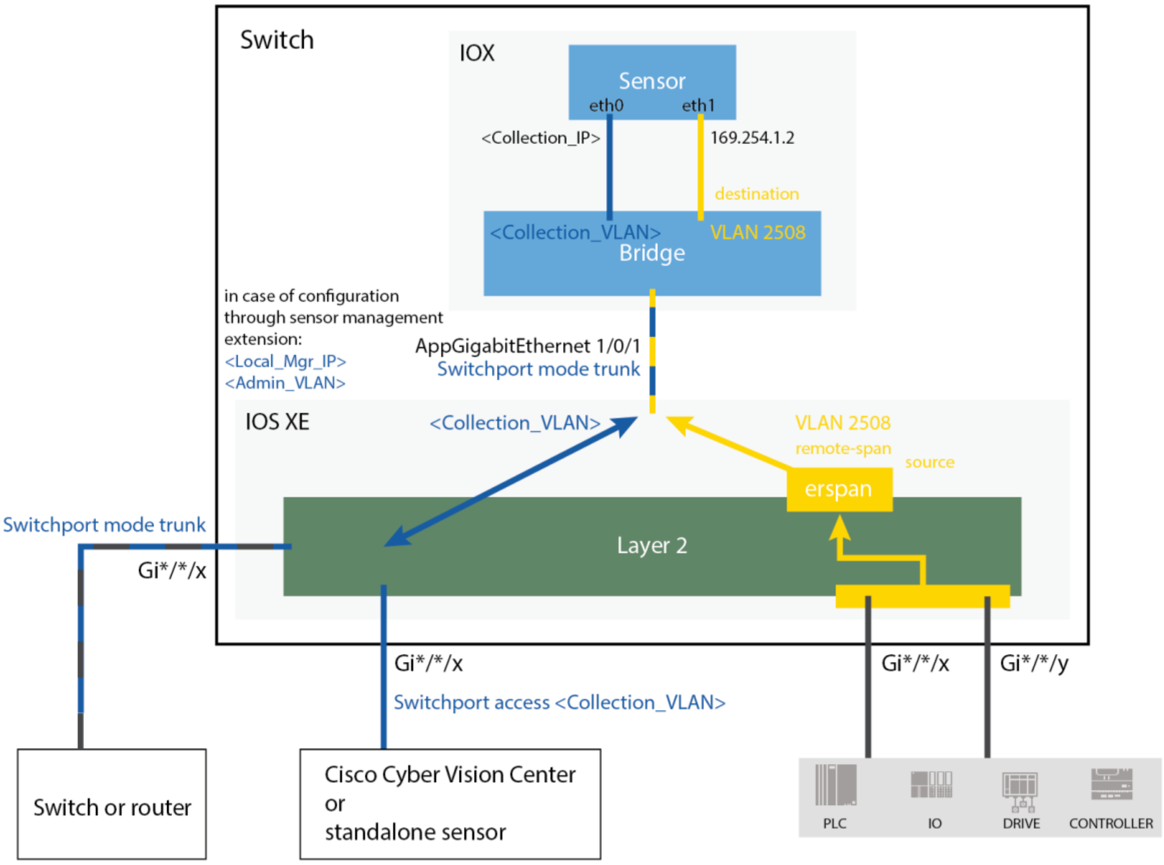
Family	Tag Name	Tag Description
System tag	ITS - Roadway	Intelligent transportation system (ITS) are systems in which information and communication technologies are applied in the field of road transport, including infrastructure, vehicles and users, and in traffic management and mobility management, as well as for interfaces with other modes of transport. Source: https://en.wikipedia.org/wiki/Intelligent_transportation_system
Component Tag	ITS Census	ITS Traffic Census Sytems which gives information across the entire transportation network.
Component Tag	ITS 2070 Controller	2070 Control unit
Component Tag	ITS Actuated traffic Signal Controller	as per NTCIP 1202 it design units part of Traffic Signal Controller systems. source : https://www.ntcip.org/document-numbers-and-status/
Component Tag	ITS CCTV Switching	as per NTCIP 1208. ITS Specifics CCTV switching systems.

Family	Tag Name	Tag Description
Component Tag	ITS Camera	as per NTCIP 1205 ITS CCTV systems.
Component Tag	ITS Data Collection and Monitoring	as per NTCIP 1206. ITS Data Collection and Monitoring systems.
Component Tag	ITS Dynamic Message Signs	as per NTCIP 1203, units part of road message signs systems
Component Tag	ITS Electrical and Lighting Management System	as per NTCIP 1213 ITS Electrical and Lighting Management System
Component Tag	ITS Environmental Sensor Station	as per NTCIP 1204. ITS Environmental Sensor Station units.
Component Tag	ITS HAR	Highways advisory radio
Component Tag	ITS LUMS	Lane Use Management Signs (LUMS) could be • Variable Speed Limit Signs (VSLS) • Electronic Speed Limit Signs (ESLS) • School Zone Signs • Integrated Speed & Lane Use Signs (ISLUS)
Component Tag	ITS Radar	vehicle detector units.
Component Tag	ITS Ramp Meter Control	as per NTCIP 1207, unit part of road ramp metering system.
Component Tag	ITS Roadside Units	as per NTCIP 1218 ITS Roadside Units
Component Tag	ITS Signal Control and Prioritization	as per NTCIP 1211 ITS Signal Control and Prioritization systems
Component Tag	ITS Signal System Master	as per NTCIP 1210l ITS Signal System Masters systems
Component Tag	ITS Transportation Sensor System	as per NTCIP 1209 Units part of road traffic counting and monitoring sensors
Flow Tag	ITS DSRC	ITS DSRC Message used for V2X communication (SAE J2735) ie MAP/SPAT messages

Sensor IOx in a Cisco Catalyst IE9300 Rugged Series Switches

In releases 4.1.4, Cisco Cyber Vision Sensor could be installed on a Catalyst IE9300. Sensor setup in this platform is detailed in the following documentation: Cisco Cyber Vision Sensor Application for Cisco Switches Installation Guide, Release 4.1.3.

Cisco Cyber Vision sensor in a IE9300



Cisco Cyber Vision Resolved Caveats

CDETS	Description
	KDB import gives some sbs-backend errors (11418)
	Preset list in main explorer page and drop-down lists should be properly sorted (11372)
	Minimap at component/device level doesn’t have a limit of displayed objects (11366)
	Add automatic cleaning of active discovery tasks (11358)
	Expired flow tables are never deleted (11328)
	sql.gz import from the GUI often causes Center to hang (10992)
	Fix Admin menu discrepancies between V3 and V2 (10989)
	Center IDS license expiration not evident from licensing page (10915)
	PCAP Upload: Snort error when uploading a capture from UI (10780)
	Extend Monitor Mode Syslog Messages (10767)
	"See technical sheet" link broken for port scan events (10695)
	Vulnerability list: counter do not match number of row (10595)
	CoDeSys DPI not working with some customers PCAP (9572)
	Home page: Info popup remain on the screen on Operational overview to Security overview (10987)
	HSR/PRP failure detection error (11279)
	Misleading message when acknowledging all differences in monitor mode (11364)
	Backend, burrow and ted stuck after a kdb update (11511)
	“Unnamed components” after uploading PCAP (11534)
	Netbios name is not updated when traffic with the new name is observed for an existing component (11675)
	Crash when license is not set in backend (11680)

Cisco Cyber Vision Open Caveats

Issues ID / CDETS	Component	Description
CSCwb12630	Center + ISE	All components are not synchronized with ISE
CSCvy57108	Center	Linux computer incorrectly tagged as Windows
CSCwd39017	Center	Missing information in the Smart License Usage

Links

Software Download

The files below can be found at the following link:
https://software.cisco.com/download/home/286325414/type

Center	Description
CiscoCyberVision-center-4.1.4.ova	VMware OVA file, for Center setup
CiscoCyberVision-center-with-DPI-4.1.4.ova	VMware OVA file, for Center with DPI setup
CiscoCyberVision-center-4.1.4.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-sensor-management-4.1.4.ext	Sensor management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-4.1.4.tar	Cisco IE3400, Cisco IE3300 10G, Cisco IE9300, Cisco IR1101 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64--4.1.4.tar	Cisco IE3400, Cisco IE3300 10G, Cisco IE9300 Cisco IR1101 Active Discovery sensor installation and update file
CiscoCyberVision-IOx-IC3K-4.1.4.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.1.4.tar	Cisco Catalyst 9x00 and Cisco Catalyst IR8340 sensor installation and update file
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.1.4.tar	Cisco Catalyst 9x00 and Cisco Catalyst IR8340 Active Discovery sensor installation and update file
Updates	**Description**
CiscoCyberVision-Embedded-KDB-4.1.4.dat	KnowledgeDB embedded in Cisco Cyber Vision 4.1.4
CiscoCyberVision-update-center-4.1.4.dat	Center update file for upgrade from release 4.0.x or 4.1.x to release 4.1.4
CiscoCyberVision-update-sensor-4.1.4.dat	Cisco IC3000 Sensor and Sentryo Sensor3, 5, 7 update file for upgrade from release 4.0.x or 4.1.x to release 4.1.4
CiscoCyberVision-update-combined-4.1.4.dat	Center, IC3000 Sensor and Legacy Sensor update file from GUI for upgrade from release 4.0.x or 4.1.x to release 4.1.4

Cisco Cyber Vision Center 4.1.4 can also be deployed on AWS (Amazon Web Services) and Microsoft Azure.

The Cisco 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

The Cisco Cyber Vision Center Plan can be found on the Microsoft azure marketplace:

https://azuremarketplace.microsoft.com/en-us/marketplace/apps/cisco.cisco-cyber-vision?tab=Overview

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.html
- Cisco Cyber Vision GUI Administration User Guide:

  Cisco_Cyber_Vision_GUI_Administration_Guide.html
- Cisco Cyber Vision Architecture Guide

  Cisco Cyber Vision Architecture Guide
- Cisco Cyber Vision Active Discovery Configuration Guide

  Cisco Cyber Vision Active Discovery Configuration Guide
- Cisco Cyber Vision Sensor Application for Cisco Switches Installation Guide:

  Cisco Cyber Vision Sensor Application for Cisco Switches Installation Guide
- 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
- Cisco Cyber Vision Network Sensor Installation Guide for Cisco IR8340:

  Cisco_Cyber_Vision_Network_Sensor_Installation_Guide_for_Cisco_IR8340
- Cisco Cyber Vision Center Appliance Installation Guide:

  Cisco_Cyber_Vision_Center_Appliance_Installation_Guide
- Cisco Cyber Vision Center VM Installation Guide:

  Cisco_Cyber_Vision_Center_VM_Installation_Guide
- Cisco Cyber Vision Center AWS Installation Guide:

  Cisco Cyber Vision for AWS Cloud Installation Guide
- Cisco Cyber Vision Center Azure Installation Guide:

  Cisco Cyber Vision for Azure Cloud Installation Guide
- Cisco Cyber Vision Integration Guide, Integrating Cisco Cyber Vision with Cisco Identity Services Engine (ISE) via pxGrid:

  Integrating-Cisco-Cyber-Vision-with-Cisco-Identity-Services-Engine-via-pxGrid_3_1_1.pdf
- Cisco Cyber Vision Smart Licensing User Guide

  Cisco_Cyber_Vision_Smart_Licensing_User_Guide