Doc type
Public

Cisco Cyber Vision Release Notes, Release 5.1.x

January 2025

© 2025 Cisco and/or its affiliates. All rights reserved.

Contents

© 2024 Cisco and/or its affiliates. All rights reserved.

© 2024 Cisco and/or its affiliates. All rights reserved.

Introduction to Cisco Cyber Vision

Cisco Cyber Vision helps industrial organizations improve operational resilience by providing continuous visibility into operational technology (OT) security posture. Cisco Cyber Vision equips you with the required insights to build secure industrial networks, reduce downtime, and enforce cybersecurity policies through seamless integration with the IT security operations center. Cisco Cyber Vision enables easy deployment within an industrial network.

Cisco Cyber Vision offers the following capabilities:

- Unmatched visibility on all assets connected to the industrial network, including their detailed profiles and communication patterns.
- Enhanced view of the OT security posture, including asset vulnerabilities, risk scores, intrusions, malicious activities, and abnormal behaviors.
- Automated network segmentation by grouping assets into zones, and sharing this information with Cisco Secure Firewall or Cisco ISE for enforcement.
- Reporting to help stakeholders implement security best practices and drive compliance with industry standards and regulations.
- Extends IT security operations to OT by integrating with security, network management, or any custom tool. Cisco Cyber Vision helps provide rich context on OT assets and communication activities to help gain a unified view of both IT and OT domains.

Cisco Cyber Vision Documentation

- Cisco Cyber Vision Admin Guide, Release 5.1.x
- Cisco Cyber Vision Upgrade Guide, Release 5.1.x
- Cisco Cyber Vision Active Discovery Configuration Guide, Release 5.1.x
- Cisco Cyber Vision Network Sensor Installation Guide for Cisco IC3000, Release 5.1.x
- Cisco Cyber Vision Network Sensor Installation Guide for Cisco IR8340, Release 5.1.x
- Cisco Cyber Vision Network Sensor Installation Guide for Cisco IR1101 and IR1800, Release 5.1.x
- Cisco Cyber Vision Sensor Application for Cisco Switches Installation Guide, Release 5.1.x
- Integrate Cisco Cyber Vision with Cisco Identity Services Engine (ISE) through pxGrid, Release 4.4.1 and Later Releases
- Cisco Cyber Vision Center Appliance Installation Guide, Release 4.4.0 and Later
- Cisco Cyber Vision Center VM Installation Guide, Release 4.4.0 and Later
- Cisco Cyber Vision for Azure Cloud Installation Guide, Release 4.4.0 and Later
- Cisco Cyber Vision for the AWS Cloud Installation Guide, Release 4.4.0 and Later
- Cisco Cyber Vision syslog notification format Configuration Guide

© 2024 Cisco and/or its affiliates. All rights reserved.

What's New in Cisco Cyber Vision Center Release 5.1.1

The Cisco Cyber Vision Center Release 5.1.x series begins with the release 5.1.1.

Deploy sensors using docker containers

You can now deploy Cisco Cyber Vision sensors using docker containers. Cisco Cyber Vision supports dockers running on Linux OS, specifically, Ubuntu releases 20.04, 22.04, and 24.04.

Device inventory report

The Device Inventory Report is an automated summary that captures data related to devices, their risk profiles, and the inventory distribution summary for a chosen preset.

Zone and conduit visualization

Cisco Cyber Vision limits the number of displayed objects to maintain performance and prevent browser issues. You can now view only top-level groups (zones) and summarized activities (conduits). The new map feature aligns zones and conduits with ISA/IEC 62443 standards.

Certificate renewal enhancement for sensors

Cisco Cyber Vision certificates are valid for two years and sensor certificates are now renewed automatically. The renewal process begins 35 days before certificate expiration. If the first attempt fails, the renewal process is initiated again later. If a certificate is not renewed before it expires, communications are interrupted until the renewal is complete.

Monitor ingestion chain follow-up

The service status page shows whether all Cisco Cyber Vision processes and extensions are running smoothly, and ensures that the data queues from sensors are not congested.

Port range entry in sensor templates

When you create a sensor template, you can now enter a range of continuous port numbers in the port mapping window.

New API for bulk acknowledgment of vulnerabilities

A new API is introduced to allow the bulk acknowledgment of vulnerabilities. To view the new API, in your Cisco Cyber Vision center, go to **Admin** > **API**.

Integrations removed

Cisco FTD is no longer supported. Cisco Firepower Management Center (FMC) is not supported as a direct integration. The Cisco Secure Dynamic Attributes Connector (CSDAC) integration can pass dynamic object attributes to Cisco FMC.

GUI enhancements

The Cisco Cyber Center UI pages for policy creation and licensing contain some visual changes. The functionalities and workflows remain unchanged.

OMRON protocol revamped

OMRON DPI is updated to standardize the protocol in alignment with other Cisco Cyber Vision protocols.

Active Discovery: New protocols added

- MMS unicast scanner
- BACnet broadcast scanner

© 2024 Cisco and/or its affiliates. All rights reserved.

Beta UI

Cisco Cyber Vision Center offers a beta UI experience, with informative, easy-to-handle dashboards that present data on assets, vulnerabilities, alerts, and organization hierarchies. You can quickly apply data filters to view necessary information.

This UI experience is a beta feature. To access the beta UI and its features, write to cv-beta@cisco.com. You will receive the command to enable the Cisco Cyber Vision Beta UI in addition to the existing classic UI.

You can also configure functional groups in the beta UI, and assign data sources to organization hierarchies.

To configure network definitions, sensors, and PCAPs, you must continue to use the classic UI. The overall task flows of Cisco Cyber Vision are currently spread across the classic and beta UIs, with the beta UI offering enhanced visualization of the center's data.

Asset visibility

The beta UI offers asset visibility, where assets refer to any physical machine of the industrial network such as a switch, an engineering station, a controller, a PC, a server, and so on. The **Asset Visibility** page allows you to filter assets by organizational hierarchy, data sources, and functional group assignment. You can also delete assets from the **Asset Visibility** page.

Functional group recommendations

Cisco Cyber Vision can analyze the network communication characteristics of assets that aren't already assigned to a functional group, and suggest a functional group assignment. In the **Cyber Vision Center Beta** UI, choose **Configuration** > **Functional Groups**, and click **Start Asset Clustering** for AI-generated grouping recommendations. You can review the recommendations and then accept or discard them.

Vulnerabilities

The Common Vulnerability Scoring System (CVSS) model is used to evaluate the score of vulnerabilities. The CVSS score ranges are:

- **0.0**: None
- **0.1–3.9**: Low
- **4.0–6.9**: Medium
- **7.0–8.9**: High
- **9.0–10.0**: Critical

You can filter and sort assets by vulnerability score in the beta UI dashboard.

Alerts

In the **Alerts** page, you can filter alerts for assets by organization hierarchies, data sources, and functional groups. The alert category **Critical vulnerabilities in monitored entities** is persistently displayed in the alerts page. The count of alerts for the category varies according to the filters used on the page.

A readily available out of box alert rule creates alerts for CVSS scores of 9 and greater. You can edit this rule or create new rules to view alerts for CVSS scores of 7 to 10. Click **Critical vulnerabilities in monitored entities** for the list of alert rules.

© 2024 Cisco and/or its affiliates. All rights reserved.

After reviewing the asset details, you can remove an alert from the dashboard by acknowledging the vulnerability.

Communications list for assets

In the **Asset Visibility > Assets > Asset Detail > Communications** page, you can view a map of an asset's communication activity. You can assess an asset's overall communications, and filter by protocol to see any specific activity.

Other enhancements

Materialized views: performance improvements

To avoid any large requests on the database during navigation, preset data is pre-computed with the help of the materialized views feature. Materialized view requests were changed to improve performance. Preset data are now computed faster than before.

SNORT memory containments

SNORT now runs with some memory limits to avoid the consumption of all sensor memory.

Tags added for ignition SCADA

Some new components and activity tags have been created to highlight ignition devices and their communications.

Refresh service status in system statistics

You can now update service status in the **System Statistics > System Health** page of the Cisco Cyber Vision center.

Sensor label added to the response for sensor list API

Sensor label is now added in the response for the API to get sensor lists.

API enhacement: force sorting on another field when pagination is used

S API route GET answers have been changed to improve usability.

sbs-diag command: disk test option added to test performance

A new option is available for the CLI command sbs-diag to compute disk performance metrics.

Monitor sbs-services monitoring service

A new service, sbs-services monitoring, is added to the service monitoring task to notify you of any failure in the **Service Status** page (**System Statistics** > **System Health** > **Service Status**).

MTU of sensor management extension changed to 1400.

The MTU of sensor management extension has been revised to 1400.

Warning message for component limit changed

The warning messages regarding the maximum number of components have been improved. The maximum allowed limit for components is 150,000, and you receive warning messages for the following scenarios:

- When the number of components is close to the maximum limit, you are notified that the center will soon stop data ingestion to preserve the system.

© 2024 Cisco and/or its affiliates. All rights reserved.

- When the limit is reached, the center stops data ingestion.

Tracking license tokens in use for the current DB

New entries are available in the **Admin** > **License** page when the center runs in Evaluation Mode, without licenses, to estimate the count needed for each license.

Known limitations

Beta UI Vulnerability page does not display device details

If the timespan setting for a device is too short, vulnerability data for the device is not displayed. If click the vulnerability link for a device fails to display data, increase the timespan setting for the device.

Cyber Vision sensor self-update

- After a Cyber Vision sensor self-update process is complete, if a platform is restarted within 5 minutes of the update the sensor returns to the previous version.
- If a Cyber Vision sensor is first updated to version *n* using the self-update feature, then to version *n+1* with the sensor management extension, the sensor remains at version n.

Address reservation in DPI configuration

The docker reserves the first address of a defined network. You must not assign the first address when you configure the DPI interface in an Encapsulated Remote Switched Port Analyzer (ERSPAN).

Compatibility

Compatible Cyber Vision Centers

Table 1. List of centers compatible with Cisco Cyber Vision Release 5.1.1.

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
CV-CNTR-M6N Cisco UCS C225 M6N	Cyber Vision Center hardware appliance (Cisco UCS® C225 M6 Rack Server) - 24 core CPU, 128 GB RAM, Two or Four 1.6 TB NVMe drives
CV-CNTR-M5S5 Cisco UCS C220 M5	Cyber Vision Center hardware appliance (Cisco UCS® C220 M5 Rack Server) - 16 core CPU, 64 GB RAM, 800GB drives
CV-CNTR-M5S3 Cisco UCS C220 M5	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

Compatible Sensors

Table 2. List of sensors compatible with Cisco Cyber Vision Release 5.1.1.

Platform	Minimum Version	Recommended Version	Description
Cisco IC3000	1.5.1	1.5.1	Cyber Vision Sensor IOx application hosted in Cisco IC3000
Cisco Catalyst IE3400	17.3.x	17.6.7,	Cyber Vision Sensor IOx application hosted in Cisco

© 2024 Cisco and/or its affiliates. All rights reserved.

Platform	Minimum Version	Recommended Version	Description
		17.9.5, or 17.12.2	Catalyst IE3400 Industrial Ethernet switches
Cisco Catalyst IE3300 10G	17.6.x	17.6.7, 17.9.5, or 17.12.2	Cyber Vision Sensor IOx application hosted in Cisco Catalyst IE3300 Industrial Ethernet switches with 10GbE ports
Cisco Catalyst IE3300 Cyber Vision application hosting is supported only when the platform has 4GB DRAM. All 4GB units starting with Version ID (VID) from -06. Use the CLI command **show platform resources** and see the Max DRAM Size field to verify if the device has a 4GB memory.	17.11.x	17.12.2	Cyber Vision Sensor IOx application hosted in Cisco Catalyst IE3300 Industrial Ethernet switches
Cisco Catalyst IE9300	17.12.x	17.12.2	Cyber Vision Sensor IOx application hosted in Cisco Catalyst IE9300 Rugged Series switches running IOS 17.12 minimum
Cisco IR1101	17.3.x	17.6.7, 17.9.5, or 17.12.2	Cyber Vision Sensor IOx application hosted in Cisco IR1101 Series Industrial Integrated Services Routers
Cisco Catalyst IR1800 Cisco Catalyst IR1835 with IOS 17.15 supports up to 3GB of memory allocated to IOX.	17.15.1	17.15.1	Cyber Vision Sensor IOx application hosted in Cisco IR1800 Rugged Series Routers
Cisco Catalyst IR8300	17.9.x	17.9.5 or 17.12.2	Cyber Vision Sensor IOx application hosted in Cisco Catalyst IR8300 Rugged Series Routers
Cisco Catalyst 9300, 9400 (Cisco Catalyst 9400 requires IOS XE 17.5.1 minimum to deploy an IOX application without SSD)	17.3.3	17.6.7, 17.9.5, or 17.12.2	Cyber Vision Sensor IOx application hosted in Catalyst 9300, 9300L, 9300X, 9400 Series switches
Docker sensors	Ubuntu 20.04 and 22.04 Docker 27.0	Ubuntu 24.04 Docker 27.x	Cyber Vision Sensor Docker application

Compatibility between the centers and sensors

There is downward compatibility of one release between the global center and synchronized centers, and between centers and sensors.

If the global Center runs release N, it can manage synchronized centers that run releases N or N-1.

For example, a global center running release 5.0.0 can manage other centers running releases 5.0.0 or 4.4.x.

If a center runs release N, it is compatible with sensors running releases N or N-1.

For example, a center running release 5.0.0 can manage sensors running releases 5.0.0 or 4.4.x.

© 2024 Cisco and/or its affiliates. All rights reserved.

Fresh Installs and Upgrades

Install Cisco Cyber Vision

In the case of fresh installs, go to Cisco Software Central, and in the **Download and Upgrade** section, click **Access Downloads**. Use the search button to find Cyber Vision, choose **Cyber Vision Center**, and choose release 5.1.1.

From the list of software displayed, download the following:

1. One center OVA or VHDX file, depending on your network architecture.
2. Cisco Cyber Vision Sensor Management Extension
3. Cisco Cyber Vision Reports Management Extension

To install the Cisco Cyber Vision center, see the guide that applies to your architecture:

- Cisco Cyber Vision Center VM Installation Guide, Release 4.4.0 and Later
- Cisco Cyber Vision Center Appliance Installation Guide, Release 4.4.0 and Later
- Cisco Cyber Vision for Azure Cloud Installation Guide, Release 4.4.0 and Later
- Cisco Cyber Vision for the AWS Cloud Installation Guide, Release 4.4.0 and Later

To install the extensions:

Software type	GUI process	CLI process
Sensor Management Extension **Install this extension in connected centers, or in the single center in your network.**	1. In your Cisco Cyber Center, go to **Admin** > **Extensions**. 2. For the sensor management extention list item, click **Update.** 3. Upload the extension file that you downloaded from Cisco Software Central.	In the Cisco Cyber Vision center CLI, use the command: `sbs-extension upgrade --run /data/tmp/CiscoCyberVision-sensor-management-<LATEST-VERSION>.ext`
Reports Management Extension	1. In your Cisco Cyber Center, go to **Admin** > **Extensions**. 2. For the reports management extention list item, click **Update.** 3. Upload the extension file that you downloaded from Cisco Software Central.	In the Cisco Cyber Vision center CLI, use the command: `sbs-extension upgrade --run /data/tmp/CiscoCyberVision-report-management-<LATEST-VERSION>.ext`

Upgrade process considerations

If you are upgrading to Cisco Cyber Vision release 5.1.1 from an earlier release, see the Cisco Cyber Vision Upgrade Guide, Release 5.1.1.

Upgrade path

Table 3. Upgrade paths to Cisco Cyber Vision Center release 5.1.1

© 2024 Cisco and/or its affiliates. All rights reserved.

Current Software Release	Upgrade Path to Release 5.1.1
4.3.x, 4.4.x, 5.x.x	Upgrade directly to 5.1.1
4.2.x	Upgrade first to 4.3.0 then to 5.1.1
4.1.x	Upgrade first to 4.3.0, then to 5.1.1
4.0.x	Upgrade first to 4.1.4, then to 4.3.0, then to 5.1.1
3.2.4	Upgrade first to 4.0.0, then to 4.1.4, then to 4.3.0, then to 5.1.1
3.2.3 or earlier	Upgrade first to 3.2.4, then to 4.0.0, then to 4.1.4, then to 4.3.0, then to 5.1.1

Cisco Cyber Vision partition size

Cisco Cyber Vision Center system has two partitions, one for the system and one for data. The system partition size must be at least 1 GB for the upgrade process to complete successfully—a lower partition size results in upgrade failure.

If your Cisco Cyber Vision center runs 3.1.0 or earlier versions, the system partition may be 512MB which is insufficient to upgrade to Cisco Cyber Vision center release 4.4.0 and later. Contact the Cisco TAC team to get support with updating the system partition to 1 GB.

To check the system partition size of your Cisco Cyber Vision center, access the center CLI and use the command:

```
lsblk
```

Sentryo hardware and Cisco IC3000 sensors

If you are upgrading to Cisco Cyber Vision release 4.4.0 or later releases:

1. Sentryo hardware are not supported. Remove any connected Sentryo hardware before you start the upgrade process.
2. Cisco IC3000 sensors must run Cyber Vision center release 4.3.0 or later releases. If the Cisco IC3000 sensors connected to your Cisco Cyber Vision center run an earlier Cyber Vision release, upgrade them to 4.3.0 or later releases before you initiate the upgrade process.

Resolved Caveats

Bug ID	Summary
CSCwi22898	Http flow wrongly tagged as MarkVI
CSCwn78259	SNORT license authorization expiration creates issues with navigation to other pages
CSCwn27044	Events page does not auto refresh
CSCwn63473	User is able to create duplicate OH level names under a given hierarchy level
CSCwk99382	Cannot import webapp certificate using AES digest
CSCwm55931	Sensor extension update can be launched multiple times simultaneaously

© 2024 Cisco and/or its affiliates. All rights reserved.

Bug ID	Summary
CSCwm55930	Prevent uninstallation of sensor management extension in some cases
CSCwn38414	Preset vulnerabilities page content is not completely refreshed when the time SPAN settings changed.
CSCwj82522	Swagger - Create Baselines method wrong description
CSCwn11766	ERSPAN decapsulation error for some Cisco Sensor MAC
CSCwn38422	Search on IP does not return an ordered list of results or provide exact match pattern
CSCwn38420	Some MMS use cases miss firmware version if played without variables enabled at sensor side
CSCwn38418	CV beta new GUI: filter by type is not working
CSCwn38417	Remove " sensor manually created" event when uploading PCAP
CSCwn38415	Events: Not observed in the Center
CSCwj30844	Device-Engine: Tag " Network Switch" is assigned to a router
CSCwj45528	Limit SNORT memory usage
CSCwm57704	Admin Events - Cisco Cyber Vision Administration
CSCwk96566	Center DPI services are not monitored
CSCwk96565	SNOT can fail to start if interface is down
CSCwm84489	Sbs-diag: missing services
CSCwm91768	Flow panic in protocol reassembly with MMS

© 2024 Cisco and/or its affiliates. All rights reserved.