Cisco Cyber Vision Classic UI Administration Guide, Release 5.6.0

Cisco Cyber Vision
Updated September 8, 2026

Topics included

1 New and changed information....6

2 Introduction to Cyber Vision....8

Cisco Cyber Vision GUI....9
Interactive help....9
Manage interactive help....10
Presets....10
Preset views....10
Default preset categories....13
Create a new category....14
Create a new preset from an existing data set....15
Understanding concepts....15
Filters....16
Components....17
Devices....19
Activities....20
Flows....21
External communications....22
Time spans....22
Network tags....23
Properties....24
Vulnerabilities....25
Credentials....27
Variable accesses....28
Group hierarchies....30
Active Discovery....32
Navigate through Cisco Cyber Vision....33
Home....33
Detail Panel....35
Reports....37
Events....39
Monitor mode....40
Search....41
System statistics....42
Create your personal account....46
Risk scores....47
Review device risk score details....48
Risk score calculation and factors....48

3 Licensing....52
Cisco Cyber Vision licenses....53
Trial licenses for Cisco Cyber Vision....53
Essentials and advantage licenses....54
Licenses for Intrusion Detection System (IDS) components....54
Cisco Smart Software Manager satellite for air-gapped networks....55
Register the license for Cyber Vision Center....55
Use specific license reservation....56
Update specific license reservation....57
Return specific license reservation....58
Managed Services License Agreement....58
Configure utility mode for MSLA....59
License usage compliance....59

4 Get started with Cisco Cyber Vision....60
Data management operations....61
Caution: Understand the impact before clearing all data....61
Data storage and expiration settings....61
Purge components from the database....62
Expiration settings....63
Ingestion configurations....63
Users....64
User roles....65
Password requirements....65
Add a new user....66
Create a user role....66
Center web server certificates....67

5 Configure Cisco Cyber Vision....70
Network organization....71
Create network groups....71
API Token....72
Create an API token....73
API Documentation....73
Active Discovery policies....76
Access Active Discovery policies....76
LDAP....77
Configure LDAP....77
Single sign-on (SSO)....79
SAML single sign-on....80
Requirement: SSO configuration for Cisco Cyber Vision Center....80
Configure SAML SSO through a reverse proxy....81

Single sign-on user accounts....82
User role mappings for SSO users....82
Microsoft Entra ID single sign-on integrations....83
Duo Single Sign-On solutions....87
Sensors....91
Sensor Explorer....91
Sensor geolocation data....99
Deploying sensors with deployment tokens....101
Templates....103
PCAP files....105
Upload a PCAP file....105
SNMP monitoring information....106
Configure SNMP....107
SNMP MIB....108

6 Integrate with Cisco Cyber Vision....110
ISE pxGrid....111
ISE-API....111
XDR....111
Configure XDR....112
XDR Ribbon....112
XDR Event Integration....113
XDR component button....114
External resources for XDR integration....114
Secure Remote Access....115
Integrate Cisco Cyber Vision Center with SRA....117
Enable Cyber Vision Center as an SRA Gateway....117
Cisco In Product Support....118
Access Cisco In Product Support....119

7 Maintain and monitor Cisco Cyber Vision....122
Monitored presets....123
Create a baseline....123
Configure monitored presets....124
Manage monitored preset differences....124
Center shutdown/reboot....126
Upgrade with a combined update file....126
Syslog configurations....128
Configure syslog....128
Database import and export....129
Update the Knowledge DB....130
Certificate fingerprints....131
Disable Cisco Cyber Vision telemetry....131
Reset to Factory Defaults....132

Snort....132
Snort rulesets and rule categories....133
Snort rules management features....134
Enable IDS on a sensor....135
Risk Score....136
Cisco Cyber Vision extensions....136
Install an extension....136

1 New and changed information

This section lists new and changed features introduced in Cyber Vision release 5.6.0.

This table summarizes the feature updates and enhancements available in the Classic UI for the Cisco Cyber Vision 5.6.0 release.

Table 1: Feature updates

Feature	Description
Cisco Cyber Vision Center new UI is the default interface	Cyber Vision New UI is the default interface for Cisco Cyber Vision Center. When you sign in, Cyber Vision opens the new UI automatically. Click **Go to Cyber Vision classic** in the top banner of your Center to access the classic UI screens.
Read-only view of network organization	The Network Organization page provides a read-only view of the network organization. To define and manage networks, use the Network Definition page in the New UI. For more information, see Network organization on page 71
Sensor Management extension removal	The Sensor Management extension is no longer available. Sensors that were previously deployed through the Sensor Management extension are now fully managed from the Sensors Management page in the New UI. For more information, see Sensors on page 91
Functional groups are no longer supported	Cisco Cyber Vision New UI introduces Cyber Vision Segmentation and replaces functional groups with asset groups for segmentation workflows.

2 Introduction to Cyber Vision

Topics:

- Cisco Cyber Vision GUI
- Interactive help
- Presets
- Understanding concepts
- Navigate through Cisco Cyber Vision
- Risk scores

Outlines the fundamental aspects of Cyber Vision, including its GUI, interactive help management, preset and group configurations, concepts such as filters, devices, components, activities, flows, external communication, time span, tags, properties, vulnerabilities, credentials, variable accesses, and core platform features like active discovery.

Cisco Cyber Vision GUI

Introduces the Cisco Cyber Vision GUI, outlining real-time network visualization, collaborative management features, licensing and role-based access requirements, sensor enrollment prerequisites, and references to setup instructions.

A Cisco Cyber Vision GUI is a user interface component of the Cisco Cyber Vision platform that

- enables real-time visualization and management of industrial network data,
- provides access to platform features according to user rights and licensing, and
- supports collaborative actions that may affect or be visible to other users.

- Real-time visualization: The GUI lets you monitor network traffic and device status as events occur.
- Collaboration: When you perform actions in the GUI, other users with permission may see or be affected by these actions.

Requirements

- Your access to some features in the GUI depends on your license type and assigned role.
- You must enroll at least one network sensor for data to appear in the GUI.
- For setup instructions or installation prerequisites, refer to the relevant quickstart guides.

Table 2: Feature History Table

Feature	Release Information	Feature Description
New UI is the default interface	Release 5.6.x	Cyber Vision New UI is the default interface for Cisco Cyber Vision Center. When you sign in, Cyber Vision opens the new UI automatically. Click **Go to Cyber Vision classic** in the top banner of your Center to access the classic UI screens.

Interactive help

Introduces the interactive help feature in Cisco Cyber Vision, which provides contextual guidance, step-by-step walkthroughs for task flows, and access to documentation resources, while noting the collection of anonymous usage data for service optimization.

The interactive help feature is a user assistance tool that

- provides contextual guidance within Cisco Cyber Vision,
- offers easy access to a wide range of documentation resources, and
- provides step-by-step walkthroughs for selected task flows.

Cisco may collect certain anonymous product usage data as described in the End User License Agreement and the Privacy Statement to optimize delivery of Interactive Help.

Users can access interactive help in Cisco Cyber Vision to quickly find instructions or guidance relevant to their current task.

Manage interactive help

Outlines procedures for enabling or disabling the Interactive Help feature to provide contextual user guidance in Cisco Cyber Vision, including access steps in different interface versions and plugin management by administrators.

Enable or disable the **Interactive Help** feature to assist users with guided support in Cisco Cyber Vision.

Interactive help provides users with contextual assistance and guides within the Cyber Vision interface.

Interactive Help is enabled by default.

Procedure

1. In the Classic UI, click the **Interactive Help** ribbon.
2. In the New UI, click **?** icon and choose **Interactive Help**.
3. To disable **Interactive Help**, choose **Admin** > **System** and disable the **Interactive Help** plugin.

Depending on your configuration, Interactive Help is enabled to provide contextual user guidance, or it is disabled and no user guidance is shown.

Presets

Introduces presets for focused network metadata filtering, rapid access to business-specific views, and efficient navigation, including enhanced visualization of groups and subgroups on the Zones and Conduits Map to monitor device communications and boundaries.

Presets are sets of selection criteria that

- enable focused filtering of network metadata processed by Cyber Vision,
- provide rapid access to views matching specific business needs, and
- offer multiple perspectives for efficient navigation of network data.

Presets are designed to simplify navigation and enhance business-oriented visibility into network activity and status, based on recommendations from Cyber Vision playbooks.

Table 3: Feature History Table

Feature	Release Information	Feature Description
Consistent Groups and Subgroups on the Zones and Conduits Map	Release 5.4.x	Easily visualize network communications to ensure devices remain within their designated boundaries. The system now supports one level of sub-zones within existing zones and conduits. You can quickly identify devices that should not communicate outside their networks.

Preset views

Introduces preset views, explaining how they store selected data elements, refresh upon user request to optimize performance, manage system workload, and describing their asynchronous behavior, update mechanisms, and impact on user experience and system resources.

A preset view is a display mode that

- stores data elements, such as components, tags, and activities,
- refreshes only when necessary or upon explicit user request to reduce system load, and
- optimizes system performance to prevent lags and application crashes, especially when managing large data flows.

Preset views help prevent system overload by showing previously computed data and relying on user actions for updates. This benefits users who interact with preset views frequently or occasionally.

Behavior of preset views

- The elements visible in preset views are based on the last completed computation.
- Data displayed in the user interface and database are asynchronous, lowering workload on the GUI.
- Computation frequency adapts to preset usage. Presets that are viewed frequently are recomputed often. Presets that are not used are skipped.
- An automated background process computes data when a preset is active, but does not auto-refresh the display.
- Two update buttons are available in preset views:
  - New data button: Appears when new computation is available, but the updated view may not show all new data.
  - Refresh button: Forces data computation and a full view refresh, which consumes more system resources. Use this when you expect changes, such as a new device or custom data updates.

Types of preset views

Outlines the available preset views, including Dashboard, Map, Device and Activity lists, Vulnerabilities, Security Insights, and Purdue Model, and guides you in accessing, filtering, and interpreting network data, vulnerabilities, and asset distribution within Cyber Vision Center.

You can access different preset views for various perspectives. To do this, open the main menu, select **Explore**, and use the top navigation bar to choose a preset.

Table 4: Views

Name	Description
Dashboard	The dashboard view appears by default and gives you a preset data overview. This tag-oriented view lets you quickly review the network at a high level.
Map	Use the map view to see how devices and components in your industrial network are connected. You can organize them into groups and explore the network structure. The map view then shows devices, components, and activity based on your selected criteria. It also shows grayed-out items if they are needed to represent preset activities, even if they don't match the criteria.
Device list and Activity list	Use these views to filter and find specific data. You can see both general and technical details for each element in the preset.

Name	Description
Vulnerabilities	This view displays and lists all vulnerabilities detected in a preset.
Security Insights	Each tab displays the most frequent requests, the least frequent requests, and a list of all requests for you to review. **Flows with no tag**: This section lists traffic that Cyber Vision Center cannot analyze, often due to the use of unsupported protocols. To resolve this, first verify that the content should be on the network. Next, determine why analysis is not possible. Finally, check flows with a high number of packets.
Purdue Model	Use the Purdue model view to see how assets in your preset are distributed across the layers of the Purdue model architecture based on tags. This view organizes assets into those layers: • Level 0–1: Process and basic control (IO Modules) • Level 2: Area supervisory control (PLCs, SCADA stations) • Level 3–4: Manufacturing zone and DMZ (all others)

Communication display options in map preset view

Outlines the three communication display options in Cyber Vision Center's map preset view, including viewing all device activities, aggregating activities by groups, and displaying only zones and conduits with support for sub-zones and ISA/IEC 62443 compliance.

Cyber Vision Center offers three options for presenting communications in the preset map view.

Table 5: Map view options

Option	Description
Show all activities	You can view all activities between groups or individual devices.
Aggregate activities by group	The system increases map readability by grouping and displaying communications between device groups.

Option	Description
Show only zones and conduits	To optimize performance with large data sets or to get a broad overview, show only top-level groups (zones) and summarized communications (conduits) between them. Devices not assigned to any zone appear in a separate group called **Ungrouped**. If group hierarchies segment the control system, the map displays zones and conduits that meet ISA/IEC 62443 standards. A conduit appears as a thick, dashed line and shows communication between two groups. If both the source and destination groups are known, an arrow indicates the direction of communication. By default, Conduits View mode is enabled. To disable it, select **Aggregate activities by group**. **Show sub-zones**: This map mode shows sub-zones embedded within zones. You can view communications involving sub-zones and communications between zones and sub-zones.

Default preset categories

Outlines the default preset categories in Cyber Vision, detailing available generic presets for data viewing, asset management, control systems monitoring, IT communication, security, and network management based on operational and recommended practices.

Generic presets are available by default in Cyber Vision, based on recommended practices and operational categories.

Table 6: Default categories

Preset category	Presets available
Basics	View all data or filter to information technology (IT) or operational technology (OT) components. • All data • Essential data • Active Discovery activities
Asset management	Identify and inventory assets associated with OT systems, facilities, and IT components. • OT devices • IT devices • IT infrastructure devices • All Microsoft Windows systems • All controllers

Preset category	Presets available
Control Systems Management	Check the state of industrial processes. • OT activities • Control system activities • Process control activities
IT Communication management	Flows categorized as OT, IT, infrastructure, IPv6 communications, and Microsoft flows • IT activities • Web activities • Email activities • File activities • Microsoft activities
Security	Remote access control and insecure activity monitoring • DNS activities • Remote procedure call activities • Remote access • Insecure activities • Encrypted activities • Authentication activities
Network Management	Network detection issue identification and resolution • IT infrastructure activities • IT technical activities • IPv6 communications • Multicast traffic only • Broadcast traffic only

Create a new category

Guides you through creating a new category to organize and locate custom presets, including steps for setup, editing, deletion, and searching within the Explore page.

Create a category to organize and locate your custom presets easily.

Use categories to order and search custom presets. You can bookmark entries saved on the **Explore** page with URL filters in your browser for quick access.

Procedure

1. From the main menu, choose **Explore**.
2. Click **New Category**.
3. Enter the name and preset details.
4. Click **Create**.

The new category appears on the **Explore** > **All Presets** page.

What to do next

- You can edit the category name and preset details or delete the category from **Explore** > **All Presets**.
- You can search for categories on the **Explore** page to view associated presets.

Create a new preset from an existing data set

Guides you through creating a customized preset from an existing data set by selecting filter criteria, naming and categorizing the new preset, and managing presets through the Explore page.

Create a customized preset by selecting criteria from an existing data set tailored to your business logic

Customized presets help you tailor views to your operational needs. Presets that you create are available to other users.

Procedure

1. From the main menu, choose **Explore** > **All Presets**.
2. Select a predefined data preset from the **All Presets** list.
3. Select the required criteria from **RISK SCORE**, **NETWORKS**, **DEVICE TAGS**, **ACTIVITY TAGS**, **GROUPS**, and **SENSORS**.
4. Click **Save as**.
5. Enter a new **Name** and select a **Category**.
6. Click **OK**.

Your new preset uses the filter criteria you selected and appears in the category you chose.

What to do next

- Search for the selected category on the **Explore** page to view the newly created preset with your filter criteria.
- You can edit or delete presets from the **Explore** page.

Understanding concepts

Guides users through core Cyber Vision concepts, including filters and their usage, component and device identification, activity and flow monitoring, external communications, time span configuration, tagging, properties, vulnerability detection and notification, credentials management, variable accesses, group hierarchies, conduits, and active discovery.

Describes the core concepts required to understand the system functionality.

Filters

Introduces filters as data visualization tools that refine dashboards and views by applying selection criteria, explains inclusive and exclusive logic, describes combining multiple filter categories, and outlines filtering sequence, including optional time-frame refinement in Cyber Vision.

A filter is a data visualization mechanism that

- enables users to refine and restrict datasets presented in dashboards and preset views,
- allows selection of devices, activities, or attributes using predefined criteria, and
- operates using inclusive or exclusive logic to control which data appears in each view.

Filters provide flexibility. They allow the combination of multiple categories, such as device tags, networks, and sensors, to produce precise visualizations. Applying different filter types helps focus analysis on specific risks, behaviors, and assets.

Filter combination

You can define filters in several categories simultaneously. The process first filters activities using all activity-based filters. Then, it filters devices using their specific criteria. This sequence results in the preset dataset that Cyber Vision uses to precompute your view. To further refine your dataset, select a time frame.

Use filters in the Cyber Vision Center

Guides you in using filters within the Cyber Vision Center to refine data views, narrow device or activity lists, and enhance analysis or monitoring in dashboards and preset views.

Use filters in the Cyber Vision Center to refine your data view.

Use filters to narrow the list of devices or activities for analysis or monitoring in dashboards and preset views.

Procedure

1. From the main menu, choose **Explore**.
2. From the navigation bar, select a preset from the preset category.

Filters become available for refining data visualization according to the chosen criteria.

Filter categories and usage options

Outlines filter categories and their usage options for organizing and viewing device and activity data, including filter types, application logic, special notes, and examples for refining dashboard and preset views.

Use filters to organize and view data about your devices and activities. Each filter helps you focus or expand the data shown in dashboards and preset views.

Table 7: Filter types

Filter type	Description
Risk score	Filters devices based on individual risk rating and supports both inclusive and exclusive ranges.

Filter type	Description
Networks	Filters based on device IP address ranges or VLAN IDs. Affects activities and devices with corresponding network attributes. The system selects activities with at least one device in the corresponding network. Only devices with at least one IP address in the network range are selected in device lists.
Device tags	Selects devices by tags using inclusive or exclusive rules. Combining tags broadens or narrows the results. Exclusive filters exclude all components with the selected device tags.
Activity tags	Filters activities with specific tags. Exclusive filtering hides activities only if all activity tags are excluded.
Groups	Filters devices by membership in groups or subgroups. Inclusive and exclusive logic applies. Activity selection requires at least one endpoint in a selected group.
Sensors	Filters based on the analyzing sensor using inclusive or exclusive rules.
Keyword	Searches devices by name, property, IP/MAC address, or tags.

Filter application logic:

- You can combine filters across multiple categories at once. The result is the intersection of all selected categories.
- When you apply both device and activity filters, you further refine datasets in dashboards or preset views.

Notes:

- Negative (exclusive) selections are not supported for multiple network filters in version 4.0.0.
- For activity tags, activities are included if at least one tag is selected. They are hidden only if all tags match the excluded tag set.

Examples:

- To remove both broadcast and ARP activities, select both tags for exclusion.
- Use device tag filters to restrict views to device types, such as controllers or HMIs. You can also see their communication partners on maps.

Components

Introduces filters as data visualization tools that refine dashboards and views by applying selection criteria, explains inclusive and exclusive logic, describes combining multiple filter categories, and outlines filtering sequence, including optional time-frame refinement in Cyber Vision.

A component is a network object that

- represents a physical or logical network endpoint such as a network interface, PC, SCADA station, broadcast, or multicast address,

- is detected through details such as MAC address and, if available, IP address, and
- is visually represented in the center by a specific icon, grouping, and border style.
- The center groups components within devices. In the UI, the components of a device appear together inside a bordered area in the drawer and on the technical sheet.
- The center displays components that are not assigned to a device with a double border.

Types of component icons

Introduces the various types of component icons used in the UI, explaining how each icon visually distinguishes component types such as manufacturers, device classes, public IPs, broadcast, and multicast, and describes how icons provide additional information in the map and component panel.

Component icons visually differentiate component types in the UI.

Table 8: Component icons

Icon type	Example image	Description
Manufacturer	  	facturer
SIEMENS PLC		A S7-300 PLC
		A Scalance X300 switch
Default cogwheel		Used when the manufacturer is undetected or icon not assigned
Public IP		Represents a public IP
Broadcast		Broadcast destination component
Multicast		Multicast destination component

Icons in both the map and the component's panel display the manufacturer, model, and additional component information.

Component detection in Cyber Vision

Outlines how Cyber Vision uses Deep Packet Inspection to detect network components, capturing attributes such as MAC and IP addresses, manufacturer, model, operating system, firmware, tags, and activity timestamps from communication flows.

Cyber Vision detects components from network activity using Deep Packet Inspection (DPI):

- Components are discovered by observing emissions or receptions on the network.
- Detection details include MAC address, IP address, manufacturer, and model. They also include operating system, firmware, tags, and activity timestamps.
- DPI inspects the communication flows between components to extract these attributes.

> **Note**
>
> MAC addresses correspond to physical network interfaces, while IP addresses depend on network configuration.

View component details

Guides you through viewing detailed information about specific components, including accessing technical details, analyzing activity for troubleshooting, and managing assets after discovering and aggregating components.

Display information about a specific component.

After you discover and aggregate components, access technical details as needed. Analyze activity to troubleshoot issues or manage assets.

Procedure

1. From the main menu, choose **Explore**.
2. Select the required preset from the preset category.
3. Select the relevant preset view.
4. Click the component count in **Devices**.
5. Select a component to display its details.

You see detailed component information in the drawer.

Devices

Introduces network devices in Cyber Vision, detailing how components are aggregated into devices using attributes and rules, simplifying management, inventory, and visualization, and providing examples of device representation and tagging in the application.

A device is a network entity that

- aggregates multiple components with similar properties,
- represents a physical machine in an industrial network, including a switch, engineering station, controller, PC, or server,
- and simplifies management, inventory, and data presentation within Cyber Vision.

Device aggregation details

- Devices aggregate components based on shared attributes such as IP address, MAC address, NetBIOS name, tags, and properties detected in network protocols.
- Aggregation logic uses rules, prioritizing attributes such as controller tags and brands to define device type and assign properties at the device level.
- Devices enhance application performance and make network visualization more effective by grouping related components under one entity.

Device representation examples

- When you click on a Schneider controller, a side panel opens to show its components grouped as a device.
- The list of a Rockwell Controller device components in Cyber Vision shows technical details like activity time, IP addresses, MAC addresses, and tags. If a “Controller” component is found, the device gets a “Controller” tag to define its type. Brand tags like “Rockwell Automation” may also be added if detected.

Device icons and visual indicators

Explains how device icons and visual indicators identify network devices, including icon types for recognition status and the use of red counter badges to display detected vulnerabilities.

Device icons and visual indicators help you identify your network devices.

- If a device has a double border, you see the manufacturer’s icon when the device is recognized, a specific model icon when it is known, or a default cogwheel when the device is unknown.
- The red counter badge on a device icon indicates the number of vulnerabilities detected for that device.

Activities

Explains how activities represent and visualize network communication between devices or components, including the display and interpretation of communication flows, mapping with arrows, and factors affecting activity visibility.

An activity is a network communications entity that

- represents the communications exchanged between devices or components,
- is represented as a connecting line or arrow that links devices or components, and
- encompasses multiple types of flows in both directions between components.

Network activity details

Activities let you see how devices or components in a network interact by showing their communication flows. The system updates the visual display depending on whether both the source and destination components are known. When possible, the mapping uses arrows.

Devices or components with no visible activity may still have communicated. The system detects a device or component only if it has participated in network activity. If you do not see visible activity, the other device or component may not be included in your current selection or preset filters.

View activity details on the map

Explains how activities represent and visualize network communication between devices or components, including the display and interpretation of communication flows, mapping with arrows, and factors affecting activity visibility.

Review detailed information about communications between your devices or components using the activity map.

Procedure

1. From the main menu, choose **Explore**.
2. Select the required preset in the preset categories.
3. Select the **Map** preset view.
4. Click the communication link between two devices or components.

   The details drawer appears and shows you information about the communication and the flows exchanged.

- You can review details such as
  - The date of the first and last communication
  - Details such as name, IP, MAC, group, and criticality
  - Flow tags, number of flows, number of packets, volume of data exchanged, and number of events

Flows

Introduces the concept of flows as network communication events, describes key flow properties, and explains how activities aggregate multiple flows between components or devices as visualized on the Map.

A flow is a network communication event that represents a single exchange of data between two system components or devices.

Flows can be analyzed for properties such as endpoints, ports, activity times, and tags.

An activity is a collection of flows that occur between two or more components or devices. The Map shows an activity using a line that links the relevant components or devices.

Access a flow

Guides you through accessing and viewing detailed information about flows, including their properties, source, destination, activity times, ports, and tags, as well as applying filters and exploring technical sheets for additional details.

You can view detailed information about a flow and its properties.

Procedure

1. From the main menu, choose **Explore**.
2. Select the appropriate preset and preset view.
3. Click a component or device on the map.
4. Open the technical sheet and select the **Activity** tab.
5. View the list of flows.

You see detailed information for each flow, including source, destination, ports, activity times, and tags.

What to do next

To manage many flows, apply filters to sort by component name, port, or tags. Choose a flow to view its technical sheet, where you can find additional properties and tags.

External communications

Explains how Cisco Cyber Vision identifies and tracks external communications between internal devices and outside entities, details the criteria for classifying IP ranges, and outlines visual indicators and data handling for external network interactions.

External communications are network interactions that

- occur between monitored network components or devices and external (non-monitored) components or devices,
- are logged and listed in Cisco Cyber Vision,
- are typically identified based on IP addresses that do not match private address formats.

External communication indicators

- By default, communications involving IP addresses outside standard private ranges are considered external. Private-format IPs are considered internal. If your industrial network uses public IPs for internal purposes, you can define which IP ranges are internal or external on the Network Organization administration page in Cyber Vision center.
- Components with external communications are shown with an icon bordered in orange. Devices are shown with a double orange border.
- External components and their flows are not stored or displayed to optimize system performance.

View external communications

Guides you in monitoring and reviewing external communications between internal devices and external endpoints using Cyber Vision, including identifying activity, viewing technical details, and optionally exporting the communication logs for security and activity tracking.

Monitor and review connections between internal devices and external endpoints for security and activity tracking.

Cyber Vision records external communications between network devices and outside endpoints. External devices and their flows are not tracked. This approach helps keep the interface clear and optimizes performance.

Procedure

1. From the main menu, choose **Explore**.
2. Select the appropriate preset and then select the **Map** preset view.
3. Select the component or device you want to review.

   Icons with an orange border (single or double) indicate external communications.
4. Click **External communications**.
5. Review the displayed list of external communications in the technical details.
6. (Optional) To save the data, click **Export to CSV**.

You can view and optionally export all logged external communications for the selected device or component.

Time spans

Introduces time spans as data viewing filters that let users focus on specific periods, customize historical or real-time monitoring views, analyze trends, detect anomalies, and investigate incidents across Cisco Cyber Vision.

A time span is a data viewing filter that

- enables users to focus on network activity during a specific period,

- determines which historical or real-time information is displayed in monitoring views, and
- helps users analyze trends, detect anomalies, or investigate incidents within the chosen interval.

Application of time spans in monitoring views

In Cisco Cyber Vision, time spans are applied throughout monitoring views to limit or expand the period of network data you analyze. This helps tailor data visualization for ongoing and retrospective investigation.

Set a time span for data visualization

Guides you through selecting and adjusting the time span for data visualization in Cisco Cyber Vision, including filtering network activity, using preset and custom periods, and troubleshooting situations when no data is displayed.

Select and adjust the period for which network data is displayed in Cisco Cyber Vision.

Use a time span to filter displayed network activity in the various preset views. This helps you focus on recent events, conduct historical analysis, or investigate specific incidents.

Procedure

1. From the main menu, choose **Explore**.
2. Select appropriate preset and preset view.
3. To set a time span, click the pencil icon.
4. To set the **TIMESPAN SETTING**, select a **Duration**, or define a custom period in the **Time window**.

   Note

   While configuring a **Time window**, if you do not select an end date, it defaults to the current date and time.

5. Click **OK**.
6. Click **Refresh** to update and display network data for the selected period.

The data view updates to reflect activity within the chosen time span.

What to do next

If no data is visible in the current view, the time span may be set to an interval when no activity occurred. If data is missing or the view is empty, adjust the time span.

Network tags

Introduces network tags as metadata used for categorizing and analyzing devices and activities, explains device and activity tag types and classification, and outlines usage for filtering, behavioral analysis, and organizing network data within industrial environments.

Network tags are metadata labels that:

- succinctly describe and categorize network components and activities,
- are visually denoted by icon color and description based on their category, and
- support network exploration, filtering, and behavioral analysis.

- Device tags: Device tags represent the functions and properties of a device or component. They are synthesized at both the component and device (aggregation) levels.
- Activity tags: Activity tags describe the protocols used in network flows. They are synthesized at both the flow and activity (group of flows) levels.

Tag classification and usage information

- Tags are added directly by the system automatically based on data received from the sensor.
- Tags are classified under categories in the filtering area.
- Device tag categories include levels such as "Device – Level 0–1" and "Device – Level 2."
- Device levels correspond to ISA–95 international standard definitions.
- You can set criteria for network views and filters by leveraging tags to organize and focus on relevant network data.
- In Monitor mode, use tags with port and flow properties to help define network behaviors inside industrial networks.

Tag types include IO Module, Wireless IO Module, and more.

Locate tag information in Cyber Vision

Guides you through locating, viewing, and analyzing tag information for devices, activities, or components in Cisco Cyber Vision to support management, filtering, and reporting tasks.

View and analyze the tags associated with devices, activities, or components in Cisco Cyber Vision.

Use this procedure to identify or review tag assignments for devices, activities, or components. This helps manage, filter, and report in your network environment.

Procedure

1. From the main menu, choose **Explore**.
2. Select the appropriate preset and preset view.
3. Select the relevant device, activity, or component.
4. Open the **Technical sheet**.
5. Click **Basics**, then **Tags**.

You can view and analyze the tags associated with the selected device, activity, or component.

Properties

Introduces properties in Cisco Cyber Vision, detailing their function as informational attributes for devices, components, and flows, their extraction and normalization, and their role in categorizing, tagging, and monitoring network behavior across protocols and vendors.

Properties are informational attributes that

- provide key details about a device, component, or flow (such as IP address, MAC address, hardware version, or serial number),
- are extracted or inferred from network traffic and device/computer identification, and
- may be normalized across all platforms or specific to certain protocols or vendors.

Application of properties

- Properties categorize and group devices, generate tags, and define network behaviors, especially in Monitor mode.
- When Cisco Cyber Vision supports new protocols, more protocol-specific and vendor-specific properties become available.
- The combination of properties and tags helps define and monitor behavior within the industrial network environment.
- Some properties apply to all devices and components. Others are unique to specific protocols or vendors and can change as support expands.

View properties

Guides you through locating and viewing the properties of devices and components in Cisco Cyber Vision using the Explore menu and technical sheet.

Locate and view the properties of your devices and components in Cisco Cyber Vision.

Procedure

1. From the main menu, choose **Explore**.
2. Select the preset and view required for your search.
3. Select a device or a component.
4. Click **Technical sheet**.
5. Under **Basics**, click **Properties**.

You see the properties grouped by type in the selected panel or technical sheet.

Vulnerabilities

Introduces vulnerabilities as security weaknesses in Cisco Cyber Vision, details how they are identified using the Knowledge database and security rules, and outlines severity measurement using the CVSS scoring system.

A vulnerability is a security weakness that

- is detected on a device or component,
- can be exploited by an attacker to perform unauthorized or harmful actions on a network, and
- may result from software flaws, misconfigurations, or unpatched components.

In Cisco Cyber Vision, vulnerabilities are identified by correlating device and component properties with security rules stored in the Knowledge database. These rules are sourced from computer emergency response teams (CERTs), manufacturers, and partner organizations such as Schneider and Siemens. When a device or component matches a rule from the Knowledge database, Cisco Cyber Vision registers a vulnerability.

> **Note**
>
> Always update the Knowledge database in Cisco Cyber Vision as soon as possible after notification of a new version. This helps protect your network against vulnerabilities.

Severity measurement

Cisco Cyber Vision uses a score based on the Common Vulnerability Scoring System (CVSS) to measure the severity of each vulnerability. This score reflects criteria such as ease of attack, potential impact, component criticality, and attack vector (remote or local), and ranges from 0 (least critical) to 10 (most critical).

Acknowledge a vulnerability for a device

Guides you through acknowledging a vulnerability for a device, including suppressing notifications, adding comments, and reversing the action if needed.

Suppress notifications and track when you have reviewed or addressed a vulnerability on a device.

Use this procedure when you have reviewed a reported vulnerability and do not want to receive further notifications for it on a specific device.

Before you begin

Make sure you have access to the device and can view vulnerabilities in the **Explore** menu.

Procedure

1. From the main menu, choose **Explore**.
2. Select the desired preset from the preset category.
3. Select the required preset view.
4. Click device.
5. Click the count for **Vulnerabilities** from the drawer.
6. Click the vulnerability you want to acknowledge.
7. Add a comment, then click **Acknowledge for the device**.

You stop receiving notifications about this issue for the device until you cancel the acknowledgement.

What to do next

Cancel the acknowledgement to reverse this action.

How vulnerability detection and event notification work

Outlines how Cisco Cyber Vision detects device vulnerabilities by matching device properties with Knowledge database rules, and describes the process of event notification for new, acknowledged, or resolved vulnerabilities.

Summary

Cisco Cyber Vision matches your device or component properties with rules in the Knowledge database to detect vulnerabilities. You receive notifications about new detections and status changes.

The key components involved in the process are:

- Knowledge database: Stores rules from computer emergency response teams (CERTs), manufacturers, and partners.

- Device and component properties: These are system-normalized details of devices or components.
- Cisco Cyber Vision detection engine: Correlates properties and rules to identify vulnerabilities.

Workflow

The process involves these stages:

1. Always update the Knowledge database in Cisco Cyber Vision as soon as possible after notification of a new version.
2. Cisco Cyber Vision checks device or component properties against the latest rules.
3. If a device or component matches a rule, Cisco Cyber Vision detects the vulnerability.
4. Cisco Cyber Vision generates an event to notify you for each vulnerable component.
5. Cisco Cyber Vision generates additional events whenever a vulnerability is acknowledged or resolved.

Result

You receive event notifications about new, acknowledged, or resolved vulnerabilities for your monitored network devices and components.

Credentials

Explains the use of credentials in network environments, highlights security risks of transmitting sensitive information, and outlines credential visibility on network monitoring platforms such as Cisco Cyber Vision.

A credential is a security element that

- includes logins and passwords exchanged between components over the network,
- sometimes carries sensitive information, such as plaintext passwords if unsafe, and
- may be visible on network monitoring platforms, thereby exposing them to anyone on the network.

Credential visibility on network monitoring platforms

Credential frames are extracted from network traffic using deep packet inspection. If credentials are visible in systems such as Cisco Cyber Vision, secure the underlying network protocols to prevent others on the network from accessing credentials.

View credentials for a component

Guides you through viewing detected credentials for a specific component in the system interface, including steps for access, prerequisite permissions, and interpretation of credential details such as protocol, username, password status, and exposure information.

Use this task to access and review credentials detected for a component, including protocol and user details.

Before you begin

Ensure you have appropriate access rights to view credentials for the desired component.

Procedure

1. From the main menu, choose **Explore**.
2. Select the desired preset and select the preset view.
3. Select the component device you want to review.

4. Click **Credentials** in the drawer to see detected credentials.

The Credentials panel displays the number of detected credentials, the transmission protocol, the associated username and password, and information about credential exposure. If any password appears in plain text, ensure it is secured, even if it is hashed in another location.

Variable accesses

Outlines how variable accesses are monitored and recorded in industrial systems, details the process for enabling variable data detection in Cisco Cyber Vision, and highlights the significance of access tracking for operational integrity and security auditing.

Variable accesses are process control monitoring records that

- track when devices, such as PLCs or data servers, read from or write to variables,
- record which component performed each access, and
- log the timestamp of each event for operational supervision and security auditing.

Table 9: Feature History Table

Feature	Release Information	Feature Description
Detect and process variable data	Release 5.3.x	Sensors capture and relay measurable variables, such as pressure or temperature, to Cisco Cyber Vision Center. Enable Variables Storage in the **Admin** > **Data Management** > **Ingestion Configuration** page of Cisco Cyber Vision Center. This allows the center to add the variables to the database for processing.

Significance of variable accesses

Industrial process equipment, like PLCs and OPC data servers, use variables to store values such as temperatures, control settings, or sensor readings. A variable access occurs whenever a system component reads or writes one of these values. Each access is associated with a specific variable name and a physical memory address on the equipment.

Monitor variable accesses to maintain process integrity. Unexpected writes can indicate an attacker attempting to influence equipment operation. Solutions like Cisco Cyber Vision automatically report detected variable accesses, helping operators identify unauthorized or abnormal activity.

Examples:

- Reading the temperature of an industrial oven from its PLC controller is a variable access.
- Writing a new temperature setpoint to the oven's PLC is also a variable access.
- Multiple controllers may access the same variable, as when one PLC reads a value that another PLC writes.

Variable accesses details

Outlines the variable accesses table fields and their meanings, and guides users on reviewing, sorting, and investigating variable activity on industrial network components for operational or security purposes.

The variable accesses table provides detailed information on each variable access detected on industrial network equipment. You can review, sort, and investigate variable activity for operational or security purposes.

Table 10: Fields in the variable accesses table

Field	Description
Variable name	The identifier or label of the variable accessed.
Type	Indicates whether access is READ or WRITE, but does not show the variable's value.
Component	Shows which device or system accessed the variable (for example, a PLC model or OPC server).
First accessed	The timestamp of the first access event for the variable by the component.
Last accessed	The timestamp of the most recent access for the variable by the component.

To locate variable access information

- To view more details about variable accesses, open the technical sheet for the component. For a focused view, select **Automation** or refer to PLC access reports.
- The component list view displays the total number of variable accesses per device. You can sort this list by the "var" column.
- For detailed information on a specific component's variable accesses, click the component.

Enable variable processing in a sensor template

Enables variable processing within a sensor template to allow the center to detect and collect measurable variables from network traffic for monitoring and analysis.

Variable processing enables the center to detect and collect measurable variables from network traffic for monitoring and analysis. Sensors identify these variables and return them to the center.

Before you begin

Enable **Variable Storage**.

1. From the main menu, choose **Admin** > **Data Management** > **Ingestion Configuration**.
2. Enable **Variable Storage** and save changes.

> **Note**
>
> **Variable Storage** is disabled by default.

Procedure

1. From the main menu, choose **Admin** > **Sensors** > **Templates**.

2. Locate the template and select **Edit** from the **Actions** column.

> **Note**
>
> You can also create a new template.

3. Locate the protocols with variable inspection capability.
4. Check the checkbox under the **Variable Processing** column.
5. Save changes.

After you complete the configuration, the center sends information to the sensors. The sensors process and identify the variables. You can view detected variables in the center.

What to do next

To view **Variable accesses** , choose **Explore** > **All Data** > **Device list**, select a device, click **Variable** in the drawer, then click **Automation**.

Group hierarchies

Introduces group hierarchies for organizing network devices and components, explains attributes and nesting structures, and outlines how groups support flexible grouping and data filtering in Cisco Cyber Vision.

A group hierarchy is a network organization method that

- allows nesting of groups within parent groups,
- enables layering and structured representation of devices and components, and
- facilitates flexible grouping based on user needs.

Filtering data using groups

You can use groups created in the system as criteria to filter data within Cisco Cyber Vision.

- Created groups are added to filters, helping to refine datasets and compose presets.
- Filtering by group improves data management and analysis.

Create and customize groups

Guides you through creating and customizing groups to organize devices and components, manage group hierarchies by location or type, and improve network visibility and administration.

Organize devices and components into a meaningful group to improve network management and representation.

Use groups to organize devices and components in a hierarchy by location, process, severity, or type. Nesting groups enables a more structured data representation.

Before you begin

Ensure your user account has Admin, Product, or Operator access.

Procedure

1. From the main menu, choose **Explore**.
2. Select the desired preset and preset view.
3. Select the devices or components to group.
4. Click **Manage selection**.
5. To create a new group, click **Create a new group with selection.**
6. Enter group details:
   - Under **Basic information**, provide the name, description, parent group, and industrial impact.
   - Under **Customization**, specify color and properties.
   - To add a custom property, click **Add new property**. Enter a **Label**, and specify a **Value**.
7. Click **OK** to create the group.

The system creates a customized group. This improves organization, visibility, and the management of devices and components.

What to do next

You can manage group hierarchies.

- To create new parent group, select groups and click **Create a new parent group** from the manage group icon.
- To move a group into another group, click **Move to existing group** from the manage group icon.
- To delete a group, select it from the preset view and click the delete icon in the drawer.

Group properties

Introduces group properties, including the use of 62443 standard classification labels and support for user-defined custom property labels to enhance group classification and organization.

Group properties allow you to store customized information about a group. This includes both standardized labels and user-defined labels.

- Predefined labels are aligned with the 62443 standard, which specifies security policies and requirements.
- Users can add custom property labels as needed for additional classification.

Lock groups

Guides you through locking groups to prevent changes to their composition, including steps to enable group locks, secure group structure, and restrict unauthorized modifications until the group is unlocked.

Prevent additions, removals, or deletion of a group to secure its structure.

Locking a group is useful when you want to freeze its composition and prevent any accidental or unauthorized changes. Once locked, you cannot add or remove components or delete the group until it is unlocked.

Procedure

1. From the main menu, choose **Explore**.
2. Select the desired preset, then choose **Map** view.

3. Select the group you want to lock.
4. Click the edit icon in the drawer.
5. Enable the lock option, then click **OK** to confirm.

The group is locked. ou cannot add components, remove components, or delete the group until you unlock it.

What to do next

If you need to make changes, unlock the group before editing its components or deleting it.

Conduits

Explains how conduits group devices and components for enhanced network visibility and simplified management.

A conduit is a network grouping mechanism that

- aggregates activity among related devices and components,
- enhances visibility into network interactions within the group, and
- simplifies monitoring and management of grouped resources.

Usage

Conduits enable you to combine multiple devices or components into a single group for tracking and analyzing network activity. With conduits, you can identify patterns, detect anomalies, and apply policies across all group members instead of configuring devices or components individually.

Active Discovery

Enforces data enrichment on the network by actively exploring traffic to identify components and gather reliable information. This optional feature improves visibility into devices that are not communicating frequently or have not been detected by passive monitoring.

Active Discovery is a feature that sends broadcast or unicast messages to targeted subnetworks or devices to accelerate network discovery and provide more reliable data than passive DPI. Returned responses are analyzed and tagged as **Active Discovery**.

- Enables data enrichment for components not detected by passive monitoring.
- Obtains information that is not frequently exchanged, such as firmware versions.
- Supports configurable execution, including fixed time intervals or one-time jobs.

Supported Protocols and Devices

The following table lists the protocols supported by Active Discovery for broadcast and unicast messaging.

Table 11: Supported Protocols

Broadcast	Unicast
EtherNet/IP	EtherNet/IP
Profinet	SiemensS7
SiemensS7	SNMPv2c
ICMPv6	SNMPv3

Broadcast	Unicast
ICMPv6	WMI

Active Discovery is available on the following devices:

- Cisco Catalyst IE3300 10G Rugged Series Switch
- Cisco Catalyst IE3400 Rugged Series Switch
- Cisco Catalyst IE9300 Rugged Series Switch
- Cisco Catalyst 9300 Series Switch
- Cisco Catalyst 9400 Series Switch
- Cisco IC3000 Industrial Compute Gateway
- Cisco IR8340 Integrated Services Router Rugged

Navigate through Cisco Cyber Vision

Describes the GUI navigation components within Cisco Cyber Vision, including the home screen, monitoring tools, reporting features, and system management settings. This guide assists users in effectively accessing dashboards, event lists, and configuration options.

Provides an overview of the Cisco Cyber Vision interface to help users locate and utilize key monitoring, reporting, and system administration features.

Home

Provides an overview of the Cisco Cyber Vision Center home page, which displays operational and security metrics for the industrial network. It also serves as the central navigation hub for accessing all primary system pages.

The Home page is a dashboard interface that provides a high-level summary of network activity and centralized access to system management tools.

- Operational Overview tab for protocol distribution and critical events.
- Security Overview tab for vulnerability and risk score analysis.
- Navigation bar for accessing core application modules.

Home Page Components and Navigation

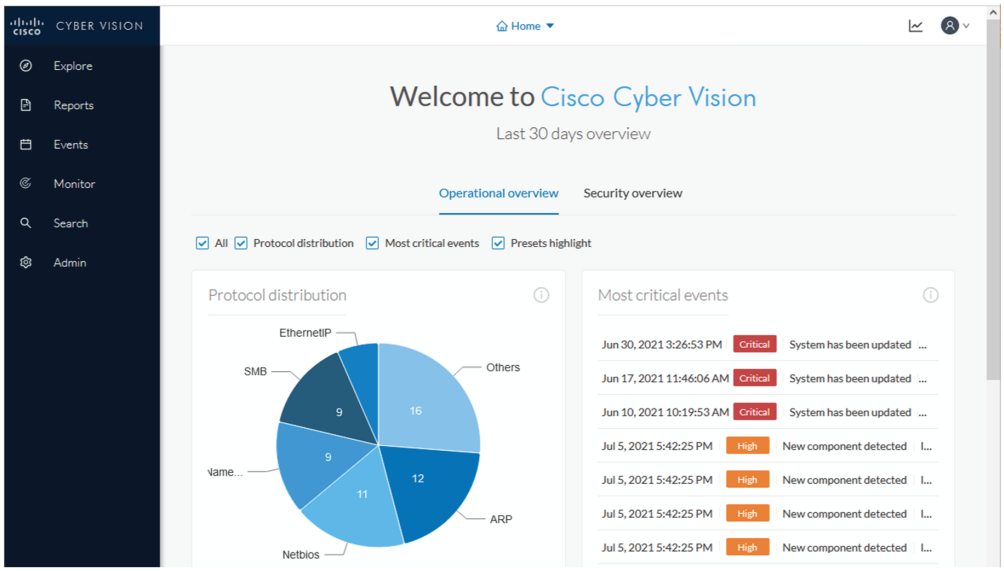
The home page is organized into two main tabs that allow users to monitor the industrial network over the last month.

The following tabs are available for monitoring:

- Operational Overview: Displays the **Protocol distribution** pie chart, a list of **Most critical events** , and **Preset highlights** .

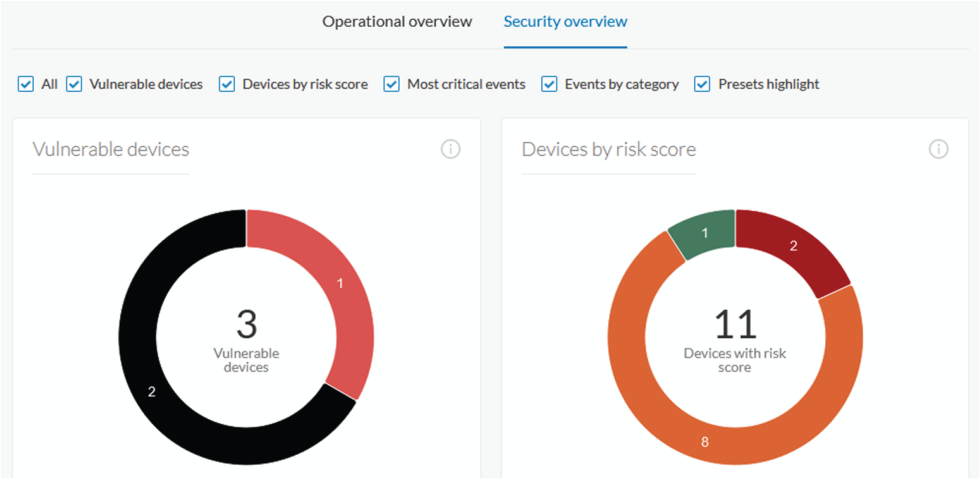
  Click **Edit favorite presets** to change what displays. Select the check boxes of the presets and click **Save**.

  Figure 1: Operational Overview



- Security Overview: Displays the **Vulnerable devices per severities** ring chart, the **Devices by risk score** ring chart, and lists for **Most critical events** , **Events by category** , and **Preset highlights**.

Figure 2: Security Overview



The navigation bar provides access to the following main pages:

- **Explore** : Shows the overview of all presets, by defaults or configured.
- **Reports** : Shows the Reports page to export valuable information about the industrial network.
- **Events** : Shows the Events page which contains graphics and a calendar of all events generated by .
- **Monitor** : Shows the Monitor mode on page 40 page to perform and automatize data comparisons of the industrial network.
- **Search** : Shows the searching area to look for precise data in the industrial network.
- **Admin** : Shows how to update the system, configure exports parameters, import and export the database, update the Knowledge DB and reset data and system settings.

Detail Panel

Provides a condensed view of information regarding a device, component, or activity without navigating away from the current background list or map. This panel allows users to quickly access specific element details and technical sheets.

A Detail panel is a condensed view about a device, a component, a group of components or an activity's information without changing the background device list or a map.

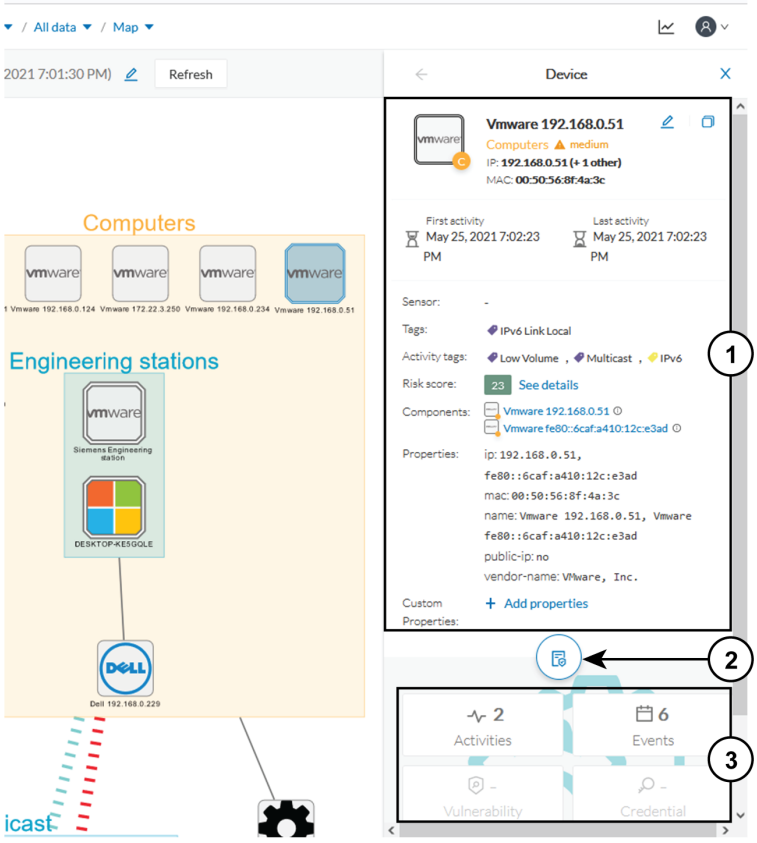
- Displays general information about the selected element.
- Provides editing capabilities for device or component names and group membership.
- Includes navigation buttons to access technical sheets and specific data categories.

Accessing and Using the Detail Panel

To access a detail panel, click a device, a component or an activity on the map or a list.

The detail panel layout includes the following components:

Figure 3: Detail Panel Interface



- Upper portion **(1)**: Provides general information about the element.
- Round button **(2)**: Opens the element's technical sheet with all relevant information.
- Rectangular buttons**(3)**: Redirect to the corresponding information inside the *technical sheet* .

Technical sheets

Introduces technical sheets as interactive documentation views that provide comprehensive information, display element-specific data dynamically, and enable direct interaction or editing for effective device, component, activity, or flow management.

A technical sheet is an interactive documentation view that

- provides comprehensive information about a device, component, activity, or flow,
- displays data differently based on the selected element, and
- allows direct interaction or editing within the sheet.

Technical sheets offer a unified interface for accessing, managing, and viewing element-specific information in the application.

Access a technical sheet

Provides instructions for accessing a technical sheet to view detailed and interactive information about a selected device, component, or activity within the application.

View the full details of a device, component, or activity by opening its technical sheet.

The technical sheet provides an interactive summary and detailed tabs for each element selected within the application.

Follow these steps to access a technical sheet.

Procedure

1. From the main menu, choose **Explore**.
2. From the top navigation bar, click the drop-down arrow of **All Presets** and select **All Data** from the drop-down list.
3. From the top navigation bar, click the drop-down arrow of the third filter and select **Map** from the drop-down list.
4. Click the **Technical sheet** icon.

The technical sheet for the selected device, component, or activity opens, displaying the relevant information and interactive functions.

Tabs in a device technical sheet

Outlines the interactive features and tab structure of the device technical sheet, including editing, grouping, and custom properties management, and describes the content and purpose of the Basics, Risk score, Security, Activity, and Automation tabs.

The device technical sheet contains relevant information and interactive functions. In a device or a component's technical sheet, you can also edit the element's name, add/remove it to/from a group, and add custom properties.

The top box of the technical sheet recaps the information found in the **Detail** panel. The rectangular buttons on the right redirect to the corresponding information inside the technical sheet.

The middle portion of the technical sheet contains tabs that vary based on the selected element. For a **Device** , the following tabs are available:

- **Basics** : Shows an element's properties, tags, and associated components.
- **Risk score** : Provides overview and detailed views of the risk assessment.
- **Security** : Displays component vulnerabilities and credentials.
- **Activity** : Shows activity flows, Mini Map , and external communications .

- **Automation** : Contains variable accesses.

Additional reference information is available for the following topics:

- properties
- tags
- risk score
- vulnerabilities
- credentials
- flows
- Mini Map
- external communications
- variables accesses

Access the mini map

Guides you to access the Mini Map for a specific device or component and view its activities.

Use this procedure to access the Mini Map.

The mini map is a visual representation restricted to a specific device or component and its activities.

Procedure

1. From the main menu, select **Explore**.
2. In the top navigation bar, click **All Presets**, and then select **All Data** from the drop-down list.
3. In the top navigation bar, click the third filter, and then select **Map** from the drop-down list.
4. Select a device from the map.
5. Click **Technical sheet** in the **Details** panel.
6. Click **Activity**.
7. Select **Show inner components** to view an exploded view of the devices.
8. Click any element in the **Mini Map**.

   The Detail panel opens, where you can access more information.

Reports

Introduces Cisco Cyber Vision reports, which export industrial network data for analysis, status reporting, and report customization.

A report is an export of industrial network data from traffic captured and processed by Cisco Cyber Vision.

Reports can uncover important information, such as sensitive entry points and acknowledged vulnerabilities for status reports.

Install the Reports extension to use the Reports page. From instruction to install the extension, refer to Install an extension on page 136.

Report data and formats

You can create reports from a Preset (default data) in Cisco Cyber Vision or from a custom one.

Reports extensions include `.docx` and `.pdf` formats.

Customize reports

You can add a logo, such as your company's logo, to customize a report. Reports display the Cisco logo by default.

Use the table of contents menu to set which content appears in the report.

Create a report

Guides you through configuring a report, generating it, accessing the output, downloading report versions, and generating a new version in Cisco Cyber Vision Reports Management.

Enable users to create custom reports, generate output, review results, and rerun or download reports as needed.

Before you begin

The Cyber Vision Reports Management extension and Cyber Vision Version must be the same to generate a report.

Only users with **Reports write** permission can create reports. Users with **Reports read** permission can download reports.

Follow these steps to create a report:

Procedure

1. From the main menu, select **Reports**.
2. Click **Create and run a Report**.
3. Enter a report name in **Name**.

   Optionally, enter a description in **Description**.
4. Select a report **Type**.

   The report types are:

   - **Security Posture**: An automated summary that captures all vulnerabilities, risky activities, and security events that Cisco Cyber Vision finds on the devices in the selected preset.
   - **Remote Access**: An automated summary that captures all Remote Access Gateways and Remote Access-related activities that Cisco Cyber Vision finds on the devices in the selected preset.
   - **Device Inventory**: An automated summary of devices, risk profiles, licensing requirements, and inventory distribution within the report scope.
5. Optionally, add a **Customer logo**.

   The logo appears on the report.

   > **Note**
   >
   > If you do not upload a customer logo, the default Cisco logo is used.
6. Select a format in **Format**, and then click **Next**.

7. Select a preset from **Preset**.
8. In **Table of content**, select the check boxes for the sections and subsections that you want to appear in the report.

   Note

   The available sections and subsections vary according to the selected report type.

9. Click **Save and Run**.

   The report appears with **Status: Processing**. When complete, the status changes to **Success** appears.

What to do next

After you generate the report, you can perform the following actions:

- To view and download a report, go to **Reports**, select the report name, and access download links in the **Details** panel. Older versions are listed under **Previous Reports**.
- To generate a new report, select … under the **Actions** column and choose**Run Again**.

Events

Introduces Events and explains how to access the Events page and manage event severity, Syslog export, and database storage.

An event is an activity, property, or change involving software or hardware components that helps you identify and track significant activities on the network.

Events include the following:

- A wrong password entered on the GUI.
- A new component connected to the network.
- An anomaly detected in Monitor Mode.
- A component detected as vulnerable.

The **Events** page is available to Admin and Product users. To access the **Events** page, go to **Admin** > **Events** from the main menu.

On the **Events** administration page, you can customize the severity of events. By default, changes apply only to future events. To apply new customized severities to past events, use **Apply severity to existing events**.

Important

This action is irreversible and can take several minutes to complete.

Select **Reset severity to default** to reset the severity settings.

Use the toggle buttons to enable or disable **Syslog export** and **Database storage**.

These options are active by default. Make sure that syslog is configured before export.

Events dashboard

Introduces the Events dashboard and its doughnut and line charts, which help you filter event data, review severity information, and access details for specific dates.

The Events dashboard is a dashboard that shows event doughnut and line charts.

Doughnut charts display color-coded event severity categories and percentages.

Doughnut charts present event numbers and percentages by category and severity.

Events dashboard filters

The Events dashboard can be accessed by selecting **Events** from the main menu. You can view the list of events for a category. For more information, refer to Events.

Use the filter in the top-right corner of the Events page to filter events by **Day**, **Week**, **Month**, or **Year**.

Use the arrows for specific dates.

Doughnut chart details

The doughnut chart opens in List view, filtered by the corresponding category and severity. This view lets you quickly access more event details.

Events graph

The Events graph appears at the bottom of the dashboard page.

Use the filter in the top-right corner to view data by **Day**, **Week**, **Month**, or **Year**.

Hover over event markers on the line chart to view event counts by category for specific dates. The **Cisco Cyber Vision Operations**, **Inventory Events**, and **Security Events** tabs provides additional details.

Access the event list

Provides instructions to access the event list and view details for individual events.

List is a chronological view in which you can view and search events.

Use the **search bar** to find events by MAC and IP addresses, component name, destination and source flow, severity, and category.

You can search events by **Day**, **Week**, **Month**, or **Year**. Use the **arrows** for exact dates.

Follow these steps to access event list.

Procedure

1. From the main menu, choose **Events** > **List**.
2. Click an event result to view more details about the event.
3. When an event is related to sensors, click **See Sensor Statistics** for more details.
4. When an event is related to a component or an activity, click **see Technical Sheet** for more details.

Monitor mode

Introduces Monitor mode, a Cisco Cyber Vision tool that detects changes in industrial networks and presents behavior changes in preset-based views.

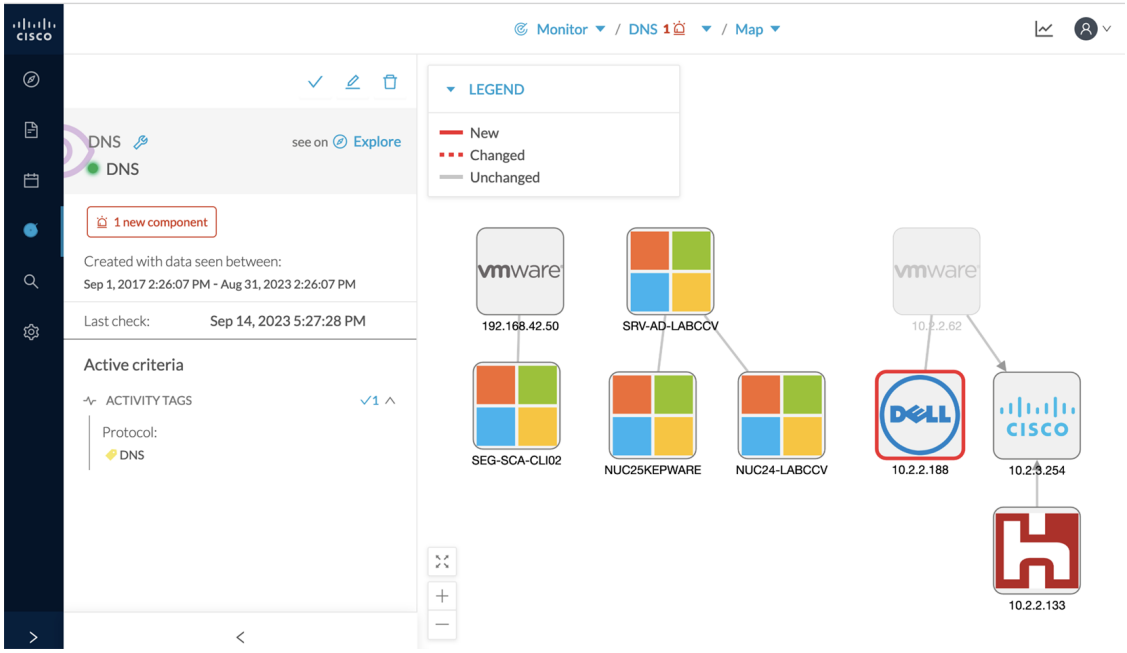
The Monitor mode is a monitoring tool in Cisco Cyber Vision that detects changes inside industrial networks. It shows the evolution of a network's behaviors, predicted or not, based on presets.

Because a network architecture, such as a PLC, switch, or SCADA, is constant and its behaviors tend to be stable over time, an established and configured network is predictable.

However, some behaviors are unpredictable and can compromise a network's operation and security.

When a behavior occurs, normal or abnormal changes are noted as differences in the Monitor mode.

Monitor mode is particularly convenient for large networks because a preset shows a network fragment, and changes are highlighted and managed separately in the Monitor mode views.



Search

Introduces **Search**, which finds components among unstructured data and supports saved presets and access to advanced component data.

Search is a page that enables you to find components among unstructured data. Components can be searched by name, custom name, IP, MAC, tag, and property value.

The **Search** page is available from the main menu. The search field accepts the content used for a search, and the **Search** control initiates the search.

> **Note**
>
> Devices are not available on this page yet.

The **Save this search as a Preset** control creates a preset from search results. Presets automatically update as new data is detected on the network.

When you hover over a component, the technical sheet **(2)** icon appears. The technical sheet provides access to advanced data about the component.

System statistics

System statistics are key performance indicators that provide visibility into the status of the Center and sensor health in Cyber Vision deployments.

A system statistic is a monitoring metric that

- reflects the operational status of the Center and sensors,
- allows administrators to track resource health and usage, and
- enables early detection of service or network issues.

Table 12: Feature History Table

Feature	Release Information	Feature Description
PCAP capture on the Cyber Vision Center interface	Release 5.4.x	You can capture PCAP data directly from the Cyber Vision Center interface, in addition to sensor based capture.
Sensor collected data quality report	Release 5.4.x	Easily monitor the quality of your sensor statistics with the **Status Overview** page. See real-time details for each sensor. Stay informed and ensure your data is always reliable.

System health statuses

This topic explains the system health statuses available in Cisco Cyber Vision Center. Use this information to understand service and queue status indicators.

To view system health, click the **System statistics** icon on any Cisco Cyber Vision Center page.

The **System Health** page helps you:

- Check if all background processes, such as services and extensions, are running correctly.
- See if background queues that collect data from sensors are free of congestion.

Table 13: System health statuses

Status	Description
Service Status	• Shows the status of Cyber Vision services and extensions. • The system regularly checks these components • If a service or extension is down, open the service status for more information. • Click **Update** to refresh the service status. • If a service is down, a warning banner appears. The banner links to this page and highlights the failed service in red.

Status	Description
Queue Status	• Displays the status of monitored sensor queues. • If a monitored queue drops messages, check the queue status to investigate. • The system lists any congested queues so you can address performance issues. • If a service is down, a warning banner appears. The banner links to the page where the failed service is highlighted in red.

System statistics for Center and sensors

This section provides a detailed reference for the main fields and indicators available on the System Statistics page, including chart descriptions, applicability, meanings, and available troubleshooting actions.

The **System Statistics** page displays

- key operational data for both the Center and its sensors, and
- helps you monitor system health and troubleshoot issues.

Table 14: System statistics charts

Chart	Applicability	Description
System Health	Center and sensors	Displays CPU, RAM, and disk usage statistics for each sensor. Minimum, maximum, and average values are shown. The table also shows current usage and hardware score to help you get support.
Captured Packets	Sensors	The chart shows the number of packets that the sensor captures on the industrial network interface in bytes per second. It also displays the number of dropped packets. When packet drops occur, this indicates that the sensor is overloaded and traffic is being lost.

Chart	Applicability	Description
Network Interfaces Bandwidth	Center and sensors	The line charts display bandwidth for Collection and Industrial network interfaces. Bytes received and sent per second by Center are shown in the charts. • **Collection Network Interface**: Data exchanged between Center and sensors. • **Capture Network Interface**: Data captured by the sensor on the industrial network through each port pair. **Note** Data sent to the Industrial network should be zero. If you detect outbound traffic, your sensor is not passive. Contact support immediately.
Disk I/O (B/s)	Center	Displays the Center hard disk usage in bytes per second.

Table 15: System statistics features

Name	Description

Generate diagnostic	• Generates a file to help with troubleshooting and support.
	  • For Sensor: Click **Generate diagnostic**; file downloads automatically once available.
	  • For Center: Click **Generate diagnostic**–then, once ready, click **Download Diagnostic** to retrieve the file.

PCAP Capture	Use the **PCAP Capture** field on the **Center** page to capture packet data directly. See Generate a PCAP file
Compute scores	Click **Compute scores** on the **Center** page to initiate system performance measurement. This action generates a new score.

Sensor status overview

This section describes the statistics provided on the Sensor Status Overview page and lists common sensor status issues you may encounter.

The **Status Overview** page displays statistics collected from each sensor, including Sensor Name, Product ID, Health Status, Components, Activities, Unicast Activities, and Sensor last reported time. Use these statistics to assess sensor operation and identify potential issues.

The statistics show data for all time periods. You cannot filter them by time range.

To view sensor statistics, choose **System statistics** > **Sensors** > **Status overview**.

The table presents common sensor issues that can occur during operation.

Table 16: Common sensor status issues

Issue	Description
Zeros everywhere (components and activities)	No data appears in the table, which means the sensor is not receiving traffic. The sensor cannot analyze packets or send information to the center. Review the sensor's monitoring setup to resolve this issue.
Zero unicast activities	If activities and components appear but no unicast activities are present, the sensor is not receiving properly mirrored traffic. The switch traffic mirroring (monitor session) may be misconfigured. The center DPI interface may also not be in promiscuous mode. In this case, the session captures only broadcast or multicast traffic.
Time mismatch	If the **Sensor last reported time** column does not closely match the actual date and time, a time synchronization issue may prevent Cyber Vision from displaying data accurately.

Generate a PCAP file

Use this task to capture and download packet data (PCAP) files directly from the interface for troubleshooting communication issues with Cyber Vision Center.

Collect network traffic data (PCAP files) from the Center interface. Use these files to diagnose and resolve communication, performance, or security issues.

Procedure

1. From the main menu, choose **System statistics** > **Center**.
2. Under **PCAP Capture**, select the desired network interface (such as **eth0** for administration or **eth1** for collection).
3. Enter filter parameters to specify the network traffic you want to capture.

> **Note**
>
> Use `tcpdump` filter syntax with Berkeley Packet Filters (BPF) to narrow the capture to the packets you want.

4. Start the capture.

> **Note**
>
> Only one PCAP capture can run at a time.

5. When finished, stop the capture.

You can download the PCAP capture file.

What to do next

When the capture is complete, click **Download** to save the capture file. Analyze the downloaded PCAP file to troubleshoot issues.

Create your personal account

Provides instructions to create your personal account in Cisco Cyber Vision Center and configure personal details, language, password, notifications, and application cookies.

You must create your personal account in Cisco Cyber Vision Center.

Follow these steps to create your personal account.

Procedure

---

1. In the **user menu** at the top right corner, click the drop-down arrow and select **My Settings**.

   The **My Settings** page appears.

2. Under the **General** field, enter **Firstname** and **Lastname**.
3. Under the **Language** field, select the radio button for your preferred interface language.
4. Enter your password.

   Passwords must contain at least 6 characters and comply with the following rules:

   - Passwords must contain a lower case character: a-z.
   - Passwords must contain an upper case character: A-Z.
   - Passwords must contain a numeric character: 0-9.
   - Passwords cannot contain the user ID.
   - Passwords must contain a special character: ~!"#$%&'()*+,-./:;<=>?@[]^_{|}.

   Important

Change your password regularly to ensure platform and industrial network security.

> **Note**
>
> Your email will be requested for login access.

5. Select the **Restore default parameters** checkbox to restore interface notifications.
6. Click **Save settings**.
7. Clear application cookies.

Risk scores

Introduces risk scores, which indicate device health and criticality, and explains how Cisco Cyber Vision uses them to identify and prioritize device risks.

A risk score is an indicator of the health and criticality level of a device. The score ranges from 0 to 100, with a color code that indicates the level of risk.

Risk score levels

Table 17: Risk score levels

Score	Color	Risk level
From 0 to 39	Green	Low
From 40 to 69	Orange	Medium
From 70 to 100	Red	High

Risk score use

Risk scores apply to the following locations:

- Filter criteria
- **Device list**
- Device technical sheet
- **Device risk score widget** on the **Home** page
- **Preset highlight widget** on the **Home** page

Risk scores help you identify the most critical devices in the overall network. They provide limited, simple information about the cybersecurity of the monitored system and are a first step in security management by showing values and providing solutions to reduce them.

The goal is to minimize values and keep risk scores as low as possible. Proposed solutions include the following:

- Patch a device to reduce the attack surface.
- Remove vulnerabilities.
- Update firmware.
- Remove unsafe protocols whenever possible, such as FTP, TFTP, and Telnet.
- Install a firewall.
- Limit external communications by removing external IPs.

Cisco Cyber Vision enables you to define the importance of devices in your system by grouping them and setting an industrial impact. This function increases or decreases the risk score, allowing you to focus on the most critical devices.

These actions reduce the risk score by affecting its variables: impact and likelihood. For example, removing unsafe protocols affects the likelihood of risk, whereas patching a device affects the impact of risk.

Risk scores provide an opportunity to update usage and maintenance habits. However, they are not intended to replace a security audit.

In Cisco Cyber Vision, risk scores also support ordering and filtering information in lists and creating presets.

Review device risk score details

Provides instructions to identify devices with high risk scores and open the technical sheet that contains detailed risk information.

Procedure

1. From the main menu, select **Explore**.
2. In the top navigation bar, select **All Data** under **Basics**.
3. In the third filter of the top navigation bar, select **Device List**.
4. In the **Risk score** column, select the sort arrow to display the highest risk scores.
5. Click a device name in the **Device** column.

   The right-side panel appears.
6. In **Risk score**, select **See details**.

   The technical sheet appears.

Risk score calculation and factors

Details the risk score formula, its impact and likelihood factors, the information shown in the technical sheet, and the calculation schedule.

Use this reference to interpret the values and factors that Cisco Cyber Vision uses to calculate a device risk score.

Risk score formula and impact

Risk score is computed as follows:

```
Risk = Impact x Likelihood
```

Impact is the device criticality: the impact that the device has on the network. A device can control a small, non-significant part of the network or a large, critical part of the network.

Impact depends on the following factors:

- Device tags: Some device types are more critical than others. Cisco Cyber Vision assigns an industrial impact score to each device type, device tag, or device tag category. For example, a simple IO device that controls a limited portion of the system and a Scada device that controls the entire factory do not have the same impact if compromised.
- Group industrial impact: Moving a device into a group and setting the group industrial impact from very low to very high affects the device impact.

Likelihood factors

Likelihood is the probability that a device is compromised. Likelihood of risk depends on the following factors:

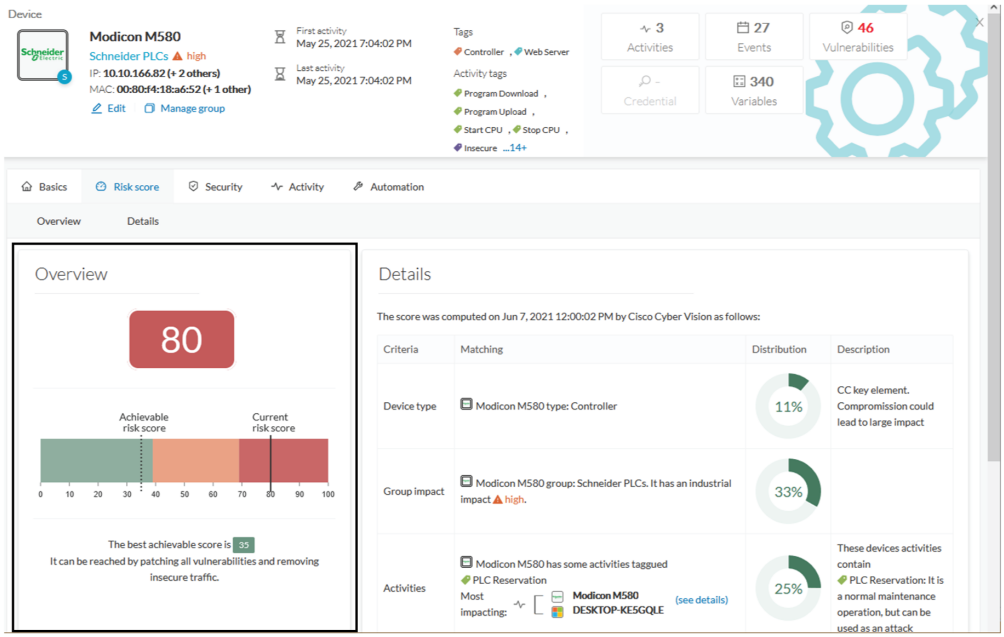
- Device activities and activity tags. Some protocols are less secure than others; for example, Telnet is less secure than ssh.
- Exposure created when a device communicates with an external subnet.
- Device vulnerabilities, taking their CVSS scoring into account.

Technical sheet risk score information

For detailed information about a risk, refer to the **Details** tab in the technical sheet.

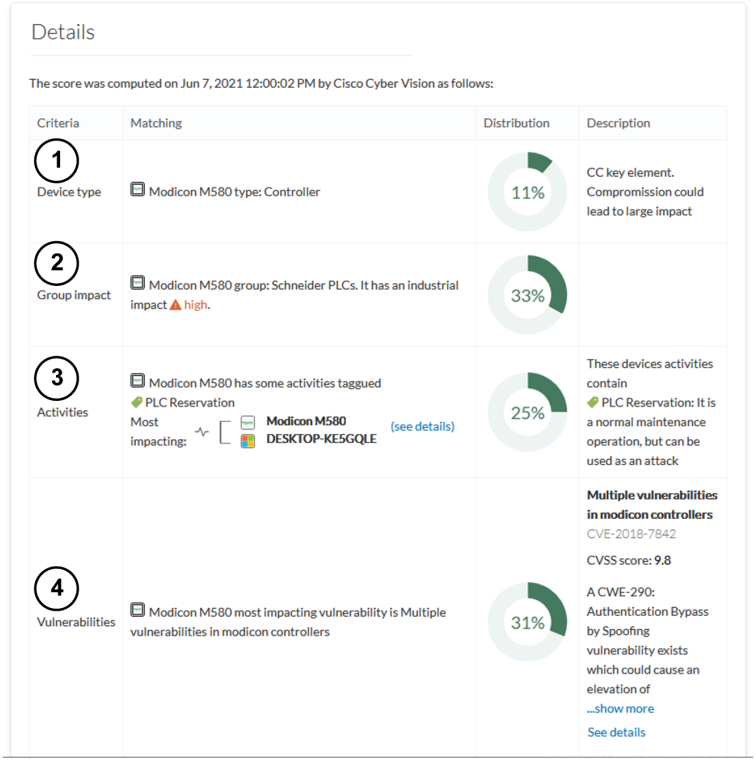
In the **Overview** tab, the **Current** risk score and the **Achievable** risk score are displayed. The achievable risk score is the best score that can be reached by patching all vulnerabilities on the device and removing all potentially insecure network activities.

The achievable risk score cannot be zero because devices have intrinsic risks from their device type and, when applicable, their group industrial impact.



The **Details** tab shows the different risks that affect the device, the percentage that each risk represents within the total risk score, and solutions to reduce or eliminate those risks.

Device type and **Group impact** affect the risk impact variable. **Activities** and **Vulnerabilities** affect risk likelihood.



Risk score calculation schedule

The risk score page shows the last time that Cisco Cyber Vision computed the risk score. Risk score computation occurs once an hour.

To force immediate computation, use the following command on the Center shell prompt:

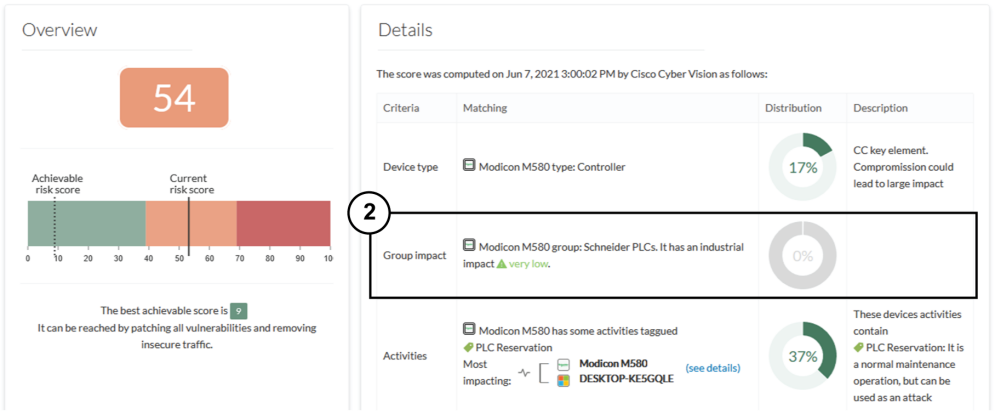
```
sbs-device-engine
```

Information from the latest computation

The most recent computation provides the following information:

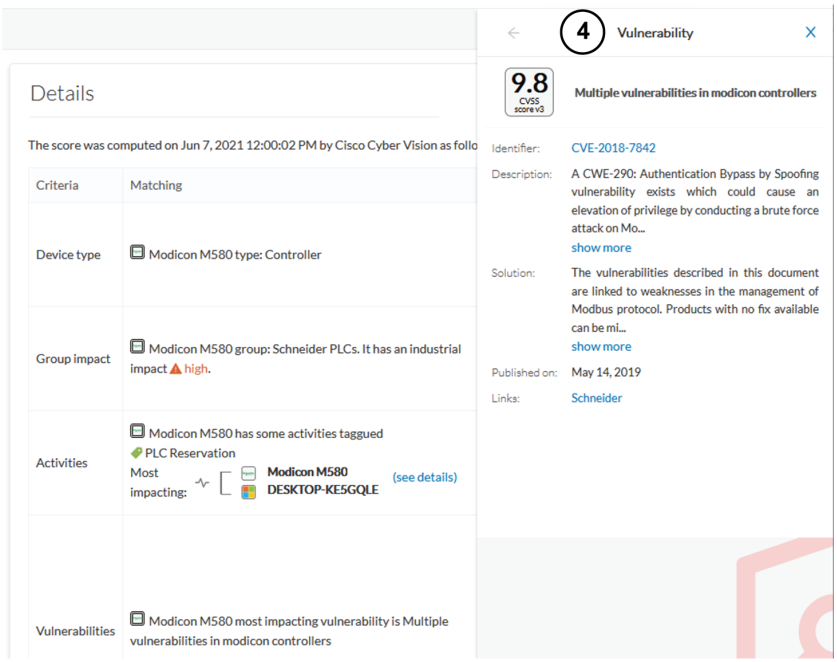
- **Device type**: Each device type corresponds to a device tag detected by Cisco Cyber Vision. No action is required at the device type level because each device tag has a default risk score.
- **Group impact**: This factor applies when the device belongs to a group. Lowering the industrial impact of the group decreases the device impact.

  For example, changing the group industrial impact from high to very low decreases the overall risk score from 80 to 54.



The new industrial impact factors into the next risk score computation, which occurs once an hour.

- **Activities**: The most impactful activity tag is displayed. Removing all potentially insecure network activities lowers the risk.
- **Vulnerabilities**: The **See details** link provides more information about patching vulnerabilities to reduce the device risk score.



By taking these actions, the risk score should decrease considerably.

3 Licensing

Topics:

- Cisco Cyber Vision licenses
- Register the license for Cyber Vision Center
- Use specific license reservation
- Managed Services License Agreement
- License usage compliance

Introduces Cisco Cyber Vision licensing, detailing license types including trial, Essentials, Advantage, IDS component licenses, and Smart Software Manager Satellite for air-gapped networks, registration steps, reservation management, MSLA, and compliance requirements.

Cisco Cyber Vision licenses

Provides an overview of Cisco Cyber Vision licensing, including center, sensor, and Talos subscription options. This information helps administrators manage license compliance and deployment through the Cisco Smart Software Manager.

Cisco Cyber Vision licenses are a collection of software entitlements required for center operations, sensor hardware appliances, and intrusion detection services.

- Center licenses
- Sensor hardware appliance licenses
- Talos subscriber licenses for intrusion detection

License management and deployment

Manage your Cisco Cyber Vision smart licenses through the Cisco Smart Software Manager (CSSM), a centralized platform to track and manage all your Cisco licenses. You have real-time visibility into license usage and availability to help easily optimize and scale usage while ensuring compliance.

For more information about the Cisco Cyber Vision license types and how to order them, see the Cisco Cyber Vision Data Sheet .

This document guides you through the registration and activation of the Cisco Cyber Vision Center licenses, Essentials, and Advantage.

You can also use CSSM satellite servers or Specific License Reservations for air-gapped networks that do not have a persistent internet connection.

> **Note**
>
> Specific license reservations require special permissions. Contact your Cisco account manager if you require this license type.

Trial licenses for Cisco Cyber Vision

Provides a 90-day evaluation period for new Cisco Cyber Vision installations to access all features. This mode ensures users can test the platform before requiring a permanent license registration.

The evaluation mode is a temporary licensing state that enables full access to Cisco Cyber Vision features for 90 days following a fresh installation.

- Automatically enabled upon initial installation.
- Valid for a duration of 90 days.
- Requires valid license registration after expiration to maintain system access.

Evaluation mode management

To view the status of your evaluation mode, log in to the Cisco Cyber Vision center and navigate to **Admin** > **License** . This page displays the remaining days and provides options to register smart licenses.

> **Note**
>
> Once evaluation licenses expire, access is restricted to the **License** page until valid licenses are registered.

Essentials and advantage licenses

Provides a comparison of the features enabled by the Cisco Cyber Vision Essentials and Advantage license tiers. These licenses allow users to manage device inventory, security, and system integrations.

Cisco Cyber Vision Center licenses are available in two tiers, Essentials and Advantage, where the Advantage license includes all features of the Essentials license plus additional advanced capabilities.

Features enabled by the Cisco Cyber Vision Essentials license include:

- **Inventory** : Device inventory, identify communication patterns, and generate inventory reports.
- **Vulnerability** : Identify device vulnerabilities and generate vulnerability reports.
- **Activities** : Track control system events and generate device activity reports.
- **RESTful API** : REST API programming interface.

Features enabled by the Cisco Cyber Vision Advantage license include all Essentials features, plus:

- **Security posture** : Device Risk Scoring.
- **Intrusion detection** : Snort IDS on supported sensors and Talos community signatures.
- **Behavior monitoring** : Create baselines for asset behaviors and alerts on deviations.
- **Advanced integrations** : XDR Ribbon, pxGrid integration with Cisco ISE, Firepower Host Attribute integration, SIEM Integration (Splunk, IBM QRadar), and ServiceNow OT Management integration.

Licenses for Intrusion Detection System (IDS) components

Identifies the licenses required to enable Talos subscriber rules for Cyber Vision IDS sensors. Each sensor consumes a license when the IDS service is enabled.

This reference provides the license IDs and their corresponding purposes for Cyber Vision IDS components, including hardware and virtual appliances.

License ID	Purpose of License
CV-IDS-CNTR	Talos subscriber rules license for Cyber Vision Center IDS (hardware and virtual appliance)
CV-IDS-IC3000	Talos subscriber rules license for Cyber Vision IDS on IC3000-2C2F-K9 sensors
CV-IDS-IR8300	Talos subscriber rules license for Cyber Vision IDS on Cisco Catalyst IR8300 sensors
CV-IDS-C9000	Talos subscriber rules license for Cyber Vision IDS on Cisco Catalyst 9300, 9300X, or 9400 sensors

Cisco Smart Software Manager satellite for air-gapped networks

Provides a local Cisco Smart Software Manager satellite server for environments where direct Internet connectivity is restricted. This solution enables license management for air-gapped Cisco Cyber Vision deployments.

A Cisco Smart Software Manager satellite is an on-premises server that provides a subset of Cisco Smart Software Manager functionality for networks without direct Internet access.

- Operates within air-gapped environments.
- Requires periodic synchronization with the Cisco portal.
- Maintains updated license purchase and utilization data.

Satellite synchronization requirements

The satellite server must communicate with the Cisco Smart Software Manager periodically to remain operational. Users must synchronize the satellite server with the Cisco portal to ensure that the most recent license purchase and utilization data are updated in both systems.

For additional guidance, refer to General CSSM On-Prem Help

Register the license for Cyber Vision Center

Register the license for Cyber Vision Center to activate your product instance and enable full functionality.

Register your Cyber Vision Center with Cisco licensing servers to activate your licensed features.

Before you begin

- For the direct HTTP connection:
  - Ensure you obtain a valid product instance registration token from Cisco Software Central.
  - For instructions, see How can I create a token from my Smart Account, in Cisco License Central?.
- For Transport Gateway:
  - Ensure you obtain a product registration token and Transport Gateway URL (if applicable) from CSSM On-Prem License Workspace.
  - For instructions, see How can I register a device from within an On-Prem deployment?.

Procedure

1. From the Cyber Vision Center main menu, choose **Admin** > **License**.
2. Click **View/Edit** next to **Transport Settings** to select a connection method:
   - Select **Direct** to connect to Cisco licensing servers through a direct HTTP connection (persistent internet required).
   - Select **Transport Gateway** to connect to Cisco licensing servers through Transport Gateway. In the **URL** field, enter the Smart Transport Registration URL you copied from Cisco Software Central.

> **Note**
>
> To connect to Cisco licensing servers through a proxy server, configure the proxy settings required for your connection method. These settings are available in the New UI. See Configure a proxy server.

3. Click **OK**.
4. Click **Register** and enter the **Product Instance Registration Tokens** obtained from your Cisco Software Central account.
5. Click **Register** to complete the license registration.

Cyber Vision Center is activated.

What to do next

- To verify registration status, navigate to **Admin** > **License** in the **Status** area. The status shows **Registered** and displays license expiration details.
- To troubleshoot license reporting or usage issues, you can reregister licenses on the same page. Click **Actions** and select **Reregister**, then generate a new registration token and repeat the registration steps.
- To deregister licenses, select **Deregister** from the **Actions** menu. Deregistration returns Cyber Vision Center to evaluation mode, and you may lose access if the evaluation period has expired.

Use specific license reservation

Reserves license entitlements on a Cisco Cyber Vision center when security requirements prevent a persistent connection to the Cisco Smart Software Manager. This method allows for offline license management through the exchange of reservation and authorization codes.

Specific license reservation is a smart licensing method that you can use when your organization's security requirements do not allow a persistent connection between Cisco Cyber Vision center and the Cisco Smart Software Manager (CSSM). Specific license reservation allows you to reserve license entitlements on a center.

The process to create and register a specific license reservation spans across Cisco Cyber Vision center and Cisco Software Manager.

If you don't want to proceed with the license reservation after you generate the reservation request code in Cisco Cyber Vision center, in the **License** page, click **Cancel Reservation Code** .

If you lose the reservation request code you created in Cisco Cyber Vision center, in the **License** page, click **View Reservation Request Code** .

Before you begin

Specific License Reservation is not available by default. If you want to use this licensing method, contact your Cisco account team to get the permission to use specific license reservation. After you licensing method is granted, you can carry out the following task to register specific license reservation on your Cisco Cyber Vision center.

Follow these steps to use specific license reservation.

Procedure

1. In the Cisco Cyber Vision center, choose **Admin** > **License**, and click **Register**.
2. In the statement **If your Smart Account is authorized for License Reservation and you wish to reserve licenses, start here.** , click **start here** .
3. Click **Yes, My Smart Account is License Reservation Enabled** .
4. Click **Generation Reservation Request Code** .
5. To copy the reservation code, click **Save to File** or **Copy to clipboard** .
6. Log in to Cisco Software Manager, and perform the following:
   a) From the main menu, choose **Smart Software Manager** > **Manage Licenses**.
   b) Choose **Inventory** > **Licenses** to view your purchased smart licenses.
   c) Click **License Reservation** .

      A **Smart License Reservation** workflow dialog box is displayed.

   d) In the **Step 1: Enter Request Code** tab, in the field that is displayed, enter the reservation code you received from Cisco Cyber Vision center, and click **Next**.
   e) In the **Step 2: Select Licenses** tab, click the **Reserve a specific license** radio button. Then, in the **Reserve** column of the table displayed, for each license type, enter the number of license entitlements you want to reserve.

      1. Click the **Reserve a specific license** radio button.
      2. In the **Reserve** column of the table displayed, for each license type, enter the number of license entitlements you want to reserve.
      3. Click **Next** .

   f) In the **Step 3: Review and Confirm** tab, review the details of your specific license reservation, and click **Generate Authorization Code** .
   g) The **Step 4: Authorization Code** tab contains a field that displays the authorization code in the XML format. This XML content includes information about the license reservation and the Cisco Cyber Vision center for which the SLR is generated. Click **Download As File** to download the .txt file to your local system.
   h) In the **License** page of your Cisco Cyber Vision center, click **Enter Reservation Authorization Code**.
   i) Paste the contents of the .txt file in the text box, or click **Upload** and choose the .txt file that you downloaded from Cisco Software Manager, and click **Install Authorization Code/File** .

Update specific license reservation

Updates the details of a specific license reservation by generating a new reservation code in Cisco Software Central and registering it through the Cisco Cyber Vision center.

If you need to update the details of your specific license reservation, create a new reservation code in Cisco Software Central. Then, register the license reservation through the Cisco Cyber Vision center.

Procedure

1. Log in to Cisco Software Manager, and from the main menu, choose **Smart Software Manager** > **Manage Licenses** .
2. Choose **Inventory** > **Product Instances** to view the product instances that report license usage to Cisco Software Central.
3. Find the Cisco Cyber Vision center for which you want to update the license reservation, and click the **Actions** drop-down menu in the same row.

4. Click **Update Reserved Licenses** .
5. In the **Step 1: Select Licenses** tab, perform the following:
   a) click the **Reserve a specific license** radio button.
   b) In the **Reserve** column of the table displayed, for each license type, enter the number of license entitlements you want to reserve.
   c) Click **Next** .
6. In the **Step 2: Review and Confirm** tab, review the details of your specific license reservation, and click **Generate Authorization Code** .
7. The **Step 3: Authorization Code** tab contains a field that displays the authorization code in the XML format. This XML content includes information about the license reservation and the Cisco Cyber Vision center for which the SLR is generated. Click **Download As File** to download the .txt file to your local system.
8. In the Cisco Cyber Vision center, choose **Admin** > **License**, and click **Update Reservation** . .
9. Enter the authorization code for the updated license reservation, and click **Register**.

Return specific license reservation

Releases reserved licenses to make them available in your smart licensing account for reuse. These licenses can be used as smart licenses or as part of another license reservation.

When you return a specific license reservation, the reserved licenses are released and available in your smart licensing account for reuse. You can use them as smart licenses or as part of another license reservation.

Procedure

1. In the Cisco Cyber Vision center, choose **Admin** > **License** .
2. Click **Return Reserved Licenses** .
3. Click **Generate Reservation Return Code** .
4. Copy the code displayed in the text box, and then click **Return License**.
5. Log in to Cisco Software Manager, and from the main menu, choose **Smart Software Manager** > **Manage Licenses** .
6. Choose **Inventory** > **Product Instances** to view the product instances that report license usage to Cisco Software Central.
7. From the **Actions** drop-down list for your specifc license reservation, choose **Remove** .
8. Enter the reservation return code that you copied in Step 4, from Cisco Cyber Vision center.
9. Click **Remove Product Instance** .

Managed Services License Agreement

Introduces the Managed Services License Agreement, outlining its post-paid utility model, provider license entitlements, multi-customer license registration, and adherence to standard license registration procedures for Cisco partners.

The Managed Services License Agreement (MSLA) is a post-paid utility service model for network providers who are Cisco partners.

- Enables payment based on actual usage at the end of a monthly billing cycle.
- Allows providers to hold license entitlements.
- Supports enabling or registering licenses for multiple customers' centers.

The license registration process remains consistent with standard procedures. For more information, see Register the license for Cyber Vision Center .

Configure utility mode for MSLA

Provides instructions for configuring utility mode on Cisco Cyber Vision center to enable MSLA license usage, including navigation to the appropriate admin and license settings.

To use an MSLA license in a Cisco Cyber Vision center, you must set the center to utility mode.

Follow these steps to set the center to utility mode.

Procedure

1. Navigate to the **Admin** > **License** page.
2. From the **Actions** drop-down list, choose **Change Utility Mode** .

License usage compliance

Describes the requirements for maintaining license validity and the operational impact of license expiration or noncompliance within Cisco Cyber Vision. This information helps administrators manage subscription renewals and resolve access restrictions effectively.

Cisco Cyber Vision Essentials and Advantage licenses are term subscriptions that require renewal to maintain feature access and product support.

- Licenses are available for 1, 3, 5, or 7-year terms.
- Expired licenses trigger alerts in the Cisco Cyber Vision center.
- Noncompliance may restrict user access to the **License** page while maintaining existing network configurations.

License noncompliance scenarios

Access to the Cisco Cyber Vision center is restricted to the **License** page under the following conditions:

- The evaluation license has expired.
- A specific license reservation is returned without other valid licenses registered.
- Essentials or Advantage licenses expire while using the Cisco Smart Software satellite connection method.

> **Note**
>
> If IDS licenses expire or overconsumption occurs because IDS is enabled on more sensors than licensed, a warning message appears in the Cisco Cyber Vision center until the issue is resolved.

4 Get started with Cisco Cyber Vision

Topics:

- Data management operations
- Users
- Center web server certificates

Outlines the foundational steps for working with Cisco Cyber Vision, including managing and purging data, understanding storage and expiration settings, configuring ingestion, defining user roles and password requirements, administering users, and setting up the center web server certificate.

Data management operations

Outlines data management operations in Cyber Vision Center, including optimizing stored data, performing clearance tasks, setting expiration policies, customizing data ingestion, and tracking feature updates such as VLAN-based data clearing to enhance system performance and storage efficiency.

Data management operations are Cyber Vision Center features that

- manage and optimize data stored on Cyber Vision Center,
- support tasks such as data clearance, setting data expiration, and customizing data ingestion, and
- improve system performance by enabling effective storage and retention policies.

Table 18: Feature History Table

Feature	Release Information	Feature Description
Clear multiple components using a VLAN ID	Release 5.3.x	When you clear data, you can enter a VLAN ID to purge all the components associated with it. You can clear data for one VLAN ID at a time.

Caution: Understand the impact before clearing all data

Outlines the critical impacts of clearing all data in Cyber Vision Center, including deletion of network information, disruption of monitoring, and preservation of configuration settings, emphasizing caution before performing this action.

Clear all data only when absolutely necessary, such as when the database becomes overloaded.

Be aware of these consequences:

- The system deletes all network data, including components, flows, events, and baselines, from Cyber Vision Center.
- The GUI becomes empty.
- The system preserves only configuration settings, such as capture modes, event severity, and syslog settings.
- Clearing all data disrupts network monitoring.

Data storage and expiration settings

Outlines storage limits, expiration policies, and purge methods for components, activities, flows, events, external communications, variables, and reports to help you manage data retention and system resources efficiently.

This table explains storage limits, expiration policies, and purge methods for each data type. You can use this information to manage system resources effectively.

Table 19: Settings

Data type	Storage	Expiration
Components or Devices	Storage is internal only. You receive a warning when you reach 120,000 components. Data ingestion stops at 150,000 components.	No expiration. Manual purge is needed.

Data type	Storage	Expiration
Activities	Activities are stored internally and do not have a high storage limit.	The data does not expire. You must purge it manually.
Flows	You can enable or disable storage configuration; there is no upper storage limit. You can then define networks.	The system automatically deletes data after seven days of inactivity.
Events	You can configure the storage for each category, with a high limit of 10,000 per event category.	No expiration. The oldest event is purged when the 10,000 limit is reached.
External communications	Communications are stored externally only. You can save up to one million communications.	The system deletes data automatically after 30 days.
Variables	You can enable or disable the storage configuration, with no high storage limit.	The system deletes data automatically after seven days of inactivity.
Reports	You can set the storage period from three months to three years. The default is six months. The storage duration also depends on the maximum number of versions you set.	The system automatically deletes data when the creation date is older than the defined period or when the number of versions exceeds the limit.

Purge components from the database

Removes obsolete network components and devices to maintain database performance and prevent data ingestion issues.

The system limits the number of components such as network interfaces, PCs, SCADA stations, and broadcast or multicast addresses to protect the database.

- If the count exceeds 120,000, a pop-up and red banner alert you to purge.
- When the number of components reaches 150,000, data ingestion stops. The system deletes new data without processing or storing it. A pop-up and red banner alert you to purge.

Before you begin

- Ensure you have Admin access.

Procedure

1. From the main menu, choose **Admin** > **Data Management** > **Clear Data**.
2. Select **Components selection** .
3. Choose the **Component Type**.
   - **IT** : This selects components in the IP range with the **IT Internal** network type.
   - **OT** : This selects components in the IP range with the **OT Internal** network type.
   - Both: This selects components in the IP range with both network types.
4. Specify any criteria for purging (all fields optional):

- IP Subnet
- VLAN ID (one at a time)
- Inactivity since
- Creation Start Time
- Creation End Time

5. Click **Clear data** and confirm when prompted.

The database removes the specified components and related devices. The updated device count appears under **Explore** > **All Data** .

> **Note**
>
> Purging components by VLAN, IP, or date triggers an event. If a Global Center is enrolled, those components are also purged in the Global Center after synchronization.

What to do next

Review the device list to ensure the correct components were removed.

Expiration settings

Outlines how to manage report retention periods and versions using expiration settings to control system storage and performance, explains automatic purging and storage impacts, and guides access through the Cyber Vision Center interface.

Expiration settings help you manage system storage and performance.

Key aspects of expiration settings:

- Expiration settings control the retention period and number of versions for reports only. Other data types (such as Components, Devices, Activities, Flows, Events, External communications, and Variables) have fixed retention periods.
- Expiration settings manage storage consumption by automatically purging reports older than the configured retention period.
- Increasing the retention period increases storage usage and may negatively impact system performance.
- Access expiration settings at **Admin** > **Data Management** > **Expiration Settings** in the Cyber Vision Center interface.

Ingestion configurations

Outlines how to configure ingestion settings to manage flow and variable data storage, explains flow aggregation options to optimize database records, and details port scan detection for identifying network probing.

An ingestion configuration is a data management feature that determines whether flow and variable traffic data are stored and processed by Cyber Vision Center.

You can enable or disable storage of flows and variables. By default, both options are disabled. To limit data storage, you can specify which flows from subnetworks are stored. These subnetworks are defined within Network Organization settings.

If flows and variables are disabled, data will not be stored in the database.

Flows Aggregation

- Cyber Vision records each flow that it detects, and includes details such as client and server ports for your reference.
- For protocols such as DNS, HTTP, or SSH, client ports can vary, so you may see many similar entries in your data.
- If you enable **Flow Aggregation**, Cyber Vision does not consider the client port for those specific protocols. This combines similar flows and limits the number of records in the database.

Port scan detection

Port scan detection helps you identify and respond to suspicious network probing, which may indicate cyberattack attempts.

Users

Outlines user account management in Cyber Vision Center, including user roles, permissions, external directory integration, user restrictions, and security settings such as password policies and access controls.

A user is an account holder in Cyber Vision Center that

- accesses and interacts with the Cyber Vision Center platform,
- is assigned one or more roles that define permissions and access privileges, and
- is managed using user management features, such as roles and security settings.

Table 20: Feature History Table

Feature	Release Information	Feature Description
Restrict users to a specific preset category	Release 5.4.x	This feature enables precise data access control by assigning preset categories to Cyber Vision user roles, limiting users to the Explore menu with read-only permissions. **Note** Once you restrict a user to a specific preset category, they will not have access to the New UI.

User roles and management

Cyber Vision Center provides default user roles such as Admin, Auditor, Operator, and Product. You can also create custom roles to tailor specific permissions and access levels for different users or groups. Roles control the actions that you can perform within the platform. You can map user roles (except Admin) to external directory groups through LDAP. To provide admin privileges through LDAP, clone the admin role and map it to the external directory group.

User security settings

The Security settings page (**Admin** > **Users** > **Security settings**) allows configuration of password policies, such as password lifetime, login attempt limits, and password reuse restrictions, to help protect user accounts.

User roles

Outlines user roles and their associated privileges, detailing access levels from full administrative control to read-only capabilities across system, sensor, event, and reporting functions within the platform.

User roles define access and administrative privileges in the platform.

Table 21: User role types and privileges

Role	Privilege
Admin	If you have the admin role, you have full rights and oversee all sensitive actions. These actions include managing user rights, updating the system, configuring syslog, and setting up sensor reset or sensor capture mode.
Product	If you have the product role, you can access system, sensor, and event administration pages and manage sensors remotely. You may manage event severity and export events to syslog if an admin allows it.
Operator	If you have the operator role, you work in monitor mode and can manage groups, but do not have administration privileges. You can access all pages except system administration.
Auditor	If you have the auditor role, you have read-only access to Explore, Reports, Events, and Search pages. You can use non-persistent sorting features and generate reports.

Password requirements

Outlines required password criteria—including character types and length—and recommends best practices for regular password changes and configuring password lifetime settings to enhance account security.

Passwords protect user accounts and systems against unauthorized access.

Passwords must meet these requirements:

- Contain at least 6 characters.
- Must include:
  - A lowercase character from a to z
  - An uppercase character from A to Z
  - A numeric character from zero to nine
  - A special character (~!"#$%&'()*+,-./:;<=>?@[]^_{|})
- Not contain your user ID.

Additional best practices:

- Change your password regularly.
- Configure password lifetime settings in **Admin** > **Users** > **Security settings**.

Add a new user

Guides administrators through adding a new user account in Cyber Vision Center, including entering user details, assigning roles, confirming creation, and using the Users management page for future edits or deletions.

Add a new user account to Cyber Vision Center to log in and access assigned roles.

Before you begin

Ensure you have administrator privileges in Cyber Vision Center.

Procedure

1. From the main menu, choose **Admin** > **Users** > **Management**.
2. Click **Add a new user**.
3. Enter the required user details: **Firstname**, **Lastname**, **Email**, **Password**, and **Confirm password**.
4. Select the appropriate role for the user.
5. Click **OK**.

You can see the new user in the **Users management** page, and the user can log in with the assigned credentials.

What to do next

To edit or delete the user later, use the **Users management** page.

Create a user role

Guides you through creating a user role in Cyber Vision, configuring custom permissions, restricting access, assigning preset categories, managing roles, and mapping them to external directory groups in LDAP settings.

Create a user role in Cyber Vision with specific permissions to meet your needs.

Use user roles to define precise access and manage permissions for each user in Cyber Vision.

Before you begin

Ensure the **Cyber Vision New UI** is enabled for your center.

Procedure

1. From the main menu, choose **Admin** > **Users** > **Role Management**.
2. Click the add button **(+)** to create a new role.
3. Enter the **Role Name** and **Role Description**.
4. Set permissions for the new user role using one method:
   - **Restrict user access to a single preset category**:
     a. Enable **Restrict user access to a single preset category**.
     b. Select a preset category and click **Save**.

> **Note**
>
> - To delete a preset category, first unassign it from any user role.
> - If a user is restricted to a preset category, they have read-only access to the **Explore** menu only.

- **Search/Add existing permission**:
  a. Select a role from **Search/Add existing permission**.
  b. Click **Save**

- **Add New Permissions**:
  a. Click **Add New Permissions**.
  b. Select required permissions (**Read** or **Read + Write**) from **Classic UI Permissions** and **New UI Permissions**.
  c. Click **Save**.

> **Note**
>
> You receive read access to **Explore** in the Classic UI and to **Assets and Vulnerabilities** in the New UI by default.

The new user role appears in the **Role Management** list.

What to do next

- You can edit or delete roles in **Role Management**.
- You can map custom roles to external directory groups in LDAP settings.

Center web server certificates

Introduces the purpose of Center web server certificates and outlines methods for managing them, including the use of default internal certificates and enterprise certificate solutions to ensure secure, trusted communication between Cyber Vision Center and client devices.

A center web server certificate is a digital security credential that

- enables encrypted communication between the Cyber Vision Center and web browsers,
- ensures data integrity and confidentiality during browser sessions, and
- allows client devices to verify the Center's identity before exchanging sensitive data.

Options for managing web server certificates

You can manage Center web server certificates in two ways:

- Default internal certificate:
  - The system automatically generates a default internal (self-signed) certificate. To establish secure communication when using this certificate, you need to download it from the Center and install it on your laptop or client device. Adding this certificate to your device's trusted certificate store secures your communications with the Center.
- Enterprise certificate management:
  - Alternatively, you can configure the Center to use an enterprise certificate. The Center can use an enterprise certificate by uploading a P12 file, generating a certificate signing request (CSR) for your Certificate Authority (CA), or using the ACME protocol. Once in place, browsers will automatically trust the Center web interface. For more information, see the "Configure the Center" chapter in the Center Installation Guide.

5 Configure Cisco Cyber Vision

Topics:

- Network organization
- API Token
- Active Discovery policies
- LDAP
- Single sign-on (SSO)
- Sensors
- PCAP files
- SNMP monitoring information

Guides the complete configuration process for Cisco Cyber Vision, covering network organization, subnet and network group definition, API token management, active discovery policy setup, LDAP and SSO integration, sensor administration, pcap file handling, and SNMP configuration.

Network organization

Explains how network organizations are defined and viewed based on IP ranges and VLAN IDs.

A network organization is a classification structure that groups devices based on networks for internal and external network types (such as OT Internal, IT External, and External).

By default, networks corresponding to private IP addresses are classified as OT Internal. This is a factory configuration that can be customized by the user after deployment to meet specific operational requirements.

In addition to these private ranges, the following special IP addresses and networks are also defined as Internal by default:

- Broadcast IPv4: 255.255.255.255
- Loopback IPv4 and IPv6: 127.0.0.1 and ::1
- Link Local Multicast IPv4 and IPv6: 224.0.0.0/8 and ff00::/8

All other IP addresses that do not fall into the defined internal or special categories are considered external by default.

The External IP addresses trigger the following system actions:

- Excludes associated flows, components, and devices from the database.
- Removes devices from the device license count.
- Omits devices from risk scoring.

To view the current network organization in the classic UI, navigate to **Admin** > **Network Organization**.

> **Note**
>
> This **Network Organization** page in the classic UI provides a read-only view of the network organization based on IP ranges and VLAN IDs.

To add or manage network organizations, go to the **Configuration** > **Network Definition** page in the New UI.

Feature history table

Feature	Release Information	Feature Description
Read-only view of network organization.	Release 5.6.0	The Network Organization page has read-only view of the network organization. Define and manage networks from the Network Detection page in the new UI.

Create network groups

Create network groups based on your defined networks to streamline device organization and support Cisco ISE integration.

Group your assests automatically according to your network definitions. These groups enable easier device management and allow you to segment your network using Cisco Identity Services Engine (ISE) integration.

Each group is named after its associated network name.

Before you begin

Ensure your network definitions are accurate and complete. From the main menu, choose **Admin** > **Network Organization** to review existing definitions.

Procedure

1. From the main menu, choose **Admin** > **Network Organization**.
2. Click **Create groups based on network**.

   Note

   - For each defined network, the system creates one group and names it after the **Network Name**.
   - Loopback, link-local, local unicast, multicast, and broadcast networks are excluded from network groups.

3. Select **Yes** or **No**, for the presented options:
   - Automatically assign any newly discovered network devices to the groups.
   - Delete the existing groups.

     Caution

     If you select **Yes**, all existing network groups and user-defined groups are deleted.

     If you have existing Cisco Identity Services Engine (ISE) and Firewall integrations, be very careful when deleting groups. Deleting groups may disrupt these integrations and affect their operation.

4. Click **Submit**.

The system creates groups using your network definitions.

What to do next

- From the main menu, choose **Explore**. Select any preset and view the groups under the **GROUPS** tab to see the created groups.
- Once groups are created based on network definitions, you can synchronize them with Cisco ISE security groups. For integration details, see the “Integrate Cisco Cyber Vision with Cisco Identity Services Engine (ISE)” guide, particularly the "Chapter: Integrate Cisco Cyber Vision and Cisco Identity Services Engine (ISE) through Cisco ISE API".

API Token

Provides a secure method for authenticating REST API requests to Cisco Cyber Vision. This mechanism enables external applications to access or modify data within the Center.

An API token is a random password used to authenticate requests to Cisco Cyber Vision for accessing or modifying data through the REST API.

- Authenticates requests from external applications.
- Allows data access and modification within the Center.
- Supports integration with external solutions like SOC.

API Token Management

Cisco Cyber Vision provides a REST API that requires a token created through the API administration page for access.

> **Note**
>
> Best practice: create one token per application so you can remove or expire accesses separately.

Create an API token

Generates a unique API token for authentication purposes within the system. This process allows users to manage access credentials through the administrative interface.

Follow these steps to create an API token.

Procedure

1. From the main menu, choose **Admin** > **API** > **Token**.
2. Click **+ New token**.

   The **Token** window appears.
3. Enter a name.
4. Use the **Status** toggle button to disable authorization for the token if you plan to use it later and want to prevent access until then.
5. Set an **Expiration time**.
6. Click **Create**.

   After the token creation, token appears in the list available on the **API** page.
7. Click **Show** to view the token.
8. Click copy icon to copy it.

What to do next

For more information about the REST API refer to the REST API user documentation available on cisco.com.

API Documentation

Provides a centralized interface for exploring API routes, testing requests, and reviewing data models. This feature enables developers to perform real-time API calls and generate curl commands for integration.

The API Documentation is a development feature that provides comprehensive route specifications, data response models (data type, code values and meaning), and request testing capabilities.

- Route exploration and parameter configuration
- Real-time request testing for GET, DELETE, and POST methods
- Data model and response type definitions

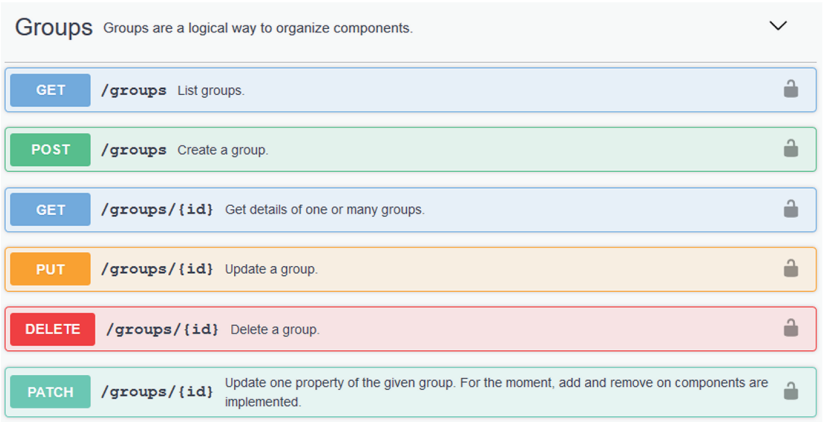
You will get real results from the Center dataset. Specifications about routes are available such as the route's structure, and parameters and arguments that can be set. An URL is generated and curl can be used in a terminal as it is.

However, for an advanced use, you must create an application that will send requests to the API (refer to the REST API documentation).

API Documentation Features and Usage

Routes are classified by 's elements type, including activities, baselines, components, flows, and groups.

The following image illustrates the category "Groups" containing all possible group routes:



Important

All routes other than GET will modify data on the Center. As some actions cannot be reversed, use DELETE, PATCH, POST, PUT with caution.

Authorize API communication

Authorizes access to routes to enable secure API communication. This procedure details the steps to configure authorization and execute API requests.

To authorize API communications:

Procedure

1. From the main page, choose **Admin** > **API**.
2. Click **Token** to create and/or copy a token .
3. Click **Documentation** .
4. Click **Authorize** .

   The **Available authorizations** panel appear.
5. Paste the token in **Value** field.
6. Click **Authorize** .

7. Click **Close**.

   Close lockers displays. They indicate that routes are secured and authorization to use them is up.

Use an API route

Executes an API route to deploy and test functionality. This process involves configuring parameters, running the request, and managing authorization tokens.

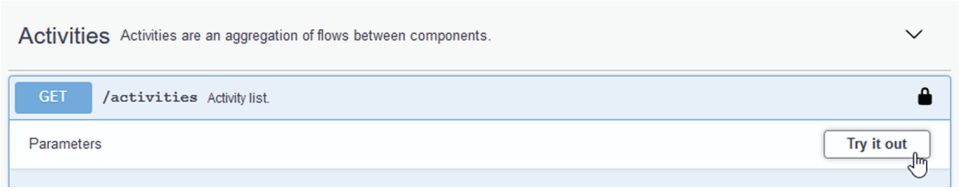
To use a route:

Procedure

1. Click a route to deploy it.

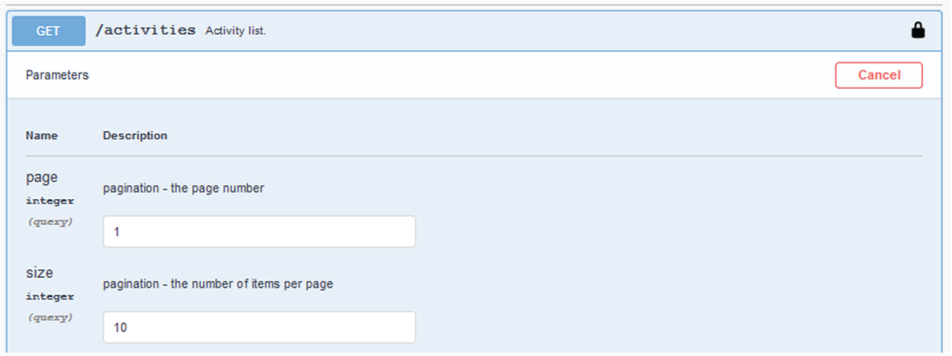
   In the example, we choose Get activity list.

2. Click **Try it out**.



3. Set the **Parameters**.

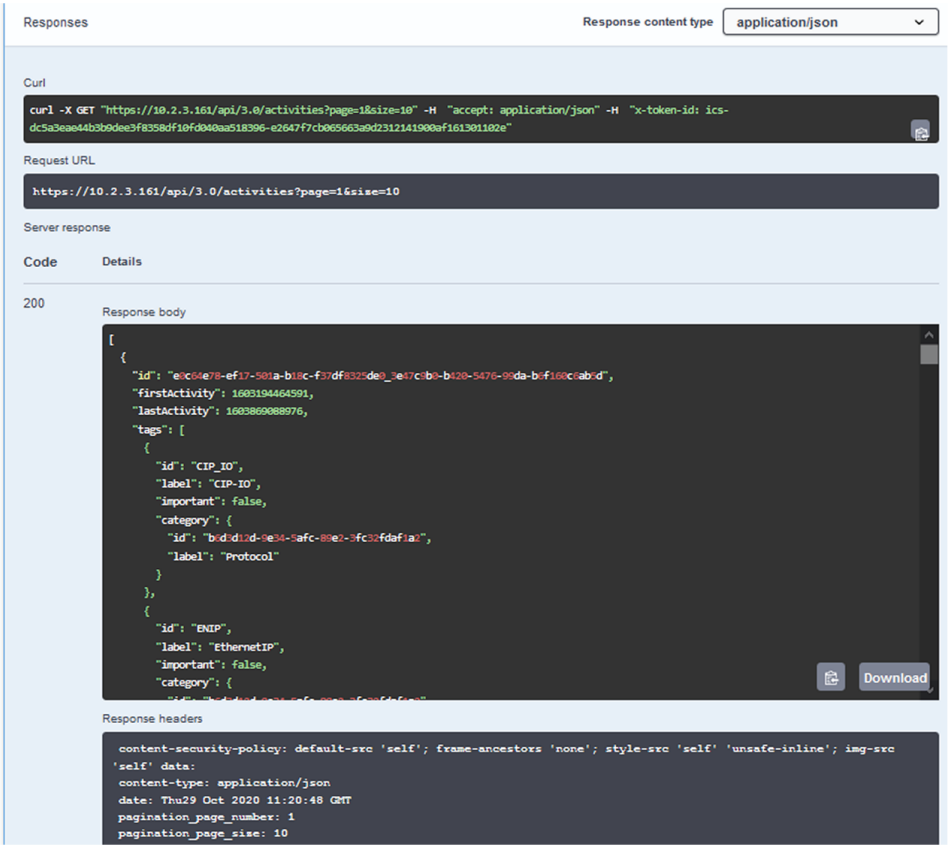
   In the example, we set page to 1 and size to 10.



4. Click **Execute**.

> **Note**
>
> You can only execute one route at a time.

   A loading icon appears for a few moments. Responses display with curl, Request URL and the server response that you can copy or even download.



5. When you are finished, click the **Authorize** button.
6. Log out to clear the token variable, and click **Close**.

Active Discovery policies

Describes Active Discovery policies used to scan industrial networks for device identification and property gathering. These policies define the protocols and parameters applied to sensors to discover unseen devices and analyze network responses.

Active Discovery is a network scanning mechanism that allows a sensor to send packets to the network to discover previously unseen devices and gather additional properties for known devices.

- Operates in Broadcast and Unicast modes.
- Analyzes responses via Cisco Cyber Vision.
- Defines protocols and parameters for industrial network scanning.

For more information, refer to the Active Discovery Configuration Guide .

Access Active Discovery policies

Displays the Active Discovery policies page to manage discovery configurations. This interface allows administrators to view and modify existing discovery settings within the system.

Follow these steps to access active discovery policies.

Procedure

1. Navigate to **Admin** .
2. Select **Active Discovery** .
3. Select **Policies** from the menu.

LDAP

Describes the integration of external LDAP services with Cisco Cyber Vision to delegate user authentication. This feature enables centralized access management using Microsoft Active Directory or AD LDS services.

LDAP is an external authentication service that allows Cisco Cyber Vision to delegate user verification to directory servers.

- Supports Microsoft Active Directory and AD LDS services.
- Enables mapping of external directory groups to internal user roles.
- Enables both unencrypted and secure certificate-based connections for authentication.

LDAP connections configuration and management

LDAP services can be configured and managed from **Admin** > **External Authentication** > **LDAP**

Role Mapping Guidelines

The following guidelines apply to role mapping and authentication:

- Role Mapping: External directory groups can be mapped to Product, Operator, Auditor, or custom roles. See Users to create custom roles.
- Admin Role: The Admin user role is reserved for internal usage and cannot be mapped to external users.

Connection Testing

After configuration, verify the LDAP connection by authenticating with valid external directory credentials using the LDAP test connection window.

Authentication Source

When logging into Cisco Cyber Vision, the login format used will determine the base (i.e. internal or external) to be queried:

The login format determines the authentication source:

- Email: Queries the internal Cisco Cyber Vision database.
- Domain format: Using <domain_name>\<user_name> (e.g. cisco\john_doe) triggers authentication via the external directory.

Configure LDAP

Configures LDAP settings in Cisco Cyber Vision to enable external authentication via unencrypted or secure connections. This process includes defining server parameters, mapping roles, and verifying the connection with user credentials.

This taskflow takes you through configuring LDAP in Cisco Cyber Vision using an unencrypted connection or a secure connection.

You can establish two types of secure connections:

- For a highly secure connection, choose the **LDAP over TLS/SSL** setting to use a CA-signed certificate with a trust chain. You must upload the certificate into the Center during the configuration task.
- For internal applications where trust is not a primary concern, choose the **Use self signed certificate** setting. The Center automatically generates and uses self-signed certificates for this connection type. You don't need to provide a self-signed certificate.

Procedure

1. From the main menu, choose **Admin** > **External Authentication** > **LDAP** .
2. Click **New Settings** .
3. In the **Settings** tab,
   a) Choose **LDAP over TLS/SSL** or **Use self signed certificate** , or neither.
   b) Enter **Primary Server Address** and **Primary Server Port** .
   c) (Optional) Enter **Secondary Server Address** and **Secondary Server Port**.
   d) In the **Base DN** field, enter the distinguished name by which LDAP API recognize this LDAP connection.
   e) (Optional) Check the **Modify search filter** check box. Then, in the **Search Filter** field, enter a search filter.

      The default search filter retrieves a user's groups by binding with the user's credentials. You can also modify the filter to target a different attribute, and the specified attribute's value is then used for both group search and binding (login).

      In the **Search Filter** field, you must include the *$user* variable. The variable is replaced with the username entered when logging in.

   f) In the **Server Response Time** field, enter a timeout value, in seconds, after which the Center attempts to connect to the secondary server instead of the primary server.
   g) (Optional) Check the **Use Service Account** check box. When an LDAP user doesn't have access to their own group, a service account is used. When this setting is enabled, the service account is used to search for and retrieve the user's groups.
      1. Enter a service account username.
      2. Enter a service account password.

   h) If you chose **LDAP over TLS/SSL** in Step a, a certificate upload field is displayed. Upload or drag-and-drop a PEM file, root or chain certificate.

      The uploaded certificate is displayed at the bottom of the settings page.
4. In the **Role Mapping** tab,
   a) Map at least one role, default (Product, Operator, or Auditor) or custom, with an Active Directory group. You can create custom roles in the **Custom roles** area.

      Note

      Enter the exact group names as configured in the remote directory for successful retrieval and mapping to user roles.

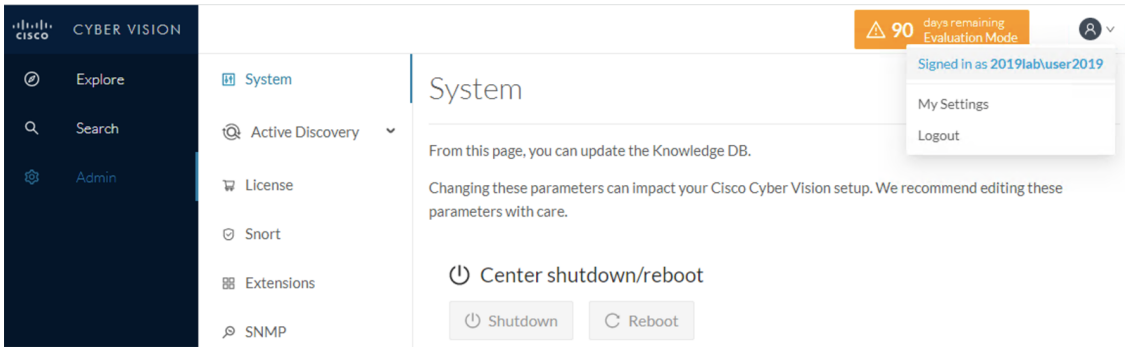
      The Admin role is not listed as a default role because it is reserved for Cisco Cyber Vision internal usage and cannot be mapped to external users.
5. Click **OK** .

6. Click **Test connection**.
7. Enter the user credentials to test the connection between Cisco Cyber Vision and Active Directory.

> **Note**
>
> For LDAP, the supported username format is *<domain_name>|<user_name>* (For example, cisco\john_doe).
>
> For LDS, the supported username formats are:
>
> - *<user_name>* (For example, john_doe).
> - *<email-address>* (For example, john@example.com)

8. Click **OK** .

You can also test the connection by logging out of Cisco Cyber Vision and logging in with different mapped user credentials. The Center menu changes according to the permissions granted to the user.



Single sign-on (SSO)

Introduces SSO as an authentication mechanism enabling access to multiple applications with a single login, details its security benefits, outlines SAML 2.0 support, and describes centralized authentication, federated service provider integration, and improved user experience.

Single sign-on (SSO) is an authentication mechanism that

- allows users to access multiple applications using a single set of credentials,
- reduces the need for multiple logins and password management, and
- enhances security by centralizing authentication.

Table 22: Feature History Table

Feature	Release Information	Feature Description
SAML 2.0 SSO authentication support	Release 5.3.x	Cisco Cyber Vision Center supports SAML 2.0 SSO authentication.

Central authentication and authorization

This security mechanism uses a central identity provider (IdP) to manage user credentials and access permissions across multiple platforms. It consolidates authentication into a streamlined process.

Federated service provider applications

Applications configured to work with SSO, allowing users to access resources through federated authentication.

Additional reference information

With SSO, a user logs in once to access all authorized service provider applications without re-entering credentials, resulting in improved user experience and streamlined access control.

SAML single sign-on

Describes an authentication approach that enables users to access multiple applications through a central identity provider. This method improves security and efficiency by eliminating the need for repeated login credentials.

SAML single sign-on is an authentication approach that:

- enables users to authenticate once and gain access to multiple applications through a central identity provider,
- uses Security Assertion Markup Language (SAML) 2.0 to securely exchange authentication and authorization data, and
- eliminates the need for repeated login credentials for each service.

After successful authentication by the identity provider (IdP), users are redirected back to their service. The browser manages all communication between the service and the IdP. As a result, services such as Cisco Cyber Vision Center do not require a direct network connection to the IdP.

SAML single sign-on integration references

The Cisco Cyber Vision Center supports SAML single sign-on with any single sign-on provider that uses the SAML 2.0 standard, such as the following:

- For Azure setup: See Microsoft Entra ID single sign-on integrations .
- For Cisco Duo setup: See Duo Single Sign-On solutions .

Requirement: SSO configuration for Cisco Cyber Vision Center

Provides requirements for configuring SSO within the Cisco Cyber Vision Center. These guidelines ensure secure authentication and proper integration with identity providers.

Ensure that you meet these requirements when configuring SSO for Cisco Cyber Vision Center:

- Only admin users authenticated internally can configure SSO.
- Use only one SSO provider at a time (for example, Azure or Duo).
- Initiate SSO only from the Cisco Cyber Vision Center, not from the identity provider (IdP).
- Review audit logs to monitor login and log out events for SSO. The Cyber Vision Center records and sends these events through syslog.
- Ensure that the Cyber Vision Center host name (FQDN) is DNS resolvable.

  Cisco Cyber Vision generates the SAML Entity ID, Assertion Consumer Service (ACS) URL, and service provider metadata by using the configured Center FQDN. If users access the Center through a reverse proxy or load balancer, the FQDN configured on the Center must match the FQDN that users enter to access the Center.

- A center can only be configured with SSO if LDAP is disabled or not configured.
- To prevent authentication conflicts, local user accounts and SSO user accounts must be distinct.

Configure SAML SSO through a reverse proxy

Guides administrators through aligning the Cyber Vision Center FQDN with the public FQDN used by clients, configuring a reverse proxy for SAML ACS requests, and updating the identity provider after the Center FQDN changes.

To ensure SAML single sign-on (SSO) works reliably for clients accessing the Cyber Vision Center through a reverse proxy by aligning FQDNs and updating configurations.

The Cyber Vision Center builds its SAML service-provider identity and URLs, including the Entity ID, metadata URL, and Assertion Consumer Service (ACS) URL, from the Center's configured FQDN. These values are not derived from the URL that a user enters in the browser.

When users access the Center through a reverse proxy or load balancer, the Center's configured FQDN must match the public FQDN used by clients.

If the reverse-proxy FQDN differs from the configured Center FQDN, SAML SSO with Microsoft Entra ID (Azure AD) can fail after IdP authentication succeeds. The browser posts the response to https://<Center FQDN>/saml/acs instead of the proxy FQDN, which users cannot reach, so login does not complete.

Before you begin

Ensure that the client machines can resolve the public FQDN used to access Cyber Vision Center.

Configure the reverse proxy to accept the public FQDN in the Host header, present a certificate valid for that FQDN, and forward requests to /saml/acs without redirecting the request or changing its POST body.

Follow these steps to configure SAML SSO through a reverse proxy.

Procedure

1. Check the currently configured Center FQDN.

   To display the current Center FQDN, run `sbs -config --get fqdn`

2. Compare the configured Center FQDN with the public FQDN that users enter in their browser to access the Center through the reverse proxy or load balancer.
3. If the configured Center FQDN and the public FQDN are different, update the Center FQDN: `sudo setup-center-cli pki <FQDN>`

   Replace <FQDN> with the public FQDN that users use to access the Center.

   The Center regenerates its internal certificate using the new FQDN.

4. If you changed the Center FQDN, restart the Center services or reboot the Center.
5. Configure the reverse proxy or load balancer:
   - Accept the public FQDN in the Host header.
   - Present a TLS certificate that is valid for the public FQDN.
   - Forward SAML ACS requests to the Center.
   - Forward POST requests to `/saml/acs` without redirecting them.
   - Preserve the request body when forwarding requests to `/saml/acs`.

6. Update the SAML service-provider configuration in Microsoft Entra ID:
   a) Import the Center service provider metadata again.

b) Set **Identifier (Entity ID)** to `https://<FQDN>/saml/metadata`. Use the currently configured Center FQDN.
c) **Reply URL** to `https://<FQDN>/saml/acs`. Use the currently configured Center FQDN.

Cyber Vision Center's SAML service-provider URLs use the public FQDN accessible through the reverse proxy. The Microsoft Entra ID SAML configuration matches these URLs, ensuring reliable single sign-on (SSO).

Single sign-on user accounts

Describes the function of single sign-on user accounts in managing identity credentials across multiple systems. This approach simplifies user access by centralizing authentication through an identity provider.

A single sign-on (SSO) user account is a user identity credential that:

- allows access to multiple applications, systems, or services with a single set of login credentials,
- uses a central identity provider (IdP) to handle authentication, and
- simplifies the user experience by removing the need for separate logins for each system.

Role and configuration of SSO accounts

The identity provider (IdP) manages users and groups directly or imports them from external directories such as Active Directory, RADIUS, or LDAP. The IdP sets most account details for SSO users, including usernames and passwords.

A single sign-on account appears on the Cisco Cyber Vision Center users page only after the user has logged in successfully for the first time.

Both single sign-on accounts and the NameID attribute provided by the IdP during SAML login require valid email addresses. By default, many IdPs use the user's username as the NameID attribute. Confirm your IdP's behavior when configuring it and when creating user accounts for SSO access to Cyber Vision Center.

User role mappings for SSO users

Describes configuration mappings that associate identity provider user groups with system roles to enable centralized access management. These mappings use dynamic attributes to determine user permissions within the environment.

Role mappings for SSO users are configuration mappings that:

- associate user groups from an identity provider (IdP) with roles in the Cyber Vision Center,
- use role attributes to determine user permissions dynamically, and
- enable centralized management of user access through SSO integration.

Coordination and configuration details

The following guidelines apply to coordinating with your IdP and managing role attributes:

- Role assignment: Set up user roles at the Cyber Vision Center and coordinate them with your SSO IdP application settings. Assign roles to groups defined in the IdP.
- SSO federation understanding: Review how users, groups, and roles are organized in your IdP and configure user role mapping effectively. Consult the IdP vendor documentation for guidance on creating or importing users or groups.
- Role attribute at the IdP: The IdP sends a role attribute, which lists the groups a user belongs to in the IdP.
- SSO configuration details: The SSO configuration specifies the name of the role attribute and includes a list of expressions mapped to Cyber Vision Center user roles.

Provide the email address attribute only if you need to migrate local users to SSO. When you configure SSO with the email address attribute, the system identifies the logged-in user's email address from the SAML assertion. If a user exists with that email address, the system removes that user from local authentication. Afterward, the user can only log in with SSO. If needed, create a new internal user.

Microsoft Entra ID single sign-on integrations

This section explains Microsoft Entra ID single sign-on integrations. It describes how these integrations provide centralized authentication, simplify user access management, and support secure connectivity for cloud and on-premises applications.

A Microsoft Entra ID single sign-on integration is an authentication solution that

- uses Microsoft's multi-tenant, cloud-based Azure Active Directory to manage user identities,
- enables secure and centralized access to both cloud and on-premises applications (such as Cyber Vision Center), and
- allows users to authenticate with a single account across multiple services through federation.

Within Azure, a tenant is an entity that manages joined devices for one or more organizations. With a single sign-on account, you can access these devices seamlessly. Familiarize yourself with the Azure tenant structure before onboarding applications like Cyber Vision Center.

Add an enterprise application to your Azure tenant

Learn how to add a custom enterprise application to your Azure tenant for integration and identity management.

Allow integration of external services or custom apps with your organization's Azure environment.

Before you begin

- Ensure you have an Azure account with an active subscription. Create a free account at Build in the cloud with an Azure account.
- Your account must have the **Application Developer** role or higher.

Procedure

1. Sign in to the Microsoft Entra admin center.
2. From the main page, choose **Applications** > **Enterprise applications** > **All applications**.
3. Select **New application** and click **Create your own application**.
4. Enter the application name.
5. Enable **Integrate any other application you don't find in the gallery (Non-gallery)**.
6. Click **Create**.
7. Enter the display name and select **Supported account types**.
8. Click **Register**.

The new application appears in **Home** > **Enterprise applications** > **All applications**.

What to do next

To configure the new application further, open it from **Home** > **Enterprise applications** > **All applications**. For further details, see Configure Azure SSO for Cyber Vision Center.

Configure Azure SSO for Cyber Vision Center

Learn how to configure Azure Single Sign-On (SSO) for Cyber Vision Center to centralize user authentication and streamline role management with Microsoft Azure Active Directory.

Set up Azure SSO integration so Cyber Vision Center users can authenticate using their Azure Active Directory credentials.

Use this procedure to integrate Cyber Vision Center with Azure SSO. This enables centralized authentication and simplifies role assignments managed via Azure groups.

Before you begin

- Create the Cyber Vision Center service provider application in Azure. See Add an enterprise application in Azure.
- Prepare your Azure tenant for integration.
- Ensure the Cyber Vision Center hostname is a resolvable DNS entry.
- Verify that usernames and NameID attributes are valid email addresses.
- You can provide multiple groups. Assign roles to users based on priority.

> **Note**
>
> If Cyber Vision Center offers multiple accessible URLs, SSO users must always use the configured login URL.
>
> The Center FQDN is used to generate the SAML Entity ID and ACS URL. Users must access the Center with the same FQDN configured on the Center, even when using a reverse proxy or load balancer. Accessing the Center with a different URL does not change the generated SAML URLs.

Procedure

1. Sign in to the Microsoft Entra admin center.
2. From the main menu, choose **Applications** > **Enterprise applications** > **All applications**.
3. Select the created application.
4. Click **Single sign-on** and select **SAML**.
5. In **Basic SAML Configuration**, enter the service provider URLs that use the Cyber Vision Center's configured FQDN:
   - For **Identifier (Entity ID)**, use: Append /saml/metadata to the Cyber Vision Center login URL.

     Format: https://<Center-FQDN>/saml/metadata
   - For **Reply URL (Assertion Consumer Service URL)**, use: Append /saml/acs to the login URL.

     Format: https://<Center-FQDN>/saml/acs

> **Note**
>
> If users access the Center through a reverse proxy or load balancer, use the FQDN configured on the Center. It must match the FQDN users use to access the Center through the proxy.

6. In **Attributes & Claims**:
   a. Click **Add a group claim**.
   b. Select **All groups** to show the groups associated with the user in the **Group Claims** panel.
   c. Select **Group ID** as a **Source attribute**.
   d. Select **Customize the name of the group claim** under **Advanced options**.
   e. Enter **Name (required)** and save.
7. Assign existing Azure users and groups to the Cyber Vision Center service application.
8. Record these details from **SAML-Based Sign-On** for later use:
   - **Login URL**
   - **Microsoft Entra Identifier**
   - **Certificate (Base64)** file (download it)
   - **Federation Metadata XML** (download it)
   - **Object ID** (Group ID)

When Cyber Vision Center is ready to support Azure SSO, you can sign in using your Azure Active Directory credentials.

What to do next

To complete Azure SSO integration, configure Cyber Vision Center. For more information, see Configure Cyber Vision Center for Azure SSO.

Configure Cyber Vision Center for Azure SSO

Configures Azure Single Sign-On authentication for users accessing the Cyber Vision Center. This procedure enables centralized identity management for the platform.

Enable Azure Single Sign-On (SSO) authentication for users accessing Cyber Vision Center.

Before you begin

- Use the SAML SSO management application to configure a service provider application for the Cyber Vision Center and assign users or groups to it. See Configure Azure SSO for Cyber Vision Center .
- Have the following Azure configuration details from Configure Azure SSO for Cyber Vision Center :
  - **Name (Required)**
  - **Federation Metadata XML**
  - **Login URL**
  - **Microsoft Entra Identifier**

- **Certificate (Base64)**
- **Object ID** (Group ID)

Procedure

1. From the main menu, choose **Admin** > **External Authentication** > **Single Sign-On** .
2. Click **New Settings** .
3. Add **Role Attribute** and **Email Attribute** (Optional).

   For **Role Attribute** , enter **Name (Required)** used for the group claim.
4. Configure Azure SSO credentials using one of these methods:
   a. Upload the **Federation Metadata XML** file under the **Upload XML file** field.
   b. For **Manual Configuration** :
      - Enter the **Login URL** in the **Identity Provider Single Sign-On (SSO) URL** field.
      - Enter the **Microsoft Entra Identifier** in the **Identity Provider (Idp) Issuer URL** field.
      - Add the **Certificate (Base64)** in the **X509** field.
5. Click **Role Mapping** .
6. Enter the **Object ID** (Group ID) in the **Default roles** or **Customer roles** field.
7. Click **OK** .

The **Login with SSO** button appears on the Cyber Vision Center login screen.

What to do next

Click **Login with SSO** to access the Cyber Vision Center using Azure SSO authentication.

Resolving SAML SSO failures through reverse proxies

Describes how to identify and resolve SAML SSO failures when accessing the Center through a reverse proxy. Provides steps to capture and analyze SAML exchanges, compare FQDNs, and verify proxy routing to isolate the cause of authentication issues.

When the reverse-proxy FQDN does not match the configured Center FQDN, SAML SSO with Microsoft Entra ID (Azure AD) can fail even after successful IdP authentication. Common issues include:

- FQDN mismatches preventing SAML SSO completion.
- Proxy routing issues leading to HTTP 503 errors and authentication failures.

Summary

This process assists administrators in diagnosing and resolving SAML SSO failures that occur when the reverse proxy FQDN differs from the Center's configured FQDN, helping ensure seamless authentication to the Center.

The key components involved in the process are:

- Administrator: Captures and analyzes SAML exchanges, inspects FQDN values, and verifies proxy routing.
- Reverse proxy: Forwards authentication requests and must correctly route SAML POSTs to the Center.

The process consists of these stages:

Workflow

1. **Capture SAML exchange**: Use SAML-tracer or browser developer tools to record SAML authentication flow details.
2. Inspect SAML response values: Examine Destination, Recipient, and Audience fields to see how the Center constructs them.
   - Destination and Recipient use https://<Center-FQDN>/saml/acs.
   - Audience uses https://<Center-FQDN>/saml/metadata.
3. **Compare FQDNs**: Check if the FQDN in the SAML response values matches the FQDN accessed via the reverse proxy.

   Ensure the configured Center FQDN equals the FQDN users use through the proxy. If mismatched, browsers may post SAML responses to unreachable addresses.
4. **Verify proxy routing**: Confirm that the reverse proxy accepts the public FQDN in the Host header and forwards the `/saml/acs` POST request properly. The proxy must present a valid certificate, preserve the POST body, and forward the request without a redirect.Verify that the reverse proxy accepts the public FQDN in the Host header and forwards the /saml/acs POST request to the Center.
5. **Troubleshoot HTTP 503 errors**: If the proxy returns HTTP 503, verify the ACS request reaches the Center's HAProxy service. If the Center FQDN and the public FQDN do not match, correct the configuration described in Configure SAML SSO through a reverse proxy on page 81.

Duo Single Sign-On solutions

Provides a cloud-hosted identity provider that simplifies user authentication and device management. It enables organizations to secure SAML and OIDC applications with robust two-factor authentication and flexible security policies.

A Duo single sign-on (SSO) is a cloud-hosted identity provider that:

- facilitates inline user enrollment,
- offers self-service device management, and
- supports various authentication methods, including passkeys and security keys, Duo Push, or Verified Duo Push in the Universal Prompt.

Duo Single Sign-On overview and policy control

You add two-factor authentication and flexible security policies to any SAML application with Duo Single Sign-On .

Cyber Vision Center uses Duo's strong authentication and flexible policy engine in the applications that comply with Security Assertion Markup Language (SAML) 2.0 or OpenID Connect (OIDC) authentication standards. Duo Single Sign-On serves as an identity provider (IdP). It authenticates users through existing on-premises Active Directory or any SAML 2.0 identity provider, and requires two-factor authentication before granting access to the service provider's application.

Duo Single Sign-On offers various plans for different needs:

- Duo Premier: Includes advanced features and support.
- Duo Advantage: Builds on the Basic plan with additional features.
- Duo Essentials: Provides essential security features.

Administrators can define application policies based on their plan. For example, some applications may enforce two-factor authentication at each login, while others limit login to once every seven days. Duo evaluates the user, device, and network against the application policy to determine access.

Requirement: Prerequisites for Duo Single Sign-On setup

Outlines the necessary administrative access, authentication sources, and infrastructure requirements for configuring Duo Single Sign-On. These prerequisites ensure successful integration and connectivity between your identity providers and the Duo environment.

Obtain Duo Admin access with one of the following roles: Owner, Administrator, or Application Manager.

Configure a primary authentication source by setting up either an Active Directory connection or a SAML 2.0 identity provider.

- Complete all authentication source setup steps for Duo Single Sign-On (SSO) separately from any directory sync setup.
- Provide a SAML 2.0 service provider or OIDC relying party web application to protect with Duo SSO.

Active Directory requirements

If you use Active Directory as your authentication source, ensure the following infrastructure requirements are met:

- Provide at least one standalone server (Windows or Linux) that can communicate with your Active Directory domain controllers.
- Supply service account credentials for Active Directory.
- Ensure access to DNS for the user email domains associated with SSO so you can add TXT records as required.

Verify the fully qualified domain name (FQDN) of the Cyber Vision Center is reachable.

Configure Cyber Vision Center application in Duo

Integrates the Cyber Vision Center application with Duo for user authentication using SAML Single Sign-On. This procedure configures Duo as a SAML identity provider for the Cyber Vision Center application.

Integrate the Cyber Vision Center application with Duo for user authentication using SAML Single Sign-On.

Before you begin

- Ensure you have users and groups configured in Duo.
- Verify that Duo users have an authentication source and a proxy. For details, see https://duo.com/docs/sso#external-authentication-sources .

Procedure

1. Log in to the Duo Admin Panel .
2. From the main menu, choose **Applications** > **Application Catalog** .
3. Locate the **Generic SAML Service Provider** labeled "SSO" and click **+ Add** .

   Use the **Documentation** link to review integration requirements and steps before adding the new application.
4. Enter **Application name** .
5. Select **User access** option.

> **Note**
>
> Users cannot access new applications until user access is granted.

6. Enter these details under **Service Provider** :
   - **Entity ID** :
     - Use the "/saml/metadata" with the Cyber Vision Center login URL.
     - Format: https://{Hostname}/saml/metadata
   - **Assertion Consumer Service (ACS) URL** :
     - Use the path "/saml/acs" with the login URL.
     - Format: https://{Hostname}/saml/acs

   The Metadata section presents SAML identity provider details for Duo Single Sign-On in the table.

Name	Description
Entity ID	The global, unique name for Duo Single Sign-On. Sometimes referred to as "Issuer."
Single Sign-On URL	The authentication URL for Duo Single Sign-On. This is sometimes referred to as "SSO URL" or "Login URL". The URL is used to start IdP-initiated authentications.
Single Log-Out URL	This optional field specifies the logout URL for Duo Single Sign-On, sometimes referred to as the “SLO URL” or “Logout Endpoint. This field is optional.
Metadata URL	This URL can be used by service providers to download the XML metadata from Duo Single Sign-On.
SHA - 1 Fingerprint	The SHA-1 fingerprint of the SAML certificate. Sometimes service providers will request a fingerprint instead of uploading a SAML certificate.
SHA - 256 Fingerprint	The SHA-256 fingerprint of the SAML certificate. Service providers may request a fingerprint instead of a SAML certificate.
Certificate	The certificate used by the service providers to validate the signature on the SAML response sent by Duo Single Sign-On. Click **Copy certificate** .
SAML Metadata	Service providers use the XML SAML Metadata from Duo Single Sign-On to configure settings. Click the **Download XML** to download the xml file.

7. In **Map attributes** :
   a. Select **Email Address** in the **IdP Attribute** field.

b. Enter an attribute name in the **SAML Response Attribute** field (for example, "email").

> **Note**
>
> Configuring the Email attribute is optional.

8. In **Role attribute** :
   a. Add an **Attribute name** , for example "GroupName".
   b. Map **Service Provider's Role** with **Duo groups** .
9. Click **Save** .

The Cyber Vision Center application is integrated with Duo and ready to use SAML for authentication.

What to do next

Configure the Cisco Cyber Vision Center for Duo. See Configure Cisco Cyber Vision Center for Duo .

Configure Cisco Cyber Vision Center for Duo

Configures SSO login on Cisco Cyber Vision Center using Duo as an identity provider. This procedure enables centralized authentication after preparing the required Duo configuration details.

Enable SSO login on Cisco Cyber Vision Center using Duo as an identity provider.

Before you begin

Obtain these Duo SSO details from Configure Cyber Vision Center application in Duo :

- **Attribute name**
- **SAML Response Attribute**
- **SAML Metadata** xml file
- **Single Sign-On URL**
- **Entity ID**
- **Certificate**
- **Service Provider's Role**

Follow these steps to centrally configure SSO authentication after preparing Duo configuration details.

Procedure

---

1. From the main menu, choose **Admin** > **External Authentication** > **Single Sign-On** .
2. Click **New Settings** .
3. Enter **Attribute name** in the **Role Attribute** field.
4. Enter **SAML Response Attribute** in the **Email Attribute** field.

> **Note**
>
> Configuring the Email attribute is optional.

5. Complete the configuration using one of these methods:
   a. Upload the **SAML Metadata** XML file under the **Upload XML file** field.
   b. For **Manual Configuration** :
      - Enter the **Single Sign-On URL** in the **Identity Provider Single Sign-On (SSO) URL** field.
      - Enter the **Entity ID** in the **Identity Provider (Idp) Issuer URL** field.
      - Add the **Certificate** in the **X509** field.
6. Select the **Role Mapping** tab.
7. Enter **Service Provider's Role** details in the **Default roles** or **Custom roles** field.
8. Click **OK** .

After you complete the configuration, the **Login with SSO** button appears on the Cyber Vision Center login screen.

What to do next

Use the **Login with SSO** button to test SSO login via Duo.

Sensors

Details sensor management, including using the Sensor Explorer, filtering and sorting, reviewing sensor statuses, managing features such as installation and updates, handling credentials, organizing sensors, setting capture modes, and managing deployment tokens, templates, and management jobs

Sensors in Cisco Cyber Vision are devices or applications deployed at strategic points within the industrial network to capture and analyze network traffic.

Sensors communicate with the Cyber Vision Center to send metadata extracted from industrial network traffic, enabling deep packet inspection and network visibility.

Sensor Explorer

Provides a centralized interface to install, manage, and monitor sensors across the industrial network. This page enables users to oversee sensor deployment and capture traffic data for network analysis.

The Sensor Explorer is a management interface that enables the administration of sensors monitoring industrial network traffic.

- Supports installation and configuration of sensors.
- Provides visibility into sensor status and network data.
- Facilitates management of both online and offline traffic capture modes.

Sensor Operational Modes

Sensors operate in specific modes depending on the deployment requirements and hardware capabilities:

- **Online mode** : A sensor is placed at a strategic network point to continually capture traffic. Applicable to Cisco IE3400, IE3300 10G, Cisco IC3000, Catalyst 9300, and Cisco IR1101.
- **Offline mode** : A sensor is connected to isolated or difficult-to-access network points to occasionally capture traffic on a USB drive for import into Cisco Cyber Vision. Only applicable to Cisco IC3000.

Table 23: Feature History

Feature	Release Information	Feature Description
Sensor Management extension removal	Release 5.6.0	The Sensor Management extension is no longer available. Sensors that were previously deployed through the Sensor Management extension are now fully managed from the Sensors Management page in the new UI.

Note

When the Cisco Cyber Vision system is updated to version 5.6.0 and rebooted, the legacy Sensor Management extension is removed. Sensors previously deployed using the Sensor Management extension are integrated into the sensor-host model in the new UI.

Manual sensor deployment, Docker sensors deployment, and Sensor VM deployment are only supported in the **Sensor Explorer** page.

Filter and Sort the Sensor List

Organizes the sensor list by applying filters or sorting columns to locate specific folders and sensors based on attributes such as IP address, health, and status.

Filtering

Use the Filter button to filter the folders and sensors in the list by label, IP address, version, location, health, and processing status.

Sorting

The sort icons next to the column titles allow you to organize sensors by label, IP address, version, location, health, and processing status in either alphabetical or ascending/descending order. The icons appear when you hover over them or apply them.

Follow these steps to filter sensor list.

Procedure

1. From the main menu, choose **Admin** > **Sensors** > **Sensor Explorer**.
2. Click the Filter icon from the top-right corner of the table.
3. Type in the field or select from the drop-down menu to locate the folder(s) or sensor(s).

4. Click **Apply**.

Sensor statuses

This section lists possible values and meanings for sensor health and processing status indicators.

Use sensor status indicators to track the enrollment stage of each sensor, check its connection to the Center, and monitor or troubleshoot deployments. Two sensor status types are available.

- **Health status**: Shows the sensor's progress in the enrollment and authorization process.
- **Processing status**: Shows the current state of network data processing and communication between a sensor and the Center.

Table 24: Health status indicators

Indicator	Description
New	The sensor's initial status when first detected. The sensor requests an IP address from the DHCP server.
Request Pending	The sensor has requested a certificate and is waiting for authorization to enroll.
Authorized	The sensor has just been authorized by an administrator or product user. Remains briefly before changing to Enrolled.
Enrolled	The sensor is successfully connected with the Center and has a certificate and private key.
Disconnected	The sensor is enrolled but not connected to the Center (may be offline or there may be a network issue).
Bad Credentials	The sensor is enrolled but credentials to access the Local Manager are not correct.

Table 25: Processing status indicators

Indicator	Description
Disconnected	The sensor is enrolled but not connected to the Center (shut down, problem, or network issue).
Not enrolled	The sensor is not enrolled (Health status is New or Request Pending). You must enroll the sensor to operate it.
Normally processing	The sensor is connected to the Center; data is being sent and processed.
Waiting for data	The sensor is connected; the Center has processed all data and is waiting for more to be sent.
Pending data	The sensor is connected; the sensor attempts to send data but the Center is processing other data.

Sensors Features

Describes the management features available for sensors within the Sensor Explorer page. These tools allow administrators to perform maintenance, configuration, and troubleshooting tasks on connected sensors.

Provides a comprehensive list of sensor management features accessible through the Sensor Explorer interface to facilitate traffic analysis, configuration, and system maintenance.

The following features are available for managing sensors:

- **Start recording** : Records a traffic capture on the sensor for traffic analysis or troubleshooting.

  > **Note**
  >
  > This feature is targeted for short captures only. Performing long captures may cause the sensor overload and packets loss.

- **Move to** : Moves the sensor through different folders. For more information, refer to Organize sensors on page 97 .
- **Download package** : Provides a configuration file for manual sensor deployment. Only applicable to the Cisco IC3000. Refer to its Installation Guide .
- **Capture Mode** : Sets a filter on a sensor sending data to the Center. Refer to the procedure for Setting a capture mode .
- **Redeploy** : Reconfigures the sensor, such as changing its IP address.
- **Enable IDS** : Enables the SNORT engine embedded in some sensors to analyze traffic using SNORT rules.
- **Reboot** : Reboots the sensor in case of a malfunction.
- **Shutdown** : Triggers a clean shutdown of the sensor from the GUI.

  > **Note**
  >
  > After performing a shutdown, you must switch the sensor ON directly and manually on the hardware.

- **Uninstall** : Removes an uninstalled sensor from the list or fully uninstalls a sensor, depending on the model or deployment mode.

Access sensor features

Manages sensor configurations and operations through the Sensor Explorer page. This interface provides tools for monitoring, maintenance, and deployment of sensors.

The Sensor Explorer page provides several features to manage and use your sensors. Some buttons are accessible directly from the Sensor Explorer page to manage one or more sensors, while other buttons become available when clicking a sensor in the list.

Follow these steps to access sesnor features.

Procedure

1. From the main menu, choose **Admin** > **Sensors** > **Sensor Explorer**.

2. Click the sensor name from the **Label** column.

   A right-side panel appears with all the features.

Install sensor

Guides you to access the Sensor Explorer page and select a supported method for installing a Cisco Cyber Vision sensor.

Use the Sensor Explorer page to begin installing a sensor.

> **Note**
>
> When the Cisco Cyber Vision system is updated to version 5.6.0 and rebooted, the legacy sensor management extension is removed. Sensors deployed through the sensor management extension are fully integrated into the sensor-host model in the new UI. Go to the Sensor Management page to onboard, manage, and monitor sensors.
>
> Docker sensors and Sensor VM are supported only on the **Sensor Explorer** page.

Procedure

---

1. Choose **Admin** > **Sensors** > **Sensor Explorer** from the main menu.
2. Select a sensor installation method.

   Choose one of the following methods:

   - Install a sensor manually.
   - Capture traffic with an offline sensor. This method applies only to Cisco IC3000.

     For more information about installing a sensor, refer to the corresponding Sensor Installation Guide.
   - Install a Cisco Cyber Vision Sensor on an appliance that runs Ubuntu and Docker.
   - Deploy a Cisco Cyber Vision Sensor VM as a virtual-machine-based sensor.

You have accessed the Sensor Explorer page and identified a supported sensor installation method.

Sensor self-update workflow

Outlines the planned Cisco Cyber Vision sensor self-update workflow, including sensor selection, job creation, update-file validation, and restart with the new version.

Cisco Cyber Vision allows sensor updates regardless of the installation method, and provides the necessary foundation for sensor self-updates. The self-update feature will be functional only in future releases.

Summary

When the feature is available, sensor self-update automatically updates the sensors that you select.

Workflow

When the feature is available, sensor self-update progresses through the following stages.

1. You select the sensors to update.
2. The Center adds a new job to the sensor queue.

3. Each sensor automatically collects and validates the update file.
4. The sensor restarts with the new version.

Update warnings

Updates a sensor when an alert appears on the Sensor Explorer page in the Cisco Cyber Vision Center. This process ensures the sensor runs the latest available software version.

In the Cisco Cyber Vision Center on the Sensor Explorer page, you receive an alert to update the sensor. When this occurs, the latest version number appears in red, and a blue arrow with a tooltip indicates the sensor is upgradeable.

Procedure

1. From the main menu, choose **Admin** > **Sensors** > **Sensor Explorer**.
2. Click the sensor that is upgradeble from the **Label** column.
3. View the right side panel that appears with sensor details.
4. Click **Update**.

Update Sensors

Updates multiple sensors simultaneously using the Sensor Explorer interface. This procedure ensures that selected devices receive the latest configuration or firmware version.

Procedure

1. From the main menu, choose **Admin** > **Senors** > **Sensor Explorer**.
2. Check the checkboxes to select multiple sensors.
3. Click the drop-down arrow of the **More Actions** button.
4. Click **Update sensor**s from the drop-down list.

   The **UPDATE SENSORS** pop-up appears.
5. Click **OK** .

   During the update, a blue circle appears in the **Update status** column. After the update is complete, the version number turns black, and a green symbol appears in the same column.

View update failure details

Guides you to view detailed failure information for an unsuccessful sensor update in the Sensor Explorer page from the main menu.

If the update is unsuccessful, the **Update Status** column displays a red cross and a detailed message.

Procedure

1. Choose **Admin** > **Sensors** > **Sensor Explorer** from the main menu.
2. Hover over the **red cross** in the **Update Status** column.

The update failure details are displayed.

Manage credentials

Guides you to register global credentials in Cisco Cyber Vision for actions that require them, including sensor installation and updates through the IOx extension.

Register global credentials in Cisco Cyber Vision after you configure or change them in Local Manager.

When you register global credentials, you enter them once in Cisco Cyber Vision. Cisco Cyber Vision uses them for actions that require them .

Only one set of global credentials can be used per Cisco Cyber Vision instance. You cannot use different global credentials for multiple sets of sensors in a single instance. If multiple sensor administrators use global credentials, they must use the same credentials registered in Cisco Cyber Vision. You can use global credentials for one set of sensors while other sensors use their own credentials.

Global credentials are stored in Cisco Cyber Vision but are set at the switch level in Local Manager.

> **Note**
>
> If you lose your global credentials, you must refer to switch customer support and documentation.

Before you begin

Configure the global credentials in Local Manager.

Procedure

1. Choose **Admin** > **Sensors** > **Sensor Explorer** from the main menu.
2. Select **Manage Cisco devices**.
3. Select **Manage credentials** from the drop-down list.

   The **SET GLOBAL CREDENTIALS** window appears.
4. Enter your **Login** and **Password**.
5. Select **Update**.

Cisco Cyber Vision uses the registered global credentials for actions that require them, including installing and updating sensors.

Organize sensors

Guides you to create a folder and move a sensor into it to organize your sensor list by location, person in charge, or sensor type.

Use folders to organize sensors by location, person in charge, or sensor type, such as disconnected sensors.

Procedure

1. From the main menu, choose **Admin** > **Sensors** > **Sensor Explorer**.
2. Select **Organize**, and select **+ Create folder** from the drop-down list.
3. Enter a name in the **folder name** field.
4. (Optional) Enter values in the **Location** and **Description** fields.
5. Select **Ok**.

A success message appears, and the new folder appears in the sensor list.

6. Select the checkbox for the sensor that you want to move.
7. Select **Move selection to**.

   The **Move selection to** pop-up appears.

8. Select the drop-down arrow for the **Destination** field.

   Use one of the following options:

   - Select the required folder to move the sensor.
   - Select **+New folder** to create a folder and move the sensor.
   - Select **Root** to move the sensor back to the primary list.

9. Select **Ok**.

   After you move a sensor into the folder, its version, health status, and processing status appear on the folder line. If you move a sensor in a disconnected state into the folder, its information appears on the folder line instead of the connected sensor information. Sensor statuses that indicate lower security are prioritized to draw your attention.

Capture modes

Describes the Capture Mode filters available for Cisco Cyber Vision sensors and their effect on the network traffic analyzed by the sensors.

Capture modes use filters on each sensor to define which types of incoming packets the sensor analyzes. You can set a different filter on each sensor according to your needs.

Use capture modes to focus monitoring on relevant traffic and reduce load on the Center. Capture Mode can improve Cisco Cyber Vision performance on large networks.

Table 26: Capture mode descriptions

Capture mode	Description
ALL	The sensor analyzes all incoming flows without applying a filter and stores all flows in the Center database.
OPTIMAL (Default)	The filter selects the most relevant flows based on Cisco Cyber Vision expertise. It does not record multicast flows. Use this capture mode for long-term capture and monitoring.
INDUSTRIAL ONLY	The filter selects only industrial protocols such as Modbus, S7, and EtherNet/IP. The sensor does not analyze IT flows on the monitored network, and they do not appear in the GUI.
CUSTOM (advanced users)	Use this capture mode to fully customize the filter. Use `tcpdump` syntax to define filtering rules. For example, a firewall filter can remove network management flows (SNMP): `not (port 161 and host 10.10.10.10)`, where `10.10.10.10` is the network management platform.

Set a capture mode

Guides you to select a Capture Mode for a sensor so that it analyzes the network communications that you want to monitor.

Set a Capture Mode for a sensor from the **Sensor Explorer** page.

Capture Mode selects which network communications a sensor analyzes.

> **Note**
>
> You can also set a capture mode in the installation wizard when enrolling sensors during Center installation. This option is recommended if you already know which filter to set.

Before you begin

Allow SSH connections from the Center to the sensors.

Procedure

1. From the main menu, choose **Admin** > **Sensors** > **Sensor Explorer**.
2. Select the sensor name in the **Label** column.

   The right-side panel appears with the sensor details.
3. Select **Capture mode**.

   The **CAPTURE MODE** window appears.
4. Select the radio button for the **Capture Mode** that you want to use.

The sensor uses the selected Capture Mode to determine which network communications it analyzes.

Sensor geolocation data

Introduces sensor geolocation data for CV sensor applications, and outlines GPS coordinates configuration methods for both manual entry and automatic discovery based on platform capabilities.

Sensor geolocation data is the GPS coordinates (longitude and latitude) of CV sensor applications deployed on network devices. This data enables accurate mapping and visualization of the platform hosting the CV sensor application, supporting effective monitoring, management, and optimization of geographically distributed deployments.

GPS coordinates configuration

You can configure GPS coordinates on sensors in two ways, depending on the platform's hardware capabilities:

- Platforms without the capability to gather GPS coordinates by themselves require manual input of the GPS coordinates on the UI. You can set the coordinates on the **Sensor Explorer** page. For more information, see Configure GPS coordinates on sensors on page 101.
- Platforms with the capability to gather GPS coordinates by themselves can automatically discover and update their GPS coordinates. Once the GPS module is activated on the platform, the sensors will seamlessly display the GPS data received from the GPS module, ensuring the coordinates are always current without further manual intervention. For more information, see Enable the GPS module on the platform on page 100.

Enable the GPS module on the platform

Guides you through activating the GPS module on a Cisco platform using CLI, configuring the cellular controller to transmit GPS NMEA data over UDP, specifying satellites, and verifying data reception in CV sensors for sensor geolocation.

Activate the GPS module on the platform to continuously transmit GPS data to the CV Center for sensor geolocation.

Use CLI commands on a Cisco router to configure the cellular controller to transmit GPS NMEA (National Marine Electronics Association) data to a specific IP destination over UDP.

Before you begin

- Verify the correct cellular controller interface name and number (For example, Cellular 0/1/0).
- Obtain the Capture VPG IP address and the sensor's Capture IP address (from eth1 of the IOx app).

Follow these steps to enable GPS module on your platform:

Procedure

1. Log in to the router using SSH.
2. Enter the privileged EXEC mode.

```
router# enable
Password:
router#
```

3. Enter Global Configuration Mode:

```
router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#
```

4. Specify the satellite from which GPS data needs to be collected.

```
router(config-if)# lte gps constellation gnss
```

5. Enable GPS on the device.

```
router(config-if)# lte gps nmea
```

6. Configure transmission of GPS NMEA data over UDP:

```
lte gps nmea ip udp <Capture_VPG_IP> <Sensor_Capture_IP> 5555 stream 1
```

   Replace <Capture_VPG_IP> and <Sensor_Capture_IP> with the actual IP addresses of your device. 5555 is the port number.

The GPS module begins transmitting NMEA data over UDP to the specified destination, and the CV sensors display current GPS coordinates in the **GPS Coordinates** field. When you hover over the value, an indicator confirms that the sensor is in GPS mode.

What to do next

Verify GPS data reception at the target IP. Confirm that the coordinates are current on the **Sensor Explorer** page.

For more information on enabling the GPS module on a router, see Configuring GPS in the *Cellular Pluggable Interface Module Configuration Guide*.

Configure GPS coordinates on sensors

Guides you through manually assigning, verifying, updating, and deleting GPS coordinates on sensors to improve geographic mapping and device management during sensor deployment.

Manually assign GPS location data to sensors for better geographic mapping and device management.

Configure GPS coordinates on sensors when deploying new sensors on network devices.

Before you begin

- Identify the sensors you want to set or update with GPS coordinates.
- Obtain the correct latitude and longitude values for each sensor location.

Follow these steps to manually set GPS coordinates on sensors:

Procedure

1. From the main menu, choose **Admin > Sensors > Sensor Explorer**.
2. On the **Sensor Explorer** page, click the sensor whose GPS coordinates you want to set.
3. On the right side, click the pencil icon next to **GPS Coordinates**.
4. In the SENSOR COORDINATES window, enter the latitude and longitude values. Click **Check on map** to verify the entered values.
5. Once the values are verified, click **Add**.
6. (Optional) To update or delete the values, click the pencil icon again.

The GPS coordinates you set appear in the **GPS Coordinates** field. When you hover over the value, an indicator confirms that the coordinates were set manually.

Deploying sensors with deployment tokens

Describes how deployment tokens support Zero Touch Provisioning of Cisco Cyber Vision sensor batches by using third-party tools such as Cisco Catalyst WAN Manager.

Use Zero Touch Provisioning with third-party tools such as Cisco Catalyst WAN Manager. Refer to the Cisco Catalyst WAN Manager documentation on cisco.com to complete sensor deployment.

On the **Deployment Tokens** page, you can create, edit, enable, disable, and delete deployment tokens for Zero Touch Provisioning.

To access the **Deployment Tokens** page, choose **Admin** > **Sensors** > **Deployment Tokens** from the main menu.

Summary

Zero Touch Provisioning automates Cisco Cyber Vision deployment on batches of sensors by using deployment tokens with third-party tools such as Cisco Catalyst WAN Manager.

Workflow

These stages describe how deployment tokens are used to deploy sensors.

1. You create a deployment phase that groups tokens and specifies their number of uses and expiration time.
2. The application requests a token that is valid for its application type.

A token contains the application name and a PSK (pre-shared key).

3. After Cisco Catalyst WAN Manager is configured, it deploys sensors and applies parameters that allow each sensor to onboard itself on Center.
4. Sensors present the PSK to Center, and Center then delivers the information necessary for enrollment.
5. Deployment fails if the number of sensors exceeds the number of tokens or if deployment occurs after the expiration time.
6. If deployment fails, you can edit the deployment phase to modify the number of uses and extend the expiration time.

Deployment files for sensors

Lists the deployment file that you use for each supported Cisco sensor platform and whether it uses Active Discovery during Zero Touch Provisioning.

Use this reference to identify the deployment file for each supported sensor platform.

Table 27: Deployment files by sensor

Sensors	Deployment files
IE3x00, IR1101, IR18xx, IE9300	`cviox-aarch64.tar`
IE3x00, IR1101, IR18xx, IE9300 with Active Discovery	`cviox-active-discovery-aarch64.tar`
IC3000	`cviox-ic3000-x86-64.tar`
IC3000 with Active Discovery	`cviox-active-discovery-x86-64.tar`
Catalyst 9300, 9400, IR8340	`cviox-x86-64.tar`
Catalyst 9300, 9400, IR8340 with Active Discovery	`cviox-active-discovery-x86-64.tar`

Create deployment tokens

Guides you to create deployment tokens by defining a deployment phase, number of uses, expiration time, and enabled state for device deployment.

Procedure

1. From the main menu, choose **Admin** > **Sensors** > **Deployment Tokens**

   The **Deployment Tokens** page appears.
2. Click **Add Tokens**.

   The **Add new deployment tokens** panel appears.
3. In the **Add new deployment tokens** panel, enter a name for the deployment phase.
4. Enter a value in **Number of uses** that corresponds to the number of devices to deploy.
5. Set the **Expiration time** for the token.
6. Select the **Enabled** toggle to enable the token and continue the deployment process.
7. Click **Create**.

The deployment phase with tokens for each device type appears.

> **Note**
>
> You can view, copy, edit, disable, and delete the token.

What to do next

Refer to Cisco Catalyst WAN Manager documentation on cisco.com to continue and complete sensor deployment.

Templates

Describes sensor templates, which define protocol DPI engines and port mappings that control how Cisco Cyber Vision sensors analyze protocol traffic.

A sensor template is a configuration that defines protocol Deep Packet Inspection (DPI) engines and UDP/TCP port mappings for a Cisco Cyber Vision sensor.

You can create and configure sensor templates, then assign them to specific sensors.

- Enable or disable protocol DPI engines.
- Map UDP and TCP ports for packets of each protocol received by the sensor.

Protocol DPI engines

Enable or disable a protocol DPI engine to select which protocols to analyze.

Disable a protocol DPI engine to avoid false positives in Cisco Cyber Vision. A false positive occurs when a protocol appears in the user interface but is not present because other non-standardized protocols can use the same UDP/TCP ports.

Default template

The Default template disables some protocols because they are not commonly used or are specific to fields such as transportation.

The Default template applies to all compatible sensors.

UDP and TCP port mappings

Although UDP/TCP port configurations are mostly standardized, conflicts can occur for field-specific protocols or protocols with limited use. Map UDP/TCP port numbers to send packets to the correct DPI engine for accurate analysis and representation in the user interface.

Sending a protocol packet to the wrong port causes related information to appear in **Security Insights/Flows** without a tag.

Template assignment and deployment

A sensor can be associated with only one template.

Template deployment fails in the following situations:

- The sensor is disconnected.
- The sensor has connection issues.
- The sensor version is too old.

Create a template

Guides you through the UI to create a sensor template, configure protocol port mappings, assign selected sensors, and send the configuration to them.

Procedure

1. Choose **Admin** > **Sensors** > **Templates** from the main menu.
2. Select **Add sensor template**.

   The **CREATE SENSOR TEMPLATE** window appears.
3. Enter a name for the template.

   You can optionally add a description.
4. Click **Next**, then type the protocol that you want to configure in the search bar.

   The list of protocol DPI engines and their basic configurations appears.
5. Under the **Port Mapping** column, select **pen** for the protocol, enter the port numbers, and click **OK**.

   > **Note**
   >
   > If you have continuous port numbers, you can enter a port range. For example, type 15000-15003 for ports 15000, 15001, 15002, and 15003.

   The port number is added to the protocol's default settings.
6. Enable **Displayed modified only** to quickly find the protocol, and click **Next**.
7. Select the checkboxes for the sensors to which you want to apply the template, and click **Next**.
8. Review the template configuration, and click **Confirm**.

The configuration is sent to the sensors. Configuration deployment can take a few moments.

The OPCUA template appears in the template list with its two assigned sensors.

Export templates

Guides you through exporting a template from one center to a local location, so that you can migrate it to another center.

Export a template when you need to migrate it to another center.

Procedure

1. From the main menu, choose **Admin** > **Sensors** > **Templates** .
2. Locate the template that you want to export, then hover over the ellipsis in the **Actions** column.
3. Select **Export** from the drop-down list.

   The system downloads the template to a local location.

Import a template

Guides you to import a sensor template, select the sensors that use it, and apply the template to those sensors.

Import a sensor template and apply it to selected sensors.

Procedure

1. From the main menu, choose **Admin** > **Sensors** > **Templates** .
2. Click **Import sensor template**.

   The local system folder opens.
3. Select the template, and then click **Open**.

   The system displays the imported template on the **Configuration Template** page.
4. Locate the template, and then hover over the **...** in the **Actions** column.
5. Select **Edit** from the drop-down list.
6. On the **Select sensors** tab, select the sensors to which you want to apply the template.
7. Click **Next**.
8. Verify the details, and then click **Update**.

   The template recovers all changes made in the previous center and is applied to the selected sensors.

PCAP files

Use this concept to understand how PCAP files help capture, analyze, and identify network traffic and assets in operational technology environments using Cyber Vision Center.

A packet capture (PCAP) file is a file format that

- records raw network traffic data captured from a network interface,
- preserves the exact communication packets that are exchanged between various assets, and
- enables network analysis and asset identification when imported into Cyber Vision Center.

PCAP file usage

To analyze traffic from your OT network, upload PCAP files to Cyber Vision Center. Use the Cyber Vision Classic UI to upload PCAP files.

When you import the file, Cyber Vision Center creates and identifies assets and associates them with their properties and communication patterns. You can then view these assets throughout the system, including on the main dashboard.

Upload a PCAP file

Learn how to upload a PCAP (Packet Capture) file for analysis or to troubleshoot network activity.

Upload a PCAP file to the system to analyze network diagnostic or security information.

Uploading a PCAP file allows you to review and inspect captured packet data using system analysis tools. This is typically performed during troubleshooting or forensic investigations.

Before you begin

- Ensure you have the required permissions to upload files.
- Have the PCAP file ready and accessible from your local system.

Procedure

1. From the main menu, choose **Admin** > **Sensors** > **PCAP Upload**.
2. Click **Upload a new file**.
3. Click **Choose a file or drag and drop to upload**. Add the file in the box.
4. Click **Upload** to start the process.

> **Note**
>
> The system displays the status for **DPI** and **Snort** during the upload.
>
> If you upload a large file, you can pause the upload. To resume, select the same PCAP file with the browse button and click **Resume**.

After you upload the PCAP file, you can analyze it in the system.

What to do next

- Review the upload confirmation.
- Analyze the uploaded PCAP if needed.

SNMP monitoring information

Details supported SNMP versions, version guidance, monitored system information, and how to open the SNMP Global Configuration page in Cisco Cyber Vision.

SNMP protocol in Cisco Cyber Vision is used for remote monitoring purposes. To access the **SNMP Global Configuration** page, choose **Admin** > **SNMP** from the main menu.

- Older SNMP versions are not supported.

Important

It is highly recommended to use SNMP version 3. SNMP version 2c is available because many infrastructures still use it; however, its security risks are higher.

Supported SNMP versions

- SNMP V2C
- SNMP V3

Information available through SNMP

- CPU % per core
- Load 0 to 100 (combination of CPU and I/O loads)
- RAM kilobytes
- Swap kilobytes
- Traffic for all physical interfaces (nb bytes in and out/interface since the SNMP service startup)
- Data storage (% - 250G)
- Packets statistics (packets/sec/int)

Configure SNMP

Guides you to enable the SNMP agent, configure monitoring access and version-specific settings, configure traps, and save the configuration on a CyberVision Center.

Configure SNMP on a CyberVision Center.

Procedure

1. From the main menu. choose **Admin** > **SNMP**.
2. Enable **SNMP agent**.

   A configuration menu appears.
3. Enter the IP address of the monitoring host in **Monitoring hosts (IPv4)**.
4. Select **Version 3** or **Version 2c**.

   > **Note**
   >
   > For security reasons, Cisco recommends SNMP version 3.

   If you select **Version 3**, select a value for **Security type** and enter the applicable settings:

   - For **NoAuth**, enter a **Username**. Only a username is required; no authentication password is required. The default username is `ics`.
   - For **Auth** with **NoPriv**, enter a **Username** and an encrypted password. The default username is `ics`. In **Authentication**, enter the required hash algorithm and its password. The password must be at least 8 characters long.
   - For **Auth** with **Priv**, only AES encryption is available. Enter a **Username**, an encrypted password, and the required AES encryption. The default username is `ics`. In **Authentication**, enter the required hash algorithm and its password. The password must be at least 8 characters long. In **Privacy**, enter the AES password. The password must be at least 8 characters long.

   If you select **Version 2c**, enter the community string so that the Center can communicate with the monitoring host.
5. Enable **Trap**.

   The configuration menu appears.

6. Configure the traps to be delivered.
   - If you selected SNMP v3, **Engine ID** (the Center ID) is displayed. Customize it as needed.
   - Set the CPU and memory rate limit and threshold values according to your needs.
7. Click **Save Configuration**.

SNMP MIB

Lists the SNMP MIB OID prefixes implemented in addition to classical MIB-II system objects, including sysDescription, name, and other system objects.

The following SNMP MIB OID prefixes are implemented in addition to the classical MIB-II system objects, including sysDescription and name.

Table 28: Implemented SNMP MIB OID prefixes

MIB	OID prefix	Description
MIB-2	.1.3.6.1.2.1.1	System
IF-MIB	.1.3.6.1.2.1.2.2.1.1	All physical interfaces
IF-MIB	.1.3.6.1.2.1.31.1.1	All physical interfaces
HOST-RESOURCES-MIB	.1.3.6.1.2.1.25.1	System
HOST-RESOURCES-MIB	.1.3.6.1.2.1.25.2.3	Storage
HOST-RESOURCES-MIB	.1.3.6.1.2.1.25.3.3	CPU
UCD-SNMP-MIB	.1.3.6.1.4.1.2021.4	Memory
UCD-SNMP-MIB	.1.3.6.1.4.1.2021.9	Disk
UCD-SNMP-MIB	.1.3.6.1.4.1.2021.10	Load
UCD-SNMP-MIB	.1.3.6.1.4.1.2021.11	CPU
UCD-DISKIO-MIB	.1.3.6.1.4.1.2021.13.15.1	Disk IO

6 Integrate with Cisco Cyber Vision

Topics:

- ISE pxGrid
- ISE-API
- XDR
- Secure Remote Access
- Cisco In Product Support

Introduces integration options for Cisco Cyber Vision, covering pxGrid connectivity, ISE-API usage, XDR integration with concepts and configuration steps, secure equipment access setup, and accessing Cisco in-product support features.

ISE pxGrid

Introduces Cisco Platform Exchange Grid and explains how to access the Platform Exchange Grid page for Cisco ISE pxGrid integration in Cisco Cyber Vision.

Cisco Platform Exchange Grid (pxGrid) is an open, scalable data-sharing and threat-control platform that enables seamless integration among multivendor identity, network, security, and asset management systems.

You can configure Cisco ISE pxGrid integration from the **Platform Exchange Grid** page.

To access the **Platform Exchange Grid** page, choose **Admin** > **Integrations** > **ISE – pxGrid** from the main menu.

For more information about this integration, refer to the *Integrating Cisco Cyber Vision with Cisco Identity Services Engine (ISE)* manual.

ISE-API

Introduces the use of Security Group Tags (SGTs) and describes how to map groups to SGTs in Cisco Cyber Vision, synchronize mappings with Cisco ISE via API, and enforce TrustSec policies across the network.

Security Group Tags (SGTs) are 16-bit labels assigned to devices or groups of devices to define their roles and associated security policies within a network.

Using Cisco Cyber Vision, you can map static subnets, network-based groups, or user-defined groups directly to SGTs. A secure, active Cisco Identity Services Engine (ISE) API connection enables the automatic synchronization of these mappings from Cisco Cyber Vision to Cisco ISE. This integration allows you to effectively enforce TrustSec policies across your network.

To create IP-to-SGT mappings based on group definitions, choose **Admin** > **Integrations** > **ISE – API** from the main menu.

For further details on IP-to-SGT mapping, refer to the *Integrate Cisco Cyber Vision with Cisco Identity Services Engine (ISE)* manual.

XDR

Introduces the Cisco Cyber Vision integration with Cisco XDR and explains the available XDR features, including their XDR SSO login requirements.

The Cisco Cyber Vision XDR integration connects Cisco Cyber Vision with Cisco XDR, a cloud-native, built-in platform that connects the Cisco Secure portfolio with your infrastructure.

Cisco XDR centralizes security events from Cisco software through an API. It can receive and correlate Cisco Cyber Vision events and firewall activities, then present them in dashboards.

The integration can significantly reduce dwell time and human-powered tasks.

The XDR integration enables the following three features in Cisco Cyber Vision:

- Without XDR SSO login, **Investigate in XDR Threat Response** appears on component technical sheets.
- With XDR SSO login, **Report to XDR** appears for certain events on the event calendar page. Use **Report to XDR** to send these events to XDR.
- With XDR SSO login, you can activate the **XDR ribbon** in Cisco Cyber Vision to access its features.

> **Note**
>
> SecureX reached end of life on 2024-07-31.

Configure XDR

Guides you to select an XDR region, enable the Cisco Cyber Vision integration, authorize access, and enable the XDR ribbon in Cisco Cyber Vision.

Configure the XDR integration in Cisco Cyber Vision.

Before you begin

Before you begin, ensure that you have Admin access to Cisco Cyber Vision Center, a Cisco Cyber Vision Center with internet access, and an XDR account with an admin role.

Procedure

1. From the main menu, choose **Admin** > **Integrations** > **XDR**.
2. Click the **Region** drop-down list and select a region.
3. Select **Enable XDR** to enable the link.

   The control turns red to indicate **Disable XDR**.

   You can now use **Investigate in XDR Threat Response**, which appears in the component technical sheet. Complete the remaining steps to install and use the XDR ribbon and **Report to XDR**.
4. In the upper-right corner of the GUI, open the user menu and select **My Settings**.

   An **XDR** menu appears on the right side of the **My Settings** page.
5. Click **Log in**.

   A **Grant Application Access** popup appears with an authentication code.
6. Click **Verify and Authorize**. In the **Security Cloud Sign On** window that opens, enter **Email** and click **Continue** to grant Cisco Cyber Vision access to **XDR**.
7. Click **Authorize Cyber Vision**.

   A **Client Access Granted** popup appears. In **Cisco Cyber Vision Center** > **My Settings**, the **XDR** menu indicates that Cisco Cyber Vision is connected to XDR.
8. Use the **Ribbon status** toggle to enable the XDR ribbon.

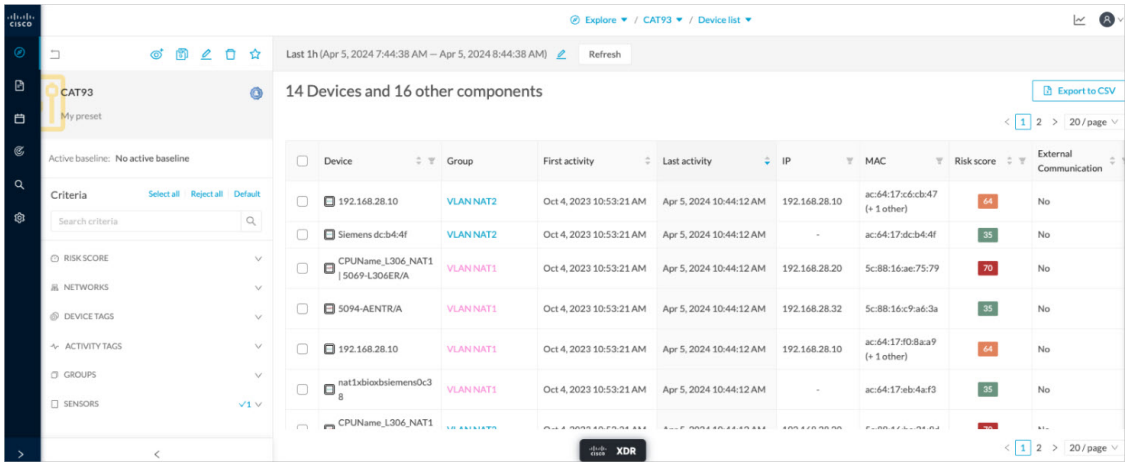
   After you enable **Ribbon status**, a message appears.
9. To log out, click **Logout of XDR**, then click **Save settings**.

XDR Ribbon

Provides access to the XDR ribbon within the Cisco Cyber Vision GUI to facilitate threat investigation. This interface allows users to identify and analyze observables directly from the Explore menu.

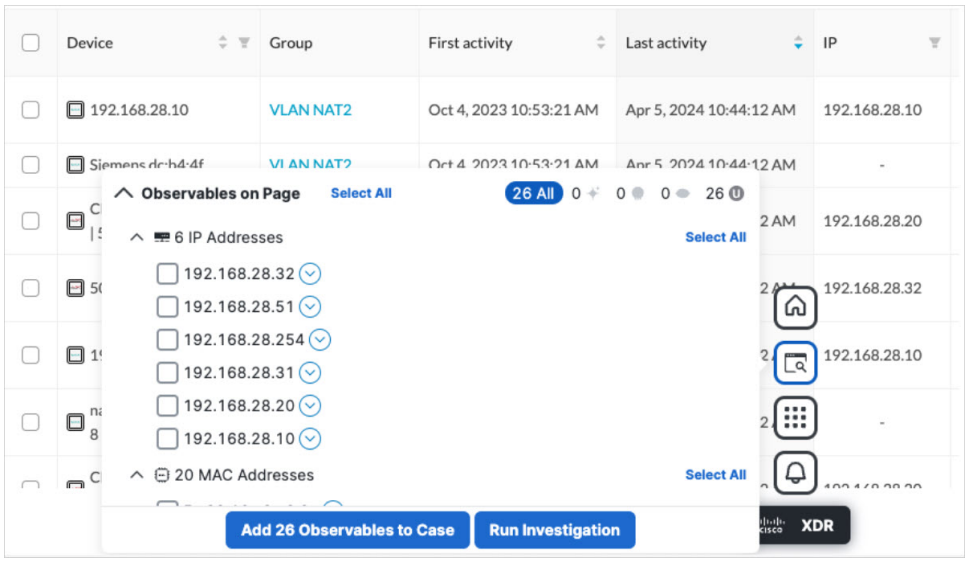
The XDR ribbon appears at the bottom of the Cisco Cyber Vision GUI in the Explore menu once it is configured and activated.

The XDR ribbon in the Device List view:



The Cisco XDR Getting Started Guide explains how to use the XDR ribbon.

For example, to find observables and investigate them in XDR Threat Response, click the **Find Observables** icon like below:



XDR Event Integration

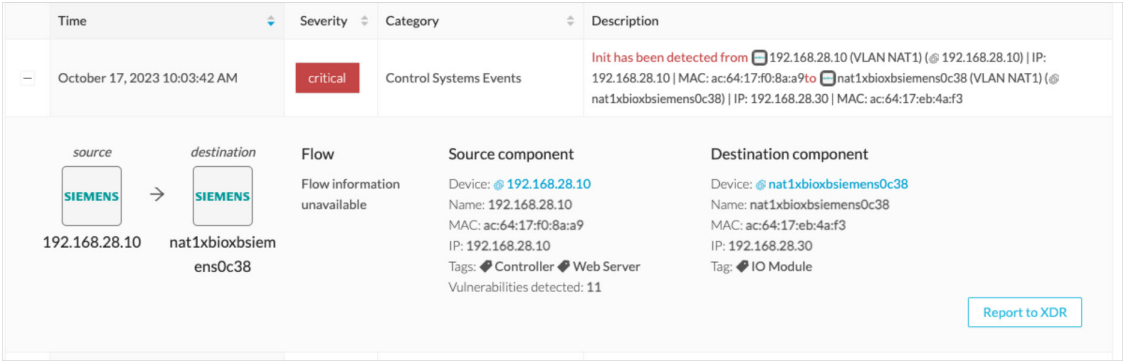
Enables the manual reporting of specific security events from Cisco Cyber Vision to XDR. This integration facilitates incident creation by pushing event data directly to the XDR platform.

After configuring XDR in Cisco Cyber Vision, the **Report to XDR** button appears for some events on the event calendar page. Selecting this button sends the event to XDR and creates an incident.

The **Report to XDR** button is available for the following event categories:

- Anomaly Detection
- Control Systems Events
- Signature Based Detection

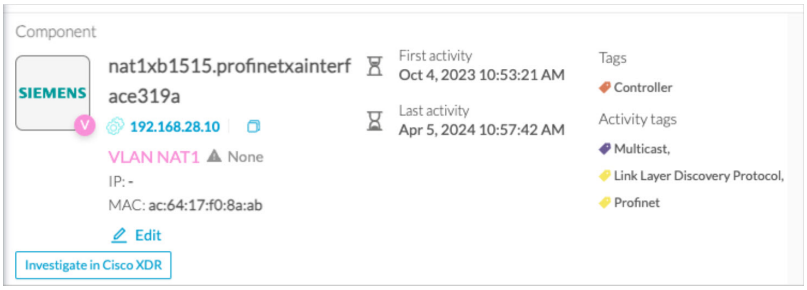
Figure 4: Report to XDR button on a Control Systems Event



XDR component button

Provides access to the Investigate in Cisco Threat Response feature within the Cisco Cyber Vision interface. This functionality allows users to initiate investigations for component IP and MAC addresses directly from the technical sheet.

After you configure XDR in Cisco Cyber Vision, the **Investigate in Cisco Threat Response** button appears on the component's technical sheet. If you use this button, XDR Threat Response investigates the component's IP and MAC addresses.



External resources for XDR integration

Lists the URLs required by the Cisco Cyber Vision Center for firewall authorization. This information ensures proper connectivity between the center and external services.

Provides the necessary URLs for Cisco XDR integration across different geographic regions to facilitate secure communication.

Center:

North America

- Cisco XDR Platform: https://visibility.amp.cisco.com/iroh/
- Cisco XDR Private Intelligence: https://private.intel.amp.cisco.com/ctia/
- Cisco XDR Automation: https://automate.us.security.cisco.com/api/

Europe

- Cisco XDR Platform: https://visibility.eu.amp.cisco.com/iroh/
- Cisco XDR Private Intelligence: https://private.intel.eu.amp.cisco.com/ctia/
- Cisco XDR Automation: https://automate.eu.security.cisco.com/api/

Asia Pacific, Japan, and China

- Cisco XDR Platform: https://visibility.apjc.amp.cisco.com/iroh/

- Cisco XDR Private Intelligence: https://private.intel.apjc.amp.cisco.com/ctia/
- Cisco XDR Automation: https://automate.apjc.security.cisco.com/api/

Web client:

- conure.apjc.security.cisco.com
- conure.us.security.cisco.com
- conure.eu.security.cisco.com

Secure Remote Access

Explains how secure equipment access solutions provide secure remote access for operations teams to manage and troubleshoot operational technology assets while reducing the need for on-site service visits.

A secure equipment access solution is a Cisco offering that

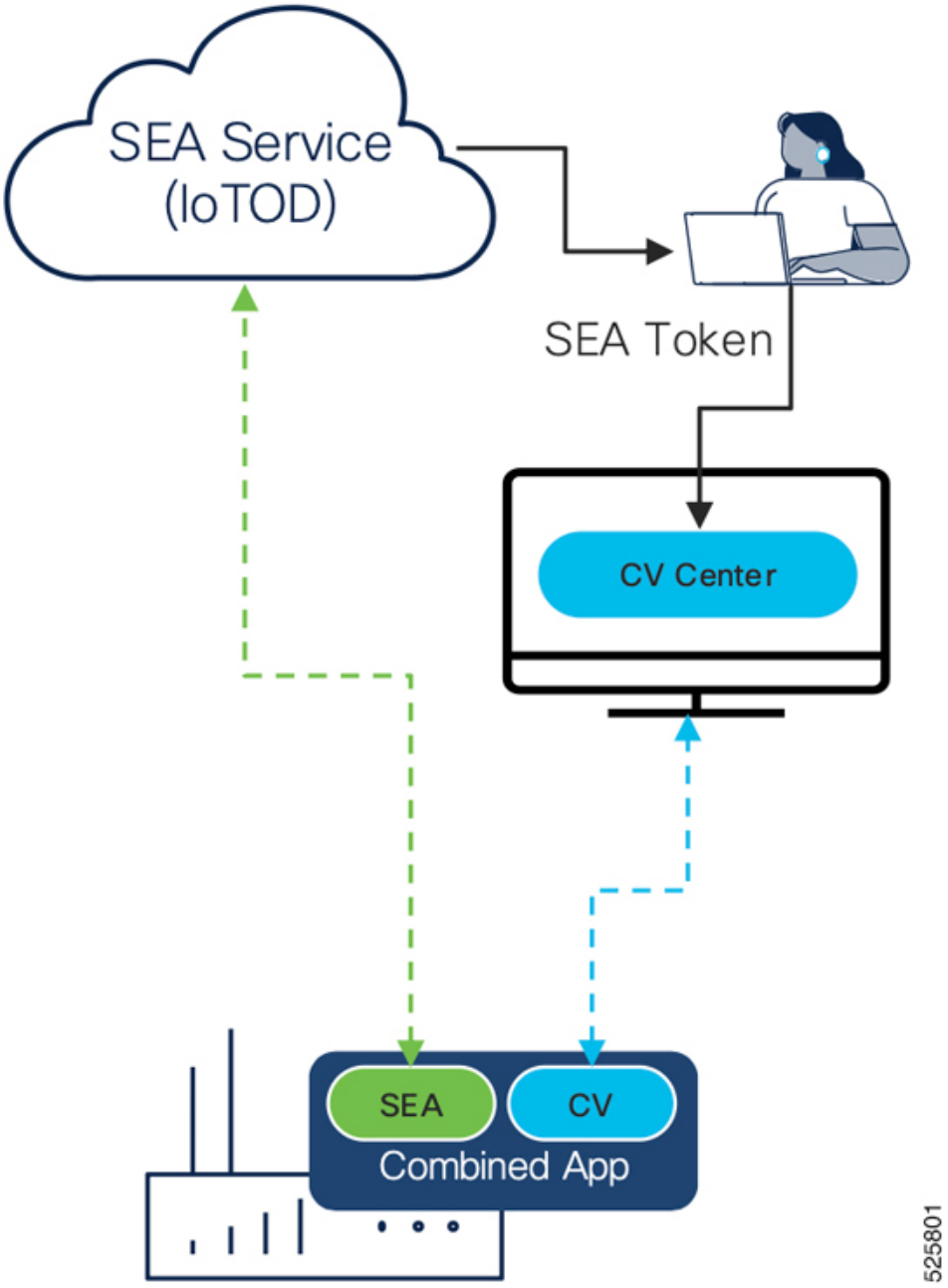
- provides secure remote access for operations teams to manage and troubleshoot operational technology assets,
- eliminates the need for costly on-site service visits,
- enables Zero Trust Network Access gateway functionality.

For more details, see the SRA documentation.

Integration with Cyber Vision

You can integrate SRA with Cyber Vision for unified management in the Cyber Vision Center. The integration requires the SRA agent (an IOx application) to run on your network device. You install the SRA agent and the Cyber Vision sensor app with the same workflow. One IOx application packages both runtimes.

Figure 5: Integrate Cyber Vision with SRA



Feature history table

Feature	Release Information	Feature Description
Enable Cyber Vision Center as an SRA Gateway	Release 5.5.x	The Secure Remote Access agent can run directly on the Cyber Vision Center. This setup eliminates the need to host the agent within an IOx application. When you enable the Center as an SRA gateway, you provide secure, remote access to the Center and its network resources through the IoT Operations Dashboard. You do not need direct inbound access.

Integrate Cisco Cyber Vision Center with SRA

Guides you to connect Cisco Cyber Vision Center to Secure Equipment Access (SRA), then enable and optionally validate the configuration.

Enable SRAmless, unified management of Secure Equipment Access (SRA) and Cisco Cyber Vision through Cisco Cyber Vision Center. The integration simplifies deployment and ongoing management of both components on the same device while keeping their operations separate.

Before you begin

Ensure that you have administrative access to Cisco Cyber Vision Center and tenant administrator access to the SRA organization that you intend to connect with Cisco Cyber Vision.

Procedure

1. Log in to Cisco Cyber Vision Center, and then choose **Admin** > **Integrations** > **SRA** from the main menu.
2. On the **SRA** page, in the **Configuration** section, select a region from the drop-down list and click **Connect**.
3. Log in to the **IoT Operations Dashboard** with your IoT OD credentials.
4. On the **IoT Operations Dashboard**, click **Connect**.
5. On the **SRA** page, verify the details in the **Configuration** section.
6. Click **Enable SRA**.
7. (Optional) Click **Validate configuration** to validate the configuration.

A success message appears on the **SRA** page, indicating that SRA is configured.

What to do next

Install the compatible sensors. For more information, refer to the *Cisco Cyber Vision Sensor Application for Cisco Switches Installation Guide*.

Enable Cyber Vision Center as an SRA Gateway

Configure the Cyber Vision Center to function as a Secure Equipment Access (SRA) gateway, enabling secure remote access and centralized asset management through the IoT Operations Dashboard.

Configure your Cyber Vision Center as a Secure Equipment Access (SRA) gateway.

Enabling Cyber Vision Center as an SRA gateway removes the need for an external IOx application. This setup offers secure remote support and allows centralized asset management through the IoT Operations Dashboard.

Before you begin

Ensure your Cyber Vision Center is connected to SRA.

Procedure

1. Log in to Cyber Vision Center.
2. From the main menu, choose **Admin** > **Integrations** > **SRA**.
3. (Optional) In the **Center as gateway** section, optionally enter a name for your center.

   If you do not add a center name, Cyber Vision Center uses the Center's Fully Qualified Domain Name (FQDN) from **Admin** > **Web Server Certificate**.

4. Click **Enable Center as Gateway**.

- Your Cyber Vision Center contacts the SRA tenant and registers itself as a new SRA agent. Log in to SRA and choose **System Management** > **Network Devices** to view the new agent. The new network device appears in the list.
- Once you enable Center as gateway, a direct link to the IoT OD SRA dashboard becomes available. If you have access to multiple tenants in IoT OD, select the correct tenant to view your new network device.

What to do next

Add new assets to your center as needed. These assets will be reachable through your Center, which now acts as a gateway. You can manage and access other assets directly from the Center. For more information, see Manually Add Assets in the IoT Operations Dashboard (IoT OD) documentation.

Cisco In Product Support

Provides a virtual assistant that offers a unified self-service experience for managing support cases, troubleshooting hardware, and interacting with support teams. This tool simplifies technical support activities for Cisco customers and partners by consolidating multiple services into a single interface.

A **Cisco In Product Support** is a virtual assistant that:

- provides customers and partners with a unified self-service experience across multiple support domains,
- offers tools for managing cases, checking bug applicability, troubleshooting hardware, and managing licensing, and
- enables users to connect directly with case owners, managers, or Technical Assistance Center (TAC) duty managers for escalations or assistance.

Feature History

Table 29: Feature History Table

Feature	Release information	Feature description
Cisco In Product Support	Release 5.3.x	Use **Cisco In Product Support** to manage your Cisco support cases and related tasks directly from the Center.

Support capabilities

Cisco In Product Support is designed to simplify and speed up support activities for Cisco customers and partners.

By using a single interface that consolidates multiple support services, you can address technical challenges and manage support team interactions efficiently.

The tool integrates with Cisco's back-end systems to provide up-to-date case tracking, bug search, and device troubleshooting resources.

Support activity examples

- A partner uses **Cisco In Product Support** to submit and track a hardware replacement (RMA) request.
- A customer uses **Cisco In Product Support** to check whether a reported bug affects their installed software version.

- A network engineer uses the self-service troubleshooting function to diagnose hardware issues without opening a formal support ticket.

Access Cisco In Product Support

Guides you to access Cisco In Product Support and sign in to interact with Cisco TAC support from the product interface.

Open **Cisco In Product Support** to interact with Cisco TAC support from your product.

Cisco In Product Support provides integrated access to Cisco TAC services. You can use **Cisco In Product Support** to open TAC cases, record screens, or upload files directly from your product interface.

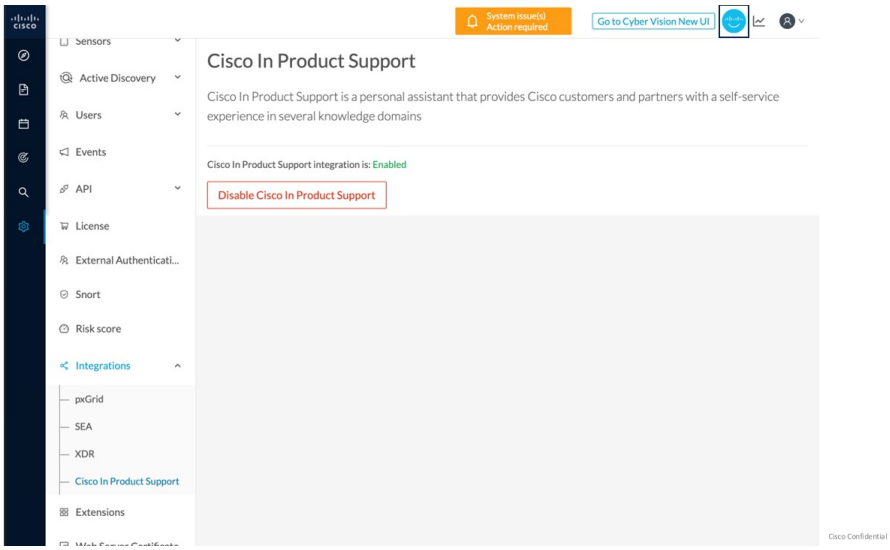
> **Note**
>
> The **Cisco In Product Support** integration is enabled by default, and its icon is available on the page.

Before you begin

Ensure that you have a Cisco account with TAC access.

Procedure

1. From the main menu, choose **Admin** > **Integrations** > **Cisco In Product Support**.



2. Click **Cisco In Product Support**.
3. Click **Sign In** to enable TAC virtual assistance.

After you enable Cisco In Product Support, you can:

- Open support cases with **Open Cisco Support Case**.
- Record your screen with **Record Screen**.
- Upload files with **Upload Local File**.

What to do next

To generate and upload diagnostics, select **System Statistics**.

7 Maintain and monitor Cisco Cyber Vision

Topics:

- Monitored presets
- Center shutdown/reboot
- Upgrade with a combined update file
- Syslog configurations
- Database import and export
- Update the Knowledge DB
- Certificate fingerprints
- Disable Cisco Cyber Vision telemetry
- Reset to Factory Defaults
- Snort
- Risk Score
- Cisco Cyber Vision extensions

Details maintenance and monitoring activities for Cisco Cyber Vision, covering preset management and baselining, system shutdown and reboot, upgrades with combined update files, syslog configuration, import/export features, Knowledge DB maintenance, certificate fingerprint handling, telemetry setup, factory reset, Snort configuration, risk scoring, and extension integration.

Monitored presets

Explains how monitored presets and baselines in Cisco Cyber Vision Center help you monitor defined subsets of network data and detect network deviations.

A monitored preset is a preset that is monitored against a baseline. To monitor your network using Cisco Cyber Vision Center, you must set up monitored presets.

On the **Explore** page, you can select a preset to view the network data that matches the preset definition. You can also export the data as a PDF file.

Presets

A preset is a customizable view that allows you to focus on specific subsets of network data. A preset filters network data based on defined criteria and gives you a focused view of an organizational network for quick, meaningful analysis.

The parameters that you can configure for a preset include:

- Time
- Risk score range
- Networks, by IP subnets or VLAN IDs
- Device tags
- Activity tags
- Groups
- Sensors

Baselines

A baseline is a snapshot of a preset. It is the reference point against which network behavior is periodically compared to detect network deviations or anomalies, such as new devices, altered communications, or unusual activities that may indicate security issues or operational problems.

Multiple baselines for a preset

You can create multiple baselines for a preset to monitor various known states of your network.

For example, network activity baselines may differ for weekdays and weekends. Create two baselines for these scenarios, and activate the baseline that accurately monitors your network on any given day.

To activate one of multiple baselines for a monitored preset, refer to Configure monitored presets on page 124.

Create a baseline

Guides you through creating a baseline from a preset in Cisco Cyber Vision Center and entering a name and description for the preset.

Establish a baseline for a preset to monitor and track network activity in Cisco Cyber Vision Center.

Follow these steps to create a baseline for a preset.

Procedure

1. From the main menu, select **Explore**.
2. Select the Create baseline icon for a preset from one of the following locations:



- The preset dashlet listed on the **Explore** page.
- The preset details page displayed when you select a preset dashlet.

3. Enter a name and description for the preset.
4. Click **Create**.

The baseline is created. You can view it from the **Monitor** page in Cisco Cyber Vision Center, where all available baselines are displayed and categorized by their respective presets.

Configure monitored presets

Guides you to configure monitoring intervals, baselines, alert severities, and event differences for monitored presets in Cisco Cyber Vision.

Configure a monitored preset to define the interval for checking the network and the types of event differences for which you want to view alerts.

Any differences between the selected baseline and the current network status result in alerts that you can review and acknowledge.

Before you begin

A monitored preset is a preset with a baseline. Refer to Create a baseline on page 123.

Procedure

1. From the main menu, select **Monitor**.
2. For each monitored preset that you want to configure, click the vertical ellipsis, then select **Monitored preset settings**.
3. Configure the monitored preset.
   a) Enter the monitoring interval in seconds.
   b) If you created more than one baseline for the preset, select the baseline that you want to activate in the **Monitored baseline** field.
   c) In the **Events severity** section, select the severity level for alerts generated for each event type.
   d) In the **Advanced settings** section, select the component, property, and activity differences for which you want to view alerts.
   e) Click **OK**.

Manage monitored preset differences

Guides you to acknowledge a reported event as normal for the network or report it as an anomaly in Cisco Cyber Vision Center.

Acknowledge or report a single monitored preset difference entry.

Acknowledge an entry to mark a reported event as normal for the network. Report an entry to identify a reported event as an anomaly and create an event in Cisco Cyber Vision Center.

After you select a baseline on the **Monitor** page, you can use the following bulk-management options:

- To acknowledge all differences across the components and activities, click the check mark in the left pane.
- To acknowledge or report multiple, specific differences in the components or activities listings, select the entries and then select **Acknowledge Selection** or **Report Selection**.

Procedure

1. From the main menu, select **Monitor**.
2. In the **What changed** area, select the baseline that you want to examine for a monitored preset.
3. View the reported differences.

   Differences are reported based on one of the following categories:

   - New components
   - New activities

4. To view the communication flows that may have caused the reported difference, click an entry to view its details, and then click the **Investigate with flows** link.
5. In the components list, click an entry to view its details.

   You can choose from the following four options:

   Table 30: Component actions

Action	Definition
Acknowledge Component	You can enter a message explaining your choice for reference. You have two acknowledgement options: • **Acknowledge and include**: Retain this alert and receive new alerts if something new happens with this component or activity. • **Acknowledge and keep warning**: Delete this alert and receive new alerts if the same event repeats.
Ack. with related activities	You can enter a message explaining your choice for reference. Select **Acknowledge and include** to retain the alert and receive alerts for any new events for the component and its activities.
Report component	You must enter a message explaining your choice for reference. You continue to receive alerts if the anomaly is detected again. Select **Report component** to create an event report for this anomaly.
Show details	View device tags and properties.

6. In the activities list, click an entry to view its details.

   You can choose from the following three options:

Table 31: Activity actions

Action	Definition
Acknowledge activity	Acknowledge the reported event as normal for the network. You can enter a message explaining your choice for reference. Two acknowledgement options are available: • **Acknowledge and include**: Retain this alert and receive alerts if something new happens with this component or activity. • **Acknowledge and keep warning**: Delete this alert and receive a new alert if the same event repeats.
Report activity	You must enter a message explaining your choice for reference. You continue to receive alerts if the anomaly is detected again. Select **Report activity** to create an event report for this anomaly.
Show details	View activity tags and variables.

Center shutdown/reboot

Introduces the Cisco Cyber Vision capability to safely shut down or reboot Center, including an appropriate use case for rebooting.

A center shutdown/reboot capability is a Cisco Cyber Vision feature that enables administrators to trigger a safe shutdown or reboot of the Center.

Use the **Reboot**function to resolve minor bugs, including system overload events, without requiring a full shutdown.

You can access the center shutdown/reboot capability from the Cisco Cyber Vision main menu by navigating to **Admin** > **System**.

Upgrade with a combined update file

Guides you through downloading, validating, and applying a Cisco Cyber Vision combined update file to the Center and applicable sensors.

Use a combined update file to update the Cisco Cyber Vision Center and applicable sensors.

Version releases include a Cisco Cyber Vision Manual Update Center update file.

Important

Rolling back to an earlier Cisco Cyber Vision version is not supported.

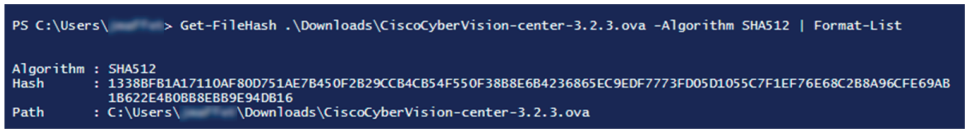
Use the SHA512 checksum provided by Cisco to verify that the downloaded file is healthy.

Procedure

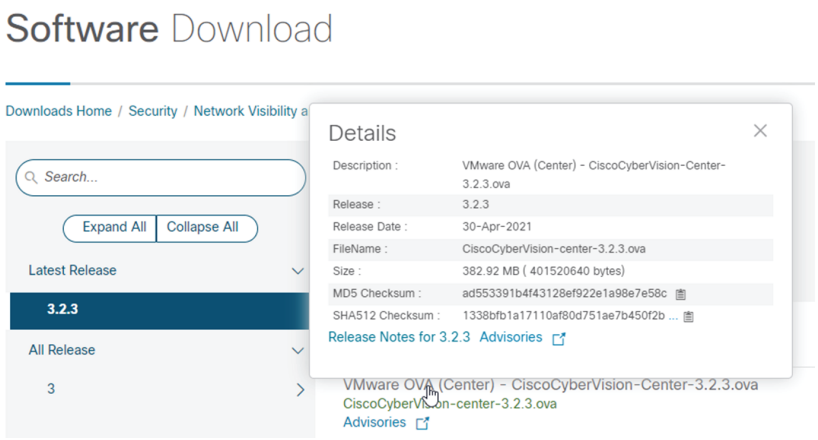
1. Retrieve the Cisco Cyber Vision combined update from cisco.com.
2. On Windows, open a shell prompt, such as Windows PowerShell, and run the following command to retrieve the file checksum:

   Example

   ```
   Get-FileHash .\CiscoCyberVision-<TYPE>-<VERSION>.<EXT> -Algorithm SHA512 |
   Format-List
   ```

3. On cisco.com, hover over the file and copy the SHA512 checksum.

4. Compare the two checksums.
   - If the checksums are identical, the file is healthy.
   - If the checksums do not match, download the file again.
   - If the checksums still do not match, contact Cisco support.
5. Log in to Cisco Cyber Vision.
6. Choose **Admin** > **System** from the main menu, and then click **System update**.
7. Select the `CiscoCyberVision-update-combined-<VERSION>.dat` update file.
8. Confirm the update.

   As the Center and sensors update, a holding page appears. When the update is complete, select Center **Reboot**. You are logged out.
9. Log in to Cisco Cyber Vision.

   If sensors were offline when the update occurred, repeat this procedure until all sensors update.

Syslog configurations

Introduces syslog configurations for forwarding Cisco Cyber Vision events and alerts to external syslog servers.

A syslog configuration is a network logging setup that

- forwards Cyber Vision events and alerts to an external syslog server,
- enables integration with Security Information and Event Management (SIEM) platforms, and
- supports Common Event Format (CEF) for standardized message structure.

Table 32: Feature History Table

Feature	Release Information	Feature Description
Non-CEF syslogs support removed	Release 5.3.x	You can no longer use non-CEF syslog formats with Cyber Vision Center. When you upgrade to Cisco Cyber Vision Center Release 5.3.x, any existing syslog connections that use non-CEF formats are automatically updated to CEF formats.

Configure syslog

Guides you through enabling and configuring event forwarding from Cyber Vision Center to an external syslog server, including protocol and format selection, secure communication options, format migration, and integration with SIEM systems.

Enable forwarding of Cyber Vision events and alerts to an external syslog server to integrate with a Security Information and Event Management (SIEM) system.

To configure syslog, follow these steps:

Before you begin

- Ensure you have administrator access to Cyber Vision Center.
- Confirm that the external syslog server is accessible. Obtain the host IP address, port, and the required protocol.
- If secure communication is required, ensure you have the P12 certificate from your SIEM administrator.
- Recent syslog format changes:
  - **Standard** and **RFC3164** formats are deprecated.
  - **Standard/CEF** is now named **CEF**.
  - **RFC3164/CEF** is now named **CEF Extended Time Precision**.

> **Note**
>
> If the deployment had **Standard** or **RFC3164** formats configured, version 5.3.x setup migrates the configuration to CEF.

Procedure

1. From the main menu, choose **Admin** > **System**.
2. Click **Configure** in the **Syslog configuration** menu.
3. Select **Protocol**.

> **Note**
>
> If secure communication is required, select **TCP + TLS** and import the P12 certificate.

4. Enter the syslog server **Host** IP address and **Port** that are accessible from Cyber Vision Center.
5. Select the required **Format**.
   - **CEF**: This format, based on the Common Event Format (CEF) standard, sends events with second-precision timestamps.
   - **CEF Extended Time Precision**: This format, based on the Common Event Format (CEF) and an extended syslog header, sends events with millisecond-precision timestamps.
6. Save the configuration.

Cyber Vision Center sends events from the Classic UI to syslog with 'Version Number = 1.0.' It sends alerts from the New UI to syslog with 'Version Number = 2.0.

What to do next

To configure notifications for specific alert types, see "Enable or disable syslog notifications for alert types" in the *Cisco Cyber Vision New UI Administrator Guide*.

To export events using syslog, see "Configure event export to syslog (Classic UI)" in the *Cisco Cyber Vision Syslog Notification Format Configuration Guide*.

Database import and export

Describes the process for importing and exporting the Cisco Cyber Vision database via the System interface. This functionality enables users to back up industrial network data or transfer databases between centers.

The Import/Export feature is a system administration tool that allows for the management of the Cisco Cyber Vision database.

- Supports database backups for industrial network data.

- Facilitates database transfers between different **Center** instances.
- Retains network data, events, users, and customizations such as groups and component names.

Database management

To access the **Import/Export** page, choose **Admin** > **System** from the main menu.

Following are constraints and requirements for database operations:

- Database export size is limited to 2 GB to prevent performance issues.
- If the database exceeds 2 GB, connect via SSH and use the `sbs-db dump` command.
- Only configurations created in the Cisco Cyber Vision GUI persist during transfers.
- When changing a **Center** , perform a basic configuration of the new Center before reconfiguring Cisco Cyber Vision. Refer to the corresponding Center Installation Guide.

> **Note**
>
> The **Import** process may take one hour for big databases. Refresh the page to check that the import remains active (i.e., no error message).

Update the Knowledge DB

Guides you to download and import the latest Knowledge DB so that Cisco Cyber Vision can recognize current vulnerabilities, icons, and threats.

Update the internal Cisco Cyber Vision database that contains recognized vulnerabilities, icons, and threats.

Important

To remain protected against vulnerabilities, always update the Knowledge DB in Cisco Cyber Vision as soon as possible after notification of a new version.

Procedure

1. Download the latest.db file available from cisco.com.
2. From the main menu, choose **Admin** > **System**.
3. Click **Import a Knowledge DB** under the **Knowledge DB** field.
4. Select the file, and then click **Open** to upload the file.

   Importing the new database rematches your existing components against any new vulnerabilities and updates the network data.

Certificate fingerprints

Introduces certificate fingerprints, explaining their role in identifying and verifying certificates, enabling secure communication between Global Centers and synchronized Centers, and outlining best practices for enrollment, renewal, and maintaining secure connectivity.

A certificate fingerprint is a unique identifier that

- identifies a digital certificate,
- verifies the authenticity of certificates during enrollment and renewal, and
- enables secure communication between Global Centers and synchronized Centers.

Validity and renewal

Use the fingerprint during enrollment with a Global Center or when updating after certificate renewal. The fingerprint validates the certificate and authorizes secure connectivity with remote hosts. For more information on Global Center, see Information and characteristics.

Certificates are valid for 2 years. Upon expiration, renewal and fingerprint exchange typically occur automatically. If automatic renewal fails, perform a manual renewal and provide the new fingerprint to the Global Center. This action restores enrollment and connectivity statuses in the Global Center. See the the Centers Installation Guides for detailed instructions.

> **Note**
>
> Always ensure the fingerprint matches the current certificate to maintain secure connections.

Disable Cisco Cyber Vision telemetry

Guides you through turning off the default feature that collects anonymous diagnostics and usage data to help Cisco understand and enhance product usage.

Telemetry monitors your system and provides anonymous diagnostics and usage data to help Cisco understand and enhance product usage. Telemetry data communication occurs as HTTPS traffic through Port 443 with connectdna.cisco.com.

Telemetry is enabled by default.

Follow these steps to disable Cisco Cyber Vision telemetry.

Procedure

1. From the main menu, choose **Admin** > **System**.
2. Under **Telemetry Collection**, click the **ON** toggle.

   The toggle turns **OFF**.

Reset to Factory Defaults

Describes the process and impact of restoring system settings to their original state. This action serves as a final troubleshooting measure when other recovery methods fail.

The **Reset to Factory Defaults** is a system recovery operation that reverts the application to its initial state.

- Requires *as a last resort* usage after all other troubleshooting attempts fail.
- Deletes GUI configuration, sensor data, and sensor configurations.
- Persists root password, certificates, and basic configuration settings.

Impact on system defaults

To access the **Reset** function, choose **Admin** > **System** from the main menu.

A **Reset to Factory Defaults** deletes the following:

- Some Center configuration data elements.
- The GUI configuration (such as user accounts, the setup of event severities, etc.).
- Data collected by the sensors.
- The configuration of all known sensors (such as IP addresses, capture modes, etc.).

> **Note**
>
> Get help from product support before proceeding.

Post-Reset Behavior

After a **Reset to Factory Defaults** occurs, the GUI refreshes with the installation wizard. See the corresponding Center Installation Guide .

Snort

Introduces Snort as a network intrusion detection system that analyzes traffic using rules, integrates with Cisco Cyber Vision for real-time alerts, outlines device availability, and describes management and configuration options on Center DPI interfaces.

A Snort instance is a network intrusion detection system (NIDS) that

- analyzes network traffic for malicious activity using a rule matching engine,
- applies a set of rules that characterize potentially harmful network activity, and
- integrates with Cisco Cyber Vision to provide real-time intrusion detection alerts and management.

Table 33: Feature History Table

Feature	Release Information	Feature Description
Enable or disable Snort on a Center DPI interface	Release 5.3.x	You can enable or disable Snort IDS or IPS on a Cisco Cyber Vision Center DPI interface. Previously, Snort was always enabled by default and could not be changed.

Additional reference information

- Cisco Cyber Vision can run the Snort engine on the Center and compatible sensors. The Center manages rule configuration and distribution. It also intercepts alerts for display in the GUI.
- Snort is disabled by default on sensors. To enable it, activate features of the Intrusion Detection System (IDS). See Enable IDS on a sensor.
- On the Center's Deep Packet Inspection (DPI), Snort is enabled by default.
- Snort is available on the following Cisco devices:
  - Cisco IC3000 Industrial Compute Gateway
  - Cisco Catalyst 9300 Series Switches
  - Cisco IR8340 Integrated Services Router Rugged
  - It is also available by default on the Center DPI.

Snort rulesets and rule categories

Outlines the structure of Snort rulesets, differentiating between Community and Subscriber access, and describes the various rule categories that target specific threat types, platforms, and vulnerabilities in operating systems, servers, browsers, files, malware, and industrial systems.

The Snort rules are organized into two main rulesets: the Community ruleset and the Subscriber ruleset.

Community ruleset

- Distributed freely and certified by Talos, including rules contributed by the open source community and integrators.
- Represents a subset of the full ruleset available to subscribers.
- Does not include the most recent Snort rules and does not guarantee coverage against the latest threats.

Subscriber ruleset

- Contains all rules released by the Talos Security Intelligence and Research Team.
- Provides rapid access to the newest rules and early coverage of exploits and vulnerabilities.
- Remains aligned with ongoing Talos research for maximum detection capability.
- Requires Advantage licensing and an IDS sensor license for each enabled sensor.

Snort rules are organized into categories, each targeting a specific threat type or platform.

Table 34: Rule categories

Category	Description
Browser	Detects vulnerabilities in major browsers (e.g., Chrome, Firefox, Internet Explorer) and browser plugins such as ActiveX.
Deleted	Contains deprecated or replaced rules.
Experimental-DoS	Rules targeting Denial of Service (DoS) activities such as TCP SYN flooding or DNS/HTTP flooding.
Experimental-Scada	Detects attacks on industrial control system assets.
Exploit-Kit	Tailored to identify exploit kit activities.
File	Addresses vulnerabilities in various file types (executables, Microsoft Office, images, Java, PDF, etc.).
Malware-Backdoor	Identifies traffic to known backdoor command channels.
Malware-CNC	Detects botnet command and control activity (call home, data exfiltration, download of dropped files).
Malware-Other	Covers other malicious tools or miscellaneous malware activity.
Misc	Rules address protocol-specific threats, policy violations such as spam and unwanted applications, and indicators not categorized elsewhere.
OS-Other	Looks for vulnerabilities in various operating systems (Linux, mobile OS, Solaris, etc.).
OS-Windows	Targets vulnerabilities in Windows operating systems.
Server-Other	Deals with vulnerabilities in multiple server types (web servers, database servers, mail servers, etc.).
Server-Webapp	Pertains to attacks against server-based web applications.

Snort rules management features

Outlines Snort rules management features in Cisco Cyber Vision Center, including default and subscriber rules, category and individual rule control, rule file downloads, custom rule import, rule synchronization across sensors, and restoring configuration to defaults.

The Snort rules management system in Cisco Cyber Vision Center includes these features:

Table 35: Snort rules management

Feature	Description
Snort community rules	Snort community rules are set by default in the Cyber Vision Center.

Feature	Description
Subscriber rules	Click **Use Subscriber Rules** from the **Admin** > **Snort** page to enable snort subscriber rules (requires Advantage and intrusion detection system (IDS) sensor licenses).
Category-based management	Enable or disable entire rule categories via the GUI.
Direct rule file download	Download rule files per category from the interface.
Individual rule control	Enable or disable specific rules within categories, independent of category status. In the downloaded rule files, locate the rule and get the sid (signature id). Go to **Admin** > **Snort** and enter it in the **Rule sid** and click **Disable** or **Enable**.
Custom rule import	Import and manage user-created rules via the **IMPORT CUSTOM RULES FILE** function from the **Admin** > **Snort** page.
Rule synchronization	Apply synchronized rule sets to sensors using the **Synchronize rules on sensors** feature from the **Admin** > **Snort** page.
Reset to default	Click **RESET TO DEFAULT** from the **Admin** > **Snort** page to restore the entire rule configuration to factory defaults and remove all custom rule files.

Enable IDS on a sensor

Guides you to enable Intrusion Detection System (IDS) on a compatible Cisco sensor and activate Snort-based intrusion detection for network security monitoring.

Enable Intrusion Detection System (IDS) on a compatible Cisco sensor to activate Snort-based intrusion detection.

Use this task to activate Snort's intrusion detection capabilities on a supported Cisco sensor for network security monitoring.

Before you begin

Ensure that your sensor is one of the following compatible devices: Cisco IC3000 Industrial Compute Gateway; Cisco Catalyst 9300 Series Switch; Cisco IR8340 Integrated Services Router Rugged; or Center DPI Interface.

Procedure

1. From the main menu, choose **Admin** > **Sensors** > **Sensor Explorer**.
2. Select the sensor on which you want to enable IDS.
3. Click **Enable IDS**.

IDS is active on the selected sensor. Snort monitors network traffic for threats.

What to do next

If required, you can disable Snort's intrusion detection capabilities. To do this, select the sensor and select **Disable IDS**.

Risk Score

Provides configuration options for the time range used in risk score computation. This setting determines the historical activity window analyzed during the hourly calculation process.

The Risk score is a configuration setting that allows you to set up the time range used for risk score computation.

- Enables selection of predefined time ranges including 30 days or 7 days.
- Supports custom time ranges with a minimum duration of one day.
- Triggers hourly computation based on the configured activity window.

You can configure the risk score by navigating to **Admin** > **Risk score** in the system interface.

For more information about risk scores, see the Risk Score Concept .

Cisco Cyber Vision extensions

Introduces optional add-ons for Cisco Cyber Vision Center that provide features for device management, detection, and integration with external services.

A Cisco Cyber Vision extension is an optional add-on to the Center that provides additional features, such as the management of new device types, additional detection engines, or integrations with external services.

From the **Extensions** page, you can manage Cisco Cyber Vision extensions.

Available extension

Currently, the following extension is available:

- Cyber Vision Reports Management

  For more information about this extension and how to use it, refer to Reports.

Install an extension

Guides you to retrieve an extension file from cisco.com and import it from the Extensions page in Cisco Cyber Vision Center.

Install an extension by retrieving and importing its extension file.

Procedure

1. Retrieve the extension file from cisco.com.
2. From the main menu, choose **Admin** > **Extensions**.
3. Click **Import a new extension file** to import the extension file.