

Introduction to Cyber Vision

- Cisco Cyber Vision GUI, on page 1
- Interactive help, on page 1
- Presets, on page 2
- Understanding concepts, on page 8
- Navigate through Cisco Cyber Vision, on page 26
- Risk scores, on page 39

Cisco Cyber Vision GUI

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.

Interactive help

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

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

Step 1 In the Classic UI, click the **Interactive Help** ribbon.

Step 2 In the New UI, click **?** icon and choose **Interactive Help**.

Step 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

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 1: 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

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

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 2: 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.
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

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

Table 3: 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.
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

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

Table 4: 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
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

Preset category	Presets available
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

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

Step 1 From the main menu, choose **Explore**.

Step 2 Click **New Category**.

Step 3 Enter the name and preset details.

Step 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

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

Step 1 From the main menu, choose **Explore** > **All Presets**.

Step 2 Select a predefined data preset from the **All Presets** list.

Step 3 Select the required criteria from **RISK SCORE**, **NETWORKS**, **DEVICE TAGS**, **ACTIVITY TAGS**, **GROUPS**, and **SENSORS**.

Step 4 Click **Save as**.

Step 5 Enter a new **Name** and select a **Category**.

Step 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

Describes the core concepts required to understand the system functionality.

Filters

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

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

Step 1 From the main menu, choose **Explore**.

Step 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

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 5: Filter types

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

Filter type	Description
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

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

Component icons visually differentiate component types in the UI.

Table 6: Component icons

Icon type	Example image	Description
Manufacturer	  	A detected manufacturer
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

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

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

Step 1 From the main menu, choose **Explore**.

Step 2 Select the required preset from the preset category.

Step 3 Select the relevant preset view.

Step 4 Click the component count in **Devices**.

Step 5 Select a component to display its details.

You see detailed component information in the drawer.

Devices

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

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

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

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

Procedure

Step 1 From the main menu, choose **Explore**.

Step 2 Select the required preset in the preset categories.

Step 3 Select the **Map** preset view.

Step 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

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

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

Procedure

Step 1 From the main menu, choose **Explore**.

Step 2 Select the appropriate preset and preset view.

Step 3 Click a component or device on the map.

Step 4 Open the technical sheet and select the **Activity** tab.

Step 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

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

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

Step 1 From the main menu, choose **Explore**.

Step 2 Select the appropriate preset and then select the **Map** preset view.

Step 3 Select the component or device you want to review.

Icons with an orange border (single or double) indicate external communications.

Step 4 Click **External communications**.

Step 5 Review the displayed list of external communications in the technical details.

Step 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

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

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

Step 1 From the main menu, choose **Explore**.

Step 2 Select appropriate preset and preset view.

Step 3 To set a time span, click the pencil icon.

Step 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.

Step 5 Click **OK**.

Step 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

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

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

Step 1 From the main menu, choose **Explore**.

Step 2 Select the appropriate preset and preset view.

Step 3 Select the relevant device, activity, or component.

Step 4 Open the **Technical sheet**.

Step 5 Click **Basics**, then **Tags**.

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

Properties

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

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

Procedure

Step 1 From the main menu, choose **Explore**.

Step 2 Select the preset and view required for your search.

Step 3 Select a device or a component.

Step 4 Click **Technical sheet**.

Step 5 Under **Basics**, click **Properties**.

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

Vulnerabilities

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

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

Step 1 From the main menu, choose **Explore**.

Step 2 Select the desired preset from the preset category.

Step 3 Select the required preset view.

Step 4 Click device.

Step 5 Click the count for **Vulnerabilities** from the drawer.

Step 6 Click the vulnerability you want to acknowledge.

Step 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

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

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

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

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

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 7: 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

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 8: Fields in the variable accesses table

Field	Description
Variable name	The identifier or label of the variable accessed.

Field	Description
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

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

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

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

Note You can also create a new template.

Step 3 Locate the protocols with variable inspection capability.

Step 4 Check the checkbox under the **Variable Processing** column.

Step 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

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

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

Step 1 From the main menu, choose **Explore**.

Step 2 Select the desired preset and preset view.

Step 3 Select the devices or components to group.

Step 4 Click **Manage selection**.

Step 5 To create a new group, click **Create a new group with selection.**

Step 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**.

Step 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

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

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

Step 1 From the main menu, choose **Explore**.
Step 2 Select the desired preset, then choose **Map** view.
Step 3 Select the group you want to lock.
Step 4 Click the edit icon in the drawer.
Step 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

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

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 9: Supported Protocols

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

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

Home

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

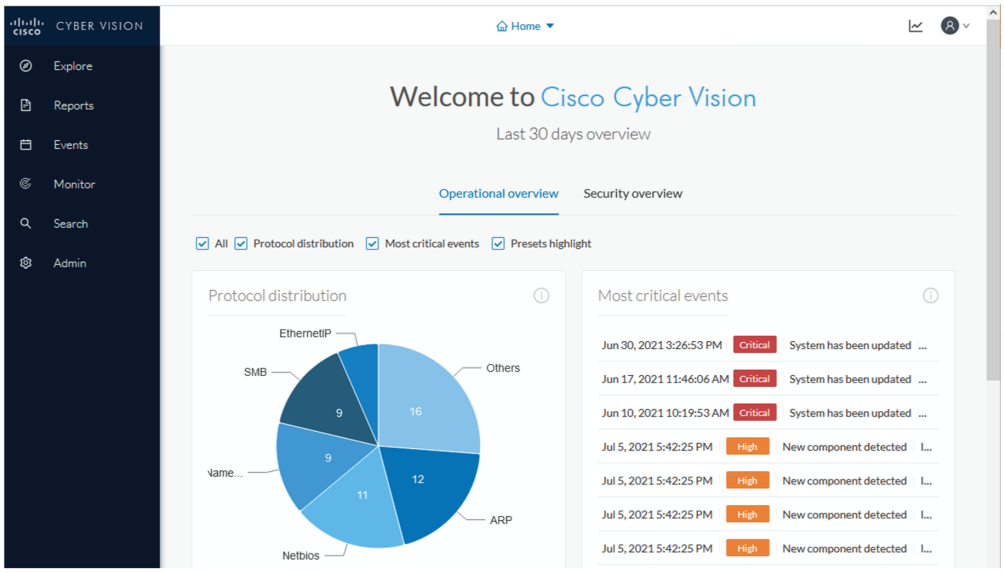
The home page is organized into two main tabs that allow users to monitor the industrial network over the last month.

The following tabs are available for monitoring:

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

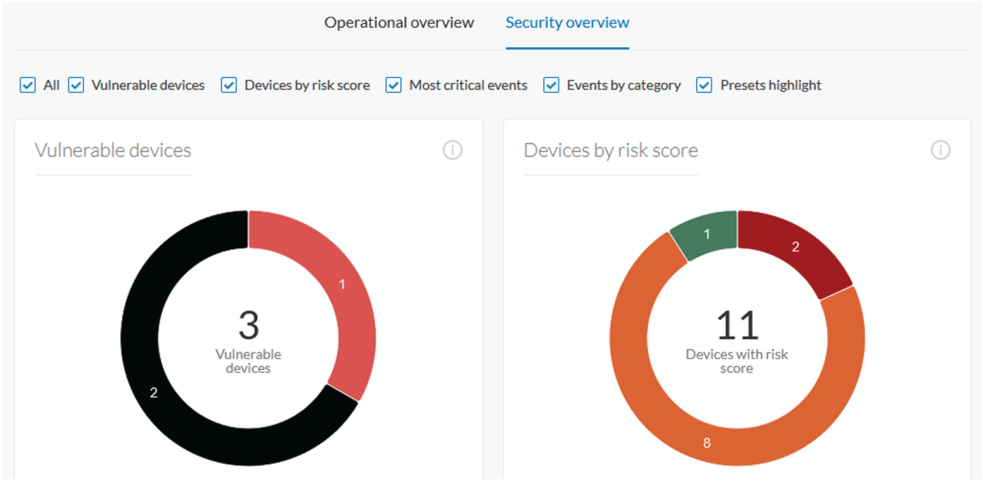
  Click **Edit favorite presets** to change what displays. Select the check boxes of the presets and click **Save**.

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 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

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.

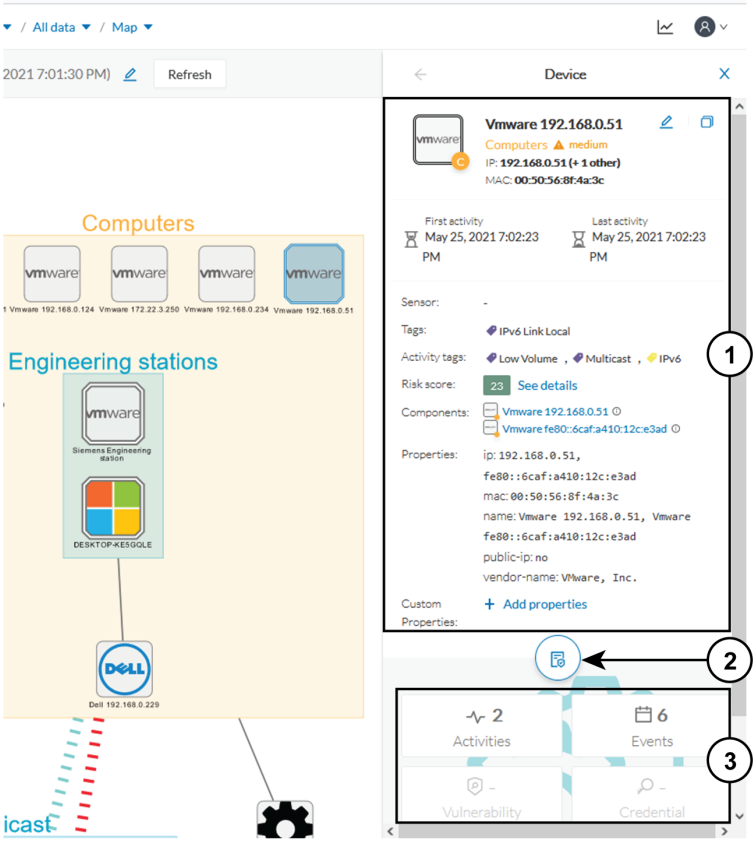
- Displays general information about the selected element.
- Provides editing capabilities for device or component names and group membership.
- Includes navigation buttons to access technical sheets and specific data categories.

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

A technical sheet is an interactive and complete view of all information related to a device, a component, an activity or a flow. The views differ depending on the type of element selected.

To access the **technical sheet** of a device, component or an activity's Detail panel, follow these steps:

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 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. 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 middle portion contains many tabs, depending on the selected element. In the above example, A **Device** detail contains the following tabs:

- **Basics** shows an element's properties and tags that are categorized with their definition. The components of the device also appear, if applicable.
- **Risk score** shows an overview and a more detailed and focused views.
- **Security** shows a component's vulnerabilities and credentials.
- **Activity** shows an activity's flows and contains a Mini Map, a view that is restricted to a device or a component and its activities. If applicable, a list of external communications with related information appears under the corresponding tab.
- **Automation** contains variable accesses.

- More information about properties.
- More information about tags.
- More information about the risk score.
- More information about vulnerabilities.
- More information about credentials.
- More information about flows.
- More information about the Mini Map.
- More information about external communications.
- More information about variables accesses.

Access the mini map

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

Step 1 From the main menu, select **Explore**.

Step 2 In the top navigation bar, click **All Presets**, and then select **All Data** from the drop-down list.

Step 3 In the top navigation bar, click the third filter, and then select **Map** from the drop-down list.

Step 4 Select a device from the map.

Step 5 Click **Technical sheet** in the **Details** panel.

Step 6 Click **Activity**.

Step 7 Select **Show inner components** to view an exploded view of the devices.

Step 8 Click any element in the **Mini Map**.

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

Reports

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.

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

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

Step 1 From the main menu, select **Reports**.

Step 2 Click **Create and run a Report**.

Step 3 Enter a report name in **Name**.

Optionally, enter a description in **Description**.

Step 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.

Step 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.

Step 6 Select a format in **Format**, and then click **Next**.

Step 7 Select a preset from **Preset**.

Step 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.

Step 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

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

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

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

Step 1 From the main menu, choose **Events** > **List**.

Step 2 Click an event result to view more details about the event.

Step 3 When an event is related to sensors, click **See Sensor Statistics** for more details.

Step 4 When an event is related to a component or an activity, click **see Technical Sheet** for more details.

Monitor mode

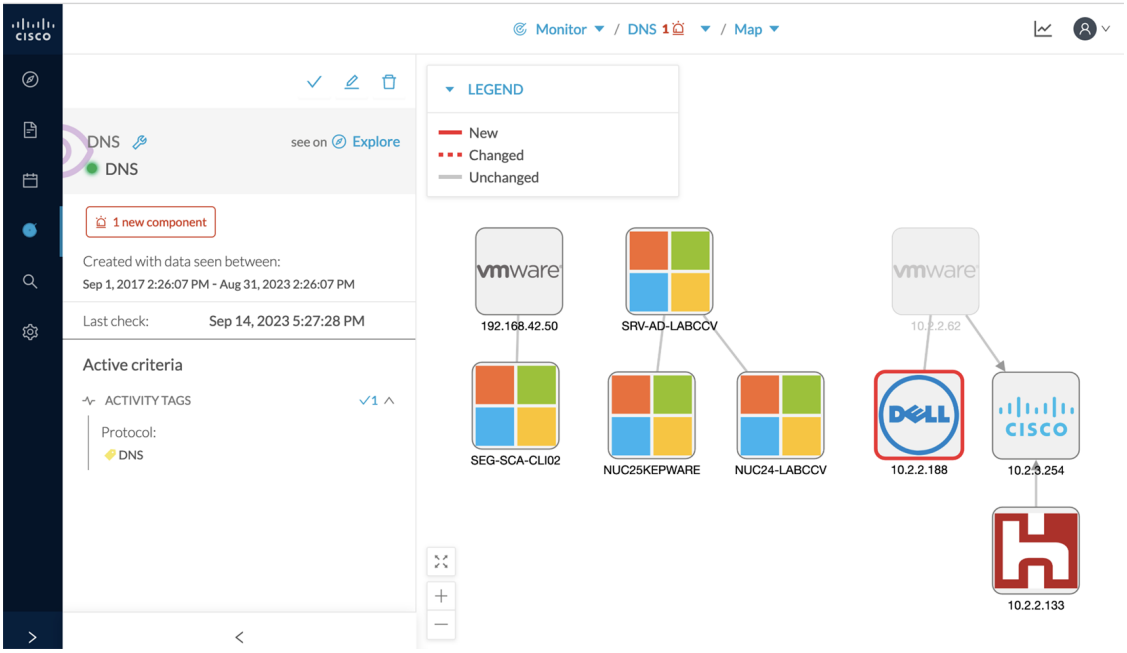
The Monitor mode is a monitoring tool in Cisco Cyber Vision that detects changes inside industrial networks. It shows the evolution of a network's behaviors, predicted or not, based on presets.

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

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

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 10: 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

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 11: 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.
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

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 12: 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.
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 13: 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

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 14: 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.

Issue	Description
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

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

Procedure

Step 1 From the main menu, choose **System statistics** > **Center**.

Step 2 Under **PCAP Capture**, select the desired network interface (such as **eth0** for administration or **eth1** for collection).

Step 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.

Step 4 Start the capture.

Note Only one PCAP capture can run at a time.

Step 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

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

Follow these steps to create your personal account.

Procedure

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

The **My Settings** page appears.

Step 2 Under the **General** field, enter **Firstname** and **Lastname**.

Step 3 Under the **Language** field, select the radio button for your preferred interface language.

Step 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.

Step 5 Select the **Restore default parameters** checkbox to restore interface notifications.

Step 6 Click **Save settings**.

Step 7 Clear application cookies.

Risk scores

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 15: Risk score levels

Score	Color	Risk level
From 0 to 39	Green	Low

Score	Color	Risk level
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.