Cisco Cyber Vision New UI Administration Guide, Release 5.6.0

Cisco Cyber Vision
Updated September 8, 2026

Topics included

1 New and changed information....8

2 Introduction to Cisco Cyber Vision New UI....10

Cyber Vision New UI....11
Change the display theme....12

3 Set up Cyber Vision Center....14

System settings....15
Configure the date and time....16
Configure proxy servers....16
Configure DNS servers....17
Audit logs....18
View audit logs....19
Configure audit log retention....19
Sensor management frameworks....20
Sensor management....20
Migrating sensors after system update....21
Host actions....22
Sensor capabilities....22
Sensor actions....23
Sensor health statuses and signals....29
Features of the sensor Advanced view....30
Network definition....31
Define new network....32
Import networks....33
Export network details....34
Assign a network to an organization hierarchy....34
Add custom properties for networks....35
Edit networks....36
Manage detected networks....37
Organization hierarchies....40
Assign multiple PCAP files to an organization hierarchy....41
Filter PLCs by organization hierarchy....41
Assets....42
Asset data management....43
Asset summary....44
Add custom properties to an asset....53
External communications in the New UI....54

Filters....55
Filter views in Cyber Vision New UI....56

4 Configure visibility....58
Alerts....59
Alert types....61
Alert states and key attributes....62
MITRE ATT and CK information for Intrusion Detection alerts....64
Supported actions for alert rules....65
Pause or resume individual alert rules....65
Create alert rules for severe vulnerabilities in monitored entities....66
Create an alert rule for inactive assets....67
Create an alert rule for external communications....68
Configure allowed scanner IP addresses for the Network Scanner alert rule....69
Asset behavior alerts....70
Mute alert instances....74
Clear alerts for specific assets....75
Syslog notification details for alert types....75
Enable or disable syslog notifications for alert types....76
Vulnerabilities....77
Vulnerability detection in Cyber Vision Center....77
Vulnerability scores....78
Vulnerabilities details....78
Acknowledge or unacknowledge vulnerabilities for a single asset....80
Acknowledge or unacknowledge multiple assets for a single vulnerability....81
Acknowledge critical vulnerabilities....81
Communication maps....82
Apply active view filters to the communication map....83
Communication map control panel....84
Exploring groups in a communication map....87
Enable IDS on a sensor....89

5 Configure segmentation....90
Cyber Vision Segmentation....91
Segmentation workspace....91
Enable segmentation on switches....92
Using Cyber Vision segmentation....93
Asset groups....93
Create a global asset group....94
Switch communications views....95
Segmentation recommendations....96
Create micro-segments from asset-group recommendations....96
Segmentation rules....97
Intra-group rules....98

Add an inter-group rule....99
Edit an inter-group rule....100
Edit the default segmentation rule....101
Common service rules....101
Add a common service rule....101
Switch-specific rules....102
Simulate segmentation rule impact....103

6 Cyber Vision Secure Remote Access....104
CV SRA....106
CV SRA Plus....106
SRA roles and permission descriptions....107
Predefined roles....108
CV SRA access methods....108
CV SRA access methods and their characteristics....109
CV SRA dashboard....109
Supported switch and router models for CV SRA....110
Cisco IoT Operations Dashboard....110
Set up first-time access to IoT Operations Dashboard....111
Log in as an existing user to IoT Operations Dashboard....111
Sign in using Cisco single sign-on (SSO)....112
Integrate a corporate identity provider (IdP) with IoT Operations Dashboard....112
Add and manage users....113
Organization statuses....113
Multi-factor authentication settings....114
How MFA enforcement works....114
Enable or disable multi-factor authentication....115
Set up MFA in Cisco identity platform....115
Multi-factor authentication scenarios....116
Network devices onboarding and CV SRA agent deployment....116
Deploy CV SRA agent on network devices using CLI commands....117
Deploy CV SRA agent on IE switches using CLI commands....119
Migrate the SRA Agent from EDM or Application Manager to CLI deployment....120
Configure CV SRA agent for proxy support....121
CV SRA HTTP proxy support....122
Configure a network device using proxy URL....123
Configure a network device using proxy form....123
Multi-VLAN and static IP capabilities....123
Requirement: VLAN configuration for CV SRA....124
VLAN configuration field descriptions....124
Configure a new CV SRA network device for VLAN support with dynamic IP addresses....125
Configure management VLAN with dynamic IP assignment....126
Configure management VLAN with static IP assignment....126
Add additional VLAN ids and IP assignments....127

Modify the VLAN configuration on a network device....127
Install and configure CV SRA agent on a device....128
Use the CV SRA Quick Wizard....128
Edit configuration details for onboarded devices....128
Multiple VRFs on CV SRA routers....129
CV SRA agent connectivity modes....130
Operational technology (OT) assets....130
Add OT assets to a network device....131
Connect a network device to a remote asset....131
Bulk configuration cloning....132
Clone the session configurations....133
View cloning history....134
Remove all assets and access methods from network devices....134
Access control groups....135
Request access in CV SRA....135
Scheduled access in CV SRA....138
How CV SRA Plus remote access works....139
Prerequisites for using CV SRA Plus....140
Download and install the CV SRA Plus application....140
Duo integration with CV SRA Plus....141
How Duo integration works with CV SRA Plus....142
Configure Duo external integration with CV SRA Plus....142
Configure CV SRA Plus policies in Duo....143
Enable Duo integration in CV SRA....144
Verify the CV SRA Plus and Duo integration....145
Configure access methods....145
Configure an SSH access method....145
Configure a telnet access method....146
Configure an RDP access method....146
Configure a VNC access method....147
Configure a Web App access method....148
Configure an CV SRA Plus access method....148
Remote asset session requests....149
Manage requests as an SRA access manager....150
Manage requests as a SRA system or access admin....150
Request outcomes....151
Request History details....151
Revoke an approval request....152
Remote session management and monitoring....152
Remote sessions....153
Monitor a user session....153
Download the session history....153
Terminate a session....154
Modify a remote session....154
Remote session recordings....154

Required IAM permissions for Cisco IoT Operations Dashboard....155
Session recording configuration guidelines....155
Set up CV SRA for session recordings with AWS S3 integration....156
Azure Blob storage for session recordings....157
Record an inline session....157
Review a recorded session....158
Alert rules....159
Alerts configuration page details....159
Configure alert rules for login from prohibited locations....160
Configure alert rules for changed login locations....161
Configure alert rules for login outside of working hours....162
Pause alerts....163
Resume an alert....164
Alerts....164
View user activity in Cisco IoT Operations Dashboard....165
Access expiration policy....167
Modify the default policy....167
Notification schedules....168
Request an access extension for an CV SRA session....168
Manage access extension requests....169
Extend access expiration without user requests....169
Best practices for expiration policy management....170
Secure file transfer....170
Secure file transfer guidelines....171
Upload files to the secure file transfer staging area....171
Review potentially unwanted files before transfer....171
Transfer files to assets....172
Request an access extension for an CV SRA session....173
Request access to a remote session....173
Connect to a remote session using the request access procedure....174
Connect to a scheduled remote session....175
Withdraw a session request....175
Best practices for accessing CV SRA remote sessions....176
Collect CV SRA agent logs from the IOx app....176
DNS resolution issues....178
DNS resolution and network problems symptoms....178
Root causes of DNS and network connectivity issues....179
Fix DNS resolution issues....179
CV SRA agent failures....180
Causes and consequences of CV SRA agent SD card failures....180
Diagnose and fix CV SRA agent installation failures due to IOx issues....180
Diagnose and fix CV SRA agent installation failures due to IOx issues....182
Resolve the "pending services update" state....183
Resolve the "pending creation" state....183
Resolve the "pending removal" state....184

1 New and changed information

Highlights newly introduced features and significant changes in this release, providing a reference point for tracking updates and modifications to the product documentation.

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

Table 1: Feature updates

Feature	Description
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.
Network Scanner alert type	The Network Scanner alert type identifies network reconnaissance and scanning attempts. IP addresses specified in the Allowed Scanner list are excluded and do not generate alerts. For more information, see Alerts on page 59.
Assets with unexpected behaviors alert type	Cisco Cyber Vision monitors the assets that are part of the alert rules, and raises an alert when any of those assets are involved in selected behaviors within the configured time window. For more information, see Alerts on page 59.
Communications page enhancement	The Communications page organizes map data by asset groups and displays communications at the asset-interface level. You can view details for asset interfaces, asset groups, and communications within an asset group. The control panel provides filter options and display settings. For more information, see Communication maps on page 82.

Feature	Description
Assets page enhancement	Asset page organizes information into the Summary, Alerts, Vulnerabilities, Communications, Behaviors, Services, Properties, and Interfaces tabs. The Summary page displays cards that provide a quick, high-level overview of the asset. For more information, see Assets on page 42.
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 Sensor management frameworks on page 20.
Network detection	The Network Definition page has been enhanced to support new network definitions. Network detection runs automatically at regular intervals, with an option for manual, on-demand execution. For more information, see Network definition on page 31.
Audit logs	Cyber Vision records supported user authentication and configuration actions in the audit log. Authorized users can review and export audit records and configure the retention period from 7 through 365 days. The default retention period is 90 days.
Display themes	You can display the Cyber Vision interface using the **Light** or **Dark** theme or use the theme configured for your system. Select the display theme from the user menu.
Segmentation	Introduces Cyber Vision Segmentation and replaces functional groups with asset groups for segmentation workflows. Users can define Security Group Tag identities, model and review rules, review recommendations, and simulate rule impact for supported IE 3x00 switches. For more information, see Configure segmentation on page 90.

2 Introduction to Cisco Cyber Vision New UI

Topics:

- Cyber Vision New UI
- Change the display theme

Describes the overall functionality and benefits of the Cisco Cyber Vision platform's new user interface, highlighting its innovative features and enhanced capabilities for managing and securing industrial networks, including foundational concepts of the new UI.

Cyber Vision New UI

Describes the new Cyber Vision user interface, outlining its key design improvements, navigation options, and functional enhancements that provide streamlined monitoring and management of industrial cybersecurity environments.

A Cyber Vision New UI is an asset-based user interface that

- organizes information around assets, which is a clearer representation of physical equipment, instead of discrete components or device entries,
- aggregates multiple network identities (including interfaces, IP addresses, and MAC addresses) that belong to the same physical equipment, and
- prioritizes the most relevant information, such as asset name, type, and version, to help users stay focused and reduce clutter.

User roles for the Cyber Vision Center New UI are defined in the Classic UI **Admin** > **Users** > **Role Management**.

Table 2: Feature History Table

Feature	Release Information	Feature Description
New UI	Release 5.3.x	Cisco Cyber Vision Center offers New UI that comprises simplified, structured views of assets, vulnerabilities, and alerts. The New UI includes a new method for automatically grouping assets using AI-based clustering. Click **Go to Cyber Vision New UI** in the top banner of your Center to get started.
Cisco Cyber Vision Center 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.
Display themes	Release 5.6.x	You can select the **Light** or **Dark** theme from the user menu. You can also select **System** to use your system's display theme.

Key differences between Classic UI and New UI

The Classic UI focuses on technical entities such as components and devices. Users need to manually define presets, such as baselines or monitoring sets. They often manage separate entries for each network identity, which results in complexity and confusion.

The Cyber Vision New UI connects the physical industrial environment and its digital representation. It visually groups all elements associated with a single physical equipment. Examples include production line equipment or customer installations.

Table 3: Contrast table

Feature	Classic UI	New UI
Entity focus	Components, devices	Assets–representation of physical equipment

Feature	Classic UI	New UI
Information grouping	Each network identity shown as a separate item	Multiple identities grouped by asset
User effort	Requires manual preset definitions	Provides automatic aggregation to improve clarity
Information display	Shows all details, often overwhelming	Displays only the most relevant attributes of each asset.

Change the display theme

Change the appearance of the Cyber Vision interface by selecting a light, dark, or system theme.

Select the display theme that you want to use for the Cyber Vision interface.

Cyber Vision provides the following display-theme options:

- **Light**: Displays the interface using the light theme.
- **Dark**: Displays the interface using the dark theme.
- **System**: Uses the display theme configured for your system.

Procedure

1. In the upper-right corner of the Cyber Vision interface, select your username to open the user menu.
2. Under **Theme**, select **Light**, **Dark**, or **System**.

Cyber Vision applies the selected theme to the interface.

3 Set up Cyber Vision Center

Topics:

- System settings
- Audit logs
- Sensor management frameworks
- Network definition
- Organization hierarchies
- Assets
- Filters

Outlines the end-to-end setup process for Cyber Vision Center, including configuring system settings, managing sensors, defining and managing networks, establishing organization hierarchies, managing assets, and configuring filters for effective network visibility and security.

System settings

Explains how system settings ensure secure, reliable operation of Cyber Vision Center.

System settings are core configuration features that

- define external communication channels for the Cyber Vision Center,
- secure and synchronize operational parameters, and
- enable access to critical external services under controlled conditions.

Table 4: Cyber Vision Center system settings

Setting	Purpose
Date and Time	Date and time synchronization is essential for system stability. A Network Time Protocol (NTP) server ensures that the Cyber Vision Center and all connected sensors share the same time. Synchronized time is required for accurate logging and communication between devices. If an NTP server is unavailable, set the time manually. However, automated synchronization is highly recommended.
DNS (Domain Name System)	DNS operates as the network's directory service. It translates human-readable domain names into IP addresses required for communication. This setting enables Cyber Vision Center to resolve and connect to other systems by name.
Proxy	In secure environments, Cyber Vision is isolated from the internet to protect sensitive data. Some advanced features require Internet connectivity. A proxy server allows Cyber Vision to safely access required external services or updates while protecting the internal network. Cyber Vision sends requests to the proxy server instead of connecting directly to the internet. The proxy handles communication and maintains security and functionality.

Feature history table

Feature	Release Information	Feature Description
Enhanced system connectivity and security settings	Release 5.5.x	The system offers intuitive user interface based settings to simplify administrative workflow. Date and time settings allow for precise time synchronization for the center and connected sensors. DNS management streamlines system access. Proxy configurations ensure secure, controlled connectivity in isolated environments.

Configure the date and time

Configure the date and time settings for your system, either by connecting to an NTP server or manually setting the time.

Synchronize the date and time across your center and all connected sensors to ensure system stability and accurate logs.

Synchronize the date and time consistently for accurate logs and device communication. Use an NTP server to automate and maintain this process. If an NTP server is unavailable, manually configure the date and time.

Procedure

1. From the main menu, choose **Configuration** > **System** > **Date and Time**.
2. Select a method to configure the date and time.

Date and time method	Steps to be taken
(Recommended) Connect to an NTP server	**a.** Enable **NTP Servers**. **b.** Click **Add New NTP Server**. **c.** Enter the IP address or hostname of your NTP server. **d.** Optionally, enter a **Key ID** or **AES-CMAC** for secure authentication. **e.** Click **Test Connection** to verify configuration. **Note** • You can delete added NTP servers as needed. • Click **Reset changes** to revert to your last saved settings.
Manually set the time, in UTC	**a.** Enable **Manually set time (UTC)**. **b.** Set the date and time manually, or click **Get Browser Time** to fetch the current time from your browser and populate the UTC field.

3. Click **Save Changes**.

The system saves the date and time configuration.

What to do next

From the main menu, choose **Configuration** > **System** > **Date and Time** and verify the UTC time.

Configure proxy servers

Configure proxy servers for secure external network connections used by features such as Smart Licensing and SEA integrations.

Set up secure proxy connectivity for features that require external access, including Smart Licensing, SEA, XDR, and other integrations.

Many integrations and licensing features require external network access. Configuring proxy servers ensures that network traffic is securely routed to these services.

Before you begin

- Obtain the IP address and port for your proxy server.
- If your proxy requires authentication, have the username and password ready.

Procedure

1. From the main menu, choose **Configuration** > **System** > **Proxy**.
2. Enable the proxy feature.
3. Enter the IP address (IPv4 or IPv6) and port details for your proxy server.
4. If required, enter the username and password for proxy authentication.
5. Click **Test connection** to verify proxy configuration.
6. Click **Save changes** to apply the configuration.

You see a confirmation message for a successful proxy check. The system applies your proxy configuration and enables network connections through the proxy.

What to do next

- If necessary, click **Reset changes** to restore previous settings.
- Verify that external connectivity for integrations or license-related features continues to function properly.

Configure DNS servers

Configure DNS servers to enable hostname resolution for Cyber Vision Center communications.

Ensure Cyber Vision Center can resolve hostnames to IP addresses for connectivity with other systems.

Configuration of Domain Name System (DNS) servers allows Cyber Vision Center to communicate with other systems that require hostname resolution.

Before you begin

Verify that you have the IP address of the DNS server.

Procedure

1. From the main menu, choose **Configuration** > **System** > **DNS**.
2. Click **Add new DNS server**.
3. Enter the IP address of the DNS server.

   You can add up to 4 DNS servers.
4. Click **Test connection** to verify that Cyber Vision Center can reach the DNS server.

   The system provides a clear notification if the connection fails.
5. Click **Save changes** to apply the settings.

Cyber Vision Center uses the configured DNS servers to resolve hostnames to IP addresses. This setting enables Cyber Vision Center to communicate with other systems.

What to do next

If necessary, click **Reset changes** to revert to your previously saved settings. Verify external connectivity, such as integration or license connectivity, to ensure proper operation.

Audit logs

Use audit logs to review supported user authentication and configuration actions in Cyber Vision.

Understand the user actions that Cyber Vision records and the information available for each audit event.

Cyber Vision records supported user actions in the audit log. Audit records help administrators review user activity and configuration changes.

Examples of recorded actions include:

- User authentication
- Creation of an organization hierarchy level
- Assignment of a network to an organization hierarchy level

> **Note**
>
> Cyber Vision does not currently record every user action. For example, sensor onboarding actions might not appear in the audit log.

Table 5: Feature History Table

Feature	Release Information	Feature Description
Audit logs	Release 5.6.x	Cyber Vision records supported user authentication and configuration actions. Authorized users can review and export audit records and configure the audit-log retention period.

Table 6: Audit record details

Field	Description
Date	Shows when the audited event occurred.
Username	Identifies the user who performed the action.
Type	Identifies the category of the audited event.
Status	Shows whether the action succeeded or failed.
Description	Provides details about the audited action. Select **View more** to display additional information.

View audit logs

Review supported user authentication and configuration actions recorded by Cyber Vision.

View audit records to review user activity and configuration changes in Cyber Vision.

Cyber Vision displays the actions that it currently supports for auditing. The Audit page is available from the user menu.

Before you begin

Ensure that your user role has **Read** permission for Audit.

Procedure

1. In the upper-right corner of the Cyber Vision interface, select your username to open the user menu.
2. Select **Audit**.
3. Review the audit records.

   The table displays the date, username, event type, status, and description for each recorded event.
4. Use the available actions as required:
   - Select **View more** to display the complete description of an event.
   - Select the filter icon to narrow the displayed audit records.
   - Select **Export** to download the audit records.

Cyber Vision displays the available audit records. If you export the records, Cyber Vision downloads the audit data.

What to do next

Configure the audit-log retention period if you need to change how long Cyber Vision retains audit records.

Configure audit log retention

Configure how long Cyber Vision retains audit records.

Set the number of days that Cyber Vision retains audit records.

Cyber Vision retains audit records for 90 days by default. You can configure the retention period from 7 through 365 days.

Before you begin

Ensure that your user role has **Write** permission for Audit.

Procedure

1. In the upper-right corner of the Cyber Vision interface, select your username to open the user menu.
2. Select **Audit**.
3. Select the settings icon.
4. In **Retention period**, enter a value from 7 through 365 days.
5. Select **Save**.

Cyber Vision retains audit records for the configured number of days.

What to do next

Review the Audit page periodically to monitor recorded user activity and configuration changes.

Sensor management frameworks

Explains how Cyber Vision sensor management enables efficient deployment, configuration, and operation of sensors and hosts in industrial networks.

A sensor management framework is a comprehensive platform that

- coordinates the deployment, configuration, and operation of Cyber Vision sensors and hosts,
- manages industrial network environments efficiently, and
- streamlines sensor and host actions, including onboarding, monitoring, and control.

Host and sensor management

- Host management: A host is the physical platform where a sensor IOx application runs. First, onboard and validate hosts. Then, deploy sensors to each host.
- Sensor management: The sensors page allows you to manage sensors and view sensor statistics, operations, and details for each deployed sensor.

Feature history table

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.
Enhancement of sensor health monitoring	Release 5.5.x	Monitor sensor health proactively with automated updates and deep insights. The sensor management system tracks each sensor's status and provides actionable updates, helping you resolve issues before they affect your operations. Use **Advanced View** to analyze performance trends and troubleshoot efficiently.

Sensor deployment overview

Cyber Vision sensors operate as IOx applications. They perform deep packet inspection (DPI) on industrial network traffic and send metadata to the Cyber Vision Center. You can manage multiple sensors concurrently across the network.

Sensor management

Introduces the host model for managing Cisco Cyber Vision sensors. You onboard a physical host before you deploy a sensor, separating device connectivity from network traffic collection.

The Sensor management provides a host model for managing Cisco Cyber Vision sensors. A sensor host is the physical device (such as routers, switches, gateways, etc.) on which Cisco Cyber Vision deploys a sensor. The host model connects Cisco Cyber Vision to the device before the sensor begins collecting network traffic.

- A sensor is deployed on a host that corresponds to the physical device.
- Onboarding makes the host reachable to Cisco Cyber Vision; it does not begin traffic collection.
- After you onboard the host, you can deploy a sensor and configure its collection interface.
- Cisco Cyber Vision uses the Product ID to identify supported switches and routers.

Sensor deployment uses two stages:

1. Onboard hosts to Cisco Cyber Vision
2. Deploy sensor apps to hosts

The collection interface supplies the address used by the sensor to send gathered network data to Cisco Cyber Vision.

Sensors previously deployed using the sensor-management extension in the classic UI are available on the Sensor Management page in the new UI following automatic migration. Refer to Migrating sensors after system update on page 21.

Migrating sensors after system update

Describes the automatic migration of legacy sensors managed by sensor-management extension to the sensor-host model after a system update, preserving sensor identity and configuration without requiring application reinstallation.

When the Cisco Cyber Vision system is updated to version 5.6.0 and rebooted, the system identifies legacy sensor-management extension data. It then migrates the sensors to the sensor-host model on the **Sensor management** page of the new UI.

Summary

The key components involved in the process are:

- System: Detects legacy sensor-management extension data and initiates migration, including a final backup before removing the sensor management extension.
- Sensors: Preserve their identity and configuration as they transition to the sensor-host model in the new UI **Sensor management** page.

Workflow

The process involves the following stages:

1. Upon the first reboot after the Cisco Cyber Vision 5.6.0 update, the system automatically migrates legacy sensors
   - Migration is fully automated; you do not need to uninstall or reinstall the sensor application.
   - For each migrated sensor, the system automatically creates hosts by extracting the host identity attributes (host address, label, credentials, product ID, serial number, and similar data) from the internal database.

Table 7: Configuration imported into the sensor-host model

Configuration area	Imported data
Host identity and access	Host address, label, credentials, Product ID, and serial number
Traffic collection	Capture and collection interfaces, VLANs, gateway, RSPAN, capture mode, and custom filter

Configuration area	Imported data
Sensor configuration	Sensor template, Active Discovery configuration, and SRA configuration

2. Post-migration management and status updates.
   - In Classic UI, the sensor management extension is removed from the **Extension** page, but sensors installed using the extension remain visible in the **Sensor Explorer** page. Sensor management actions (reconfigure, undeploy) are no longer exposed for these sensors.
   - In new UI, the migrated sensors appear in the **Sensor Management** page with a status of **Deployment successful**. These sensors are no longer labeled as Externally managed.
   - The initial host status is QUEUED. Background discovery can update the host status to READY, UNREACHABLE, WRONG_CREDENTIALS, or NOT_READY.
   - When the host is in Ready state and the sensor deployment succeeds, redeploy, uninstall, and update actions are available.

Result

The legacy sensor-management extension is removed, and sensors are fully integrated into the sensor-host model without additional downtime.

What's next

To onboard, manage, or monitor sensors, navigate to the new UI Sensor Management page.

Host actions

Lists the available host actions and their descriptions for Cyber Vision sensor management.

Hosts can be onboarded either by uploading a CSV file for multiple hosts or by manually entering host information individually. For detailed instructions, refer to the Onboard hosts to Cisco Cyber Vision section in the *Deploy Cisco Cyber Vision Sensor on Switches and Routers* guide.

This table lists the available host actions for managing Cyber Vision sensors and describes each action:

Action	Description
Host Status	Check the host readiness status to ensure IOx is running and necessary conditions for deployment are met.
Deploy Sensor	Deploy the sensor application on the selected host.
Change Credentials	Update the username and password stored in the system to access the host.
Remove Host	Remove the host from the list.

Sensor capabilities

Provides a reference to sensor host model capabilities available after sensor migration and deployment in the Sensor management page.

This reference provides details on managing sensor capabilities through the Sensor management page.

Capabilities

On the **Sensor management** page, each sensor lists its configuration under the **Capabilities** column. You can click on a listed capability to modify its settings as needed.

The table shows the most common capabilities listed under the **Capabilities** column:

Table 8: Deployed Sensor capabilities

Capability	Configuration
Snort	Change the Snort status - Enable or Disable
Active Discovery	Configure Active Discovery
Secure Remote Access (SRA)	Change Secure Remote Access configuration: Use center as proxy, Direct, or Proxy.

Sensor actions

This reference lists the sensor actions you can use to manage Cyber Vision sensors and explains their purpose.

Cisco Cyber Vision sensor deployment follows host onboarding. The sensor collects network data from the host and sends it to Cisco Cyber Vision using a dedicated collection-interface address. For detailed instructions on deploying sensors, refer to the Deploy sensor apps to hosts section in the *Deploy Cisco Cyber Vision Sensor on Switches and Routers guide*.

This table lists the available sensor actions you can use and describes how each helps you manage Cyber Vision sensors.

Action	Description
Redeploy	Send the IOx package to redeploy the sensor. You can reconfigure parts such as IP parameters.
Update	When a new Cyber Vision Center version is deployed, a new sensor version becomes available. Use **Update** to upgrade.
Assign to Organization Hierarchy	Map sensors to an organizational hierarchy to organize asset data and operational context. See Assign sensors to the Organization Hierarchy on page 24
Change GPS Location	Manually update the GPS coordinates of the sensor to reflect its location. For more information on the GPS coordinates configuration, see Sensor geolocation data.
Configure Snort	Enable or Disable Snort.
Configure Active Discovery	Configure Active Discovery or change to Passive only to disable Active Discovery.
Configure Secure Remote Access	Enable Secure Remote Access and configure proxy setting.
Uninstall	Remove the sensor from the list and uninstall the application from IOx.

Assign sensors to the Organization Hierarchy

Assign one or more sensors to an organization hierarchy so asset creation is enabled within Cyber Vision.

Enable asset creation within Cyber Vision by mapping sensors to an organization hierarchy.

Use this task to map sensors in your environment to a defined organization hierarchy. This enables Cyber Vision to structure asset data and operational context according to organizational boundaries.

Procedure

1. From the main menu, choose **Configuration** > **Sensor Management** > **Sensors**.
2. Check the checkboxes of the sensors.
3. Select **Assign to Organization Hierarchy** from the **More actions** list.
4. Select the organization hierarchy you want to assign the sensors to.
5. Click **Assign** to confirm.

Cyber Vision assigns the selected sensors to the organization hierarchy you specified. Each assigned sensor enables asset creation within Cyber Vision based on its organizational context.

Configure Snort

Configure Snort intrusion detection on compatible Cisco sensors to monitor network traffic for suspicious activities using Snort rules.

Enable Snort to detect and alert on malicious network activity on Cisco sensors.

Snort is an intrusion detection system (IDS) that raises alerts for suspicious or malicious network activity based on predefined rules. By default, Snort is disabled on sensors but enabled on the Center's Deep Packet Inspection (DPI)

Enabling Snort on compatible sensors helps monitor assets for threats.

For further details on Snort, refer to the Snort topic in the *Cisco Cyber Vision Classic UI Administration Guide*.

For information on the Snort-related intrusion detection alert rules, refer Alerts on page 59.

Before you begin

- Ensure your sensor is deployed on a device compatible with Snort:
  - Cisco IC3000 Industrial Compute Gateway
  - Cisco Catalyst 9300 Series Switches
  - Cisco IR8340 Integrated Services Router Rugged
  - Center DPI Interface
- Configure Snort rules for the Intrusion Detection alert type.

Follow these steps to configure Snort on Cisco sensors.

Procedure

1. From the main menu, choose **Configuration** > **Sensor Management**.
2. Click the **Sensors** tab.
3. Locate the sensor on which you want to enable Snort.

4. Under **Capabilities**, click **Snort**. Alternatively, under **Action**, click the horizontal ellipsis (...) icon and choose **Configure Snort**.

   You can also select multiple sensors and then choose **More actions** > **Configure Snort**.

5. In the **Configure Snort** dialog, click **Enable Sort**.

   A check mark appears next to **Snort** under **Capabilities**, confirming that Snort is enabled.

Snort actively monitors network traffic on the selected sensors for suspicious or malicious activity according to the configured rules.

Disable Snort

Configure a sensor to disable Snort-based intrusion detection when monitoring is no longer required.

Disable Snort intrusion detection on a sensor to cease monitoring traffic for threats.

Perform this task when Snort monitoring is no longer needed for a given sensor in your environment.

Before you begin

Ensure Snort is currently enabled on the sensor.

Follow these steps to disable Snort on a sensor.

Procedure

---

1. From the main menu, choose **Configuration** > **Sensor Management**.
2. Click the **Sensors** tab.
3. Locate the sensor on which you want to disable Snort.
4. Under **Capabilities**, click **Snort**. Alternatively, under **Action**, click the horizontal ellipsis (...) icon and choose **Configure Snort**.

   You can also select multiple sensors and then choose **More actions** > **Configure Snort**.

5. In the **Configure Snort** dialog, click **Disable Snort**.

   Snort is disabled on the selected sensor(s). The check mark next to **Snort** under **Capabilities** disappears.

Configure Active Discovery on a sensor

Provides instructions to enable Active Discovery from Sensor Management, select the discovery interface, and add dedicated interfaces.

Enable active discovery to collect asset properties on the network using a compatible Cisco Cyber Vision sensor.

You can configure Active Discovery on a compatible Cisco Cyber Vision sensor after the sensor is deployed. Active discovery sends requests from the sensor to assets in the network and collects their properties.

To configure active discovery on a switch, router, or Cisco IC3000, sensors must be deployed using the IOx sensor application file that supports active discovery.

On a Cisco IC3000, you can configure Active Discovery by performing a manual configuration.

Before you begin

- Deploy a sensor with correct settings, including IP address, VLAN, gateway, or routes.
- Confirm the sensor platform supports active discovery. Supported devices include:

- Cisco IE3300, Cisco IE3400, and Cisco IE9300.
- Cisco IC3000 Industrial Compute Gateway.
- Cisco Catalyst 9300, Cisco Catalyst 9300X and Cisco Catalyst 9400.

Follow these steps to configure active discovery.

Procedure

1. From the main menu, choose **Configuration** > **Sensor Management**.
2. Click the **Sensors** tab.
3. Locate the sensor on which you want to enable or update Active Discovery.

   Note

   You can configure active discovery only if it is shown in the **Capabilities** column for that sensor.

4. Under **Capabilities**, click **Active Discovery**. Alternatively, under **Action**, click the horizontal ellipsis (...) icon and choose **Configure Active Discovery**.

   Active Discovery must be configured for each sensor individually.

5. In the **Configure Active Discovery** dialog, do the following:
   a) If you want Active Discovery to use the sensor's collection network, select **Use collection interface**.

      The collection network interface can perform discovery on the same subnet as the sensor IP address or through the sensor's collection gateway.

   b) To perform Active Discovery on additional subnets, enter **IP address**, **Prefix length**, and **VLAN number**.

      For Cisco IC3000, select a physical **Interface** from the drop-down list.

      These settings define the dedicated network interface used for active discovery.

   c) To add another network interface, click **+Add network interface**.
   d) Click **Configure Active Discovery**.

   A check mark appears next to **Active Discovery** under **Capabilities**, indicating configuration is successful.

Active discovery is enabled on the sensor, and it is now ready to scan assets using the configured interfaces.

What to do next

To complete the center-side Active Discovery configuration, set the required policy and profile in the classic UI under **Admin** > **Active Discovery**. The policy selects the protocols to use; the profile specifies the assets and sensor. Only sensors with active discovery activated appear in the sensor list. For more information, refer to *Cisco Cyber Vision Active Discovery Configuration Guide*.

Disable Active Discovery on a sensor

Guides you through changing a configured sensor to Passive only and disabling Active Discovery from the Configure Active Discovery dialog.

Ensure a sensor stops Active Discovery and operates in passive-only mode.

Active Discovery allows a sensor to actively query network assets to gather information. Disabling Active Discovery ensures the sensor remains passive and only observes network traffic.

Before you begin

Confirm you have access to a sensor currently configured with Active Discovery.

Follow these steps to disable Active Discovery for a sensor:

Procedure

1. From the main menu, choose **Configuration** > **Sensor Management**.
2. Click the **Sensors** tab.
3. Locate the sensor for which you want to disable Active Discovery.
4. Under **Capabilities**, select **Active Discovery**. Alternatively, under **Action**, select the horizontal ellipsis (...) icon and then select **Configure Active Discovery**.
5. In the **Configure Active Discovery** dialog, select **Passive only**.
6. Click **Disable Active Discovery**.

Active Discovery is disabled for the sensor, and the sensor is set to passive-only mode.

Configure Secure Remote Access on a sensor

Guides you through enabling Secure Remote Access on one deployed sensor, selecting the center, direct, or proxy connection method, and providing proxy connection details when required.

Enable Secure Remote Access on a sensor and configure its connection method to reach remote services securely.

Use Sensor Management to configure Secure Remote Access for individual sensors. The sensor uses the chosen method (center as proxy, direct, or proxy) to connect to Cisco services and the IoT Operations Dashboard.

Before you begin

Make sure center-side Secure Remote Access integration is enabled and configured for the target IoT Operations Dashboard tenant (In the classic UI, navigate to **Admin** > **Integrations** > **SRA** > **Configuration**).

Ensure Active Discovery is enabled on the sensor; this feature requires only a compatible platform. Refer to the Active Discovery configuration documentation - Configure Active Discovery on a sensor on page 25

Follow these steps to configure Secure Remote Access on a sensor.

Procedure

1. From the main menu, choose **Configuration** > **Sensor Management**.
2. Click the **Sensors** tab.
3. Locate the sensor to configure Secure Remote Access.

   Configure Secure Remote Access for one sensor at a time.

4. Under **Capabilities**, click **SRA**. Alternatively, under **Action**, click the horizontal ellipsis (...) icon and choose **Configure Secure Remote Access** .

   Configure Secure Remote Access for one sensor at a time.

5. In the **Configure Secure Remote Access** dialog, do the following:
   a) Toggle **Use SRA** to enable Secure Remote Access.

The configuration dialog identifies the sensor whose Secure Remote Access configuration you are changing. Enable SRA, and then choose the proxy or another connection method.

b) Select a connection method:

- **Use center as proxy** - If the sensor uses the Center to reach Cisco services.
- **Direct** - If a Collection gateway is specified.
- **Proxy** - If the sensor uses another server for Cisco services.

If you select **Proxy**, enter the details as shown in the table.

Table 9: Proxy settings

Field	Description
http:// or **https://**	Depending on your requirements, choose either **http://** or **https://** from the drop-down list.
Server	Enter the Server IP address.
Port	Enter the Port number.
Username and **Password**	(Optional) Enter the username and password.
Primary DNS and **Secondary DNS**	(Optional) Enter the primary and secondary DNS.

6. Click **Configure Secure Remote Access**.

A check mark appears next to **SRA** under **Capabilities**, confirming Secure Remote Access is configured.

The Center updates the sensor and IoT Operations Dashboard configuration, creates and deploys the Secure Remote Access agent as needed.

7. To validate the SEA Agent Connection, do the following:
   a) Log in to the IoT Operations Dashboard with your IoT OD credentials.
   b) In **Secure Equipment Access**, choose **System Management** > **Network Devices.**.
   c) Verify the SEA Agent Connection is **Up** for the configured network device.

When the connection is up, the sensor can access remote assets on the network.

Secure Remote Access is configured for the sensor. When the connection is established, the sensor can access remote assets through the chosen method.

Disable Secure Remote Access on a sensor

Guides you through disabling Secure Remote Access for a configured sensor from the Configure Secure Remote Access dialog.

Prevent a sensor from accessing remote assets by disabling Secure Remote Access.

Disable Secure Remote Access for a sensor when remote access is no longer needed, one sensor at a time, from Sensor Management.

Before you begin

Ensure Secure Remote Access is configured and available for the sensor under **Capabilities**.

Follow these steps to disable Secure Remote Access on a sensor.

Procedure

1. From the main menu, choose **Configuration** > **Sensor Management**.
2. Click the **Sensors** tab.
3. Locate the sensor for which you want to disable Secure Remote Access.

   Secure Remote Access can be disabled for one sensor at a time.
4. Under **Capabilities**, select **SRA**. Alternatively, under **Action**, select the horizontal ellipse (...) icon and choose **Configure Secure Remote Access**.
5. In the **Configure Secure Remote Access** dialog, disable the **Use SRA** option.
6. Click **Configure Secure Remote Access**.

Secure Remote Access is disabled for the selected sensor.

Sensor health statuses and signals

Lists and explains the key sensor health statuses and signals used in the system, including what each status and signal means, and how to interpret them for device health management.

Health statuses

You can view the current health status for each sensor. The status helps you decide when to take action.

Status	What this status means
Unknown	The sensor is managed by Classic UI.
Critical	The sensor has stopped communicating and is not sending data to the Center.
Needs Attention	The sensor is connected and sends data, but one or more health signals are outside the allowed thresholds. You may need to reconfigure the sensor or take other action.
Healthy	The sensor operates within normal parameters and no health signals are active.
Pending	The sensor is connected. The system updates the health status after it collects initial data. This process may take up to an hour.

To view the current health status for each sensor, from the main menu choose **Configuration** > **Sensor Management**.

Sensor health signals

When a sensor's health status is **Needs Attention**, the Cyber Vision Center provides these health signals to explain the issue and suggest mitigation steps.

Table 10: Health signals

Signal	What this signal means
With Time Drift	The time difference between the sensor and the Center exceeds the configured threshold.

Signal	What this signal means
Degraded Flow Health	The overall traffic from the sensor to the Center after connection is less than expected. You can use this information to decide if traffic integrity falls below the configured threshold.
Degraded Traffic Health	Unicast traffic is lower than expected. You see this signal when the ratio of unicast traffic to broadcast or multicast traffic is too low.

To view remediation details for a sensor with the **Needs Attention** health status:

- Select the sensor in **Configuration** > **Sensor Management**.
- Access the remediation card to see health signals, issue descriptions, sensor summaries, and mitigation steps.

For more information about system health, network metrics, and network interface bandwidth, see **System statistics for Center and sensors** topic in the Cisco Cyber Vision Classic UI Administrator Guide.

Features of the sensor Advanced view

Provides a comprehensive reference for the sensor Advanced view, including behavioral trends, real-time statistics, and key metrics used to monitor and troubleshoot sensor performance.

In the sensor **Advanced view**, you can:

- Examine sensor behavioral trends and performance.
- Troubleshoot sensor issues using real-time statistics.

Collection Details

Monitor sensor connection health, uptime, and network statistics, with options to filter by time periods.

Detail	Description
Connection Status	Provides sensor connection information with the Center, including online or offline status with date and time.
Link Status	Indicates two link statuses: • If the sensor is connected to the Center, the status is UP. • If the sensor is rebooted or restarted, the status is DOWN.
Time Drift	Calculates the time difference between sensor time and Center time when system information is received.
TX/RX Queue	TX and RX queues are memory buffers. They temporarily store outgoing (Transmit) and incoming (Receive) data packets. This helps manage traffic flow and prevents data loss between the network interface and the system Transmission Control Protocol/Internet Protocol (TCP/IP) stack.

Detail	Description
Retransmits	Number of TCP retransmits to resend packets lost, corrupted, or unacknowledged during initial transmission. This ensures reliable and complete delivery.
TCP Connection - Connection Reset & TCP State	Displays the TCP connection status from the Center to the sensor and shows connection reset events. These events indicate port changes or reestablishments. The connection state may change rapidly with each reset.

Data Quality

Displays information about network traffic, packet distribution, and flow statistics.

Detail	Description
Flow Count	Shows the number of traffic flows over the selected period. Receiving traffic flows indicates good sensor health.
Total Bytes	Shows the total size of each packet within the selected interval.
Total Packets	Shows the packet count within the selected interval.
Protocol Distribution	Provides the count of TCP, UDP, and other protocols detected in the traffic.
Flow Type Distribution	Shows counts for traffic flow types such as Unicast, Broadcast, and Multicast.

Access the sensor advanced view

To access advanced sensor details:

- From the main menu choose **Configuration** > **Sensor Management** and select the sensor.
- Click **Advanced view**.

Network definition

Introduces network definition in Cyber Vision, guiding you through configuring subnetworks, classifying IP addresses as internal or external, managing asset grouping and metadata, and handling exceptions for IP address classification and their impact on security assessments.

A network definition is a network configuration element that can be used to define IP ranges and classify them as internal (OT), internal (IT), or external. This configuration helps you group or exclude assets for security assessments and manage metadata by assigning custom properties network-wide to all assets.

IP address classification

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.

To treat an external IP address as **OT Internal**, create a custom network containing the IP address and set its network type as **OT Internal**. This is useful for industrial sites that use public IP addresses in private networks.

Marking a set of IP addresses as **External** triggers the following system actions:

- Excludes associated assets.
- Stores external assets with limited properties and only when they are associated with communications to an internal asset.
- Suppresses component and asset creation and redirects the relationship to external communication data.

Feature history table

Feature	Release Information	Feature Description
Network detection	Release 5.6.0	The Network Definition page has been enhanced to support new network definitions. Network detection runs automatically at regular intervals, with an option for manual, on-demand execution.

Define new network

Guides you through defining new networks and subnetworks by specifying IP ranges, VLANs, network types, and custom properties to enable precise device grouping and monitoring within your network organization.

Facilitate precise management and monitoring of devices by defining networks and subnetworks.

Use this task to add a new network to your network organization. Customize IP ranges, VLANs, network types, and custom properties to improve device grouping and monitoring.

Before you begin

- Ensure you have the required IP addresses and subnets.
- Ensure you have **Network Definition** permission with **read/write** access.
- (optional) Obtain VLAN ID information if applicable.

> **Note**
>
> The VLAN ID is an advanced, optional parameter intended for specific use cases. Only configure a VLAN ID when explicitly required. Specifying a VLAN ID when not necessary may result in unexpected network behavior, such as inaccurate traffic classification or asset grouping errors.

Follow these steps to define new networks.

Procedure

1. From the main menu, choose **Configuration** > **Network Definition**.
2. Click **Define a new network**.
3. Select the **Network Type** (Options include **OT Internal**, **IT Internal**, or **External**).

   The selected network type affects Cyber Vision performance, flow storage, device risk scoring, and device license count.
4. Enter an IP address and its subnet in the **IP address/Prefix** field.
5. Enter the network **Name**.
6. (Optional) Expand **Advanced settings**, and enter the **VLAN ID** to enable overlapping networks.

   > **Note**
   >
   > Only set the VLAN ID if required.

7. (Optional) Expand **Custom properties**.

   Example
   To assign an owner name to a network, enter “Owner” as the key and the owner’s name as the value.

   When you set custom properties at the network level, those properties automatically apply to all associated assets to ensure consistency and reduce repetitive data entry.

   a) Enter a custom **Key**.
   b) Enter the corresponding **Value** for the Key.
   c) Click **Add**.
   d) To add multiple custom properties, repeat the steps and click **Add**.
8. Click **Save**.

You have added a network with the specified IP range, VLAN, network type, and custom properties. This enables accurate grouping and monitoring of assets.

Import networks

Import new networks or update existing network details by uploading a CSV template.

Enable efficient network creation and update in bulk using a standardized CSV template.

This task allows you to add multiple networks or update existing network information by importing a CSV file. Download the template, fill in the necessary network details, and upload the completed file to update your network inventory.

> **Note**
>
> You can export detected networks using the **Export** > **Recommended networks** option, update the required details in the exported CSV file, and then import the file. This approach simplifies bulk updates to multiple subnets.

Follow these steps to import networks using a CSV template.

Procedure

1. From the main menu, choose **Configuration** > **Network Definition**.
2. Click **Import** in the **Network Definition** page.

   The **Import networks** window appears.
3. Click **Download template** to download the CSV file for network import.

   The template file is saved to your local device.
4. Fill in the template with the required network details, VLAN ID, and custom properties, and then save it on your local computer.
5. In the **Import networks** window, upload the completed network template by either: click the upload icon to browse the updated network template or drag and drop the network template to the area to upload.
   - Clicking the upload icon and browsing to your updated CSV file, or
   - Dragging and dropping the template into the upload area.

   The Import completed success message is displayed.
6. (Optional) To import another CSV file of your networks, click **Import another CSV**.
7. Click **Close** to exit the import window.

The imported networks appear in the Network Definition page, and you can review the updated or newly added network entries.

Export network details

Configure options to export network and subnetwork definitions as CSV files for external analysis or record-keeping.

Export the network and subnetworks listed in the Network Definition page as CSV files.

You may need to export network details to facilitate documentation, perform external analysis, or maintain backup records.

Follow these steps to export network details.

Procedure

1. From the main menu, choose **Configuration** > **Network Definition**.
2. Click **Export** and select one of the following options:
   - **Defined networks**
   - **Recommended networks** (includes only detected networks)
   - **All networks** (includes both defined and detected networks)

   The corresponding CSV file is downloaded to your local drive.

The selected network details are exported as CSV files and saved to your local drive for further use.

Assign a network to an organization hierarchy

Configure and associate a network with a specified organization hierarchy level to align management access and policies.

Assign a specific network to a designated level within the organization hierarchy, ensuring policy controls and access are tied to organizational structure.

Use this task to organize network resources, apply hierarchical policies, or update organizational assignments for networks.

Before you begin

Ensure you have Network Definition permission with **read/write** access.

Follow these steps to assign a network to an organization hierarchy.

Procedure

1. From the main menu, choose **Configuration** > **Network Definition**.
2. In the list of available networks, locate and select the network you want to assign.
3. Click **Assign to Organization Hierarchy**.

   The **Assign to Organization Hierarchy** pane opens on the right side of the page.
4. In the right pane, search for and select the desired organization hierarchy level.
5. Click **Assign**.

The selected network is now associated with the specified level in the organization hierarchy.

Add custom properties for networks

Learn how to configure custom properties to manage metadata for assets, improving emergency response and maintenance operations.

Efficient metadata management is achieved by assigning custom properties network-wide to all assets.

Custom properties at the network level automatically propagate to all associated assets, ensuring consistency and reducing repetitive data entry. Properties defined at the network level cannot be edited at the asset level, preserving data integrity. Asset-level custom properties apply only to the individual asset and do not update or override properties defined at the network level.

Before you begin

- Ensure you have **Network Definition** permission with **read/write** access.

Follow these steps to add custom properties to a network.

Procedure

1. From the main menu, choose **Configuration** > **Network Definition**.
2. Select the network to which you want to add custom properties.
3. Click the ellipses icon (...) located at the end of the network row.
4. Click **Add Custom Properties** from the context menu.
5. Enter a custom key and its corresponding value and click **Add**.

   Example
   To add an owner name for a network, set the key to "Owner" and the value to the owner's name.

   To add multiple custom properties, repeat this step for each key-value pair.

6. Click **Save**.

The custom properties are assigned at the network level and automatically propagate to all associated assets, maintaining consistency across your environment.

> **Note**
>
> The custom properties set at the network level cannot be edited at the asset level.

Edit custom properties for networks

Configure custom properties for a network to store additional attributes, such as metadata or classification details.

Update the custom properties for a network to reflect necessary changes and maintain accurate network information.

Custom properties allow you to tag networks with metadata or other relevant information.

> **Note**
>
> Custom properties set at the network level cannot be edited at the asset level.

Before you begin

- Ensure you have **Network Definition** permission with **read/write** access.

Procedure

1. From the main menu, choose **Configuration** > **Network Definition**.
2. Select the network to which you want to edit custom properties to.
3. Click the ellipses icon (...) located at the end of the network row.
4. Click **Edit Custom Properties** from the context menu.
5. Click the edit icon associated with the properties.
6. Update the custom key or its corresponding value as needed.
7. Click **Save**.

The custom properties for the selected network are updated, and the changes are applied to the network configuration.

Edit networks

Configure and update existing network details, or perform bulk edits for multiple networks.

Update network information efficiently, including IP address, name, type, and delete networks as needed.

Use this task to manage and maintain your network definitions as your environment changes. Editing network details allows you to keep your configurations current, ensuring accurate device management.

Follow these steps to edit network details or perform bulk edits.

Procedure

1. From the main menu, choose **Configuration** > **Network Definition**

   The **Network Definition** page displays all current networks and subnetworks.

2. To edit multiple network details, click **Edit networks**.
   a) Update the fields for **IP address**, **Name**, **Type** as needed.

      Use available filters to search for networks based on criteria such as IP address, name, type, or VLAN.

      If you need to undo changes, use the revert icon.

   b) To delete networks, select the relevant check boxes and click the **Remove** button.
      Alternatively, click the trash icon next to the network.

      If you need to undo changes of the selected networks, use the **Revert** button.

   c) Click **Save changes** to apply your edits.
3. To edit an individual network, select the network check box and click **Edit**.
   a) Change the **IP address**, **Name**, **Type** as required.

      Use available filters to search for networks based on criteria such as IP address, Name, and Type.

      If you need to undo changes, use the revert icon.

   b) To delete the network, select its check box and click the **Remove** button.
      Alternatively, click the trash icon next to the network.

      If you need to undo changes of the selected network, use the **Revert** button.

   c) Click **Save changes** to apply your edits.

Manage detected networks

Configure and validate the detected network using manual detection in Cyber Vision Center.

Use this task to run the network detection, and then manage the detect networks by either accepting, updating, or discarding them.

Cyber Vision Center automatically runs network detection at regular intervals. You can also run network detection from the **Network Definition** page and review the detected networks.

Before you begin

Ensure that network traffic data is available in Cyber Vision Center. If required, use the Cyber Vision Classic UI to upload PCAP files containing OT network traffic.

Follow these steps to manually detect, review, and manage your networks

Procedure

1. From the main menu, choose **Configuration** > **Network Definition**.
2. Click **Run detection**.

   Cyber Vision Center starts the network detection process and displays a success message when the process is complete.

3. Click **Verify detected networks**.

The **Verify detected networks** window opens with a list of detected networks.

4. Review the detected networks and perform any of the following actions, as required:
   - Accept the detected networks on page 38
   - Update the detected networks on page 38
   - Discard the detected network on page 39
5. Click **Save changes**.

Accept the detected networks

Configure and verify detected networks, then accept selected networks for monitoring and management.

Use this task after running the network detection process in Cyber Vision Center to review and accept discovered networks for system integration.

Follow these steps to accept the detected networks.

Procedure

1. From the main menu, choose **Configuration** > **Network Definition**.
2. Click **Run detection**.

   Cyber Vision Center starts the network detection process and displays a success message when the process is complete.
3. Click **Verify detected networks**.

   The **Verify detected networks** window opens with a list of detected networks.
4. Accept the applicable detected networks.

   To accept individual networks:

   a) Locate the networks using available search criteria (for example, IP address, name, or type).
   b) Click the check mark icon for that network to accept the network.

      To undo the action, click the revert icon available for that network.

   Or,

   To accept multiple networks,

   a) Locate the network using available search criteria (for example, IP address, name, or type).
   b) Select the check box for each network to be accepted.
   c) Click the **Accept** button.

      To undo the action, click the **Revert** button.
5. Click **Save changes**.

Update the detected networks

Configure and update the details of detected networks before accepting them.

When networks are detected by Cyber Vision Center, you have the opportunity to review, modify, and accept the network details. This process allows you to correct any inaccuracies before accepting the networks.

> **Note**
>
> You can export detected networks using the **Export** > **Recommended networks** option, update the required details in the exported CSV file, and then import the file. This approach simplifies bulk updates to multiple subnets.

Follow these steps to review and update detected networks.

Procedure

1. From the main menu, choose **Configuration** > **Network Definition**.
2. Click **Run detection**.

   Cyber Vision Center starts the network detection process and displays a success message when the process is complete.
3. Click **Verify detected networks**.

   The **Verify detected networks** window opens with a list of detected networks.
4. Update the detected networks as required.

   To update a single network:

   a) Locate the networks using available search criteria (for example, IP address, name, or type).
   b) Update the **IP address**, **Name**, or **Type** fields as needed.

      To undo the changes, click the revert icon available for that network.

   c) Click the check mark to accept the updated network.

   Or,

   To update multiple networks,

   a) Locate the network using available search criteria (for example, IP address, name, or type).
   b) Select the check box for each network to be updated.
   c) Update the **IP address**, **Name**, or **Type** fields as needed.

      To undo the changes, click the **Revert** button.

   d) Click the **Accept** button.
5. Click **Save changes**.

Discard the detected network

Configure Cyber Vision Center to remove unwanted detected networks by selecting and discarding them from the list.

At times, network detection discovers networks that are not relevant for your environment. Discarding such networks helps ensure the inventory reflects only valid, required networks.

Follow these steps to discard detected networks:

Procedure

1. From the main menu, choose **Configuration** > **Network Definition**.
2. Click **Run detection**.

   Cyber Vision Center starts the network detection process and displays a success message when the process is complete.

3. Click **Verify detected networks**.

   The **Verify detected networks** window opens with a list of detected networks.

4. Discard the detected network that are not relevant.

   To discard individual networks:

   a) Locate the networks using available search criteria (e.g., IP address, name, or type).
   b) Click the trash icon for that network.

      To undo the action, click the revert icon available for that network.

   Or,

   To discard multiple networks,

   a) Locate the network using available search criteria (e.g., IP address, name, or type).
   b) Select the check box for each network to be discarded.
   c) Click the **Discard** button.

      To undo the action, click the **Revert** button.

5. Click **Save changes**.

   Note

   The discarded network suggestions can be restored by clicking the **Review discarded networks** button on the **Network Definition** page. This button appears only when at least one network suggestion has been discarded.

Organization hierarchies

Outlines the structure and management of organization hierarchies in Cisco Cyber Vision Center, including grouping assets and sensors, configuring hierarchical levels, nesting constraints, and administering levels for effective organization and access control.

Organization hierarchies are structural models that

- group assets, sensors, and data sources within Cisco Cyber Vision Center,
- arrange those entities in a hierarchical tree of levels (nodes), and
- enable granular organization, management, and access control across multiple subdivisions.

Hierarchy management

- Each node in the hierarchy is a level.
- The system defines the Global level and places it at the top of the hierarchy. You cannot delete this level.
- You can add, edit, or delete levels. However, if a level contains child levels or assigned entities such as sensors or PCAPs, the system prevents deletion.
- The system supports nesting up to five sub-levels; after this limit, no additional levels can be added.
- You can add, edit, or delete levels in the hierarchy through **Configuration** > **Organization Hierarchy**.

Assign multiple PCAP files to an organization hierarchy

Guides you through assigning multiple PCAP files to an organization hierarchy to organize assets and automate asset creation in Cisco Cyber Vision.

Before you begin

- Confirm you have appropriate permissions to assign PCAP files.
- Ensure the required PCAP files have already been uploaded.

Assign multiple packet capture (PCAP) files to an organization hierarchy to enable automated asset creation in Cisco Cyber Vision.

Use this task to organize and manage multiple PCAP files for asset management within an organization hierarchy.

Follow these steps to assign multiple PCAP files to the organization hierarchy:

Procedure

1. From the main menu, choose **Configuration** > **PCAPs**.
2. Select the PCAP files you want to assign to an organization hierarchy.
3. Click **Assign Selected to Organization Hierarchy**.
4. Choose the appropriate organization hierarchy.
5. Click **Assign**.

The selected PCAP files are assigned to the chosen organization hierarchy, automatically initiating asset creation in Cisco Cyber Vision.

Each PCAP initiates asset creation in Cisco Cyber Vision.

Filter PLCs by organization hierarchy

Guides you through organizing and reviewing PLC assets by applying filters based on organization hierarchy, including necessary prerequisites and step-by-step instructions for viewing PLCs at different organizational levels.

Organize and review your PLC assets based on the organization hierarchy.

Before you begin

- Create your organization hierarchy.
- Assign sensors, networks, and PCAP to your organization hierarchy.

Procedure

1. From the main menu, choose **Organization**.
2. Select **Sensors** or **Networks**.
3. Select the organization level.
4. Click **Edit** on the active view bar.
5. Apply the **Asset types** filter for PLCs.
6. Click **Apply**.

The list displays PLCs organized by the selected organization hierarchy level.

Assets

Outlines the definition, categorization, and management of assets in Cisco Cyber Vision, including modular asset structures, feature enhancements such as summary views and custom properties, asset search capabilities, CSV export improvements, and details on interface identification and visualization.

An asset is a network entity that

- serves as a core physical component within an industrial network, such as a programmable logic controller (PLC), a switch, a controller, or a server,
- may represent one or more modules with distinct identifiers, which may include serial number, reference, or type, even when MAC and IP addresses overlap; and
- is defined, categorized, and managed according to established rules in Cisco Cyber Vision to ensure effective asset inventory and operations.

Modular assets: If an asset is modular, such as a chassis with multiple modules, its summary shows details including slot, model name, type, firmware version, and serial number. Each module, such as a CPU, communication module, or I/O module, appears as a separate block in the chassis view.

Table 11: Feature History Table

Feature	Release Information	Feature Description
Assets page enhancement	Release 5.6.x	The **Assets** page includes the following tabs for each asset: **Summary**, **Alerts**, **Vulnerabilities**, **Communications**, **Behaviors**, **Services**, **Properties**, and **Interfaces** The cards on the **Summary** page provide high-level information about an asset before you open a related details tab.
Custom properties	Release 5.5.x	Add custom properties to Cisco Cyber Vision assets. You can view, add, and edit these properties, with strict validation rules enforced to maintain data integrity.

Feature	Release Information	Feature Description
Search bar	Release 5.3.x	New UI contains a search bar in the global top banner. You can search for an asset by name, IP address, or MAC address.
Asset list CSV enhancements	Release 5.3.x	The CSV that you download from Cyber Vision Center includes a column that lists the sensors that have detected assets.

Asset data management

Outlines the main functions for managing asset data on the Assets page, including filtering, searching, deleting, exporting, customizing table views, and sorting or adjusting columns to organize and review asset information effectively.

The table presents the main functions available for managing asset data in the **Assets** page. It describes the specific capabilities and behavior of each function.

Function	Description
Use widgets to filter assets table	The widgets at the top of the Assets page allow you to filter data in the asset table. You can select any of these widgets to display the corresponding data: • Active Alerts • Vulnerabilities • Discovered in last 7 days • Discovered in last 30 days
Delete assets	By default, the system deletes assets removed from the production line after 30 days. You can manually delete assets detected due to misconfiguration. If sensors detect the assets again, the system may re-add them to the inventory.
Search for assets	Enter at least three characters from an asset's name, IP address, or MAC address in the search bar to quickly locate details.
Export	Export all asset data to a CSV file. The export includes asset IDs so you can distinguish assets with the same name.

Function	Description
Manage asset table view	On the **Assets** page, you can switch among the predefined table views: • **Security** (default view) • **Network** • **Inventory** The system saves your most recently selected view and restores it when you reopen the **Assets** page in a new session. Several new columns have been added to the asset table view to display additional asset properties, such as Asset Group, OS, Firmware, Model, Behaviors, and Services. Use the table **Settings** menu to show or hide columns as needed.

Asset summary

Explains how asset summaries bring security information together so you can identify areas for further investigation.

An asset summary provides a quick view of the security information available for the asset.

The **Summary** tab includes asset metadata, and the available summary cards provide high-level information about an asset before you open a related details tab. The Summary tab includes these cards:

- **Alerts**
- **Vulnerabilities**
- **Behaviors**
- **Services**
- **Communications**
- **Rack Slot**

Information in asset summary cards

This table depicts the available cards on the **Summary** page. The cards and values that appear depend on the asset data and the features available in your deployment.

Table 12: Information in asset summary cards

Card	Information shown
Alerts	The card shows the number of active alerts. The card's visual indicator reflects the highest criticality among those alerts.
Vulnerabilities	Vulnerability information such as the total count and indicators for confirmed vulnerabilities, known exploits, a network attack vector, or the highest Common Vulnerability Scoring System (CVSS) value.

Card	Information shown
Behaviors	The card shows the number of unique behaviors observed for the asset, along with tags for the most recently observed behaviors.
Services	The service count shown for the asset.
Communications	The card shows the number of internal and external peers that communicate with the asset, when available.
Rack Slot	Available only for modular PLCs (Programmable Logic Controllers) assets. The card provides a quick inventory view of the PLC's installed modules details such as the model name, slot type, firmware version, and serial number.

View asset summary

View an asset's Summary tab to quickly assess asset metadata and high-level status cards.

Use the **Summary** tab of an asset to view essential metadata and summary cards, such as alerts, vulnerabilities, behaviors, Services, and communications. This allows you to identify the asset's status and select summary cards for more detailed analysis.

Follow these steps to view the asset's Summary page.

Procedure

1. From the main menu, select **Assets**.

   The **Assets** page lists all available assets.

2. Select an asset to open its details.

   The **Summary** tab opens by default.

3. Review the asset metadata and summary cards to assess its overall status.
4. Select a summary card, such as **Alerts**, **Vulnerabilities**, **Behaviors**, **Services**, or **Communications** to view related details.

View asset alerts

Provides instructions for reviewing alert counts, filtering and sorting the alert table, and opening related alert details for an asset.

Assets may generate multiple types of alerts. Reviewing and organizing these alerts helps users identify current issues and prioritize investigation.

The **Alerts** card depicts the total count of active alerts on the asset. The card also provide count of each alert category and the last alert detected data.

Use the asset's **Alerts** tab to review all alerts associated with an asset without opening alert instances individually.

Follow these steps to view alerts for an asset.

Procedure

1. From the main menu, select **Assets**.
2. Select an asset to open its details page.

   The **Summary** tab displays asset metadata and summary cards. The **Alert** card shows the total number of active alerts and the alert counts by category.

3. On the **Alerts** card, select an alert category, such as Communication, Intrusion Detection, Property, or Vulnerability.

   The **Alerts** tab opens and displays alerts associated with the selected asset.

   > **Note**
   >
   > In the alert table, the **Alert Type** column identifies the type of alert. The **Context** column identifies the related entity for the alert. Refer the context-related values in Alert triggers and instances in assets on page 46.

4. On the **Alerts** tab, perform any of the following actions:
   a) Review alert count widgets by **Category** or **Severity**. Category is selected by default.
      - **Category** - Communication, Intrusion Detection, Property, and Vulnerability
      - **Severity** - Critical, High, Medium, and Low

   b) Select a widget to filter the alert table by that category or severity.
   c) Sort the alert table by selecting a column header: **Alert Category**, **Alert Type**, **Severity**, or **Last detected**.
   d) Click **Details** for an alert to view additional information about that alert instance.

      The **Alerts** page opens with the alert details. If the asset is an alert instance, the page is filtered by the asset name. If the asset triggered the alert, the page displays additional information about the alert instance. For additional details, refer to Alert triggers and instances in assets on page 46.

Alert triggers and instances in assets

Explains how alert triggers and instances relate to a selected asset and why the destination that opens for an alert can vary by alert type.

An alert trigger is the condition that causes an alert. An alert instance represents an affected entity; depending on the alert type, it is usually an asset but can be another entity.

An alert can have one trigger and multiple instances. Grouping related instances under a trigger reduces the number of alert entries that you need to review.

- Depending on the alert type, the selected asset can be an alert instance or the alert trigger.
- On the **Alerts** tab of an asset, the **Context** column identifies the other entity: the trigger when the selected asset is an instance, or the instance when the selected asset is the trigger.
- The **Details** button on the **Alerts** page opens the related alert instance page. When the selected asset is an instance, the page can open with the asset filter applied; when it is the trigger, the page can open without an asset filter.

Note

The **Details** button is available only when you have the appropriate permission.

Table 13: Alert instance page destination by alert type

Alert type	Context value	Alert instance page destination
Severe vulnerabilities in monitored entities	CVE ID and CVE title	Opens the alert instance page filtered by the asset.
Prohibited vendors	Vendor name	Opens the alert instance page filtered by the asset.
Assets with unexpected external communications	Number of remote domains or addresses	Opens the alert instance page without an asset filter.
Inactive assets	Alert rule name	Opens the alert instance page filtered by the asset.
Intrusion detection	Snort rule ID and Snort rule	Opens the alert instance page filtered by the source asset.
Network Scanner	Number of scan events	Opens the alert instance page without an asset filter.
Assets with unexpected behavior	Asset name	Opens the alert instance page.

View asset vulnerabilities

View the vulnerability list for a selected asset and apply filters based on CVSS score to focus your review on priority findings.

Review vulnerabilities associated with a chosen asset in Cisco Cyber Vision to help prioritize remediation efforts.

Cisco Cyber Vision uses an internal knowledge database to match asset properties with recognized vulnerabilities, icons, and threats. For additional details on vulnerabilities, refer to the Vulnerabilities on page 77 section.

Before you begin

Ensure you have access to the Assets and Vulnerabilities dashboards in Cyber Vision Center. You may need to check your permissions under **Configuration** > **Users** > **Role Management**.

Follow these steps to view asset vulnerabilities details.

Procedure

1. From the main menu, select **Assets**.

   The **Assets** page lists all available assets.

2. Select the asset that you want to review.

The **Summary** tab opens and displays asset details and summary cards. The **Vulnerabilities** card shows confirmed and potential vulnerability counts, the highest CVSS score, network attack vector count, and known-exploit count.

3. Click the **Vulnerabilities** card.

   The **Vulnerabilities** tab opens and displays the vulnerabilities identified for the selected asset.

4. On the **Vulnerabilities** tab, perform any of the following actions as needed:
   a) Select **Cisco Security Risk Score** or **CVSS Score**, and then select a widget to apply its associated score filter to the vulnerability table.
   b) Sort the table by columns such as Alert, Vulnerability ID, Name, Risk Score, or Status.
   c) Optionally, enable **Show Acknowledged** to include acknowledged vulnerabilities.
   d) If required, **Acknowledge** or **Unacknowledge** vulnerabilities. For detailed steps, refer to the following topics:

      Acknowledge or unacknowledge vulnerabilities for a single asset on page 80

      Acknowledge or unacknowledge multiple assets for a single vulnerability on page 81

   e) Click **Export** to download the vulnerability list as a CSV file.

The vulnerability list for the selected asset is displayed. Applied filters help you identify and prioritize critical vulnerabilities.

View asset communications

Provides instructions for opening an asset communications map and using its filters and grouping options to investigate the traffic observed for the asset.

Use the **Communication** card to investigate communication patterns for a selected asset.

Use the Communications tab to examine internal and external interactions of the asset, and review communication details for monitoring or auditing purposes. For additional information on **Communication** tab, refer to Communication maps on page 82.

Follow these steps to view asset communications.

Procedure

---

1. From the main menu, select **Assets**.

   The **Assets** page lists all assets.

2. Select the asset you want to view.

   The **Summary** tab opens and displays asset metadata and summary cards. The **Communications** card shows the number of internal assets, network interfaces, external resources, ASN organization information for external communications, and last unicast days.

   > **Note**
   >
   > Investigate any external communication count greater than zero.

3. Click the **Communications** card to open the **Communication** tab.
4. On the **Communications** tab, perform the following actions as needed.
   a) Use the **Map** or **List** view to review internal and external communication patterns.

b) Apply filters, such as time, protocol, communication type, or focus filters (Asset, Network, or Country), to narrow the results.
c) Use search to find and investigate specific remote assets.
d) If external communications exist, use the **ASN Info** toggle in the **Map** view to review details about the external traffic.

The communications map displays the selected asset's network interactions based on the filters you apply.

Asset communication map features

This section lists the features of the asset communication map and their descriptions, including details about icon indicators.

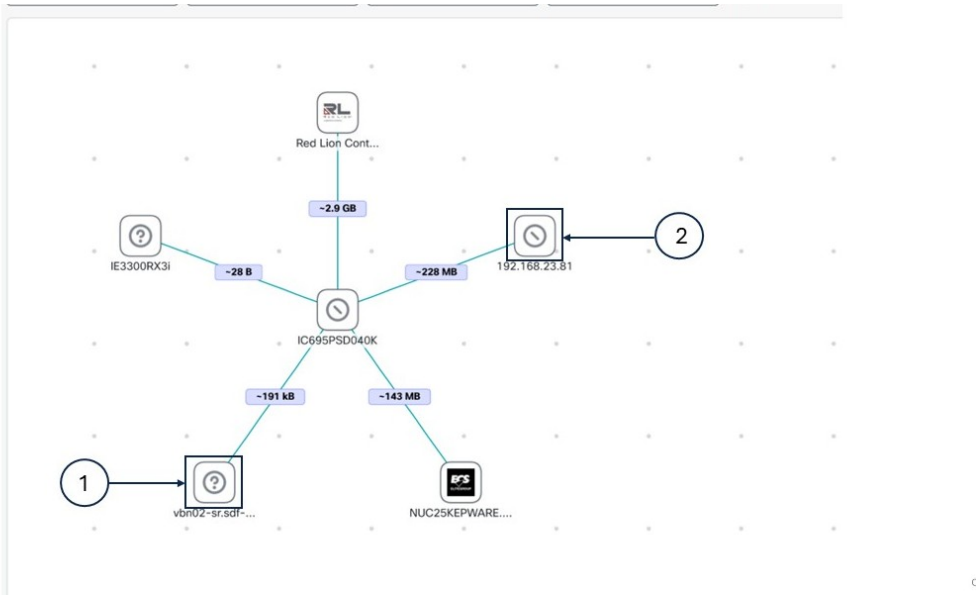
The asset communication map shows all communications between a selected asset and other individual assets in your environment. It provides a detailed view of communication patterns, offers several useful filters, and supports multiple identification methods to help you analyze network communications easily.

Table 14: Features of the asset communication map

Feature	Description
Search	Lets you search for assets within the current map and view their communication details.
Time filter	• Lets you focus on communications for specific time periods to analyze trends or activity. • The **Last 7 days** filter is enabled by default.
Group communications	• Lets you group assets by **Asset** , **Network**, or **Country** to organize the map. • Group nodes show communications between assets from the same group. Individual links show details of communication between groups: observed protocols, data exchange volumes, and information about the asset source or destination. • If an asset communicates with another asset you did not include in the active view filter, the map displays the node and links for that asset as a dotted line. • Non-communicating groups appear in grid view on the map.
Communication type	Filters the map by external or internal communications. When parent and sub-domains exist in external communications, click the parent domain node in **Map** view to display communications between sub-domains. Breadcrumbs show your current location.
Protocol filter	• Lists all protocols used between assets. • All protocols appear by default, but **Traffic-Heavy Protocols** are deselected to improve clarity.

Feature	Description
Assets identification	For each asset, the map shows the vendor icon and name. If this information is unavailable, you see the asset's IP address or MAC address.

Figure 1: Icon descriptions



Icon	Description
(1)	This icon indicates that vendor information for the asset is unavailable.
(2)	This icon indicates that the vendor is known, but its icon is unavailable.

View behaviors for an asset

Configure and review the asset behavior timeline on Cisco Cyber Vision.

Use the **Behaviors** card to analyze the distinct behaviors associated with an asset for security and operational insights.

The **Behaviors** card shows a count of distinct observed behaviors and the most recently observed behavior, such as Program Upload, Start CPU, Stop CPU, Read Var, Write Var, Restart CPU, or Network Configuration.

The **Behaviors** tab provides a view of all behaviors observed for the asset. The Behaviors Timeline displays data with daily granularity, showing date-grouped entries with the behavior name, category, description, first or last seen, and related asset when applicable. Each behavior is color coded based on its importance.

Follow these steps to view asset behaviors.

Procedure

1. From the main menu, select **Assets**.

   The **Assets** page displays a list of all assets.

2. Select the asset that you want to review.

   The asset **Summary** tab opens. The **Behavior** card shows the most recently observed behavior and when it occurred.

3. Click the **Behavior** card.

   The **Behaviors** tab opens and displays the asset's observed behaviors, grouped by date, along with a timeline.

   The **Behaviors** tab opens, displaying the list of behaviours observed for the asset grouped by date, and timeline of those behaviors.

   > **Note**
   >
   > If you select a behavior badge on the card, the timeline is filtered to show only that behavior.

4. On the **Behaviors** tab, use the available options as needed:
   a) Review timeline entries, including the behavior name, category, description, first- or last-seen time, and related asset, when applicable.
   b) Select a related asset link to open that asset's **Summary** page.
   c) Use the **Search** field to find a specific behavior.
   d) Select **Daily**, **Weekly** , or **Monthly** to change the timeline granularity.

   > **Note**
   >
   > - Daily data is retained for 31 days.
   > - Weekly data shows up to 31 days in 7-day windows.
   > - Monthly records are retained for 13 months.

   e) Filter behaviors by **Directions**.
   f) Select a behavior from the drop-down list to view its details.

      Behavior entries are color-coded to indicate their importance.

View asset services

Configure Cyber Vision to view the services detected for a selected asset using the Services tab.

In Cisco Cyber Vision, a Service refers to an active program, network infrastructure, or specialized industrial application detected on a monitored asset. Cyber Vision uses Deep Packet Inspection (DPI) to identify and display detailed information about services on each asset.

On the asset's **Summary** page, the **Services** card provides the total count of services. The most recently detected services are listed as badges on the card, such as Windows, HTTP Server, DNS Server, SSH, and engineering software like Ignition or FactoryTalk.

Use the **Services** tab to review the services displayed for a selected asset.

Follow these steps to view asset services.

Procedure

1. From the main menu, select **Assets**.

   The **Assets** page lists all available assets.

2. Select the asset you want to review.

   The **Summary** tab opens. The **Service** card shows the number of detected services and may display recently detected services, such as Windows, HTTP Server, DNS Server, SSH, Ignition, or FactoryTalk.

3. Click the **Service** card.

   The **Service** tab opens and lists the detected generic and port-based services, including when each service was first and last observed.

4. On the **Services** tab, use the available controls as needed:
   a) Use **Search** to find a specific service.
   b) Use the **Protocol** drop-down list to filter services by protocol.
   c) Use the **Service** drop-down list to select services and view their details.

You can now review the services detected for the selected asset.

View asset properties

Provides instructions to verify asset identity and review network-collected properties by protocol.

Use the **Properties** tab to review properties collected from the network for a selected asset. Reviewing asset properties ensures accurate asset identification and helps validate the information collected from the network.

Cisco Cyber Vision organizes the asset properties by protocol in the **Properties** tab.

Follow these steps to view asset properties.

Procedure

1. From the main menu, select **Assets**.

   The **Assets** page lists all available assets.

2. Select the asset you want to review.

   The **Summary** tab opens and displays asset metadata and summary information.

3. Click the **Properties** tab.
4. Review the property groups and the properties listed for each protocol.

View asset interfaces

Provides instructions for reviewing the interface values that Cisco Cyber Vision uses to identify the asset.

Use the **Interfaces** tab to review the interfaces that Cisco Cyber Vision identifies for a selected asset.

Assets use different network interfaces to communicate within the network. Interfaces may include MAC addresses, IP addresses, VLAN IDs, or combinations of these. The system collects interface properties from network traffic. It selects one interface as the primary interface for visualizations.

The **Interfaces** tab shows all interfaces for the asset, including the primary and additional interfaces. If multiple interfaces are available, you can change which interface is designated as the primary interface.

Follow these steps to view asset interfaces.

Procedure

1. From the main menu, select **Assets**.

   The **Assets** page lists all available assets.

2. Select the asset you want to review.

   The **Summary** tab opens and shows the asset metadata in the left pane.

3. In the left pane, review the **Primary Interface** details.
4. To view every interface detected for the asset, select the **View all < > interfaces** link under **Primary Interface** .

   The **Interface** tab opens and lists the primary and additional interfaces.

5. To designate a different primary interface, locate the **Primary Interface** column and select the interface you want to use.

Add custom properties to an asset

Configure custom properties to enrich metadata for individual assets, enabling improved emergency and maintenance communications.

Custom properties feature allows you to add any custom property without content limitation on assets apart from current asset information.

Add custom properties such as:

- owner name,
- email, or
- contact number

to individual assets for enhanced metadata management and operational efficiency.

Asset-level custom properties allow you to include information that is not inherited from the network, giving you granular control over asset metadata.

You cannot edit custom properties that you set for a network from the assets. Setting the custom property value at the network level overrides the value set at the asset level.

Before you begin

- Ensure you have the **Assets** permission with read/write access.

Procedure

1. From the main menu, click **Assets**.
2. Click the asset that you want to add custom properites to.
3. On **Custom Properties**, click **Add/Edit**.
4. Enter a custom key and its corresponding value.

Example
To add an owner name for an asset, set the key to "Owner" and the value to the owner's name.

To add multiple custom properties, repeat this step for each key-value pair.

5. Click **Save**.

External communications in the New UI

This section provides the criteria used to classify network communication as external in the New UI.

The system classifies and displays external communications in the New UI using specific criteria.

Criteria for classifying external communications

External communication appears in the New UI when:

- The communication is to or from networks that are explicitly marked as **External** in the New UI.
- If no external networks are defined (in the New UI under **Configuration** > **Network Definition**), any communication not assigned to an **IT Internal** or **OT Internal** network counts as external communication.

View external communications for an asset

Verify and review all external communications associated with a specific asset.

Enable you to identify and analyze all external connections for a chosen asset.

Use this task to determine which external resources a specific asset interacts with, and to analyze communication details for monitoring or auditing.

Procedure

1. From the main menu, select **Assets**.
2. Click your asset that has external communications.
3. Open the **Communications** tab for the selected asset..
4. In the **All Communications** filter, select **External** to display only external communications in either map or list view.

All external communications associated with the selected asset are displayed, including details about each connection.

Filters and map indicators for monitoring external communications

Lists the available filters and visual indicators used to monitor external communication, helping you identify network exposure and interpret the map display.

Visualization and monitoring

When you visualize external communications, you can identify unexpected network paths that might expose your organization to external threats. Available filters for external connections include:

- **Country**: Displays the country identified for the IP.
- **ASN**: Displays unique ID assigned to a network or a group of networks managed by a single organization.
- **ASN Organization**: Displays the origin organization that initiated the external communication.

Note

- Country, ASN, and ASN Organization details are available only if your local center is enrolled in Cyber Vision Site Manager (CVSM) and an active cloud connection with Cisco exists.
- In asset communications:
  - **List view**: The ASN and ASN Organization columns are disabled by default.
  - **Map view**: If external communications are available, the **ASN Info** field appears. It shows details for external communications (disabled by default).

Table 15: External communication indicators in map view

Visual indicators	Description
Single circle outside the node	Indicates one remote address communicating with your asset.
Multiple circles outside the node	Indicates that multiple remote addresses communicate with your asset.
Globe icon on the node	Indicates that IP to country mapping is unavailable or multiple countries are involved.
Node displays country's flag	Indicates that a single country has been identified.
Question mark icon in the node	Indicates an IP address without country mapping. The country column in list view shows **Unknown**. Some IPs cannot be resolved to a country based on available data feeds.

Filters

Introduces filters in Cyber Vision, explaining how they narrow displayed information, enable users to focus on specific assets, network segments, or alerts, and describes filter options by organization hierarchy, sensor, network, and other criteria across non-configuration pages.

A filter is a New UI feature that

- narrows the information displayed on core Cyber Vision pages,
- allows users to focus on specific assets, network segments, or alerts, and
- leaves configuration actions unaffected.

Table 16: Feature History Table

Feature	Release Information	Feature Description
Filter Cyber Vision Center data by organization hierarchy	Release 5.3.x	All the data views in New UI can be filtered by organization hierarchy, sensors, or networks associated with an asset. At the top of the left menu, in the **Organization** filter, choose the hierarchy level you want to focus on. **Global** is the default choice and covers all assets.
Filter data in Cyber Vision Center by active view filter	Release 5.3.x	A product-level banner in the New UI allows you to filter data on every page except configuration pages. If you have not applied any filters, **No filter applied** is displayed. Click **Edit** to apply one or more filters from functional group, network or sensor, asset type, and vendor categories.

Filter views in Cyber Vision New UI

Refines the information displayed in Cyber Vision by applying filters to the Dashboard, Alerts, Assets, Vulnerabilities, and Communications pages. This action helps focus on specific assets, network segments, or alerts.

Narrow the information displayed in Cyber Vision New UI by applying filters to the Dashboard, Alerts, Assets, Vulnerabilities, and Communications pages.

Use filters to focus on specific assets, network segments, or alerts in Cyber Vision. This action does not affect Configuration pages.

Procedure

1. From the main menu, choose **Organization** .
2. Select either **Sensors** or **Networks** .

> **Note**
>
> The **Sensors** tab is selected by default.

- To select all sensors or networks at a hierarchy level, select that level.
- To choose specific sensors or networks from a selected hierarchy level: open the organization drawer again, open **Sensor selection** or **Network selection** , select items, then click **Apply** .

> **Note**
>
> To select assets not linked to sensors or networks, choose **Unknown** .

- Use the search box to find sensors or networks by name.

3. To clear your selected sensors or networks and return to the complete organization hierarchy, open the **Organization Hierarchy** drawer again and click the **Reset selection** icon.
4. To edit the sensor or network selection for the selected organization hierarchy only, open the **Organization Hierarchy** drawer again and click the **Edit selection** icon.
5. To refine your filter, click **Edit** on the active view bar.
6. Use the **Select** buttons to add filters as needed.
7. Click **Apply** to update or **Reset** to clear the filters.

The views show only data that matches your filter criteria.

What to do next

Review the filtered data on Dashboard, Alerts, Assets, Vulnerabilities, or Communications pages.

4 Configure visibility

Topics:

- Alerts
- Syslog notification details for alert types
- Vulnerabilities
- Communication maps
- Enable IDS on a sensor

Guides the configuration of visibility features, including managing alert rules and types, enabling syslog notifications, organizing asset clusters, addressing vulnerabilities, mapping communications, and activating IDS on sensors to optimize security monitoring and incident response across the network.

Alerts

Explains how alerts notify users about significant activity or irregularities in an industrial network, categorize data, and provide warnings to aid security monitoring.

Alerts are system-generated notifications that

- indicate significant activity or irregularities detected within an industrial network,
- categorize information based on type, associated data, and network components, and
- provide warnings to help with security monitoring and response.

An alert is a notification that triggers when a user-defined rule's condition is met. Cyber Vision sends alerts through Syslog when they are raised, cleared, or their status changes. For details about this configuration, see Enable or disable syslog notifications for an alert type.

Table 17: Feature History Table

Feature	Release Information	Feature Description
Pause and resume individual alert rules	Release 5.6.x	You can pause or resume individual alert rules. Pausing a rule does not affect other rules associated with the same alert type. Alert type-level pause and resume are no longer available.
MITRE ATT and CK information for Intrusion Detection alerts	Release 5.6.x	Intrusion Detection alerts display the MITRE ATT and CK tactics and techniques associated with the Snort rule that generated the alert.
Assets with unexpected behaviors alert type	Release 5.6.x	Cisco Cyber Vision monitors the assets that are part of the alert rules, and raises an alert when any of those assets are involved in selected behaviors within the configured time window.
Alert rule configuration changes	Release 5.6.x	You can no longer configure alert rules for functional groups. When you upgrade to Release 5.6.x, Cyber Vision automatically deletes existing alert rules configured for functional groups.
Network Scanner alert type	Release 5.6.x	The Network Scanner alert type identifies network reconnaissance and scanning attempts. IP addresses specified in the Allowed Scanner list are excluded and do not generate alerts.
Inactive assets alert type	Release 5.5.x	Inactive assets alert type detects assets that stop communicating due to failure or misconfiguration. Define custom rules for the inactivity period to reduce manual monitoring.

Feature	Release Information	Feature Description
Intrusion detection alert type	Release 5.5.x	Intrusion detection alert type monitors network traffic using the Snort intrusion detection system. It raises an alert when suspicious or malicious network activity is detected on monitored assets, based on Snort rules.
Assets with unexpected external communications alert type	Release 5.5.x	Assets with unexpected external communications alert type monitors asset communications. It raises an alert if an asset communicates to external IP addresses or domains.
Network-based organization hierarchy alert configuration	Release 5.4.x	You can configure alerts at the organization hierarchy level with one additional entity type: **Organization Hierarchy (Networks)**. The system changes all existing alert rules with the entity type **Organization Hierarchy** to **Organization Hierarchy (Sensors)** automatically.
Mute or unmute alert instances for prohibited vendor alert type	Release 5.4.x	You can use the mute and unmute feature to control prohibited vendor alerts. Mark alert instances as reviewed and not urgent so they remain in the system but are not active. Select the duration to mute an alert instance; after that period, the alert becomes active again.
Active and cleared alerts	Release 5.3.x	The Alerts page displays two types of alerts: • Active • Cleared
Pause alert creations	Release 5.3.x	You can pause an alert type in the **Configure** > **Alerts**
Change vulnerability scoring system for alerts	Release 5.3.x	The Cisco Security Risk Score is the default scoring system applied to alert configurations. However, you can choose to update an alert configuration to apply the CVSS scoring system instead.
Alert for severe vulnerabilities in monitored entities	Release 5.3.x	Create and edit rules for the **Severe vulnerabilities in monitored entities** alert based on the Cisco Security Risk Score or the CVSS score.

Feature	Release Information	Feature Description
Alert for prohibited vendors	Release 5.3.x	The **Configure** > **Alerts** page contains a default alert for prohibited vendors. The alert rule is based on an editable list of prohibited vendors.

Alert types

Lists the main alert types monitored by Cyber Vision and provides descriptions and associated rule information for each.

Cyber Vision provides alert types that monitor security conditions and activity across your assets and network. Each alert type contains rules that define what Cyber Vision monitors and when it generates alerts. To view and configure alert types and rules, choose **Configuration** > **Alerts**.

Alert type	Description
Severe vulnerabilities in monitored entities	• Cyber Vision Center raises alerts when it detects high-severity vulnerabilities in your assets. • The default rule for this alert type is **Default_OH_Global**. • To clear alerts for this alert type, acknowledge the vulnerabilities on the affected assets. To restore the alerts, unacknowledge the vulnerabilities. For more information, see Acknowledge or unacknowledge vulnerabilities for a single asset and Acknowledge or unacknowledge multiple assets for a single vulnerability.
Prohibited vendors	• Cyber Vision triggers alerts when your assets are linked to prohibited vendors. • The default rule for this alert type is **Prohibited_list**.
Inactive assets	• Cyber Vision automatically detects assets that have stopped communicating due to failure or misconfiguration. It then alerts you about the issue. • Define rules to set the inactivity threshold for triggering alerts, reducing manual monitoring.
Intrusion Detection	• This alert type monitors network traffic using the Snort intrusion detection system. Enable Intrusion Detection System (IDS) on a compatible sensor to activate Snort-based intrusion detection. See Enable IDS on a sensor. • The default rule for this alert type is **Default_Snort_Global**. • Detects suspicious network activity identified by Snort rules. When mapping information is available, the alert displays the associated MITRE ATT and CK tactics and techniques.

Alert type	Description
Assets with unexpected external communications	• This alert type raises an alert if assets communicate with external IP addresses. • The default rule for this alert type is **Default_Monitored_Asset_Types**, which monitors external communications for all assets with type PLC, IED, or IO.

Network Scanner	• Cisco Cyber Vision triggers alert when it detects network reconnaissance and scanning activity such as:
	  • Vertical scan - One source IP scans multiple ports on a single target host.
	  • Horizontal scan - One source IP scans a single port across multiple hosts.
	  • Combined scan - Combination of vertical and horizontal scanning, where multiple ports on multiple hosts are scanned.
	  • Industrial scan - Scan targets industrial protocol traffic and anomaly detection specific to operational technology (OT) environments.
	  • Burst scan - Large number of scan attempts in a very short period.
	  • Targeted scan - Focused reconnaissance against specific high-value assets.
	• The default rule for this alert type is **Default_Scan_Global**.

Assets with unexpected behaviors	Cisco Cyber Vision triggers an alert when an asset that is part of the alert rule is involved in one of the selected behaviors, in the configured role, within the configured time window.

Alert states and key attributes

Lists the states, alert types, rules, and key attributes used for alerts in the Cyber Vision center. This reference also provides information to help users understand alert progression and categorization.

Cyber Vision manages alerts by tracking their progression through defined states. Alerts are organized by type, and rules specify when and how alerts are triggered.

How Cyber Vision organizes alerts

Cyber Vision organizes alerts by alert type, rule, trigger, instance, and occurrence. An alert rule defines the monitored condition. A trigger identifies the condition that generated the alert. An instance identifies an affected entity or activity. An occurrence records each time Cyber Vision detects that condition for the instance.

Alert states

You can monitor alerts as they move through distinct states:

- **Active**: Displays current unresolved alerts. Alerts stay active while the underlying problem exists.
- **Muted**: When you mute alert instances related to the **Prohibited vendors**, **Inactive assets**, **Intrusion Detection**, **Assets with unexpected behaviors**, and **Assets with unexpected external communications** alert types, those alerts appear in the **Muted** tab.
- **Cleared**: After you resolve alerts, they appear in the **Cleared** tab. Cyber Vision keeps cleared alerts for a set number of days before removing them. The retention period is different for each type of alert. You can manually clear alert instances only for the **Inactive assets**, **Network Scanner**, **Assets with unexpected behaviors**, and **Assets with unexpected external communications** alert types.

Alert details

To view the alert details, from the main menu choose **Alerts**.

Name	Description
Alert Type	Specifies the category of alert generated by the system. Each type shows the nature of the underlying issue detected.
Trigger	Identifies the condition or detected object that caused the alert rule to generate an alert. The displayed information depends on the alert type.
Instances	Identifies an entity or activity affected by the trigger. One trigger can have multiple instances.
Occurrence	Records each time Cyber Vision detects the alert condition for an instance.
Severity	Severity levels include Critical, High, Medium, and Low. Use these levels to prioritize your response.
Triggered By	The alert category triggers the alert.
Last Detected	Shows the date and time when the alert was last triggered.

Note

- The **Alerts** dashboard for the **Assets with unexpected external communications** alert type is relevant for last month only.
- The trigger, instance, and occurrence information displayed in the Alerts page depends on the alert type.

Alert information by alert type

Alert type	Trigger	Instance	Occurrence
Severe vulnerabilities in monitored entities	A vulnerability that meets the configured scoring threshold	An asset affected by the vulnerability	A detection of the vulnerability on the asset

Alert type	Trigger	Instance	Occurrence
Prohibited vendors	A vendor included in the prohibited-vendor list	An asset associated with the prohibited vendor	A detection of the prohibited vendor on the asset
Network Scanner	Network reconnaissance or scanning activity from an asset or IP address that is not on the Allowed scanners list.	A target asset scanned by that source IP address.	A detection of scanner activity on the target asset, including the scanned ports.
Assets with unexpected behaviors	A behavior detected on a monitored asset.	A monitored asset that participates in the behavior in the role specified by the alert rule: Initiator, Target, or Both.	Each detection of the selected behavior involving that monitored asset during the rule's configured time window.
Inactive assets	An alert rule whose configured inactivity threshold is met.	An asset that has stopped communicating.	A detection that the asset has remained inactive for the configured duration.
Intrusion Detection	A Snort rule that detects suspicious or malicious network activity.	A source asset involved in traffic that matches the Snort rule.	Each detection of the Snort rule involving the source asset.
Assets with unexpected external communications	A monitored asset that communicates with an external address or domain.	An external IP address or domain contacted by the monitored asset.	Each detected communication between the monitored asset and the external address or domain.

MITRE ATT and CK information for Intrusion Detection alerts

Describes the MITRE ATT and CK tactics and techniques displayed for Snort-generated Intrusion Detection alerts.

Use the MITRE ATT and CK information in an Intrusion Detection alert to understand the objective and method of the activity detected by a Snort rule.

MITRE ATT and CK mapping

Cyber Vision maps the Snort rule that generates an **Intrusion Detection** alert to the corresponding MITRE ATT and CK tactics and techniques.

A Snort rule uses a GID:SID pair to identify the generator and signature that detected the activity. When a MITRE ATT and CK mapping exists for the GID:SID pair, Cyber Vision displays the mapped information in the alert preview and summary.

Cyber Vision displays the MITRE ATT and CK information in the following locations:

- The expanded alert preview displays the associated MITRE ATT and CK tactics.
- The alert **Summary** tab displays the GID:SID pair and the associated MITRE ATT and CK tactics and techniques.
- A tooltip displays the technique name when you hover over a MITRE ATT and CK technique ID.

> **Note**
>
> A Snort rule can map to one or more MITRE ATT and CK tactics. Each tactic can include one or more techniques.

MITRE ATT and CK alert details

From the main menu, choose **Alerts**, expand an **Intrusion Detection** alert, and click **View alert summary**.

Table 18: MITRE ATT and CK information

Field	Description
GID:SID	Identifies the Snort generator and signature that generated the alert.
MITRE ATT and CK Tactic	Identifies the objective that the detected activity attempts to achieve.
MITRE ATT and CK Technique	Identifies how the detected activity attempts to achieve the objective. Hover over a technique ID to view the technique name.

Supported actions for alert rules

Outlines the management actions supported for each Cyber Vision alert rule type, detailing permitted operations such as creating, editing, duplicating, deleting, pausing, or resuming rules according to alert type.

Identify the management actions that Cyber Vision supports for each alert rule type.

Alert type	Permitted alert rule actions
Severe vulnerabilities in monitored entities	Create, edit, duplicate, delete, pause, or resume alert rules.
Prohibited vendors	Edit, pause, or resume the alert rule.
Inactive assets	Create, edit, delete, pause, or resume alert rules.
Assets with unexpected external communications	Create, edit, duplicate, delete, pause, or resume alert rules.
Intrusion Detection	Pause or resume the default alert rule. You cannot create, edit, duplicate, or delete the default alert rule.
Network Scanner	Edit, pause, or resume the alert rule.
Assets with unexpected behaviors	Create, edit, duplicate, delete, pause, or resume alert rules.

Pause or resume individual alert rules

Explains how to pause or resume individual alert rules to manage alerting behavior effectively.

Starting from Cisco Cyber Vision Release 5.6.x, you can pause or resume individual alert rules.

Pausing an alert rule temporarily stops that rule from generating new alerts. Other rules associated with the same alert type remain active.

Here are few things for you to consider before pausing or resuming individual alert rules.

- Resuming a paused alert rule allows it to generate new alerts again.
- Pause and resume actions are no longer available at the alert-type level.

  Migration note: When you upgrade from Release 5.5.x to Release 5.6.x, Cyber Vision sets every rule associated with a paused alert type to **Paused**. After the upgrade, resume individual rules as needed.

Pause or resume individual alert rules

Pause or resume one or more individual alert rules and control whether they generate new alerts.

Pause one or more alert rules to temporarily stop them from generating new alerts, or resume paused rules to restart alert generation.

Pausing an alert rule affects only the selected rule. Other rules associated with the same alert type remain active. Pausing a rule does not change existing alerts.

Before you begin

- Ensure that your user role allows you to manage alert rules.
- Identify the alert type and rules that you want to pause or resume.

Procedure

1. From the Cisco Cyber Vision main menu, choose **Configuration** > **Alerts**.
2. Select an alert type.
3. Select the check boxes for one or more alert rules that you want to pause or resume.
4. Click **Pause** or **Resume**.
5. Confirm the action if prompted.

When you pause the selected alert rules, Cyber Vision stops generating new alerts for those rules. Existing alerts remain unchanged. Other rules associated with the same alert type remain active.

When you resume the selected alert rules, Cyber Vision allows them to generate new alerts again.

The status of each selected rule changes to **Paused** or **Active**.

Create alert rules for severe vulnerabilities in monitored entities

Configure alert rules to monitor asset vulnerabilities and receive timely notifications about severe threats.

Enable proactive vulnerability monitoring by creating alert rules that trigger notifications for severe vulnerabilities within monitored assets.

Starting with Release 5.6.x, you cannot configure alert rules for functional groups. When you upgrade to Release 5.6.x, Cyber Vision automatically deletes existing alert rules configured for functional groups.

Create alert rules under the **Severe vulnerabilities in monitored entities** alert type to automatically notify you when assets meet specific vulnerability criteria. This helps ensure timely response to critical security threats.

Procedure

1. From the main menu, choose **Configuration** > **Alerts**.
2. Select the **Severe vulnerabilities in monitored entities** alert type.
3. Click **Create new rule**.
4. Enter an **Alert Rule Name**, select the **Severity** and **Entity type**.

Entity types:

- **Organization Hierarchy (Sensors)**: Triggers alerts for assets linked to sensors assigned to the selected organization hierarchy levels.
- **Organization Hierarchy (Networks)**: Triggers alerts for assets linked to networks assigned to the selected organization hierarchy levels.

5. On the **Entity selection** page, select the organization hierarchy levels.
   - If you select assets based on organization hierarchy (Networks), check **Assets seen in Unknown networks** to include unidentified or unmapped assets.
   - If you select assets based on organization hierarchy (Sensors), check **Assets seen by Unknown data sources** to include unidentified or unmapped assets.

   Note

   The available **Entity selection** options depend on the **Entity type** you select in the **Rule name and entity type** step.

6. In the **Scoring system and threshold** tab, select one scoring system:
   - For **Cisco Security Risk Score**, enter a threshold number between 34 and 100.
   - For **CVSS**, enter a threshold number between 7 and 10.

   Note

   Cisco Security Risk Score is the default, but you can select **CVSS**.

7. Review your selections in the **Summary** and click **Save**.

The new alert rule appears on the **Configuration** > **Alerts** > **Severe vulnerabilities in monitored entities** page. You receive alerts when asset vulnerabilities match the new rule.

What to do next

- Regularly review the **Configuration** > **Alerts** page to manage and update alert rules as needed.
- To manage alert rules, navigate to **Configuration** > **Alerts**, select an alert type, and choose to edit, duplicate, or delete actions.

Create an alert rule for inactive assets

Configure a rule to trigger alerts when assets become inactive for a specified period.

You receive timely notifications and can take action when assets have not communicated for a set timeframe.

You can monitor asset activity and automatically generate alerts when assets are inactive for longer than a set threshold.

Before you begin

Identify the assets you want to monitor.

Procedure

1. From the main menu, choose **Configuration** > **Alerts**.
2. Select the **Inactive assets** alert type.
3. Click **Create new rule**.
4. Specify the **Alert Rule Name**, **Severity**, and the timeframe for inactivity (**Since inactive**).

   > **Note**
   >
   > You will receive an alert if an asset does not communicate within the selected period.

5. Select the assets you want to monitor.
6. View the summary and click **Save**.

When an asset is inactive for the specified period, the system triggers an alert. The **Alerts** page displays a summary of the alert and its instances.

Create an alert rule for external communications

Configure a rule to generate alerts for assets when unexpected external communications are detected.

You can establish an alert rule that enables the detection and notification of any monitored asset communicating externally, ensuring timely identification and response to potential security risks.

When an asset communicates with external IP addresses or domains, the alert rule triggers a notification in the **Alerts** dashboard. This allows you to manage asset security proactively.

Procedure

1. From the main menu, choose **Configuration** > **Alerts**.
2. Select the **Assets with unexpected external communications** alert type.
3. Click **Create new rule**.
4. Enter an **Alert Rule Name** and select **Severity** and **Entity type**.

   Entity types include:

   - **Organization Hierarchy (Sensors)**: Triggers alerts for assets linked to sensors assigned to the selected organization hierarchy levels.
   - **Organization Hierarchy (Networks)**: Triggers alerts for assets linked to networks assigned to the selected organization hierarchy levels.
   - **Asset Types**: Triggers alerts for assets linked to the selected asset types.

5. Select the relevant organization hierarchy levels or asset types in the **Entity selection** page.

   To include unidentified or unmapped assets:

- Select **Assets seen by Unknown data sources** for the **Organization Hierarchy (Sensors)** entity type.
- Select **Assets seen in Unknown networks** for the **Organization Hierarchy (Networks)** entity type.

> **Note**
>
> The available **Entity selection** options depend on the **Entity type** you select in the **Rule name and entity type** step.

6. Review your selections in the **Summary** and click **Save**.

The new alert rule appears under **Configuration** > **Alerts** > **Assets with unexpected external communications** alert type.

What to do next

- Regularly review the **Configuration** > **Alerts** page to manage and update alert rules as needed.
- Navigate to **Configuration** > **Alerts**, select the alert type, and choose the appropriate action to edit, duplicate, or delete alert rules.

Configure allowed scanner IP addresses for the Network Scanner alert rule

Guides you through adding allowed scanner IP addresses to Default_Scan_Global. Port scans from addresses on the allowed scanner list are exempt from detection and do not trigger alerts.

Use this task to manage allowed scanner IP addresses for **Default_Scan_Global**, the default **Network Scanner** alert rule.

Adding IP addresses under Allowed scanners exempts them from detection and alert generation. Port scans from IPs not included as Allowed scanners will trigger a new alert instance.

Follow these steps to configure allowed scanner IP addresses for Network Scanner alert rules:

Procedure

---

1. From the main menu, choose **Configuration** > **Alerts**.
2. On **Alerts**, select **Network Scanner**.
3. In **Alert Rules**, select **Default_Scan_Global** and then select the **Edit** under **Actions**.
4. On **Rule name and severity**, keep the default values and click **Next**.
5. Under **Allowed scanners**, enter an IP address in **Allowed scanner IP**, or search by asset name and select the associated IP address. Then click **Add**.
6. Click **Next** to open **Summary**.
7. Review the **Allowed scanners** count and IP address selection, then click **Save**.

The system updates Default_Scan_Global with the specified allowed scanner IP addresses. Port scans from these addresses are exempt from detection and do not trigger alerts.

What to do next

Next, from the main menu, select **Alerts** and review alerts for Network Scanner alerts generated by scanner activity that is not exempt from detection. Open an alert and review **Summary** to identify the scanner, scanned targets, and scanned ports. View alerts in a table and export them to a CSV file if you need to retain a trace.

Under **Assets**, open the scanner asset for more details, then review the alert from its **Alerts** tab.

Asset behavior alerts

Introduces unexpected asset behavior alerts, the rule criteria that trigger them, and the asset roles that determine how Cyber Vision matches observed behavior.

The **Assets with unexpected behaviors** alert type raises alerts when selected assets participate in a behavior selected in an active rule during its configured time window. Unexpected asset behavior refers to behavior that matches a rule you configured for this alert type.

- A rule specifies the assets to monitor, their required role for behavior, the behaviors to watch, a time window, and an alert severity.

  Note

  The time window can be from 1 to 30 days. The default is 7 days.

- An alert is raised when a matching behavior is observed. If Syslog notification is enabled for the alert type, Cisco Cyber Vision also sends a corresponding event to the configured Syslog server.

Asset roles for behavior

An asset behavior describes a meaningful action inferred from network communications, for example, Program Download, Restart CPU, Read Var, and so on. Every behavior has two roles:

- Initiator (source) – The asset that performs the behavior.
- Target (destination) – The asset on which the behavior is performed.

Note

Some behaviors are role-agnostic. They match only rules configured for both initiator and target roles.

Table 19: Asset roles for behavior alert rules

Rule role	Use it when	Example
Initiator	The configured assets must perform the selected behavior.	Monitor a jump host that initiates an OT command.
Target	The configured assets must receive the selected behavior.	Monitor a PLC that receives a program change.
Both	Either role is meaningful, or you need to include role-agnostic behaviors.	Monitor a critical asset that participates in either role.

Create an alert rule for unexpected asset behaviors

Provides instructions to create a rule that alerts when selected assets participate in selected behaviors during the configured lookback window.

Create a focused alert rule to monitor behaviors that have a clear operational or security purpose.

The alert rule includes steps for specifying identity, scope, entities, time window, and behaviors, and for conducting a final summary review.

Follow these steps to create an alert rule for unexpected asset behaviors.

Procedure

1. From the main menu, choose **Configuration** > **Alerts**.
2. Select **Assets with unexpected behaviors**, then click **Create new rule**.
3. Under **Rule name and entity type** ,
   a) Enter a descriptive **Alert Rule Name**.
   b) Select the **Severity**.

   > **Note**
   >
   > Choose severity based on operational consequence, not protocol alone.

   c) Select one **Entity type**:
      - **Organization Hierarchy (Sensors)**: Triggers alerts for assets linked to sensors assigned to the selected organization hierarchy levels.
      - **Organization Hierarchy (Networks)**: Triggers alerts for assets linked to networks assigned to the selected organization hierarchy levels.
      - **Assets**: Triggers alerts for assets linked to the selected asset types.

   d) Click **Next**.

   The selected severity applies to every instance raised by the rule.
4. Under **Entity selection**,
   a) Select the relevant organization hierarchy levels or asset types.

> **Note**
>
> The available **Entity selection** options depend on the **Entity type** you select in the **Rule name and entity type** step.
>
> - If you select assets based on organization hierarchy (Networks), check **Assets seen in Unknown networks** to include unidentified or unmapped assets.
> - If you select assets based on organization hierarchy (Sensors), check **Assets seen by Unknown data sources** to include unidentified or unmapped assets.
> - If you select Assets, you can filter assets by name, IP address, MAC address, or network. Verify the selection counter before you continue; a filter narrows the visible table but does not remove previously selected assets.

b) Click **Next**.

5. Under **Time window and scope**,
   a) Set the lookback window in **Time window**. The default time window is 7 days. You can set the time window from 1 to 30 days.

   > **Tip**
   >
   > A longer window keeps infrequent behaviors active. A shorter window makes alerts clear sooner after the last observation.

   b) Under **Match configured assets as**, select the asset role:
      - **Target**: The behavior is performed on the selected asset.
      - **Initiator**: The selected asset performs the behavior.
      - **Both initiator and target**: Both initiator and target roles match.

   c) Click **Next**.
6. Under **Behaviors**,
   a) Select one or more behaviors from the catalog. Use search as needed, and switch between **Important behaviors** and **Other behaviors** to review the category and description of each behavior.

   > **Note**
   >
   > Important behaviors are visually emphasized in alerts. Their importance does not override the severity you assign to the rule.

   b) Click **Next**.

7. Under **Summary**, review the rule name, severity, entity type, selected entities, time window, role, and behaviors, then click **Save**.

Evaluation starts automatically. Matching observations already present within the configured time window can produce alerts without waiting for a new packet.

Verify asset behavior alerts instance

Verify unexpected asset behavior alert instances and identify their source, target, behavior, and related rule context

Review active asset behavior alert instances to determine their origins, affected targets, observed behaviors, and associated rule context.

Asset behavior alerts in Cisco Cyber Vision remain active as long as the triggering behavior persists within a matching rule's time window. An alert clears when no running rule matches. This occurs, for example, when observations age out, or when the rule, asset, behavior, or applicable role changes.

- Alerts are grouped by their source asset, even when the configured assets are targets. Each instance identifies the target asset and behavior.
- If several rules match the same source, target, behavior, and orientation, Cisco Cyber Vision displays one instance and lists the applied rules.

Follow these steps to verify asset behavior alerts instance.

Procedure

1. From the main menu, select **Alerts** and click the **Active** tab.

   You can select the **Muted** or **Cleared** tab to review alerts in those states.

2. Locate and expand the Assets with unexpected behaviors alert that you want to review.

   Alert rows are grouped by source asset. This arrangement keeps the potential initiator visible as the alert trigger. Each instance also identifies the exact target and behavior.

3. Click **View alert summary** to view the behavior and the corresponding source or target details.
4. Click the **Instances** tab and review each column:
   - **Source asset** - shows the initiator.
   - **Target asset** - shows the destination.
   - **Behavior** - displays the observed action.
   - **Severity** - indicates the applicable rule severity.
   - **Alert Rules** - lists the number of matching rules.
   - **Last Detected** - shows the most recent observation.

> **Note**
>
> Repeated observations update the existing instance and its last-detected time. They do not create a new row for each occurrence.

5. Under **Alert Rules**, click the count to open the instance drawer and review comprehensive details: behavior, both source and target assets, available type, vendor, addresses, networks, sensors, applied rule, severity, configured role, and time window.

   For a target-oriented rule, the configured asset appears under **Target asset**. The source remains the initiator and is the starting point for review.

You can identify the observed behavior, affected assets, and rule context that produced each alert instance.

Mute alert instances

Mute alert instances to prevent repeated reviews of acknowledged alerts for non-critical issues.

Temporarily suppress non-critical alert instances so you do not need to review known, non-urgent alerts repeatedly.

Mute alerts for **Prohibited vendors**, **Inactive assets**, **Intrusion Detection**, **Assets with unexpected behaviors**,and **Assets with unexpected external communications** alert types. This helps you focus on critical issues. The mute feature marks specific asset alerts as reviewed and not urgent. Muted alert instances remain in the system and are inactive until the mute period ends.

Procedure

---

1. From the main menu, choose **Alerts**.
2. On the **Active** tab, find the relevant alert type and click the alert **Instances** count.
3. Select the alert instances you want to mute.
4. Click **Mute**.
5. Select the mute duration.
   - You can select from three available durations: **Forever**, **For 7 days**, or **For 30 days**.
   - To specify a custom period, select **Custom** and enter a number of days from 1 to 180.

> **Note**
>
> After the selected mute duration (except for **Forever**), alerts become active again.

6. (Optional) Add a comment.
7. Click **Mute** to confirm.

Muted alerts move from the **Active** tab to the **Muted** tab.

What to do next

- To unmute an alert instance, go to **Alerts** > **Muted**, select the alert instance, and click **Unmute**.
- After you unmute, the instance drawer of the active alert shows when it was last muted.

Clear alerts for specific assets

Clear alerts for designated assets to ensure only current, unresolved alerts remain after issues are resolved.

Clear resolved alerts from assets so the alert dashboard reflects current alerts only.

Perform this task when asset-related issues are resolved, but the system still lists alerts for those assets. Clearing alerts helps maintain accurate alert tracking.

Procedure

1. From the main menu, choose **Alerts** > **Active**.
2. Click the instance count for either the **Inactive assets**, **Network Scanner**, **Assets with unexpected behaviors**, or **Assets with unexpected external communications** alert types.
3. Select the asset you want to clear alerts for.
4. Click **Clear**.

After you clear alerts, the system moves the selected alert from the **Active** tab to the **Cleared** tab to show that its alerts are cleared.

Syslog notification details for alert types

Provides a lookup of common and alert-type-specific fields in Cisco Cyber Vision syslog notifications to help you track and investigate alert events.

Cisco Cyber Vision sends syslog notifications to the configured syslog server when an alert is raised, cleared, or its status changes. The notifications include information that helps you track and investigate events.

Cisco Cyber Vision sends alert notifications in Common Event Format (CEF). Each notification contains common alert fields and fields specific to the alert type. Some fields appear only when the associated asset or enrichment information is available.

Common alert fields

Every alert syslog notification contains the following common fields.

Field	Description	Presence
`alertId`	Identifies the alert.	Always
`alertRuleId`	Identifies the alert rule that generated the alert.	Always
`assetId`	Identifies the asset associated with the alert instance.	Always
`assetName`	Specifies the name of the associated asset.	When asset information is available

Field	Description	Presence
`sensorNames`	Lists the sensor names and packet-capture filenames associated with the asset, separated by semicolons.	When asset information is available

Alert-specific fields

In addition to the common fields, syslog notifications contain the following fields for each alert type.

Alert type	Alert-specific fields
Severe vulnerabilities in monitored entities	`vulnCSRS`, `vulnCVSSscore`, `vulnCveId`, `vulnName`
Prohibited vendors	`vendorName`
Intrusion Detection	`snortSignature`
Network Scanner	`scanEventId`, `scanType`, `scannerIP`, `targetCount`, `targetIPs`, `targetPorts`
Inactive assets	`inactiveDuration`
Assets with unexpected external communications	`asnOrganization`, `assetInterface`, `country`, `remoteAddress`, `remoteDomain`
Assets with unexpected behaviors	`behaviorId`, `behaviorLabel`, `behaviorDirection`, `sourceAssetId`, `sourceAssetName`, `targetAssetId`, `targetAssetName`

Enable or disable syslog notifications for alert types

Provides instructions for enabling or disabling syslog notifications for specific alert types in Cyber Vision Center, including prerequisites, navigation steps, and the effects of syslog notification settings on alert message delivery.

You can manage whether the Cyber Vision Center sends syslog notifications for alerts of specific alert types to your configured syslog server.

Follow these steps to enable or disable syslog notifications for an alert type:

Before you begin

- Ensure you have administrator access to Cyber Vision Center.
- Confirm that a syslog server is configured. Refer to **Configure syslog** topic in Cisco Cyber Vision Classic UI Administration Guide.

Procedure

1. From the Cyber Vision New UI, choose **Configuration** > **Alerts**.
2. Select an alert type.
3. Enable or disable **Syslog Notification**.

When you enable syslog notifications in the Cyber Vision Center, you receive syslog messages on the configured syslog server whenever the system raises (or unmutes), clears, or mutes an alert.

Vulnerabilities

This concept explains what vulnerabilities are, how they are detected within the system, and their implications for asset security.

A vulnerability is a system weakness that

- enables attackers to gain unauthorized access or perform malicious actions,
- results from flaws in system design, implementation, or configuration, and
- requires mitigation through security measures to prevent exploitation.

Feature history table

Feature	Release Information	Feature Description
Bulk vulnerability acknowledgment for assets	Release 5.5.x	You can now acknowledge or unacknowledge multiple vulnerabilities at once from the asset vulnerability table. This change removes manual processing, saving time for asset security.
Asset vulnerability insights in New UI	Release 5.5.x	Cyber Vision Center matches asset properties against the knowledge database to detect vulnerabilities. You can view the matched asset properties in the New UI. This process provides clear, actionable insights into your security posture.

Vulnerability detection in Cyber Vision Center

Provides information about how the Cyber Vision Center detects device vulnerabilities using asset properties and knowledge database rules.

Cyber Vision Center detects vulnerabilities on assets by matching their properties (such as vendor, reference, and firmware version) against a knowledge database of detection rules. This database regularly receives updates from external sources such as Computer Emergency Response Teams (CERTs), device manufacturers, and leading industry partners (e.g., Schneider and Siemens).

Key attributes of vulnerability detection:

- The vulnerability detection process is automated and relies on the latest rule database updates.
- Viewing asset vulnerability information allows security teams to assess risk exposure and prioritize remediation efforts.

To view the asset properties used for vulnerability detection in the system:

- From the main menu, choose **Assets**.
- Select the asset with vulnerabilities.
- Click **Vulnerabilities** and select the relevant vulnerability.

Vulnerability scores

Details the Cisco Security Risk Score and Common Vulnerability Scoring System, including the risk and severity categories associated with each score.

Vulnerability scores indicate the potential risk level and impact associated with specific vulnerabilities. Vulnerability scores include the following scoring systems.

Cisco Security Risk Score (CSRS)

The Cisco Security Risk Score, which is powered by Cisco Vulnerability Management, is represented on a scale from 0 to 100.

CSRS quantifies the risk of a vulnerability by looking beyond technical severity to determine how real-world attackers are leveraging the vulnerability in the wild, if at all. The score considers vulnerability and threat variables, including predictive modeling to forecast the weaponization of vulnerabilities, the availability of recorded exploits or exploit kits, the presence of near real-time exploitation, and more.

A click-through product demo supports self-paced exploration of Cisco Vulnerability Management and the Cisco Security Risk Score.

Common Vulnerability Scoring System (CVSS)

The Common Vulnerability Scoring System (CVSS) captures the principal characteristics of a vulnerability and produces a numerical score that reflects its severity. The numerical score can be translated into a qualitative representation, such as low, medium, high, and critical, to help organizations assess and prioritize vulnerability management processes.

For more information, refer to the CVSS website.

Vulnerabilities details

Outlines the details available on the Vulnerabilities page, including CVE IDs, names, Cisco Security Risk Score, CVSS scores, MITRE ATT and CK tactics, attack vectors, and affected assets for each identified vulnerability.

The **Vulnerabilities** page lists all identified vulnerabilities and their details.

Table 20: Vulnerability field descriptions

Field name	Description	Possible values/examples
CVE ID	CVE ID stands for Common Vulnerabilities and Exposures Identifier. It is a unique, standardized identifier assigned to publicly known cybersecurity vulnerabilities. This ID allows for consistent referencing of specific vulnerabilities across different security products and databases.	CVE-2023-20198
Name	This field provides a concise, descriptive title for the vulnerability.	Out-of-bounds Write Vulnerability in Rockwell ControlLogix Communication Modules

Field name	Description	Possible values/examples
Cisco Security Risk Score (CSRS)	This is a proprietary risk assessment score developed by Cisco. It provides an evaluation of the vulnerability's severity and potential impact based on Cisco's internal analysis and threat intelligence. It's typically presented as a numerical score along with a severity level (e.g., High, Medium, Low).	• 67-100: High vulnerability • 34-66: Medium severity vulnerability • 0-33: Low severity vulnerability
CVSS Score	It is the industry standard for assessing the severity of computer system security vulnerabilities. It provides a numerical score (0-10) and a qualitative severity rating (Low, Medium, High, Critical) based on various metrics like attack vector, complexity, impact on confidentiality, integrity, and availability. Security teams use CVSS scores to prioritize severe vulnerabilities and strengthen system security.	• 9-10: Critical vulnerability • 7-8.9: High severity vulnerability • 4-6.9: Medium severity vulnerability • 0.1-3.9: Low severity vulnerability
MITRE ATT and CK Tactics	Indicates whether the vulnerability can be associated with specific tactics from the MITRE ATT and CK® framework. Tactics represent the "why" of an attack (for example, gaining initial access, privilege escalation). A technique describes the specific actions or methods an attacker uses to achieve a tactic. Each tactic may be achieved through multiple techniques. To view detailed information about the tactics and techniques associated with a specific vulnerability, click the CVE ID link and review the MITRE ATT and CK section. The "3 Tactics matched" (for example) indicator suggests that the system has identified activities corresponding to three different MITRE ATT and CK tactics. Under each tactic, you can find one or more techniques used. For additional details, visit https://attack.mitre.org.	Execution, Exfiltration, Persistence
Attack Vector	Describes the path or means by which an attacker can exploit the vulnerability. It indicates the context from which the vulnerability can be exploited (example, locally, over a network, physically).	Network, Adjacent Network, Local, Physical

Field name	Description	Possible values/examples
Affected Assets	This number indicates how many of your monitored assets are currently identified as being vulnerable to this specific CVE. Clicking on the CVE ID provides a detailed list of these assets.	1 for CVE-2023-20198, 2 for CVE-2024-20437

Acknowledge or unacknowledge vulnerabilities for a single asset

Acknowledge vulnerabilities affecting an asset, or revert previous acknowledgements to manage security alerts in Cyber Vision Center.

Enable efficient management of security alerts by acknowledging or unacknowledging vulnerabilities detected for a single asset.

Perform this task to prioritize remediation efforts and maintain an accurate security dashboard. When you acknowledge a vulnerability, its alerts are removed from the **Alerts** dashboard. If you revert the acknowledgement, the alerts will appear in the **Alerts** dashboard again.

Before you begin

Ensure you have access to the **Assets** and **Vulnerabilities** dashboards in Cyber Vision Center. You may need to check your permissions under **Admin** > **Users** > **Role Management**.

Procedure

1. From the main menu, choose **Assets**.
2. Select an asset.
3. Select the **Vulnerabilities** tab.
4. To view an acknowledged vulnerability in the **Alerts** dashboard again and revert the acknowledgement:
   a. Check the checkboxes for the vulnerabilities you want to acknowledge.

      Check all the checkboxes to select all vulnerabilities at once.

   b. Click **Acknowledge**.

   c. Enter a comment if needed and confirm your acknowledgement.

5. To unacknowledge vulnerabilities:
   a. Click **Show Acknowledged** to see acknowledged vulnerabilities.

   b. Check the checkboxes for the vulnerabilities you want to unacknowledge.

   c. Click **Unacknowledge**.

- When you acknowledge a vulnerability, the system removes the alerts for that vulnerability from the **Alerts** dashboard.
- When you revert an acknowledgement, the alerts reappear in the **Alerts** dashboard.

What to do next

View the **Alerts** dashboard to verify the updated status of vulnerabilities.

Acknowledge or unacknowledge multiple assets for a single vulnerability

This task enables you to acknowledge or unacknowledge multiple assets for a single vulnerability, which helps you efficiently update remediation status and maintain accurate vulnerability records.

Simplify vulnerability management by acknowledging or unacknowledging multiple affected assets in a single operation. This reduces the time required to process vulnerability changes across several assets.

Use this task when the same vulnerability is detected across multiple devices in your environment. Bulk acknowledgment or unacknowledgment helps keep your security status accurate without repeating actions for each asset.

Procedure

1. From the main menu, choose **Vulnerabilities**.
2. Select the vulnerability you want to manage.
3. To acknowledge assets:
   a. In the **Affected** tab, check the checkboxes for the assets you want to acknowledge.
   b. Add a comment to provide context for the acknowledgment.
   c. Click **Acknowledge selected assets** and confirm.
4. To unacknowledge assets:
   a. In the **Acknowledged** tab, check the checkboxes for the assets you want to unacknowledge.
   b. Click **Unacknowledge**.

The system acknowledges or unacknowledges the selected assets for the specified vulnerability.

What to do next

Review the updated vulnerability list to confirm the changes.

Acknowledge critical vulnerabilities

Provides instructions for filtering and acknowledging critical vulnerabilities with high CVSS scores to declutter dashboards, reduce alert noise, and streamline risk management for assets.

Acknowledge critical vulnerabilities with a CVSS score greater than 9.0 to declutter dashboards, and reduce alert noise.

Use this task when you need to focus on vulnerabilities of the highest severity for an asset by filtering and acknowledging them.

Before you begin

- Ensure you have permission to view and acknowledge vulnerabilities.

Procedure

1. From the main menu, choose **Assets** and click asset name.
2. View the **Vulnerabilities** list for the selected asset.
3. Click the filter icon of the table.
4. Select **Critical** from the drop-down list in the **CVSS Score** column.

5. Click **Acknowledge**.

When you acknowledge vulnerabilities, they no longer appear in dashboard counters and alerts. This simplifies ongoing risk management.

What to do next

Review acknowledged items periodically to ensure they remain appropriate.

Communication maps

Describes how communication maps visually represent communication flows among industrial assets to help teams quickly investigate and assess risks based on abnormal flows, observed protocols, and asset relationships.

A communication map is a network visualization tool that

- Displays communication patterns at the asset-interface level.
- Organizes map data by asset groups and enables filtering of the displayed data.
- Supports investigation with details about asset interfaces, asset groups, and intra-group communications, including observed protocols, data exchange volumes, and source and destination asset-interface information.

This functionality enables operational technology (OT) and information technology (IT) teams to quickly visualize and understand the communication context of industrial assets. It provides a clear visual reference to abnormal communications and potential risks.

Feature history table

Feature	Release Information	Feature Description
Communications page enhancement	Release 5.6.x	The Communications page organizes map data by asset groups and displays communications at the asset-interface level. Asset groups can be network groups or custom groups. Functional groups are no longer supported. You can view details for asset interfaces, groups, and communications within a group. The control panel provides filter options and display settings.
External IP country mapping	Release 5.5.x	You can view the countries of external IP addresses your asset connects with. Use this map to identify geographical locations and quickly decide which communications to investigate, improving your network insight and security.

Feature	Release Information	Feature Description
ASN and ASN organization insight for external communications	Release 5.5.x	You can view ASN (Autonomous System Number) and ASN Organization information for external communications. Use this information to identify traffic sources and network owners so that you can quickly detect suspicious communications and reduce investigation time.
Communication maps and their filter enhancements	Release 5.4.x	Easily spot communications between assets, including those outside your active view. Communication maps highlight assets outside your active view filter with dotted lines.
External communications visibility	Release 5.4.x	View all communications between a selected asset and external entities. You can identify unexpected external communications that may expose your organization to attacks.
Group by network functionality in communications	Release 5.4.x	The communication map displays all communications between network groups and simplifies network interaction analysis.
See functional group-centric views of the communication map	Release 5.3.x	The communications map displays the communication activity between the configured functional groups. The communication links between groups are not actionable.
Using asset vendor names and icons	Release 5.3.x	In the New UI, communication maps include vendor icons that make asset identification easier.

Apply active view filters to the communication map

Apply filters in the communication map to focus on specific assets and their communications.

Use the common active-view filtering procedure to filter the Dashboard, Alerts, Assets, Vulnerabilities, and Communications pages. For that procedure, refer to Filter views in Cyber Vision New UI on page 56.

The active view lets you filter assets and communication links in the communication map so you can focus on specific groups. Any asset or communication outside the applied filters is shown as a dotted line, indicating it is excluded from your current view.

Follow these steps to apply active view filters to the communication map.

Procedure

1. From the main menu, select **Communications**.
2. On the **Communications** page, click the **Edit** link in the upper-right corner.
3. Under **Available filters**, configure the filters you need:

a) Click the **Select** link next to **Networks**, **Asset types**, or **Vendors** .
b) Choose the values to include for each filter.
c) Click **Apply**.

4. Click **Apply filters** to update the map.

The selected filter tags appear at the top of the **Communications** page. The map and control panel refresh to show the groups, assets, communications, and protocols associated with the active filters.

Communication map control panel

Introduces the communication map control panel, detailing features for viewing and analyzing network communications, accessing subnet details, and using panel views such as Filter Options, Settings, and Legend to filter, adjust display settings, and interpret map data.

Use the control panel on the map to view and analyze network communications and subnet details for each node on the map.

Control panel views

You can access the communication map from the **Communications** option in the main menu. The collapsible control panel appears on the left side of the map. Use it to filter map data, adjust the display, and understand map legends.

- **Filter Options**
- **Settings**
- **Legend**

The table lists the available views in the control panel and describes their uses.

Table 21: Control panel views

View	Use
Filter Options	Filter map data by time interval, Layer 2 network visibility, group, and protocol. Refer to Filter communications on the map on page 84.
Settings	Configure the map layout, visibility, communication scope, and asset labels. Refer to Configure communication map display settings on page 85.
Legend	Identify the symbols and line styles used for groups and communications. Refer to View communication map legend indicators on page 86.

You can collapse the control panel to an icon-only bar to create more space for the map. Expand it again whenever you need to update a control.

Filter communications on the map

Provides instructions for limiting the communications displayed on the map by time, L2-network visibility, group, and protocol.

Filtering communications allows you to view specific traffic and network details, making it easier to analyze patterns or anomalies.

Follow these steps to filter communications on the map.

Procedure

1. From the main menu, select **Communications**.
2. In the left control panel, click the filter icon to open **Filter Options**.
3. Under **Filter Options**, set the filters you need:

Filter Options	Use
Interval	Select the required time filter to focus on communications during specific periods. The **Last 7 days** filter is selected by default.
Show unknown (L2 Network)	Select this option to display subnets that contain MAC addresses but no IP addresses.
Groups	Select one or more asset groups to focus on their assets. Asset groups can be network groups or custom groups. Functional groups are no longer supported. IPv4 and IPv6 link-local addresses are excluded by default; select them when needed for local network discovery.
Protocols	Select the protocols to display. All protocols are selected by default, except **Traffic-heavy Protocols**, which are excluded to keep the map easier to read. Select them manually to include their data.

4. Click **Apply** to update the map.

   The **Clear** button removes the current, unapplied filter selections.

The map displays only the communications that match the selected filters.

Configure communication map display settings

Configure communication map arrangement, visibility, communication scope, and asset labels.

Use display settings to emphasize specific assets or communications, control map arrangement, and modify labels for improved clarity during investigations.

Follow these steps to configure communication map display settings.

Procedure

1. From the main menu, select **Communications**.
2. In the left-side control panel, select the Settings icon to open **Settings**.
3. Under **Settings**, configure any of the following settings:

Settings	Use
Assets & Groups	

Settings	Use
Allow rearranging	Reposition nodes on the map by dragging them. Changes are temporary and are lost when you exit the map view. This setting is enabled by default.
Hide assets outside active view	Hide assets that are outside the current active view. This setting is disabled by default.
Show only assets with communications	Display only asset interfaces with observed communications. This setting is enabled by default.
Communications	
Show all communications	Display all non-aggregated communication links at the asset-interface level. This setting is disabled by default.
Show internal communications	Display internal communications within a group. This setting is enabled by default. **Note** If you enable **Show all communications**, the **Show internal communications** setting is automatically disabled.
Asset Label	
IP address	Show only the IP address on each asset label. This option is selected by default.
Asset name (IP address)	Show the asset name and IP address on each asset label. This option is not selected by default.

The communication map updates based on your selections.

View communication map legend indicators

Identify legend indicators on the communication map to understand group types and asset status within or outside the active view.

Use the communication map legend to identify group types, assets, and communication lines shown within or outside the active view.

Follow these steps to view communication map legends indicators.

Procedure

1. From the main menu, select **Communications**.
2. In the left control panel, select the **Legend** icon.
3. Review the legend indicators.

   The legend includes the following types:

Table 22: Communication map legend

Indicator	Meaning
Asset Group Type	
Network Group	Identifies a network group.
Custom Group	Identifies a custom group.
Assets & Groups	
Within active view	Identifies assets and groups within the active view.
Outside active view	Identifies assets and groups outside the active view.
Communications	
Within active view	Identifies an asset, group, or communication that matches the active-view.
Outside active view	Identifies an asset, group, or communication that is shown for context but does not match the active-view.
Aggregated between groups	Identifies communications aggregated between two groups.

You can now clearly identify the group types and communication status of map elements.

Exploring groups in a communication map

Describes how a communication map reveals group and conduit details in place while maintaining the surrounding network communication context.

This process helps you examine asset interfaces and communications as groups are expanded or collapsed, without losing map context.

Summary

Group exploration on a communication map allows users to examine assets and communication paths within a group, without losing visibility of the overall network context.

The key components involved in the process are:

- Asset groups: Collections of assets and communication paths that can be expanded or collapsed.
- Child group: An asset group can contain child groups. When you expand a parent asset group, its child groups appear within it on the map.

- Assets interfaces: Individual interfaces within an asset group., each with associated communication and summary details. However, when **Show only assets with communications** is turned off, the map can display asset interfaces that have no observed communications.
- Conduits: Aggregated communication links between groups that display both summary and detailed information.

Workflow

The following stages describe group exploration on the communication map.

1. Select a group on the map.

   A details pop-up opens with information such as the group's assets, type, protocols, and communication summary. The map continues to show the other groups.

2. Expand the group.

   Use **Expand group** in the details pop-up to expand the group. You can also use the drop-down arrow in the group label to expand the group. The map displays the group's assets, subgroups, and internal communications while keeping nearby groups visible.

3. View asset details.

   Select an asset in an expanded group. In the details pop-up, you can select:

   - **Communication Details** to view communication details of the interface in the right pane.
   - **View assets summary** to open the asset summary page in a new tab.

4. Review inter-group communication.

   When a group is expanded, communications between groups appear as aggregated conduits. Each conduit summarizes the communication between two groups to maintain cross-group context.

5. Expand a conduit for more detail.

   Expanding a conduit shows the individual communication links, including observed protocols and total data volume. Select a communication link to view the protocol and payload size.

   Collapse the conduit to return to the aggregated view.

6. Collapse groups when finished.

   Collapsing a group returns it to a summarized node and hides its internal assets and communications. Select **Collapse All** to return the entire map to the initial group-level view.

Use the communication map context menu

Navigate the communication map using context menu actions to view groups, inspect elements, and adjust map display.

Use the context menu to navigate the communication map, view group details, and adjust how the map is displayed.

Follow these steps to access context menus and adjust the communication map display:

Procedure

1. From the main menu, select **Communications**.
2. Right-click an empty area of the map canvas to open the context menu.
3. Select the action you need:

Option	Usage
Fit to view	Display all groups and nodes in the map.

Option	Usage
Collapse All	Return every group to the group-level view.
Show all communications	Display communication links at the asset-interface level.
Show internal communications	Display communications within a group using a non-aggregated-link view.

4. To work with a specific group, right-click the group and select one of the following options:
   - **Expand group** - Shows the contents of the group.
   - **Fit group** - Focus the map on the group.
   - **Open details** - Opens the group details.

The map updates to reflect the action you select.

Enable IDS on a sensor

Enable the Intrusion Detection System (IDS) on a compatible Cisco sensor to activate Snort-based intrusion detection.

Use this task to activate Snort intrusion detection on a supported Cisco sensor for network security monitoring.

Before you begin

Ensure that your sensor is one of these compatible devices:

- Cisco IC3000 Industrial Compute Gateway
- Cisco Catalyst 9300 Series Switch
- Cisco IR8340 Integrated Services Router Rugged
- 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

To disable Snort intrusion detection, select the sensor and click **Disable IDS**.

5 Configure segmentation

Topics:

- Cyber Vision Segmentation
- Asset groups
- Switch communications views
- Segmentation rules
- Simulate segmentation rule impact

Introduces segmentation in Cyber Vision, describing segmentation concepts and workspace, enabling segmentation on switches, using Cyber Vision segmentation processes, managing asset groups, analyzing switch communications, defining and editing segmentation rules, and simulating policy impacts to enhance network security and micro-segmentation.

Cyber Vision Segmentation

Introduces Cyber Vision Segmentation in Release 5.6.0 and explains how asset groups, segmentation rules, recommendations, simulation, and switch capability fit together.

Segmentation for industrial networks is introduced in Cyber Vision Release 5.6.0 to help you define, recommend, and simulate segmentation policy on IE3300, IE3400, IE3500, and IE9300 switches.

Use Segmentation to plan policy with observed network evidence. You can review global policy objects, inspect what a switch observes, evaluate recommendations, and simulate the impact of the segmentation rules you want to apply, before applying the rules.

- Asset groups provide segmentation identities, and segmentation rules define the permissions between those identities.
- Asset group identities map to Security Group Tags (SGTs), and permissions map to Security Group ACLs (SGACLs).

You cannot deploy SGT mappings, generate switch-ready SGACL configuration, manage active policy state, or synchronize policy to switches in this release.

You can create and edit asset group membership, review and accept group recommendations, create and edit logical segmentation rules, define common-service relationships, and simulate policy impact.

You can evaluate a segmentation model against one year of observed traffic and review logical pseudo-SGACL output for training and simulation.

Cyber Vision filters the switches displayed on the **Segmentation** page according to the selected organization hierarchy level. Selecting a lower sensor-based hierarchy level limits the list to switches associated with that level and hides switches outside the selected context. If you select a network-based organization hierarchy, the **Segmentation** page does not display segmentation data. In the switches table, Cyber Vision shows whether each switch has **Simulation** or **Enforcement** capability in later releases of Cisco Cyber Vision.

- IE3300 and IE3400 only support simulation. Data from these switches can only be used for simulation.
- IE3500 and IE9300 can support enforcement. You can apply segmentation rules on these devices in later releases of Cyber Vision.
- After upgrading to Cisco Cyber Vision Release 5.6.x, wait a few days before enabling segmentation. This delay allows Cyber Vision to populate the sensor-to-communication link data required for segmentation.

Table 23: Feature History Table

Feature	Release	Feature Description
Cyber Vision segmentation	Release 5.6.0	Introduces tools to model industrial network segmentation using observed switch communications. You can create and manage asset groups, review segmentation recommendations, configure inter-group, intra-group, default, and common-service rules, and simulate policy impact on supported switches.

Segmentation workspace

Details the Segmentation entry point, global and switch-specific work areas, and organization hierarchy behavior in Release 5.6.0.

The **Segmentation** pages separate global definitions from switch detail pages.

Workspace areas

Global definitions represent reusable policy objects. In the **Segmentation** page, select the dashlets for groups or segmentation rules to view all the groups and rules available.

Switch detail pages display the rules and communications associated with the selected switch. The simulation results provided apply to the selected switch.

The switches that are listed on the **Segmentation** page are filtered by the organization hierarchy applied in Cyber Vision Center.

Only sensor-based organization hierarchies apply to **Segmentation** pages. If you apply a network organization hierarchy, the **Segmentation** pages do not display any data.

Use this table to understand the **Segmentation** pages in Cyber Vision Center.

Table 24: Segmentation workspace areas

Area	Use it to
Segmentation page	Review global definition counts and segmentation-capable switches.
Global definitions: Asset groups	Review custom groups, network groups, SGTs, and the switches that a rule is used in.
Global definitions: Segmentation rules	Review global inter-group, intra-group, and common-service rules.
Switch detail: Communications	Inspect observed group-to-group communications in map, table, and participating-groups views.
Switch detail: Segmentation rules	Review the rules that apply to the selected switch.
Switch detail: Simulation	Simulate the effect of the current policy model on observed traffic from a switch.
Disabled-switch state	Select **Enable segmentation** only when you intend to include a disabled switch in segmentation analysis.

Enable segmentation on switches

Provides instructions for enabling segmentation on switches so Cyber Vision includes device data in recommendation and simulation workflows.

You must enable segmentation on a switch to include the data from the device in the recommendation and simulation workflows.

By default, segmentation is disabled on switches.

Procedure

1. From the Cyber Vision menu, choose **Segmentation**.
2. Select one or more switches from the list.
3. Select **Enable segmentation**.

Using Cyber Vision segmentation

This topic introduces the process flow of selecting a switch, grouping assets based on observed communications, creating segmentation rules, and validating the rules before you apply any segmentation rules to a device.

Summary

Use the observed communications for a selected switch to define zones and conduits, review group-to-group communications, build rules, and simulate the rules before refining them.

Workflow

For each switch, carry out the following process.

1. Select a switch to review the communications observed on the device.
2. Use the map view to build zones and conduits, and create asset groups. The asset groups define the zones, by network group, common services, or recommended micro-segments.
3. Review the communications between asset groups.
4. Build the segmentation rules.
5. Simulate the rules and review the impact of the designed rules. You can adjust the rules as needed before finally applying them on the target device.

Result

After you adjust the rules based on the simulation, repeat the process for the next switch.

Asset groups

Explains asset groups as the segmentation identity model, including interface-based membership, custom and network groups, global and local scope, SGT precedence, and fallback behavior.

Asset groups are the segmentation identities that Cyber Vision uses to evaluate policy. When an asset interface belongs to an asset group, that group determines the SGT for the interface and the rules that can apply to its traffic.

Cyber Vision includes an asset group for a switch only after it has seen at least one asset interface from that group in traffic related to that switch.

When Cyber Vision has seen interfaces from two asset groups on the same switch, it can evaluate rules between those groups for that switch. The two groups do not need to have communicated directly with each other on that switch.

If Cyber Vision has not seen any interface from an asset group on a switch, Cyber Vision excludes that group from that switch. Rules that involve that group are not evaluated for that switch.

Group membership is based on asset interfaces, not an asset. One asset can have multiple IP addresses, and different interfaces of the same asset can belong to different groups.

Global and local group behavior

Use this table to distinguish asset group families.

Table 25: Asset group families

Group family	Source of membership	Segmentation role
Custom asset group	User-created or recommendation-derived membership from observed asset interfaces.	Explicit segmentation identity with an SGT. The group can be global or local.

Group family	Source of membership	Segmentation role
Network group	Subnet-backed membership from Cyber Vision network definitions.	Fallback segmentation identity when an interface has no effective custom group.

Global groups are the default and preferred model for shared segmentation intent. A global assignment follows the interface wherever that interface is observed.

Local groups are switch-scoped. They are visible only on the switch where they are defined and override global membership on that switch. The local SGT replaces the policy context; it does not add another permission layer on top of the global group.

An observed interface can have only one effective SGT on a switch. Cyber Vision resolves identity in this order:

Table 26: Effective identity precedence

Order	Effective identity
1	Local custom group on the selected switch.
2	Global custom group assigned to the observed interface.
3	Network group fallback for the network that contains the interface.

Use this fallback behavior to predict what happens when local or custom group membership changes.

Table 27: Fallback behavior

Situation	Effective behavior
An interface is assigned to a local custom group on the selected switch.	The local group is the effective identity on that switch, even if the interface also has a global group.
An interface has no local custom group but has a global custom group.	The global group is the effective identity.
An interface has no effective custom group.	The network group for the interface network is the fallback identity.
A local group is deleted.	Former member interfaces fall back to a global custom group when one exists. Otherwise, they fall back to the network group for their network.

Create a global asset group

Provides instructions for creating a global asset group that applies the same segmentation identity to selected asset interfaces wherever Cyber Vision observes them.

Use a global asset group when the same segmentation identity should apply to selected asset interfaces wherever Cyber Vision observes them.

> **Caution**
>
> Adding an asset interface to a group can change the segmentation identity and permissions that apply to that interface.

Before you begin

Identify the observed asset interfaces that should share the group.

Procedure

1. From the main menu, choose **Segmentation**.
2. Select the **Groups** dashlet.
3. Select **Asset groups**, select **Custom groups**, and then select **Add**.
4. Enter a unique name in **Name**.
5. Enter a description in **Description**, if needed.
6. Optional: Select a value from the **Parent group** drop-down list to filter the interfaces that belong to the selected network group.
7. Find and select the asset interfaces to add to the group from the list of **Available assets**.

   You can search or filter by **Network**, **Asset group**, **Asset type**, or **Vendor**. Review **Current group** before you select an asset interface.
8. Select **Create**.

A new global asset group is added in Cyber Vision Center. The group can be used by rules, recommendations, and simulation wherever Cyber Vision observes its member interfaces.

Switch communications views

Describes the switch communications views that show asset groups, protocols, and traffic observed for a selected switch.

On the **Segmentation** page, select a switch from the list to view the communications data observed on the switch. The **Communications** tab displays the asset groups, protocols, and traffic that Cyber Vision observed for the selected switch.

Communications views

Use this table to choose the communications view that matches what you need to inspect.

Table 28: Communications views

View	Shows	Use it to
Graph	Group relationships in a visual layout.	Understand how observed asset groups relate to each other.
Table	Group-to-group communications, protocols, and packet counts.	Inspect the protocol and traffic details behind the observed relationships.

View	Shows	Use it to
Participating groups	Asset groups observed by the switch or manually added to the switch.	Confirm which groups are available for switch-specific rule review and simulation.

Segmentation recommendations

Defines the recommendation types that Cyber Vision can propose from observed communication and explains how you can respond to each recommendation.

Cyber Vision proposes asset groups or rule changes from observed communication. You can accept, edit, or discard each recommendation.

Recommendation scope

Asset-group recommendations support microsegmentation inside one selected network group at a time. When Cyber Vision analyzes communications across a single switch, it first presents the networks that communicate across that switch. The clustering algorithm considers only assets in the selected network and checks communities using IP addresses that communicate through the switch.

Recommendations are based on observed communications, not inferred device intent. Review each recommendation before you accept it.

Cyber Vision does not need to place every interface in a new group. If it is not clear which child cluster an asset should belong to, Cyber Vision leaves that asset in the parent network group.

Existing grouped assets are not moved out of their groups. Only ungrouped assets can be recommended into existing groups.

Segmentation rules are recommendation at various levels.

Recommendation types and actions

Use this table to compare recommendation types and user responses.

Table 29: Recommendation types

Recommendation type	What you can do
Asset group recommendation	Accept as a global group, accept as a local group, edit the recommendation, or discard it.
New rule recommendation	Create an explicit rule when observed traffic would otherwise match the default rule, or discard the recommendation.
Rule update recommendation	Apply the recommended change to an existing rule, or discard the recommendation to keep the rule unchanged.

You can edit a saved rule at any time.

Create micro-segments from asset-group recommendations

Provides a source-grounded workflow for using asset-group recommendations to divide one network group into smaller logical zones.

Use micro-segmentation recommendations when you want to divide one network group into smaller logical zones before you model rules between groups.

Before you begin

Choose one network group whose observed communication patterns you want to review.

Procedure

1. In **Segmentation**, open the switch context where Cyber Vision observed communication for the network group.
2. Review the communication patterns for the selected network group.
3. Run the asset-group recommendation workflow for the selected network group.
4. Review the recommended clusters as a set.

   Cyber Vision presents the recommendations together and graphically so that you can review the relationships between the proposed groups.
5. Edit, accept, or discard each recommendation.
6. Accept a recommendation as global when the selected asset interfaces should move into a global group everywhere Cyber Vision observes those interfaces.
7. Accept a recommendation as local when the selected asset interfaces should move into a local group only in the selected switch context.
8. Leave unclear asset interfaces in the parent network group.

   Cyber Vision does not need to place every interface in a new micro-segment. Interfaces that do not form a distinct cluster continue to use the network group fallback identity.

Accepted asset-group recommendations create custom asset groups that act as micro-segments inside the selected network group. The new groups can be used by segmentation rules, recommendations, and simulation.

Segmentation rules

Provides lookup details for segmentation rule categories, actions, catch-all behavior, and default rule behavior.

Segmentation rules define permissions between asset groups. Cyber Vision models and simulates rules in Release 5.6.0, but it does not deploy them to switches.

Table 30: Rule categories

Rule category	Purpose
Inter-group rule	Defines permissions between two different asset groups.
Intra-group rule	Defines permissions within the same asset group.
Common service rule	Defines reusable service access between one service group and many subscriber groups.
Default rule	Provides the global baseline when no explicit inter-group or common-service rule applies.

Inter-group rules are unique by group pair. One pair has one shared action and one catch-all behavior, with separate directional protocol lists for each direction.

Segmentation rules table

From the main menu, choose **Segmentation**, and then select the **Segmentation rules** dashlet to manage global rules. Use the **Inter-group rules**, **Intra-group rules**, and **Common service rules** tabs to view each rule category.

Search for rules or filter them by asset group, action, protocol, or catch-all rule. Expand a rule to view the action and protocols configured for each traffic direction.

Table 31: Segmentation rule information

Field	Description
Asset group	Identifies the asset groups to which the rule applies. Inter-group rules display two different groups. Intra-group rules display the same group on both sides.
Action	Shows whether the rule allows or denies traffic that matches a configured protocol.
Protocol	Lists the protocols configured for the rule. Expand the rule to review protocols by traffic direction.
Catch all rule	Shows the action applied to traffic that does not match a configured protocol. Cyber Vision sets this value to the opposite of the configured rule action.
In use	Shows the number of switches associated with the rule. Select the number to open the **Segmentation rule in use summary** and review the switches.

Default rule behavior

The default rule is a single global baseline rule. Its default action is **Allow**, and you can edit the default action at any time.

When observed traffic hits the default rule and you create an override, Cyber Vision creates a new explicit group-pair rule instead of editing the default rule.

Select **Show** next to **Default rule** to display the group-pair rules derived from the default action. Select **Hide default rules** to display only explicit rules.

Use this table to interpret the configured action and protocol rows.

Table 32: Action and catch-all behavior

Configured action	Specific protocols	Any protocol
Allow	Allows the selected protocols and denies all other traffic between the groups.	Allows the listed protocols and denies all other traffic between the groups.
Deny	Denies the selected protocols and allows all other traffic between the groups.	Denies all traffic and locks the catch-all behavior.

Intra-group rules

Introduces how Cyber Vision models traffic inside one asset group in Release 5.6.0.

An intra-group rule defines how Cyber Vision models traffic within one asset group. The traffic uses the same effective SGT on both sides of the relationship.

In Release 5.6.0, Cyber Vision initializes each intra-group rule as an explicit allow-any rule with deny catch-all behavior. This setup permits traffic inside the group because traffic matches the allow-any rule before it reaches the catch-all behavior.

Cyber Vision creates intra-group rules for relevant asset groups. You cannot create additional intra-group rules. You can review and edit an existing rule when you need to model traffic inside a group differently.

Cyber Vision Release 5.6.0 does not generate recommendations for intra-group rules.

Edit an intra-group rule

Edit an existing intra-group rule to control how Cyber Vision models traffic within an asset group.

Edit an intra-group rule to allow or deny selected protocols between members of the same asset group.

Cyber Vision creates intra-group rules for relevant asset groups. You cannot create additional intra-group rules, but you can change the action and protocols of an existing rule.

Before you begin

Identify the asset group and the protocols that you want to allow or deny within the group.

Procedure

1. From the main menu, choose **Segmentation**.
2. Select the **Segmentation rules** dashlet.
3. Select **Intra-group rules**.
4. Open the actions menu for the asset group that you want to configure, and then select **Edit**.
5. Select **Allow** or **Deny** in **Action**.
6. Add or remove protocols for traffic within the asset group.

   Select a predefined protocol, or select **Custom rules** to define a protocol by port or port range.
7. Review the catch-all behavior and generated command preview.
8. Select **Save**.

Cyber Vision updates the intra-group rule. The rule retains the same asset group and uses the updated action and protocols in segmentation simulations.

Add an inter-group rule

Provides instructions for adding an inter-group rule that models traffic between two asset groups.

Use an inter-group rule to define how Cyber Vision models traffic between two asset groups.

Before you begin

Identify the two asset groups, the expected traffic direction, and the protocols that should be allowed or denied.

If the required protocol is not available in the predefined list, identify the transport protocol, port or port range, and optional protocol tag for the custom rule.

Review existing rules first because an inter-group rule is unique for a group pair.

Procedure

1. From the main menu, choose **Segmentation**.
2. Select the **Segmentation rules** dashlet.

3. Select **Inter-group rules**, and then select **Add**.
4. Select the first asset group in **Group A**.
5. Select the second asset group in **Group B**.
6. Select **Allow** or **Deny** in **Action**.
7. Review the **Catch all rule** that applies to traffic between the two groups that does not match a protocol row.
8. Add protocols for the direction from **Group A** to **Group B**, the direction from **Group B** to **Group A**, or both directions.

   Select protocols from the predefined list, or select **Custom rules** to define a protocol by port or port range.

9. To add a custom protocol, select **Add custom rule**, configure the protocol and port values, and then select **Save**.

   Add a protocol tag when you need a recognizable label for the custom protocol.

10. Review the generated command preview.

    Use the inline or side-by-side view to verify how the selected action and directional protocols change the logical configuration.

11. Select **Save**.

Cyber Vision adds the inter-group rule and displays it in the **Inter-group rules** table. The rule can be used in simulations for switches where both groups are relevant.

Edit an inter-group rule

Edit the action or directional protocols of an existing inter-group segmentation rule.

Edit an inter-group rule when you need to change how Cyber Vision models traffic between two asset groups.

An inter-group rule retains its Group A and Group B association. You can change its action and the protocols configured for either traffic direction.

Before you begin

Identify the inter-group rule and the protocols that you want to allow or deny.

Procedure

---

1. From the main menu, choose **Segmentation**.
2. Select the **Segmentation rules** dashlet.
3. Select **Inter-group rules**.
4. Select the rule that you want to change, and then select **Edit** in the rule details.
5. Select **Allow** or **Deny** in **Action**.
6. Add or remove protocols for either traffic direction.

   Select a predefined protocol, or select **Custom rules** to define a protocol by port or port range.

7. Review the catch-all behavior and generated command preview.
8. Select **Save**.

Cyber Vision updates the inter-group rule and uses the updated action and protocols in segmentation simulations.

Edit the default segmentation rule

Change the action that Cyber Vision applies when no explicit segmentation rule matches traffic between asset groups.

Edit the default rule to allow or deny traffic that does not match an explicit inter-group or common service rule.

The default rule is global. A change to its action affects the modeled behavior for all group pairs that rely on the default rule.

Before you begin

Review the explicit segmentation rules and determine whether unmatched traffic should be allowed or denied.

Procedure

1. From the main menu, choose **Segmentation**.
2. Select the **Segmentation rules** dashlet.
3. On the **Inter-group rules** tab, locate **Default rule**, and then select **Edit**.
4. Select **Allow** or **Deny** in **Action**.
5. Select **Save**.

Cyber Vision updates the default action. Group-pair traffic that does not match an explicit rule uses the updated action in segmentation simulations.

What to do next

Select **Show** next to **Default rule** to review the group-pair rules derived from the updated default action.

Common service rules

Details the common service rule model, including service groups, subscribers, local group subscriptions, and conversion warnings.

Common service rules reduce repeated pair rules for shared services such as DNS, NTP, infrastructure services, and quarantine services. A common service rule connects one service group with many subscriber groups.

Common service groups

A common service group is not a special group type. It is an asset group that has common service rules associated with it.

Common service groups are global.

Local group subscriptions

Local groups cannot themselves be common service groups. A local group can explicitly subscribe to a global common service from the switch. Local groups do not automatically inherit parent or global common-service subscriptions.

After a group is configured as a common service, relationships involving that group are managed through common service rules. Regular inter-group rules are not allowed for common service groups. Converting an existing group into a common service can replace regular rules, which can affect multiple switches.

Add a common service rule

Provides instructions for adding a common service rule when many groups need the same access to one shared service group.

Use a common service rule when many groups need the same access to one shared service group, such as a DNS or NTP server group.

> ⚠ **Caution**
>
> After an asset group is configured for common services, relationships to and from that group are managed through common service rules instead of regular inter-group rules.

Before you begin

Identify the service group, the groups that need access to that service group, and the protocols that should be allowed or denied.

Procedure

1. From the main menu, choose **Segmentation**.
2. Select the **Segmentation rules** dashlet.
3. Select **Common service rules**, and then select **Add**.
4. Select the asset group that provides the shared service in **Select group**.
5. Select **Allow** or **Deny** in **Action**.
6. Add protocols under **Outbound traffic**, **Inbound traffic**, or both.

   Use **Outbound traffic** for traffic that the service group initiates to included groups. Use **Inbound traffic** for traffic that included groups initiate to the service group.
7. Review the **Catch all rule**.

   Groups that are included in the rule use this common service rule. Groups that are not included follow the system-wide default rule.
8. Under **Inclusions**, select the groups that the common service rule applies to.
9. Select **Add**.

Cyber Vision adds the common service rule for the selected service group and included groups.

Switch-specific rules

Describes how the switch-specific segmentation rules view shows the rules associated with asset groups for the selected switch.

On the **Segmentation** page, select a switch from the list to view the segmentation rules relevant to that switch. The **Segmentation rules** tab displays the inter-group and intra-group rules associated with asset groups available on the selected switch.

Common service rules are global rules. Manage them from **Global definitions** > **Segmentation rules** > **Common service rules**.

Use this view to review the rules that apply to the selected switch and whether switch-local behavior differs from global intent. The switch-specific view limits the available asset groups and rules to those that are relevant to the selected switch.

You can add an inter-group rule from the switch-specific view. Cyber Vision limits the **Group A** and **Group B** selections to groups available for that switch.

In the global rules table, select a value in the **In use** column to identify the switches associated with a rule.

Simulate segmentation rule impact

Provides instructions for evaluating observed traffic against the current segmentation model before changing segmentation rules on a device.

Use simulation to evaluate how segmentation rules would allow or deny observed traffic before you change the rules.

Simulation is calculated on traffic observed across all segmentation-enabled switches while showing only asset groups observed on the selected switch.

Procedure

1. On the **Segmentation** page, select a switch.
2. Select the **Simulation** tab.
3. Review observed, denied, and allowed traffic totals.
4. Use **Source**, **Action**, **Protocol**, and **Destination** filters to isolate flows in the sankey chart representation.
5. Inspect high-hit source and destination flows.
6. Select **Reset to default** only when you want to clear simulation filters.

The simulation helps you understand which rules would match the observed communication, the resulting allow or deny action, whether the traffic matched an explicit protocol row or the catch-all behavior, and the switch used for evaluation.

6 Cyber Vision Secure Remote Access

Topics:

- CV SRA
- SRA roles and permission descriptions
- CV SRA access methods
- CV SRA dashboard
- Supported switch and router models for CV SRA
- Cisco IoT Operations Dashboard
- Add and manage users
- Organization statuses
- Multi-factor authentication settings
- Network devices onboarding and CV SRA agent deployment
- Operational technology (OT) assets
- Bulk configuration cloning
- Access control groups
- How CV SRA Plus remote access works
- Duo integration with CV SRA Plus
- Configure access methods
- Remote asset session requests
- Remote session management and monitoring
- Remote session recordings
- Alert rules
- Alerts
- View user activity in Cisco IoT Operations Dashboard
- Access expiration policy
- Secure file transfer
- Request an access extension for an CV SRA session
- Request access to a remote session
- Connect to a remote session using the request access procedure
- Connect to a scheduled remote session
- Withdraw a session request
- Best practices for accessing CV SRA remote sessions
- Collect CV SRA agent logs from the IOx app
- DNS resolution issues
- CV SRA agent failures

Use this chapter to understand Cyber Vision Secure Remote Access (CV SRA), which provides secure remote connectivity to OT assets.

- Resolve the "pending services update" state
- Resolve the "pending creation" state
- Resolve the "pending removal" state

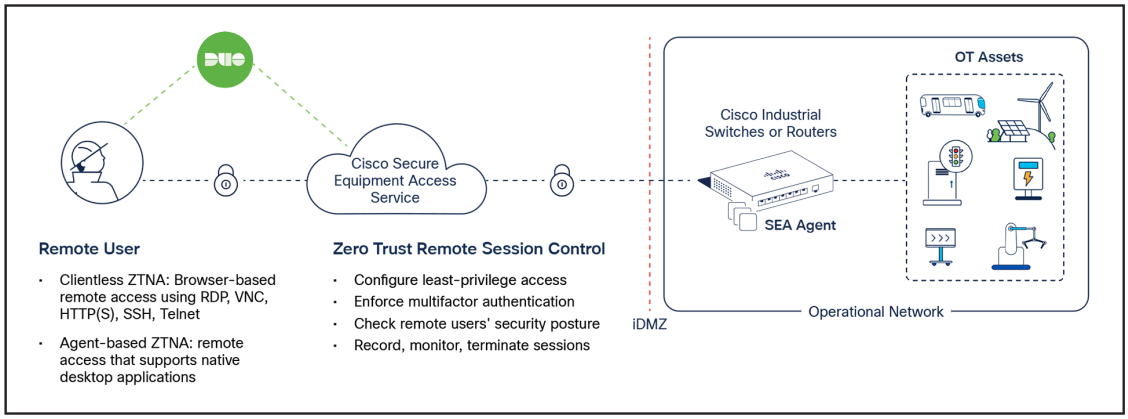
CV SRA

Introduces Cyber Vision Secure Remote Access (CV SRA), which provides secure remote connectivity to OT assets using ZTNA gateway functionality embedded in Cisco industrial switches and routers.

CV SRA provides secure, scalable remote access to operational technology (OT) assets by embedding Zero Trust Network Access (ZTNA) gateway functionality directly into Cisco industrial switches and routers, enabling centralized management, strict authentication, and flexible access methods.

- Embeds ZTNA gateway functionality directly into Cisco industrial switches and routers.
- Enables centralized management and strict authentication through a cloud portal trust broker.
- Offers flexible access methods, including clientless and agent-based ZTNA for differing operational needs.

Figure 2: CV SRA operations



Key features and capabilities of CV SRA

CV SRA simplifies remote access deployment, eliminates dedicated hardware, and removes the need for complex firewall rules. It centralizes management and enforces zero trust security using a cloud portal as a ZTNA trust broker. Access is strictly authenticated and adaptively granted based on identity, context, and time, with assets hidden from discovery and IP addresses never exposed in the iDMZ.

Key CV SRA features include:

- Simplified Deployment: Remote access is enabled as a software feature on existing Cisco industrial equipment.
- Elimination of Hardware: No need for dedicated point hardware solutions.
- No Complex Firewalls: Removes the need for complex iDMZ firewall rules.
- Strict Authentication: Remote personnel must authenticate through the cloud portal before access is allowed.
- Adaptive Trust: Access is granted based on identity, context, and time, ensuring a default deny posture.
- Enhanced Protection: Assets are hidden from discovery, lateral movement is prevented, and IP addresses are not exposed in the IDMZ.

For example, operations teams can use CV SRA to configure equipment such as traffic signal controllers, in-vehicle dispatch systems, cameras, and other systems deployed in the field and connected using Cisco industrial routers.

CV SRA Plus

Explains CV SRA Plus tiers, the premium advanced access options designed for scenarios that require more than a simple browser window, such as using engineering software tools or transferring large files between devices.

CV SRA Plus is a premium advanced tier designed for users who need capabilities beyond a standard browser window, such as running engineering software or transferring large files.

- Requires installation of a lightweight client application on the user's computer (currently Windows supported).
- Establishes a direct, secure data tunnel similar to a specialized, granular VPN.
- Enables use of native engineering tools and applications as if directly connected to the remote machine.

Key features of CV SRA Plus

CV SRA Plus offers deeper flexibility for equipment that requires more than a simple browser session.

- Lightweight Client: Requires a small application to be installed on the user's computer (currently Windows supported).
- Secure Tunneling: Creates a direct, secure data tunnel that acts like a specialized, granular VPN.
- Native Application Support: Operates at the network layer, allowing use of native engineering tools and diagnostic apps as if directly connected to the machine.

SRA roles and permission descriptions

Describes the principal roles in CV SRA, their permissions, and available menu options.

There are three principal roles used in CV SRA. Each role has permissions specific to that role.

The roles with accompanying permissions and available menu options are listed here.

Table 33: SRA roles, permissions, and menu options

Role name	Permissions	SRA menu options
SRA System Admin	• Remote System Management • Remote Access Management • Remote Access	• **Remote Sessions**: Launch remote sessions • **Access Management**: Launch remote sessions and manage access groups • **System Management**: View and manage network devices, connected clients, and access methods
SRA Access Admin	• Access Management • Remote Access	• **Remote Access Management**: Manage access groups • **Remote Sessions**: Launch remote sessions
SRA Access Manager	• Access Approver • Remote Access	• Approve access requests for access methods within a group • Launch remote sessions
SRA User	• Remote Access	• **Remote Sessions**: Launch remote sessions

Predefined roles

List the predefined roles in CV SRA to define access control responsibilities.

CV SRA offers role-based access control (RBAC) for four predefined roles.

SRA roles

Role	Access permissions granted to this role...
SRA Access Admin	View and manage network devices, connected clients, and access methods.
SRA Access Manager	Review access requests created using the Request Access feature. View and launch remote sessions.
SRA System Admin	Launch remote sessions and manage access groups.
SRA User	Launch remote sessions.

CV SRA access methods

Describes the mechanisms available for accessing OT assets through CV SRA access methods, including both clientless and agent-based groups for secure and flexible remote access.

CV SRA access methods are categorized connection mechanisms that allow users to interact with OT assets, supporting various protocols and use cases for efficient remote asset control.

- Two main groups: Group A (clientless) and Group B (agent-based).
- Group A enables access through supported web browsers without local client installation.
- Group B uses the SRA Plus App, a lightweight VPN client, for secure communications on Windows 10+ systems.

Types and characteristics of CV SRA access methods

CV SRA solutions provide two main groups of access methods, each supporting specific protocols and use cases to control remote assets efficiently.

- Group A (Clientless): SSH, RDP, VNC, Web App, Telnet–access from a supported web browser for quick, browser-based access.
- Group B (Agent-based): SRA Plus application–requires installation for advanced, secure communications.

Comparison of CV SRA access method groups:

Table 34: CV SRA access method groups comparison

Group	Approach	Methods
A	Clientless	SSH, RDP, VNC, Web App, Telnet
B	Agent-based	SRA Plus application (lightweight VPN client for secure channel on Windows 10+)

CV SRA access methods and their characteristics

Explains the supported CV SRA access methods and summarizes their key characteristics, security considerations, and usage requirements.

The following table provides an overview of the supported CV SRA access methods.

Table 35: CV SRA access methods overview

Access method	Description	Key requirements	Security notes
SSH	Secure Shell Protocol for remote command-line administration. Lets users access, control, and modify remote servers over the internet.	Username and password or key authentication.	All communication is encrypted; secure alternative to Telnet.
RDP	Microsoft Remote Desktop Protocol provides remote display and input for Windows-based applications.	Username and password. If left blank, user prompted at login.	Encrypted session; prompts for credentials if fields are left blank.
VNC	Virtual Network Computing enables screen sharing and remote control across multiple operating systems (default port: 5900).	Password required; prompted if left blank.	Session is not encrypted by default; prompt for credentials increases security.
Web App	Application software accessed through a web browser over HTTP/HTTPS. Web servers handle client requests and serve content.	Network connection and browser.	Uses HTTP or HTTPS; HTTPS recommended for secure data exchange.
Telnet	Provides two-way text-based remote sessions using TCP/IP.	Port number must be specified; username/password not required.	Communication is unencrypted. Not recommended for sensitive operations.
SRA Plus	Application that allows remote access using IP-based protocols (TCP, UDP, or ICMP), enabling file transfers and secure channels.	SRA Plus App installed (Windows 10+).	Operates as a lightweight VPN client to create a secure communication channel.

CV SRA dashboard

Describes the essential features and key components of the CV SRA dashboard, which provides a centralized, real-time interface for administrators to monitor and manage CV SRA efficiently.

The CV SRA dashboard is a centralized, real-time interface that enables administrators to monitor and manage CV SRA, supporting oversight of alerts, requests, sessions, users, agents, access control groups, trends, and data usage.

- **Active Alerts** section: Displays alert counts by severity: Critical, High, Medium, and Low. Use **View all alerts** to open the alert list.
- **Pending requests** section: Displays counts for pending **Remote access** and **Access expiration** requests.
- **Status** section: Displays dashlets for Active Sessions, SRA Agents, Access Control Groups, SRA Users, and SRA User Roles, allowing quick access to related management screens.
- **Trends** area: Presents visual graphs showing activity and patterns for Web App, SSH, VNC, SRA Plus, RDP, and Telnet access methods over selectable time periods.
- **Data Usage** section: Summarizes access methods used, usage times, and total data transferred, with color-coding for quick interpretation.

Key features and components of the CV SRA dashboard

The CV SRA dashboard includes several sections and dashlets that provide administrators with actionable insights and management capabilities.

- **Active Sessions** dashlet: Displays a list of current users and their sessions, with navigation to Access Management for detailed oversight.
- **SRA Agents** dashlet: Lists network devices with the SRA agent installed and provides their status information.
- **Access Control Groups** dashlet: Shows defined access groups and offers management actions.
- **Trends** graphs: Support tooltips that provide on-demand session details and access method information for deeper insight.
- **Active Alerts** dashlet: Displays the number of active alerts in the Critical, High, Medium, and Low severity categories and links to the alert list.
- **Pending requests** dashlet: Displays pending Remote access and Access expiration request counts.
- **SRA Users** dashlet: Displays user counts by Active, Inactive, and Blocked status.
- **SRA User Roles** dashlet: Displays user counts for Remote Users and Admin Users.

CV SRA dashboard usage examples

The **Status** section helps administrators jump directly to management pages for sessions, SRA agents, users, roles, or groups. **Active Alerts** and **Pending requests** highlight items that may require attention. **Trends** graphs highlight changes in remote access activity, helping identify usage patterns. The **Data Usage** section summarizes which access methods were used, when, and the volume of data transferred. Color-coding improves quick data interpretation.

Supported switch and router models for CV SRA

Identifies the compatible IE switch and router models for IoT OD services, specifying their software and hardware prerequisites to ensure proper deployment and support.

For a list of the Cisco Industrial Ethernet (IE) switches and Industrial Routers (IR) support CV SRA, see Cisco Cyber Vision Data Sheet.

All the listed IR routers and IE switches support the IOx framework and can host IOx applications for IoT OD Services.

Cisco IoT Operations Dashboard

Streamline user and organizational management by assigning roles, grouping assets, and securing access with multi-factor authentication.

The Cisco IoT Operations Dashboard is a cloud-based platform designed to empower operational technology (OT) teams to remotely deploy, manage, monitor, and maintain industrial IoT networks and assets at scale.

- Simplifies provisioning and management of Cisco industrial routers, gateways, and connected equipment.
- Enables faster deployment and ongoing visibility with built-in IT-managed security standards.
- Supports multiple authentication methods and enhanced login experiences for first-time and returning users.

Authentication methods and user access options

The IoT Operations Dashboard supports several authentication methods to provide secure and flexible access for users.

- Single Sign-On (SSO)
- Identity Provider (IdP) integration

Set up first-time access to IoT Operations Dashboard

Provides instructions to activate your IoT Operations Dashboard account and log in for the first time.

Activate your account and complete your initial login to the IoT Operations Dashboard.

This task is for users who have received a welcome email and are accessing IoT Operations Dashboard for the first time.

Before you begin

- Ensure you have received the activation email from Cisco Identity Platform.

Procedure

1. Open the welcome email from Cisco and locate the activation link.
2. Click the activation link to begin account setup.

   Note

   The activation link is valid for 1 hour.

3. Follow the prompts to create your password and complete your Cisco Identity Platform account registration.
4. After activation, use the link in the email to log in to your IoT Operations Dashboard organization.
5. If you already have a Cisco Identity Platform account from a different application, follow the instructions in the email to link your existing Cisco account to your IoT Operations Dashboard organization.

Your account is active and you are logged in to the IoT Operations Dashboard.

Log in as an existing user to IoT Operations Dashboard

Provides instructions to access IoT Operations Dashboard as a returning user and select your organization.

Sign in and access the appropriate organization in Cisco IoT Operations Dashboard.

Use this task if you already have an IoT Operations Dashboard account.

Before you begin

- Confirm you have valid login credentials.

Procedure

1. Go to the Cisco IoT Operations Dashboard URL (https://us.ciscoiot.com or https://eu.ciscoiot.com).
2. On the login screen, enter your registered email address and click **Continue**.
3. If your email is associated with a Cisco Identity Platform account, complete multi-factor authentication (MFA) if prompted.
4. If prompted, select the organization you want to access.
5. If you have recently been added to a new organization, locate and open the welcome email for your login link.
6. Upon login, the dashboard will load your last accessed service.

You are logged in to the selected organization with access to previously used dashboard features.

Sign in using Cisco single sign-on (SSO)

Provides instructions to authenticate to IoT Operations Dashboard using Cisco Single Sign-On (SSO).

Access IoT Operations Dashboard with your Cisco SSO credentials.

Use this procedure if your account uses Cisco SSO for authentication.

Before you begin

- Confirm your account is associated with the Cisco Identity Platform.

Procedure

1. Navigate to the IoT Operations Dashboard login page.
2. Enter your email address.You are automatically redirected to the Cisco Identity Platform for authentication.
3. Complete the Cisco SSO authentication steps as prompted.
4. Upon successful authentication, you are signed in to the IoT Operations Dashboard.

You are authenticated and granted access to the IoT Operations Dashboard.

Integrate a corporate identity provider (IdP) with IoT Operations Dashboard

Provides instructions to integrate your corporate IdP with IoT Operations Dashboard for SAML-based SSO.

Enable SSO using your organization's corporate IdP (SAML 2.0) for users accessing IoT Operations Dashboard.

Perform this task if your organization requires integration with a corporate IdP for single sign-on.

Before you begin

- Designate a Tenant Admin for your organization.
- Prepare your corporate IdP metadata.

Procedure

1. Contact Cisco at iotod-account-request@cisco.com to initiate IdP integration.

2. Share your organization's IdP metadata with Cisco and obtain the Service Provider (SP) metadata for your IdP.
3. Configure your IdP to recognize IoT Operations Dashboard as the SP.
4. Ensure your Tenant Admin maps IdP roles to the appropriate organizations and roles within IoT Operations Dashboard before users attempt to log in.
5. Confirm that your SAML response includes the user's Email ID and Role(s).

Users are able to authenticate to IoT Operations Dashboard using your corporate IdP.

What to do next

Test SSO functionality with a pilot user to ensure correct role mapping and access.

Add and manage users

Provides instructions for adding new users to your organization, assigning roles and permissions, and managing user access.

Use this task to add new users to your organization and assign appropriate access permissions.

Before you begin

- Ensure you have administrative access to the system's Access Control features.
- Obtain the email addresses of users who need to be added.
- Verify you know which roles and permissions are required for each user.

Procedure

1. Click the profile icon and choose **Access Control**.
2. Click **Users** >**Add user**.
3. Enter a valid email address.
   - A welcome email with login and password instructions will be sent to this address.
   - If your organization uses SSO, users receive an email but are not prompted to enter a password. They uses their corporate credentials to log in instead.
4. Select one or more roles to define the user's access permissions.

   The list includes predefined roles and your organization's custom roles.
5. Click **Add**.
6. If the user is not present in Cisco identity platform, enter additional parameters for the user, such as First Name, Last Name and Country / Region. Click **Add**.

The user receives two emails: one to activate the Cisco identity platform account and change the password, and another to welcome and log in to IOT OD.

Organization statuses

Describes the possible statuses for an organization and their meanings.

This topic explains the possible statuses for an organization and what each status means.

Table 36: Organization statuses and meanings

Status	Meaning
Active	The organization and all associated Operations Dashboard services are fully functional.
Pending Creation	An error occurred while adding services; the organization is not yet accessible.
Pending Service Update	At least one service is not operational due to an error; others might be active.
Pending Removal	Devices or data remain; errors can occur if not removed before service deletion.

Multi-factor authentication settings

Describes multi-factor authentication (MFA), a security feature requiring two or more independent verification factors, enhancing the security of IoT deployments by protecting user accounts from unauthorized access.

Multi-factor authentication (MFA) is a security feature that strengthens access control by requiring users to provide multiple forms of verification before accessing Cisco IoT Operations Dashboard.

- Requires users to provide two or more independent verification factors.
- Enhances the security of IoT deployments by protecting user accounts from unauthorized access.
- Integrates with Cisco identity platform for robust authentication.

Multi-factor authentication (MFA) strengthens access control by demanding multiple forms of verification—typically something a user knows (like a password) and something they have (like a one-time password or authenticator app). Cisco IoT Operations Dashboard leverages this capability to ensure only authorized individuals can access critical IoT services and data.

How MFA enforcement works

Describes how multi-factor authentication (MFA) is enforced, outlining the main actors and the sequence of actions that ensure only authenticated users gain access.

MFA enforcement strengthens security by requiring users to provide multiple forms of verification before accessing organization resources.

Summary

The following are the key components involved in the MFA enforcement process:

- Administrator: Enables or disables MFA for the organization and manages MFA settings.
- User: Completes MFA setup and uses it during each login.
- Cisco identity platform: Facilitates user authentication, including MFA verification.
- Authenticator app: Generates one-time passwords (OTP) for user verification.

This process ensures that only authenticated users can access CV SRA by requiring multiple forms of verification.

Workflow

These stages describe how MFA is enforced in CV SRA.

1. The administrator logs in to CV SRA and enables MFA at the organization level.
2. Users log in to id.cisco.com, install an authenticator app on their mobile device, and set up MFA using the Cisco identity platform.
3. Users access CV SRA using their credentials.
4. After credential verification, the authenticator app generates a one-time password.
5. Users enter the OTP to complete authentication and gain access to CV SRA features and services according to their role.

Result

MFA becomes a required part of the login process for all users in enabled organizations, ensuring that only authenticated users can access CV SRA, enhancing overall security.

Enable or disable multi-factor authentication

Provides instructions for enabling or disable multi-factor authentication (MFA) for an organization in Cisco IoT Operations Dashboard.

Allow administrators to enable or disable MFA for an organization in Cisco IoT Operations Dashboard.

Use these steps to modify MFA enforcement for your organization according to your security needs.

Before you begin

- Log in as a tenant admin or system admin on Cisco IoT Operations Dashboard.

Procedure

1. Log in to the Cisco IoT Operations Dashboard as a tenant admin or system admin.
2. Click the “people icon” at the far right of the header, then click Access Control.
3. Select the **Organizations** tab.
   a) Select the organization that requires MFA access; the organization’s detail page opens.
   b) Click **Edit Organization**.
   c) Select or clear the **Enable Multi-Factor Authentication** check box from the Features list.
   d) Click **Save**.

MFA is enabled or disabled for the selected organization as specified.

What to do next

Users must log out and log back in to use MFA if it was just enabled.

Set up MFA in Cisco identity platform

Provides instructions to enroll in multi-factor authentication (MFA) for your Cisco identity account using an authenticator app.

Use this task to enroll in Multi-Factor Authentication (MFA) using Cisco’s identity service.

Users must set up MFA through their Cisco identity platform account and an authenticator app.

Before you begin

- Ensure you have access to your Cisco identity account and a mobile device for the authenticator app.

Procedure

1. Log in to Cisco identity platform.
2. Go to the **Security** tab.
3. Under **Account Security** , enable the **Multi-Factor Authentication (MFA)** toggle button.

   A window appears requesting your password.
4. Enter your password and click **Verify**.

   The Enroll in Multi-Factor Authentication window lets you select your authenticator app, such as Cisco Duo or Google Authenticator.
5. Select your preferred authenticator app and click **Next**.

   A window displaying a QR Code opens.
6. Open your authenticator app and scan the QR Code.

   The app generates a 6-digit code on your phone.
7. Enter the code in the window and click **Submit**.

   A confirmation window appears indicating successful enrollment.

Your account is now enrolled in MFA and can be used for secure logins to Cisco IoT Operations Dashboard.

Multi-factor authentication scenarios

Lists common multi-factor authentication (MFA) scenarios and explains how MFA enforcement applies in various contexts within Cisco IoT Operations Dashboard.

This reference describes how multi-factor authentication (MFA) enforcement applies in various Cisco IoT Operations Dashboard scenarios.

- **Using your own identity provider (IdP):** If your organization uses an external IdP (such as Active Directory), MFA settings in Cisco have no effect—users log in as usual based on your own IdP policies.
- **Mixed IdP environments:** Organizations may use different IdPs. Only users in organizations using Cisco's IdP are subject to MFA enforcement.
- **Switching from a non-MFA to MFA organization:** Users must log out and re-authenticate with the appropriate IdP when switching to an organization that requires MFA.
- **Switching organizations within the same IdP:** Users can move seamlessly between organizations that use the same IdP without an additional login.
- **Switching IdPs:** Users are prompted to log out and re-authenticate when changing between different identity providers.

Network devices onboarding and CV SRA agent deployment

Guide users through onboarding supported network devices and deploying the CV SRA agent using the step-by-step configuration flow in the CV SRA User Interface.

The process of network device onboarding and CV SRA agent deployment enables efficient configuration and activation of the CV SRA agent on supported devices.

- A guided configuration flow in the CV SRA UI.
- A way to generate device-specific CLI configuration commands and to copy and run them on the device console.
- Reliable onboarding of the network device and activation of the CV SRA agent.
- Migration of an agent from EDM or Application Manager deployment to CLI deployment while retaining the associated assets, access method definitions, and access control groups.
- Proxy and multi-VLAN configuration options for supported network devices.

Deploy CV SRA agent on network devices using CLI commands

Onboard and register industrial network devices with the CV SRA service by deploying the CV SRA agent using CLI commands.

This task enables CV SRA on your network devices by generating device-specific CLI commands after guided configuration in the CV SRA user interface.

Use this procedure to add a network device to the CV SRA service using the CLI deployment method.

Before you begin

- Depending on the cluster in use, the device must always have access to us.ciscoiot.com or eu.ciscoiot.com.
- If you use an external DNS server, configure your firewall rules to allow your CV SRA gateway access to IoT OD and DNS.
- Ensure you get the client ID of the device by running this command:

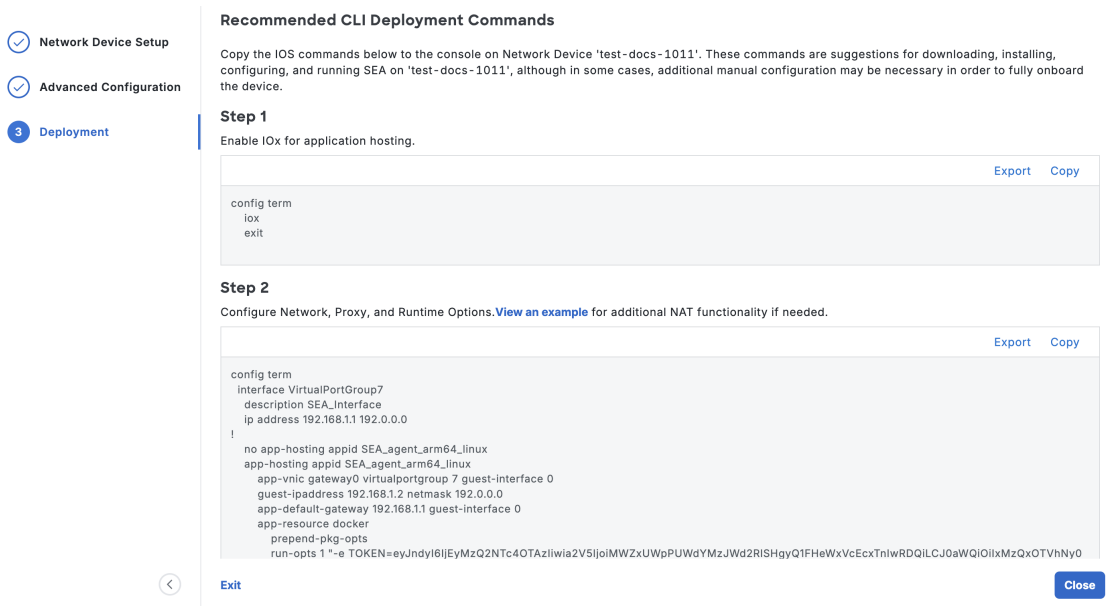
```
Device# show license udi
```

Procedure

1. On the **Service** panel, click **SRA** > **System Management** > **Add Network Device**.
2. On the **Add Network Device** page, select **CLI Deployment** in the **Selection Method** drop-down list.
3. Enter a unique device name in the **Network Device Name** field and the device serial number in the **Client ID** field.
4. To select a specific device series:
   a) Select a device type (router or switch) from the **Network Device Model** drop-down list.
   b) Select a specific model from the **Network Device Model** drop-down list.
   c) Click **Next**.
5. In the **Advanced Configuration** tab, enter the network configurations, and click **Add**.

   The UI displays the CLI commands required to configure your network device and install the CV SRA agent. These commands are specifically generated for the device currently being onboarded and are organized into three sequential steps: **Step 1**, **Step 2**, and **Step 3**.

   Figure 3: CLI deployment commands



6. Copy the generated commands from **Step 1** and **Step 2** and sequentially run them on your device console. You have successfully enabled IOx application hosting and configured the required network and proxy settings.
7. To install the CV SRA agent:
   a) Download the CV SRA agent package to your local device by clicking **Download SRA agent** in **Step 3**.
   b) Copy the package to the flash drive of your device and run the command in **Step 3** to install the package.
8. Click **Close** after the commands have finished running.

After successfully running the commands, the status of the network device changes to **active** on the **System Management** page. The CLI commands are automatically saved. To view them at a later time, click **View Deployment Commands** under **Deployment Details**.

Network configuration field descriptions

Explains the descriptions and purposes of the fields used in network configuration, including proxy, IP address, subnet, and DNS settings.

This section provides descriptions for each field in the network configuration to assist with proper device setup and management.

Table 37: Network configuration fields

Field	Description
Enable HTTP Connect Proxy	A setting to activate or deactivate the use of an HTTP proxy server for device connections.
Management VPG IP Address	The IP address assigned for administrative and management access to the device.
Subnet Mask	The subnet mask used to define the network segment of the IP address.
CV SRA agent IP Address	The required IP address of the device where the CV SRA agent is deployed.
VRF	The name of the Virtual Routing and Forwarding instance used to maintain separate routing tables for network segmentation.

Field	Description
Primary DNS IP Address	The IP address of the main Domain Name System (DNS) server used by the device for hostname resolution.
Secondary DNS IP Address	The IP address of the backup DNS server used for redundancy if the primary server is unavailable.

HTTP connect proxy field descriptions

Explains the available fields and configuration options for enabling and setting up an HTTP connect proxy on a device.

This section describes each field used to configure an HTTP connect proxy.

Table 38: HTTP connect proxy field descriptions

Field	Description
Enable HTTP Connect Proxy	A toggle switch to activate the device's use of an HTTP proxy server for outbound connections.
Choose an HTTP Connect Proxy Configuration Mode	Selects the method for entering the proxy details: either as a single URL string or in separate form fields.
Proxy URL	Configuration mode where proxy details (server, port, authentication) are entered as a single URL.
Proxy Form	Configuration mode where proxy details are entered into separate fields.
Enter URL	Complete proxy server URL, typically including authentication, server address, and port.

Deploy CV SRA agent on IE switches using CLI commands

Lists the recommended method and steps to install the CV SRA agent on supported IE switches using CLI commands.

The following information summarizes how to install the CV SRA agent on Cisco Industrial Ethernet (IE) switches using CLI commands:

- The recommended approach for activating CV SRA on standalone (CLI-managed) devices is to use the CLI commands provided by the CV SRA User Interface.
- Use the guided configuration flow in the CV SRA User Interface to generate the appropriate CLI commands.
- Copy and apply the suggested CLI commands directly to your IE switch to enable the CV SRA agent.
- For a video demonstration, refer to Onboarding devices with CLI method.

Note

Previously, the network device onboarding and installing the CV SRA agent involved several steps: creating a device profile, adding the network device to the Application Manager service, configuring the device with CLI commands for the IoT Operations Dashboard connectivity, and then installing the CV SRA agent.

Migrate the SRA Agent from EDM or Application Manager to CLI deployment

Migrate an SRA Agent from an EDM or Application Manager deployment to CLI-based deployment while retaining the associated assets, access method definitions, and access control groups.

Use this task to move an existing SRA Agent deployment from EDM or Application Manager to CLI-based deployment.

The migration does not change the assets, access method definitions, or access control groups associated with the network device.

Devices that you can migrate

- IR1101 and IR18xx series routers.
- IE3300, IE3400, IE3500, and IE9300 series switches.

Before you begin

- Have SRA System Admin access to Cisco IoT Operations Dashboard.
- Have console or SSH access to the network device with privileges to run Cisco IOS XE application-hosting commands.
- For IR1101 and IR18xx routers, gather the network values required for CLI configuration, including the management VPG IP address, subnet mask, SRA Agent IP address, VRF, DNS IP addresses, and HTTP Connect proxy settings.

Note

Remote sessions to the associated assets are unavailable until you apply the CLI commands and the SRA Agent status changes to **Up**.

Procedure

1. From the main menu, choose **System Management** > **Network Devices**.
2. Filter the device list by **App Manager**.
3. For the device that you want to migrate, open the actions menu and select **Migrate to CLI**.
4. In the **Migrate to CLI Deployment** wizard:
   a) In the **Network Device** step, review the automatically populated network device details.
   b) In the **Advanced Configuration** step, enter the required values for an IR router. For an IE switch, the values are automatically populated. You can edit the values as needed.
   c) Click **Migrate**, and then select **Confirm Migration**.

   The deployment method changes to CLI-based management, and the SRA Agent changes to **Unknown** until you apply the generated CLI commands on the device. The associated assets, access method definitions, and access control groups remain unchanged.

5. In the **Deployment** step, use **Copy** or **Export** to save the generated command sections.
   a) Run `show app-hosting list` to check the application ID.
   b) If an SRA Agent is listed, run the generated **Cleanup Existing Application** commands to stop, deactivate, and uninstall the existing application. For example:

      Example

      ```
      !Replace <app-id> with the application ID returned by show app-hosting
      list.
      app-hosting stop appid <app-id>
      app-hosting deactivate appid <app-id>
      app-hosting uninstall appid <app-id>
      ```

   c) Run the generated **Step 1** commands to enable IOx for application hosting.
   d) Run the generated **Step 2** commands to configure the network, proxy, VLAN, and runtime options. For example:

      Example

      ```
      !Example
      configure terminal
         no interface VirtualPortGroup0
         interface VirtualPortGroup7
         description SRA_Interface
            !This command is required if VRF is configured
            vrf forwarding ${VRF NAME/NUMBER}
            ip address ${management VPG ip} ${subnet mask}
            ip nat inside
      end
      ```

   e) Select **Download SRA Agent** to download the SRA Agent application binary.
   f) Copy the downloaded SRA Agent application binary to the device flash. For example:

      Example

      ```
      bash scp output/sra_agent_app/<tar-file>
      <device-username>@<device-ip>:flash:/<tar-file>
      ```

   g) Run the generated SRA Agent installation command on the device.

   Save the generated commands in your local workspace. You cannot view the commands again after you leave the page. For IR router migration, the first three commands are not displayed again after you leave the page.

6. In **System Management** > **Network Devices**, wait for **SRA Agent Connection** to change from **Unknown** to **Up**.

The network device is migrated from EDM or Application Manager management to CLI management. The SRA Agent is managed through the generated Cisco IOS XE commands, and the existing assets, access method definitions, and access control groups remain associated with the device.

Configure CV SRA agent for proxy support

Provides instructions for adding a network device in CV SRA and configuring it for HTTP(S) proxy communication by selecting your preferred proxy configuration method.

This initial setup enables you to add a new device, select proxy support, and choose your preferred proxy configuration input method.

This task describes how to add a network device in CV SRA and configure it for HTTP(S) proxy support, allowing you to select the proxy configuration method that best fits your needs.

Before you begin

- Ensure you have an IE3x00 switch, CV SRA application access, and IDA version 17.14.1 or above.
- Verify you have access to the CV SRA application.
- Confirm the device runs IDA version 17.14.1 or above.

Procedure

1. In the **SRA** > **System Management** > **Network Devices**, configure the proxy settings.
2. Click **Add Network Device** .
3. Use the **Select from list (recommended)** option and choose the **Network Device** you want to add.
4. Click **Next** to open the **Network Device Details** screen.
5. Enable the **HTTP Connect Proxy switch** to open proxy settings.
6. Choose either **Proxy URL** (default setting) or **Proxy Form** and enter the proxy configuration. Select the option and enter the information that fits your needs.

> **Note**
>
> **Proxy Form** and **Proxy URL** serve the exact same purpose; they provide different ways of entering the same information, and you can pick the one most convenient for you.

The network device configuration screen is ready for you to enter proxy settings using either URL or form.

CV SRA HTTP proxy support

Explains how CV SRA HTTP proxy support enables secure and flexible proxy sessions for network device communication through CV SRA.

A CV SRA HTTP proxy support feature is a network communication mechanism that enables customer-controlled proxy sessions for secure device communication.

- Enables customer-controlled proxy sessions for secure device communication
- Increases flexibility for network configuration using the CV SRA application
- Maintains strict security requirements for network equipment access

Supported devices and requirements for CV SRA HTTP(S) proxy support

The HTTP(S) proxy feature is specifically for customers installing IE3x00 switches.

- Proxy configuration is supported only in the CV SRA application.
- Device communication through the proxy requires IDA version 17.14.1 or above.

Configure a network device using proxy URL

Provides instructions for adding proxy configuration to a network device by entering the proxy URL directly. Use this procedure when you want to specify the full proxy URL in standard format.

Add proxy configuration for a network device using the Proxy URL method.

Use this method when you wish to enter a complete proxy URL in standard format.

Before you begin

Complete the initial device add workflow and select the URL method.

Procedure

1. Enter the **URL** for the device using this format: `http(s)://username:password@server:port`
2. Click **Add Network Device** located in the bottom right corner of the screen.

   Note

   If the configuration fails, the reason is posted on a banner at the top of the screen.

   You are notified that the device is successfully added.

The device is added with proxy support using your specified URL.

Configure a network device using proxy form

Provides instructions for adding proxy configuration for a network device using the Proxy Form input method.

Select this path if you prefer entering proxy details in separate fields.

Before you begin

- Complete the initial device add workflow and select the Form method.

Procedure

1. Depending on your requirements, choose either `http://` or `https://` from the drop-down list.
2. Enter the **Server IP address** .
3. Enter the **Port number** .
4. (Optional) Enter the **Username** and **Password** .
5. Click **Add Network Device** located in the bottom right corner of the screen.

   You are notified that the device is successfully added.

The device is added with proxy support through the form entry.

Multi-VLAN and static IP capabilities

Explains multi-VLAN and static IP capabilities in CV SRA.

A multi-VLAN and static IP capability is a network configuration feature that enables network segmentation and allows the CV SRA agent to access multiple VLANs on IE switches without requiring L2NAT or similar techniques.

- Enables network segmentation by allowing the CV SRA agent to be mapped to specific VLANs on customer-managed devices.
- Relies on the existing device VLAN configuration without requiring device-side changes.
- Allows the CV SRA agent to access multiple VLANs on IE switches without the need for L2NAT or similar techniques.

Additional reference information

Installing the CV SRA agent on a customer-managed IE3x00 is almost identical to installation on IoT OD-managed IR1101 or IR1800 devices, with one exception: for the IE switch, you must specify the target VLAN for the CV SRA agent's Ethernet interface. This chosen VLAN must provide DHCP, a default route to the internet and cloud, and DNS resolution. Multi-VLAN and static IP assignments are only supported on IE switches, not on IR routers.

Requirement: VLAN configuration for CV SRA

Outlines the requirements for manually configuring VLANs and selecting appropriate network services to ensure successful deployment of the CV SRA agent.

To ensure effective deployment and operation of the CV SRA agent, follow these requirements and guidelines:

- You must manually configure all required VLANs on the IE3x00 device using the CLI or a DNAC template before deploying the CV SRA agent. The CV SRA agent does not configure VLANs automatically.
- When deploying the CV SRA agent, select the appropriate VLAN for the agent interface. The selected VLAN must provide:
  - DHCP services to allocate an IP address to the CV SRA agent interface, or if no DHCP server is present, configure a static IP address for the CV SRA agent,
  - a default route for the CV SRA agent to access the internet and IoT OD cloud, and
  - DNS services to resolve IoT OD and other hostnames.
- You can use up to 10 VLANs per device, including the initial VLAN and up to 9 additional VLANs.
- Multi-VLAN and static IP assignments are supported only on IE switches; IR routers do not support these features.

VLAN configuration field descriptions

Explains the fields and controls available on the VLAN Configuration screen, including management and additional VLAN options, limits, and actions for configuring VLANs.

This section provides an overview of the VLAN Configuration screen, describing each field, control, and available options.

Table 39: VLAN configuration screen fields and controls

Section	Field/control	Description	Options/notes
Management Interface	VLAN ID	Enter or view the VLAN ID for device management.	Default: `1`

Section	Field/control	Description	Options/notes
Management Interface	IP Assignment	Select IP assignment mode for the management VLAN.	`Dynamic IP (DHCP)` , `Static IP`
Additional VLANs	Enable Additional VLAN Configurations	Toggle to enable configuration of up to 9 additional VLANs.	ON/OFF toggle
Additional VLANs	Add VLAN	Add a new VLAN entry for additional segmentation.	`+ Add VLAN` button
Additional VLANs	VLAN Table	Displays all configured additional VLANs.	Columns: `VLAN ID` , `IP Assignment` , `IP/Prefix`
Additional VLANs	Delete Action	Remove an unwanted VLAN entry from the list.	Delete icon/action per VLAN row
Limits	Max VLANs	Maximum number of VLANs supported (Management + Additional).	Up to 10 (`1 Management + 9 Additional`)
General	Save/Apply	Apply changes after configuring VLAN settings.	Save or Apply button (not shown in image)

Configure a new CV SRA network device for VLAN support with dynamic IP addresses

Provides instructions for adding a new network device in CV SRA for VLAN support using dynamic IP addressing.

Add a new network device in CV SRA for VLAN support using dynamic IP addressing.

Use this procedure when integrating a new device with multiple VLANs and enabling CV SRA agent deployment using DHCP.

Before you begin

- Verify that all target VLANs are already configured on the IE3x00 device.
- Confirm the target VLAN provides DHCP services, internet access, and DNS.

Procedure

1. From the **Services** panel, choose **SRA** > **System Management** > **Network Devices**.
2. Click **Add Network Device** .
3. Choose the **Select from list (recommended)** option and select the **Network Device** you want to add and install the CV SRA agent.
4. Click **Next** to open the **Network Device Details** screen.

The device is ready for management VLAN configuration.

Configure management VLAN with dynamic IP assignment

Provides instructions for assigning the management VLAN for the CV SRA agent using dynamic IP (DHCP) addressing, enabling automatic assignment of management IP addresses when the VLAN provides DHCP service.

Assign the management VLAN for the CV SRA agent using dynamic IP (DHCP) addressing.

Use when the target VLAN provides DHCP and automatic IP assignment is preferred.

Before you begin

Ensure that the management VLAN has DHCP enabled.

Procedure

1. In the Management VLAN field, enter the desired VLAN ID or use the default (1).

   Note

   The default VLAN ID is 1. Valid VLAN ID range is 1-4093.

2. For IP Assignment, choose Dynamic IP (default setting).

The CV SRA agent receives its management IP address through DHCP on the designated VLAN.

Configure management VLAN with static IP assignment

Provides instructions for assigning a static IP address to the management VLAN for the CV SRA agent.

Use this method when the management VLAN does not provide DHCP, or when a fixed IP address is required.

Before you begin

Ensure you have the required static IP parameters for the management VLAN.

Procedure

1. From the **IP Assignment** drop-down list, choose **Static IP** .
2. Enter and confirm the following:
   - **IP Address**

- **Subnet Mask** (use Classless Inter-Domain Routing notation, range 0-32, format:

```
/Prefix
```

)

- **DNS**
- **Default Gateway IP**

The CV SRA agent uses the specified static IP details for the management VLAN.

Add additional VLAN ids and IP assignments

Provides instructions for adding up to ten VLANs per device, each with dynamic or static IP assignment for the CV SRA agent.

Use this procedure to expand access and support for additional segmented OT assets as needed.

Before you begin

Verify all necessary VLANs are set up on the IE3x00 and support the required IP assignment method.

Procedure

---

1. Click **Enable Additional VLAN Configurations** .
2. Follow the steps for adding either a **VLAN** with a **Dynamic IP Address** or **Static IP Address** .
3. Finish the VLAN configuration by clicking **Add Network Device** .

The device is configured with access to multiple VLANs as required, each with appropriate DHCP or static assignment.

Modify the VLAN configuration on a network device

Provides instructions to update the VLAN configuration of an existing CV SRA-managed network device, including adding, editing, or removing VLANs and their assignments.

Use this task to update the VLAN configuration of a CV SRA-managed network device, including adding, editing, or removing VLANs and their assignment details.

Use when network segmentation changes, or when updating IP assignment for operational needs.

Before you begin

Confirm which VLANs and IP info must be changed and ensure the device supports the new configuration.

Procedure

---

1. From the **Services** menu, choose **SRA Service** > **System Management** > **Network Devices**.
2. Choose the **Device name** to be modified.
3. In the **Additional Configuration** section of the **Network Device Details** screen, click **View Details** . The **Additional Configuration** panel opens.
4. In the **Edit Additional Configuration** screen, perform one of the following:
   - Click **VLAN** to add a new VLAN(s) if none are configured.

- Add, modify, or delete appropriate **VLAN parameters** .

5. Click **Apply and Reinstall** .
6. Click **Reinstall** in the reinstall app confirmation prompt.

   Depending on the network, the reinstallation process can take several minutes.

The network device now operates with the new or modified VLAN configuration in CV SRA.

Install and configure CV SRA agent on a device

Provides instructions for installing and configuring an CV SRA agent on a selected network device.

Use this task to enable CV SRA on a selected network device.

Before you begin

- Ensure you are signed in as an SRA System Admin user.
- Identify the network device for agent installation.

Procedure

---

1. Click **Quick Wizard**.
2. Select **Install SRA agent** and click **Start Configuration** .
3. In the **Install SRA agent** screen, select an existing **Network Device** from the list and click **Next** . The **Advanced Configuration** screen opens.
4. The **Advanced Configuration** screen opens. The screen differs based on the selected device (router or switch).

   Note

   For information about router or switch configuration, refer to CV SRA HTTP proxy support on page 122 or Multi-VLAN and static IP capabilities on page 123.

5. After configuring the network device, click **Deploy** . It may take 3-5 minutes to enable the device.

The CV SRA agent is installed and enabled on the selected device.

Use the CV SRA Quick Wizard

The CV SRA Quick Wizard helps you install an agent or connect to a remote asset.

Choose **Quick Wizard** to start either of these independent workflows:

- Install a CV SRA agent on a network device.
- Connect a network device to a remote asset and configure an access method.

Edit configuration details for onboarded devices

Provides instructions for modifying device and advanced settings for onboarded devices.

Use this task to edit device or advanced settings for onboarded devices and apply the changes using the updated CLI commands.

Any changes to device or advanced settings require regeneration and manual application of new CLI commands.

Before you begin

- Confirm you have administrative access to the device.

Procedure

1. On the **System Management** page, click **Network Device Details** > **Edit**.
2. In the **Edit Network Device Details** window, edit the required details, and click **Save**.
3. To edit network details such as proxy URL and VLAN configurations:
   a) In the **Additional Configuration** section, click **View Details**.
   b) Click **Edit**, modify the desired settings, and click **Save**.

Based on your input, CLI commands are updated. You can copy these commands under the **CLI Restart Commands** section to run on the device's console.

Multiple VRFs on CV SRA routers

Use multiple virtual routing and forwarding (VRF) instances to reach assets through a CV SRA router.

A router in CV SRA has a required management VRF and can have up to three additional VRFs. Multiple VRFs let you associate an asset with the routing instance through which the router can reach it. This capability applies to routers, not switches.

When adding or editing an asset, select the asset VRF from the VRFs configured on its router. The same IP address can be associated with different VRFs, but the same IP address and VRF combination cannot be added twice to one router. Any number of assets can use a configured VRF.

After you add an additional VRF in the UI, the generated router CLI configuration changes. Copy and apply the updated CLI configuration on that router; saving the UI settings alone does not configure the router.

When you clone assets to another network device, all cloned assets are associated with the target device's management VRF. The clone does not preserve their source VRF associations. Review and change those associations on the target device as needed.

Table 40: Feature History

Feature	Release	Feature description
Multiple VRFs on CV SRA routers	September 2026 release	Configure up to three additional VRFs on a router and select the VRF used to reach each asset.

Configure additional VRFs on a router

Add routing instances for assets that are not reachable through the router's management VRF.

Configure up to three additional VRFs on a router in CV SRA.

Before you begin

Onboard the router and configure its mandatory management VRF. Identify the VRF names and the assets or asset subnets reachable through each VRF.

Procedure

1. In CV SRA, open **System Management** and select the router.
2. Edit the router configuration and add the required additional VRFs.

   You can configure a maximum of four VRFs in total: the management VRF and up to three additional VRFs.
3. Save the router configuration.

   The generated CLI configuration includes commands for the additional VRFs and their access networks.
4. Copy the updated CLI configuration and apply it to the selected router.

   Saving the settings in the UI does not apply the generated commands to the router.
5. Verify that the router can reach the assets through the configured VRFs.

What to do next

When adding or editing assets or asset subnets, select the VRF through which the router can reach them. The asset VRF choices become available after the network device has connected to the cloud.

CV SRA agent connectivity modes

Explains the different CV SRA agent connectivity modes and how they govern secure communication between the CV SRA agent and the IoT Operations Dashboard.

CV SRA agent connectivity mode is the operational state that

- Determines how the CV SRA agent establishes a secure connection with the IoT Operations Dashboard.
- Starts in recovery mode during initial device onboarding.
- Switches to rotation mode after successful connection.

Recovery and rotation modes

CV SRA agent supports two connectivity modes:

- **Recovery Mode**: When a device is onboarded for the first time, it enters recovery mode for 48 hours. During this period, the CV SRA agent uses the recovery key to establish its initial secure connection to Cisco IoT Operations Dashboard. Recovery mode also lets the device restore connectivity if reconnection is needed.
- **Rotation Mode**: After the CV SRA agent successfully connects to the IoT Operations Dashboard using the recovery key, it transitions to rotation mode. In this mode, the CV SRA agent periodically rotates or renews its security credentials (keys) to maintain secure communication. If the connection using the rotated key fails, you can switch the Agent back to recovery mode so it can reconnect by using the recovery key.

You can manually switch the CV SRA agent back to recovery mode by clicking the three dots (…) next to the **View Deployment Commands** area in the **Deployment Details** section in the management interface.

Operational technology (OT) assets

Explains OT assets and their importance in IIoT network.

An OT asset is a physical device such as a PLC, sensor, or industrial controller that directly monitors or manipulates physical industrial processes.

- Represents critical physical endpoints within an IIoT network.
- Requires robust, authenticated access controls to ensure operational integrity and security.

Add OT assets to a network device

Streamline device management by associating additional OT assets to network devices through a manual process.

Use this procedure to manually add an asset for a device.

This task lets you add an OT asset to a network device.

For routers with multiple VRFs, choose the VRF through which the router can reach the asset. The VRF choices are available after the network device has connected to the cloud.

Procedure

1. From the **System Management** page, choose a **Network Device**.
2. From the **Network Device Details** page, click **Add Asset**.
3. On the **Add Asset** page, choose one of the following options:
   - **Select from list (Recommended)**
   - **Manual entry**
4. After you choose the option, enter the asset name, IP address or host name, and description. If the router has multiple VRFs, select the VRF through which it can reach the asset. Click **Add**.

   Note

   To access this asset using the CV SRA Plus protocol, you must enter the IP address only. Entering the hostname will cause the CV SRA Plus connection to fail.

   For a given router, an IP address and VRF combination must be unique. You can use the same IP address in a different VRF.

The asset is associated with the network device.

Connect a network device to a remote asset

Provides instructions for connecting a network device to a remote asset through Cyber Vision Secure Remote Access (CV SRA) by specifying the asset details, access method, and assigning access control groups as needed.

Establish secure remote connectivity between a selected network device and a remote asset through the CV SRA platform.

Perform this task when you need to enable managed remote access for a network device by defining connection and access method parameters. The configuration is typically required for secure administration or integration with third-party assets.

Before you begin

- Ensure you are logged in as an SRA System Admin user.
- Confirm that required access control groups exist.

Procedure

1. Click **Quick Wizard** in the CV SRA platform.
2. Click **Connect to Asset**.
3. Select the desired network device from the available list.
4. Specify the asset details:
5. Choose an access method for the asset and provide the necessary connection information.
6. (Optional) Assign the device to an access control group.
7. Test the configuration to verify connectivity to the asset.
8. Launch a remote session to confirm successful connection.
9. Complete the configuration process.

The remote asset is now configured with the specified access method. The newly added network device is listed in the network device table under System Management.

What to do next

(Optional) Review the newly-configured device entry to verify correct connectivity and group assignment.

Bulk configuration cloning

Enable efficient replication of CV SRA configurations by copying assets and access methods from a source device to multiple target devices using bulk configuration clones.

A bulk configuration clone is a network automation feature that enables you to efficiently replicate CV SRA configurations by copying assets and access methods from a source device to multiple target devices.

- Replicates CV SRA configurations from one device to many devices.
- Copies assets and access methods efficiently across selected targets.
- Ensures operational consistency by transferring details such as IP addresses, URLs, and credentials.

Requirements and behavior when cloning assets and remote sessions

When performing a bulk configuration clone, consider the following requirements and behaviors:

- Each asset must include at least one remote session; otherwise, the asset will not be copied during cloning.
- If a target device already contains a remote session with the same name as a cloned session, the system automatically appends "-copy" (for example, "Ubuntu-Server-copy 1") to the new session name to avoid conflicts.
- If the remote sessions in the source device are associated with access control groups, the same associations will be made for the cloned remote sessions in the target devices. This means that the users who had access to the remote sessions in the source device will automatically have access to the cloned remote sessions in the target device after cloning.
- All cloned assets are associated with the target device's management VRF. Their source VRF associations are not preserved, even if matching additional VRFs exist on the target device. Review the asset VRF assignments after cloning.

Suppose you have configured a source device with all required CV SRA assets and remote sessions. Using the bulk configuration clone feature, you can copy these settings to multiple target devices, ensuring consistency and saving time. If a target already has a session with the same name, the system will rename the cloned session to prevent conflicts.

Clone the session configurations

Provides instructions for copying asset and remote session configurations from a source network device to multiple target devices for faster setup and to ensure consistent configuration.

Copy asset and remote session configurations from a source network device to multiple target devices for faster setup and consistent configuration.

Use this task in Cisco IoT Operations Dashboard when you want to replicate CV SRA assets and remote sessions to other devices in your network.

Before you begin

- Ensure you have SRA System Admin role access.
- Identify the source network device with the desired configuration.

Procedure

1. Log in to the Cisco IoT Operations Dashboard as a user with SRA System Admin role.
2. Choose **SRA** > **System Management**.
3. On the **System Management** pane, select the network device whose configuration you want to clone, and then select **Clone Remote Session Configuration** in the **Action** column.
4. On the **Clone Remote Session Configuration** page, select the remote sessions you want to clone, and then click **Next**.
5. In the **Assign Access Control Group** area, choose one of the following options:
   - **Add all cloned remote sessions to all the original access control groups** - Use this option if you want to keep the cloned remote sessions associated with the original access control groups.
   - **Do not add any cloned remote sessions to the original access control groups** - Use this option if you do not want to associate the cloned remote sessions with the original access control groups. In this case, you can associate the cloned remote sessions with different access control groups.
6. Click **Next**.
7. In the **Choose Target Network Devices** area, select the target devices from the list.

   The remote sessions and the assets are copied to these devices.

   All cloned assets are assigned to each target device's management VRF, regardless of their source VRF. Review the warning before continuing.
8. Click **Done**.

   You receive a success message indicating that cloning of remote sessions and assets is initiated.

The selected sessions and assets are cloned from the source device to the chosen target devices. You receive a success message indicating that the process has started.

What to do next

Review cloned configurations on each target device and update session details or access control groups if specific values are required.

If assets must use an additional VRF on a target router, edit their VRF associations after cloning.

View cloning history

Provides instructions for reviewing details of all bulk configuration cloning activities performed on the Cisco IoT Operations Dashboard.

Review details of all bulk configuration cloning activities performed on the Cisco IoT Operations Dashboard.

Use this task to track and audit session and asset cloning actions, including the source network device, the user who initiated the cloning, the cloned remote sessions, the cloned assets, the target devices, and the date and time of the cloning.

Before you begin

- Ensure you have SRA System Admin role access.

Procedure

1. Log in to the Cisco IoT Operations Dashboard as a user with SRA System Admin role.
2. Choose **SRA** > **System Management**.
3. On the **SRA** pane, select **View Cloning History** from the **More Actions** drop-down list.
4. To view the cloning history for a specific period, select start and end dates in the box preceding the Search Table.

   The cloning history specific to the given period appears. The history may include one or more cloning activities.
5. To get the details of a specific cloning activity, click the associated job name.

you can view full details of current and past cloning activities, including source device, cloned items, initiating user, target devices, and the date and time of each cloning event.

What to do next

Use the history information to verify cloning activity or troubleshoot configuration changes if needed.

Remove all assets and access methods from network devices

Provides instructions for removing all assets and access methods from one or more network devices in a single action.

Remove all assets and access methods from one or more network devices in a single action.

Use this task when you need to reset the configuration of selected network devices on the Cisco IoT Operations Dashboard by deleting their CV SRA asset and access information.

Before you begin

- Ensure you have SRA System Admin role access.

Procedure

1. Log in to the Cisco IoT Operations Dashboard as a user with SRA System Admin role.
2. Choose **SRA** > **System Management**.
3. On the **System Management** pane, select the network devices whose configuration you want to clear, and then select **Clear All Assets and Access Methods** from **More Actions**.
4. On the confirmation window, click **Delete**.

The configurations of the selected network devices are cleared.

Access control groups

Define and manage secure remote access for groups of SRA users to specific remote assets.

An access control group is a security feature that provides administrators with the ability to define and manage secure remote access for groups of SRA users to specific remote assets.

- Provides granular control over who can access what and when.
- Enables creation of groups and assignment of permissions for remote access.
- Supports multiple access control group types for flexible access management.

Types of access control groups

There are three types of access control groups you can configure:

- **Always Active** – users in this group can always access remote sessions defined in this group.
- **Scheduled Access** – users in the group can log in to the IoT Operations Dashboard and access the remote sessions during the configured time window. No approvals required.
- **Request Access** – users must explicitly request access to the remote assets, and they can access the assets only after the Access manager (approver) approves the requests.

Request access in CV SRA

Describes how the Request Access feature in Cyber Vision Secure Remote Access (CV SRA) enforces strict permissions for remote asset connectivity, ensuring that every session is individually requested, reviewed, and approved within the IoT Operations Dashboard to strengthen security controls.

Request Access is a feature in CV SRA that requires users to explicitly submit a request to access remote assets through the IoT Operations Dashboard.

- Users must submit an access request before starting a remote session.
- An Access Manager (approver) must review and approve each request.
- No access is allowed until approval is granted, enhancing security and auditability.

A user needs to access a remote OT device for troubleshooting. The user submits a request through the IoT Operations Dashboard. The Access Manager receives a notification, reviews the request, and, if appropriate, approves it. Only after approval does the user gain access to the remote asset.

How remote session access requests work

Describes how remote session access requests enable administrators to control who can access OT assets and when, using access groups, roles, and approval workflows.

Remote session access requests provide a secure, policy-driven method for controlling access to OT assets through the IoT Operations Dashboard.

Summary

The following actors and components participate in the remote session access request process:

- **SRA System Admin** or **SRA Access Admin**: Creates and configures access groups with request controls.
- **Remote access user**: Requests access to the asset through the dashboard.
- **SRA Access Manager** (or other approvers): Reviews and approves or rejects access requests.

- **IoT Operations Dashboard**: Hosts the user interfaces for all actions.

This process ensures that only authorized users can access assets, with all actions subject to approval and audit.

Workflow

These stages describe how remote session access requests are processed:

1. The SRA System Admin or SRA Access Admin logs in to the IoT Operations Dashboard and creates an access control group with the Request Access feature enabled. At least one SRA user and one asset must be assigned to the group.
2. The remote access user logs in and requests access to an asset within an enabled group.
3. The SRA Access Manager (or other permitted roles such as SRA System Admin, SRA Access Admin, or any role with Access Approver permission) reviews and approves (or rejects) the access request.
4. Upon approval, the remote access user gains access to the asset for the specified time period.

Result

The system enforces policy-driven, auditable, and time-bound access for OT assets, minimizing the risk of unauthorized usage.

Create access control groups for scheduled or request access

Provides instructions for creating a new access control group in CV SRA, allowing you to define which users can access specific remote assets and under what conditions.

Creating access control groups in CV SRA enables you to control remote access by grouping users and assets under defined access conditions.

Access control groups allow administrators to manage remote access for users and assets, supporting both scheduled and request-based workflows. Groups can be temporarily disabled during device upgrades, repairs, or other periods when access should be restricted.

Before you begin

- You must be an SRA System Admin or SRA Access Admin.

Procedure

1. From the **Service** panel, choose **SRA** > **Access Management**.
2. On the **Access Management** page, review the **Access Control Groups** table to refer to the available groups and their details, including group names and the number of users assigned.
3. Click **Add Group** and enter a name and a description.
4. Select the group type:
   - **Request Access**: Use request-based workflow for access.
   - **Scheduled Access**: Set the time zone, start date/time, and end date/time for scheduled access.
5. (Optional) Click the **Group Enabled** toggle switch to disable the group as needed. When disabled, users cannot access remote sessions in the group.
6. (Optional) Click the **Enforce Inline (SSH/RDP/VNC) Recording** toggle switch if you want to record remote sessions accessed by group members, and click **Next**.
7. (Optional) In the **Assign Users** section, select the users you want to add to the group and click **Next**. These users will be authorized to access the remote sessions assigned to the group.
8. (Optional) In the **Assign Remote Sessions** section, choose the assets you want the group's users to access and click **Next**.

9. Review all settings and confirm to create the access control group.

A new access control group is created with your chosen settings. Group members can access assigned remote sessions according to scheduled or request access conditions. If inline recording is enabled, remote sessions are automatically recorded.

What to do next

For request access groups, assign approvers who will handle access requests from group members.

Add users to an access control group

Provides instructions for adding users to an existing access control group to grant them remote access permissions.

Add users to an existing access control group to grant them remote access permissions.

Group membership can be updated after creation to provide selected users with the necessary access permissions.

Before you begin

- Ensure you have either an SRA System Admin or SRA Access Admin role.

Procedure

1. From the **Service** panel, select **SRA > Access Management**.
2. Select the desired access control group.
3. In the **Users** tab, click **Add Users**.
4. Select the users to add to the group, then click **Save**.
   - If the required user is not listed, they must be added through CV SRA System Management. Contact your SRA System Admin for assistance.

The selected users become members of the access control group.

Assign assets to an access control group

Provides instructions for assigning asset access to a user group, allowing them to view remote sessions for specific assets in the IoT Operations Dashboard.

Use this task to define asset access for group members. After assets are assigned, users can view remote sessions in the IoT Operations Dashboard (connection rights may depend on further approval).

Procedure

1. From the left **Service** panel, choose **SRA > Access Management**.
2. Choose a **group** from the **Access Management** page.
3. Click the **Asset Access** tab and click **Add Asset Access** .
4. Choose **Assets** from the list by clicking the **checkbox** next to the asset.

Group members can now view the designated remote sessions for the assigned assets in the IoT Operations Dashboard. They cannot connect to the remote sessions until further approval is granted, according to group policy.

What to do next

You can optionally assign a specific approver for the access request. If approvers are assigned, they will be responsible for reviewing and approving the request. If no approver is assigned, all admins (both SRA Access Admins and SRA System Admins) in your organization receives email notifications, and any of them can review and approve the request.

Assign approvers to an access control group

Provides instructions for assigning approvers who review and approve requests for access in "Request Access" groups.

This process is essential for groups configured with the Request Access type, ensuring requests are explicitly approved.

Before you begin

- The approver must have the **Access Admin** or **Access Manager** role.

Procedure

1. From the **Service** panel, choose **SRA** > **Access Management**.
2. On the **Access Management** page, click the name of the access group created for the **Request Access** feature.
3. In the **Access Approvers** section, click **Add access approver**.
4. In the **Add access approver** window, select an approver from the available list, and click **Save**.

The selected approvers receive an email notification when a member of the group requests access to a session. Even if you are a tenant admin, you will not receive the email notification unless you are explicitly selected as an approver. The approvers can log in to the IoT Operations Dashboard and manage the access requests.

Scheduled access in CV SRA

Explains how scheduled access features in CV SRA enable designated user groups to initiate remote sessions during pre-configured time windows.

Scheduled access is a feature in CV SRA that enables users within a designated group to log in to the IoT Operations Dashboard and initiate remote sessions during a pre-configured time window.

- Access is limited to the configured time window.
- Only users in the specified group are eligible.
- No manual approvals are needed for each session during the allowed period.
- Enhances operational efficiency by automating access control.

If scheduled access is set from 9:00 AM to 5:00 PM, group members can log in and access equipment remotely through the IoT Operations Dashboard at any time within this interval, without waiting for additional approval steps.

Send invitations to group members for a scheduled meeting

Provides instructions to notify group members of upcoming scheduled meetings by email invitation.

Invite some or all group members to participate in scheduled remote access sessions.

Before you begin

- You must be an SRA System Admin or SRA Access Admin.

Procedure

1. Go to **SRA** > **Access Management**.
2. Select a group that has the meeting scheduled.
3. In the **Actions** column, choose **Send Invitation** from the drop-down list.
4. In the **Select members for invitation notification** window, select the group members to whom you want to send the invitation.
5. After choosing members, click **Send**.

Each member receives an email with meeting information.

Schedule statuses

Describes the current access state for each session and indicates when and how access is available.

The **Schedule** column in the **Access Control Groups** page indicates the current access state for a remote session.

- Determines when remote access is available.
- Distinguishes between ongoing, scheduled, active, and expired sessions.

When you go to **SRA** > **Access Management** > **Access Control Groups**, the **Schedule** column lists the four possible statuses for a remote session.

- **Always Active**: No specific time for access; access is always available.
- **Scheduled**: A specific time span for access to a session has been scheduled for a future date.
- **Active**: The scheduled time for access to a session is currently in progress.
- **Schedule Expired**: The scheduled time for access to a session has expired.

Note

If a scheduled session is listed as **Schedule Expired**, you can update that expired session for a future date without creating a new scheduled session.

How CV SRA Plus remote access works

Describes how administrators configure CV SRA Plus access and how users install the app, connect to a remote session, and use native applications to access an OT asset.

CV SRA Plus provides client-based access for sessions that require native engineering or diagnostic applications, large file transfers, or other capabilities beyond a browser-based session.

The process requires an administrator to configure a CV SRA Plus access method and assign the appropriate users and assets before a user can connect.

Summary

The following actors and components participate in the CV SRA Plus remote access process:

- SRA System Admin or another authorized administrator: Configures the access method, access group, asset, and user permissions.

- SRA Plus App: Establishes the client-based connection that enables native applications to access the remote asset.
- Remote access user: Installs the app, connects to an available session, and performs authorized work on the asset.

Workflow

These stages describe how CV SRA Plus remote access becomes available and how a user connects:

1. An authorized administrator adds the asset and configures a CV SRA Plus access method with the required protocol and port settings.
2. The administrator assigns the asset and the remote access user to an access control group that permits the user to access the session.
3. The remote access user meets the CV SRA Plus prerequisites and installs the CV SRA Plus App.
4. The user opens **Cyber Vision SRA** > **Remote Sessions** and locates the assigned asset.
   - For request-based access, the user submits a request and waits for an authorized approver to approve it.
   - For scheduled access, the user waits until the session is available within its scheduled time window.
5. When the session is available, the user selects **Connect**. The CV SRA Plus App establishes the configured connection and enables the user to use the supported native application or engineering tool.
6. The user performs authorized work during the session's permitted access period and ends the session after completing the work.

Result

The user accesses the assigned OT asset through the configured CV SRA Plus method for the permitted session period.

Prerequisites for using CV SRA Plus

Outlines the system, compatibility, licensing, and installation requirements you must meet before using the CV SRA Plus App.

Before using the CV SRA Plus App, ensure the following requirements are met.

- **Supported operating system:** You must use a supported operating system. The CV SRA Plus App currently supports Windows 10 (minimum version) only.
- **Application compatibility:** Do not use the CV SRA Plus App with other VPN clients running in active mode on your computer.
- **Antivirus configuration:** Verify your virus scanner does not block the CV SRA Plus application.
- **Licensing:** CV SRA Plus features are premium and require an Advantage license on IoT OD.
- **Feature activation:** CV SRA Plus must be activated for your organization on IoT OD. Contact Cisco if you are unsure of your activation status.

Download and install the CV SRA Plus application

Provides instructions for downloading and installing the CV SRA Plus user application to enable secure device access.

Download and set up the CV SRA Plus application so you can securely access Cisco devices using the CV SRA Plus method.

Use this task when you need to connect to Cisco devices through the CV SRA Plus access method.

Before you begin

- Ensure you meet all prerequisites for CV SRA Plus usage.

- Verify that the CV SRA agent is installed on a managed Cisco device.
- Confirm you have access to a remote session with the CV SRA Plus access method configured on IoT OD.

Procedure

1. From the **CV SRA** menu, choose **Remote Sessions**.
2. Click **Download SRA Plus App**.
3. From the displayed list of different versions of the SRA plus app, download the version that you want to use.
4. When the CV SRA Plus App Wizard opens, follow the on-screen instructions to complete the installation.

The CV SRA Plus application is downloaded and installed on your computer, ready for configuration.

What to do next

Configure the CV SRA Plus application to begin secure device access as needed.

Duo integration with CV SRA Plus

Enable automated device posture checks with Duo integration to ensure only compliant devices access critical OT assets.

Secure OT access with Duo device posture checks is a security approach that enforces device compliance before granting access to Operational Technology (OT) assets.

- Automates system posture checks using Duo integration.
- Ensures devices meet security requirements prior to OT access.
- Protects critical OT assets such as PLC, HMI, and robotics software from unauthorized access and lateral movement.

Risks of weak security posture and benefits of Duo integration

Standard workstations used for diverse tasks are vulnerable to unauthorized access if not properly managed. Weak security posture can expose sensitive data, create entry points for lateral movement, and endanger critical OT assets.

- Exposure of sensitive data
- Entry points for lateral movement into remote networks
- Endangerment of critical OT assets (PLCs, HMIs, robotics software)

To mitigate these risks, integrate Duo to enforce device posture checks before granting access to OT assets.

1. Integrate Duo with your access management system.
2. Configure automated posture checks for devices.
3. Grant access to OT assets only if device meets security requirements.

For instance, when a user attempts to access a remote PLC through the CV SRA Plus method, Duo verifies that the workstation has up-to-date security patches and endpoint protection. Only compliant devices are allowed to connect, reducing the risk of unauthorized access to critical OT systems.

How Duo integration works with CV SRA Plus

Duo integration with CV SRA Plus enforces a device security check before allowing remote access to OT assets, ensuring that only compliant devices are granted access.

Duo integration with CV SRA Plus ensures that only devices meeting security posture requirements can access sensitive OT assets remotely.

- Only devices that satisfy Duo security posture policies can access sensitive OT assets using CV SRA Plus.

Summary

The following are the key components and actors involved in the Duo integration process with CV SRA Plus:

- SRA System Admin: Configures Duo integration with CV SRA Plus and manages policy requirements.
- Duo administrator: Maintains Duo settings and policies.
- Duo authentication service: Assesses the security posture of the user's device and provides access status.
- End user: Attempts to access remote OT assets through CV SRA Plus.

This process ensures that only compliant devices are granted access to OT assets through CV SRA Plus by enforcing Duo security posture checks.

Workflow

These stages describe how Duo integration with CV SRA Plus enforces device security posture before granting access to OT assets:

1. The SRA System Admin sets up the Duo integration and policies.
2. The end user activates CV SRA Plus access for a remote session.
3. Duo evaluates the user's device against defined security posture requirements.
    - If the device passes, the Duo indicator turns green and enables CV SRA Plus connectivity.
    - If the device fails, the user receives an error message, and access is denied.
4. Users can review Duo session details for compliance feedback.
5. If Duo integration is not enabled, posture checks do not occur, but CV SRA Plus access remains available (without posture validation).

Configure Duo external integration with CV SRA Plus

Provides instructions for setting up Duo integration within CV SRA Plus to enable device posture verification for OT asset access.

Enable posture-based device security checks for users accessing OT assets through CV SRA Plus by integrating Duo.

Use this configuration when you want CV SRA Plus to enforce device posture checks for remote access. Note that Duo integration for user login and SSO follows a separate process.

Before you begin

- Ensure you have a Duo Admin account and the unique URL for your Duo environment.
- Confirm you have access to the CV SRA Plus instance as a System Admin.
- Verify that Duo policies exist to enforce security posture checks for remote OT asset access.
- The integration process applies only to CV SRA Plus sessions—not to system login.

- To evaluate the solution, you may request a free 30-day Duo trial compatible with IoT OD at Duo.com .

Procedure

1. In your Duo Admin account, create a new Web SDK application for CV SRA Plus.
   - Select **Applications > Protect an Application**.
   - Choose **Web SDK** and select **Protect**.
2. In the **Duo Admin** dashboard, rename the Web SDK application to "CV SRA Plus".
   - Go to **Applications > Web SDK**.
   - Under **Settings**, update the Name field to "CV SRA Plus".
   - Click **Save**.
3. Locate the integration key, secret key, and API hostname for the CV SRA Plus application in Duo.
4. In the CV SRA Plus admin console, enter the Duo integration key, secret key, and API hostname in the **Duo external integration** section.
5. Apply and save the changes to complete the integration.

Duo integration with CV SRA Plus is enabled. Device posture verification is now enforced for all users accessing OT assets through CV SRA Plus.

What to do next

- Test the integration by initiating a CV SRA Plus session and confirming that Duo posture checks are applied as expected.
- Adjust Duo policies or CV SRA Plus settings as needed.

Configure CV SRA Plus policies in Duo

Provides instructions for configuring a Duo policy that enforces device posture criteria for CV SRA Plus access.

These policies determine which devices can access OT assets through CV SRA Plus.

Before you begin

- Familiarize yourself with Duo policy documentation as needed.

Procedure

1. In Duo, go to **Policies** .
2. In **Custom Policies** , click **New Policy** .
3. Enter a policy name.
4. Configure these policy settings for CV SRA Plus users:
   - **Authentication Policy** : Select **Enforce 2FA** (to enable device posture checks).
   - **User Location** : Allow chosen countries (**No Action**), deny all others (**Deny Access**).

- **Device Health Application** : For Windows, require the app, firewall, and system password. Block access if an endpoint security agent is not running.
- **Operating Systems** : Allow only **Windows devices** .
- **Networks** > **Authorized Networks**: In **Allow access without 2FA from these networks**, enter **0.0.0.0-255.255.255.255** to disable 2FA for CV SRA Plus.
- Click **Save Policy** .

5. Go to **Applications** in Duo and select the **Web SDK** application for CV SRA Plus.
6. In the Policy section, click **Apply a policy to all users** .
7. Select the new **Policy** from the drop-down menu.
8. Click **Apply Policy** .
9. Click **Save** at the bottom of the page.

Devices are now evaluated against these policies during CV SRA Plus posture checks.

Enable Duo integration in CV SRA

Provides instructions for enabling and connecting the Duo integration within IoT OD for CV SRA Plus.

Link CV SRA Plus with Duo to enforce security posture using Duo integration.

Before you begin

- Have Duo Client ID, Client Secret, and API Host information ready from the Web SDK application.

Procedure

1. In the left **Service** panel, navigate to **SRA** > **System Management** > **External Integrations**.
2. Click **Add External Integration** to open the Add External Integration panel.
3. Choose **Duo** from the Integration **Type** drop-down list.
4. Enter an appropriate name and a description.

> **Note**
>
> Switch back to Duo and choose **Applications** > **Details** to retrieve the Client ID, Client Secret, and API Hostname. Beside each field, click Copy (the lettering switches to Copied), then switch back to CV SRA and perform a paste in the appropriate field.

5. (Required) Enter the **Duo Account Settings** from the CV SRA Plus application created in Duo:
   a) Paste the **Client ID** (Alphanumeric Duo application key).
   b) Paste the **Client Secret** (Alphanumeric Duo application password key).
   c) Paste the **API Host** (API server that validates the login request).
6. When finished, click **Add Integration** (bottom right). The **Enable External Integration** prompt opens, stating that enabling the new integration record will disable any previously enabled Duo Integration. With the Duo integration enabled, you can now activate CV SRA Plus with the integrated Duo posture check.

> **Note**
>
> The external integration for Duo allows adding multiple Duo accounts to CV SRA Plus, for example, for troubleshooting purposes. But only one Duo account can be chosen as Active in CV SRA Plus at any moment.

Duo integration is now live and ready for enforcing posture checks on CV SRA Plus sessions.

Verify the CV SRA Plus and Duo integration

Provides instructions for verifying that Duo integration with CV SRA Plus has been successfully activated and posture enforcement is operational.

Ensures posture enforcement is ready and functioning.

Before you begin

- Complete all prior configuration steps.

Procedure

1. In IoT OD, from the left pane, choose **SRA** > **System Management**.
2. Click the **External Management** tab.
3. Verify that the Duo integration is **Active** .

What to do next

CV SRA Plus and Duo integration is verified as active and posture enforcement is functioning correctly.

Configure access methods

Set up various access methods for remote access to meet operational and security requirements.

Use the available access methods to support remote access requirements for operational and security needs.

CV SRA provides two groups of access methods.

After you add a network device and asset, open the asset details, choose **Add Access Method**, select an access method, and enter the method-specific information. You can also configure an access method through **Quick Wizard**.

Group	Type	Access methods
Group A	Clientless	SSH, RDP, VNC, Web App, and Telnet.
Group B	Agent-based	SRA Plus, which uses the local SRA Plus application.

Configure an SSH access method

Provides instructions for configuring SSH as an access method for a network device in CV SRA.

Set up secure SSH connections to manage devices remotely.

SSH is commonly used to provide secure remote CLI access. You may need to enable advanced settings for customizations.

Before you begin

- Ensure the network device is already added to the system.
- Obtain valid device credentials of the OT asset.

Procedure

1. In the Services panel, navigate to **SRA > System Management > Network Devices**.
2. In the **Network Devices** list, click the device name in the **Assets** table to open the **Asset Details** page.
3. Click **Add Access Method**.
4. Select **SSH** from the **Access Method** list.
5. Enter the required details in the **Add Access Method** section and click **Add**.

SSH is now set as an access method for the selected device; users with the appropriate permissions can initiate secure sessions.

Configure a telnet access method

Provides instructions for configuring a Telnet access method in CV SRA to enable authorized users to initiate terminal sessions with network devices using the Telnet protocol.

Add a Telnet access method to a network device for remote management.

Configuring a Telnet access method in CV SRA allows authorized users to initiate terminal sessions with network devices using the Telnet protocol.

Before you begin

- Ensure the network device is already added as an asset.

Procedure

1. In the **Services** panel, click **SRA > System Management > Network Devices**.
2. Click the name of the device that is attached to the asset.
3. In the **Assets** table, click the desired asset to open its **Asset Details** page.
4. Click **Add Access Method**.
5. Select **Telnet** from the **Access Method** list.
6. Enter the required details in the **Add Access Method** section, and click **Add**.

The Telnet access method is added to the device and available for user assignment through **Access Management**.

Configure an RDP access method

Provides instructions for setting up a Remote Desktop Protocol (RDP) access method for a managed network device to enable secure remote desktop connectivity through your network management system.

Set up a Remote Desktop Protocol (RDP) access method for a managed network device.

Use this procedure to enable secure remote desktop connectivity through your network management system.

Before you begin

- Verify you have added the desired network device as an Asset.
- Gather credentials and connection details for the target device.

Procedure

1. In the **Service** panel, navigate to **SRA > System Management > Network Devices**.
2. In the **Assets** table, click the device name to open the **Asset Details** screen.
3. Click the name of the device that is attached to the asset.
4. In the **Assets** table, click the desired asset to open its **Asset Details** page.
5. Click **Add Access Method,** then from the **Access Method** list, select **RDP**.
6. Enter the required details in the **Add Access Method** section.
7. In **Advanced Settings**, complete relevant options as required for your access method.
8. Click **Add**.

The device is now configured with an RDP access method, enabling authorized users to establish secure remote desktop sessions according to your defined settings.

Configure a VNC access method

Provides instructions for configuring the VNC access method as an optional means to remotely access and manage network device assets using CV SRA and VNC password authentication.

Configure the VNC access method as an optional means to remotely access and manage network device assets. The method uses VNC password authentication through the CV SRA UI.

Use this procedure to set up VNC access for a network device using the CV SRA interface.

Before you begin

- Ensure the required network devices and assets are added to your system. (See: Add Network Devices and Assets to a group.)
- Review your VNC server's vendor documentation to configure the server for use with non-vendor VNC viewers.
- Set up the VNC access method to use only password authentication; this is the only supported authentication type.
- If you require other authentication methods (such as username and password), use the CV SRA Plus access method with a local VNC client instead.

Procedure

1. In the **Services** panel, go to **SRA > System Management > Network Devices**.
2. Click the name of the device that is attached to the asset.
3. In the **Assets** table, select the device name to open the **Asset Details** screen.
4. Click **Add Access Method** and from the **Access Method** list, select **VNC**.
5. Enter the required details in the **Add Access Method** section, and click **Add**.

The VNC access method is configured for the device, allowing authorized users password-authenticated remote VNC access.

What to do next

Assign user access if needed to ensure authorized remote VNC sessions.

Configure a Web App access method

Provides instructions for configuring the Web App access method on a device asset so users can securely interact with web interfaces through the CV SRA environment.

Add the Web App access method to a device asset so that users can interact with web interfaces securely.

Use this configuration to enable remote access to web servers operating on managed assets within the CV SRA environment.

Before you begin

- Ensure the target device is already added as an asset.
- Evaluate the website's design before using the Web App access method. If the site relies on URL redirects to static IP addresses, redirects may not work properly.
- Note that websites using websockets may not function correctly through the Web App access method.
- If unsure whether the Web App access method is suitable, use CV SRA Plus as an alternative for compatibility.

Procedure

1. In the **Services** panel, navigate to **SRA > System Management > Network Devices**.
2. Select a device name from the **Assets** table to open its **Asset Details** page.
3. Click the name of the device that is attached to the asset.
4. Click **Add Access Method**, then from the drop-down list select **Web App**.
5. Enter the required details in the **Add Access Method** section, and click **Add**.

The Web App access method is successfully added. Users with appropriate permissions can open secure web sessions to the specified URL through the CV SRA environment.

Configure an CV SRA Plus access method

Provides instructions for setting up a CV SRA Plus access method for your managed Cisco devices in IoT OD, enabling secure remote sessions.

Link your network device, protocol, and user permissions for secure access.

Configure the CV SRA Plus access method in IoT OD to enable secure remote sessions for authorized users.

Before you begin

- Ensure the CV SRA Plus App is installed.
- Ensure the asset was added using its IP address, not its hostname.
- Ensure that no other VPN client is active and that antivirus software does not block the CV SRA Plus application.

Procedure

1. Navigate to **SRA > System Management > Network Devices** and select the network device you want to configure.
2. Click the name of the device that is attached to the asset.

3. Choose an asset to open its details, then click **Add Access Method**.
4. Select **SRA Plus** from the **Access Method** list.
5. Choose a protocol definition and port configuration. Use the filter to display all, custom, or predefined protocol definitions. Legacy CV SRA Plus access methods are read-only.
6. Optional: Configure the cross-launch settings:
   a) Enter an application cross-launch URL to open a web application for the asset.
   b) Enter an application cross-launch path to launch a local application.
   c) Enter application cross-launch parameters, such as a password, port, or local directory.
7. Review or edit the prepopulated **Access Name** and **Name**. Optionally enter a description of up to 150 characters, and click **Add Access Method**.

The CV SRA Plus access method is configured and available for authorized users to initiate secure remote sessions.

Remote asset session requests

Describe how remote asset session requests are managed and approved within Cyber Vision Secure Remote Access (CV SRA), outlining their key attributes and responsible roles.

A remote asset session request is a workflow in CV SRA that enables authorized users to request access to specific assets, designates Access Managers as the primary approvers for session requests, and permits SRA System Admins or SRA Access Admins to approve requests if Access Managers are unavailable.

- Enables authorized users to request access to specific assets.
- Designates Access Managers as the primary approvers for session requests.
- Permits SRA System Admins or SRA Access Admins to approve requests if Access Managers are unavailable.

User roles and permissions for remote asset session requests

The following table lists the user roles and their permissions for managing remote asset session requests in CV SRA.

Table 41: User roles and permissions for remote asset session requests

User role	Permissions
SRA System Admins	Manage all requests in the organization
SRA Access Admins	Manage all requests in the organization
SRA Access Managers	Manage requests only for groups where they are assigned as approvers

Possible causes for 512 errors by protocol

The following conditions can cause a 512 error when you connect to a remote session:

Access method	Possible causes
SSH	• Internal server error. • The asset host key could not be retrieved. • An error occurred while checking the host key. • The provided host key does not match a known host key.
RDP and Telnet	Internal server error.
VNC	• Internal server error. • Unsupported credential type.

Manage requests as an SRA access manager

Provides instructions for reviewing, approving, or denying pending remote asset session requests as an SRA Access Manager in the Cisco IoT Operations Dashboard.

Review, approve, or deny pending remote asset session requests submitted by users in groups you manage.

SRA Access Managers handle access requests for assigned groups. Requests appear in the dashboard only if you are set as an approver for the group.

Before you begin

Ensure you have the SRA Access Manager role and are assigned to the relevant group.

Procedure

1. Log in to the Cisco IoT Operations Dashboard as an SRA Access Manager.
2. Choose **SRA** > **Access Management**.
3. On the **Access Management** pane, select the **Pending Requests** tab.

   The **My pending requests** tab appears.

   All requests for which you are an approver are listed in this tab. These requests are submitted by users within your group.
4. In the **Actions** column, select **Approve**, **Deny**, or **View**.

The request is approved or denied.

What to do next

Users with SRA User role can connect to the remote session by logging in to the IoT Operations Dashboard.

Manage requests as a SRA system or access admin

Provides instructions to approve or deny pending remote asset session requests as a System Admin or Access Admin in the Cisco IoT Operations Dashboard.

Approve or deny any pending remote asset session requests organization-wide.

SRA System admins and access admins can manage all session requests, including those assigned to specific access managers.

Before you begin

Ensure you are logged in as either a System Admin or Access Admin.

Procedure

1. Log in to the Cisco IoT Operations Dashboard as a System or Access Admin.
2. Choose **SRA** > **Access Management** > **Pending Requests** > **All pending requests**.

   All requests in your organization that need approval are listed here, including those assigned to the Access Managers.
3. In the **Actions** column, select **Approve**, **Deny**, or **View**.

Request outcomes

Explains the outcomes that occur after a request is approved or denied in Cisco IoT Operations Dashboard, including user notifications, session access, and the need to re-initiate requests in certain scenarios.

A request outcome is a remote access management state that determines what happens after a request is approved or denied in Cisco IoT Operations Dashboard.

- Sends an email notification to the SRA user after a request is approved or denied.
- Provides instructions to the user regarding next steps based on the request decision.
- Allows access to the requested remote session upon approval or requires re-initiating the request if denied.

Additional reference information about request outcomes

When a request is approved, the user can access and connect to the remote session by clicking the **View** button in the notification email, which directs them to the **Remote Sessions** page of Cisco IoT Operations Dashboard. If a request is denied, the remote session status changes to **Request Access**, and the user must submit a new request to obtain access.

Request History details

Explains how the Request History tab displays access request entries based on your user role, including which requests are visible to different types of administrators and managers.

The Request History tab displays access request entries that vary depending on your user role.

You can view the history of all access requests in the *Request History* tab. The entries displayed in the *Request History* tab vary depending on your user role.

Table 42: Request History tab entries by user role

User role	Request History tab entries
SRA System Admins	All approved, denied, expired, revoked, and withdrawn requests for all users across all groups in the organization
SRA Access Admins	All approved, denied, expired, revoked, and withdrawn requests for all users across all groups in the organization
SRA Access Managers	All approved, denied, expired, revoked, and withdrawn requests of all users in the group where they are assigned as approvers. They cannot refer to the entries of a group where they are not the approvers.

Revoke an approval request

Provides instructions to revoke an approved remote asset session request to prevent new connections while allowing active sessions to continue until timeout.

Cancel an approved remote asset session request if it was authorized in error.

Revoking a request removes approval but does not affect any currently active sessions. Sessions continue until timeout, but new connections based on the revoked request are blocked. All revoked requests appear in the **Request History** tab. The request history can be sorted or downloaded for further review.

Before you begin

Ensure you have the necessary permissions (such as SRA Access Manager, Access Admin, or System Admin role).

Procedure

1. Go to the **Request History** tab.
2. Select the request you want to revoke.
3. Click **Revoke** in the **Actions** menu.
4. Alternatively, select **View** in the **Actions** menu and then click **Revoke** on the View Details page.

The request status changes to "revoked" in the **Request History** tab. The current session remains active until timeout, but users cannot initiate new connections with the revoked request.

What to do next

You may sort or filter the **Request History** by various criteria or download the list as a CSV file for auditing.

Remote session management and monitoring

Monitor and manage live remote sessions by viewing details, supervising activities, and terminating sessions to enhance security administration.

Session management is an administrative function that

- Enables SRA System Admins and SRA Access Admins to join live remote sessions.
- Allows monitoring of session activity in real time.
- Provides the ability to terminate sessions when necessary.

Active sessions and session details

An active session is a remote access instance that records key details about the connection and user, enables administrators to monitor and supervise ongoing activities, and provides security options to join or terminate sessions as needed.

Within the **SRA Service** > **Access Management** > **Active Sessions** tab, you can view the details for each current session:

- **Connected Client** : The currently open remote session.
- **Access Method** : The access method used (for example, Web App, SSH, VNC, SRA Plus, RDP, or Telnet).
- **User** : The user who is currently active in the session.
- **Session Start** : The date and time the session began.

- **Duration** : How long the session has been active.
- **Schedule Duration**: The allotted time for the session according to its schedule or policy.
- **Country**: The geographic origin of the session based on the user location.
- **Monitor** : Provides the option to **Join Session** for supported methods.
- **Security** : Provides the **Terminate** option.

Use the **Session History** tab to review completed sessions. Session history can include the session start time, duration, asset, access method, user, country, total bytes transferred, termination status, recording status, and available actions.

You can filter session history by its columns and configure the columns displayed in the table. Sessions with zero duration and data can indicate a failed or immediately terminated access attempt.

To export session history, choose **Access Management** > **Session History**, select a date range, optionally select **Only Show Recorded Sessions**, and choose **Download Session History**. The export is a CSV file and uses UTC for the export date and time.

Remote sessions

Describe how remote sessions work in CV SRA.

A remote session in CV SRA is a secure, authenticated, and time-bound connection between a remote user (such as a maintenance contractor or operations staff) and an industrial asset (like a PLC or sensor).

- Provides secure connectivity between remote users and industrial assets.
- Ensures authentication of users before granting access.
- Limits access duration to a defined time window.

Monitor a user session

Provides instructions to monitor a user's live remote session for supervision or training using the Access Management interface.

View a user's live remote session for supervision or training.

Use this task to observe user activity in real time without interacting directly with the session.

Procedure

1. From the **Access Management** screen, go to the **Active Sessions** tab.
2. Select a session from the list.
3. In the **Monitor** column, click **Join Session**.

You can view the user's session in real time. You are restricted to monitoring only; you cannot interact with the session except to terminate it if necessary.

Download the session history

Provides instructions for downloading a record of session history as a.csv file for auditing or review purposes.

Export a record of sessions for auditing or review.

Use this task to generate a.csv file containing session details from a specified date range.

Before you begin

Follow these steps to download session history:

Procedure

1. From the **SRA** panel, go to **Access Management** > **Session History**.
2. Select your desired date range using the calendar pop-up.
3. *(Optional)* Check the **Only Show Recorded Sessions** box to filter your results.
4. Click **Download Session History**.

The session history file is saved to your computer's Downloads directory as a.csv file.

Terminate a session

Provides instructions to immediately end a user's live session if you detect suspicious or potentially harmful activity.

Immediately end a user's live session if you detect suspicious or potentially harmful activity.

Use this task to remove access from a remote user in real time.

Procedure

1. In the **Security** column of the **Active Sessions** list, click **Terminate** .
2. Confirm the action when prompted.

The session ends for the user. A "Session Timed Out" notice appears on their screen, and the session is listed in the **Session History** tab with a **Yes** in the **Terminated** column.

Modify a remote session

Provides instructions to change the details of an existing remote session.

Only sessions viewed in List View can be modified.

Procedure

1. To modify a remote session, hover over the **3 dots** in the **Actions** column and the **Edit** option opens.
2. Click **Edit** . The **Session Details** panel opens.
3. Click the **Edit** icon and edit the session details.
4. Click **Close** to save your changes.

Session details are updated according to your changes.

Remote session recordings

Explain how to configure CV SRA for remote session recordings, enabling activity capture during remote access.

A remote session recording is a CV SRA feature that enables organizations to record, store, and enforce session recordings for auditing or educational purposes.

- Enables recording of user sessions for auditing or education.
- Stores recordings through a configured AWS S3 or Azure Blob external integration.
- Allows CV SRA System or Access Admins to enforce session recording requirements within access groups.

Additional reference information

Remote session recordings are managed as part of CV SRA. Configure a supported external storage integration before enabling recording.

For more information on AWS S3, refer to What is S3?.

Required IAM permissions for Cisco IoT Operations Dashboard

Explains the specific AWS S3 permissions required for the IAM role or user used by the Cisco IoT Operations Dashboard to function properly.

Ensure the following specific AWS S3 permissions are present for the IAM role or user leveraged by the Cisco IoT Operations Dashboard.

Table 43: Required AWS S3 permissions

Permission	Description	Condition/note
"s3:PutObject"	Allows the dashboard to upload files to the S3 bucket.	Required for data creation.
"s3:GetObject"	Allows the dashboard to retrieve files from the S3 bucket.	Required for data reading.
"s3:ListBucket"	Allows the dashboard to list the contents of the S3 bucket.	Required for browsing and file discovery.
"s3:DeleteObject"	Allows the dashboard to delete files from the S3 bucket.	Required only if deletion functionality from the dashboard is needed.
"s3:GetObjectTagging"	Allows retrieval of S3 object tags.	Required only if session metadata needs to be retrieved by the dashboard.

Session recording configuration guidelines

Provides guidelines for configuring session recording in CV SRA. Understand the supported access methods, storage limitations, and administrative requirements for session recording integration.

Follow these session recording configuration guidelines to understand supported access methods, storage behavior, and administrative limitations.

- Session recording supports SSH, RDP, VNC, and Telnet access methods.
- Recording videos are always limited to 640x480 resolution, 25 FPS, and encoded in h264 (MPEG-4-AVC), regardless of the original session screen definition.
- Recorded session files are stored as MP4 through the configured external storage integration. With AWS S3, the files are stored in the integrated bucket.

- For AWS S3 integrations, you can configure multiple buckets, but only one bucket can be active at a time.
- For an AWS S3 integration, if the Secret Access Key changes for any reason, you must delete and recreate the integration, as the existing integration cannot be updated.
- Only one AWS S3 recording bucket can be active at any moment.
- Session recordings from all users in a group with enforced recording are accessible by the SRA Admin.

Set up CV SRA for session recordings with AWS S3 integration

Provides instructions to integrate an AWS S3 bucket with CV SRA to store recorded remote session files as MP4 videos for compliance and recordkeeping.

Use this procedure to configure session recordings in CV SRA by integrating an AWS S3 bucket, enabling external storage of session video files.

Inline session recording in CV SRA supports regulatory compliance and recordkeeping by storing recordings externally, using AWS S3 integration.

Before you begin

- Prepare an AWS S3 bucket and gather the AWS Region and bucket name.
- Ensure that an AWS S3 bucket is set up and integrated with the CV SRA service. For more information, refer to Get Started With S3.
- You have an AWS account with necessary permissions and access keys. For more information, refer to AWS Account and Key Access.
- For Assume Role authentication, create an IAM role that SRA can assume. Configure its trust policy to allow `sts:AssumeRole` with the required external ID, grant the required S3 permissions, and obtain the role ARN and external ID.

Procedure

1. Choose **SRA** > **System Management** > **External Integrations**.
2. Click **Add External Integration**.
3. In the **Add External Integration Details** pane, select **S3**.
4. Enter a name and description in **External Integration Details** section.
5. Enter the AWS Region and bucket name in the **Inline Monitoring Settings Details** section.
6. In **Credential Details**, select the authentication method:
   a) For **Access Credential**, enter the AWS access key and secret access key.
   b) For **Assume Role**, enter the IAM **Role ARN** and **External ID**. Use the predefined role-name prefix required by your deployment. The default prefix is `SRA_ext_access_`; hover over the **Role ARN** information icon to confirm the required prefix.
7. Click **Add**. The External Integration record is added to the External Integration table.

Your AWS S3 bucket is now linked to CV SRA, and future session recordings will be stored in the specified location.

What to do next

If the Secret Access Key is updated, you must delete and re-add the integration.

Azure Blob storage for session recordings

Configure Azure Blob storage as an external integration for CV SRA session recordings.

In addition to the existing AWS S3 integration, CV SRA provides an Azure Blob external integration for storing remote-session recordings. Configure the integration under **System Management** before selecting it for recording storage.

The integration requires a directory ID, application ID, client secret, storage account name, and container name. **Test Connection** checks the supplied connection details. A failed test does not prevent you from saving the integration; you can edit its details later. Verify the connection before using the integration for recordings.

Table 44: Feature History

Feature	Release	Feature description
Azure Blob external integration	September 2026 release	Add and test an Azure Blob integration for remote-session recording storage.

Configure an Azure Blob external integration

Add Azure Blob storage to CV SRA for remote-session recordings.

Connect CV SRA to an Azure Blob container.

Before you begin

Obtain the Azure directory ID, application ID, client secret, storage account name, and container name. Ensure the Azure application can access the intended container.

Procedure

1. In CV SRA, choose **System Management** > **External Integrations**.
2. Click **Add External Integration** and select **Azure Blob**.
3. Enter an integration name, directory ID, application ID, client secret, account name, and container name.
4. Click **Test Connection** and review the result.

   If the test fails, check the Azure credentials, account, container, and application permissions. A failed test does not prevent you from saving the integration.
5. Save the integration.

The Azure Blob integration is available in the external integrations list. You can edit its settings later.

What to do next

Verify that the connection test succeeds before selecting the integration for recording storage.

Record an inline session

Provides instructions for recording a remote inline session to comply with auditing or monitoring requirements, including steps for session initiation, recording, and verification in Access Management.

Use this procedure to record a remote session for auditing or monitoring purposes. Inline session recording is enforced for groups with the monitoring and recording setting enabled.

Inline session recording ensures that all remote sessions in specified groups are captured and stored for compliance and review.

Before you begin

- Confirm that the group is enabled and the **Enforce Monitoring and Recording (Enforce Inline (SSH/RDP/VNC) Recording)** setting is also enabled.
- The S3 integration should be active.

Procedure

1. Go to **SRA** > **Remote Sessions**.
2. Select the group with session recording enabled, then start the session intended for recording.
3. Click **Open Session** in the **Actions** column for the desired session.
4. When the session window opens, the remote session begins and recording is active.
   - You may be prompted for credentials, depending on the access method.
5. When finished, close the session window. The system automatically transcribes and saves the recording as MP4 in the S3 bucket; processing may take several minutes.

The system lists the session as recorded in **Access Management**; the video file is available in your S3 bucket.

Review a recorded session

Provides instructions for reviewing, downloading, or managing previously recorded remote sessions using Access Management, including viewing audit information and handling video files.

Access Management pane lets you inspect audited sessions and manage video recordings, offering options to download, view, or delete these files as required.

Before you begin

Ensure you have access to session history.

Procedure

1. Navigate to **Access Management > Session History**.
2. Select your desired session from the history list.
3. Click **Actions**, then choose one of the following options:
   - **View Full Auditing Info**: Inspect detailed session records.
   - **View Screen Recording**: Watch the video recording (MP4 format).
   - **Download Screen Recording**: Download the video to your local device.
   - **Delete Screen Recording**: Permanently remove the recording from the system.
4. Alternatively, choose **View Inline Recording** or download the video file directly.

You can view session details, audit records, download, or delete screen recordings as needed for compliance, review, or training purposes.

Alert rules

Define alert rules to help detect unusual user activities, specify monitored behaviors, and outline how alerts are presented for action.

An alert rule is a security monitoring policy that defines specific user activities or behaviors to watch for, triggers an alert when these activities deviate from expected patterns or violate set policies, and presents such alerts in the system for review and management.

- Defines specific user activities or behaviors to monitor.
- Triggers an alert when monitored activities deviate from expected patterns or violate set policies.
- Presents alerts in the system for review and management.

Additonal reference information

When an alert rule detects an unusual activity, it triggers an alert that appears in the Alerts tab. In this tab, you can review alert details, sort by severity, and take further action as needed. Alert rules help organizations automatically identify and respond to potential security incidents by continuously monitoring user activity patterns.

- Detecting logins from locations outside a user's typical countries.
- Detecting logins from countries disallowed by your organization’s policies.
- Detecting logins occurring outside of standard working hours for a user.

Alerts configuration page details

Explains the details and columns available on the Alerts configuration page, including descriptions and actions for each alert type.

The Alerts configuration page provides the following details about alert types, categories, rules, and actions.

Table 45: Alerts configuration page columns

Column	Description
Alert Type	The name of the alert policy. Each is a clickable link to view or edit details. Examples: • *Changed Login Location* • *Login From Prohibited Location* • *Login Outside of Working Hours*
Alert Category	The category of the alert. In this case, all are under **User Activity** .
Alert Rules	The number of active rules associated with each alert type.
Last Updated	Shows when the alert configuration was last modified.
Action	Lets you control the alert’s state: • **Pause** (red): Temporarily disables an active alert. • **Resume** (blue): Reactivates a paused alert.

> **Note**
>
> You can configure multiple alert rules within each category to trigger alerts for different scenarios.

Configure alert rules for login from prohibited locations

Provides instructions for configuring alert rules to notify administrators when users log in to CV SRA from blocked or unapproved countries using allowlist or blocklist rule definitions.

Set up alerts to notify administrators when users log in to CV SRA from blocked or unapproved countries.

Before you begin

- Determine which countries should be allowed or blocked according to organizational policies.
- Set a rule definition using either an Allowlist or Blocklist. The Allowlist should include locations to permit, while the Blocklist should list locations to flag.

Procedure

1. On the **Alerts** page, click **Login From Prohibited Location**.

   The **Login From Prohibited Location** page displaying the default configuration appears. By default, the severity of the rules is medium.

2. To modify the default rule definition and severity:
   a) Click **Edit**.
   b) In the **Edit Configuration** panel, set the default severity level of the alert to Critical, High, Medium, or Low, depending on how urgently the alert should be addressed.
   c) Select the rule definition, either Blocklist or Allowlist.
   d) Click **Save**.
3. To configure an alert rule:
   a) Click **Add** on the **Login From Prohibited Location** page.
   b) In the **Configure Alert** section, select the scope of users the alert applies to:
      - **All users** – Default option. Applies the alert to all users.
      - **Selected user roles** – Apply the alert to users assigned to specific user roles. For example, SRA users.
      - **Selected access control groups** – Apply the alert to users in specific access control groups.
4. To add locations to the rule definition, select a country from the **Add Location** drop-down list, and click **Add**.
   - The selected country is added to the configured rule definition. You can add as many countries as you want.
   - If your configured rule definition is Allowlist, then an alert will be triggered when users access CV SRA from locations other than the ones you added.
   - If your configured rule definition is Blocklist, then an alert will be triggered when users access CV SRA from the locations you just added.
5. Click **Next**.
6. To set email notifications, specify who should receive email alerts in the **Set Notification** section:

- **Selected Users** – Choose this option to send notifications to specific users. For example, SRA users.
- **Selected User Roles** – Choose this option to notify users assigned to specific roles.
- **Do not send email notification** – Select this option if you do not want email notifications to be sent when the alert is triggered.

7. Click **Next**.
8. To enter a rule name and review the details:
   a) On the **Review** page, enter a rule name in the **Alert Rule Name** field.
   b) Verify all the configured alert details.
   c) Click **Back** to navigate to the previous pages and make changes.
9. Click **Create** to save the alert rule and enable it.

The new alert rule is added to the **Login From Prohibited Location** configuration.

When a user logs in to CV SRA from a country that is configured in the Allowlist, no alert is generated. When a user logs in from a country that is in the Blocklist, an alert is generated.

> **Note**
>
> **Blocklist** does not really block users from accessing CV SRA.

Configure alert rules for changed login locations

Provides instructions for configuring alert rules that notify administrators when users log in to CV SRA from locations different from their previous access points.

Set up alerts that notify administrators when users log in to CV SRA from locations different from their previous access points.

This process helps identify suspicious account activity and potential security incidents by monitoring users' login locations.

Before you begin

- Decide which user roles or groups should be monitored.

Procedure

---

1. On the **Alerts** page, click **Changed Login Location**.

   The **Changed Login Location** page appears, allowing you to configure the alert settings. This page lists the changed login location alert rules you have previously configured. By default, the severity of the rules is medium.

2. To modify the default severity:
   a) Click **Edit**.
   b) In the **Edit Configuration** panel, set the default severity level of the alert to Critical, High, Medium, or Low, depending on how urgently the alert should be addressed.
   c) Click **Save**.
3. To configure an alert rule:
   a) Click **Add** on the **Changed Login Location** page.

b) In the **Configure Alert** section, select the scope of users the alert applies to:

- **All users** – Default option. Applies the alert to all users.
- **Selected user roles** – Apply the alert to users assigned to specific user roles.
- **Selected access control groups** – Apply the alert to users in specific access control groups.

4. Click **Next**.
5. To set email notifications, specify who should receive email alerts in the **Set Notification** section:
   - **Selected Users** – Choose this option to send notifications to specific users.
   - **Selected User Roles** – Choose this option to notify users assigned to specific roles.
   - **Do not send email notification** – Select this option if you do not want email notifications to be sent when the alert is triggered.
6. Click **Next**.
7. To enter a rule name and review the details:
   a) On the **Review** page, enter a rule name in the **Alert Rule Name** field.
   b) Verify all the configured alert details.
   c) Click **Back** to navigate to the previous pages and make changes.
8. Click **Create** to save the alert rule and enable it.

The new alert rule is listed on the **Changed Login Location** page.

When users log in to CV SRA from a country that is different from their previous login location, an alert is generated.

Configure alert rules for login outside of working hours

Provides instructions for configuring alert rules that notify administrators when users access CV SRA outside approved working days and times.

Set up alerts that notify administrators when users access CV SRA outside approved working days and times.

Use these rules to enforce security policies and monitor access that occurs outside organizational working hours.

Before you begin

- Determine the days, times, and timezone for allowed access.
- Decide which users, roles, or groups will be monitored.

Procedure

---

1. On the **Alerts** page, click **Login Outside of Working Hours**.

   The **Login Outside of Working Hours** page displaying the default configuration appears. By default, the severity of the rules is medium.

2. To modify the default severity:
   a) Click **Edit** .
   b) In the **Edit Configuration** panel, set the default severity level of the alert to Critical, High, Medium, or Low, depending on how urgently the alert should be addressed.
   c) Click **Save**.

3. To configure an alert rule:
   a) Click **Add** on the **Login Outside of Working Hours** page.
   b) In the **Configure Alert** section, select the scope of users the alert applies to:
      - **All users** – Default option. Applies the alert to all users.
      - **Selected user roles** – Apply the alert to users assigned to specific user roles. For example, device operator, SRA users.
      - **Selected access control groups** – Apply the alert to users in specific access control groups.
   c) In the **Configure Rules** section, set the time and days when you want to allow users to access CV SRA.
      - Choose the days from the **Allowed days of the week** drop-down list.
      - Choose the start and end times in the **Allowed working hours** field.
      - Select a timezone from the **Timezone** drop-down list.
4. Click **Next** .
5. To set email notifications, specify who should receive email alerts in the **Set Notification** section:
   - **Selected Users** – Choose this option to send notifications to specific users.
   - **Selected User Roles** – Choose this option to notify users assigned to specific roles.
   - **Do not send email notification** – Select this option if you do not want email notifications to be sent when the alert is triggered.
6. Click **Next**.
7. To enter a rule name and review the details:
   a) On the **Review** page, enter a rule name in the **Alert Rule Name** field.
   b) Verify all the configured alert details.
   c) Click **Back** to navigate to the previous pages and make changes.
8. Click **Create** to save the alert rule and enable it.

The new alert rule is listed on the **Login Outside of Working Hours** page.

When a user logs in to CV SRA outside the time and days configured by you, an alert is generated.

Pause alerts

Provides instructions to temporarily disable alert rules for a selected alert type using the **Alerts** dashboard.

Temporarily disable alert rules for a selected alert type.

Use this option during maintenance periods or when you do not want alerts triggered for certain activities.

Procedure

---

1. Navigate to the **Alerts** dashboard.
2. Click **Pause** against the alert type you want to pause.

All alert rules configured in the alert type will be disabled, and no alerts will be triggered for those rules.

Resume an alert

Provides instructions to resume alerts by reactivating alert rules for a previously paused alert type.

Reactivate alert rules for a previously paused alert type.

Use this when you are ready to resume normal monitoring and alerting for the selected alert type.

Procedure

1. Locate the alert that is paused.
2. Click **Resume** in the **Action** column.

Alert rules for the selected alert type are reactivated, and alerts will be triggered according to the configured rules.

Alerts

Defines alerts as security notifications that categorize issues by status and severity, providing information to help you investigate and respond to security events.

An alert is a security notification that informs users about potential or detected security issues, categorizes each issue by its current status and severity, and provides detailed information to help users investigate and respond effectively.

- Alerts inform users about potential or detected security issues.
- Alerts categorize each issue by its current status (active, muted, cleared) and severity (critical, high, medium, low).
- Alerts provide detailed information to help users investigate and respond effectively.

Alert categories, severity levels, and key attributes

Alerts are organized by categories, severity levels, and key attributes to help users prioritize and respond to security events.

Table 46: Alert categories

Category	Description
Active	Alerts that are currently open and require attention.
Muted	Alerts that have been temporarily silenced.
Cleared	Alerts that have been resolved or acknowledged.

Table 47: Alert severity levels

Severity	Description
Critical	Indicates high-priority issues requiring immediate action.
High	Represents significant security events.
Medium	Denotes moderate-level concerns.
Low	Flags informational issues.

Table 48: Key alert attributes

Attribute	Description
Alert Type	Describes the nature of the alert (for example, login from prohibited location).
Trigger	Identifies the event or condition that caused the alert.
Instances	Shows how many times the specific trigger occurred.
Category	Groups the alert by type (for example, user activity).
Last Detected	Time of the most recent occurrence.
Severity	Indicates the impact level (for example, medium).

To view detailed information of an alert, click the field in the **Trigger** column, then the corresponding number in the **Occurrences** column.

For example, if a user logs in from a prohibited location, an alert is generated with Critical severity. The alert appears as active until it is acknowledged or resolved, and users can click the **Trigger** and **Occurrences** columns to investigate further.

View user activity in Cisco IoT Operations Dashboard

Provides instructions to view individual user activities and access privileges within the Cisco IoT Operations Dashboard, including reviewing session history, access levels, and account status.

Examine individual user activities and access privileges within the Cisco IoT Operations Dashboard.

Use this task to review details about users in your Cyber Vision Secure Remote Access (CV SRA) environment, including session history, access levels, and account status.

Before you begin

- Ensure you have administrator access to the Cisco IoT Operations Dashboard.

Follow these steps to view the user activity on Cisco IoT Operations Dashboard.

Procedure

1. Log in to the Cisco IoT Operations Dashboard as an SRA Admin.
2. Choose **SRA** > **Access Management**.
3. On the **Access Management** pane, select the **Users** tab.

   The **Users** tab lists the following information for each user:

Field	Description
User	The email ID of the user

Field	Description
Status	The status can have the following values: • **Active** - The user has logged in to CV SRA one or more times in the last 30 days. • **Inactive** - The user hasn't logged in to CV SRA at least once in the last 30 days. • **Blocked** - The user is blocked by the administrator.
Highest Role	Users may have multiple roles assigned to them. Highest role is the one with the highest privileges.
Assets	Number of assets the user can access.
Access Control Groups	Number of access control groups which the user belongs to.
Last Connected	The date when the user last connected to a remote session.
Last Login	The date when the user last logged in to CV SRA.
Remote Sessions	Number of remote sessions the user owns.
Network Devices	Number of network devices associated with the assets the user owns.

Note

The number of fields varies depending on your selection on the **Table Settings** page.

4. To view detailed information for a particular user, click the user's email ID.

   A new page opens with sections for **User Details**, **Assets** , **Last Known Device Status**, **Remote Session History**, and **Access Control Groups**. Explore each section for more information.

5. To block a user, click **Block** in the **User Details** section.

Note

- Blocking users immediately prevents them from accessing CV SRA and terminates all active sessions. The user's access remains suspended until explicitly unblocked by an administrator.
- Admin users cannot be blocked because they can unblock themselves. Attempting to block an admin user results in the 'Cannot perform user action block' message.

You can review user activity data and block suspicious accounts directly from the dashboard.

What to do next

After blocking a user, monitor the dashboard to confirm access is suspended and review any additional activity for security assurance.

Access expiration policy

Enforce access expiration policies to ensure only legitimate users retain CV SRA access by managing user validity and enhancing security.

The access expiration policy is a security measure that manages the validity period of user access to CV SRA.

- By default, the maximal access duration for each user role is unlimited.
- Specific expiration times (60, 90, or 180 days) can be set for user roles other than SRA System Admin.
- SRA System Admins have permanent, unlimited access.

Default expiration settings and user role management

The access expiration policy enhances security by ensuring that only authorized users retain access to CV SRA, and allows administrators to configure access duration for different user roles.

Change the default maximum access duration from **Configuration** > **Policies**. Changes are processed during the nightly system check. If the current expiration is shorter than the new setting, no change is made. If the current expiration is longer than the new setting, it is reduced to the new value.

For example, a user with the SRA Operator role can be assigned an access expiration of 90 days, after which their access will be revoked unless renewed. In contrast, a user with the SRA System Admin role will retain access indefinitely.

Administrator-initiated extensions

Administrators can extend a user's access without waiting for an extension request. From **Cyber Vision Secure Remote Access** > **Access Management** > **Users**, select a user, choose **Edit Expiration**, and select **Reset to maximum** or **Set access expiration date**.

If a user is blocked for a reason other than access expiration, you can select **Unblock user** while extending access. If the user is blocked because access expired, unblocking resets the expiration to the default policy value before you set a specific date.

Modify the default policy

Provides instructions to change the maximum access duration for user roles in CV SRA by modifying the default expiration policy to meet security requirements.

Change the maximum access duration for user roles to meet security requirements.

CV SRA lets you limit the length of time different user roles retain access by adjusting the expiration policy.

Before you begin

Ensure you have administrator privileges in CV SRA.

Procedure

1. Choose **Configuration** > **Policies**.

> **Note**
>
> The **Policies** page displays the default access expiration policies for different user roles.

2. On the **Policies** page, click **Edit**.
3. In the **Edit Maximum Access Expiration** dialog box, locate the field for the user role whose policy you want to modify.
4. Select a value from the drop-down list, and click **Save**.

The new settings do not apply immediately to existing users. Changes are processed during the nightly system check based on the following logic:

If...	Then...
The current expiration time is shorter than the new setting	No changes are made.
The current expiration time is longer than the new setting	The expiration will be reduced to match the new value.

Notification schedules

Explains the notification schedule for users regarding impending access expiration, including the timing of email notifications and the process for reviewing extension requests.

The notification schedule defines when users are alerted about upcoming access expiration and outlines the process for handling extension requests.

- Users receive email notifications at specific intervals before their access expires.
- Notifications are sent 7 days, 3 days, and 1 day prior to expiration.
- System or Access Admins can review and approve or reject extension requests based on justification.

Request an access extension for an CV SRA session

Provides instructions for requesting additional time for your remote session access if your current access is about to expire and you have a business need to extend it.

Request additional time for your remote session access beyond the current expiration date.

Use this task if your remote session access is about to expire and you have a business need to extend it. The request must be approved by administrators in your organization.

Before you begin

- Ensure you have access to CV SRA and are logged in.

Procedure

1. Log in to CV SRA.

2. Navigate to the **Remote Sessions** page.
   - If your access is nearing its revocation date, a banner is displayed.
3. Click **Request an access expiration extension**.
4. Enter your business justification in the provided text box.
5. Click **Request**.

Your request is sent to all administrators in your organization. If approved, your remote session access will be extended.

What to do next

Monitor your email or notifications for administrator approval or further action, if required.

Manage access extension requests

Provides instructions for reviewing and approving or rejecting users' requests for more access time using the Access Management interface.

Use this procedure to review and manage user requests for additional access time in your system.

Administrators can view and manage all pending access extension requests in the Access Management interface.

Before you begin

Ensure you have administrator access.

Procedure

1. From the left service panel, select **SRA** > **Access Management**.
2. On the Access Management page, click **Pending Requests** > **Access expiration requests**.
3. Select the request you wish to review, and then click **Approve** in the **Action** column.
4. In the **Approve Request** dialog box, choose one of these options:
   - **Reset to maximum** - This option resets the expiration value to the default value defined in the **Policy** tab.
   - **Set access expiration date** - Choose this to pick a specific expiration date from the calendar.
5. Click **Save**.

An email notification is sent to users, informing them of your decision. The requests will be moved to the **Request History** > **Access extension requests** tab for auditing.

Extend access expiration without user requests

Provides instructions for proactively extending user access expiration in CV SRA without waiting for a user request. Use this procedure to directly modify access for users who require extended access.

Enable SRA administrators to directly extend user access periods, even when a user has not submitted an extension request.

Use this procedure when you need to proactively extend a user's access in CV SRA, bypassing the typical requirement for a user-initiated request.

Before you begin

- Ensure you have the necessary privileges to modify user access in CV SRA.

Procedure

1. From the left service panel, select **SRA > Access Management**.
2. On the **Access Management** page, click the **Users** tab.
3. In the user table, select one or more users whose access you want to extend.
4. In the **User details** section, click **Edit Expiration**.
5. In the **Edit Access Expiration** dialog box, choose one of the following options:
   - **Reset to maximum** : Resets the expiration date to the default value set in the Policy tab.
   - **Set access expiration date** : Select a specific expiration date from the calendar.
6. Click **Save** to apply your changes.
7. (Optional) If users are currently blocked:

If...	Then...
The block is for reasons other than access expiration	Click **Unblock** user when extending access.
The block is due to expired access	You cannot immediately set a new expiration date. When you unblock the user, access expiration resets automatically to the default value in the **Policy** tab. You can then set a custom expiration date as needed.

The selected users' access expiration is extended according to your chosen option, and access status is updated immediately.

What to do next

As needed, review access and policy settings for the updated users to confirm successful extension.

Best practices for expiration policy management

Provides guidelines for managing expiration policies to ensure security, auditability, and user awareness in your organization.

Regularly review and update expiration policies so they align with current security requirements and organizational needs.

Document all manual extensions of expiration periods, including the reasons for each extension, to maintain clear audit trails.

Communicate all changes to expiration policies and notification schedules to users, ensuring stakeholders are informed and aware of policy updates.

Secure file transfer

Enable secure file transfer to safeguard file exchanges with integrated automatic malware checks.

Secure file transfer is a feature that lets users securely transfer files between CV SRA and remote assets, ensuring that files are scanned for malware before transfer.

- Available for all user roles, including SRA User roles.

- Files are uploaded to a staging area on CV SRA and scanned for malware.
- Malicious files are automatically deleted and cannot be transferred, but their file names remain visible in the Staging Files section.
- Files identified as potentially unwanted applications are not transferable until approved. Review the scan result in the **Staging Files** table before deciding whether to approve or reject the file.

For example, when a user uploads a file to the CV SRA staging area, the system scans the file for malware. If the file is clean, it becomes available for transfer during a remote session. If malware is detected, the file is deleted, but its name still appears in the Staging Files section.

Secure file transfer guidelines

Provides guidelines for enabling secure file transfer for RDP sessions to ensure proper configuration and compliance with file size limitations.

Enable secure file transfer only for RDP sessions and ensure the feature is activated during RDP access method configuration.

- Secure file transfer is available exclusively for RDP sessions.
- File transfer functionality must be enabled when configuring the RDP access method.
- Do not upload files larger than 1 GB when using secure file transfer for RDP sessions.

Upload files to the secure file transfer staging area

Provides instructions for uploading local files to the Secure File Transfer (CV SRA) staging area for later transfer to assets.

Add local files to the Secure File Transfer staging area for later transfer to assets.

Use this task to transfer files to or from the staging area and your assets.

Before you begin

- Ensure you have access to CV SRA.
- Verify you have the required files located on your local system.

Procedure

1. Navigate to **SRA** > **Secure File Transfer**.
2. On the **Secure File Transfer** page, click **Upload File**, and browse your local system to find and select the file you wish to upload.
3. After selecting the file, click **Open** to confirm your choice. The file transfer will begin.

After you initiate the upload, the file is automatically scanned for malware. If a file is malicious, it cannot be transferred or downloaded because the physical file is not stored; only its entry is added to the **Staging Files** list with the Malware Found status.

Review potentially unwanted files before transfer

Control whether a file flagged as a potentially unwanted application can be transferred to a remote asset.

After a file is uploaded to the secure file transfer staging area, CV SRA displays its scan status and whether it is transferable. A file identified as a potentially unwanted application (PUA) is not transferable until it is explicitly approved. The **Remarks** column identifies the detection and provides an approval or rejection action.

An approved PUA file becomes available for transfer during a remote session. A rejected file remains unavailable for transfer. This review does not override the handling of files detected as malware.

Table 49: Feature History

Feature	Release	Feature description
PUA file review	September 2026 release	Approve or reject staged files identified as potentially unwanted applications before remote-session transfer.

Approve or reject a potentially unwanted file

Review a staged file identified as a potentially unwanted application before transferring it to an asset.

Decide whether a PUA-flagged file can be transferred during a remote session.

Before you begin

Upload the file and wait until its scan status is **Scanned**.

Procedure

1. Choose **SRA** > **Secure File Transfer**.
2. In the **Staging Files** table, locate the file whose **Scan Status** is **Potential Unwanted Application**.
3. Review the detection in **Remarks**, and click the approval or rejection link in that column.
4. Approve the file if it is permitted for transfer, or reject it to keep it unavailable.
5. Check the **Transferable** column to verify the resulting status.

   Only a file marked **Yes** is available for transfer during a remote session.

The staging area records the decision and indicates whether the file can be transferred.

Transfer files to assets

Provides instructions for transferring files between the CV SRA staging area and remote assets during a remote session using CV SRA.

Move uploaded files from the CV SRA staging area to assets during a remote session.

Use this task to transfer files to or from remote assets after uploading them to the staging area.

Before you begin

- Ensure a file is available in the staging area.
- Verify that an RDP remote session is available.

Procedure

1. Navigate to **SRA** > **Remote Sessions**.
2. On the Remote Sessions page, click **Connect** to the RDP session you want to connect to.

3. Once you are connected, click **File Transfer** that is located at the bottom of the page.
4. Use the **Secure File Transfer** window to move files between the **Staging Files** and **Asset Files** sections.
5. To move files from **Staging Files** to **Asset Files** , select files from the **Staging Files** section and click the left arrow (<) to move them to the **Asset Files** section.

> **Note**
>
> When you move files from the **Asset Files** section to the **Staging Files** section, the files will be automatically scanned for malware before they are available in the **Staging Files** section.

Upon successful transfer, files sent from CV SRA to remote assets are located in the **SRA Drive on IoTOD** network drive, and files sent from remote assets to CV SRA are in the **Staging Files** section.

Request an access extension for an CV SRA session

Provides instructions for requesting additional time for your remote session access if your current access is about to expire and you have a business need to extend it.

Request additional time for your remote session access beyond the current expiration date.

Use this task if your remote session access is about to expire and you have a business need to extend it. The request must be approved by administrators in your organization.

Before you begin

- Ensure you have access to CV SRA and are logged in.

Procedure

1. Log in to CV SRA.
2. Navigate to the **Remote Sessions** page.
   - If your access is nearing its revocation date, a banner is displayed.
3. Click **Request an access expiration extension**.
4. Enter your business justification in the provided text box.
5. Click **Request**.

Your request is sent to all administrators in your organization. If approved, your remote session access will be extended.

What to do next

Monitor your email or notifications for administrator approval or further action, if required.

Request access to a remote session

Provides instructions for requesting access to a remote session using CV SRA.

This feature enables SRA users to request access to an asset. Once the request is approved by the designated approvers, you can remotely access the resource for a specific time.

Submit a request to remotely access an asset assigned to you through CV SRA. After you are added to an access group with Request Access feature enabled, you must submit a session request to gain access. Your request is subject to approval by an Access Manager or other authorized approver.

Before you begin

- Confirm that your SRA System Admin or SRA Access Admin has assigned you to an appropriate access group.
- Ensure that Request Access feature is enabled for your assigned group.

Procedure

1. Log in to the IoT OD as an SRA user.
2. Choose **SRA** > **Remote Sessions**.
3. Choose the **Remote Access Group** that contains the session you need to access.
4. In the **session** you need access, click **Request Access**.
5. In the **Request Access** pop-up, perform the following actions:
   - (Optional) Enter a relevant comment in the **Requester Comments** field.
   - (Required) Select a **Start Group Access Date** and **Time** using the **Calendar** and **Clock** icons.
   - (Required) Select an **End Group Access Date and Time** using the **Calendar** and **Clock** icons.
6. Click **Request** . The screen opens to show a **View Request** button. A **Success** pop-up opens at the bottom right corner of the screen.
7. Click **View Request** to open the **Sent Access Request** panel that shows the status as **Pending**.
8. Once the request is approved, the session status changes to **Connect**.

Your request is submitted for approval and, once approved, you can access the specified asset within the scheduled window.

Connect to a remote session using the request access procedure

Provides instructions for establishing a remote session with an OT asset through CV SRA using the request access procedure.

Establish a remote session with an OT asset through CV SRA using the request access procedure.

Use this procedure when you need to remotely access an OT asset to perform maintainence operations.

Before you begin

- Verify you have SRA user credentials.
- Ensure you have session approval from an administrator.

Procedure

1. Log in to IoT OD with your CV SRA credentials.
2. Navigate to **SRA** > **Remote Sessions**.

3. Locate your approved session. Once approved, the **Connect** button appears enabled.
4. Click **Connect** to start the remote session.
    - If prompted, follow any additional authentication.

You are now connected to the remote asset, and can perform authorized activities as an SRA user.

What to do next

Log out or end the session after completing your work to maintain equipment security.

Connect to a scheduled remote session

Provides instructions for connecting to a scheduled remote session or view details for upcoming or expired sessions using the CV SRA interface.

Enable you to join a currently active remote session or view details for upcoming or expired sessions.

Remote sessions may be scheduled for future access, currently available, or expired. You can access a currently available session or view details of upcoming or past schedules.

Before you begin

- Verify you have SRA user credentials.
- Ensure you are part of a group that is enabled for scheduled access.

Follow these steps to connect to a scheduled remote session:

Procedure

---

1. Log in to CV SRA and navigate to the **Remote Session** page.
2. Identify your session in the list.
    - If the session is scheduled for the future, review its start time, end time, and duration. No interactive actions are available until the session is available.
    - If the session has expired, review its details. No interactive actions are available.
    - If the session is currently available, join by clicking the **Connect** button.
3. Click **Connect** .
4. Wait for the session to launch.

- If you connect to an available session, you enter the remote session and may now interact as permitted.
- If you view a future or expired session, you can view relevant scheduling details but cannot access the session.

Withdraw a session request

Provides instructions to withdraw a previously submitted session access request to cancel or reschedule a remote session.

Remove a previously submitted session access request.

Use this task if you need to reschedule or cancel a session by withdrawing your request.

Before you begin

Procedure

1. Navigate to **SRA** > **Remote Sessions**.
2. From the Sent Access Request panel, click **Withdraw** (located at the bottom right corner in red).
3. In the **Withdraw Access Request** pop-up, type in **Your Reason**.
4. Click **Withdraw**. The session returns to **Request Access** status.

The session access request is canceled, and the session status changes to Request Access, allowing you to submit a new access request for the session if needed.

What to do next

- Confirm that your access request no longer appears as pending or active in your session list.
- If you need to reschedule, submit a new access request for the desired session time.

Best practices for accessing CV SRA remote sessions

Provides guidelines for accessing CV SRA remote sessions to ensure you follow approval, scheduling, and notification requirements, and to avoid disruptions or access issues.

Request access to sessions: Some remote sessions require approval for access. Submit a request to access the session for a specified duration. After approval, you can access the session for the approved time period.

Scheduled sessions: Access remote sessions only during the time window configured by your SRA administrator. Sessions are inactive outside the scheduled duration.

SRA System Access situations: Notify the SRA administrator in advance to avoid your access being flagged or blocked if you plan to:

- Log in to CV SRA from countries outside your usual location.
- Log in from countries restricted by your organization's policies.
- Log in outside of the working hours defined by the policy on the system.

SRA Access Expiration : Monitor your access expiry notifications in your email. Request an extension with a valid business justification before access expires if continued access is needed.

Collect CV SRA agent logs from the IOx app

Provides instructions to collect logs from the CV SRA agent app running on a Cisco IE switch and transfer them to your local system for analysis or Cisco TAC support.

Collect logs from the CV SRA agent app running on a Cisco IE switch and transfer them to your local system for analysis or TAC support.

Use this procedure when troubleshooting CV SRA agent app issues or when Cisco TAC requests diagnostic logs.

Before you begin

- Ensure SSH and SCP are enabled and configured on your Cisco IE switch.

- Obtain the switch's management IP address and administrator credentials.

Procedure

1. Connect to the Cisco IE switch using SSH from your machine by running the following command in the terminal:

   Example

   ```
   ssh admin@<switch-ip>
   ```

2. Verify the CV SRA agent app is running by executing the following command in the CLI:

   Example

   ```
   show app-hosting list
   ```

3. Identify the agent application ID in the command output and use it in the following commands. Confirm that the application shows the state as **RUNNING** . If the app is not running, start it with the following command:

   Example

   ```
   app-hosting start appid <app-id>
   ```

4. Copy the CV SRA agent app logs to the switch's bootflash by running:

   Example

   ```
   app-hosting copy appid <app-id> src /iox_data/logs/stdout.log dest
   bootflash:stdout.log
   ```

5. (Optional) Verify the file is present in bootflash by running:

   Example

   ```
   dir bootflash: | include stdout.log
   ```

6. Transfer the **stdout.log** file to your machine by running the following command from the device's terminal:

   Example

   ```
   scp admin@<switch-ip>:/bootflash/stdout.log ~/Downloads/
   ```

   Optionally, confirm the transfer completed by running:

   ```
   ls -lh ~/Downloads/stdout.log
   ```

7. (Optional) Collect IOx trace logs if requested by Cisco TAC by running:

   Example

   ```
   app-hosting move appid <app-id> log to bootflash:
   ```

   The CLI will provide the generated log file path.

Example

```
/flash/ioxapplogs/iox_<ID>.bin.gz
```

8. Transfer the trace log to your machine by running:

Example

```
scp admin@<switch-ip>:/flash/ioxapplogs/iox_<ID>.bin.gz ~/Downloads/
```

9. (Optional) Verify the file on your machine by running:

Example

```
ls -lh ~/Downloads/iox_<ID>.bin.gz
```

Log files from the CV SRA agent app are saved on your machine, ready for analysis or to be shared with Cisco TAC for troubleshooting.

What to do next

- If requested by Cisco TAC, attach the saved log files to your support case or email.

DNS resolution issues

Describes DNS resolution issues, which are network connectivity problems that prevent devices from converting domain names into IP addresses, often resulting in failures to communicate with external services.

DNS resolution issues are network connectivity problems that prevent a device from converting domain names, such as **us.ciscoiot.com** , into IP addresses.

- They often lead to failures in communication with external endpoints or authentication services.
- They manifest through observable error messages, repeated application restarts, or timeouts when accessing network resources.

DNS resolution and network problems symptoms

Explains the common symptoms that may indicate DNS or general network connectivity issues, including error messages, application restarts, and specific log entries.

The following symptoms may indicate DNS or general network connectivity issues.

- Error obtaining an authentication token, such as:

```
Get "https://us.ciscoiot.com/sramgmt/auth/token": dial tcp: lookup
us.ciscoiot.com on 8.8.1.1:53: i/o timeout
```

- The application restarts frequently.
- Log messages including:

```
WRN ProxyUrl env variable isn't set
```

```
Successful JWT token generation, but failure occurs during token request.
```

```
DNS query timeout on server 8.8.1.1
```

Root causes of DNS and network connectivity issues

Explains the typical root causes of DNS and network connectivity issues, including DNS resolution failures, firewall restrictions, connectivity problems, and network misconfigurations.

This topic describes the typical causes of DNS and network connectivity issues.

- The device cannot resolve domain names (such as `us.ciscoiot.com`) using the configured DNS server (for example, `8.8.1.1`).
- Firewall or network restrictions are blocking DNS requests (UDP on port 53).
- The device cannot reach external internet endpoints due to connectivity issues.
- Network misconfigurations, such as incorrect MTU settings, default gateway, or routing tables.

Fix DNS resolution issues

Provides instructions to diagnose and resolve DNS resolution issues by testing domain name resolution, updating DNS server settings, and verifying network connectivity on your device.

Confirm that your device can resolve domain names and, if necessary, configure it to use a working DNS server.

DNS resolution failures can prevent applications from contacting required services. These steps help you diagnose and correct DNS configuration issues.

Before you begin

Follow these steps to check and correct DNS resolution:

Procedure

1. Test domain name resolution from your device:

   Example

   ```
   nslookup us.ciscoiot.com 8.8.8.8
   nslookup us.ciscoiot.com 8.8.1.1
   ```

2. If the DNS queries fail, configure your system to use a reachable DNS server:

   Example

   ```
   echo "nameserver 8.8.8.8" >> /etc/resolv.conf
   ```

3. Confirm the device's default gateway and routing table are correct.
4. Check if you can reach the cluster URL:

Example

```
ping us.ciscoiot.com
curl -v https://us.ciscoiot.com/sramgmt/auth/token
```

The device should now be able to resolve `us.ciscoiot.com` and similar domains using the updated DNS server.

CV SRA agent failures

Highlights CV SRA agent failures, which are system problems that prevent the CV SRA agent from starting, installing, or operating properly, and often require troubleshooting to restore normal function.

CV SRA agent failures are system problems that prevent the CV SRA agent from starting, installing, or operating properly, and often require targeted troubleshooting to restore normal function.

- Can result from hardware faults, configuration errors, or connectivity issues.
- Disrupt essential operations and typically trigger error messages or log alerts.
- Often require targeted troubleshooting to restore normal function.

CV SRA agent failure causes and impact

CV SRA agent failures can occur due to a variety of underlying issues and typically require troubleshooting to resolve.

Examples of CV SRA agent failures

- The CV SRA agent goes down after a power outage and fails to restart.
- The CV SRA agent cannot be installed because IOx status cannot be verified.
- “Failed to install CV SRA agent. Device is unreachable” error appears during installation.

Causes and consequences of CV SRA agent SD card failures

Explains the causes and consequences of SD card failures in the CV SRA agent, including the effects of power outages and the need for manual intervention.

A power outage can cause the SD card used by the CV SRA agent to become faulty or switch automatically to “read-only mode.”

When this happens:

- The SD card develops a fault that prevents normal device operations.
- The SD card’s file system changes to read-only, blocking necessary writes and agent activities.

If either issue occurs, manual intervention is required to repair or replace the SD card. Automatic recovery is not possible.

Diagnose and fix CV SRA agent installation failures due to IOx issues

Provides instructions to troubleshoot and resolve CV SRA agent installation failures that are caused by IOx configuration or service status issues on managed devices.

Diagnose and resolve CV SRA agent installation failures related to IOx configuration or service status.

Installation errors such as “Installation of the CV SRA agent failed due to inability to verify IOx status” often occur when IOx services are down, application management is not enabled, or the device appears “down” in IoTOD.

Before you begin

Gather device details and ensure you have access to Application Manager and device event logs.

Procedure

1. Verify event logs and confirm that “application management is enabled.”
2. Check IOx status.
   - For externally managed devices:
     - Go to Application Manager > Devices > Device > Summary.
     - If IOx is down, review “View Details” and event logs.
     - Use “Refresh IOx” and retry installation.
     - Or, run

       ```
       show IOx
       ```

       from Application Manager > Devices > Troubleshooting > IOS Show Commands.

3. If the device appears “down” in IoTOD, perform the following checks.
   - Confirm IOx is enabled.
   - Ensure the IOx interface is active (

     ```
     no shut
     ```

     ):
     - Check the g2 interface for IR809
     - Check the g5 interface for IR829
   - Validate NAT configuration with

     ```
     show run | sec IOx
     ```

     .
   - Run

     ```
     show IOx
     ```

     to confirm IOx services are running.
   - Download the tech support bundle (if available) and analyze CAF logs.
4. For externally managed IE3000 devices, verify configuration.
   - Verify that the CLI configuration matches the CV SRA workflow configuration.
   - Ensure all management VLAN settings (VLAN ID, IP address, subnet, DNS, and gateway) are correct.

The CV SRA agent installs successfully once IOx services and configurations are corrected.

What to do next

Monitor event logs to confirm the installation and health of the agent.

Diagnose and fix CV SRA agent installation failures due to IOx issues

Provides instructions to troubleshoot and resolve CV SRA agent installation failures that are caused by IOx configuration or service status issues on managed devices.

Diagnose and resolve CV SRA agent installation failures related to IOx configuration or service status.

Installation errors such as “Installation of the CV SRA agent failed due to inability to verify IOx status” often occur when IOx services are down, application management is not enabled, or the device appears “down” in IoTOD.

Before you begin

Gather device details and ensure you have access to Application Manager and device event logs.

Procedure

1. Verify event logs and confirm that “application management is enabled.”
2. Check IOx status.
   - For externally managed devices:
     - Go to Application Manager > Devices > Device > Summary.
     - If IOx is down, review “View Details” and event logs.
     - Use “Refresh IOx” and retry installation.
     - Or, run

       ```
       show IOx
       ```

       from Application Manager > Devices > Troubleshooting > IOS Show Commands.
3. If the device appears “down” in IoTOD, perform the following checks.
   - Confirm IOx is enabled.
   - Ensure the IOx interface is active (

     ```
     no shut
     ```

     ):
     - Check the g2 interface for IR809
     - Check the g5 interface for IR829
   - Validate NAT configuration with

     ```
     show run | sec IOx
     ```

     .
   - Run

     ```
     show IOx
     ```

to confirm IOx services are running.

- Download the tech support bundle (if available) and analyze CAF logs.

4. For externally managed IE3000 devices, verify configuration.
   - Verify that the CLI configuration matches the CV SRA workflow configuration.
   - Ensure all management VLAN settings (VLAN ID, IP address, subnet, DNS, and gateway) are correct.

The CV SRA agent installs successfully once IOx services and configurations are corrected.

What to do next

Monitor event logs to confirm the installation and health of the agent.

Resolve the "pending services update" state

Provides instructions to resolve issues when an organization is stuck in a “Pending Services Update” state and restore it to Active.

Resolve “Pending Services Update” issues so the organization can return to Active status.

Organizations may become stuck in the “Pending Services Update” state due to incomplete or failed service updates during configuration.

Before you begin

Ensure you have access to the parent organization and the necessary privileges for editing organization services.

Procedure

---

1. Log into the parent organization, ideally the one used to create the affected organization.
2. Select **Access Control** and switch to the **Organizations** tab.
3. Click the affected organization to view details.
4. Address any error messages that require user action, following the provided guidance.
5. If services remain in a pending state, wait a couple of minutes to allow for system recovery.
6. If still unresolved, click **Edit Organization**, deselect the problematic service, and save.
7. Re-select the service and save again. Verify its status is **Active.** If not, remove and re-add the service as needed.
8. For services in “pending removal,” edit the organization, add the service back and save, then remove it again. Repeat until the state is Active.

The organization's status returns to Active.

Resolve the "pending creation" state

Provides instructions to fix situations where an organization is stuck in a “Pending Creation” state and activate it.

Activate an organization that is stuck in the “Pending Creation” state.

Errors during organization creation may prevent activation and leave the status as “Pending Creation.”

Before you begin

Make sure you can delete and recreate organizations if required.

Procedure

1. Log into the parent organization.
2. Go to **Access Control > Organizations** and select the affected organization.
3. Resolve any error messages shown for services in pending creation.
4. Wait briefly to see if the service restores itself.
5. If the status remains stuck, delete the organization and recreate it.
6. After recreating, verify the status is Active.
   - If the status becomes “pending removal,” follow the procedure for that scenario.

The organization's status is set to Active or you are ready to resolve a “Pending Removal” situation.

Resolve the "pending removal" state

Provides instructions to complete the deletion of an organization stuck in a “Pending Removal” state.

Remove organizations that are stuck in the “Pending Removal” state.

Organizations may remain in the “Pending Removal” state if there are unresolved dependencies or system delays.

Before you begin

Confirm that device dependencies are removed and you have permission to delete organizations.

Procedure

1. Log into the parent organization and go to Organizations.
2. Select the target organization to view error details.
3. Resolve any outstanding issues (for example, remove devices if prompted).
4. If the service is stuck in pending removal without any error, wait a few minutes and try again.
5. Retry deletion as needed until the organization is fully removed.

The organization is successfully deleted.