

Cisco IQ Virtual Appliance Operations Guide

v1.2.0

Introduction

Cisco IQ™ provides you with enhancements and features designed to improve asset visibility, deliver smarter insights across their environments, and streamline case management. In addition, AI features such as the Cisco IQ AI Assistant optimize operational outcomes and the Cisco IQ user experience by providing contextual understanding that empowers you to make proactive, informed decisions and streamline processes for customer engagement and success.

Cisco IQ On-Prem Air-Gapped is one of the deployment modes of Cisco IQ, designed for customers in highly regulated industries with stringent compliance, data sovereignty, and security requirements. In this mode, Cisco IQ is delivered as a self-contained Virtual Machine (VM) referred to as the Cisco IQ Virtual Appliance (VA). The VA runs entirely on the customer's premises and operates in complete isolation from external networks. To maintain this isolation, software updates and maintenance packages are obtained from Cisco IQ SaaS and transferred to the VA through an approved, manual process.

Cisco IQ On-Prem Air-Gapped extends key capabilities of Cisco IQ SaaS to air-gapped environments, enabling mission-critical teams to operate with speed and diagnostic intelligence comparable to cloud-connected enterprises.

To access the Cisco IQ VA, open a supported browser and navigate to <https://<fqdn-of-the-appliance>>. Log in using the admin username and password set during the installation process.



Note: The Cisco IQ VA is currently limited to customers enrolled in the Controlled Availability program. Download access for the VA system software and additional operational packages (modules, rules, and entitlements) from Cisco IQ portal is available exclusively to select customers. Please contact your account representative for more information.

Connection Management (Data Collection)

Cisco IQ VA is an on-premises solution for network data collection to provide deep visibility into your infrastructure. It collects data through Catalyst Center and Direct Connection. It simplifies how you manage network authentication and device discovery. Configuring data collection consists of:

- **Creating Credential Sets:** Establish the authentication protocols (for example, Simple Network Management Protocol (SNMP) v1/v2c/v3) to communicate with your network devices. Centralizing credentials by security zone or location (for example, “SanJose-SNMPv3”) allows you to update passwords in one location, with changes automatically propagating to all associated devices.
- **Mapping credentials to Inventory:** Map your Credential Sets with your Inventory Assets to automate the authentication process. By creating rules that link specific IP ranges to defined Credential Sets, the system automatically applies the correct

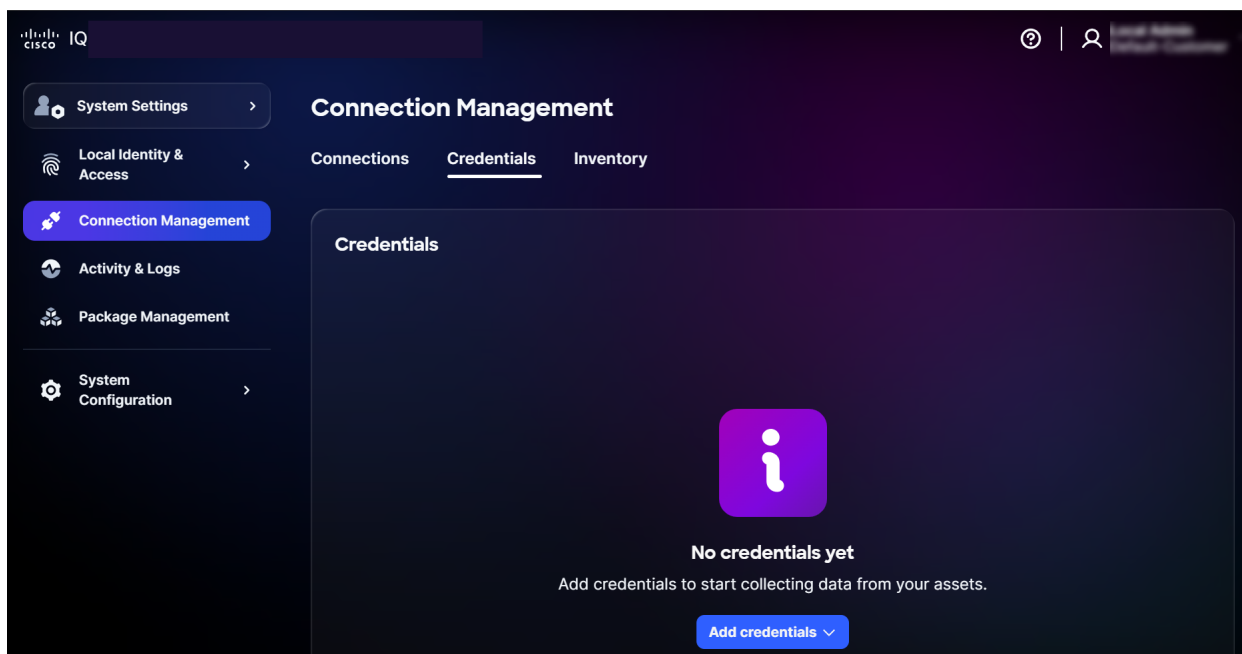
authentication during data collection. This eliminates manual entry errors and ensures your configuration remains accurate as your network grows.

 **Note:** SNMPv2c/SNMPv3 and SSH are required for device discovery, and HTTP/HTTPS credentials must be provided before configuring Catalyst Center.

Adding Credentials

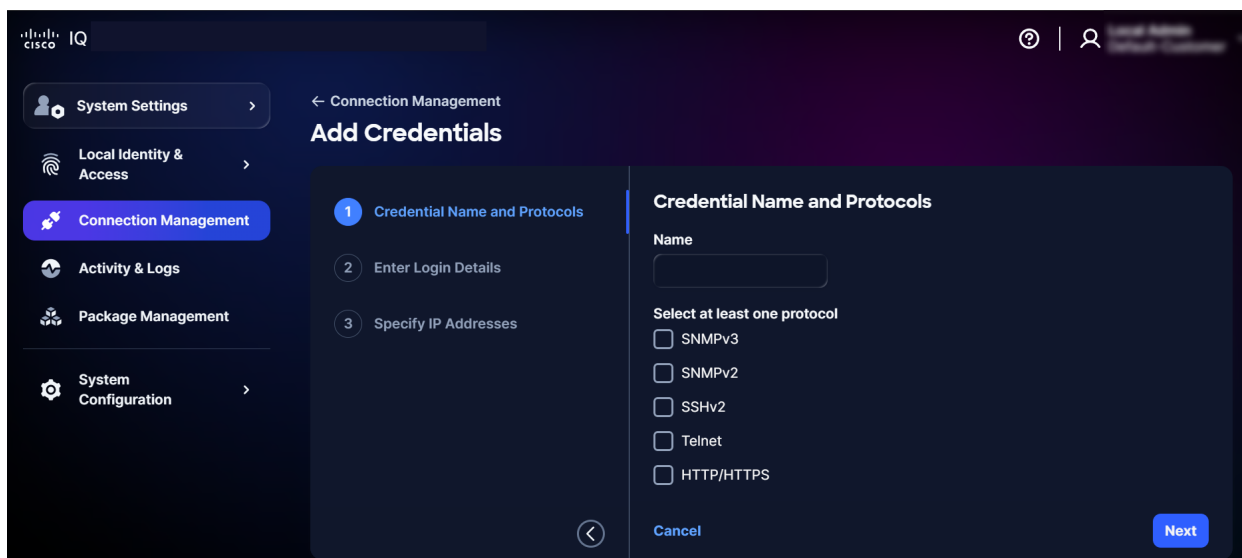
You must first add credentials to perform data collection. To add credentials:

1. From **System Settings**, choose **Connection Management**. The **Connection Management** page displays.
2. Click the **Credentials** tab.



Credentials Tab

3. Click **Add credentials**.



Add Credentials

4. Enter a **Name**.
5. Check all applicable protocol check boxes.
6. Click **Next**.

The screenshot shows the 'Add Credentials' wizard in Cisco IQ. The left sidebar contains navigation links: System Settings, Local Identity & Access, Connection Management (highlighted), Activity & Logs, Package Management, and System Configuration. The main panel is titled 'Add Credentials' and shows a progress bar with three steps: 1. Credential Name and Protocols (checked), 2. Enter Login Details (active), and 3. Specify IP Addresses. The 'Enter Login Details' section is for 'SNMPv3' and includes fields for Username, Engine ID (optional), Authorization algorithm, Authorization password (with a 'Show' button), Privacy algorithm (optional), and Privacy password (with a 'Show' button). At the bottom are 'Cancel', 'Back', and 'Next' buttons.

Add Credentials Details

 **Note:** For the image above, the view when all protocols are selected in the previous step is illustrated. Your interface only displays the protocols you chose.

7. Enter the login details for each protocol that was selected.
8. Click **Next**.

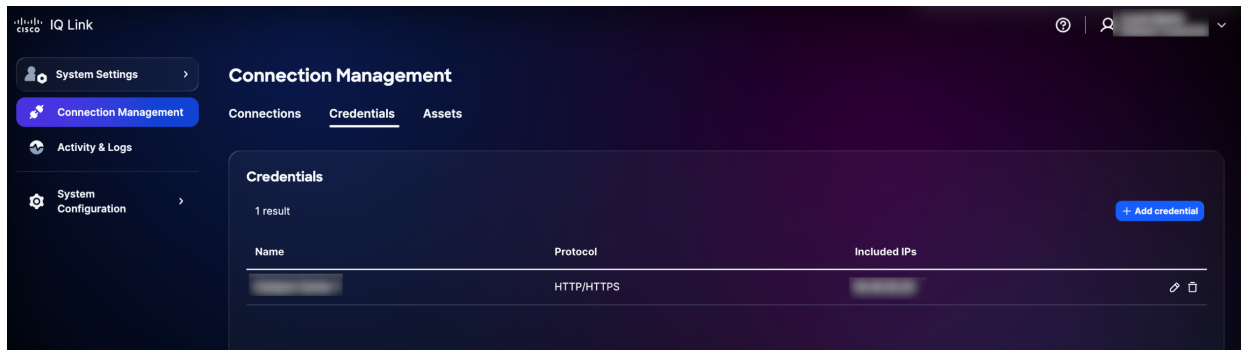
The screenshot shows the 'Add Credentials' wizard in Cisco IQ, Step 3: Specify IP Addresses. The left sidebar is the same as the previous screenshot. The main panel shows the progress bar with steps 1, 2, and 3 (active). The 'Specify IP Addresses' section has a text area for 'Included IPs' with a placeholder example: 'e.g. *.*.*.*, 192.168.1.0/24, 172.16.*.*'. At the bottom are 'Cancel', 'Back', 'Save and add another credential', and 'Save' buttons.

Specify IP Addresses

9. Enter the **Included IPs**.

 **Note:** This field defines the IP addresses or IP ranges where the credentials can be used to establish a connection. It supports a mix of IPs and IP masks (using wildcard notation). For details on supported formats, see [Credential Selection and Matching Logic](#).

10. Click **Save**. A confirmation displays and you are redirected to the **Credentials** tab.



Credentials Added

You can edit the credentials by clicking the **Edit** icon and delete them by clicking the **Delete** icon.

Credential Selection and Matching Logic

The telemetry engine employs a priority-based matching logic to determine which credentials to apply during discovery and collection. Understanding this hierarchy ensures that the correct credentials are used for the intended devices.

- **Priority Ranking:** When multiple credential sets apply to a device, Cisco IQ evaluates them based on how specifically they match the device; the system applies the following priority, with more specific matches taking precedence:
 - **Exact IP match:** Highest priority
 - **Trailing Wildcard Match:** Priority depends on the number of trailing stars; fewer stars indicate a more specific match and therefore higher priority
- **Wildcard Formatting Rules:** Wildcards (*) are only supported as trailing characters in an IP address; they must be applied from right to left.
 - Supported Formats:
 - 1.2.3.* (highest priority)
 - 1.2.*.*
 - 1.*.*.*
 - *.*.*.* (lowest priority)
 - Unsupported Formats:
 - Leading wildcards (for example, *.1.2.3)
 - Wildcards between octets (for example, 10.10.*.20)
 - Use of dashes or other non-standard delimiters

Credential Selection Example:

The following table illustrates how the telemetry engine selects the most appropriate credential set when a device matches multiple defined patterns.

Table 1: Credential Selection Example

Device IP	Available Credential Sets	Selected Credential Set
10.10.1.5	10.10.1.5, 10.10.1., 10.10..*	10.10.1.5 (Exact Match)
10.10.2.15	10.10.2., 10.10..*	10.10.2.* (More specific)
10.10.5.50	10.10., ...	10.10.. (More specific)

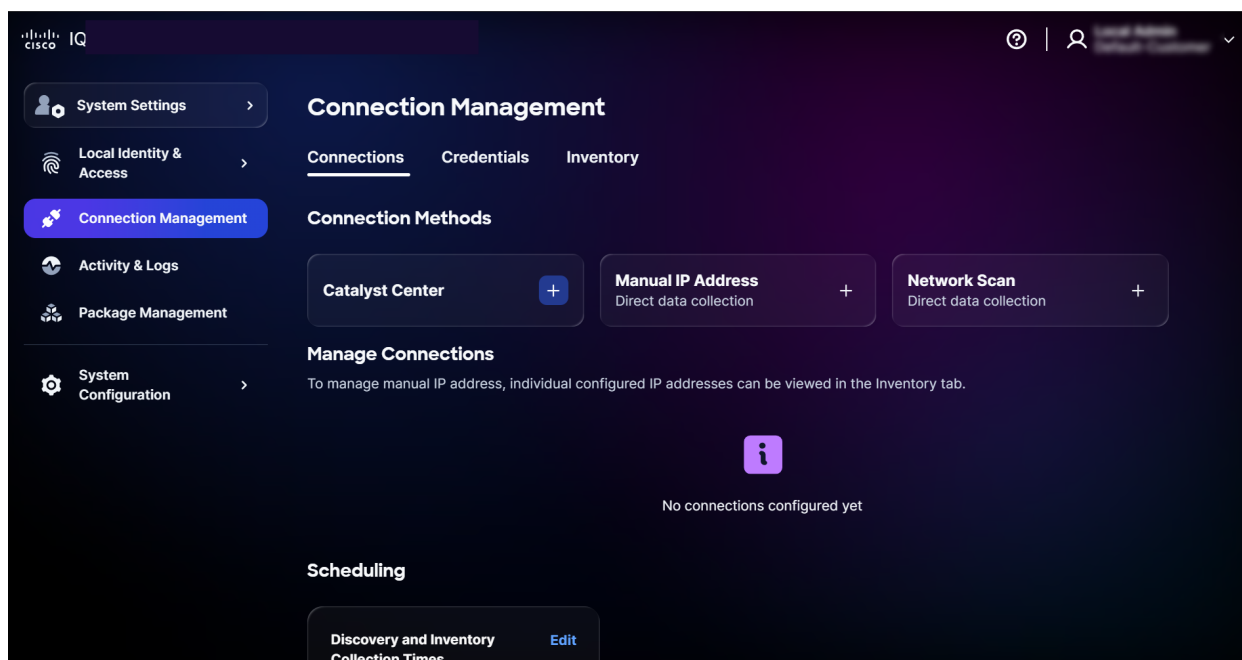
 **Note:** If a device falls into multiple overlapping categories, the system always selects the credential set with the highest specificity (in other words, the fewest trailing wildcards).

Data Collection Using Catalyst Center

You can connect up to 20 Catalyst Centers (non-cluster) for each instance of Cisco IQ VA.

For data collection using Catalyst Center:

1. From **System Settings**, choose **Connection Management**. The **Connection Management** page displays.



Connection Management

2. Click the **Catalyst Center** option.

Add Catalyst Center

3. Enter the **IP Address** or **FQDN**.
4. Choose a configured HTTP/HTTPS credential from the **Select credential** drop-down list.
5. Click **Submit**. A confirmation displays (can take up to 75 minutes). You can view the newly added Catalyst Center under Configured Connections.
6. Schedule a collection. See [Scheduling](#) for more details.

 **Note:** Cisco IQ VA is pre-configured with an automated scheduling setup and the system initiates a default automated collection schedule. It is highly recommended that you edit the schedule to align with your organization's requirements and maintenance windows.

Manual Data Collection

To add devices for direct data connection:

1. From **System Settings**, choose **Connection Management**. The **Connection Management** page displays.

Discovery and Inventory Collection Times	
Discovery	Weekly on Sundays at 07:30 AM IST

Connection Management

2. Click **Manual IP Address**. The **Direct Connection** page displays with two (2) options to collect data.

The screenshot shows the Cisco IQ interface for 'Direct Connection'. On the left is a sidebar with navigation links: System Settings, Local Identity & Access, Connection Management (highlighted), Activity & Logs, Package Management, System Configuration, and System Configuration. The main content area is titled 'Direct Connection' and features a warning message: 'Add credentials before form submission to ensure an immediate, successful discovery. Re-discovery will run on schedule until credentials are provided.' Below this, the 'Choose a Method of Entry' section has two radio buttons: 'Upload a file' (selected) and 'Specify individual devices'. A text prompt says 'Download the template and add your device information. Then attach the file below.' A large dashed box contains an upload icon and the text 'Click or drag file to this area to upload' and 'Only one CSV file can be uploaded. 50,000 assets maximum.' At the bottom are 'Submit' and 'Cancel' buttons.

Upload File

3. Click the preferred option from **Choose a Method of Entry** and provide your device information using one of the following methods:

- **Upload a file:** Click or drag-and-drop the file

This screenshot shows the same Cisco IQ interface, but the 'Specify individual devices' radio button is now selected. The 'Enter hostnames or IP addresses' text box is visible, containing the example text 'e.g. 1.111.111.00.1.1, hostname.local, 1.1.1.1, hostname.dmz.local'. The 'Submit' and 'Cancel' buttons remain at the bottom.

Specify individual devices

- **Specify individual devices:** Enter either a single hostname, IP addresses, or a comma-separated list of hostnames and/or IP addresses

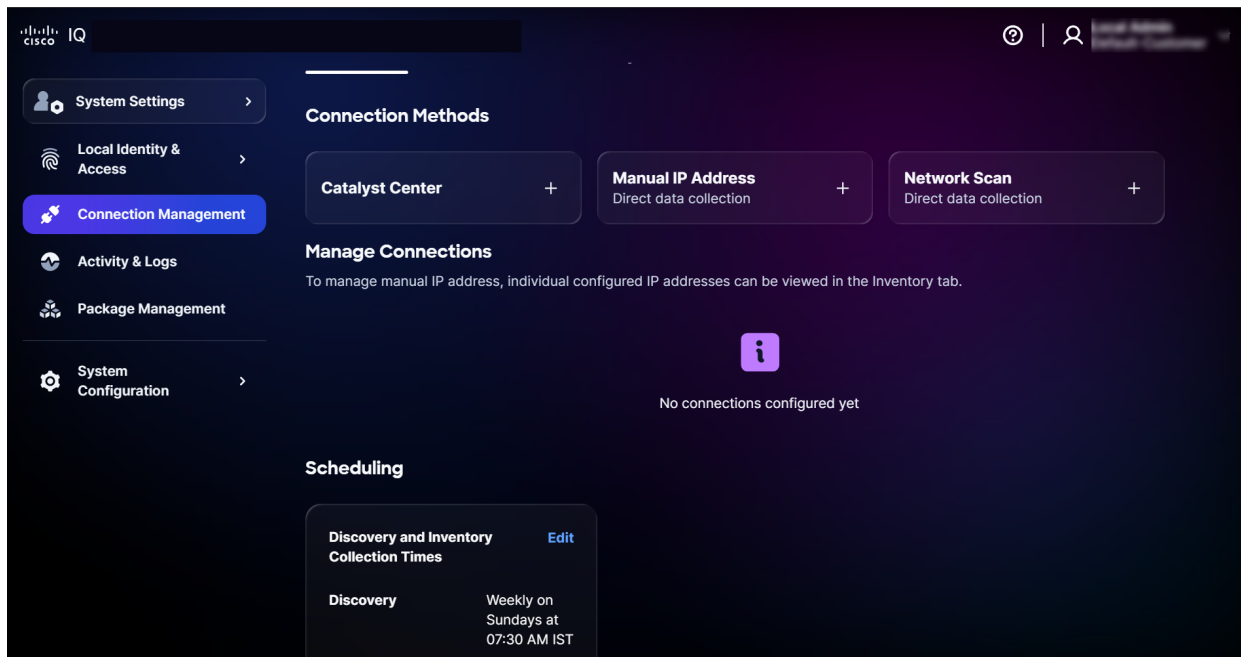
4. Click **Submit**. You are redirected to the **Assets** tab after successful submission.

5. Schedule a collection. See [Scheduling](#) for more details.

 **Note:** Cisco IQ VA is pre-configured with an automated scheduling setup and the system initiates a default automated collection schedule. It is highly recommended that you edit the schedule to align it with your organization's requirements and maintenance windows.

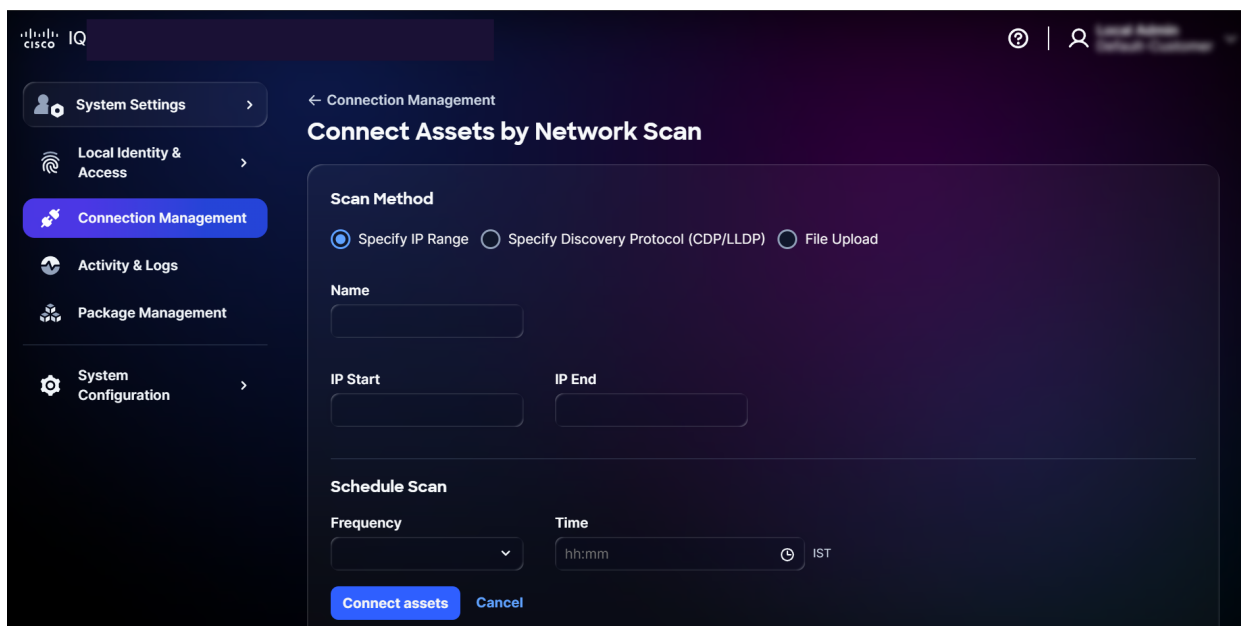
Network Scan

1. From **System Settings**, choose **Connection Management**. The **Connection Management** page displays.



Network Scan

2. Click **Network Scan**. The **Connect Assets by Network Scan** page displays with three (3) options.



- **Specify IP Range:** Define a range of IP addresses to target devices within that range for network discovery or management tasks
 - **Specify Discovery Protocol (CDP/LLDP):** Choose the network discovery protocol to use
 - **File Upload:** Upload a file, such as configuration files or data
3. Enter **Name**.
 4. Enter IP Start and IP End.
 5. Under **Schedule Scan**, choose Frequency and Time.
 6. Click **Connect assets**.

Scheduling

Scheduling allows you to define when Cisco IQ VA performs automated data collection. To schedule collection:

1. In the **Scheduling** section on the **Connection Management** page, click **Edit** for the schedule you want to modify. The **Edit Schedule** page displays.

Edit Schedule

2. In the **Schedule Discovery** section, choose your preferred **Frequency** and **Day** from the drop-down lists and enter your desired start **Time**.
3. In the **Schedule Inventory Collection** section, choose your preferred **Frequency** from the drop-down lists and enter your desired start **Time**.
4. Click **Submit**.



Note: Allow 5–10 minutes for any changes made to discovery or collection schedules to synchronize and reflect accurately within Virtual Appliance.

Installing Packages (Modules, Rules, and Entitlements)

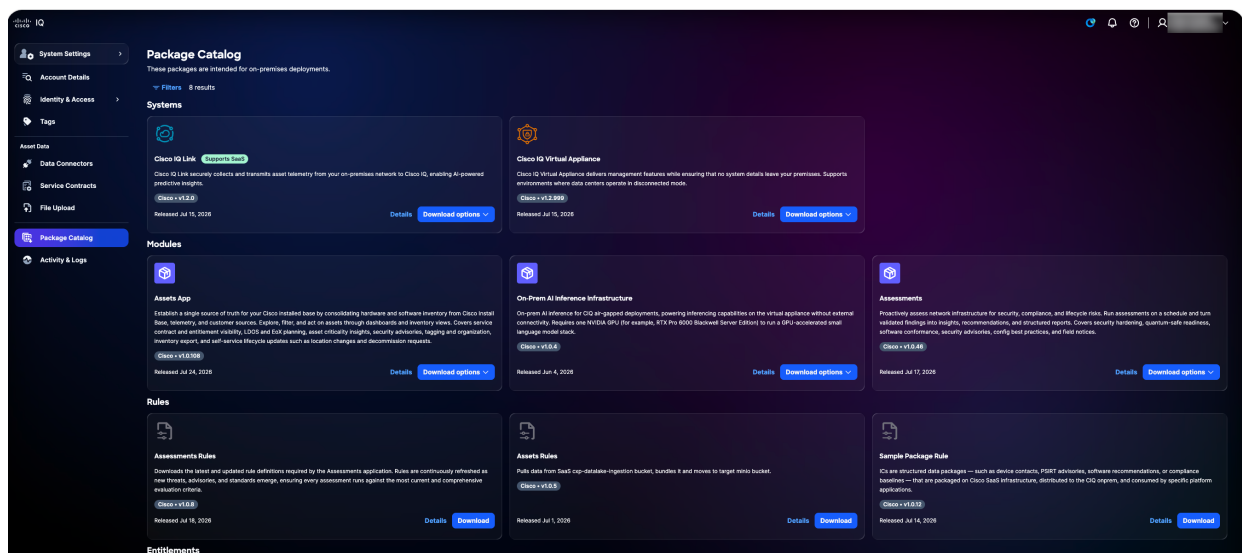
You can manage the software lifecycle (that is, installation and configuration) of operational

modules, rules, entitlements, and specialized AI-powered features within the VA. You can install them by downloading the latest versions from Cisco IQ (SaaS) by navigating to the **Package Catalog**. The Package Catalog displays software instances available to you. It empowers you to monitor and manage updates seamlessly, ensuring efficient tracking and management of your system instances.

Adding Modules

A module is a standalone software package providing core functionality within the VA. It is an independent service with its own lifecycle, allowing for installation, maintenance, and resizing. The resource consumption—including CPU, Graphics Processing Unit (GPU), and RAM—is dynamically assigned based on the deployment size (Small, Medium, or Large) selected during the initial installation.

1. Log in to [Cisco IQ](#).
2. Navigate to **System Settings > Package Catalog**.

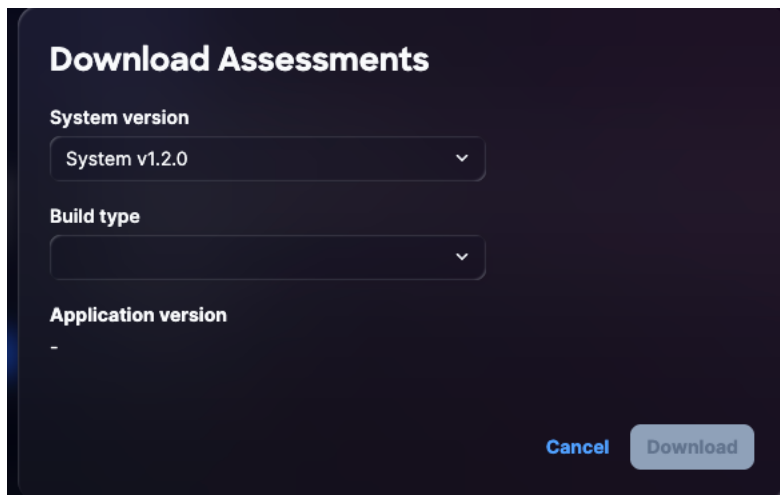


Package Catalog

3. From the desired module card, click **Download options > Installation packages**. The **Download** window opens.



Note: The Assessment module is used for the example images.

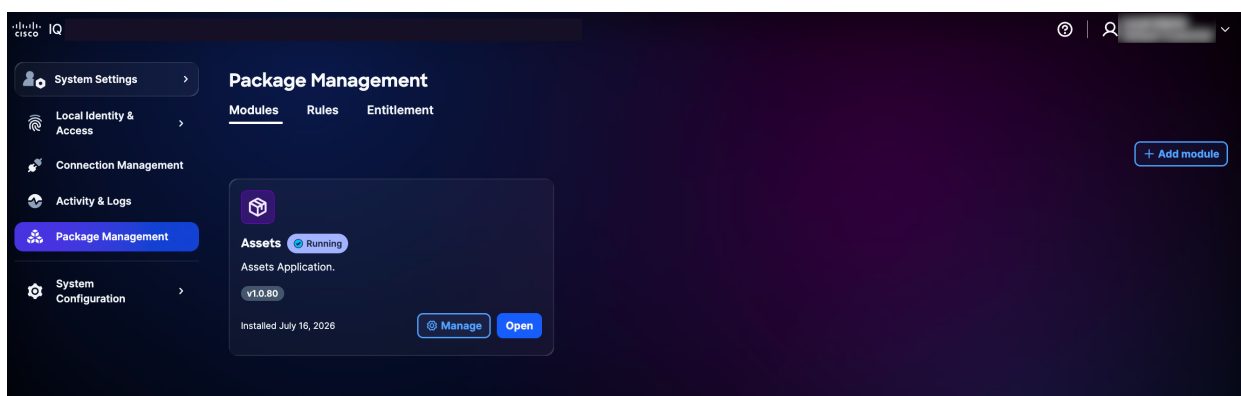


Download

4. Choose a **System Version** from the drop-down list.
5. Choose a **Build type** from the drop-down list.
6. Click **Download** to save the file locally.

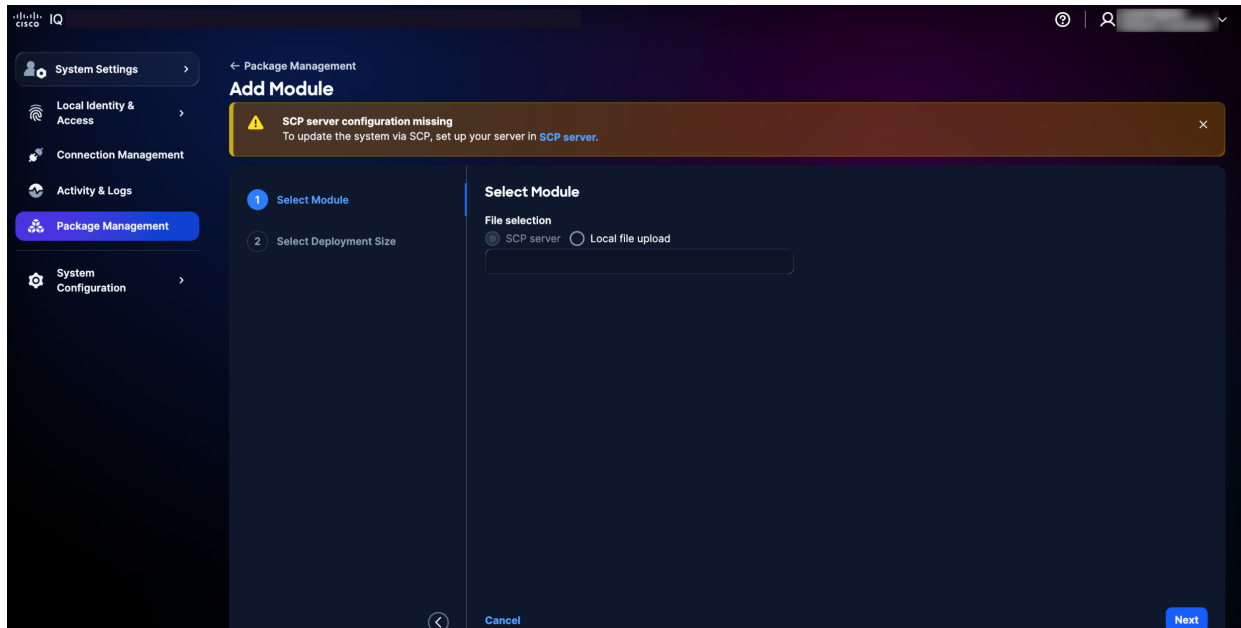
 **Note:** The installation files are large (10-25 GB); ensure you have sufficient disk space before downloading.

7. Navigate to VA.
8. Navigate to **Home > System Settings > Package Management**. The **Package Management** page displays with the following tabs:
 - Modules
 - Rules
 - Entitlements



Modules

9. Click **Add module**.

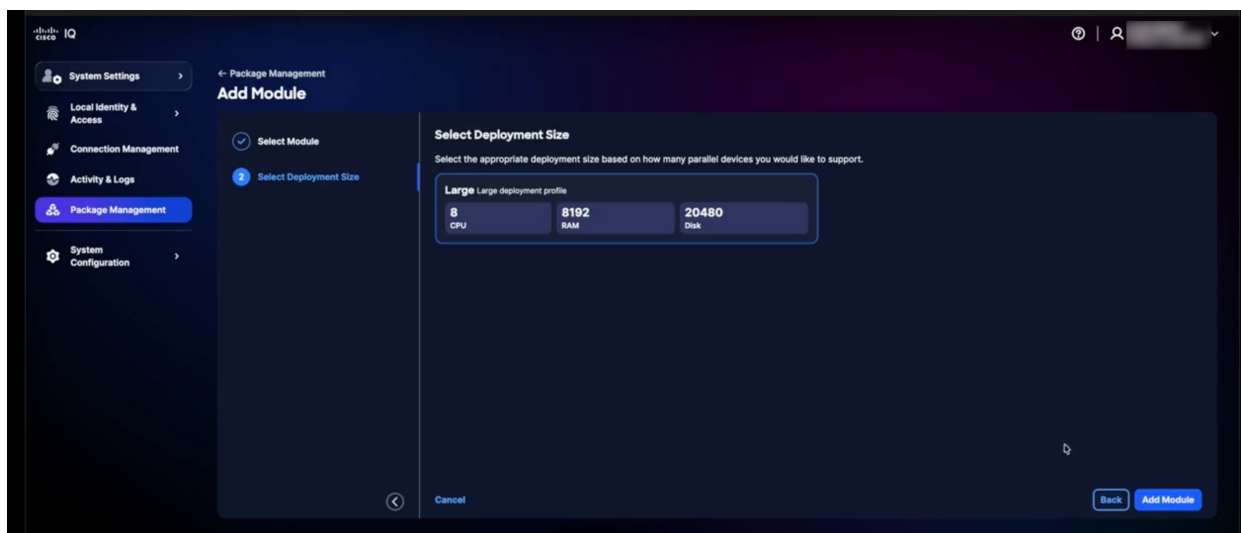


Add Module

10. Choose your preferred **File selection** option:

- **SCP server:** Enter the exact file name of the installation package (recommended for large files)
- **Local file upload:** Drag-and-drop the downloaded installation file (not recommended for files 30 GB or larger due to upload time)

11. Click **Next**.



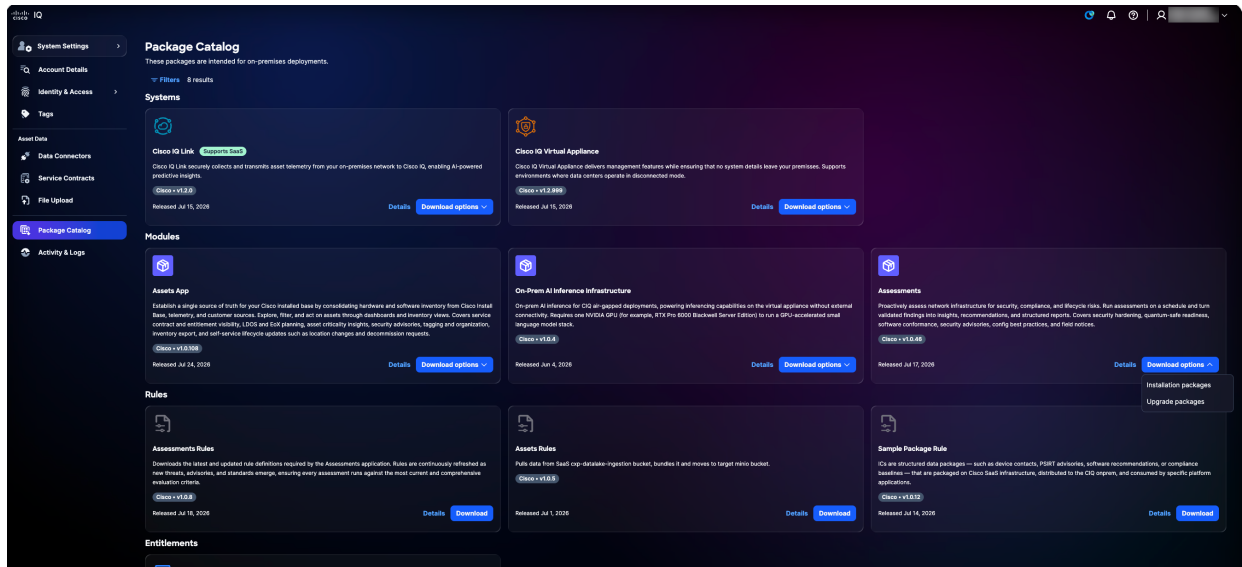
Deployment Size

12. Choose the **Deployment Size** (for example, Small, Medium, or Large). These sizes are pre-defined and dictate the resource requirements.

13. Click **Add Module**. The newly installed module display on the **Modules** tab in **Package Management**. Once complete, the module status changes to “Running,” and the **Open** button becomes available.

Upgrading a Module

The latest modules are continuously being updated in **Package Catalog** (in Cisco IQ). To upgrade to the latest version:



Connect Assets by Network Scan

1. From the desired module card, click **Download options** > **Upgrade packages**. The **Download** window opens.



Note: The Assessment module is used as an example for the images.

Upgrade Assessments

System version

System v1.2.0

Current app version

Build type

Application version

-

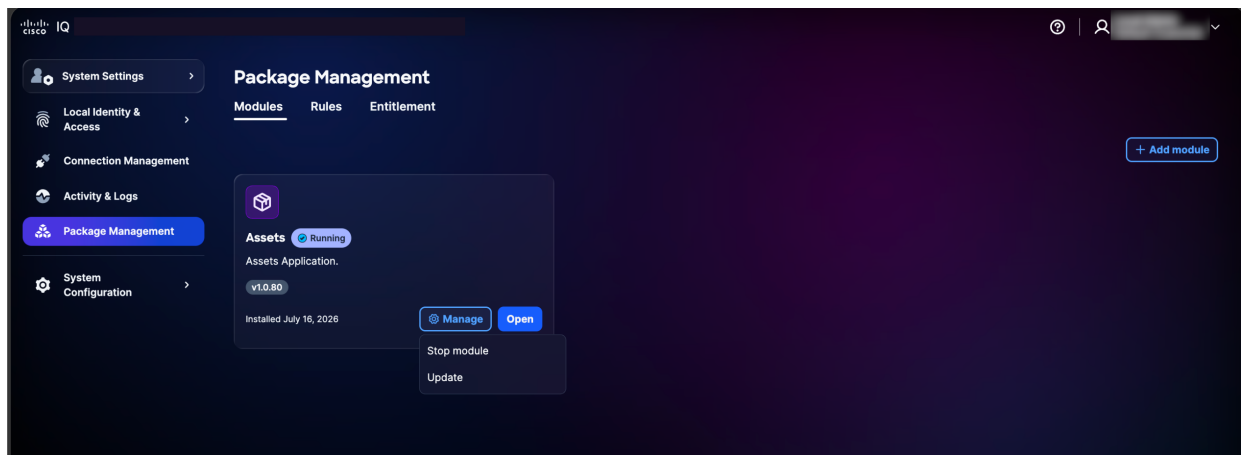
Cancel **Download**

Download

2. Choose a **System version** from the drop-down list.
3. Choose a **Current app version** from the drop-down list.
4. Choose a **Build type** from the drop-down list.
5. Click **Download** to save the file locally.
6. Navigate to VA and complete the installation of downloaded file.

Managing Modules

After adding a module, you can modify it from the **Package Management** page by clicking **Manage**. The available modification options include resizing and upgrading to a higher version. To manage a module:



Update Type

1. From the **Package Management** page, click **Manage > Update** for the desired module.
2. Choose the **Update type**:
 - **Change deployment size only**
 - **Update version**
3. If **Change deployment size** is selected, click **Next** and choose the new deployment size on following page.

OR

If **Update Version** is selected, the **File selection** option displays. Choose either **SCP Server** and enter the exact file name of the installation package or choose **Local file upload** and drag-and-drop the downloaded installation file.

4. Click **Next**. The **Select Update Schedule** page displays.
5. Choose from the following radio button options to update the schedule:
 - **Update Now**
 - **Update Later**



Note: Some modules support updates without any downtime. If downtime is required, a banner displays the details.

6. If **Update later** is selected, enter the **Date** and **Time**.
7. Click **Next**. The **Update Summary** displays.

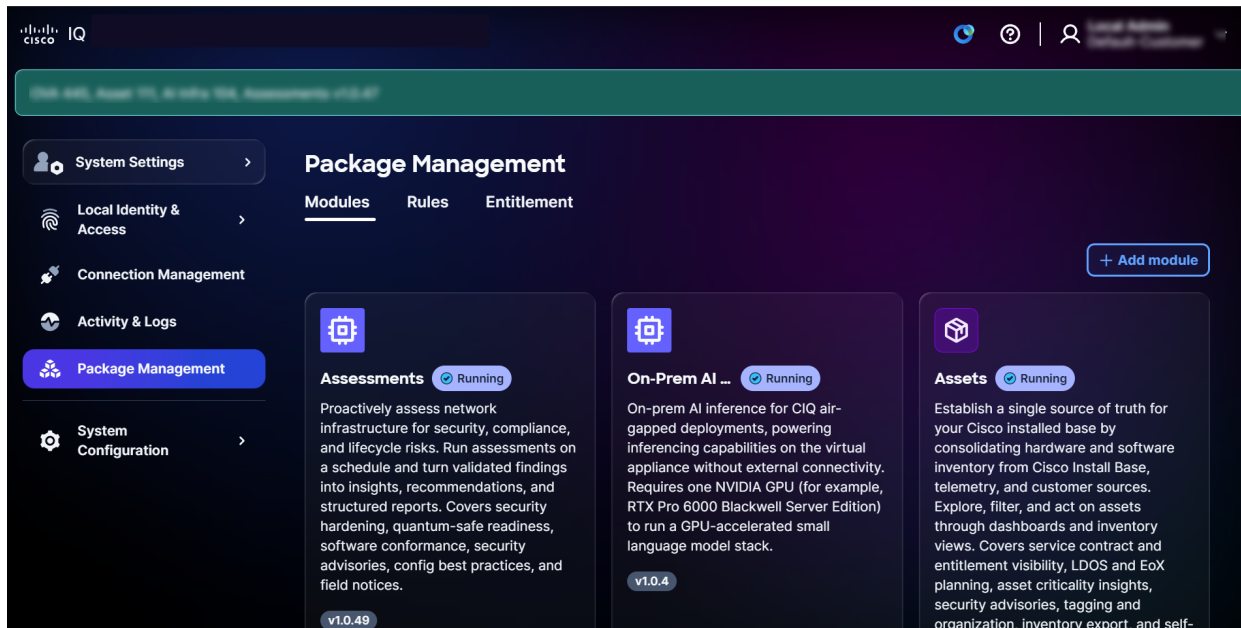


Note: You can access Release Notes from the **Update Summary**.

8. Click **Update Module** and navigate to the **Module** tab. The module displays an “update scheduled” status.

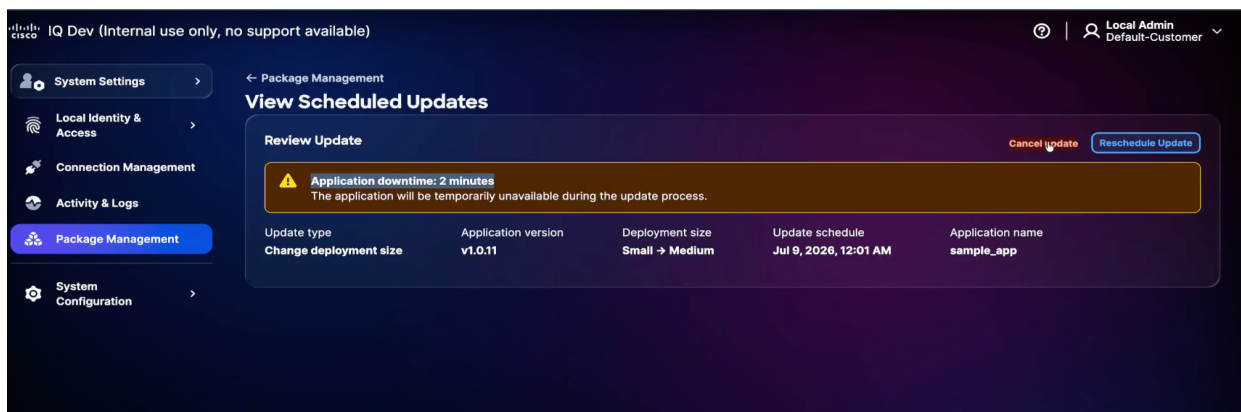
Editing Schedules

You can also view, edit, or cancel scheduled updates. To edit or cancel a scheduled update:



Editing Schedule

1. From the **Package Management** page, click **Manage > View Scheduled update** of the desired module. The **View Scheduled Updates** window displays.



Schedule Updates

2. Click **Cancel Update** or **Reschedule Update** as required.
3. Follow the on-screen instructions to complete the operations.

 **Note:** If a module operation (for example, installation, upgrade, or resize) fails, choose one of the following options:

Retry: The UI displays a Retry button, allowing you to attempt the operation again.

Logs: If an error persists, click Logs to view detailed diagnostic information. This is the primary method for identifying the cause of installation or runtime failures.

Installing Rules

A rule is a specialized component or “add-on” that extends or modifies the functionality

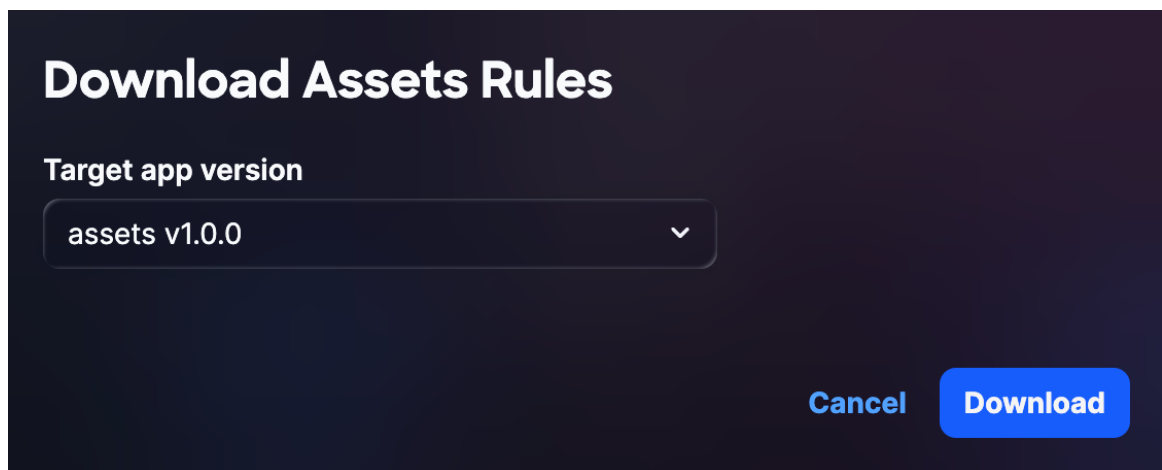
of an existing module. Rules are not designed to run as stand-alone programs; they are “plugged into” a module to provide specific rules, logic, or features. Rules are tied to specific modules. When a rule is installed, it is linked to the module it supports. Rules allow the system to be updated or customized without requiring a full upgrade of the core module. If a new set of rules or features is needed, you can simply add a new rule to the existing module.

To download a rule:

1. Log in to [Cisco IQ](#).
2. Navigate to System Settings > Package Catalog.
3. From the desired rule card, click **Download**.



Note: The following example image is for an Assets rule.



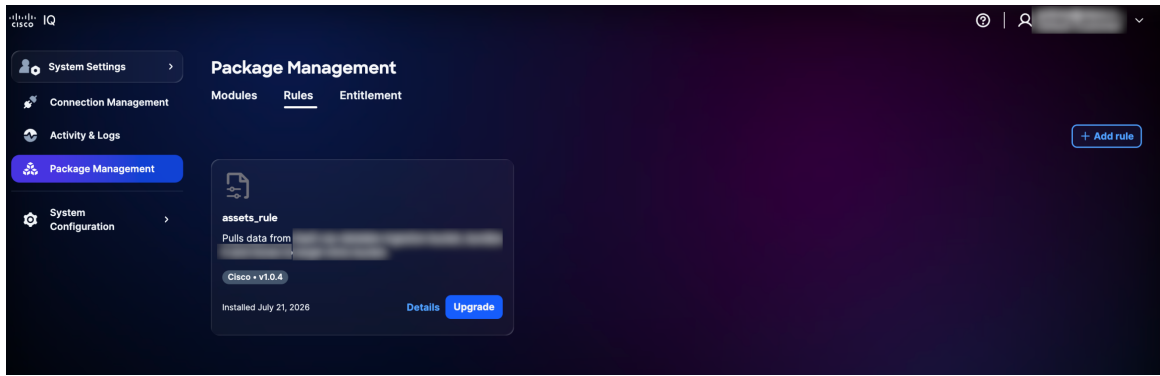
Download

4. Choose a **Target app version** from the drop-down list.
5. Click **Download** to save the file locally.



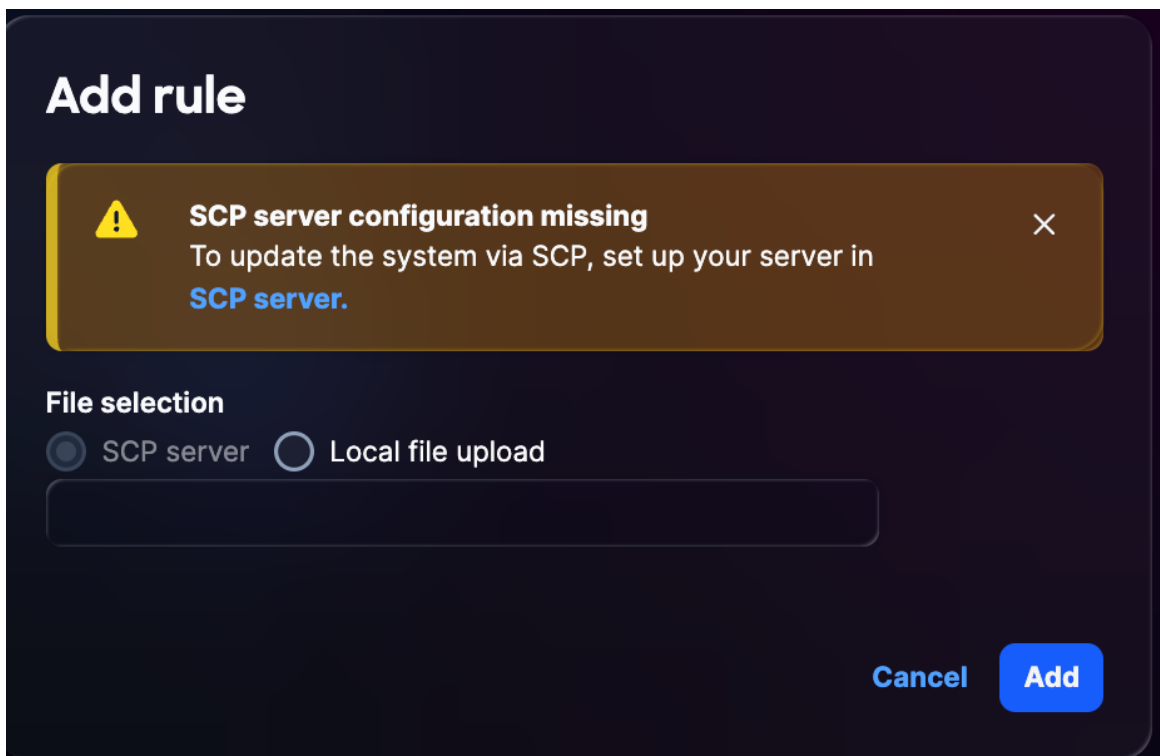
Note: Installation files are large (10-25 GB); ensure you have sufficient disk space before downloading.

6. Navigate to VA.
7. Navigate to **Home > System Settings > Package Management**. The **Package Management** page displays with the following tabs.
 - Modules
 - Rules
 - Entitlements
8. Click the **Rules** tab.



Package Management

9. Click **Add rule**.



Add Rule

10. Choose your preferred **File selection** option:

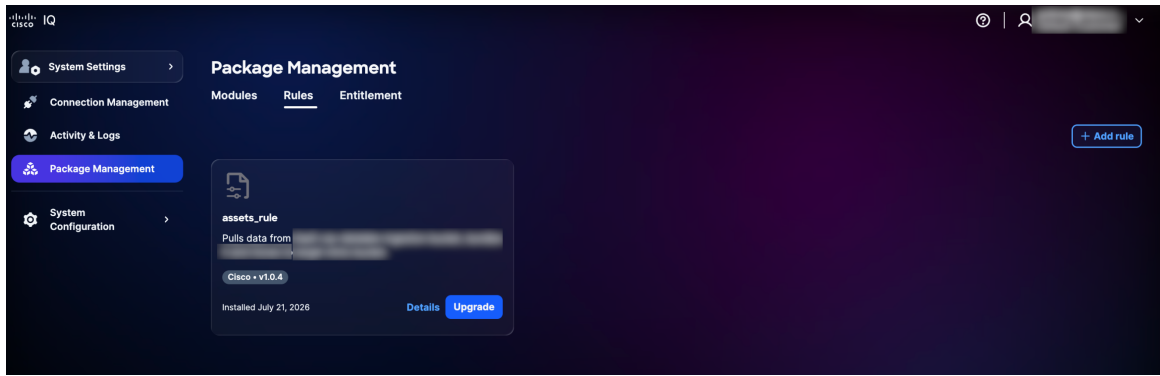
- **Secure Copy Protocol (SCP) server:** Enter the exact file name of the installation package. This method is recommended for large files.
- **Local file upload:** Drag-and-drop the downloaded installation file.

11. Click **Add**. The added rule displays in **Package Management**.

Upgrading Rules

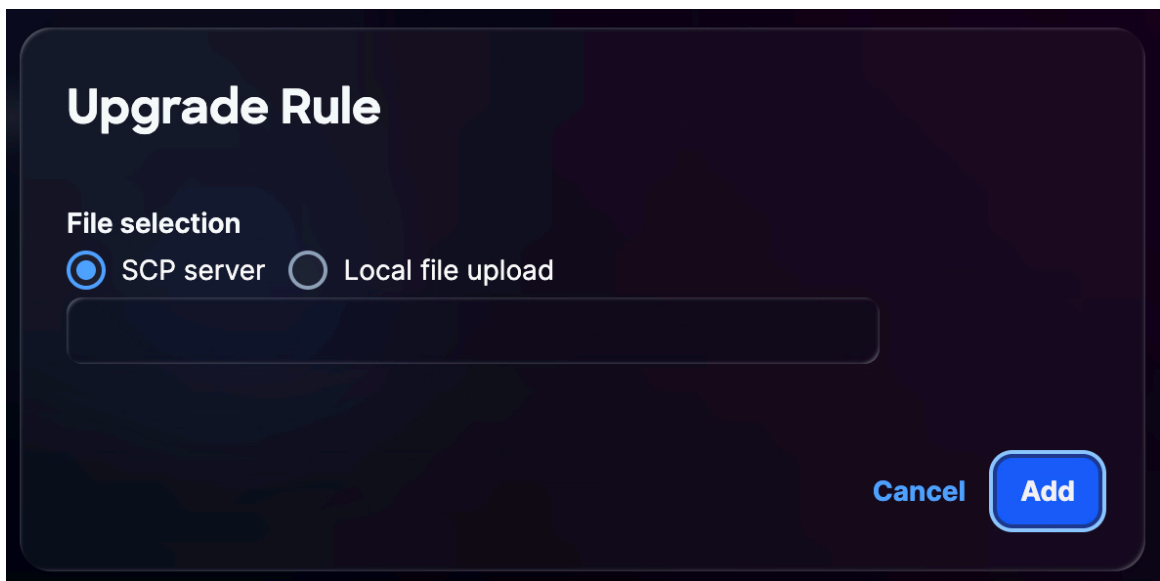
To upgrade rules:

1. Navigate to System Settings > Package Management in VA.



Upgrade

2. From the desired rule, click **Upgrade**. The **Upgrade Rule** window opens.



Upgrade Rule

3. Choose your preferred **File selection** option:
 - **Secure Copy Protocol (SCP) server:** Enter the exact file name of the installation package. This method is recommended for large files.
 - **Local file upload:** Drag-and-drop the downloaded installation file.
4. Click **Add**.

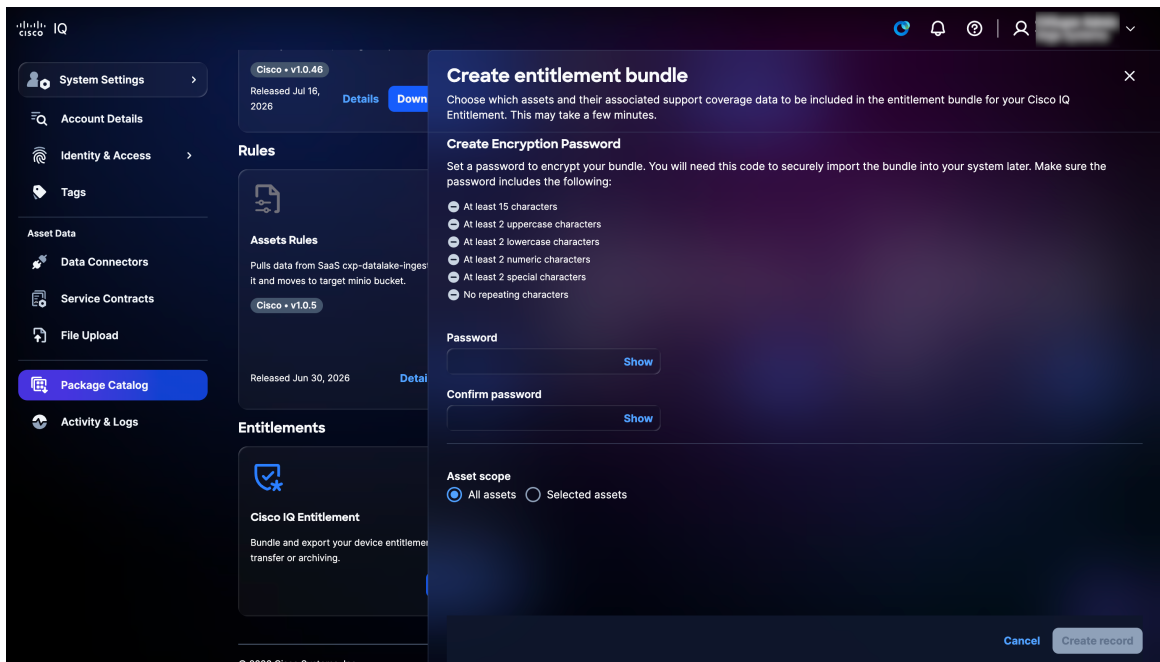
 **Note:** These rules are applied at the recurring scheduled device telemetry collection. For immediate application, you can manually initiate device telemetry collection.

Installing Entitlements

An **Entitlement** provides validation of your organization's right to use specific software features, modules, or services. To install an entitlement:

1. Log in to [Cisco IQ](#).

2. Navigate to **System Settings > Package Catalog**.
3. From the entitlement card, click **Create record**. The **Create entitlement bundle** window opens.



Create Entitlement Bundle

4. Enter a **Password**. Refer to the password creation rules that display on-screen.
5. Enter the same password again in **Confirm Password**.
6. Choose the preferred **Asset scope** radio button.
 - **All assets**: Includes all assets linked to you
 - **Selected assets**: Allows you to pick specific devices aligned with your environment; if this option is selected, check the checkboxes of all applicable assets
7. Click **Create record** to save the file locally.

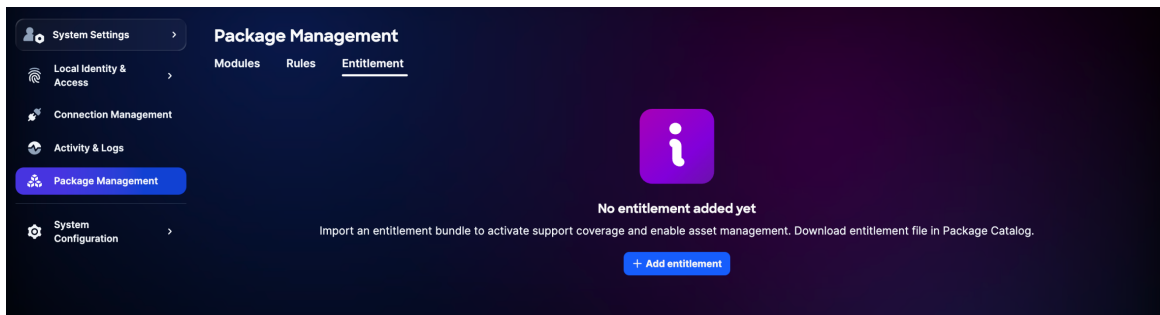
 **Note:** After creating the entitlement bundle, do not navigate away from the current screen. If you navigate to another page, the bundle is invalidated and you must regenerate it to enable the download option.

 **Note:** Installation files are large (10-25 GB); ensure you have sufficient disk space before downloading.

8. Log in to VA.
9. Navigate to **Home > System Settings > Package Management**. The **Package Management** page contains the following tabs:
 - Modules

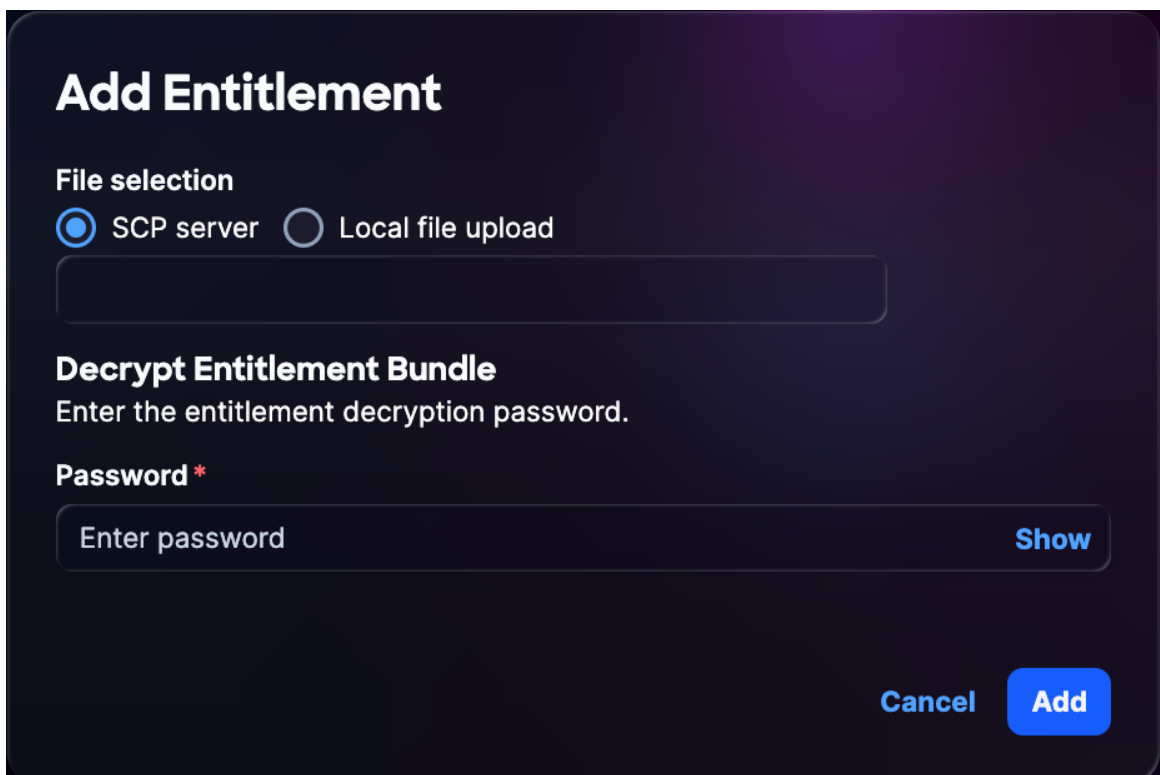
- Rules
- Entitlements

10. Click **Entitlements** tab.



Entitlement Tab

11. Click **Add Entitlement**.



Add Entitlement

12. Choose your preferred **File selection** option.

- **Secure Copy Protocol (SCP) server:** Enter the exact file name of the installation package; this method is recommended for large files
- **Local file upload:** Drag-and-drop the downloaded installation file

13. Enter a **Password**.

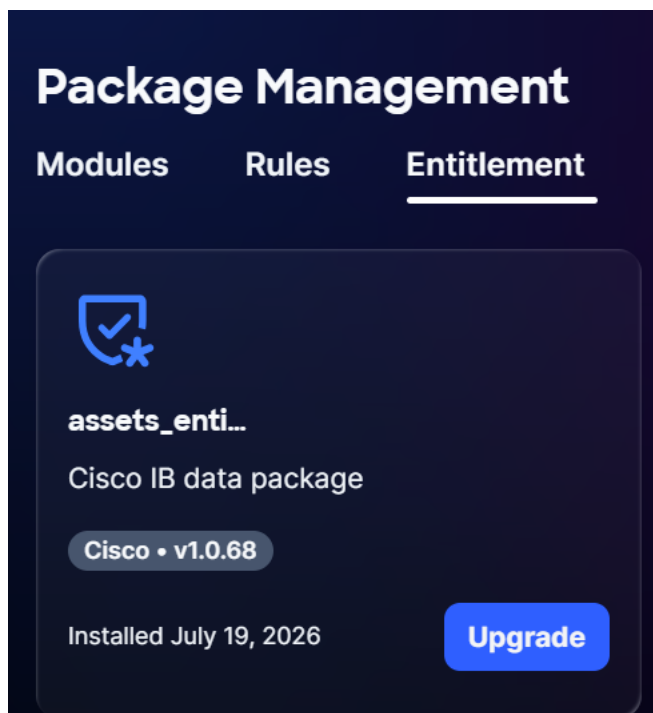
14. Click **Add**. The newly installed entitlement displays on the **Entitlement** tab in **Package Management**.

15. To enable entitlements, wait 5 to 10 minutes after adding them, then initiate the device telemetry collection.

 **Note:** Adding a service contract in the entitlement process adds all devices linked to that contract to the on-premises device asset inventory. You have options to filter devices by serial number, use multiple account IDs, or select specific devices to manage entitlements.

Upgrading Entitlements

To upgrade an entitlement:



Entitlement Upgrade

1. From the desired Entitlement, click **Upgrade**.

Upgrade Entitlement

File selection

☒ SCP server ☐ Local file upload

Decrypt Entitlement Bundle

Enter the entitlement decryption password.

Password *

Enter password Show

Cancel Add

Upgrade Entitlement

2. Choose your preferred **File selection** option:
 - **Secure Copy Protocol (SCP) server:** Enter the exact file name of the installation package; this method is recommended for large files
 - **Local file upload:** Drag-and-drop the downloaded installation file
3. Enter a **Password**.
4. Click **Add**.

AI-Powered Features

The On-Prem AI Inference Infrastructure module enables on-premises AI-powered capabilities in VA. It runs a Small Language Model (SLM) locally, allowing the system to respond to AI-powered prompts. Once installed, you can interact with it directly within the VA interface.

The following query types are supported:

- **Assets:** Identify assets at risk due to end-of-life status, software currency or non-conformance, security vulnerabilities, and contract coverage gaps
- **Inventory:** Request AI-driven analysis about assets in your inventory

The On-Prem AI Inference Infrastructure installation package is available from the Cisco IQ Package Catalog and is distributed in the same way as other modules, such as Assets.

 **Note:** Only one (1) On-Prem AI Inference Infrastructure can run per GPU at a time. The installation takes approximately 40–45 minutes to complete. The installation files are large (approximately 30 GB); ensure you have sufficient disk space before downloading.

Prerequisites for On-Prem AI Inference Infrastructure

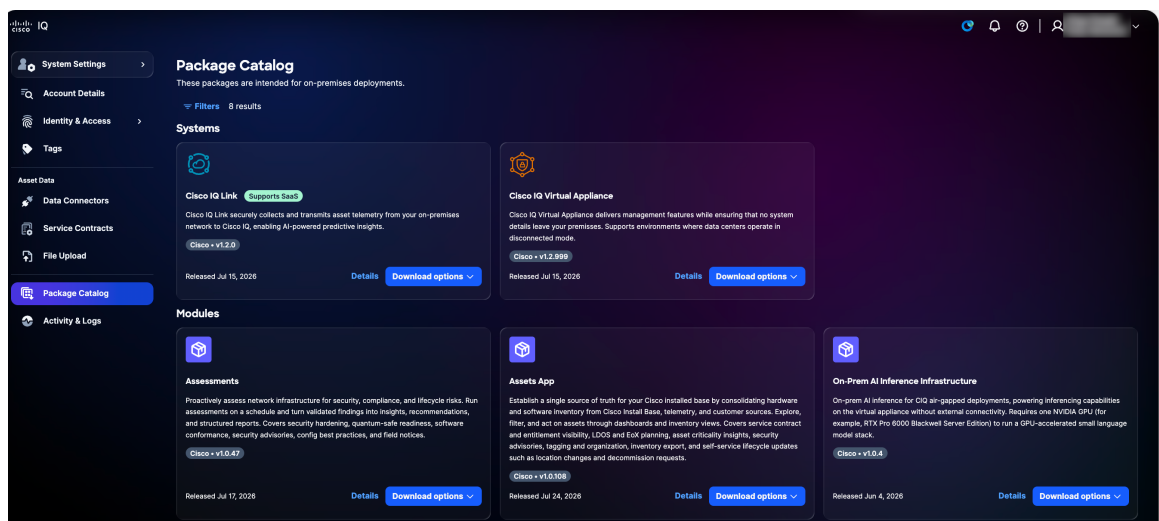
Before installing the On-Prem AI Inference Infrastructure, the following conditions must be met:

- The VA must include a VM with GPU access; the SLM requires a GPU and cannot run without one
- The GPU VM must have 80GB or more of GPU VRAM available

Installing On-Prem AI Inference Infrastructure

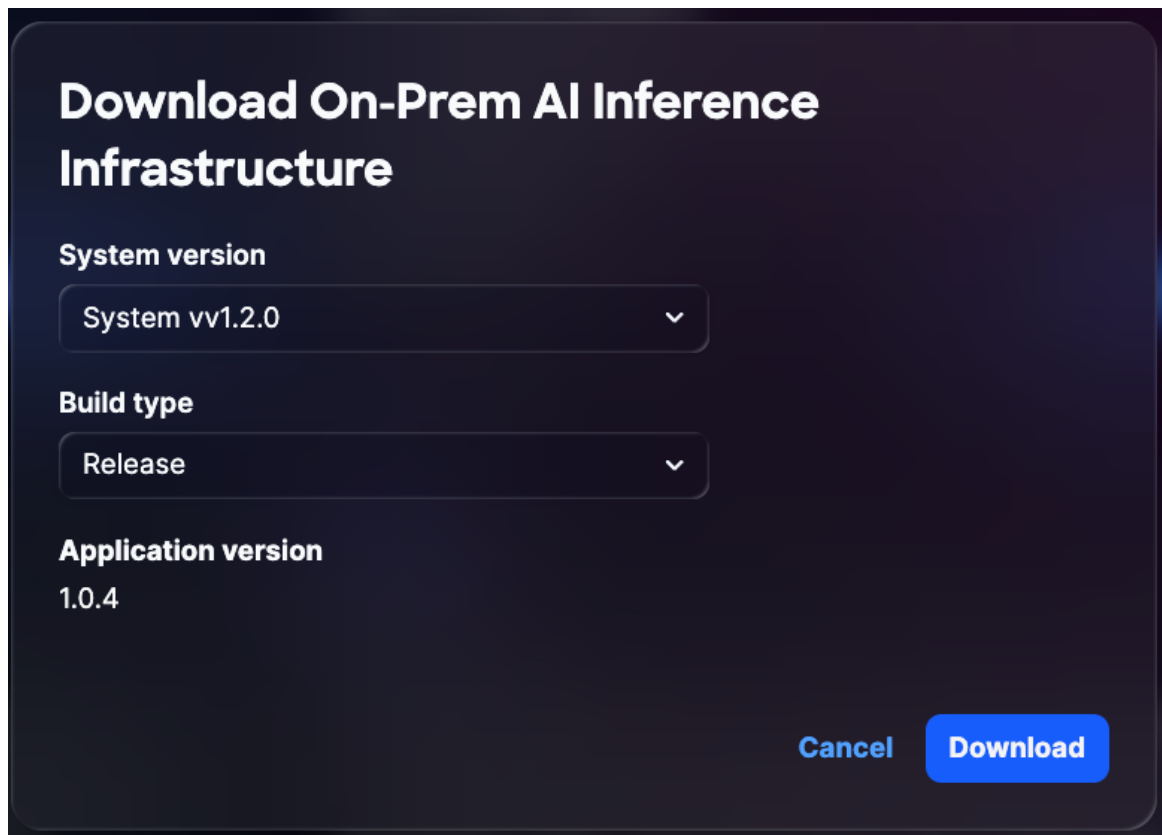
To install the On-Prem AI Inference Infrastructure on the VA, download the On-Prem AI Inference Infrastructure module from Cisco IQ SaaS:

1. Log in to [Cisco IQ](#).
2. Navigate to **System Settings > Package Catalog**.



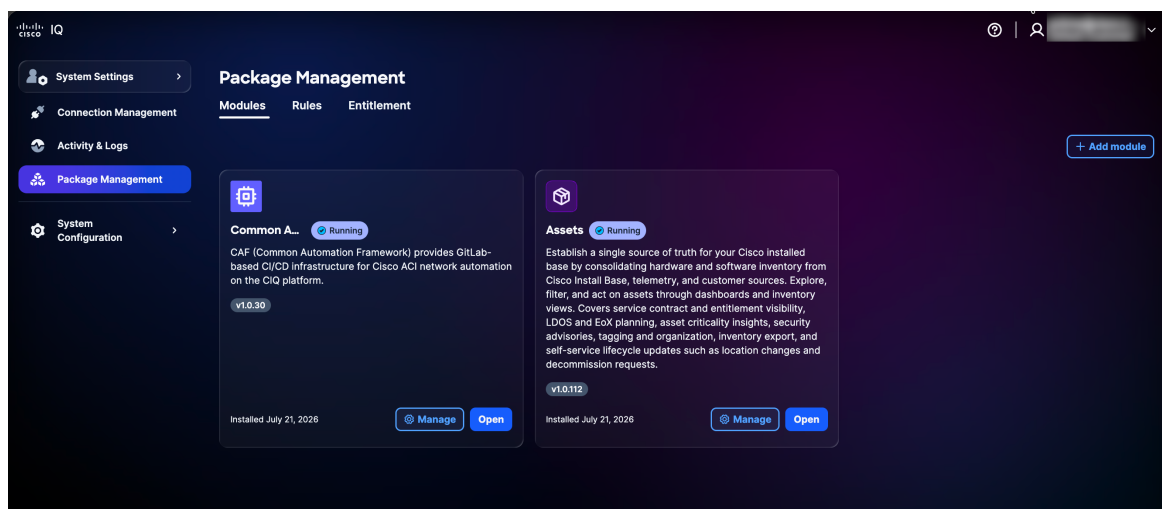
Install Package

3. From the **On-Prem AI Inference Infrastructure** card, click **Download options > Installation packages**. The **Download Application** window opens.



Download AI Inference Infrastructure

4. Choose a **System version** from the drop-down list.
5. Choose a **Build type** from the drop-down list.
6. Click **Download**.
7. Navigate to VA.

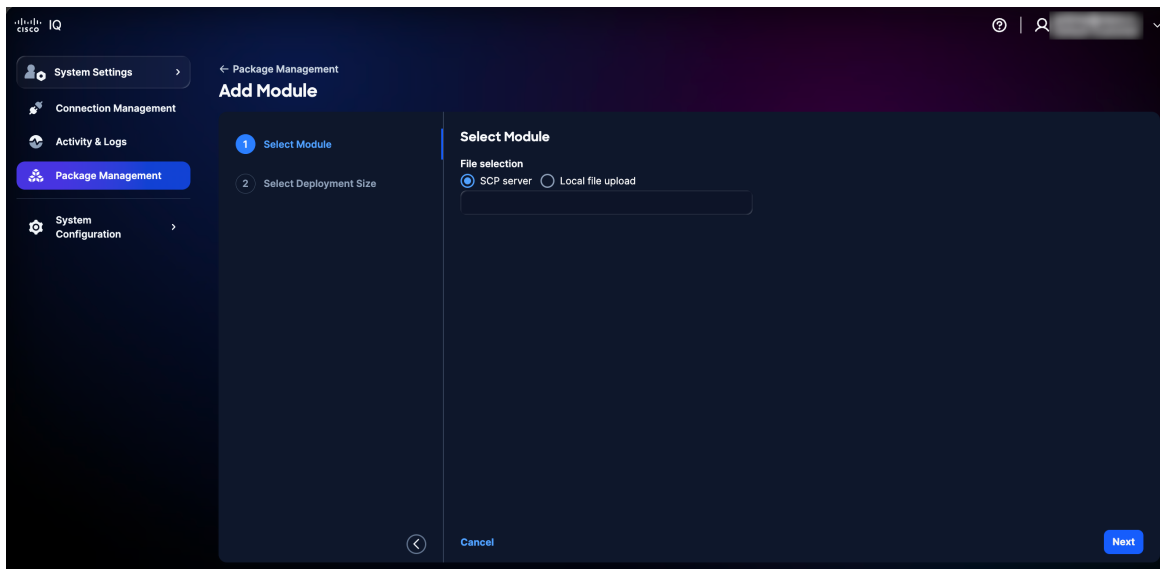


Package Management

8. Navigate to **Home > System Settings > Package Management**. The **Package Management** page displays with the following tabs:
 - Modules

- Rules
- Entitlements

9. From the **Modules** tab, click **Add modules**.



Select Module

10. Choose your preferred **File selection** option:

- **SCP server:** Enter the exact file name of the installation package (recommended for large files).
- **Local file upload:** Drag-and-drop the downloaded installation file (not recommended for files 30 GB or larger due to upload time). **Note:** *The local file upload method has a 20-minute threshold. If the upload process exceeds this duration, the installation fails. Using an SCP server is the preferred method to ensure a successful and stable installation.*

11. Click **Next**. The system begins uploading the file.

12. Choose a **Deployment Size** (for example, Small, Medium, or Large).

13. Click **Add Module**. The installation begins and takes approximately 40–45 minutes to complete.

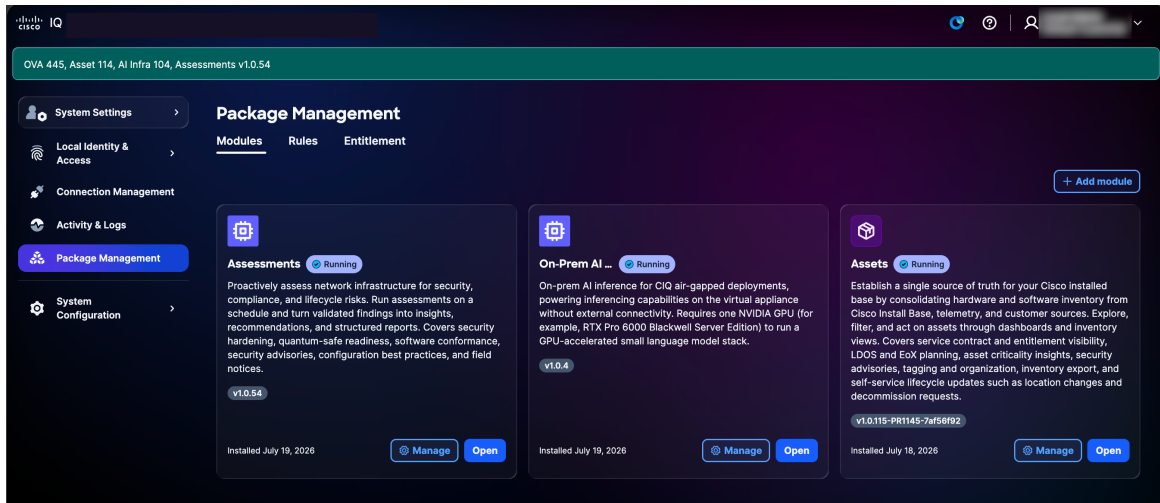
Once the installation is complete, On-Prem AI Inference Infrastructure displays on the **Module** tab in **Package Management**.



Note: Only one On-Prem AI Inference Infrastructure module can run per GPU. The module uses approximately 90% of GPU VRAM. Attempting to install an additional instance on the same GPU is not supported.

Managing the On-Prem AI Inference Infrastructure Module

Once installed, the On-Prem AI Inference Infrastructure module can be managed from the **Applications** tab in **Package Management**.



Editing AI Inference Infrastructure

To manage the module, click **Manage** next to the On-Prem AI Inference Infrastructure module. See [Managing Modules](#) for more details.

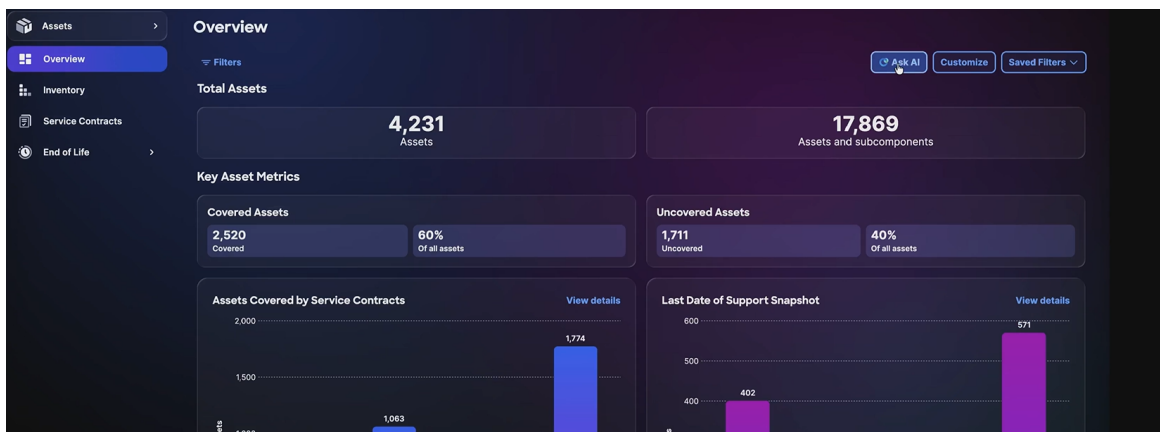
Using AI-Powered Features

After the On-Prem AI Inference Infrastructure module is successfully installed, the **Ask AI** button becomes available in the VA interface.

Ask AI in Assets

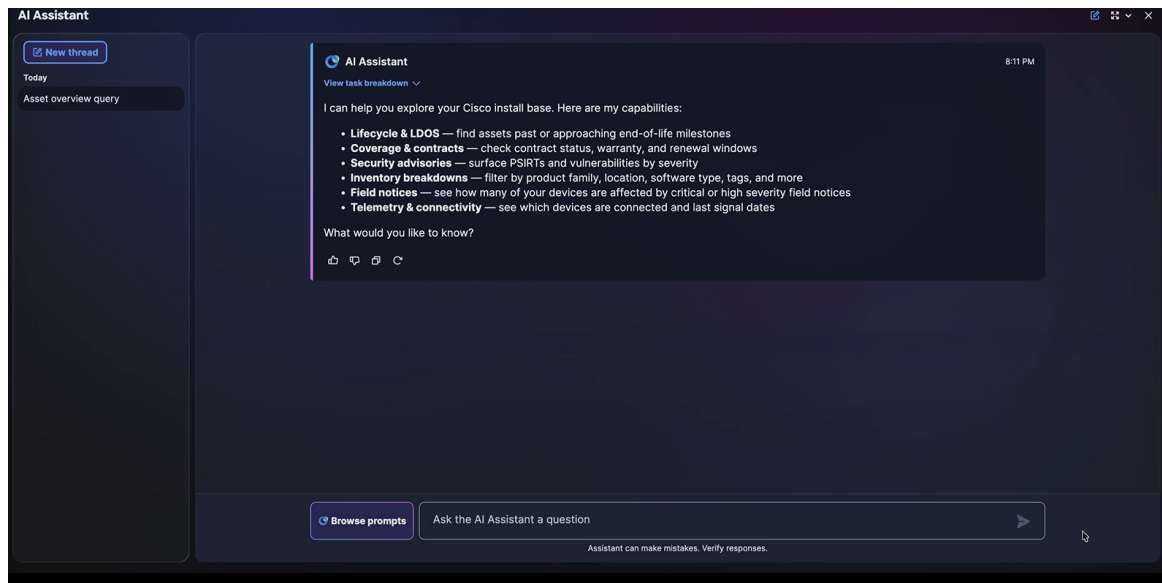
To use Ask AI in Assets:

1. Choose the **Home** menu > **Assets**. The **Assets** page displays.



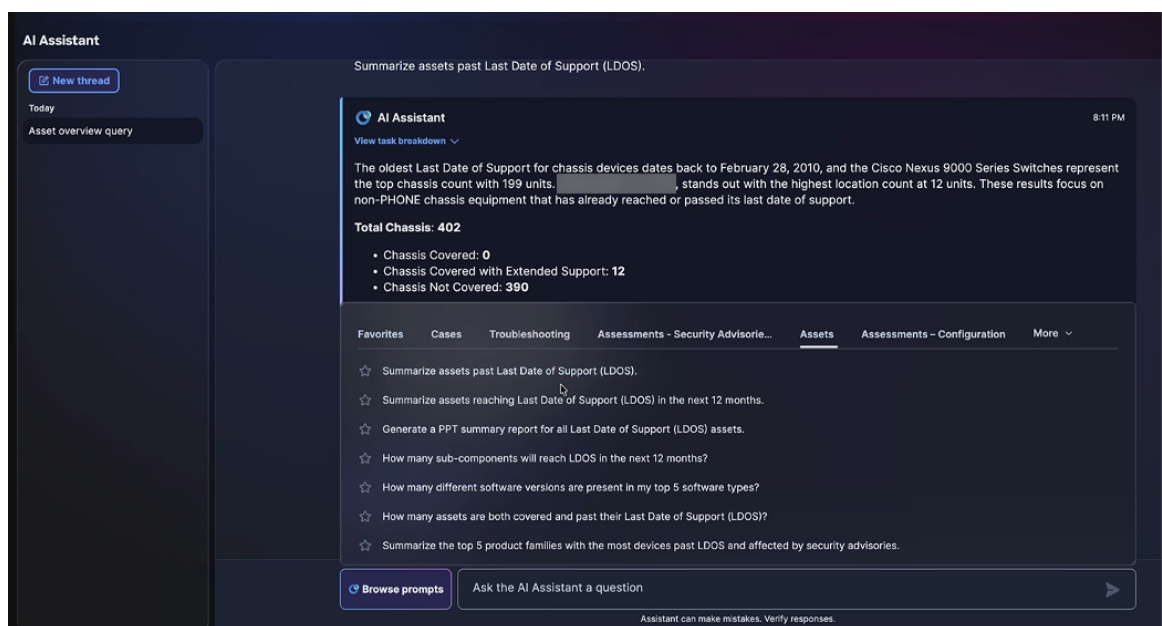
Assets Page

2. Click **Ask AI**. The On-Prem AI Inference Infrastructure launches.



Browse Prompts

3. Either click **Browse prompts** to view available prompts or enter a custom question in the **Ask the AI Assistant a question** field.



Set of Prompts

4. Click the desired prompt or press **Enter**. The on-premises SLM generates a response.

AI Analysis in Inventory

The On-Prem AI Inference Infrastructure module provides automated AI-driven analysis in the **Inventory** section. Analysis results display automatically once inventory data is populated.

To view AI analysis in Inventory:

1. Select the **Home** menu > **Inventory**. The **Inventory** page displays.

Name	Product ID	Product Type	Equipment Type	Serial Number	Next Milestone	Next Milestone...	Contract Number	Coverage Status	Telemetry Status	Security Advisories	
			Chassis			Jun 25, 2028	—	🔴	🟢	0	
			Chassis			—	204599980	🟢	🟢	35	
			Chassis			—	204599980	🟢	🟢	35	
			Chassis			Oct 29, 2028	—	🔴	🟢	3	
			Chassis			Apr 28, 2028	—	🔴	🟢	7	
			Chassis			Jul 31, 2027	—	🔴	🟢	7	
			Chassis			—	—	🔴	🟢	2	

Inventory

2. View the AI-generated analysis. Results display in the inventory view once data is available.



Note: Click **Full Analysis** for visualizations like graphs, dashboards, and charts which provide additional insights.

Common Features for Modules

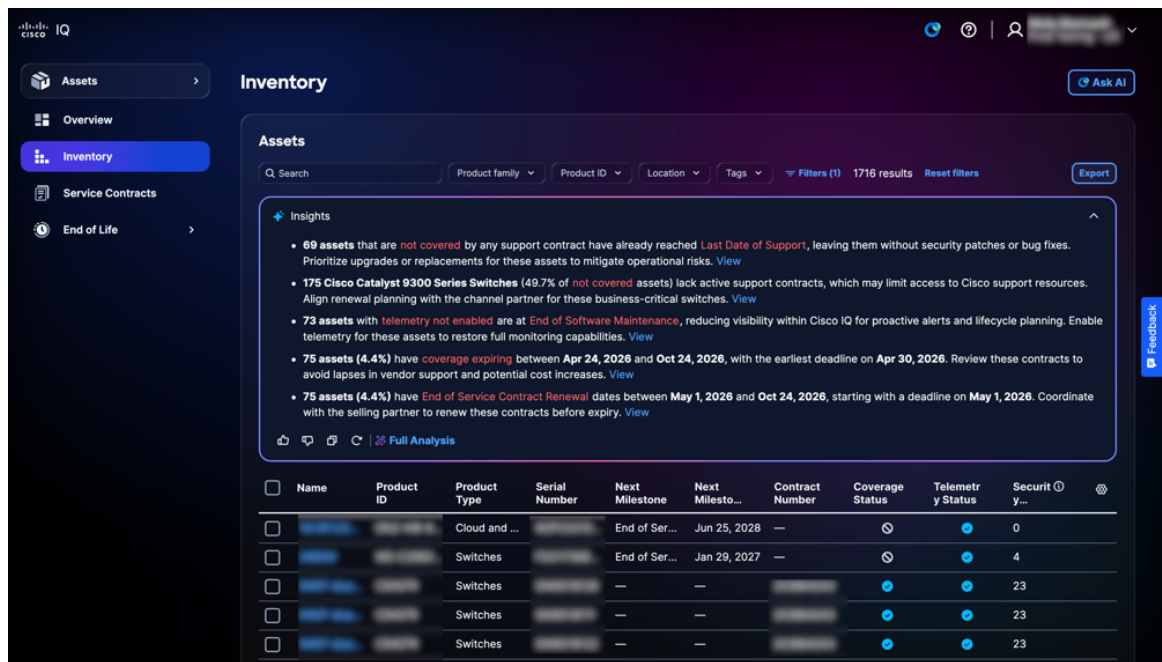
This section details the core functionalities shared across all modules. These features offer a consistent user experience, optimize system performance, and streamline administrative workflows

Analyzing Data

The **Insights** panel delivers AI-driven analysis of the data on that page, providing actionable insights to improve the security and health of your network environment.



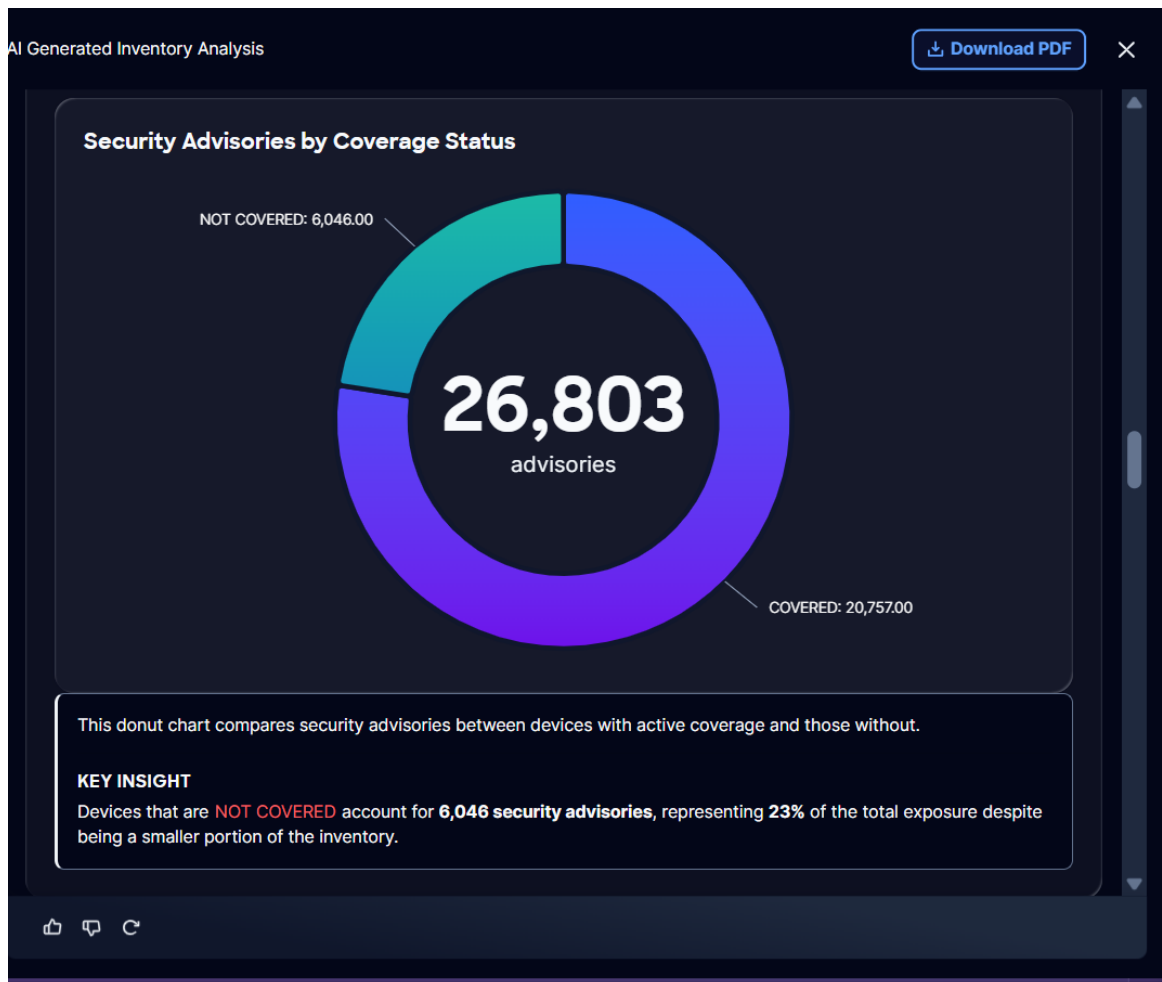
Note: The Analysis feature is only available on select pages.



Insights Panel

The following options are available inside the Insights panel:

- Click the **Expand** icon to expand the panel and display additional insights
- Click the **Thumbs Up** or **Thumbs Down** icon to provide feedback on the AI-generated information
- Click **Full Analysis** to display additional information, deeper analysis, and visualizations like graphs, dashboards, and charts



Full Analysis

The following options are available within a full analysis:

- Click **Download PDF** to save an offline copy of the analysis for your records or for collaboration

Exporting Information

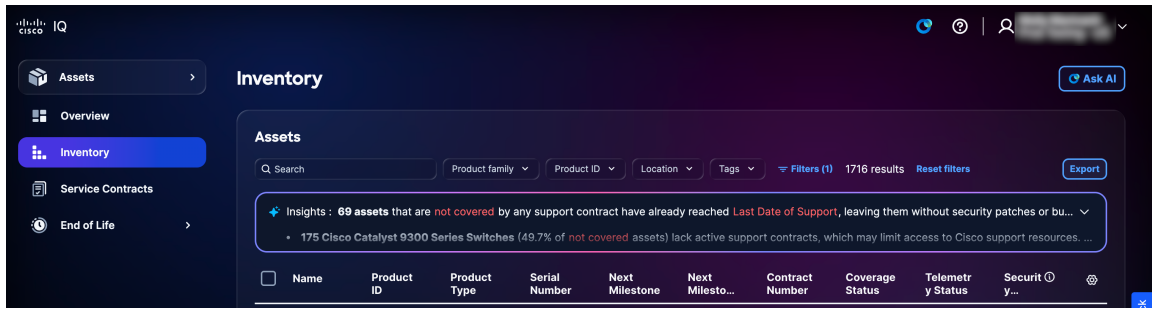
The export feature allows you to export custom views for Assets and Security information in .xls or .csv format.



Note: The export feature is only available for select pages.

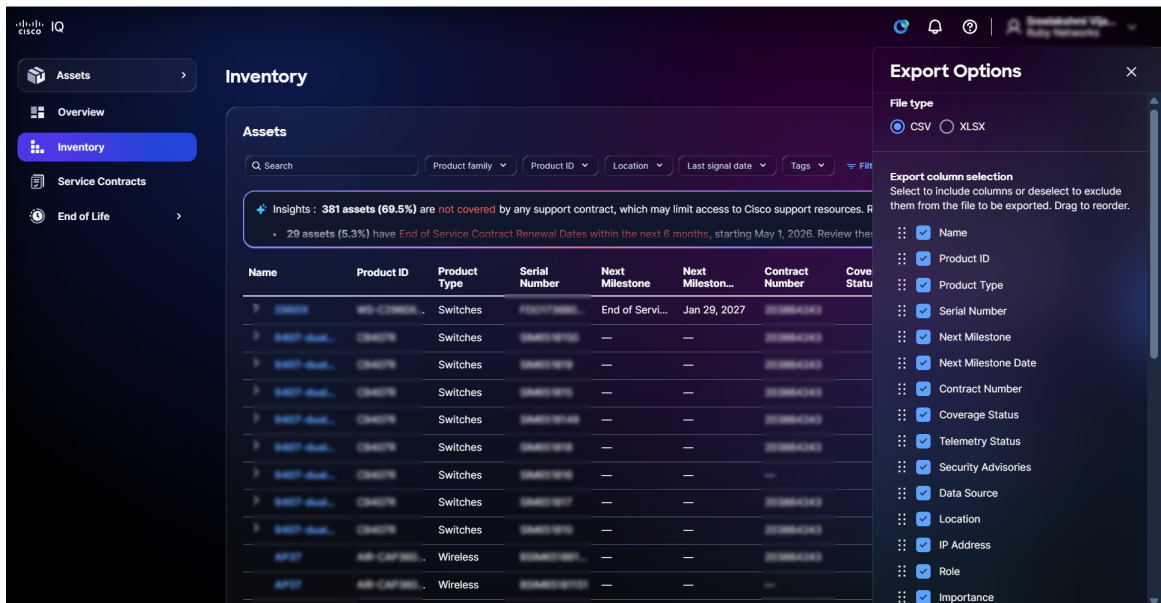
To export information from a page:

1. Navigate to the page.



Exporting Inventory in the Assets Module

2. Click **Export**. The **Export Options** display.



Export Options

3. Select a **File type**.

4. Check the check box(es) in the desired column(s).

5. Click **Export**. The file downloads to the browser's local download folder.

Table Settings

You can configure table settings to create custom and refined views for different module features.

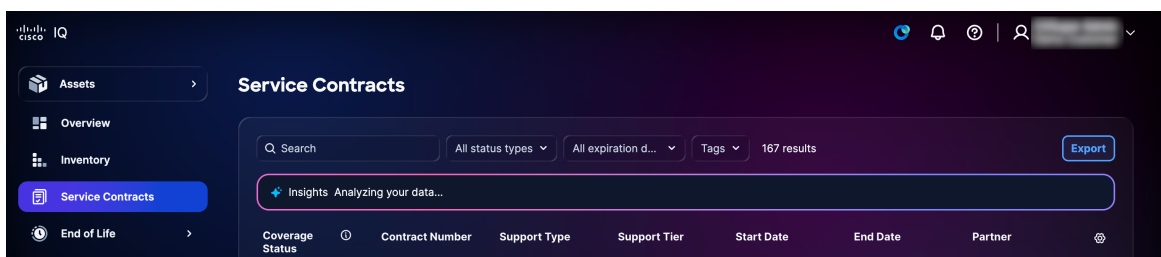


Table Settings

To change the columns that display on selected pages, click the **Table Settings** icon. The

Table settings display.

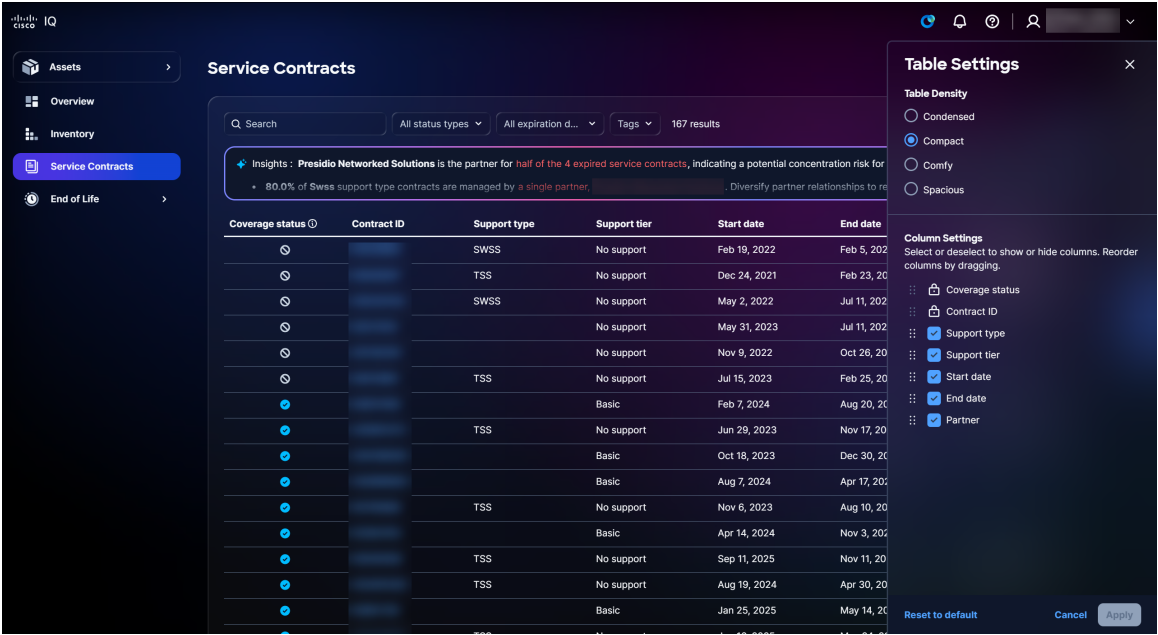


Table Setting Options

Changing Table View

To change the table view:

1. Select one of the following **Table Density** options:
 - **Condensed:** Minimizes visual elements and spacing to display more information
 - **Compact:** Reduces whitespace and tightens spacing between UI elements
 - **Comfy:** Utilizes more whitespace and larger spacing between elements
 - **Spacious:** Emphasizes abundant whitespace and larger UI elements
2. Click **Apply**.

Adding and Removing Columns

To add or remove columns:

1. Select or clear the **Column Settings** check box(es).
2. Click **Apply**.

 **Note:** The **Name** column cannot be removed from the table view.

Changing Column Order

To change the column order:

1. Drag-and-drop the column name to arrange the items in the desired order.

2. Click **Apply**.

Customizing Dashboards

The Custom Dashboard feature enables you to personalize standard dashboards through a range of intuitive customization options:

- Rearrange dashboard widgets or panels using the drag-and-drop functionality
- Remove any components that are not relevant to your workflow
- Your personalized dashboard layout is securely stored to your user profile and automatically applied across all sessions and devices
- Restore the original dashboard layout with a simple reset option

To customize a dashboard:

1. Navigate to the dashboard.



Customize

2. Click **Customize**.



Edit Dashboard

3. Change the dashboard as desired:

- **Rearrange:** Drag-and-drop the widgets into the desired layout
- **Remove:** Click the **Delete** icon to remove a widget
- **Reset:** Click **Reset to default** to reset the dashboard to its original layout

4. Click **Save**. A **Dashboard Saved** message displays.

Your dashboard layout is automatically applied across all sessions and devices.

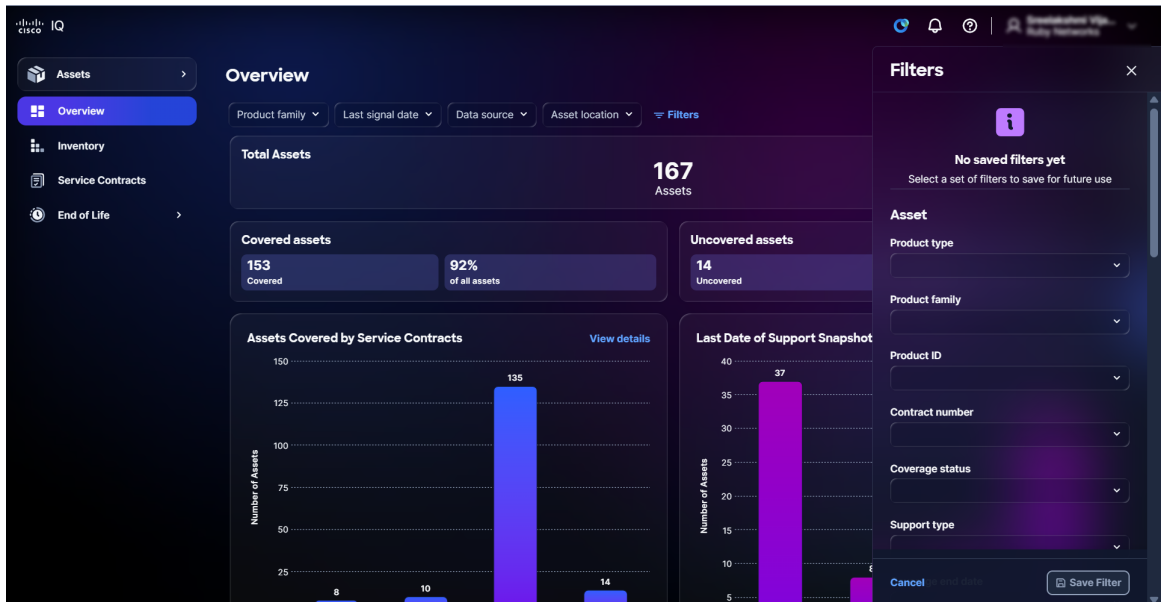
Customizing Filters

You can save custom filter configurations for any dashboard view, enabling you to easily return to your preferred settings as needed. All filter preferences are securely stored on a per-user, per-account basis, ensuring a personalized and consistent experience each time you access Cisco IQ.

Creating a Filter

To create a custom filter:

1. Navigate to the dashboard.
2. Click **Filters**.



Filters

3. Choose the desired filters from the drop-down lists.
4. Click **Save Filter**. The Name Saved Filter window opens.

The screenshot shows a dialog box titled 'Name saved Filter'. It contains a label 'Filter name *' followed by a text input field with the placeholder text 'Custom Filter |'. At the bottom left is a 'Cancel' button, and at the bottom right is a 'Save Filter' button.

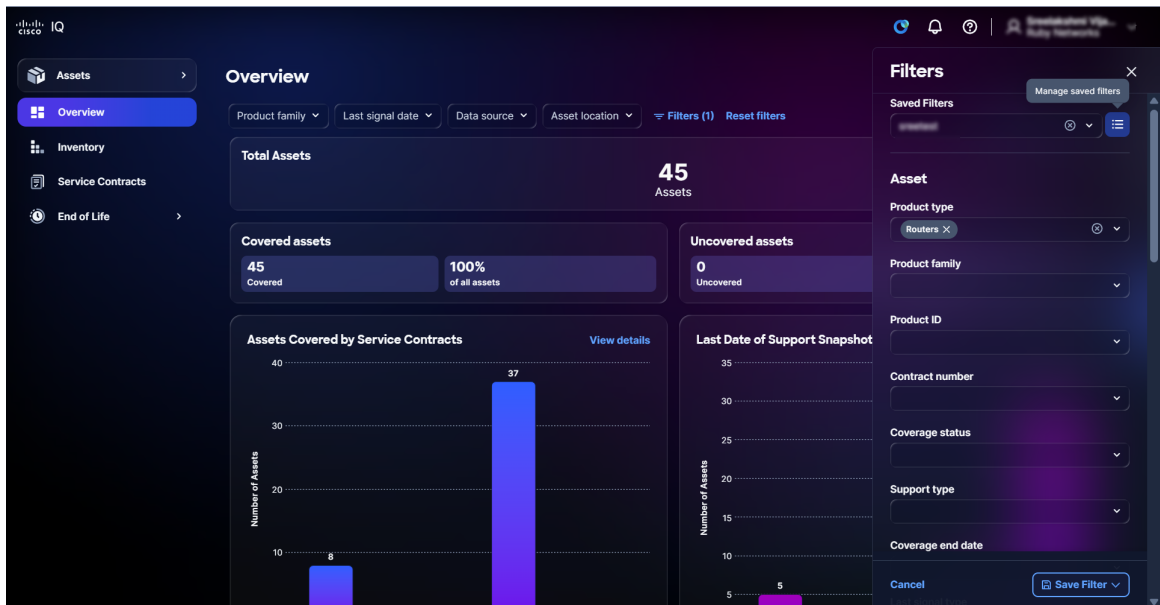
Filter Name

5. Enter a Filter name.
6. Click **Save Filter** to confirm.

Editing a Filter Name

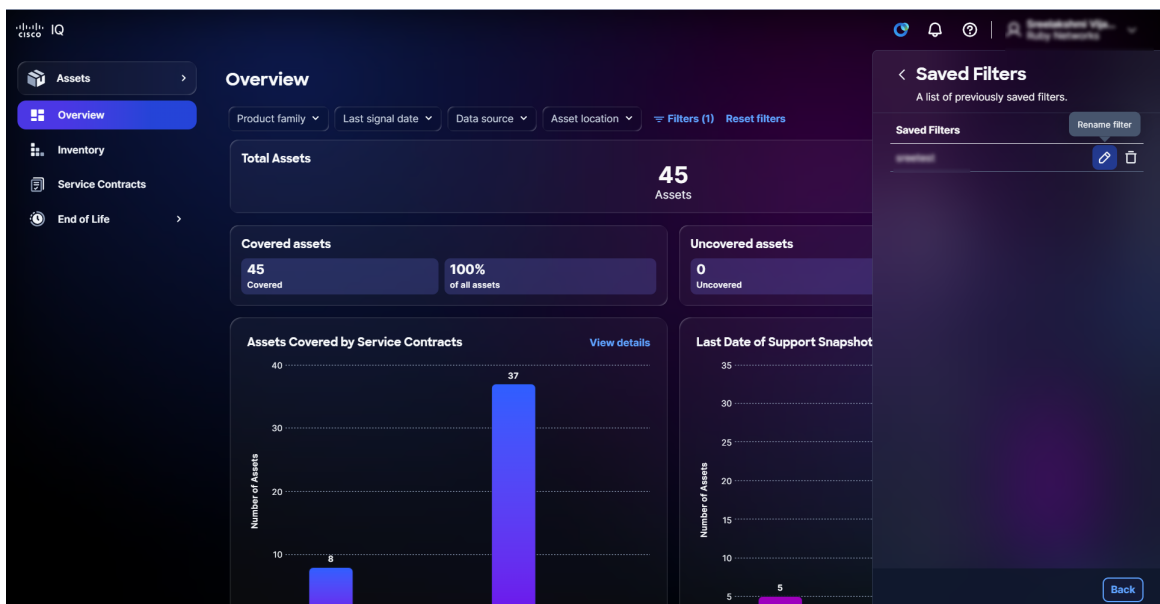
To edit a custom filter:

1. Click **Filters**.



Manage Saved Filters

2. Click the Manage saved filters icon.
3. Navigate to the filter.



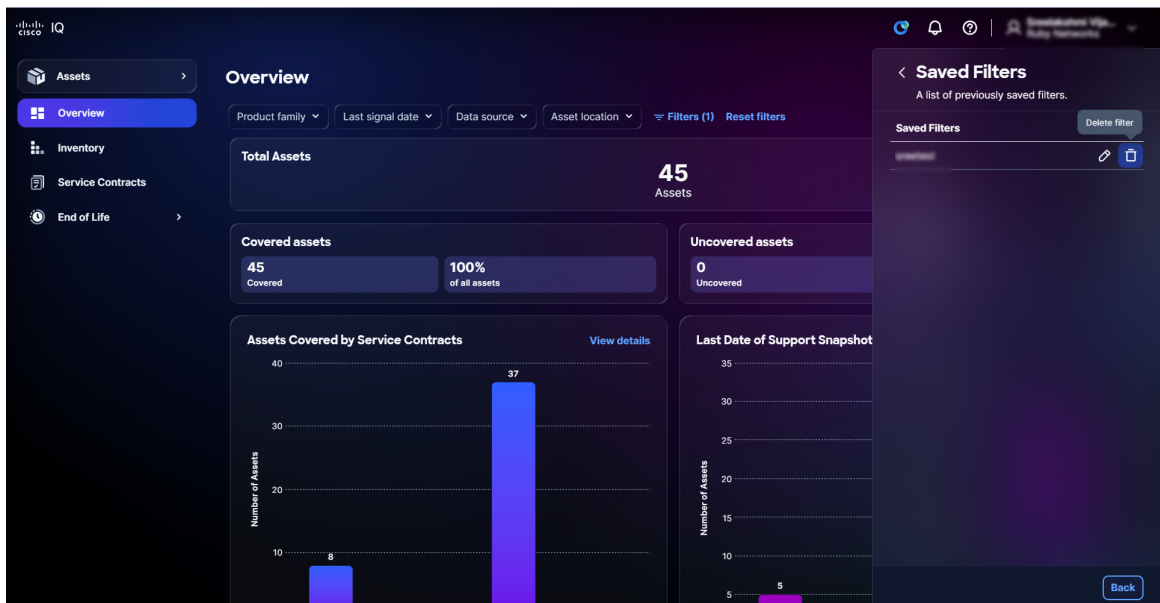
Edit Filter

4. Click the **Edit** icon. The **Name saved Filter** window opens.
5. Edit the filter name.
6. Click **Save Filter** to confirm.

Deleting a Filter

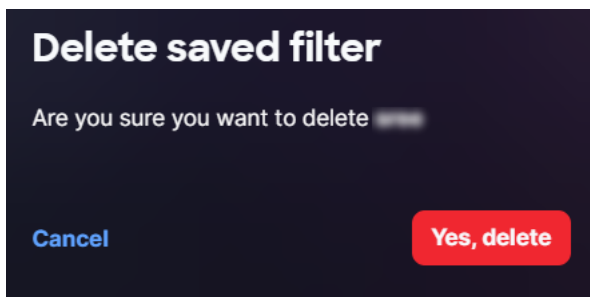
To delete a custom filter:

1. Click **Filters**.
2. Click the Managed Saved Filters icon
3. Navigate to the filter.



Delete Saved Filter

4. Click the **Delete** icon. The **Delete saved filter** window opens.



Delete Saved Filter Confirmation

5. Click **Yes, delete** to confirm.

Assets Module

The Assets module delivers comprehensive visibility and management capabilities for Cisco assets and serves as the foundation of Cisco IQ, providing a centralized listing of all devices within an organization. By collecting information from multiple sources, it acts as a single source of truth for device inventory. Maintaining a complete and accurate asset list is essential, as other modules within Cisco IQ—such as the Assessments module—rely on this data to assess the health and security of your devices.

Core Concepts

The Assets module is built on the following core concepts:

- **Asset:** Any physical device, hardware, or software that is inventoried and managed as part of Cisco's service delivery with detailed tracking of its identity, function, service coverage, and lifecycle
- **Contract-Sourced Assets:** Assets ingested into inventory directly from linked Service Contract data, rather than through telemetry. Cisco IQ ingests the following equipment types from contract data: Chassis, Modules, Power Supplies, and Fans. These assets are visible in the Inventory even if no telemetry connection is present
- **Last Date of Support (LDOS):** End-of-life and end-of-support milestone tracking for Cisco products
- **Service Coverage:** Active support contracts, warranties, and entitlement levels associated with a specific piece of hardware or software
- **Asset Tag:** A user-defined label assigned to an asset for organization, filtering, and operational workflows
- **Device Signal:** Refers to when Cisco last observed a device (by its serial number) based on device telemetry, support cases, and contract renewals; Asset telemetry data is ingested and enriched through a multi-layer data pipeline

Accessing Assets Module

To access asset management features in Cisco IQ, choose the **Home** menu > **Assets** or click **Assets** from the **Application** section of the **Home** page > **Launchpad** tab. The **Overview** page displays.

Assets Overview

The **Overview** page displays a dashboard that enables you to quickly evaluate the health and status of devices.

≡ Filters

Total Assets

Assets

Assets and subcomponents

Key Asset Metrics

Covered Assets

186

Covered

93%

Of all assets

Uncovered Assets

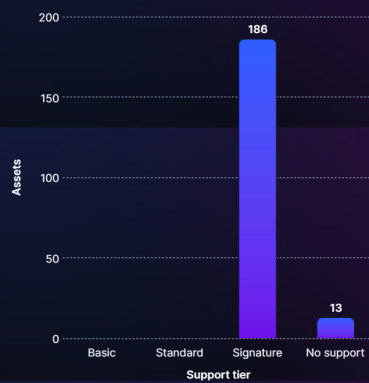
13

Uncovered

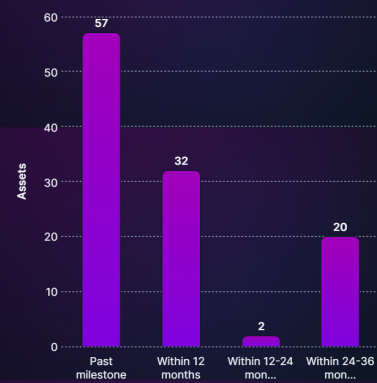
7%

Of all assets

Assets Covered by Service Contracts [View details](#)



Last Date of Support Snapshot [View details](#)



Assets With Telemetry Enabled

186

With telemetry

93

Of all assets

Assets Without Telemetry Enabled

13

Without telemetry

7%

Of all assets

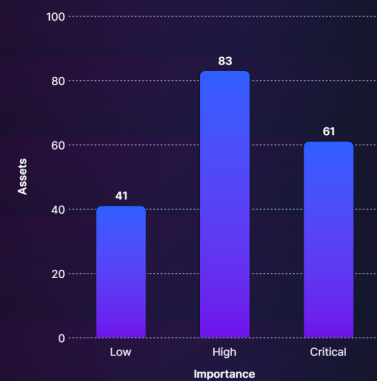
Assets With Critical or High Security Advisories



Of the 186 assets with telemetry enabled, **170** have critical or high Security Advisories

[Assets by Importance](#) [View details](#)

Importance can be evaluated for 185 assets.

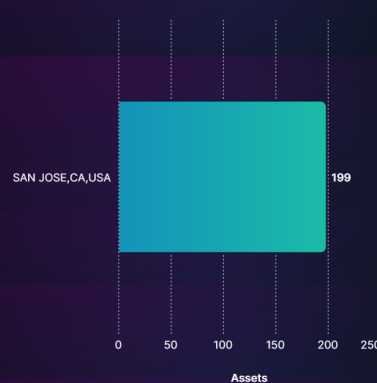


Asset Breakdown

Top 5 Product Families [View details](#)



Top 5 Install-At Locations [View details](#)



: Additional key metrics such as telemetry status, critical security advisories, and LDOS information

- **Covered Assets:** The total number and percentage of assets covered by service contracts
- **Uncovered Assets:** The total number and percentage of assets not covered by service contracts
- **Assets Covered by Service Contracts:** A breakdown of the number of assets—hardware or software—that service contracts cover, categorized by entitlement level
- **Last Date of Support Snapshot:** A breakdown of the number of assets past LDOS or reaching LDOS
- **Assets with Telemetry Enabled:** Total number and percentage of assets with telemetry enabled
- **Assets without Telemetry Enabled:** Total number and percentage of assets without telemetry enabled
- **Assets with Critical or High Security Advisories:** The percentage of total assets with telemetry enabled and that have critical or high security advisories
- **Assets by Importance:** A breakdown of the priority assigned to a device relative to other devices in the network.
- **Asset Breakdown:** A detailed display of asset information, such as product families, install-at locations, software versions, and asset roles

Filtering Views for Assets

You can filter the dashboard view by choosing a filter from the drop-down lists or clicking **Filters** and choosing an option from the list of available filters.



Note: Some filters may be hidden depending on screen zoom settings. Different filters are available depending on your roles and permissions.

Viewing Details for Assets

When clicking **View Details**, the page redirects to the **Inventory** page. See [Inventory](#) for more information.

Asset Criticality Insights

Cisco IQ includes Asset Criticality Insights, a new capability in the Assets module that predicts the functional role and business importance of network devices. By analyzing device configurations and enabled features, Asset Criticality Insights helps you identify which assets have the greatest impact on your network — so you can prioritize them for security remediation, software upgrades, End-of-Life (EOL) planning, and coverage decisions.

 **Note:** Asset Criticality Insights are available exclusively for assets with **Standard** or **Signature** levels that have active telemetry connections. Please ensure your assets meet the configuration requirements to populate these insights within the dashboard.

Asset Criticality Insights are available in the Assets app in the following areas:

- **Assets Overview:** Filter and view summary breakdowns by Asset Criticality Insights attributes
- **Assets Inventory:** Display, search, filter, and sort devices by Role and Importance
- **Asset Details:** View Role and Importance for individual devices, with informational tooltips explaining each value

Overriding Role and Importance Classifications

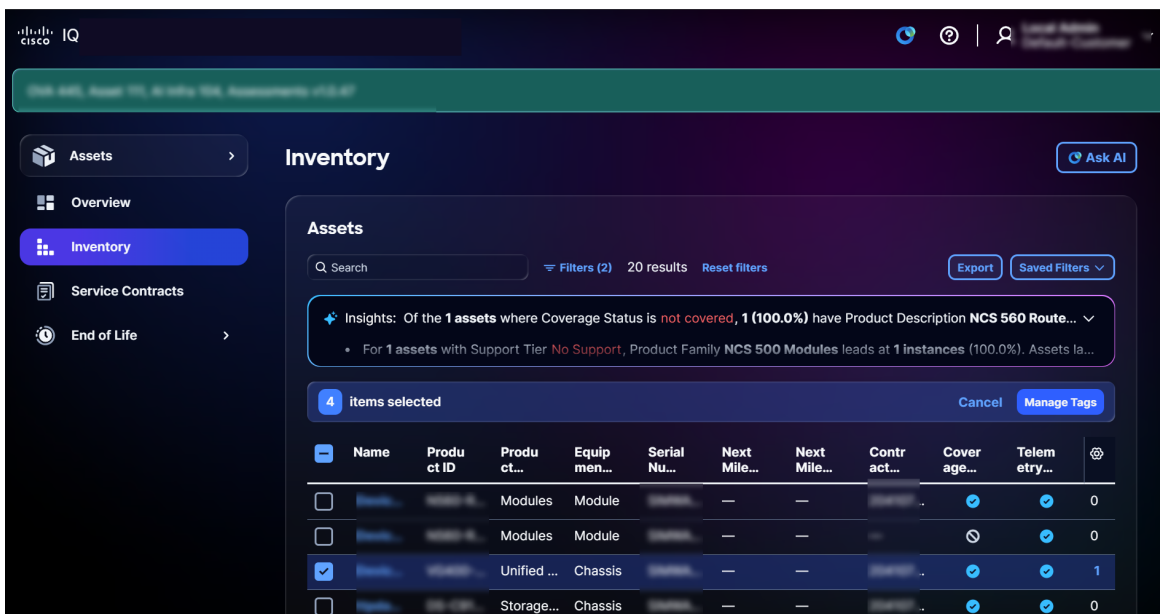
Cisco IQ automatically predicts the Role and Importance of each asset based on telemetry data. Account Administrators can manually correct these classifications when the automated prediction does not accurately reflect the asset's function or criticality in the network.

 **Note:** Override controls are available to Account Administrators only. Role and Importance values are read-only for all other user roles.

Overriding Classifications from the Inventory Table

To override Role or Importance for one or more assets:

1. Navigate to **Assets > Inventory**.
2. Click the check box of the desired asset row. To update multiple assets simultaneously, select multiple check boxes.



The screenshot shows the Cisco IQ Assets Inventory page. The left sidebar contains navigation links: Assets, Overview, Inventory (selected), Service Contracts, and End of Life. The main content area is titled 'Inventory' and shows a table of assets. The table has columns: Name, Product ID, Product Name, Equipment Name, Serial Number, Next Mile, Next Mile, Contract, Coverage, Telemetry, and a final column with a gear icon. The table displays 20 results, with 4 items selected. The selected items are highlighted in blue. The table also includes a search bar, filters (2), and buttons for Export and Saved Filters. An insight banner at the top of the table states: 'Insights: Of the 1 assets where Coverage Status is not covered, 1 (100.0%) have Product Description NCS 560 Route...'. Below the insight, a note mentions: 'For 1 assets with Support Tier No Support, Product Family NCS 500 Modules leads at 1 instances (100.0%). Assets la...'. The table rows show various assets, including 'Modules', 'Unified ...', and 'Storage...'. The 'Unified ...' row is selected, showing a '1' in the final column.

	Name	Product ID	Product Name	Equipment Name	Serial Number	Next Mile	Next Mile	Contract	Coverage	Telemetry	
☐	...	...	Modules	Module	...	—	—	...	✓	✓	0
☐	...	...	Modules	Module	...	—	—	...	✗	✓	0
☒	...	...	Unified ...	Chassis	...	—	—	...	✓	✓	1
☐	...	...	Storage...	Chassis	...	—	—	...	✓	✓	0

Role and Importance

3. In the **Role** or **Importance** column, choose the correct value from the asset row drop-down list.
4. Click **Apply** to confirm the override.

Assets with manually overridden values display a visual indicator in the Role or Importance column.



Note: To remove a previously configured override and return to the automated prediction, select the dash (—) option from the **Role** or **Importance** drop-down list.

Overriding Classifications from Asset Details

To override Role or Importance from the asset detail view:

1. Navigate to **Assets > Inventory** and click an asset.
2. In the asset details panel, locate the **Role** and **Importance** fields.
3. Click the drop-down for the field you want to update and select the correct value.
4. Click **Apply** to confirm.

An asset's detail view also displays an explanation of the telemetry attributes that informed the original automated prediction, to assist in determining whether an override is appropriate.

Viewing the Override Audit Trail

All Role and Importance overrides are recorded in an account-level audit trail. To access the audit trail:

1. Choose **Home > System Settings > Activity & Logs**.
2. Choose **Filters > Action Type > override** to display only override events.

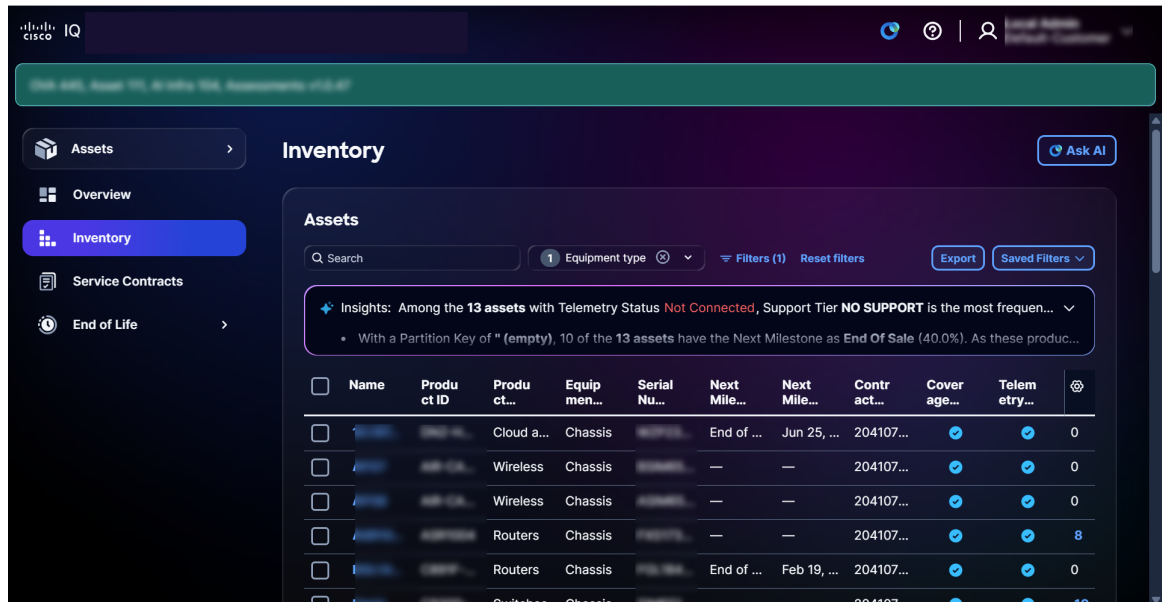
The audit trail displays the asset name, the previous and new values, the user who made the change, and the date and time of the change. The audit trail can be exported using the **Export** option.



Note: The audit trail can be filtered by date range, user, and asset name.

Inventory

The **Inventory** page provides a list of all Cisco assets within the Cisco IQ account.



Inventory

Searching and Filtering Views for Asset Inventory

You can filter the list view by choosing a filter from the drop-down lists or clicking **Filters** and choosing an option from the list of available filters. You can also search for assets by entering the asset name in the **Search** field.

Note:

- Some filters may be hidden depending on screen zoom settings.
- Different filters are available depending on your roles and permissions.

Inventory Analysis

The **Insights** panel on the **Inventory** page displays an AI-driven analysis that provides a summary of assets with a focus on support coverage, connectivity, and milestones. Click **Full Analysis** for visualizations like graphs, dashboards, and charts which provide additional insights. See [Analyzing Data](#) in Common Module Features for more details.

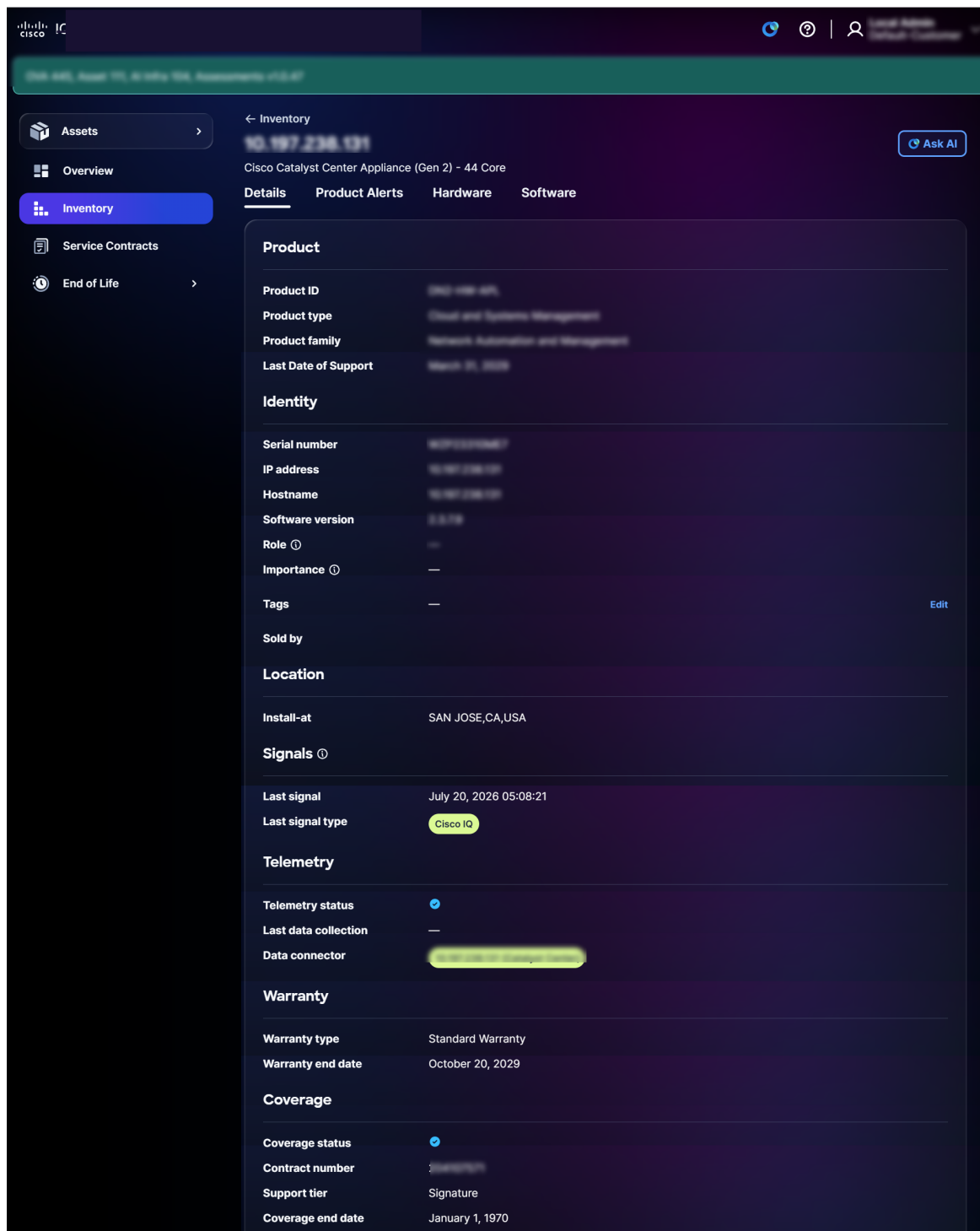
Exporting Inventory

Click **Export** to save a filtered inventory list in .xls or .csv format. See [Exporting Information](#) in Common Module Features for more details.

Viewing Asset Details

Click an asset to view asset details. An asset's detail view displays with the following tabs:

- **Details:** Displays asset details such as product, signal data, identity, location, warranty, and coverage information



Asset Details

- **Product Alerts:** Displays related product alerts such as Security Advisories and Field Notices
- **Hardware:** Provides a detailed timeline view for hardware EOL (for example, **End of Sale**, **Last Ship**, and **Last Date of Support** dates)
- **Software:** Provides a detailed timeline view for software EOL

Asset Tags

Asset tags are custom labels you assign to inventory assets in Cisco IQ. A tag is a

key:value pair—for example, Environment:Prod or Label:Campus—that you define. You can assign tags to individual assets or many assets at once, and you can filter your inventory by tag to quickly find the assets you care about.

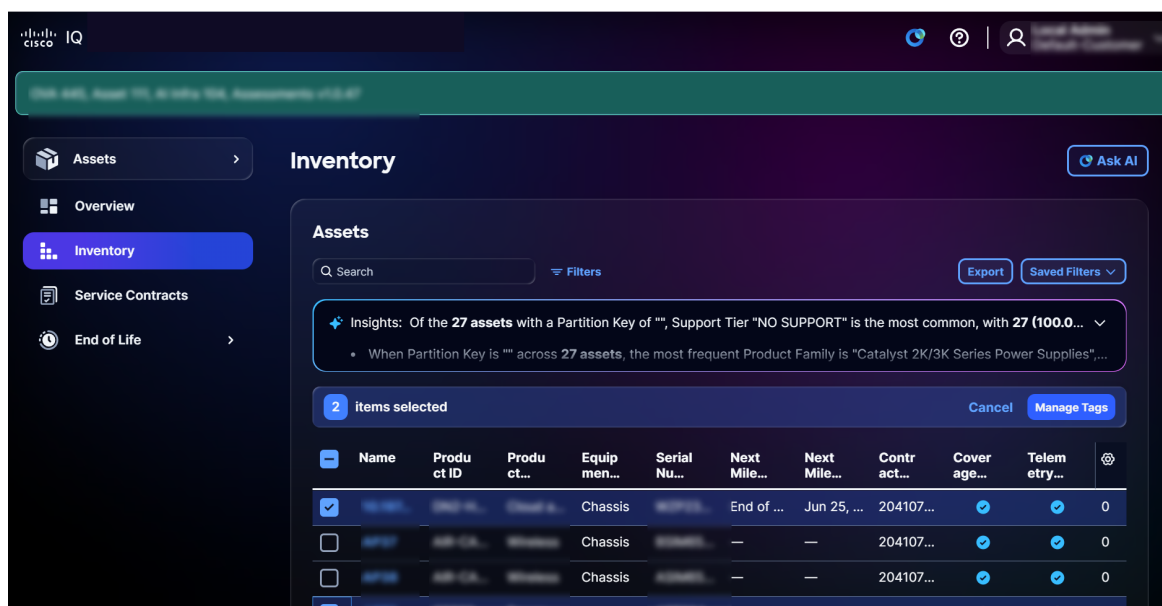
 **Note:** After a tag is created by an Account Administrator, users can assign a tag to an asset.

Assigning Tags

Assigning tags to selected assets in the **Inventory** view enables the organization and categorization of assets for enhanced filtering, reporting, and management.

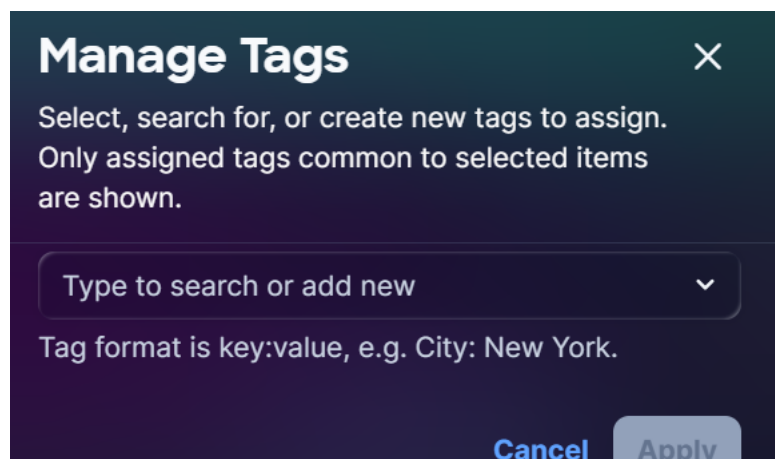
To assign a tag to an asset:

1. Navigate to **Assets > Inventory**.



Tagging Assets

2. Select the check boxes of the desired assets.
3. Click **Manage Tags**. The **Manage Tags** window opens.



Assigning Tags

4. In the text field, input or select the tag name from the existing options and press **Enter**.



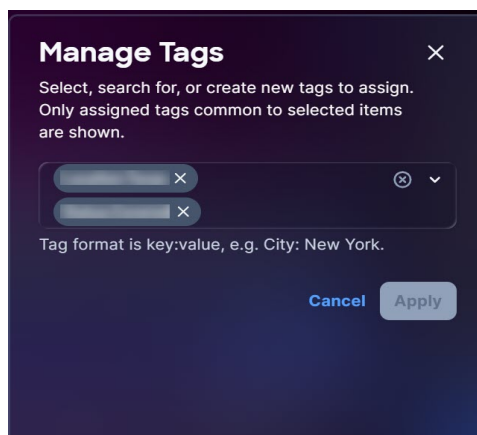
Note: Tags are in **key:value** format (for example, City:NYC).

5. Click **Apply**.

Removing Asset Tags

To remove a tag from one or more assets:

1. Navigate to **Assets > Inventory**.
2. Select the check box next to one or more assets.
3. Click **Manage tags**. The **Manage tags** window opens.



Removing Tags

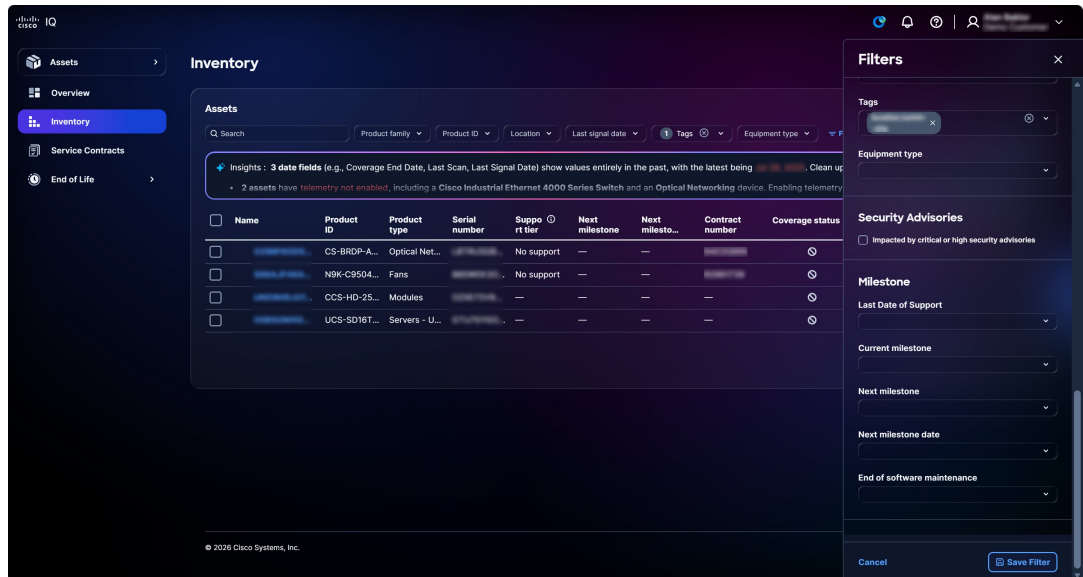
4. Click the **X** on any tag to remove it from the selection.
5. Click **Apply**.

Using Asset Tags as Filters

After creating a tag, you can use the tag as a filter.

To use a tag as a filter:

1. Navigate to the **Inventory** page.
2. Click **Filters**. The **Filters** window opens.

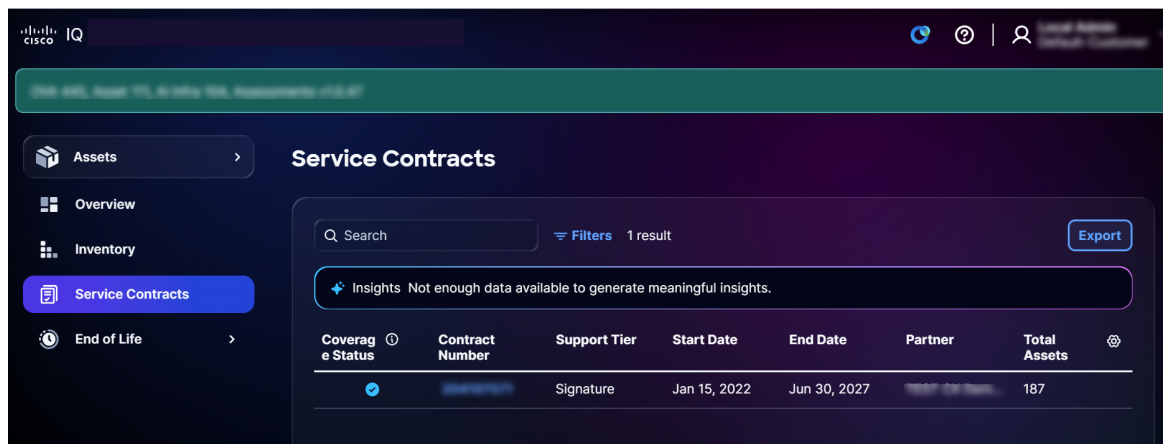


Using Tag as Filter

- From the **Tags** drop-down list, check the check boxes of the desired tags. After selecting the tag, the view on the **Inventory** page updates to the filtered view.

Service Contracts

The **Service Contracts** page streamlines support contract oversight by providing summaries and detailed contract information, supporting effective renewal planning and coverage strategies.



Service Contracts

Searching and Filtering Views for Service Contracts

You can filter the list view by choosing a filter from the drop-down lists. You can also search for service contracts by entering the contract number in the **Search** field.

Exporting Service Contracts

Click **Export** to save a filtered list of contracts in .xls or .csv format. See [Exporting Information](#) in Common Module Features for more details.

Services EA Summary

The **Services Enterprise Agreement (EA) Summary** page provides a consolidated view of install Base growth across your asset portfolio. Data is sourced directly from Cisco's Install Base records, giving you and Account teams a consistent view of portfolio changes over time.

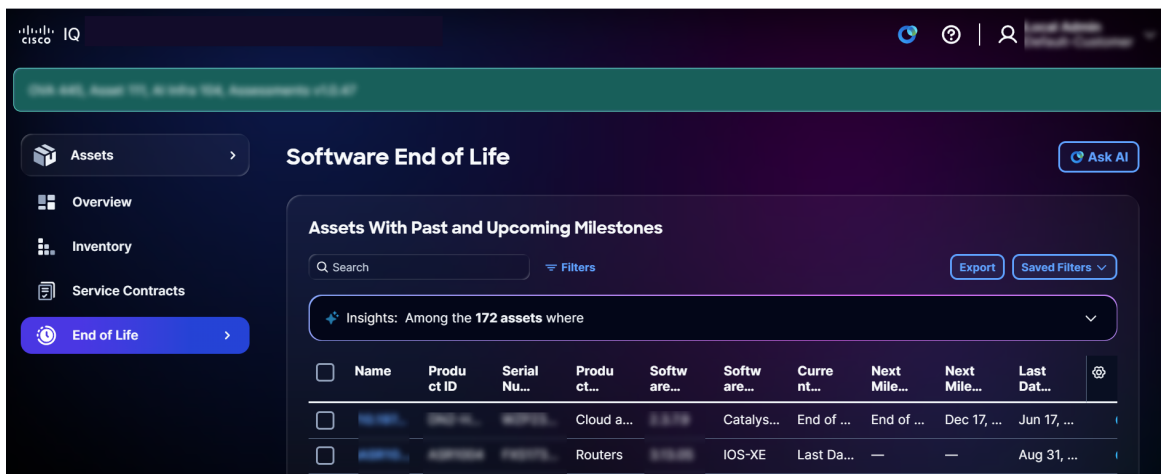
The **Services EA Summary** page displays the following information:

- **Assets Added:** New assets added to the Install Base during the reporting period
- **Net Change:** The overall change in Install Base size for the reporting period

 **Note:** Access to the **Services EA Summary** page may be subject to role and permission requirements. Contact your Account Administrator if this page is not visible in your navigation.

End of Life

The **Hardware End of Life** and **Software End of Life** pages provide detailed EOL information, equipping users with the support needed to proactively manage product refresh cycles and support coverage. Clicking an asset on the **End of Life** pages redirects you to the relevant asset on the **Inventory** page.



☐	Name	Product ID	Serial Number	Product Name	Software Version	Software Name	Current Milestone	Next Milestone	Next Milestone Date	Last Date
☐	Cloud a...			Cloud a...	2.2.19	Catalys...	End of ...	End of ...	Dec 17, ...	Jun 17, ...
☐	Routers			Routers	2.2.19	IOS-XE	Last Da...	—	—	Aug 31, ...

Software End of Life

End of Life Analysis

The **Insights** panel on the **End of Life** page displays an AI-driven overview of assets with a defined Last Day of Support. Click **Full Analysis** for visualizations like graphs, dashboards, and charts which provide additional insights. See [Analyzing Data](#) in Common Module Features for more details.

Exporting End of Life

Click **Export** to save a filtered list of EOL assets in .xls or .csv format. See [Exporting Information](#) in Common Module Features for more details.

Assessments Module

The Assessments module provides an assessment framework that enables you to proactively investigate and mitigate risks related to security, stability, capacity, compliance, and aging, keeping networks secure, stable, and reliable.

Core Concepts

The Assessments module is built on the following core concepts:

- **Assessment:** A systematic evaluation of infrastructure entities against predefined criteria to measure performance, compliance, security, or operational capability; Assessments are triggered on demand, on a schedule, or by an event
- **Assessment Execution:** An instance or single run of an assessment; Each execution creates a new execution record that tracks the scope, trigger mechanism, timestamp, and resulting data produced by the evaluation
- **Finding:** A validated, actionable observation identifying a gap, risk, issue, or noteworthy state. Findings represent the ground-level data during an evaluation
- **Insight:** A higher-level analytical conclusion derived from patterns or trends across multiple findings. Insights interpret what findings mean in a broader business or operational context
- **Recommendation:** A specific, actionable prescription linked to findings or insights; Recommendations provide clear guidance on the necessary steps to address identified issues or capitalize on opportunities
- **Report:** A structured document that aggregates findings, insights, and recommendations for a target audience; Reports are the primary deliverable for communicating assessment outcomes to customers, executives, and technical teams

Accessing Assessments Module

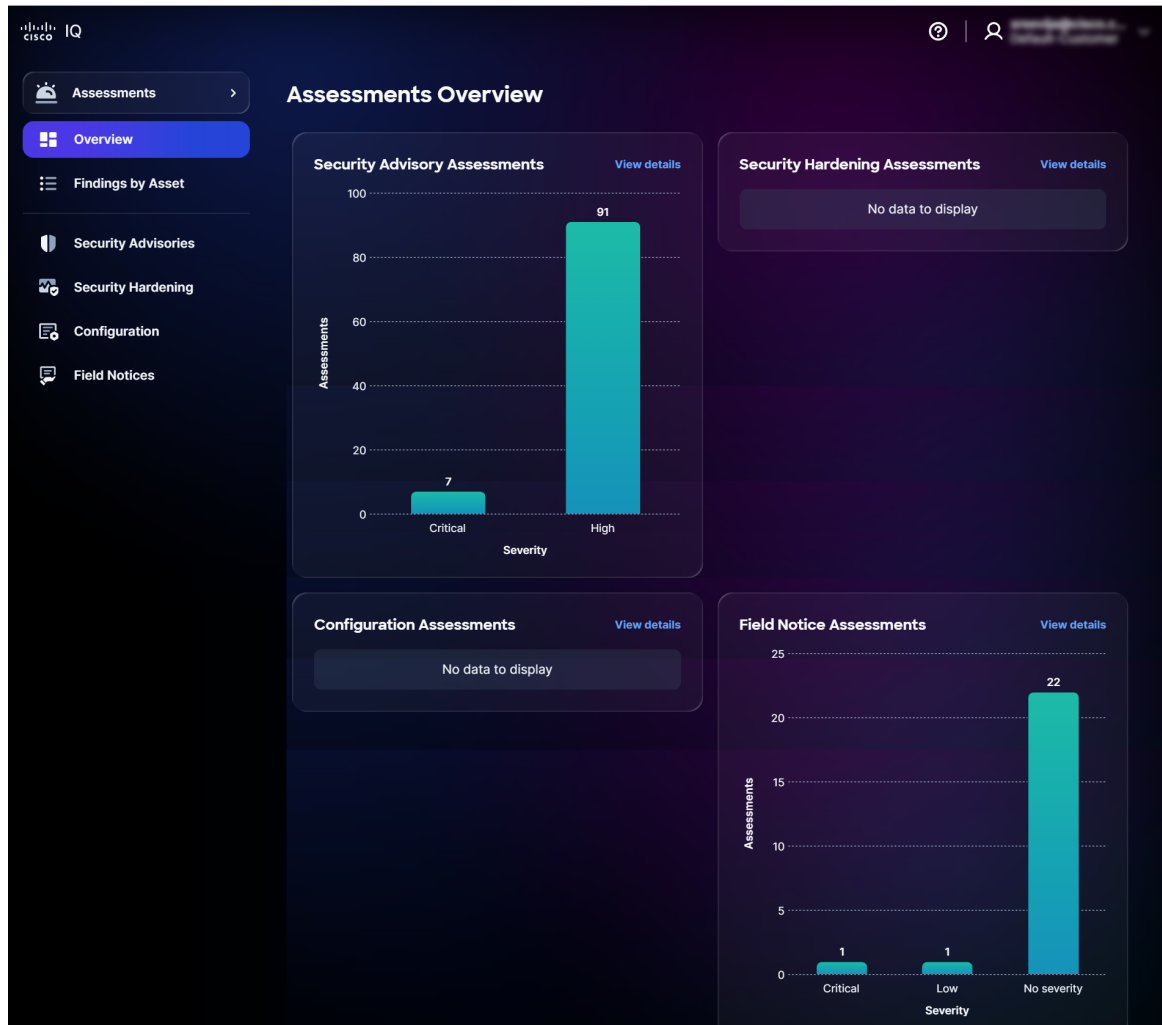
To access security and assessment features in Virtual Appliance, choose the **Home** menu > **Assessments** or click **Assessments** from the **Application** section of the **Home** page > **Launchpad** tab. The **Assessments Overview** page displays.



Note: Assessment module can be also launched from **System Configuration** > **Package Management**.

Assessments Overview

The **Assessments Overview** page displays the following dashboard:



Assessments Overview

The dashboard displays the following information:

- **Security Advisory Assessments:** Displays assessments of security advisories, categorized by Critical and High severity
- **Security Hardening Assessments:** Displays assets failing security hardening rules, categorized by High, Medium, Low and Informational severity
- **Configuration Assessments:** Displays assets failing configuration compliance rules, categorized by Critical, High, Medium, Low and Informational severity
- **Field Notice Assessments:** Displays assessments of field notices, categorized by Critical, High and Not applicable severity



Note: You can only view the assets that you are entitled to access.

Findings by Asset

The **Findings by Asset** page provides you with a list of assets that have been evaluated using at least one of the following assessments: **Security Advisories**, **Security Hardening**, **Configuration** and **Field Notices**.

Name	Importance	IP Address	Serial Number	Security Advisories	Security Hardening	Configuration	Field Notices	Signature
Security A	Low	10.10.10.10	10000000	5	11	32	1	Signature
Security A	Low	10.10.10.10	10000000	5	11	32	1	Signature
Security A	Low	10.10.10.10	10000000	5	11	32	1	Signature
Security A	Low	10.10.10.10	10000000	5	11	32	1	Signature
Security A	Low	10.10.10.10	10000000	5	11	32	1	Signature

Findings By Assets

Searching and Filtering Views for Findings by Asset

You can filter the list view by choosing a filter from the drop-down lists or clicking **Filters** and choosing an option from the list of available filters. You can also search for **Findings by Asset** in the **Search** field.

Note:

- Some filters may be hidden depending on screen zoom settings.
- Different filters are available depending on your roles and permissions.

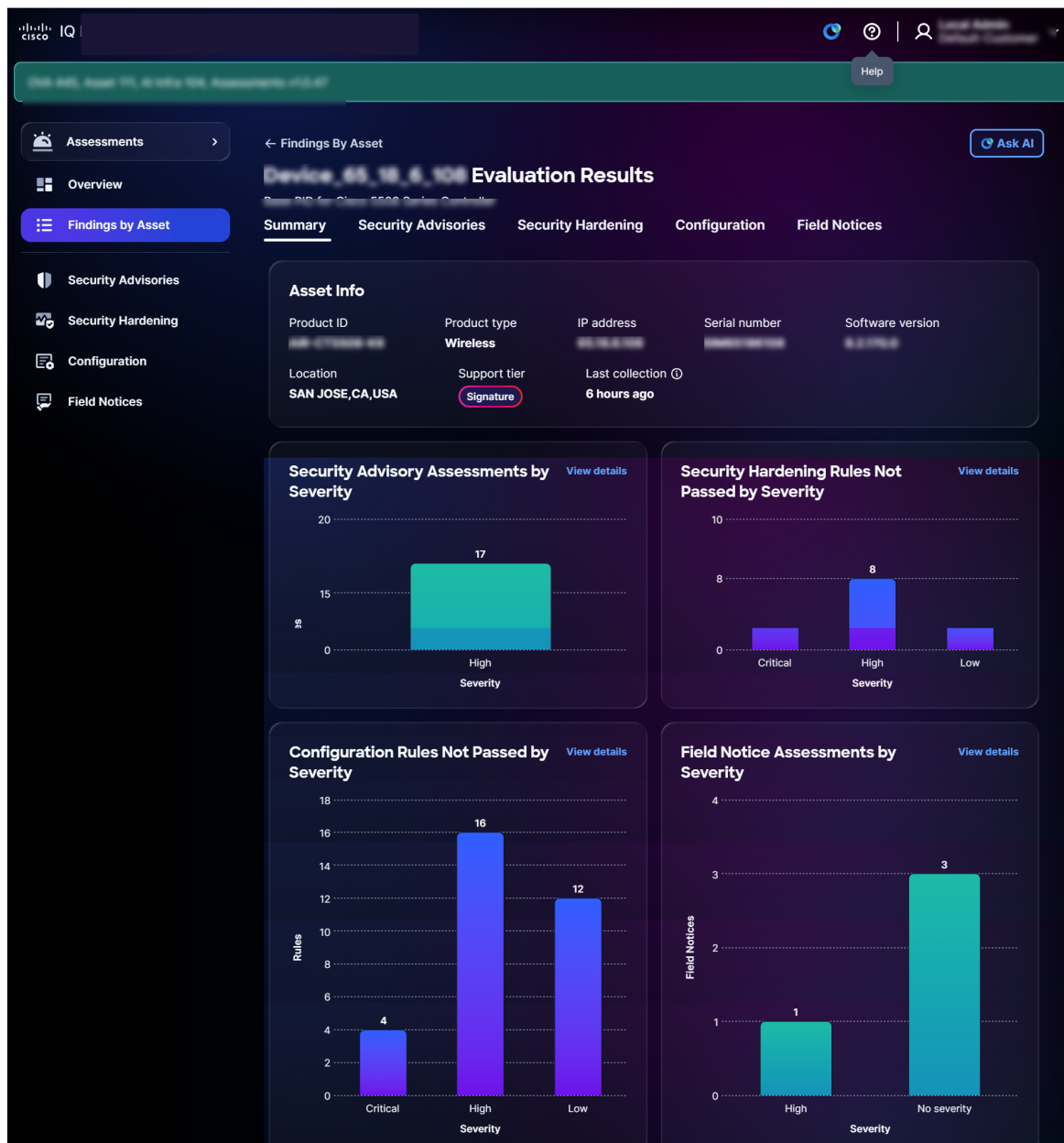
Exporting Findings by Asset

To export the Findings by Asset list view, click **Export**. See [Exporting Information](#) for more information.

Viewing Findings by Asset Details

To view **Findings by Asset** details, click an **Asset**. The following tabs display details for the selected asset:

- **Summary:** Provides detailed asset information including the number of **Security Advisories**, **Security Hardening**, **Configuration** and **Field Notices**
- **Security Advisories:** Provides a list of related Security Advisory assessments
- **Security Hardening:** Provides a list of assets failing Security Hardening rules
- **Configuration:** Provides a list of assets failing Configuration Best Practice rules
- **Field Notices:** Provides a list of related Field Notice assessments



Findings by Asset Details

When clicking **View Details** on a tile, the page redirects to the relevant page within the module.

When clicking **View full asset details**, the asset detail view page displays.

Security Advisories

Security Advisory assessments identify vulnerabilities and prioritize them based on their risk, severity, and criticality, thereby enhancing the organization's risk management capabilities. Security Advisories deliver granular insights into vulnerabilities, help accelerate mitigation of critical threats, and ensure alignment with compliance and business objectives. This strengthens security posture, optimizes resource allocation, and fosters resilience against evolving threats across the enterprise. Security Advisories are automatically updated in Cisco IQ as soon as they are released.

The **Security Advisories** page provides a list of all Security Advisories with vulnerabilities detected within the organization. Clicking an advisory from the Security

Advisory assessments list navigates to the corresponding detail view.

Assessment	Severity	Affected Assets	Potentially Affected...	CVE	Last Updated
Cisco IOS and I...	High	0	12		Oct 4, 2019
Cisco IOS and I...	High	0	1		Sep 25, 2019
Cisco IOS and I...	High	1	0		Mar 23, 2016
Multiple Vulner...	High	0	1		Jan 11, 2016
Cisco IOS and I...	High	0	1		Jul 26, 2017
Cisco IOS and I...	High	1	0		Sep 28, 2016

Security Advisories

Searching and Filtering Views for Security Advisories

You can filter the list view by choosing a filter from the drop-down list. You can also search for Security Advisory assessments by entering the assessment name in the **Search** field.

 **Note:** Some filters may be hidden depending on screen zoom settings. Some filters may be hidden depending on screen zoom settings. Different filters are available depending on your roles and permissions. Missing severity values display as “–” with a descriptive tooltip.

Exporting Security Advisories

To export Security Advisory assessments, click **Export**. See [Exporting Information](#) for more information.

Viewing Security Advisory Assessment Details

Click an **Assessment** to view additional details about it. The details page provides information such as **Common Vulnerability Scoring System (CVSS) Score**, **Common Vulnerabilities and Exposures (CVE)**, **Severity**, and a link to the referenced Cisco Security Advisory.

You can view the following types of results in the **Assessment outcome** table:

- **Affected:** Indicates that the asset or component has a confirmed vulnerability that can be exploited by an attacker, requiring remediation
- **Potentially Affected:** Indicates that the asset or component shows signs that may lead to vulnerability, but it is not definitively confirmed; further investigation may be needed

Security Advisories

← Security Advisories

Cisco IOS and IOS XE Software Session Initiation Protocol Denial of Service Vulnerability

About the Assessment

A vulnerability in the common Session Initiation Protocol (SIP) library of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to insufficient sanity checks on an internal data structure....
[Show more](#)

Severity	CVE	CVSS score
High		8.8
Version	First published	Last updated
1.1	Sep 25, 2019	Oct 4, 2019
References		
Security Advisory		

Asset Results

Q Search Filters 12 results Export Saved Filters

Asset	Result	Product ID	IP Address	Serial Number	Support Tier
ISR44...	Potentially Affected				Signature
ISR43...	Potentially Affected				Signature
Isr4431	Potentially Affected				Signature
ISR43...	Potentially Affected				Signature
ISR44...	Potentially Affected				Signature
ISR44...	Potentially Affected				Signature
ISR44...	Potentially Affected				Signature
ISR44...	Potentially Affected				Signature
ISR43...	Potentially Affected				Signature

Security Advisories Details

Searching and Filtering Views for Asset Assessment Results

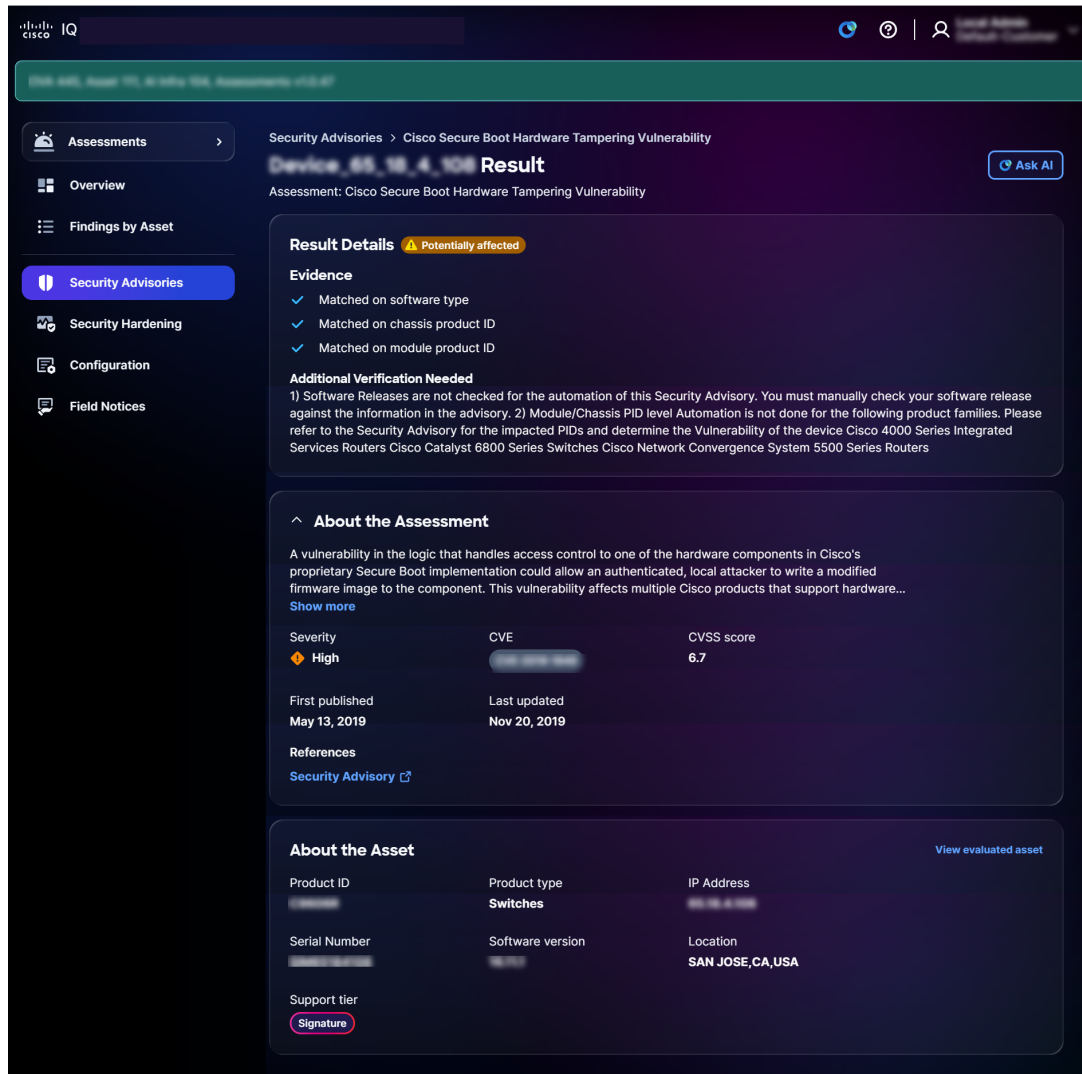
You can filter the list view by choosing a filter from the drop-down lists or clicking **Filters** and choosing an option from the list of available filters. You can also search for assets by entering the asset name in the **Search** field.



Note: Some filters may be hidden depending on screen zoom settings. Different filters are available depending on your roles and permissions.

Viewing Asset Assessment Results

To view details of an assessment result, click an asset from the **Assessment Outcome** table. The asset's **Assessment Result** details page displays.



Result

Assessment: Cisco Secure Boot Hardware Tampering Vulnerability

Result Details ⚠️ Potentially affected

Evidence

- ✓ Matched on software type
- ✓ Matched on chassis product ID
- ✓ Matched on module product ID

Additional Verification Needed

1) Software Releases are not checked for the automation of this Security Advisory. You must manually check your software release against the information in the advisory. 2) Module/Chassis PID level Automation is not done for the following product families. Please refer to the Security Advisory for the impacted PIDs and determine the Vulnerability of the device Cisco 4000 Series Integrated Services Routers Cisco Catalyst 6800 Series Switches Cisco Network Convergence System 5500 Series Routers

About the Assessment

A vulnerability in the logic that handles access control to one of the hardware components in Cisco's proprietary Secure Boot implementation could allow an authenticated, local attacker to write a modified firmware image to the component. This vulnerability affects multiple Cisco products that support hardware...

[Show more](#)

Severity: High CVE: CVSS score: 6.7

First published: May 13, 2019 Last updated: Nov 20, 2019

References: [Security Advisory](#)

About the Asset [View evaluated asset](#)

Product ID	Product type	IP Address
	Switches	
Serial Number	Software version	Location
		SAN JOSE, CA, USA
Support tier	Signature	

Result Details

Exporting Asset Results for Security Advisories

To export asset results, click **Export**. See [Exporting Information](#) for more information.

Security Hardening

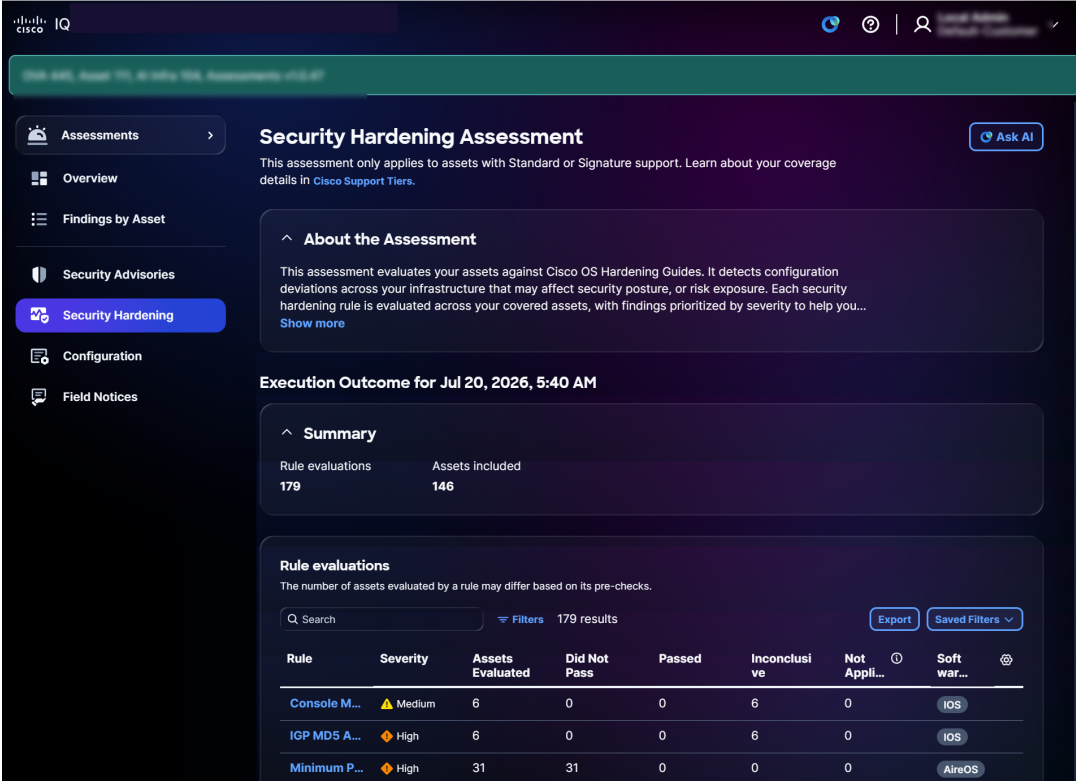
Security Hardening provides automated, near real-time visibility into the security posture of your network infrastructure by continuously evaluating routers, switches, and firewalls against industry-standard benchmarks. It identifies configuration gaps and provides actionable remediation guidance, enabling Account Administrators to effectively reduce the attack surface and maintain consistent alignment with Cisco's rigorous security best practices. By centralizing compliance monitoring and simplifying the hardening process, the module transforms security management from a reactive task into a proactive, data-driven strategy, ensuring a resilient and secure enterprise network.



Note: Security Hardening Assessments are available exclusively for assets with **Standard** support tiers.

Viewing Security Hardening Assessments

The **Security Hardening Assessment** page displays the following information:



Security Hardening Assessment

This assessment only applies to assets with Standard or Signature support. Learn about your coverage details in [Cisco Support Tiers](#).

About the Assessment

This assessment evaluates your assets against Cisco OS Hardening Guides. It detects configuration deviations across your infrastructure that may affect security posture, or risk exposure. Each security hardening rule is evaluated across your covered assets, with findings prioritized by severity to help you... [Show more](#)

Execution Outcome for Jul 20, 2026, 5:40 AM

Summary

Rule evaluations	Assets included
179	146

Rule evaluations

The number of assets evaluated by a rule may differ based on its pre-checks.

Search: Filters: 179 results [Export](#) [Saved Filters](#)

Rule	Severity	Assets Evaluated	Did Not Pass	Passed	Inconclusive	Not Applicable	Software
Console M...	Medium	6	0	0	6	0	IOS
IGP MD5 A...	High	6	0	0	6	0	IOS
Minimum P...	High	31	31	0	0	0	AireOS

Security Hardening

- **About the Assessment:** Provides additional details by summarizing the purpose of the assessment
- **Execution Outcome:** Provides a summary of asset assessment results, including the total number of **Rule evaluations** and **Assets included**
- **Rule evaluations:** Provides detailed information about the rule, including **Severity**, **Assets Evaluated**, **Did Not Pass**, **Passed**, **Inconclusive**, **Not Applicable**, and **Software type**
- **Severity:** Provides the level of importance or impact of the rule evaluation
- **Assets Evaluated:** Provides the total number of assets that were assessed against the rule criteria
- **Did Not Pass:** Provides the assets that failed to meet the rule criteria during the assessment
- **Passed:** Provides the assets that met the rule criteria during the assessment
- **Inconclusive:** Provides the assets for which the assessment could not determine failure
- **Not Applicable:** Indicates the assets or scenarios where the rule does not apply or is not relevant

- **Software type:** Provides the software type of assets

Searching and Filtering Views for Rules

You can filter the list view by choosing a filter from the drop-down lists or clicking **Filters** and choosing an option from the list of available filters. You can also search for a rule by entering the rule name in the **Search** field.



Note: Some filters may be hidden depending on screen zoom settings. Different filters are available depending on your roles and permissions.

Viewing Rule Evaluation Details

To view additional details about a rule evaluation, click a rule. The rule's evaluation details page displays with the following information:

The screenshot shows the Cisco IQ interface for a Security Hardening Assessment. The main heading is "Minimum Password Length Policy", evaluated on Jul 20, 2026, at 5:39 AM. The left sidebar contains navigation options: Assessments, Overview, Findings by Asset, Security Advisories, Security Hardening (selected), Configuration, and Field Notices. The main content area includes an "About the Rule" section with a description, severity (High), software type (AireOS), and 31 assets evaluated. Below this is a "Results Summary" showing 0 Passed, 31 Didn't pass, 0 Inconclusive, and 0 Not applicable. The "Asset Results" section displays a table with columns: Asset, Result, Product ID, Serial Number, IP Address, and Support Tier. The table shows five rows, all with "Didn't pass" results and "Signature" support tier.

Asset	Result	Product ID	Serial Number	IP Address	Support Tier
Device...	Didn't pass	...	...	...	Signature
Device...	Didn't pass	...	...	...	Signature
Device...	Didn't pass	...	...	...	Signature
Device...	Didn't pass	...	...	...	Signature
Device...	Didn't pass	...	...	...	Signature

Rule View

- **About the Rule:** Provides details about the rule such as **Severity**, **Software type**, **Version**, and **Assets evaluated** and includes descriptive labelled links to relevant source documentation
- **Results Summary:** Provides a summary of asset results related to the rule such as **Passed**, **Did not pass**, **Inconclusive**, and **Not applicable**
- **Assets Results:** Provides a list of assets with details such as **Asset**, **Result**, **Product ID**, **Serial Number**, **IP Address**, and **Support Tier**



Note: Cisco IQ provides clear guidance when an assessment finding is “Inconclusive,” explaining the cause (for example, missing telemetry, or unsupported OS) and recommending steps like verifying data collection, updating credentials, or refreshing data. Labelled links to relevant documentation are also provided to help resolve issues.

Searching and Filtering Views for Asset Rules

You can filter the list view by choosing a filter from the drop-down lists or clicking **Filters** and choosing an option from the list of available filters. You can also search for asset assessment results by entering the asset name in the **Search** field.



Note: Some filters may be hidden depending on screen zoom settings. Different filters are available depending on your roles and permissions.

Exporting Asset Results

To export assessment results for rules, click **Export**. See [Exporting Information](#) for more information.

Searching and Filtering Views for Asset Results

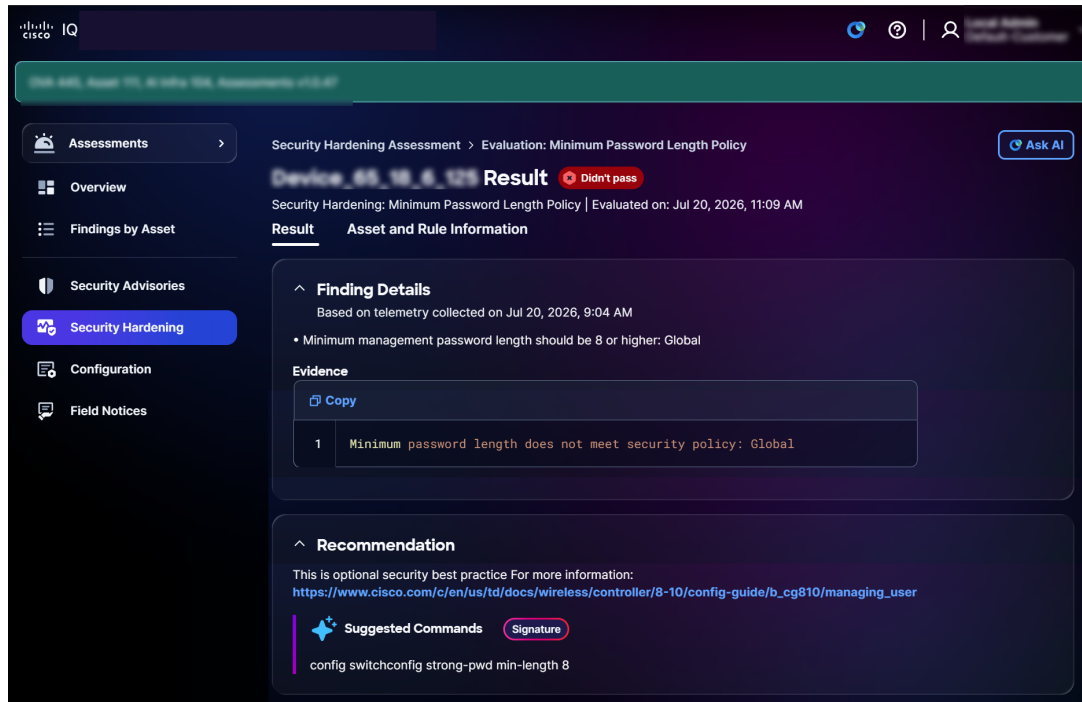
You can filter the list view by choosing a filter from the drop-down lists or clicking **Filters** and choosing an option from the list of available filters. You can also search for asset results by entering the asset name in the **Search** field.



Note: Some filters may be hidden depending on screen zoom settings. Different filters are available depending on your roles and permissions.

Viewing Asset Results for Security Hardening

Click an asset from **Asset Results** to view its details. The asset’s result details page displays information according to your entitlement level or tier.



Security Hardening Standard Tier

- **Standard Tier**
- **Finding Details:** Provides information about the configuration deviations identified during the assessment along with evidence logs
- **Recommendations:** Provides guidance to address the findings and ensure configuration consistency

Viewing Asset and Rule Information for Security Hardening

To view the details of an Asset and its rules, click the **Asset and Rule Info** tab. The **Asset and Rule Info** page displays.

About the Asset: Provides the details of the asset such as **Product ID**, **Product type**, **IP address**, **Serial number**, **Software version**, **Location**, and **Support Tier**

- **About the Rule:** Provides rule details (including **Severity** and **Software type**) and the importance of that particular hardening check

Configuration

Configuration assessments evaluate your assets against recommended best practices based on Cisco's proven expertise to detect configuration deviations that may affect availability, security, or performance across your infrastructure. Each best practice rule is assessed across your covered assets, and findings are prioritized by severity to ensure configuration consistency, enhanced resilience, and reduced operational risk.

 **Note:** Configuration Assessments are available exclusively for assets with **Standard** support tiers.

Viewing Configuration Assessments

The **Configuration Assessment** page displays the following information:

Configuration Assessment

This assessment only applies to assets with Standard and Signature support. Learn about your coverage details in [Cisco Support Tiers](#).

About the Assessment

This assessment evaluates your assets against recommended best practices based on Cisco's proven expertise. It detects configuration deviations across your infrastructure that may affect availability, security, or performance. Each best practice rule is evaluated across your covered assets, with findings prioritized b... [Show more](#)

Execution Outcome for Jul 20, 2026, 05:40 AM

Summary

Rule evaluations	Assets included
729	146

Rule Evaluations

The number of assets evaluated by a rule may differ based on its pre-checks.

Q Search Filters 729 results Export Saved Filters

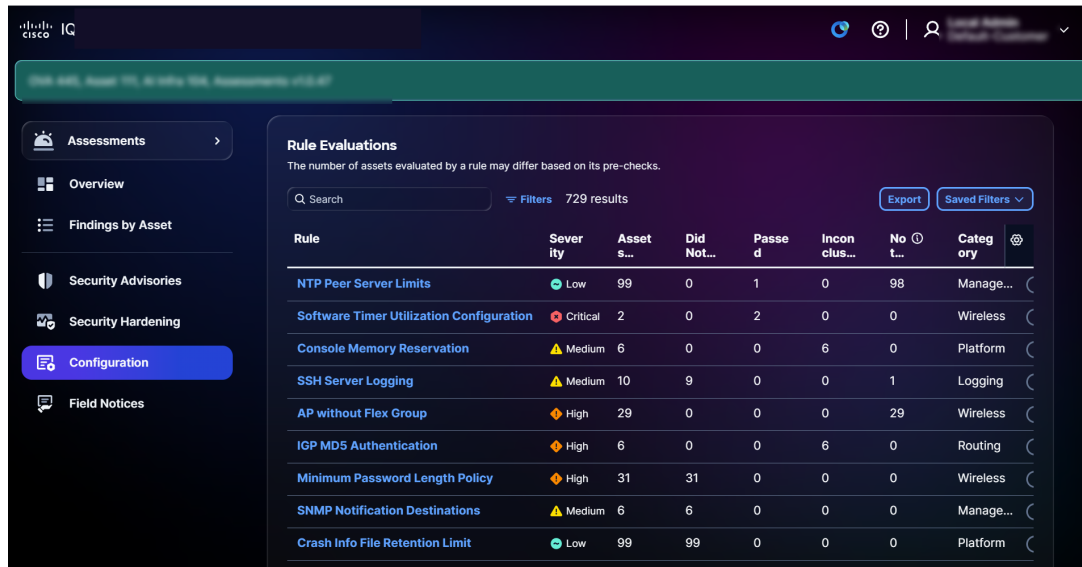
Rule	Severity	Assets	Did Not...	Passed	Inconcl...	No t...	Category
NTP Peer Server Limits	Low	99	0	1	0	98	Manage...
Software Timer Utilization Configuration	Critical	2	0	2	0	0	Wireless
Console Memory Reservation	Medium	6	0	0	6	0	Platform
SSH Server Logging	Medium	10	9	0	0	1	Logging

Configuration Assessment

- **About the Assessment:** Provides additional details by summarizing the purpose of the assessment
- **Summary:** Provides a summary of configuration execution like **Rules evaluated** and **Assets evaluated**
- **Insights:** Provides insights into identified configuration gaps generated through pattern analysis and a correlation of findings; they are displayed as intelligently grouped key cards to highlight the most critical areas that require attention
- **Rule Evaluations:** Provides detailed information about the rule, including **Severity**, **Assets Evaluated**, **Did Not Pass**, **Passed**, **Inconclusive**, **Not Applicable**, **Category**, and **Software type**
- **Severity:** Provides the level of importance or impact of the rule evaluation
- **Assets Evaluated:** Provides the total number of assets that were assessed against the rule criteria
- **Did Not Pass:** Provides the total number of assets that failed to meet the rule criteria during the assessment
- **Inconclusive:** Provides the total number of assets for which the assessment could not run

- **Passed:** Provides the assets that met the rule criteria during the assessment
- **Not Applicable:** Indicates the assets or scenarios where the rule does not apply or is not relevant
- **Category:** Provides the domain area to which the rule belongs
- **Software Type:** Indicates the type of software assets to which the rule applies

Searching and Filtering Views for Rules



The screenshot shows the Cisco IQ interface for Rule Evaluations. The left sidebar contains navigation links: Assessments, Overview, Findings by Asset, Security Advisories, Security Hardening, Configuration (highlighted), and Field Notices. The main content area is titled 'Rule Evaluations' and includes a search bar, a filter button, and a table of results. The table has columns for Rule, Severity, Asset s..., Did Not..., Passe d, Incon clus..., No t..., and Categ ory. The table lists several rules with their respective severities and counts.

Rule	Severity	Asset s...	Did Not...	Passe d	Incon clus...	No t...	Categ ory
NTP Peer Server Limits	Low	99	0	1	0	98	Manage...
Software Timer Utilization Configuration	Critical	2	0	2	0	0	Wireless
Console Memory Reservation	Medium	6	0	0	6	0	Platform
SSH Server Logging	Medium	10	9	0	0	1	Logging
AP without Flex Group	High	29	0	0	0	29	Wireless
IGP MD5 Authentication	High	6	0	0	6	0	Routing
Minimum Password Length Policy	High	31	31	0	0	0	Wireless
SNMP Notification Destinations	Medium	6	6	0	0	0	Manage...
Crash Info File Retention Limit	Low	99	99	0	0	0	Platform

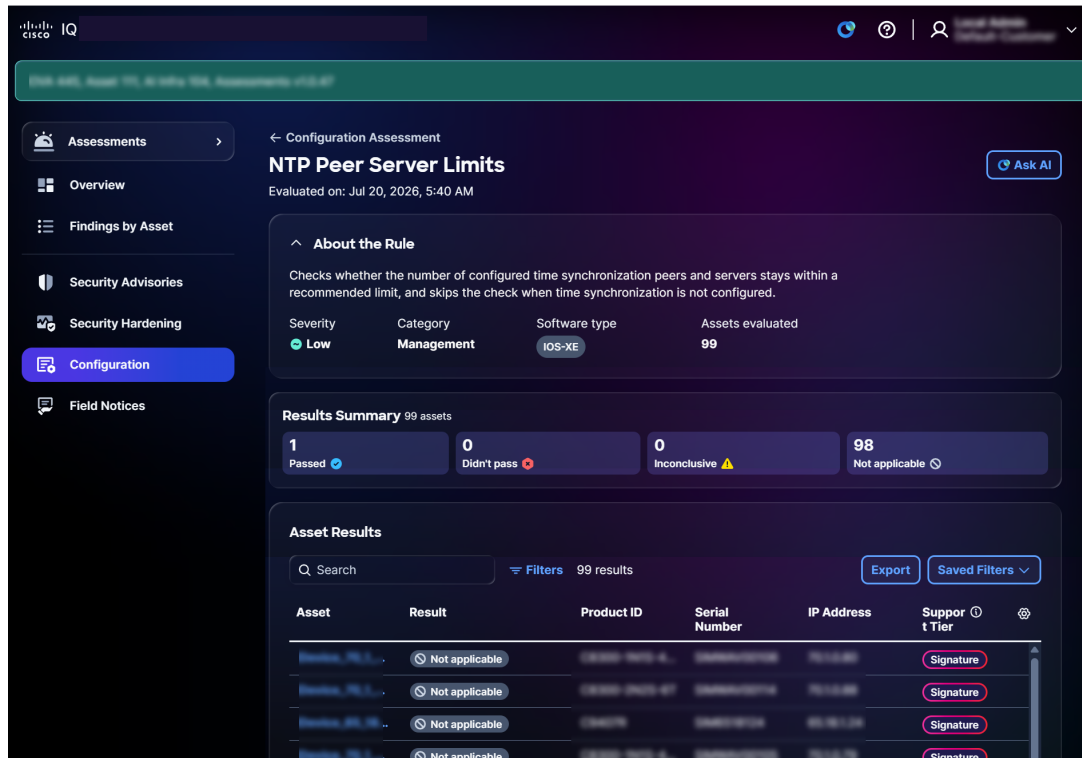
Rule Evaluations

You can filter the list view by choosing a filter from the drop-down lists or clicking **Filters** and choosing an option from the list of available filters. You can also search for a rule by entering the rule name in the **Search** field.

 **Note:** Some filters may be hidden depending on screen zoom settings. Different filters are available depending on your roles and permissions.

Viewing Rule Evaluation Details

To view additional details about a rule evaluation, click any rule. The rule's evaluation details page displays with the following information:



Evaluation

- **About the Rule:** Provides details about a rule like **Severity**, **Category**, **Software type**, and **Assets evaluated** and includes descriptive labelled links to relevant source documentation
- **Results Summary:** Provides overall asset results by displaying the number of assets in **Passed**, **Did not pass**, **Inconclusive**, and **Not applicable** statuses
- **Asset Results:** Provides a list of assets impacted by the selected rule with result status



Note: Cisco IQ provides clear guidance when an assessment finding is "Inconclusive," explaining the cause (for example, missing telemetry, or unsupported OS) and recommending steps like verifying data collection, updating credentials, or refreshing data. Labelled links to relevant documentation are also provided to help resolve issues. The Assessment module supports multi-category selection for rules, enabling simultaneous processing and evaluation across multiple rule categories.

Exporting Asset Results

To export asset results for rules, click **Export**. See [Exporting Information](#) for more information.

Searching and Filtering Views for Asset Results

You can filter the list view by choosing a filter from the drop-down lists or clicking **Filters** and choosing an option from the list of available filters. You can also search for asset results by entering the asset name in the **Search** field.

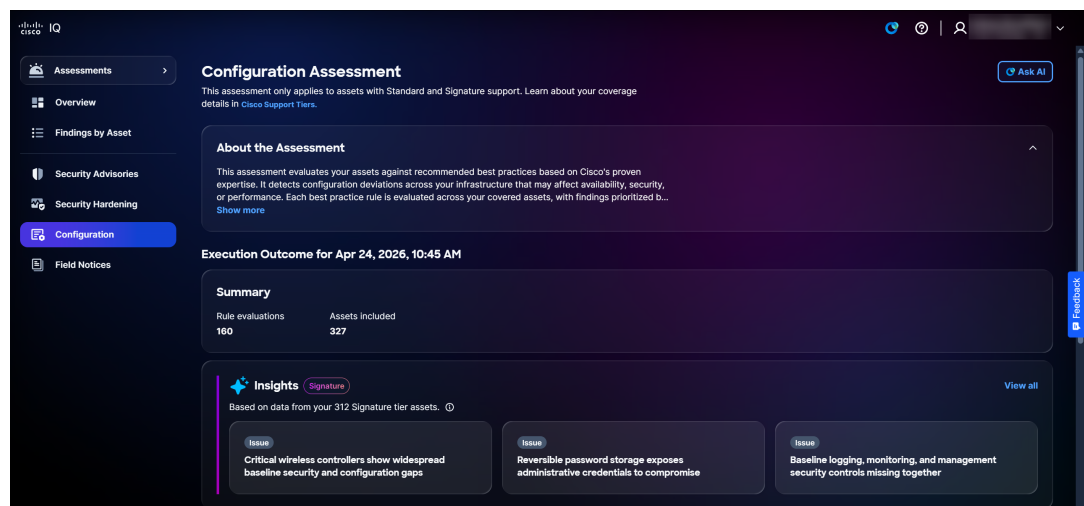
Asset and Rule Info

The **Asset and Rule Info** page displays with the following information:

- **About the Asset:** Provides the details of an asset, such as **Product ID**, **Product type**, **IP address**, **Serial number**, **Software version**, **Location** and **Support tier**
- **About the Rule:** Provides details of a rule such as **Severity**, **Category**, and **Software type**

Viewing Insights

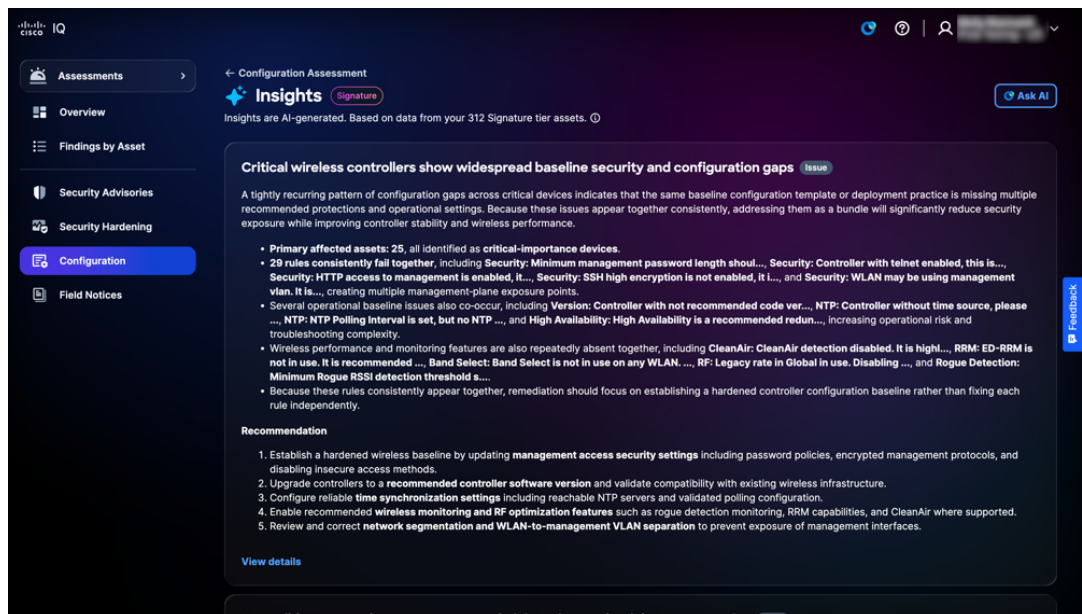
Insights are AI-generated and serve as an intelligent dashboard that synthesizes assessment data into prioritized key cards, highlighting critical configuration disparities across multiple findings. It enables you to address the most impactful infrastructure risks efficiently by focusing on these urgent areas. It also highlights strengths by identifying areas where your infrastructure is performing well as per best practices.



Insights

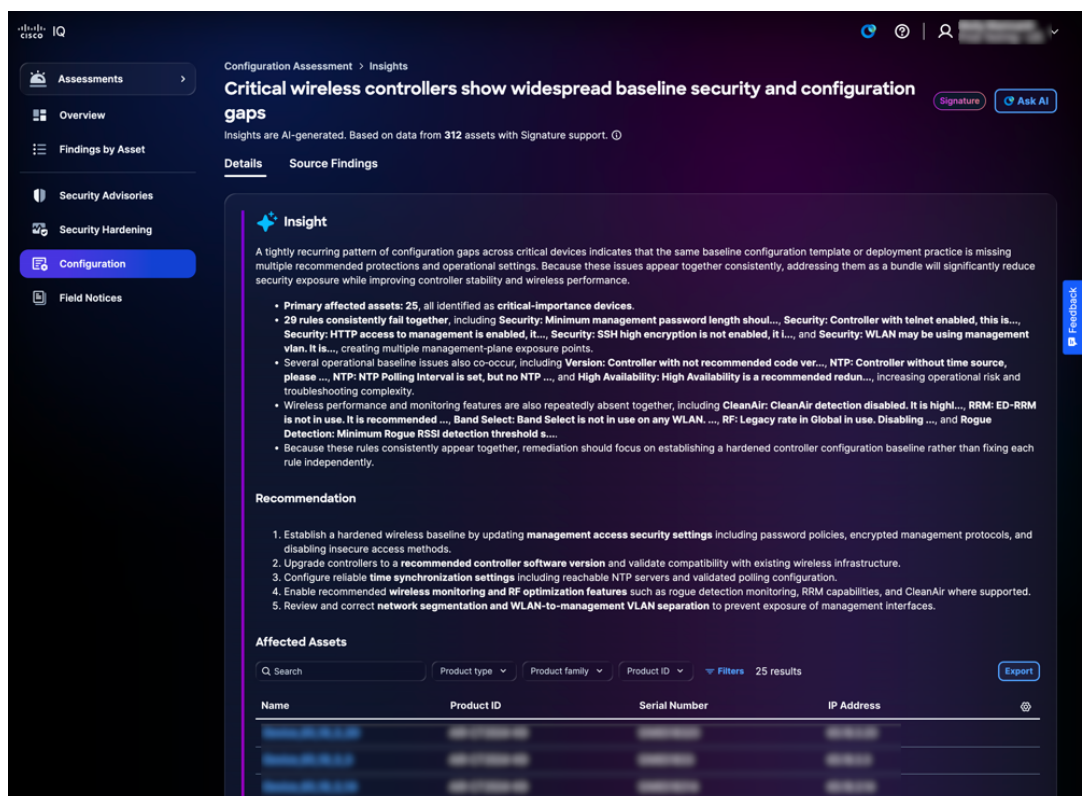
To view Insights details:

1. From the Insights panel, click **View all**. The **Insights** page displays all insights.



Insights Page

2. Click **View details** or click any card. The Insights detail page displays with the following information:



Insights Detail

- **Insight:** Provides a summary that highlights recurring patterns of configuration deviations identified through comprehensive analysis across multiple findings, as well as areas of excellence in your infrastructure where configurations align with best practices
- **Recommendation:** Provides actionable steps to remediate the identified configuration gaps

- **Affected Assets:** Provides a list of specific devices where the configuration deviation has been identified as defined under the **Insight** section
3. Click **Source Findings**. The **Source Findings** page displays the detailed individual findings that support your insights.

The screenshot shows the Cisco IQ Configuration Assessment Insights page. The main heading is "Critical wireless controllers show widespread baseline security and configuration gaps". Below this, it states "Insights are AI-generated. Based on data from 312 assets with Signature support." The page is divided into two tabs: "Details" and "Source Findings", with "Source Findings" being the active tab. A table displays 725 results, filtered by "Severity" and "Result". The table has columns for Asset, Rule, Severity, Serial Number, and Result. The results show multiple instances of "High Availability: High Availa..." with a "Low" severity and "Did not pass" result.

Asset	Rule	Severity	Serial Number	Result
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass

Source Findings

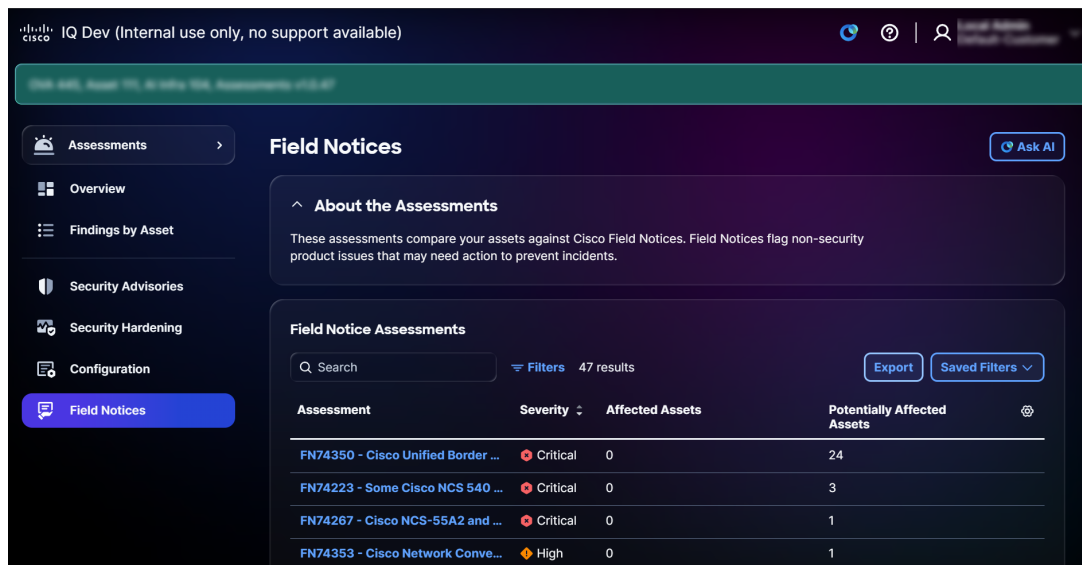
You can filter the table view by choosing a filter from the **Severity** and **Result** drop-down lists.



Note: Recommendations and Affected Assets are optional depending on the output of each insight.

Field Notices

Field Notices identify significant non-security-related product issues and organize them based on their impact severity and criticality, enhancing the organization’s ability to manage product risks. Field Notices deliver actionable insights into product defects, accelerate mitigation through recommended upgrades or workarounds, and ensure alignment with operational and business objectives. This strengthens product reliability, optimizes resource allocation, and fosters resilience against evolving product challenges across the enterprise.



Field Notices

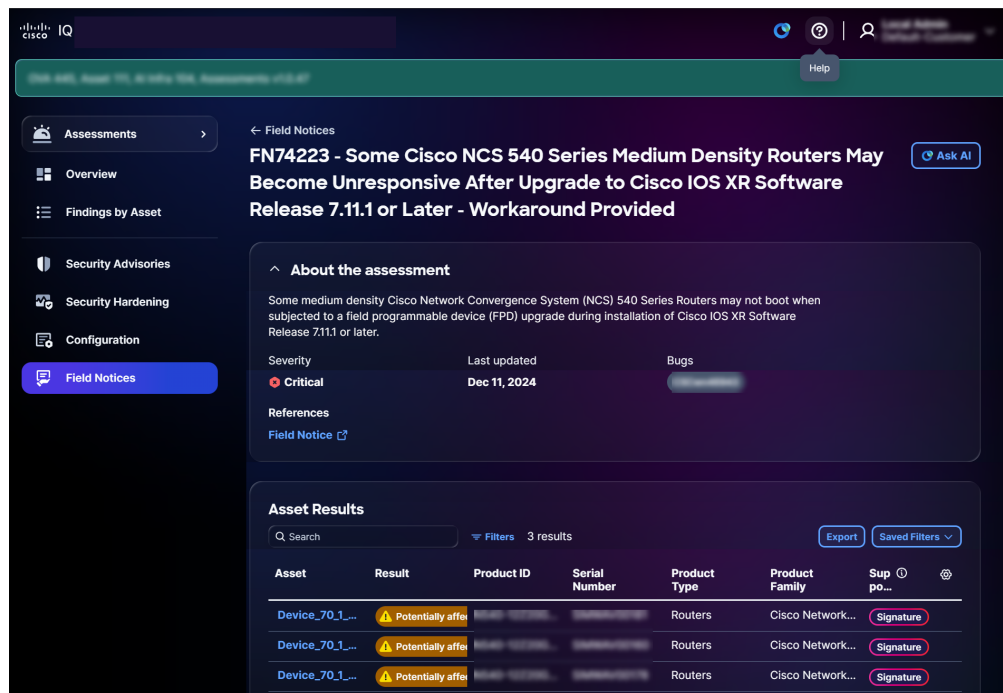
Searching and Filtering Views for Field Notices

You can filter the list view by choosing a filter from the drop-down lists. You can also search for field notice assessments by entering the assessment name in the **Search** field.

Viewing Assessments for Field Notices

To view additional details about a field notice, click an **Assessment**. The following assessment details display:

- **About the Assessments:** Provides additional details by summarizing the purpose of the assessment
- **Field Notice Assessments:** Displays a list of assets impacted by the selected field notice, including assets with detected vulnerabilities



Viewing Assessments for Field Notices

Searching and Filtering Views for Asset Results for Field Notices

You can filter the list view by choosing a filter from the drop-down lists or clicking **Filters** and choosing an option from the list of available filters. You can also search for asset results by entering the asset name in the **Search** field.



Note: Some filters may be hidden depending on screen zoom settings. Different filters are available depending on your roles and permissions.

Exporting Asset Results for Field Notices

To export assessment asset results for field notices, click **Export**. See [Exporting Information](#) for more information.

Viewing Asset Assessment Results for Field Notices

To view an asset's assessment result details, click an asset from **Asset Assessment Results**. The asset's assessment result details page displays.

You can view the following types of results:

- **Affected:** Indicates assets that meet all the criteria automatically checked for a Field Notice and require no additional manual verification to confirm they are impacted
- **Potentially Affected:** Indicates assets that meet all the automatically checked criteria for a Field Notice but require additional manual verification to confirm if they are truly impacted

The following prompts are available under the **Assessments – Security Hardening** tab:

- What are Cisco security hardening best practices for network devices?
- How do I harden my Cisco IOS XE devices?
- List key security hardening steps for routers and switches.
- What are recommended baseline hardening settings for Cisco devices?
- How many assets are in violation of security hardening best practices?

Local Authentication

Account Administrators should use the following credentials to successfully log in to VA:

- **Default Username:** admin
- **Default Password:** The password that is set during the VA installation process; refer to the *Getting Started Guide* for more information
- **Default Account Context:** Default-Customer

Upon login, the default user, “admin”, and the account name, “Default-Customer” display on the home page.

Setting Local Admin Security

You can change your password and set up security questions through the **User Profile** menu in **Home page**.

Lockout Settings

The following account lockout settings are configurable during deployment:

- **Lockout Status:** Enables or disables the account lockout feature.
- **Maximum Login Attempts:** Sets the maximum number of consecutive failed attempts allowed before an account is locked (Default: 3; Range: 0–10).
- **Rolling Time Window:** Defines the time period for tracking failed attempts (Default: 15 minutes; Range: 0–60 minutes).
- **Duration:** Sets the duration for which an account remains locked after the maximum number of attempts is reached (Default: 30 minutes; Range: 0–60 minutes).



Note: You have three (3) attempts to enter the correct password within a 15-minute period. If all three (3) attempts are unsuccessful, your account temporarily locks for 30 minutes to protect your security. You cannot attempt to log in during the lockout period. The system displays the message: “Account locked due to too many failed attempts. Please try again later.”, including the time the lockout expires. Your account

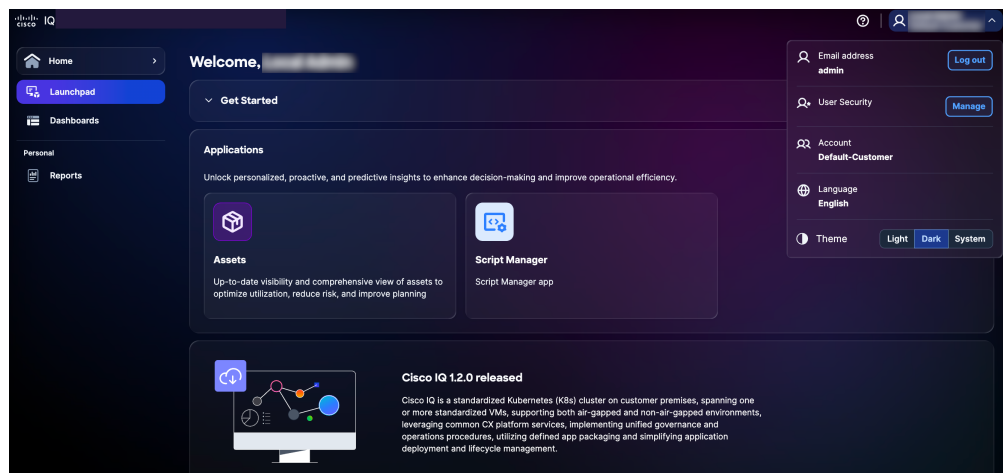
 automatically unlocks after 30 minutes, at which point you may attempt to log in or reset your password.

Setting Up Security Questions and Answers

Security questions help verify your identity if you forget your password. Account Administrators must set up answers to five (5) security questions to enable the password reset feature. This is a one-time setup.

To set up security questions:

1. From **Home** page, click your **User Profile** icon. The dropdown menu opens.



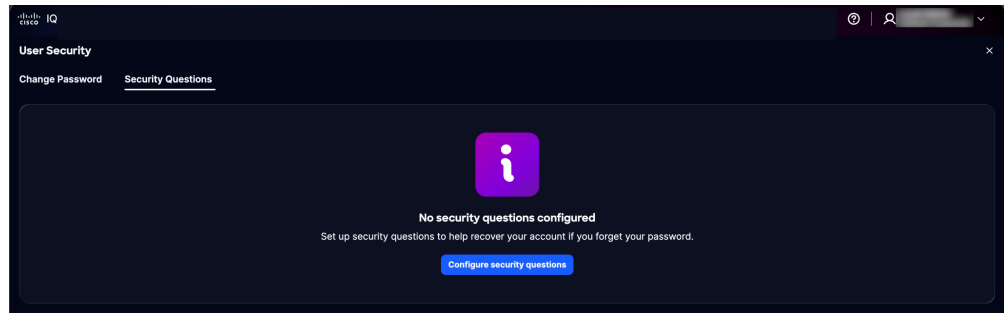
Use Security

2. Click **Manage** in User security. The **User Security** page displays.



Security Questions

3. Click **Security Questions** to open the tab.



Security Questions Tab

4. Click **Configure security questions**.

A screenshot of the Cisco IQ User Security interface, specifically the 'Security Questions' tab. The page title is 'User Security' with sub-tabs 'Change Password' and 'Security Questions'. The 'Security Questions' tab is active, showing a heading 'Security Questions' and a sub-heading 'Set up security questions to help recover your account if you forget your password. You must answer all questions.' Below this, there are five questions to configure. Each question consists of a dropdown menu labeled 'Select a security question' and a text input field labeled 'Answer *'. The questions are labeled 'Question 1 *', 'Question 2 *', 'Question 3 *', 'Question 4 *', and 'Question 5 *'.

Configure Security Questions

5. Choose any five (5) security questions from the drop-down lists.
6. Enter your response for each question.
7. Click **Save**.



Note: Answers are not case-sensitive, for example, “SMITH” and “smith” are considered the same. Extra spaces are ignored, meaning “ Smith “ and “Smith” are treated identically. Remember how you entered your answer (for example, full names versus nicknames). Use straightforward answers you will remember years later. Pick questions with answers that will not change over time.



Note: You can update your answers later if needed. When you update your answers, all previous answers are replaced, so you must provide answers to all five (5) questions again and not just the ones you want to change.

Managing Passwords

Account Administrators and local users can manage the password for Cisco IQ.

To ensure the security of your account, the following password policies are enforced:

- **Reuse Restriction:** Your new password cannot match any of your previous five (5) passwords. This policy applies to Sign-up, Forgot Password, and Change Password flows.
- **Character Variation:** When changing your password while authenticated, at least eight (8) characters from your current password must be different in your new password.
- **Minimum Change Interval:** By default, you must wait 24 hours before changing your password again. If a different interval is configured, you will be unable to update your password until that time has elapsed.
- **Password Expiration:** Passwords expire every 60 days. Upon your first login following the expiration date, you will be required to set a new password before you can access the system (if configured to 0, password expiration is disabled.)

Prerequisites

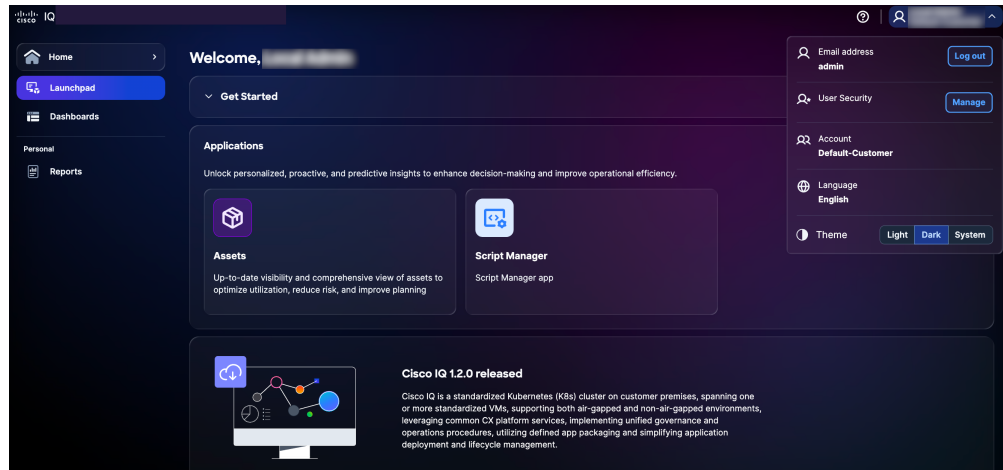
To manage passwords, the following conditions must be met:

- You are a local Account Administrator or user
- You are using a local account (not Single Sign-On (SSO) or external authentication)
- You are logged in to Cisco IQ
- You know the current password

Changing Passwords

To change the password:

1. From **Home page**, click your **User Profile** icon. The drop-down menu opens.



Manage User Security

2. Click **Manage** in User security. The **User Security** page displays.



Change Password

3. Enter the current **Password**.
4. Enter the **New password**.
5. Enter the new password again to confirm.
6. Click **Save**.

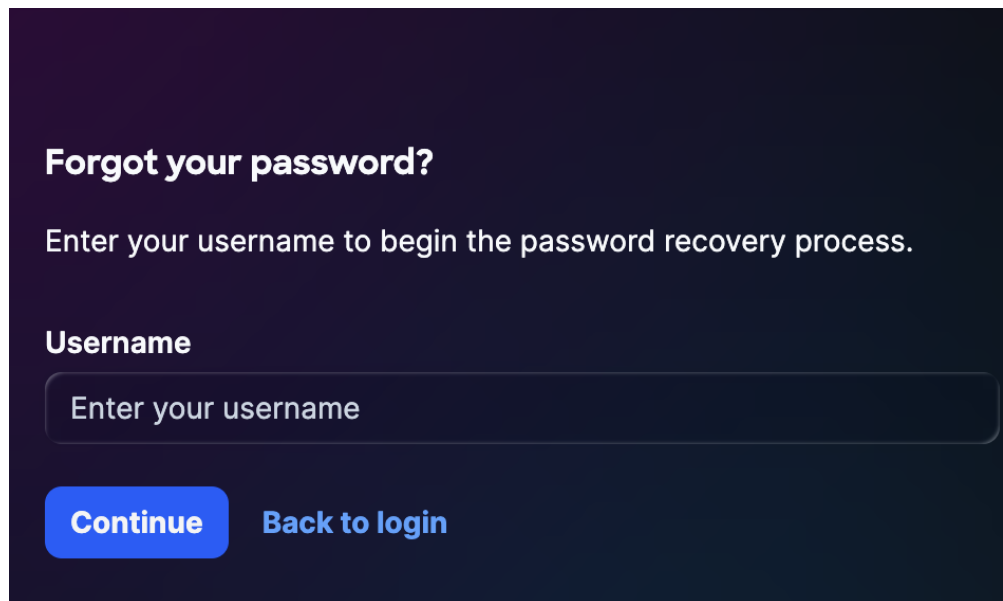
The password is updated in the Cisco IQ system, including the Cisco IQ VM.

Resetting a Forgotten Password

You can reset a password using the security question verification process.

To reset a forgotten password:

1. Navigate to the Cisco IQ VA login page.
2. Click **Forgot Password**.



Forgot your password?

Enter your username to begin the password recovery process.

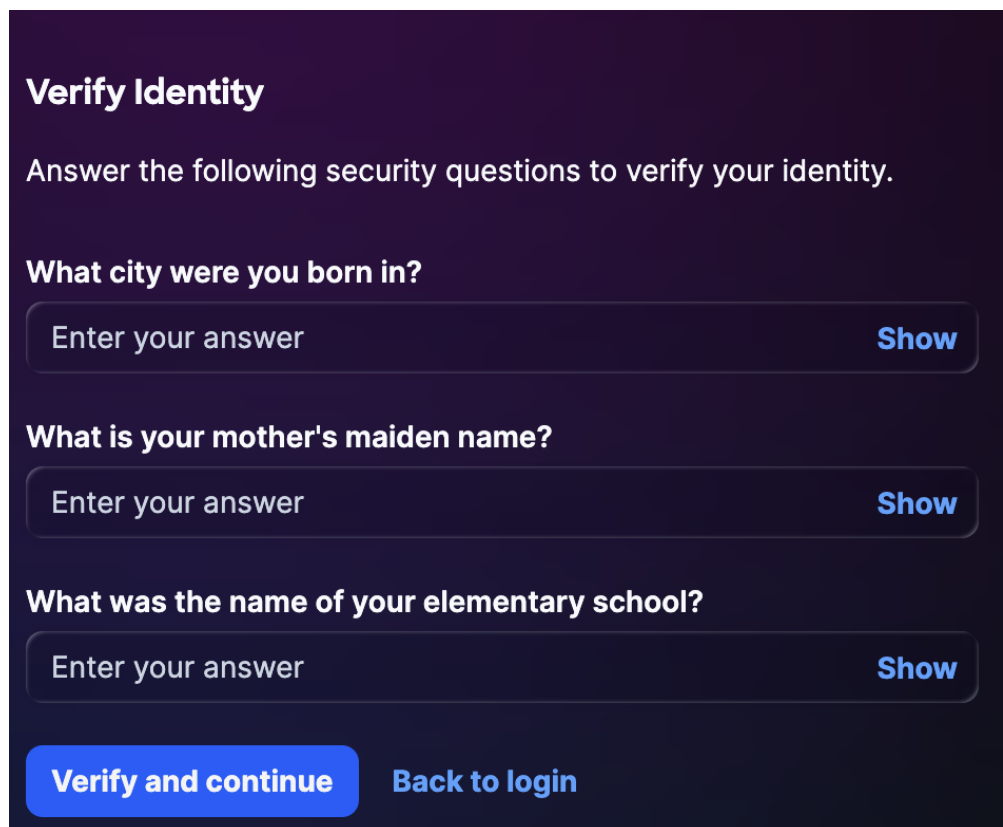
Username

Enter your username

Continue [Back to login](#)

Forgot Password

3. Enter the **Username**.
4. Click **Continue**. The **Verify Identity** page displays three (3) random security questions out of the five (5) questions that were previously configured.



Verify Identity

Answer the following security questions to verify your identity.

What city were you born in?

Enter your answer [Show](#)

What is your mother's maiden name?

Enter your answer [Show](#)

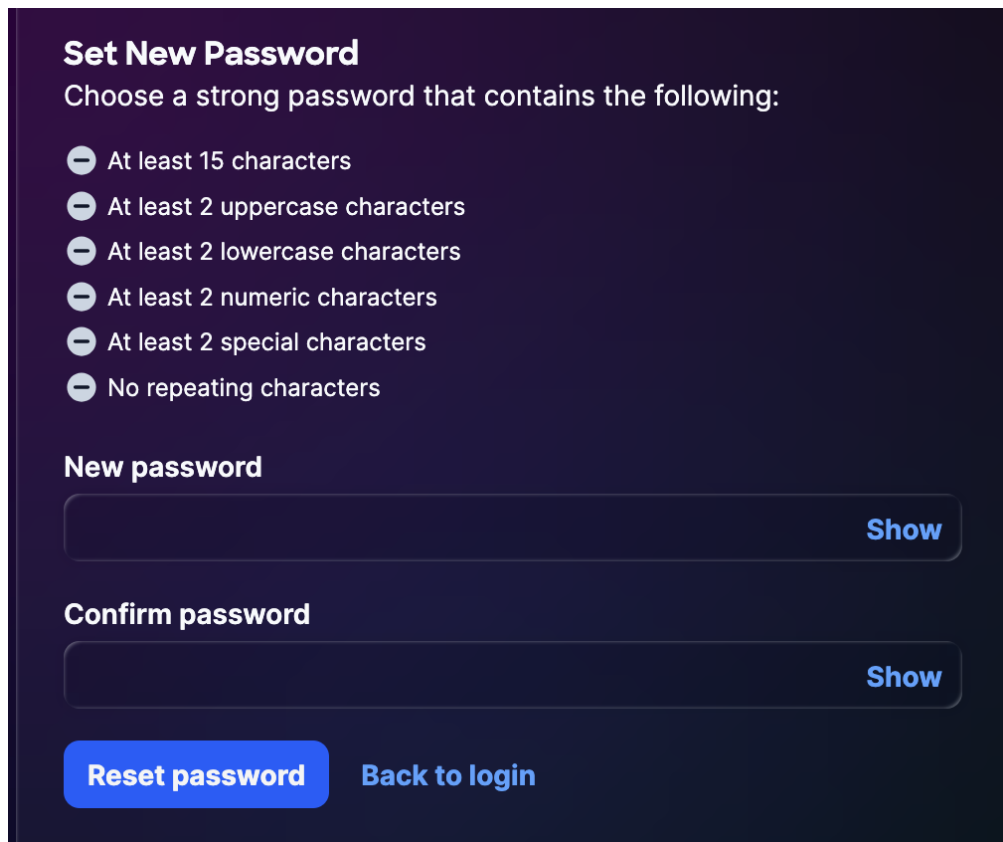
What was the name of your elementary school?

Enter your answer [Show](#)

Verify and continue [Back to login](#)

Verify Identity

5. Enter the responses for all three (3) displayed questions.
6. Click **Verify and continue**. If the submitted response matches your previously saved responses, you are prompted to enter a new password.



Reset Password

 **Note:** You have three (3) attempts to enter the correct password within a 15-minute period. If all three (3) attempts are unsuccessful, your account temporarily locks for 30 minutes to protect your security. You cannot attempt to log in during the lockout period. The system displays the message: “Account locked due to too many failed attempts. Please try again later.”, including the time the lockout expires. Your account automatically unlocks after 30 minutes, at which point you may attempt to log in or reset your password.

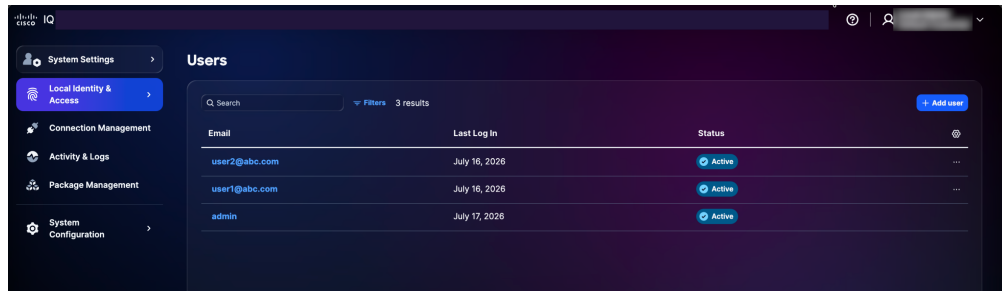
7. Enter the new password.
8. Enter the password again to confirm.
9. Click **Submit**.

Adding Local Users

Account Administrators can add users to the Cisco IQ account. To add a new user:

1. Navigate to **System Settings > Local Identity & Access > Users**. The

Users page displays. It lists all existing local users along with their status.

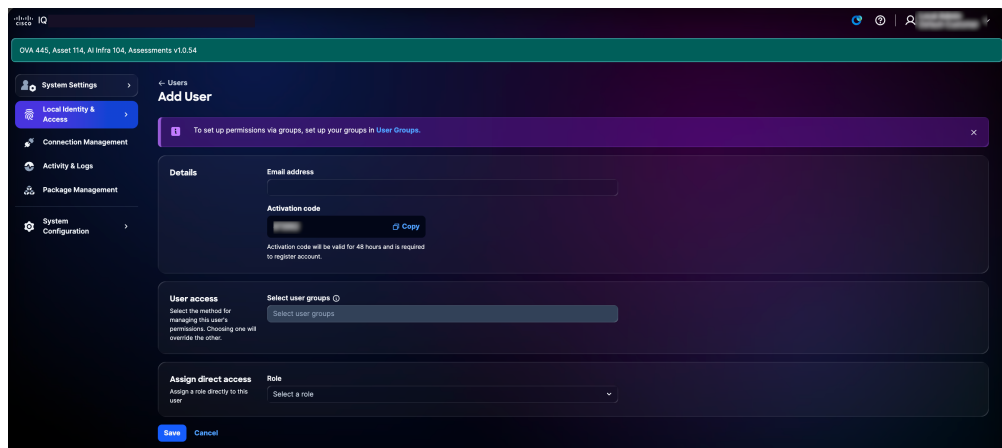


Users Page



Note: Do not share the activation code over insecure channels. If the code is lost or compromised, use the Menu icon to regenerate a new activation code, which invalidates the previous one. Activation codes are valid for 48 hours. If your code expires, please contact your Account Administrator to request a new one.

- Click **Add users**. The **Add User** page displays.



Add User

3. Enter the **Email address**.

4. Enter **Activation code**.



Note: The activation code is displayed by default. Share the displayed activation code with the user, as it is required for registration.

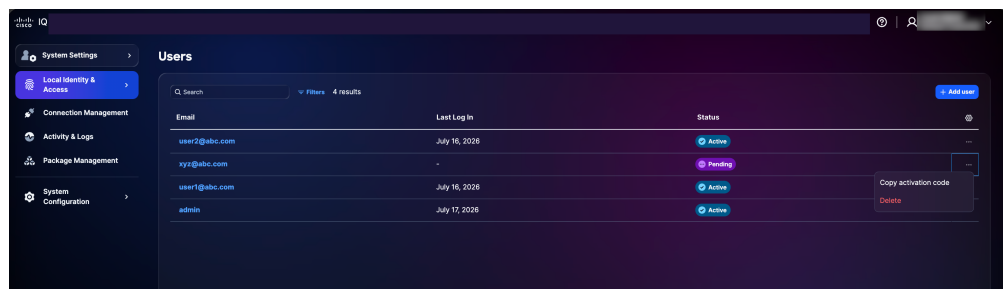
5. In **User access**, choose the user group from the **Select user groups** drop-down list.



Note: Users inherit access from the selected group.

6. In **Assign direct access**, choose role from the **Role** drop-down list. There are two (2) roles available:

- **Viewer:** View and access applications
 - **Account Administrator:** Access modules and manage system settings except System Management and Identity Provider (IDP)
7. Click **Save**. The new user is created and displays in the user list in **Pending** state. Pending indicates the user has not yet completed self-activation.
 8. Locate the newly created user in the list and confirm that the **Status** column displays **Pending**.
 9. Click the **More Options** Icon next to the newly created user.



Copy Activation Code

10. Select the **Copy activation code** from the drop-down list. The activation code is copied to your clipboard.
11. Share this code with the user securely (for example, via a secure internal channel). The activation code is for one-time use and is required to complete registration.

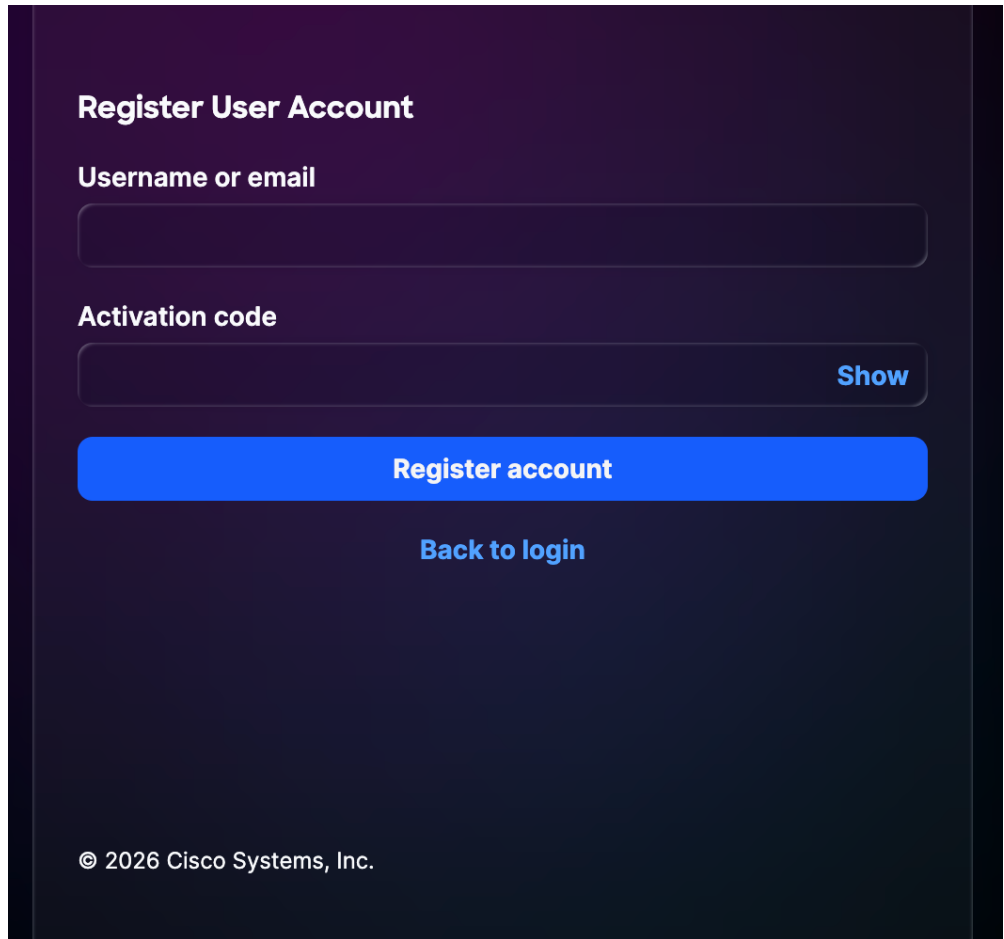
 **Note:** Do not share the activation code over insecure channels. If the code is lost or compromised, use the **Menu** icon to regenerate a new activation code, which invalidates the previous one. Activation codes are valid for 48 hours. If your code expires, please contact your Account Administrator to request a new one.

12. To logout, click the **User Profile** icon in the top-right corner and select **Logout**. You are returned to the **Cisco IQ** login page.

Registering New User Accounts

To register the new user account:

1. On the login page, click the **Register a new user account** link.

A screenshot of a 'Register User Account' form. The form is set against a dark purple background. It features two input fields: 'Username or email' and 'Activation code'. The 'Activation code' field has a 'Show' button to its right. Below the input fields is a prominent blue button labeled 'Register account'. Underneath this button is a link that says 'Back to login'. At the bottom left of the form, there is a copyright notice: '© 2026 Cisco Systems, Inc.'

Register User Account

Username or email

Activation code [Show](#)

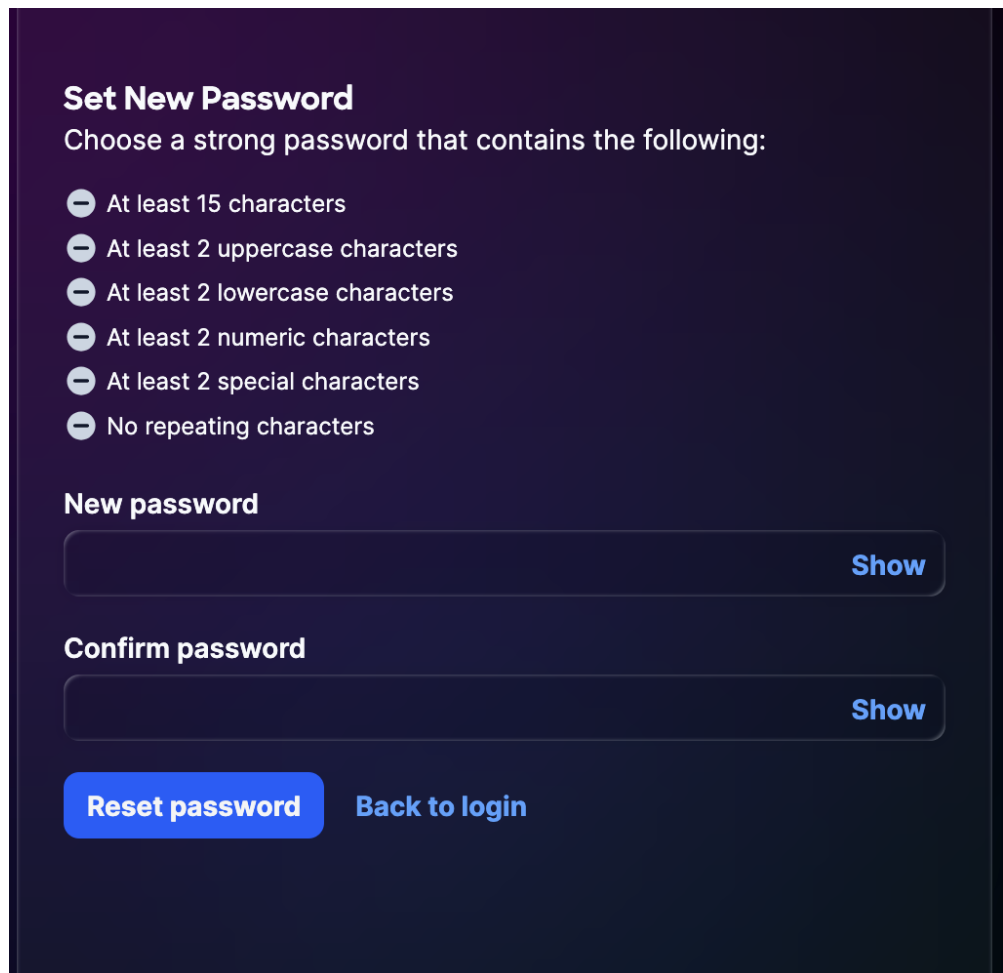
Register account

[Back to login](#)

© 2026 Cisco Systems, Inc.

New User Account

2. Enter the **Username or email address** used when the user was created (for example, user1@abc.com)
3. Enter the **Activation Code** shared by the Account Administrator.
4. Click **Register account**. The **Set New Password** window displays.



Set New Password

Choose a strong password that contains the following:

- At least 15 characters
- At least 2 uppercase characters
- At least 2 lowercase characters
- At least 2 numeric characters
- At least 2 special characters
- No repeating characters

New password

Confirm password

Reset password **Back to login**

New User Account Password

5. Enter a New password.
6. Enter the password again in **Confirm password**.
7. On the first successful login, the user is prompted to configure five (5) security questions. (See [Setting Up Security Questions](#)).

Managing Local User Groups

User groups enable the Account Administrator to manage roles for multiple local users at once. Instead of assigning a role to each user individually, you can create a group, attach a role and set of users to it, and update the role or membership in one place. All user group management is performed from the **Local Identity & Access** page.

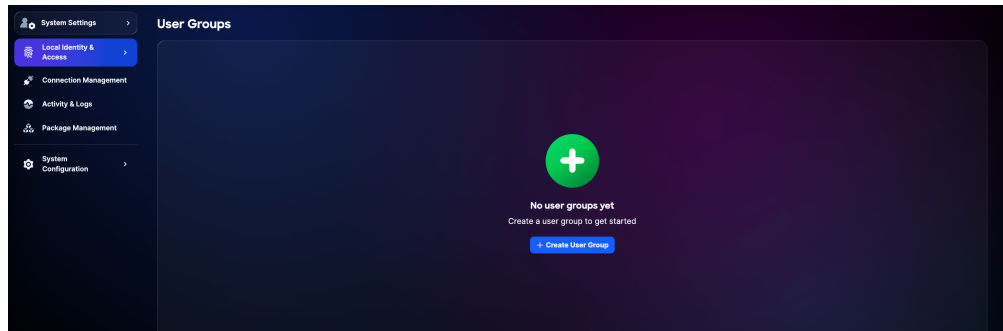


Note: Only an Account Administrator can create, edit, or delete user groups. Groups are made up of existing local users; users must be created before they can be added to a group. Refer to [Adding Local Users](#) for more information.

Creating a User Group

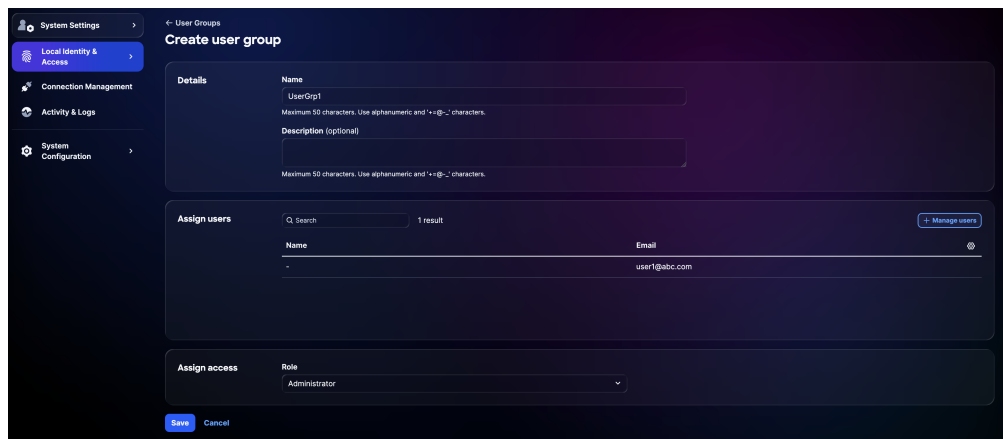
To create a user group:

1. From **System Settings**, choose **Local Identity & Access > User Groups**. The **User Groups** page displays.



User Groups

2. Click **Create User Group**. The **Create user group** page displays.



Create User Group

3. Complete the following sections:
 - **Details**
 - **Name:** Enter a unique name for the group (for example, Read-Only Operators)
 - **Description (Optional):** A brief description of the group (maximum 50 characters; alphanumeric and + = @ - _ characters are allowed)
 - **Assign Users:** Search for and select one or more existing local users to add to the group. *Note: To add users who are not yet listed, click **Manage users**.*
 - **Assign access**
 - **Role:** Select the system role to assign to all members of this group. The following roles are available:
 - **Viewer:** View and access modules (read-only)
 - **Administrator:** Access modules and manage system settings

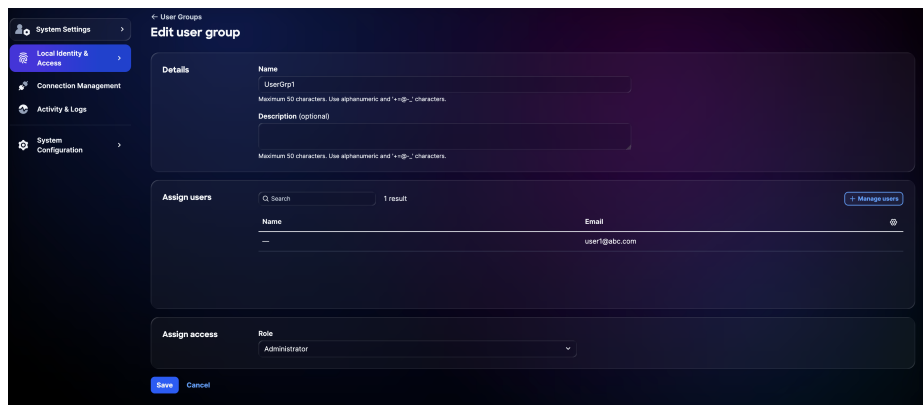
4. Click **Save**.

The new user group displays in the **User Groups** list along with its assigned role and member count.

Editing a User Group

To edit a user group:

1. From the **User Groups** list, locate the group you want to modify.
2. Choose the **More Options** icon > **Edit** of the desired group. The **Edit user group** page displays.



Edit User Group

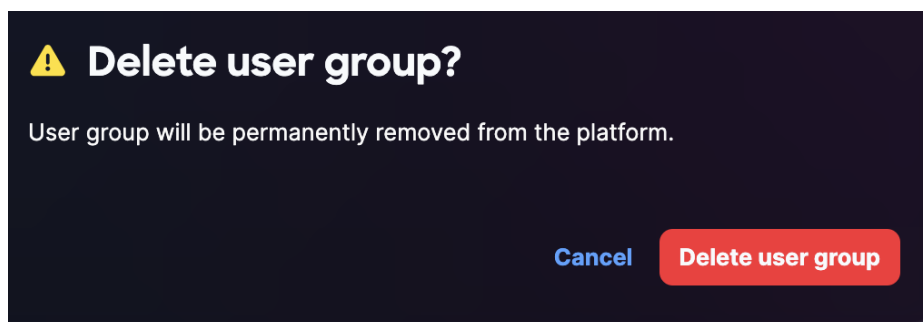
3. Make the desired changes.
4. Click **Save**.

The updated group displays in the **User Groups** list. The new role takes effect for all members of the group.

Deleting a User Group

To delete a user group:

1. From the **User Groups** list, locate the group you want to delete.
2. Click the **More Options** icon next to the group and select **Delete**.



Delete User Group

3. Confirm the deletion when prompted.

The group is removed from the **User Groups** list.



Note: Deleting a user group removes the group-based role assignment from all members. The individual user accounts are not deleted.

Configuring Identity Provider

Once logged in to VA, Account Administrators can configure various settings. Account Administrators can log in using local administration or IDP configuration.

Okta IDP SAML Configuration for SSO

Prerequisites to Configure IDP SAML

- Local Administrator access to Cisco IQ
- Access to IDP portal

IDP SAML Configuration for SSO

To configure IDP Security Assertion Markup Language (SAML) for SSO:

1. Navigate to your IDP portal.

Table 2: Cisco IQ Attributes

Field	Value
Application Name	<Application Name>
Environment	ESP business application
Application Owner Groups	Owner of the IDP settings
Team Mailer	Mailer for the team
Audience	Non-workforce
Onboarding Category	Select “New Onboarding”

Table 3: SAML Configuration Parameters

Parameter	Configuration	Example
Audience (Entity ID)	Fully Qualified Domain Name (FQDN)	mymanagementhost.mydomain.com
	SAML Assertion Customer Service (ACS)	https://mymanagementhost.mydomain.com/saml/acs
	Single Sign-On URL	

Parameter Configuration Example

endpoint	
Name ID Format	Email address NA
Application Username	Username NA

5. Configure the attribute statements.



Note: IDP attribute changes depend on the specific provider and configuration. Cisco IDP and its attributes are shared below as an example.

- First Entry
 - **Name:** Username
 - **Value:** user.login
- Second Entry
 - **Name:** Primary email
 - **Value:** user.email
- Group Attribute Statements
 - **Name:** groups
 - **Filter:** REGEX
 - **Value:** .*

6. Configure the **Single Logout (SLO)** settings in the application.

Table 4: SLO Configuration Settings

Field	Value
Signature Certificate	For Okta, this certificate is required only if you choose to enable SLO. Download the Signature Certificate using the Download SP Certificate in Identity Providers . Save the file as <i>sp-public-key.crt</i> . See Single Logout Configuration for more details.
SP metadata	The Service Provider (SP) metadata is required for ADFS IDP only (and not for Okta).
Do you want to enable Single Logout	Yes or No
Single Logout URL	https://mymanagementhost.mydomain.com/saml/logout
SP Issuer (Audience/Entity ID or ACS URL)	https://mymanagementhost.mydomain.com

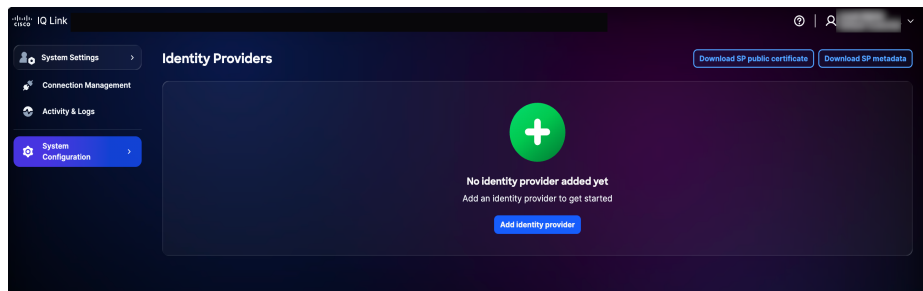
8. Click the **Download** icon to download the “IDP Metadata XML” file.

9. Provision or create the application as required by the provider.

Adding Okta IDP

To add an IDP in Cisco IQ:

1. From **System Settings**, choose **System Configuration** > **Identity Providers**. The **Identity Providers** page displays.



IDP Home Page



Note: Only one (1) IDP can be added at a given time.

2. Click **Add Identity Provider**. The **Add Identity Provider** page displays.

A screenshot of the 'Add Identity Provider' page in the Cisco IQ Link interface. The left sidebar is the same as the previous screenshot. The main content area has a title 'Add Identity Provider' and a back arrow. It contains three main sections: 1. 'Identity provider name' with a text input field and a placeholder 'Enter identity provider name'. 2. 'Domains' with a text input field 'Enter domain names' and a blue 'Add' button. 3. 'Organization IDP metadata' with a dashed border box containing an upload icon and the text 'Select or drag file to this area to upload' and 'Only one file can be uploaded at 5 MB or less'. At the bottom, there is a toggle switch for 'Enable single log out (SLO)' and two buttons: 'Save' and 'Cancel'.

Add Identity Provider

3. Enter the Identity provider name.
4. Click **Add** to add a Cisco IQ configured domain name to the

Domain(s) field.

5. Drag-and-drop or upload the SAML metadata file obtained from the IDP application in the **Organization IDP metadata** field. This file contains certificate details and SP entity details.
6. (Optionally) turn on the **Enable single logout** toggle button. You can enable the SLO later as well.
7. Click **Save**.

Role Mapping Configuration

1. From the added IDP, choose the **More Options** icon > **Map Roles**. The **Map user roles** page displays.

Map identity provider roles to system roles to assign permissions.

Map User Roles

IDP Role	System Role
iq-demo-user	General Account...

+ Add identity provider role

Save

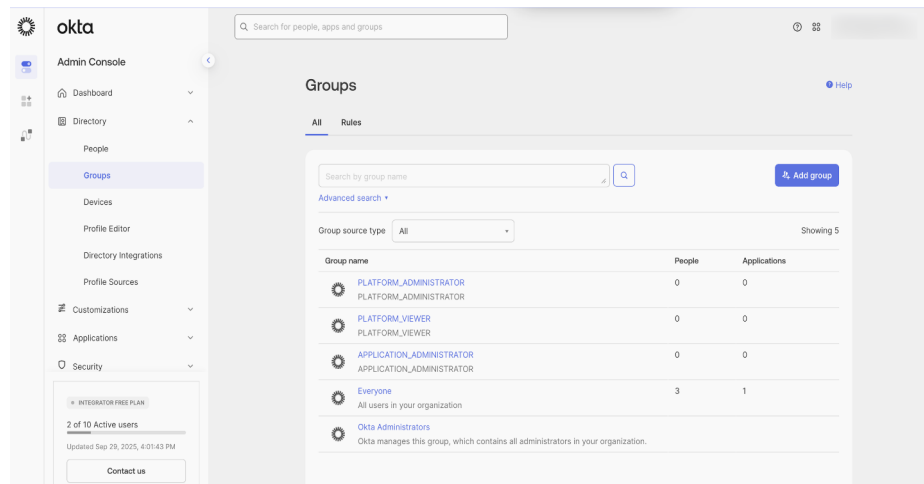
Map User Roles

2. Enter an **IDP role** for the selected **System role**. The following system roles are supported:

- **General Account Administrator:** The General Account Administrator has full permissions to perform all the actions in the product
- **General Account Viewer:** The General Account Viewer has read only access

 **Note:** The **IDP role** is an open-text field. It must match exactly with the group or role name configured in your

 organization's IDP. An example of Okta groups is shared below.



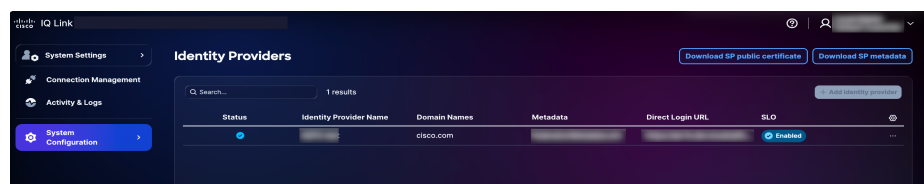
Role Mapping Reference

3. Map additional roles as required by clicking **Add identity provider role**.
4. Click **Save**. Once configured, the login page displays an option to log in with SSO (via IDP).

Single Logout Configuration

If you choose to enable SLO, you must upload metadata that includes the SLO URL. You can configure this by editing your Identity Provider settings and turning the toggle on for **Enable Single Log Out**. To complete SLO configuration:

1. From the Identity Providers home page, click **Download SP public certificate**.



SP Public Certificate

2. Save the downloaded file as *sp-public-key.crt*.
3. Navigate to your IDP portal.
4. Upload the signature certificate file generated in [IDP SAML Configuration for SSO](#).
5. Enter the SLO URL (for example, <https://ciq-xxx-xxx-37-160.cx-hub-rtp.cisco.com/saml/logout>).

6. Enter the SP issuer (for example, ciq-xxx-xxx-37-160.cx-hub-rtt.cisco.com).
7. Click **Submit**.
8. Download the IDP metadata file again.
9. On the **Identity Providers** page, choose the added IDP's **More Options** icon > **Edit**.
10. Turn on the **Enable single log out (SLO)** toggle button.
11. Upload the newly downloaded metadata file.
12. Use the following checklist to verify SSO and SLO functionality:

Verification Checklist:

- Local administrator login is successful
- IDP portal is configured and provisioned
- IDP is added to Cisco IQ with a "Success" status
- Role mappings are configured and tested
- SP metadata is downloaded and the certificate is extracted
- If SLO is enabled, SLO configuration is complete with the real signature certificate
- End-to-end SSO and SLO flow is tested successfully

Troubleshooting IDP Issues

The following tables lists common issues and possible solutions to help quickly identify and resolve problems related to IDP status, certificate errors, SSO login failures, and SLO configuration:

Table 5: Troubleshooting

Issue	Solution
IDP status shows as "Incomplete"	Verify the role mapping configurations
Certificate errors	Verify certificate format and validity
SSO login failures	Validate attribute mapping and group assignments
SLO not working as expected	Ensure the certificate is properly uploaded and SLO URLs are configured

ADFS IDP SAML Configuration for SSO

This section provides guidance to configure Microsoft Active Directory (AD) Federation Services (FS) as the SAML IDP for Cisco IQ, supporting password-based and Public Key Infrastructure (PKI) or certificate-based authentication.

Prerequisites to Configure ADFS IDP SAML for SSO

- ADFS 6.0+ is recommended
- Windows Server 2016 + (recommended 2019)
- Configured AD integration with user accounts
- SSL/TLS certificates on ADFS server
- Administrator access to Cisco IQ
- Administrative access to ADFS server (Windows Server)
- PowerShell access on ADFS server
- Network connectivity between ADFS and Cisco IQ
- Enterprise Certificate Authority (CA) (installed or reachable)
- Domain Administrator or Enterprise Administrator privileges (required for PKI only)
- ADFS server configuration details (as listed in the table below)

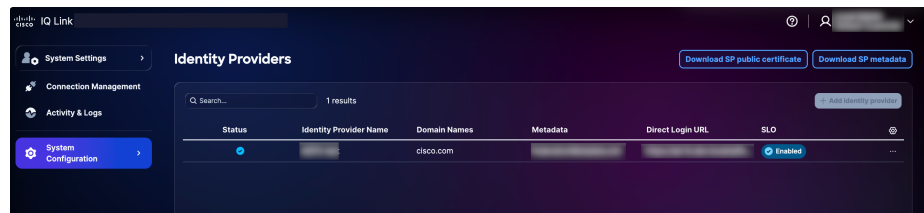
Table 6: Authentication Flow Overview

Item	Description	Example
Cisco IQ FQDN	User deployment hostname	<Your-CIQ-FQDN> For example, dev35-23.cx-xxx-xxx.cisco.com
ADFS Server URL	User ADFS server address	https://<Your-ADFS-HOSTNAME> For example, https://adfs.dev.local
Company Domain	Email domain	<Your-Domain> CN=Role - CXIQ
AD Groups	Active Directory group Domain Names (DN)	Developers OU=Groups, DC=dev, DC=local
CA Name (PKI)	Enterprise CA name	<Your-CA-Name>
Cert Auth Port (PKI)	ADFS alternate TLS port	49443
SSL Certificate Thumbprint	ADFS server SSL certificate	<Your-SSL-CERT-THUMBPRINT>

Configuring Base ADFS SAML

To configure ADFS:

1. From **System Settings**, choose **System Configuration > Identity Providers**. The **Identity Providers** page displays.



Download Options

2. Click **Download SP public certificate** and **Download SP metadata** to download these files.
3. Copy and save the *service-provider-metadata.xml* and *service-provider-certificate.crt* files to the ADFS server (for example, C:\).
4. Log in to the ADFS server.
5. From the **ADFS Management** menu, click **Relying Party Trusts**.
6. From the **Relying Party Trusts** menu, click **Add Relying Party Trusts**. The new wizard opens.
7. Click the **Claims Aware** radio button.
8. Click **Start** to proceed with the configuration.
9. Click **Import data about the relying party from a file** to get details from the file which is saved as part of step 3.
10. Click **Browse** to select the service provider metadata file and complete the file upload.
11. Click **Next**.
12. Enter a display name (for example, “Cisco IQ”), add any relevant notes, and click **Next**.
13. On the **Choose Access Control Policy** page, click **Permit everyone** (or the policy required by your organization’s security configuration).
14. Click **Next** through the remaining screens.
15. Click **Close** to complete the Relying Party Trust configuration.



Note: Do not select “Permit Everyone with MFA” unless your ADFS server has a registered Multi-Factor Authentication (MFA) adapter (for example, Azure MFA, *Time-Based One-*

 Time Password (TOTP)) configured.

If this policy is enabled without a configured MFA provider, ADFS authenticates the user but ultimately denies the request with status `urn:oasis:names:tc:SAML:2.0:status:RequestDenied`. Since the SAML response contains no assertion, the plugin fails and reports a “missing email” error.

Issue: “Permit Everyone with MFA” is selected.

Workaround: In PowerShell, check current policy by running the following command.

```
Get-AdfsRelyingPartyTrust -Name
"<YOUR-RP-NAME>").AccessControlPolicyName
To set “Permit everyone” (no MFA requirement), run the following command:
Set-AdfsRelyingPartyTrust -TargetName "<YOUR-RP-NAME>"
-AccessControlPolicyName "Permit everyone"
You can also create the trust through PowerShell:
-Add-AdfsRelyingPartyTrust `
=Name "<YOUR-RP-NAME>" `
-Identifier "<YOUR-SP-ENTITY-ID>" `
-SamlEndpoint (New-AdfsSamlEndpoint -Binding POST -Protocol
SAMLAssertionConsumer -Uri "<YOUR-ACS-URL>") `
-AccessControlPolicyName "Permit everyone" `
-IssuanceAuthorizationRules '=> issue(Type =
"http://schemas.microsoft.com/authorization/claims/permit", Value =
"true");
```

Configuring ADFS Claim Rules

To configure ADFS Claim rules, perform the steps listed in the following sections.

Required Claims

Refer to the following table for required claims.

Table 7: Required Claims

Claim	Purpose	Source
Email	User identifier	AD Mail
Display Name	User’s full name	AD Display Name
UPN	PKI/certificate authentication	ADFS maps the client certificate to an AD user via UPN
NameID	SAML subject	Transformed from email
Groups	Role-based access	AD Group Membership (memberOf)

Applying Claim Rules

1. Define the name of your **Relying Party Trust** (for example, “Cisco IQ - Production”).

```
$relyingPartyName = "Your-RP-Name"
```

2. Define claim rules to send user information and group membership to Cisco IQ.

```
$claimRules = @'
@RuleTemplate = "LdapClaims"
@RuleName = "Send Email and Name"
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsa
=> issue(store = "Active Directory", types = ("http://schemas.xmlsoap.org/ws
@RuleTemplate = "LdapClaims"
@RuleName = "Send UPN"
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsa
=> issue(store = "Active Directory",
types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"),
query = ";userPrincipalName;{0}", param = c.Value);
@RuleName = "Transform Email to NameID"
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddre
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/namei
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, Value
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/t
@RuleName = "Send Group Membership"
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsa
=> issue(store = "Active Directory",
types = ("http://schemas.xmlsoap.org/claims/Group"),
query = ";memberOf;{0}", param = c.Value);
'@
```

3. Apply the claim rules by running the following command:

```
Set-AdfsRelyingPartyTrust -TargetName $relyingPartyName
-IssuanceTransformRules $claimRules
```

```
Write-Host "Claim rules configured successfully!" -ForegroundColor
Green
```

Warning: Each AD user account must have the mail attribute populated. If this attribute is missing, the SAML assertion does not contain an email claim, resulting in an authentication rejection.

To update a user's email address, execute the following PowerShell command:

```
Set-ADUser -Identity "<USERNAME>" -EmailAddress  
"<USER-EMAIL>"
```

Verifying User Groups

1. Set the username to check user's group membership by running the following command:

```
$username = "username"
```

2. Run the following commands to find the user's account:

```
$searcher = [adsisearcher]"(samaccountname=$username)"  
$user = $searcher.FindOne()
```

3. Display the groups the user belongs to using the following command:

```
$user.Properties.memberof
```

Example Output:

```
CN=Role - CXIQ Developers,OU=Role Groups,DC=dev,DC=local
```

Configuring ADFS to Trust the SP Signing Certificate

1. In the ADFS server, import the SP certificate into the TrustedPeople store:

```
Import-Certificate -FilePath "C:-provider-certificate.crt"  
-CertStoreLocation "Cert:"
```

2. Choose one of the following options:



Note: The SP certificate is issued by an internal CA that ADFS cannot validate through the standard chain-of-trust.

- Disable chain validation globally for this relying party

```
Set-AdfsRelyingPartyTrust `   
-TargetIdentifier "<Your_sp_entity_id>" `   
-SigningCertificateRevocationCheck None `   
-EncryptionCertificateRevocationCheck None
```

- If the SP certificate is issued by a CA (not self-signed), import the issuing CA certificate into the Root certificate store

```
Import-Certificate -FilePath "C:-ca.cer" -CertStoreLocation
"Cert:"
```

3. Apply the changes by restarting the ADFS service.

```
Restart-Service adfssrv
```

Setting Up PKI/Certificate Authentication

This section describes how to add certificate-based (that is, smart card or software certificate) authentication alongside passwords. This section can be skipped if password-only authentication is sufficient.

Installing the AD CS CA Role

To install the AD Certificate Services (CS) CA role:

1. Verify if an Enterprise CA already exists in your domain by running the following command:

```
certutil -config - -ping
```

If the command returns a valid response, you can skip the remainder of this section. Your environment is already configured. If the command indicates no CA is found, proceed to step 2.

2. Install the CA role by running the following command:

```
install-WindowsFeature AD-Certificate -IncludeManagementTools
```

3. Configure the CA role by running the following command:

```
install-AdcsCertificationAuthority `
-CAType EnterpriseRootCA `
-CACommonName "
" `
-KeyLength 2048 `
-HashAlgorithmName SHA256 `
-CryptoProviderName "RSA#Microsoft Software Key Storage Provider" `
-ValidityPeriod Years `
-ValidityPeriodUnits 10 `
-Force
```

4. Verify the installation by running the following command:

```
certutil -ca
```

5. Confirm the service is active and reachable by running the following command:

```
certutil -config - -ping
```

Configuring a Certificate Template

To configure a certificate template with the Client Authentication Enhanced Key Usage (EKU):

1. Open *certsrv.msc* and expand the CA node.
2. Right-click **Certificate Templates > Manage**.
3. Duplicate the User template.



Note: The built-in User template is functional or valid only if the certificate issued from it includes Client Authentication EKU.

4. Configure the settings on the following tabs:

- **General:** Enter “CIQ User Authentication” in the **Name** field with a validity period of one (1) year
- **Request Handling:** Select **Signature and encryption** from the **Purpose** drop-down list and check the **Allow private key to be exported** check box
- **Subject Name:** Select **Build from Active Directory Information** and include an e-mail in both the **Subject** and **SAN** fields

Warning: The **Subject** and **SAN** fields must contain a user’s User Principal Name (UPN) or an email that matches an AD account. ADFS maps the certificate to an AD user using these fields.

- **Extensions:** Ensure the **Application Policies** include “Client Authentication (1.3.6.1.5.5.7.3.2)”
- **Security:** Add domain users and grant them **Read** and **Enroll** permissions

5. Publish the template using the following command:

```
Add-CATemplate -Name "CIQUserAuthentication" -Force
```

Enrolling a User Certificate

1. Log in as the target user.
2. Enroll the certificate by running the following command:

```
certreq -enroll -user "CIQUserAuthentication"
```

3. Verify the certificate installation by running the following command:

```
Get-ChildItem Cert:| Where-Object {  
    $_.EnhancedKeyUsageList.ObjectId -contains "1.3.6.1.5.5.7.3.2"} | Form
```

Exporting a User Certificate from Windows and Installing on Client (Mac)

To export a user certificate from Windows to Mac:

1. Export the certificate from Windows as a PFX file by running the following commands:

```
$cert = Get-ChildItem Cert:| Where-Object { $_.Subject -like "*" }
```

```
*" }
```

```
$password = ConvertTo-SecureString -String "
```

```
" -Force -AsPlainText
```

```
Export-PfxCertificate -Cert $cert -FilePath "C:-cert.pfx" -Password $p
```

2. Transfer the *user-cert.pfx* file to your Mac device.

3. Import the certificate into the Mac Keychain by running the following command:

```
security import user-cert.pfx -k ~/Library/Keychains/login.keychain-db
```



Note: After importing the certificate, your browser must be closed and reopened for it to be recognized.

4. Trust the CA on Mac by running:

```
sudo security add-trusted-cert -d -r trustRoot \  
-k /Library/Keychains/System.keychain ca-certificate.cer
```

Enabling ADFS Certificate Authentication Endpoints

To enable ADFS certificate authentication endpoints:

1. Enable the required ADFS certificate endpoints by running the following commands:

```
Enable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/2005/cert  
Enable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/2005/certi  
Enable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/13/certifi  
Enable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/13/certifi
```

2. Verify that all endpoints are enabled by running the following command:

```
Get-AdfsEndpoint | Where-Object { $_.AddressPath -like "*cert*" } | Fo
```

Enabling Certificate Authentication as the Primary

To enable the certificate authentication as the primary:

1. Configure the primary authentication providers for intranet and extranet access using the following command:

```
Set-AdfsGlobalAuthenticationPolicy `\  
-PrimaryIntranetAuthenticationProvider @"CertificateAuthentication",  
-PrimaryExtranetAuthenticationProvider @"CertificateAuthentication",
```


2. Verify that both lists include CertificateAuthentication and FormsAuthentication using the following commands:

```
(Get-AdfsGlobalAuthenticationPolicy).PrimaryIntranetAuthenticationProv  
(Get-AdfsGlobalAuthenticationPolicy).PrimaryExtranetAuthenticationProv
```

3. Check the current TLS client port configuration using the following command:

```
Get-AdfsProperties | Select-Object HostName, HttpsPort, TlsClientPort
```

4. If the TlsClientPort is not 49443, update the port and restart the ADFS service using the following commands:

```
Set-AdfsProperties -TlsClientPort 49443  
Restart-Service adfssrv
```

SChannel/TLS Fixes (CRITICAL for PKI)

The steps in the following sections resolve CERT_E_UNTRUSTEDROOT (0x800B0109) errors which prevent certificate authentication from working.

Binding SSL Certificates on Port 49443

To bind SSL certificates on Port 49443:

1. Remove any existing SSL certificate binding(s) on port 49443 by using the following command:

```
>netsh http delete sslcert  
hostnameport=<YOUR-ADFS-HOSTNAME>:49443
```

2. Create a new binding with client certificate negotiation enabled by using the following command:

```
netsh http add sslcert hostnameport=
```

```
certname=CN=MyApp,OU=MyOrg,O=MyOrg,C=US:49443`  
certhash=
```

```
appid="{5d89a20c-beab-4389-9447-324788eb944a}"`  
certstorename=MY`  
clientcertnegotiation=enable`  
verifyclientcertrevocation=disable`
```

3. Verify that client certificate negotiation is enabled using the following command:

```
http show sslcert  
hostnameport=<YOUR-ADFS-HOSTNAME>:49443
```

Cleaning Up the Certificate Store (CRITICAL)

To clean up the certificate store:

Warning: Windows SChannel rejects all client certificates if non-self-signed certificates are present in the Trusted Root store. This is the main root cause of PKI failures.

1. Identify non-self-signed certificates in the Trusted Root store by running the following command:

```
$bad = Get-ChildItem Cert:| Where-Object { $_.Issuer -ne $_.Subject }  
$bad | ForEach-Object { Write-Host "PROBLEM: $($_.Subject) | Issuer: $_.Issuer"
```

2. Move these certificates to the intermediate CA store by running the following command:

```
$bad | Move-Item -Destination Cert:\IntermediateCA  
Write-Host "Moved $($bad.Count) cert(s) from Root to Intermediate CA store"
```

3. Verify that no non-self-signed certificates remain in the Trusted Root store by running the following command:

```
Get-ChildItem Cert:| Where-Object { $_.Issuer -ne $_.Subject }
```

SChannel Registry Fixes (CRITICAL)

To configure the SChannel registry settings to ensure proper certificate authentication:

1. Define the registry path variable using the following command:

```
$regPath = "HKLM:"
```

2. Apply the registry settings defined in the table below using the following commands:

```
Set-ItemProperty -Path $regPath -Name "ClientAuthTrustMode" -Value 2 -
Set-ItemProperty -Path $regPath -Name "SendTrustedIssuerList" -Value 0
```

Table 8: SChannel Registry Settings

Setting	Value	Purpose
ClientAuthTrustMode	2	Enables exclusive CA trust to correct the default validation path.
SendTrustedIssuerList	0	Prevents the server from sending the full trusted issuer list during the TLS handshake.

Verifying the CA Certificate Store

To verify the CA certificate store:



Note: The CA certificate that issues user certificates must be in the SystemCertificatesstore to ensure it is correctly recognized.

1. Define the thumbprint of your CA certificate using the following command:

```
$caThumbprint = "<YOUR-CA-CERT-THUMBPRINT>"
```

2. Verify the CA certificate is already present in the

*LocalMachinestore** using the following command:

```
$exists = Test-Path "HKLM:\caThumbprint"
```

If the certificate is not found, import it into the LocalMachine store:

```
if (-not $exists) {
    Import-Certificate -FilePath "C:\YOUR-CA-CERT>.cer" `
        -CertStoreLocation "Cert:"
}
```

Rebooting the ADFS Server (MANDATORY)

Restart the ADFS server by using the following command:

Restart-Computer -Force



 **Note:** The ClientAuthTrustMode registry change only takes effect after the server is restarted.

Exporting ADFS Metadata

You can download your ADFS metadata using either PowerShell or your web browser.

PowerShell

To export ADFS metadata using PowerShell:

1. Open PowerShell on your ADFS server.
2. Run the following commands to download the metadata file.

```
$metadataUrl = (Get-AdfsEndpoint | Where-Object {$_.Protocol -eq "FederationProtocol"}).MetadataUrl
Invoke-WebRequest -Uri $metadataUrl.AbsoluteUri -OutFile "C:-metadata.xml"
Write-Host "ADFS metadata exported to C:-metadata.xml" -ForegroundColor Green
```

After running the commands, the metadata file is saved to C:-metadata.xml.

Web Browser

To export ADFS metadata using a web browser:

1. Navigate to `https://<your-adfs-server>/FederationMetadata/2007-06/FederationMetadata.xml`, replacing “<your-adfs-server>” with the hostname of your ADFS server.
2. Save the metadata XML file to your computer when prompted.

Configuring on Cisco IQ

To configure on Cisco IQ:

1. Transfer *adfs-metadata.xml* to your workstation.
2. In Cisco IQ, navigate to System Settings > System Configuration > Identity Providers.
3. Upload the **ADFS metadata** file to automatically extract the IDP certificate, Entity ID, and SSO URL.
4. Save the configuration.



Note: If ADFS performs an automatic token-signing certificate rollover, you must re-export the metadata file and upload it to Cisco IQ to ensure continued authentication.

Adding ADFS IDP

1. On the **Identity Providers** page, click **Add identity provider**.
2. Enter the Identity provider name.
3. Enter the **Domain(s)** (for example, company.com).
4. (Optionally) turn on the **Enable single logout** toggle button, if required.
5. Drag-and-drop or upload the SAML metadata file obtained from the IDP application in the **Upload IDP Metadata** field.
6. Click **Save**.



Note: The status displays as “Incomplete” until role mapping is complete; this is expected behavior.

Configuring Role Mapping

Before proceeding to configure role mapping, ensure you can find groups from AD to use for mapping. To find groups from AD, run the following PowerShell command:

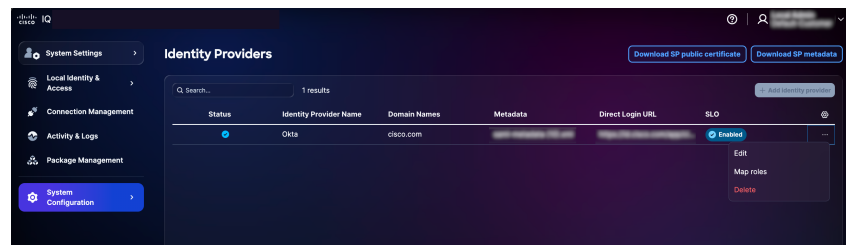
```
$searcher = New-Object DirectoryServices.DirectorySearcher
$searcher.Filter = "(&(objectClass=group)(cn=Role - CXIQ*))"
$searcher.PropertiesToLoad.Add("distinguishedName") | Out-Null
$searcher.PropertiesToLoad.Add("cn") | Out-Null
$searcher.FindAll() | ForEach-Object { $_.Properties["distinguishedName"]
```

The system queries AD directly via Lightweight Directory Access Protocol (LDAP), requiring no additional modules. Group information is returned in full Distinguished Name format, for example:

CN=Role - CXIQ Developers, OU=Groups, DC=dev,
DC=example, DC=com CN=Role - CXIQ Viewers,
OU=Groups, DC=dev, DC=example, DC=com

If the required groups are not listed, they must be created in AD by an Account Administrator before you can complete the ADFS role mapping.

To configure role mapping:



Role Mapping

1. From the added IDP, choose the **More Options** icon > **Map Roles**. The **Map user roles** page displays.

Cisco IQ Link_IDP

Map identity provider roles to system roles to assign permissions.

Map user roles

IDP role	System role
	General Account... ✕ ▼ 🗑️
	General Account... ✕ ▼ 🗑️
	Select option ▼ 🗑️
	Select option ▼ 🗑️
	Select option ▼ 🗑️

+ Add identity provider role

Save

Role Mapping

- Enter an **IDP role** for the selected System role. The following system roles are supported:
 - General Account Administrator:** The General Account Administrator has full permissions to perform all actions in the product. The IDP Role (parsed name) is CXIQ Admins.
 - General Account Viewer:** The General Account Viewer has read-only access. The IDP Role (parsed name) is CXIQ Developers and CXIQ Viewers.



Note: Use parsed names (for example, CXIQ Developers) and not full DNs.

- Click **Save**. The status updates to **Success**.

SChannel Client Cert Test

To verify that SChannel is correctly configured to accept client certificates, open a new PowerShell window and execute the

following command:

```
curl.exe -insecure `
-cert "CurrentUser\YOUR-USER-CERT-THUMBPRINT>" `
-v "https://

:49443/adfs/ls/"
```

The expected output is an HTTP response (for example, a redirect or the ADFS page). If a TLS handshake error occurs, the connection has failed.

End-to-End Browser Testing for PKI Flow

Before you begin end to end browser testing for PKI flow, ensure the user certificate is installed in MacOS Keychain (see [Importing the User Certificate on Client Machine \(MacOS\)](#)). To test:

1. Navigate to the application SAML login URL. The ADFS presents certificate and password options.
2. Choose **Certificate Authentication**. The browser prompts for certificate.
3. Upload the certificate. The ADFS authenticates the user, redirects the request with a SAML response, and establishes a new session.

End-to-End Browser Testing for Password Flow

Before you begin end-to-end browser testing for password flow:

1. Navigate to the application SAML login URL. The ADFS presents certificate and password options.
2. Select **Password/Forms Authentication**.
3. Enter **Username**.
4. Enter **Password**.
5. Verify for successful login.



Note: Both the flows must work simultaneously.

Troubleshooting ADFS Issues

The following list outlines common issues and possible solutions to help quickly identify and resolve problems related to ADFS status, certificate errors, SSO login failures, and SLO configuration.

Table 9: ADFS Issues

Issue	Symptoms / Description	Causes / Checks / Workarounds and Fixes
Groups Not Extracted	No roles after login	◦ Missing claim rule: Re-run the instructions in Configuring ADFS Claim Rules
Decryption Failed	“Failed to decrypt assertion” in logs	Check configuration on ADFS certificate configuration ◦ Invalid ACS URL: Verify: https://your-fqdn/saml/acs
Login Loop	Stuck in authentication or login loop	◦ Cookie mismatch: Check browser cookies for the correct domain

Diagnostics Commands to Troubleshoot

To ensure a successful integration between your ADFS environment and Cisco IQ, use the following diagnostic commands. These commands help verify metadata accessibility, certificate configurations, and endpoint settings.

- **Verify ADFS metadata accessibility:** Confirms that the ADFS Federation Metadata is reachable and publicly accessible; this is a critical step for establishing the initial trust

```
curl -k https://<your-adfs-domain>/FederationMetadata/2007-06/Federati
```

- **Validate the encryption certificate:** Ensures that the correct encryption certificate is associated with the Cisco IQ Relying Party Trust

```
Get-AdfsRelyingPartyTrust -Name "Cisco IQ - Production" |  
Select-Object EncryptionCertificate | Format-List
```

- **Review SAML Endpoint Configuration:** Verifies the SAML endpoints for the Cisco IQ trust are correctly configured and that authentication requests and assertions are routed to the expected URLs

```
Get-AdfsRelyingPartyTrust -Name "Cisco IQ - Production" |
Select-Object SamlEndpoints
```

Microsoft Entra ID SAML Configuration for SSO

This section provides guidance to configure Microsoft Entra ID (Entra ID) as the SAML IDP for Cisco IQ, supporting both password-based and PKI or Certificate-Based Authentication (CBA).

Prerequisites to Configure Entra ID SAML for SSO

- Entra ID tenant (for example, "ciqtestdev.onmicrosoft.com")
- Global Administrator or Application Administrator role access to Cisco IQ
- Connectivity between Entra ID (cloud) and Cisco IQ
- Enterprise CA installed or reachable (required for PKI only)
- Certificate Revocation List (CRL) Distribution Point reachable from the internet (required for PKI only)

Table 10: Entra ID Server Configuration

Item	Description	Example
Tenant ID	Entra ID tenant identifier	37352d8f-0ebe-4762-8161-8775ffe897cb
Cisco IQ FQDN	Deployment hostname	<YOUR-CIQ-FQDN>
IDP Entity ID	Entra ID issuer URL	https://sts.windows.net/<TENANT-ID>/
IDP SSO URL	SAML login endpoint	https://login.microsoftonline.com/<TENANT-ID>/saml2
Company Domain	Email domain for users	<YOUR-DOMAIN>

Configuring Entra ID SAML Application

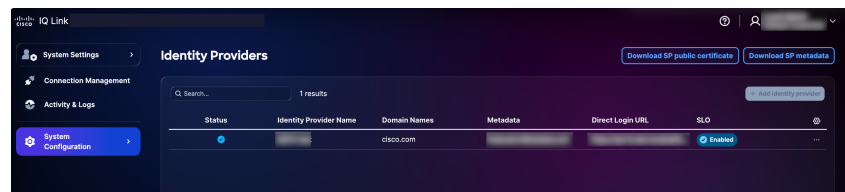
Creating an Enterprise Application

1. Sign in to the [Microsoft Entra admin center](#).
2. Navigate to **Identity > Applications > Enterprise applications**.
3. Click **New application > Create your own application**.
4. Enter the name (for example, “Cisco IQ”).
5. Choose **Integrate any other application you don’t find in the gallery (non-gallery)**.
6. Click **Create**.

Configuring SAML Single Sign-On

To configure SAML single sign-on, you must upload the SP metadata file. You can obtain it by performing the following steps from VA:

1. From **System Settings**, choose **System Configuration > Identity Providers**. The **Identity Providers** page displays.



Download Options

2. Click **Download SP metadata** to download. This downloaded SP metadata file is uploaded to complete SAML single sign-on configuration.
3. Click **Upload Metadata file** button to upload SP metadata file. The data from the SP metadata file will auto-populate in **SAML-Based Single Sign-on** screen after successful upload.

You can also opt to manually enter these details to configure the single sign-on settings. To manually configure SAML Single sign-on:

4. In the Enterprise Application, navigate to **Single sign-on** and choose **SAML**.
5. In the **Basic SAML Configuration** section, click **Edit** and enter the following:
 - **Identifier (Entity ID)** : <YOUR-CIQ-FQDN>

- **Reply URL (ACS URL)** : https://<YOUR-CIQ-FQDN>/saml/acs
- **Sign on URL** : https://<YOUR-CIQ-FQDN>/saml/login
- **Logout URL**: https://<YOUR-CIQ-FQDN>/saml/logout

6. Click **Save**.



Note: The Entity ID must match exactly what Cisco IQ uses as its SP Entity ID. This is typically the FQDN of the deployment.

7. To configure SAML Attributes and claims, click **Edit** in the **Attributes and Claims** section.

8. Configure the following claims:

Table 11: Required SAML Claims

Claim	Source Attribute	Namespace
Unique User Identifier (NameID)	user.userprincipalname (default)	
emailaddress	user.mail	http://schemas.xmlsoap.org/ws/2005/05/i
givenname	user.givenname	http://schemas.xmlsoap.org/ws/2005/05/i
surname	user.surname	http://schemas.xmlsoap.org/ws/2005/05/i
name	user.userprincipalname	http://schemas.xmlsoap.org/ws/2005/05/i
groups	user.assignedroles	(EMPTY — clear the namespace)



Note: For the **groups** claim:

- Use **user.assignedroles** as the source — not **user.groups**
- The **Namespace** field must be empty. This ensures the attribute name in the SAML assertion is simply *groups* instead of a full Uniform Resource Identifier (URI)
- Do not add a duplicate group claim with **user.groups** as this causes conflicts

Configuring App Roles

App Roles are configured in the App Registration (not the Enterprise Application); to configure App Roles:

1. Navigate to Identity > **Applications** > **App registrations**.
2. Find and choose your application.

3. Go to **App roles > Create app role**.

4. For each role needed, configure the following:

- **Display name** : For example, Cisco IQ Admins
- **Allowed member types** : Users/Groups
- **Value**: For example, Cisco IQ Admins
- **Description**: For example, Cisco IQ Administrators

5. Click **Apply**.



Note: Create roles matching your Cisco IQ role mapping requirements (for example, CXIQ Admins, CXIQ Developers, or CXIQ Viewers).

App Roles are used instead of group claims for the following reasons:

- *Cloud-only tenants cannot send group display names without a P1 or P2 license*
- *sAMAccountName only works for groups synced from on-premises AD*
- *Group ID source sends Universally Unique Identifier (UUIDs) which are difficult to map*
- *App Roles send exact string values matching Cisco IQ role expectations*

Assigning Users to App Roles

To assign users to App Roles:

1. Go back to the **Enterprise Application > Users and groups**.
2. Click **Add user/group**.
3. Choose the user(s) and assign the appropriate App Role.
4. Click **Assign**. Role values display as readable strings in the SAML assertion groups attribute.

Downloading IDP Metadata and Certificate

To download IDP Metadata and Certificate:

1. From the Enterprise Application, choose to **Single Sign-On > SAML Signing Certificate**.

2. Download Federation Metadata XML (save as entra-id-metadata.xml).

Or

Download Certificate (Base64) for manual certificate entry.

3. Take note of the following values from the **Set up** section:
 - Login URL (IDP SSO URL)
 - Azure AD Identifier (IDP Entity ID)
 - Logout URL (IDP SLO URL)



Note: As the Entra ID rotates signing certificates periodically, you must re-download the metadata and upload it to VA whenever the active certificate changes to ensure uninterrupted SSO service.

Adding Entra ID IDP



Note: APISIX routes for SAML are automatically created when an IDP is added in Cisco IQ, eliminating the need for manual route configuration.

To add Entra ID IDP:

1. Log in to VA as an Account Administrator.
2. Navigate to **System Settings > System Configuration > Identity Providers**.
3. Click **Add identity provider**.
4. Enter the **Name** of the IDP (for example, “Entra ID”).
5. Enter the **Domain(s)** (for example, “ciqtestdev.onmicrosoft.com” or your company domain).
6. (Optionally) turn on the **Enable single logout** toggle button, if required.
7. Drag-and-drop or upload the *entra-id-metadata.xml* file obtained from Entra ID in the **Upload IDP Metadata** field.
8. Click **Save**.



Note: The status remains “Incomplete” until role mapping is finished; this is the expected behavior.

Configuring Role Mapping

To configure Role Mapping:

1. From the added IDP, choose the **More Options** icon > **Map Roles**. The **Map user roles** page displays.
2. Enter an IDP role for each **System Role**. The following system roles are supported:

Table 12: System Roles

System Role	IDP Role (App Role Value)	Description
general_account_administrator	CXIQ Admins	Full permissions for all actions
general_account_viewer	CXIQ Developers	Read-only access
general_account_viewer	CXIQ Viewers	Read-only access

 **Note:** Use the App Role Value strings exactly as configured in Entra ID (see [Configuring App Roles](#) for more details)

4. Click **Save**. The status updates to **Success**.

Verifying the SAML Flow (Password Authentication)

To verify the SAML flow:

1. Open a browser in Incognito or Private mode.
2. Navigate to `https://<YOUR-CIQ-FQDN>/saml/login`.
3. Verify that you are redirected to the Microsoft login page.
4. Authenticate with your credentials (and MFA if configured).
5. After authentication, verify that you are redirected back to `/saml/acs` and that the Cisco IQ application is displayed.
6. Verify group extraction by running the following command:

```
kubectl -ncxue logs deployment/apisix -since=5m | grep -E "authenticat
```

Expected Output

SAML 2.0 compliant authentication successful for user:
user@domain.com with full name: N/A and 1 groups

Extracted group: CXIQ Admins (original: CXIQ Admins)

Total groups extracted: 1

Configuring Certificate-Based Authentication

This section describes how to add CBA alongside passwords. This section can be skipped if password-only authentication is sufficient.

Prerequisites for CBA

- Windows Server with AD CS with Enterprise CA configured (for example, “DEV-ADCS-CA”)
- PowerShell administrator access on the CA server
- Certificate UPN must match the Entra ID userPrincipalName
- CRL Distribution Point must be accessible from the internet

Creating a Certificate Template on AD CS

1. Open *certtmpl.msc* on the CA server.
2. Duplicate the User template and name it “EntraUserCert”.
3. Configure the template:
 - **General:** Display name EntraUserCert, validity 1–2 years
 - **Request Handling:** Purpose = Signature and encryption
 - **Subject Name:** Select **Supply in the request**
 - **Extensions:** Application Policies must include Client Authentication (1.3.6.1.5.5.7.3.2)
 - **Security:** Grant **Read** and **Enroll** permissions to Authenticated Users
4. Publish the template using the following command:

```
Add-CATemplate -Name “EntraUserCert” -Force
```


Requesting and Issuing a User Certificate

1. Create a Certificate Configuration (INF) file (for example, *C:-cert.inf*) by using the following PowerShell script:

```
@”
[Version]
Signature = “`$Windows NT`$”
[NewRequest]
Subject = “CN=

”

KeyLength = 2048
KeySpec = 1
KeyUsage = 0xa0
MachineKeySet = FALSE
ProviderName = “Microsoft RSA SChannel Cryptographic Provider”
RequestType = PKCS10
[RequestAttributes]
CertificateTemplate = EntraUserCert
[EnhancedKeyUsageExtension]
OID = 1.3.6.1.5.5.7.3.2
OID = 1.3.6.1.4.1.311.20.2.2
[Extensions]
2.5.29.17 = “{text}”
_continue_ = “upn=

&”
_continue_ = “email=

”
"@ | Out-File -FilePath C:-cert.inf -Encoding ASCII
```

2. Replace <USER-UPN> with your Entra ID UPN (for example, user@ciqtestdev.onmicrosoft.com).
3. To generate the certificate, run the following commands:

```
certreq -new C:-cert.inf C:-cert.csr
```

4. To submit the request to the CA, run the following command:

```
certreq -submit -config "<CA-SERVER>\<CA-NAME>" C:-cert.csr C:-cert.cer
```

5. To install certificate to the CA, run the following command:

```
certreq -accept C:-cert.cer
```

Exporting Certificates

To export the user certificate as a PFX file (for client), run the following script:

```
$cert = Get-ChildItem Cert:| Where-Object { $_.Subject -like "*<USER-NAME>*" }
$password = ConvertTo-SecureString -String "<EXPORT-PASSWORD>" -Force
Export-PfxCertificate -Cert $cert -FilePath C:-cert.pfx -Password $password
```

To export the CA Root certificate (for Entra ID), run the following script:

```
Get-ChildItem Cert:| Where-Object { $_.Subject -like "<CA-NAME>*" } |
Select-Object -First 1 | Export-Certificate -FilePath C:-root.cer -Type Cert
```

Importing the User Certificate on Client Machine (MacOS)

To import the user certificate (PFX), run the following command:

```
security import /path/to/entra-cert.pfx -k ~/Library/Keychains/login.keychain
```

To import the CA root certificate, run the following command:

```
security import /path/to/ca-root.cer -k ~/Library/Keychains/login.keychain
```

To set the CA certificate to Always Trust in Keychain Access:

1. Open Keychain Access.

2. Find the CA certificate and click **Get Info**.
3. Under **Trust**, set to “Always Trust”.



Note: After importing, quit and reopen your browser for the certificate to be recognized.

Uploading the CA Root Certificate to Entra ID

1. Sign in to the [Microsoft Entra admin center](#).
2. Navigate to Protection > Security > Certificate authorities.
3. Click **Upload** and select the ca-root.cer file.
4. Mark it as a root CA certificate.
5. Enter the **CRL Distribution Point URL** (must be publicly reachable).

Enabling CBA in Entra ID Authentication Methods

1. Navigate to **Protection > Authentication methods > Policies**.
2. Click **Certificate-based authentication** to configure.
3. Enable **CBA** and add the target users or groups.
4. Under Configure, set protection level to Single-factor authentication.

Configuring Username Binding

In the CBA configuration, go to the **Username binding** tab and set the following binding:

- **Certificate Field:** PrincipalName
- **User Attribute:** userPrincipalName

This maps the UPN in the certificate’s Subject Alternative Name (SAN) to the Entra ID user.

Verifying the CBA Flow

1. Open a browser in Incognito or Private mode.
2. Navigate to <https://<YOUR-CIQ-FQDN>/saml/login>.
3. In the **Microsoft** login page, enter the user’s email and click **Next**.

4. Choose **Use a certificate or smart card** (or it may auto-prompt).
5. Choose the applicable user certificate when the browser prompts for certificate selection.
6. Verify that Entra ID validates the certificate, redirects with a SAML response, and creates a session.



Note: Ensure you select the correct client certificate. Selecting a wrong certificate (for example, a different user's certificate or an expired certificate) causes authentication failure.

Troubleshooting Entra ID Issues

The following list outlines common issues and possible solutions to help quickly identify and resolve problems related to Entra ID SAML configuration.

Table 13: Troubleshooting

Issue	Cause	Fix
Invalid SAML Response - missing email	SAML assertion has no NameID or email attribute	Verify Entra ID claims configuration (see Configuring SAML Single Sign-On for more details). Check that the user has the mail attribute populated. Use user.assignedroles as the source.
Total groups extracted: 0	Groups claim not configured or wrong source	Ensure the user is assigned to an App Role (see Assigning Users to App Roles for more details).
Duplicate groups claims	Both user.groups and user.assignedroles active	Remove the user.groups claim. Keep only user.assignedroles .
Groups showing as UUIDs	Source attribute is "Group ID"	Use the App Roles approach (see Configuring App Roles for more details).
Attribute Name shows long URI	Namespace field is not empty	Clear the Namespace field in the groups claim

Issue	Cause	Fix
Invalid SAML signature	IdP certificate rotated or mismatch	settings. Re-download the metadata from the Entra ID and re-upload to Cisco IQ. Publish the CRL to a publicly accessible URL, or use the
AADSTS500191	CRL not reachable from internet	self-signed CA approach (see CRL Workaround for Reachability Issues for more details). Verify that the user certificate is imported in MacOS Keychain Access (see Importing the User Certificate on Client Machine (MacOS) for more details), CBA is enabled in Entra ID with the required settings (see Enabling CBA in Entra ID Authentication Methods for more details), and Chrome is restarted to apply changes.
Certificate not prompted	Certificate not in Keychain, CA not trusted on client, or CBA not enabled	Increase <code>clock_skew_seconds</code> in the plugin configuration (the default is 300; use 30000 for the lab). Complete role mapping (see Configuring Role Mapping for more details).
SAML assertion expired	Clock skew between systems	
Status “Incomplete” in Virtual Appliance	Role mapping not yet configured	

CRL Workaround for Reachability Issues

If your CA’s CRL Distribution Point is not reachable from the internet (common in lab setups), use a self-signed CA with no CRL requirements:

```

powershell
# Create self-signed CA
$rootCA = New-SelfSignedCertificate `
-Subject "CN=CIQ-Test-CA" `
-CertStoreLocation "Cert:" `
-KeyUsage CertSign, CRLSign `
-KeyLength 2048 `
-NotAfter (Get-Date).AddYears(5) `
-TextExtension @("2.5.29.19={text}ca=TRUE")
# Create user cert signed by the CA
$userCert = New-SelfSignedCertificate `
-Subject "CN=

" `
-CertStoreLocation "Cert:" `
-Signer $rootCA `
-KeyUsage DigitalSignature `
-KeyLength 2048 `
-NotAfter (Get-Date).AddYears(2) `
-TextExtension @(
"2.5.29.37={text}1.3.6.1.5.5.7.3.2",
"2.5.29.17={text}upn=

&email=

"
)

```

Upload only the root CA cert to Entra ID. Since it is self-signed with no Cisco Discovery Protocol (CDP), Entra ID does not attempt CRL validation.

Complete Setup Checklist

This section describes a complete setup checklist for configuring VA with Microsoft Entra ID SAML Application and optional CBA.

Entra ID SAML Application Setup

- Create an Enterprise Application (non-gallery) in Entra ID
- Configure a Basic SAML Configuration by manually entering SP metadata

- Configure Attributes & Claims (including email, name, and groups with user.assignedroles)
- Create App Roles in App Registration
- Assign users to App Roles
- Download the Federation Metadata XML

Cisco IQ Configuration

- Add an IDP in Cisco IQ by uploading Entra ID metadata
- Configure the Role Mapping to map App Role values to Cisco IQ system roles
- Verify password-based login works end-to-end
- Verify groups are extracted correctly in logs

Certificate-Based Authentication (optional)

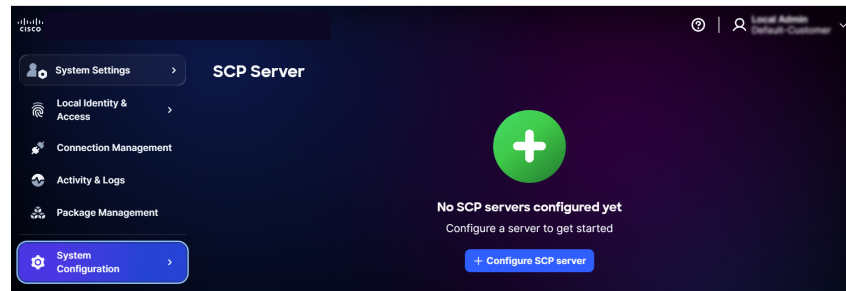
- Create certificate template on AD CS with Client Authentication EKU
- Issue a user certificate with a UPN matching the Entra ID user
- Export a user certificate as a PFX file and install it on the client machine
- Trust the CA certificate on the client machine
- Upload the CA root certificate to Entra ID under **Protection > Certificate authorities**
- Enable the CBA in Authentication methods
- Configure username binding (PrincipalName and userPrincipalName)
- Verify CBA login works end-to-end

Adding SCP Server

An SCP server is a prerequisite for importing upgrade files that are essential for adding, upgrading, or fixing the Cisco IQ installation.

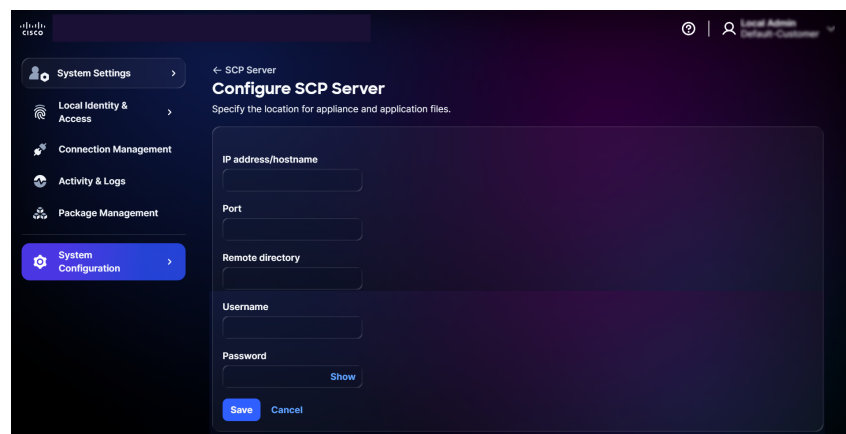
To add an SCP Server:

1. From **System Settings**, choose **System Configuration > SCP Server**. The **SCP Server** page displays.



SCP Server Home page

2. Click **Configure SCP server**. The **Configure SCP Server** page displays.



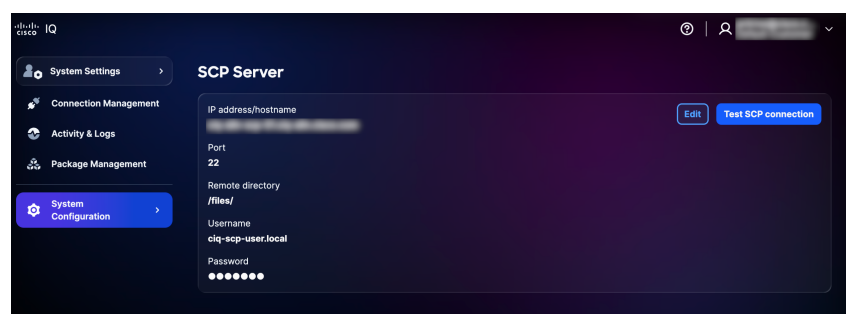
Configure SCP Server

3. Enter an **IP address/hostname**.
4. Enter a **Port**.
5. Enter a **Remote directory**.
6. Enter a **Username**.
7. Enter a **Password**.
8. Click **Save**. A confirmation displays.

Editing an Existing SCP Server

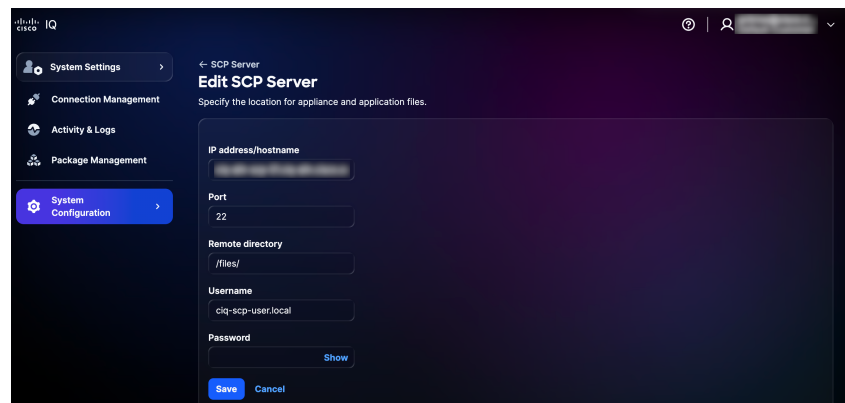
To edit an existing SCP server:

1. Navigate to the **SCP Server** page.



Added SCP Server

2. Click **Edit** of the desired existing SCP server.



Editing SCP Server

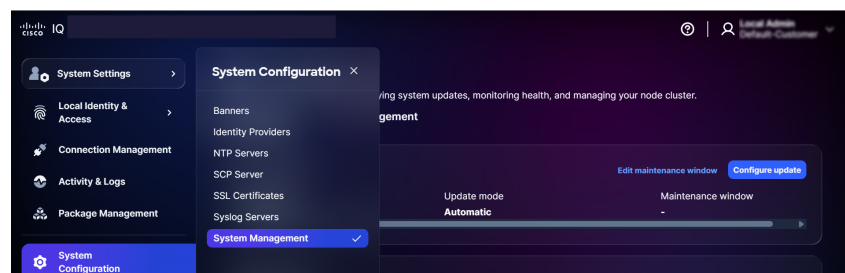
3. Modify details as required.
4. Click **Save**.

System Management

You can upgrade to the latest Cisco IQ VA version through the UI. You can also verify from the **Cisco IQ Data Connectors** page.

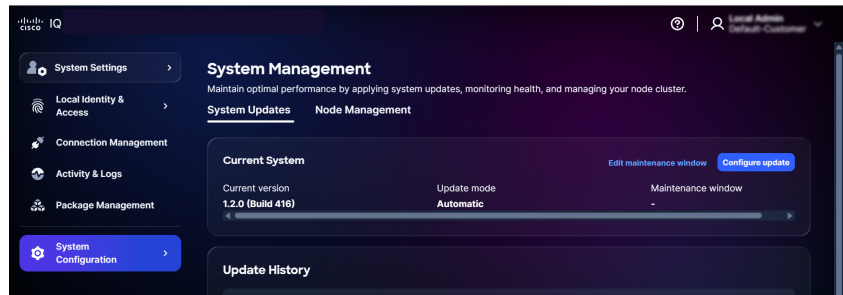
Rescheduling System Update

To reschedule the system update:



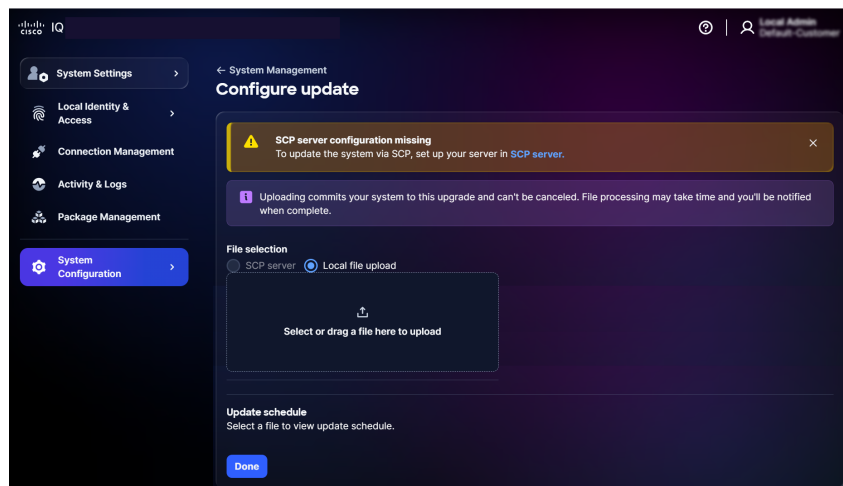
System Management

1. From **System Settings**, choose **System Configuration** > **System Management**. The **System Management** page displays. This page displays the system version that is currently running; if no updates have been configured, the **Update History** section is empty.



System Upgrade

2. Click **Configure update**. The **Configure update** page displays.



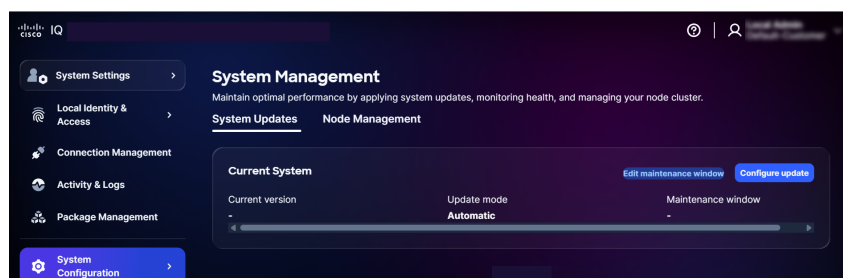
Configure Upgrade

3. Choose the **Update schedule** to schedule another time.
4. Wait for the file upload to complete; the duration depends on the bundle size and network speed.

Confirm successful update by verifying the check mark icon displayed under the **Update Status** column.

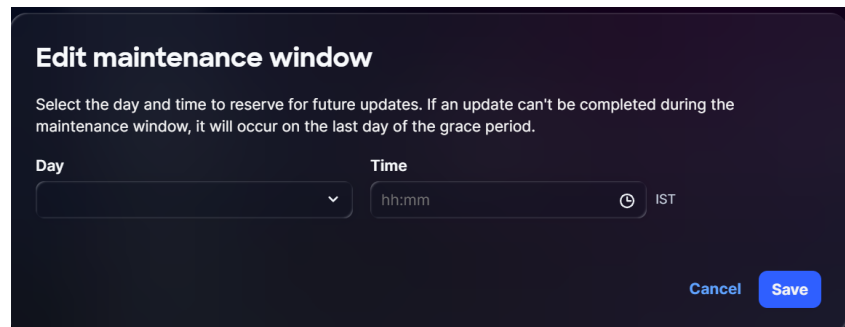
Editing System Upgrade Schedules

You can create a custom schedule for system upgrades. If a custom schedule is configured, upgrades occur on user-defined dates provided they remain within the maximum grace period. To create a system upgrade schedule:



Edit Maintenance

1. From the **Current System** section on the **System Management** page, click **Edit maintenance window**.



Edit maintenance window

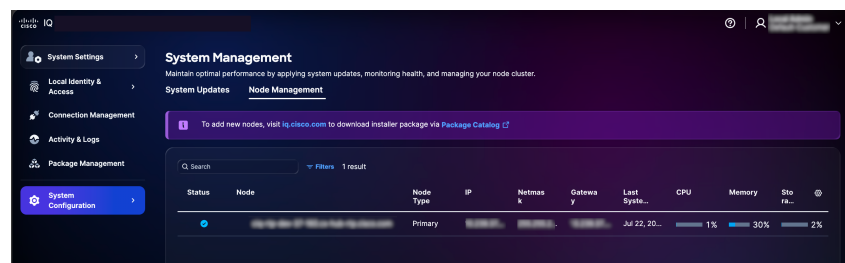
2. Choose an option from the **Day** and **Time** drop-down lists.
3. Click **Save**. The maintenance window has been successfully scheduled. The update is triggered according to the displayed schedule.



Note: If no upgrade schedule is configured, the system defaults to grace periods of two (2) weeks for non-reboot upgrades and four (4) weeks for upgrades requiring a reboot. After these grace periods, updates must be performed manually. In case of an upgrade failure, the system performs up to two (2) automatic retries. A third attempt is scheduled but requires manual initiation.

Node Management

1. Navigate to **System Configuration > System Management > Node Management** to view and manage the nodes in your cluster.



Status	Node	Node Type	IP	Netmask	Gateway	Last Sync	CPU	Memory	Storage
Active	10.10.10.10	Primary	10.10.10.10	255.255.255.0	10.10.10.1	Jul 22, 2023	1%	30%	2%

Node Management

2. The node list displays each node's status, hostname, node type, IP address, netmask, gateway, and last sync time.

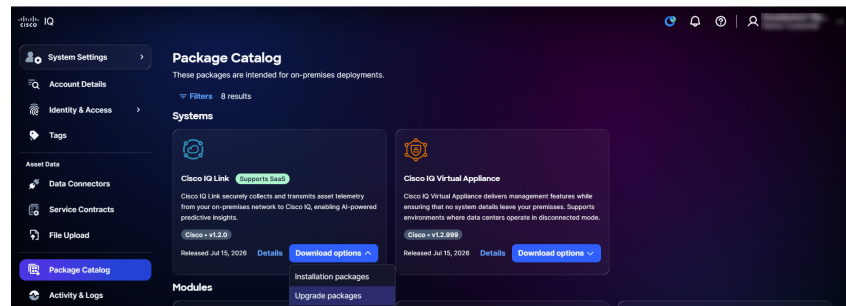


Note: A blue checkmark in the **Status** column indicates the node is active.

Manually Upgrading the System

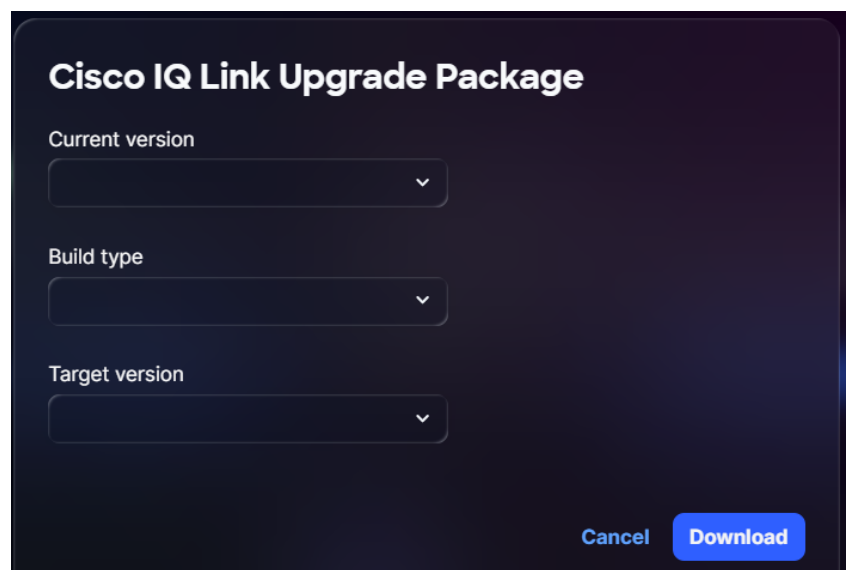
In scenarios where automatic distribution from Cisco IQ SaaS is either unavailable or delayed, you can manually perform a system upgrade by downloading the upgrade bundle directly from Cisco IQ SaaS. To manually upgrade the system:

1. Log in to [Cisco IQ SaaS](#).
2. Navigate to **Home > System Settings > Package Catalog**.



Software Catalog

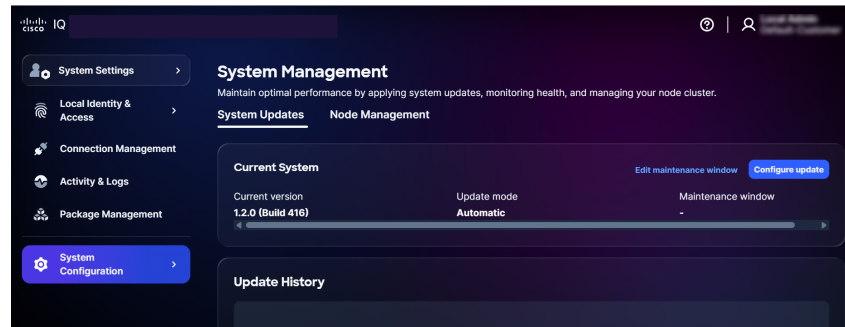
3. In the **Cisco IQ Virtual Appliance** card, click **Download options > Upgrade packages**.



Upgrade Package

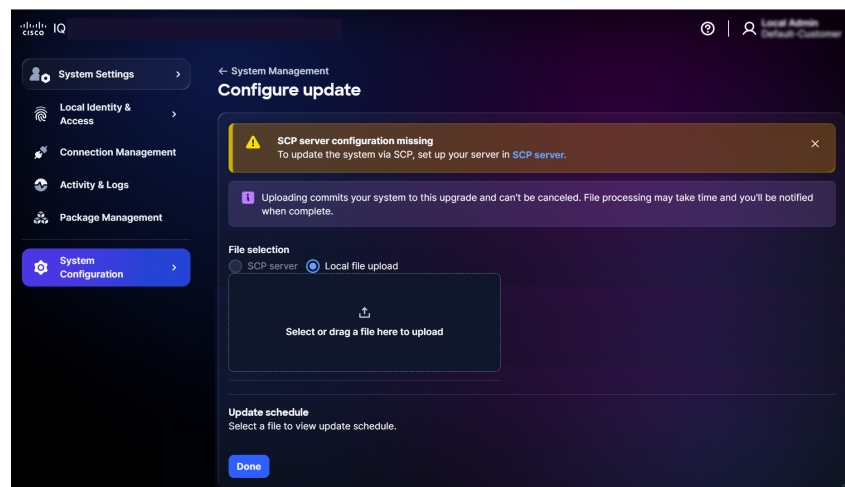
4. Choose the **Current version** from the drop-down list.
5. Choose the **Build type** from drop-down list.
6. Choose the **Target version** from drop-down list.
7. Click **Download**. The upgrade bundle downloads.
8. Navigate to Cisco IQ VA.

9. From **System Settings**, choose **System Configuration** > **System Management**.



Configure Update

10. Click **Configure update**.



Local File Upload

11. Click the **Local file upload** radio button.
12. Select or drag the downloaded upgrade bundle file into the upload field.
13. Wait for the file upload to complete; the duration depends on the bundle size and network speed.

SSL Certificates Configuration

A default self-signed certificate is pre-installed and enabled in Cisco IQ, but you can optionally upload custom SSL certificates. When a custom SSL certificate is enabled, it is used for HTTPS connections; if the certificate is disabled or deleted, the system automatically reverts to the default certificate. The default SSL certificate cannot be edited or deleted.

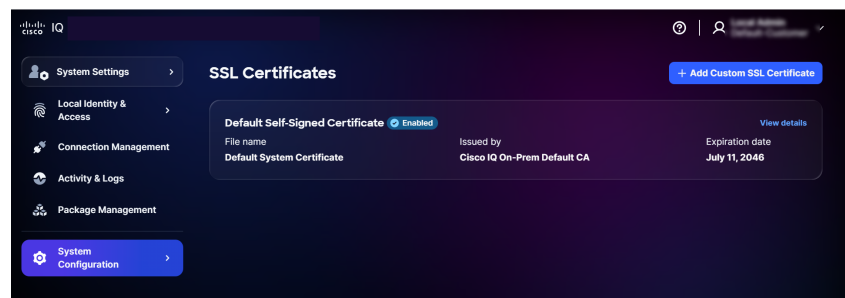
 **Note:** The certificate must have at least 90 days of validity remaining. A certificate is considered “nearing expiry” when it has less than 90 days remaining until expiration.

 After adding, editing, or deleting an SSL certificate, you must upload the new SSL certificate as outlined in [Completing SLO Configuration](#) for the Okta IDP or the ADFS IDP.

Adding Custom SSL Certificate

To add a custom SSL certificate:

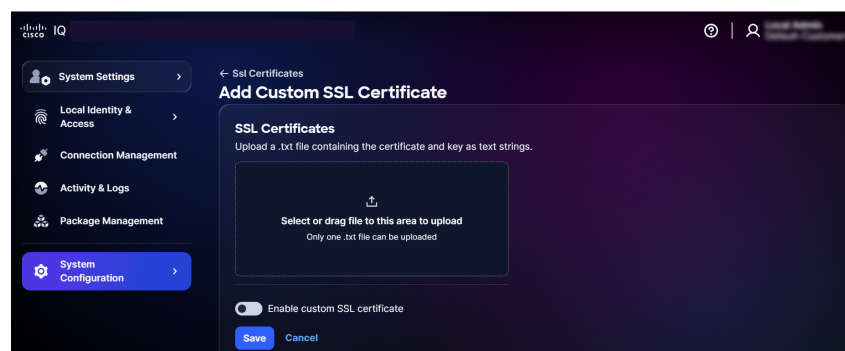
1. From **System Settings**, choose **System Configuration** > **SSL Certificates**. The **SSL Certificates** page displays, listing all SSL certificates for your system.



Adding SSL Certificate

2. Click **Add Custom SSL Certificate**.

 **Note:** Upload a .txt file that includes both the Privacy-Enhanced Mail-encoded certificate and key as text strings. Only one .txt file can be uploaded at a time. The file must contain both the certificate and the private key.



Upload SSL Certificate

3. Drag-and-drop or upload the custom SSL certificate under the **SSL Certificate** section.
4. Turn on the Enable custom SSL certificate toggle button.

Enable Certificate?

Enabling custom SSL certificate will disable the default self-signed certificate.

Cancel

Enable certificate

Enable Certificate



Note: Keep the toggle OFF if you want to upload the certificate without activating it immediately.

5. Click Enable certificate.
6. Click **Save**.

The custom SSL certificate is enabled and active. The default system certificate is automatically deactivated.

Editing Custom SSL Certificate

You can edit the custom SSL certificate to upload a new certificate or to disable the currently enabled certificate. To edit:

1. Navigate to the desired custom SSL certificate.
2. Choose the **More Options** icon > **Edit**. The **Edit SSL Certificate** page displays.
3. Edit the certificate details as required.
4. Click **Save**.

Deleting Custom SSL Certificate

Warning: A custom SSL certificate can be deleted at any time, but it is an irreversible action; you can upload a new custom certificate at any time after deletion.

To delete:

1. Navigate to the desired personal SSL certificate.
2. Choose the **More Options** icon > **Delete**.
3. Click **Delete Certificate**. The custom certificate is deleted, and the default certificate is automatically reactivated.

Syslog Server Configuration

Users with the Account Administrator role can configure external syslog servers to export system logs. Up to two (2) syslog servers can be configured.

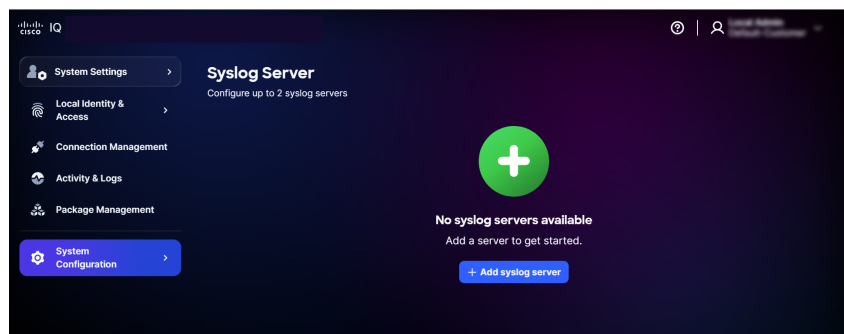


Note: The Syslog server must be specified as an IP address and not as a Fully Qualified Domain Name (FQDN).

Adding Syslog Server

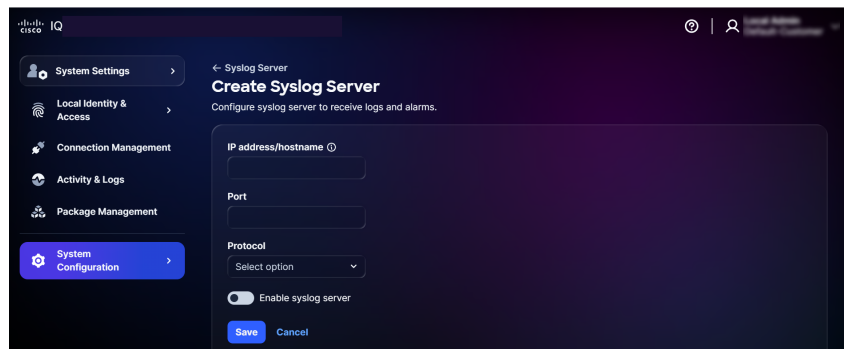
To add a syslog server:

1. From **System Settings**, choose **System Configuration** > **Syslog Server**. The **Syslog Server** page displays.



Add Syslog Server

2. Click **Add syslog server**. The **Create Syslog Server** page displays.



Create Syslog Server

3. Enter the **IP address/hostname**.
4. Enter **Port**.
5. Select the applicable protocol from the **Protocol** drop-down list (for example, UDP, TCP).
6. Turn on the **Enable syslog server** toggle button.
7. Click **Save**. A confirmation displays and the newly added syslog server displays on the Syslog Server page.

Editing Configured Syslog Server

To edit a configured syslog server:

1. Navigate to the desired syslog server.
2. Choose the **More Options** icon > **Edit**. The **Edit Syslog Server** page displays.
3. Edit details or turn off the **Enable syslog server** toggle, as required.
4. Click **Save**.

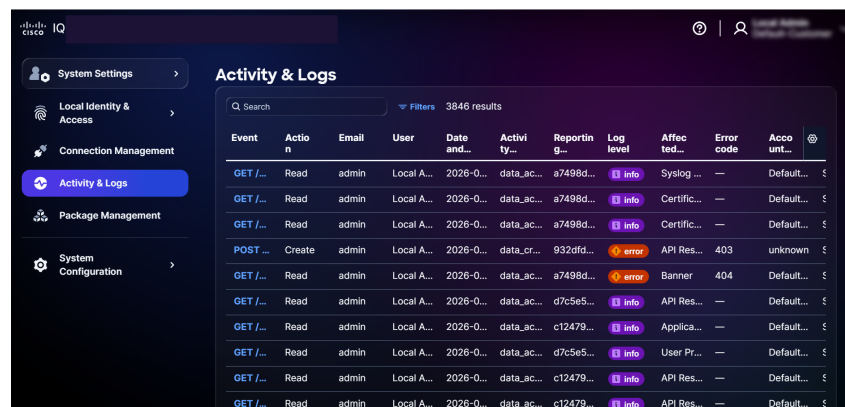
Deleting Configured Syslog Server

To delete a configured syslog server:

1. Navigate to the desired syslog server.
2. Choose the **More Options** icon > **Delete**. A confirmation displays.
3. Click **Delete syslog server**.

Activity & Logs

Activity & Logs provide a detailed record of user actions and changes in Cisco IQ, allowing Account Administrators to track user activities and maintain transparency.



Event	Action	Email	User	Date and time	Activity ID	Report ID	Log level	Affected resource	Error code	Account	
GET /...	Read	admin	Local A...	2026-0...	data_ac...	a7498d...	info	Syslog ...	—	Default...	⋮
GET /...	Read	admin	Local A...	2026-0...	data_ac...	a7498d...	info	Certific...	—	Default...	⋮
GET /...	Read	admin	Local A...	2026-0...	data_ac...	a7498d...	info	Certific...	—	Default...	⋮
POST /...	Create	admin	Local A...	2026-0...	data_cr...	932df...	error	API Res...	403	unknown	⋮
GET /...	Read	admin	Local A...	2026-0...	data_ac...	a7498d...	error	Banner	404	Default...	⋮
GET /...	Read	admin	Local A...	2026-0...	data_ac...	d7c5e5...	info	API Res...	—	Default...	⋮
GET /...	Read	admin	Local A...	2026-0...	data_ac...	c12479...	info	Applica...	—	Default...	⋮
GET /...	Read	admin	Local A...	2026-0...	data_ac...	d7c5e5...	info	User Pr...	—	Default...	⋮
GET /...	Read	admin	Local A...	2026-0...	data_ac...	c12479...	info	API Res...	—	Default...	⋮
GET /...	Read	admin	Local A...	2026-0...	data_ac...	c12479...	info	API Res...	—	Default...	⋮

Activity & Logs

To view activity and logs, select **Activity & Logs** from the **System Settings** menu.

Activity & Logs:

- Records all API operations at the gateway level
- Supports filters, pagination, and search capabilities to help you easily find and manage information

The following filter options are available:

- **Last logged date:** Filters logs to a specific time range
- **Log level:** Filters logs by severity (for example, error, warning, and info)
- **Activity type:** Filters logs by the type of system activity
- **Error code:** Filters for a specific error code

Banners

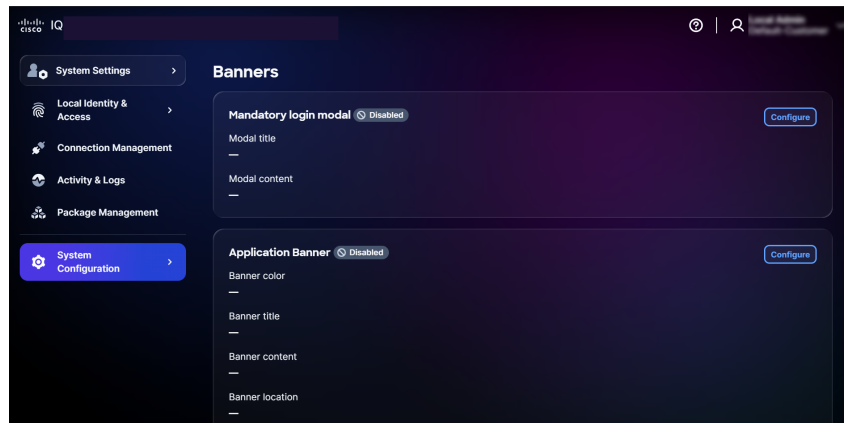
Account Administrators can configure system-wide banners to meet security and compliance standards.

- **Mandatory Login Modal:** You must acknowledge the mandatory banner before proceeding to the login screen.
- **Application Banner:** These are customized banners that display across the application after successful authentication.

Configuring Mandatory Login Modal Banners

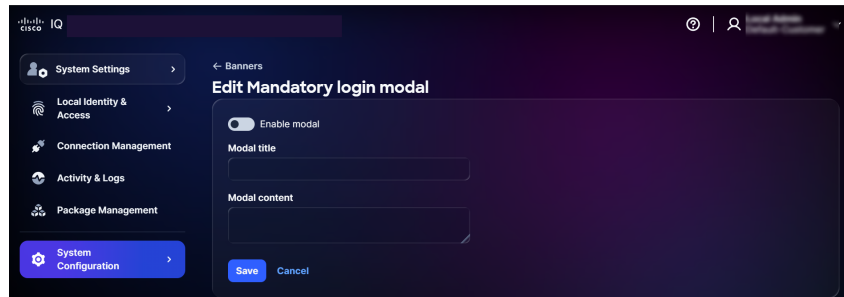
To configure a mandatory banner:

1. From **System Settings**, choose **System Configuration > Banners**. The **Banners** page displays.



Configure Mandatory Banner

2. Click **Configure** in the **Mandatory login modal**. The **Edit Mandatory login modal** page displays.



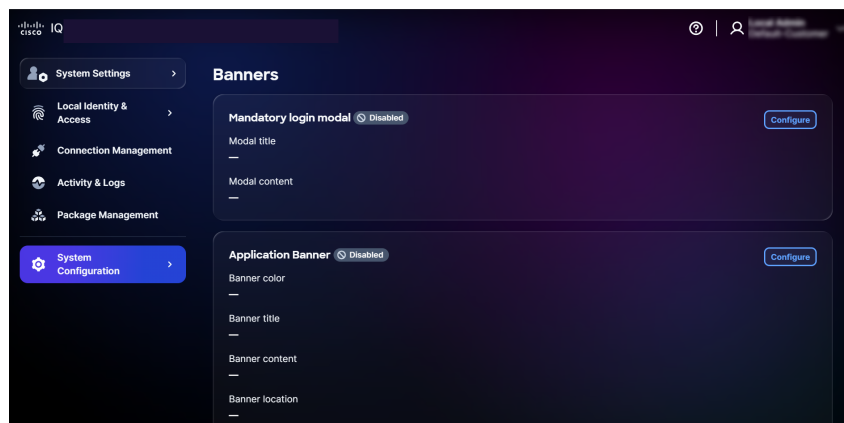
Edit Mandatory login modal Banner

3. Click the toggle to enable or disable the banner.
4. Enter the **Modal title**.
5. Enter the **Modal content**.
6. Click **Save**. The Mandatory login modal is saved.

Configuring Application Banners

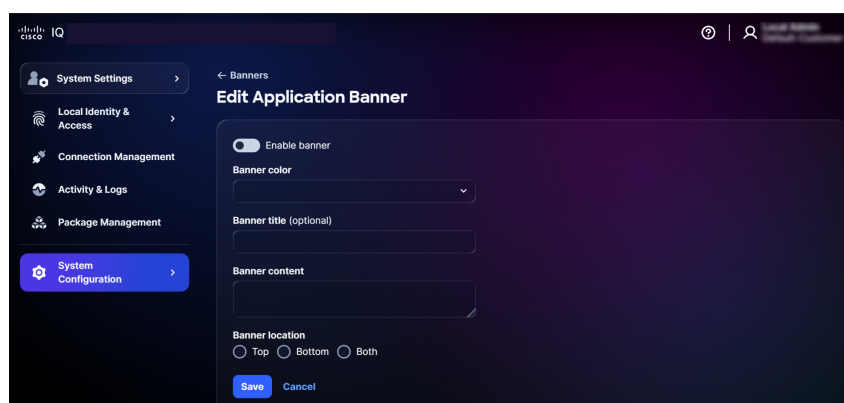
To configure an application banner:

1. From **System Settings**, choose **System Configuration > Banners**. The **Banners** page displays.



Configure Banner

2. Click **Configure** in Application Banner. The **Edit Application Banner** page displays.



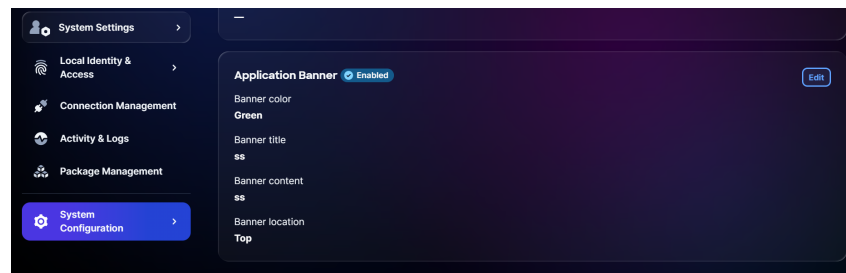
Edit Application Banner

3. Click the toggle to enable or disable the banner.
4. Choose a **Banner color**.
5. Enter the **Banner title**.
6. Enter the **Banner content**.
7. Choose a **Banner location**.
8. Click **Save**. The banner displays across the application.

Editing Banners

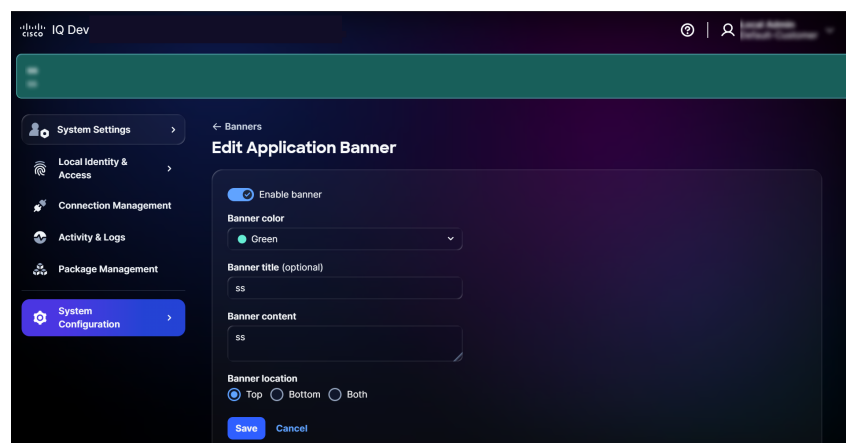
To edit a banner:

1. From **System Settings**, choose **System Configuration > Banners**. The **Banners** page displays.



Edit Banners

2. Click **Edit**. The **Edit Application Banner** page displays.



Edit Application Banner

3. Edit the desired details.
4. Click the toggle to enable or disable the banner.
5. Click **Save**.

Troubleshooting

You can collect diagnostic and log files from the Cisco IQ system and securely transfer them to a SCP server. These files can be shared with the Support Team when reporting issues to provide valuable context and assist with troubleshooting.

To collect diagnostic and log files:

1. Log in to Cisco IQ.



```

Cisco IQ

Navigation Main Menu

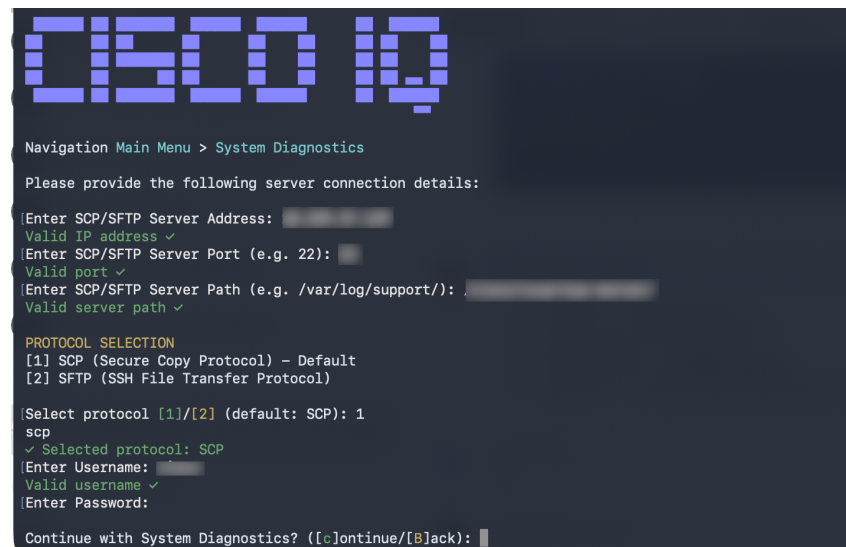
SYSTEM STATUS
Cisco IQ On-Prem   Installed

CONFIGURATION SETTINGS
IP Address/Mask
Gateway IP
DNS List
Search Domain
NTP List
Hostname

MAIN MENU
[1] Configure Network Settings DISABLED because the platform is installed
[2] Configure System Orchestrator DISABLED because the platform is installed
[3] System Diagnostics
[4] Help
[5] About
[q] Quit
```

Main Menu

2. From the Cisco IQ **Main Menu**, enter “3” and press **Enter** to select **System Diagnostics**.



```

Cisco IQ

Navigation Main Menu > System Diagnostics

Please provide the following server connection details:

[Enter SCP/SFTP Server Address: ]
Valid IP address ✓
[Enter SCP/SFTP Server Port (e.g. 22): ]
Valid port ✓
[Enter SCP/SFTP Server Path (e.g. /var/log/support/): ]
Valid server path ✓

PROTOCOL SELECTION
[1] SCP (Secure Copy Protocol) – Default
[2] SFTP (SSH File Transfer Protocol)

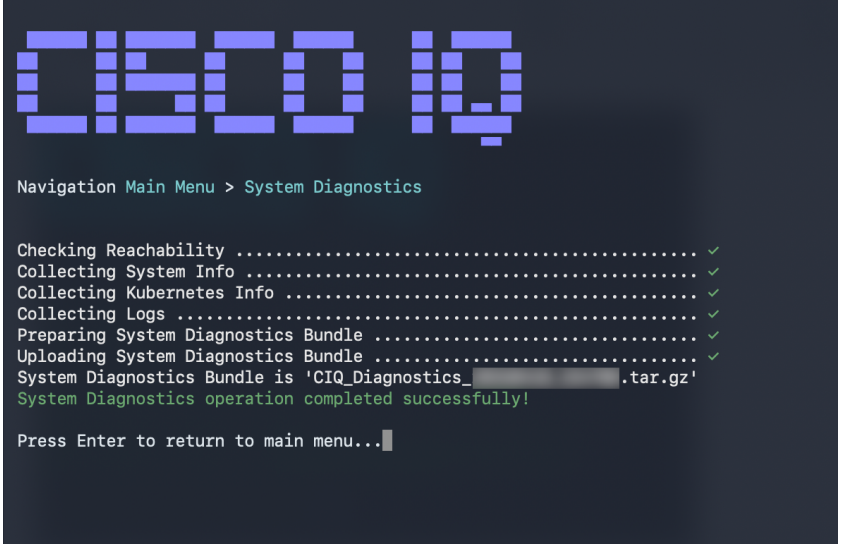
[Select protocol [1]/[2] (default: SCP): 1]
scp
✓ Selected protocol: SCP
[Enter Username: ]
Valid username ✓
[Enter Password: ]

Continue with System Diagnostics? ([c]ontinue/[B]ack):
```

System Diagnostics

3. Enter the **SCP/SFTP Server Address**.
4. Enter the **SCP/SFTP Server Port**.
5. Enter the **SCP/SFTP Server Path**.

6. Select a **protocol**.
7. Enter the **Username**.
8. Enter the **Password**.
9. Enter “C” and press **Enter** to continue with system diagnostics.



```
Navigation Main Menu > System Diagnostics

Checking Reachability ..... ✓
Collecting System Info ..... ✓
Collecting Kubernetes Info ..... ✓
Collecting Logs ..... ✓
Preparing System Diagnostics Bundle ..... ✓
Uploading System Diagnostics Bundle ..... ✓
System Diagnostics Bundle is 'CIQ_Diagnostics_XXXXXX.tar.gz'
System Diagnostics operation completed successfully!

Press Enter to return to main menu...
```

System Diagnostic Operation Complete

The system begins the diagnostic process and performs the following actions:

- Checking Reachability
- Collecting System Information
- Collecting Kubernetes Information
- Collecting Logs
- Preparing System Diagnostics Bundle
- Uploading System Diagnostics Bundle

Once complete, a confirmation message displays indicating the generated bundle name.

Support Module

You can create VA and module-specific support cases from Cisco IQ SaaS. The Support module is available in Cisco IQ SaaS and offers a consolidated view of your support cases. It enables you to filter, sort, and customize the case list view, providing visibility into both open and closed cases you are entitled to access. For more detailed information about the Support module in Cisco IQ SaaS, see the [Cisco IQ SaaS Getting Started Guide](#).



Note: Cisco IQ VA customers can access most Cisco IQ SaaS Support module features, including opening Technical Assistance Center (TAC) cases related to Cisco IQ VA and its modules, as well as creating and managing product cases.

Creating a Support Case

You can create VA and module-specific cases in Cisco IQ SaaS. To create a case:

1. Log in to [Cisco IQ \(SaaS\)](#).
2. Click the **Help** icon > **Report an Issue**. The **Report an Issue** window opens.

The screenshot shows the 'Report an Issue' form. At the top, it says 'Report an Issue' and 'Experiencing an issue with Cisco IQ? Let us know what's going on and we'll open a support case for you.' Below this is the 'Issue type' section with four radio buttons: 'Portal login issues', 'Error message', 'Data discrepancy', and 'Other'. The 'Error message' option is selected. Below that is the 'Issue description' section with a text area labeled 'Describe what happened.' and a note 'The more detail you give, the faster we can help.' Below the text area is the 'Preferred contact method' section with three radio buttons: 'Telephone', 'Email', and 'Virtual space via Webex'. The 'Email' option is selected. Below that is the 'Include recipients (optional)' section with a dropdown menu labeled 'Select or add email addresses' and a note 'Select or enter email addresses to include.' At the bottom right are 'Cancel' and 'Submit' buttons.

Report an Issue

3. Provide the required details.
4. Click **Submit**.