# Cisco IQ Link Operations Guide v1.1.0

## Introduction

Cisco IQ™ provides customers 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 users to make proactive, informed decisions and streamlines processes for customer engagement and success.

Cisco IQ Link securely collects and transmits asset telemetry from your on-premises network to Cisco IQ, enabling AI-powered predictive insights that help you improve network visibility, anticipate issues, and drive operational efficiency.

## Local Authentication

Administrators should use the following credentials to log in to Cisco IQ Link:

- **Default Username**: admin
- **Default Password**: password that is set during the Cisco IQ Link installation process; see the *Cisco IQ Link Getting Started Guide* for more information

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

### Setting Local Admin Security

You can change your password and set up security questions through the **Local Admin Security** menu in **System Configuration**.

*You have three (3) attempts to enter the correct password within a ten (10) minute period. If all three (3) attempts are unsuccessful, your account temporarily locks for 60 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.*

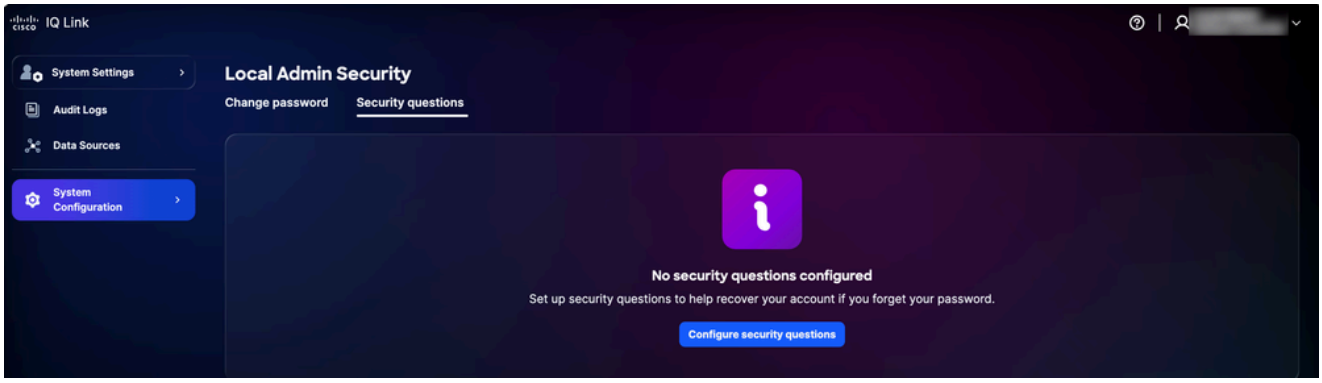
*Your account automatically unlocks after 60 minutes, at which point you may attempt to log in or reset your password.*

### Setting Up Security Questions and Answers

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

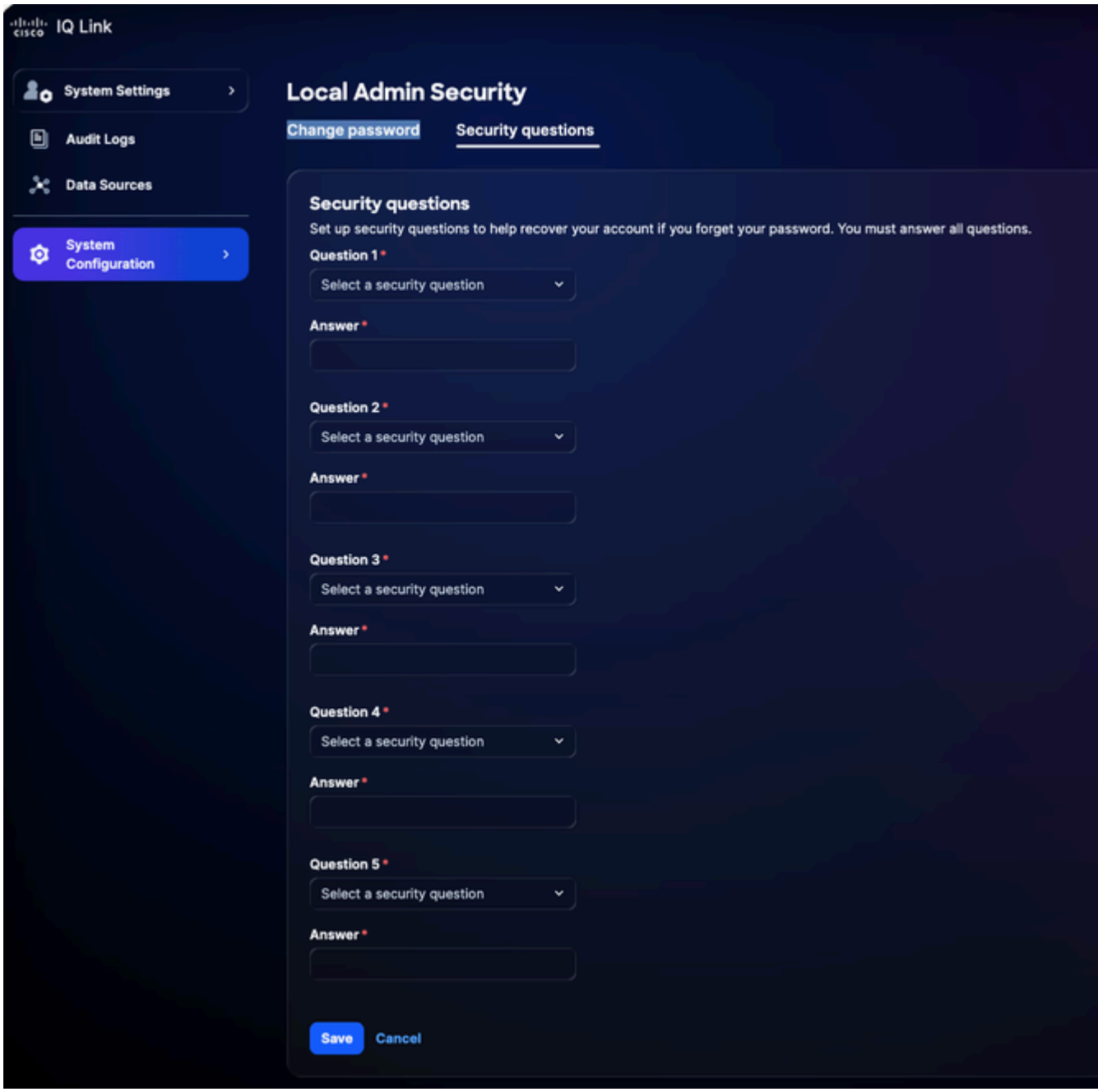
To set up security questions:

1. From **System Settings**, choose **System Configuration** > **Local Admin Security** > **Security Questions**.




*Security Questions*

2. Click **Configure security questions**.




*Security Questions*

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

**Notes**:
• 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

**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

Only local Administrators can manage the password for Cisco IQ.

#### Prerequisites

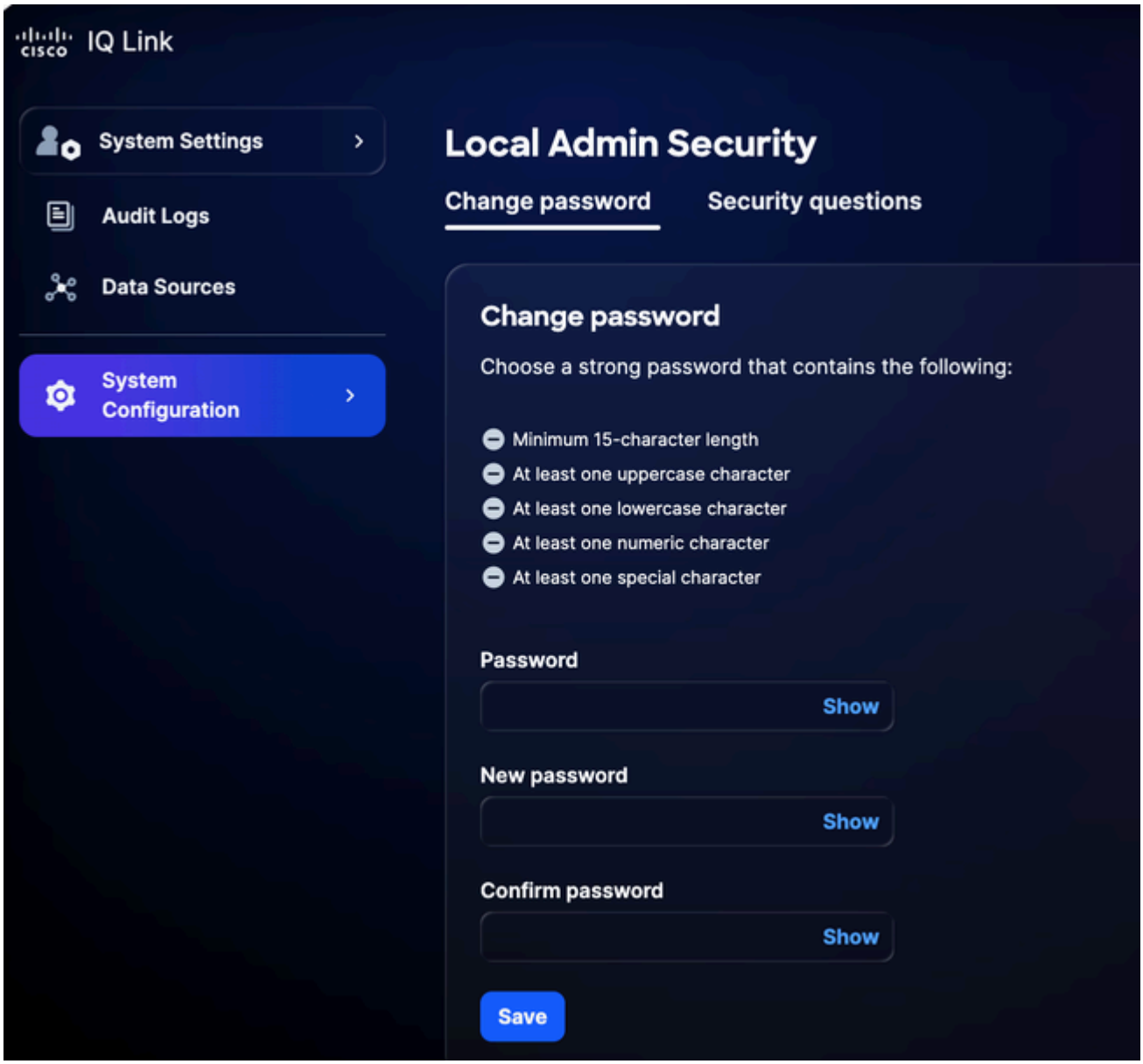
To manage passwords, the following conditions must be met:

- You are a local Administrator
- You are using a local Administrator 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 **System Settings**, navigate to **System Configuration** > **Local Admin Security** > **Change Password.**




*Change Password*

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

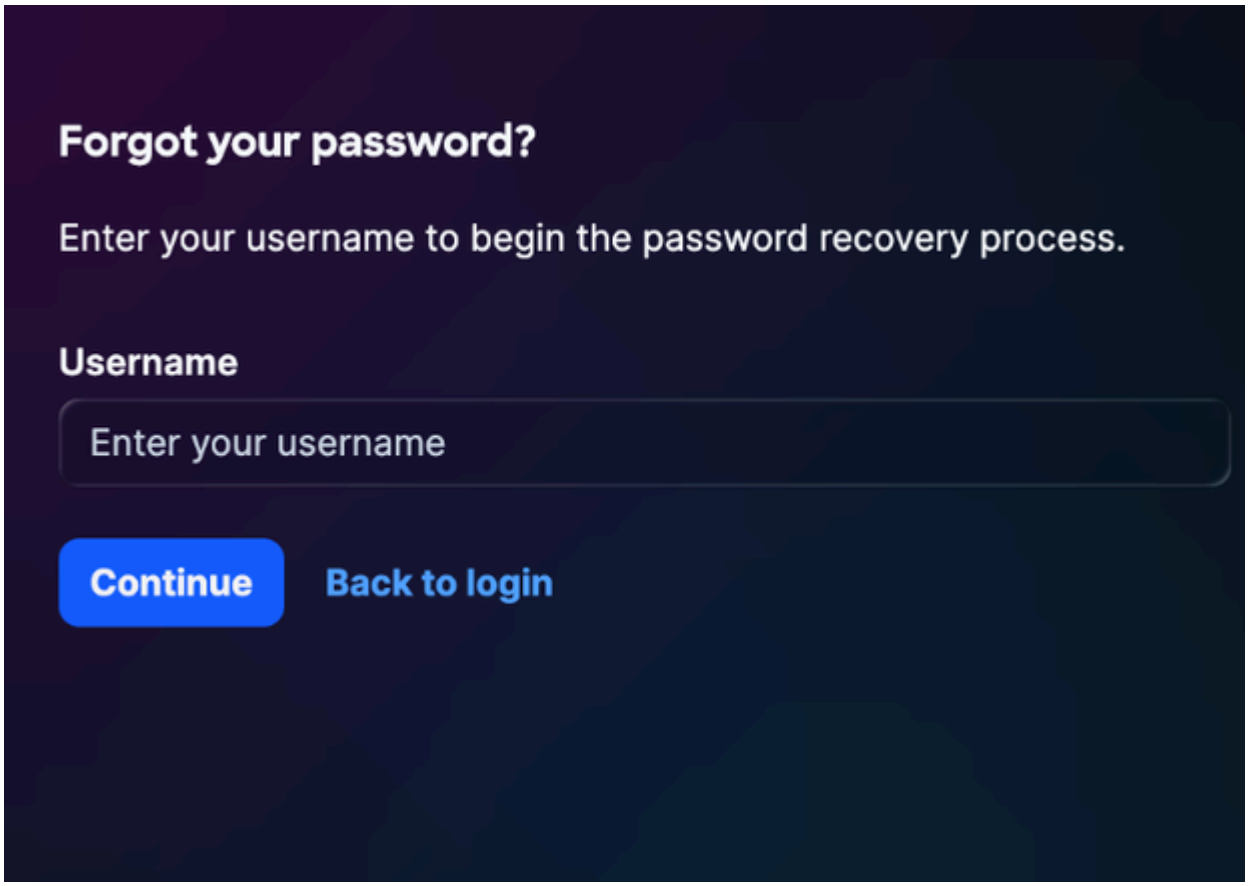
The password is updated in the Cisco IQ system, including the Cisco IQ Virtual Machine (VM).

#### Resetting a Forgotten Password

You can reset a forgotten password using the security question verification process, if you have set up the security questions earlier. See Setting Up Security Questions and Answers for more details.

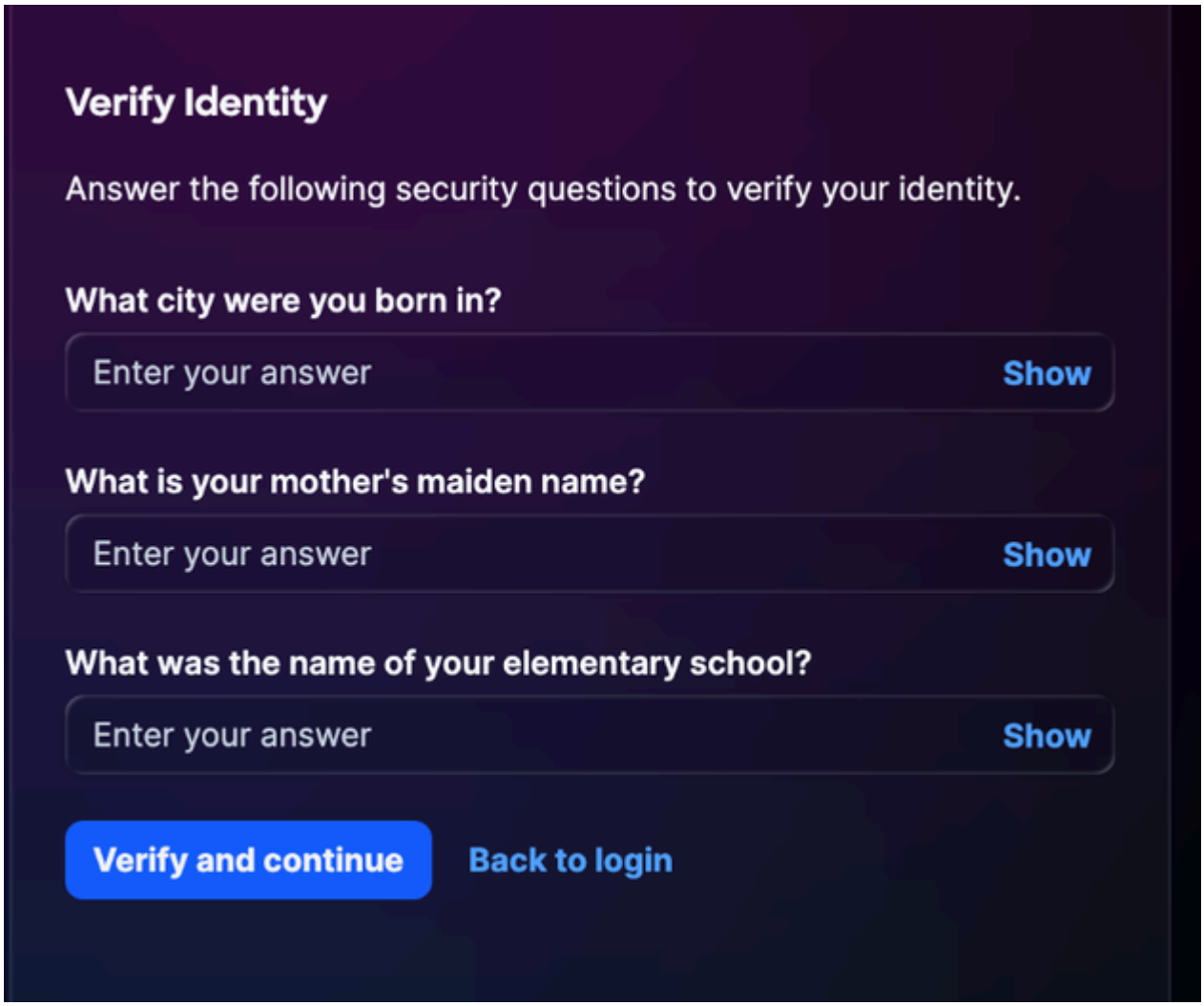
To reset a forgotten password:

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




*Forgot Password*

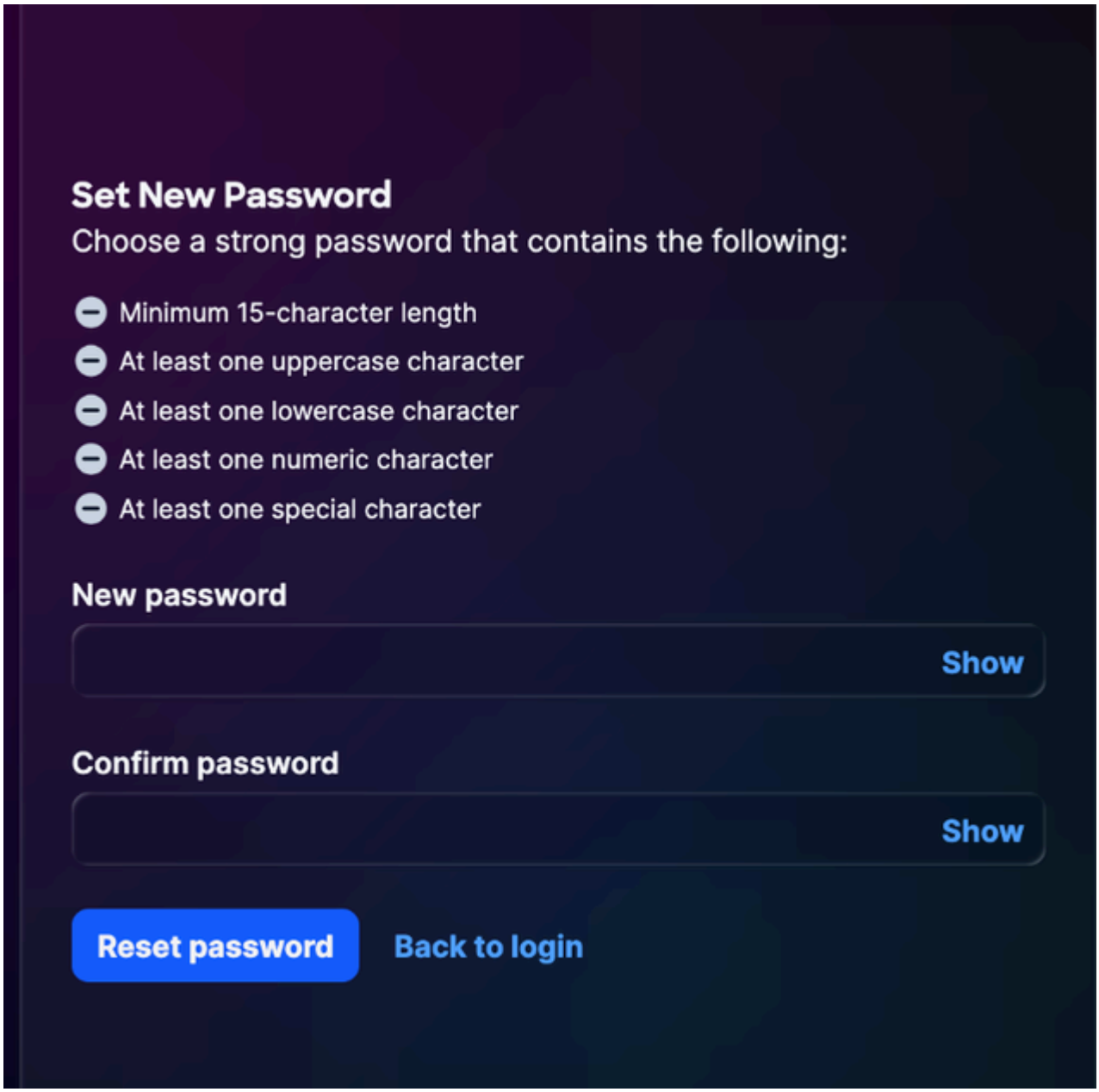
3. Enter the **Username**.
4. Click **Continue**. The **Verify Identity** page displays three (3) random security questions out of the five (5) questions that were previously configured.




*Verify Identity*

**Note**: The security questions displayed above are user-specific and will vary accordingly.

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 answer the security questions correctly within a ten (10) minute period. If all three (3) attempts are unsuccessful, your account temporarily locks for 60 minutes to protect your security.

You cannot reset your password during the lockout period. The system displays the message: "Account locked due to too many failed verification attempts. Please try again later.", including the time the lockout expires.

Your account automatically unlocks after 60 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**.

# Configuring Identity Provider

Once logged in to Cisco IQ Link, Administrators can configure various settings. Administrators can log in to Cisco IQ Link using local administration or Identity Provider (IDP) configuration.

## Okta IDP SAML Configuration for SSO

### Prerequisites to Configure IDP SAML

- Local Administrator access to Cisco IQ Link
- 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.
2. Set the following attributes for the Cisco IQ Link instance.

Cisco IQ Link 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" |

SAML Configuration Parameters

| **Parameter** | **Configuration** | **Example** |
|---|---|---|
| Audience (Entity ID) | FQDN name | mymanagementhost.mydomain.com |
| Single Sign-On URL | SAML ACS endpoint | https://mymanagementhost.mydomain.com/saml/acs |
| Name ID Format | Email Address | NA |
| Application Username | Username | NA |

3. Configure the following mandatory 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**: .*

4. Configure the Single Logout (SLO) settings in the application.

SLO Configuration Settings

| **Field** | **Value** |
|---|---|
| Signature | For Okta, this certificate is required only if you choose to enable SLO. Download the |

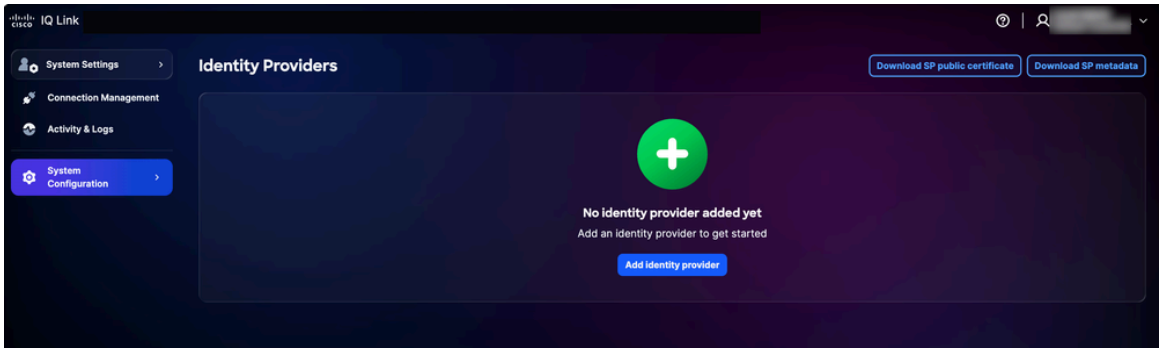
| Field | Value |
|---|---|
| Certificate | Signature Certificate using the **Download SP Certificate** in **Identity Providers**. Save the file as *sp-public-key.crt*. See Single Logout Configuration for more details. |
| SP metadata | The SP metadata is required for ADFS IDP only (and not for Okta). |
| 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 |

5. Click the **Download** icon to download the “SP Metadata” file.
6. Provision or create the application as required by the provider.

### Adding IDP

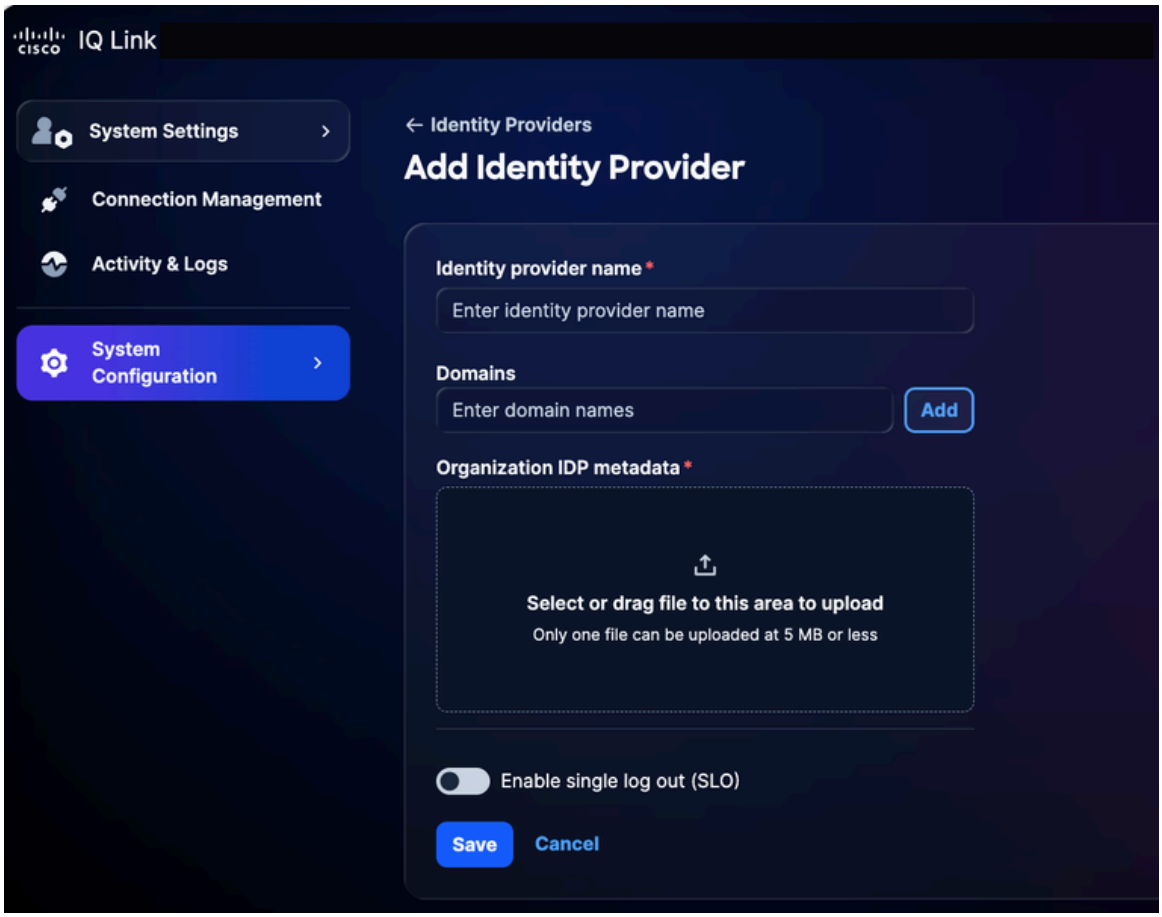
To add an IDP in Cisco IQ Link:

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




*IDP Home page*

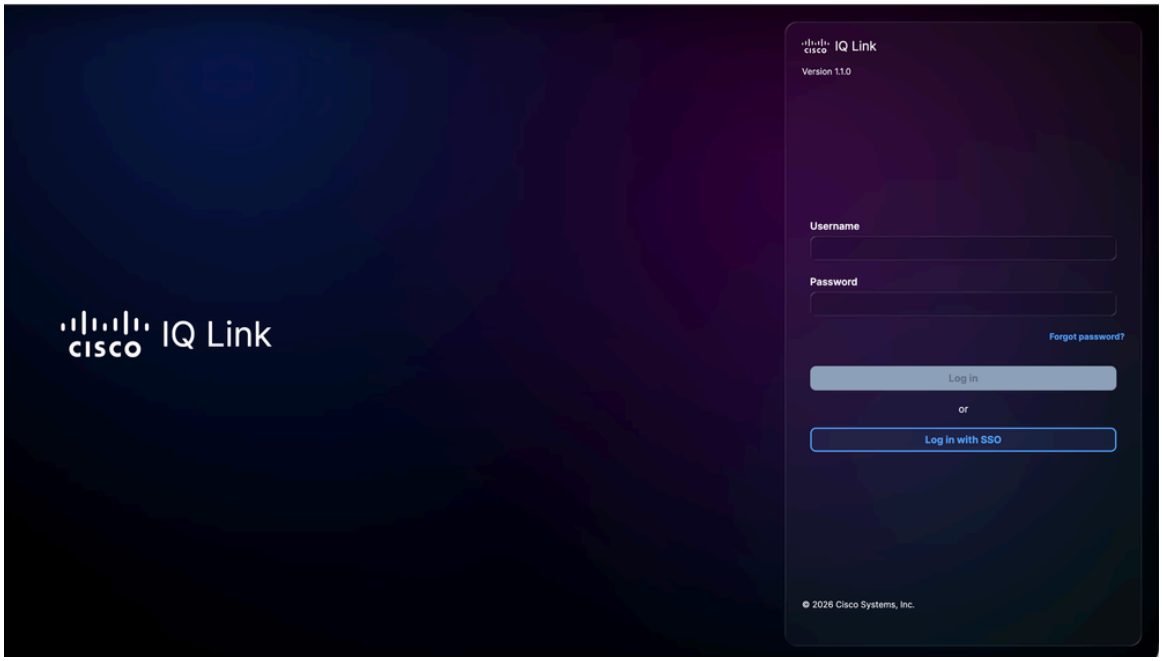
2. Click **Add Identity Provider**. The **Add Identity Provider** page displays.




*Add Identity Provider*

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

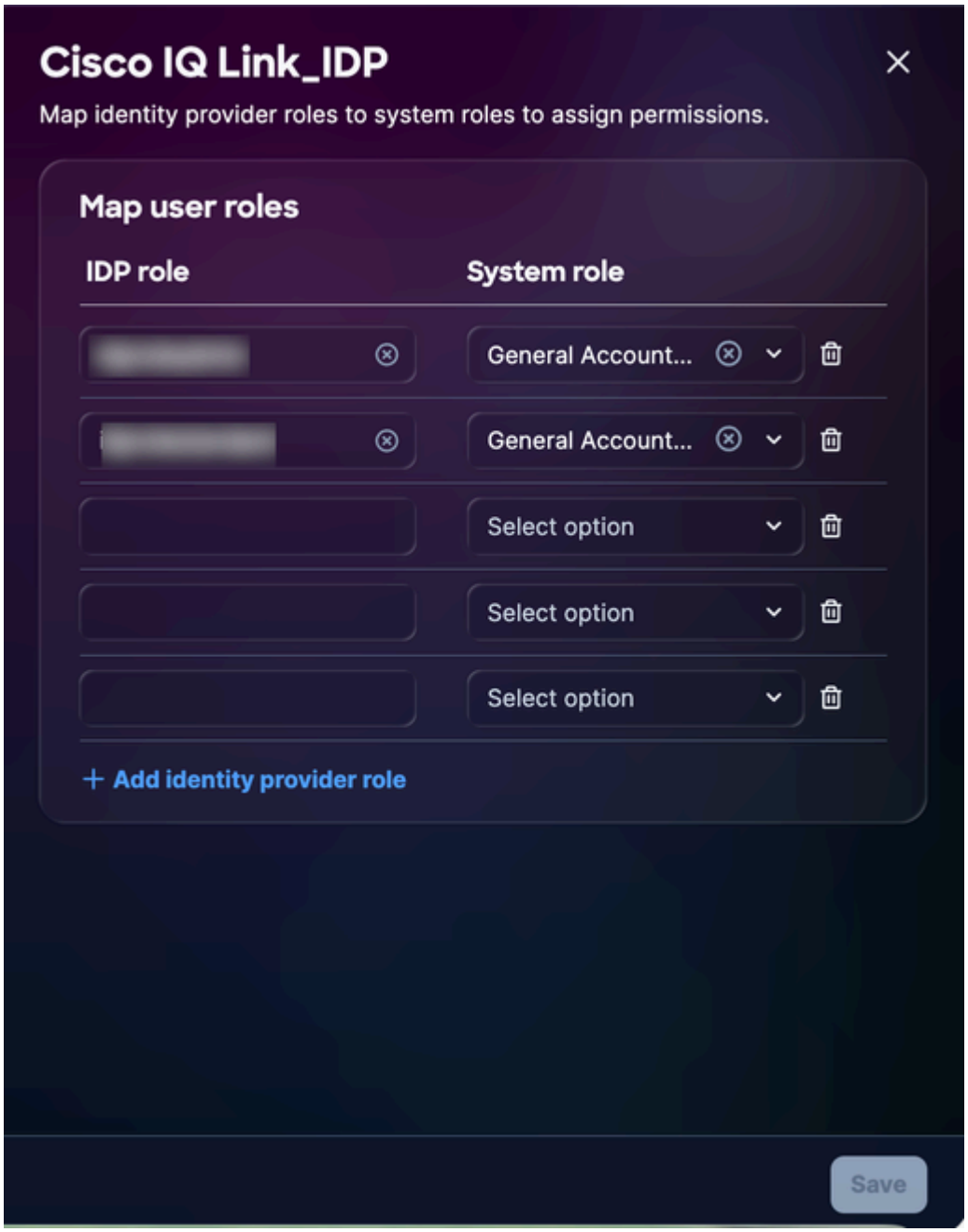
3. Enter the **Identity provider** name.
4. Click **Add** to add a Cisco IQ Link configured domain name to the **Domains** field.
5. Drag-and-drop or upload the SAML metadata file obtained from the IDP application in the **Organization IDP metadata** field. This file contains certificate details and Service Provider (SP) entity details.
6. (Optionally) Turn on the **Enable single logout** toggle button. You can enable the SLO later as well.
7. Click **Save**.
8. Once configured, the login page displays an option to log in with SSO (via IDP).




*Cisco IQ Link Login*

## Role Mapping Configuration

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




*User Role Mapping*

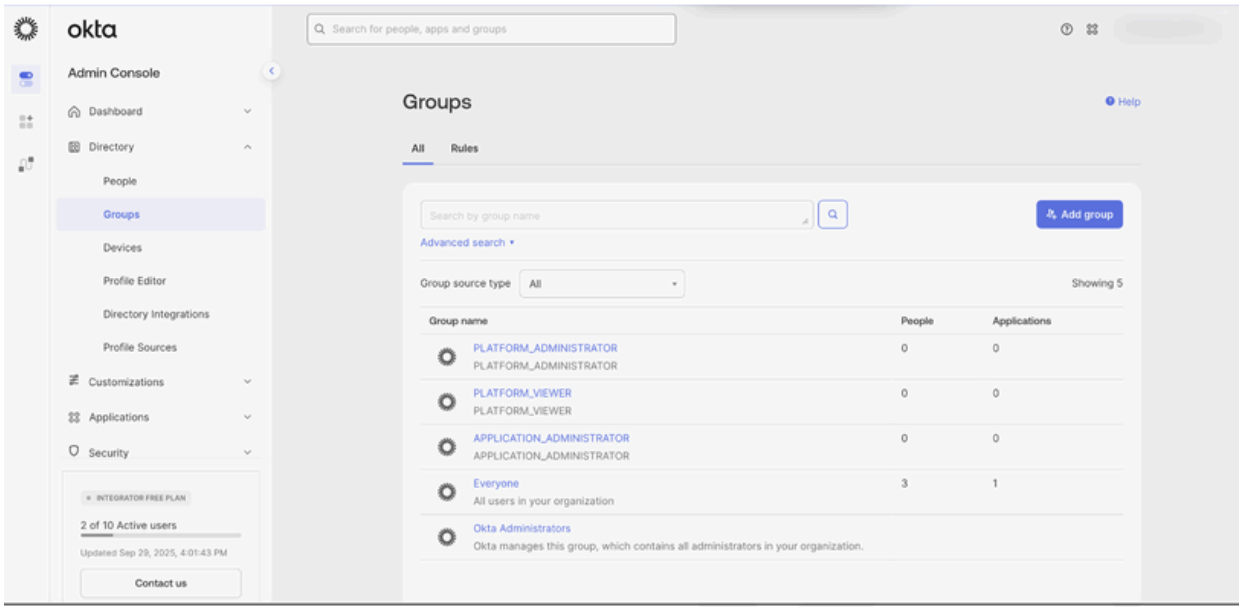
2. Enter an **IDP role** for the selected **System role**. The following system roles are supported:

    - **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.

---



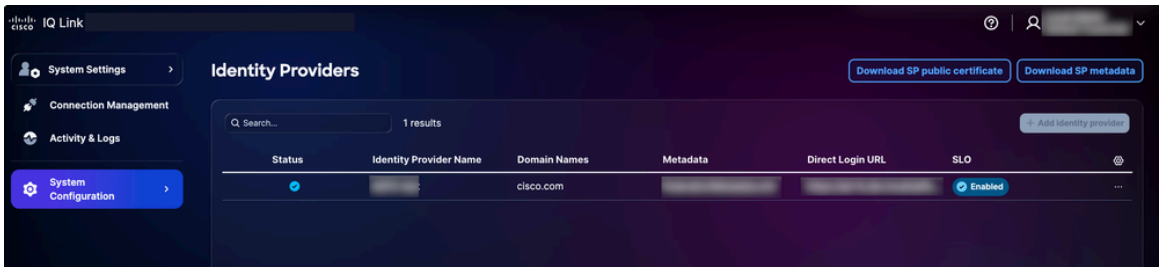

*Role Mapping Reference*

3. Map additional roles as required by clicking **Add identity provider role**.
4. Click **Save**.

### Single Logout Configuration

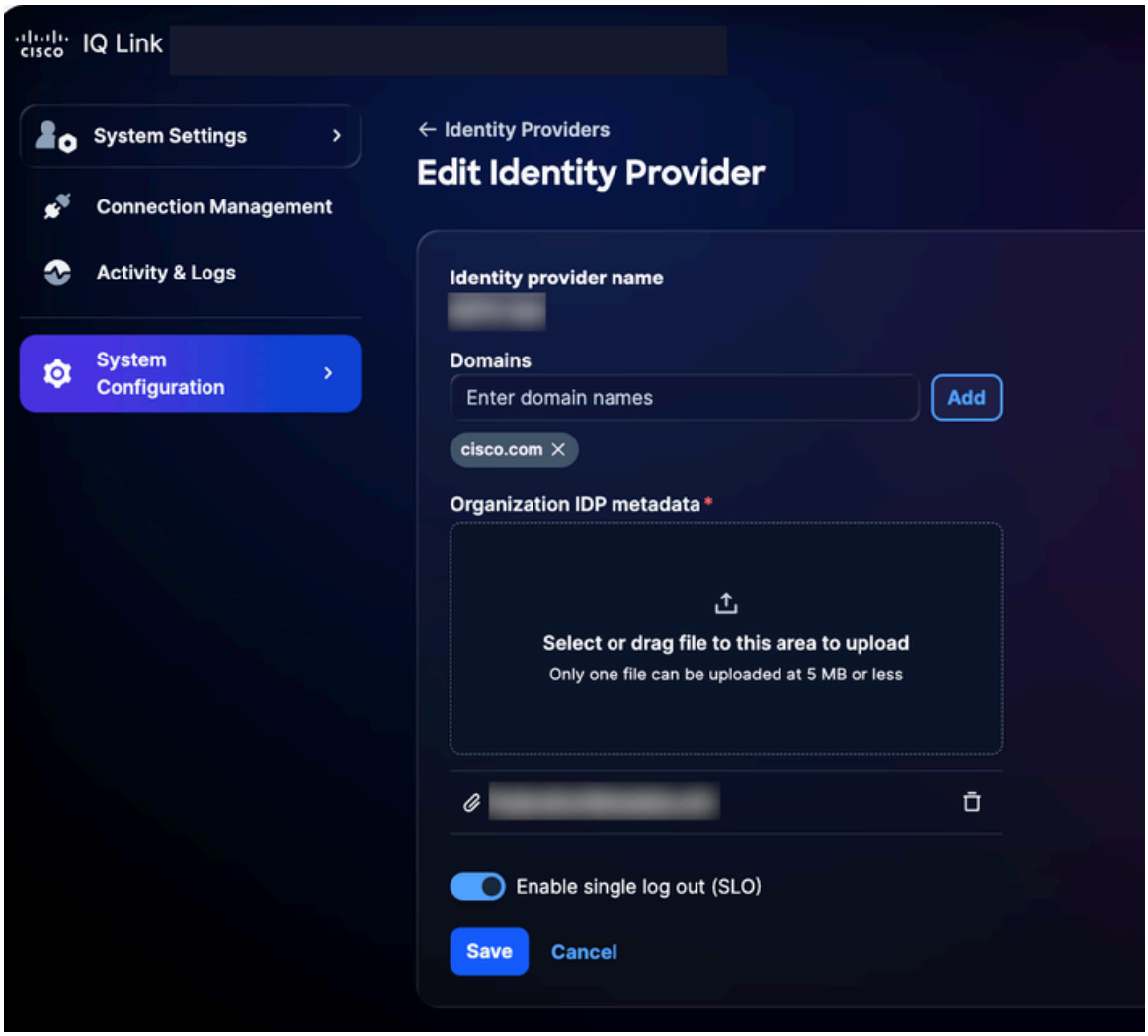
If you choose to enable SLO, you must upload metadata that includes the SLO URL. You can configure this by editing your Identity Provider settings and turning the toggle on for **Enable Single Log Out**. To complete SLO configuration:

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




*Download Public Certificate*

2. Save the download file as *sp-public-key.crt*.
3. Navigate to your IDP portal.
4. Upload the signature certificate file generated in the IDP SAML Configuration for SSO section.
5. Download the IDP metadata file again.
6. On the **Identity Providers** page, choose the added IDP's **More Options** icon > **Edit**.




*Edit Identity Provider*

7. Turn on the **Enable single log out (SLO)** toggle button.
8. Upload the newly downloaded meta data file.
9. 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/SLO flow is tested successfully

### Troubleshooting IDP Issues

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

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 Federation Services (ADFS) as the SAML IDP for Cisco IQ.

### Prerequisites to Configure ADFS IDP SAML for SSO

- ADFS 6.0+ is recommended
- Windows Server 2012 R2+
- Configured Active Directory integration
- SSL/TLS certificates on ADFS
- Administrator access to Cisco IQ
- Administrative access to ADFS server (Windows Server)
- PowerShell access on ADFS server

- Network connectivity between ADFS and Cisco IQ
- ADFS server configuration details (as listed in the table below)

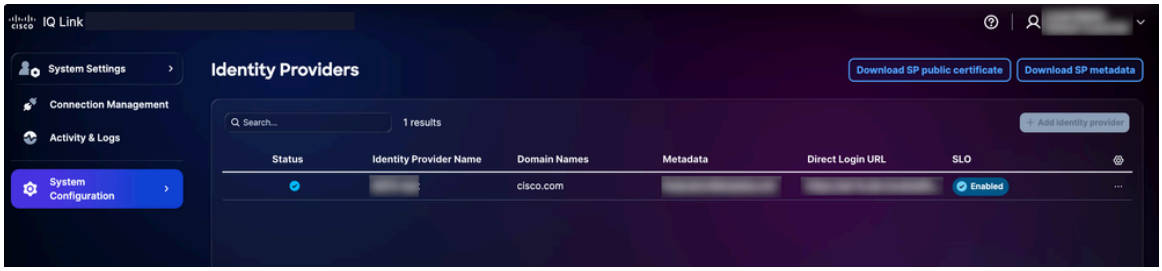
ADFS Server Configuration

| Item | Description | Example |
|---|---|---|
| **Cisco IQ FQDN** | User deployment hostname | devxx-23.cx-xxx-xxx.cisco.com |
| **ADFS Server URL** | User ADFS server address | https://ad-fs.dev.local |
| **Company Domain** | Email domain | company.com |
| **AD Groups** | Active Directory group Domain Names (DN) | CN=Role - CXIQ Developers |

**Configuring ADFS Servers**

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* directory (for example, C:-certificate.crt).
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.
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, “CIQ-Stage”), 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.

## 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.

Required Claims

| **Claim** | **Purpose** | **Source** |
|---|---|---|
| **Email** | User identifier | AD Mail |
| **Display Name** | User’s full name | AD Display Name |
| **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 - Stage”).

```
$relyingPartyName = “Cisco IQ - Stage”
```

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/windowsaccountname", Issuer == "AD
=> issue(store = "Active Directory", types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/em

@RuleName = "Transform Email to NameID"
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer = c.Issu

@RuleName = "Send Group Membership"
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD
=> issue(store = "Active Directory", types = ("http://schemas.xmlsoap.org/claims/Group"), query = ";mem
'@@
```

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

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

**Verifying User Groups**

1. Set the username to check user's group membership.

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

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.

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

Example Output:

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

### Configure 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 Certificate Authority that ADFS cannot validate via the standard chain-of-trust.

---

- Disable chain validation globally for this relying party

```
Set-AdfsRelyingPartyTrust `
    -TargetIdentifier “<sp_entity_id>” `
    -SigningCertificateRevocationCheck None `
    -EncryptionCertificateRevocationCheck None
```

OR

- Import the issuing CA certificate into the Trusted Root Certification Authorities store

```
Import-Certificate -FilePath “C:-iq-onprem-ca.cer” -CertStoreLocation “Cert:”
```

3. Apply the changes by restarting the ADFS service.

```
Restart-Service adfssrv
```

## 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 “Federation Metadata”}).FullUrl

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*.
2. Replace <your-adfs-server> with the hostname of your ADFS server.
3. Save the metadata XML file to your computer when prompted.

## 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 Active Directory to use for mapping. To find groups from Active Directory, 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”] }
```

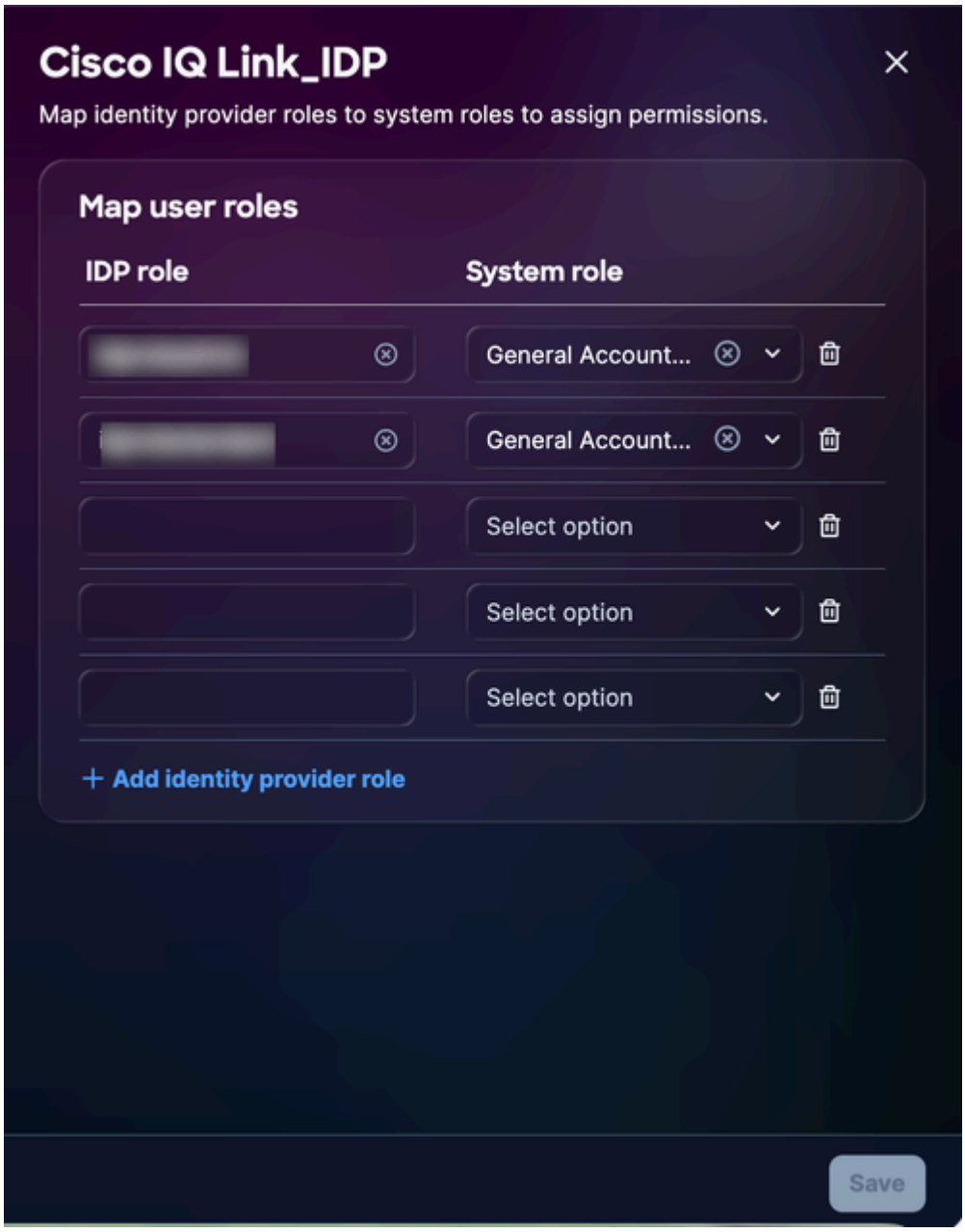
The system queries Active Directory directly via LDAP, requiring no additional modules. Group information is returned in full Distinguished Name (DN) format, for example:

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 Active Directory by an Administrator before you can complete the ADFS role mapping.

To configure role mapping:

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




*Role Mapping*

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 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 Domain Names.

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

**Verification and Testing**

#### Testing Authentication

1. In an Incognito or Private mode browser, navigate to *https://your-cisco-iq-domain.com/login*.
2. Log in using your Active Directory credentials in domain\username or user@domain.local format.
3. Verify that you are redirected to the **Cisco IQ Home** page (after successful authentication).
4. Confirm that the assigned roles display the correct parsed group names (for example, CXIQ Developers) in your user profile.

#### Testing Logout

To test logout, click **Log out from Cisco IQ**. The “Logging out, please wait…” message displays and you are redirected to the **Cisco IQ Login** page. The system also terminates the ADFS session. If you try to access ADFS directly, you are prompted to log in again.

### 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.

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<br>• **Wrong group attribute**: Must be http://schemas.xmlsoap.org/claims/Group<br>• User is not in AD groups |
| **Decryption Failed** | "Failed to decrypt assertion" in logs | Check configuration on ADFS certificate configuration |
| **Login Loop** | Stuck in authentication or login loop | • **Invalid ACS URL**: Verify: *https://your-fqdn/saml/acs*<br>• **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/FederationMetadata.xml
```

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

```
Get-AdfsRelyingPartyTrust -Name “Cisco IQ - Stage” | 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

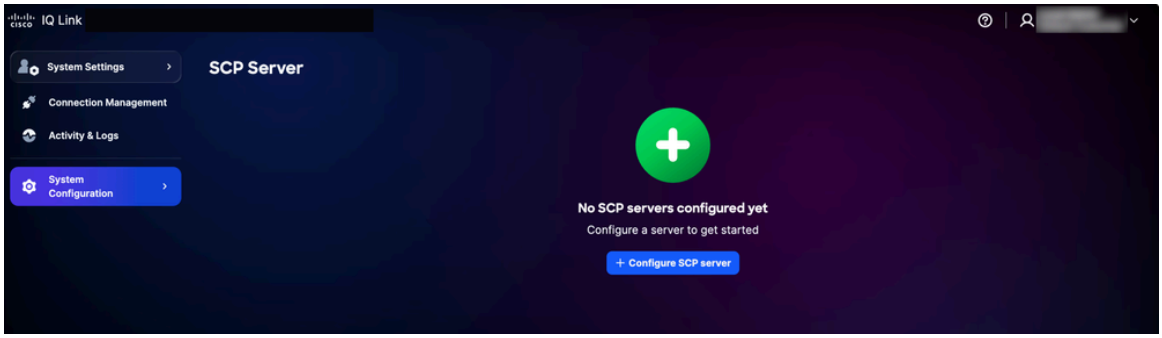
```
Get-AdfsRelyingPartyTrust -Name “Cisco IQ - Stage” | Select-Object SamlEndpoints
```

# Adding SCP Servers

This Secure Copy Protocol (SCP) server is a prerequisite for importing upgrade files that are essential for adding, upgrading, or fixing the Cisco IQ installation.

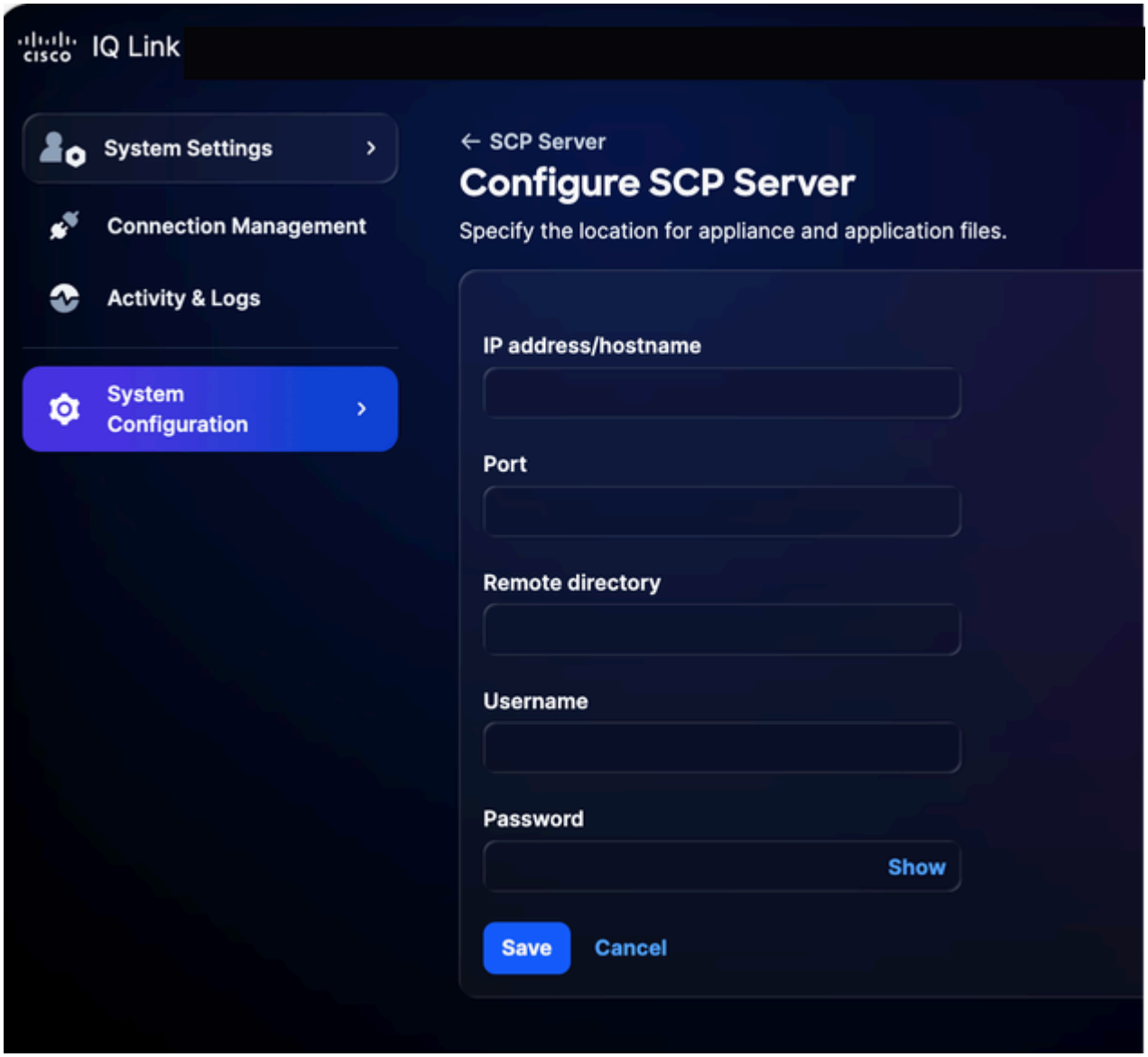
To add a SCP Server:

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



*SCP Server Home page*

2. Click **Configure SCP Server**.




*Configure SCP Server*

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

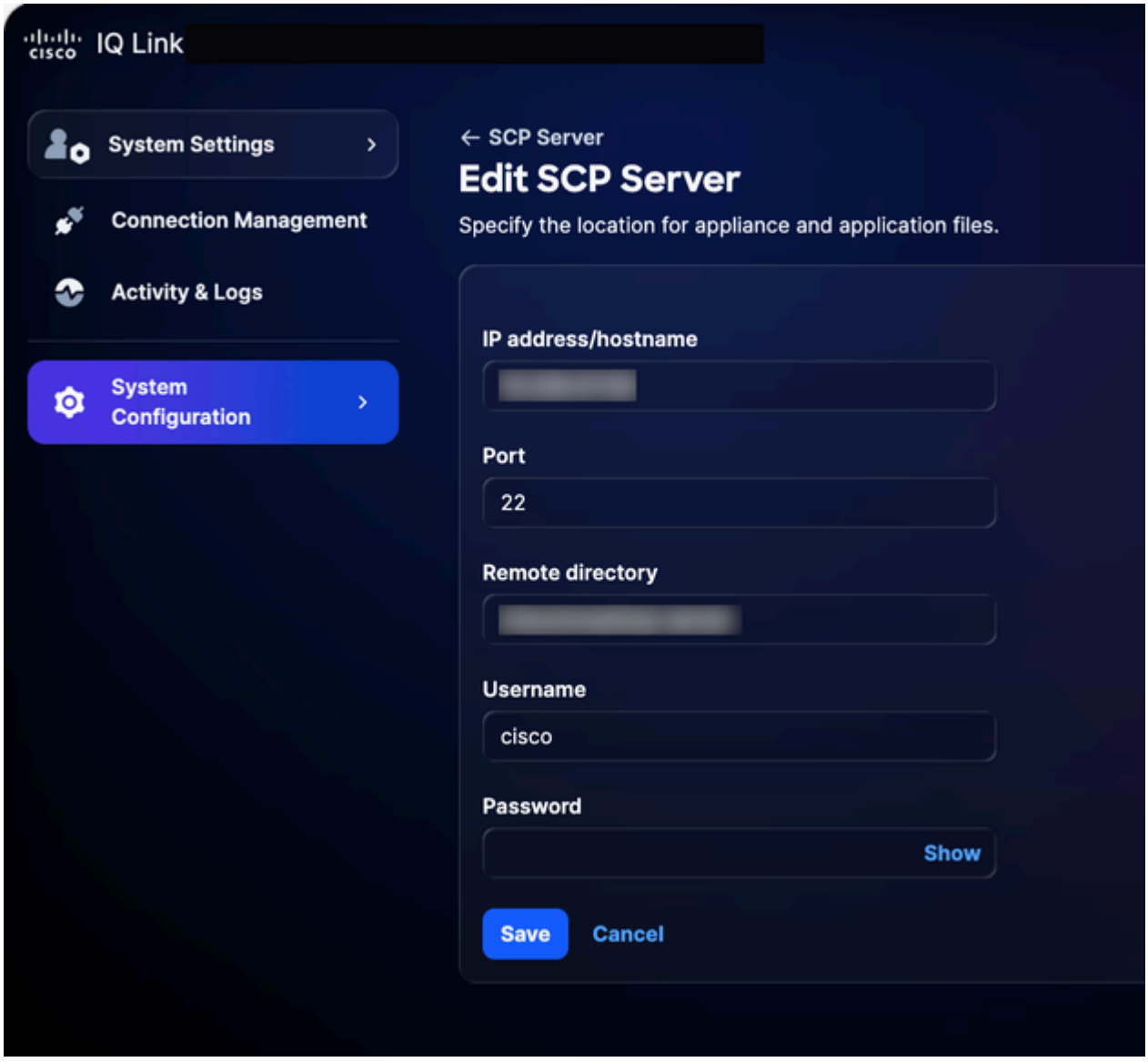
## Editing Existing SCP Servers

To edit an existing SCP server:

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


*SCP Server*

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




*Editing SCP Server*

3. Modify details as required.

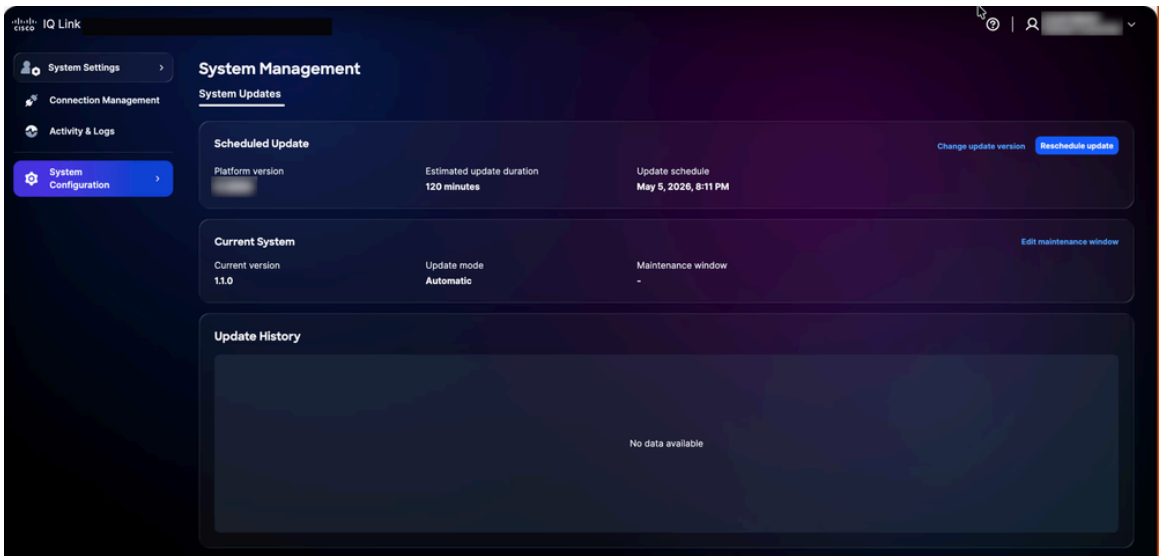
4. Click **Save**.

# System Management

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

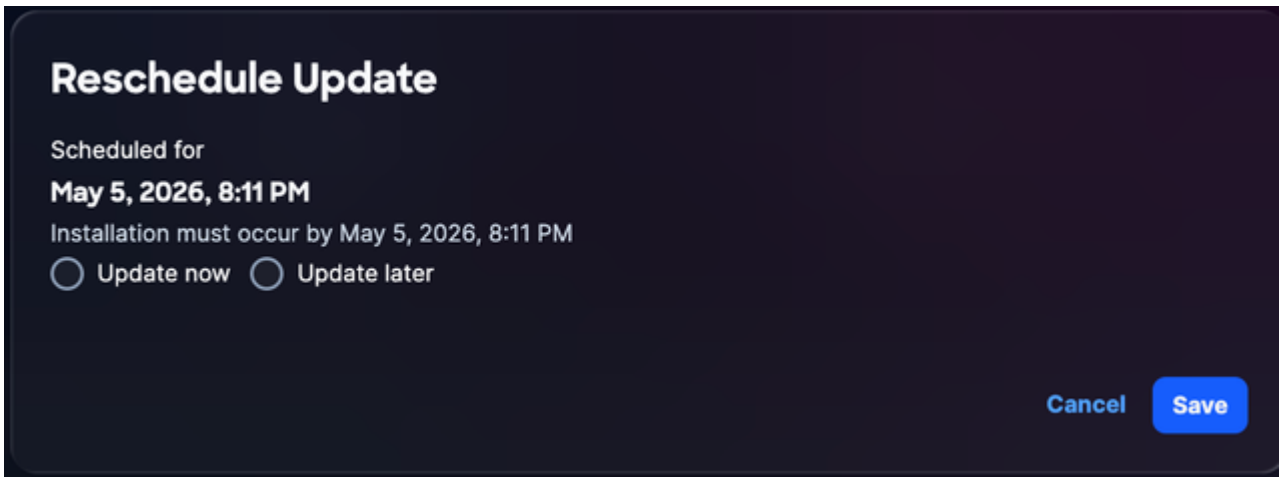
To reschedule the system update:

1. From **Administration**, 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*

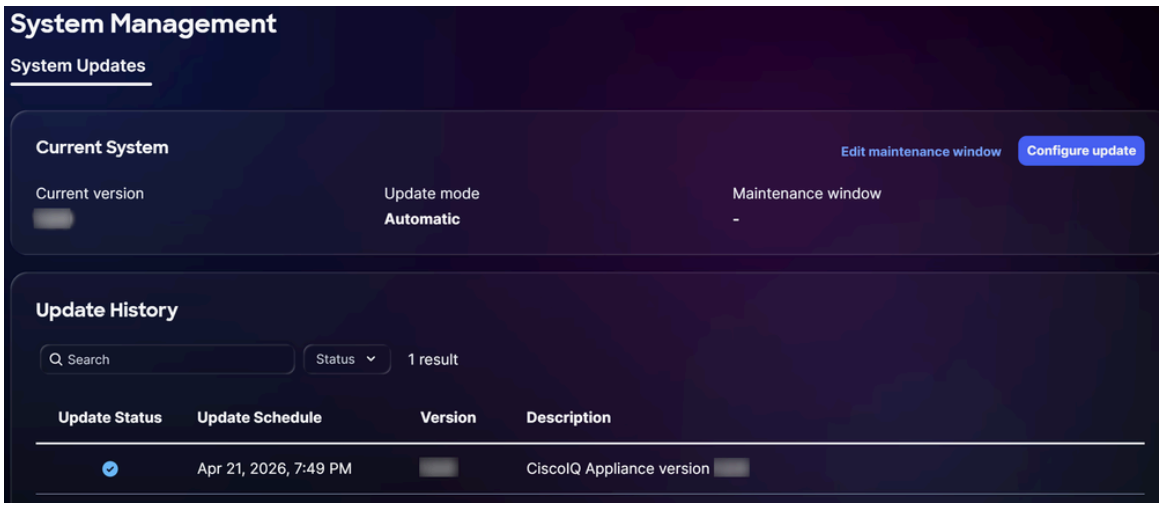
2. Click **Reschedule update**.




*Reschedule Upgrade*

3. Click **Update Now** for immediate rescheduling or **Update Later** to schedule another time.

4. Click **Save**. A confirmation displays and you are redirected to the **System Update** Home page.




*Successful Upgrade*

# SSL Certificates Configuration

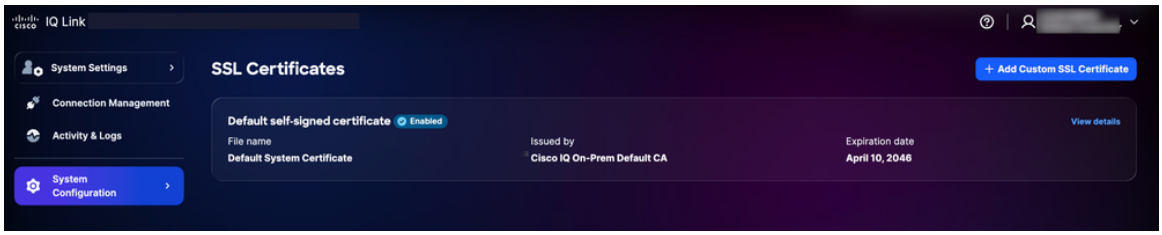
A default self-signed certificate is pre-installed and enabled in Cisco IQ, but users can upload custom SSL certificates. When a custom SSL certificate is enabled, it is used for HTTPS connections; if the certificate is disabled or deleted, the system automatically reverts to the default certificate.

**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, the customer must upload the new SSL as outlined in the Completing SLO Configuration section for the Okta IDP or the ADFS IDP.

## Adding Custom SSL Certificate

To add a custom SSL certificate:

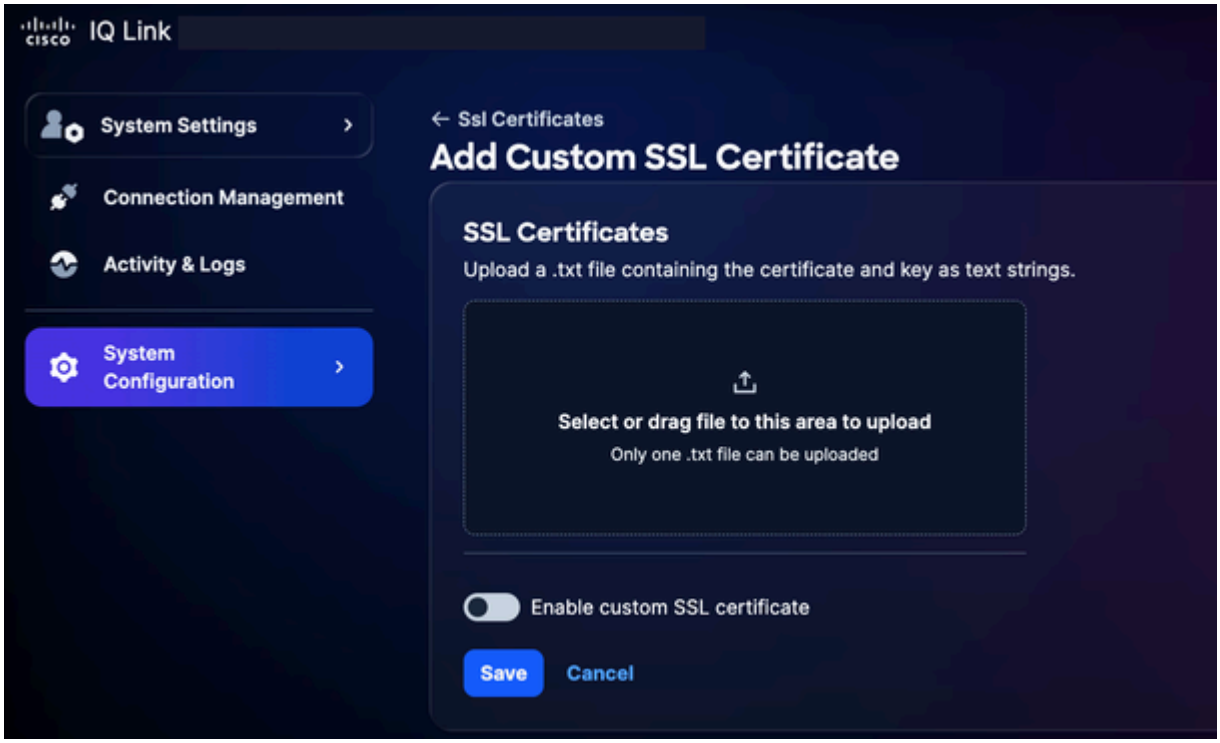
1. From **System Settings**, choose **System Configuration** > **SSL Certificates**. The **SSL Certificates** page displays, listing all SSL certificates for your system.




*Adding SSL Certificate*

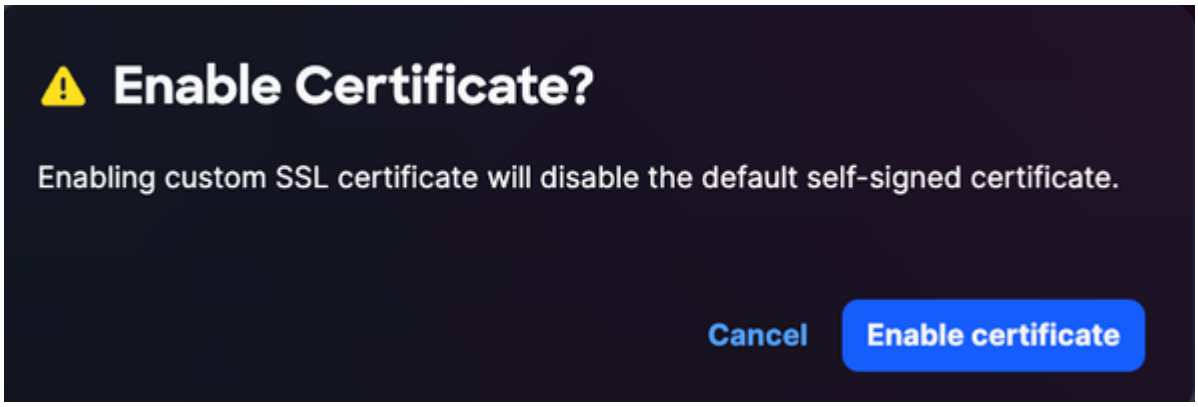
2. Click **Add Custom SSL Certificate**.

**Notes**:
• 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 Certificates*

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




*Enable Certificate*

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

5. Click **Enable certificate**.

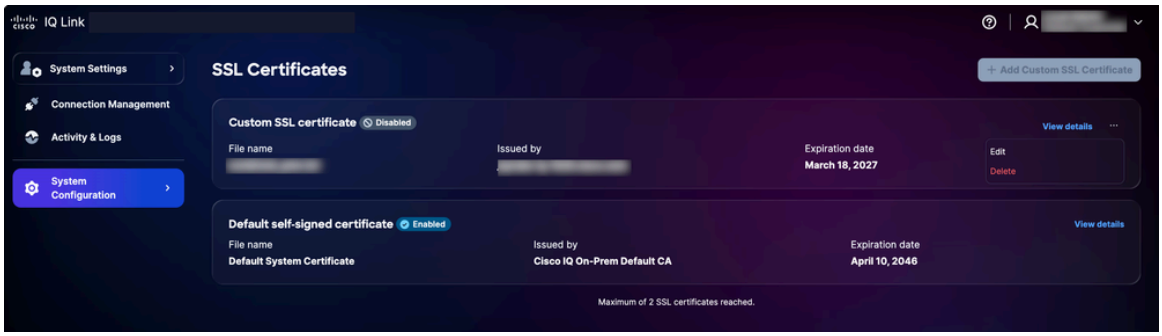
6. Click **Save**.

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

## Editing Custom SSL Certificates

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.




*Edit SSL Certificate*

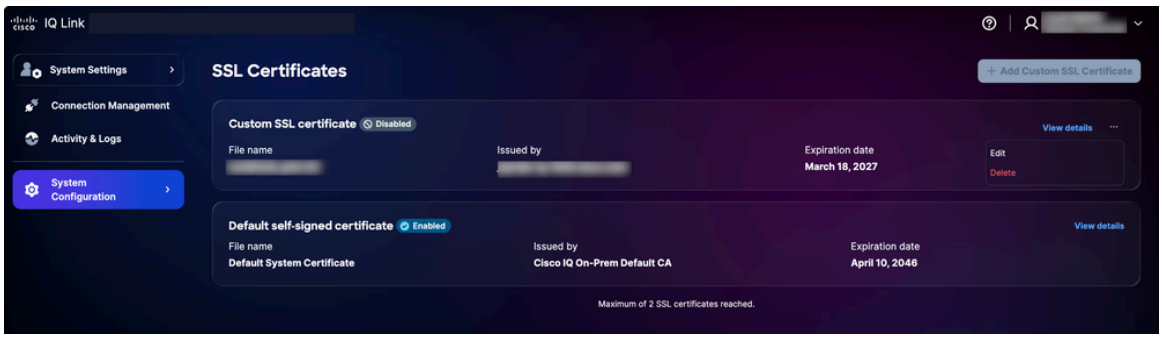
2. Choose the **More Options** icon > **Edit**. The **Edit SSL Certificate** page displays.
3. Edit the certificate details as required.
4. Click **Save**.

## Deleting Custom SSL Certificates

**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.



*Delete 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 Administrator role can configure external syslog servers to export system logs. Up to two (2) syslog servers can be configured.

---

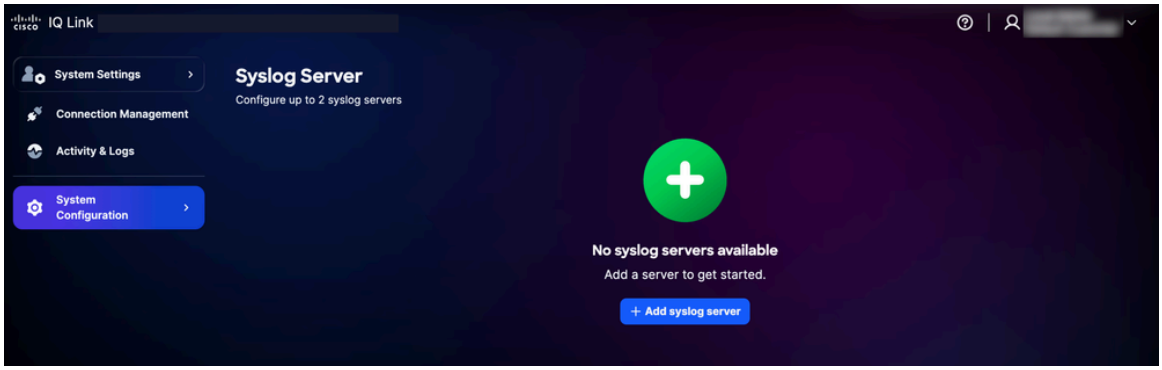
**Note**: The Syslog server must be specified as an IP address, not a Fully Qualified Domain Name (FQDN).

---

## Adding Syslog Servers

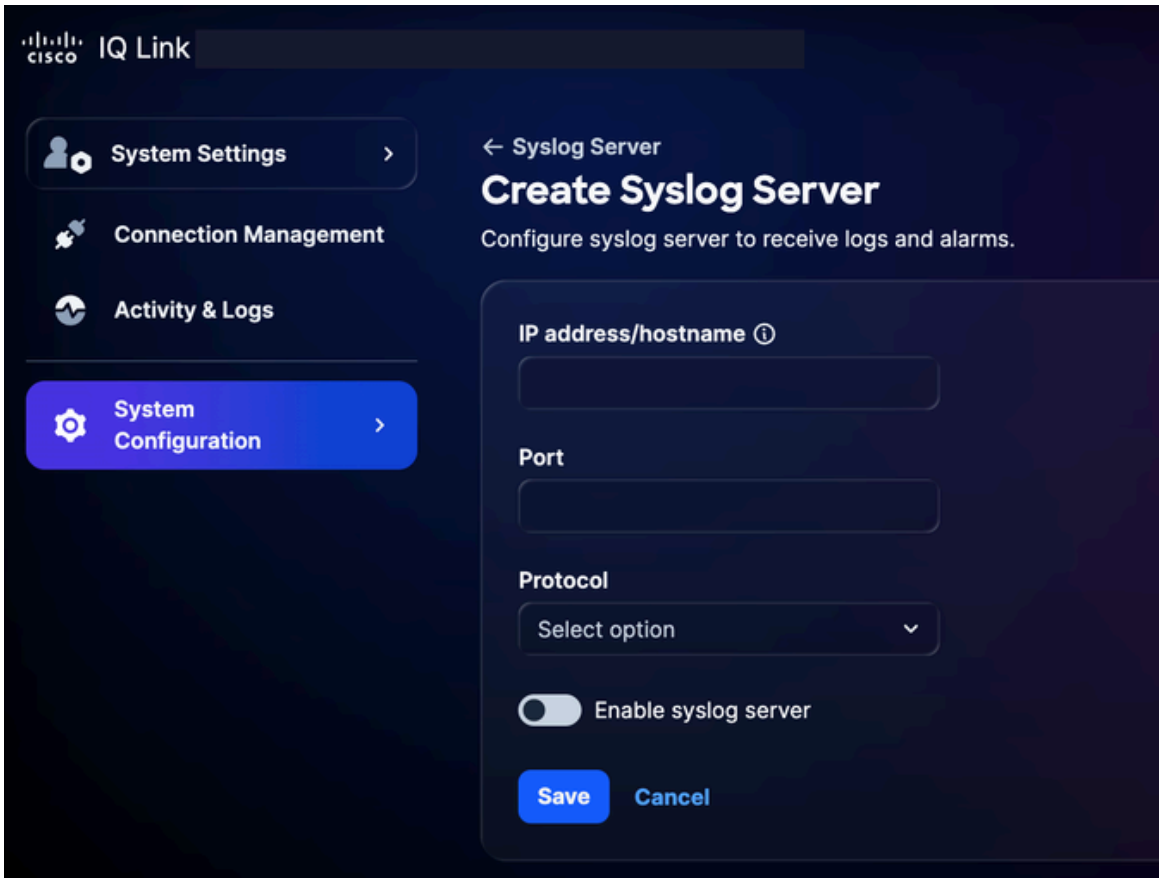
To add a syslog server:

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.



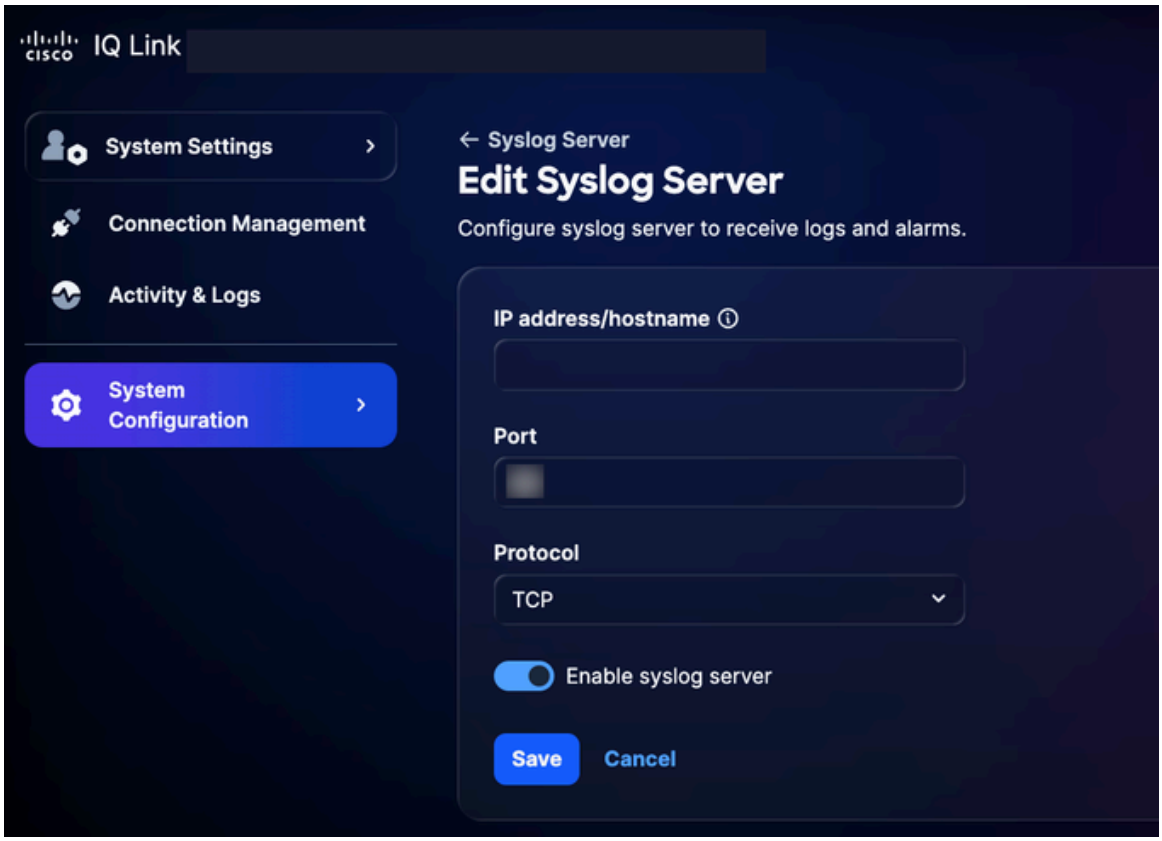

*Create Syslog Server*

3. Enter the **IP address/hostname**.
4. Enter a **Port** number.
5. Select the applicable protocol from the **Protocol** drop-down list (for example, UDP or 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 home page.

## Editing Configured Syslog Servers

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.



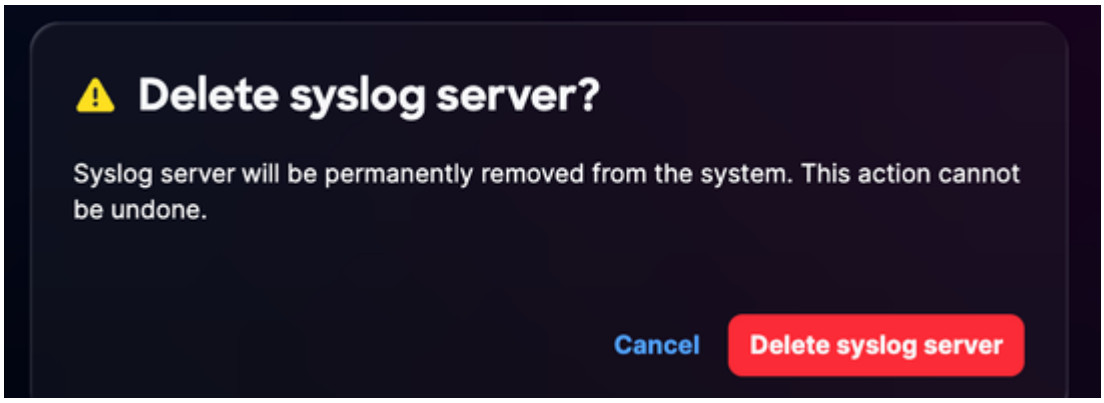

*Edit Syslog Server*

3. Edit details or turn off the **Enable syslog server** toggle, as required.
4. Click **Save**.

## Deleting Configured Syslog Servers

To delete a configured syslog server:

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

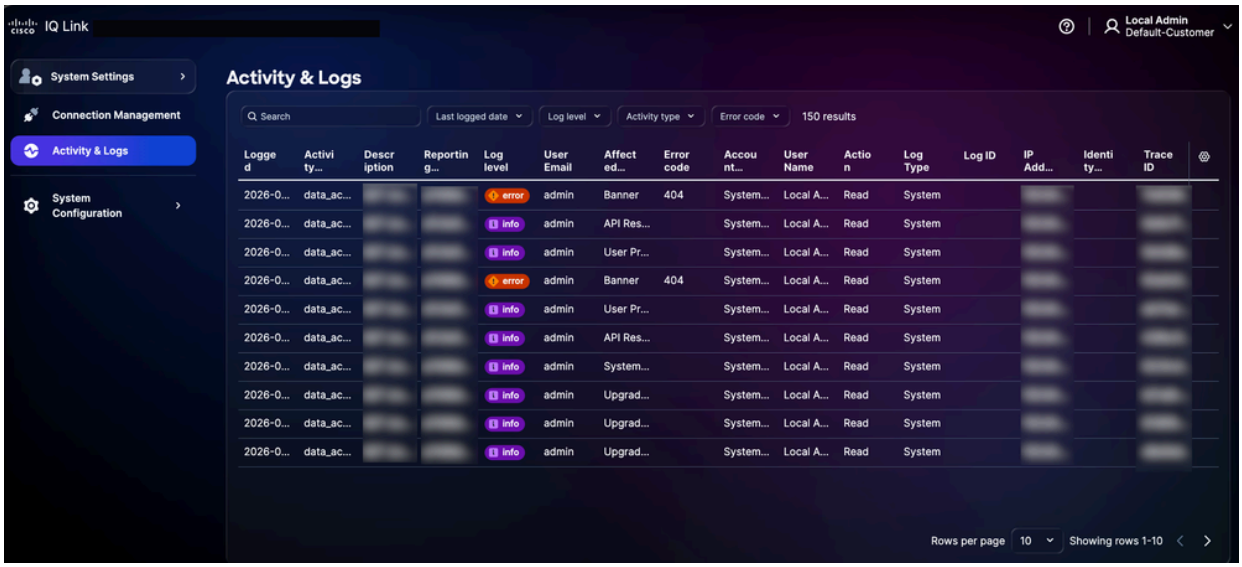



*Confirmation*

3. Click **Delete syslog server**.

# Activity & Logs

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




*Activity and Logs*

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

Activity and Logs:

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

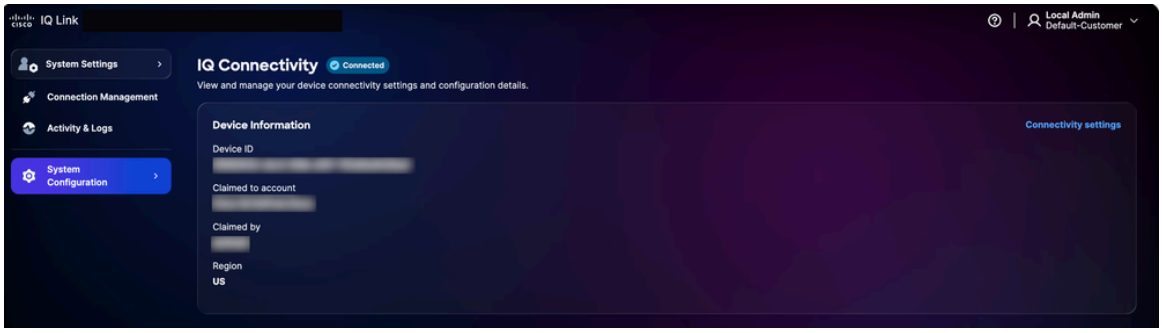
The following filter options are available:

- **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 logs for a specific error code

# IQ Connectivity

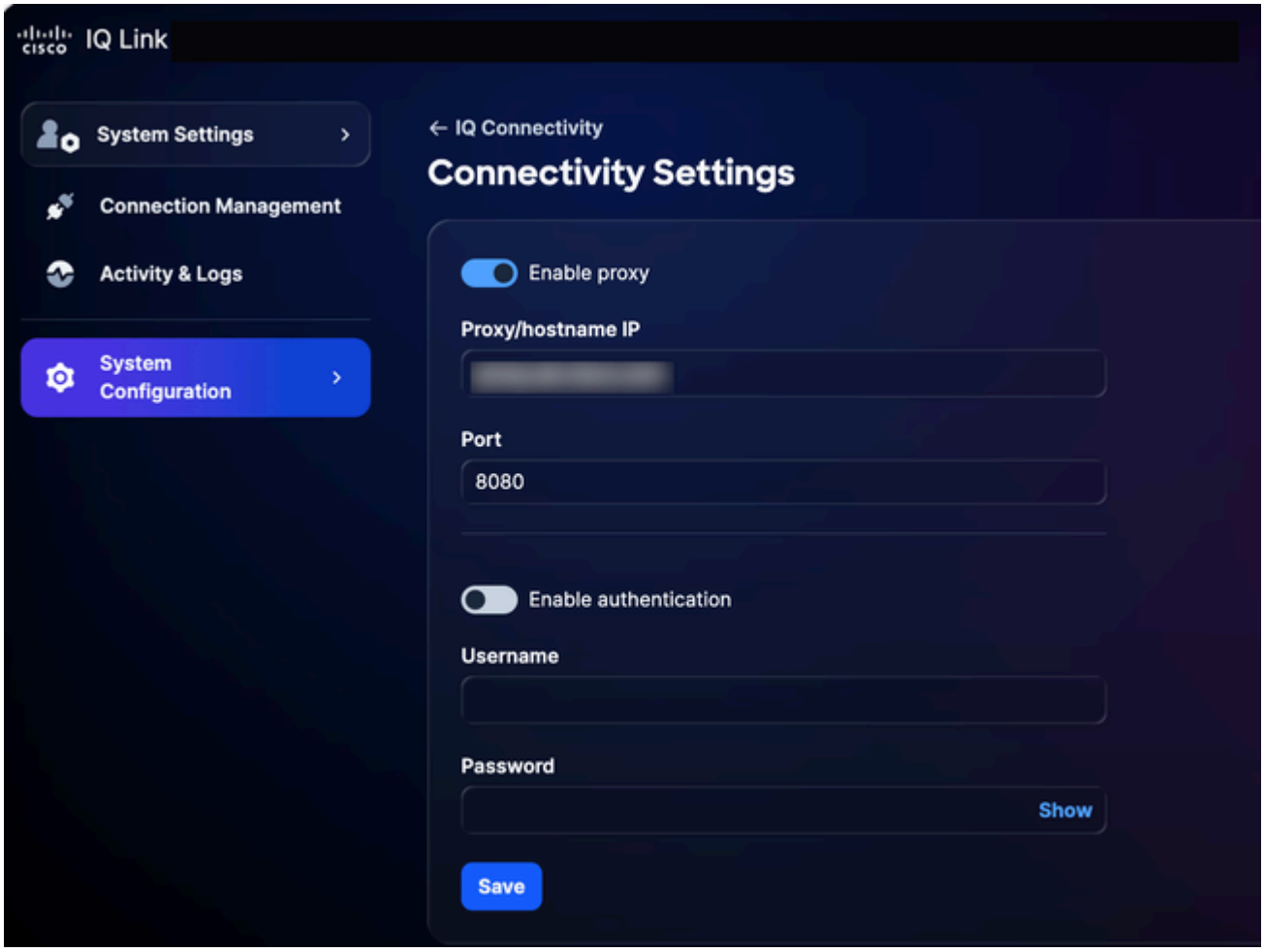
To view and manage your device connectivity settings and configuration details:

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




*IQ Connectivity*

2. Click **Connectivity settings**.




*Connectivity Settings*

3. Update details as required.

4. Click **Save**.

# Connection Management (Data Collection)

Cisco IQ Link is an on premises deployed solution for network data collection, designed 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 can be summarized as shared below:

- **Creating Credential Sets**: Establish the authentication protocols (for example, 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.

---

**Note**: Cisco IQ Link requires a user account configured with privilege level 15 on the device to authenticate directly connected assets.

---

- **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.

---

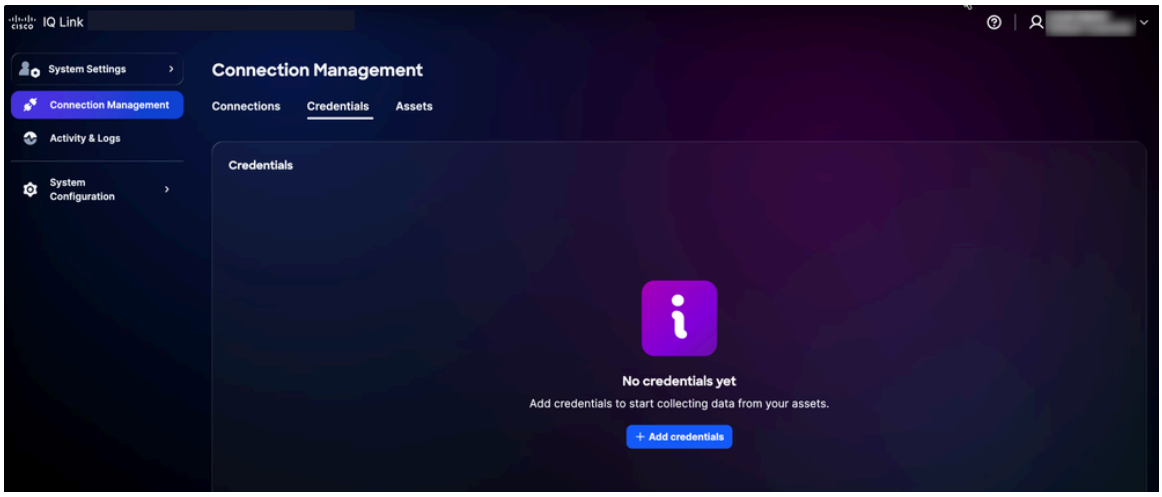
**Note**: SNMPv2c/SNMPv3 and SSH are required for device discovery and HTTP/HTTPS credentials must be provided before configuring Catalyst Center.

---

## Adding Credentials

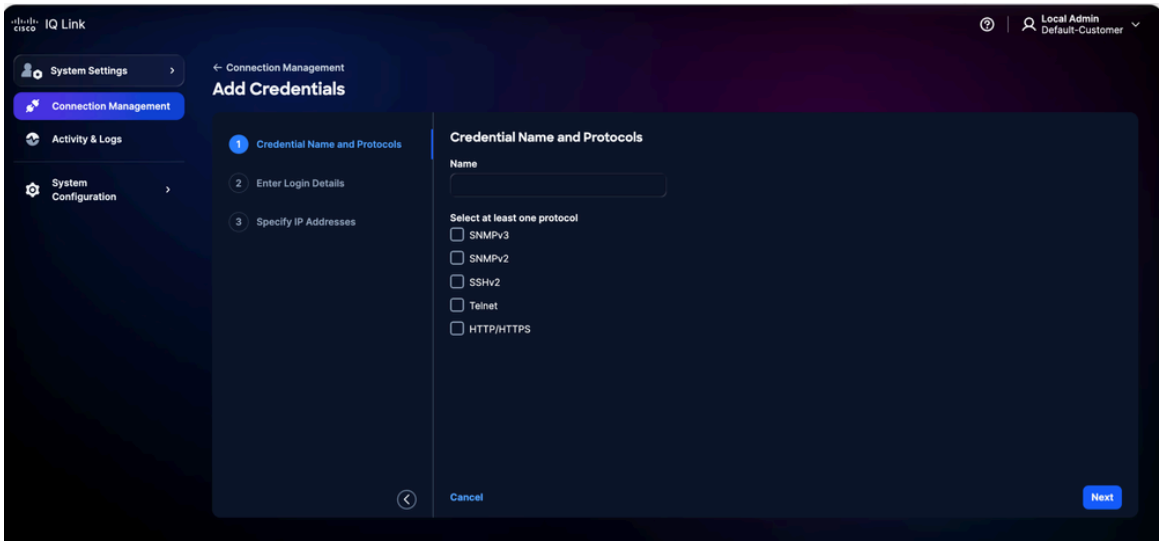
You must first add credentials to perform data collection. To add credentials:

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




*Credentials Tab*

3. Click **Add credentials**.

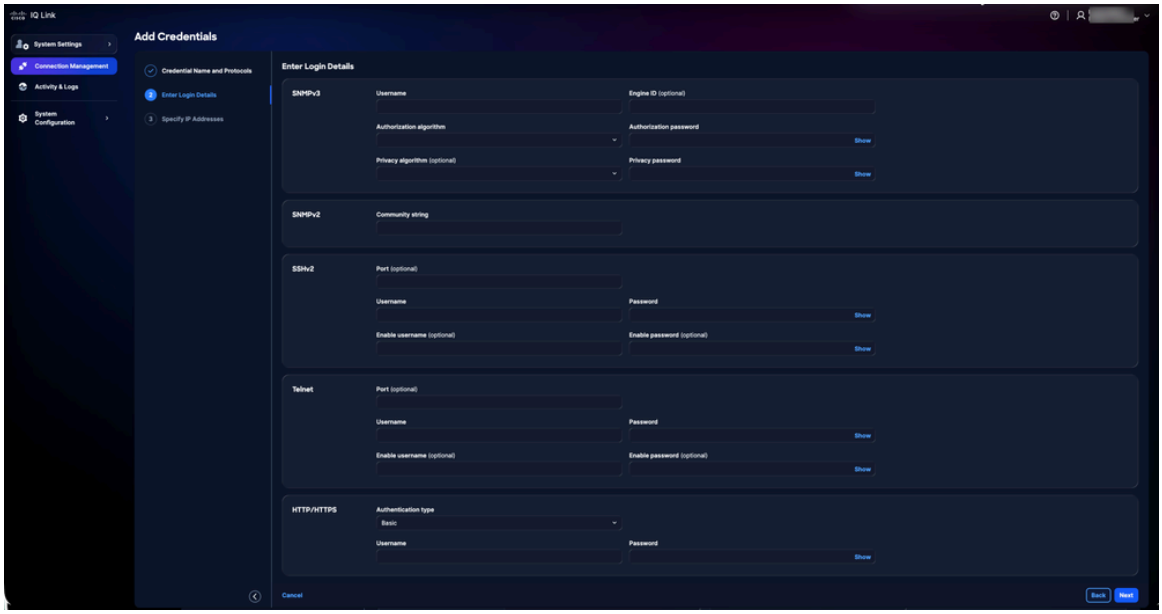



*Add Credentials*

4. Enter **Name**.

5. Check all applicable protocol check boxes.

6. Click **Next**.

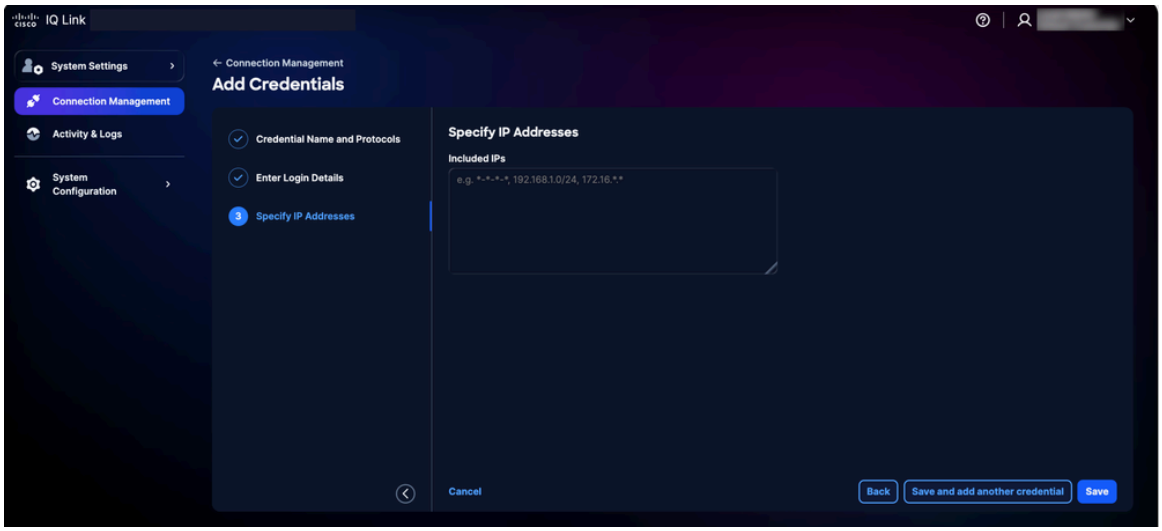



*Add Credentials Details*

**Note**: For the image above, we illustrate the view when all protocols are selected in the previous step. Your interface will display only the specific protocols you chose.

7. Enter the login details for each protocol that was selected.

8. Click **Next**.




*Specify IP Addresses*

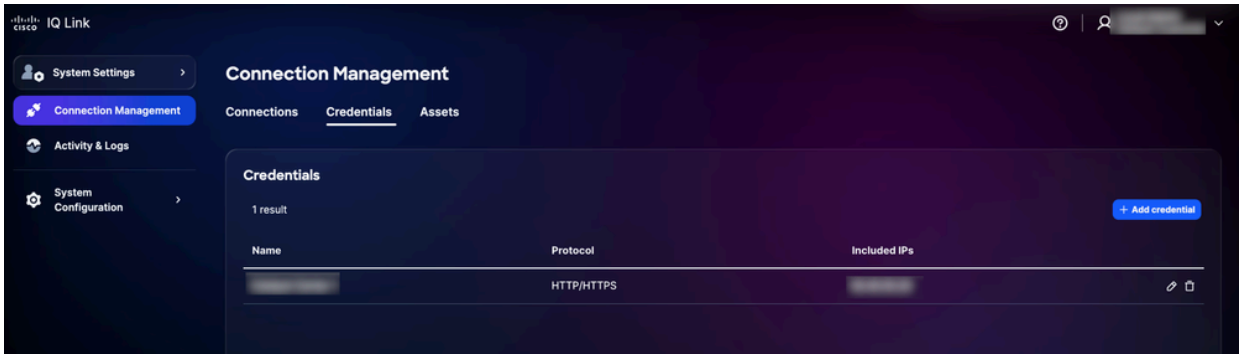
9. Enter the **Included IPs**.

---

**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 among wildcards)

    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.

Credential Selection Example

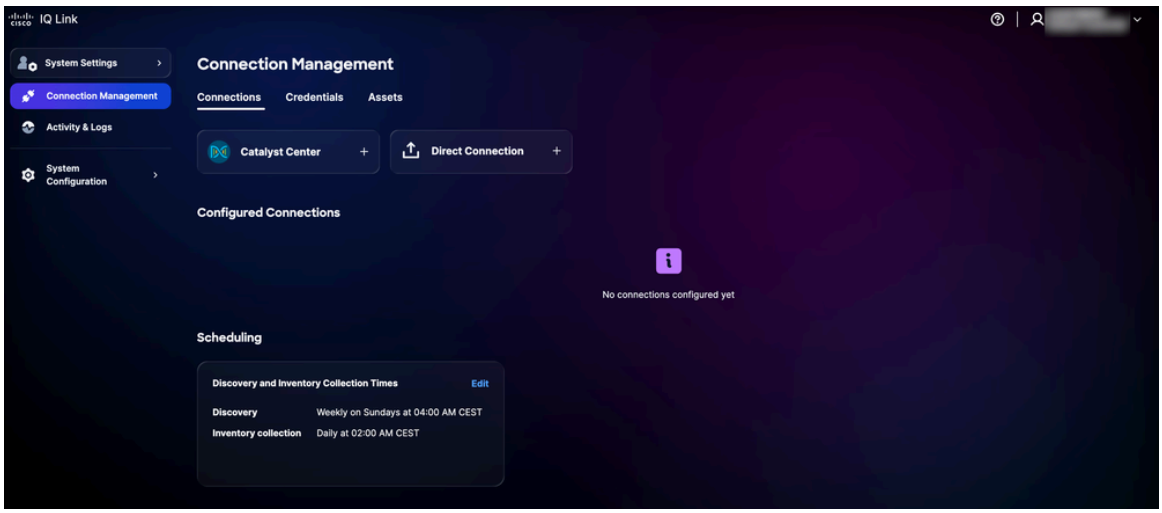
| **Device IP** | **Available Credential Sets** | **Selected Credential Set** |
|---|---|---|
| 10.10.1.5 | 10.10.1.5, 10.10.1., *10.10.*.* | 10.10.1.5 (Exact Match) |
| 10.10.2.15 | 10.10.2., *10.10.*.* | 10.10.2.* (More specific) |
| 10.10.5.50 | 10.10.., ... | 10.10.. (More specific) |

**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

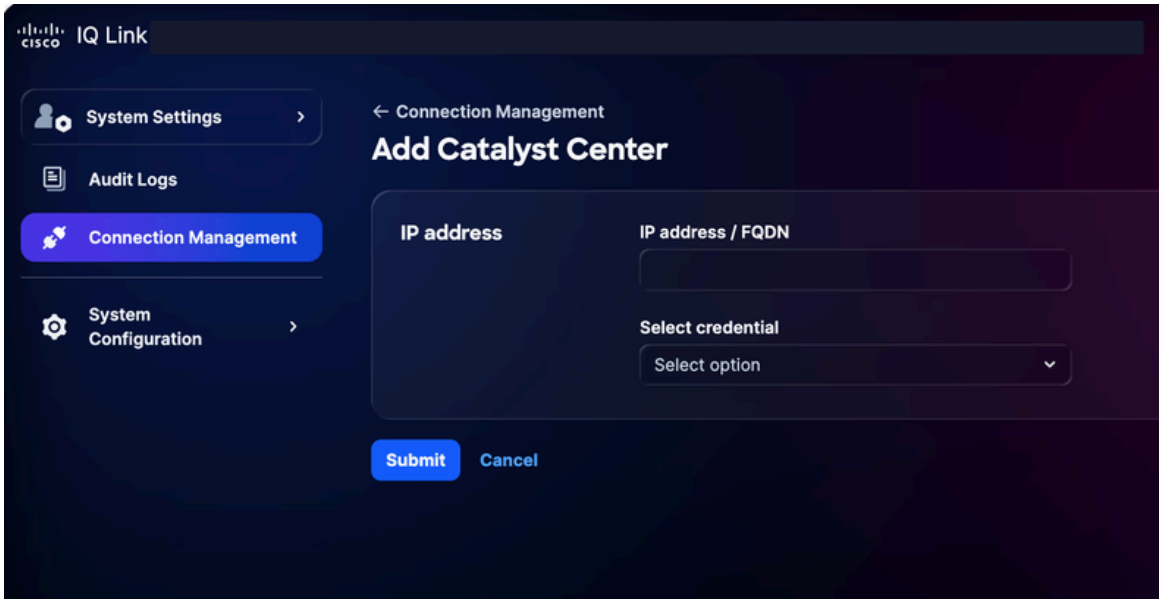
For data collection using Catalyst Center:

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



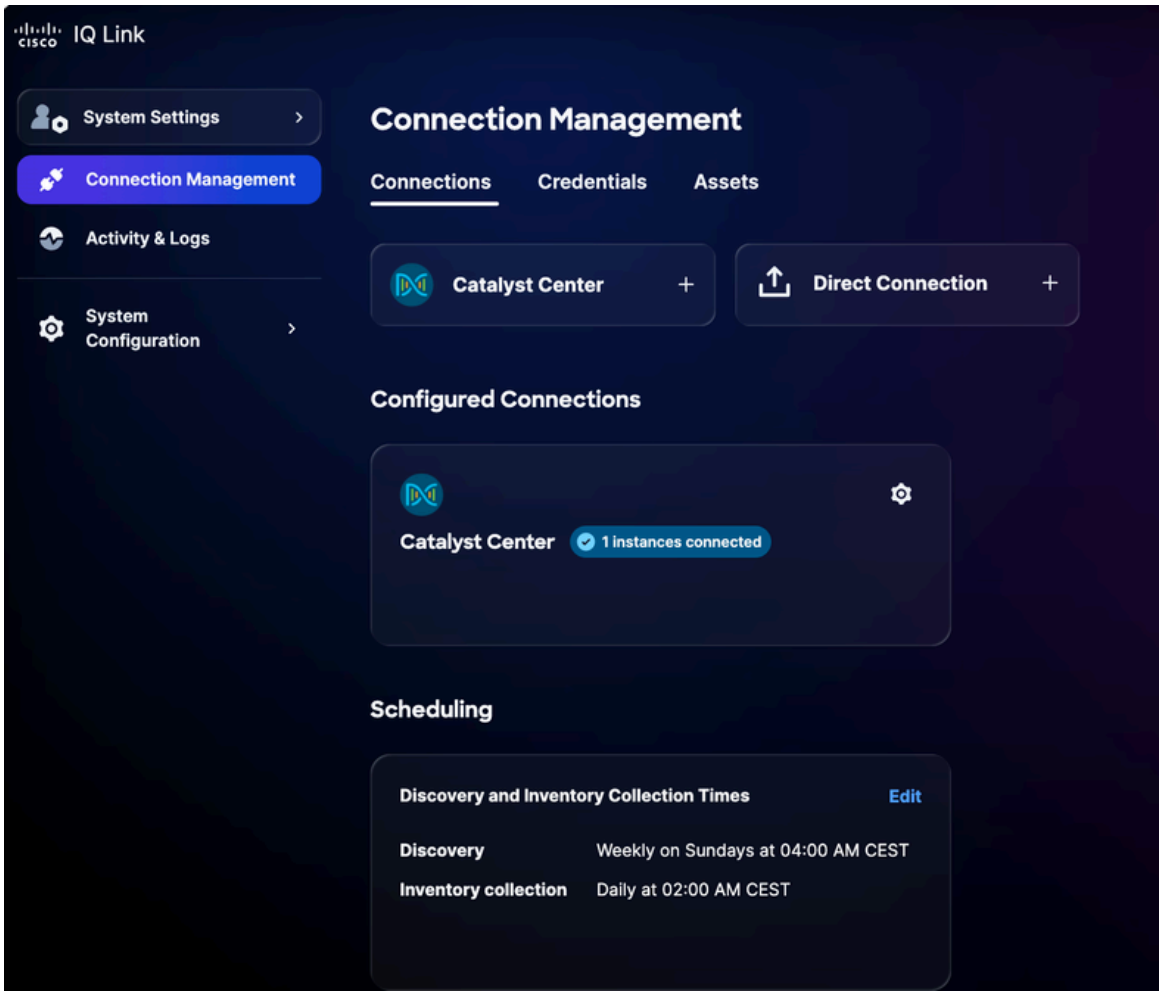

*Connection Management*

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 drop-down list.
5. Click **Submit**. A confirmation displays (it may take up to 75 minutes). You can view the newly added Catalyst Center under **Configured Connections**.




*Catalyst Center Added Successfully*

6. Schedule a collection. See Scheduling for more details.

---

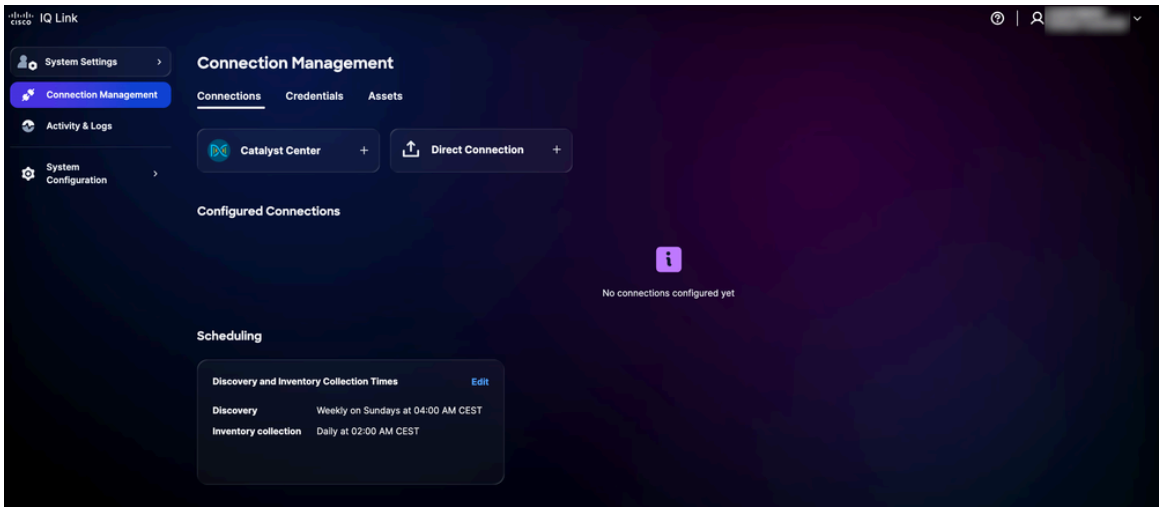
**Note**: Cisco IQ Link is pre-configured with an automated scheduling setup and the system initiates a default automated collection schedule. It is highly recommended that you edit the schedule to align it with your organization's requirements and maintenance windows.

---

## Direct Connection

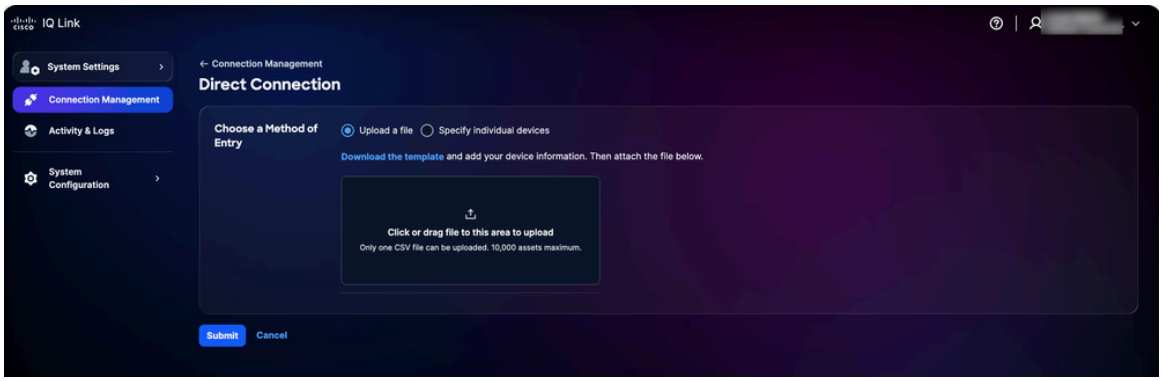
To add devices for direct connection:

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



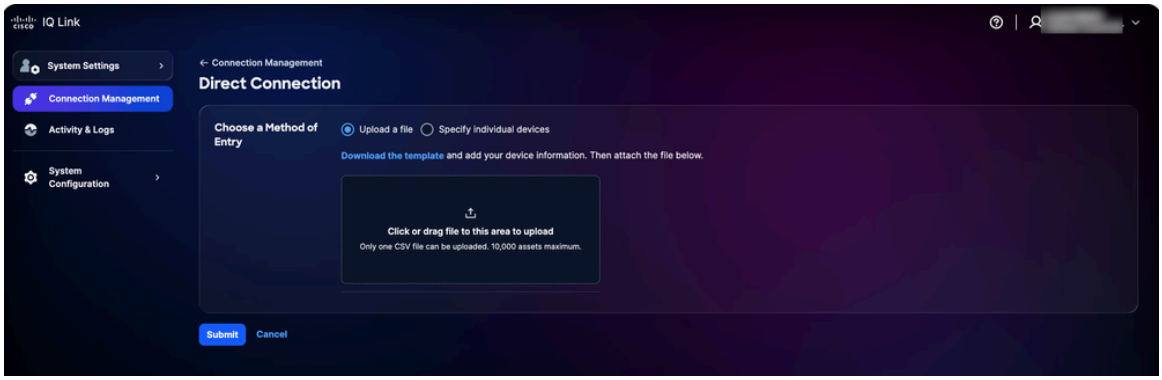

*Connection Management*

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



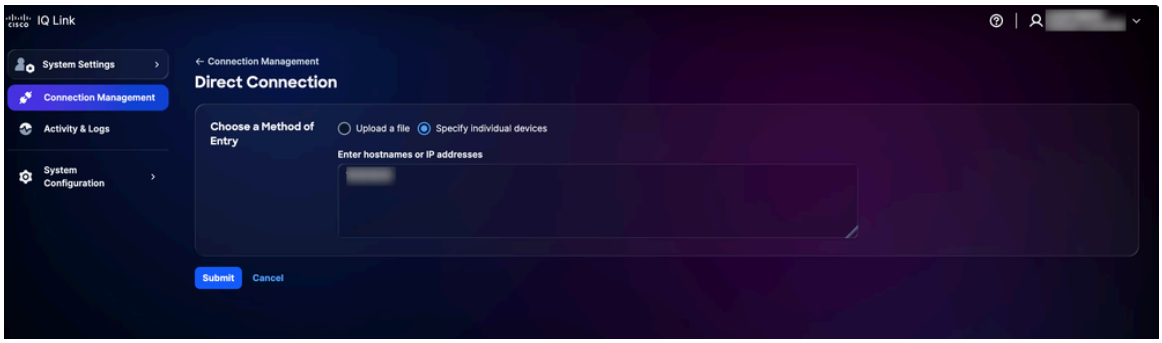

*Upload File*

3. Click the preferred option for **Choose a Method of Entry** and submit your devices using one of the following methods:




*Upload a File*

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




*Specify individual devices*

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

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

4. Schedule a collection. See Scheduling for more details.

---

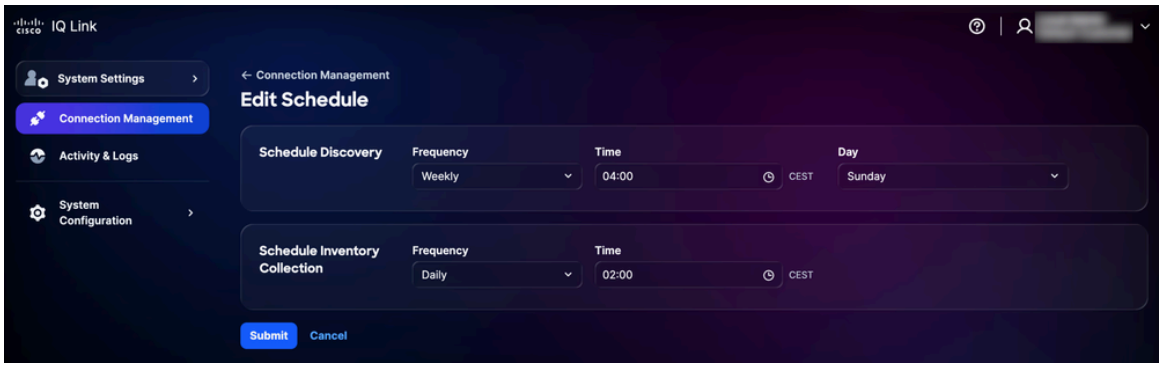
**Note**: Cisco IQ Link is pre-configured with an automated scheduling setup and the system initiates a default automated collection schedule. It is highly recommended that you edit the schedule to align it with your organization's requirements and maintenance windows.

---

## Scheduling

The Scheduling allows you to define when Cisco IQ Link 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 Cisco IQ Link.

# Banners

Administrators can configure customized banners that display across the application.

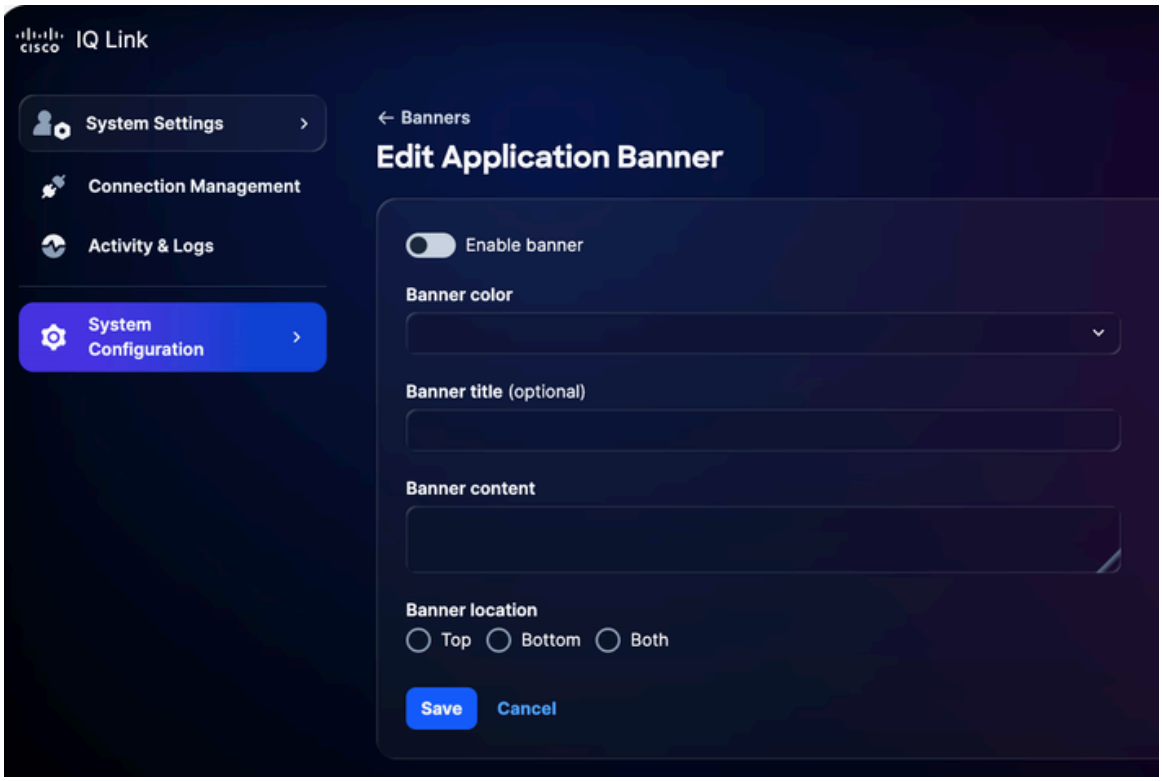
## Configuring Banners

To configure a banner:

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


*Configure Banner*

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




*Edit Application Banner*

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

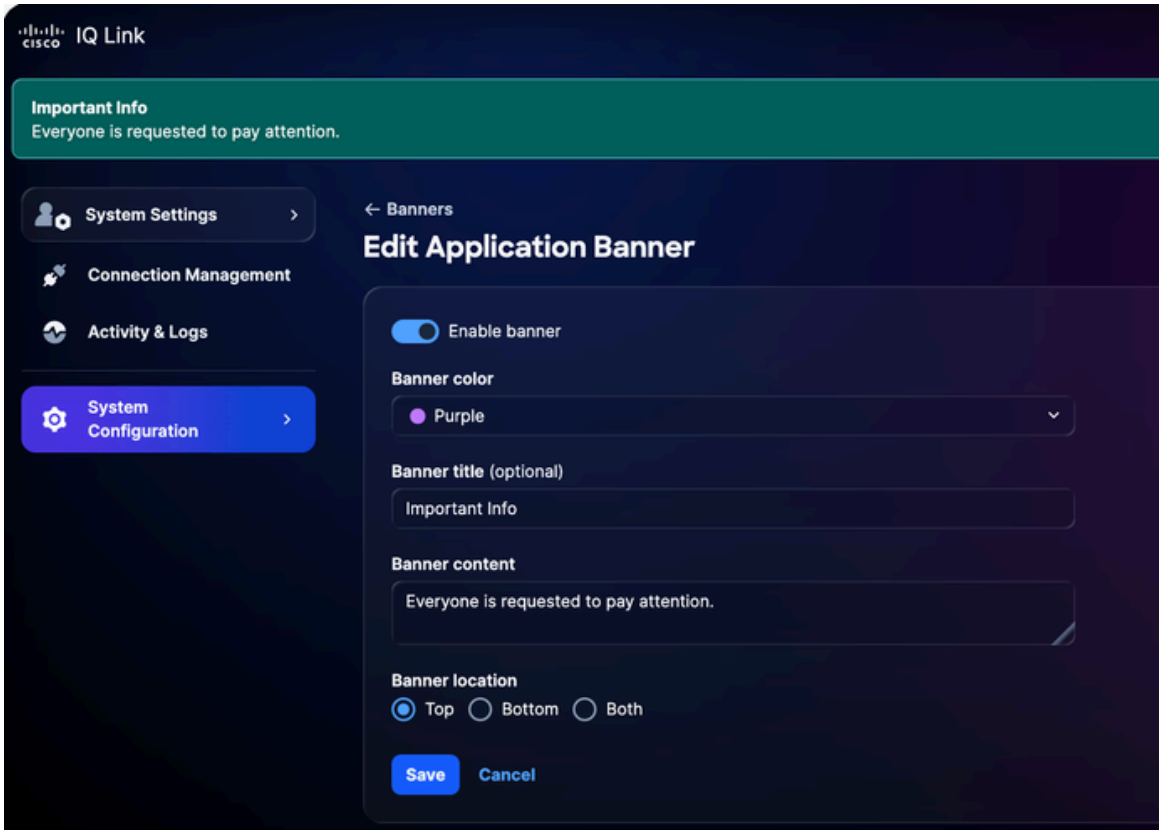
## Editing Banners

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

Customers 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.


*Main Menu*

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


*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.


*System Diagnostic Operation CoSystem Diagnostic Operation Completemplete*

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.