Cisco IQ Link Operations Guide v1.2.0

Introduction

Cisco IQ™ provides you with enhancements and features designed to improve asset visibility, deliver smarter insights across your environments, and streamline case management. In addition, AI features such as the 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 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

Account 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
- **Default Account Context**: Default-Customer

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

Setting Local Administrator Security

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

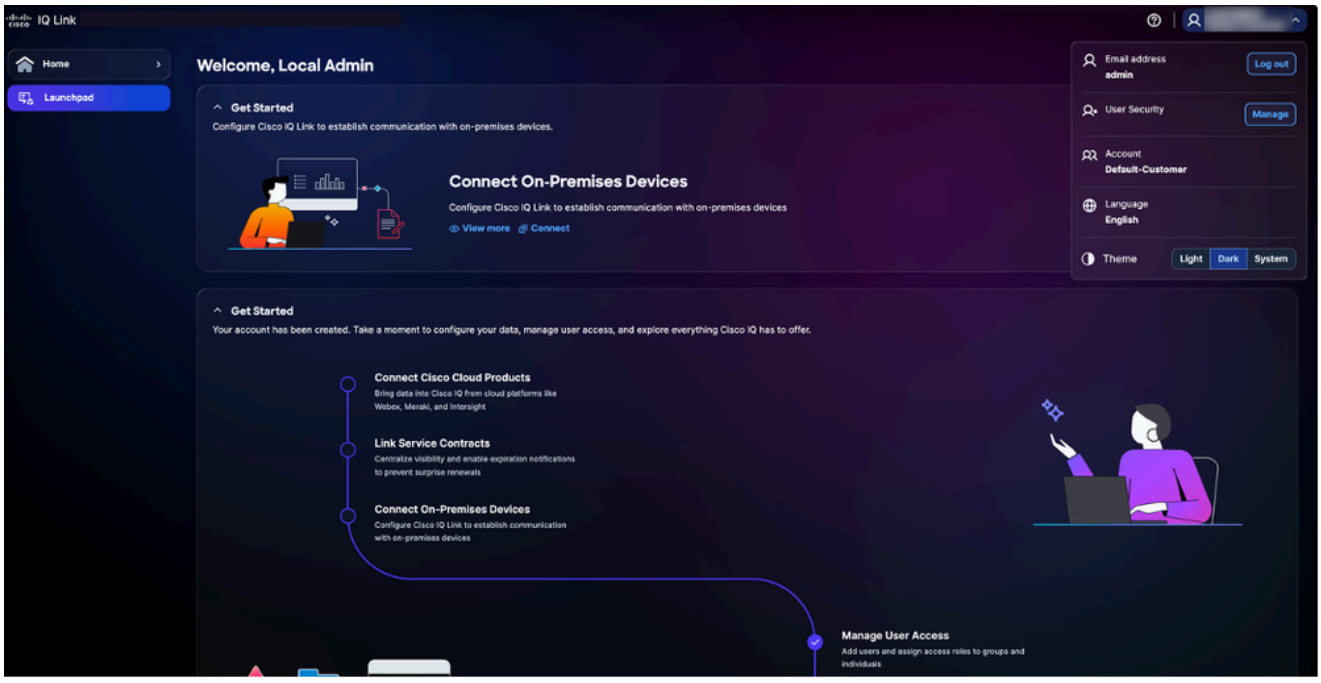
Your account automatically unlocks after 30 minutes, at which point you may attempt to log in or reset your password.

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.

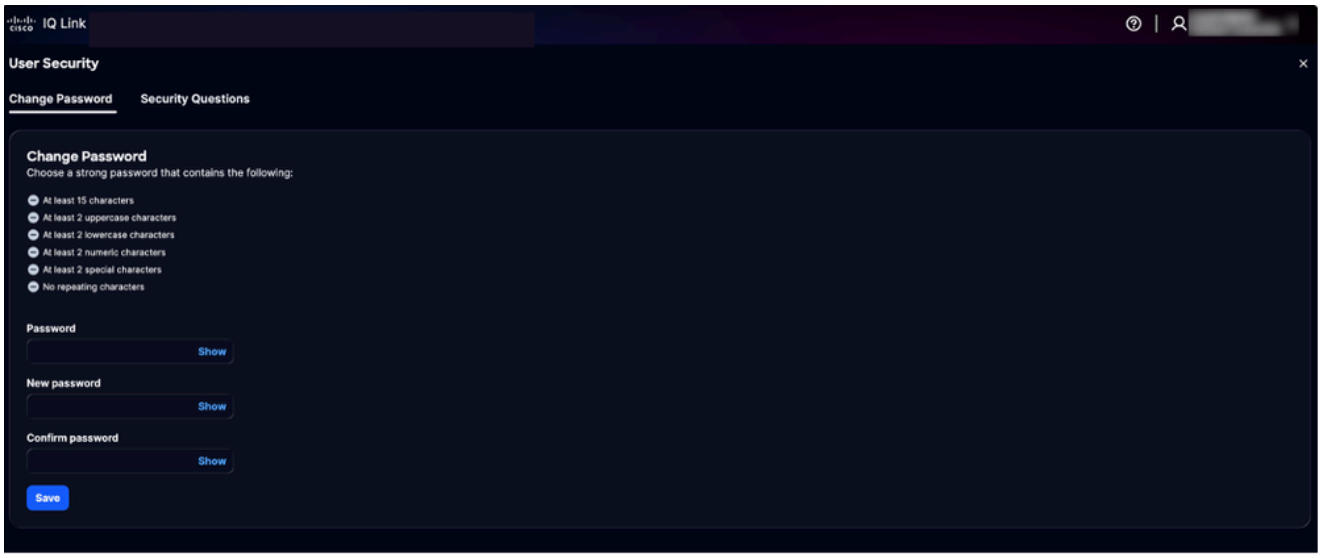
To set up security questions:

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



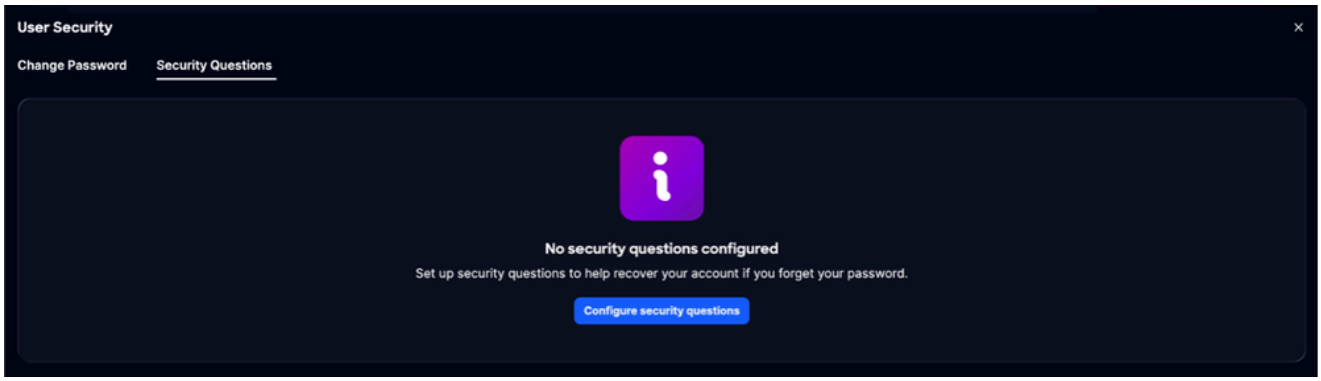
User Profile Menu

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



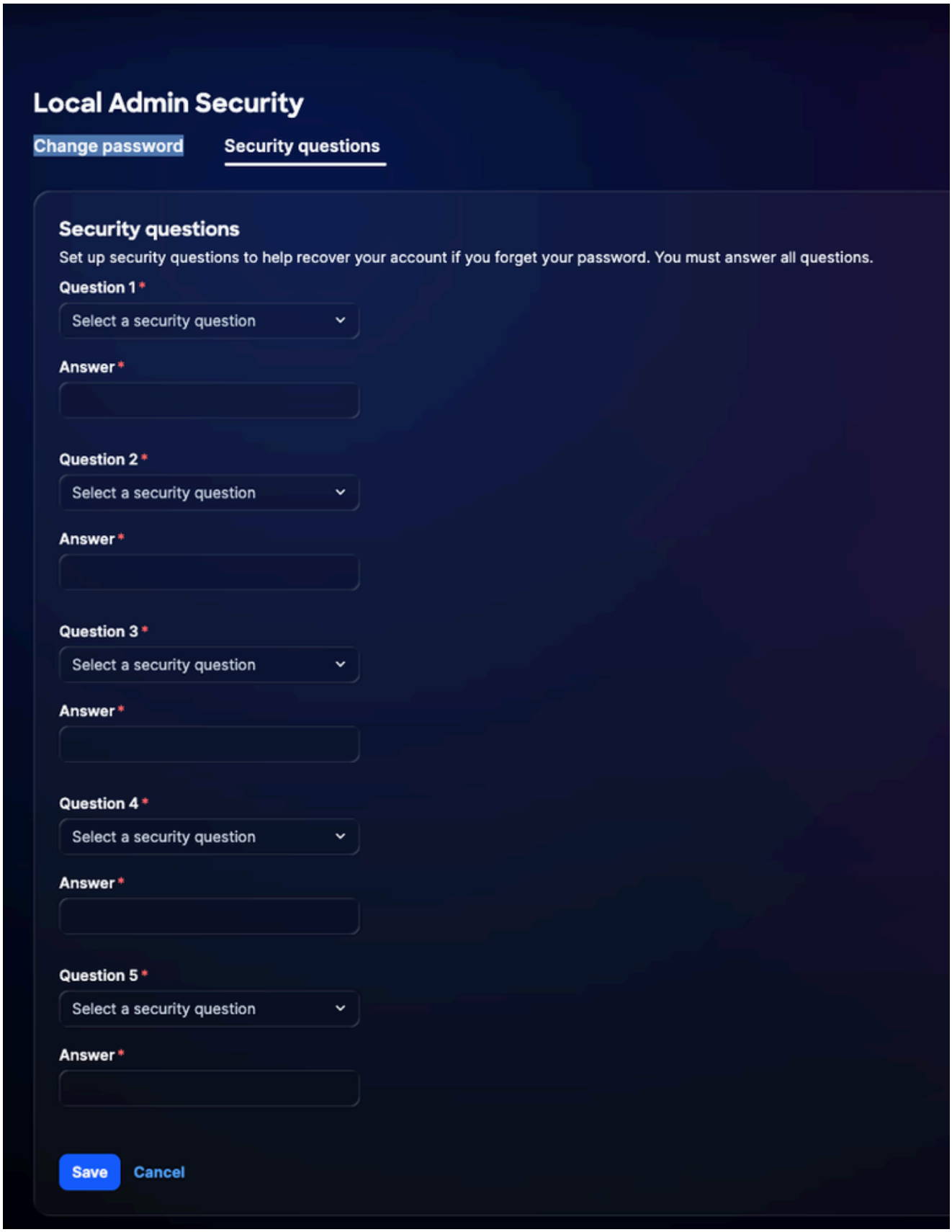
Change Password

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



Security Questions

4. Click **Configure security questions**.



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 same. Extra spaces are ignored, for example, " Smith" and "smith" are considered same.

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 passwords 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

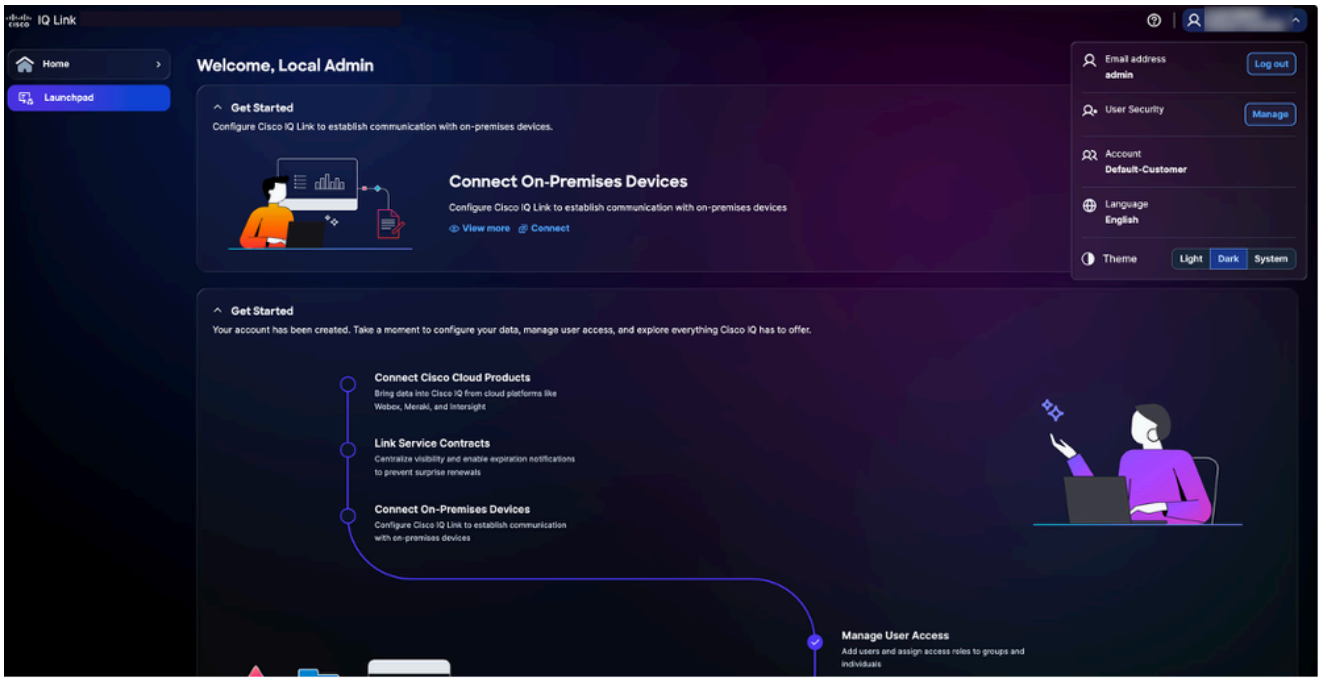
To manage passwords, the following conditions must be met:

- 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 Link
- You know the current password

Changing Passwords

To change a password:

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



User Profile Menu

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**.

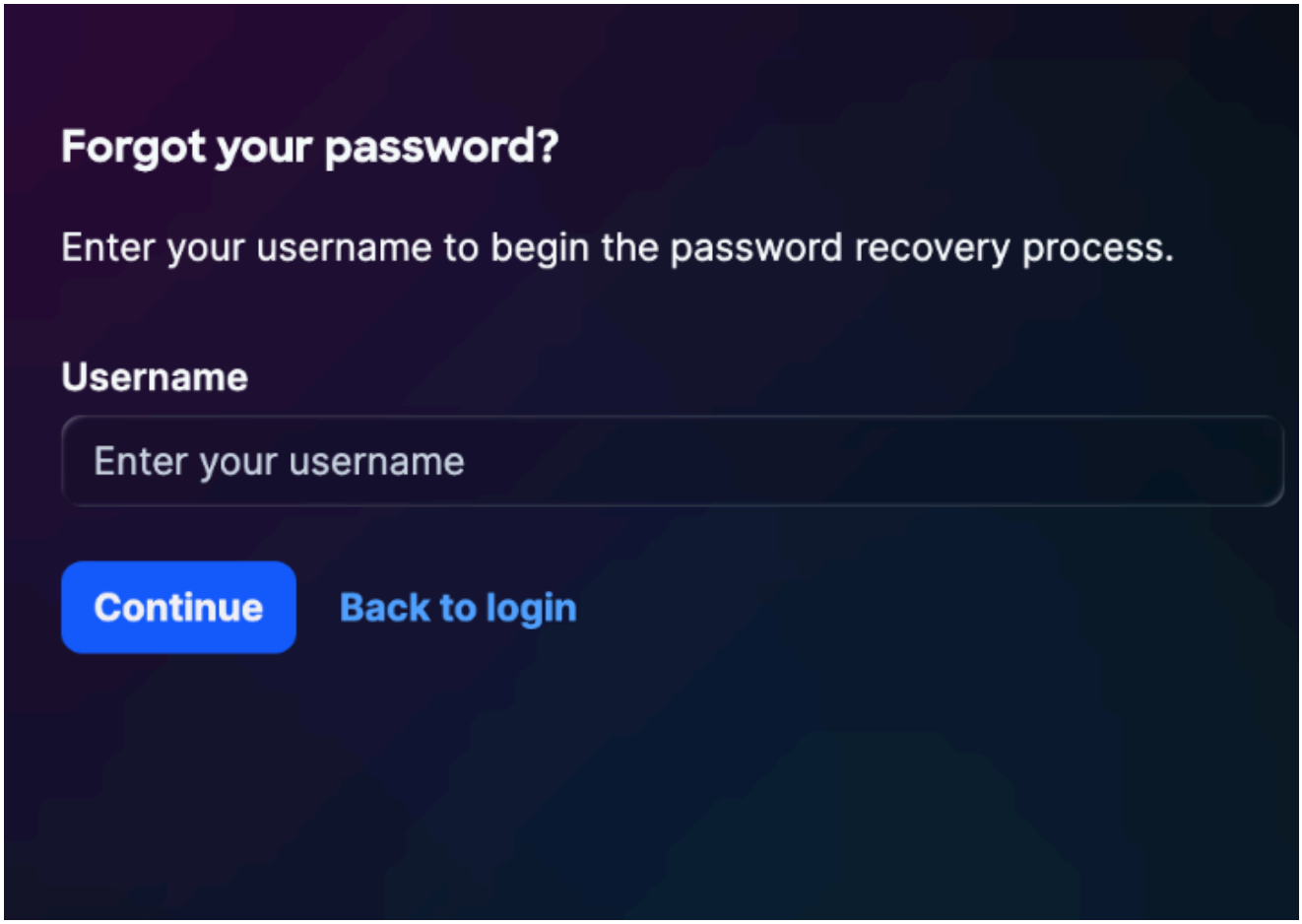
The password is updated in the Cisco IQ system, including the Cisco IQ Virtual Machine (VM).

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.

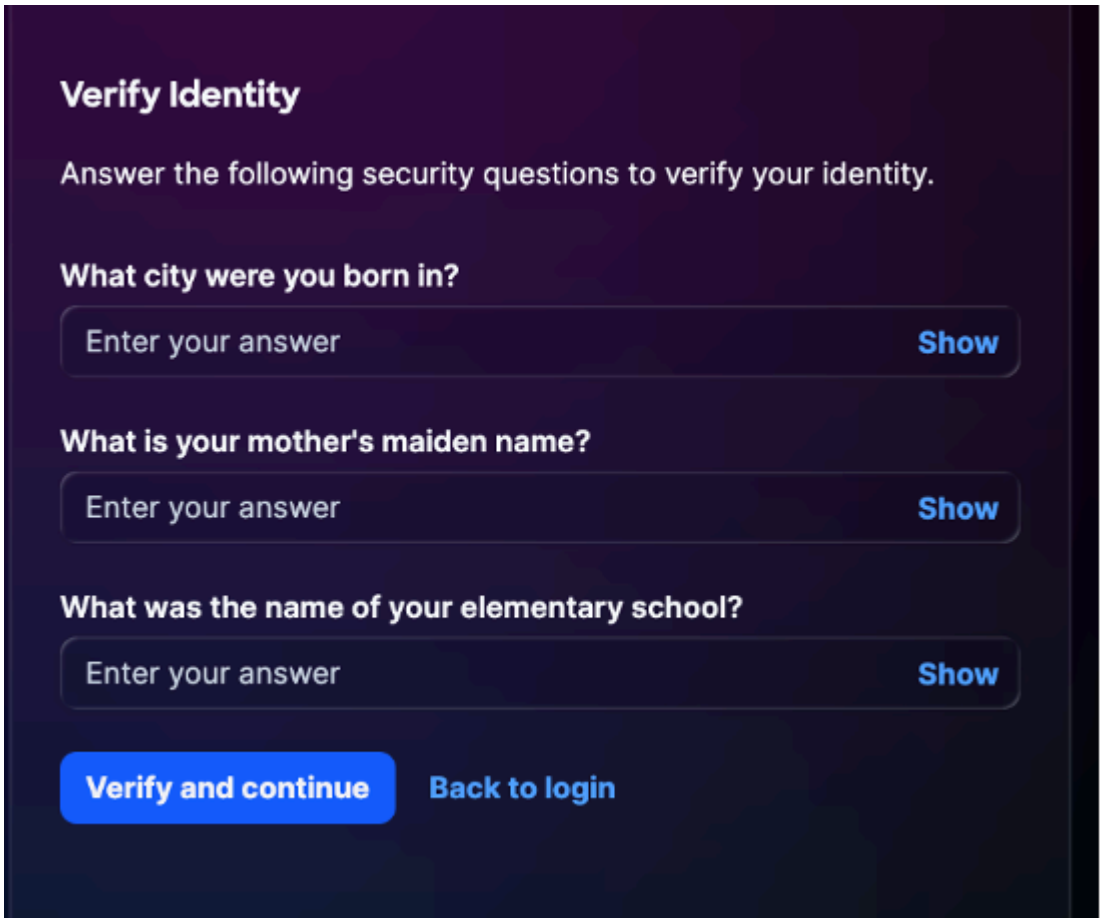
To reset a forgotten password:

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.



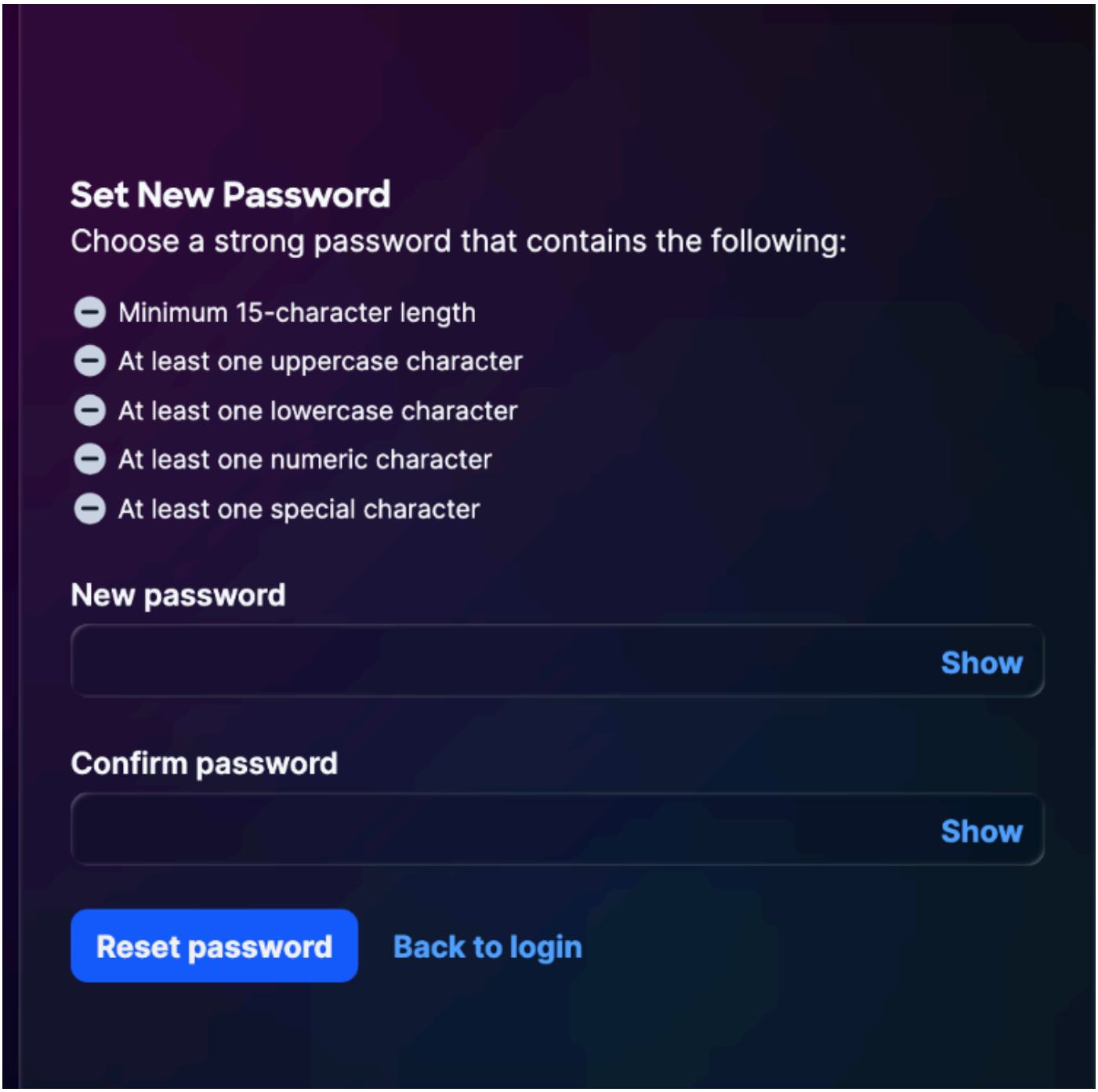
Verify Identity

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

You have three (3) attempts to answer the security questions correctly 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 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 30 minutes, at which point you may attempt to log in or reset your password.

---

7. Enter the **New password**.

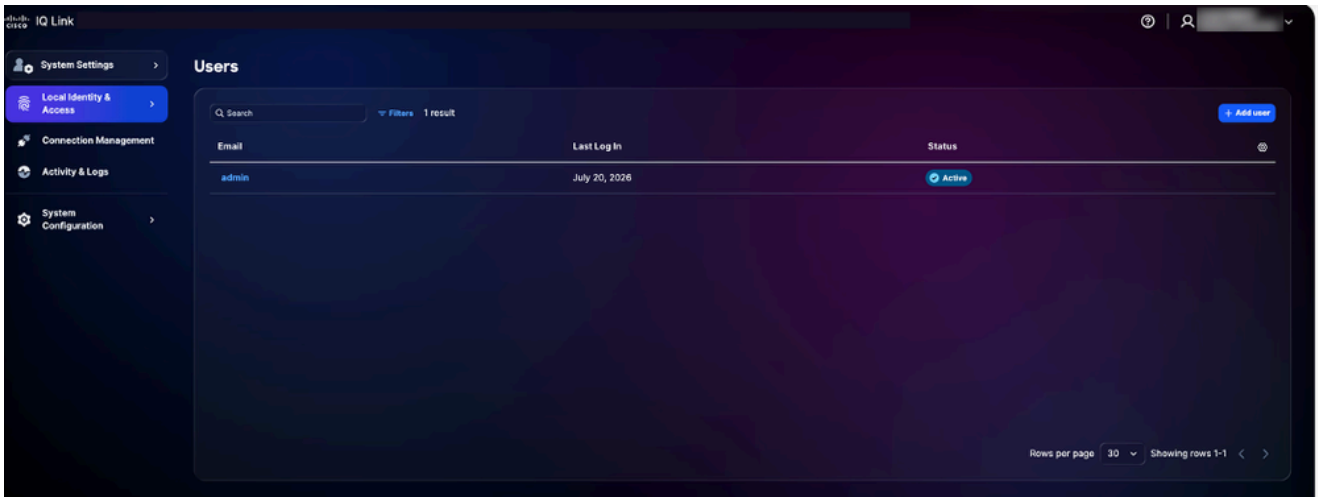
8. Enter the password again to confirm.

9. Click **Submit**.

Adding Local Users

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

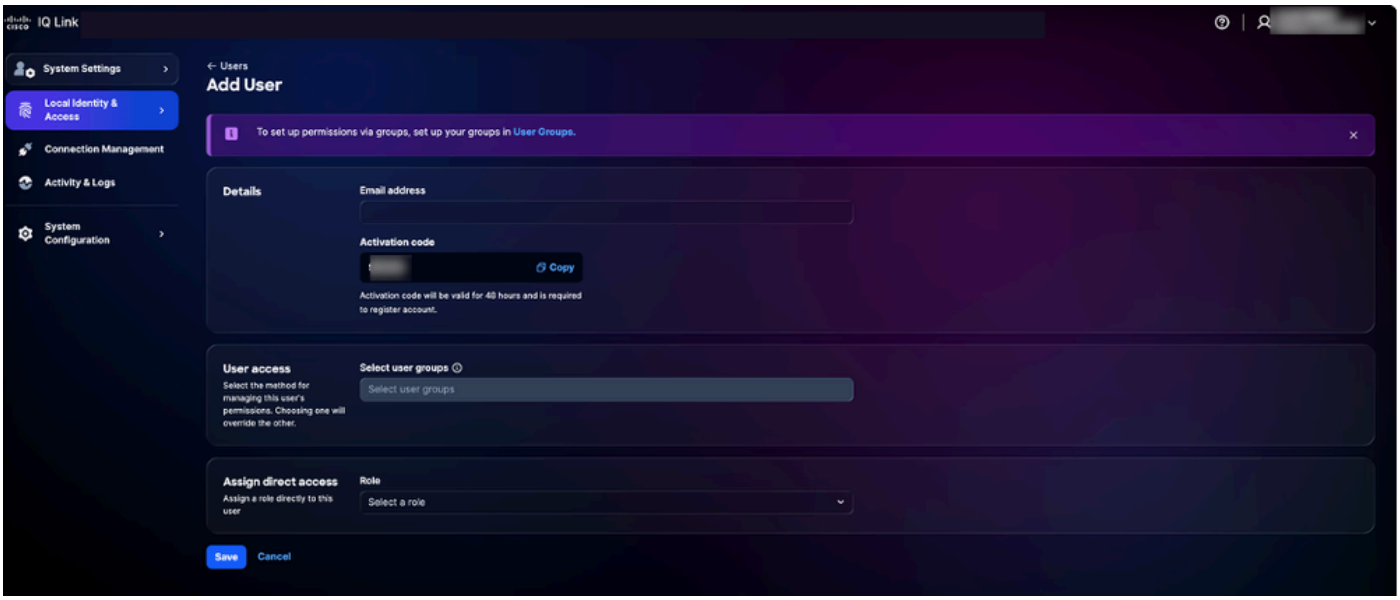
1. Navigate to **System Settings** > **Local Identity & Access** > **Users**. The **Users** page displays. It lists all existing local users along with their status.



Users Page

Note: The **More Options** icon is not displayed for Account Administrators (as shown in the image above).

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



Add User

3. Enter the **Email address**.

4. Enter the **Activation code**.

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

---

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

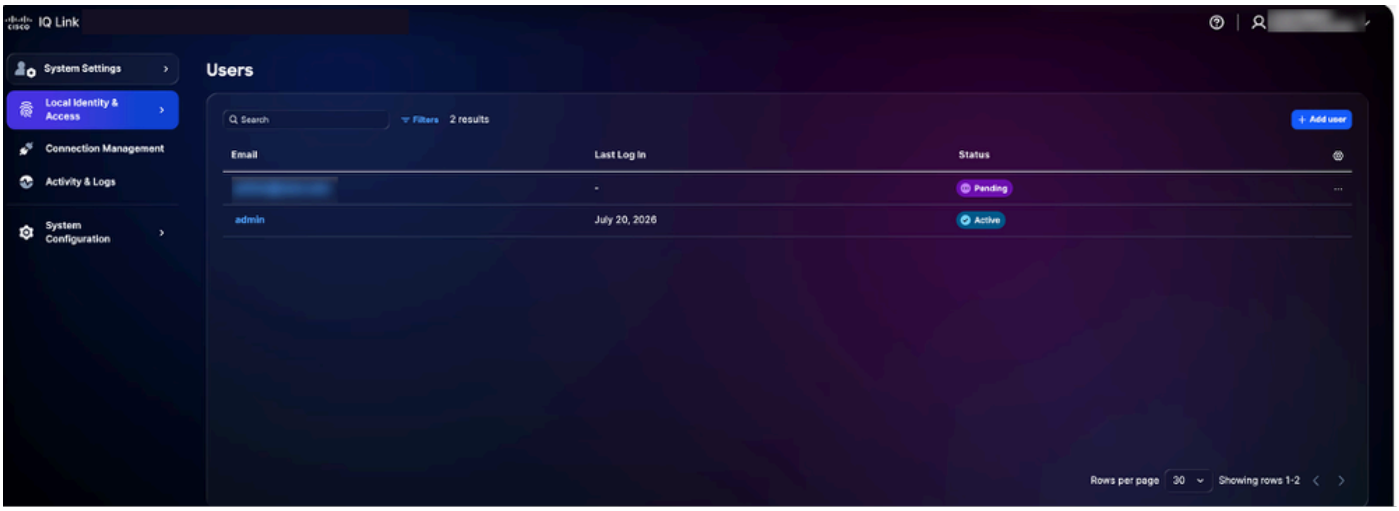
Note: Users inherit access from the selected group.

---

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

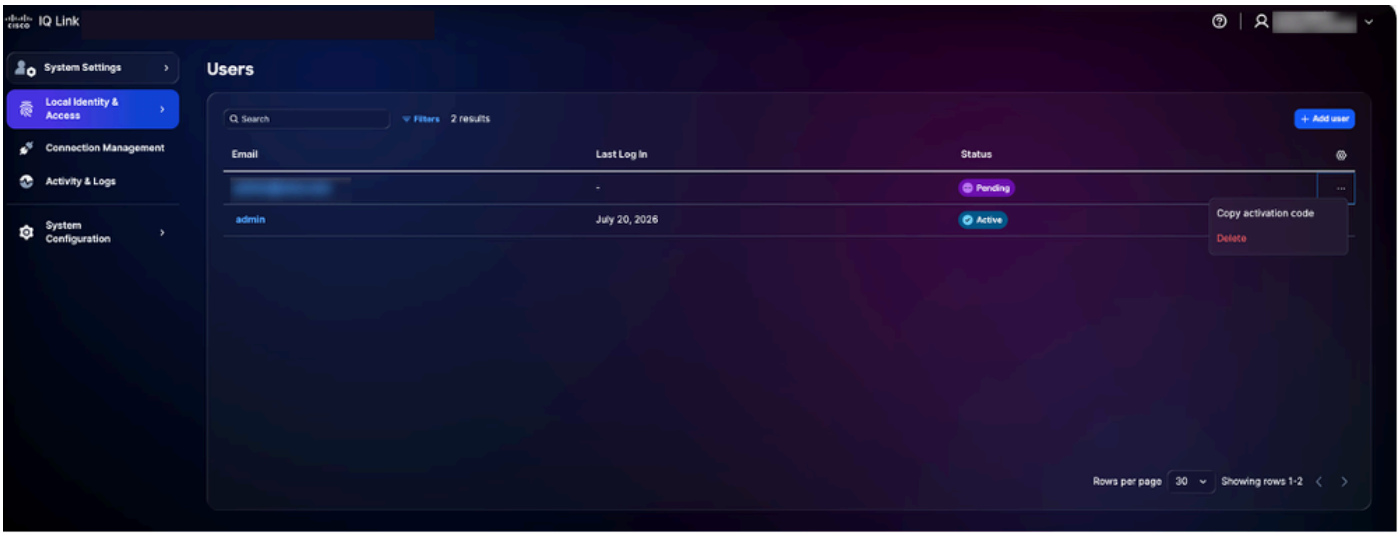
- **Viewer**: View and access applications
- **Administrator**: Access applications and manage system settings, except System Management and IDP

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.



Newly Added User

8. Locate the newly created user in the list and confirm that the **Status** column displays **Pending**.



Copy Activation Code

9. Click the **More Options** icon > **Copy activation code** next to the newly created user. The activation code is copied to your clipboard.

10. 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

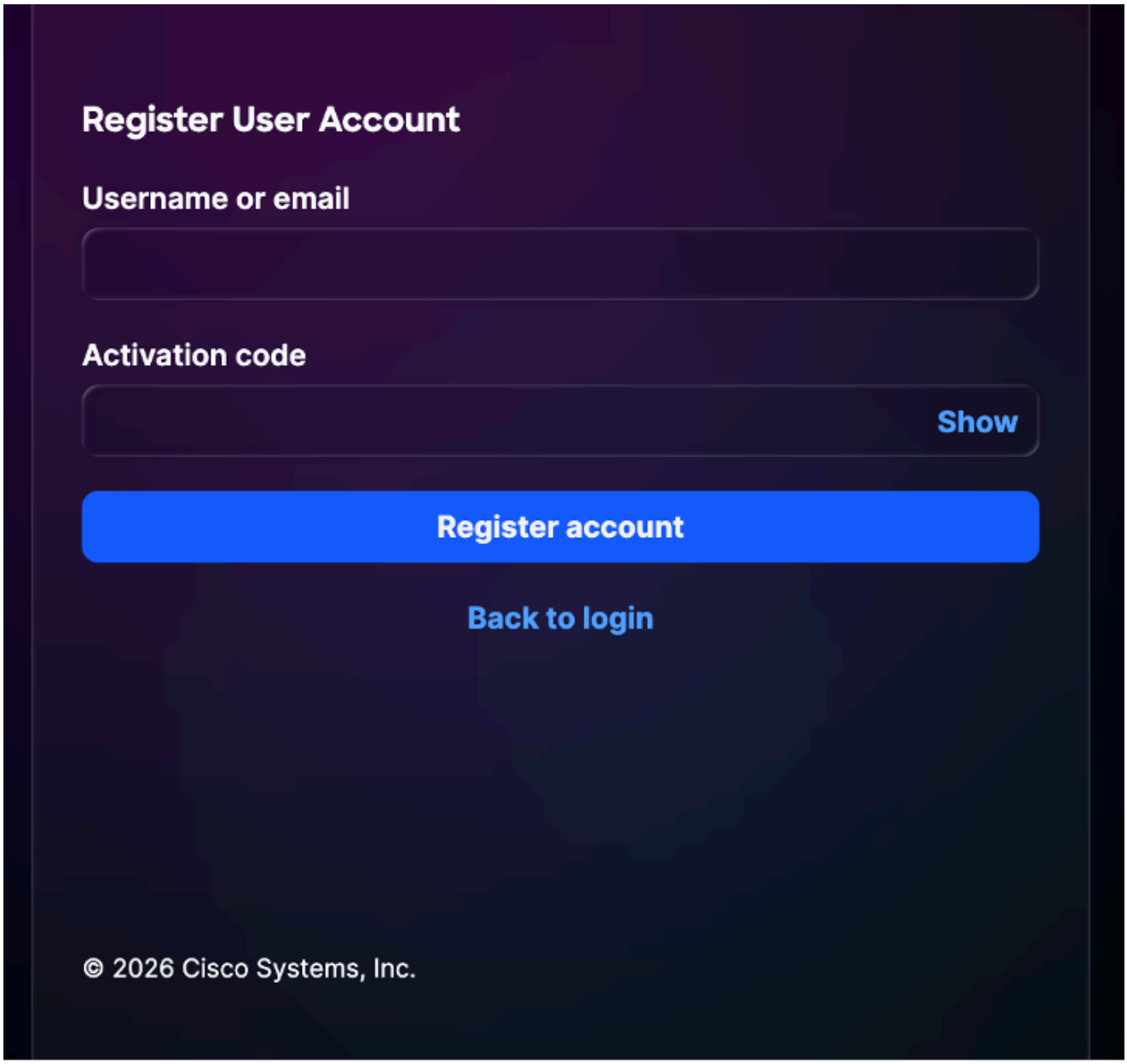
Note: Activation codes are valid for 48 hours. If your code expires, please contact your Account Administrator to request a new one.

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

Registering New User Account

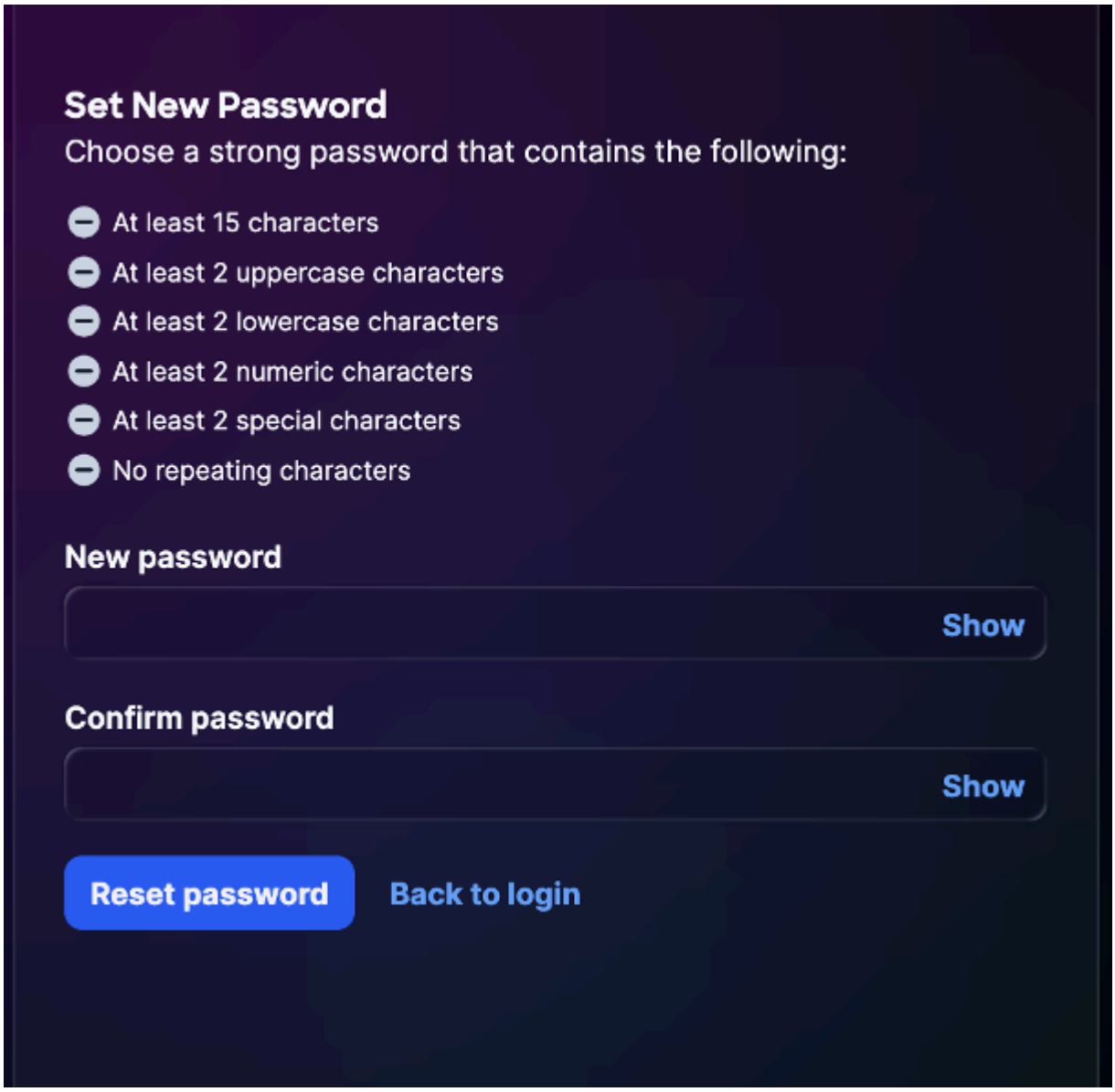
To register the new user account:

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



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.



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 and Answers for more information).

Managing Local User Groups

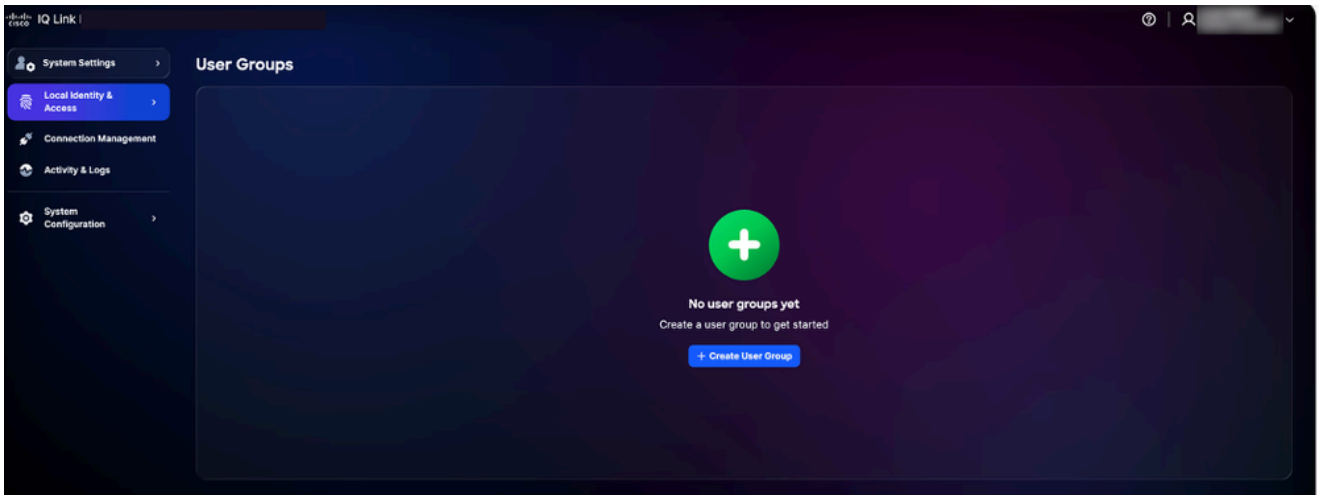
User Groups enable Account Administrators to manage roles for multiple local users together. Instead of assigning a role to each user individually, an Account Administrator can create a group, attach a role and a set of users to it, and update the role or membership in one place. All user group management 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.

Creating a User Group

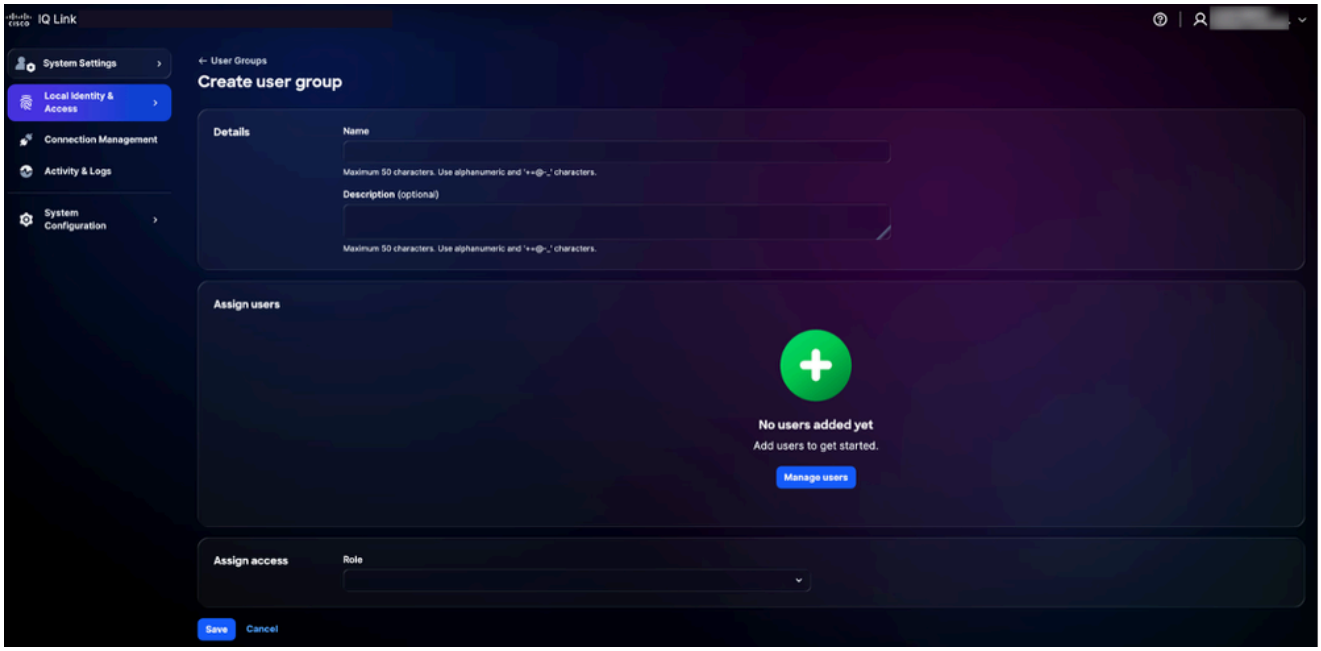
To create a user group:

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 applications (read-only)
    - **Administrator**: Access applications and manage system settings

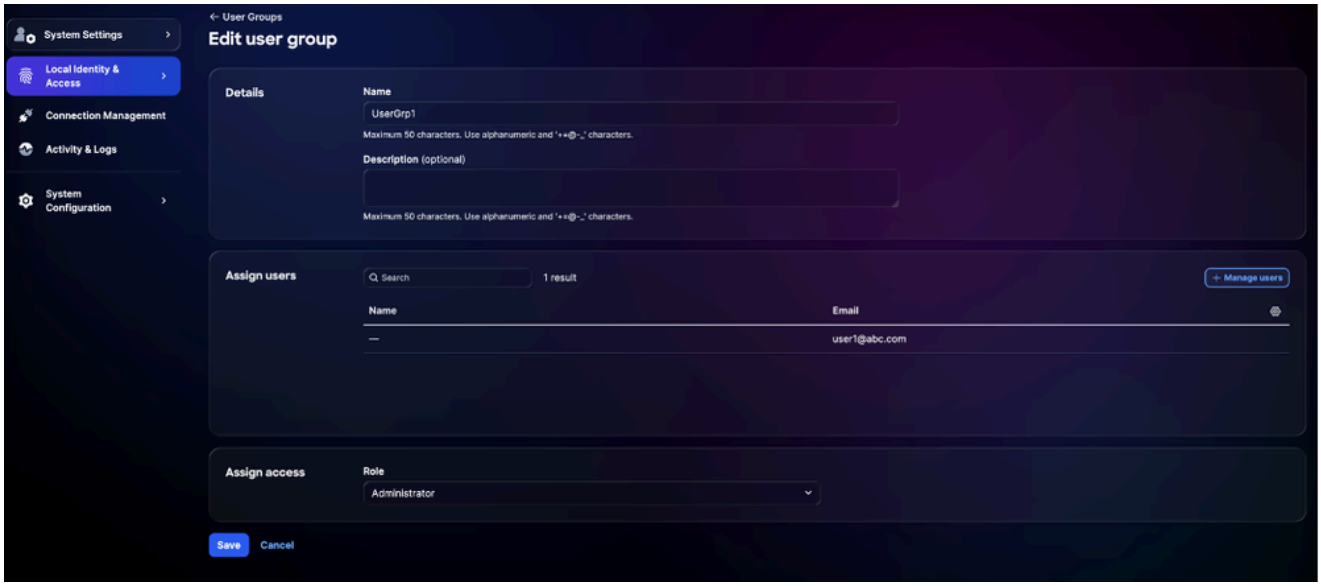
4. Click **Save**.

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. Click the **More** icon next to the group and choose **Edit**. The **Edit user group** page displays.



Edit User Group

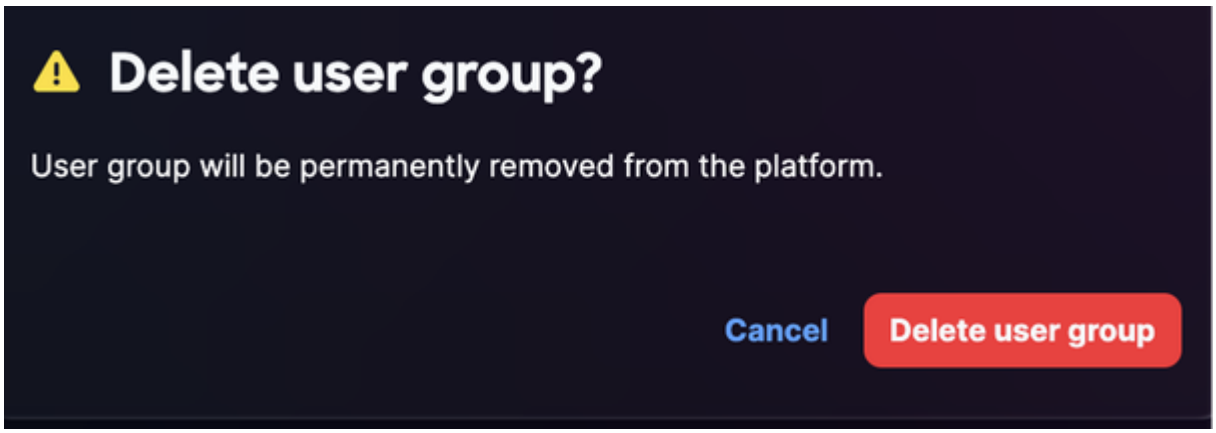
3. Make the desired changes.
4. Click **Save**.

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 Cisco IQ Link, Account Administrators can configure various settings. Account 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 Account 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.
Table 1: 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”

Table 2: SAML Configuration Parameters

Parameter	Configuration	Example
Audience (Entity ID)	Fully Qualified Domain Name (FQDN)	mymanagementhost.mydomain.com
Single Sign-On URL	SAML Assertion Consumer Service (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.

Table 3: 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 *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

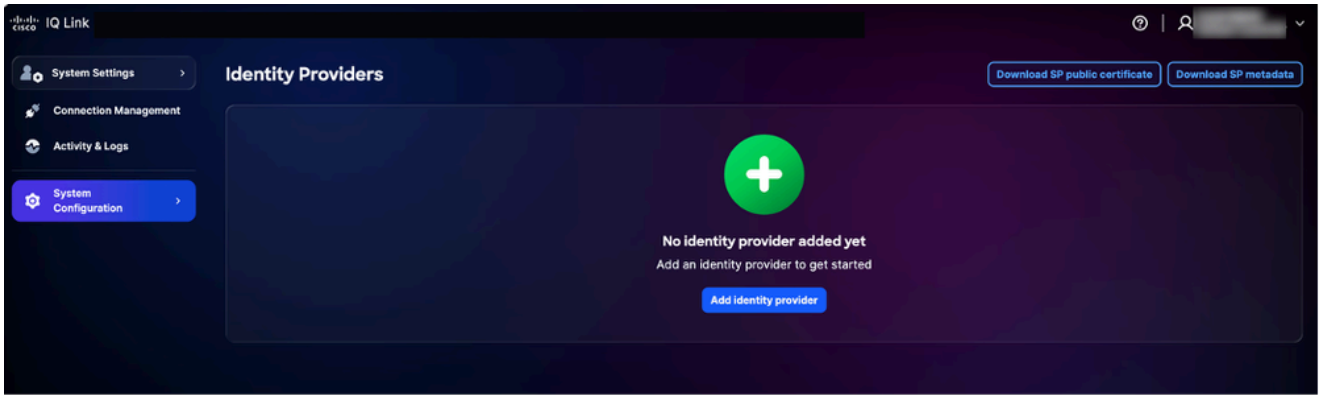
5. Click the **Download** icon to download the “SP Metadata” file.

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

Adding Okta IDP

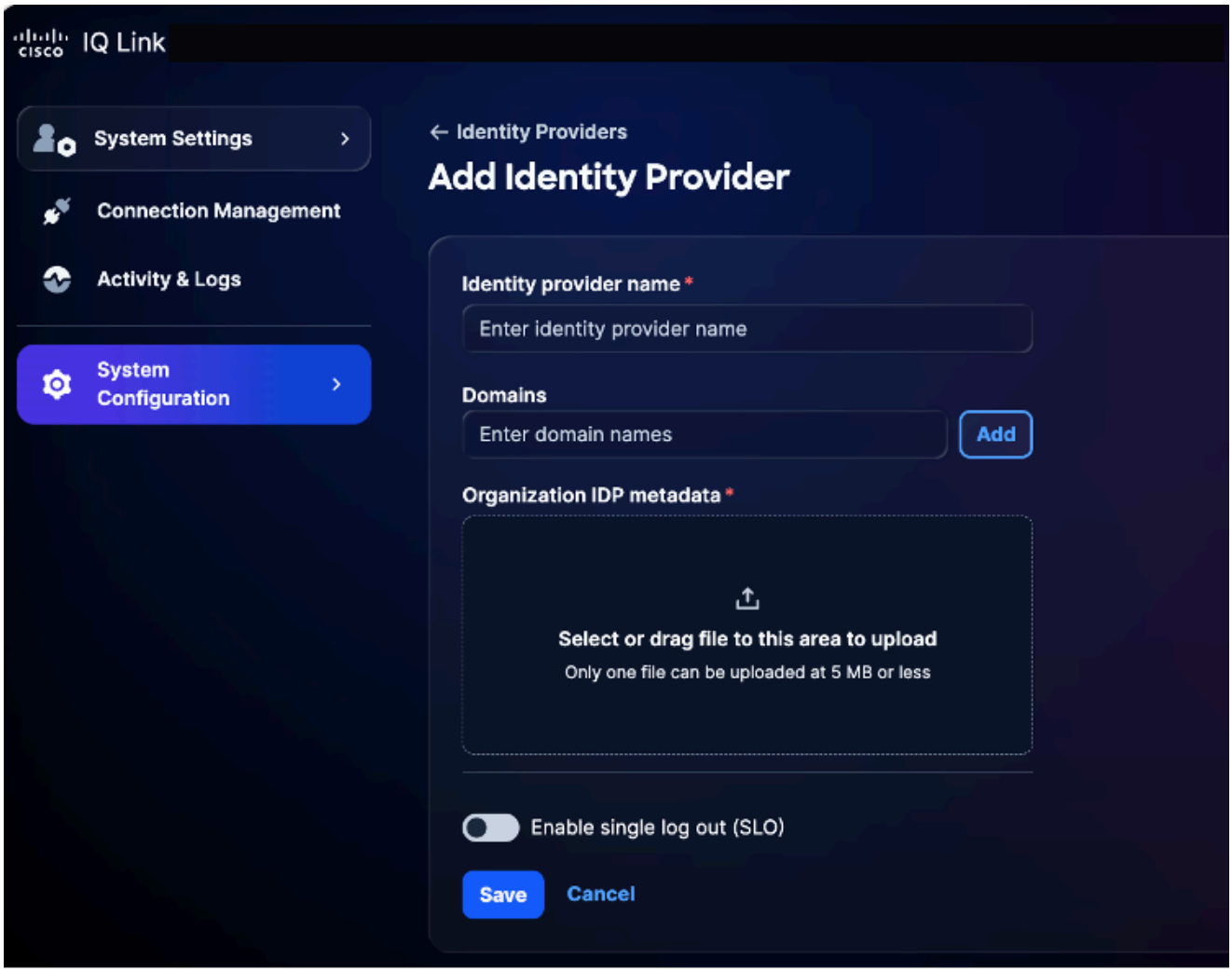
To add an IDP in Cisco IQ Link:

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**.

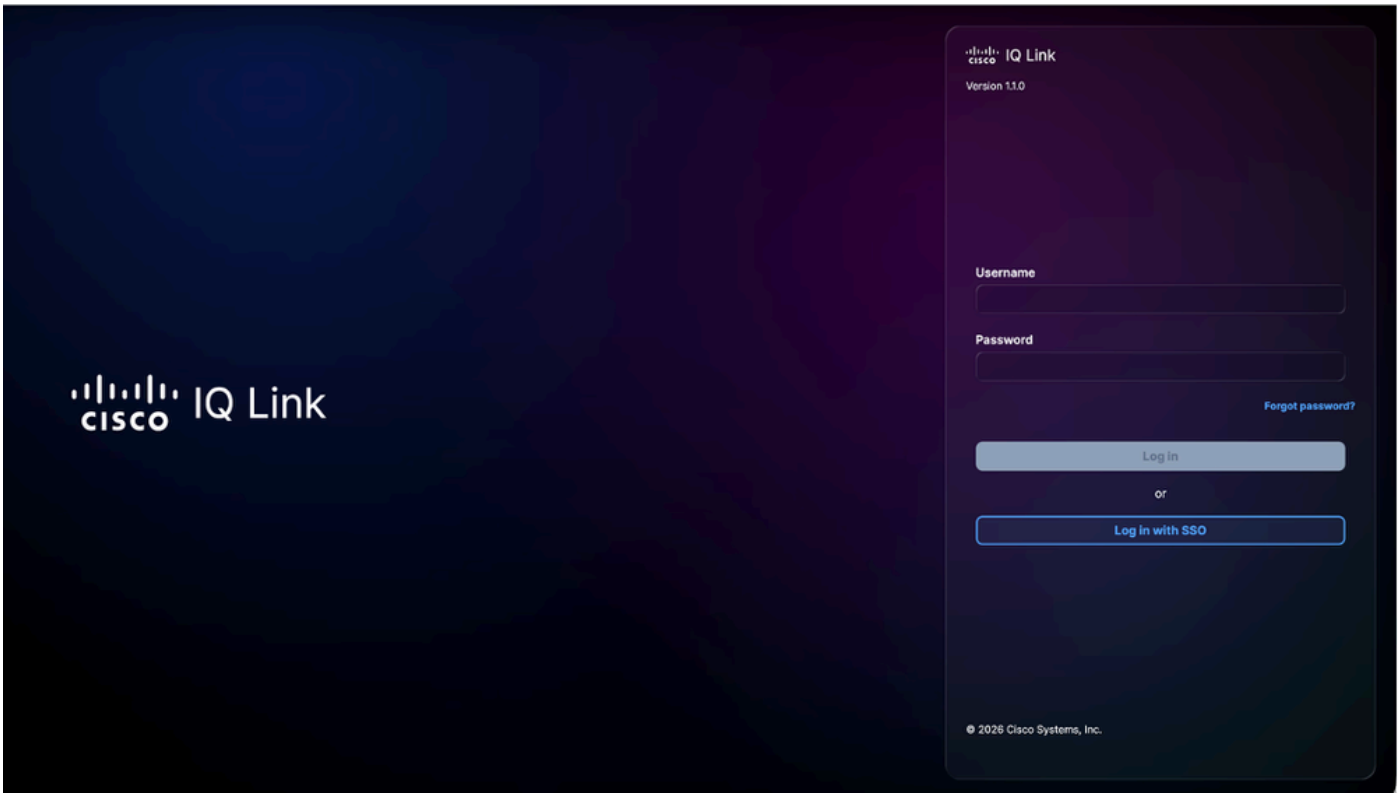
4. Click **Add** to add a Cisco IQ Link configured domain name to the **Domains** field.

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 logou**t toggle button. You can enable the SLO later as well.

7. Click **Save**.

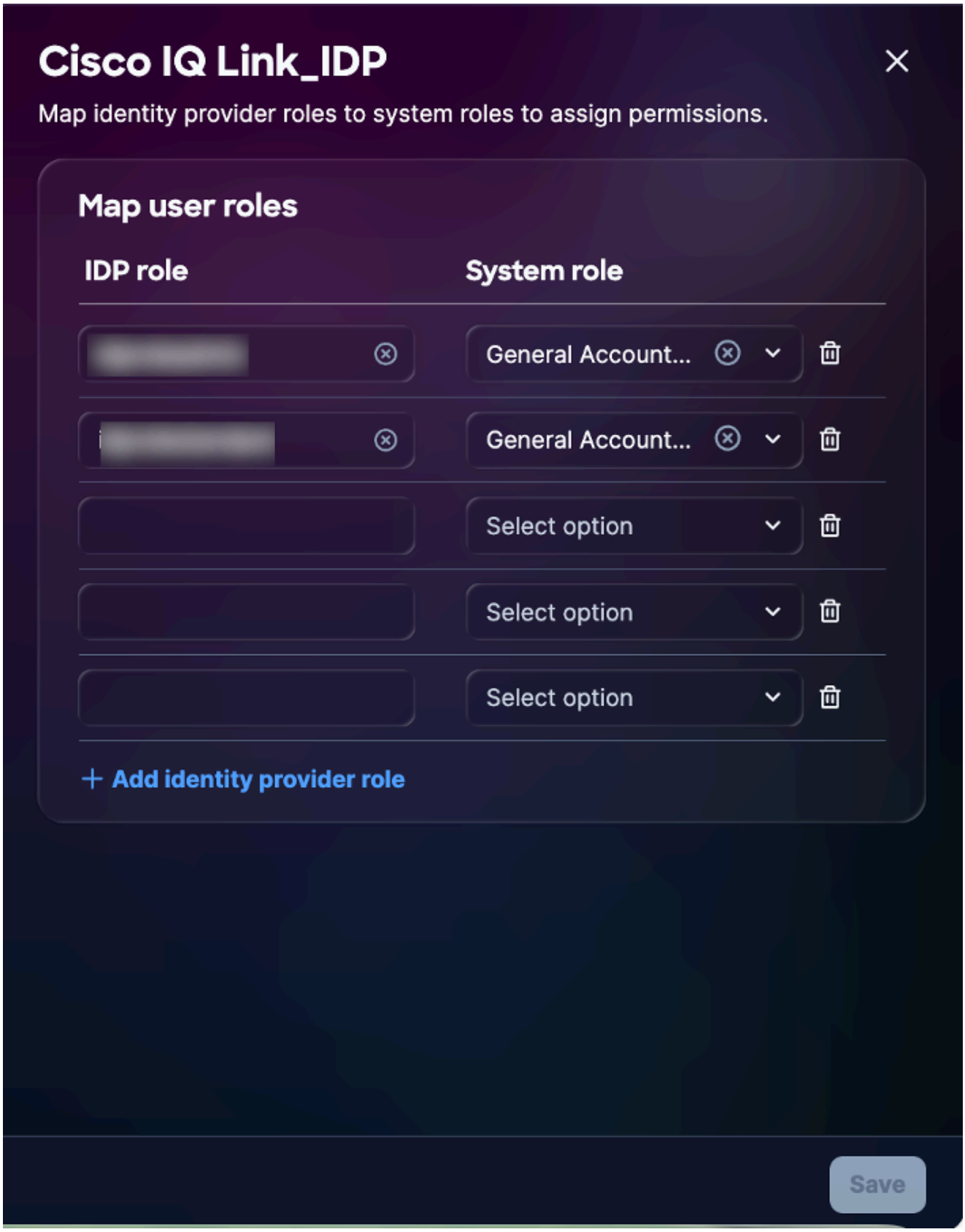
Once configured, the login page displays an option to log in with SSO (via IDP).



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

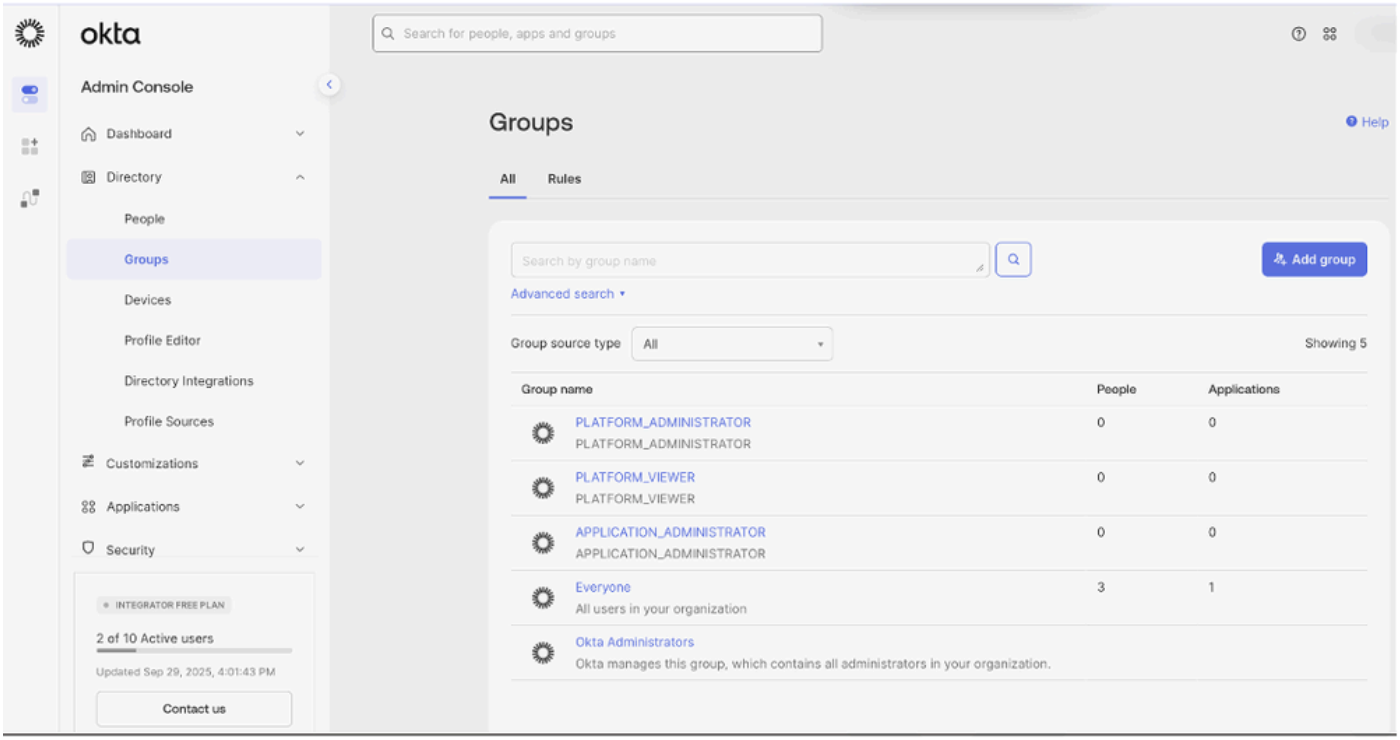
2. Enter an **IDP role** for the selected **System role**. The following system roles are supported:

- **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**.

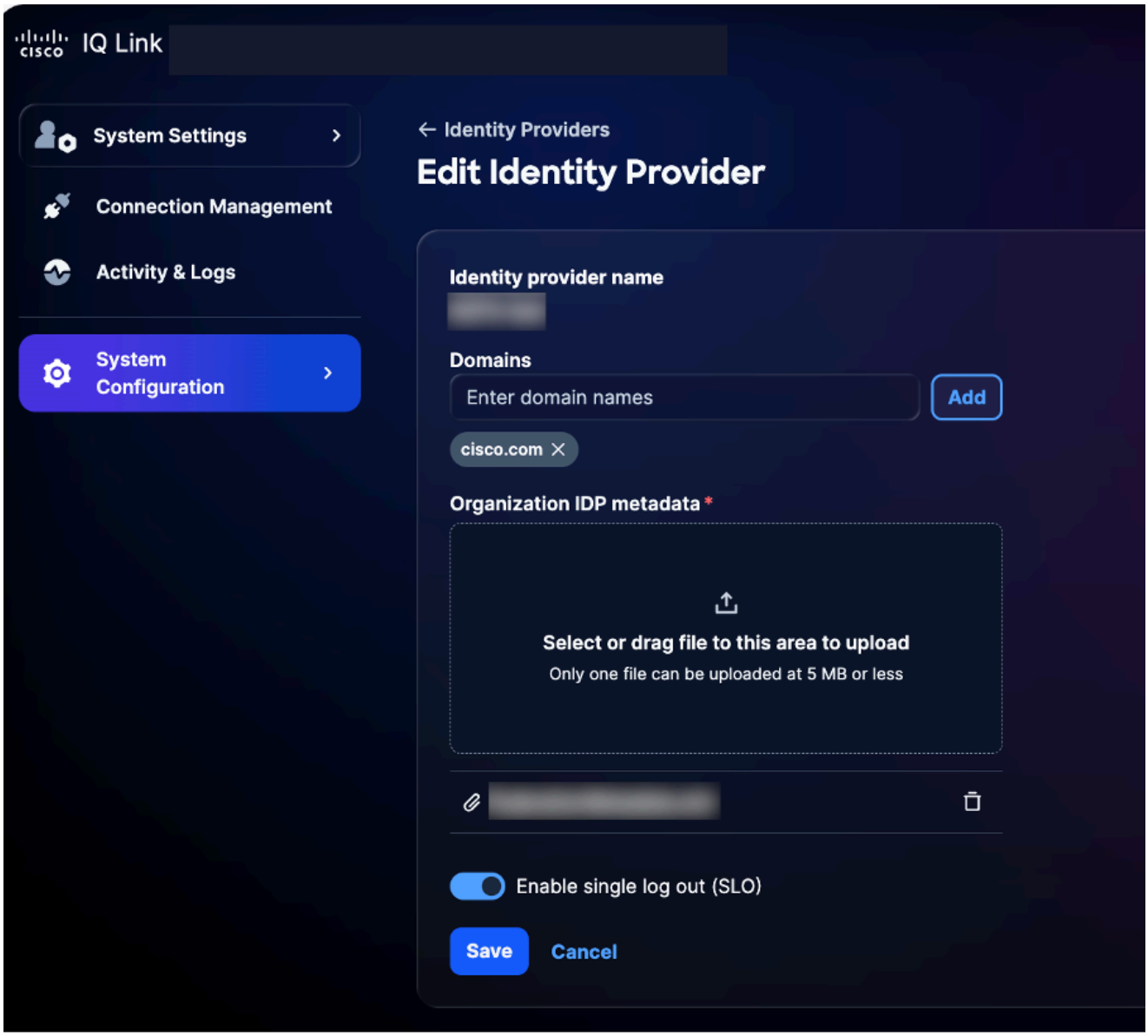
Single Logout Configuration

If you choose to enable Single Logout Configuration (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 IDP SAML Configuration for SSO.
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 metadata file.
9. Use the following checklist to verify SSO and SLO functionality:

Verification Checklist:

- Local Account 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:

Table 4: 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 (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 AD integration
- SSL/Transport Layer Security (TLS) certificates on ADFS
- Account 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)

Table 5: 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	AD 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** to get details from the file which is saved as part of step 3.
10. Click **Browse** to select the SP 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.

Note: Do not select “Permit Everyone with MFA” unless your ADFS server has a registered Multi-Factor Authentication (MFA) adapter (for example, Azure MFA or *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 relying party 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/per
```

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 6: Required Claims

Claim	Purpose	Source
Email	User identifier	AD Mail
Display Name	User's full name	AD Display Name
UPN	Public Key Infrastructure (PKI)/certificate authentication	ADFS maps the client certificate to an AD user via User Principal Name (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 - 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.Iss

@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

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 the 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
```

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 Certificate Authority (CA) 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

- 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:-iq-onprem-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 “<YOUR-CA-NAME>” `
    -KeyLength 2048 `
    -HashAlgorithmName SHA256 `
    -CryptoProviderName “RSA#Microsoft Software Key Storage Provider” `
    -ValidityPeriod Years `
    -ValidityPeriodUnits 10 `
    -Force
```

4. 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 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”
} | Format-Table Subject, Thumbprint, NotAfter -AutoSize
```

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 “*<USERNAME>*” }

$password = ConvertTo-SecureString -String “<EXPORT-PASSWORD>” -Force -AsPlainText

Export-PfxCertificate -Cert $cert -FilePath “C:-cert.pfx” -Password $password
```

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 -P “<EXPORT-PASSWORD>”
```

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/certificate

Enable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/2005/certificatetransport

Enable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/13/certificate

Enable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/13/certificatetransport
```

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

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

Format-Table AddressPath, Enabled, Proxy -AutoSize
```

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”, “WindowsAuthentication”, “FormsAu
-PrimaryExtranetAuthenticationProvider @(“CertificateAuthentication”, “FormsAuthentication”, “Microsoft
```

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

```
(Get-AdfsGlobalAuthenticationPolicy).PrimaryIntranetAuthenticationProvider

(Get-AdfsGlobalAuthenticationPolicy).PrimaryExtranetAuthenticationProvider
```

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=<YOUR-ADFS-HOSTNAME>:49443 `
    certhash=<YOUR-SSL-CERT-THUMBPRINT> `
    appid="{5d89a20c-beab-4389-9447-324788eb944a}" `
    certstorename=MY `
    clientcertnegotiation=enable `
    verifyclientcertrevocation=disable
```

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

```
netsh 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)" -ForegroundColor Red
```

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

```
$bad | Move-Item -Destination Cert:
Write-Host “Moved $($bad.Count) cert(s) from Root to Intermediate CA store” -ForegroundColor Green
```

3. Verify that no non-self-signed certificates remain in the 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 -Type DWord

Set-ItemProperty -Path $regPath -Name “SendTrustedIssuerList” -Value 0 -Type DWord
```

Table 7: 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 LocalMachinestore:

```
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 “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.

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.

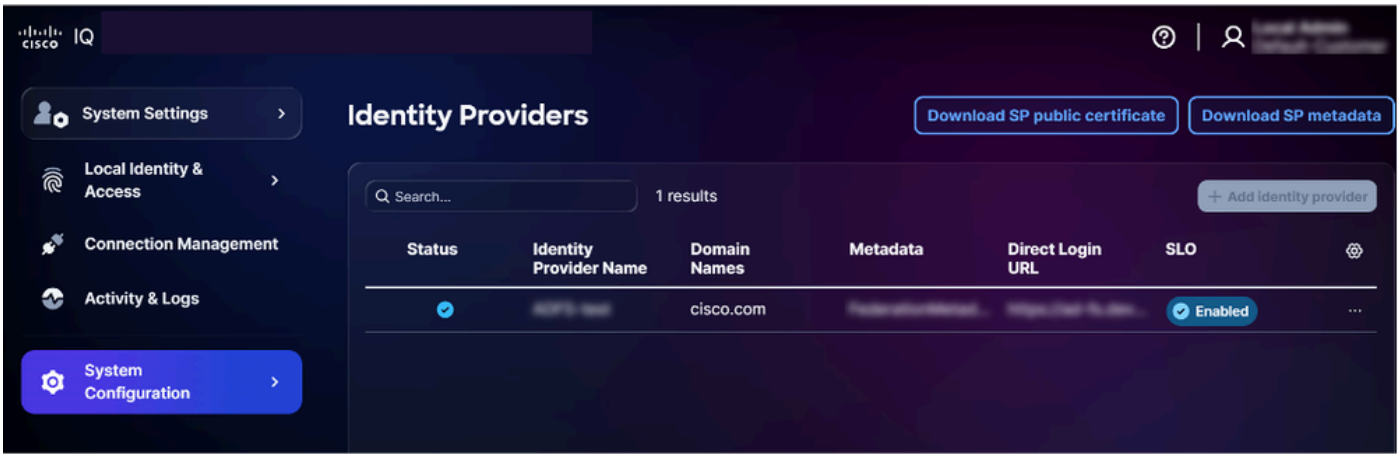
```
$searcher = New-Object DirectoryServices.DirectorySearcher
$searcher.Filter = “(&(objectClass=group)(cn=Role - CXIQ*))”
$searcher.PropertiesToLoad.Add(“distinguishedName”) | Out-Null
$searcher.PropertiesToLoad.Add(“cn”) | Out-Null
$searcher.FindAll() | ForEach-Object { $_.Properties[“distinguishedname”]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

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

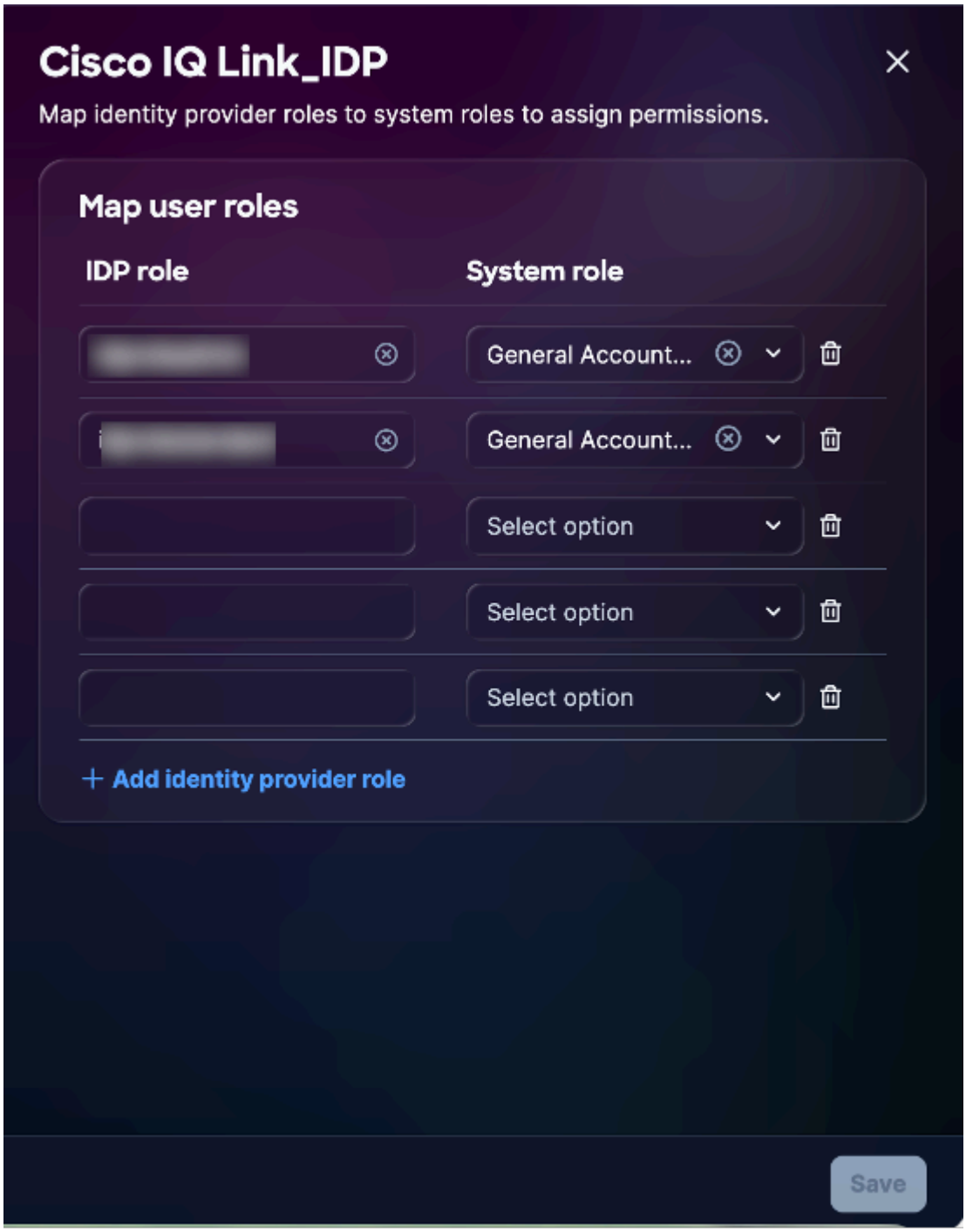
If the required groups are not listed, they must be created in AD by an Account Administrator before you can complete the ADFS role mapping.

To configure role mapping:



Map Roles

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 r**ole. 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**.

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://<YOUR-ADFS-HOSTNAME>: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) underConfiguring Certificate-Based Authentication for more information).

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 the 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 that login is successful.

Note: Both 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 8: 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 • **Wrong group attribute**: Must be *http://schemas.xmlsoap.org/cla ims/Group* • 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* • **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
```

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/certificate-based authentication (CBA).

Prerequisites to Configure Entra ID SAML for SSO

- Microsoft 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 9: 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

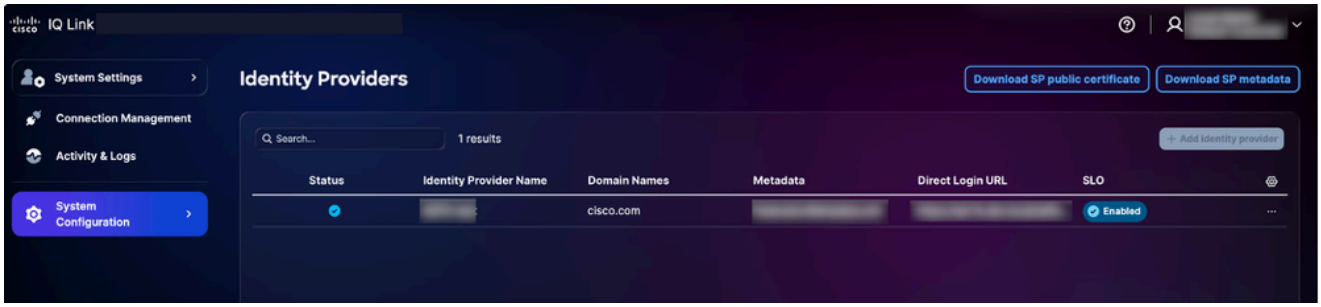
Creating an Enterprise Application

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 Virtual Appliance (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 the SP metadata file. The data from the SP metadata file will auto-populate in the **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:

1. In the Enterprise Application, navigate to **Single sign-on** and choose **SAML**.
2. In the **Basic SAML Configuration** section, click **Edit** and enter the following:
    a. **Identifier (Entity ID)** : <YOUR-CIQ-FQDN>
    b. **Reply URL (ACS URL)** : https://<YOUR-CIQ-FQDN>/saml/acs

c. **Sign on URL** : https://<YOUR-CIQ-FQDN>/saml/login

d. **Logout URL**: https://<YOUR-CIQ-FQDN>/saml/logout

3. 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.

---

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

5. Configure the following claims:

Table 10: Required SAML Claims

Claim	Source Attribute	Namespace
Unique User Identifier (NameID)	user.userprincipalname	*(default)*
emailaddress	user.mail	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
givenname	user.givenname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
surname	user.surname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
name	user.userprincipalname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
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, 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 Identifiers (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, go to **Single sign-on** > **SAML Signing Certificate** section.
2. Download Federation Metadata XML (save as entra-id-metadata.xml).

   Or

   Download Certificate (Base64) for manual certificate entry.
3. Take a 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 11: 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 under Configuring Entra ID SAML Application for more details).

3. 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 “authentication successful|Extracted group|To
```

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 Certificate Services (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=<USER-UPN>”
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=<USER-UPN>&”
_continue_ = “email=<USER-UPN>”
“@ | 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 command:

```
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-UPN>*” }
$password = ConvertTo-SecureString -String “<EXPORT-PASSWORD>” -Force -AsPlainText
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-db -P “<EXPORT-PASSWORD>”
```

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

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

- 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 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. At 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 cert or an expired cert) 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 12: 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 under Configuring Entra ID SAML Application for more details). Check that the user has mail attribute populated.
Total groups extracted: 0	Group claims not configured or wrong source	Use user.assignedroles as the source. Ensure the user is assigned to an App Role (see Assigning Users to App Roles under Configuring Entra ID SAML Application for more details).
Duplicate group claims	Both user.groups and user.assignedroles active	Remove the user.groups claim. Keep only user.assignedroles.
Groups showing as UUIDs	Source attribute is	Use the App Roles approach (see Configuring

Issue	Cause	Fix
	“Group ID”	App Roles under Configuring Entra ID SAML Application for more details).
Attribute Name shows long URI	Namespace field is not empty	Clear the **Namespace** field in the groups claim settings.
Invalid SAML signature	IdP certificate rotated or mismatch	Re-download metadata from Entra ID and re-upload to Cisco IQ.
AADSTS500191	CRL not reachable from internet	Publish the CRL to a publicly accessible URL, or use self-signed CA approach (see CRL Workaround for Lab Environments for more details).
Certificate not prompted	Certificate not in Keychain, CA not trusted on client, or CBA not enabled	Verify that the user certificate is imported in macOS Keychain Access (see Importing the User Certificate on Client Machine (macOS) underConfiguring Certificate-Based Authentication for more details), CBA is enabled in Entra ID with required settings (see Enabling CBA in Entra ID Authentication Methods under Configuring Certificate-Based Authentication for more details) and Chrome is restarted to apply changes.
SAML assertion expired	Clock skew between systems	Increase clock_skew_seconds in plugin config (default 300, use 30000 for lab).
Status “Incomplete” in VA	Role mapping not yet configured	Complete role mapping (see Configuring Role Mapping for more details).

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=<USER-UPN>” `
    -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=<USER-UPN>&email=<USER-UPN>”
)
```

Upload only the root CA cert to Entra ID. Since it is self-signed with no 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 Enterprise Application (Non-gallery) in Entra ID
- Configure 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 Federation Metadata XML

Cisco IQ Configuration

- Add Identity Provider in Cisco IQ by uploading Entra ID metadata
- Configure 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 user certificate with UPN matching Entra ID user
- Export user certificate as PFX and install on client machine
- Trust the CA certificate on the client machine
- Upload CA root certificate to Entra ID under **Protection** > **Certificate authorities**
- Enable CBA in Authentication methods

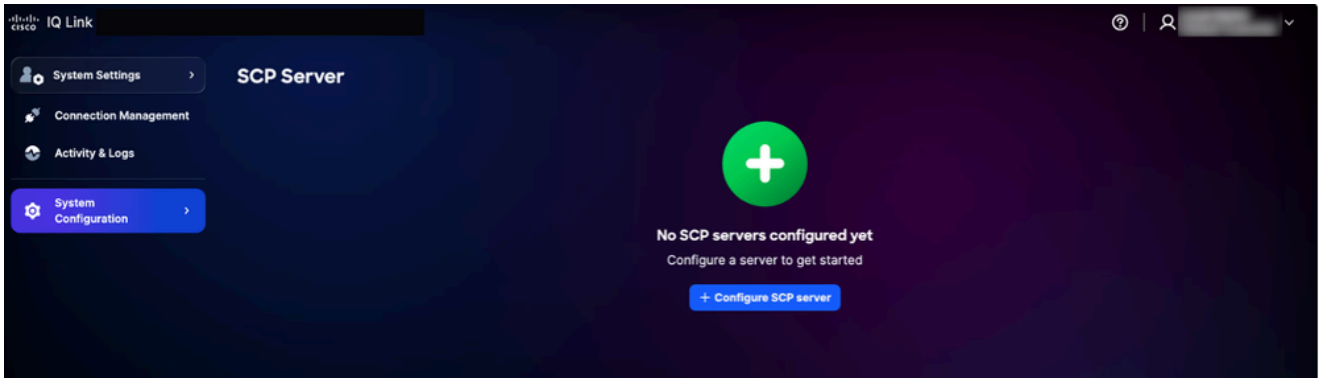
- Configure username binding (*PrincipalName* and *userPrincipalName*)
- Verify CBA login works end-to-end

Adding SCP Servers

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

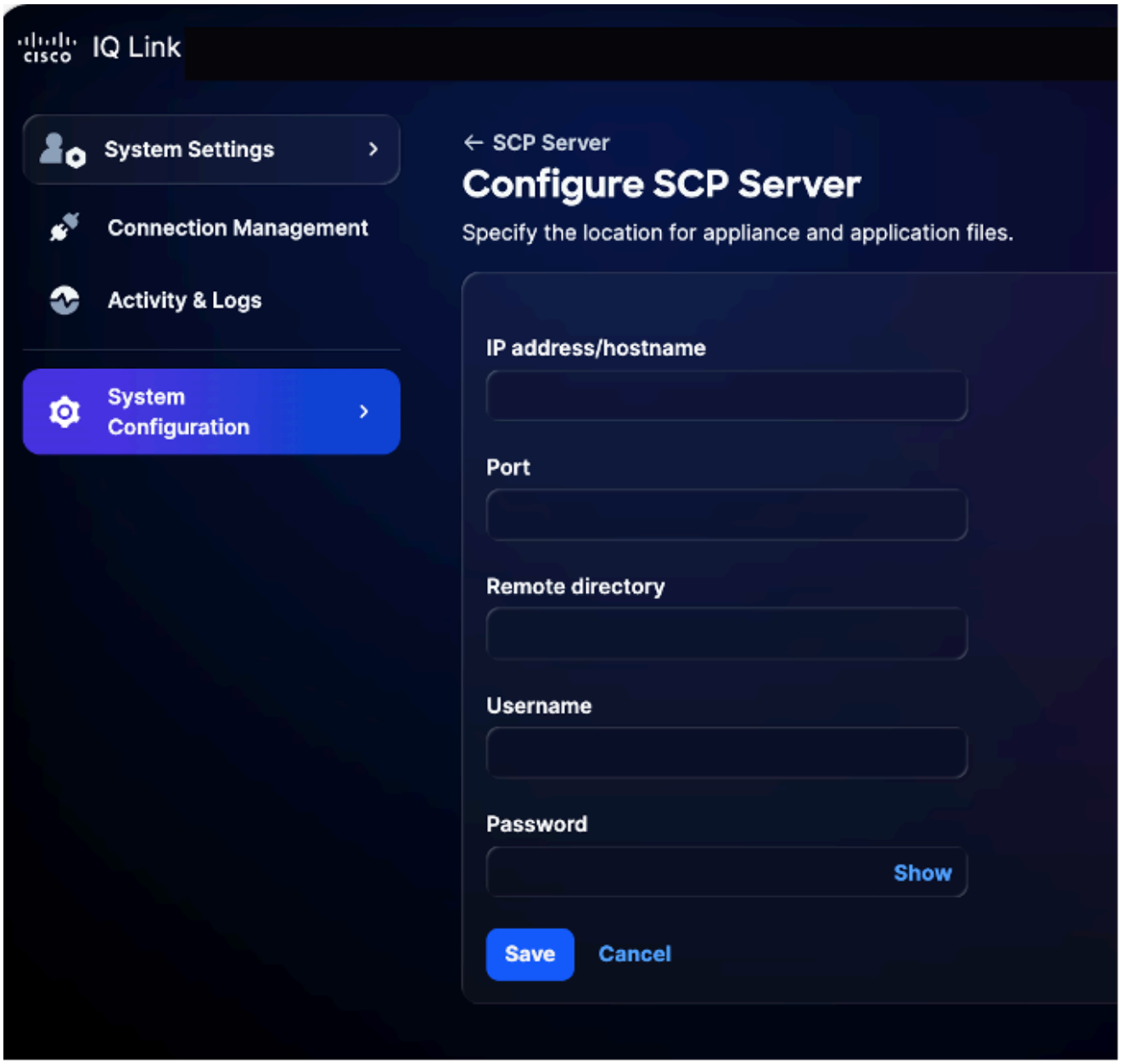
To add a SCP Server:

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.

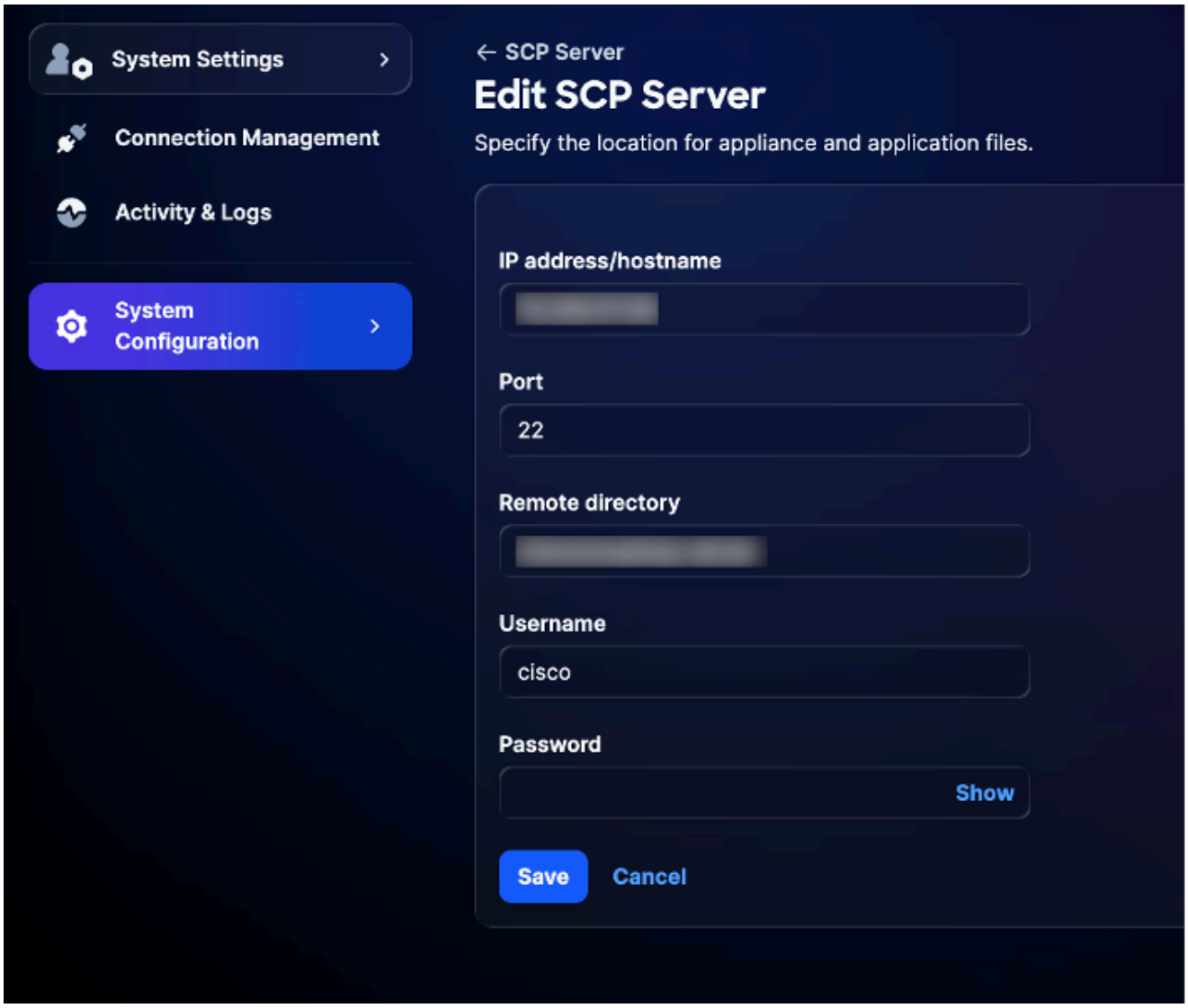
Editing Existing SCP Servers

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**.

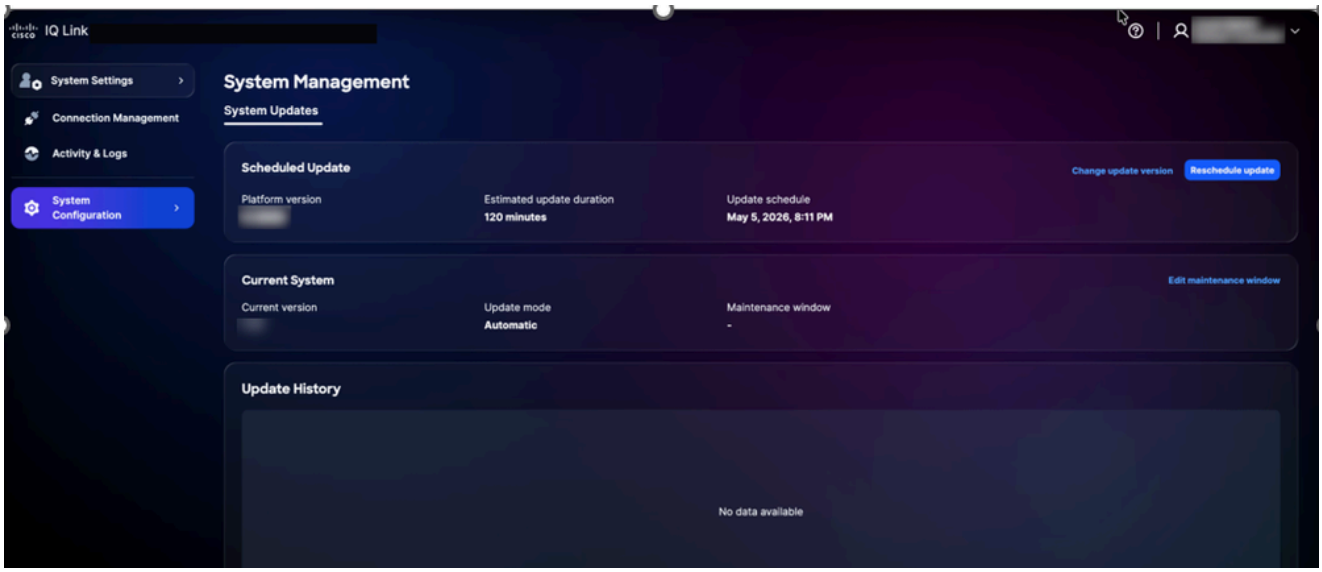
System Management

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

Rescheduling System Update

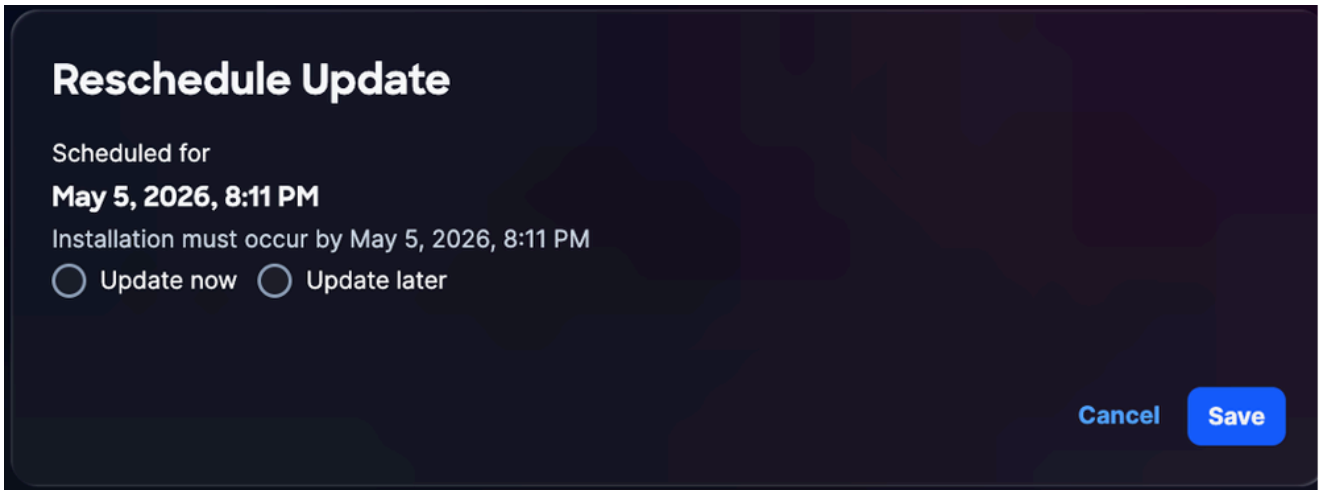
To reschedule the system update:

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**.

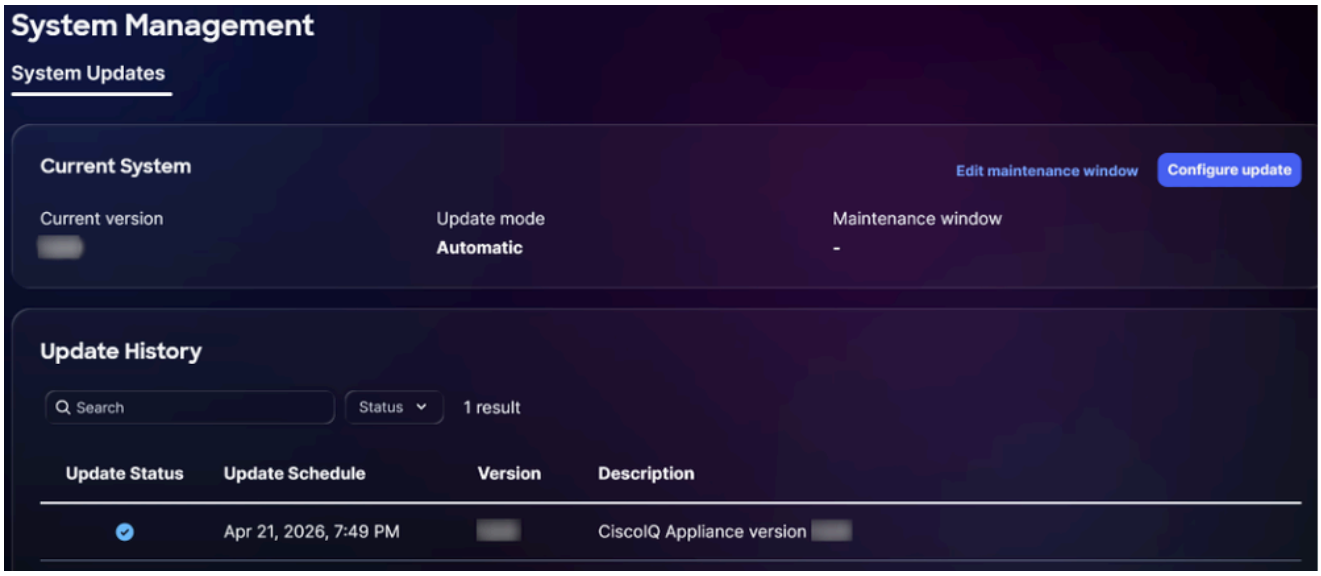


Reschedule Upgrade

3. Choose the **Update Now** radio button for immediate rescheduling or the **Update Later** radio button to

schedule another time.

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

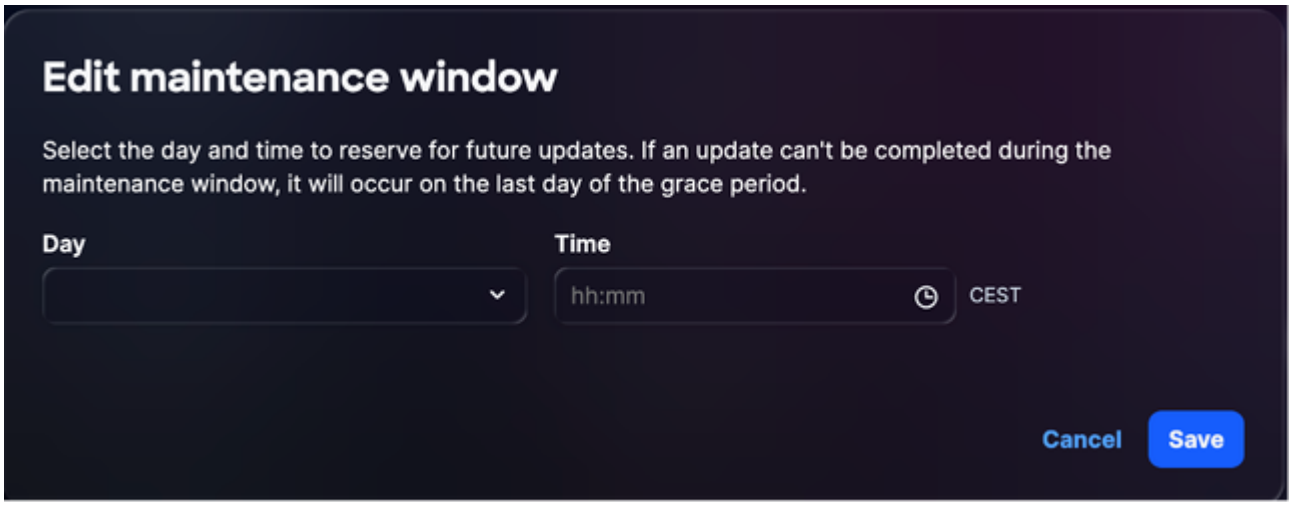


Successful Upgrade

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:

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.

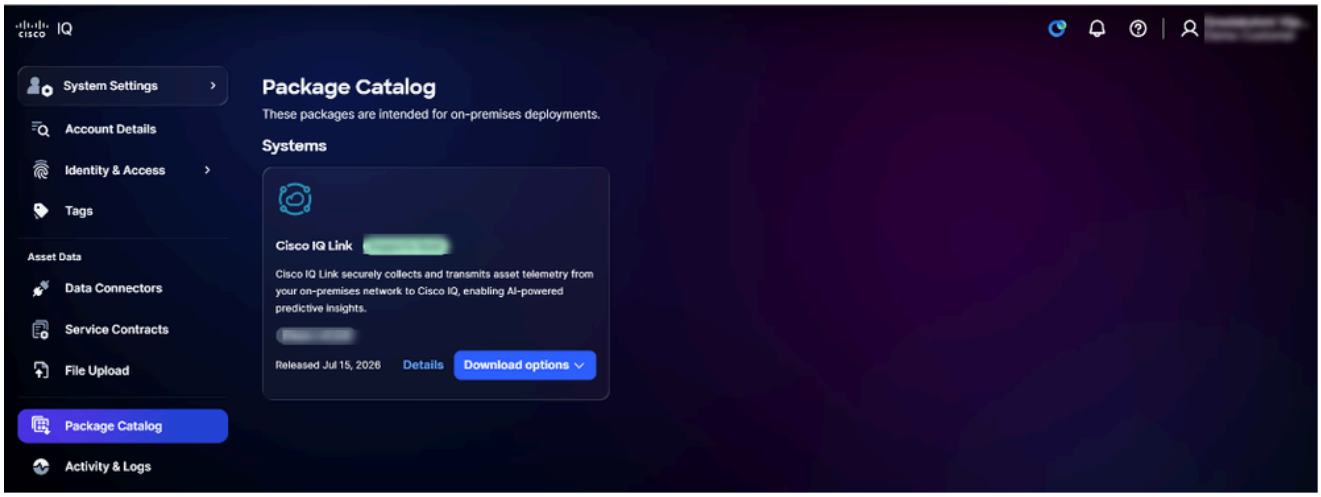
3. Click **Save**. The maintenance window has been successfully scheduled. The update is triggered according to the displayed schedule.

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.

Manually Upgrading the System

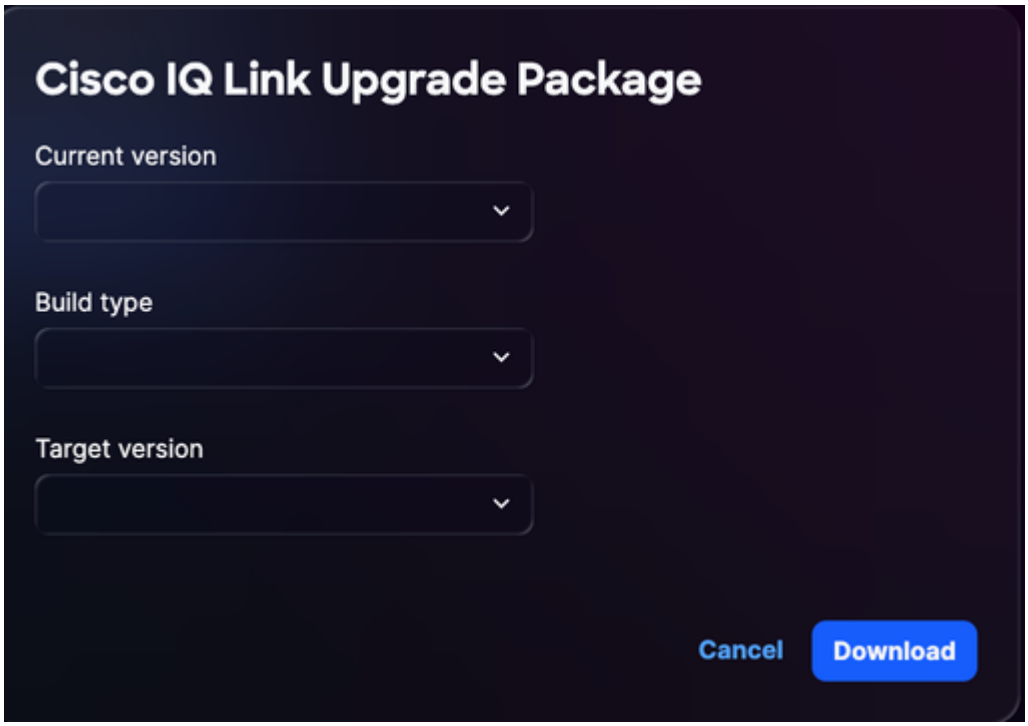
In scenarios where automatic distribution from Cisco IQ SaaS is either unavailable or delayed, you can manually perform a system upgrade by downloading the upgrade bundle directly from Cisco IQ SaaS. To manually upgrade the system:

1. Log in to Cisco IQ SaaS choose **Home** > **System Settings** > **Package Catalog**.



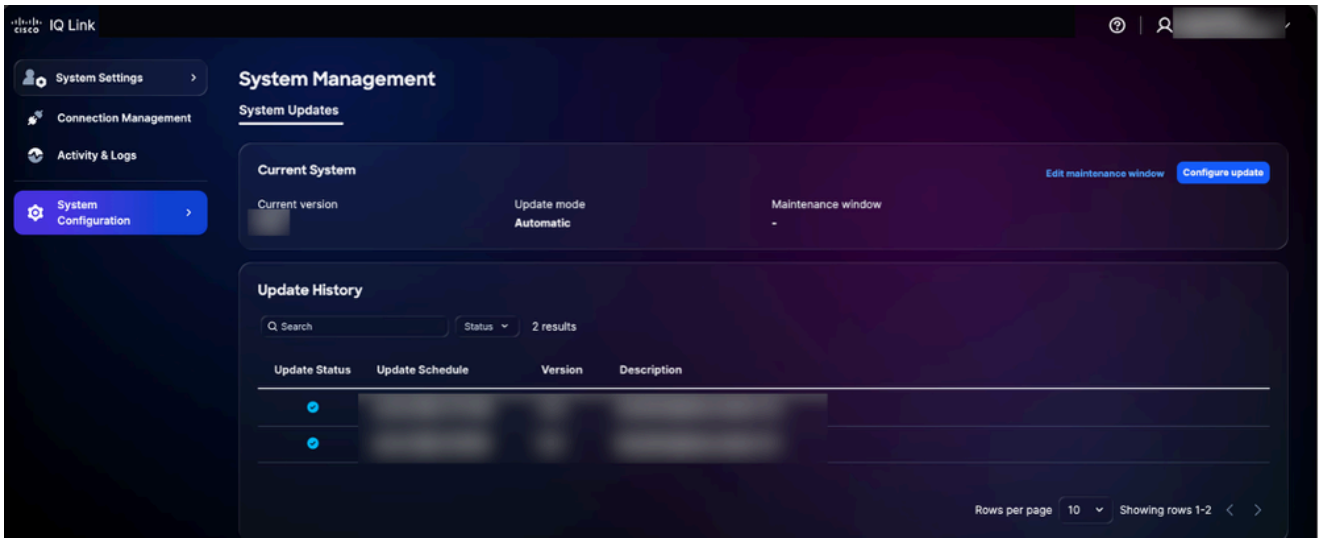
Package Catalog

2. In **Cisco IQ Link** section, click **Download options** > **Upgrade packages**.



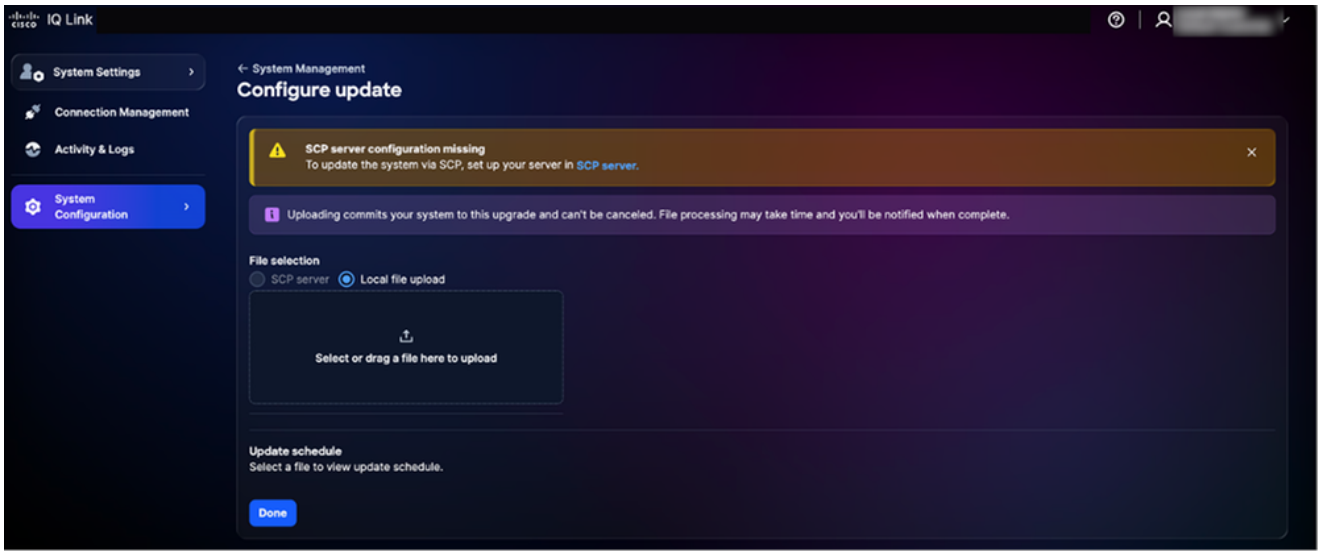
Upgrade Package

3. Choose the **Current version** from the drop-down list.
4. Choose the **Build type** from the drop-down list.
5. Choose the **Target version** from the drop-down list.
6. Click **Download**. The upgrade bundle downloads.
7. Navigate to Cisco IQ Link.
8. From **System Settings**, choose **System Configuration** > **System Management**.



Configure Update

9. Click **Configure update**.



Local File Upload

10. Click the **Local file upload** radio button.

11. Select or drag the downloaded upgrade bundle file into the upload field.
12. Click **Done**. A confirmation message displays after the system is successfully updated.

SSL Certificates Configuration

A default self-signed certificate is pre-installed and enabled in Cisco IQ, but you 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.

The default SSL certificate cannot be edited or deleted.

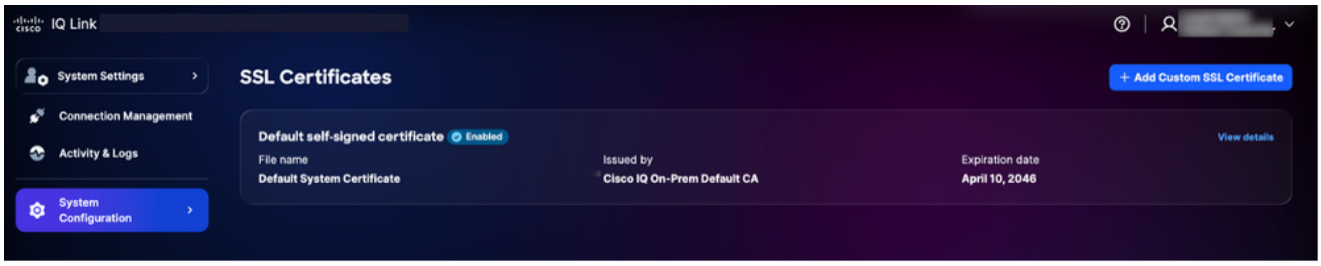
Note: The certificate must have at least 90 days of validity remaining. A certificate is considered "nearing expiry" when it has less than 90 days remaining until expiration.

After adding, editing, or deleting an SSL certificate, you must upload the new SSL certificate as outlined in Single Logout 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.

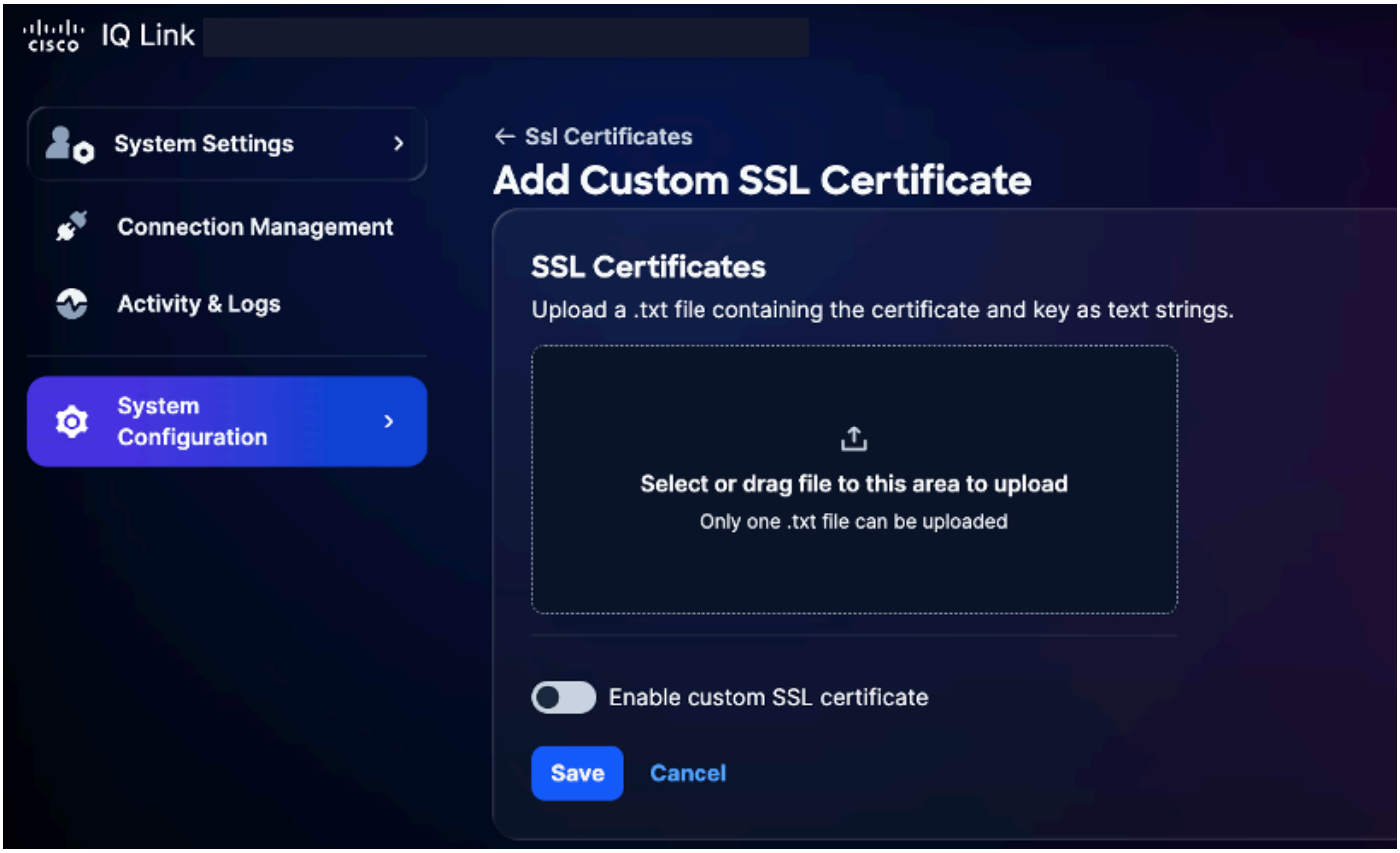


Adding SSL Certificate

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

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

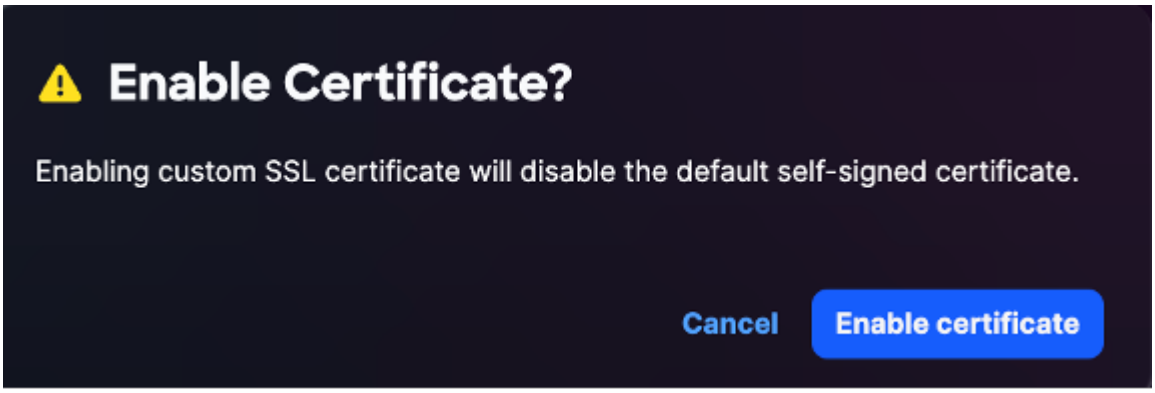
---



Upload SSL Certificate

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.



Edit SSL Certificate

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

5. Click **Enable certificate**.

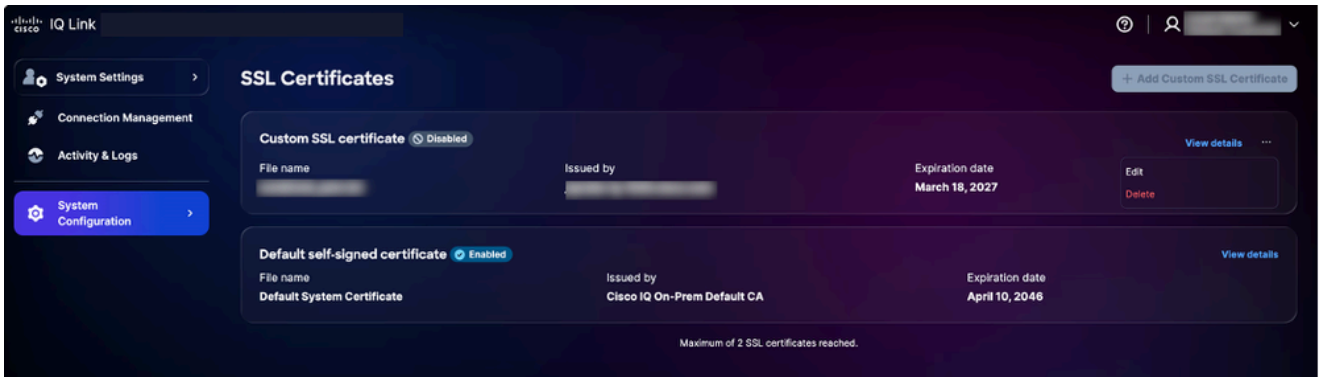
6. Click **Save**.

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

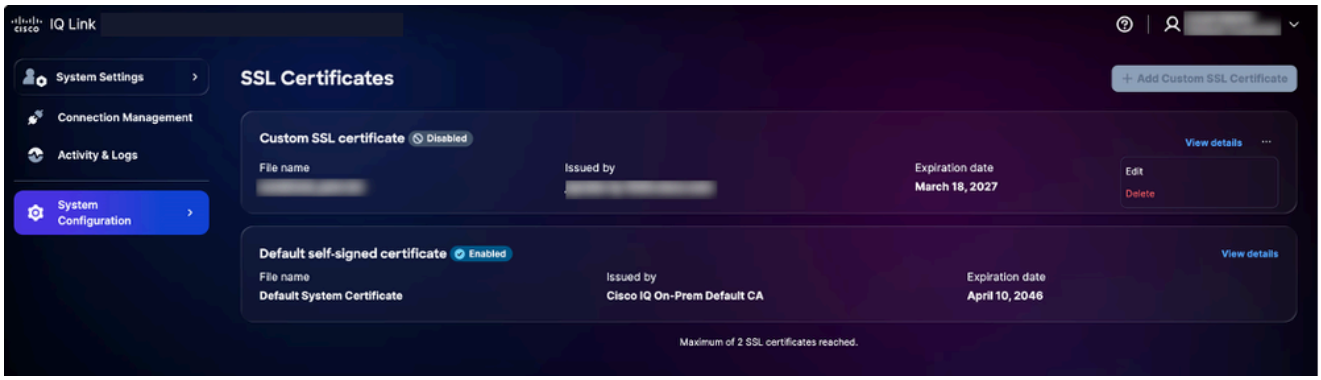
2. Choose the **More Options** icon > **Edit**. The **Edit SSL Certificate** page displays.
3. Edit the certificate details as required.
4. Click **Save**.

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 custom 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

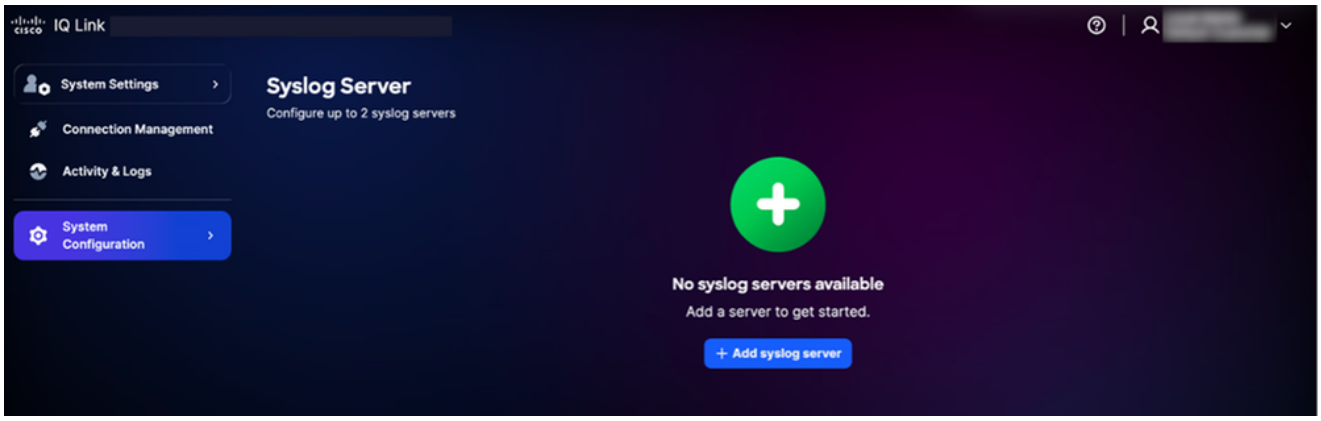
Users with the Account Administrator role can configure external syslog servers to export system logs. Up to two (2) syslog servers can be configured.

Note: The Syslog server must be specified as an IP address, not a FQDN.

Adding Syslog Servers

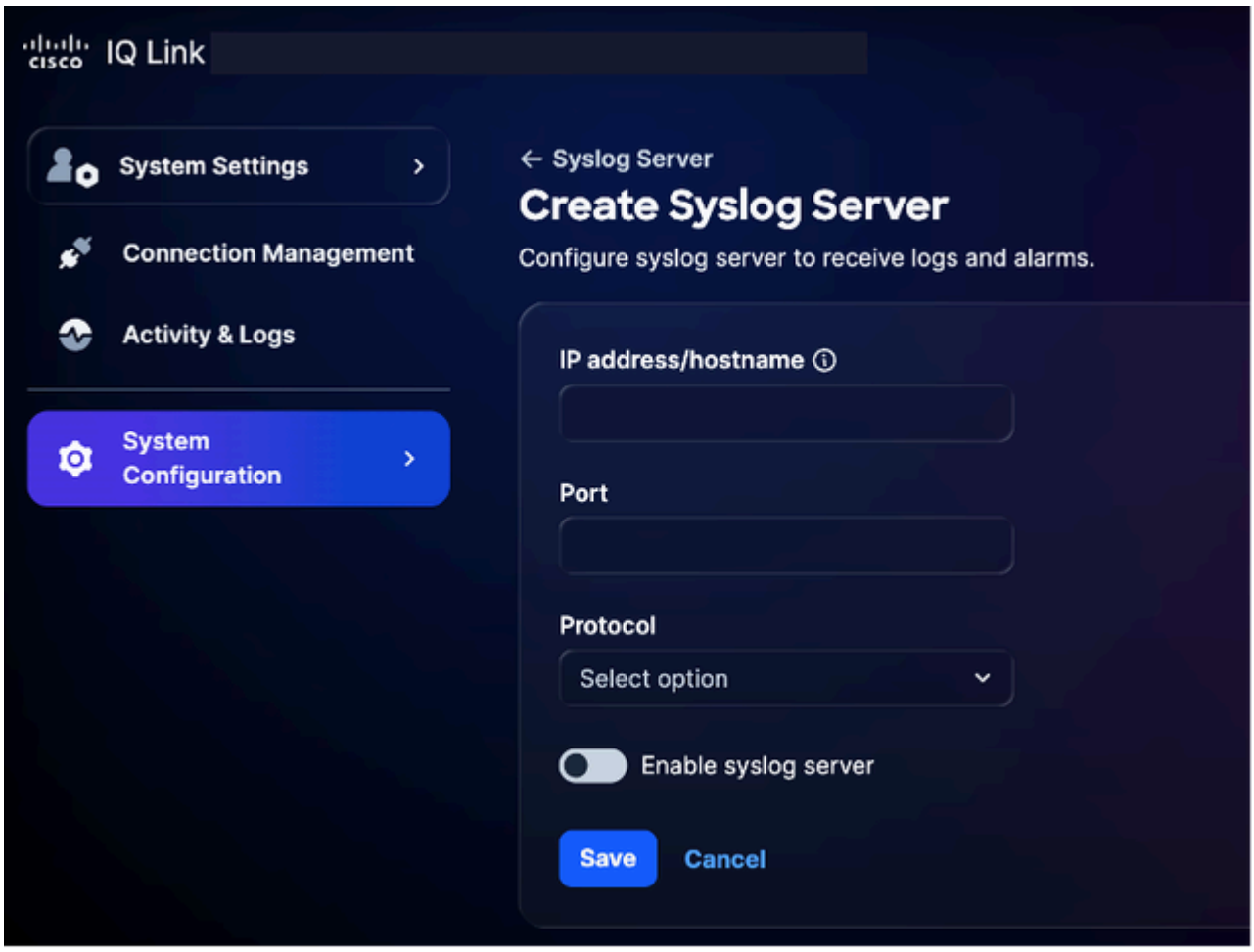
To add a syslog server:

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.



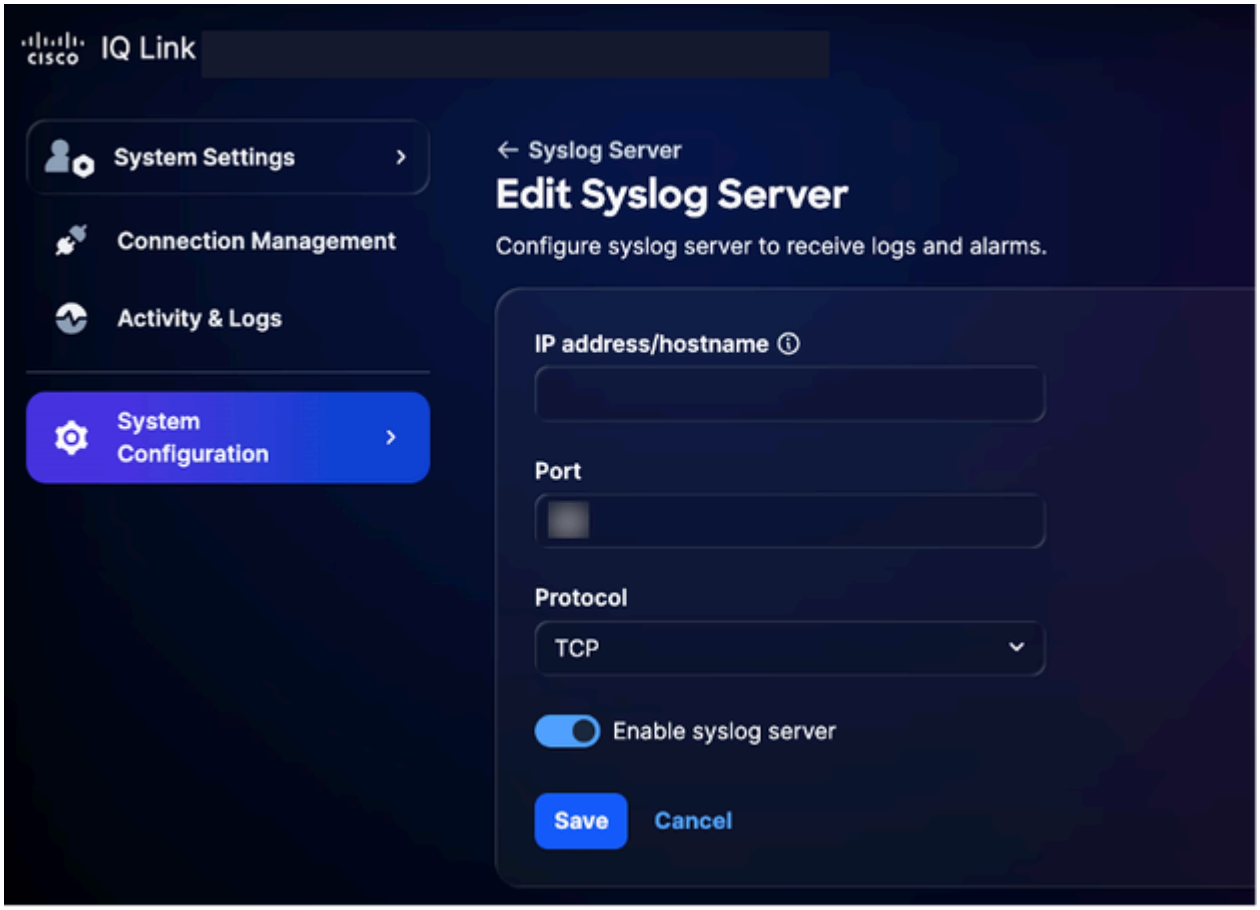
Create Syslog Server

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.



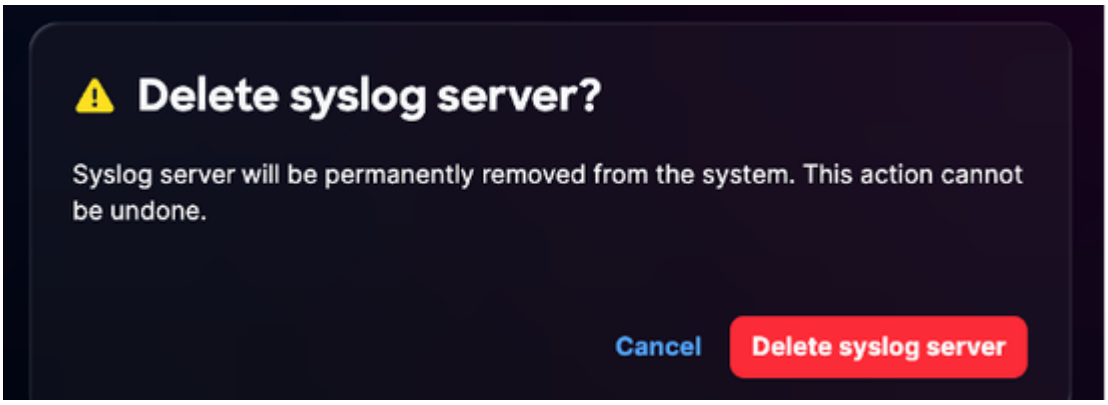
Edit Syslog Server

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.

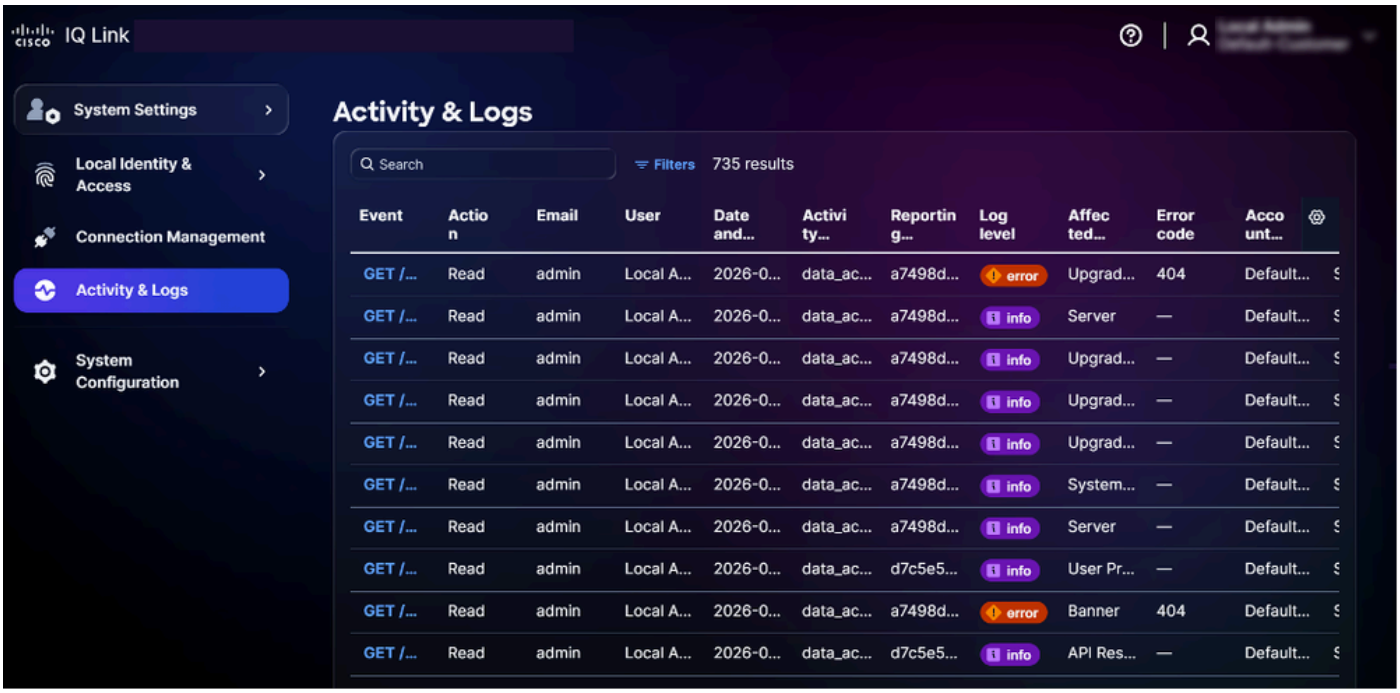


Confirmation

3. Click **Delete syslog server**.

Activity & Logs

Activity & Logs provide a detailed record of user actions and changes in Cisco IQ, allowing Account 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:

- Supports filters, pagination, and search capabilities to help easily find and manage information

- Records all API operations at the gateway level

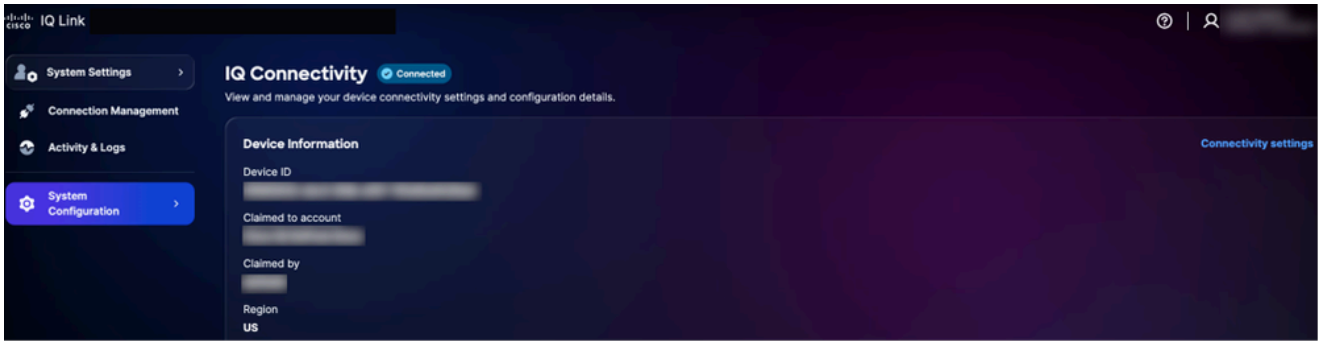
The following filter options are available:

- **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

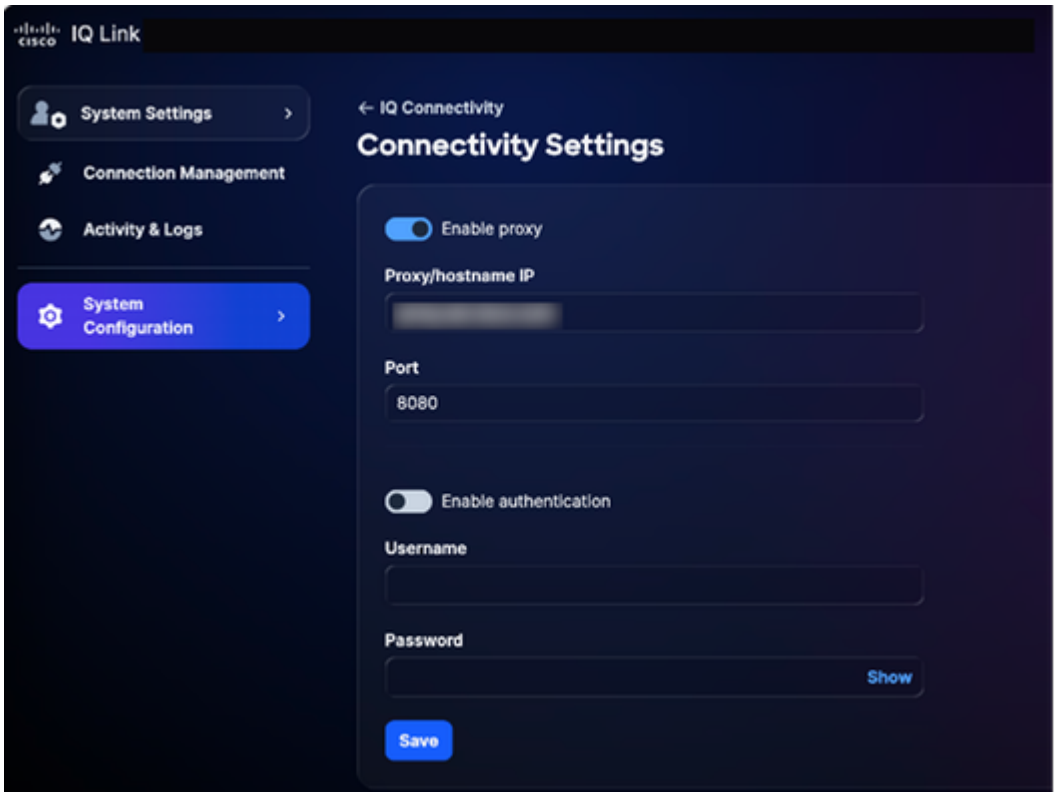
To view and manage your device connectivity settings and configuration details:

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 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 is summarized below:

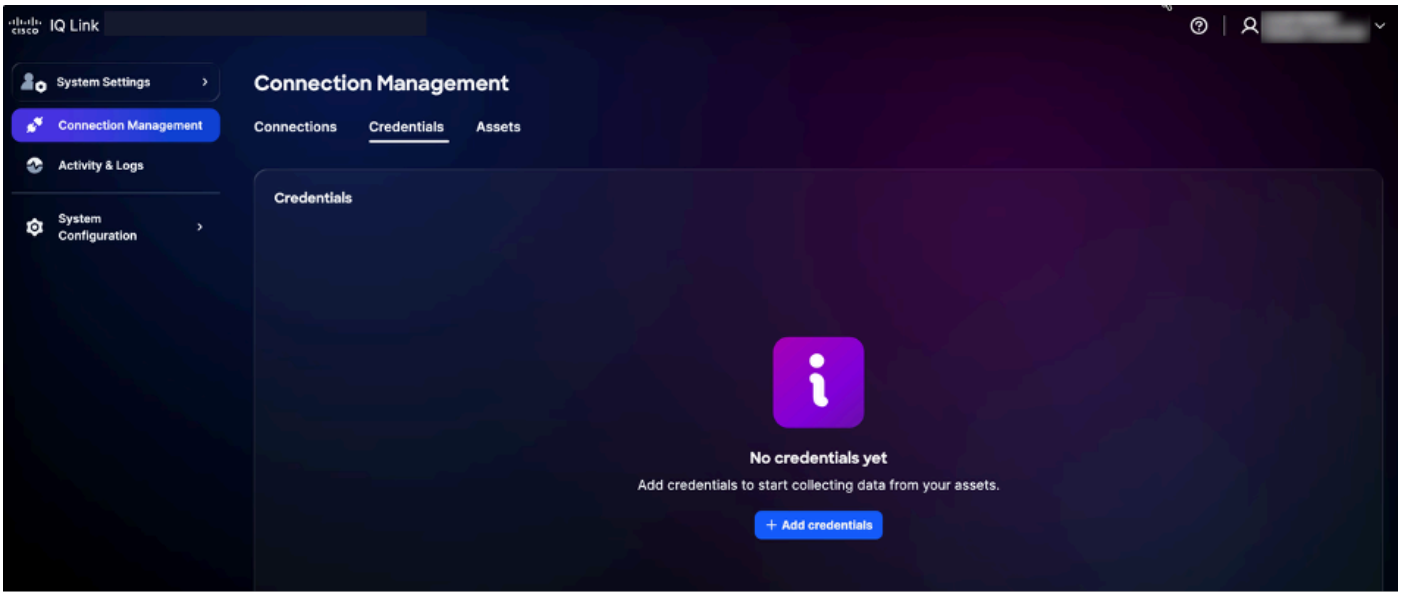
- **Creating Credential Sets**: Establish the authentication protocols (for example, Simple Network Management Protocol (SNMP) v1/v2c/v3) to communicate with your network devices. Centralizing credentials by security zone or location (for example, “SanJose-SNMPv3”) allows you to update passwords in one 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

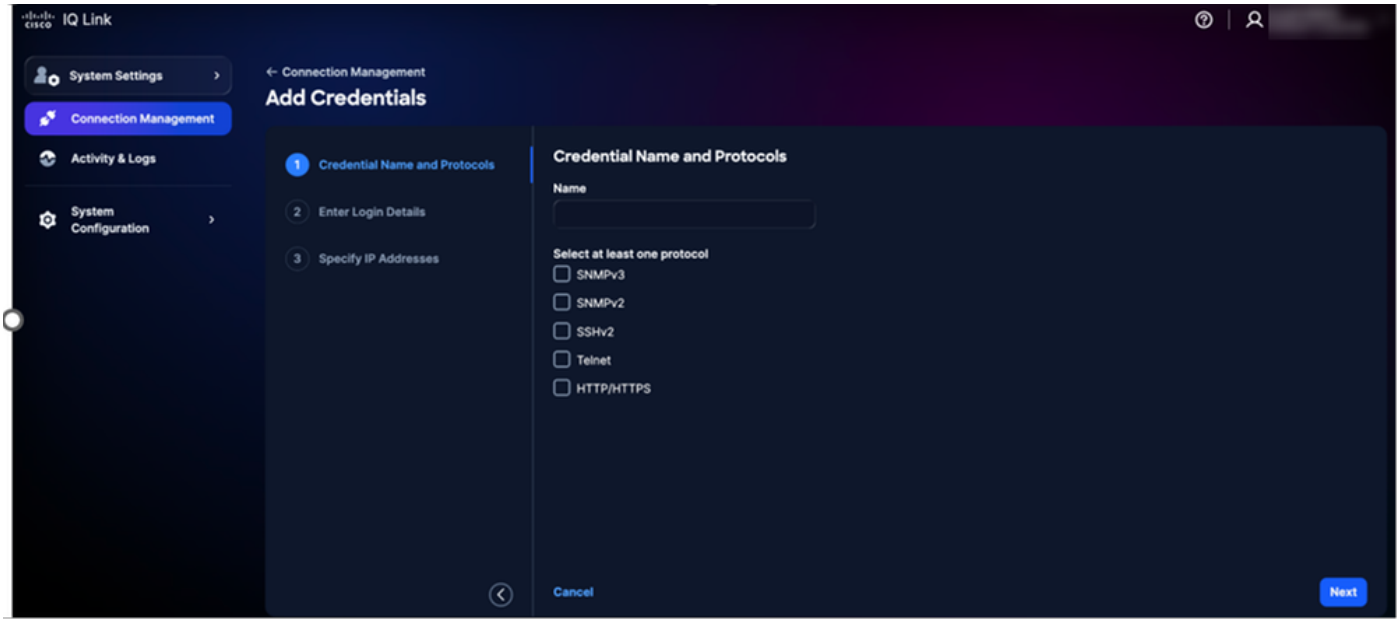
You must first add credentials to perform data collection. To add credentials:

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



Credentials Tab

3. Click **Add credentials**.

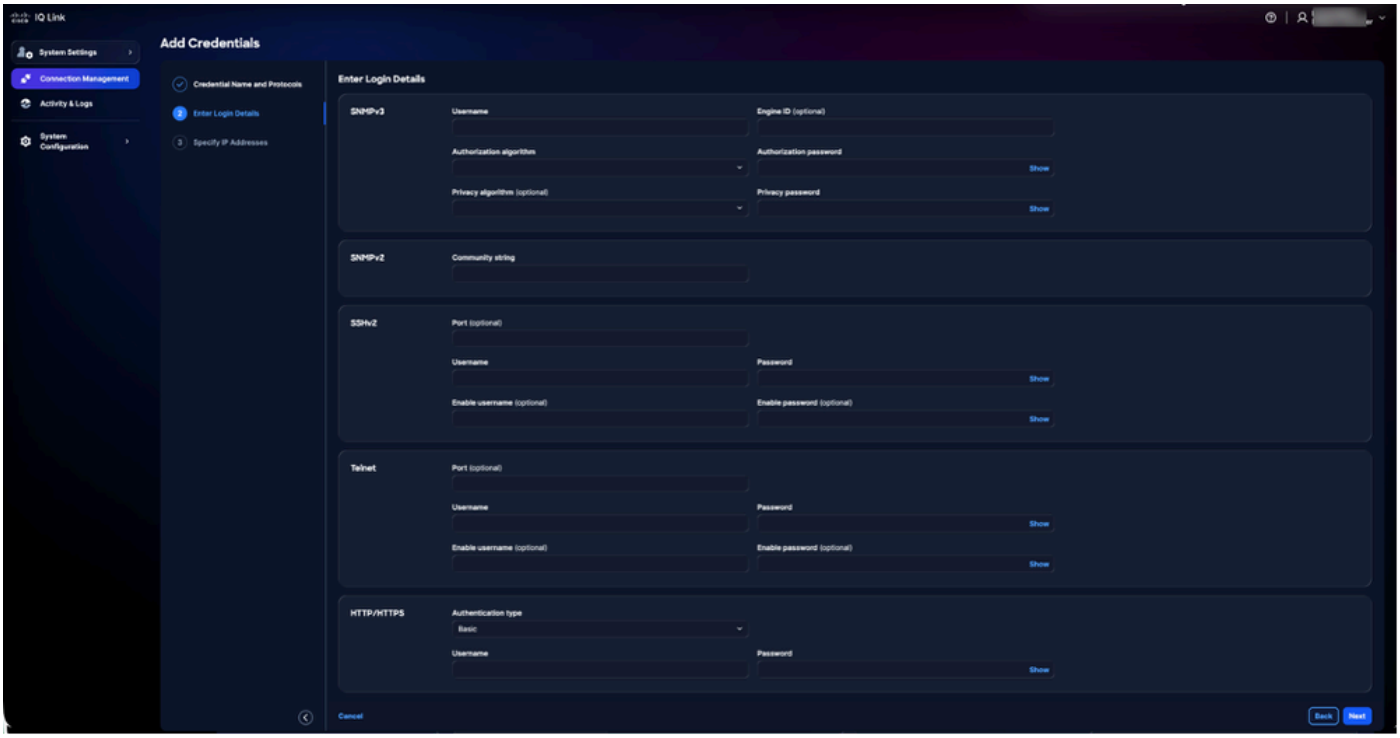


Add Credentials

4. Enter **Name**.

5. Check all applicable protocol check boxes.

6. Click **Next**.



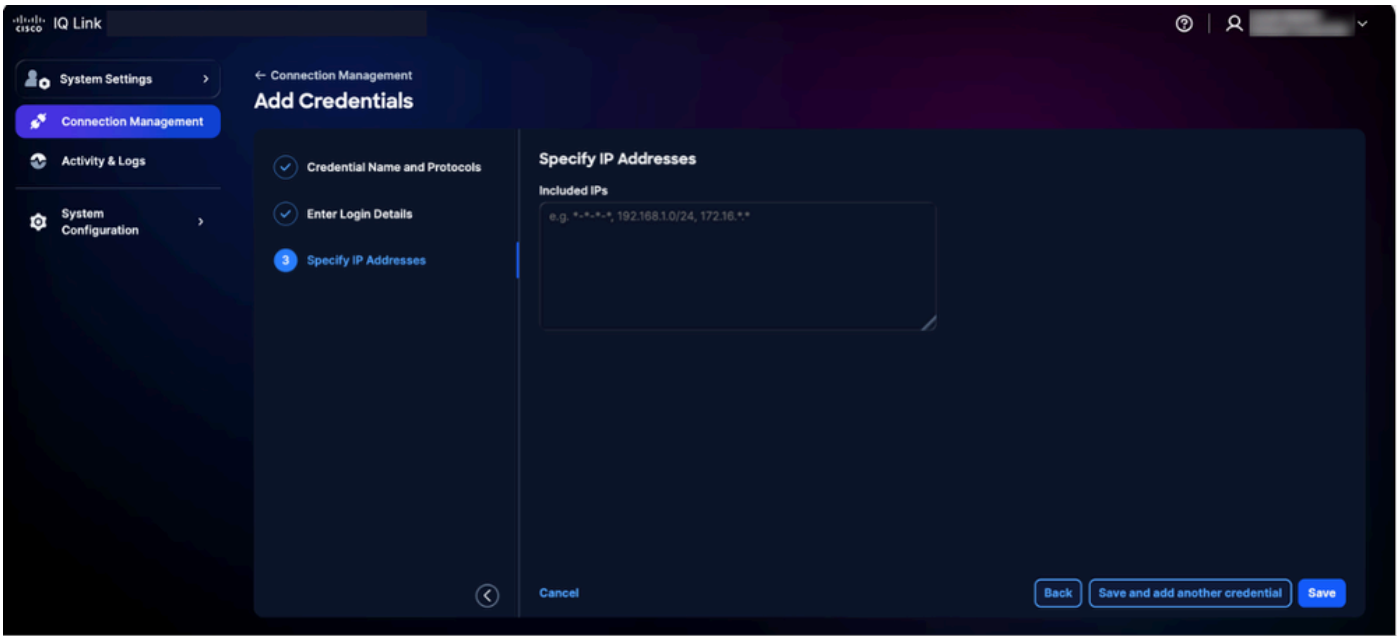
Add Credentials Details

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

---

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

8. Click **Next**.



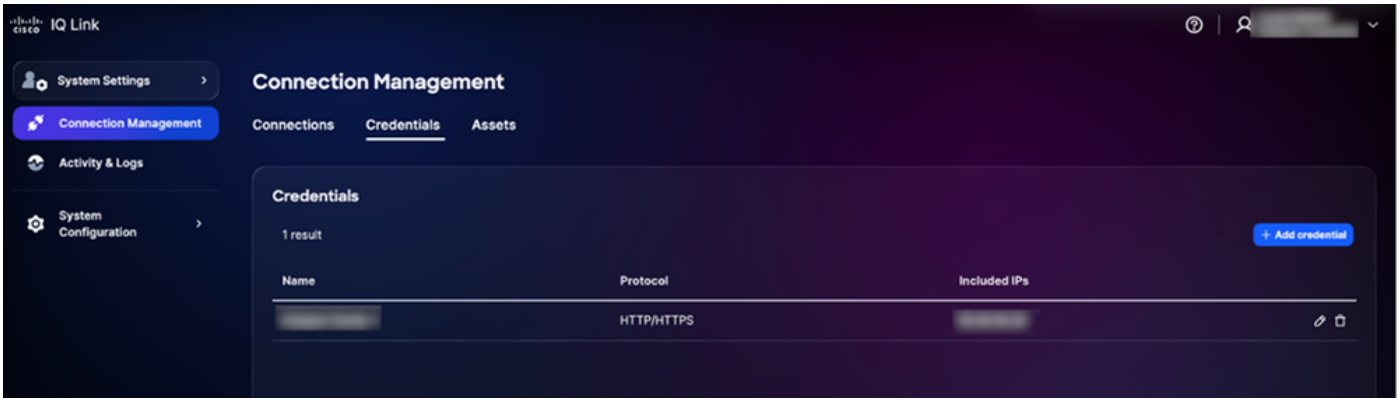
Specify IP Addresses

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.

Table 13: 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)

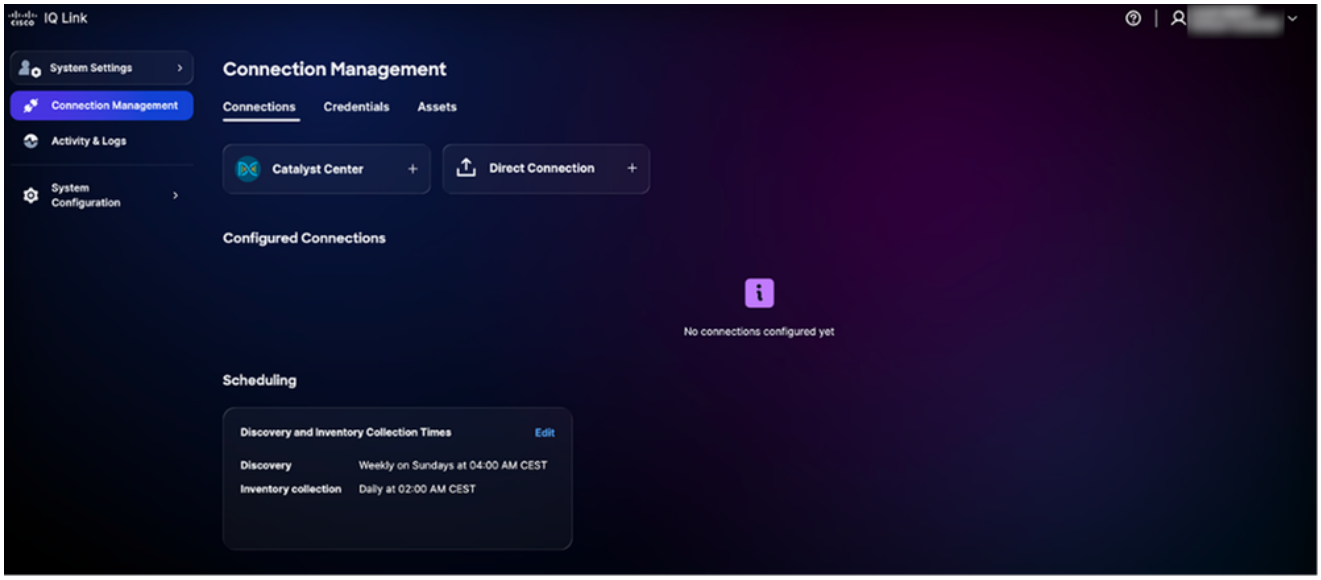
Note: If a device falls into multiple overlapping categories, the system always selects the credential set with the highest specificity (in other words, the fewest trailing wildcards).

Data Collection Using Catalyst Center

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

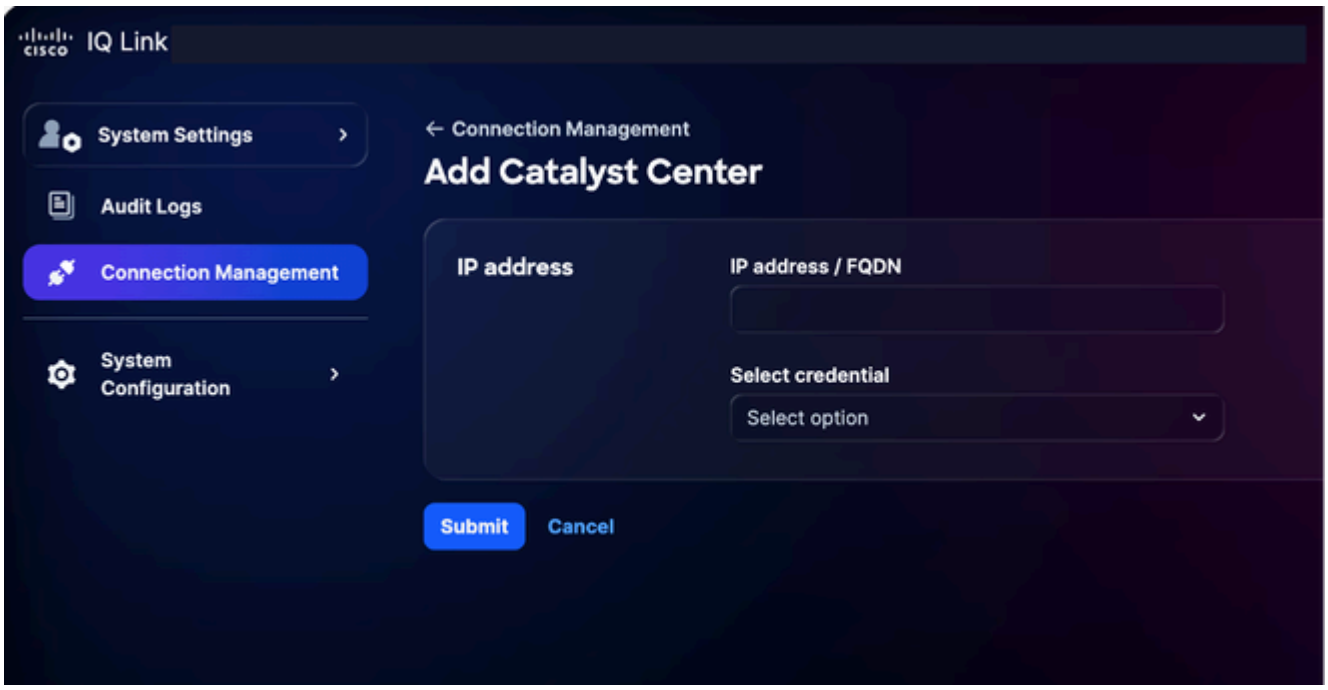
For data collection using Catalyst Center:

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



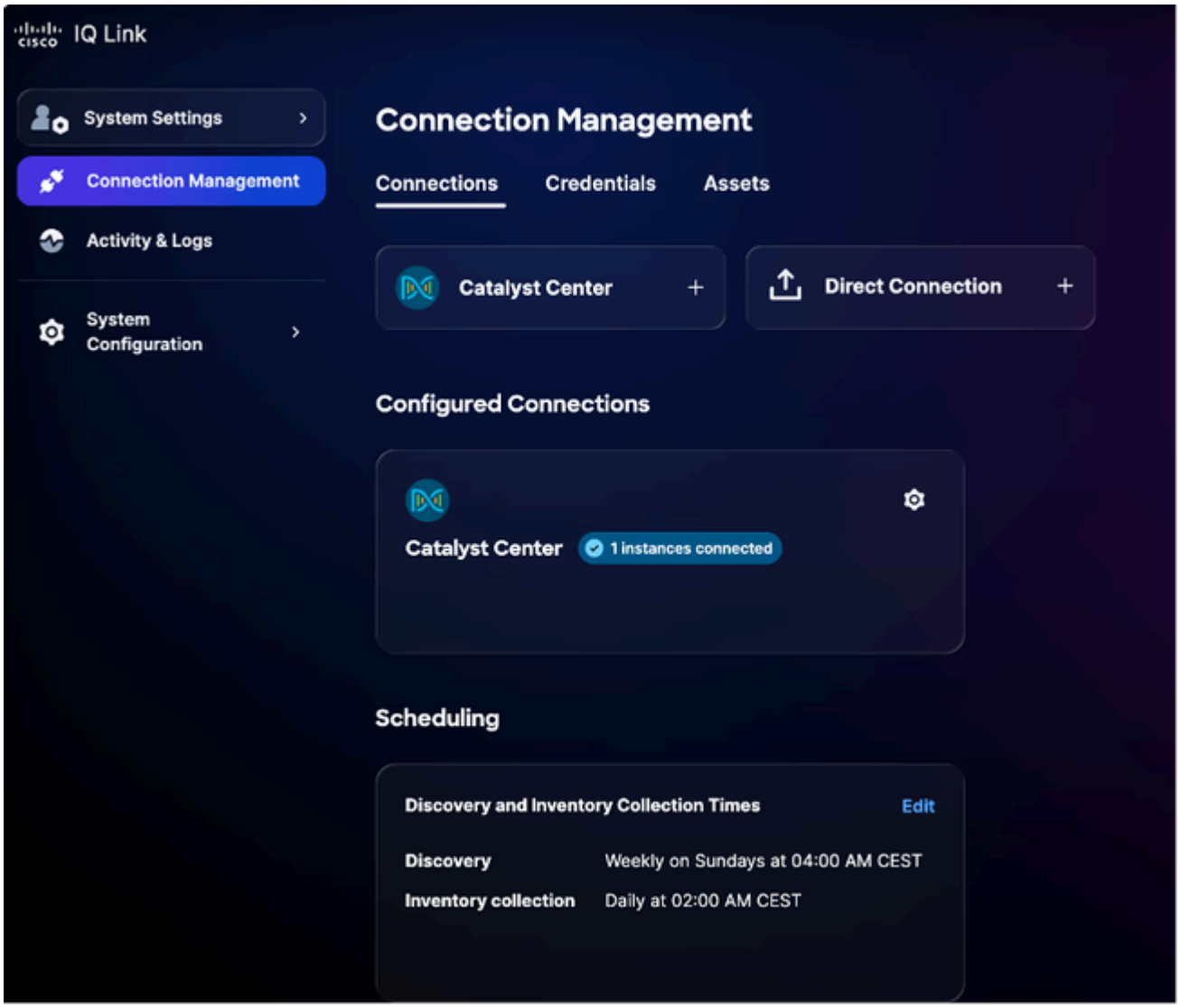
Connection Management

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

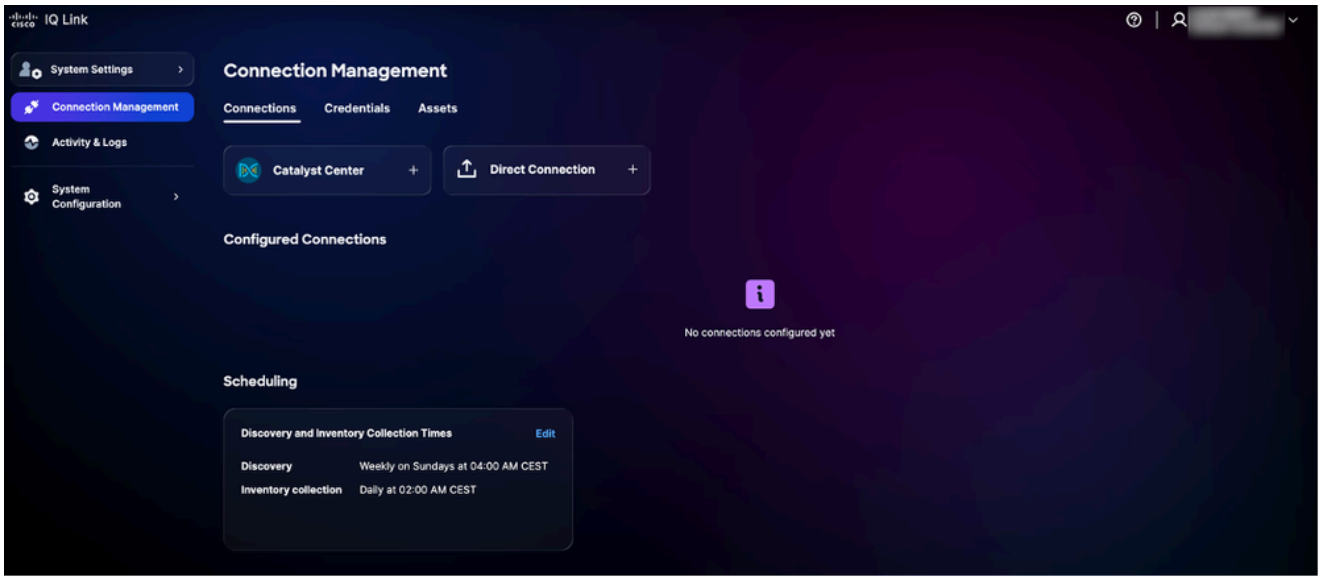
6. Schedule a collection. See Scheduling for more details.

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

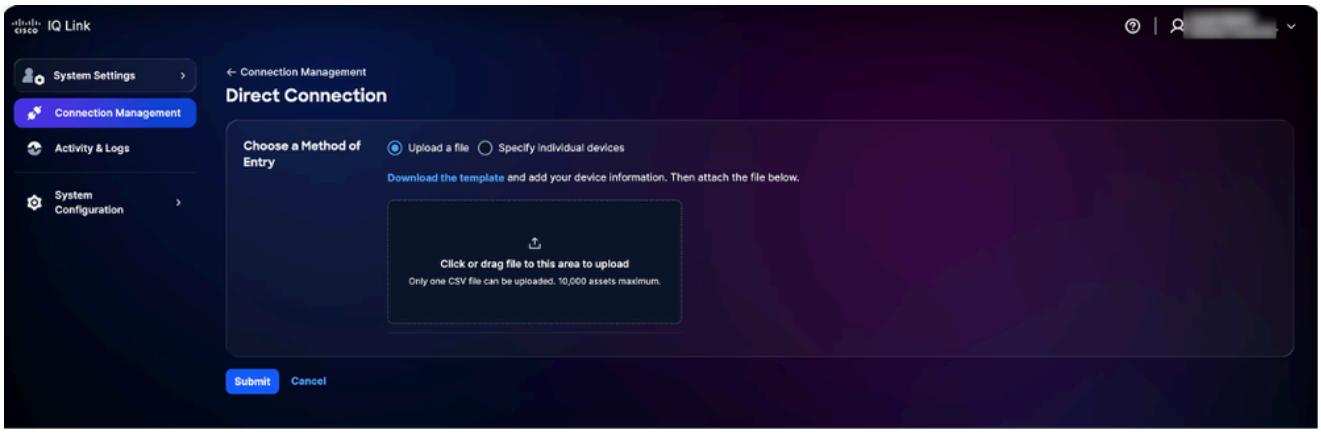
To add devices for direct connection:

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



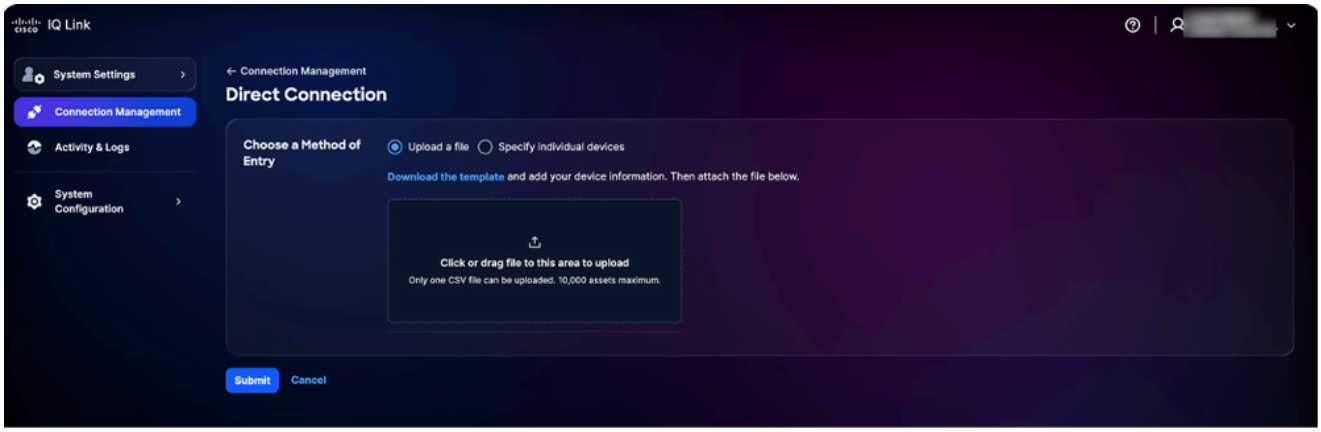
Connection Management

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



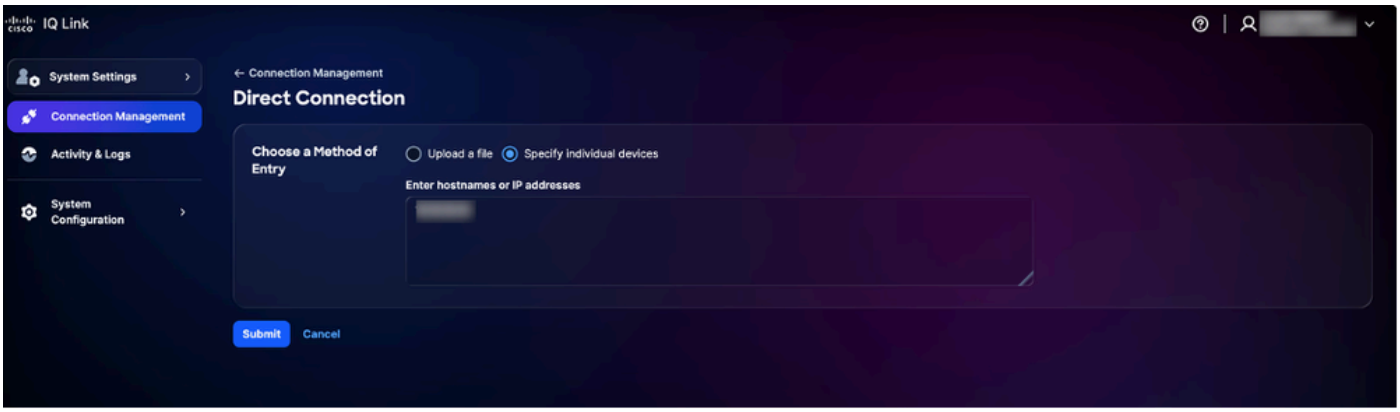
Upload File

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 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.

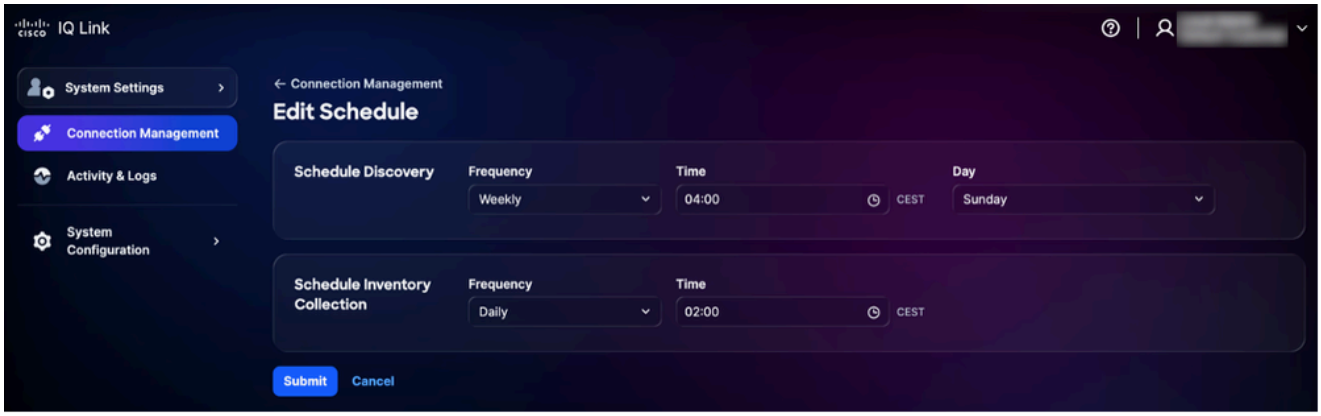
4. Schedule a collection. See Scheduling for more details.

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

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

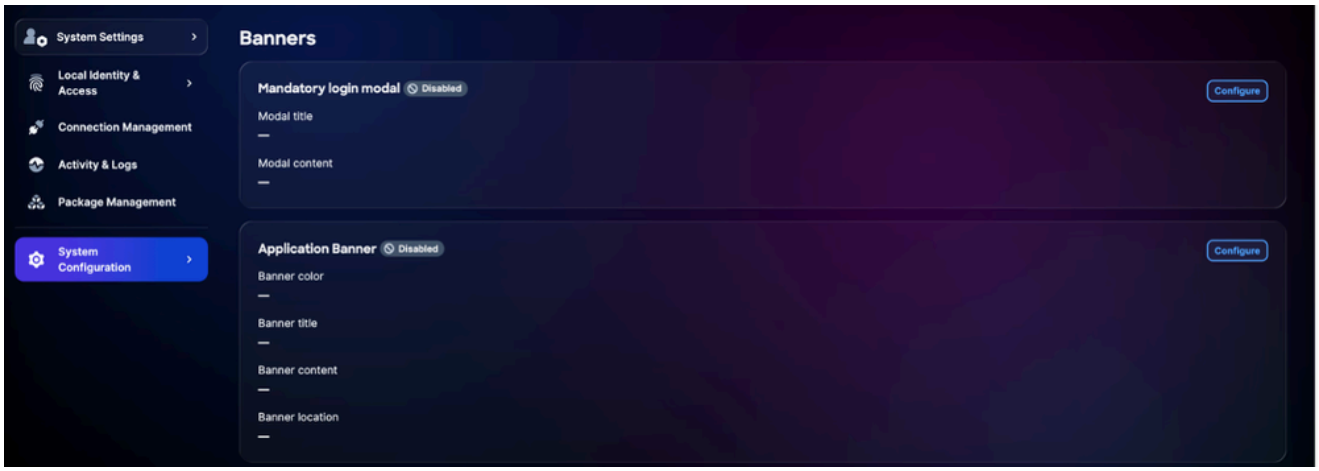
Account Administrators can configure system-wide banners to meet security and compliance standards.

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

Configuring Mandatory Login Modal Banners

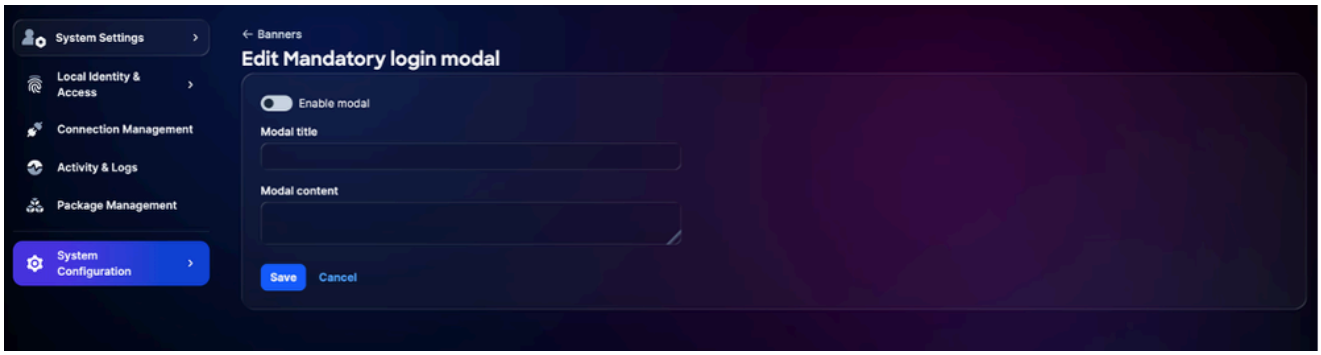
To configure a mandatory banner:

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.



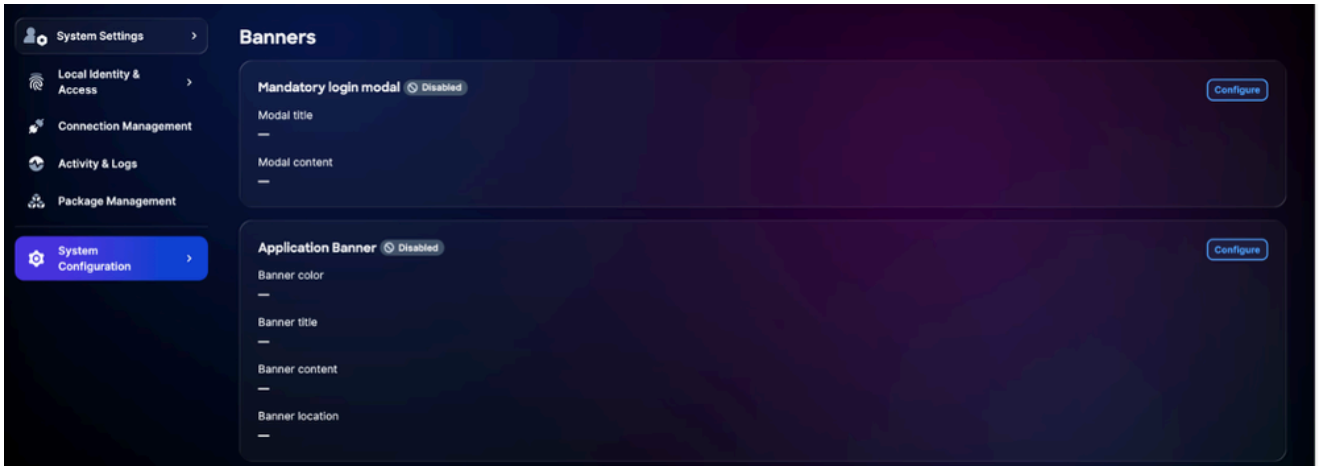
Edit Mandatory login modal Banner

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

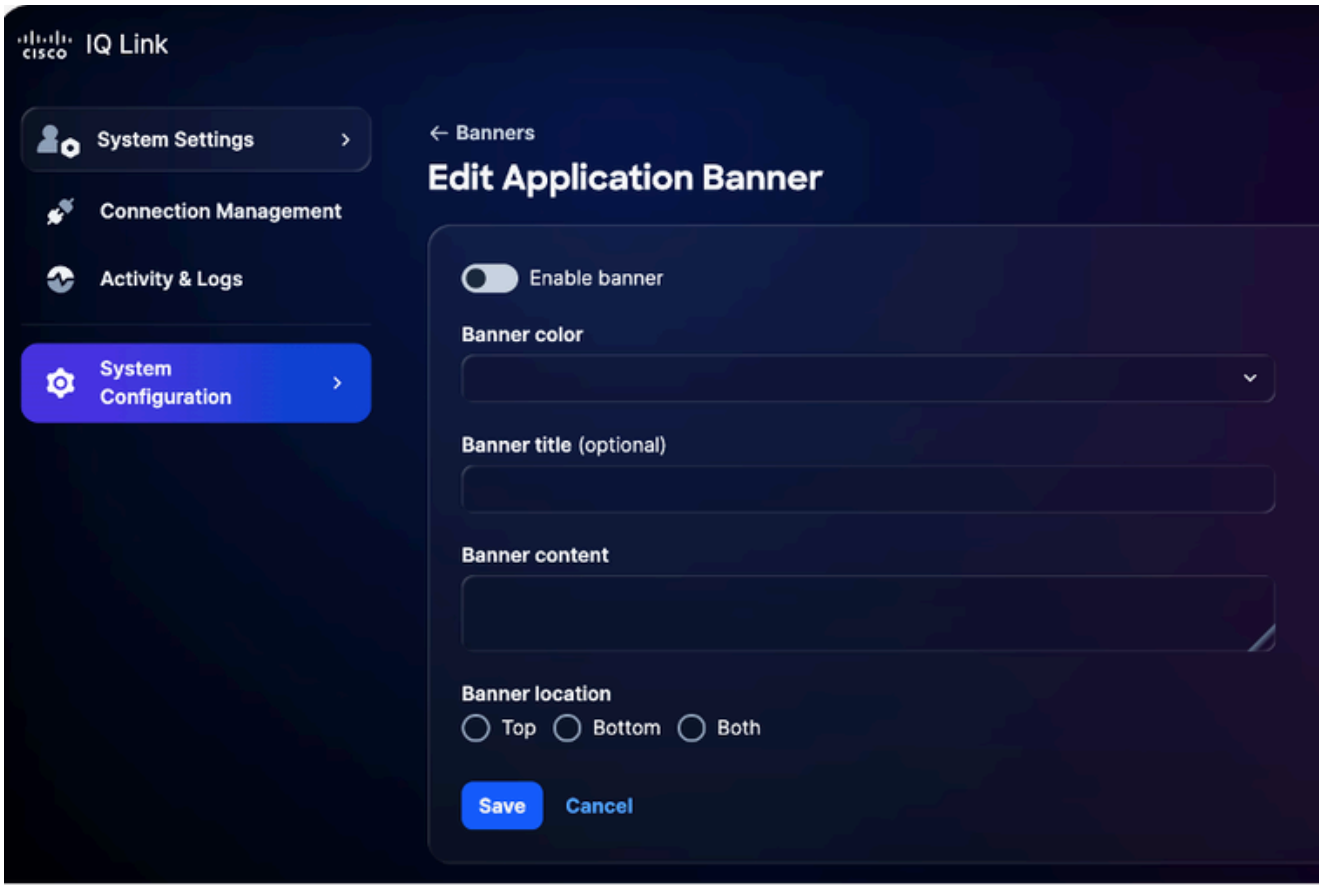
To configure an application banner:

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

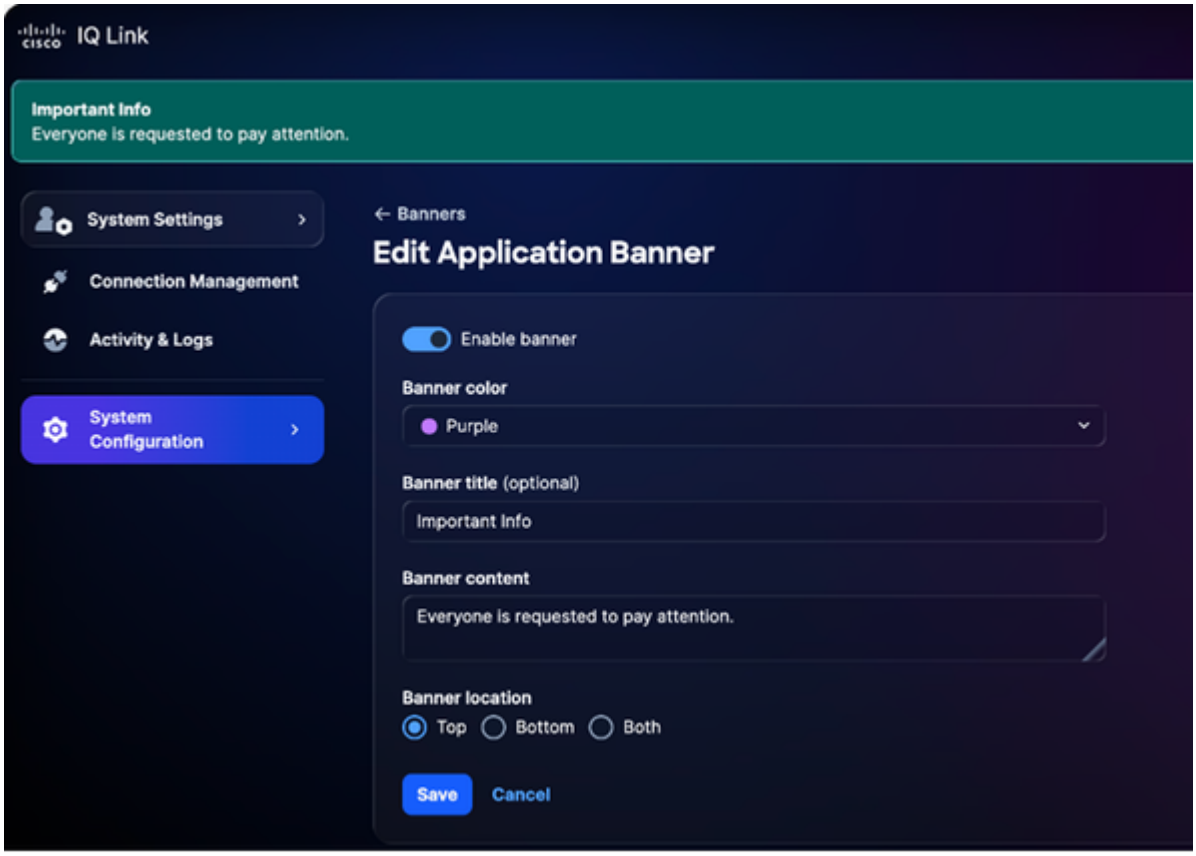
3. Click the toggle to enable or disable the banner.
4. Select a **Banner color**.
5. Enter the **Banner title**.
6. Enter the **Banner content**.
7. Select a **Banner location**.
8. Click **Save**. The banner displays across the application.

Editing Banners

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

Edit Application Banner

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.

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 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.