Cisco IQ Link Operations Guide v1.1.0

Einleitung

Cisco IQ™ bietet Kunden Verbesserungen und Funktionen, die darauf ausgelegt sind, die Transparenz ihrer Ressourcen zu verbessern, intelligentere Einblicke in ihre Umgebungen zu liefern und das Fallmanagement zu optimieren. Darüber hinaus optimieren KI-Funktionen wie der Cisco IQ AI Assistant die Betriebsergebnisse und die Benutzererfahrung mit Cisco IQ, indem sie kontextbezogene Kenntnisse bereitstellen, die es Benutzern ermöglichen, proaktive, fundierte Entscheidungen zu treffen, und Prozesse optimieren, die das Kundenengagement und den Erfolg fördern.

Cisco IQ Link sammelt und überträgt die Telemetriedaten über Ressourcen von Ihrem lokalen Netzwerk an Cisco IQ. So erhalten Sie KI-gestützte, vorausschauende Informationen, mit denen Sie die Netzwerktransparenz verbessern, Probleme vorhersehen und die Betriebseffizienz steigern können.

Lokale Authentifizierung

Administratoren sollten die folgenden Anmeldeinformationen verwenden, um sich bei Cisco IQ Link anzumelden:

- Standard-Benutzername: Administrator
- Standardkennwort: Kennwort, das während der Installation von Cisco IQ Link festgelegt wird; Weitere Informationen finden Sie im Cisco IQ Link Getting Started Guide

Nach der Anmeldung werden auf der Startseite der Standardbenutzer "admin" und der Kontoname "Default-Customer" angezeigt.

Festlegen der lokalen Administratorsicherheit

Sie können Ihr Kennwort ändern und Sicherheitsfragen über das Menü Sicherheit für lokalen Administrator in der Systemkonfiguration einrichten.

Sie haben drei (3) Versuche, innerhalb von zehn (10) Minuten das richtige Passwort einzugeben. Wenn alle drei (3) Versuche nicht erfolgreich sind, wird Ihr Konto vorübergehend für 60 Minuten gesperrt, um Ihre Sicherheit zu schützen.

Sie können nicht versuchen, sich während der Sperrzeit anzumelden. Das System zeigt folgende Meldung an: "Das Konto wurde aufgrund zu vieler fehlgeschlagener Versuche gesperrt. Versuchen Sie es später erneut.", einschließlich der Zeit, zu der die Sperre abläuft.

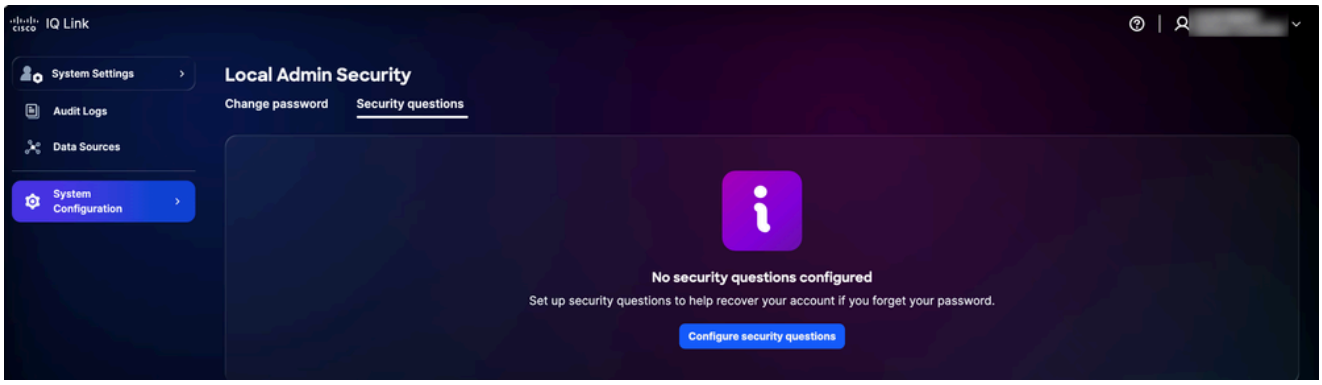
Nach 60 Minuten wird Ihr Konto automatisch entsperrt. Sie können dann versuchen, sich anzumelden oder Ihr Kennwort zurückzusetzen.

Einrichten von Sicherheitsfragen und -antworten

Sicherheitsfragen helfen dabei, Ihre Identität zu verifizieren, wenn Sie Ihr Kennwort vergessen haben. Administratoren müssen Antworten auf fünf (5) Sicherheitsfragen einrichten, um die Funktion zum Zurücksetzen von Kennwörtern zu aktivieren. Dies ist eine einmalige Konfiguration.

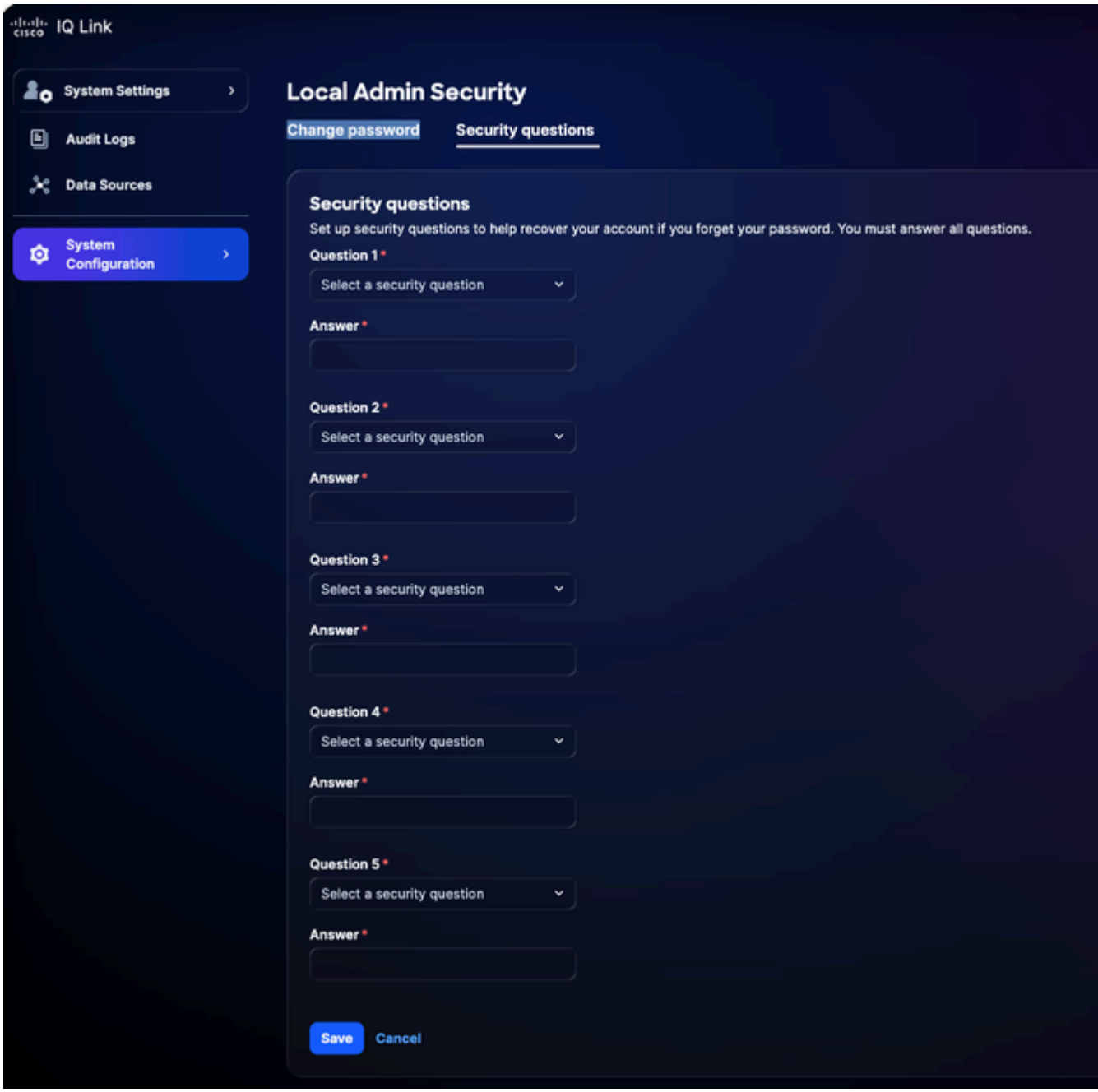
So richten Sie Sicherheitsfragen ein:

1. Wählen Sie in den Systemeinstellungen die Option Systemkonfiguration > Lokale Admin-Sicherheit > Sicherheitsfragen aus.



Sicherheitsfragen

2. Klicken Sie auf Sicherheitsfragen konfigurieren.



Sicherheitsfragen

3. Wählen Sie aus den Dropdown-Listen fünf (5) Sicherheitsfragen aus.

4. Geben Sie Ihre Antwort für jede Frage ein.

5. Klicken Sie auf Speichern.

Hinweise:

- Bei den Antworten wird nicht zwischen Groß- und Kleinschreibung unterschieden, z. B. "SMITH" und "Smith" werden als identisch betrachtet.
- Zusätzliche Leerzeichen werden ignoriert, was bedeutet, dass "Smith" und "Smith" identisch behandelt werden.

Anmerkung: Sie können Ihre Antworten bei Bedarf später aktualisieren. Wenn Sie Ihre Antworten aktualisieren, werden alle vorherigen Antworten ersetzt. Sie müssen daher alle fünf (5) Fragen erneut beantworten und nicht nur die, die Sie ändern möchten.

Verwalten von Kennwörtern

Nur lokale Administratoren können das Kennwort für Cisco IQ verwalten.

Voraussetzungen

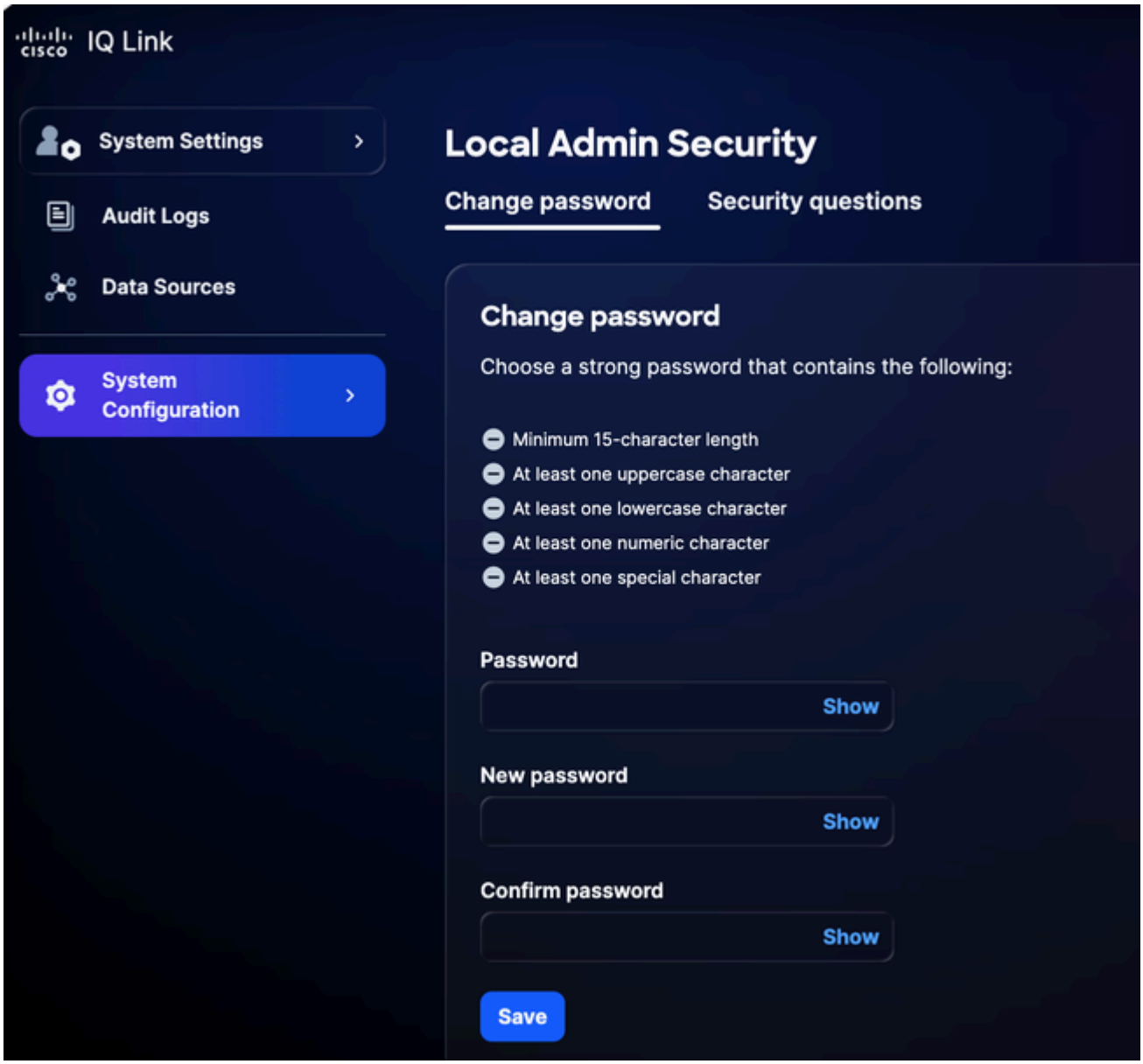
Um Kennwörter zu verwalten, müssen die folgenden Bedingungen erfüllt sein:

- Sie sind ein lokaler Administrator
- Sie verwenden ein lokales Administratorkonto (kein Single Sign-On (SSO) oder externe Authentifizierung).
- Sie sind bei Cisco IQ angemeldet.
- Sie kennen das aktuelle Kennwort.

Kennwörter ändern

So ändern Sie das Kennwort:

1. Navigieren Sie unter Systemeinstellungen zu Systemkonfiguration > Sicherheit für lokalen Administrator > Kennwort ändern.



Kennwort ändern

2. Geben Sie das aktuelle Kennwort ein.
3. Geben Sie das neue Kennwort ein.
4. Geben Sie zur Bestätigung erneut das neue Kennwort ein.
5. Klicken Sie auf Speichern.

Das Kennwort wird im Cisco IQ-System aktualisiert, einschließlich des virtuellen Systems Cisco IQ.

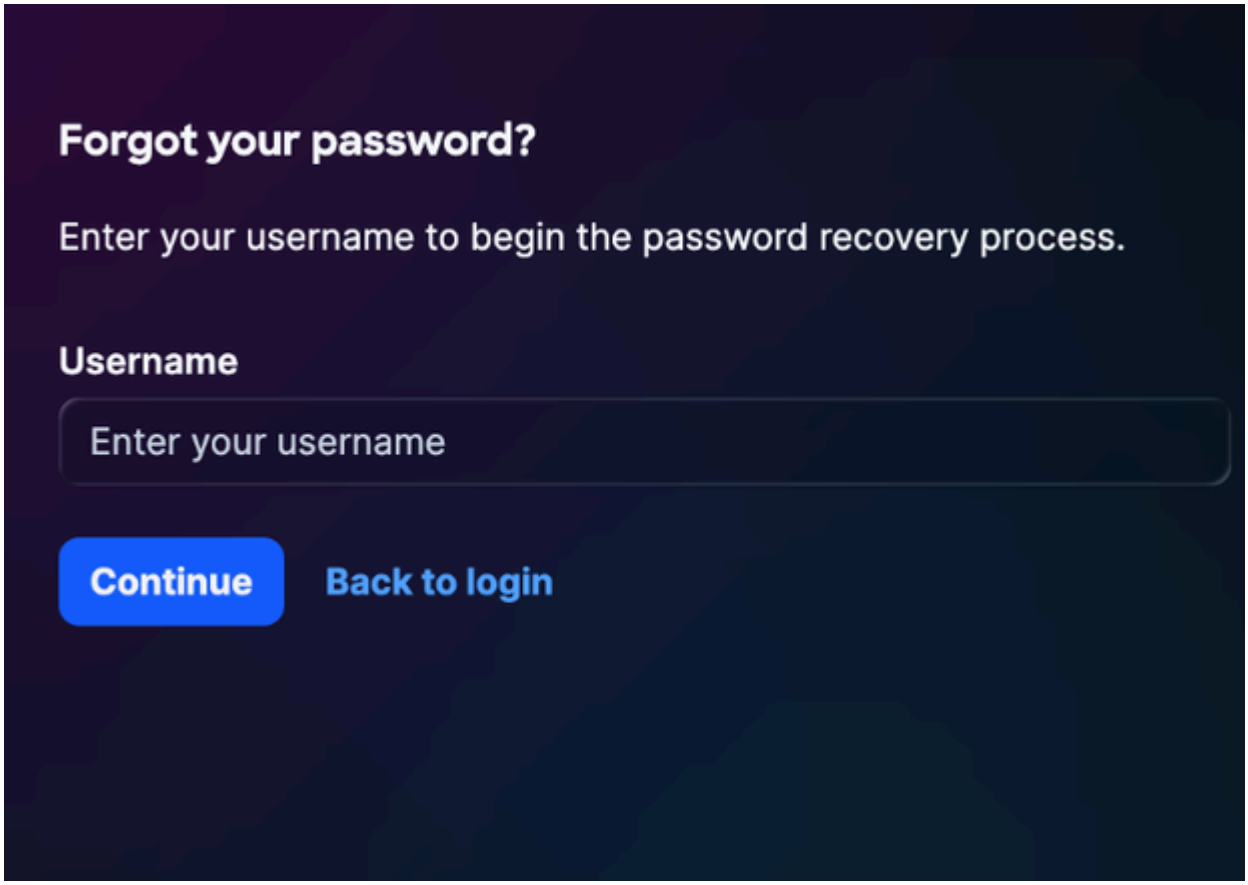
Zurücksetzen eines vergessenen Kennworts

Sie können ein vergessenes Kennwort zurücksetzen, indem Sie die Sicherheitsfrage überprüfen,

wenn Sie die Sicherheitsfragen zuvor eingerichtet haben. Weitere Informationen finden Sie unter Sicherheitsfragen und -antworten einrichten.

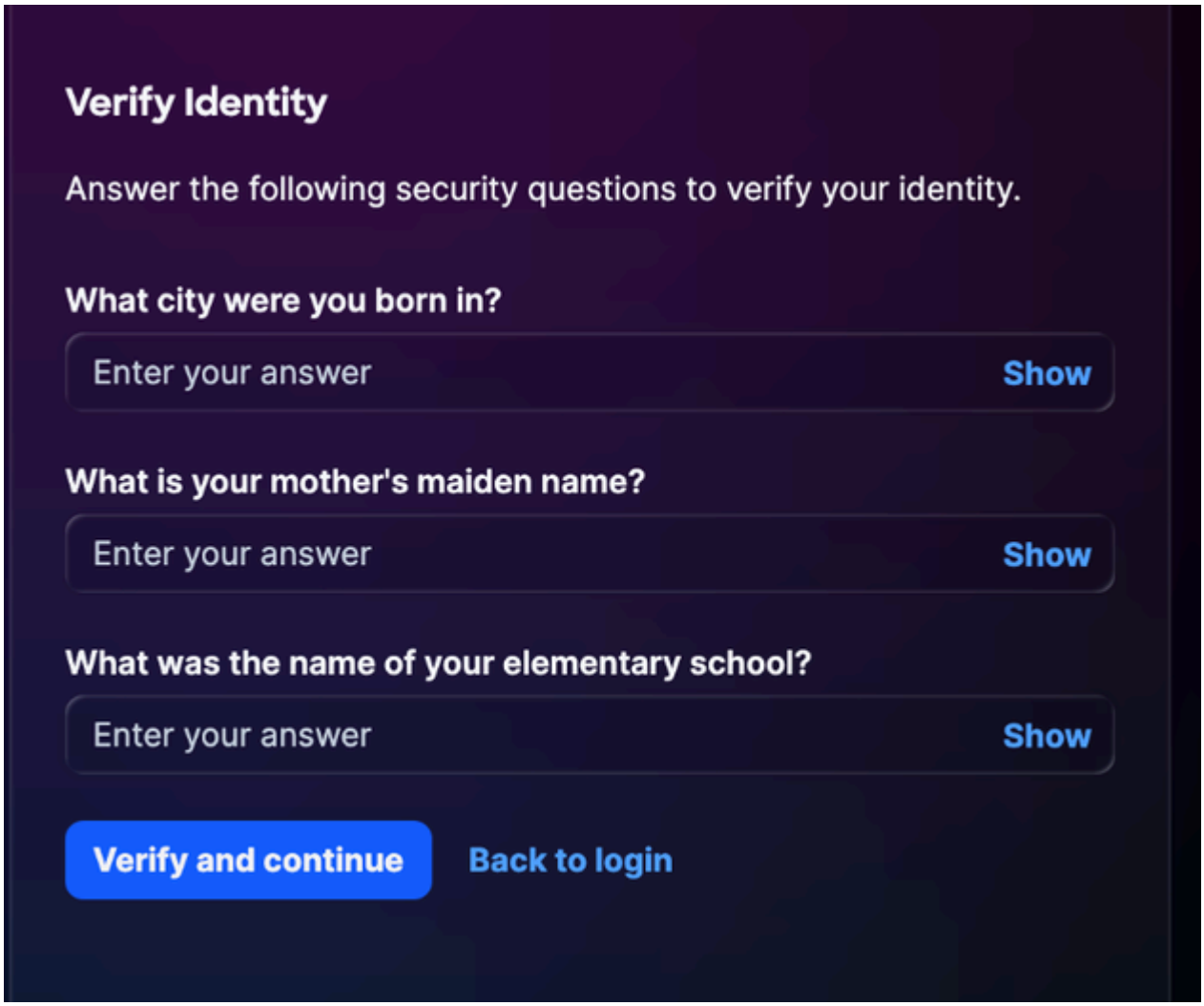
So setzen Sie ein vergessenes Kennwort zurück:

1. Navigieren Sie zur Anmeldeseite von Cisco IQ Link.
2. Klicken Sie auf Kennwort vergessen.



Passwort vergessen

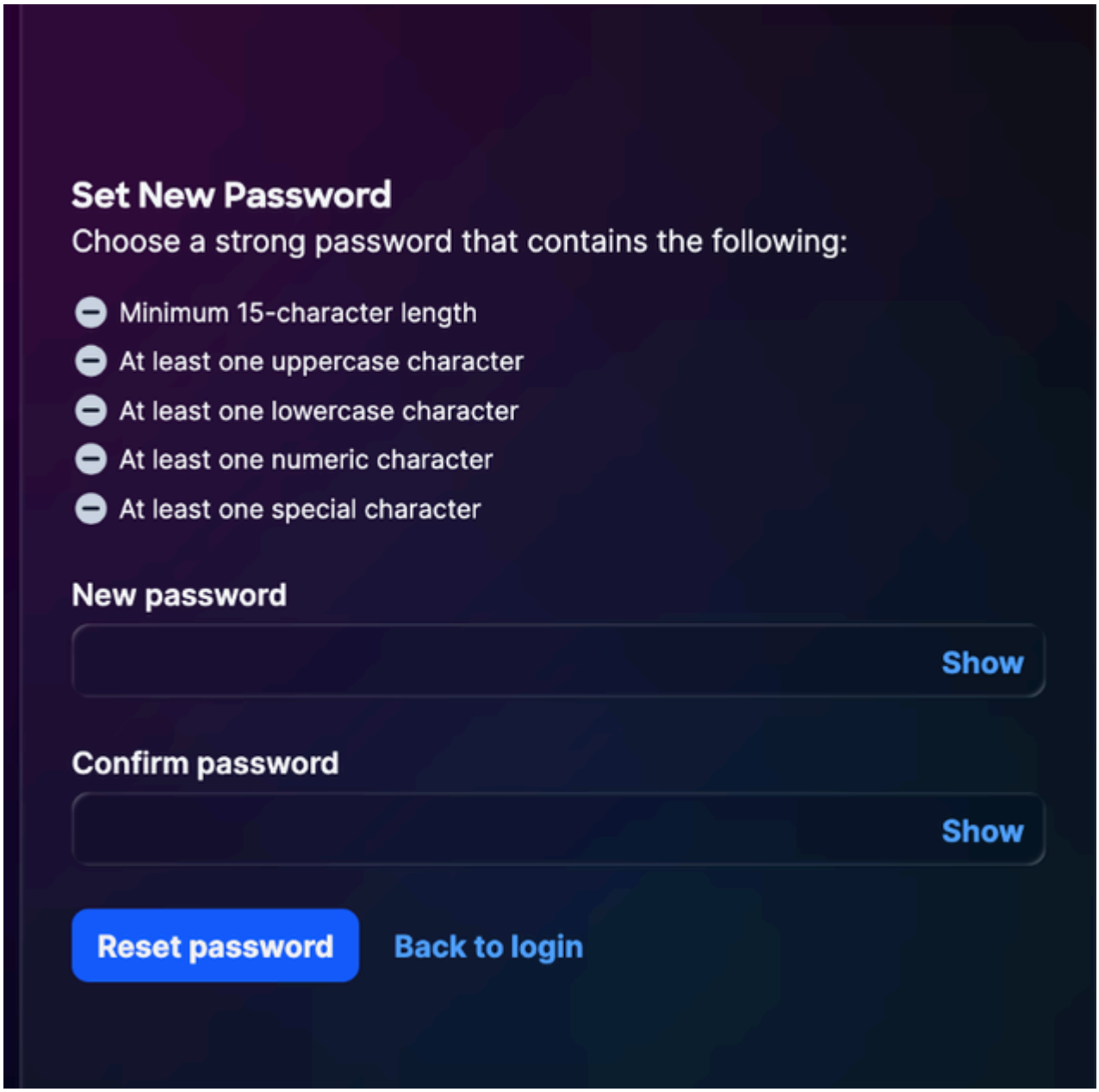
3. Geben Sie den Benutzernamen ein.
4. Klicken Sie auf Continue (Weiter). Auf der Seite Identität überprüfen werden drei (3) zufällige Sicherheitsfragen von den fünf (5) Fragen angezeigt, die zuvor konfiguriert wurden.



Identität überprüfen

Anmerkung: Die oben angezeigten Sicherheitsfragen sind benutzerspezifisch und variieren entsprechend.

5. Geben Sie die Antworten für alle drei (3) angezeigten Fragen ein.
6. Klicken Sie auf Überprüfen, und fahren Sie fort. Wenn die eingesendete Antwort mit den zuvor gespeicherten Antworten übereinstimmt, werden Sie aufgefordert, ein neues Kennwort einzugeben.



Kennwort zurücksetzen

Anmerkung: Sie haben drei (3) Versuche, die Sicherheitsfragen innerhalb von zehn (10) Minuten richtig zu beantworten. Wenn alle drei (3) Versuche nicht erfolgreich sind, wird Ihr Konto vorübergehend für 60 Minuten gesperrt, um Ihre Sicherheit zu schützen.

Sie können Ihr Kennwort während der Sperrzeit nicht zurücksetzen. Das System zeigt folgende Meldung an: "Das Konto wurde aufgrund zu vieler fehlgeschlagener Verifizierungsversuche gesperrt. Versuchen Sie es später erneut.", einschließlich der Zeit, zu der die Sperre abläuft.

Nach 60 Minuten wird Ihr Konto automatisch entsperrt. Sie können dann versuchen, sich anzumelden oder Ihr Kennwort zurückzusetzen.

---

7. Geben Sie das neue Kennwort ein.

8. Geben Sie zur Bestätigung erneut das Kennwort ein.
9. Klicken Sie auf Senden.

Identitätsanbieter konfigurieren

Nach der Anmeldung bei Cisco IQ Link können Administratoren verschiedene Einstellungen konfigurieren. Administratoren können sich über die lokale Administration oder die IDP-Konfiguration (Identity Provider) bei Cisco IQ Link anmelden.

Okta IDP SAML-Konfiguration für SSO

Voraussetzungen für die Konfiguration von IDP SAML

- Lokaler Administratorzugriff auf Cisco IQ Link
- Zugang zum IDP-Portal

IDP SAML-Konfiguration für SSO

So konfigurieren Sie die IDP Security Assertion Markup Language (SAML) für SSO:

1. Navigieren Sie zu Ihrem IDP-Portal.
2. Legen Sie die folgenden Attribute für die Cisco IQ Link-Instanz fest.

Cisco IQ Link-Attribute

Feld	Wert
Anwendungsname	<Anwendungsname>
Umwelt	ESP-Geschäftsanwendung
Anwendungsbesitzergruppen	Eigentümer der IDP-Einstellungen
Team-Mailer	Mailer für das Team

Feld	Wert
Zielgruppe	Nicht-Mitarbeiter
Onboarding-Kategorie	Wählen Sie "New Onboarding".

SAML-Konfigurationsparameter

Parameter	Konfiguration	Beispiel
Zielgruppe (Element-ID)	FQDN-Name	mymanagementhost.mydomain.com
URL für einmalige Anmeldung	SAML-ACS-Endpunkt	https://mymanagementhost.mydomain.com/saml/acs
Name ID-Format	E-Mail-Adresse	NA
Anwendungsbenutzername	Benutzername	NA

3. Konfigurieren Sie die folgenden obligatorischen Attributanweisungen.

Anmerkung: Änderungen der IDP-Attribute hängen vom jeweiligen Anbieter und der jeweiligen Konfiguration ab. Cisco IDP und seine Attribute werden nachfolgend als Beispiel genannt.

- Erster Eintrag
    - Name: Benutzername
    - Wert: user.login
- Zweiter Eintrag
    - Name: Primäre E-Mail
    - Wert: Benutzer.E-Mail
- Gruppenattribut-Anweisungen
    - Name: Gruppen

- Filter: REGELN
- Wert: .*

4. Konfigurieren der Einstellungen für die einmalige Abmeldung (SLO) in der Anwendung

SLO-Konfigurationseinstellungen

Feld	Wert
Signaturzertifikat	Für Okta ist dieses Zertifikat nur erforderlich, wenn Sie SLO aktivieren. Laden Sie das Signaturzertifikat mithilfe von Download SP Certificate in Identity Providers herunter. Speichern Sie die Datei unter dem Namen sp-public-key.crt. Weitere Informationen finden Sie unter Single Logout Configuration (Einzelabmeldekonfiguration).
SP-Metadaten	Die SP-Metadaten sind nur für ADFS-IDP (und nicht für Okta) erforderlich.
Möchten Sie Single Logout aktivieren?	Ja oder Nein
URL für einzelne Abmeldung	https://mymanagementhost.mydomain.com/saml/logout
SP-Aussteller (Zielgruppe/Objektkennung oder ACS-URL)	https://mymanagementhost.mydomain.com

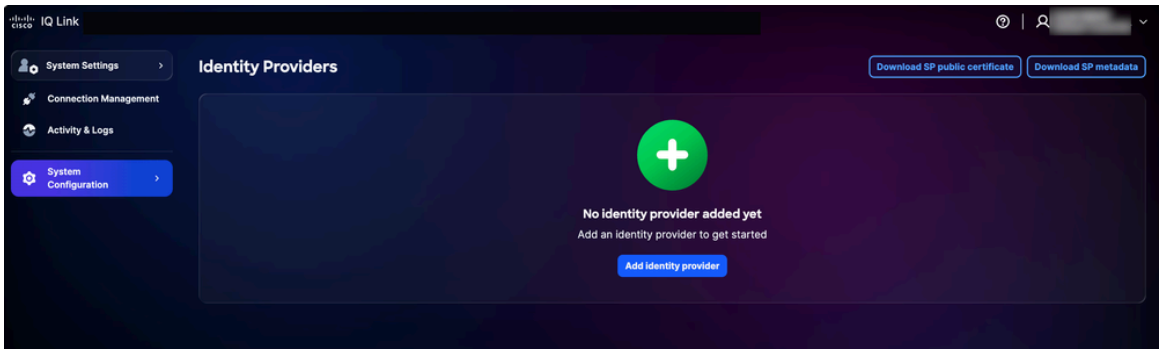
5. Klicken Sie auf das Symbol Download, um die "SP Metadata"-Datei herunterzuladen.
6. Stellen Sie die Anwendung gemäß den Anforderungen des Anbieters bereit, oder erstellen Sie sie.

Hinzufügen von IDP

So fügen Sie einen IDP in Cisco IQ hinzu:

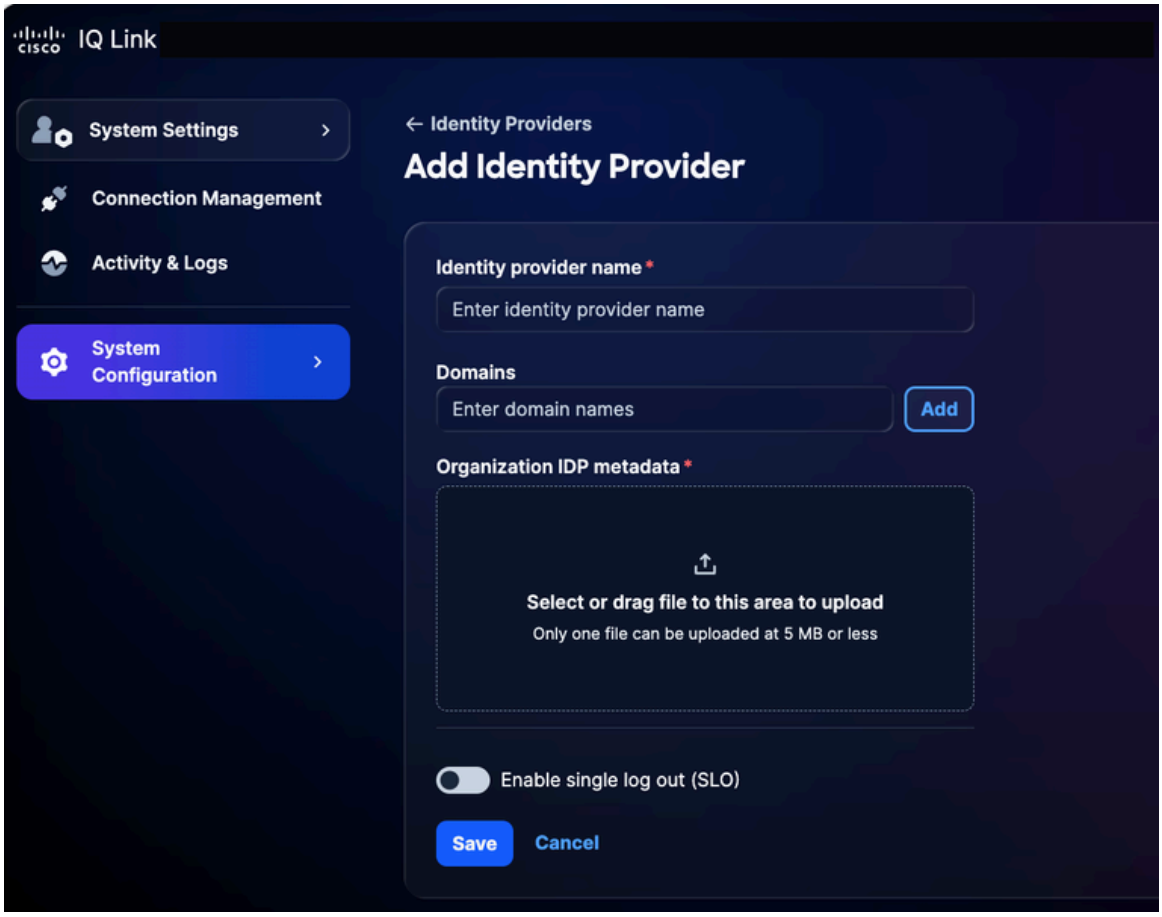
1. Wählen Sie in den Systemeinstellungen die Option Systemkonfiguration > Identitätsanbieter

aus. Die Seite "Identitätsanbieter" wird angezeigt.



IDP-Startseite

2. Klicken Sie auf Identitätsanbieter hinzufügen. Die Seite Identitätsanbieter hinzufügen wird angezeigt.



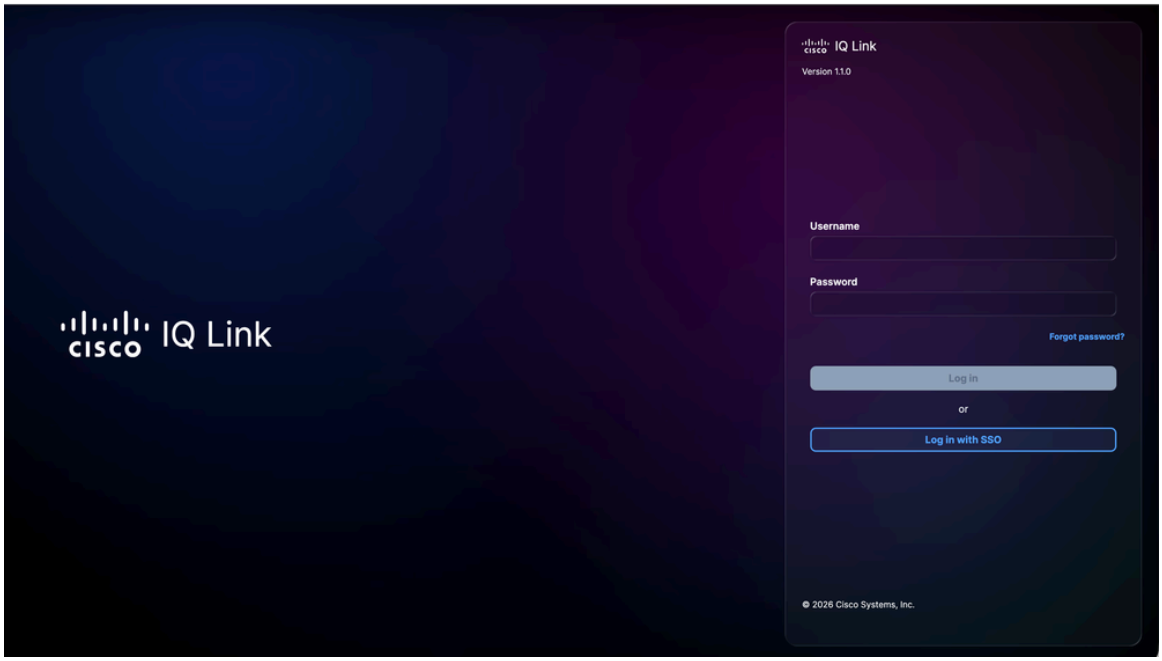
Identitätsanbieter hinzufügen

Anmerkung: Es kann jeweils nur ein (1) IDP hinzugefügt werden.

3. Geben Sie den Namen des Identitätsanbieters ein.

4. Klicken Sie auf Add (Hinzufügen), um dem Feld Domains (Domänen) einen für Cisco IQ Link konfigurierten Domänennamen hinzuzufügen.

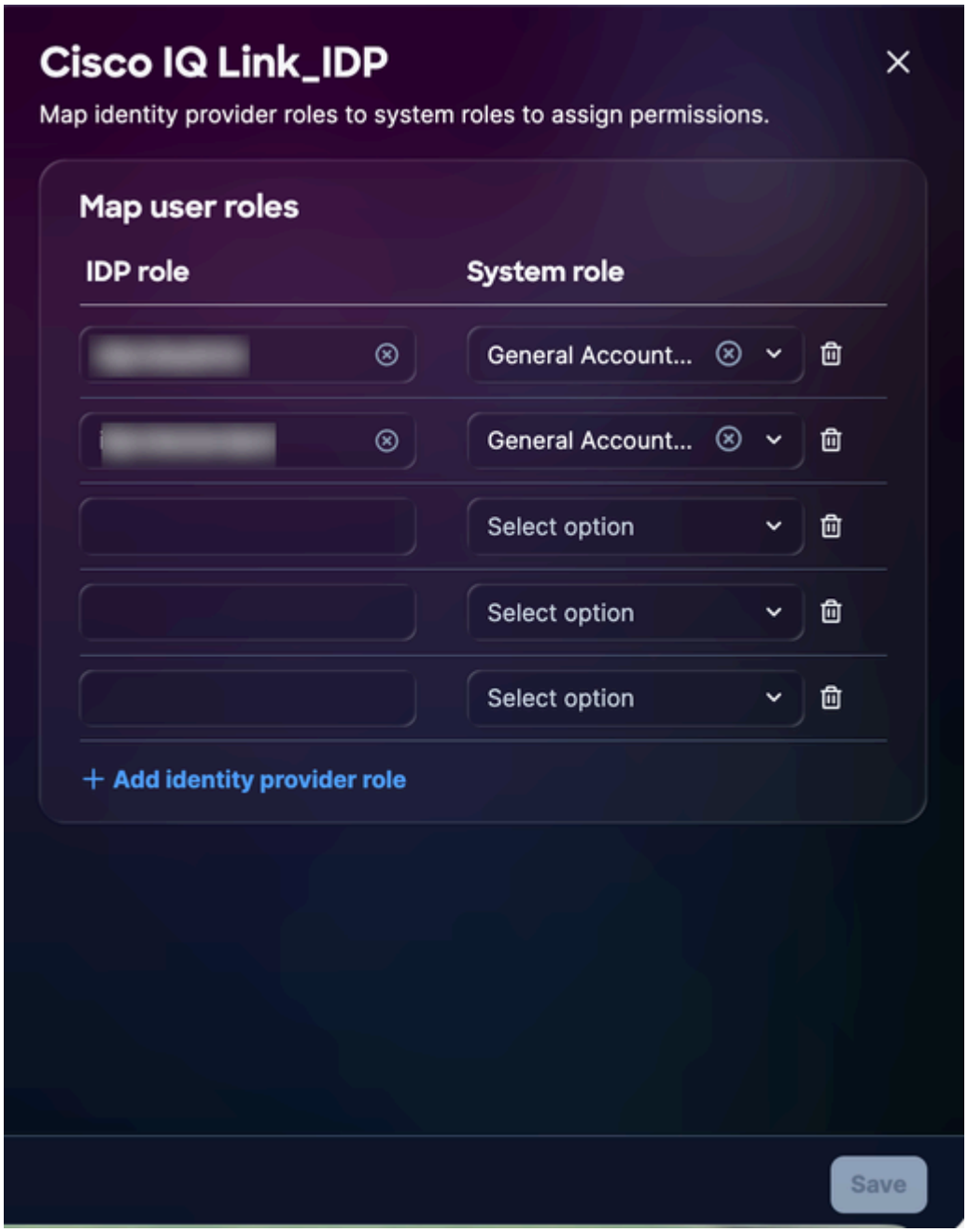
5. Ziehen Sie die aus der IDP-Anwendung erhaltene SAML-Metadatendatei per Drag-and-Drop in das Feld Organization IDP-Metadaten, oder laden Sie sie hoch. Diese Datei enthält Zertifikatdetails und Details zur Service Provider (SP)-Entität.
6. (Optional) Aktivieren Sie die Umschaltfläche Einzelnes Abmelden aktivieren. Sie können das SLO auch später aktivieren.
7. Klicken Sie auf Speichern.
8. Nach der Konfiguration wird auf der Anmeldeseite eine Option zur Anmeldung mit SSO (über IDP) angezeigt.



Cisco IQ Link-Anmeldung

Konfiguration der Rollenzuordnung

1. Wählen Sie aus dem hinzugefügten IDP das Symbol More Options (Weitere Optionen) > Map Roles (Rollen zuordnen). Die Seite Benutzerrollen zuordnen wird angezeigt.

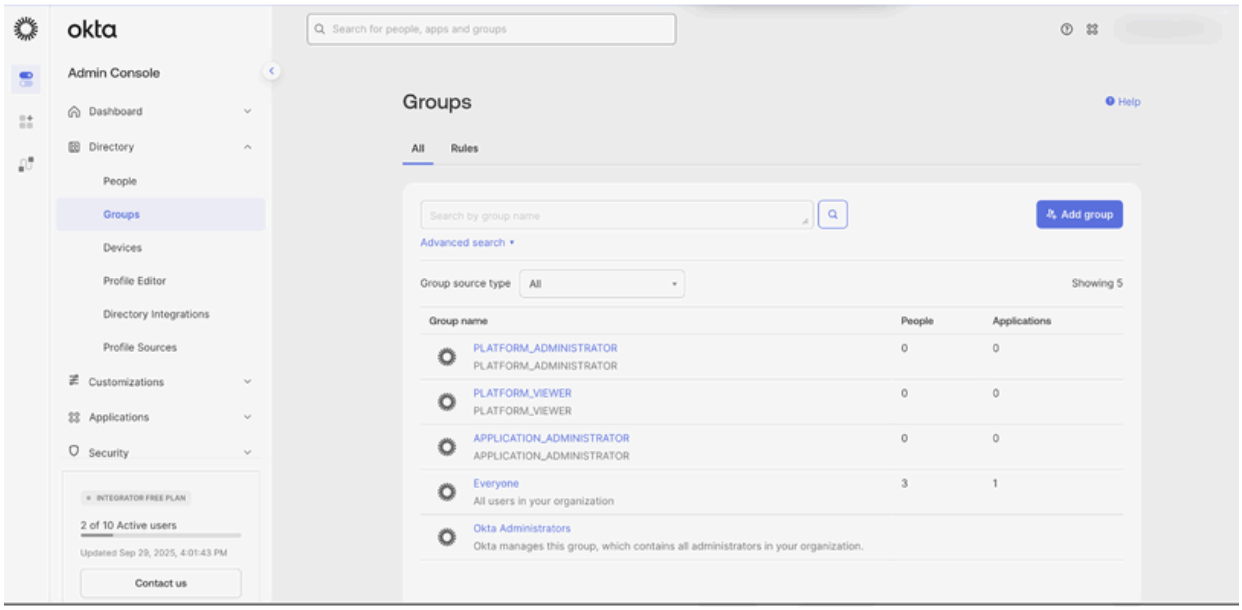


Benutzerrollenzuordnung

2. Geben Sie eine IDP-Rolle für die ausgewählte Systemrolle ein. Folgende Systemrollen werden unterstützt:

    - general_account_administrator: Der allgemeine Kontoadministrator verfügt über alle Berechtigungen zum Ausführen aller Aktionen im Produkt.
    - general_account_viewer: Die allgemeine Kontoanzeige verfügt über schreibgeschützten Zugriff.

✎ Anmerkung: Die IDP-Rolle ist ein offenes Feld. Er muss genau mit dem Gruppen- oder Rollennamen übereinstimmen, der im IDP Ihrer Organisation konfiguriert wurde. Ein Beispiel für Okta-Gruppen finden Sie weiter unten.



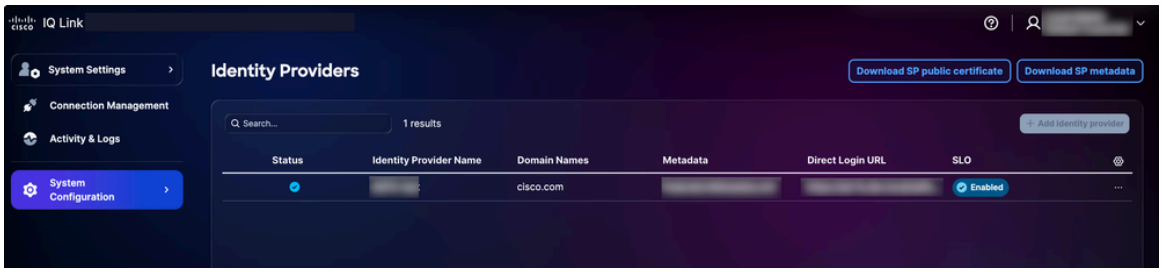
Referenz zur Rollenzuordnung

3. Ordnen Sie ggf. weitere Rollen zu, indem Sie auf Identitätsanbieterrolle hinzufügen klicken.
4. Klicken Sie auf Speichern.

Konfiguration für einmaliges Abmelden

Wenn Sie SLO aktivieren, müssen Sie Metadaten hochladen, die die SLO-URL enthalten. Sie können dies konfigurieren, indem Sie die Einstellungen für den Identitätsanbieter bearbeiten und den Umschalter für einmaliges Abmelden aktivieren aktivieren. SLO-Konfiguration abschließen:

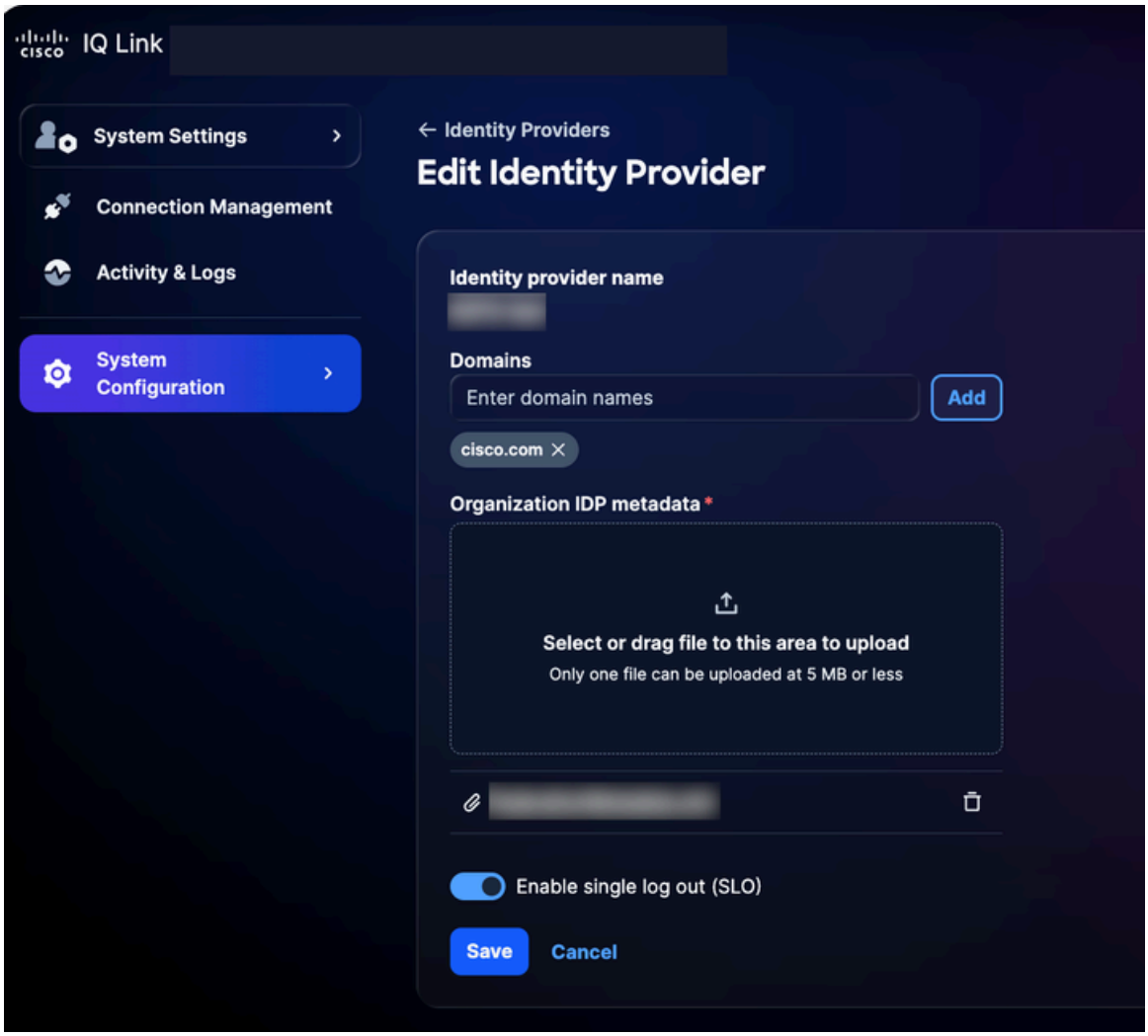
1. Klicken Sie auf der Seite Identitätsanbieter auf Öffentliches SP-Zertifikat herunterladen.



Öffentliches Zertifikat herunterladen

2. Speichern Sie die Download-Datei unter sp-public-key.crt.
3. Navigieren Sie zu Ihrem IDP-Portal.
4. Laden Sie die Signaturzertifikatdatei hoch, die im Abschnitt IDP SAML Configuration for SSO generiert wurde.
5. Laden Sie die IDP-Metadatendatei erneut herunter.

6. Wählen Sie auf der Seite Identity Providers (Identitätsanbieter) das Symbol More Options (Weitere Optionen) des hinzugefügten IDP > Edit (Bearbeiten).



Identitätsanbieter bearbeiten

7. Aktivieren Sie die Umschaltfläche Enable single log out (SLO).
8. Laden Sie die neu heruntergeladene Metadatendatei hoch.
9. Verwenden Sie die folgende Checkliste, um die SSO- und SLO-Funktionalität zu überprüfen:

Verifizierungs-Checkliste:

- Anmeldung beim lokalen Administrator erfolgreich
- IDP-Portal wird konfiguriert und bereitgestellt
- IDP wird dem Cisco IQ mit dem Status "Success" hinzugefügt
- Rollenzuordnungen werden konfiguriert und getestet.
- SP-Metadaten werden heruntergeladen, und das Zertifikat wird extrahiert.

- Wenn SLO aktiviert ist, ist die SLO-Konfiguration mit dem echten Signaturzertifikat abgeschlossen
- Der gesamte SSO/SLO-Fluss wurde erfolgreich getestet.

Fehlerbehebung bei IDP-Problemen

In der folgenden Liste werden häufige Probleme und mögliche Lösungen im Zusammenhang mit der schnellen Identifizierung und Behebung von Problemen im Zusammenhang mit dem IDP-Status, Zertifikatfehlern, SSO-Anmeldefehlern und der SLO-Konfiguration aufgeführt:

Fehlerbehebung

Problem	Lösung
Der IDP-Status wird als "Incomplete" (Unvollständig) angezeigt.	Überprüfen der Konfigurationen für die Rollenzuordnung
Zertifikatfehler	Format und Gültigkeit des Zertifikats überprüfen
SSO-Anmeldefehler	Attributzuordnung und Gruppenzuweisungen validieren
SLO funktioniert nicht wie erwartet	Stellen Sie sicher, dass das Zertifikat ordnungsgemäß hochgeladen und SLO-URLs konfiguriert wurden.

ADFS IDP SAML-Konfiguration für SSO

Dieser Abschnitt enthält Anleitungen zur Konfiguration von Microsoft Active Directory Federation Services (ADFS) als SAML IDP für Cisco IQ.

Voraussetzungen für die Konfiguration von ADFS IDP SAML für SSO

- ADFS 6.0+ wird empfohlen
- Windows Server 2012 R2+
- Konfigurierte Active Directory-Integration
- SSL/TLS-Zertifikate bei ADFS
- Administratorzugriff auf Cisco IQ
- Administratorzugriff auf den ADFS-Server (Windows Server)
- PowerShell-Zugriff auf ADFS-Server
- Netzwerkverbindung zwischen ADFS und Cisco IQ
- Details zur ADFS-Serverkonfiguration (wie in der unten stehenden Tabelle aufgeführt)

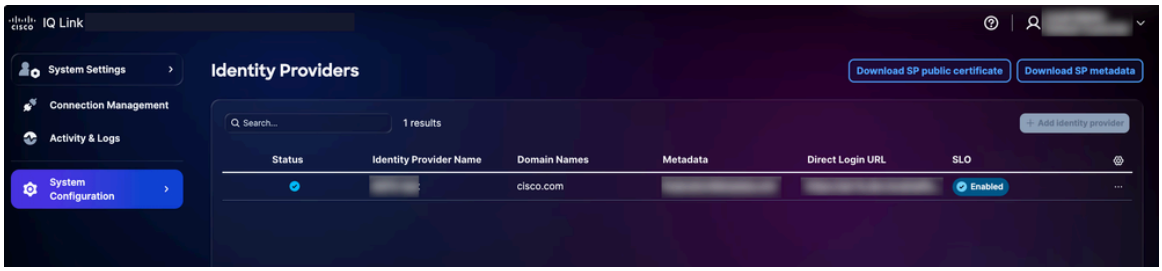
ADFS-Serverkonfiguration

Posten	Beschreibung	Beispiel
Cisco IQ-FQDN	Hostname der Benutzerbereitstellung	devxx-23.cx-xxx-xxx.cisco.com
ADFS-Server-URL	Benutzer ADFS-Serveradresse	https://ad-fs.dev.local
Firmendomäne	E-Mail-Domäne	company.com
AD-Gruppen	Domänennamen (DN) der Active Directory-Gruppe	CN=Rolle - CXIQ-Entwickler

Konfigurieren von ADFS-Servern

ADFS konfigurieren:

1. Wählen Sie in den Systemeinstellungen die Option Systemkonfiguration > Identitätsanbieter aus. Die Seite "Identitätsanbieter" wird angezeigt.



Download-Optionen

2. Klicken Sie auf Öffentliches SP-Zertifikat herunterladen und auf SP-Metadaten herunterladen, um diese Dateien herunterzuladen.
3. Kopieren und speichern Sie die Dateien service-provider-metadaten.xml und service-provider-certificate.crt in das ADFS-Verzeichnis (z. B. C:-certificate.crt).
4. Melden Sie sich beim ADFS-Server an.
5. Klicken Sie im Menü ADFS Management (ADFS-Verwaltung) auf Relying Party Trusts (Vertrauenswürdige Partei).
6. Klicken Sie im Menü Vertrauenswürdige Partei auf Vertrauenswürdige Partei hinzufügen. Der neue Assistent wird geöffnet.
7. Klicken Sie auf das Optionsfeld Claims Aware (Ansprüche bekannt).
8. Klicken Sie auf Start, um die Konfiguration fortzusetzen.
9. Klicken Sie auf Daten über die vertrauende Partei aus einer Datei importieren.
10. Klicken Sie auf Durchsuchen, um die Metadatendatei des Dienstanbieters auszuwählen und den Datei-Upload abzuschließen.
11. Klicken Sie auf Next (Weiter).
12. Geben Sie einen Anzeigenamen ein (z. B. "CIQ-Stage"), fügen Sie relevante Notizen hinzu, und klicken Sie auf "Weiter".
13. Klicken Sie auf der Seite Choose Access Control Policy (Zugriffskontrollrichtlinie auswählen) auf Permit everyone (Alle zulassen) (oder auf die Richtlinie, die für die Sicherheitskonfiguration Ihres Unternehmens erforderlich ist).
14. Klicken Sie durch die übrigen Bildschirme auf Weiter.
15. Klicken Sie auf Schließen, um die Vertrauensstellungskonfiguration für die vertrauende Seite abzuschließen.

ADFS-Anspruchsregeln konfigurieren

Führen Sie zum Konfigurieren der ADFS-Anspruchsregeln die in den folgenden Abschnitten aufgeführten Schritte aus.

Erforderliche Forderungen

Die erforderlichen Ansprüche finden Sie in der folgenden Tabelle.

Erforderliche Forderungen

Forderung	Zweck	Quelle
E-Mail	Benutzer-ID	AD-Mail
Anzeigename	Vollständiger Name des Benutzers	AD-Anzeigename
NameID	SAML-Betreff	Aus E-Mail umgewandelt
Gruppen	Rollenbasierter Zugriff	AD-Gruppenmitgliedschaft (Mitglied von)

Anspruchsregeln anwenden

1. Definieren Sie den Namen Ihres Vertrauens der vertrauenden Partei (z. B. "Cisco IQ - Stage").

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

2. Definieren Sie Anspruchsregeln, um Benutzerinformationen und die Gruppenmitgliedschaft an Cisco IQ zu senden.

```
$claimRules = @’

@RuleTemplate = “LdapClaims”

@RuleName = “Send Email and Name”

c:[Type == “http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname”, Issuer == “AD A
=> issue(store = “Active Directory”, types = (“http://schemas.xmlsoap.org/ws/2005/05/identity/claims/ema
```

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

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

3. Wenden Sie die Anspruchsregeln an, indem Sie den folgenden Befehl ausführen:

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

Überprüfen von Benutzergruppen

1. Legen Sie den Benutzernamen fest, um die Gruppenmitgliedschaft des Benutzers zu überprüfen.

```
$username = “testuser”
```

2. Führen Sie die folgenden Befehle aus, um das Benutzerkonto zu finden:

```
$searcher = [adsisearcher]“(samaccountname=$username)”

$user = $searcher.FindOne()
```

3. Zeigt die Gruppen an, zu denen der Benutzer gehört.

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

Beispiel:

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

Konfigurieren von ADFS als vertrauenswürdig für das SP-Signaturzertifikat

1. Importieren Sie im ADFS-Server das SP-Zertifikat in den TrustedPeople-Speicher.

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

2. Wählen Sie eine der folgenden Optionen aus:

Anmerkung: Das SP-Zertifikat wird von einer internen Zertifizierungsstelle ausgestellt, die ADFS nicht über die standardmäßige Vertrauenskette validieren kann.

- Globale Kettenvalidierung für diese vertrauende Partei deaktivieren

```
Set-AdfsRelyingPartyTrust `
    -TargetIdentifier “


     ” `
    -SigningCertificateRevocationCheck None `
    -EncryptionCertificateRevocationCheck None
```

ODER

- Das ausstellende Zertifizierungsstellenzertifikat in den Speicher der vertrauenswürdigen Stammzertifizierungsstellen importieren

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

3. Wenden Sie die Änderungen an, indem Sie den ADFS-Dienst neu starten.

```
Restart-Service adfssrv
```

ADFS-Metadaten exportieren

Sie können Ihre ADFS-Metadaten entweder über PowerShell oder Ihren Webbrowser herunterladen.

PowerShell

So exportieren Sie ADFS-Metadaten mit PowerShell:

1. Öffnen Sie PowerShell auf Ihrem ADFS-Server.
2. Führen Sie die folgenden Befehle aus, um die Metadatendatei herunterzuladen.

```
$metadataUrl = (Get-AdfsEndpoint | Where-Object {$_.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
```

Nach der Ausführung der Befehle wird die Metadatendatei in C:-metadaten.xml gespeichert.

Webbrowser

So exportieren Sie ADFS-Metadaten mit einem Webbrowser:

1. Navigieren Sie zu https://<your-adfs-server>/FederationMetadata/2007-06/FederationMetadata.xml.
2. Ersetzen Sie <your-adfs-server> durch den Hostnamen Ihres ADFS-Servers.
3. Speichern Sie die XML-Metadatendatei auf Ihrem Computer, wenn Sie dazu aufgefordert werden.

Hinzufügen von ADFS IDP

1. Klicken Sie auf der Seite Identitätsanbieter auf Identitätsanbieter hinzufügen.
2. Geben Sie den Namen des Identitätsanbieters ein.
3. Geben Sie die Domäne(n) ein (z. B. company.com).

4. (Optional) Aktivieren Sie ggf. die Umschalttaste Enable single logout (Einmaliges Abmelden aktivieren).
5. Ziehen Sie die aus der IDP-Anwendung erhaltene SAML-Metadatendatei per Drag-and-Drop in das Feld Upload IDP Metadata (IDP-Metadaten hochladen).
6. Klicken Sie auf Speichern.

Anmerkung: Der Status wird als "Incomplete" (Unvollständig) angezeigt, bis die Rollenzuordnung abgeschlossen ist. Dies ist ein erwartungsgemäßes Verhalten.

Konfigurieren der Rollenzuordnung

Bevor Sie mit der Konfiguration der Rollenzuordnung fortfahren, stellen Sie sicher, dass Sie Gruppen aus Active Directory finden, die für die Zuordnung verwendet werden sollen. Führen Sie den folgenden PowerShell-Befehl aus, um Gruppen aus Active Directory zu suchen.

```
$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”] }
```

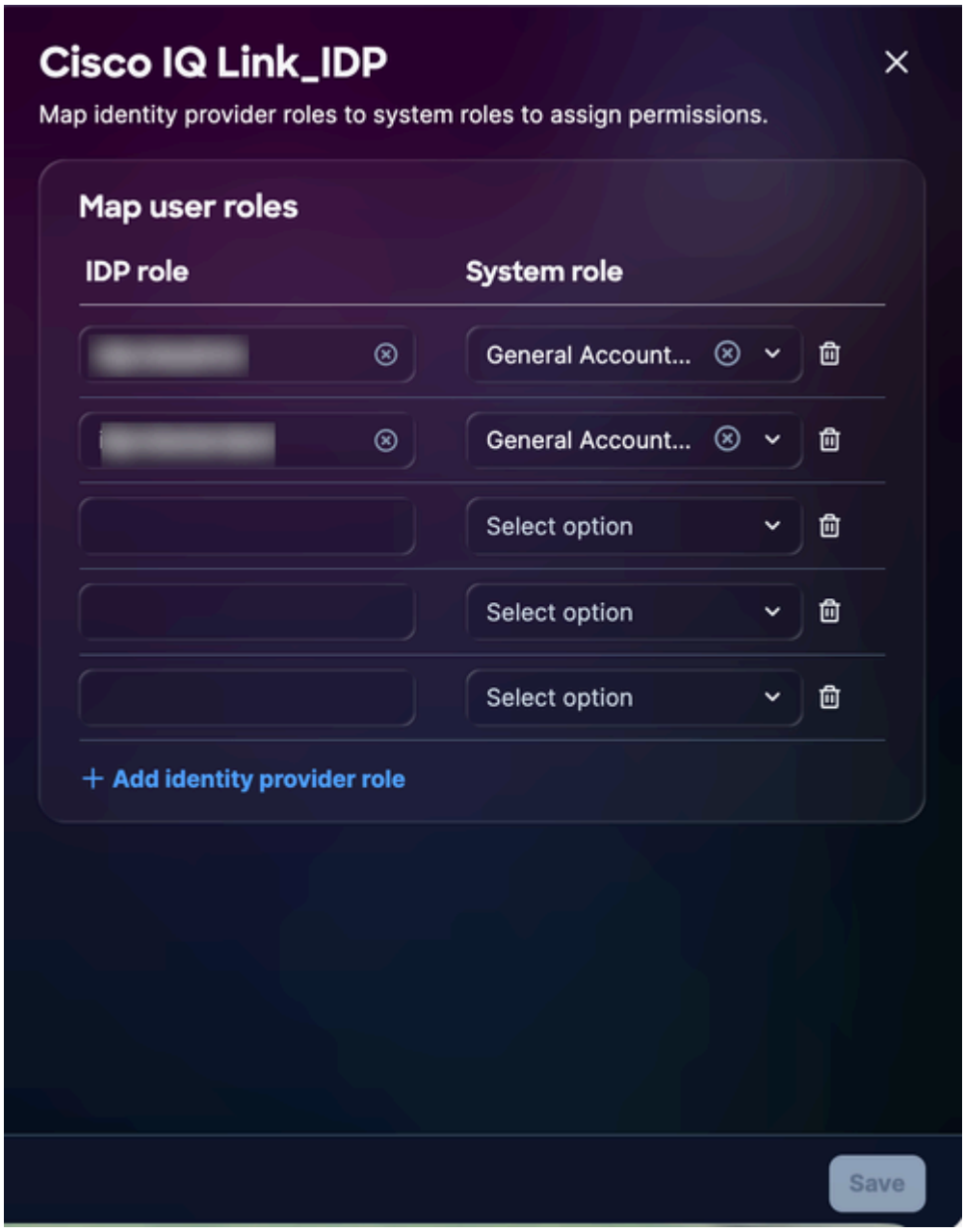
Das System fragt Active Directory direkt über LDAP ab und benötigt keine zusätzlichen Module. Die Gruppeninformationen werden im vollständigen DN-Format (Distinguished Name) zurückgegeben, z. B.:

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

Wenn die erforderlichen Gruppen nicht aufgeführt sind, müssen sie von einem Administrator in Active Directory erstellt werden, bevor Sie die ADFS-Rollenzuordnung abschließen können.

So konfigurieren Sie die Rollenzuordnung:

1. Wählen Sie aus dem hinzugefügten IDP das Symbol More Options (Weitere Optionen) > Map Roles (Rollen zuordnen). Die Seite Benutzerrollen zuordnen wird angezeigt.



Rollenzuordnung

2. Geben Sie eine IDP-Rolle für die ausgewählte Systemrolle ein. Folgende Systemrollen werden unterstützt:

    - general_account_administrator: Der allgemeine Kontoadministrator verfügt über umfassende Berechtigungen zum Ausführen aller Aktionen im Produkt. Die IDP-Rolle (analysierter Name) lautet CXIQ Admins.
    - general_account__viewer: Die allgemeine Kontoanzeige verfügt über schreibgeschützten Zugriff. Die IDP-Rolle (analysierter Name) ist CXIQ-Entwickler und CXIQ-Viewer.

    Anmerkung: Verwenden Sie analysierte Namen (z. B. CXIQ-Entwickler) und nicht vollständige Domänennamen.

    ---

3. Klicken Sie auf Speichern. Der Status wird auf Erfolgreich aktualisiert.

Verifizierung und Tests

Testen der Authentifizierung

1. Navigieren Sie in einem Browser mit Inkognito- oder privatem Modus zu https://your-cisco-iq-domain.com/login.
2. Melden Sie sich mit Ihren Active Directory-Anmeldeinformationen im Format Domäne\Benutzername oder user@domain.local an.
3. Stellen Sie sicher, dass Sie zur Cisco IQ-Startseite weitergeleitet werden (nach erfolgreicher Authentifizierung).
4. Vergewissern Sie sich, dass die zugewiesenen Rollen die richtigen analysierten Gruppennamen (z. B. CXIQ-Entwickler) in Ihrem Benutzerprofil anzeigen.

Testen der Abmeldung

Zum Testen der Abmeldung klicken Sie auf Abmelden vom Cisco IQ. Die Meldung "Logging out, please wait..." (Abmelden, bitte warten...) wird angezeigt, und Sie werden zur Seite Cisco IQ-Anmeldung weitergeleitet. Das System beendet auch die ADFS-Sitzung. Wenn Sie versuchen, direkt auf ADFS zuzugreifen, werden Sie aufgefordert, sich erneut anzumelden.

Fehlerbehebung bei ADFS-Problemen

In der folgenden Liste werden häufige Probleme und mögliche Lösungen beschrieben, um Probleme im Zusammenhang mit dem ADFS-Status, Zertifikatfehlern, SSO-Anmeldefehlern und der SLO-Konfiguration schnell zu identifizieren und zu beheben.

ADFS-Probleme

Problem	Symptome / Beschreibung	Ursachen/Prüfungen/Problemumgehungen und Korrekturen
Nicht extrahierte Gruppen	Keine Rollen nach der Anmeldung	• Anspruchsregel fehlt: Führen Sie die Anweisungen unter Konfigurieren der ADFS-Anspruchsregeln erneut aus.

Problem	Symptome / Beschreibung	Ursachen/Prüfungen/Problemumgehungen und Korrekturen
		• Falsches Gruppenattribut: Muss sich auf http://schemas.xmlsoap.org/claims/Group befinden. • Benutzer ist nicht in AD-Gruppen
Entschlüsselung fehlgeschlagen	Fehler beim Entschlüsseln der Assertion in Protokollen.	Konfiguration der ADFS-Zertifikatkonfiguration überprüfen
Anmelde-Schleife	In Authentifizierungs- oder Anmelde-Schleife feststecken	• Ungültige ACS-URL: Überprüfen Sie: https://your-fqdn/saml/acs • Cookie-Diskrepanz: Browser-Cookies auf die richtige Domain überprüfen

Diagnosebefehle zur Fehlerbehebung

Um eine erfolgreiche Integration zwischen Ihrer ADFS-Umgebung und Cisco IQ sicherzustellen, verwenden Sie die folgenden Diagnosebefehle. Mit diesen Befehlen können der Zugriff auf Metadaten, die Zertifikatkonfigurationen und die Endpunkteinstellungen überprüft werden.

- Zugänglichkeit von ADFS-Metadaten überprüfen: bestätigt, dass die ADFS-Verbundmetadaten erreichbar und öffentlich zugänglich sind; Dies ist ein wichtiger Schritt zur Einrichtung des anfänglichen Vertrauens.

```
curl -k https://

    /FederationMetadata/2007-06/FederationMetadata.xml
```

- Validieren Sie das Verschlüsselungszertifikat: Stellt sicher, dass das richtige Verschlüsselungszertifikat mit dem Cisco IQ Relying Party Trust verknüpft ist

```
Get-AdfsRelyingPartyTrust -Name “Cisco IQ - Stage” | Select-Object EncryptionCertificate | Format-List
```

- Überprüfen der SAML-Endpunktkonfiguration: Überprüft, ob die SAML-Endpunkte für die Cisco IQ-Vertrauensstellung richtig konfiguriert sind und Authentifizierungsanforderungen und -assertionen an die erwarteten URLs weitergeleitet werden

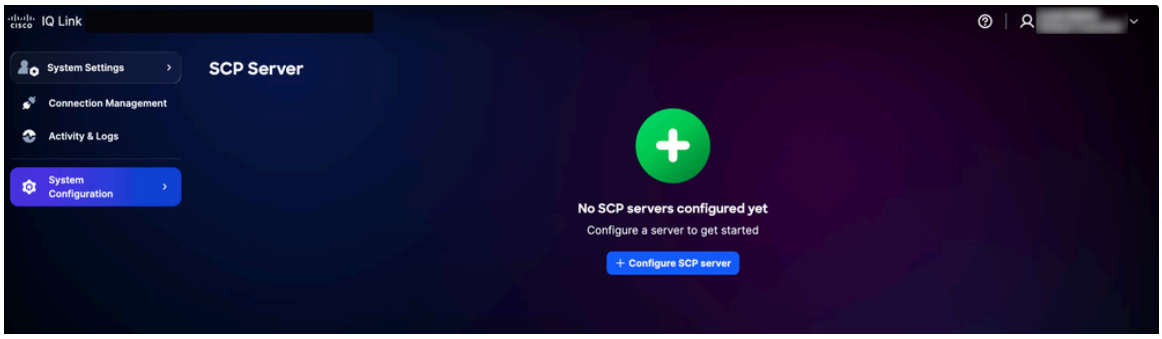
```
Get-AdfsRelyingPartyTrust -Name “Cisco IQ - Stage” | Select-Object SamlEndpoints
```

SCP-Server hinzufügen

Dieser SCP-Server (Secure Copy Protocol) ist eine Voraussetzung für den Import von Upgrade-Dateien, die zum Hinzufügen, Aktualisieren oder Reparieren der Cisco IQ-Installation erforderlich sind.

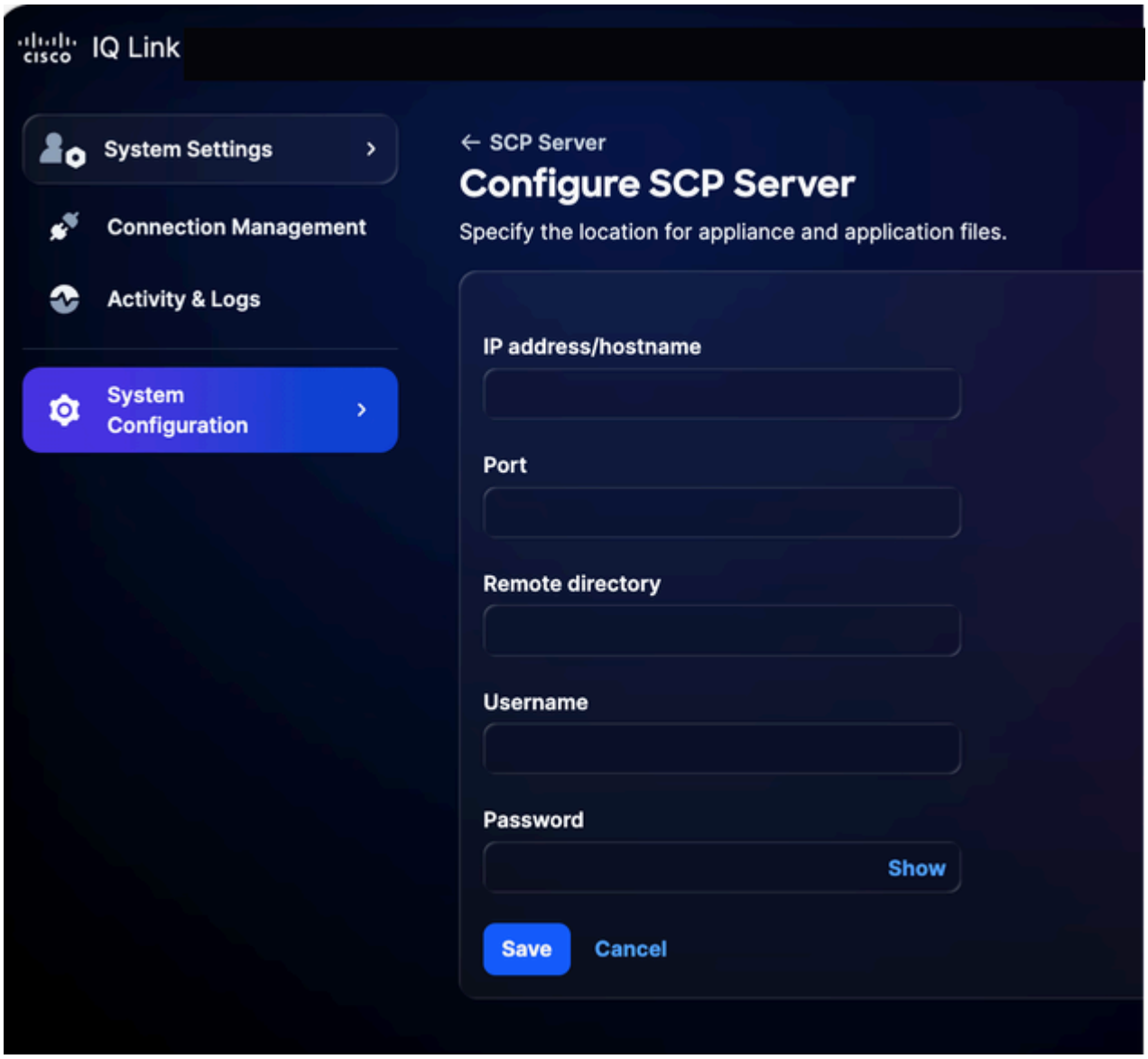
SCP-Server hinzufügen:

1. Wählen Sie in den Systemeinstellungen die Option Systemkonfiguration > SCP-Server aus. Die Seite SCP Server wird angezeigt.



SCP-Server-Startseite

2. Klicken Sie auf SCP-Server konfigurieren.



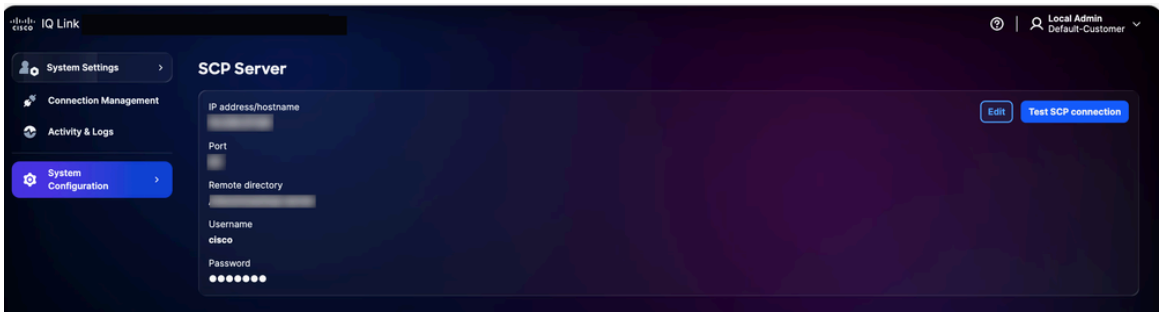
SCP-Server konfigurieren

3. Geben Sie die IP-Adresse/den Hostnamen ein.
4. Geben Sie eine Portnummer ein.
5. Geben Sie das Remote-Verzeichnis ein.
6. Geben Sie einen Benutzernamen ein.
7. Geben Sie ein Kennwort ein.
8. Klicken Sie auf Speichern. Es wird eine Bestätigung angezeigt.

Bearbeiten vorhandener SCP-Server

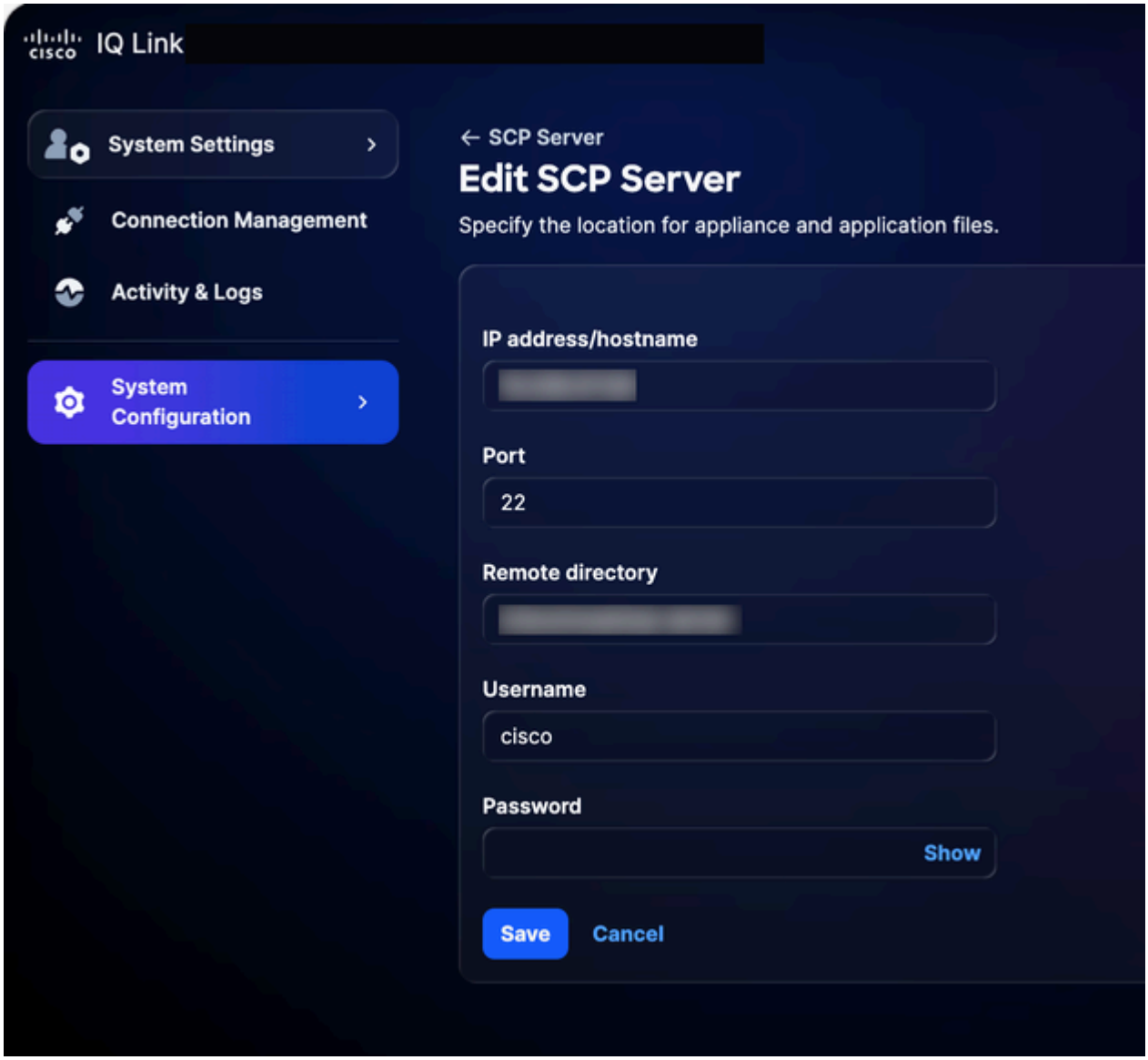
So bearbeiten Sie einen vorhandenen SCP-Server:

1. Navigieren Sie zur Seite SCP-Server.



SCP-Server

2. Klicken Sie für den gewünschten vorhandenen SCP-Server auf Edit.



SCP-Server bearbeiten

3. Ändern Sie die Details nach Bedarf.

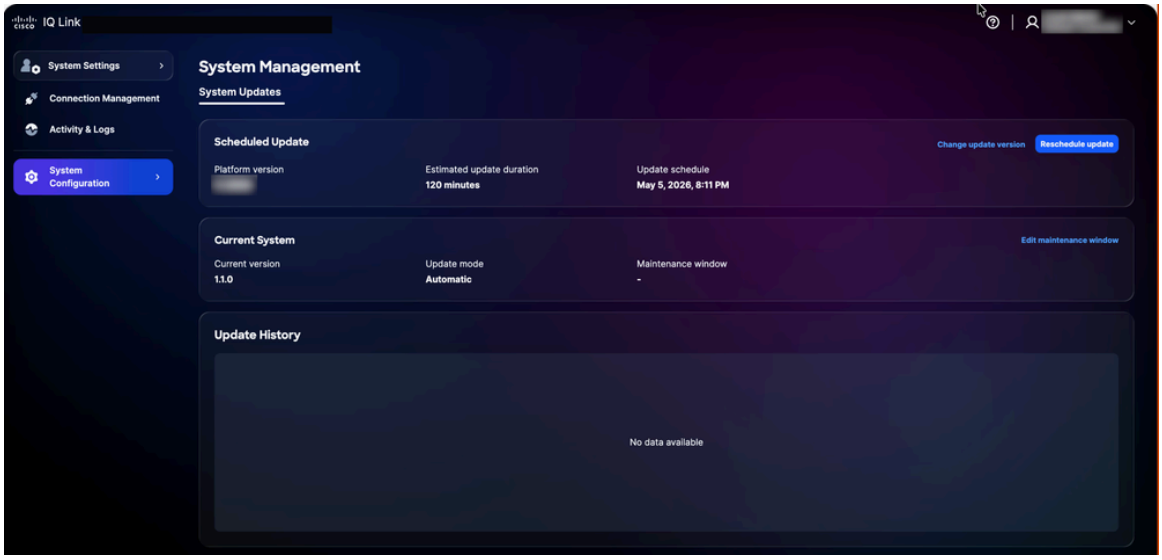
4. Klicken Sie auf Speichern.

Systemverwaltung

Kunden können über die Benutzeroberfläche ein Upgrade auf die neueste Cisco IQ Link-Version durchführen. Sie können dies auch auf der Seite Cisco IQ Data Connectors überprüfen.

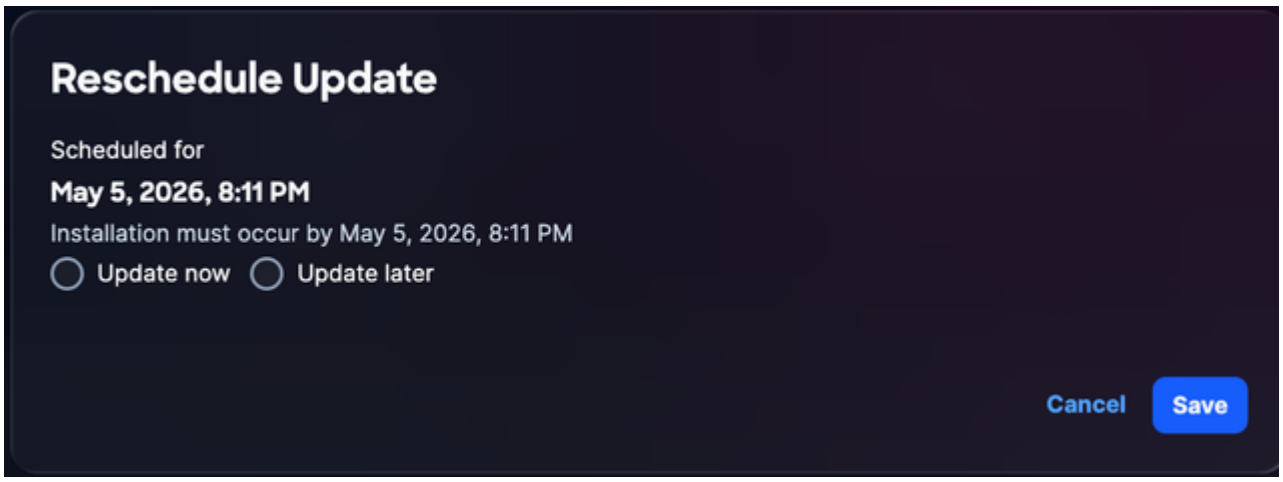
So planen Sie die Systemaktualisierung neu:

1. Wählen Sie in Administration die Option System Configuration > System Management (Systemkonfiguration > Systemverwaltung) aus. Die Seite Systemverwaltung wird angezeigt. Auf dieser Seite wird die Systemversion angezeigt, die derzeit ausgeführt wird. Wenn keine Updates konfiguriert wurden, ist der Abschnitt Aktualisierungsverlauf leer.



System-Upgrade

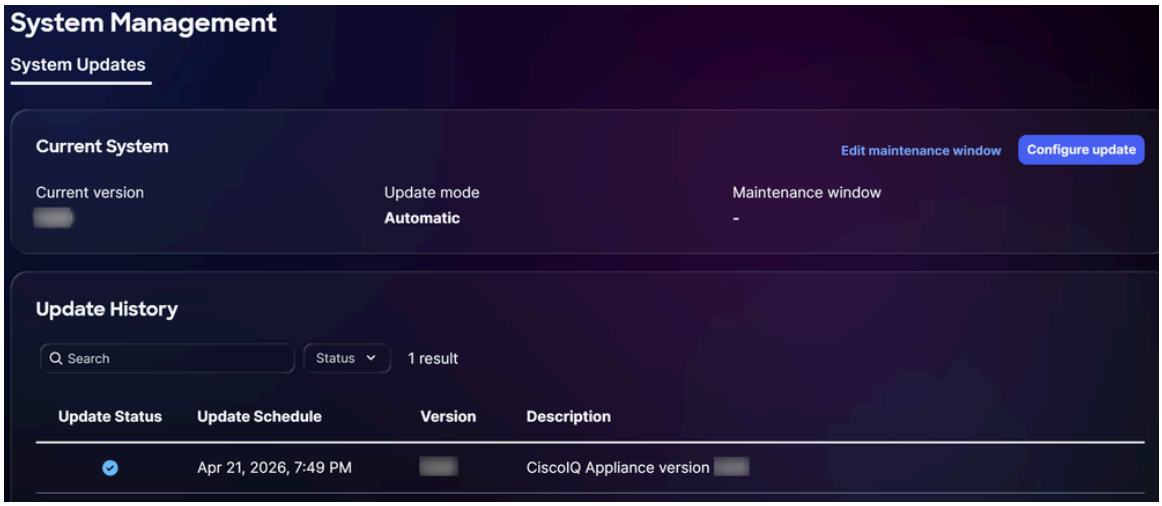
2. Klicken Sie auf Update neu planen.



Upgrade neu planen

3. Klicken Sie auf Jetzt aktualisieren, um eine sofortige Neuplanung vorzunehmen, oder auf Später aktualisieren, um einen anderen Termin zu vereinbaren.

4. Klicken Sie auf Speichern. Eine Bestätigung wird angezeigt, und Sie werden zur Startseite für das Systemupdate weitergeleitet.



Erfolgreiches Upgrade

Konfiguration von SSL-Zertifikaten

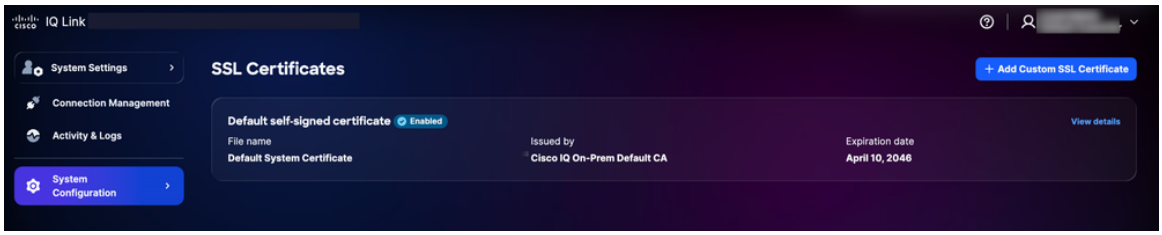
Ein standardmäßig selbst signiertes Zertifikat ist vorinstalliert und in Cisco IQ aktiviert. Benutzer können jedoch benutzerdefinierte SSL-Zertifikate hochladen. Wenn ein benutzerdefiniertes SSL-Zertifikat aktiviert ist, wird es für HTTPS-Verbindungen verwendet. Wenn das Zertifikat deaktiviert oder gelöscht wird, wird automatisch das Standardzertifikat wiederhergestellt.

Anmerkung: Das Zertifikat muss noch mindestens 90 Tage gültig sein. Ein Zertifikat gilt als "bald abgelaufen", wenn es weniger als 90 Tage bis zum Ablauf hat. Nach dem Hinzufügen, Bearbeiten oder Löschen eines SSL-Zertifikats muss der Kunde das neue SSL hochladen, wie im Abschnitt Completing SLO Configuration (SLO-Konfiguration abschließen) für den Okta IDP oder den ADFS IDP beschrieben.

Hinzufügen eines benutzerdefinierten SSL-Zertifikats

So fügen Sie ein benutzerdefiniertes SSL-Zertifikat hinzu

1. Wählen Sie in den Systemeinstellungen die Option Systemkonfiguration > SSL-Zertifikate aus. Die Seite SSL-Zertifikate wird angezeigt, auf der alle SSL-Zertifikate für Ihr System aufgeführt sind.

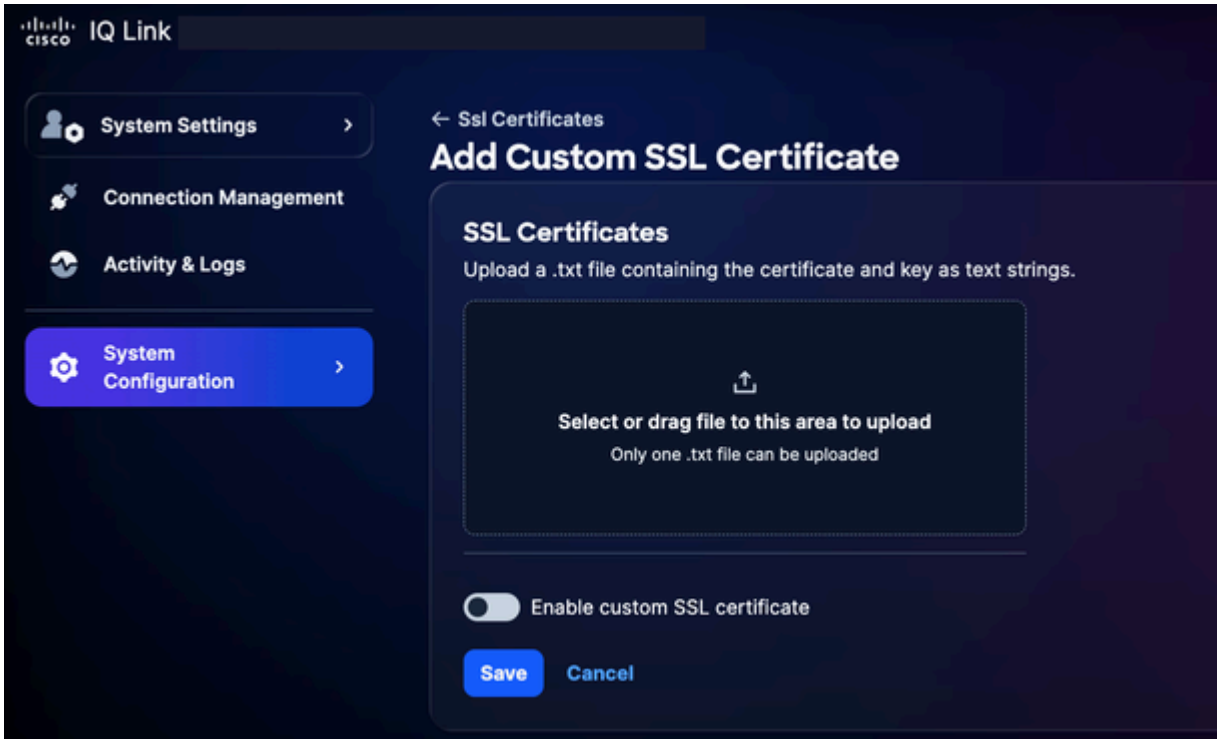


Hinzufügen eines SSL-Zertifikats

2. Klicken Sie auf Benutzerdefiniertes SSL-Zertifikat hinzufügen.

Hinweise:

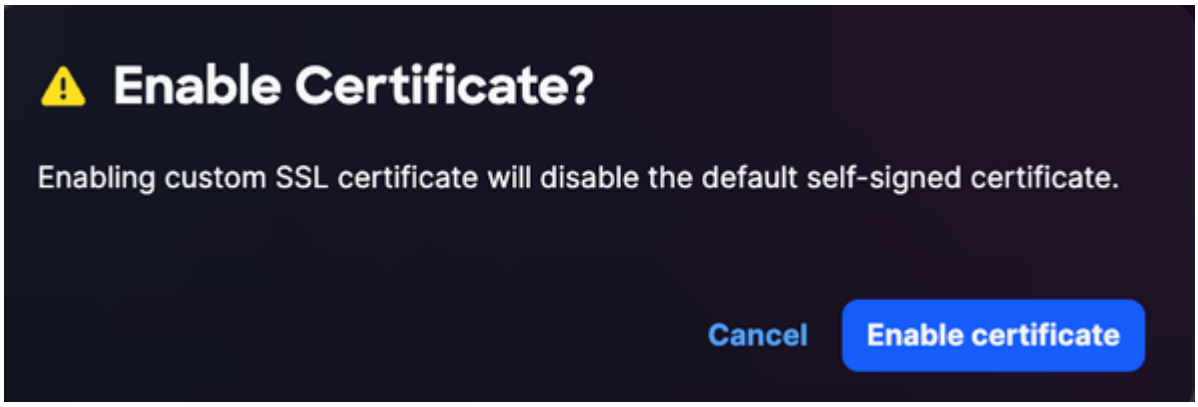
- Laden Sie eine TXT-Datei hoch, die sowohl das Privacy-Enhanced Mail-codierte Zertifikat als auch den Schlüssel als Textzeichenfolgen enthält
- Es kann jeweils nur eine TXT-Datei hochgeladen werden.
- Die Datei muss das Zertifikat und den privaten Schlüssel enthalten.



SSL-Zertifikate hochladen

3. Ziehen Sie das benutzerdefinierte SSL-Zertifikat per Drag-and-Drop in das Feld SSL-Zertifikat, oder laden Sie es hoch.

4. Aktivieren Sie die Schaltfläche Benutzerdefiniertes SSL-Zertifikat aktivieren.



Zertifikat aktivieren

Anmerkung: Lassen Sie den Schalter AUS, wenn Sie das Zertifikat hochladen möchten, ohne es sofort zu aktivieren.

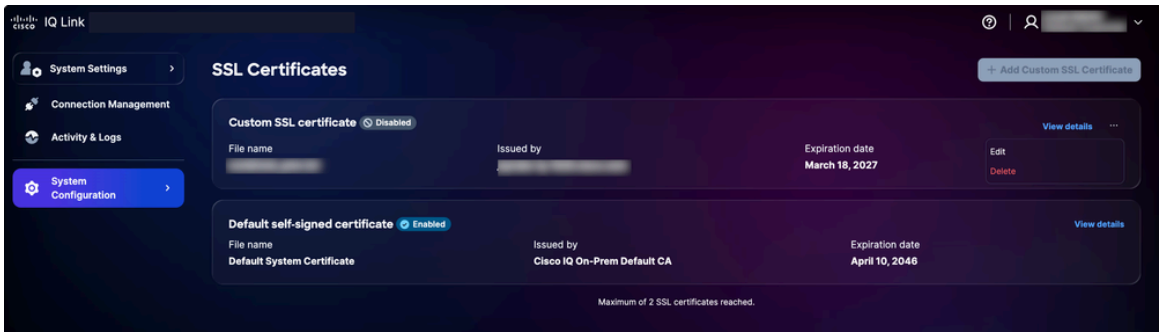
5. Klicken Sie auf Zertifikat aktivieren.
6. Klicken Sie auf Speichern.

Das benutzerdefinierte SSL-Zertifikat ist aktiviert und aktiv. Das Standard-Systemzertifikat wird automatisch deaktiviert.

Bearbeiten benutzerdefinierter SSL-Zertifikate

Sie können das benutzerdefinierte SSL-Zertifikat bearbeiten, um ein neues Zertifikat hochzuladen oder das aktuell aktivierte Zertifikat zu deaktivieren. So bearbeiten Sie:

1. Navigieren Sie zum gewünschten benutzerdefinierten SSL-Zertifikat.



SSL-Zertifikat bearbeiten

2. Wählen Sie das Symbol Weitere Optionen > Bearbeiten aus. Die Seite SSL-Zertifikat bearbeiten wird angezeigt.
3. Bearbeiten Sie die Zertifikatdetails nach Bedarf.

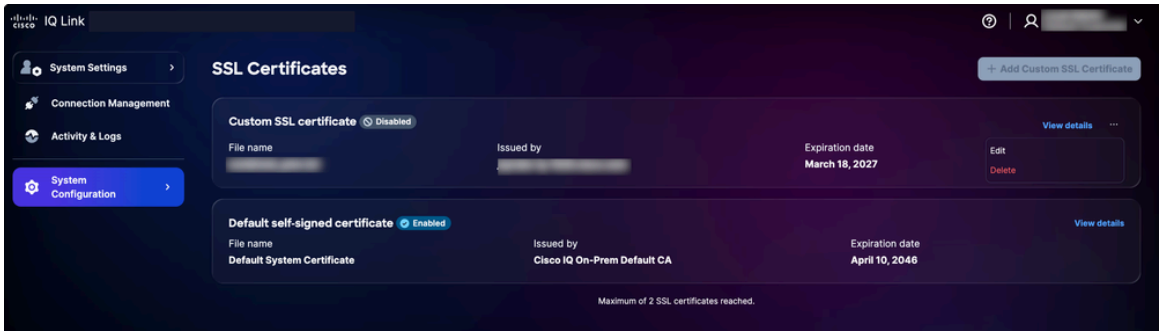
4. Klicken Sie auf Speichern.

Benutzerdefinierte SSL-Zertifikate löschen

Warnung: Ein benutzerdefiniertes SSL-Zertifikat kann jederzeit gelöscht werden, es handelt sich jedoch um eine unumkehrbare Aktion. Sie können jederzeit nach dem Löschen ein neues benutzerdefiniertes Zertifikat hochladen.

So löschen:

1. Navigieren Sie zum gewünschten persönlichen SSL-Zertifikat.



SSL-Zertifikat löschen

2. Wählen Sie das Symbol Weitere Optionen > Löschen.
3. Klicken Sie auf Zertifikat löschen. Das benutzerdefinierte Zertifikat wird gelöscht, und das Standardzertifikat wird automatisch wieder aktiviert.

Syslog-Serverkonfiguration

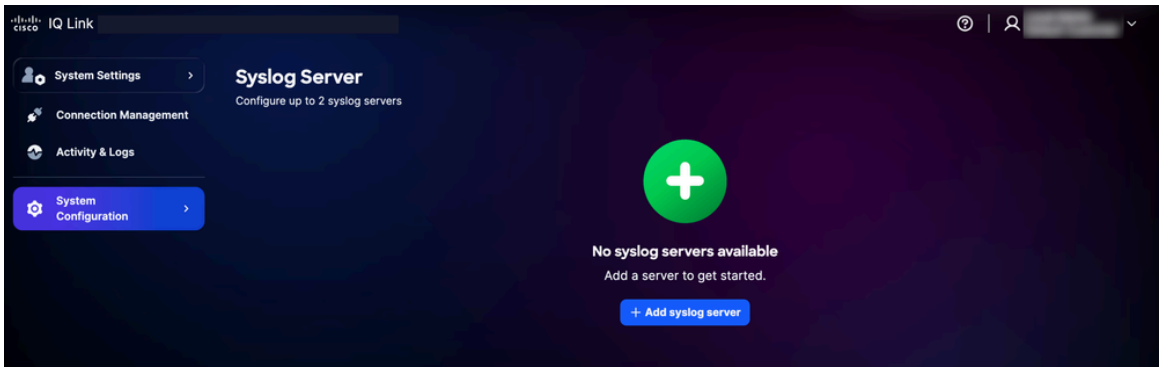
Benutzer mit der Administratorrolle können externe Syslog-Server für den Export von Systemprotokollen konfigurieren. Es können bis zu zwei (2) Syslog-Server konfiguriert werden.

Anmerkung: Der Syslog-Server muss als IP-Adresse und nicht als FQDN (Fully Qualified Domain Name) angegeben werden.

Hinzufügen von Syslog-Servern

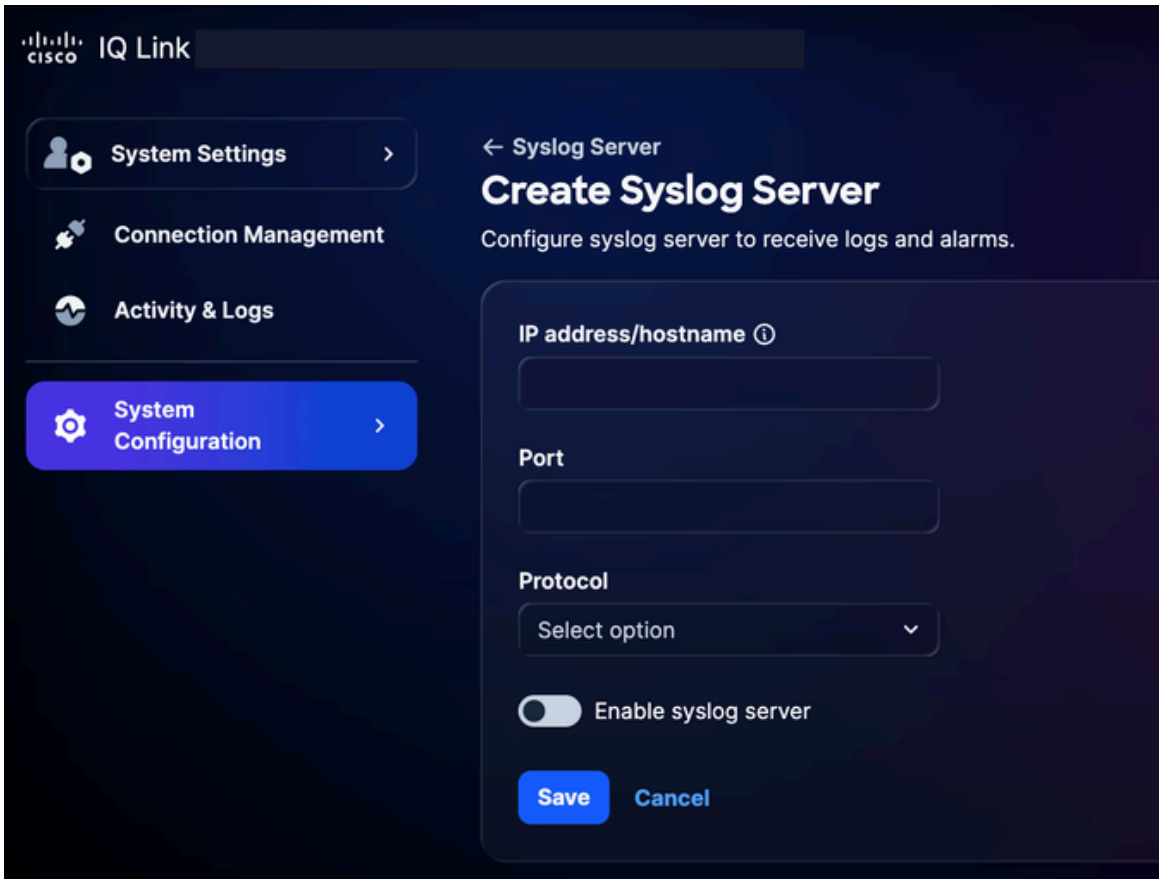
Syslog-Server hinzufügen:

1. Wählen Sie in den Systemeinstellungen die Option Systemkonfiguration > Syslog-Server aus. Die Seite Syslog-Server wird angezeigt.



Syslog-Server hinzufügen

2. Klicken Sie auf Syslog-Server hinzufügen. Die Seite Syslog-Server erstellen wird angezeigt.



Syslog-Server erstellen

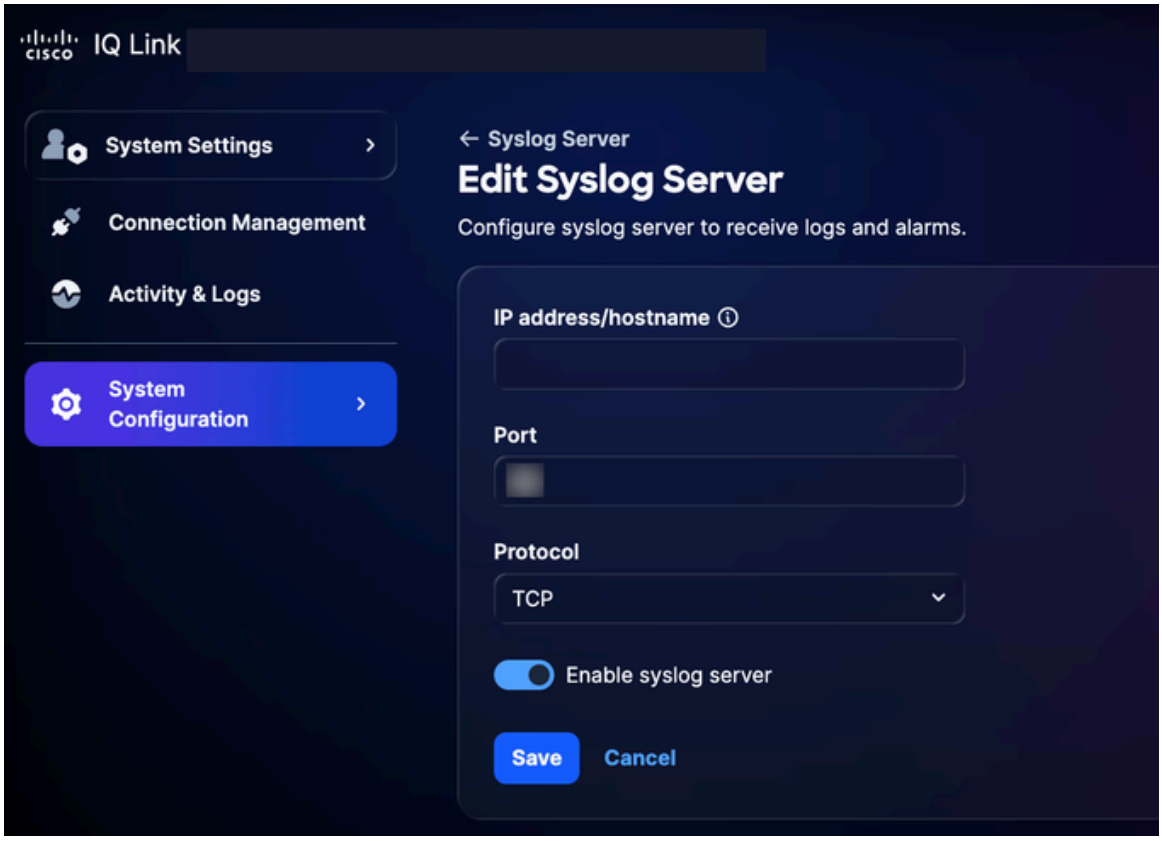
3. Geben Sie die IP-Adresse/den Hostnamen ein.
4. Geben Sie eine Port-Nummer ein.
5. Wählen Sie das entsprechende Protokoll aus der Dropdown-Liste "Protocol" (Protokoll) aus (z. B. UDP oder TCP).
6. Aktivieren Sie die Umschaltfläche Syslog-Server aktivieren.

7. Klicken Sie auf Speichern. Es wird eine Bestätigung angezeigt, und der neu hinzugefügte Syslog-Server wird auf der Syslog-Server-Startseite angezeigt.

Bearbeiten konfigurierter Syslog-Server

So bearbeiten Sie einen konfigurierten Syslog-Server:

1. Navigieren Sie zum gewünschten Syslog-Server.
2. Wählen Sie das Symbol Weitere Optionen > Bearbeiten aus. Die Seite "Syslog-Server bearbeiten" wird angezeigt.



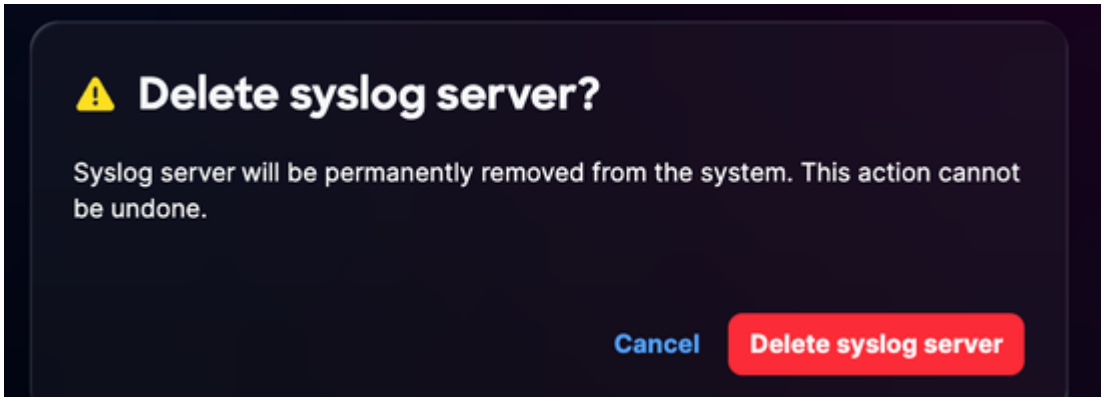
Syslog-Server bearbeiten

3. Bearbeiten Sie nach Bedarf Details, oder deaktivieren Sie den Umschalter Syslog-Server aktivieren.
4. Klicken Sie auf Speichern.

Konfigurierte Syslog-Server löschen

Einen konfigurierten Syslog-Server löschen:

1. Navigieren Sie zum gewünschten Syslog-Server.
2. Wählen Sie das Symbol Weitere Optionen > Löschen aus. Es wird eine Bestätigung angezeigt.

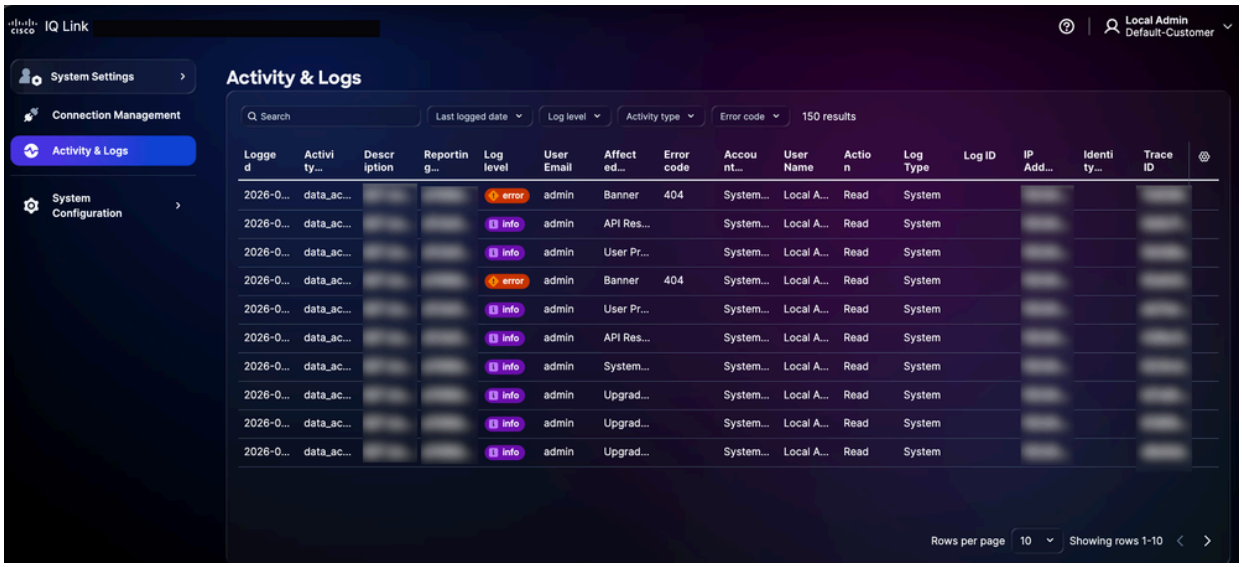


Bestätigung

3. Klicken Sie auf Syslog-Server löschen.

Aktivität und Protokolle

Aktivität und Protokolle bieten eine detaillierte Aufzeichnung von Benutzeraktionen und Änderungen in Cisco IQ, sodass Administratoren Benutzeraktivitäten nachverfolgen und die Transparenz beibehalten können.



Aktivität und Protokolle

Um Aktivitäten und Protokolle anzuzeigen, wählen Sie Aktivität und Protokolle aus dem Menü Systemeinstellungen.

Aktivität und Protokolle:

- Unterstützung von Filtern, Paginierung und Suchfunktionen für eine einfache Suche und Verwaltung von Informationen
- Aufzeichnen aller API-Vorgänge auf Gateway-Ebene

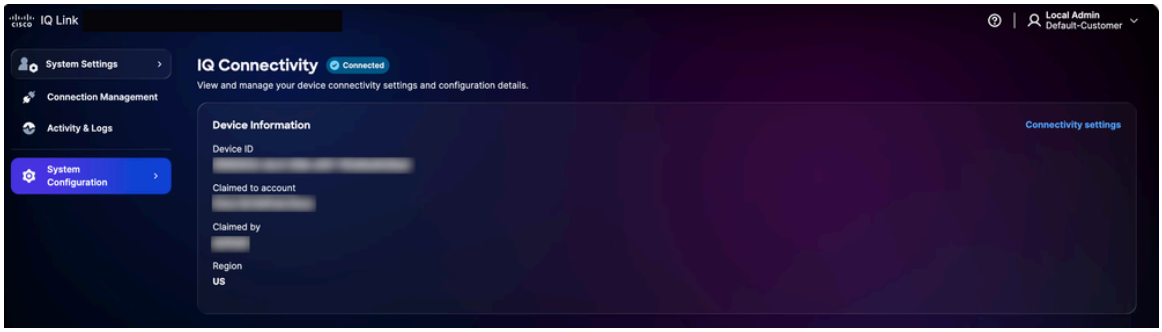
Folgende Filteroptionen sind verfügbar:

- Datum: Filtert Protokolle auf einen bestimmten Zeitraum
- Protokollstufe: Filtert Protokolle nach Schweregrad (z. B. Fehler, Warnungen und Informationen)
- Aktivitätstyp: Filtert Protokolle nach Art der Systemaktivität
- Fehlercode: Filtert Protokolle nach einem bestimmten Fehlercode

IQ-Konnektivität

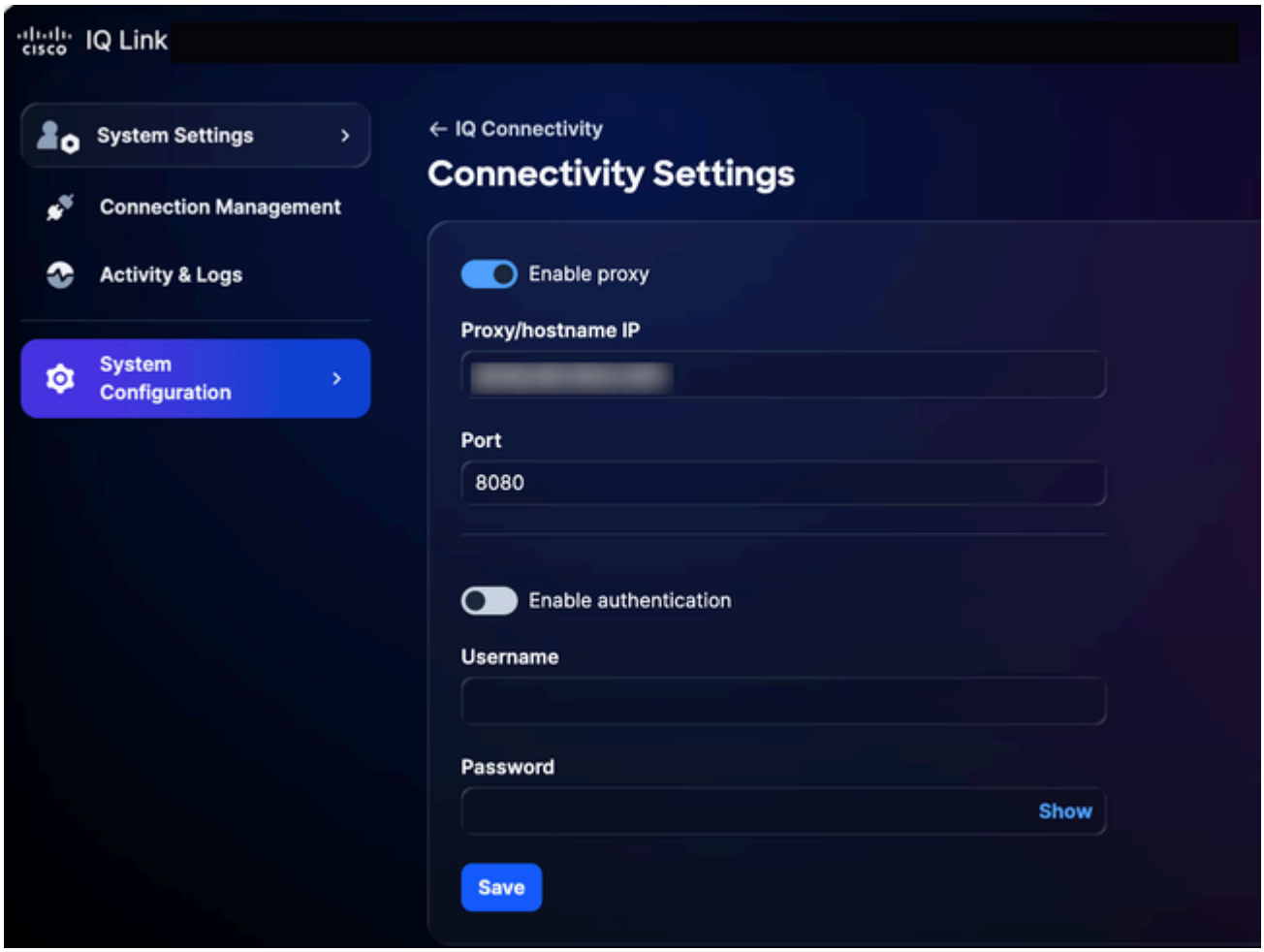
So zeigen Sie Verbindungseinstellungen und Konfigurationsdetails für Geräte an und verwalten diese:

1. Wählen Sie in den Systemeinstellungen die Option Systemkonfiguration > IQ-Verbindung aus. Die Seite "IQ Connectivity" wird angezeigt.



IQ-Konnektivität

2. Klicken Sie auf Verbindungseinstellungen.



Verbindungseinstellungen

3. Aktualisieren Sie die Details nach Bedarf.
4. Klicken Sie auf Speichern.

Verbindungsverwaltung (Datensammlung)

Cisco IQ Link ist eine vor Ort bereitgestellte Lösung für die Erfassung von Netzwerkdaten und sorgt für umfassende Transparenz in Ihrer Infrastruktur. Es erfasst Daten über Catalyst Center und Direct Connection. Es vereinfacht das Management der Netzwerkauthentifizierung und Geräteerkennung. Die Konfiguration der Datenerfassung kann wie folgt zusammengefasst werden:

- Erstellen von Anmeldeinformationssätzen: Richten Sie die Authentifizierungsprotokolle (z. B. SNMP v1/v2c/v3) für die Kommunikation mit den Netzwerkgeräten ein. Durch die Zentralisierung der Anmeldeinformationen nach Sicherheitszone oder Standort (z. B. "SanJose-SNMPv3") können Sie Kennwörter an einem Standort aktualisieren, wobei die Änderungen automatisch auf alle verbundenen Geräte übertragen werden.

Anmerkung: Für Cisco IQ Link ist ein Benutzerkonto erforderlich, das mit der Berechtigungsstufe 15 auf dem Gerät konfiguriert wurde, um direkt verbundene Ressourcen zu authentifizieren.

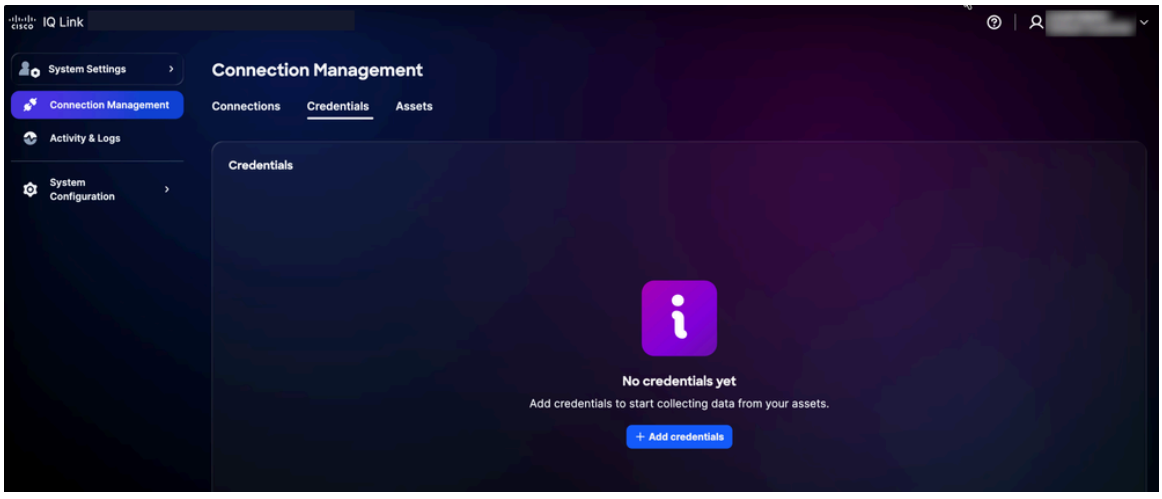
- Zuordnen von Anmeldeinformationen zum Bestand: Ordnen Sie Ihre Berechtigungssätze den Bestands-Ressourcen zu, um den Authentifizierungsprozess zu automatisieren. Durch das Erstellen von Regeln, die bestimmte IP-Bereiche mit definierten Berechtigungssätzen verknüpfen, wendet das System während der Datenerfassung automatisch die richtige Authentifizierung an. So werden manuelle Eingabefehler vermieden und sichergestellt, dass die Konfiguration mit wachsendem Netzwerk immer fehlerfrei abläuft.

Anmerkung: Für die Geräteerkennung sind SNMPv2c/SNMPv3 und SSH erforderlich, und vor der Konfiguration von Catalyst Center müssen HTTP/HTTPS-Anmeldeinformationen angegeben werden.

Hinzufügen von Anmeldeinformationen

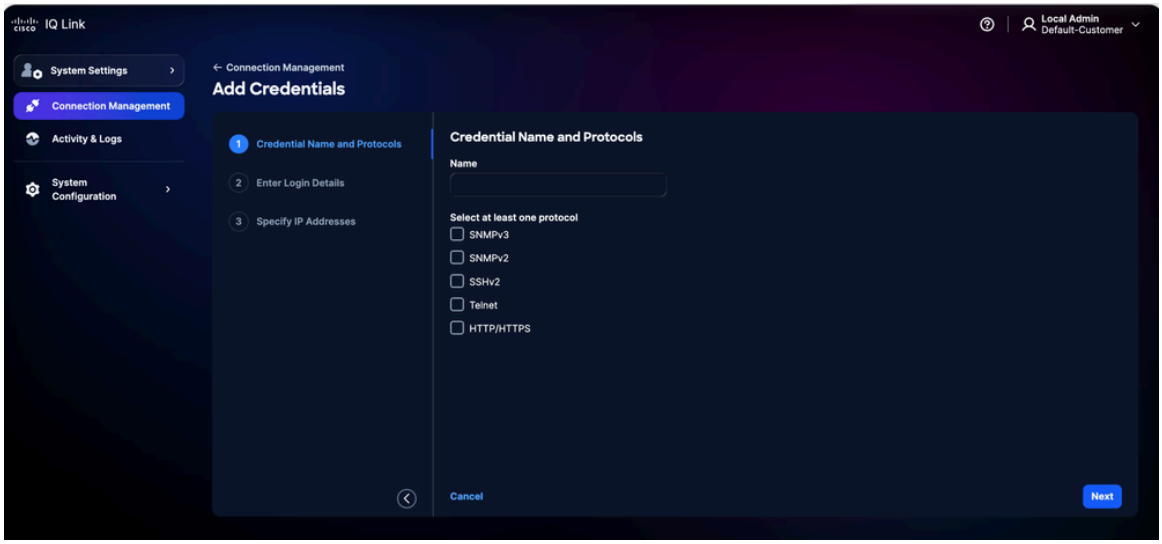
Sie müssen zunächst Anmeldeinformationen hinzufügen, um die Datensammlung durchzuführen. So fügen Sie Anmeldeinformationen hinzu:

1. Wählen Sie unter Systemeinstellungen die Option Verbindungsverwaltung aus. Die Seite Verbindungsverwaltung wird angezeigt.
2. Klicken Sie auf die Registerkarte Anmeldedaten.



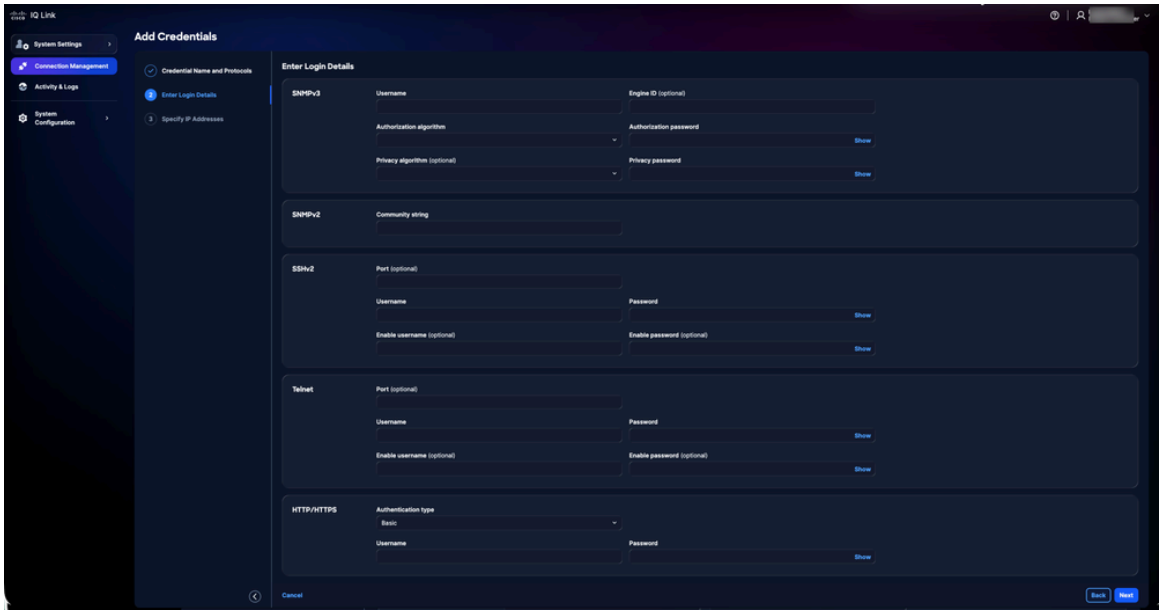
Registerkarte "Anmeldeinformationen"

3. Klicken Sie auf Anmeldedaten hinzufügen.



Anmeldeinformationen hinzufügen

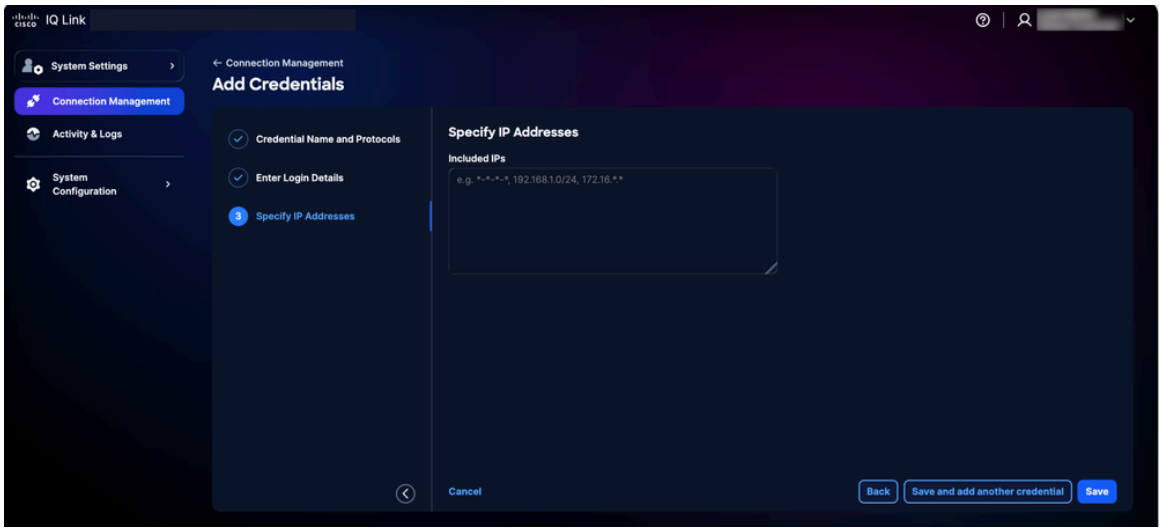
4. Geben Sie einen Namen ein.
5. Aktivieren Sie alle zutreffenden Kontrollkästchen für das Protokoll.
6. Klicken Sie auf Next (Weiter).



Anmeldeinformationsdetails hinzufügen

Anmerkung: Für das obige Bild zeigen wir die Ansicht, wenn alle Protokolle im vorherigen Schritt ausgewählt wurden. Ihre Schnittstelle zeigt nur die ausgewählten Protokolle an.

7. Geben Sie die Anmeldedetails für jedes ausgewählte Protokoll ein.
8. Klicken Sie auf Next (Weiter).



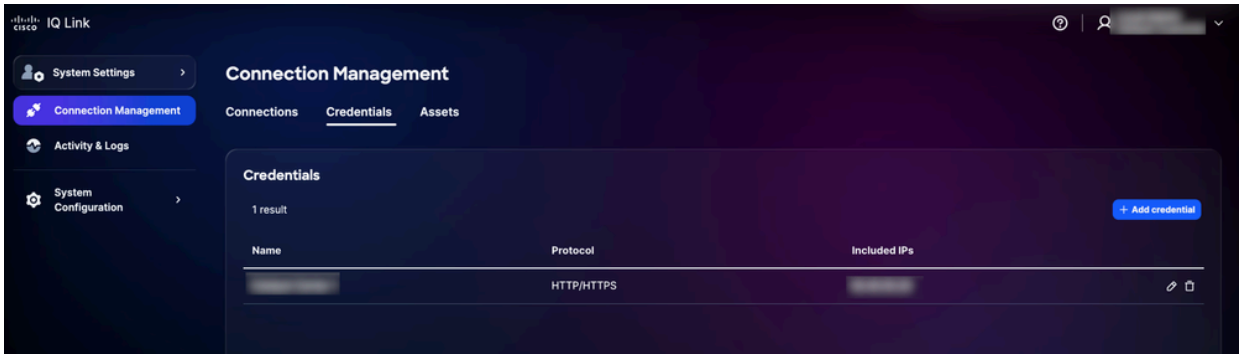
IP-Adressen angeben

9. Geben Sie die enthaltenen IPs ein.

Anmerkung: Dieses Feld definiert die IP-Adressen oder IP-Bereiche, in denen die Anmeldeinformationen zum Herstellen einer Verbindung verwendet werden können. Es unterstützt eine Mischung aus IPs und IP-Masken (in der Schreibweise mit Platzhaltern). Ausführliche Informationen zu unterstützten Formaten finden Sie unter Anrechnungsauswahl und Zuordnungslogik.

---

10. Klicken Sie auf Speichern. Eine Bestätigung wird angezeigt, und Sie werden zur Registerkarte Anmeldedaten weitergeleitet.



Anmeldeinformationen hinzugefügt

Sie können die Anmeldeinformationen bearbeiten, indem Sie auf das Symbol Bearbeiten klicken und sie löschen, indem Sie auf das Symbol Löschen klicken.

Logik für die Auswahl und den Abgleich von Anmeldeinformationen

Die Telemetrie-Engine verwendet eine priorisierungsbasierte Abgleichlogik, um zu bestimmen,

welche Anmeldeinformationen bei der Erkennung und Erfassung angewendet werden sollen. Wenn Sie diese Hierarchie verstehen, wird sichergestellt, dass die richtigen Anmeldeinformationen für die beabsichtigten Geräte verwendet werden.

- Rangfolge der Prioritäten: Wenn für ein Gerät mehrere Berechtigungssätze gelten, werden diese von Cisco IQ auf der Grundlage der Übereinstimmung mit dem Gerät ausgewertet. Das System wendet die folgende Priorität an, wobei spezifischere Übereinstimmungen Vorrang haben:
    - Genaue IP-Übereinstimmung: Höchste Priorität
    - Trailing Wildcard Match:** **Priority hängt von der Anzahl der nachlaufenden Sterne ab; Weniger Sterne stehen für eine spezifischere Übereinstimmung und daher für eine höhere Priorität.
- Platzhalterformatierungsregeln: Platzhalter (*) werden nur als nachfolgende Zeichen in einer IP-Adresse unterstützt. Sie müssen von rechts nach links angewendet werden.
    - Unterstützte Formate:

      1.2.3.* (Höchste Priorität unter Platzhaltern)

      1.2.*

      1.*.*

      ..*.* (niedrigste Priorität)
    - Nicht unterstützte Formate:

      Führende Platzhalter (z. B. *.1.2.3)

      Platzhalter zwischen Oktetten (z. B. 10.10.*.20)

      Verwendung von Bindestrichen oder anderen nicht standardmäßigen Trennzeichen

Beispiel zur Auswahl von Anmeldeinformationen:

In der folgenden Tabelle wird veranschaulicht, wie die Telemetrie-Engine den am besten geeigneten Berechtigungssatz auswählt, wenn ein Gerät mehreren definierten Mustern entspricht.

Beispiel zur Auswahl von Anmeldeinformationen

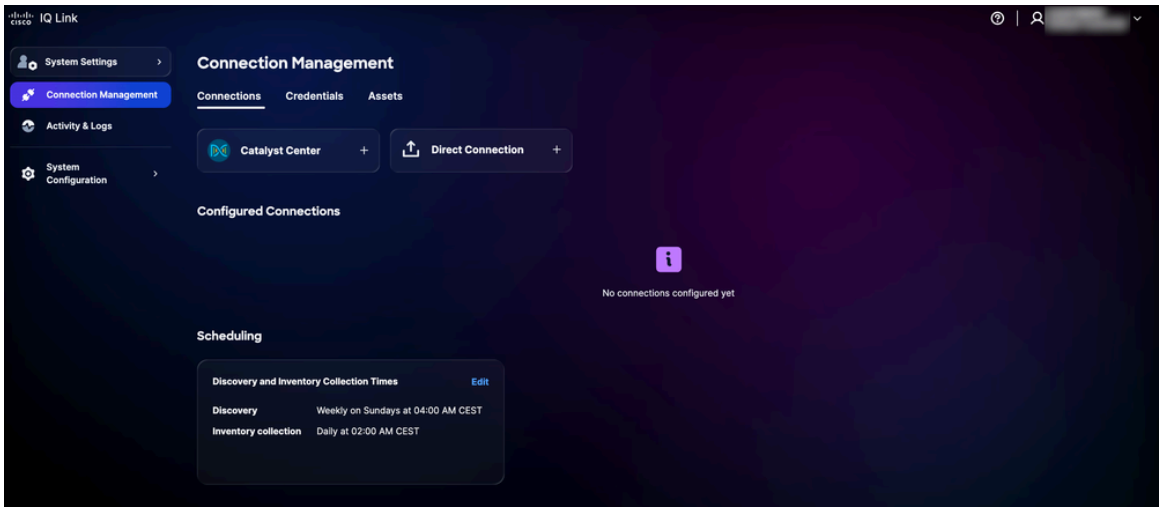
Geräte-IP	Verfügbare Berechtigungssätze	Ausgewählter Berechtigungssatz
10.10.1.5	10.10.1.5, 10.10.1., 10.10..*	10.10.1.5 (Genaue Übereinstimmung)
10.10.2.15	10.10.2., 10.10..*	10.10.2.* (Näheres)
10.10.5.50	10.10.	10.10.. (Genauere Angaben)

Anmerkung: Fällt ein Gerät in mehrere sich überschneidende Kategorien, wählt das System immer den Berechtigungssatz mit der höchsten Spezifität aus (d. h. mit den wenigsten Platzhaltern am Ende).

Datenerfassung mit Catalyst Center

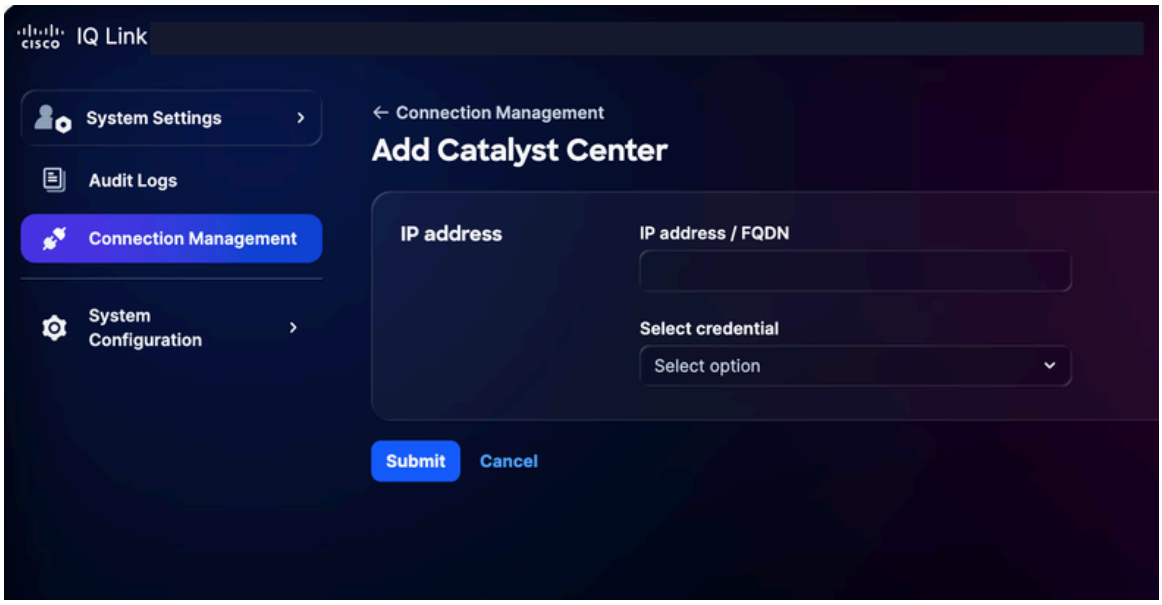
Datenerfassung mit Catalyst Center:

1. Wählen Sie unter Systemeinstellungen die Option Verbindungsverwaltung aus. Die Seite Verbindungsverwaltung wird angezeigt.



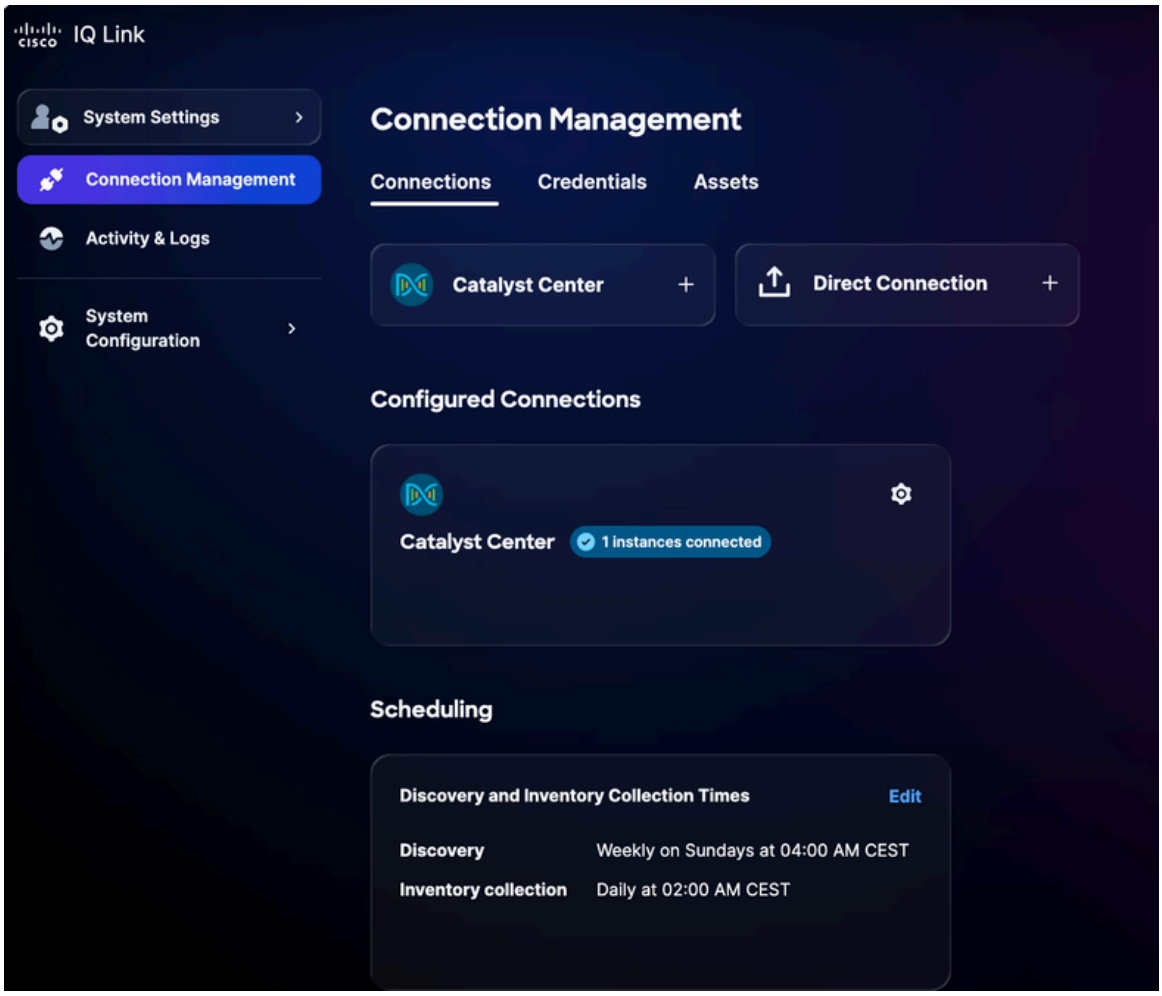
Verbindungsmanagement

2. Klicken Sie auf die Option Catalyst Center.



Catalyst Center hinzufügen

3. Geben Sie die IP-Adresse oder den FQDN ein.
4. Wählen Sie aus der Dropdown-Liste eine konfigurierte HTTP-/HTTPS-Anmeldeinformation aus.
5. Klicken Sie auf Senden. Es wird eine Bestätigung angezeigt (dies kann bis zu 75 Minuten dauern). Sie können das neu hinzugefügte Catalyst Center unter Konfigurierte Verbindungen anzeigen.



Catalyst Center erfolgreich hinzugefügt

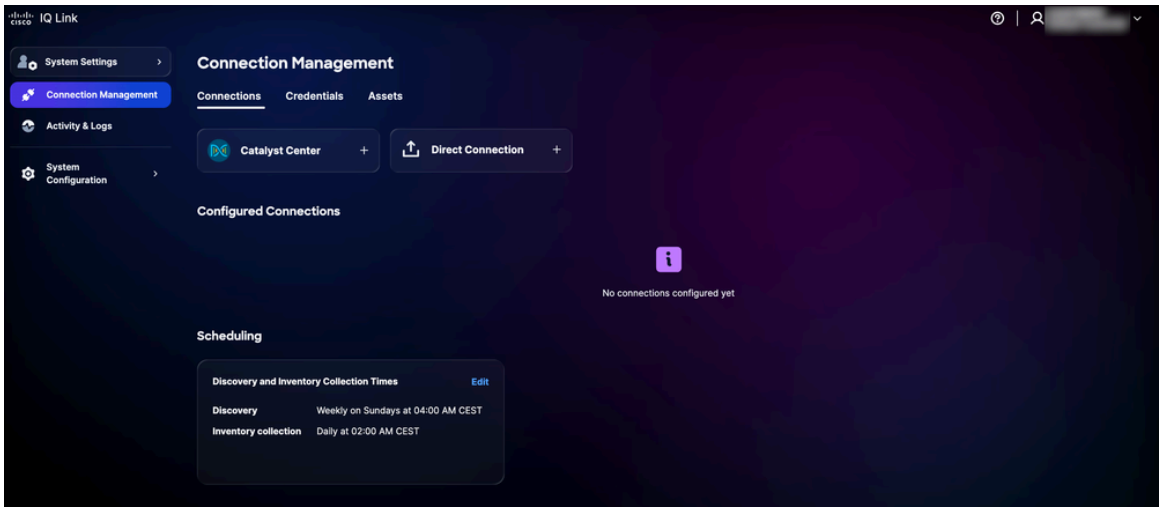
6. Planen einer Sammlung. Weitere Informationen finden Sie unter Planen.

Anmerkung: Cisco IQ Link ist mit einer automatisierten Einrichtung für die Zeitplanung vorkonfiguriert, und das System initiiert einen standardmäßigen automatisierten Zeitplan für die Erfassung. Es wird dringend empfohlen, den Zeitplan entsprechend den Anforderungen und Wartungsfenstern Ihres Unternehmens zu bearbeiten.

Direkte Verbindung

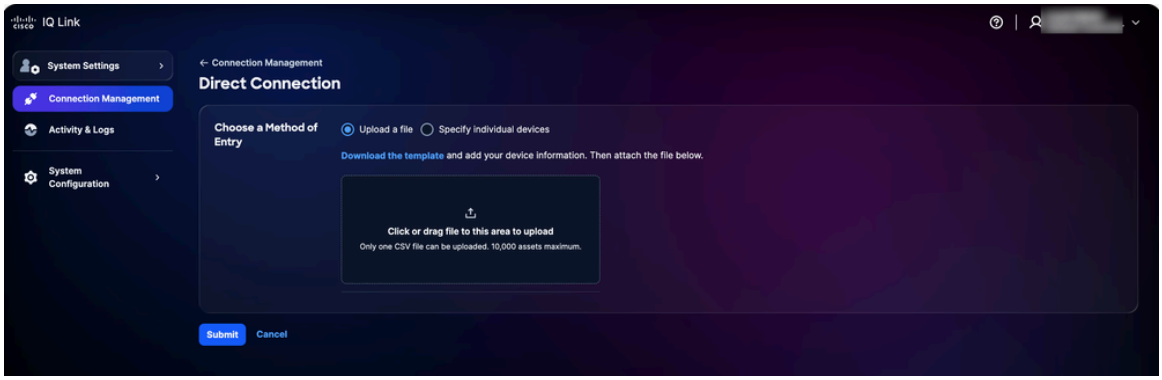
So fügen Sie Geräte für Direktverbindungen hinzu:

1. Wählen Sie unter Systemeinstellungen die Option Verbindungsverwaltung aus. Die Seite Verbindungsverwaltung wird angezeigt.



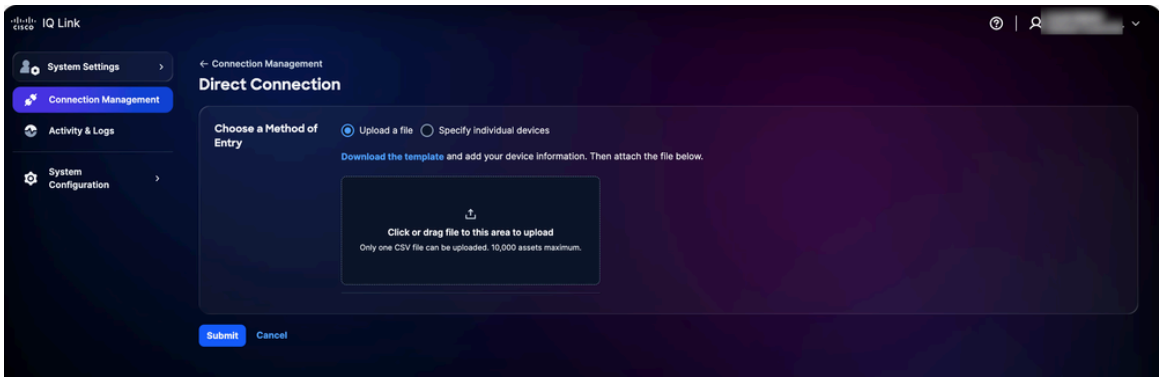
Verbindungsmanagement

2. Klicken Sie auf Direktverbindung. Die Seite "Direktverbindung" wird mit zwei (2) Optionen zum Sammeln von Daten angezeigt.



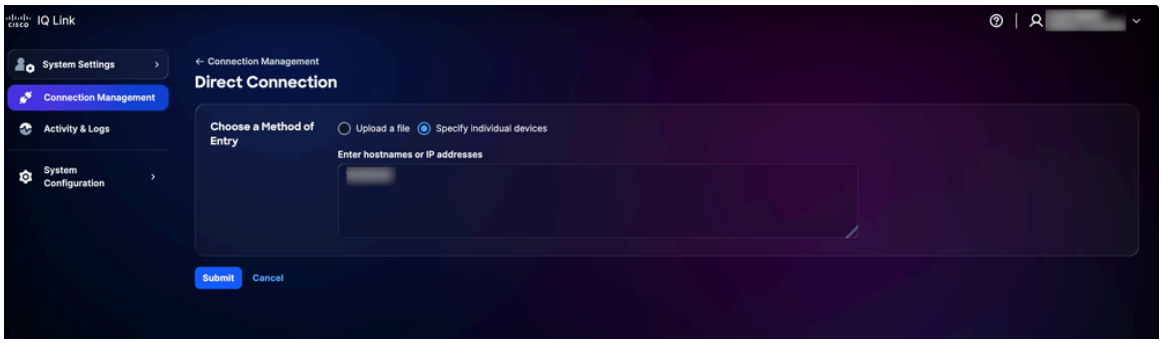
Datei hochladen

3. Klicken Sie auf die bevorzugte Option für Choose a Method of Entry (Eingabemethode auswählen) und senden Sie Ihre Geräte mit einer der folgenden Methoden:



Datei hochladen

- Datei hochladen: Klicken Sie auf die Datei, ziehen Sie sie und legen Sie sie ab, und klicken Sie auf Senden



Individuelle Geräte angeben

- Geben Sie einzelne Geräte an: Geben Sie einen Hostnamen, eine IP-Adresse oder eine kommagetrennte Liste mit Hostnamen und/oder IP-Adressen ein, und klicken Sie dann auf Senden

Nach erfolgreicher Einsendung werden Sie auf die Registerkarte Ressourcen weitergeleitet.

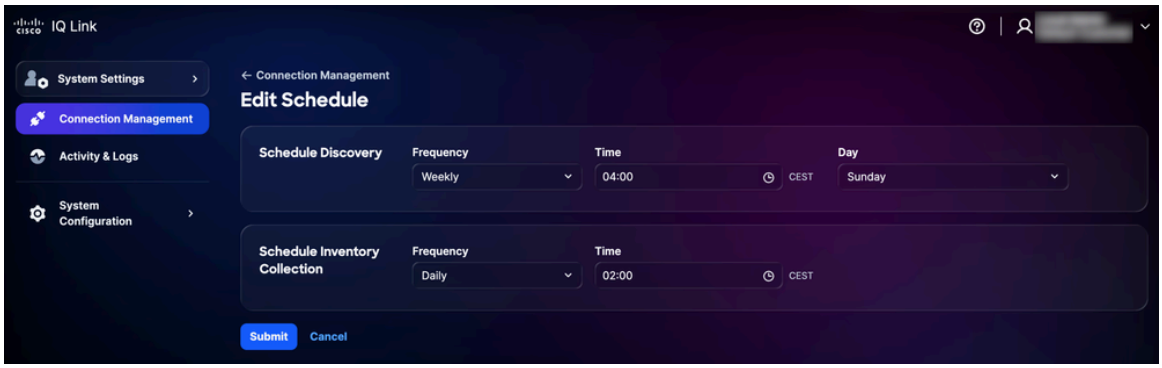
4. Planen einer Sammlung. Weitere Informationen finden Sie unter Planen.

Anmerkung: Cisco IQ Link ist mit einer automatisierten Einrichtung für die Zeitplanung vorkonfiguriert, und das System initiiert einen standardmäßigen automatisierten Zeitplan für die Erfassung. Es wird dringend empfohlen, den Zeitplan entsprechend den Anforderungen und Wartungsfenstern Ihres Unternehmens zu bearbeiten.

Terminplanung

Mit der Option "Scheduling" (Planung) können Sie festlegen, wann Cisco IQ Link die automatisierte Datenerfassung durchführt. So planen Sie die Erfassung:

1. Klicken Sie im Abschnitt "Planung" auf der Seite "Verbindungsverwaltung" auf Bearbeiten, um den Zeitplan zu ändern. Die Seite "Zeitplan bearbeiten" wird angezeigt.



Zeitplan bearbeiten

2. Wählen Sie im Abschnitt Schedule Discovery aus den Dropdown-Listen Ihre bevorzugte

Häufigkeit und Ihren gewünschten Tag aus, und geben Sie die gewünschte Startzeit ein.

3. Wählen Sie im Abschnitt "Schedule Inventory Collection" (Bestandserfassung planen) aus den Dropdown-Listen Ihre bevorzugte Häufigkeit aus, und geben Sie die gewünschte Startzeit ein.

4. Klicken Sie auf Senden.

Anmerkung: Bei Änderungen an Erkennungs- oder Erfassungszeitplänen dauert es 5-10 Minuten, bis diese innerhalb von Cisco IQ Link synchronisiert und korrekt wiedergegeben werden.

Banner

Administratoren können benutzerdefinierte Banner konfigurieren, die in der gesamten Anwendung angezeigt werden.

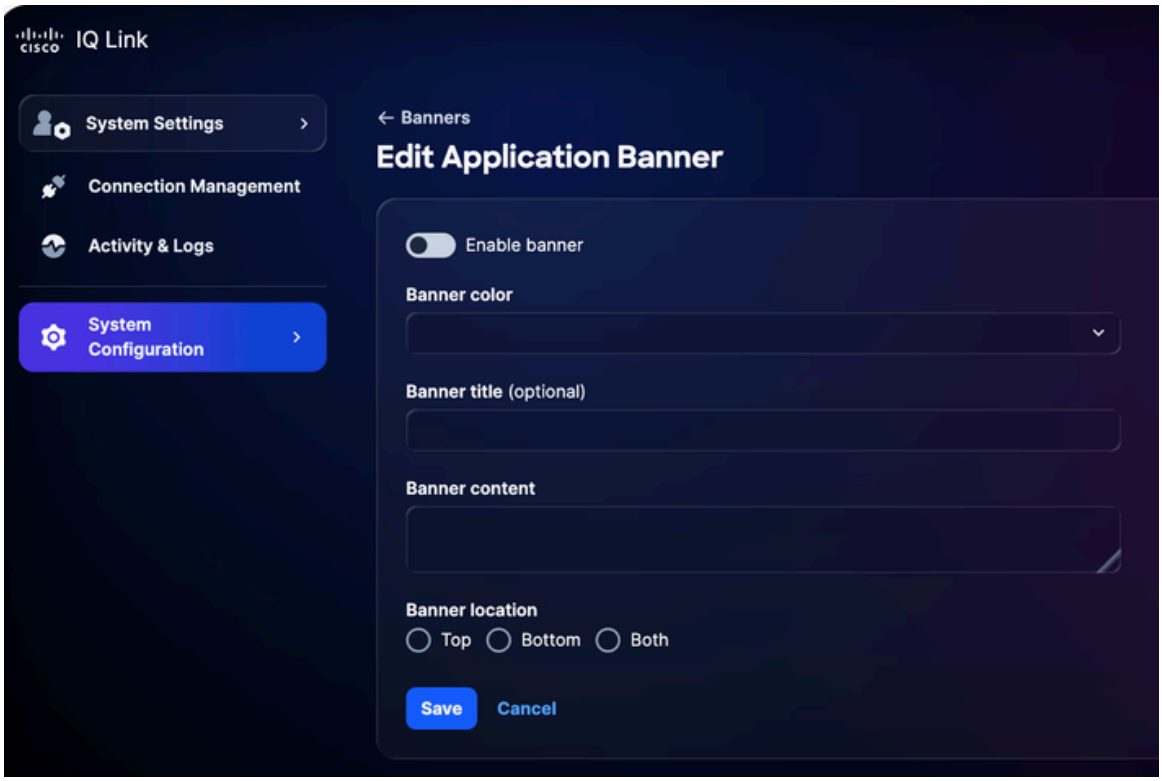
Banner konfigurieren

So konfigurieren Sie ein Banner:

1. Wählen Sie in den Systemeinstellungen die Option Systemkonfiguration > Banner aus. Die Seite Banner wird angezeigt.

Banner konfigurieren

2. Klicken Sie auf Configure (Konfigurieren). Die Seite Bewerbungsbanner bearbeiten wird angezeigt.



Anwendungsbanner bearbeiten

3. Klicken Sie auf den Umschalter, um den Banner zu aktivieren oder zu deaktivieren.
4. Wählen Sie eine Bannerfarbe aus.
5. Geben Sie den Bannertitel ein.
6. Geben Sie den Bannerinhalt ein.
7. Wählen Sie einen Bannerstandort aus.
8. Klicken Sie auf Speichern. Das Banner wird in der gesamten Anwendung angezeigt.

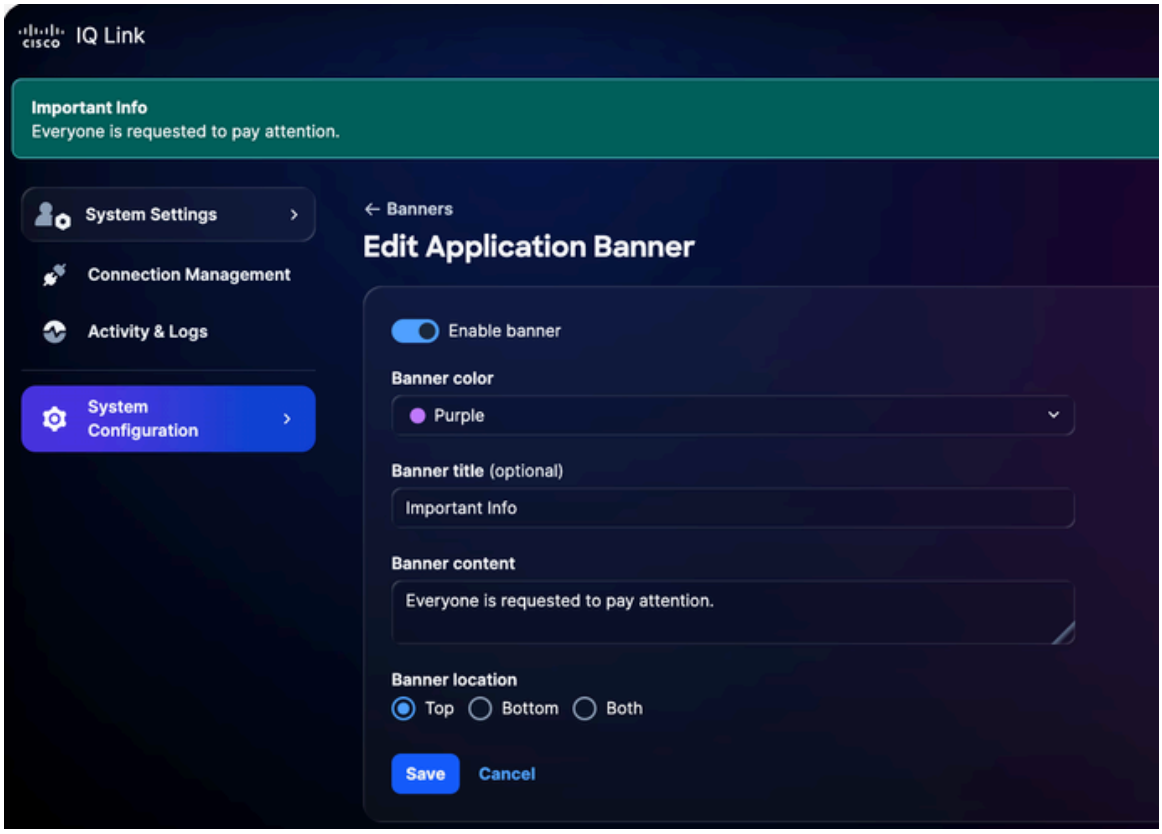
Banner bearbeiten

So bearbeiten Sie ein Banner:

1. Wählen Sie in den Systemeinstellungen die Option Systemkonfiguration > Banner aus. Die Seite Banner wird angezeigt.

Banner bearbeiten

2. Klicken Sie auf Bearbeiten. Die Seite Bewerbungsbanner bearbeiten wird angezeigt.



Anwendungsbanner bearbeiten

3. Bearbeiten Sie die gewünschten Details.
4. Klicken Sie auf den Umschalter, um den Banner zu aktivieren oder zu deaktivieren.
5. Klicken Sie auf Speichern.

Fehlerbehebung

Kunden können Diagnose- und Protokolldateien vom Cisco IQ-System sammeln und sicher auf einen SCP-Server übertragen. Diese Dateien können für das Support-Team freigegeben werden, wenn Probleme gemeldet werden, um wertvollen Kontext zu schaffen und die Fehlerbehebung zu

unterstützen.

So sammeln Sie Diagnose- und Protokolldateien:

1. Melden Sie sich bei Cisco IQ an.

Hauptmenü

2. Geben Sie im Cisco IQ-Hauptmenü "3" ein, und drücken Sie die Eingabetaste, um Systemdiagnose auszuwählen.

Systemdiagnose

3. Geben Sie die SCP-/SFTP-Serveradresse ein.
4. Geben Sie den SCP-/SFTP-Server-Port ein.
5. Geben Sie den SCP-/SFTP-Serverpfad ein.
6. Wählen Sie ein Protokoll aus.
7. Geben Sie den Benutzernamen ein.
8. Geben Sie das Kennwort ein.
9. Geben Sie "C" ein, und drücken Sie die Eingabetaste, um mit der Systemdiagnose fortzufahren.

Systemdiagnosevorgang CoSystemdiagnosevorgang abgeschlossen

Das System startet den Diagnoseprozess und führt die folgenden Aktionen aus:

- Überprüfen der Erreichbarkeit
- Erfassen von Systeminformationen
- Sammeln von Kubernetes-Informationen
- Protokolle werden gesammelt
- Vorbereiten des Systemdiagnosepakets

- Hochladen des Systemdiagnosepakets

Nach Abschluss des Vorgangs wird eine Bestätigungsmeldung mit dem generierten Paketnamen angezeigt.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.