Cisco IQ Link Operations Guide v1.2.0

Einleitung

Cisco IQ™ bietet Ihnen Erweiterungen und Funktionen zur Verbesserung der Bestandstransparenz, zur Bereitstellung intelligenterer Einblicke in Ihre Umgebungen und zur Optimierung des Fallmanagements. Darüber hinaus optimieren KI-Funktionen wie der KI-Assistent die Betriebsergebnisse und die Benutzererfahrung mit Cisco IQ, indem sie kontextbezogene Kenntnisse bereitstellen, die Sie in die Lage versetzen, proaktive, fundierte Entscheidungen zu treffen und Prozesse für Kundenengagement und -erfolg zu optimieren.

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

Kontoadministratoren müssen die folgenden Anmeldeinformationen verwenden, um sich bei Cisco IQ Link anzumelden:

- Standard-Benutzername: admin
- Default Password (Standardkennwort): Kennwort, das während der Installation von Cisco IQ Link festgelegt wird; Weitere Informationen finden Sie im Cisco IQ Link Getting Started Guide
- Standard-Kontenkontext: Standard-Kunde

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

Sicherheit für lokalen Administrator festlegen

Sie können Ihr Kennwort ändern und Sicherheitsfragen über das Menü Benutzerprofil auf der Startseite einrichten.

Sperreinstellungen

Die folgenden Kontosperrungseinstellungen können während der Bereitstellung konfiguriert werden:

- Lockout Status (Sperrstatus): Aktiviert oder deaktiviert die Kontosperrungsfunktion.
- Maximum Login Attempts (Maximale Anmeldeversuche): Legt die maximale Anzahl der aufeinander folgenden fehlgeschlagenen Anmeldeversuche fest, die vor dem Sperren eines Kontos zulässig sind (Standard: 3; Bereich: 0–10).
- Rolling Time Window: Definiert den Zeitraum für die Nachverfolgung fehlgeschlagener Versuche (Standard: 15 Minuten; Bereich: 0-60 Minuten).
- Duration (Dauer): Legt die Dauer fest, für die ein Konto gesperrt bleibt, nachdem die maximale Anzahl von Versuchen erreicht wurde (Standard: 30 Minuten; Bereich: 0-60 Minuten).

Anmerkung: Sie haben drei (3) Versuche, innerhalb von 15 Minuten das richtige Kennwort einzugeben. Wenn alle drei (3) Versuche nicht erfolgreich sind, wird Ihr Konto vorübergehend für 30 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.

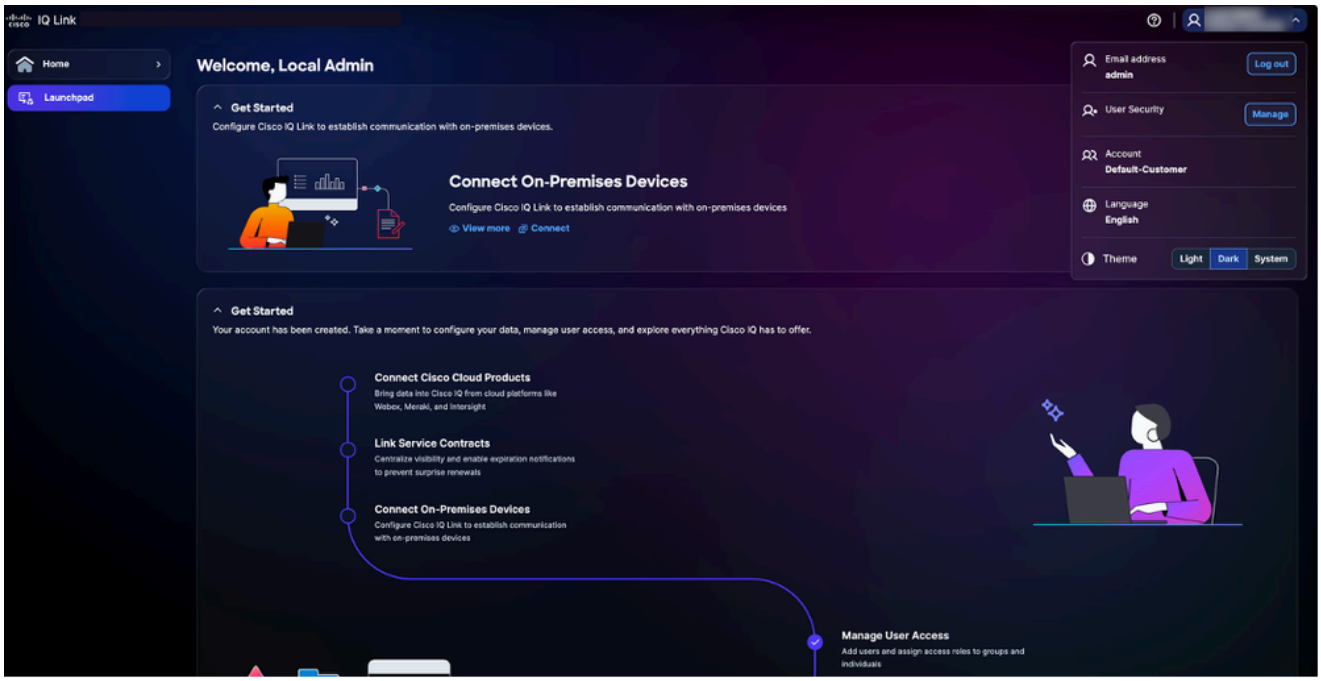
Nach 30 Minuten wird Ihr Konto automatisch entsperrt. Sie können dann versuchen, sich anzumelden oder Ihr Kennwort zurückzusetzen.

Einrichten von Sicherheitsfragen und -antworten

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

So richten Sie Sicherheitsfragen ein:

1. Klicken Sie auf der Startseite auf das Symbol Benutzerprofil. Das Dropdown-Menü wird geöffnet.

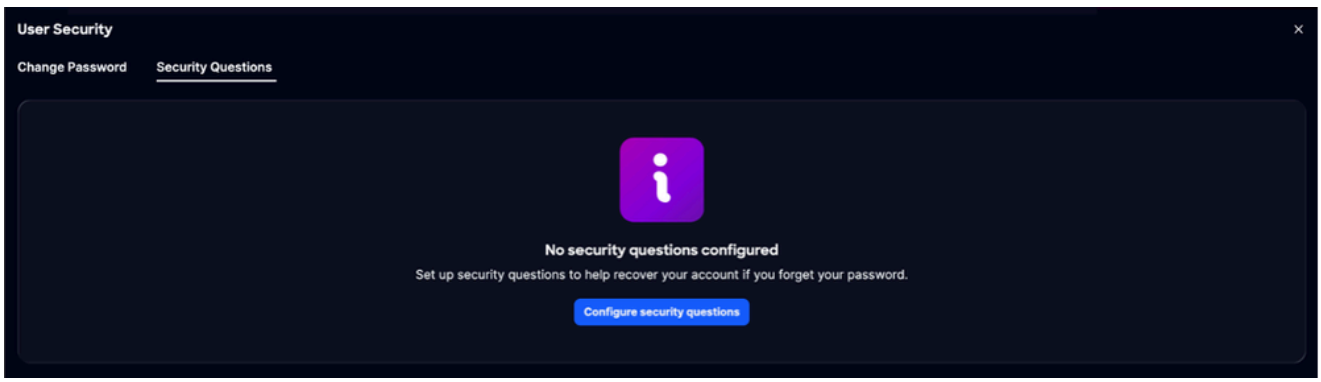


Menü "Benutzerprofil"

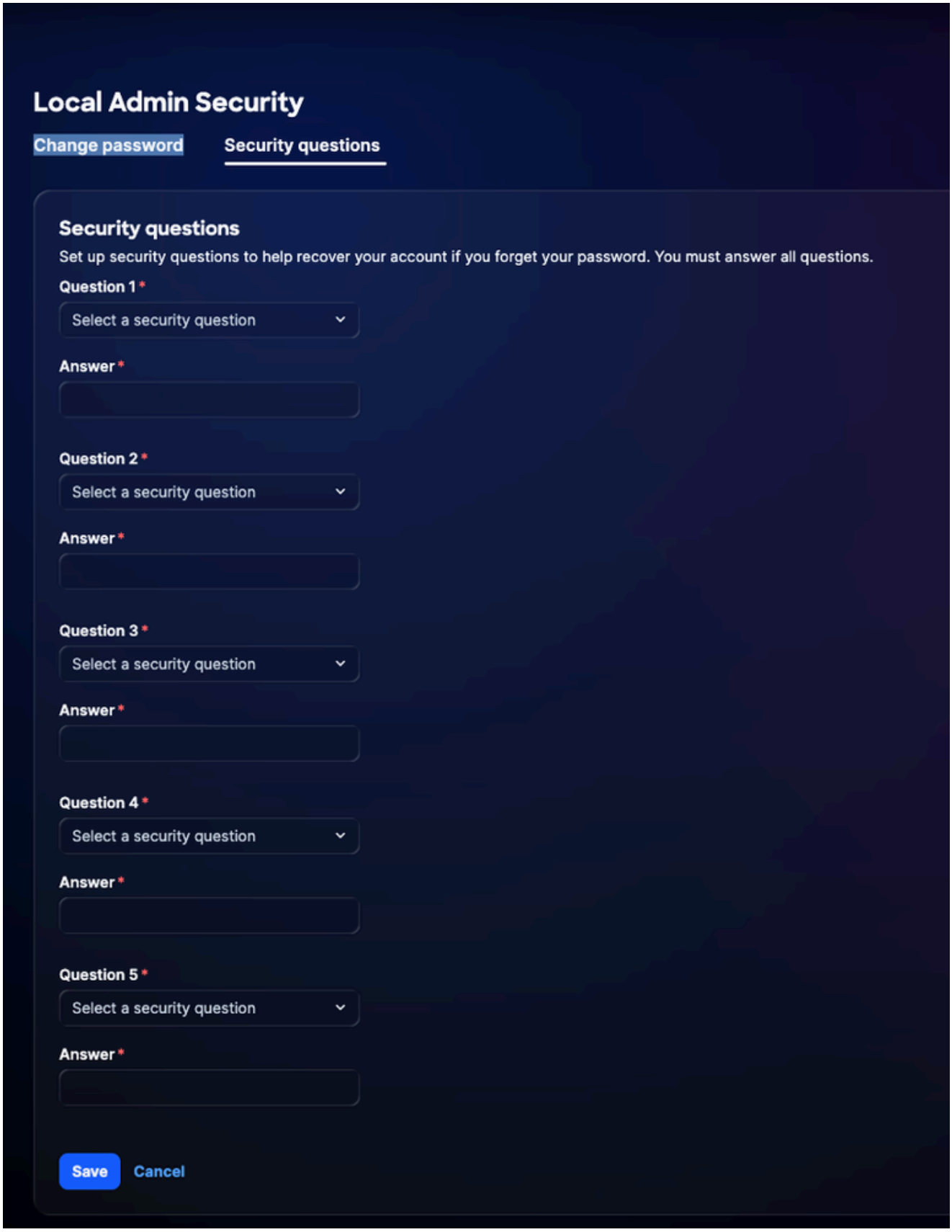
2. Klicken Sie unter Benutzersicherheit auf Verwalten. Die Seite User Security (Benutzersicherheit) wird angezeigt.

Kennwort ändern

3. Klicken Sie auf Sicherheitsfragen, um die Registerkarte zu öffnen.



4. Klicken Sie auf Sicherheitsfragen konfigurieren.



5. Wählen Sie aus den Dropdown-Listen fünf (5) Sicherheitsfragen aus.
6. Geben Sie Ihre Antwort für jede Frage ein.
7. Klicken Sie auf Speichern.

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

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

Kontoadministratoren und lokale Benutzer können Kennwörter für Cisco IQ verwalten.

Um die Sicherheit Ihres Kontos zu gewährleisten, werden die folgenden Kennwortrichtlinien durchgesetzt:

- Einschränkung der Wiederverwendung: Ihr neues Kennwort kann mit keinem Ihrer vorherigen fünf (5) Kennwörter übereinstimmen. Diese Richtlinie gilt für die Abläufe "Anmeldung", "Kennwort vergessen" und "Kennwort ändern".
- Zeichenvarianz: Wenn Sie Ihr Kennwort ändern, während Sie authentifiziert sind, müssen sich mindestens acht (8) Zeichen von Ihrem aktuellen Kennwort in Ihrem neuen Kennwort unterscheiden.
- Minimales Änderungsintervall: Standardmäßig müssen Sie 24 Stunden warten, bevor Sie Ihr Kennwort erneut ändern können. Wenn ein anderes Intervall konfiguriert wird, können Sie Ihr Kennwort erst nach Ablauf dieses Zeitraums aktualisieren.
- Kennwort läuft ab: Kennwörter laufen alle 60 Tage ab. Bei Ihrer ersten Anmeldung nach dem Ablaufdatum müssen Sie ein neues Kennwort festlegen, bevor Sie auf das System zugreifen können. (Bei Konfiguration auf 0 ist die Kennwortablaufzeit deaktiviert.)

Voraussetzungen

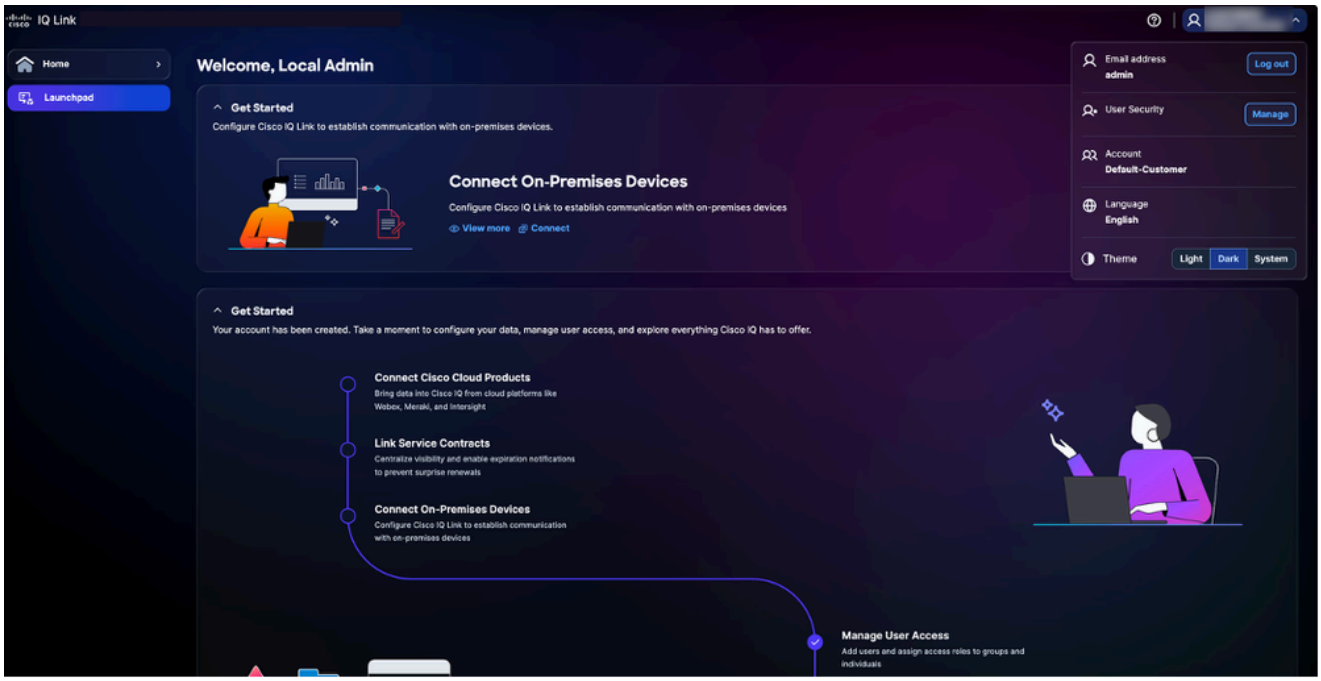
Um Kennwörter zu verwalten, müssen die folgenden Bedingungen erfüllt sein:

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

Kennwörter ändern

So ändern Sie ein Kennwort:

1. Klicken Sie auf der Startseite auf das Symbol Benutzerprofil. Das Dropdown-Menü wird geöffnet.



Menü "Benutzerprofil"

2. Klicken Sie unter Benutzersicherheit auf Verwalten. Die Seite User Security (Benutzersicherheit) wird angezeigt.

Kennwort ändern

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

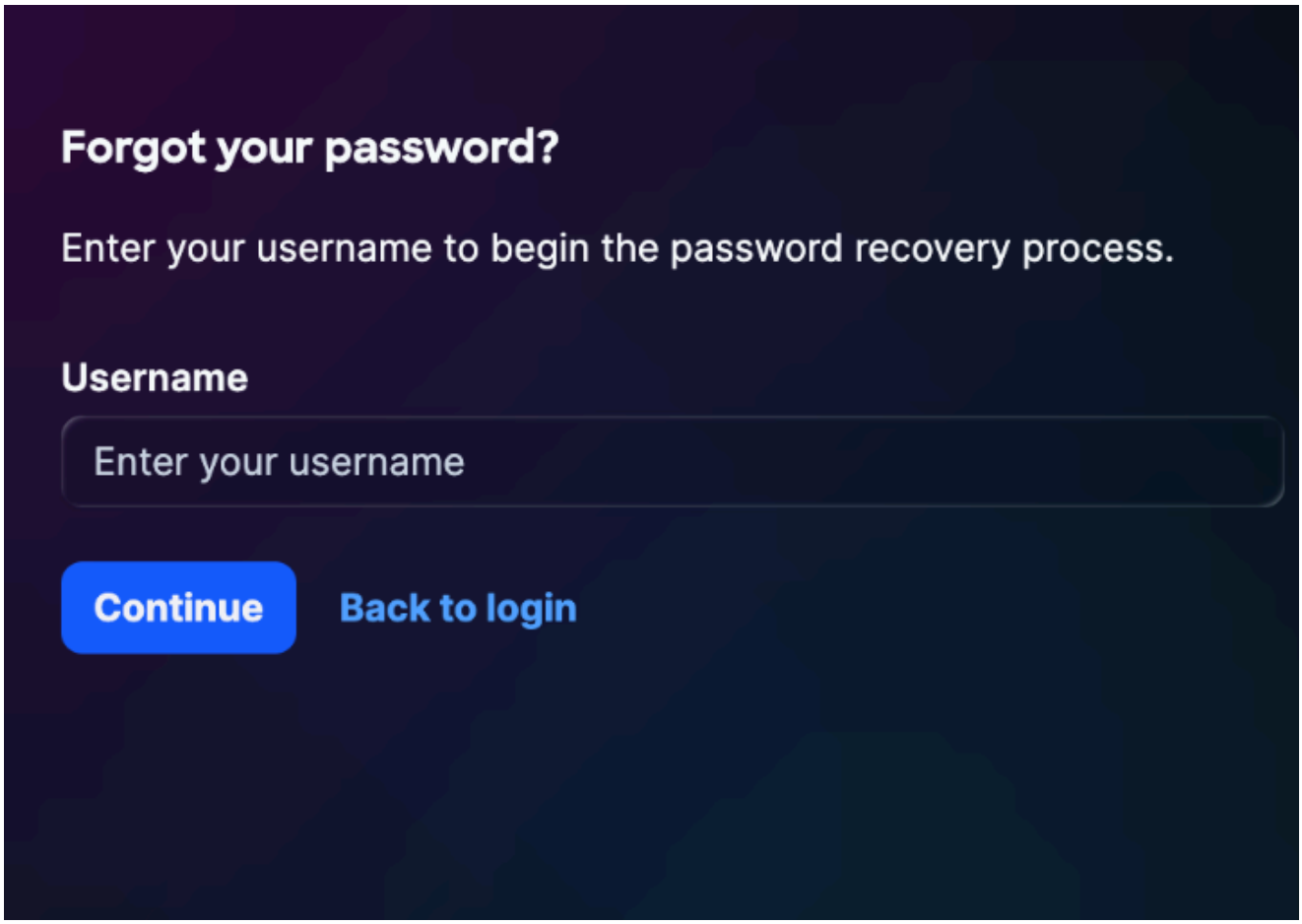
Das Kennwort wird im Cisco IQ-System aktualisiert, einschließlich des virtuellen Systems Cisco IQ.

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.

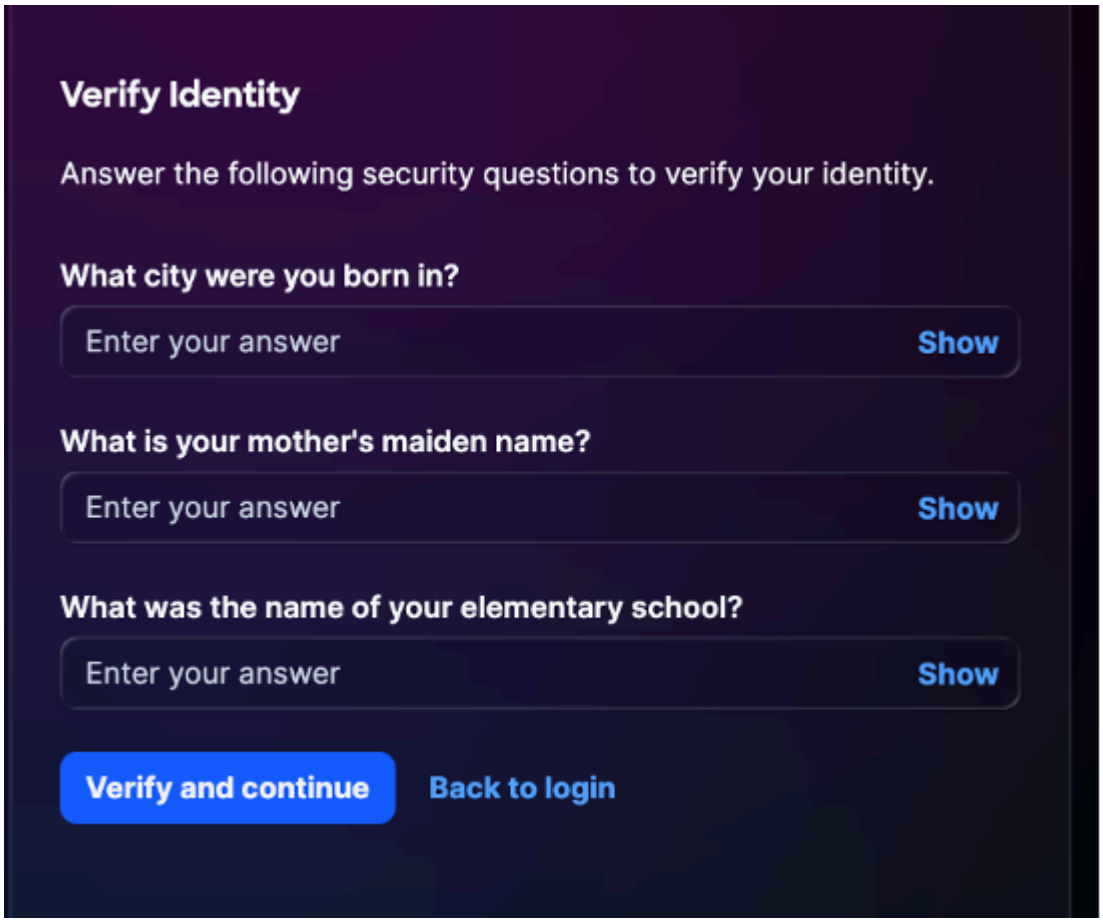
So setzen Sie ein vergessenes Kennwort zurück:

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.



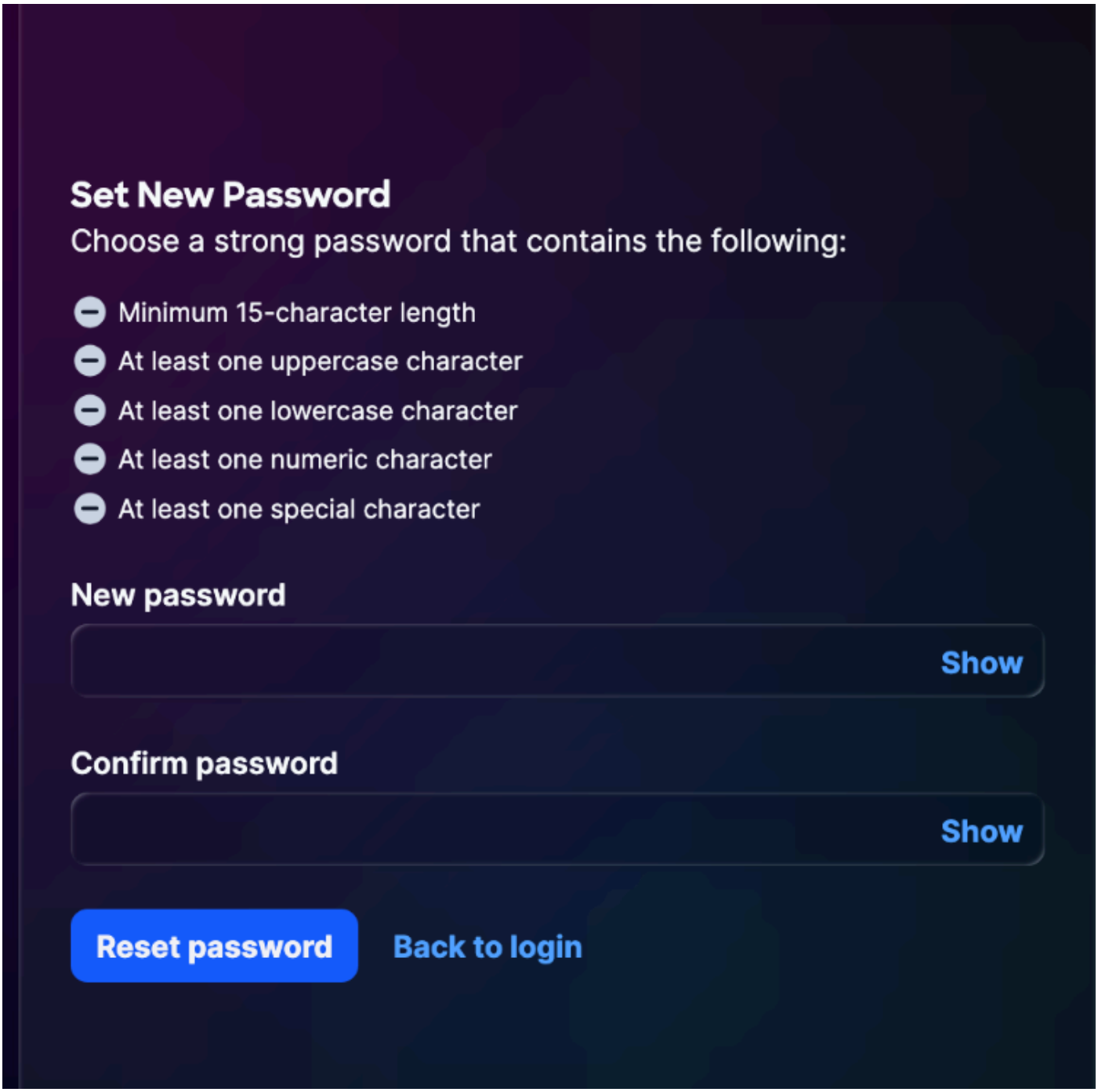
Identität überprüfen

✎ 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

Sie haben drei (3) Versuche, die Sicherheitsfragen innerhalb von 15 Minuten richtig zu beantworten. Wenn alle drei (3) Versuche nicht erfolgreich sind, wird Ihr Konto vorübergehend für 30 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 30 Minuten wird Ihr Konto automatisch entsperrt. Sie können dann versuchen, sich anzumelden oder Ihr Kennwort zurückzusetzen.

7. Geben Sie das neue Kennwort ein.

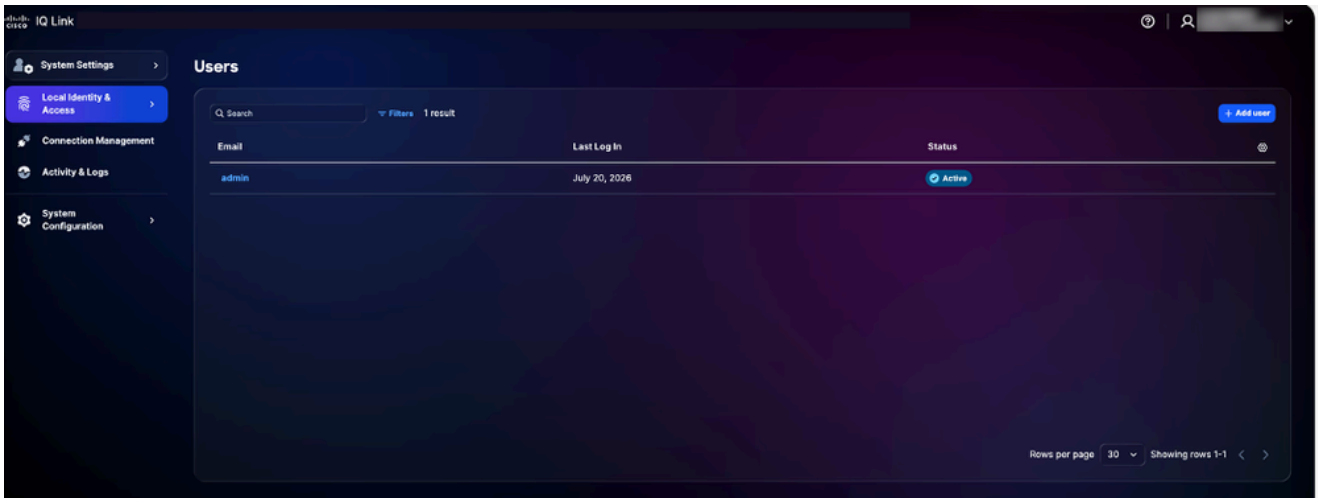
8. Geben Sie das Kennwort erneut ein, um es zu bestätigen.

9. Klicken Sie auf Senden.

Hinzufügen von lokalen Benutzern

Kontoadministratoren können Benutzer zum Cisco IQ-Konto hinzufügen. So fügen Sie einen neuen Benutzer hinzu

1. Navigieren Sie zu Systemeinstellungen > Lokale Identität und Zugriff > Benutzer. Die Seite Benutzer wird angezeigt. Es listet alle vorhandenen lokalen Benutzer zusammen mit ihrem Status auf.

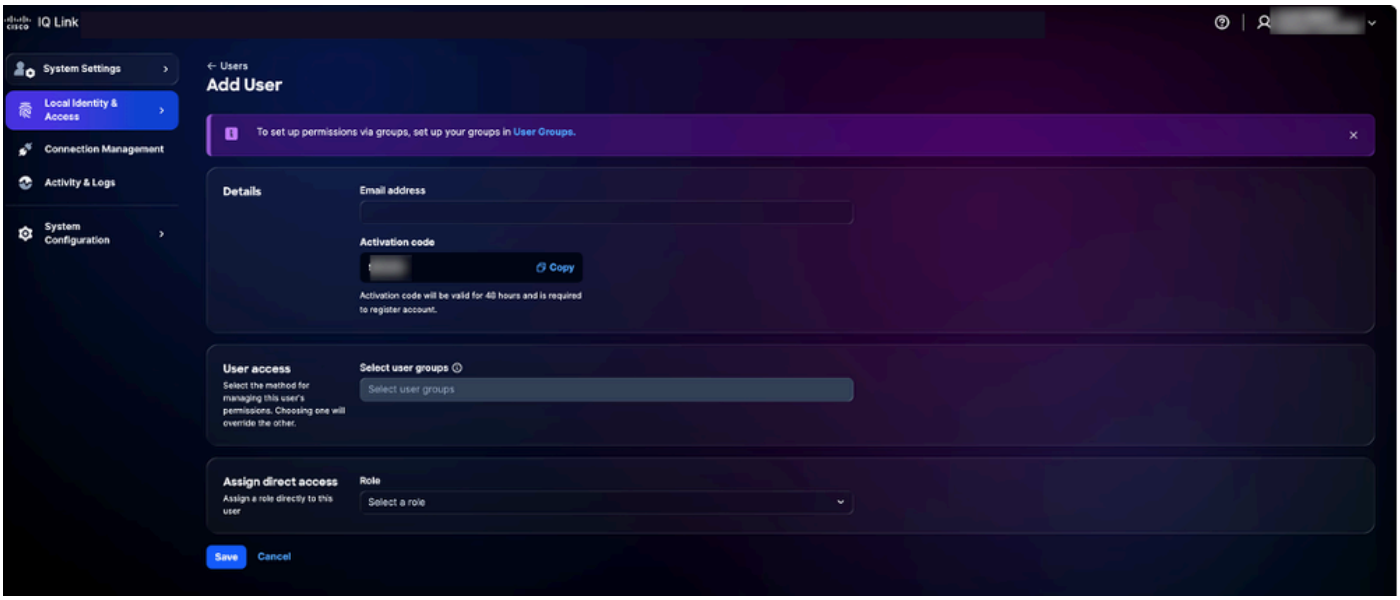


Seite Benutzer

Anmerkung: Das Symbol More Options (Mehr Optionen) wird für Kontoadministratoren nicht angezeigt (wie in der Abbildung oben gezeigt).

---

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



Benutzer hinzufügen

3. Geben Sie die E-Mail-Adresse ein.

4. Geben Sie den Aktivierungscode ein.

Anmerkung: Der Aktivierungscode wird standardmäßig angezeigt. Geben Sie die Informationen für den Benutzer frei, wenn Sie die Registrierung abschließen möchten.

---

5. Wählen Sie im Feld Benutzerzugriff die Benutzergruppe aus der Dropdown-Liste Benutzergruppen auswählen.

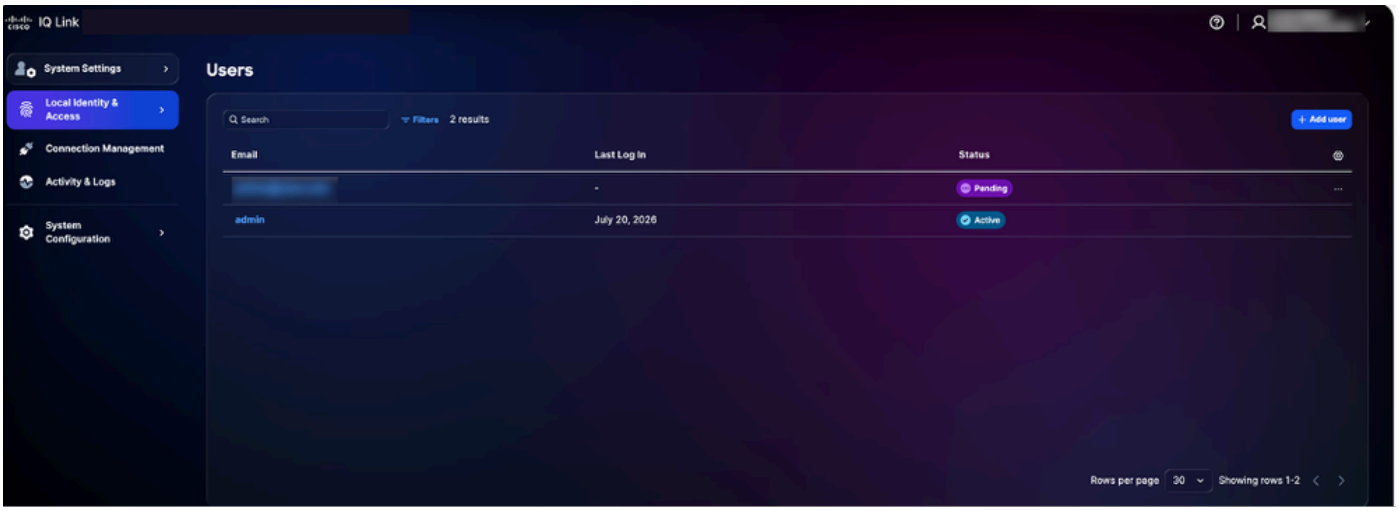
Anmerkung: Benutzer erben den Zugriff der ausgewählten Gruppe.

---

6. Wählen Sie unter Direktzugriff zuweisen in der Dropdown-Liste Rolle die Option Rolle aus. Es sind zwei (2) Rollen verfügbar:

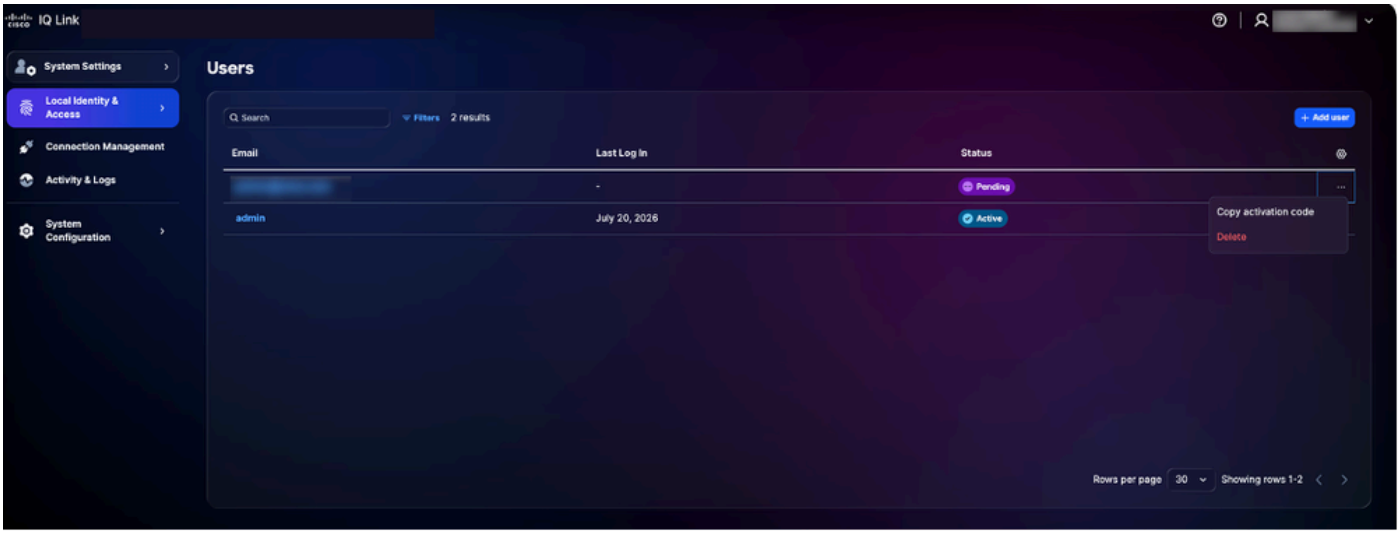
- Viewer: Anzeigen und Zugreifen auf Anwendungen
- Administrator: Zugriff auf Anwendungen und Verwaltung von Systemeinstellungen, mit Ausnahme von Systemverwaltung und IDP

7. Klicken Sie auf Speichern. Der neue Benutzer wird erstellt und in der Benutzerliste im Status Ausstehend angezeigt. Pending (Ausstehend): Der Benutzer hat die Selbstaktivierung noch nicht abgeschlossen.



Neu hinzugefügter Benutzer

8. Suchen Sie den neu erstellten Benutzer in der Liste, und stellen Sie sicher, dass in der Spalte Status die Meldung Pending (Ausstehend) angezeigt wird.



Aktivierungscode kopieren

9. Klicken Sie auf das Symbol Weitere Optionen > Aktivierungscode kopieren neben dem neu erstellten Benutzer. Der Aktivierungscode wird in die Zwischenablage kopiert.

10. Geben Sie diesen Code sicher für den Benutzer frei (z. B. über einen sicheren internen Kanal). Der Aktivierungscode ist nur einmal verwendbar und für die vollständige Registrierung erforderlich.

Anmerkung: Geben Sie den Aktivierungscode nicht über unsichere Kanäle frei. Wenn der Code verloren geht oder kompromittiert wurde, verwenden Sie das Menü-Symbol, um einen neuen Aktivierungscode zu generieren, der den vorherigen ungültig macht.

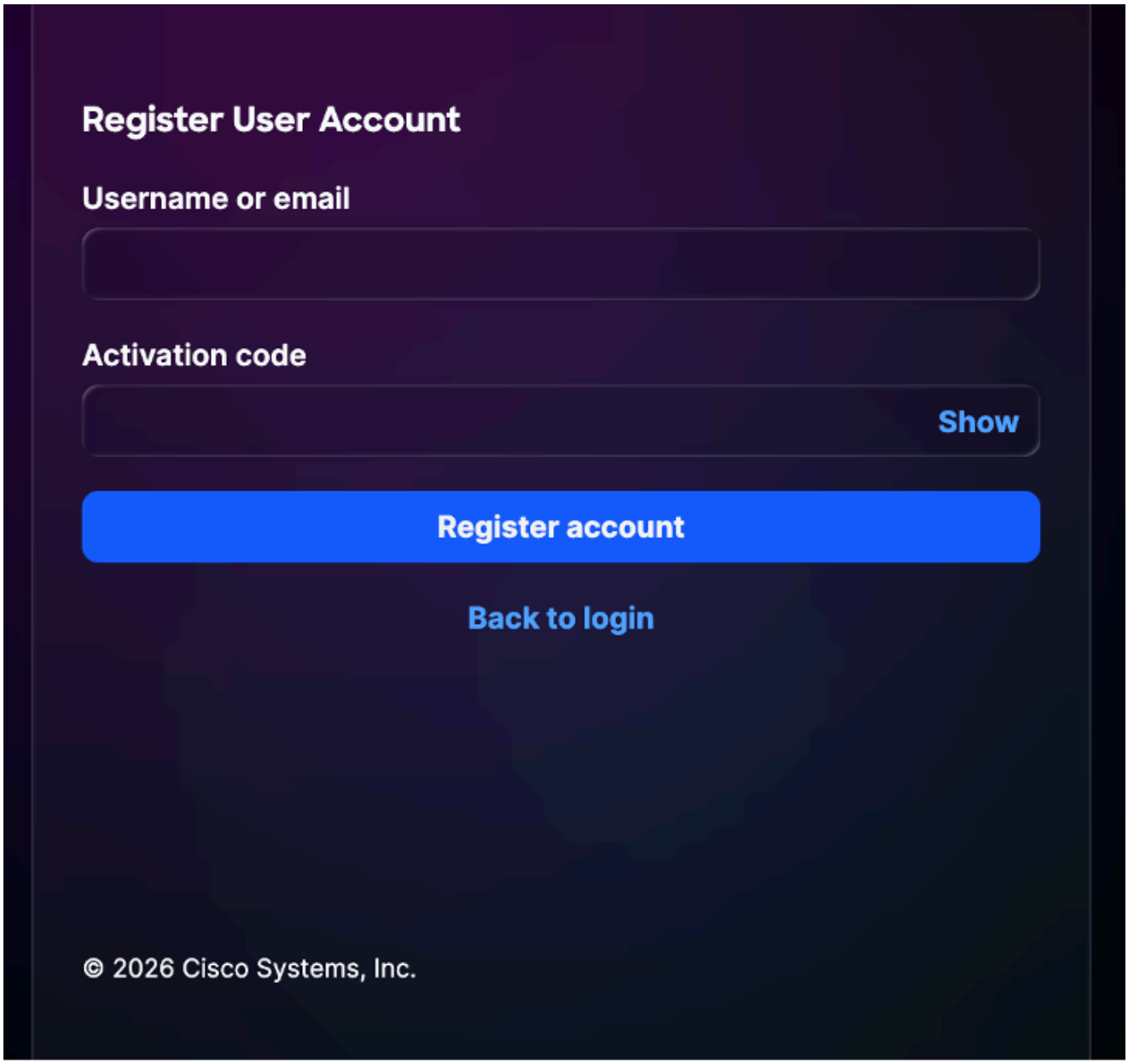
Hinweis: Aktivierungscodes sind 48 Stunden gültig. Wenn Ihr Code abläuft, wenden Sie sich an Ihren Kontoadministrator, um einen neuen Code anzufordern.

11. Um sich abzumelden, klicken Sie auf das Symbol User in der rechten oberen Ecke, und wählen Sie Logout (Abmelden). Sie kehren zur Cisco IQ-Anmeldeseite zurück.

Neues Benutzerkonto wird registriert

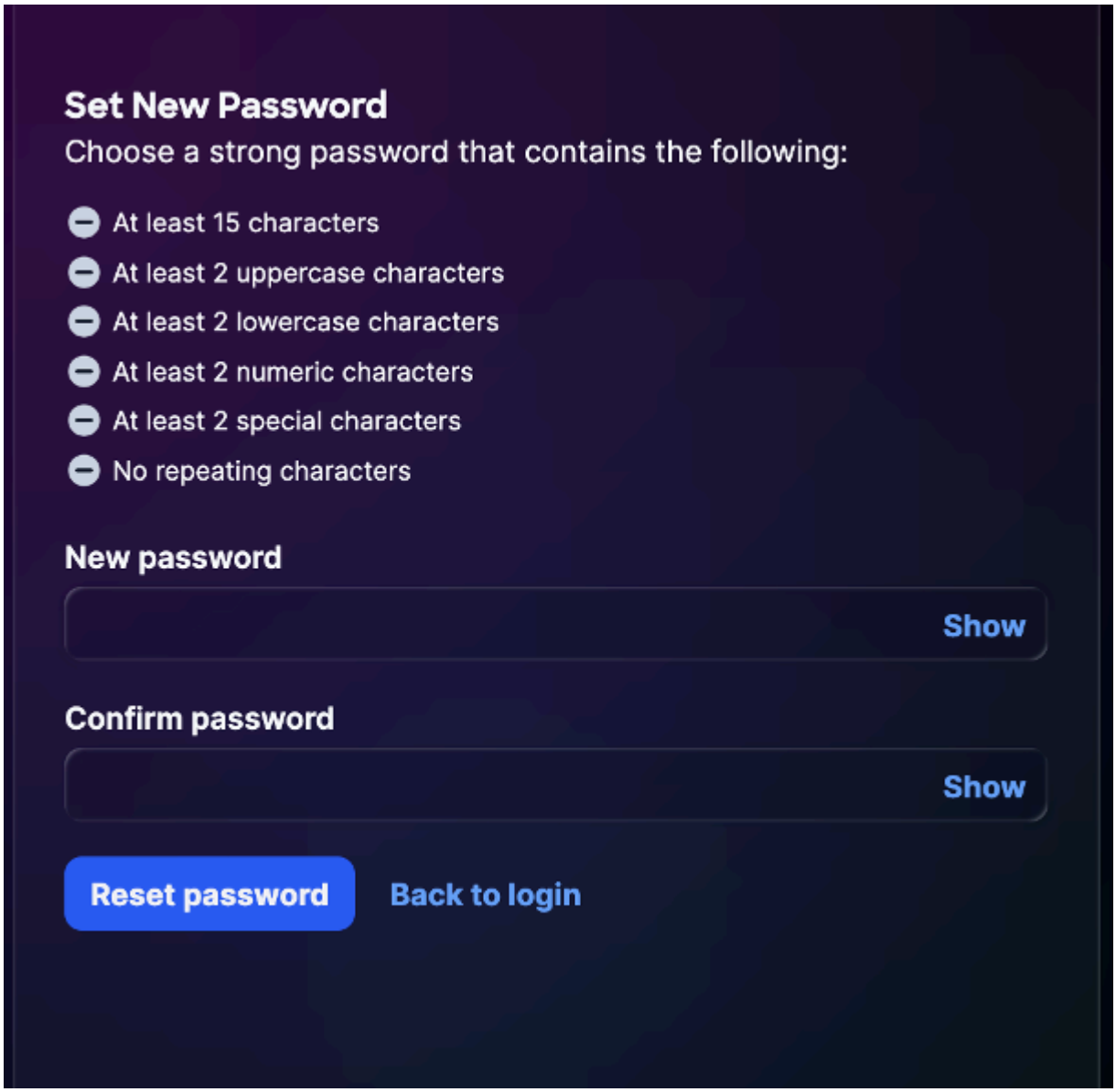
So registrieren Sie das neue Benutzerkonto:

1. Klicken Sie auf der Anmeldeseite auf den Link Neues Benutzerkonto registrieren.



Neues Benutzerkonto

2. Geben Sie den Benutzernamen oder die E-Mail-Adresse ein, die bei der Erstellung des Benutzers verwendet wurde (z. B. user1@abc.com).
3. Geben Sie den vom Kontoadministrator freigegebenen Aktivierungscode ein.
4. Klicken Sie auf Konto registrieren. Das Fenster Neues Kennwort festlegen wird angezeigt.



Kennwort für neues Benutzerkonto

5. Geben Sie ein neues Kennwort ein.
6. Geben Sie das Kennwort unter Kennwort bestätigen erneut ein.
7. Bei der ersten erfolgreichen Anmeldung wird der Benutzer aufgefordert, fünf (5) Sicherheitsfragen zu konfigurieren (weitere Informationen finden Sie unter Sicherheitsfragen und -antworten einrichten).

Verwalten lokaler Benutzergruppen

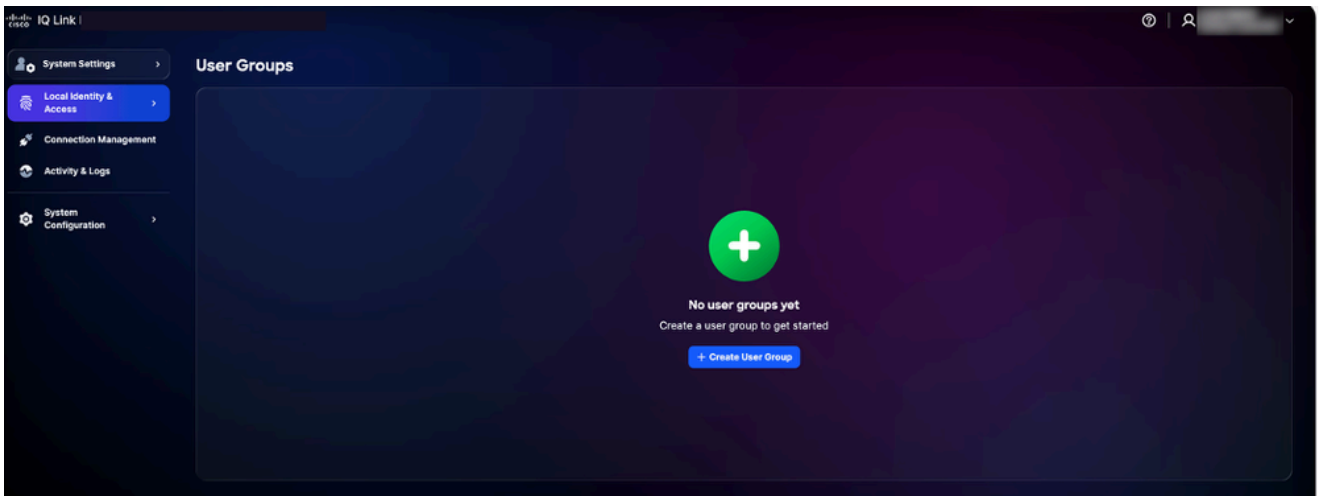
Benutzergruppen ermöglichen es Kontoadministratoren, Rollen für mehrere lokale Benutzer gemeinsam zu verwalten. Anstatt jedem Benutzer einzeln eine Rolle zuzuweisen, kann ein Kontoadministrator eine Gruppe erstellen, eine Rolle und eine Gruppe von Benutzern hinzufügen und die Rolle oder die Mitgliedschaft an einem Ort aktualisieren. Die gesamte Benutzergruppenverwaltung erfolgt über die Seite Lokale Identität und Zugriff.

Anmerkung: Nur ein Kontoadministrator kann Benutzergruppen erstellen, bearbeiten oder löschen. Gruppen bestehen aus vorhandenen lokalen Benutzern; Benutzer müssen erstellt werden, bevor sie einer Gruppe hinzugefügt werden können.

Erstellen einer Benutzergruppe

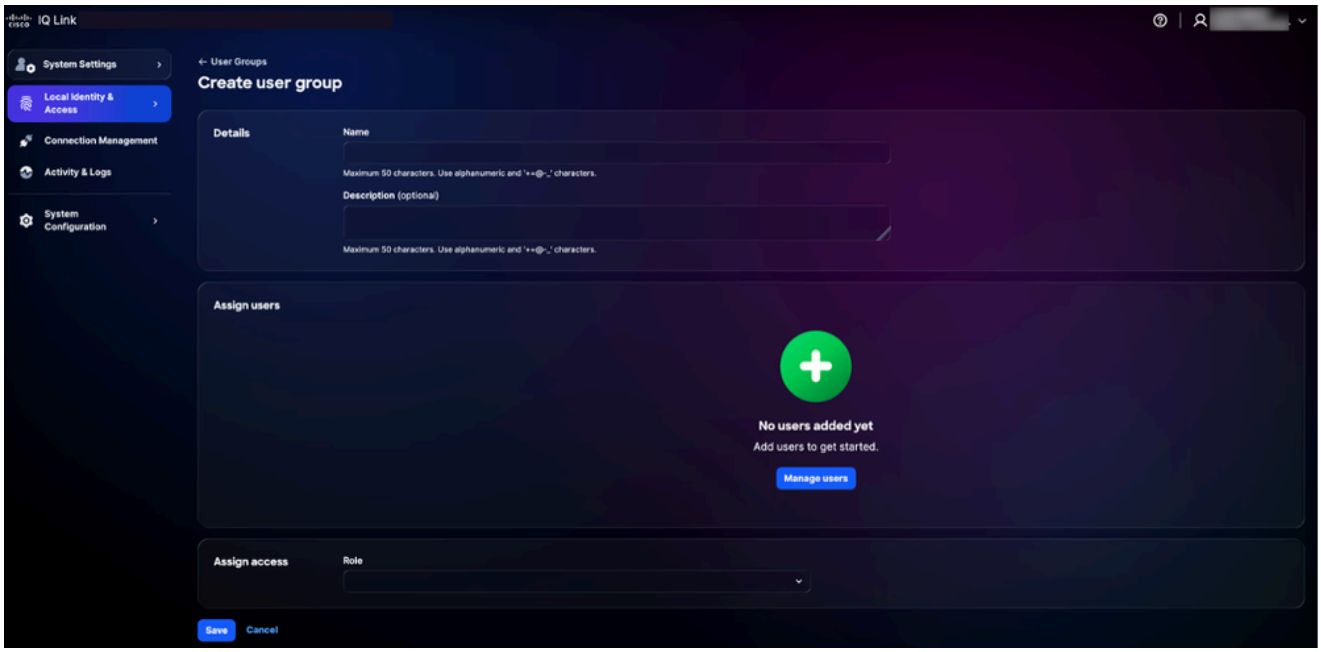
Erstellen einer Benutzergruppe:

1. Wählen Sie in den Systemeinstellungen die Option Lokale Identität und lokaler Zugriff > Benutzergruppen aus. Die Seite Benutzergruppen wird angezeigt.



Benutzergruppen

2. Klicken Sie auf Benutzergruppe erstellen. Die Seite Benutzergruppe erstellen wird angezeigt.



Benutzergruppe erstellen

3. Füllen Sie die folgenden Abschnitte aus:

- Details
  - Name: Geben Sie einen eindeutigen Namen für die Gruppe ein (z. B. Schreibgeschützte Operatoren).
  - Beschreibung (optional): Eine kurze Beschreibung der Gruppe (maximal 50 Zeichen; alphanumerische Zeichen und + = @ - _ Zeichen sind zulässig)

- Benutzer zuweisen

  Suchen Sie nach einem oder mehreren vorhandenen lokalen Benutzern, die der Gruppe hinzugefügt werden sollen, und wählen Sie sie aus.

  Anmerkung: Um noch nicht aufgelistete Benutzer hinzuzufügen, klicken Sie auf Benutzer verwalten.

- Zugriff zuweisen

  - Rolle: Wählen Sie die Systemrolle aus, die allen Mitgliedern dieser Gruppe zugewiesen werden soll. Folgende Rollen sind verfügbar:

    - Viewer: Anzeigen von Anwendungen und Zugriff auf diese (schreibgeschützt)

    - Administrator: Zugriff auf Anwendungen und Verwaltung von Systemeinstellungen

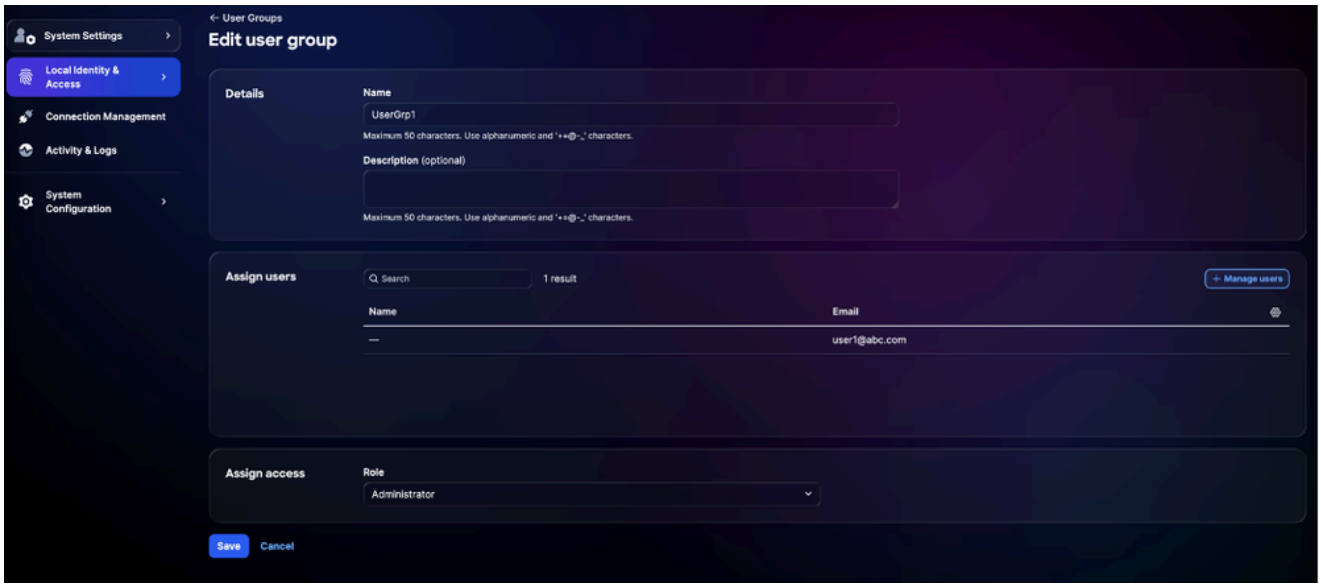
4. Klicken Sie auf Speichern.

Die neue Benutzergruppe wird in der Liste Benutzergruppen zusammen mit der zugewiesenen Rolle und der Mitgliederanzahl angezeigt.

Bearbeiten einer Benutzergruppe

So bearbeiten Sie eine Benutzergruppe:

1. Suchen Sie in der Liste Benutzergruppen die Gruppe, die Sie ändern möchten.
2. Klicken Sie auf das Symbol More (Mehr) neben der Gruppe, und wählen Sie Edit (Bearbeiten). Die Seite Benutzergruppe bearbeiten wird angezeigt.



Benutzergruppe bearbeiten

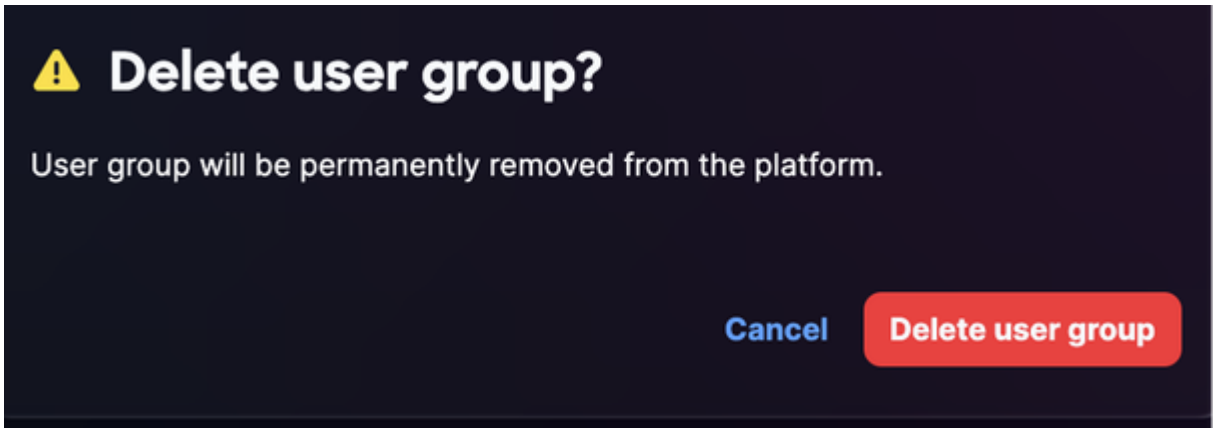
3. Nehmen Sie die gewünschten Änderungen vor.
4. Klicken Sie auf Speichern.

Die aktualisierte Gruppe wird in der Liste Benutzergruppen angezeigt. Die neue Rolle tritt für alle Mitglieder der Gruppe in Kraft.

Löschen einer Benutzergruppe

So löschen Sie eine Benutzergruppe:

1. Suchen Sie in der Liste Benutzergruppen nach der Gruppe, die Sie löschen möchten.
2. Klicken Sie auf das Symbol Weitere Optionen neben der Gruppe, und wählen Sie Löschen aus.



Benutzergruppe löschen

3. Bestätigen Sie den Löschvorgang, wenn Sie dazu aufgefordert werden.

Die Gruppe wird aus der Liste Benutzergruppen entfernt.

Anmerkung: Beim Löschen einer Benutzergruppe wird die gruppenbasierte Rollenzuweisung von allen Mitgliedern entfernt. Die einzelnen Benutzerkonten werden nicht gelöscht.

Identitätsanbieter konfigurieren

Nach der Anmeldung bei Cisco IQ Link können Kontoadministratoren verschiedene Einstellungen konfigurieren. Kontoadministratoren 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 Account Administrator-Zugriff 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.
Tabelle 1: Cisco IQ Link-Attribute

Feld	Wert
Anwendungsname	<Anwendungsname>
Umwelt	ESP-Geschäftsanwendung
Anwendungsbesitzergruppen	Eigentümer der IDP-Einstellungen
Team-Mailer	Mailer für das Team
Zielgruppe	Nicht-Mitarbeiter
Onboarding-Kategorie	Wählen Sie "New Onboarding".

Tabelle 2: SAML-Konfigurationsparameter

Parameter	Konfiguration	Beispiel
Zielgruppe (Element-ID)	Vollqualifizierter Domänenname (FQDN)	mymanagementhost.mydomain.com
URL für einmalige Anmeldung	SAML Assertion Consumer Service (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 Sie die SLO-Einstellungen (Single Logout) in der Anwendung.

Tabelle 3: 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

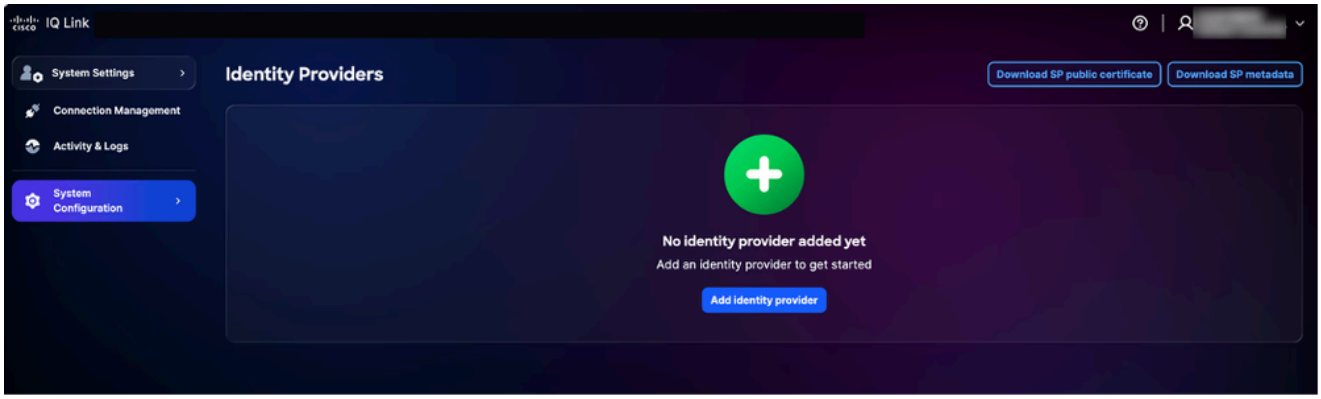
5. Klicken Sie auf das Download-Symbol, um die "SP Metadata"-Datei herunterzuladen.

6. Stellen Sie die Anwendung nach Bedarf des Anbieters bereit, oder erstellen Sie sie.

Hinzufügen von Okta IDP

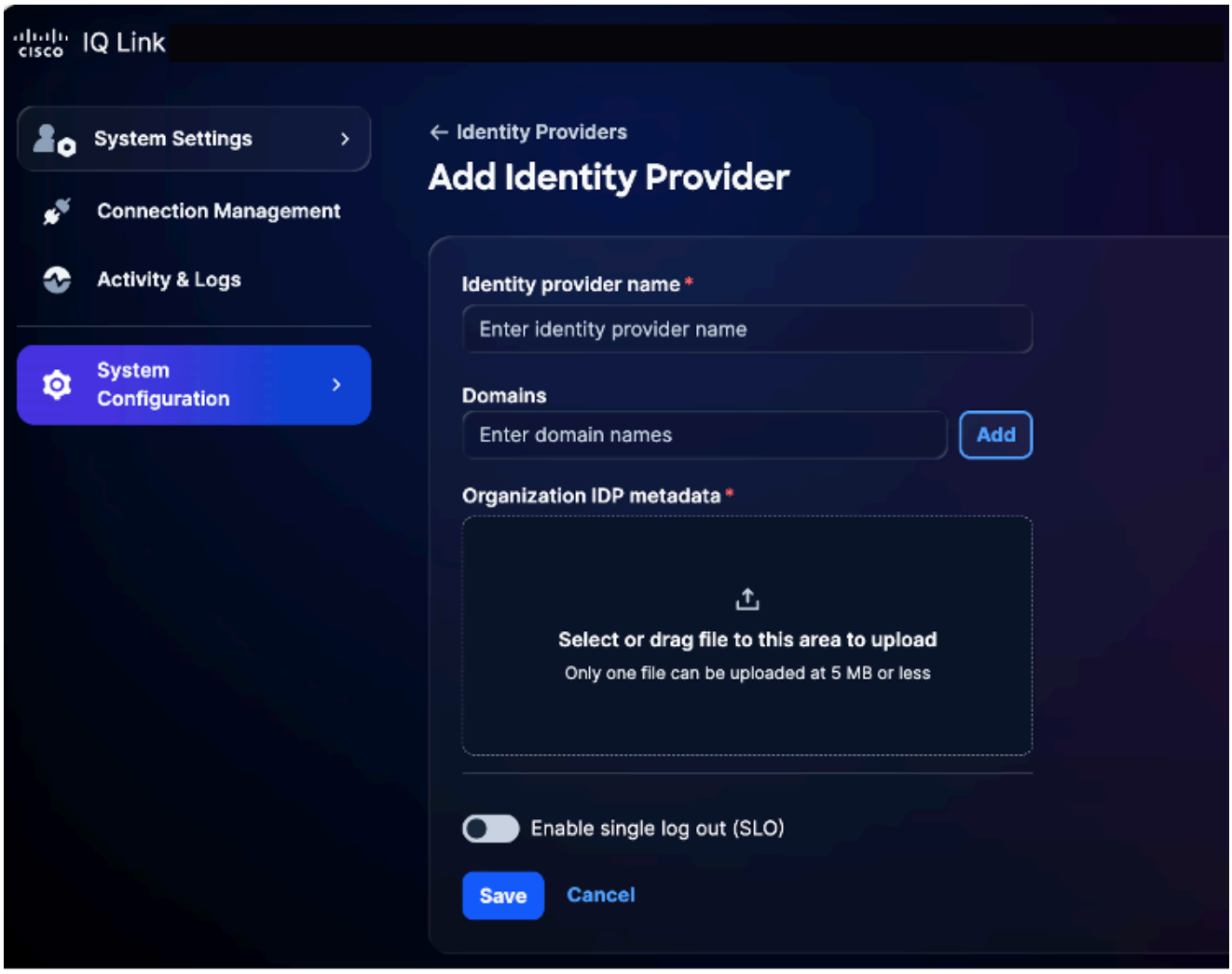
So fügen Sie einen IDP in Cisco IQ hinzu:

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.

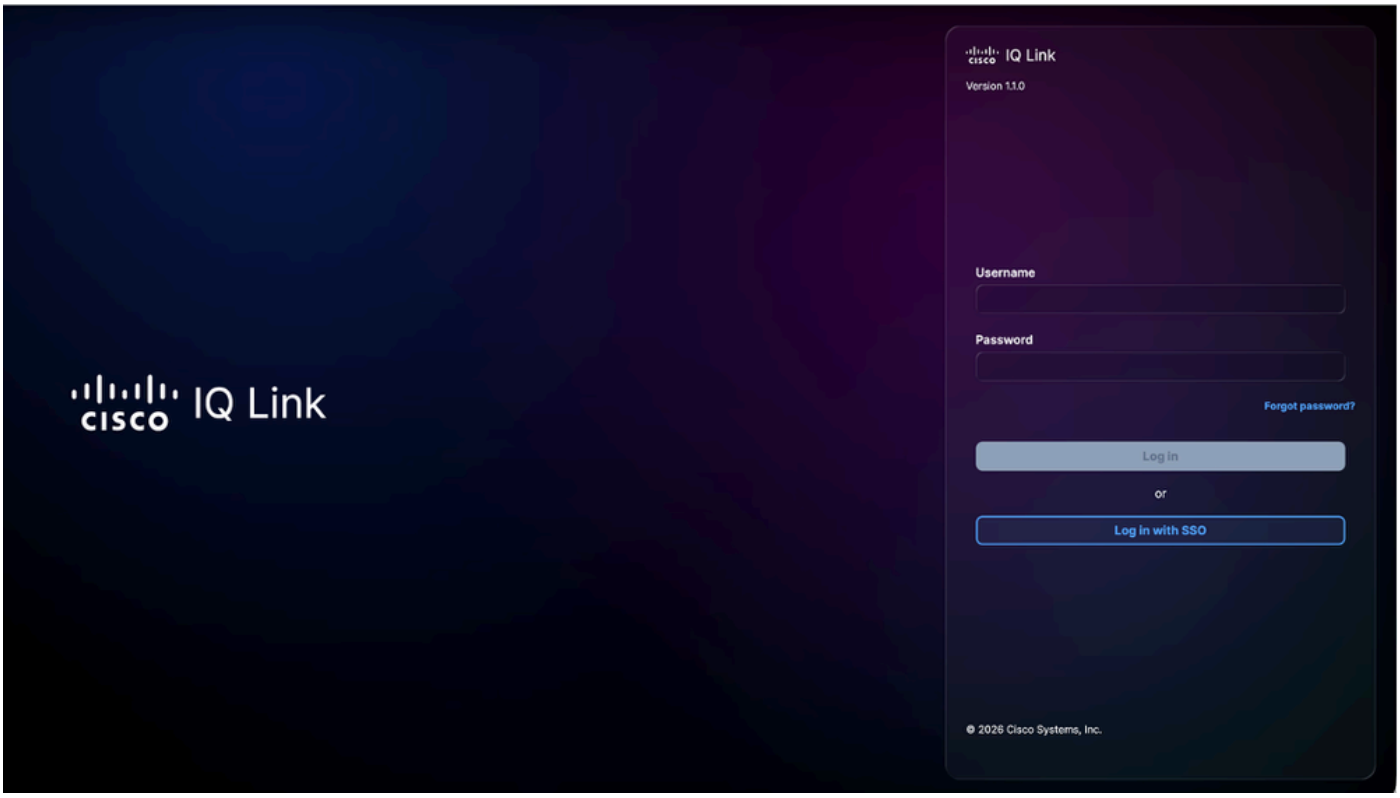
4. Klicken Sie auf Hinzufügen, um dem Feld "Domains" einen für Cisco IQ Link konfigurierten Domänennamen hinzuzufügen.

5. Ziehen Sie die SAML-Metadatendatei, die Sie von der IDP-Anwendung erhalten haben, per Drag-and-Drop in das Feld Organization IDP-Metadaten. Diese Datei enthält Zertifikatdetails und Details zur Service Provider (SP)-Entität.

6. (Optional) Aktivieren Sie die Umschaltfläche Single Logout aktivieren. Sie können das SLO auch später aktivieren.

7. Klicken Sie auf Speichern.

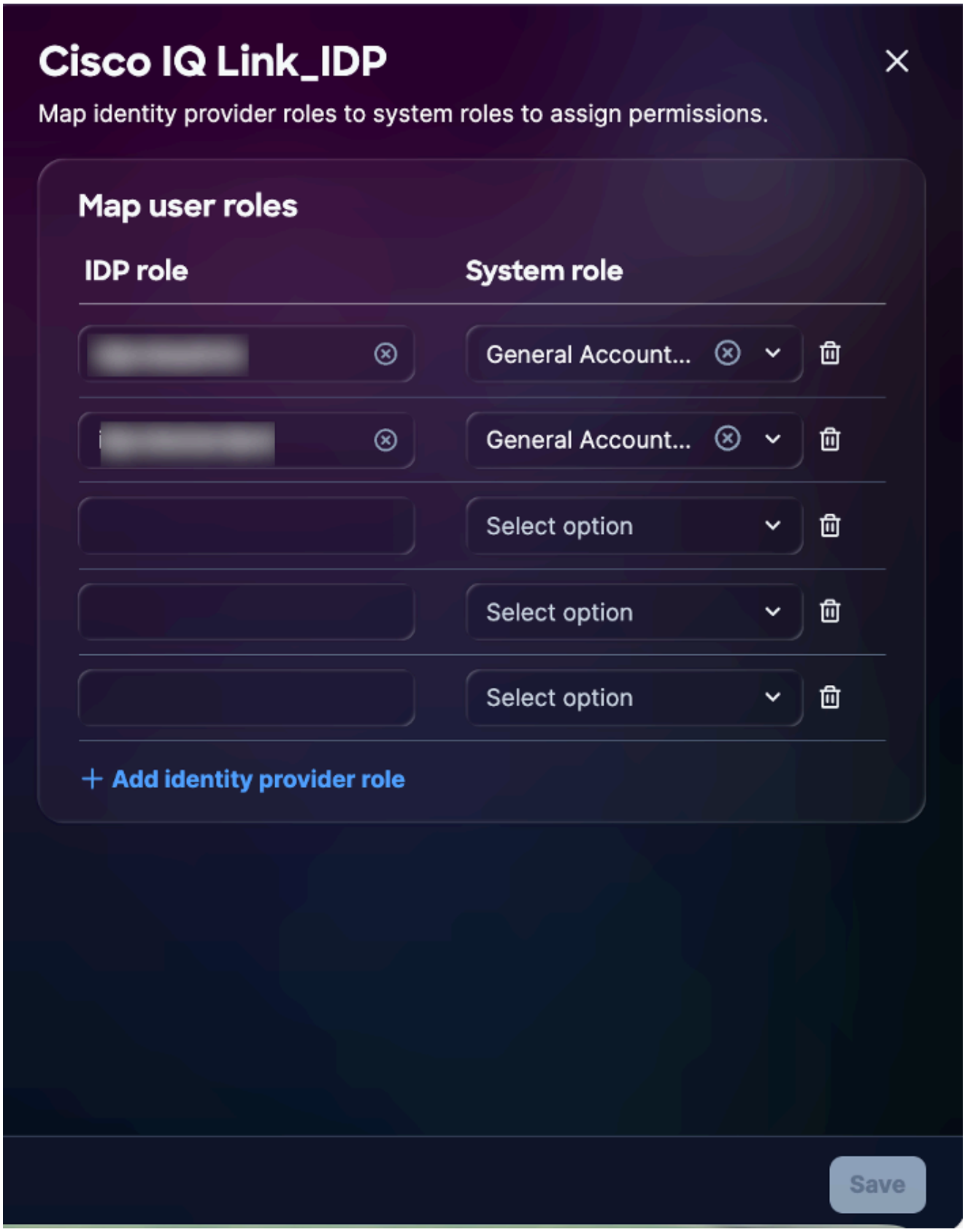
Nach der Konfiguration wird auf der Anmeldeseite eine Option zur Anmeldung mit SSO (über IDP) angezeigt.



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

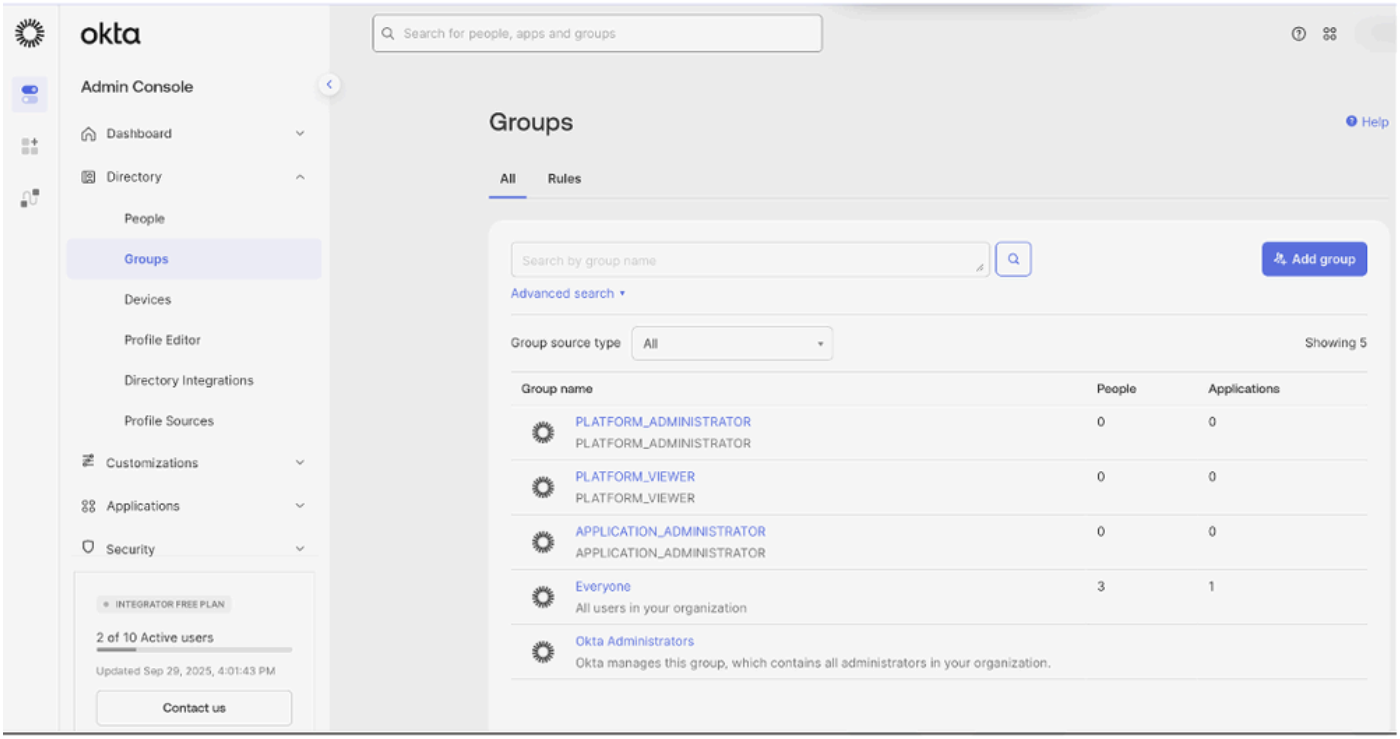
2. Geben Sie eine IDP-Rolle für die ausgewählte Systemrolle ein. Folgende Systemrollen werden unterstützt:

- Allgemeiner Kontoadministrator: Der allgemeine Kontoadministrator verfügt über die vollen

Berechtigungen zum Ausführen aller Aktionen im Produkt.

- Allgemeine Kontoanzeige: 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.

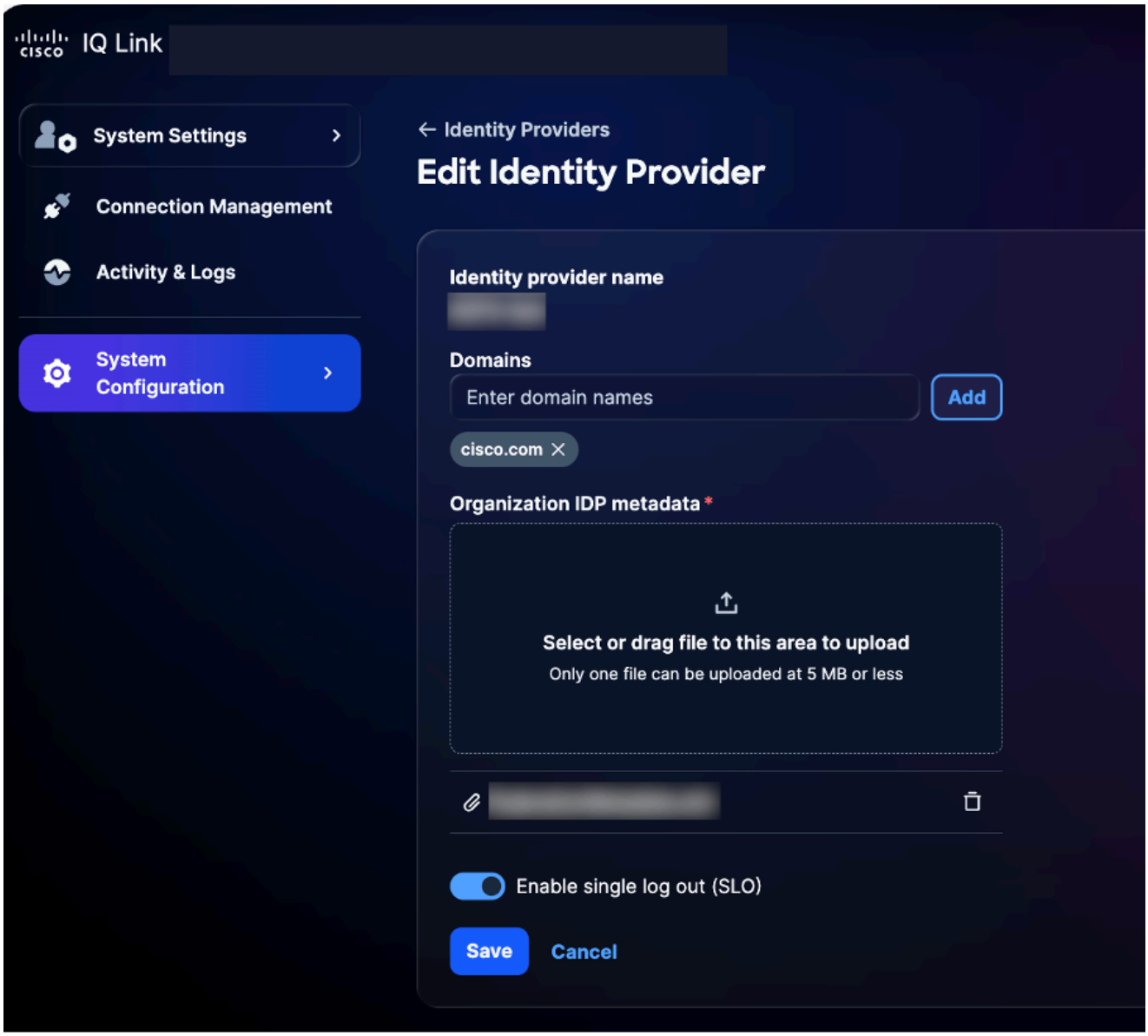
Konfiguration für einmaliges Abmelden

Wenn Sie die Single Logout Configuration (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 in der IDP SAML-Konfiguration für 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 Kontoadministrator 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:

Tabelle 4: 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 (AD) 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 AD-Integration
- SSL-/TLS-Zertifikate (Transport Layer Security) auf ADFS
- Account-Administrator-Zugriff 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)

Tabelle 5: 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	AD-Gruppen-Domänennamen (Domain Names, DN)	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 den vertrauenden Teilnehmer aus einer Datei importieren, um Details aus der Datei abzurufen, die als Teil von Schritt 3 gespeichert wird.
10. Klicken Sie auf Durchsuchen, um die SP-Metadatendatei 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.

✎ Anmerkung: Wählen Sie nicht "Jeden mit MFA zulassen" aus, es sei denn, Ihr ADFS-Server verfügt über einen registrierten MFA-Adapter (Multi-Factor Authentication) (z. B. Azure MFA oder *Time-Based One-Time Password (TOTP)).
Wenn diese Richtlinie ohne einen konfigurierten MFA-Anbieter aktiviert wird, authentifiziert ADFS den Benutzer, verweigert jedoch die Anforderung mit dem Status urn:oasis:names:tc:SAML:2.0:status:RequestDenied. Da die SAML-Antwort keine Assertion enthält, schlägt das Plugin fehl und meldet einen "Missing Email"-Fehler.

Problem: Wählen Sie "Jeden Benutzer mit MFA zulassen" aus.

Problemumgehung: Überprüfen Sie in PowerShell die aktuelle Richtlinie, indem Sie den folgenden Befehl ausführen.

```
Get-AdfsRelyingPartyTrust -Name “

    ”).AccessControlPolicyName
```

Führen Sie den folgenden Befehl aus, um "Allow everyone" (Alle zulassen) festzulegen (keine MFA-Anforderung):

```
Set-AdfsRelyingPartyTrust -TargetName “

     ” -AccessControlPolicyName “Permit everyone”
```

Sie können die Vertrauensstellung der vertrauenden Seite auch über PowerShell erstellen:

```
Add-AdfsRelyingPartyTrust `
    -Name “

     ” `
    -Identifier “

      ” `
-SamlEndpoint (New-AdfsSamlEndpoint -Binding POST -Protocol SAMLAssertionConsumer -Uri “

       ”) `
    -AccessControlPolicyName “Permit everyone” `
    -IssuanceAuthorizationRules ’=> issue(Type = “http://schemas.microsoft.com/authorization/claims/per
```

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.

Tabelle 6: Erforderliche Forderungen

Forderung	Zweck	Quelle
E-Mail	Benutzer-ID	AD-Mail
Anzeigename	Vollständiger Name des Benutzers	AD-Anzeigename
UPN	Public Key Infrastructure (PKI)/Zertifikatauthentifizierung	ADFS ordnet das Clientzertifikat einem AD-Benutzer über den Benutzerprinzipalnamen (User Principal Name, UPN) zu.
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
=> 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. Wenden Sie die Anspruchsregeln an, indem Sie den folgenden Befehl ausführen:

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

Write-Host “Claim rules configured successfully!” -ForegroundColor Green
```

 Warnung: Für jedes AD-Benutzerkonto muss das E-Mail-Attribut ausgefüllt werden. Wenn dieses Attribut fehlt, enthält die SAML-Assertion keinen E-Mail-Anspruch, was zu einer Ablehnung der Authentifizierung führt.

Um die E-Mail-Adresse eines Benutzers zu aktualisieren, führen Sie den folgenden PowerShell-Befehl aus:

```
Set-ADUser -Identity “

     ” -EmailAddress “

      ”
```

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. Anzeigen der Gruppen, zu denen der Benutzer gehört

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

Beispiel:

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

Konfigurieren von ADFS, um dem SP-Signaturzertifikat zu vertrauen

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:

 Anmerkung: Das SP-Zertifikat wird von einer internen Zertifizierungsstelle (Certificate Authority, CA) 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

- Wenn das SP-Zertifikat von einer Zertifizierungsstelle ausgestellt wurde (nicht selbstsigniert), importieren Sie das ausstellende Zertifizierungsstellenzertifikat in den Stammzertifikatsspeicher:

```
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
```

PKI-/Zertifikatauthentifizierung einrichten

In diesem Abschnitt wird beschrieben, wie Sie zertifikatbasierte (d. h. Smartcard- oder Softwarezertifikate) Authentifizierung neben Kennwörtern hinzufügen. Dieser Abschnitt kann übersprungen werden, wenn eine nur mit einem Kennwort durchgeführte Authentifizierung ausreichend ist.

Installieren der AD CS CA-Rolle

So installieren Sie die Zertifizierungsstellenrolle "AD Certificate Services (CS)":

1. Überprüfen Sie, ob in Ihrer Domäne bereits eine Enterprise CA vorhanden ist, indem Sie den folgenden Befehl ausführen:

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

Wenn der Befehl eine gültige Antwort zurückgibt, können Sie den Rest dieses Abschnitts überspringen. Ihre Umgebung ist bereits konfiguriert. Wenn der Befehl anzeigt, dass keine CA gefunden wurde, fahren Sie mit Schritt 2 fort.

2. Installieren Sie die Zertifizierungsstellenrolle, indem Sie den folgenden Befehl ausführen:

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

3. Konfigurieren Sie die Zertifizierungsstellenrolle mit dem folgenden Befehl:

```
Install-AdcsCertificationAuthority `
    -CAType EnterpriseRootCA `
    -CACommonName “


     ” `
    -KeyLength 2048 `
    -HashAlgorithmName SHA256 `
    -CryptoProviderName “RSA#Microsoft Software Key Storage Provider” `
    -ValidityPeriod Years `
    -ValidityPeriodUnits 10 `
    -Force
```

4. Installation mit folgendem Befehl:

```
certutil -ca
```

5. Bestätigen Sie mit dem folgenden Befehl, dass der Dienst aktiv und erreichbar ist:

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

Konfigurieren einer Zertifikatvorlage

So konfigurieren Sie eine Zertifikatvorlage mit der erweiterten Clientauthentifizierungsschlüsselverwendung (Client Authentication Enhanced Key Usage, EKU):

1. Öffnen Sie certsrv.msc, und erweitern Sie den CA-Knoten.
2. Klicken Sie mit der rechten Maustaste auf Zertifikatvorlagen > Verwalten.
3. Duplizieren Sie die Benutzervorlage.

Anmerkung: Die integrierte Benutzervorlage ist nur dann funktionsfähig oder gültig, wenn

---

das von ihr ausgestellte Zertifikat die Clientauthentifizierungs-EKU enthält.

4. Konfigurieren Sie die Einstellungen auf den folgenden Registerkarten:

- Allgemein: Geben Sie "CIQ User Authentication" in das Feld Name mit einer Gültigkeitsdauer von einem (1) Jahr ein.
- Anforderungsverarbeitung: Wählen Sie Signatur und Verschlüsselung aus der Dropdown-Liste Zweck aus, und aktivieren Sie das Kontrollkästchen Privaten Schlüssel exportieren zulassen.
- Betreffname: Wählen Sie Aus Active Directory-Informationen erstellen aus, und fügen Sie eine E-Mail in die Felder Betreff und SAN ein.

Warnung: Die Felder Betreff und SAN müssen die UPN eines Benutzers oder eine E-Mail enthalten, die mit einem AD-Konto übereinstimmt. ADFS ordnet das Zertifikat mithilfe dieser Felder einem AD-Benutzer zu.

- Durchwahlen: Stellen Sie sicher, dass die Anwendungsrichtlinien "Client Authentication (1.3.6.1.5.5.7.3.2)" enthalten.
- Sicherheit: Hinzufügen von Domänenbenutzern und Gewähren von Lese- und Registrierungsberechtigungen

5. Veröffentlichen Sie die Vorlage mit dem folgenden Befehl:

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

Registrieren eines Benutzerzertifikats

1. Melden Sie sich als Zielbenutzer an.
2. Registrieren Sie das Zertifikat mit dem folgenden Befehl:

```
certreq -enroll -user “CIQUserAuthentication”
```

3. Überprüfen Sie die Zertifikatinstallation, indem Sie den folgenden Befehl ausführen:

```
Get-ChildItem Cert:| Where-Object {
    $_.EnhancedKeyUsageList.ObjectId -contains “1.3.6.1.5.5.7.3.2”
} | Format-Table Subject, Thumbprint, NotAfter -AutoSize
```

Exportieren eines Benutzerzertifikats aus Windows und Installieren auf dem Client (Mac)

So exportieren Sie ein Benutzerzertifikat von Windows nach Mac:

1. Exportieren Sie das Zertifikat von Windows als PFX-Datei, indem Sie die folgenden Befehle ausführen:

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

     *” }

$password = ConvertTo-SecureString -String “

      ” -Force -AsPlainText

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

2. Übertragen Sie die Datei user-cert.pfx auf Ihr Mac-Gerät.

3. Importieren Sie das Zertifikat in die Mac Keychain, indem Sie den folgenden Befehl ausführen:

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

     ”
```

Anmerkung: Nach dem Importieren des Zertifikats muss der Browser geschlossen und erneut geöffnet werden, damit das Zertifikat erkannt werden kann.

4. Vertrauen Sie der Zertifizierungsstelle auf dem Mac, indem Sie Folgendes ausführen:

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

Endpunkte für die Authentifizierung mit ADFS-Zertifikaten aktivieren

So aktivieren Sie Endpunkte für die ADFS-Zertifikatauthentifizierung:

1. Aktivieren Sie die erforderlichen ADFS-Zertifikatendpunkte, indem Sie die folgenden Befehle ausführen:

```
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. Stellen Sie sicher, dass alle Endpunkte aktiviert sind, indem Sie den folgenden Befehl ausführen:

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

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

Aktivieren der Zertifikatauthentifizierung als primäres Kriterium

So aktivieren Sie die Zertifikatauthentifizierung als primäre Authentifizierung:

1. Konfigurieren Sie die primären Authentifizierungsanbieter für den Intranet- und Extranet-Zugriff mithilfe des folgenden Befehls:

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

2. Stellen Sie sicher, dass beide Listen CertificateAuthentication und FormsAuthentication enthalten. Verwenden Sie hierzu die folgenden Befehle:

```
(Get-AdfsGlobalAuthenticationPolicy).PrimaryIntranetAuthenticationProvider

(Get-AdfsGlobalAuthenticationPolicy).PrimaryExtranetAuthenticationProvider
```

3. Überprüfen Sie die aktuelle TLS-Client-Port-Konfiguration mit dem folgenden Befehl:

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

4. Wenn der TlsClientPort nicht 49443 ist, aktualisieren Sie den Port und starten Sie den ADFS-Dienst mithilfe der folgenden Befehle neu:

```
Set-AdfsProperties -TlsClientPort 49443

Restart-Service adfssrv
```

SChannel/TLS-Korrekturen (WICHTIG für PKI)

Mit den Schritten in den folgenden Abschnitten werden CERT_E_UNTRUSTEDROOT-Fehler (0x800B0109) behoben, die verhindern, dass die Zertifikatauthentifizierung funktioniert.

Binden von SSL-Zertifikaten an Port 49443

SSL-Zertifikate an Port 49443 binden:

1. Entfernen Sie alle vorhandenen SSL-Zertifikatsbindungen auf Port 49443, indem Sie den folgenden Befehl verwenden:

```
netsh http delete sslcert hostnameport=

     :49443
```

2. Erstellen Sie eine neue Bindung mit aktivierter Clientzertifikataushandlung, indem Sie den folgenden Befehl verwenden:

```
netsh http add sslcert hostnameport=

     :49443 `
    certhash=

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

3. Stellen Sie sicher, dass die Client-Zertifikataushandlung mit dem folgenden Befehl aktiviert ist:

```
netsh http show sslcert hostnameport=

     :49443
```

Löschen des Zertifikatspeichers (KRITISCH)

So bereinigen Sie den Zertifikatspeicher:

Warnung: Windows SChannel lehnt alle Clientzertifikate ab, wenn im vertrauenswürdigen Stammspeicher nicht selbstsignierte Zertifikate vorhanden sind. Dies ist die Hauptursache für PKI-Fehler.

---

1. Identifizieren Sie nicht selbstsignierte Zertifikate im Speicher für vertrauenswürdige Stammverzeichnisse, indem Sie den folgenden Befehl ausführen:

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

```
$bad | ForEach-Object { Write-Host “PROBLEM: $($_.Subject) | Issuer: $($_.Issuer)” -ForegroundColor Red
```

2. Verschieben Sie diese Zertifikate in den Zwischenspeicher der Zertifizierungsstelle, indem Sie den folgenden Befehl ausführen:

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

3. Vergewissern Sie sich, dass keine nicht selbstsignierten Zertifikate im Stammspeicher verbleiben, indem Sie den folgenden Befehl ausführen:

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

SChannel-Registrierungsreparaturen (KRITISCH)

So konfigurieren Sie die SChannel-Registrierungseinstellungen, um eine ordnungsgemäße Zertifikatsauthentifizierung sicherzustellen:

1. Definieren Sie die Registrierungspfadvariable mit dem folgenden Befehl:

```
$regPath = “HKLM:”
```

2. Wenden Sie die in der Tabelle unten definierten Registrierungseinstellungen mit den folgenden Befehlen an:

```
Set-ItemProperty -Path $regPath -Name “ClientAuthTrustMode” -Value 2 -Type DWord

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

Tabelle 7: Einstellungen für die Kanalregistrierung

Einstellung	Wert	Zweck
ClientAuthTrustMode	2	Aktiviert exklusive Zertifizierungsstellenvertrauensstellung, um den Standardüberprüfungspfad zu korrigieren.

Einstellung	Wert	Zweck
VertrauenswürdigeAusstellerlisteSenden	0	Verhindert, dass der Server während des TLS-Handshakes die vollständige Liste vertrauenswürdiger Aussteller sendet.

Überprüfen des Zertifizierungsstellen-Zertifikatspeichers

So überprüfen Sie den Zertifikatspeicher der Zertifizierungsstelle:

Anmerkung: Das Zertifizierungsstellenzertifikat, das Benutzerzertifikate ausstellt, muss sich im SystemCertificatesStore befinden, um sicherzustellen, dass es richtig erkannt wird.

---

1. Definieren Sie den Fingerabdruck Ihres Zertifizierungsstellenzertifikats mit dem folgenden Befehl:

```
$caThumbprint = “

    ”
```

2. Vergewissern Sie sich, dass das Zertifizierungsstellenzertifikat bereits im LocalMachinestore vorhanden ist. Verwenden Sie hierzu den folgenden Befehl:

```
$exists = Test-Path “HKLM:\caThumbprint”
```

Wenn das Zertifikat nicht gefunden wird, importieren Sie es in den LocalMachinestore:

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

Neustarten des ADFS-Servers (OBLIGATORISCH)

Starten Sie den ADFS-Server mit dem folgenden Befehl neu:

```
Restart-Computer -Force
```

Anmerkung: Die Registrierungsänderung ClientAuthTrustMode wird erst nach dem Neustart des Servers wirksam.

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.

Konfiguration im Cisco IQ

Konfiguration auf Cisco IQ:

1. Übertragen Sie adfs-metadaten.xml auf Ihre Workstation.
2. Navigieren Sie in Cisco IQ zu Systemeinstellungen > Systemkonfiguration > Identitätsanbieter.
3. Laden Sie die ADFS-Metadatendatei hoch, um das IDP-Zertifikat, die Element-ID und die SSO-URL automatisch zu extrahieren.
4. Speichern Sie die Konfiguration.

Anmerkung: Wenn ADFS einen automatischen Rollover für Tokensignaturzertifikate durchführt, müssen Sie die Metadatendatei erneut exportieren und in Cisco IQ hochladen, um eine kontinuierliche Authentifizierung sicherzustellen.

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 Umschaltfläche Single Logout 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 von AD finden, die für die Zuordnung verwendet werden sollen. Führen Sie den folgenden PowerShell-Befehl aus, um Gruppen aus AD zu suchen.

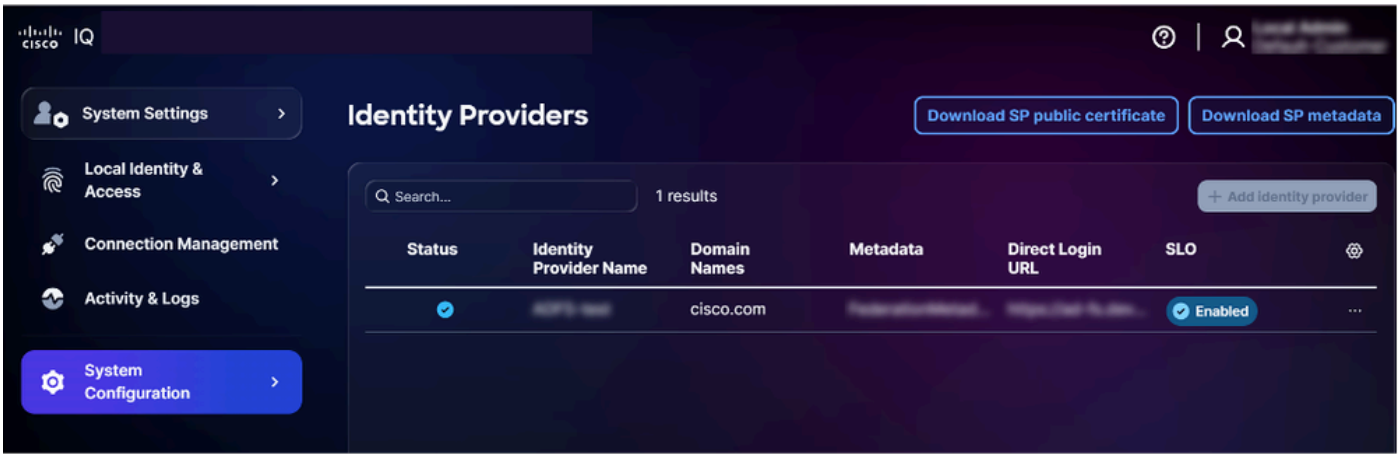
```
$searcher = New-Object DirectoryServices.DirectorySearcher
$searcher.Filter = "(&(objectClass=group)(cn=Role - CXIQ*))"
$searcher.PropertiesToLoad.Add("distinguishedName") | Out-Null
$searcher.PropertiesToLoad.Add("cn") | Out-Null
$searcher.FindAll() | ForEach-Object { $_.Properties["distinguishedname"]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

Das System fragt AD direkt über das Lightweight Directory Access Protocol (LDAP) ab und benötigt keine zusätzlichen Module. Die Gruppeninformationen werden im vollständigen Distinguished Name-Format 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

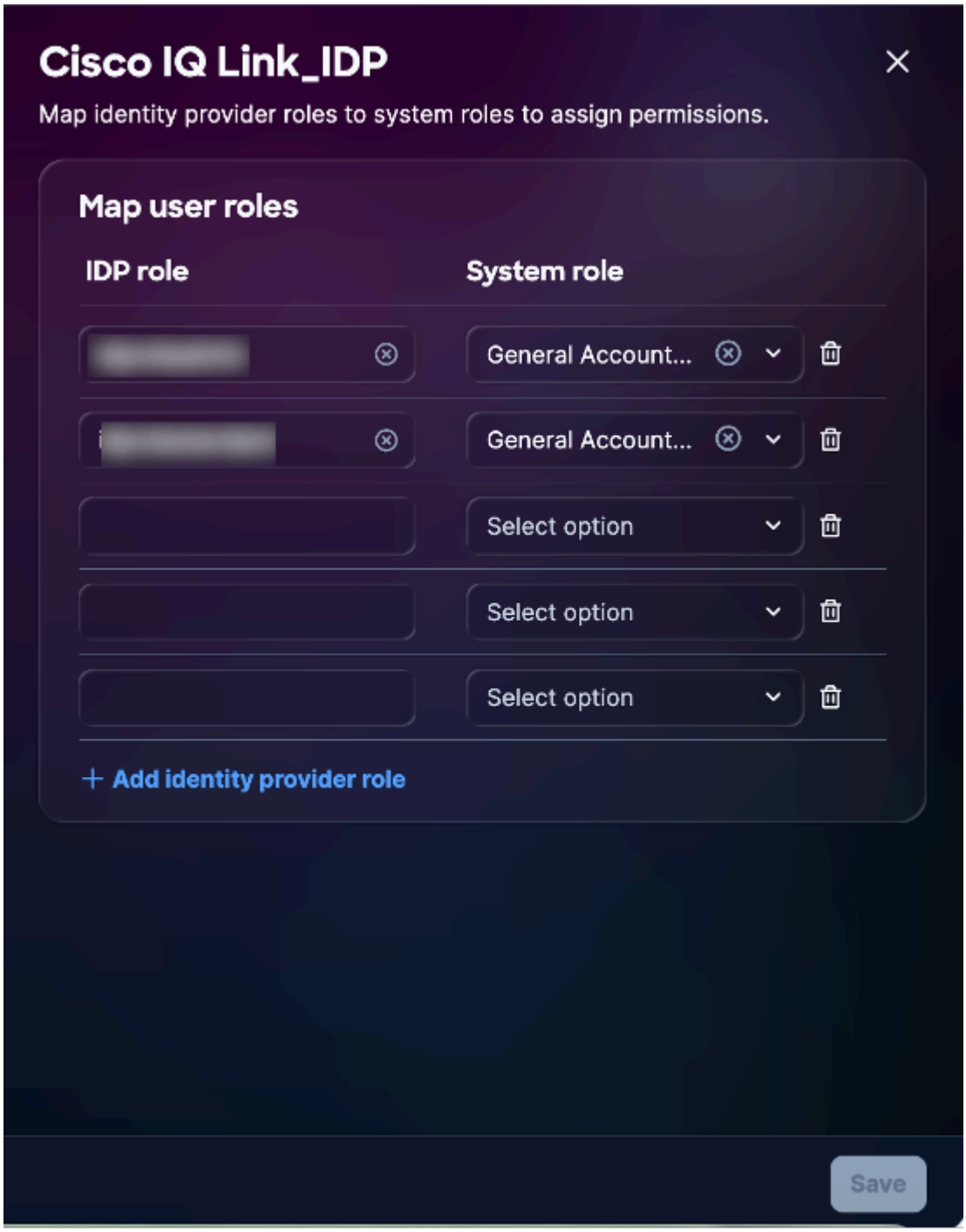
Wenn die erforderlichen Gruppen nicht aufgeführt sind, müssen sie von einem Kontoadministrator in AD erstellt werden, bevor Sie die ADFS-Rollenzuordnung abschließen können.

So konfigurieren Sie die Rollenzuordnung:



Zuordnen von Rollen

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 System-Rolle ein. Folgende Systemrollen werden unterstützt:

- Allgemeiner Kontoadministrator: Der allgemeine Kontoadministrator verfügt über alle Berechtigungen zum Ausführen aller Aktionen im Produkt. Die IDP-Rolle (analysierter Name) lautet CXIQ Admins.
- Allgemeine Kontoanzeige: 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.

SChannel-Clientzertifikattest

Öffnen Sie ein neues PowerShell-Fenster, und führen Sie den folgenden Befehl aus, um zu überprüfen, ob SChannel ordnungsgemäß für die Annahme von Client-Zertifikaten konfiguriert ist:

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


     :49443/adfs/ls/”
```

Die erwartete Ausgabe ist eine HTTP-Antwort (z. B. eine Umleitung oder die ADFS-Seite). Tritt ein TLS-Handshake-Fehler auf, ist die Verbindung fehlgeschlagen.

End-to-End-Browsertest für PKI-Fluss

Bevor Sie mit End-to-End-Browsertests für den PKI-Fluss beginnen, stellen Sie sicher, dass das Benutzerzertifikat in macOS Keychain installiert ist (weitere Informationen finden Sie unter Importieren des Benutzerzertifikats auf dem Client-Computer (macOS) unterKonfigurieren der zertifikatbasierten Authentifizierung).

So testen Sie:

1. Navigieren Sie zur SAML-Anmelde-URL der Anwendung. Das ADFS stellt die Zertifikat- und Kennwortoptionen dar.
2. Wählen Sie Zertifikatsauthentifizierung aus. Der Browser fordert Sie zur Eingabe des Zertifikats auf.
3. Zertifikat hochladen Das ADFS authentifiziert den Benutzer, leitet die Anforderung mit einer SAML-Antwort um und erstellt eine neue Sitzung.

End-to-End-Browser-Tests auf Passwortfluss

Bevor Sie mit dem End-to-End-Browser-Testen des Kennwortflusses beginnen:

1. Navigieren Sie zur SAML-Anmelde-URL der Anwendung. Das ADFS stellt die Zertifikat- und Kennwortoptionen dar.
2. Wählen Sie Kennwort/Formularauthentifizierung aus.
3. Geben Sie einen Benutzernamen ein.
4. Geben Sie ein Passwort ein.
5. Überprüfen Sie, ob die Anmeldung erfolgreich war.

Anmerkung: Beide Datenflüsse müssen gleichzeitig funktionieren.

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.

Tabelle 8: 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. • Falsches Gruppenattribut: Muss sich um http://schemas.xmlsoap.org/cla ims/Group handeln • 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

Problem	Symptome / Beschreibung	Ursachen/Prüfungen/Problemumgehungen und Korrekturen
		• Cookie-Konflikt: 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
```

Microsoft Entra ID SAML-Konfiguration für SSO

Dieser Abschnitt enthält Anleitungen zur Konfiguration der Microsoft Entra ID (Entra ID) als SAML

IDP für Cisco IQ und unterstützt sowohl die kennwort- als auch die PKI/certificate-basierte Authentifizierung (CBA).

Voraussetzungen für die Konfiguration von Entra ID SAML für SSO

- Microsoft Entra ID-Tenant (z. B. "ciqtestdev.onmicrosoft.com")
- Globaler Administrator oder Anwendungsadministrator mit Rollenzugriff auf Cisco IQ
- Verbindung zwischen Entra ID (Cloud) und Cisco IQ
- Enterprise CA installiert oder erreichbar (nur für PKI erforderlich)
- Der CRL-Verteilungspunkt (Certificate Revocation List) ist über das Internet erreichbar (nur für PKI erforderlich).

Tabelle 9: Konfiguration des Entra-ID-Servers

Posten	Beschreibung	Beispiel
Tenant-ID	Tenant-ID (Eingabe)	37352d8f-0ebe-4762-8161-8775ffe897cb
Cisco IQ-FQDN	Bereitstellungs-Hostname	<IHR CIQ-FQDN>
ID der IDP-Einheit	URL des Einwahl-Ausstellers	https://sts.windows.net/<TENANT-ID>/
IDP SSO-URL	SAML-Anmeldeendpunkt	https://login.microsoftonline.com/<TENANT-ID>/saml2
Firmendomäne	E-Mail-Domäne für Benutzer	<IHRE-DOMÄNE>

Konfiguration der Entra ID SAML-Anwendung

Erstellen einer Unternehmensanwendung

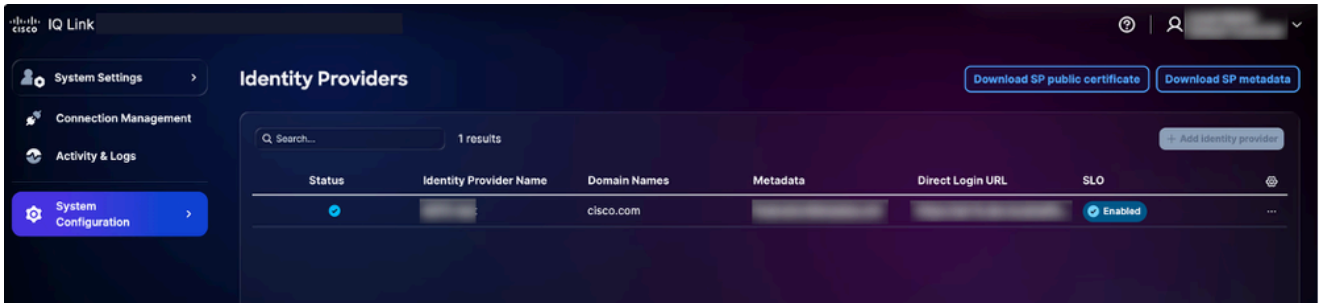
1. Melden Sie sich beim Microsoft Entra Admin Center an.
2. Navigieren Sie zu Identität > Anwendungen > Unternehmensanwendungen.

3. Klicken Sie auf Neue Anwendung > Eigene Anwendung erstellen.
4. Geben Sie den Namen ein (z. B. "Cisco IQ").
5. Wählen Sie Alle anderen Anwendungen integrieren, die Sie nicht in der Galerie finden (Nicht-Galerie).
6. Klicken Sie auf Erstellen.

Konfigurieren der SAML-einmaligen Anmeldung

Um die SAML Single Sign-On zu konfigurieren, müssen Sie die SP-Metadatendatei hochladen. Sie können es über die virtuelle Appliance (VA) wie folgt beziehen:

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



Download-Optionen

2. Klicken Sie auf SP-Metadaten herunterladen, um sie herunterzuladen. Diese heruntergeladene SP-Metadatendatei wird hochgeladen, um die Konfiguration der einmaligen Anmeldung (Single Sign-on, SAML) abzuschließen.
3. Klicken Sie auf die Schaltfläche Metadatendatei hochladen, um die SP-Metadatendatei hochzuladen. Die Daten aus der SP-Metadatendatei werden nach dem erfolgreichen Upload automatisch im SAML-basierten Single Sign-on-Bildschirm ausgefüllt.

Sie können diese Angaben auch manuell eingeben, um die Einstellungen für die einmalige Anmeldung zu konfigurieren. So konfigurieren Sie die SAML-einmalige Anmeldung manuell:

1. Navigieren Sie in der Enterprise-Anwendung zu Single Sign-On, und wählen Sie SAML.
2. Klicken Sie im Abschnitt SAML-Basiskonfiguration auf Bearbeiten, und geben Sie Folgendes ein:
    a. Kennung (Element-ID): <IHR CIQ-FQDN>
    b. Antwort-URL (ACS-URL): https://<YOUR-CIQ-FQDN>/saml/acs

c. Anmelde-URL: https://<YOUR-CIQ-FQDN>/saml/login

d. Abmelde-URL: https://<YOUR-CIQ-FQDN>/saml/abmelden

3. Klicken Sie auf Speichern.

Anmerkung: Die Element-ID muss genau der von Cisco IQ als SP-Element-ID verwendeten ID entsprechen. Hierbei handelt es sich in der Regel um den FQDN der Bereitstellung.

---

4. Um SAML-Attribute und -Ansprüche zu konfigurieren, klicken Sie im Abschnitt Attribute und Ansprüche auf Bearbeiten.

5. Konfigurieren Sie die folgenden Ansprüche:

Tabelle 10: Erforderliche SAML-Ansprüche

Forderung	Quellattribut	Namespace
Eindeutige Benutzerkennung (NameID)	user.userprincipalname	(standard)
Email-Adresse	Benutzer.Mail	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
Givenname	user.givenname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
Nachname	Benutzer.Nachname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
name	user.userprincipalname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
Gruppen	user.assignedroles	(LEER — leerer Namespace)

Anmerkung: Für die Gruppen Anspruch:
- Verwenden Sie user.assignedroles als Quelle - nicht Benutzer.Gruppen
- Das Feld Namespace muss leer sein. Dadurch wird sichergestellt, dass der Attributname in der SAML-Assertion einfach Gruppen anstatt eines vollständigen URI (Uniform Resource Identifier) ist
- Fügen Sie keinen doppelten Gruppenanspruch mit user.groups hinzu, da dies Konflikte verursacht.

Konfigurieren von App-Rollen

App-Rollen werden in der App-Registrierung konfiguriert (nicht in der Enterprise-Anwendung). So konfigurieren Sie Anwendungsrollen:

1. Navigieren Sie zu Identität > Anwendungen > App-Registrierungen.
2. Suchen Sie Ihre Anwendung aus und wählen Sie sie aus.

3. Gehen Sie zu App-Rollen > App-Rolle erstellen.
4. Konfigurieren Sie für jede erforderliche Rolle Folgendes:

- Anzeigename: Cisco IQ-Administratoren beispielsweise
- Zulässige Membertypen: Benutzer/Gruppen
- Wert: Cisco IQ-Administratoren beispielsweise
- Beschreibung: Beispielsweise Cisco IQ-Administratoren

5. Klicken Sie auf Anwenden.

Anmerkung: Erstellen Sie Rollen, die Ihren Cisco IQ-Rollenzuordnungsanforderungen entsprechen (z. B. CXIQ-Administratoren, CXIQ-Entwickler, CXIQ-Viewer).

Anstelle von Gruppenansprüchen werden aus folgenden Gründen App-Rollen verwendet:

- Nur-Cloud-Tenants können Gruppen-Anzeigenamen ohne P1- oder P2-Lizenz nicht senden.
- sAMAccountName funktioniert nur für Gruppen, die von lokalen AD synchronisiert werden
- Die Group ID-Quelle sendet UUIDs (Universally Unique Identifiers), die schwer zuzuordnen sind.
- App-Rollen senden exakte Zeichenfolgenwerte, die den Erwartungen der Cisco IQ-Rolle entsprechen

Zuweisen von Benutzern zu Anwendungsrollen

So weisen Sie Benutzern App-Rollen zu:

1. Gehen Sie zurück zu Enterprise Application > Users and groups.
2. Klicken Sie auf Benutzer/Gruppe hinzufügen.
3. Wählen Sie die Benutzer aus, und weisen Sie die entsprechende App-Rolle zu.
4. Klicken Sie auf Zuweisen. Rollenwerte werden im SAML-Assertionsgruppenattribut als lesbare Zeichenfolgen angezeigt.

IDP-Metadaten und -Zertifikat herunterladen

IDP-Metadaten und -Zertifikate herunterladen:

1. Gehen Sie in der Enterprise-Anwendung zu Single Sign-on > SAML Signing Certificate (einmalige Anmeldung > SAML-Signaturzertifikat).
2. Verbundmetadaten-XML herunterladen (als entra-id-metadaten.xml speichern).

   ODER

   Laden Sie das Zertifikat (Base64) für die manuelle Zertifikatseingabe herunter.
3. Beachten Sie die folgenden Werte aus dem Abschnitt Einrichtung:

- Anmelde-URL (IDP SSO-URL)
- Azure AD Identifier (IDP Entity ID)
- Abmelde-URL (IDP SLO-URL)

Anmerkung: Da die Entra-ID sich regelmäßig dreht, müssen Sie die Metadaten erneut herunterladen und bei jeder Änderung des aktiven Zertifikats in die VA hochladen, um einen unterbrechungsfreien SSO-Dienst sicherzustellen.

Hinzufügen von Entra ID IDP

Anmerkung: APISIX-Routen für SAML werden automatisch erstellt, wenn ein IDP im Cisco IQ hinzugefügt wird. Somit ist keine manuelle Routenkonfiguration erforderlich.

So fügen Sie Entra ID IDP hinzu:

1. Melden Sie sich bei VA als Kontoadministrator an.
2. Navigieren Sie zu Systemeinstellungen > Systemkonfiguration > Identitätsanbieter.
3. Klicken Sie auf Identitätsanbieter hinzufügen.
4. Geben Sie den Namen des IDP ein (z. B. "Entra ID").
5. Geben Sie die Domäne(n) ein (z. B. "ciqtestdev.onmicrosoft.com" oder Ihre Unternehmensdomäne).
6. (Optional) Aktivieren Sie ggf. die Umschaltfläche Single Logout aktivieren.
7. Ziehen Sie die Datei entra-id-metadates.xml, die von Entra ID abgerufen wurde, per Drag-and-Drop in das Feld Upload IDP Metadata (IDP-Metadaten hochladen).
8. Klicken Sie auf Speichern.

Anmerkung: Der Status bleibt "Incomplete" (Unvollständig), bis die Rollenzuordnung abgeschlossen ist. Dies ist das erwartete Verhalten.

Konfigurieren der Rollenzuordnung

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

Tabelle 11: Systemrollen

Systemrolle	IDP-Rolle (Wert der App-Rolle)	Beschreibung
Allgemeiner Kontoadministrator	CXIQ-Administratoren	Vollständige Berechtigungen für alle Aktionen
Allgemeine Kontoanzeige	CXIQ-Entwickler	Schreibgeschützter Zugriff
Allgemeine Kontoanzeige	CXIQ-Viewer	Schreibgeschützter Zugriff

Anmerkung: Verwenden Sie die Zeichenfolgen für den Wert der App-Rolle genau so, wie sie in Entra ID konfiguriert sind (weitere Informationen finden Sie unter Konfigurieren von App-Rollen unter Konfigurieren der Entra ID-SAML-Anwendung).

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

Überprüfen des SAML-Ablaufs (Kennwortauthentifizierung)

So überprüfen Sie den SAML-Fluss:

1. Öffnen Sie einen Browser im Inkognito- oder Privat-Modus.
2. Navigieren Sie zu https://<YOUR-CIQ-FQDN>/saml/login.
3. Stellen Sie sicher, dass Sie zur Microsoft-Anmeldeseite weitergeleitet werden.
4. Authentifizieren Sie sich mit Ihren Anmeldeinformationen (und MFA, wenn konfiguriert).
5. Überprüfen Sie nach der Authentifizierung, ob Sie zurück zu /saml/acs geleitet werden und

ob die Cisco IQ-Anwendung angezeigt wird.

6. Überprüfen Sie die Gruppenextraktion, indem Sie den folgenden Befehl ausführen:

```
kubectl -ncxue logs deployment/apisix –since=5m | grep -E “authentication successful|Extracted group|To
```

Erwartete Ausgabe

```
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
```

Konfigurieren der zertifikatbasierten Authentifizierung

In diesem Abschnitt wird beschrieben, wie Sie neben Kennwörtern auch eine CBA hinzufügen. Dieser Abschnitt kann übersprungen werden, wenn eine nur mit einem Kennwort durchgeführte Authentifizierung ausreichend ist.

Voraussetzungen für CBA

- Windows-Server mit AD-Zertifikatdiensten (CS) mit konfigurierter Enterprise-CA (z. B. "DEV-ADCS-CA")
- PowerShell-Administratorzugriff auf dem CA-Server
- Zertifikat-UPN muss mit der Entra-ID userPrincipalName übereinstimmen
- Der Zugriff auf den CRL Distribution Point muss über das Internet möglich sein.

Erstellen einer Zertifikatvorlage in AD CS

1. Öffnen Sie certtmpl.msc auf dem Zertifizierungsstellenserver.
2. Duplizieren Sie die Benutzervorlage, und nennen Sie sie "EntraUserCert".
3. Konfigurieren Sie die Vorlage:

- Allgemein: Anzeigename EntraUserCert, Gültigkeit 1-2 Jahre

- Anforderungsverarbeitung: Zweck = Signatur und Verschlüsselung
- Betreffname: Wählen Sie in der Anforderung "Bedarfsdeckung"
- Durchwahlen: Die Anwendungsrichtlinien müssen die Clientauthentifizierung (1.3.6.1.5.5.7.3.2) umfassen.
- Sicherheit: Authentifizierten Benutzern Lese- und Registrierungsberechtigungen gewähren

4. Veröffentlichen Sie die Vorlage mit dem folgenden Befehl:

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

Anfordern und Ausstellen eines Benutzerzertifikats

1. Erstellen Sie eine Zertifikatskonfigurationsdatei (INF) (z. B. C:-cert.inf) mithilfe des folgenden PowerShell-Skripts:

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

[NewRequest]
Subject = “CN=



     ”
KeyLength = 2048
KeySpec = 1
KeyUsage = 0xa0
MachineKeySet = FALSE
ProviderName = “Microsoft RSA SChannel Cryptographic Provider”
RequestType = PKCS10

[RequestAttributes]
CertificateTemplate = EntraUserCert

[EnhancedKeyUsageExtension]
OID = 1.3.6.1.5.5.7.3.2
OID = 1.3.6.1.4.1.311.20.2.2

[Extensions]
2.5.29.17 = “{text}”
_continue_ = “upn=



      &”
_continue_ = “email=
```

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

2. Ersetzen Sie <USER-UPN> durch Ihre Entra-ID UPN (z. B. user@ciqtestdev.onmicrosoft.com).

3. Führen Sie den folgenden Befehl aus, um das Zertifikat zu generieren:

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

4. Führen Sie den folgenden Befehl aus, um die Anforderung an die Zertifizierungsstelle zu senden:

```
certreq -submit -config “

     \CA-NAME>” C:-cert.csr C:-cert.cer
```

5. Führen Sie den folgenden Befehl aus, um das Zertifikat auf der Zertifizierungsstelle zu installieren:

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

Exportieren von Zertifikaten

- Um das Benutzerzertifikat als PFX-Datei (für Client) zu exportieren, führen Sie das folgende Skript aus:

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

```
     *” }
$password = ConvertTo-SecureString -String “


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

- Führen Sie das folgende Skript aus, um das Zertifikat für den Zertifizierungsstellen-Stamm (für die Entra-ID) zu exportieren:

```
Get-ChildItem Cert:| Where-Object { $_.Subject -like “*


     *” } |
Select-Object -First 1 | Export-Certificate -FilePath C:-root.cer -Type CERT
```

Benutzerzertifikat auf Client-Computer (macOS) importieren

- Führen Sie den folgenden Befehl aus, um das Benutzerzertifikat (PFX) zu importieren:

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


     ”
```

- Führen Sie den folgenden Befehl aus, um das CA-Stammzertifikat zu importieren:

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

- So legen Sie das Zertifizierungsstellenzertifikat auf Always Trust in Keychain Access fest:

1. Öffnen Sie Keychain Access.
2. Suchen Sie das Zertifizierungsstellenzertifikat, und klicken Sie auf Informationen abrufen.
3. Setzen Sie unter Vertrauenswürdig die Einstellung auf Immer vertrauen.

Anmerkung: Beenden Sie nach dem Importieren den Browser, und öffnen Sie ihn erneut, damit das Zertifikat erkannt wird.

Hochladen des CA-Stammzertifikats in die Entra-ID

1. Melden Sie sich beim Microsoft Entra Admin Center an.
2. Navigieren Sie zu Schutz > Sicherheit > Zertifizierungsstellen.
3. Klicken Sie auf Hochladen, und wählen Sie die Datei ca-root.cer aus.
4. Markieren Sie es als Stammzertifikat der Zertifizierungsstelle.
5. Geben Sie die URL des Zertifikatsperrlisten-Verteilungspunkts ein (muss öffentlich erreichbar sein).

Aktivieren von CBA bei Entra-ID-Authentifizierungsmethoden

1. Navigieren Sie zu Schutz > Authentifizierungsmethoden > Richtlinien.
2. Klicken Sie auf Zertifikatsbasierte Authentifizierung, um sie zu konfigurieren.
3. Aktivieren Sie CBA, und fügen Sie die Zielbenutzer oder -gruppen hinzu.
4. Setzen Sie unter Konfigurieren die Schutzstufe auf Single-Factor Authentication.

Konfigurieren der Benutzernamenbindung

Wechseln Sie in der CBA-Konfiguration zur Registerkarte Username binding, und legen Sie die folgende Bindung fest:

- Zertifikatfeld: PrincipalName
- Benutzerattribut: BenutzerPrincipalName

Dadurch wird der UPN im alternativen Antragstellernamen des Zertifikats dem Entra-ID-Benutzer zugeordnet.

Überprüfen des CBA-Datenflusses

1. Öffnen Sie einen Browser im Inkognito- oder Privat-Modus.
2. Navigieren Sie zu https://<YOUR-CIQ-FQDN>/saml/login.
3. Geben Sie auf der Microsoft-Anmeldeseite die E-Mail-Adresse des Benutzers ein, und klicken Sie auf Weiter.
4. Wählen Sie Zertifikat oder Smartcard verwenden (oder Sie werden automatisch dazu aufgefordert).
5. Wählen Sie das entsprechende Benutzerzertifikat aus, wenn der Browser zur Zertifikatauswahl auffordert.
6. Überprüfen Sie, ob die Entra-ID das Zertifikat validiert, mit einer SAML-Antwort umleitet und eine Sitzung erstellt.

Anmerkung: Stellen Sie sicher, dass Sie das richtige Clientzertifikat auswählen. Wenn Sie ein falsches Zertifikat auswählen (z. B. ein Zertifikat eines anderen Benutzers oder ein abgelaufenes Zertifikat), schlägt die Authentifizierung fehl.

Fehlerbehebung bei Entra-ID-Problemen

Die folgende Liste enthält allgemeine Probleme und mögliche Lösungen, um Probleme im Zusammenhang mit der Entra ID SAML-Konfiguration schnell zu identifizieren und zu beheben.

Tabelle 12: Fehlerbehebung

Problem	Ursache	Beheben
Ungültige SAML-Antwort - fehlende E-Mail	SAML-Assertion hat keine NameID oder kein E-Mail-Attribut	Überprüfen Sie die Entra ID-Anspruchskonfiguration (weitere Informationen finden Sie unter Konfigurieren der SAML-einmaligen Anmeldung unter Konfigurieren der Entra ID-SAML-Anwendung). Überprüfen Sie, ob das E-Mail-Attribut des Benutzers ausgefüllt ist.
Insgesamt extrahierte Gruppen: 0	Gruppenansprüche nicht konfiguriert oder falsche Quelle	Verwenden Sie user.assignedroles als Quelle. Stellen Sie sicher, dass der Benutzer einer App-Rolle zugewiesen ist

Problem	Ursache	Beheben
		(weitere Informationen finden Sie unter Zuweisen von Benutzern zu App-Rollen unter Konfigurieren der Entra ID-SAML-Anwendung).
Gruppenansprüche duplizieren	Sowohl user.groups als auch user.assignedroles aktiv	Entfernen Sie den user.groups-Anspruch. Behalten Sie nur user.assignedroles bei.
Gruppen werden als UUIDs angezeigt	Quellattribut ist "Gruppen-ID"	Verwenden Sie den Ansatz "Anwendungsrollen" (weitere Informationen finden Sie unter Konfigurieren von Anwendungsrollen unter Konfigurieren der Entra ID SAML-Anwendung).
Attributname zeigt langen URI an	Namespace-Feld ist nicht leer.	Löschen Sie das Feld Namespace in den Gruppenanspruchseinstellungen.
Ungültige SAML-Signatur	IdP-Zertifikat gedreht oder stimmt nicht überein	Metadaten erneut von der Entra-ID herunterladen und erneut in Cisco IQ hochladen.
ADSTS500191	CRL vom Internet aus nicht erreichbar	Veröffentlichen Sie die Zertifikatsperrliste unter einer öffentlich zugänglichen URL, oder verwenden Sie einen selbstsignierten Zertifizierungsstellenansatz (weitere Informationen finden Sie unter CRL Workaround for Lab Environments).
Zertifikat nicht angefordert	Zertifikat nicht in Schlüsselbund, CA auf Client nicht vertrauenswürdig oder CBA nicht aktiviert	Vergewissern Sie sich, dass das Benutzerzertifikat in macOS Keychain Access importiert wird (siehe Importieren des Benutzerzertifikats auf Client-Computer (macOS) unterKonfigurieren der zertifikatbasierten Authentifizierung für weitere Informationen), CBA wird in Entra ID mit den erforderlichen Einstellungen aktiviert (siehe Aktivieren von CBA in Entra ID Authentication Methods unter Konfigurieren der zertifikatbasierten Authentifizierung für weitere Informationen) und Chrome wird erneut gestartet Änderungen anwenden.
SAML-Assertion abgelaufen	Schrägstellung der Uhr zwischen den Systemen	Erhöhen Sie clock_skew_seconds in plugin config (default 300, verwenden Sie 30000 für Übung).
Status "Unvollständig" in VA	Rollenzuordnung noch nicht konfiguriert	Vollständige Rollenzuordnung (weitere Informationen finden Sie unter Konfigurieren der Rollenzuordnung).

Umgehung der Sperrliste für Probleme mit der Erreichbarkeit

Wenn der CRL Distribution Point Ihrer Zertifizierungsstelle nicht über das Internet erreichbar ist (was in Laborumgebungen üblich ist), verwenden Sie eine selbstsignierte Zertifizierungsstelle ohne die Anforderungen für die Sperrliste:

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

# Create user cert signed by the CA
$userCert = New-SelfSignedCertificate `
    -Subject “CN=



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



      &email=



       ”
)
```

Laden Sie nur das Zertifikat der Stammzertifizierungsstelle in die Entra-ID hoch. Da die Entra-ID ohne CDP selbstsigniert ist, wird keine CRL-Validierung versucht.

Abschließen der Setup-Checkliste

In diesem Abschnitt wird eine vollständige Setup-Checkliste für die Konfiguration der VA mit der Microsoft Entra ID SAML-Anwendung und der optionalen CBA beschrieben.

Setup der Eingangs-ID-SAML-Anwendung

- Enterprise-Anwendung (ohne Galerie) in Entra-ID erstellen
- Konfigurieren der grundlegenden SAML-Konfiguration durch manuelles Eingeben von SP-Metadaten
- Konfigurieren von Attributen und Ansprüchen (einschließlich E-Mail, Name und Gruppen mit user.assignedroles)
- App-Rollen bei der App-Registrierung erstellen
- Zuweisen von Benutzern zu Anwendungsrollen
- Verbundmetadaten-XML herunterladen

Cisco IQ-Konfiguration

- Identitätsanbieter in Cisco IQ durch Hochladen von Entra-ID-Metadaten hinzufügen
- Konfigurieren der Rollenzuordnung zum Zuordnen von App-Rollenwerten zu Cisco IQ-Systemrollen
- Überprüfung, ob die kennwortbasierte Anmeldung durchgängig funktioniert
- Überprüfen, ob Gruppen in Protokollen richtig extrahiert wurden

Zertifikatbasierte Authentifizierung (optional)

- Zertifikatvorlage auf AD CS mit Clientauthentifizierungs-EKU erstellen
- Benutzerzertifikat mit UPN-entsprechendem Entra-ID-Benutzer ausstellen
- Benutzerzertifikat als PFX exportieren und auf Client-Computer installieren
- Vertraut dem Zertifizierungsstellenzertifikat auf dem Clientcomputer
- CA-Stammzertifikat in Entra-ID unter Schutz hochladen > Zertifizierungsstellen
- CBA in Authentifizierungsmethoden aktivieren
- Konfigurieren der Bindung des Benutzernamens (PrincipalName und userPrincipalName)

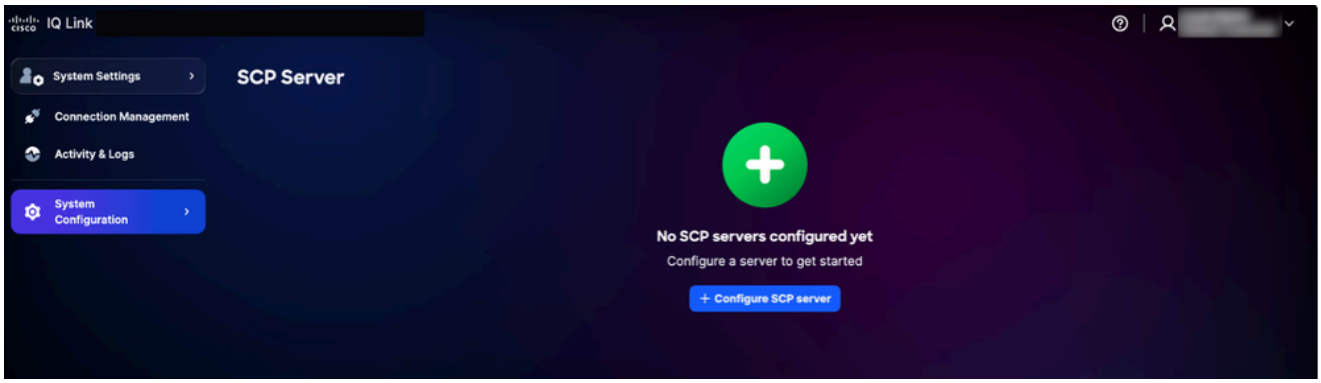
- Überprüfung, ob die CBA-Anmeldung durchgängig funktioniert

SCP-Server hinzufügen

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

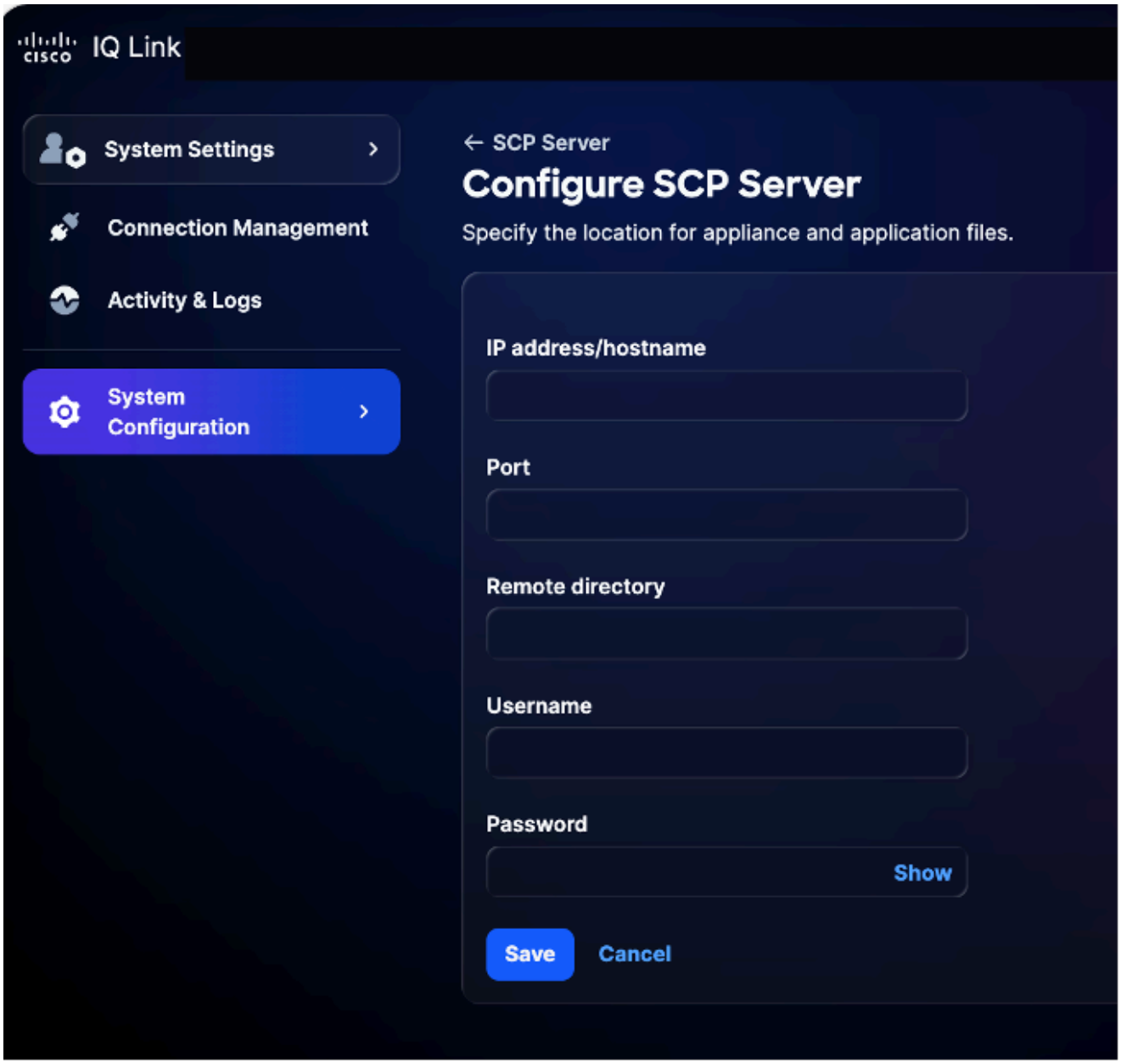
SCP-Server hinzufügen:

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 Port-Nummer 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.

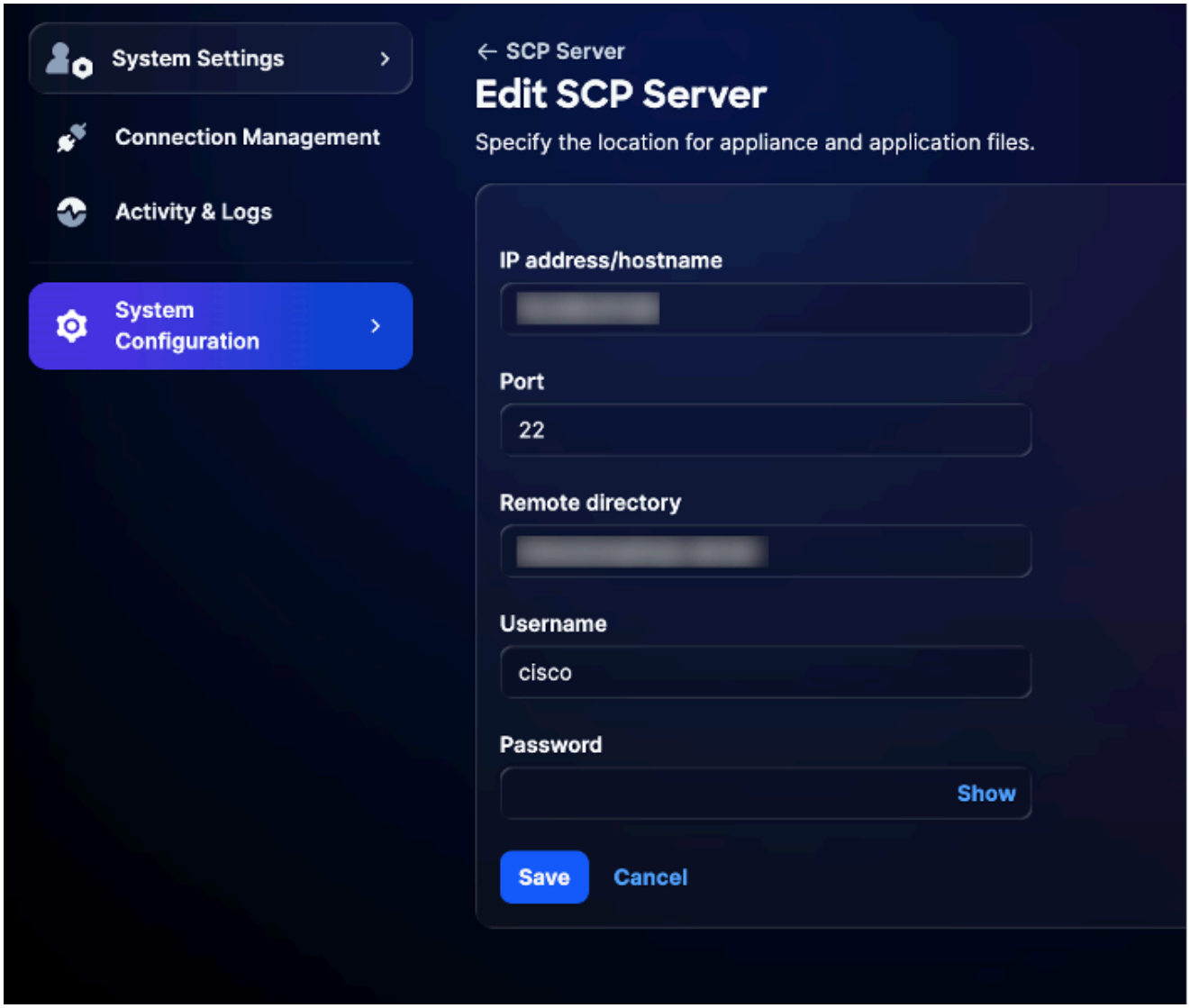
Bearbeiten vorhandener SCP-Server

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.

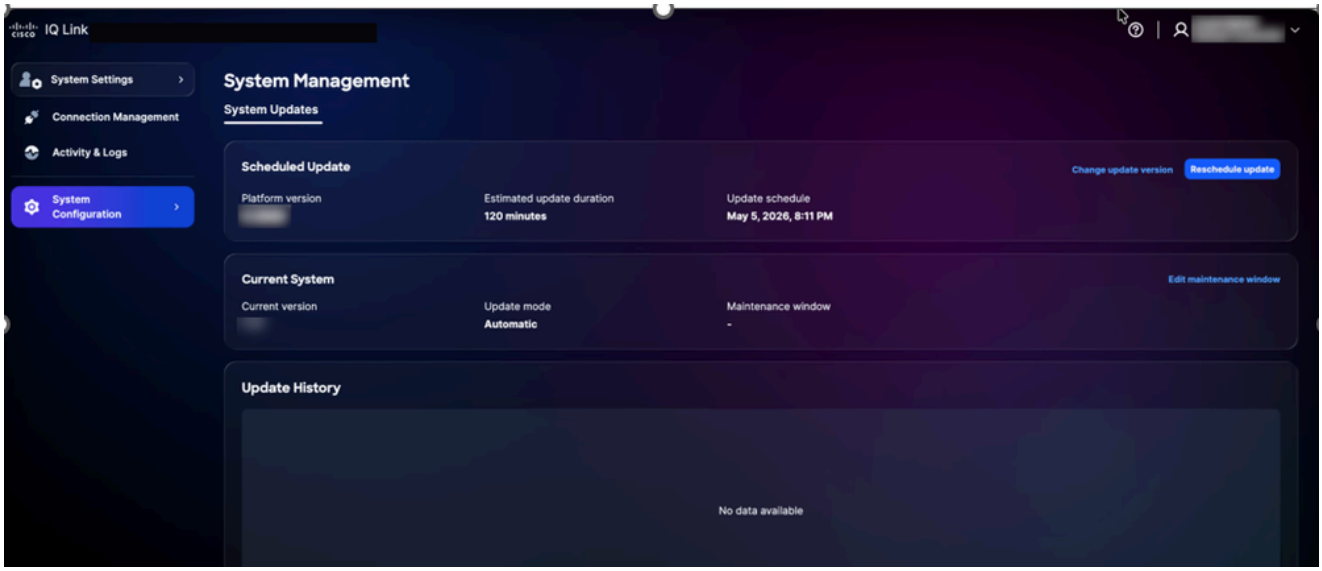
Systemverwaltung

Sie 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.

Neuplanung der Systemaktualisierung

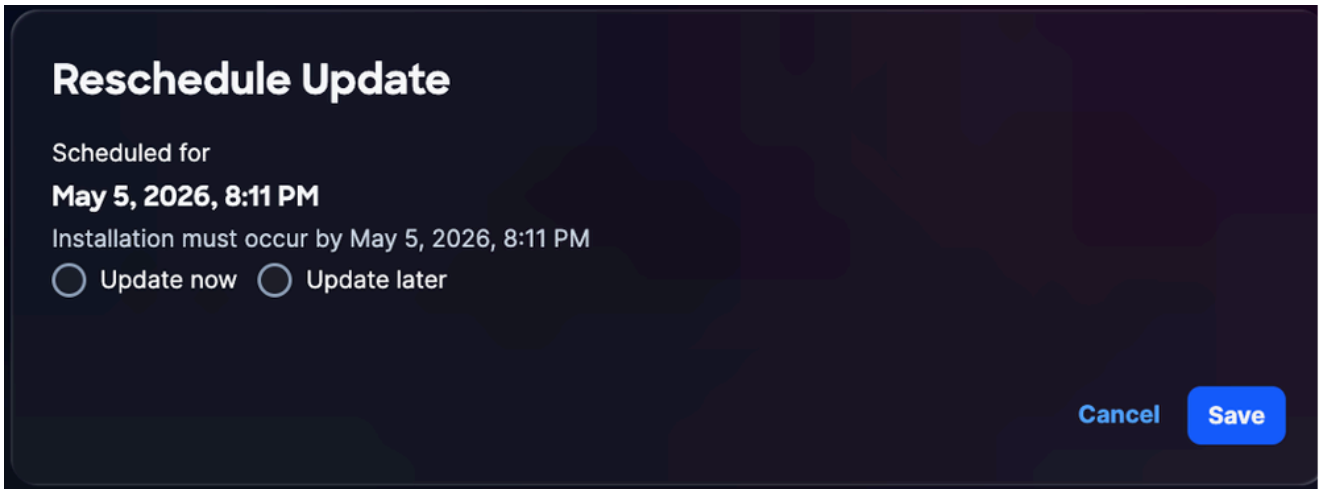
So planen Sie die Systemaktualisierung neu:

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.



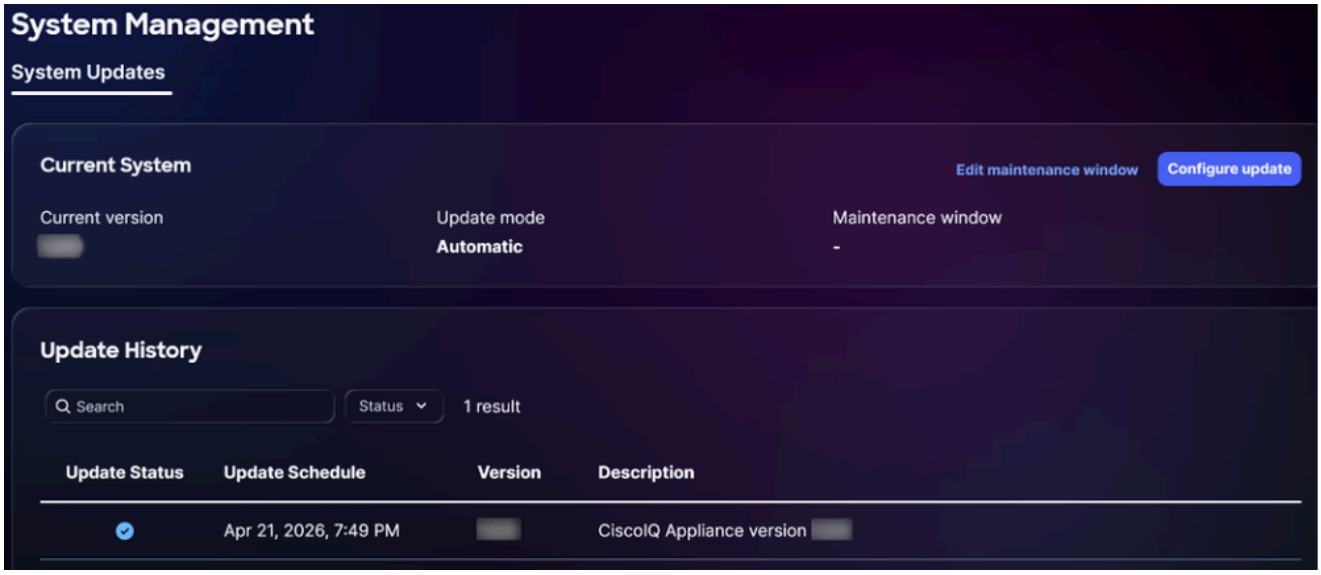
System-Upgrade

2. Klicken Sie auf Update neu planen.



Upgrade neu planen

3. Wählen Sie das Optionsfeld Jetzt aktualisieren für eine sofortige Neuplanung oder das Optionsfeld 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.

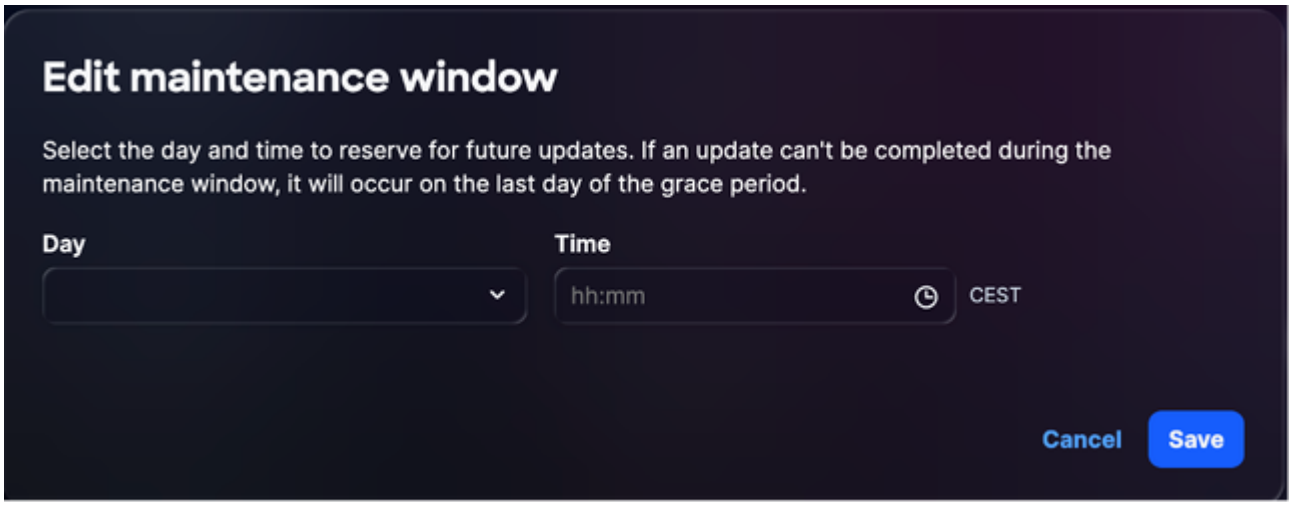


Erfolgreiches Upgrade

Bearbeiten von Systemaktualisierungsplänen

Sie können einen benutzerdefinierten Zeitplan für System-Upgrades erstellen. Wenn ein benutzerdefinierter Zeitplan konfiguriert wird, erfolgen Upgrades zu benutzerdefinierten Terminen, sofern sie innerhalb der maximalen Kulanzfrist erfolgen. So erstellen Sie einen Zeitplan für das System-Upgrade:

1. Klicken Sie im Abschnitt Aktuelles System auf der Seite Systemverwaltung auf Wartungsfenster bearbeiten.



Wartungsfenster bearbeiten

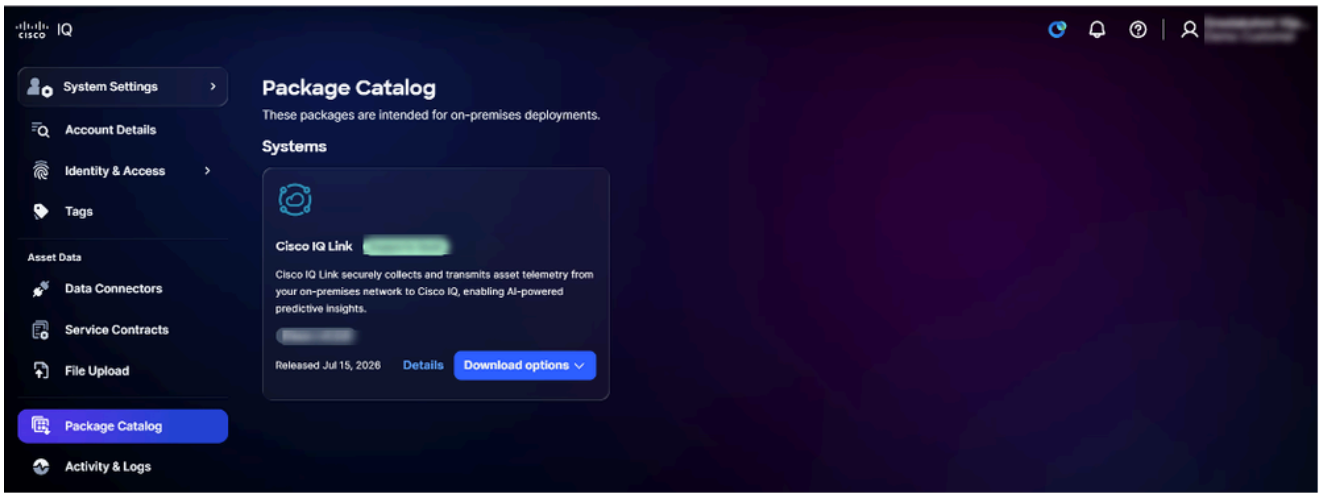
2. Wählen Sie eine Option aus den Dropdown-Listen Tag und Uhrzeit aus.
3. Klicken Sie auf Speichern. Das Wartungsfenster wurde erfolgreich geplant. Die Aktualisierung wird entsprechend dem angezeigten Zeitplan ausgelöst.

Anmerkung:
- Wenn kein Aktualisierungszeitplan konfiguriert ist, beträgt die Frist für Upgrades ohne Neustart standardmäßig zwei (2) Wochen und für Upgrades ohne Neustart vier (4) Wochen. Nach diesen Kulanzperioden müssen die Updates manuell durchgeführt werden.
- Bei einem Upgrade-Fehler führt das System bis zu zwei (2) automatische Wiederholungsversuche durch. Ein dritter Versuch ist geplant, erfordert jedoch die manuelle Initiierung.

Manuelles Aktualisieren des Systems

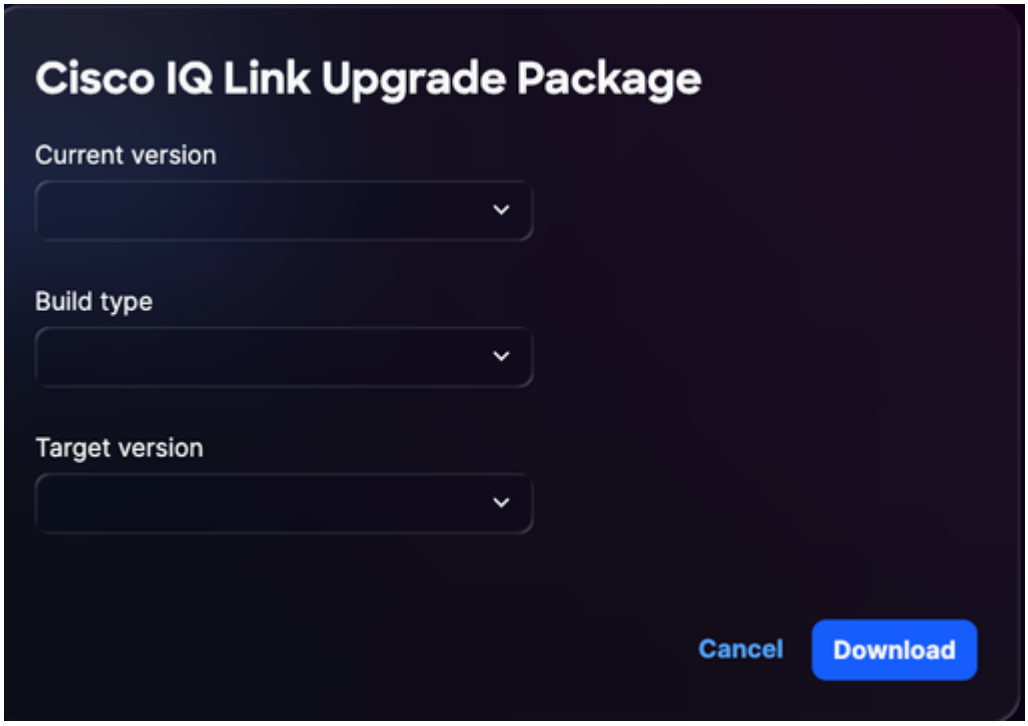
In Szenarien, in denen die automatische Verteilung über Cisco IQ SaaS entweder nicht verfügbar ist oder verzögert wird, können Sie ein System-Upgrade manuell durchführen, indem Sie das Upgrade-Paket direkt von Cisco IQ SaaS herunterladen. So aktualisieren Sie das System manuell:

1. Melden Sie sich bei Cisco IQ SaaS an, und wählen Sie Home > System Settings > Package Catalog (Startseite > Systemeinstellungen > Paketkatalog).



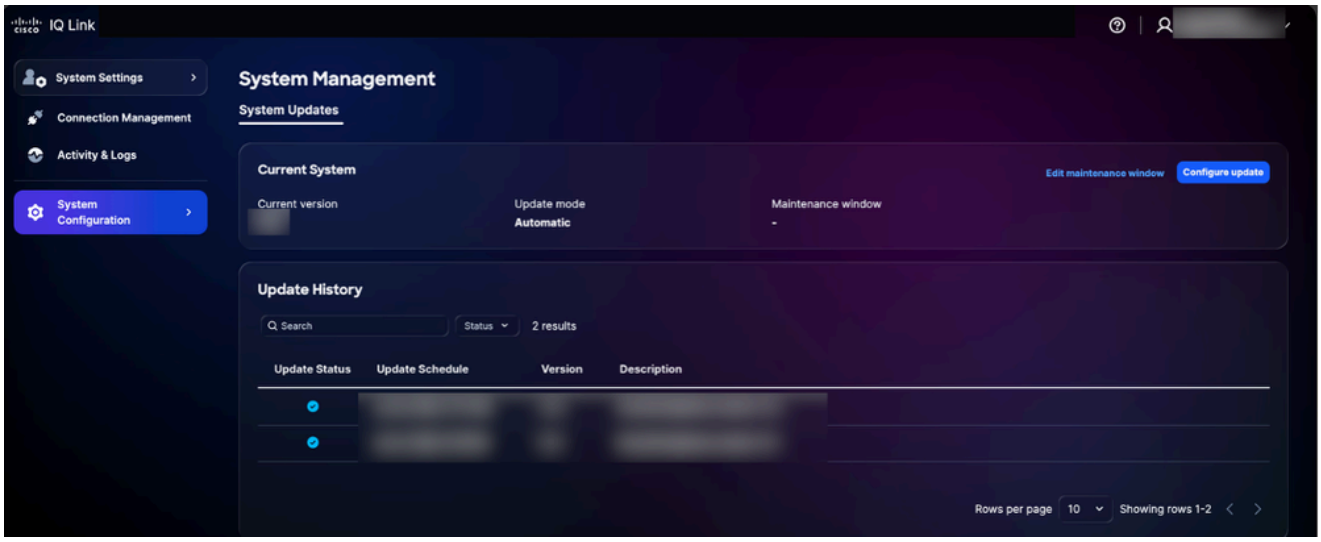
Paketkatalog

2. Klicken Sie im Abschnitt Cisco IQ Link auf Download options > Upgrade packages.



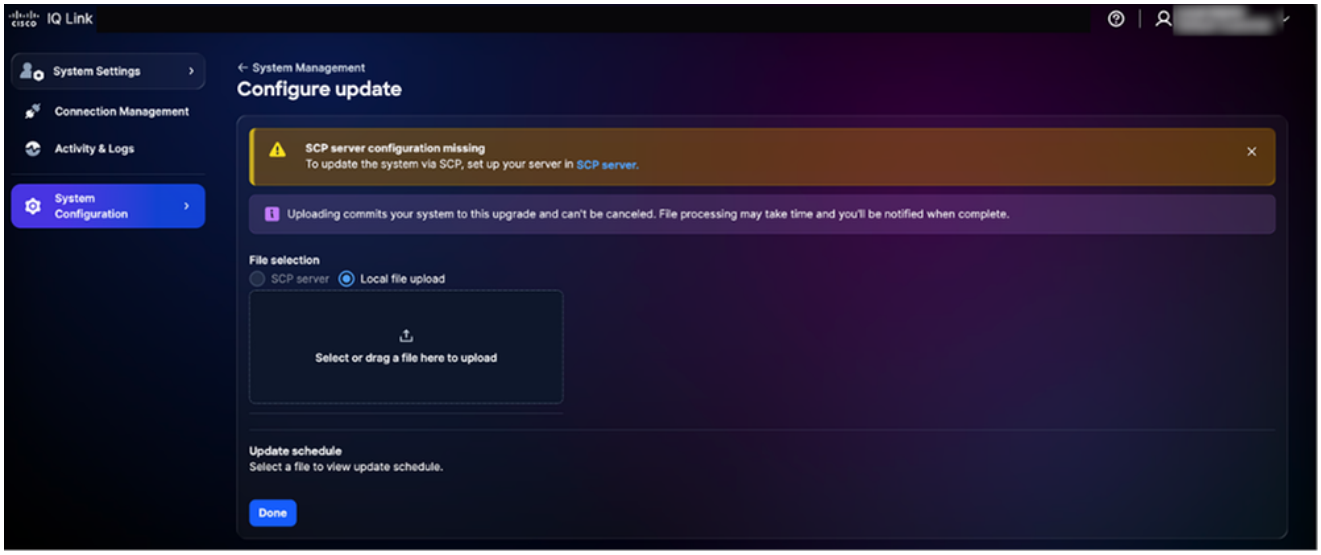
Upgrade-Paket

3. Wählen Sie die aktuelle Version aus der Dropdown-Liste aus.
4. Wählen Sie den Buildtyp aus der Dropdown-Liste aus.
5. Wählen Sie die Zielversion aus der Dropdown-Liste aus.
6. Klicken Sie auf Download (Herunterladen). Das Upgrade-Paket wird heruntergeladen.
7. Rufen Sie den Cisco IQ Link auf.
8. Wählen Sie in den Systemeinstellungen die Option Systemkonfiguration > Systemverwaltung aus.



Update konfigurieren

9. Klicken Sie auf Update konfigurieren.



Hochladen lokaler Dateien

10. Klicken Sie auf das Optionsfeld Lokaler Datei-Upload.
11. Wählen Sie die heruntergeladene Upgrade-Paketdatei aus, oder ziehen Sie sie in das Uploadfeld.
12. Klicken Sie auf Done (Fertig). Nach der erfolgreichen Aktualisierung des Systems wird eine Bestätigungsmeldung angezeigt.

Konfiguration von SSL-Zertifikaten

Ein standardmäßig selbst signiertes Zertifikat ist vorinstalliert und in Cisco IQ aktiviert. Sie 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.

Das SSL-Standardzertifikat kann nicht bearbeitet oder gelöscht werden.

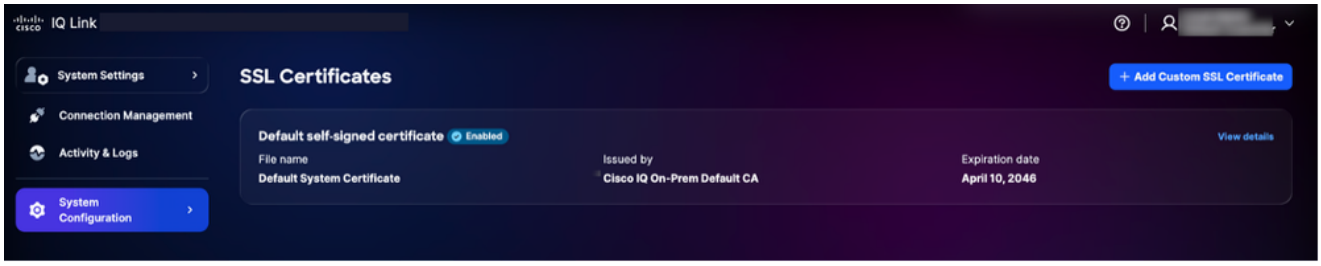
Anmerkung: Das Zertifikat muss noch mindestens 90 Tage gültig sein. Ein Zertifikat gilt als "bald abgelaufen", wenn es weniger als 90 Tage bis zum Ablauf hat.

Nachdem Sie ein SSL-Zertifikat hinzugefügt, bearbeitet oder gelöscht haben, müssen Sie das neue SSL-Zertifikat hochladen, wie in Single Logout Configuration 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.

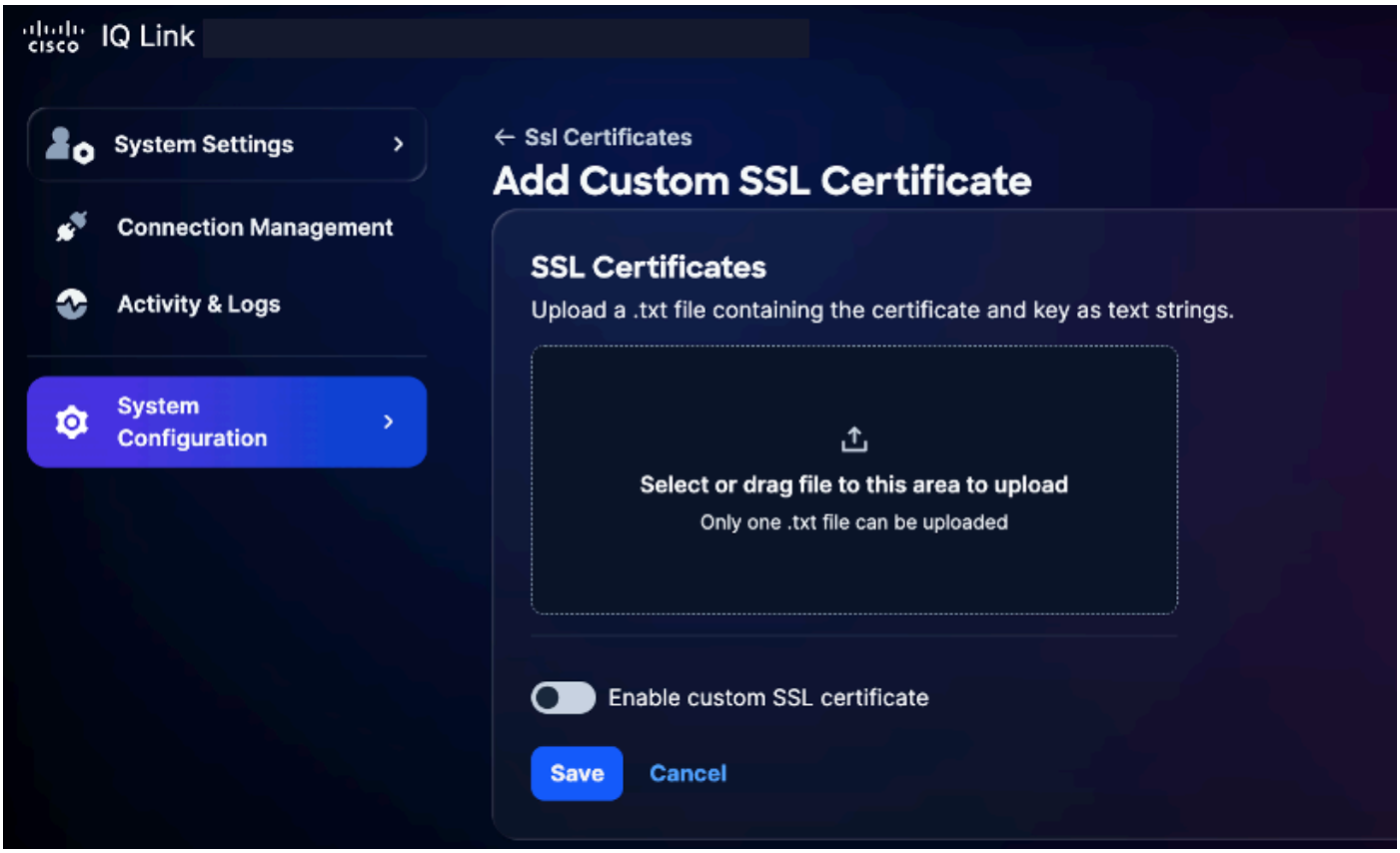


Hinzufügen eines SSL-Zertifikats

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 Textstrings enthält.
- Es kann jeweils nur eine TXT-Datei hochgeladen werden.
- Die Datei muss sowohl das Zertifikat als auch den privaten Schlüssel enthalten

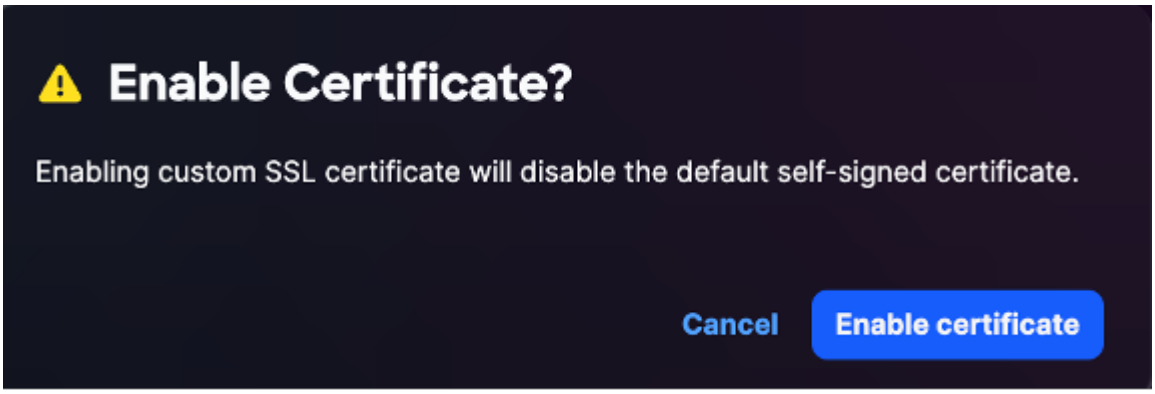
---



SSL-Zertifikat 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.



SSL-Zertifikat bearbeiten

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

5. Klicken Sie auf Zertifikat aktivieren.

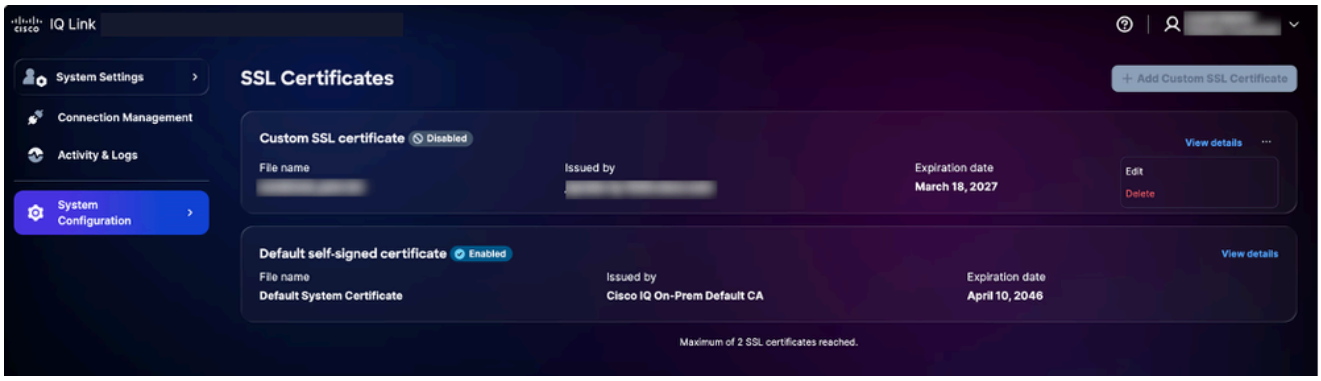
6. Klicken Sie auf Speichern.

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

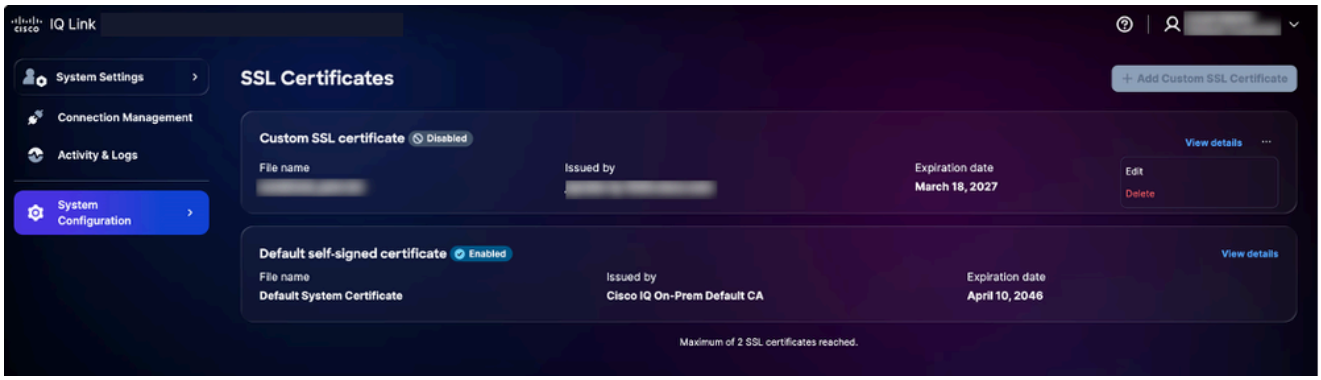
2. Wählen Sie das Symbol Weitere Optionen > Bearbeiten aus. Die Seite SSL-Zertifikat bearbeiten wird angezeigt.
3. Bearbeiten Sie die Zertifikatdetails nach Bedarf.
4. Klicken Sie auf Speichern.

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 benutzerdefinierten 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

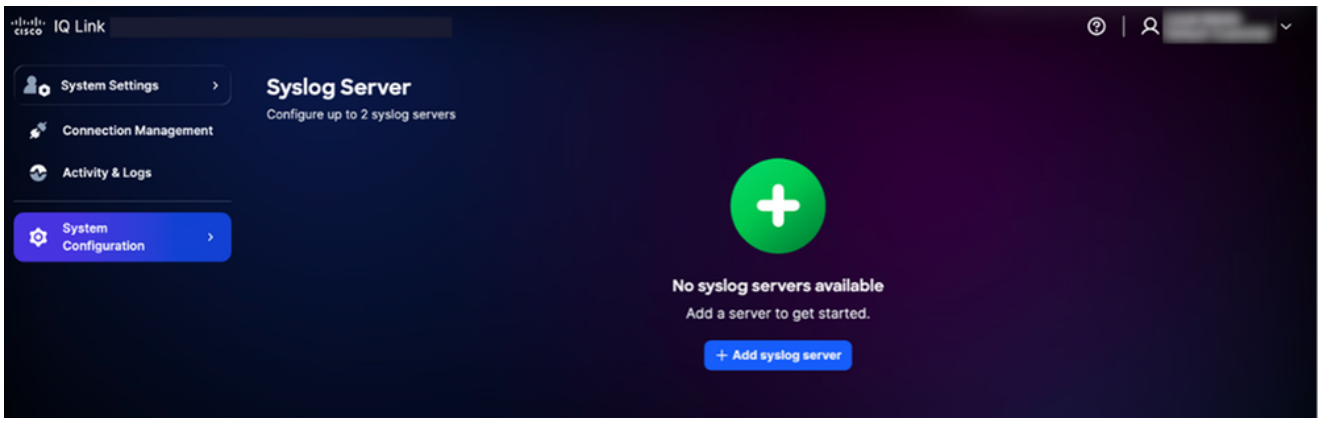
Benutzer mit der Kontoadministratorrolle können externe Syslog-Server für den Export von Systemprotokollen konfigurieren. Es können bis zu zwei (2) Syslog-Server konfiguriert werden.

Anmerkung: Der Syslog-Server muss als IP-Adresse und nicht als FQDN angegeben werden.

Hinzufügen von Syslog-Servern

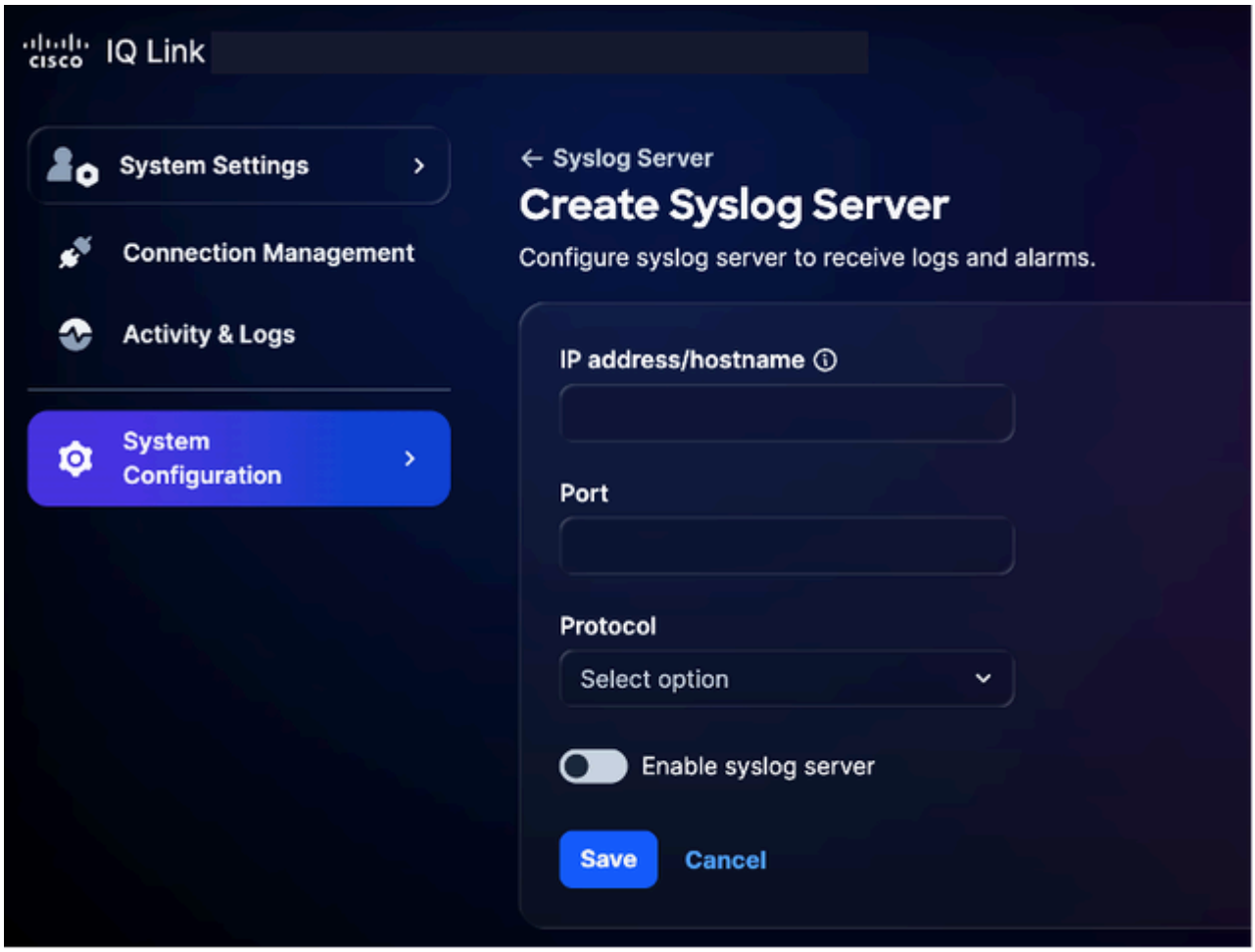
Syslog-Server hinzufügen:

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

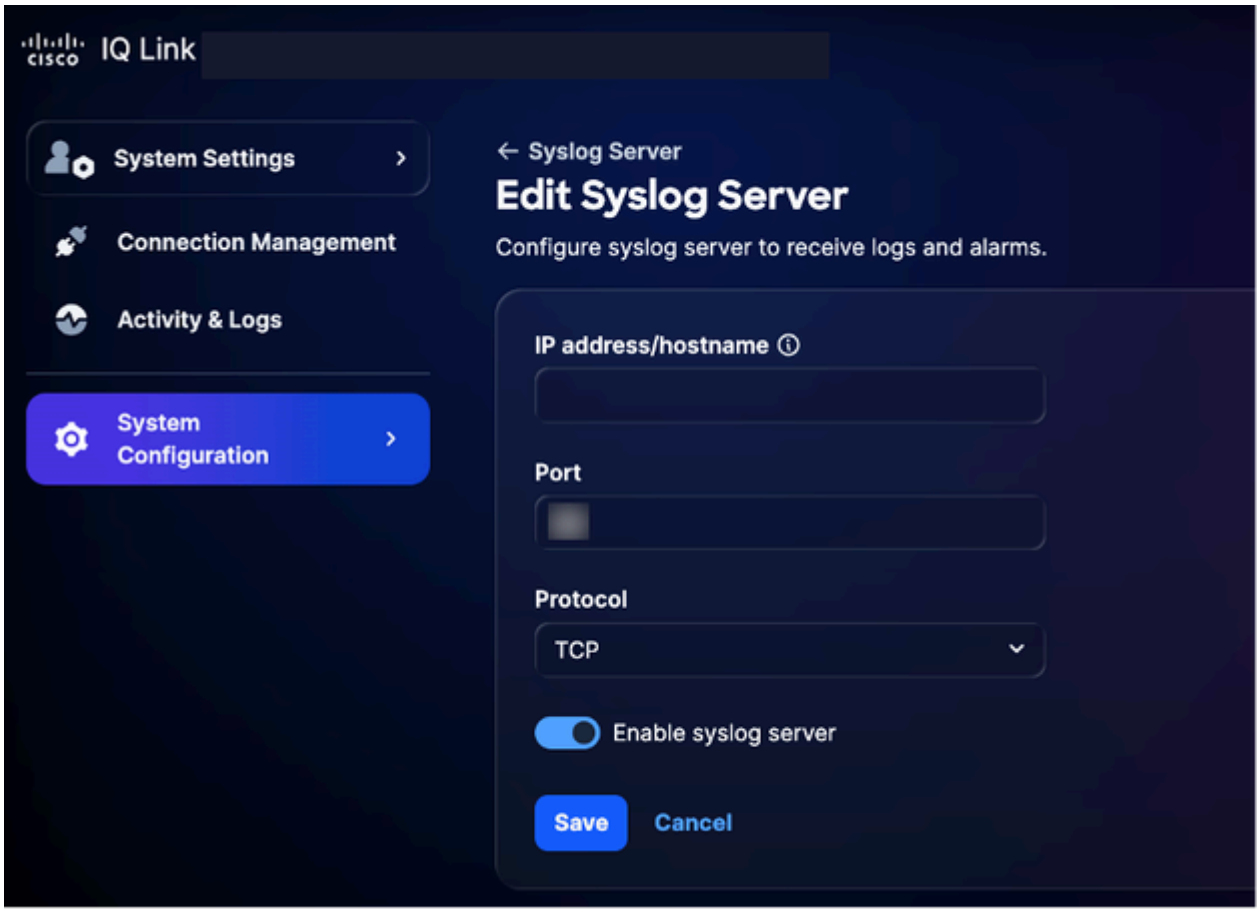
3. Geben Sie die IP-Adresse/den Hostnamen ein.
4. Geben Sie eine Port-Nummer ein.
5. Wählen Sie das entsprechende Protokoll aus der Dropdown-Liste "Protocol" (Protokoll) aus (z. B. UDP oder TCP).
6. Aktivieren Sie die Umschaltfläche Syslog-Server aktivieren.
7. Klicken Sie auf Speichern. Es wird eine Bestätigung angezeigt, und der neu hinzugefügte Syslog-Server wird auf der Startseite des Syslog-Servers 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.



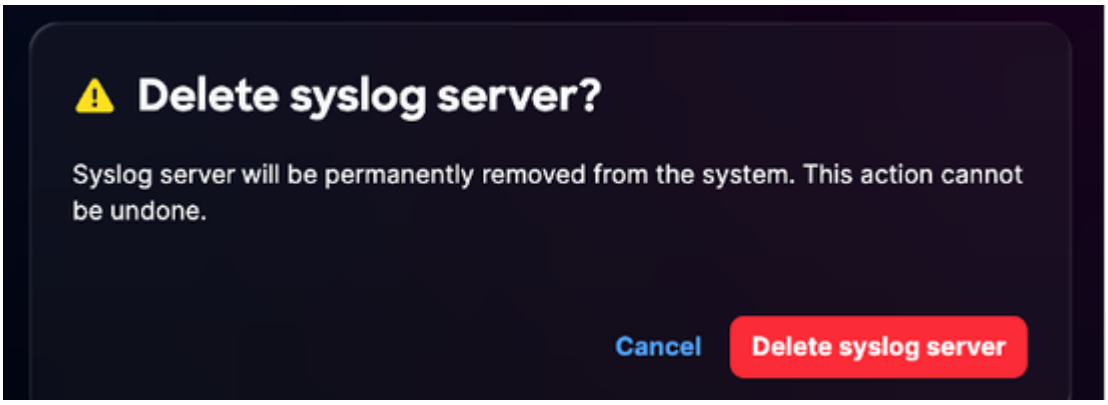
Syslog-Server bearbeiten

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.

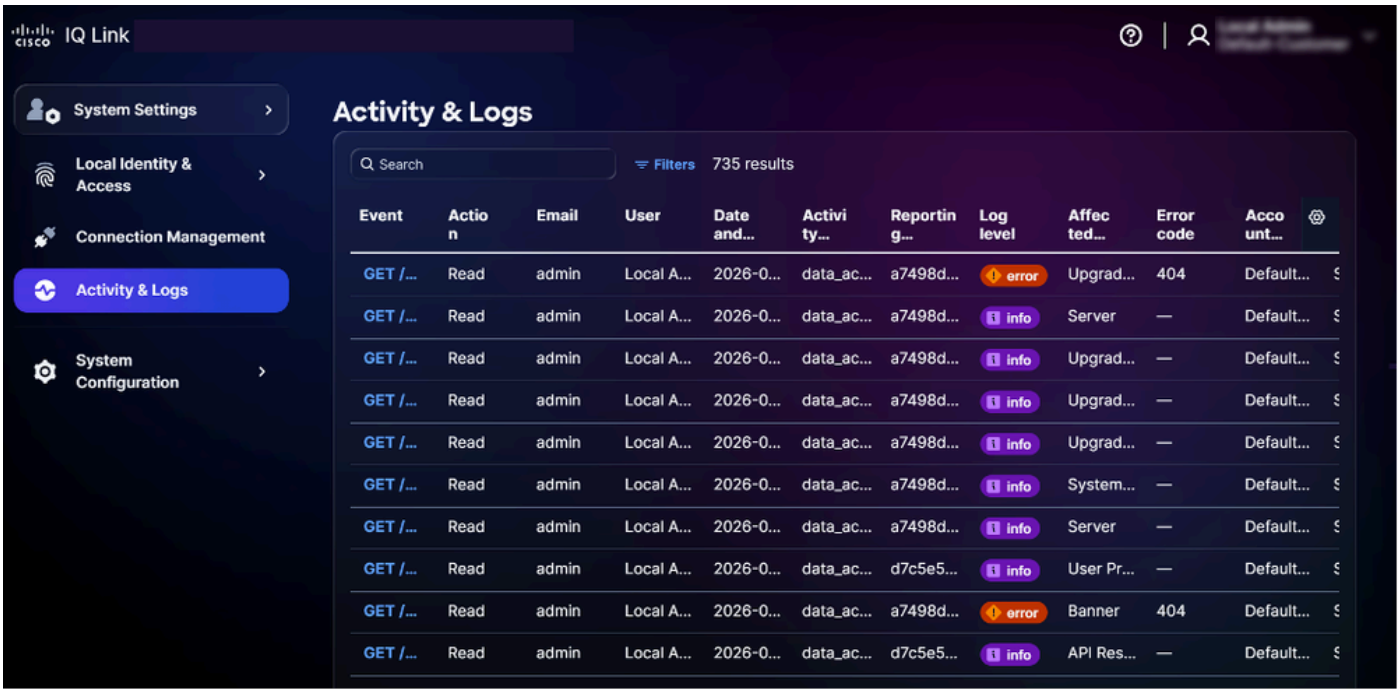


Bestätigung

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 Kontoadministratoren Benutzeraktivitäten nachverfolgen und die Transparenz aufrechterhalten können.



Aktivität und Protokolle

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

Aktivität und Protokolle:

- Unterstützt Filter, Paginierungs- und Suchfunktionen, die das Auffinden und Verwalten von Informationen vereinfachen
- Protokolliert alle API-Vorgänge auf Gateway-Ebene

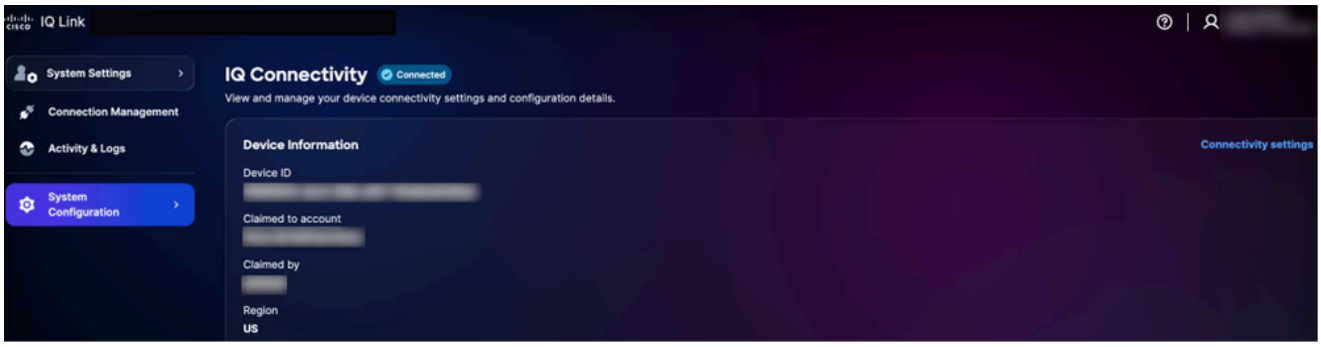
Folgende Filteroptionen sind verfügbar:

- 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

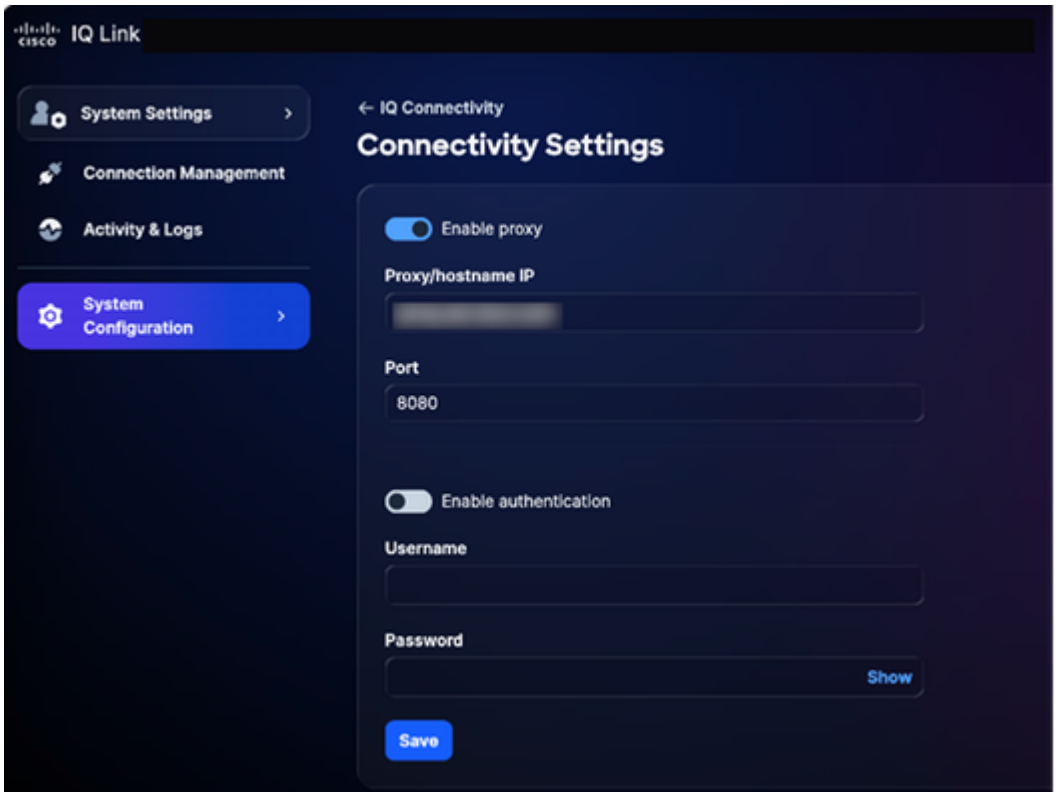
So zeigen Sie Verbindungseinstellungen und Konfigurationsdetails für Geräte an und verwalten diese:

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 standortbasierte Lösung zur Erfassung von Netzwerkdaten, die einen umfassenden Überblick über Ihre Infrastruktur ermöglicht. Es erfasst Daten über Catalyst Center und Direct Connection. Es vereinfacht das Management der Netzwerkauthentifizierung und Geräteerkennung. Nachfolgend wird die Konfiguration der Datenerfassung zusammengefasst:

- Erstellen von Anmeldeinformationssätzen: Richten Sie die Authentifizierungsprotokolle (z. B. Simple Network Management Protocol (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.
- 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

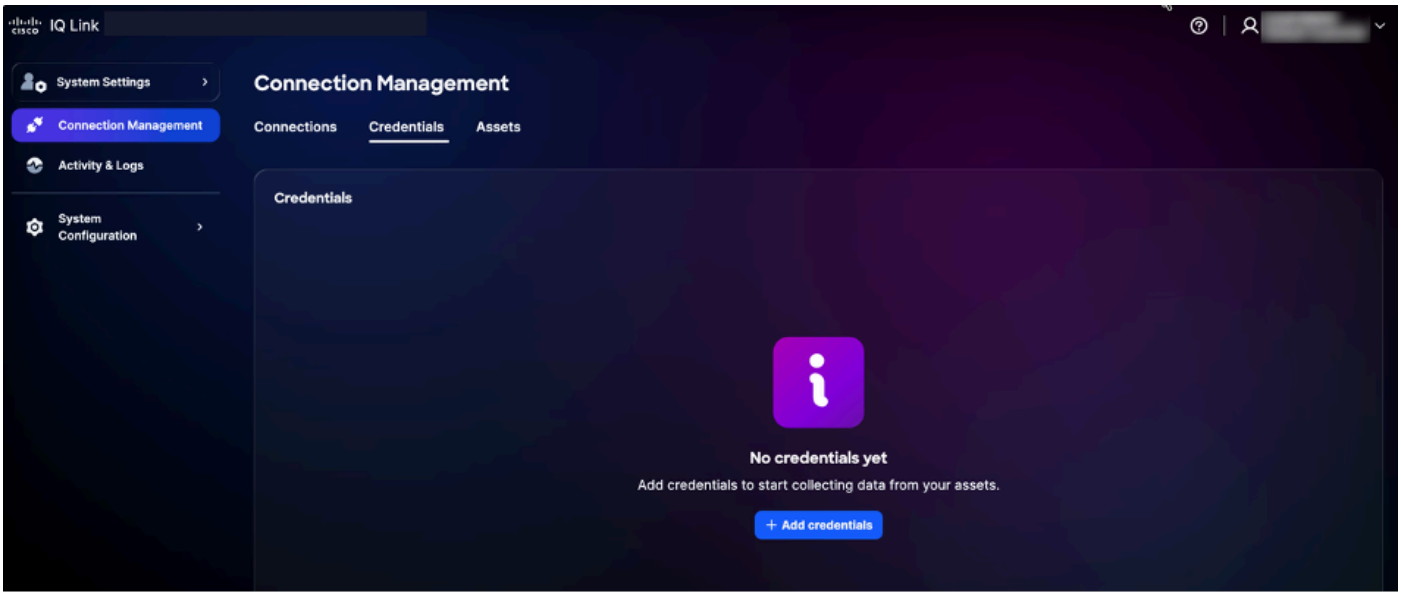
die Konfiguration mit wachsendem Netzwerk immer fehlerfrei abläuft.

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

Hinzufügen von Anmeldeinformationen

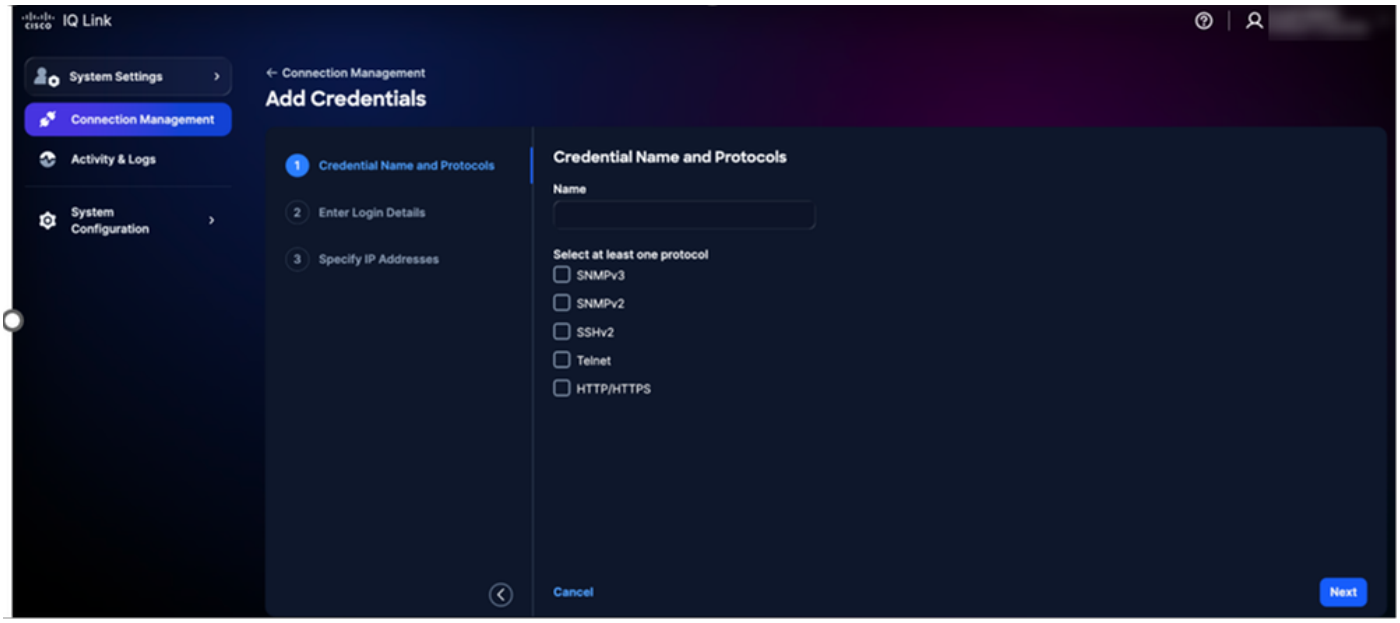
Sie müssen zunächst Anmeldeinformationen hinzufügen, um die Datensammlung durchzuführen. So fügen Sie Anmeldeinformationen hinzu:

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.

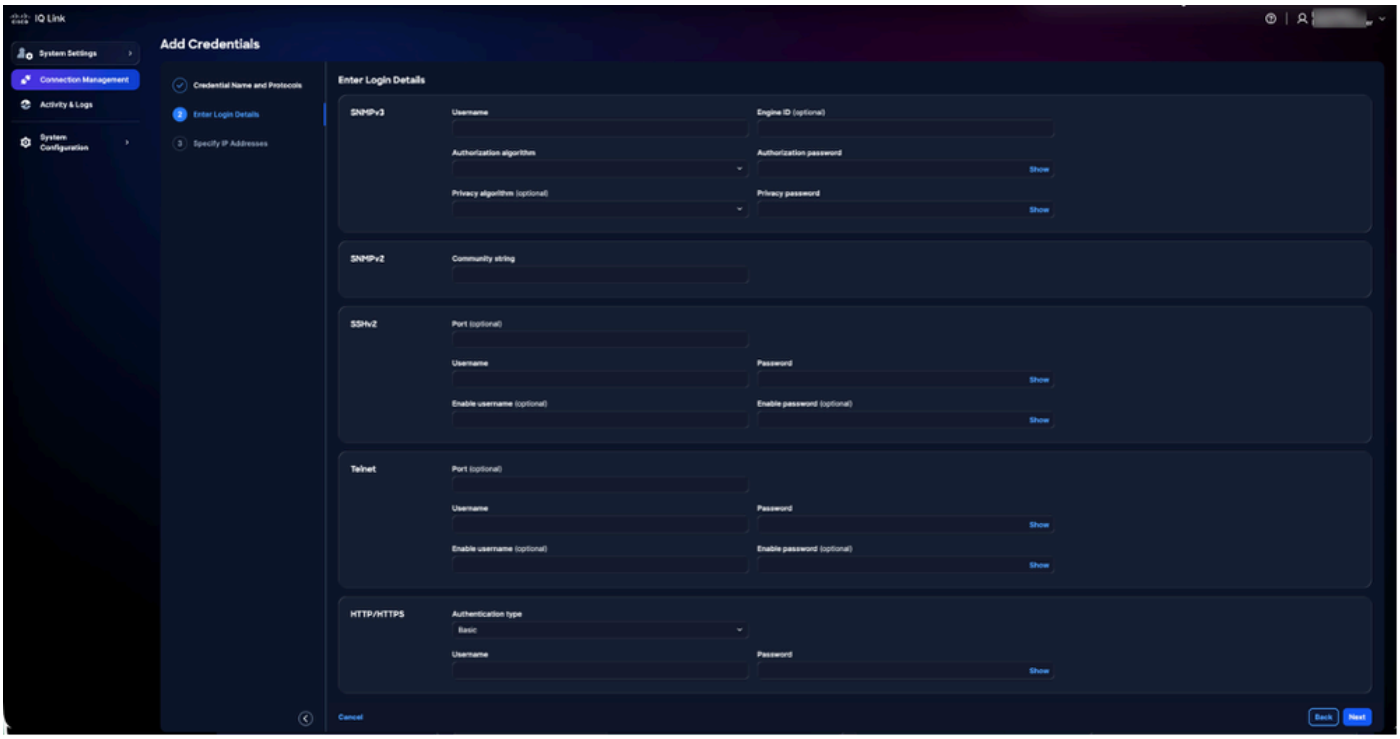


Anmeldeinformationen hinzufügen

4. Geben Sie einen Namen ein.

5. Aktivieren Sie alle Kontrollkästchen für das entsprechende Protokoll.

6. Klicken Sie auf Weiter.

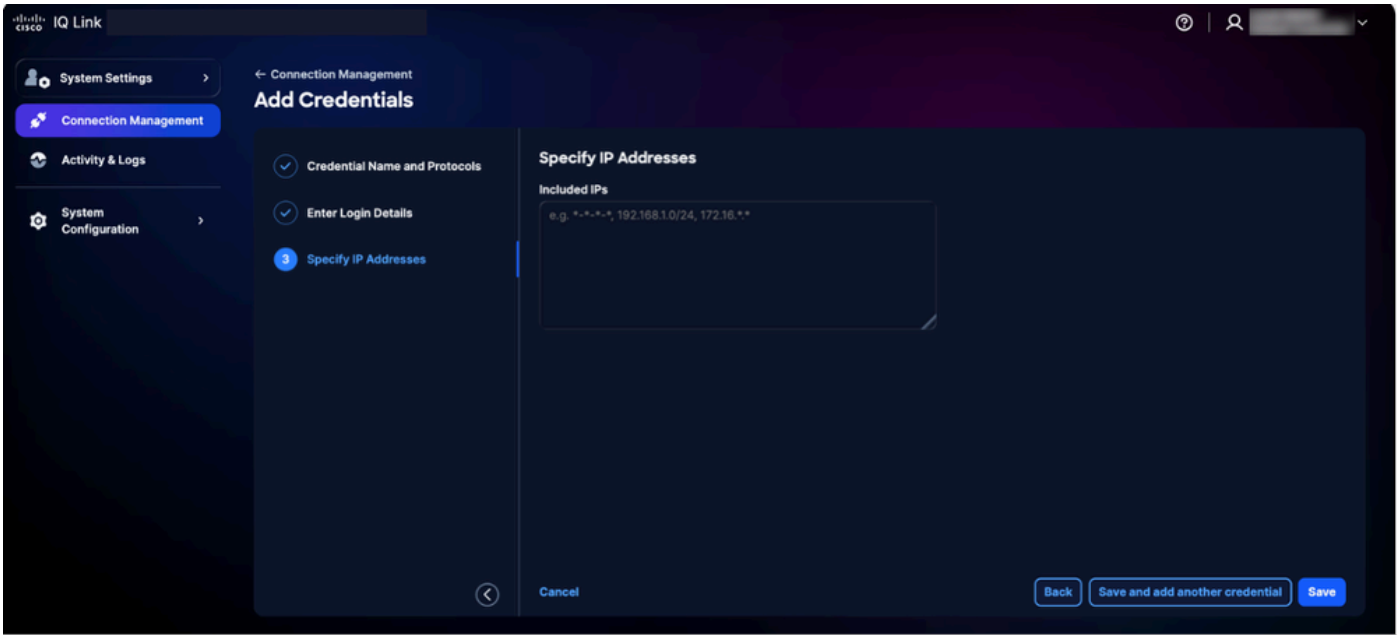


Anmeldeinformationsdetails hinzufügen

Anmerkung: Für das obige Bild wird die Ansicht dargestellt, 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 Weiter.

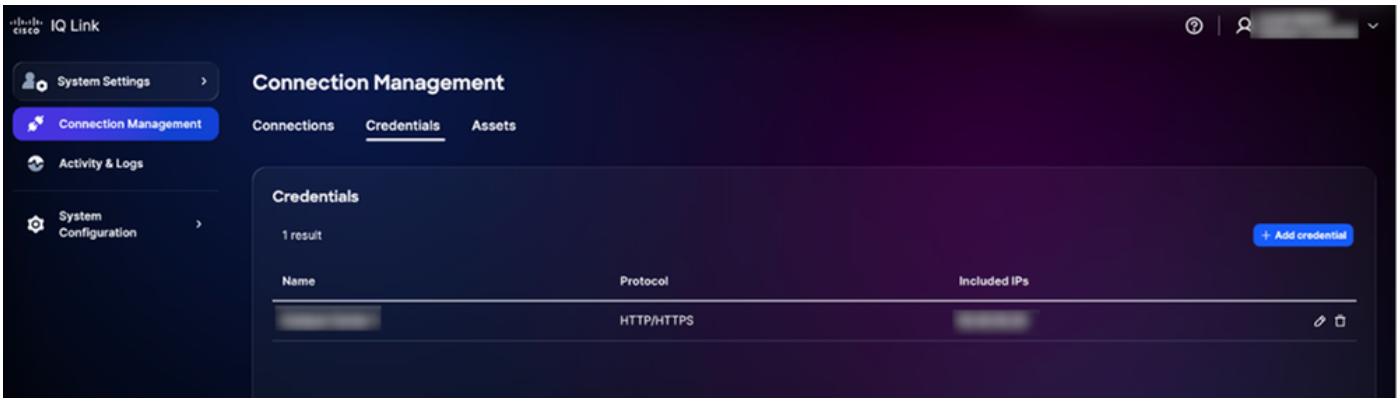


IP-Adressen angeben

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: Priorität hängt von der Anzahl der nachlaufenden Sterne; 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:

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.

Tabelle 13: 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)

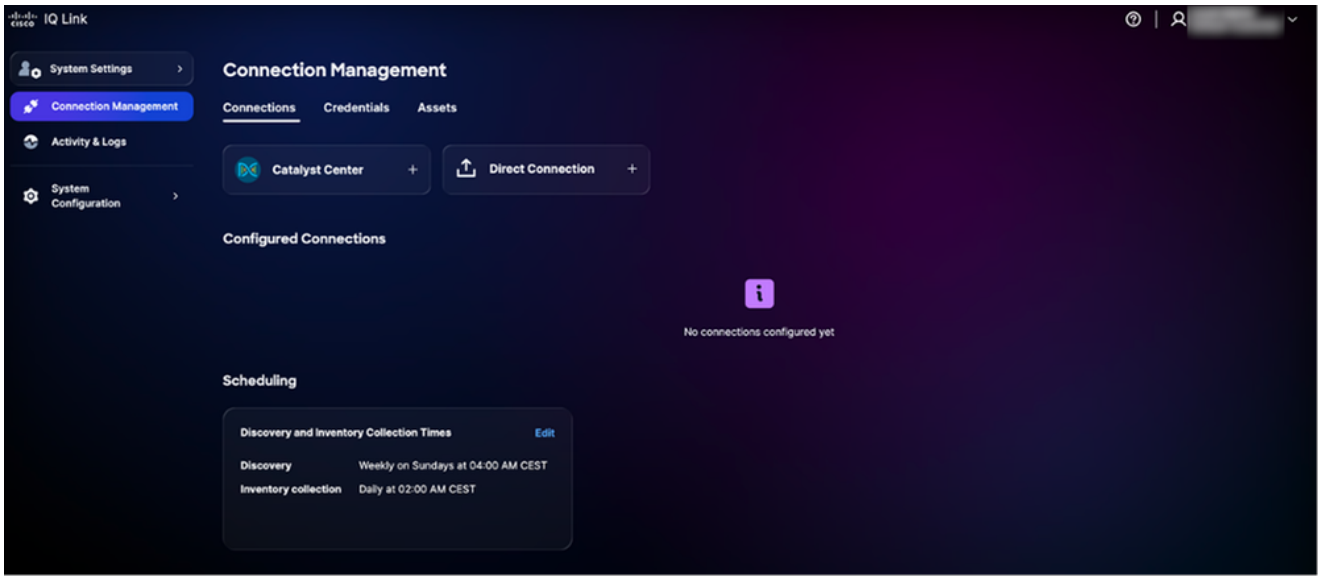
Anmerkung: Fällt ein Gerät in mehrere sich überschneidende Kategorien, wählt das System immer den Berechtigungssatz mit der höchsten Spezifität aus (d. h. mit den wenigsten Platzhaltern am Ende).

Datenerfassung mit Catalyst Center

Sie können bis zu 20 Catalyst Center (nicht-Cluster) für jede Instanz von Cisco IQ Link anschließen.

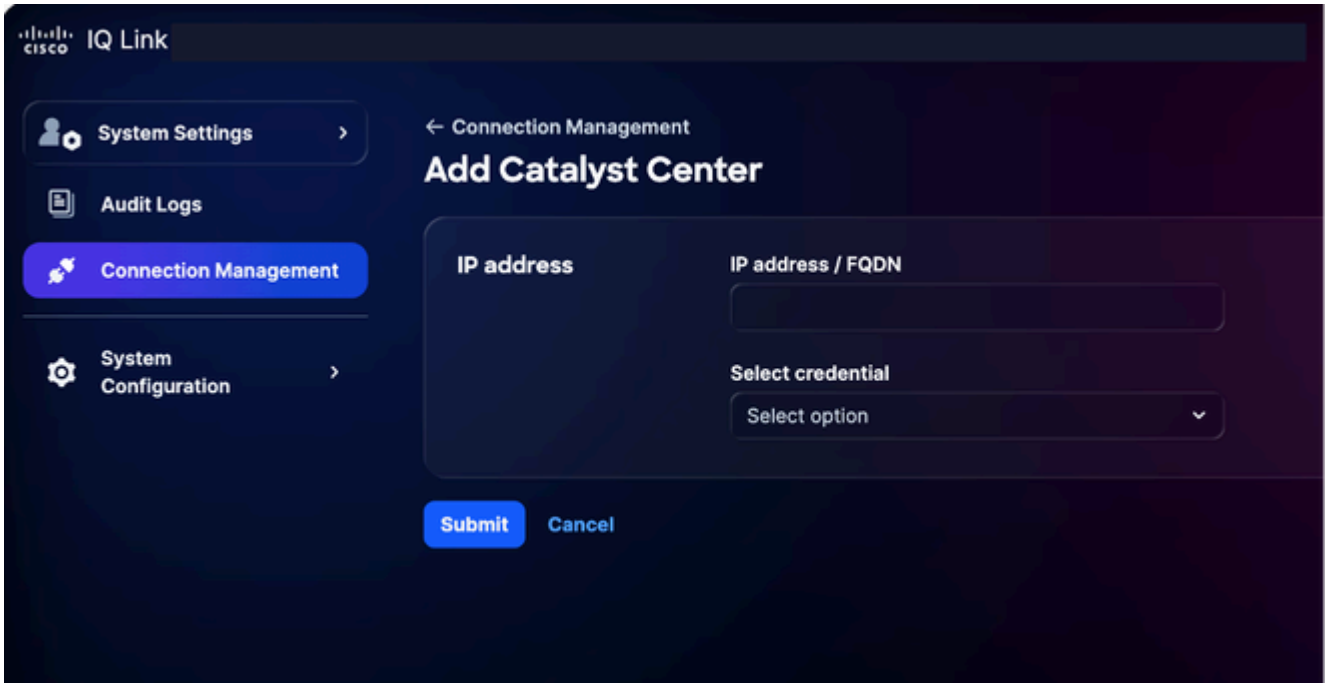
Datenerfassung mit Catalyst Center:

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



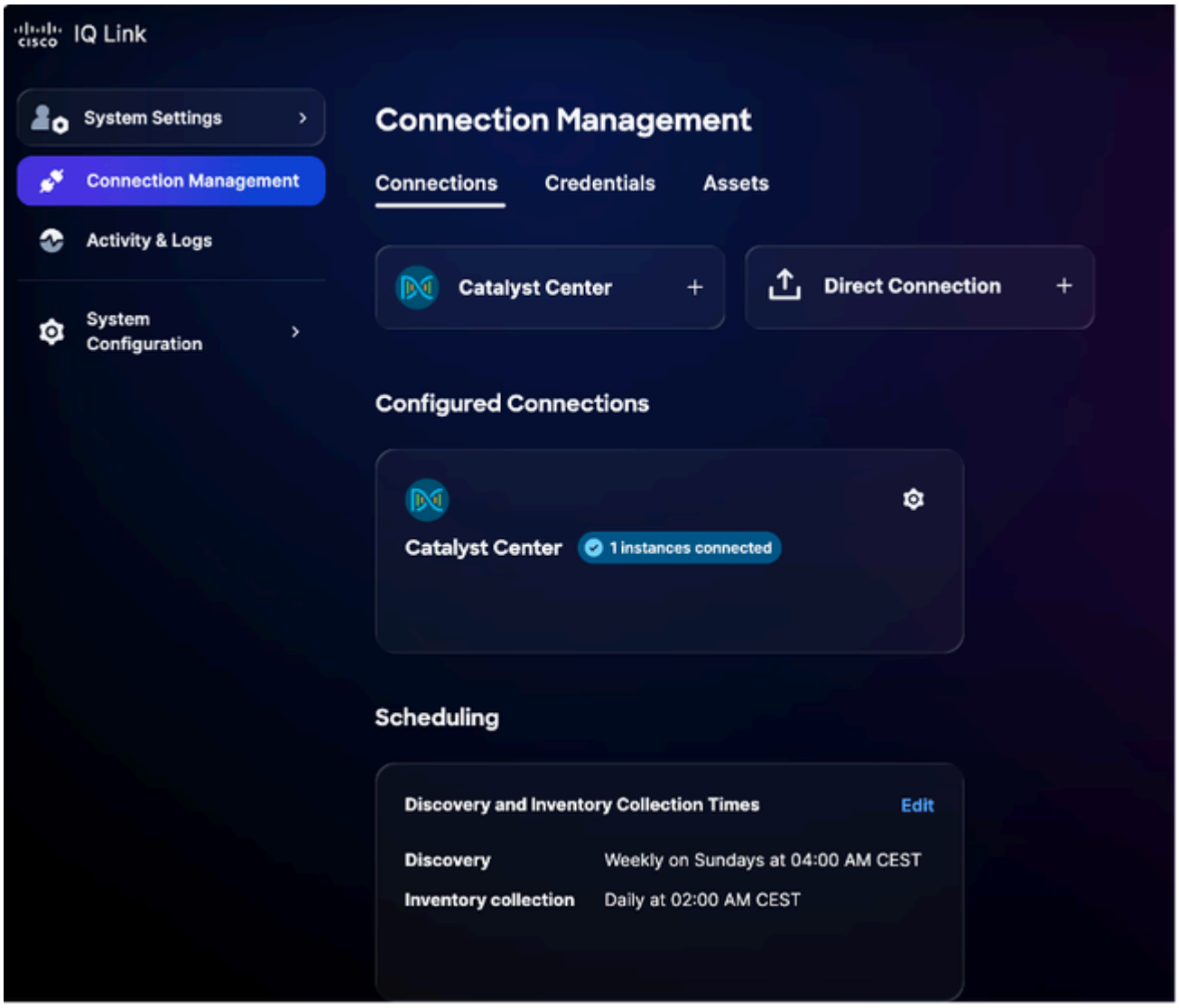
Verbindungsmanagement

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

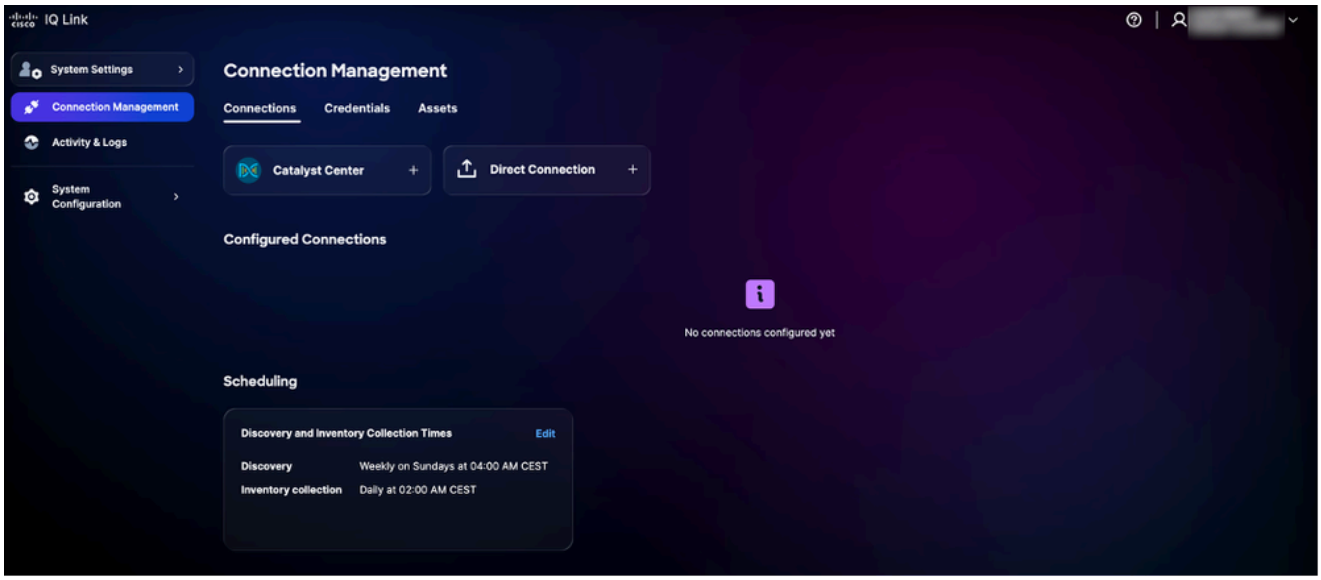
6. Planen einer Sammlung. Weitere Informationen finden Sie unter Planen.

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

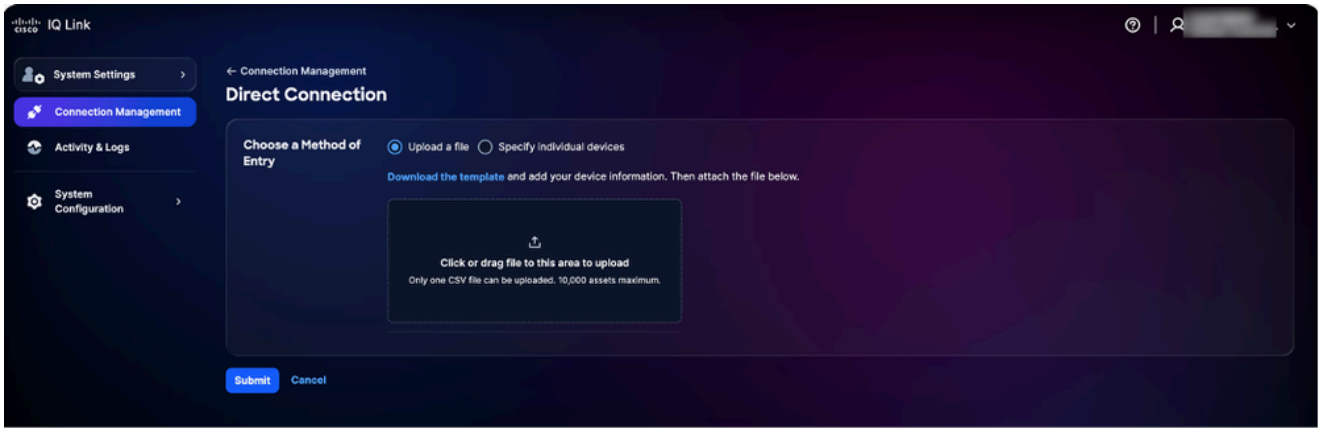
So fügen Sie Geräte für Direktverbindungen hinzu:

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



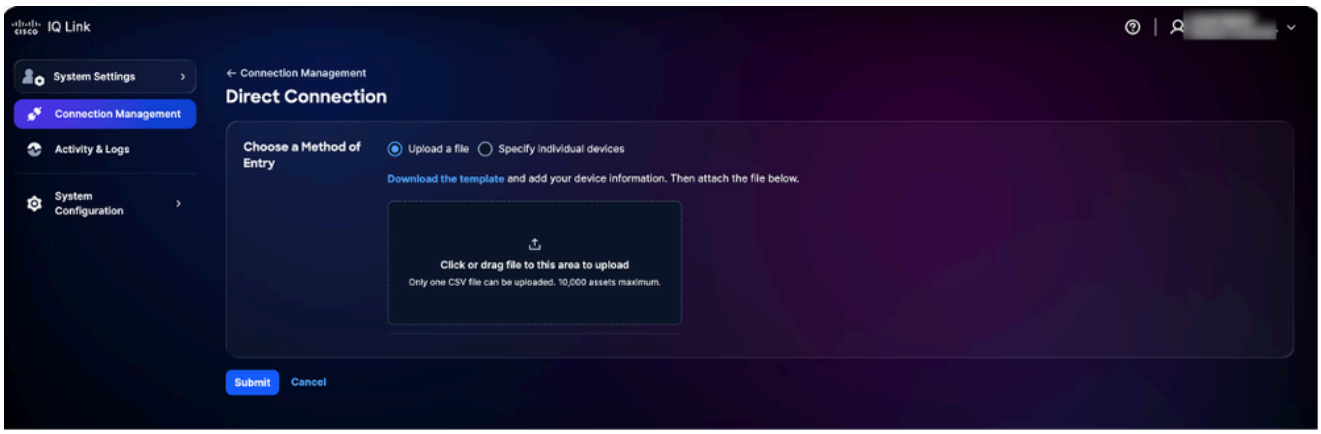
Verbindungsmanagement

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



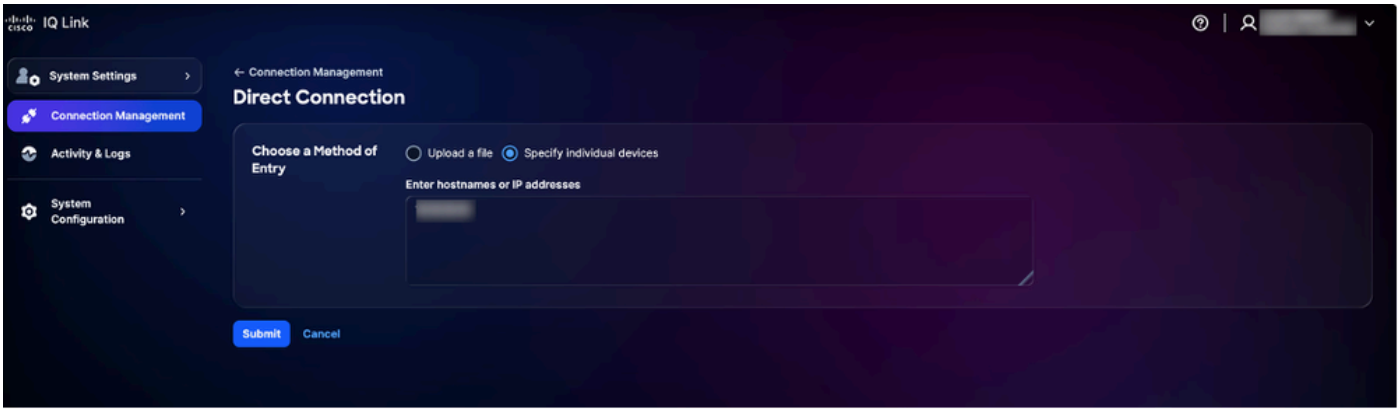
Datei hochladen

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.

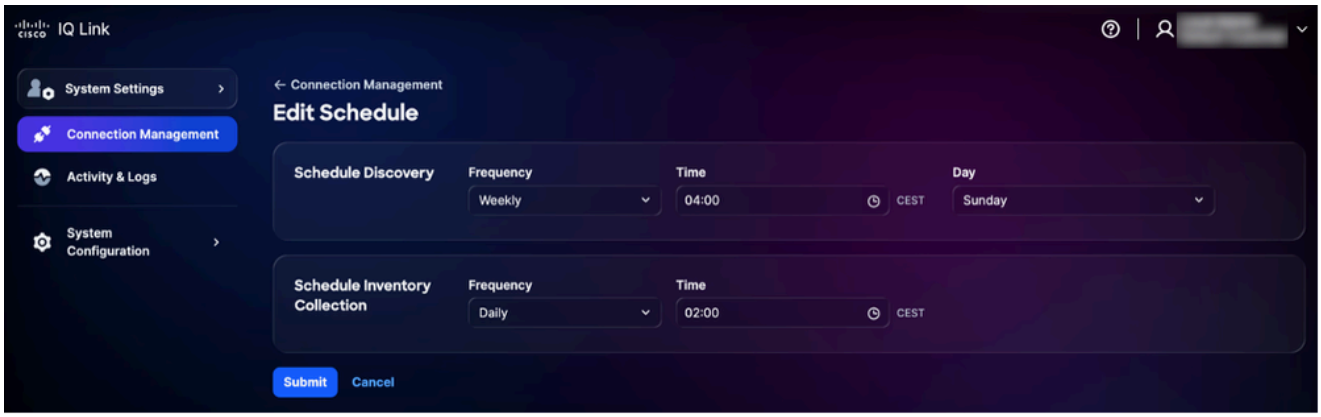
4. Planen Sie eine Sammlung. Weitere Informationen finden Sie unter Planen.

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

Mithilfe der Zeitplanung 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

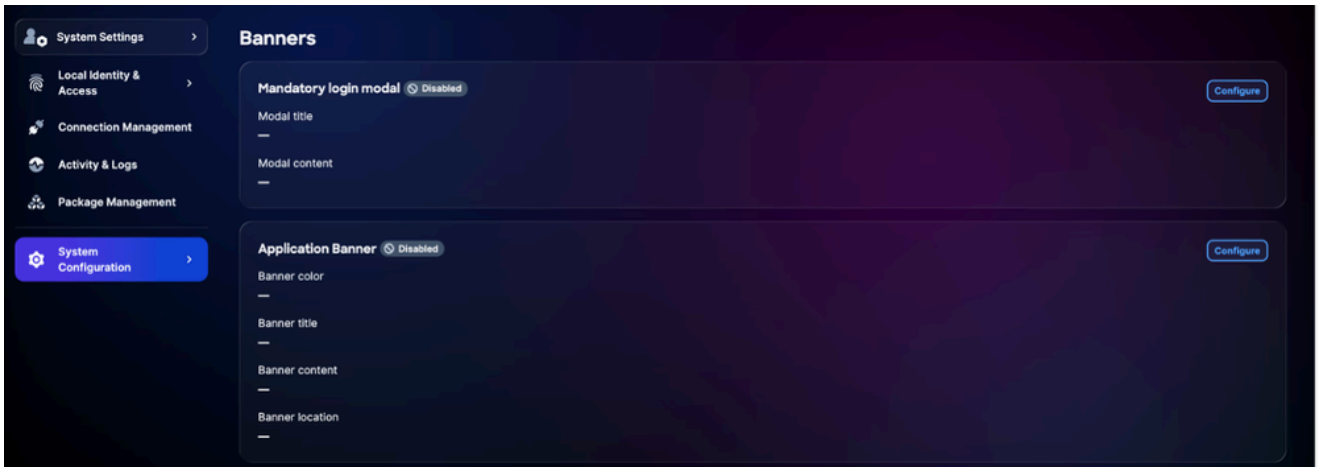
Kontoadministratoren können systemweite Banner konfigurieren, um Sicherheits- und Compliance-Standards zu erfüllen.

- Obligatorischer Anmeldemodus: Sie müssen das erforderliche Banner bestätigen, bevor Sie zum Anmeldebildschirm wechseln.
- Anwendungs-Banner: Hierbei handelt es sich um angepasste Banner, die nach der erfolgreichen Authentifizierung in der gesamten Anwendung angezeigt werden.

Konfigurieren von Modal-Bannern für obligatorische Anmeldung

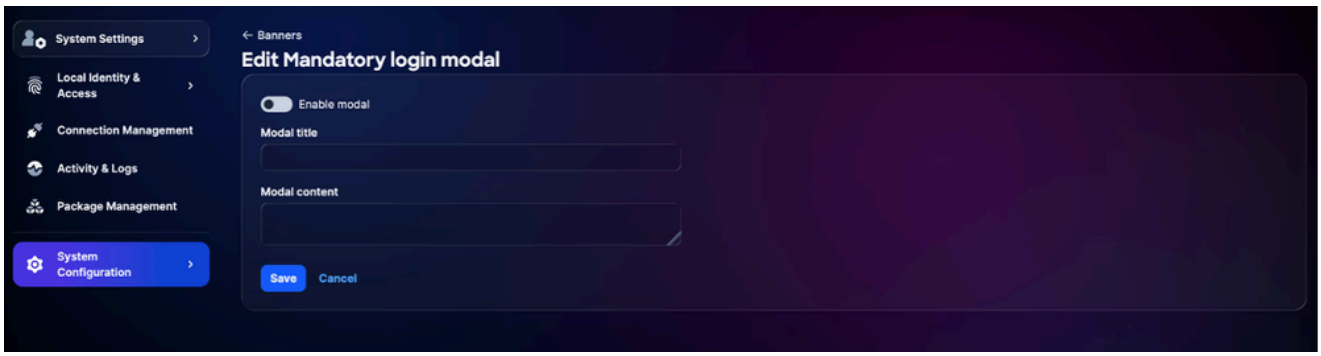
So konfigurieren Sie ein obligatorisches Banner:

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



Pflichtbanner konfigurieren

2. Klicken Sie im Modus für obligatorische Anmeldung auf Konfigurieren. Die Seite "Obligatorische Anmeldung bearbeiten" wird angezeigt.



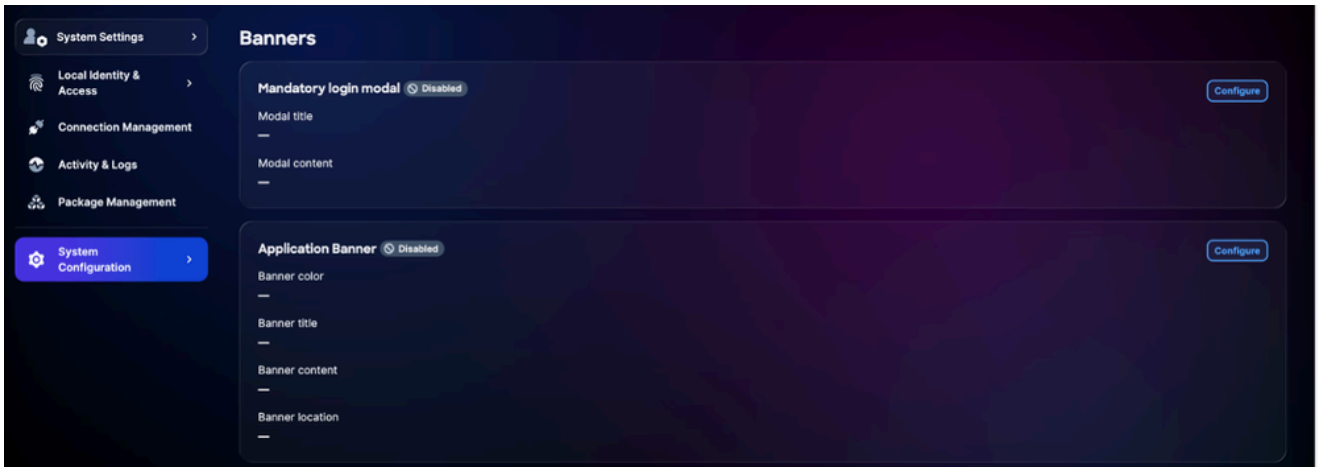
Bearbeiten Modales Banner für obligatorische Anmeldung

3. Klicken Sie auf den Umschalter, um den Banner zu aktivieren oder zu deaktivieren.
4. Geben Sie den Titel Modal (Modal) ein.
5. Geben Sie den Modal-Inhalt ein.
6. Klicken Sie auf Speichern. Der Modus für die obligatorische Anmeldung wird gespeichert.

Konfigurieren von Anwendungsbannern

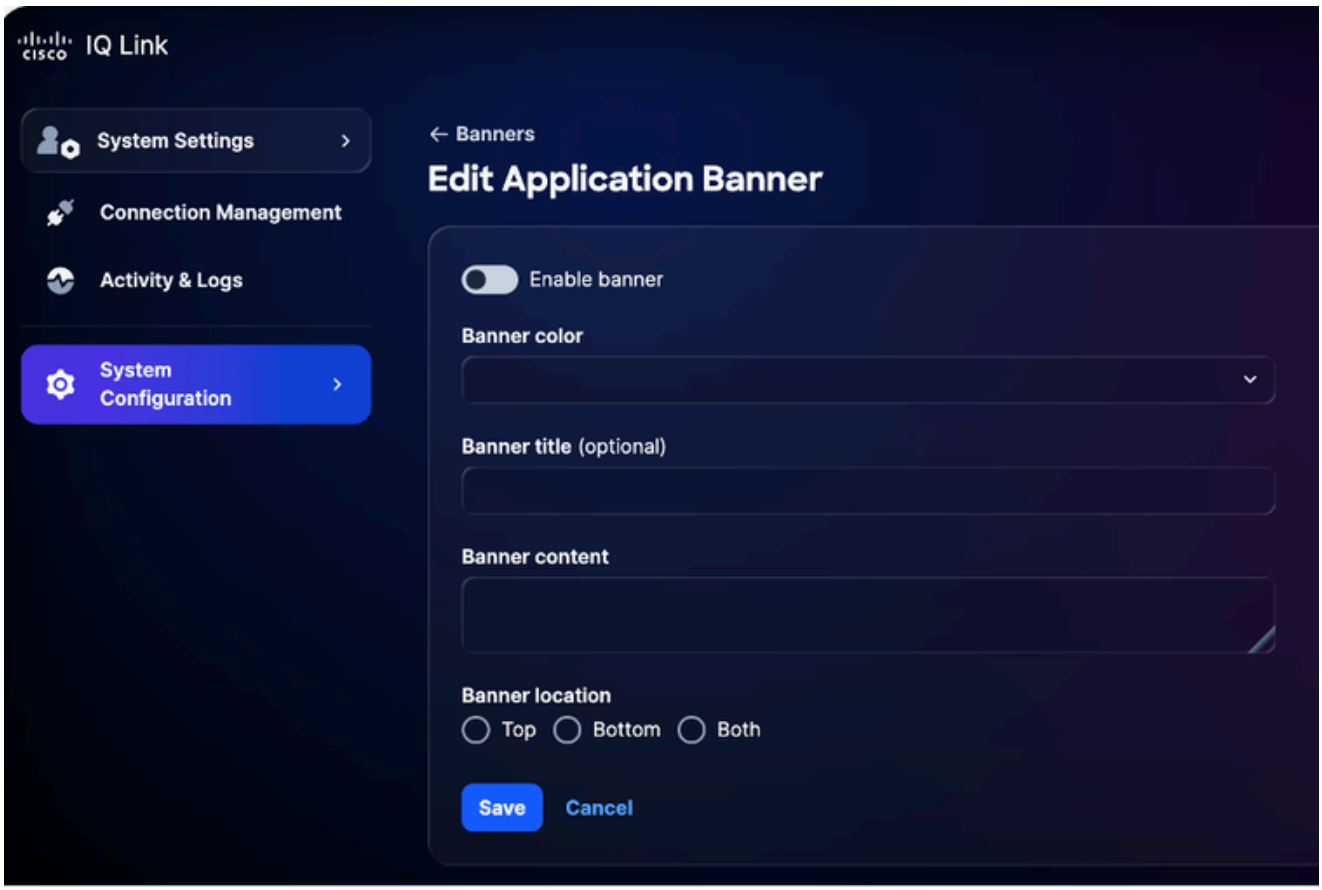
So konfigurieren Sie ein Anwendungsbanner:

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



Banner konfigurieren

2. Klicken Sie auf In Anwendungs-Banner 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.

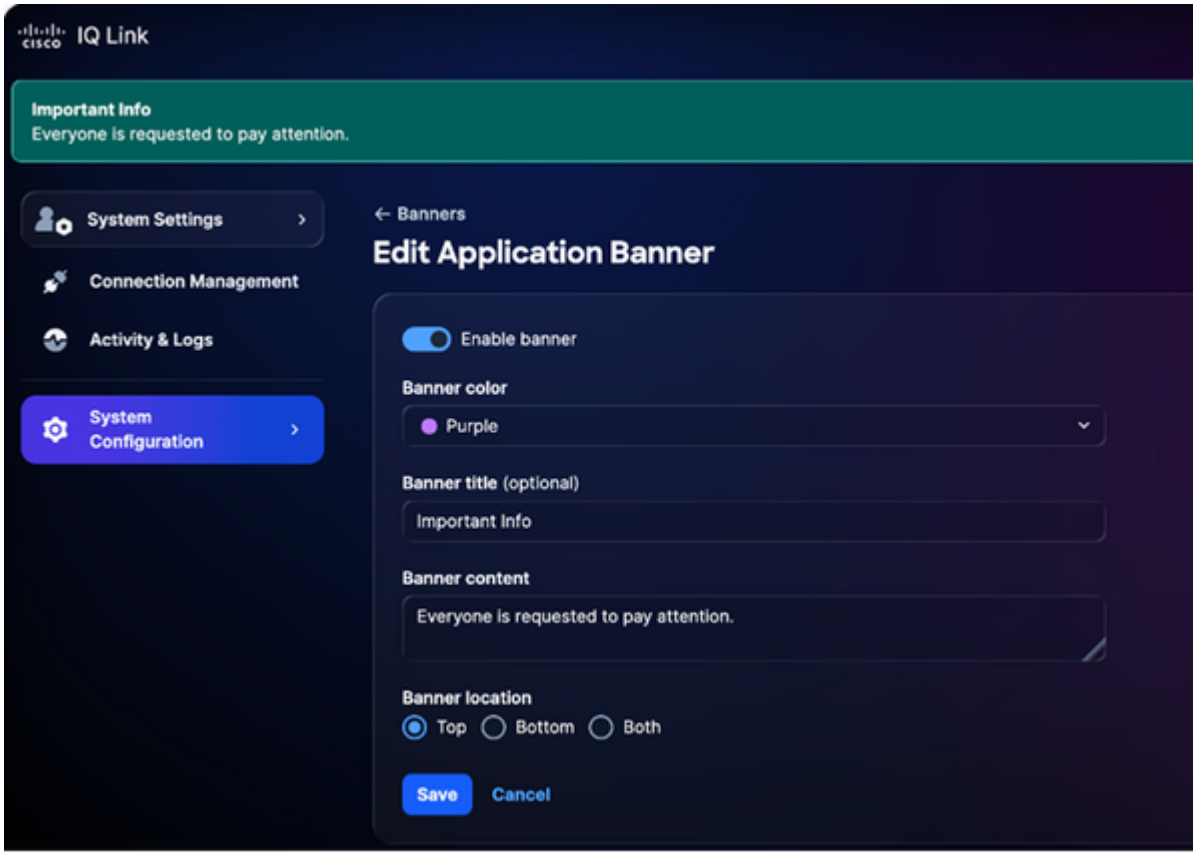
7. Wählen Sie einen Bannerstandort aus.
8. Klicken Sie auf Speichern. Das Banner wird in der gesamten Anwendung angezeigt.

Banner bearbeiten

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

Anwendungsbanner 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

Sie 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:

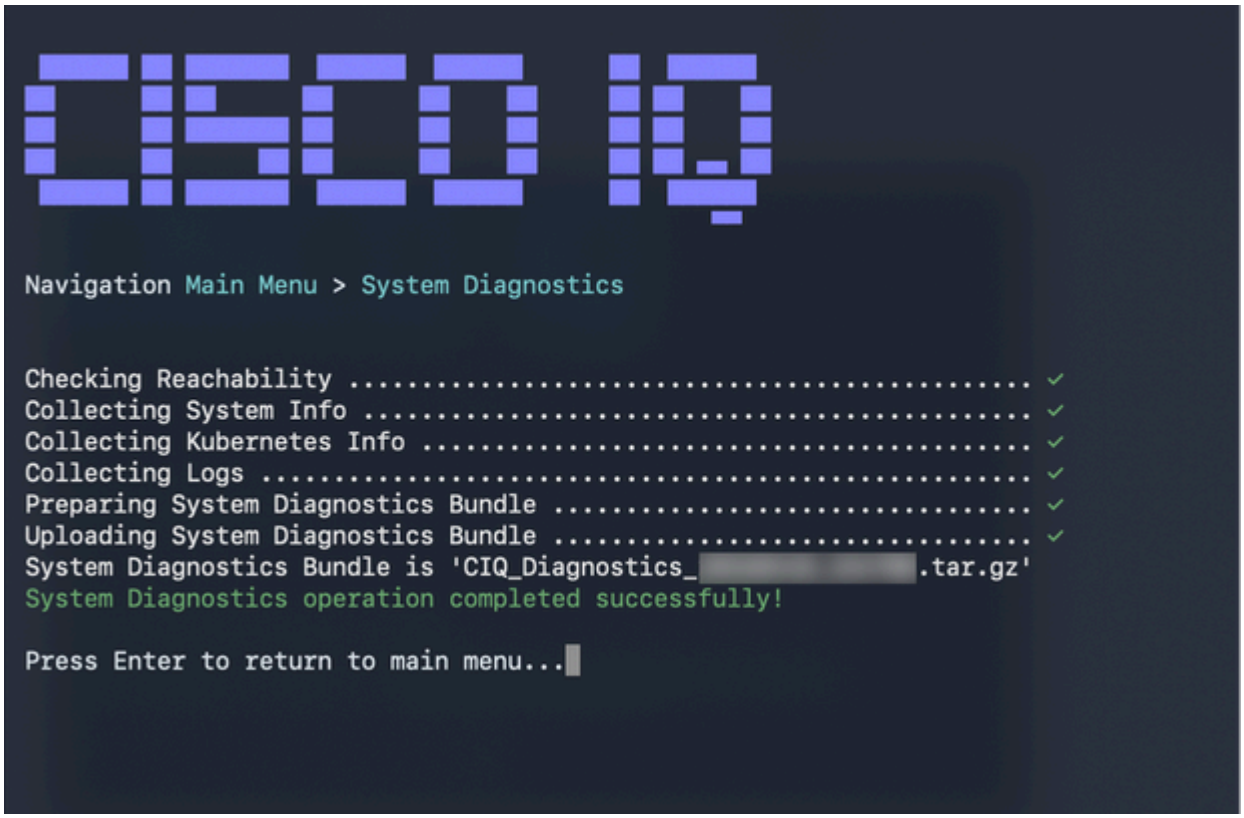
1. Melden Sie sich bei Cisco IQ an.

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 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.