Cisco IQ Link Operations Guide v1.2.0

Inleiding

Cisco IQTM biedt u verbeteringen en functies die zijn ontworpen om de zichtbaarheid van bedrijfsmiddelen te verbeteren, slimmere inzichten te bieden in uw omgevingen en het beheer van casestudy's te stroomlijnen. Daarnaast optimaliseren AI-functies zoals de AI Assistant de operationele resultaten en de Cisco IQ-gebruikerservaring door contextueel inzicht te bieden dat u in staat stelt proactieve, geïnformeerde beslissingen te nemen en processen voor klantbetrokkenheid en succes te stroomlijnen.

Cisco IQ Link verzamelt en verzendt veilig asset telemetrie van uw on-premises netwerk naar Cisco IQ, waardoor AI-aangedreven voorspellende inzichten u helpen de zichtbaarheid van het netwerk te verbeteren, problemen te anticiperen en operationele efficiëntie te stimuleren.

lokale verificatie

Accountbeheerders dienen de volgende referenties te gebruiken om in te loggen op Cisco IQ Link:

- Standaardgebruikersnaam: admin
- Standaardwachtwoord: wachtwoord dat is ingesteld tijdens het installatieproces van Cisco IQ Link; zie de handleiding Cisco IQ Link Aan de slag voor meer informatie
- Standaardaccountcontext: standaardklant

Bij aanmelding worden de standaardgebruiker, "admin", en de accountnaam, "Default-Customer", weergegeven op de startpagina.

Beveiliging van lokale beheerder instellen

U kunt uw wachtwoord wijzigen en beveiligingsvragen instellen via het menu Gebruikersprofiel op de homepage.

Lockout-instellingen

De volgende instellingen voor accountvergrendeling kunnen tijdens de implementatie worden geconfigureerd:

- Vergrendelingsstatus: hiermee wordt de functie voor het vergrendelen van accounts in- of uitgeschakeld.
- Maximale aanmeldingspogingen: hiermee wordt het maximum aantal opeenvolgende mislukte pogingen ingesteld dat is toegestaan voordat een account is vergrendeld (standaard: 3; bereik: 0-10).
- Rollingstijdvenster: definieert de tijdsperiode voor het bijhouden van mislukte pogingen (standaard: 15 minuten; bereik: 0-60 minuten).
- Duur: hiermee wordt de duur ingesteld waarvoor een account vergrendeld blijft nadat het maximale aantal pogingen is bereikt (standaard: 30 minuten; bereik: 0-60 minuten).

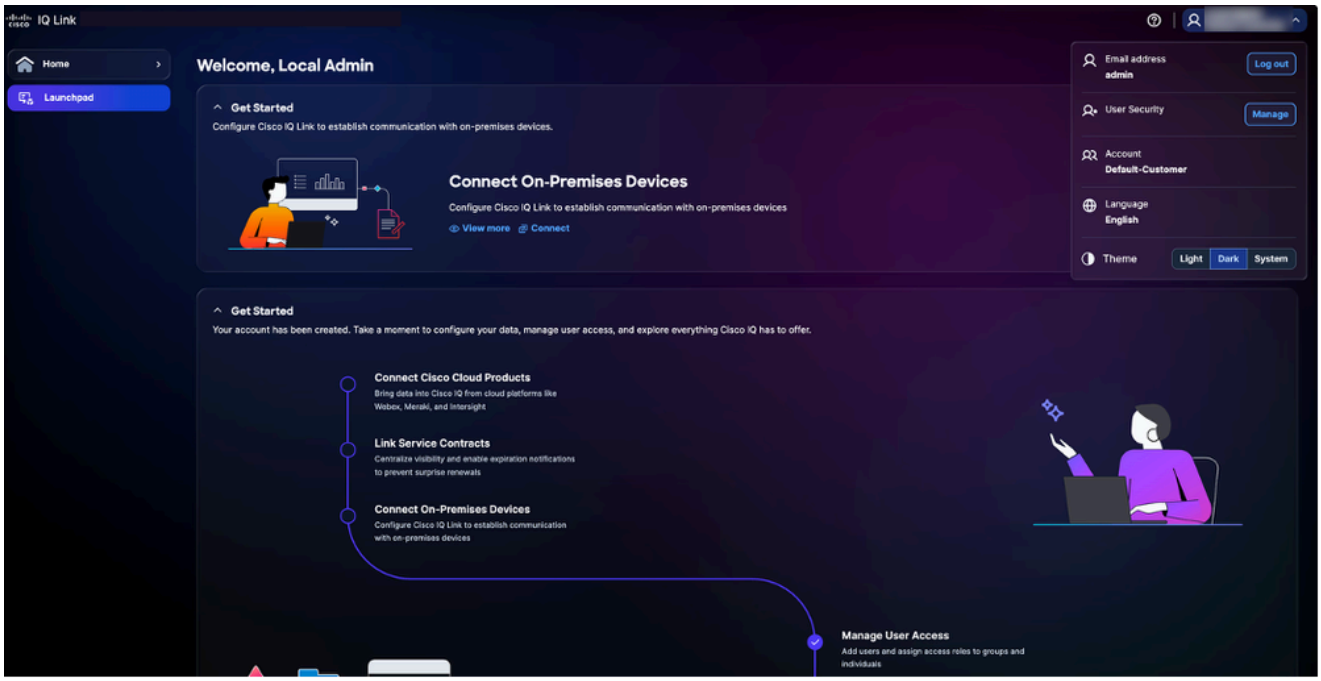
Opmerking: u hebt drie (3) pogingen om het juiste wachtwoord binnen een periode van 15 minuten in te voeren. Als alle drie (3) pogingen niet succesvol zijn, wordt uw account tijdelijk gedurende 30 minuten vergrendeld om uw beveiliging te beschermen.
U kunt niet proberen in te loggen tijdens de lockout periode. Het systeem geeft het bericht weer: "Account vergrendeld vanwege te veel mislukte pogingen. Probeer het later opnieuw.", inclusief de tijd dat de vergrendeling verloopt.
Uw account wordt automatisch ontgrendeld na 30 minuten, waarna u kunt proberen in te loggen of uw wachtwoord opnieuw in te stellen.

Beveiligingsvragen en -antwoorden instellen

Beveiligingsvragen helpen bij het verifiëren van uw identiteit als u uw wachtwoord bent vergeten. Accountbeheerders moeten antwoorden op vijf (5) beveiligingsvragen instellen om de functie voor het opnieuw instellen van wachtwoorden in te schakelen. Dit is een eenmalige installatie.

Beveiligingsvragen instellen:

1. Klik op de homepage op het pictogram Gebruikersprofiel. Het vervolgkeuzemenu wordt geopend.

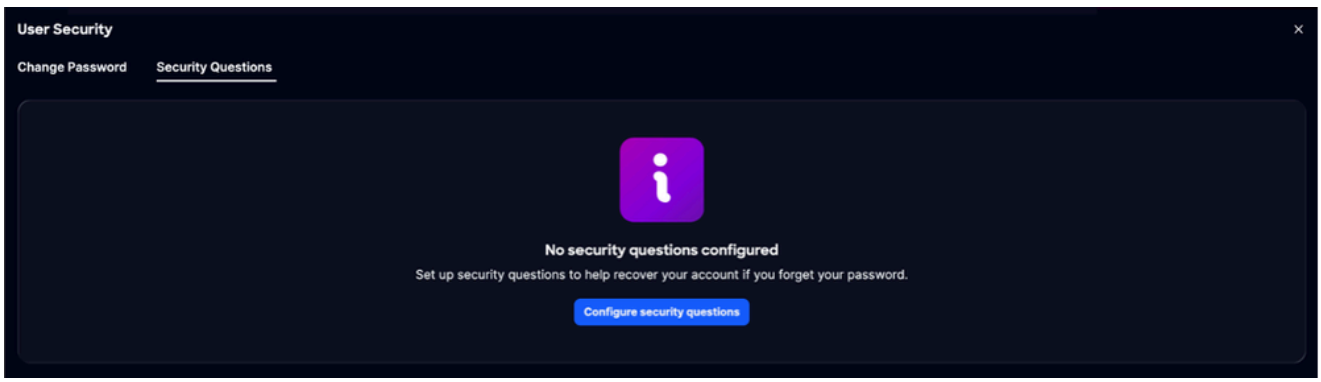


Menu Gebruikersprofiel

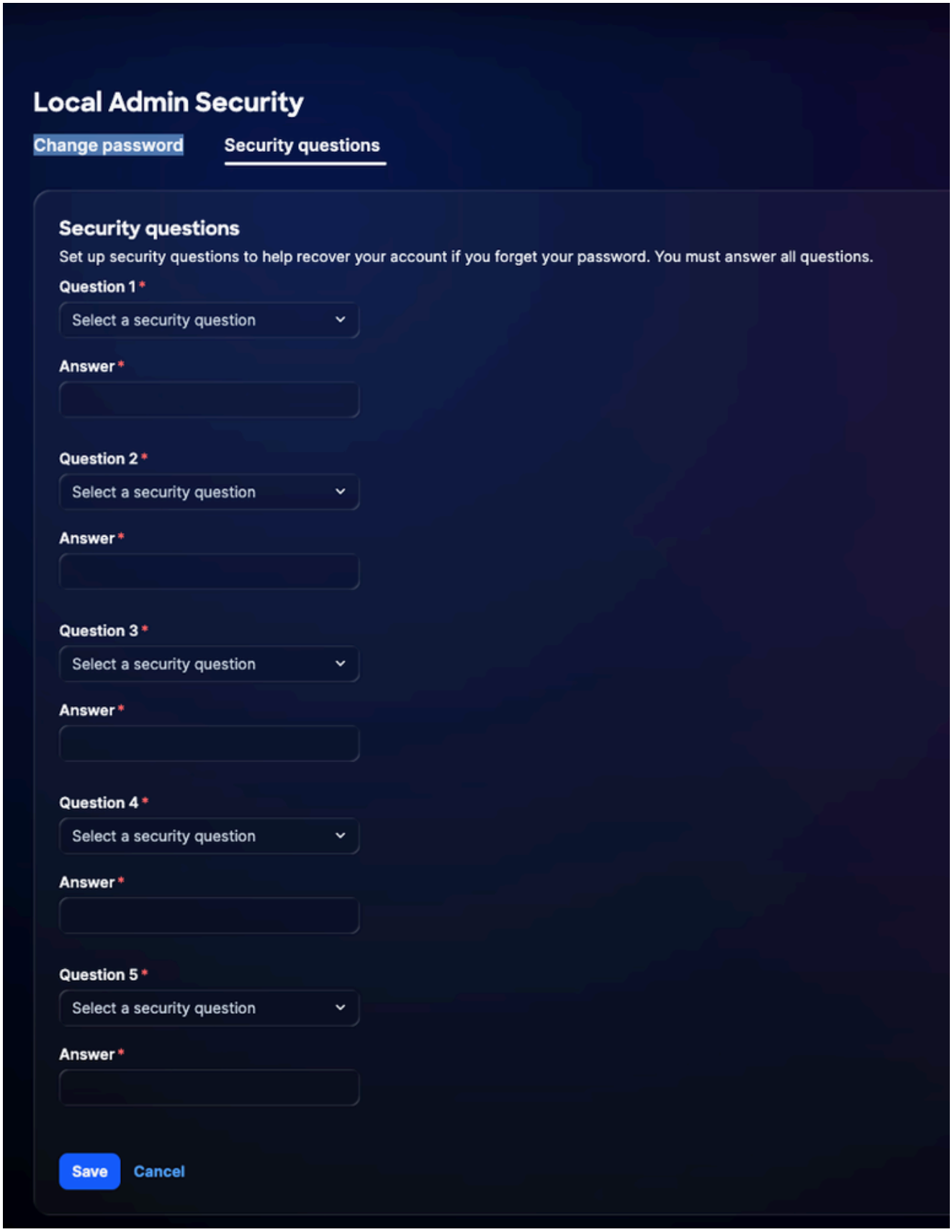
2. Klik op Beheren in Gebruikersbeveiliging. De pagina Gebruikersbeveiliging wordt weergegeven.

Wachtwoord wijzigen

3. Klik op Beveiligingsvragen om het tabblad te openen.



4. Klik op Beveiligingsvragen configureren.



5. Kies vijf (5) beveiligingsvragen uit de vervolgkeuzelijsten.
6. Voer uw antwoord in voor elke vraag.
7. Klik op Save (Opslaan).

Opmerking: Antwoorden zijn niet hoofdlettergevoelig, bijvoorbeeld, "SMITH" en "smith" worden als hetzelfde beschouwd.
Extra ruimtes worden genegeerd, bijvoorbeeld, "Smith" en "smith" worden als hetzelfde beschouwd.

Opmerking: u kunt uw antwoorden later bijwerken als dat nodig is. Wanneer u uw antwoorden bijwerkt, worden alle eerdere antwoorden vervangen, dus u moet opnieuw antwoorden geven op alle vijf (5) vragen en niet alleen op de vragen die u wilt wijzigen.

Wachtwoorden beheren

Accountbeheerders en lokale gebruikers kunnen wachtwoorden voor Cisco IQ beheren.

Om de veiligheid van uw account te garanderen, worden de volgende wachtwoordbeleidslijnen toegepast:

- Beperking voor hergebruik: uw nieuwe wachtwoord kan niet overeenkomen met een van uw vorige vijf (5) wachtwoorden. Dit beleid is van toepassing op aanmelden, wachtwoord vergeten en wachtwoordstromen wijzigen.
- Tekenvariatie: bij het wijzigen van uw wachtwoord terwijl u bent geverifieerd, moeten ten minste acht (8) tekens van uw huidige wachtwoord verschillen in uw nieuwe wachtwoord.
- Minimum wijzigingsinterval: standaard moet u 24 uur wachten voordat u uw wachtwoord opnieuw wijzigt. Als er een ander interval is geconfigureerd, kunt u uw wachtwoord pas bijwerken nadat die tijd is verstreken.
- Wachtwoordvervaldatum: Wachtwoorden vervallen elke 60 dagen. Bij uw eerste aanmelding na de vervaldatum moet u een nieuw wachtwoord instellen voordat u toegang krijgt tot het systeem. (Als het wachtwoord is ingesteld op 0, is de wachtwoordvervaldatum uitgeschakeld.)

Voorwaarden

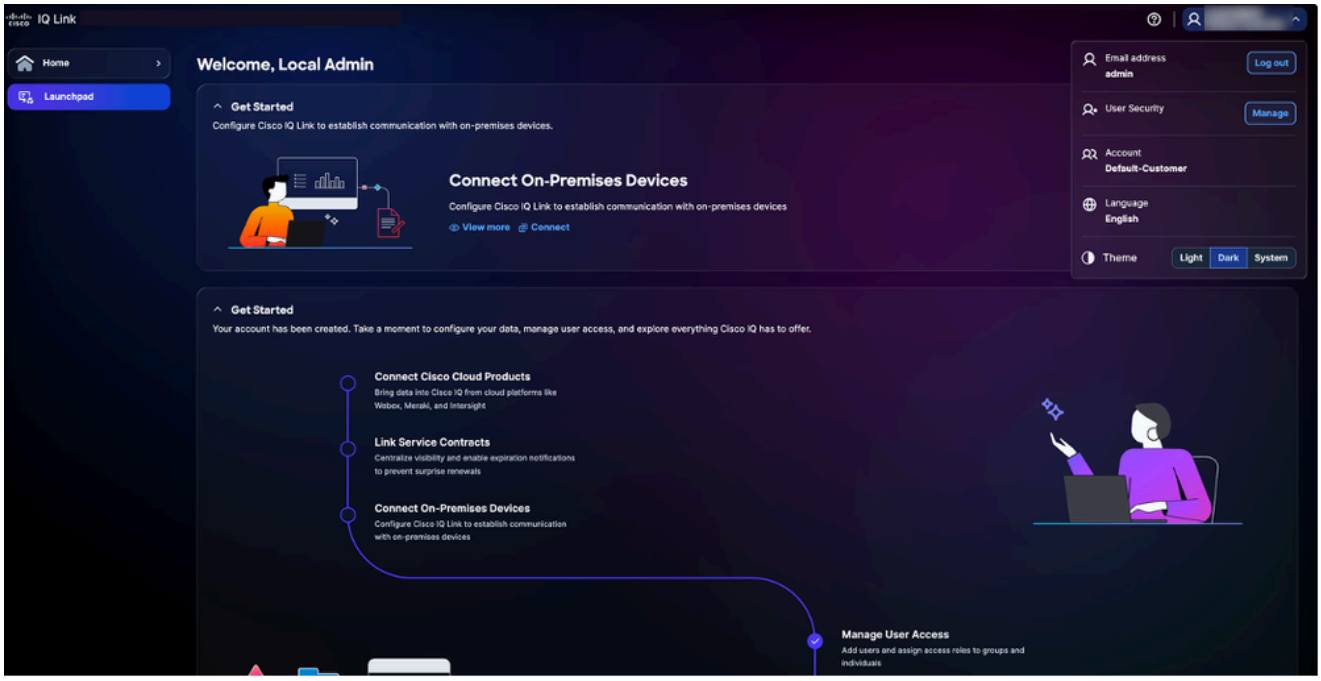
Om wachtwoorden te beheren, moet aan de volgende voorwaarden worden voldaan:

- U bent een lokale accountbeheerder of -gebruiker
- U gebruikt een lokaal account (geen eenmalige aanmelding of externe verificatie)
- Je bent ingelogd op Cisco IQ Link
- U kent het huidige wachtwoord

Wachtwoorden wijzigen

U wijzigt als volgt een wachtwoord:

1. Klik op de homepage op het pictogram Gebruikersprofiel. Het vervolgkeuzemenu wordt geopend.



Menu Gebruikersprofiel

2. Klik op Beheren in Gebruikersbeveiliging. De pagina Gebruikersbeveiliging wordt weergegeven.

Wachtwoord wijzigen

3. Voer het huidige wachtwoord in.
4. Voer het nieuwe wachtwoord in.
5. Voer het nieuwe wachtwoord opnieuw in om te bevestigen.
6. Klik op Save (Opslaan).

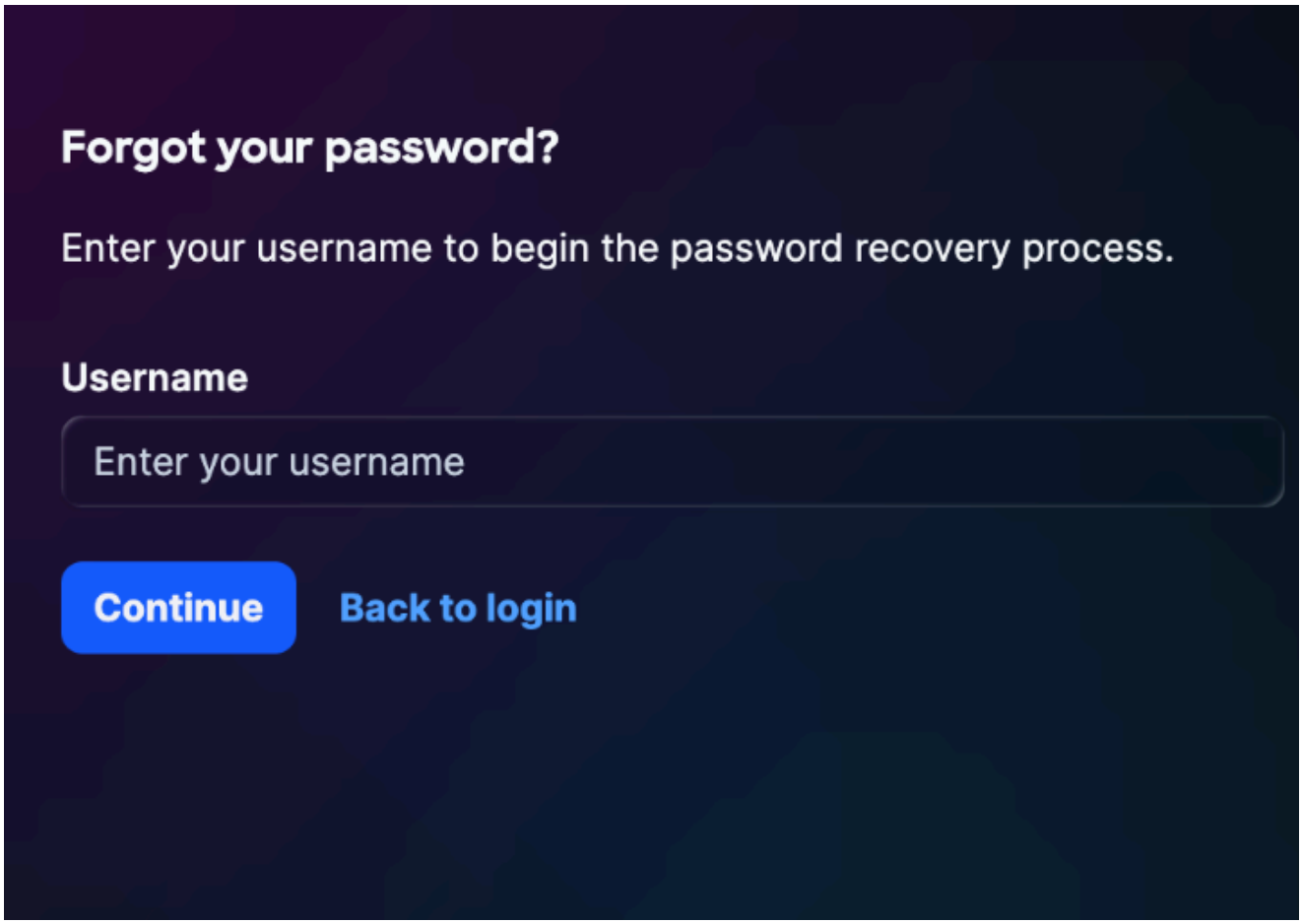
Het wachtwoord wordt bijgewerkt in het Cisco IQ-systeem, inclusief de Cisco IQ Virtual Machine (VM).

Een vergeten wachtwoord opnieuw instellen

U kunt een vergeten wachtwoord opnieuw instellen met behulp van het verificatieproces voor beveiligingsvragen, als u de beveiligingsvragen eerder hebt ingesteld. Zie Beveiligingsvragen en -antwoorden instellen voor meer informatie.

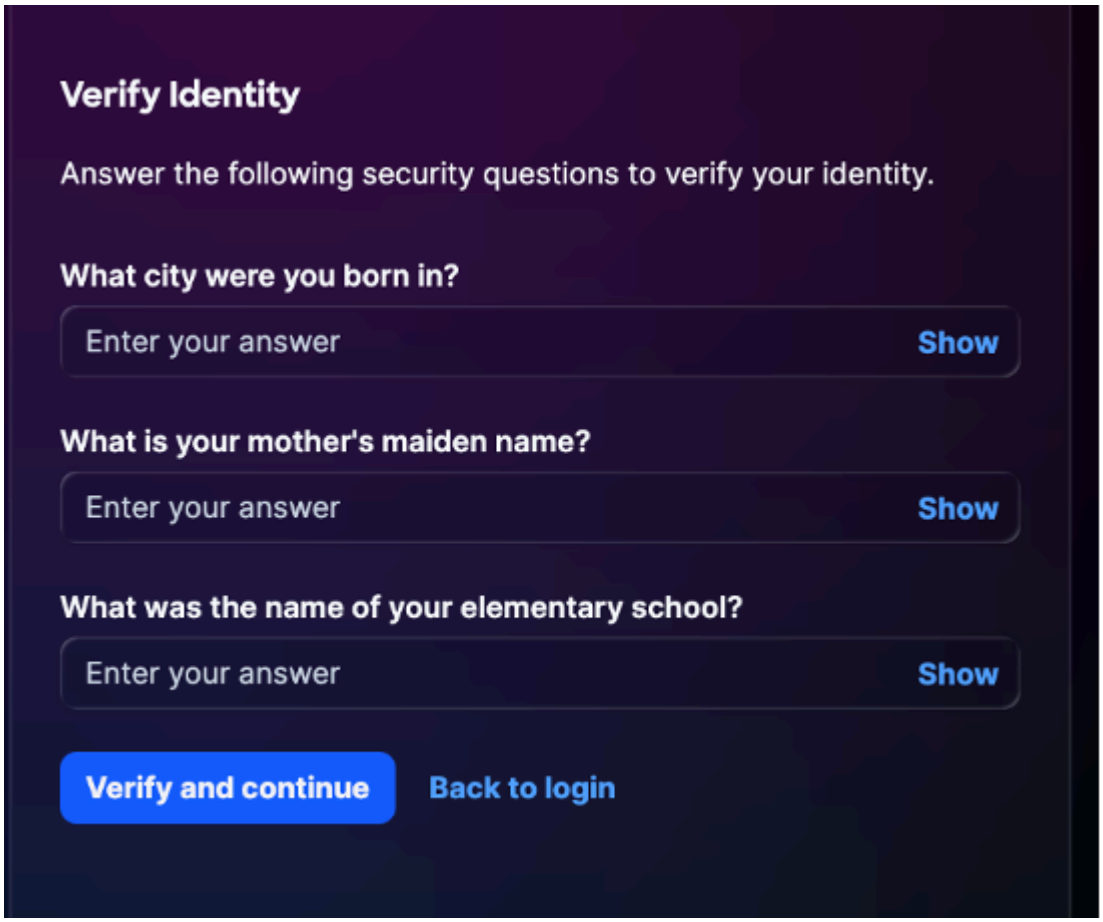
Om een vergeten wachtwoord opnieuw in te stellen:

1. Navigeer naar de Cisco IQ Link-aanmeldingspagina.
2. Klik op Wachtwoord vergeten.



Wachtwoord vergeten

3. Voer de gebruikersnaam in.
4. Klik op Continue (Doorgaan). Op de pagina Identiteit verifiëren worden drie (3) willekeurige beveiligingsvragen weergegeven van de vijf (5) vragen die eerder zijn geconfigureerd.



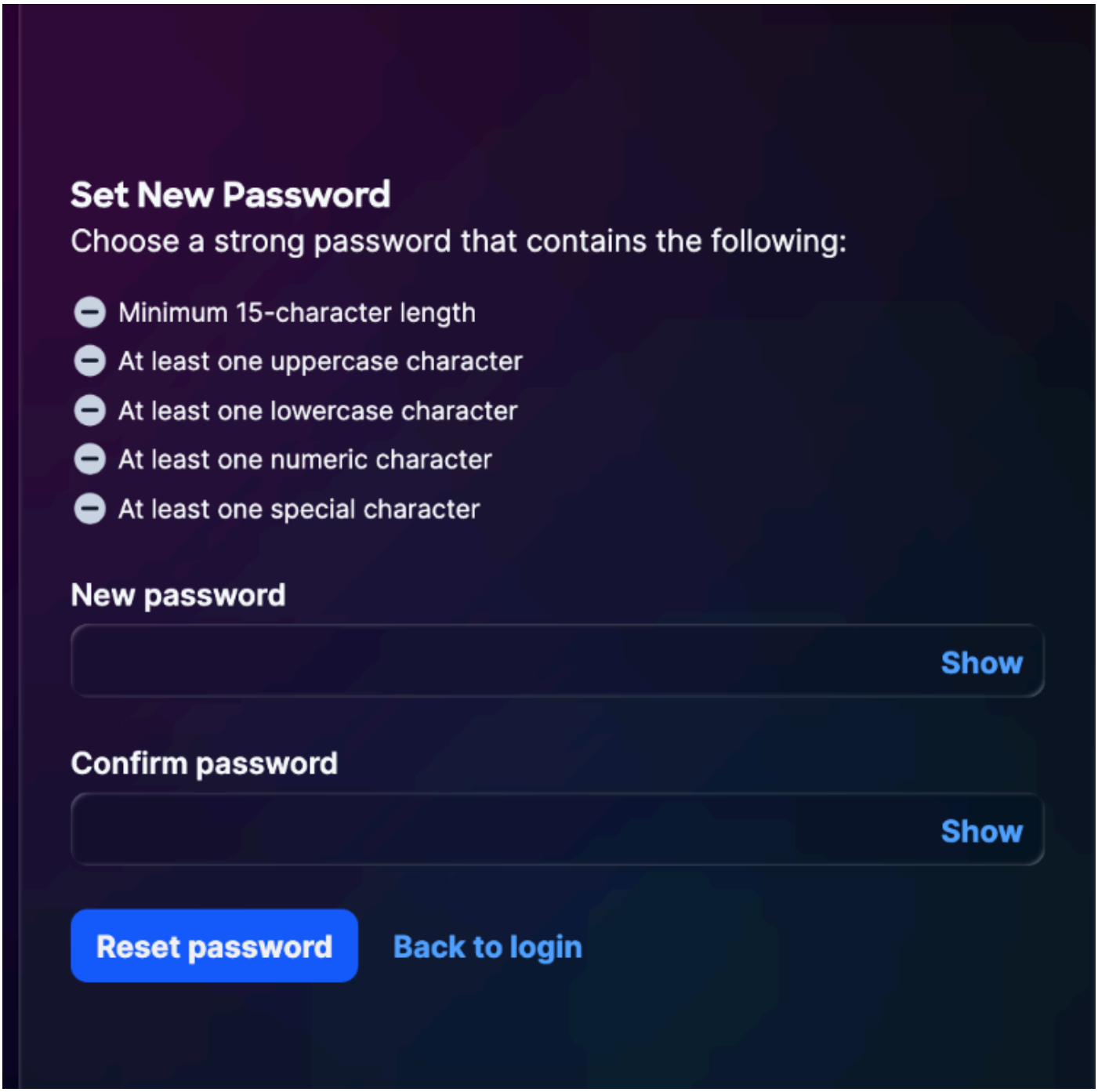
Identiteit verifiëren

✎ Opmerking: de hierboven weergegeven beveiligingsvragen zijn gebruikersspecifiek en zullen dienovereenkomstig variëren.

---

5. Voer de antwoorden in voor alle drie (3) weergegeven vragen.

6. Klik op Verifiëren en doorgaan. Als het ingediende antwoord overeenkomt met uw eerder opgeslagen antwoorden, wordt u gevraagd een nieuw wachtwoord in te voeren.



Wachtwoord herstellen

Je hebt drie (3) pogingen om de beveiligingsvragen binnen een periode van 15 minuten correct te beantwoorden. Als alle drie (3) pogingen niet succesvol zijn, wordt uw account tijdelijk gedurende 30 minuten vergrendeld om uw beveiliging te beschermen. U kunt uw wachtwoord niet opnieuw instellen tijdens de vergrendelingsperiode.
Het systeem geeft het bericht weer: "Account vergrendeld vanwege te veel mislukte verificatiepogingen. Probeer het later opnieuw.", inclusief de tijd dat de vergrendeling verloopt.
Uw account wordt automatisch ontgrendeld na 30 minuten, waarna u kunt proberen in te loggen of uw wachtwoord opnieuw in te stellen.

7. Voer het nieuwe wachtwoord in.

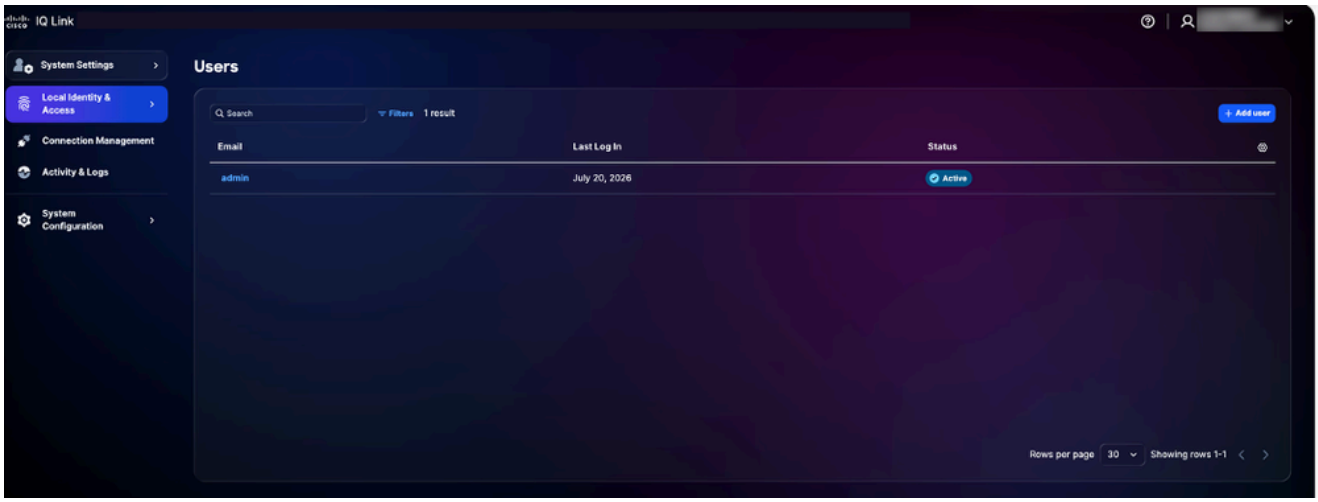
8. Voer het wachtwoord opnieuw in om te bevestigen.

9. Klik op Indienen.

Lokale gebruikers toevoegen

Accountbeheerders kunnen gebruikers toevoegen aan het Cisco IQ-account. Een nieuwe gebruiker toevoegen:

1. Navigeer naar Systeeminstellingen > Lokale identiteit en toegang > Gebruikers. De pagina Gebruikers wordt weergegeven. Het geeft een overzicht van alle bestaande lokale gebruikers, samen met hun status.

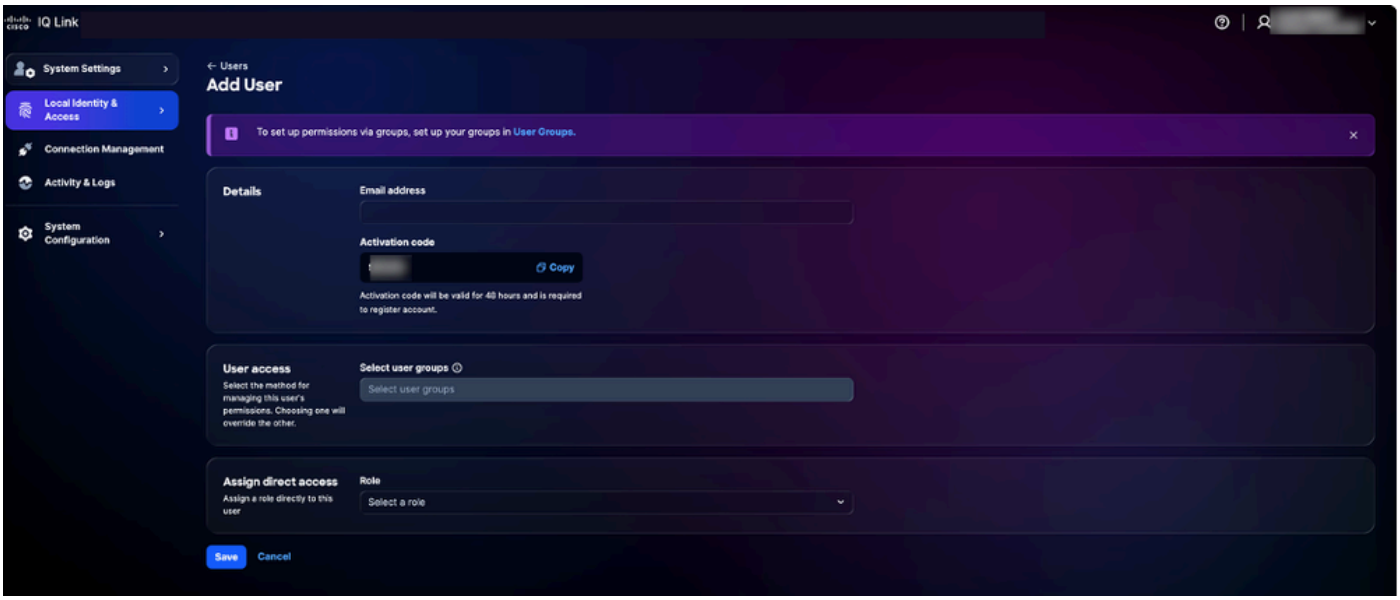


Gebruikerspagina

Opmerking: het pictogram Meer opties wordt niet weergegeven voor accountbeheerders (zoals weergegeven in de afbeelding hierboven).

---

2. Klik op Gebruikers toevoegen. De pagina Gebruiker toevoegen wordt weergegeven.



Gebruiker toevoegen

3. Voer het e-mailadres in.

4. Voer de activeringscode in.

Opmerking: de activeringscode wordt standaard weergegeven. Deel het met de gebruiker, want het is vereist om de registratie te voltooien.

---

5. Kies in de vervolgkeuzelijst Gebruikerstoegang de gebruikersgroep in de vervolgkeuzelijst Gebruikersgroepen selecteren.

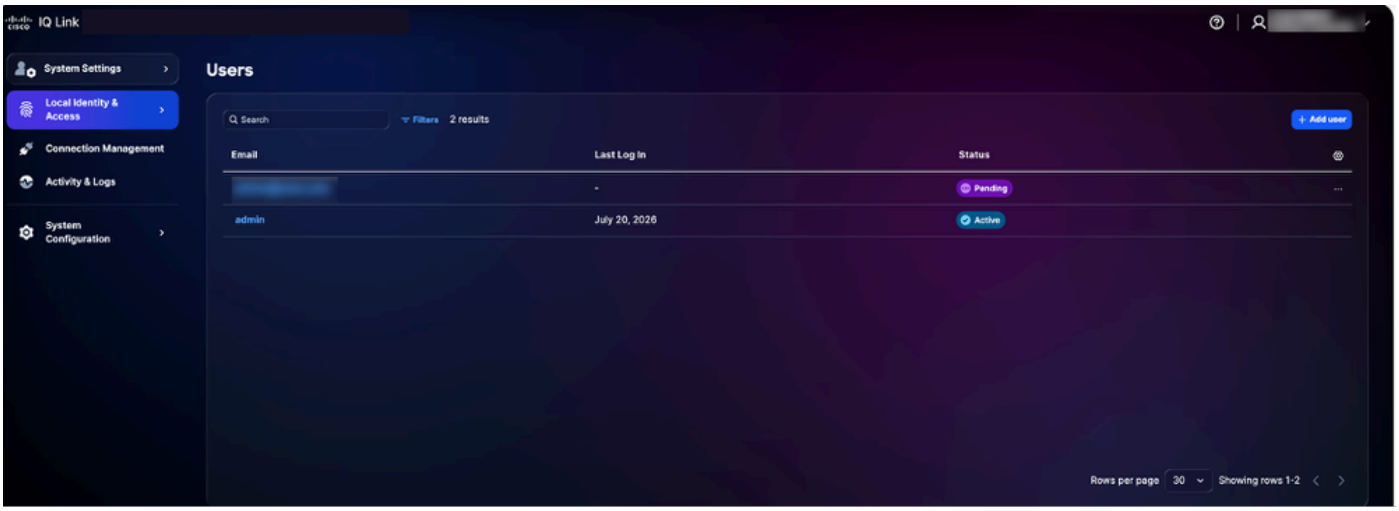
Opmerking: gebruikers erven toegang van de geselecteerde groep.

---

6. Kies bij Rechtstreekse toegang toewijzen de rol in de vervolgkeuzelijst Rol. Er zijn twee (2) rollen beschikbaar:

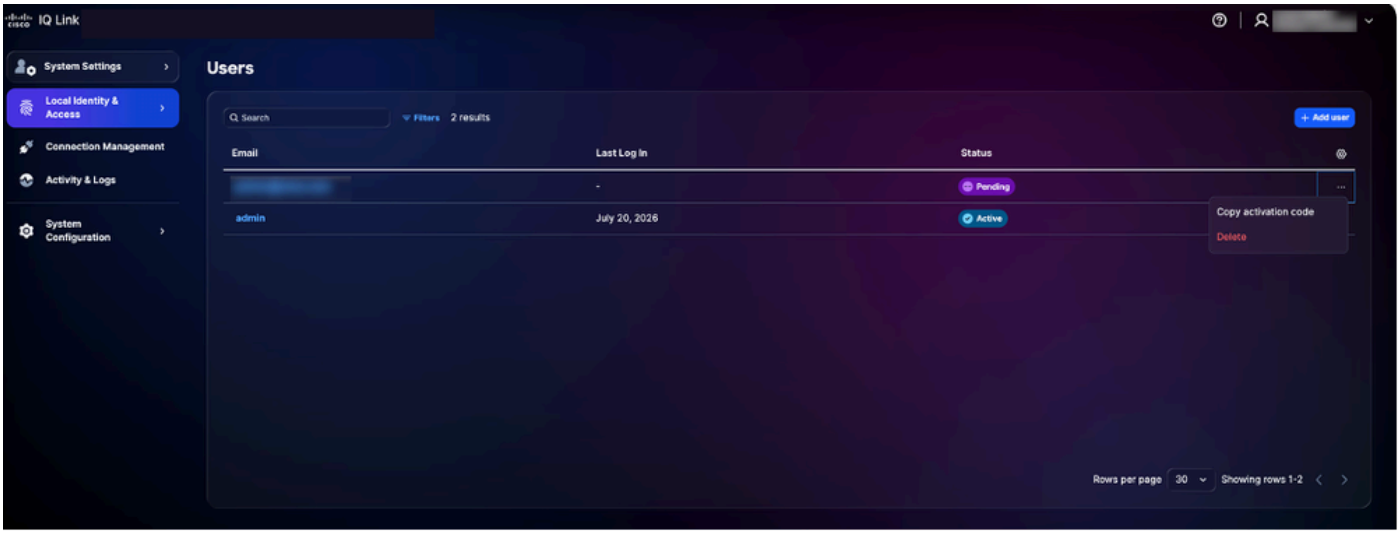
- Viewer: toepassingen weergeven en openen
- Beheerder: toegang tot toepassingen en beheer systeeminstellingen, behalve Systeembeheer en IDP

7. Klik op Opslaan. De nieuwe gebruiker wordt gemaakt en in de gebruikerslijst weergegeven in de status In behandeling. In behandeling geeft aan dat de gebruiker de zelfactivering nog niet heeft voltooid.



Nieuw toegevoegde gebruiker

8. Zoek de nieuwe gebruiker in de lijst en bevestig dat de kolom Status in behandeling wordt weergegeven.



Activeringscode kopiëren

9. Klik op het pictogram Meer opties > Activeringscode kopiëren naast de nieuwe gebruiker. De activeringscode wordt naar het klembord gekopieerd.

10. Deel deze code veilig met de gebruiker (bijvoorbeeld via een beveiligd intern kanaal). De activeringscode is voor eenmalig gebruik en is vereist om de registratie te voltooien.

Opmerking: deel de activeringscode niet via onveilige kanalen. Als de code verloren gaat of in gevaar komt, gebruikt u het menupictogram om een nieuwe activeringscode te genereren, waardoor de vorige ongeldig wordt

---

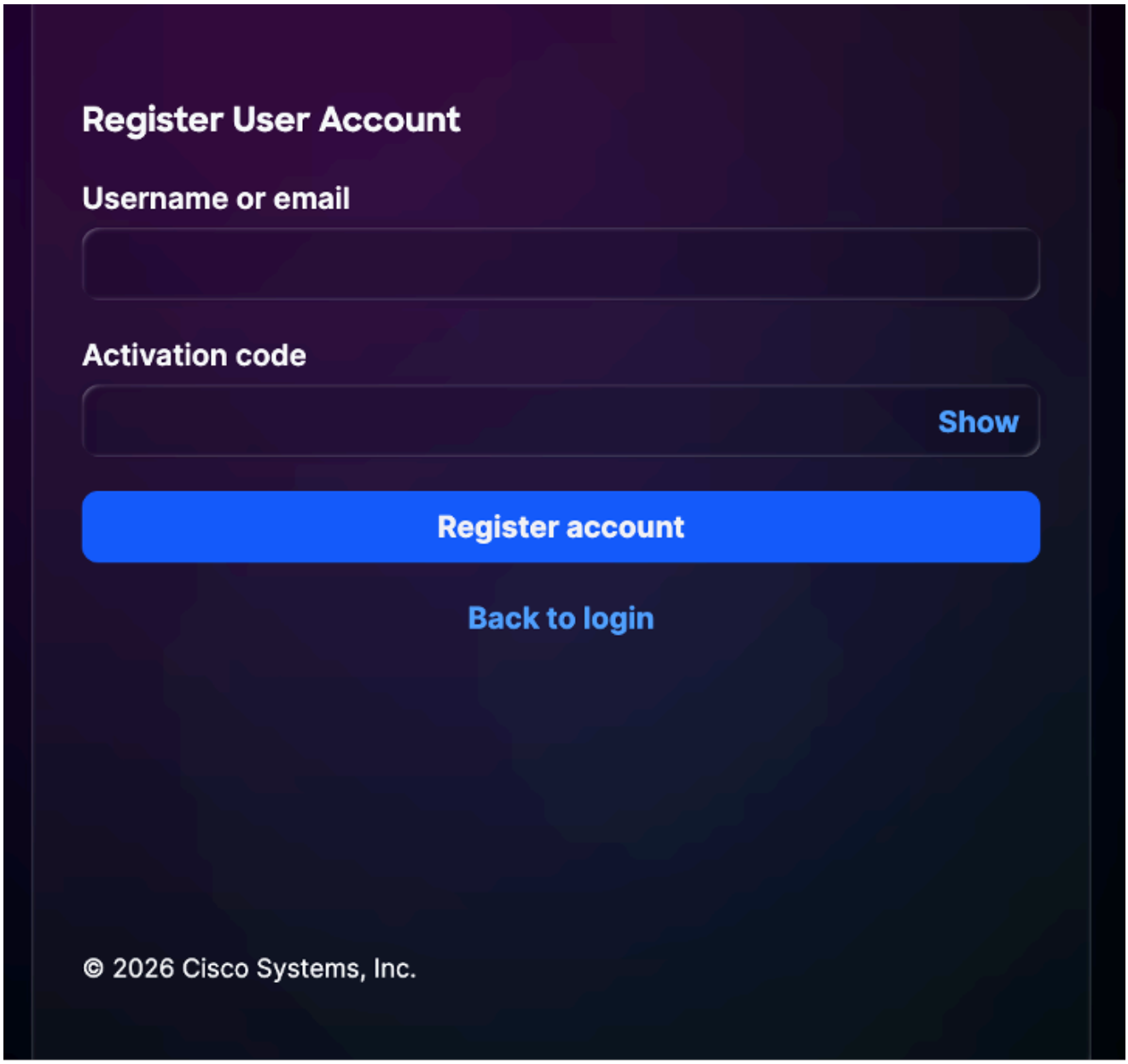
Opmerking: activeringscodes zijn 48 uur geldig. Neem contact op met uw accountbeheerder om een nieuwe code aan te vragen als de code verloopt.

11. Klik op het pictogram van de gebruiker in de rechterbovenhoek en selecteer Afmelden. U keert terug naar de aanmeldingspagina van Cisco IQ.

Nieuwe gebruikersaccount registreren

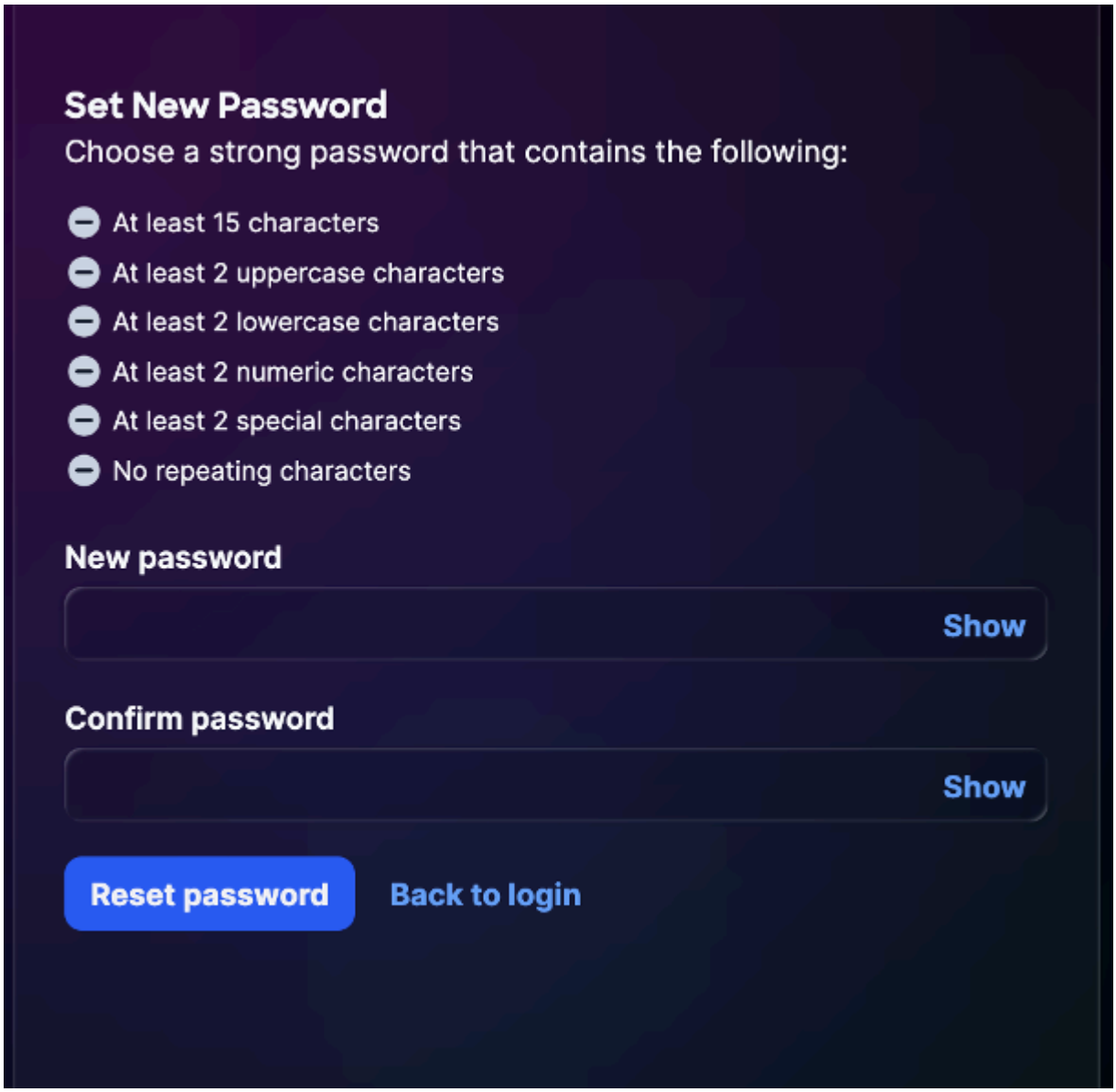
Om de nieuwe gebruikersaccount te registreren:

1. Klik op de aanmeldingspagina op de link Een nieuwe gebruikersaccount registreren.



Nieuwe gebruikersaccount

2. Voer de gebruikersnaam of het e-mailadres in dat werd gebruikt toen de gebruiker werd aangemaakt (bijvoorbeeld user1@abc.com).
3. Voer de activeringscode in die door de accountbeheerder wordt gedeeld.
4. Klik op Account registreren. Het venster Nieuw wachtwoord instellen wordt weergegeven.



Wachtwoord voor nieuwe gebruikersaccount

5. Voer een nieuw wachtwoord in.
6. Voer het wachtwoord opnieuw in Wachtwoord bevestigen.
7. Bij de eerste succesvolle aanmelding wordt de gebruiker gevraagd om vijf (5) beveiligingsvragen te configureren (zie Beveiligingsvragen en antwoorden instellen voor meer informatie).

Beheren van lokale gebruikersgroepen

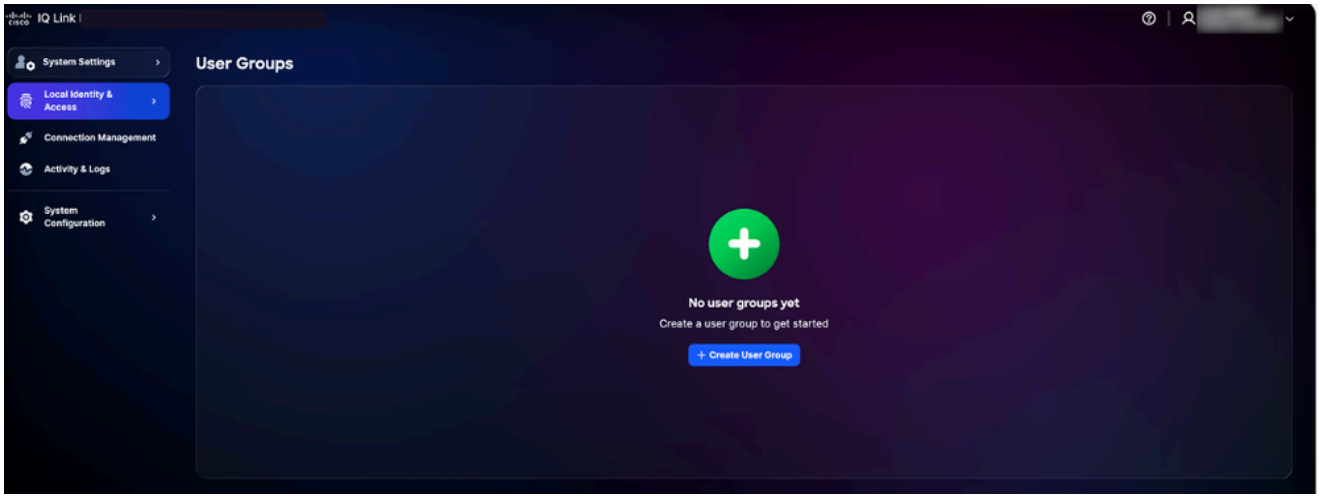
Gebruikersgroepen stellen accountbeheerders in staat om rollen voor meerdere lokale gebruikers samen te beheren. In plaats van een rol aan elke gebruiker afzonderlijk toe te wijzen, kan een accountbeheerder een groep maken, er een rol en een set gebruikers aan koppelen en de rol of het lidmaatschap op één plaats bijwerken. Alle gebruikersgroepbeheer wordt uitgevoerd vanaf de pagina Lokale identiteit en toegang.

✎ Opmerking: alleen een accountbeheerder kan gebruikersgroepen maken, bewerken of verwijderen. Groepen bestaan uit bestaande lokale gebruikers; gebruikers moeten worden gemaakt voordat ze aan een groep kunnen worden toegevoegd.

Een gebruikersgroep maken

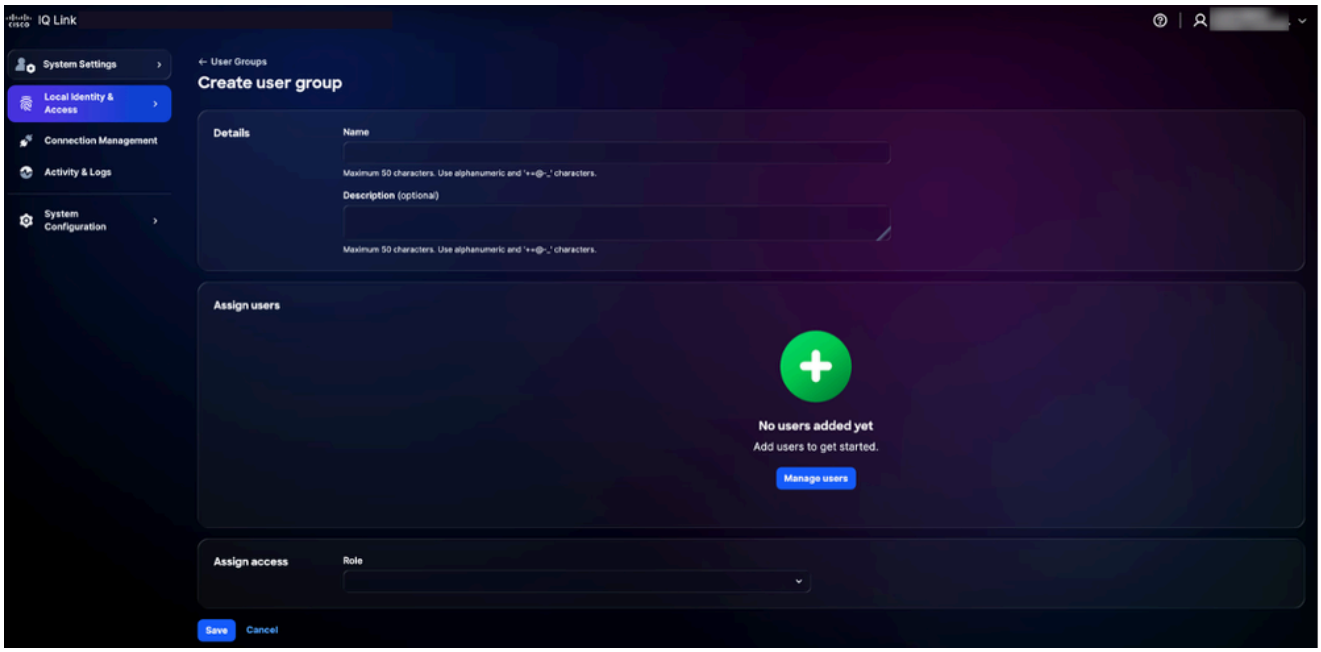
U maakt als volgt een gebruikersgroep:

1. Kies in Systeeminstellingen de optie Lokale identiteit en toegang > Gebruikersgroepen. De pagina Gebruikersgroepen wordt weergegeven.



Gebruikersgroepen

2. Klik op Gebruikersgroep maken. De pagina Gebruikersgroep maken wordt weergegeven.



Gebruikersgroep aanmaken

3. Voltooi de volgende secties:

- Details
  - Naam: Voer een unieke naam in voor de groep (bijvoorbeeld Alleen-lezen operatoren)
  - Beschrijving (optioneel): Een korte beschrijving van de groep (maximaal 50 tekens; alfanumeriek en + = @ - _ tekens zijn toegestaan)

- Gebruikers toewijzen

  Zoek en selecteer een of meer bestaande lokale gebruikers om aan de groep toe te voegen.

  ✎ Opmerking: klik op Gebruikers beheren om gebruikers toe te voegen die nog niet zijn vermeld.

- Toegang toewijzen

  - Rol: Selecteer de systeemrol die aan alle leden van deze groep moet worden toegewezen. De volgende rollen zijn beschikbaar:

    - Viewer: toepassingen weergeven en openen (alleen-lezen)
    - Beheerder: toegang tot toepassingen en beheer systeeminstellingen

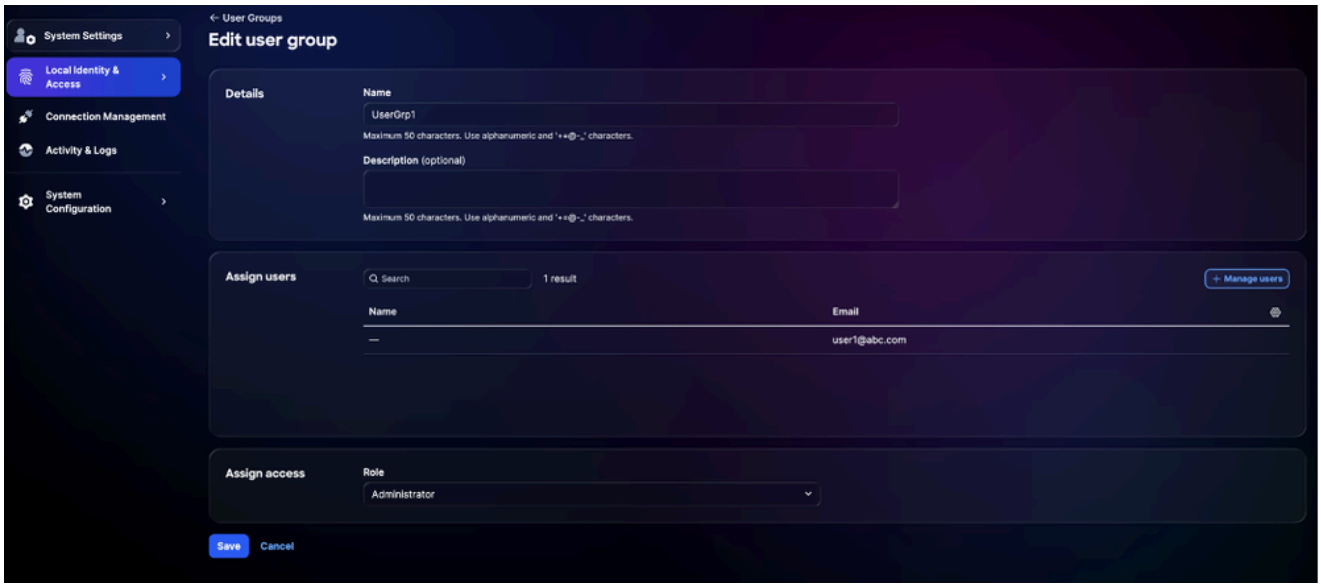
4. Klik op Opslaan.

De nieuwe gebruikersgroep wordt weergegeven in de lijst Gebruikersgroepen, samen met de toegewezen rol en het aantal leden.

Een gebruikersgroep bewerken

Een gebruikersgroep bewerken:

1. Zoek in de lijst Gebruikersgroepen de groep die u wilt wijzigen.
2. Klik op het pictogram Meer naast de groep en kies Bewerken. De pagina Gebruikersgroep bewerken wordt weergegeven.



Gebruikersgroep bewerken

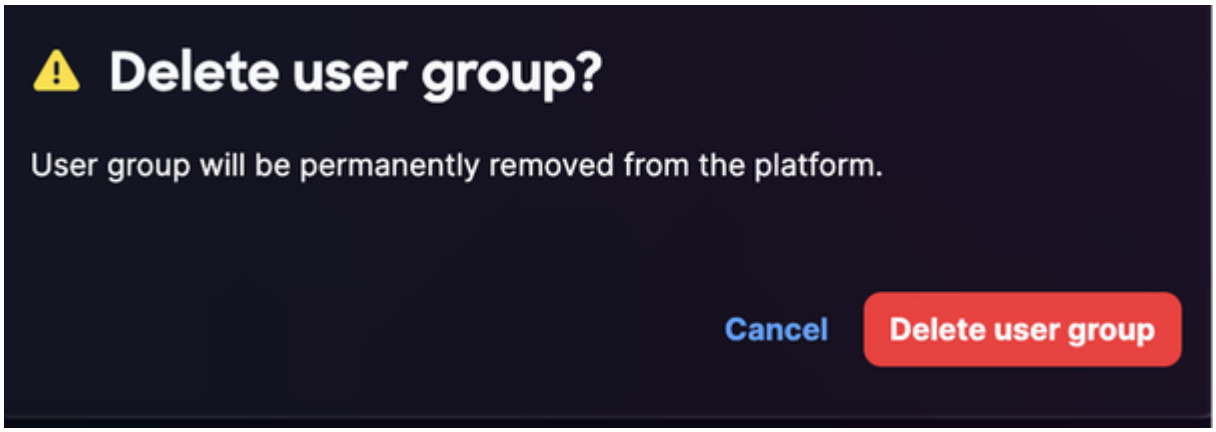
3. Breng de gewenste veranderingen aan.
4. Klik op Save (Opslaan).

De bijgewerkte groep wordt weergegeven in de lijst Gebruikersgroepen. De nieuwe functie geldt voor alle leden van de groep.

Een gebruikersgroep verwijderen

U verwijdert als volgt een gebruikersgroep:

1. Zoek in de lijst Gebruikersgroepen de groep die u wilt verwijderen.
2. Klik op het pictogram Meer opties naast de groep en selecteer Verwijderen.



Gebruikersgroep verwijderen

3. Bevestig de verwijdering wanneer daarom wordt gevraagd.

De groep wordt verwijderd uit de lijst Gebruikersgroepen.

Opmerking: als u een gebruikersgroep verwijdert, wordt de roltoewijzing op basis van een groep van alle leden verwijderd. De individuele gebruikersaccounts worden niet verwijderd.

Identiteitsprovider configureren

Zodra u bent ingelogd bij Cisco IQ Link, kunnen accountbeheerders verschillende instellingen configureren. Accountbeheerders kunnen zich aanmelden bij Cisco IQ Link met behulp van lokale administratie of IDP-configuratie (Identity Provider).

Okta IDP SAML-configuratie voor SSO

Vereisten voor het configureren van IDP SAML

- Toegang van lokale accountbeheerder tot Cisco IQ Link
- Toegang tot IDP-portal

IDP SAML-configuratie voor SSO

IDP Security Assertion Markup Language (SAML) configureren voor SSO:

1. Navigeer naar uw IDP-portal.

2. Stel de volgende kenmerken in voor de Cisco IQ Link-instantie.
Tabel 1: Cisco IQ Link-kenmerken

Veld	Waarde
Naam van toepassing	<Naam van toepassing>
milieu	ESP-bedrijfstoepassing
Groepen van eigenaar van toepassing	Eigenaar van de IDP-instellingen
Teammailer	Mailer voor het team
publiek	niet-beroepsbevolking
Onboarding-rubriek	Selecteer "Nieuwe onboarding"

Tabel 2: SAML-configuratieparameters

Parameter	Configuratie	Voorbeeld
Publiek (Entiteit-ID)	Volledig gekwalificeerde domeinnaam (FQDN)	mymanagementhost.mydomain.com
URL voor eenmalige aanmelding	SAML Assertion Consumer Service (ACS) eindpunt	https://mymanagementhost.mydomain.com/saml/acs
Naam-ID-indeling	E-mailadres	NA
Gebruikersnaam van toepassing	Username	NA

3. Configureer de volgende verplichte attribuutinstructies.

Opmerking: wijzigingen in IDP-kenmerken zijn afhankelijk van de specifieke provider en configuratie. Cisco IDP en de bijbehorende kenmerken worden hieronder als voorbeeld gedeeld.

- eerste binnenkomst
  - Naam: Gebruikersnaam
  - Waarde: user.login

- tweede inschrijving
  - Naam: Primaire e-mail
  - Waarde: user.email

- Attribuutoverzichten van groep
  - Naam: groepen
  - Filter: REGEX
  - Waarde: .*

4. Configureer de Single Logout (SLO)-instellingen in de toepassing.

Tabel 3: Configuratie-instellingen voor SLO

Veld	Waarde
handtekeningcertificaat	Voor Okta is dit certificaat alleen vereist als u ervoor kiest om SLO in te schakelen. Download het Handtekeningcertificaat met behulp van het Download SP-certificaat in Identiteitsproviders. Sla het bestand op als sp-public-key.crt. Zie Configuratie eenmalige aanmelding voor meer informatie.
SP-metagegevens	De SP-metagegevens zijn alleen vereist voor ADFS IDP (en niet voor Okta).
Wilt u Single Logout inschakelen?	Ja of nee
Enkelvoudige afmeldings-URL	https://mymanagementhost.mydomain.com/saml/logout
SP Uitgever (Publiek/Entiteit ID of ACS URL)	https://mymanagementhost.mydomain.com

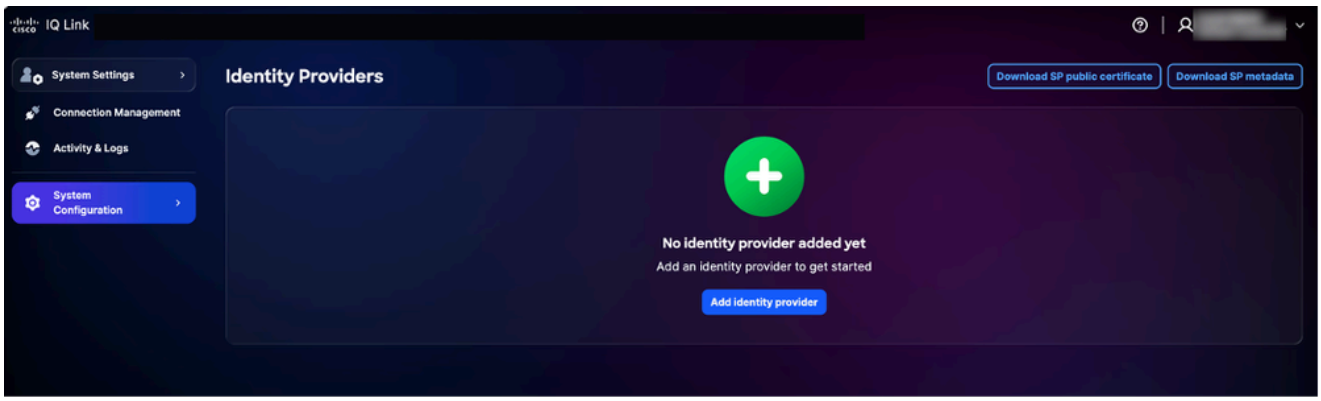
5. Klik op het pictogram Download om het bestand "SP Metadata" te downloaden.

6. Verstrekking of creatie van de applicatie zoals vereist door de aanbieder.

Okta IDP toevoegen

Een IDP toevoegen in Cisco IQ Link:

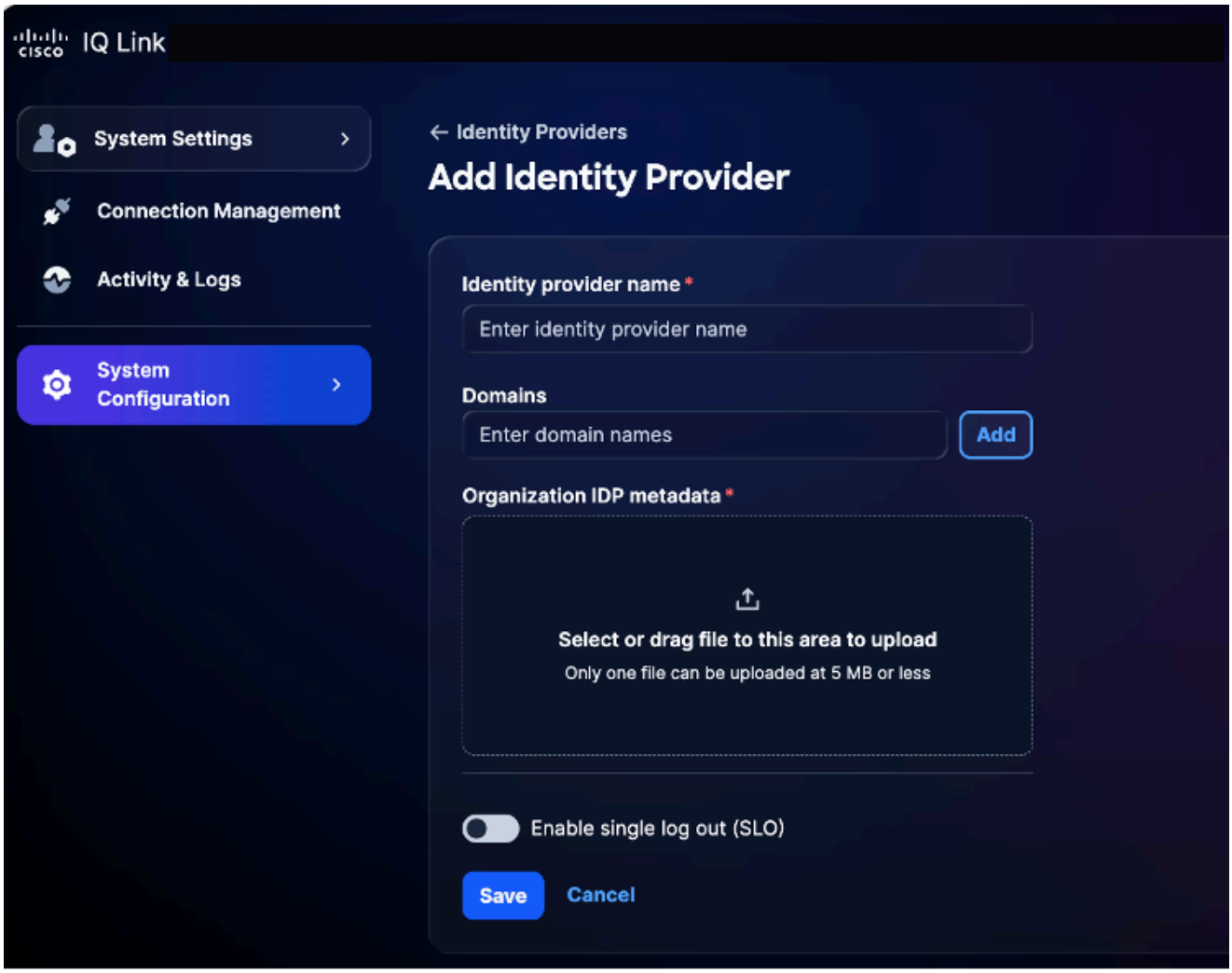
1. Kies in Systeeminstellingen de optie Systeemconfiguratie > Identiteitsproviders. De pagina Identiteitsproviders wordt weergegeven.



IDP-startpagina

2. Klik op Identiteitsprovider toevoegen. De pagina Identiteitsprovider toevoegen wordt

weergegeven.



Identiteitsprovider toevoegen

Opmerking: Er kan slechts één (1) IDP op een bepaald moment worden toegevoegd.

3. Voer de naam van de identiteitsprovider in.

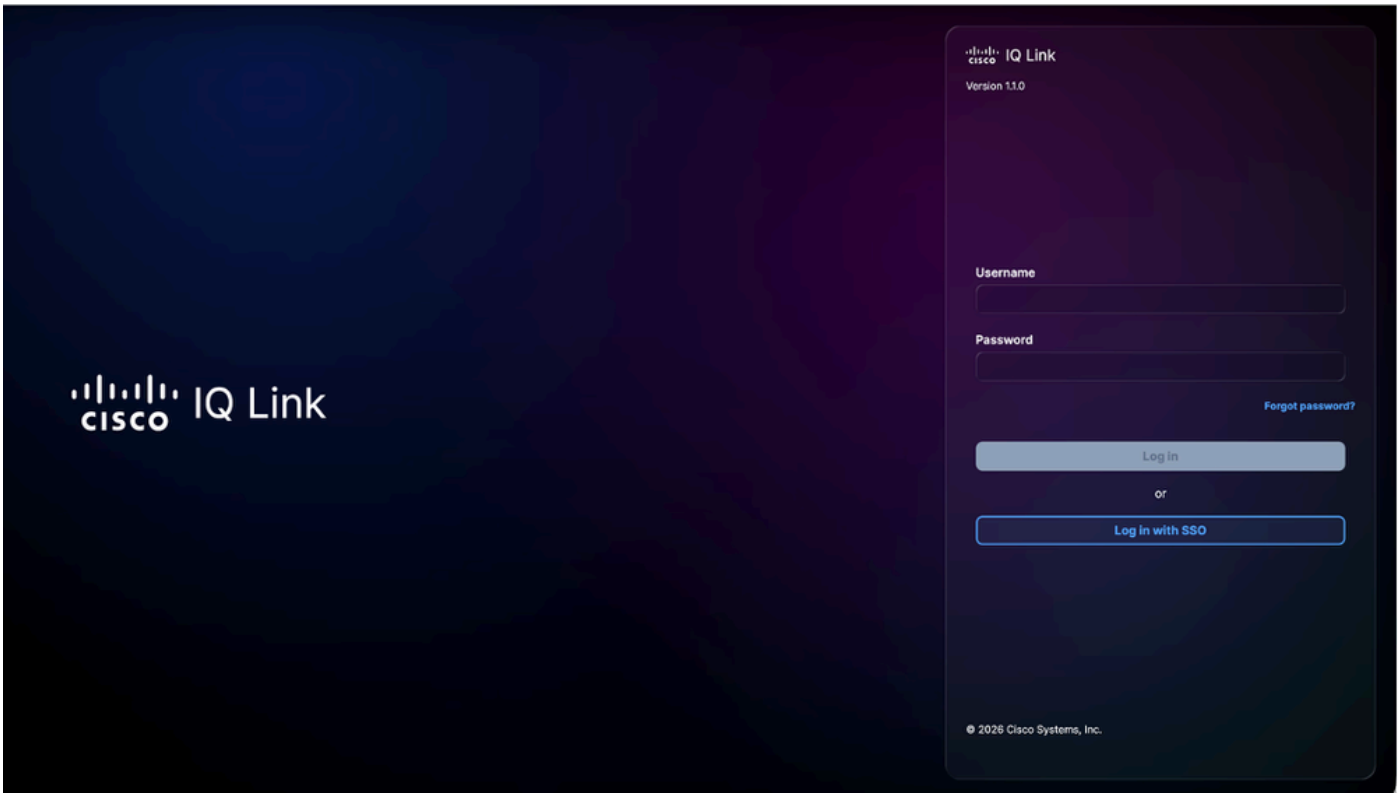
4. Klik op Toevoegen om een door Cisco IQ Link geconfigureerde domeinnaam toe te voegen aan het veld Domeinen.

5. Sleep of upload het SAML-metagegevensbestand dat is verkregen uit de IDP-toepassing in het veld IDP-metagegevens van de organisatie. Dit bestand bevat certificaatgegevens en gegevens over de entiteit van de Serviceverlener (SP).

6. (Optioneel) Schakel de knop Enkelvoudige uitlogknop inschakelen in. U kunt de SLO later ook inschakelen.

7. Klik op Opslaan.

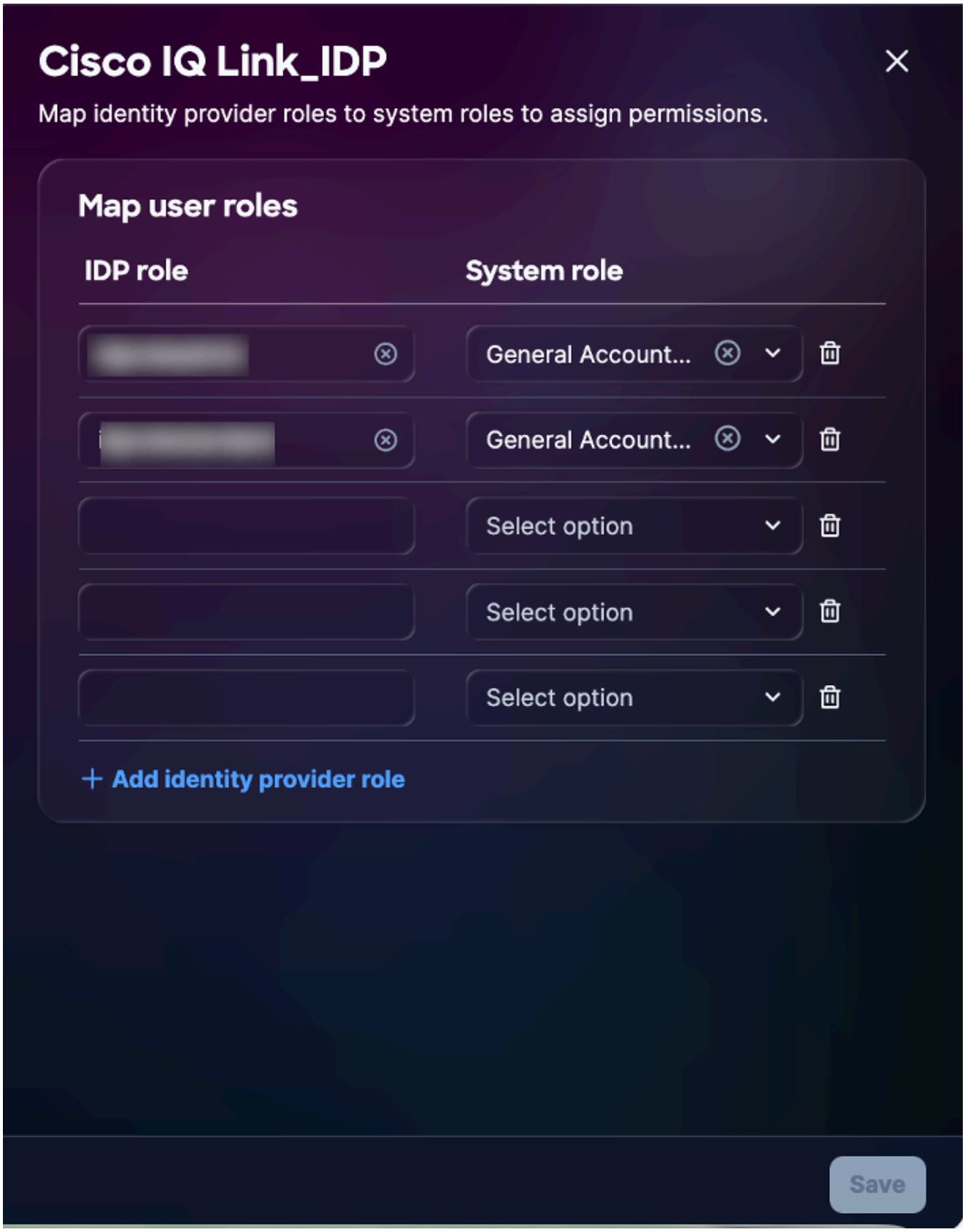
Eenmaal geconfigureerd, geeft de aanmeldingspagina een optie weer om in te loggen met SSO (via IDP).



Aanmelden bij Cisco IQ Link

Configuratie roltoewijzing

1. Selecteer in de toegevoegde IDP het pictogram Meer opties > Rollen toewijzen. De pagina Gebruikersrollen toewijzen wordt weergegeven.



Toewijzing van gebruikersrollen

2. Voer een IDP-rol in voor de geselecteerde systeemrol. De volgende systeemrollen worden ondersteund:

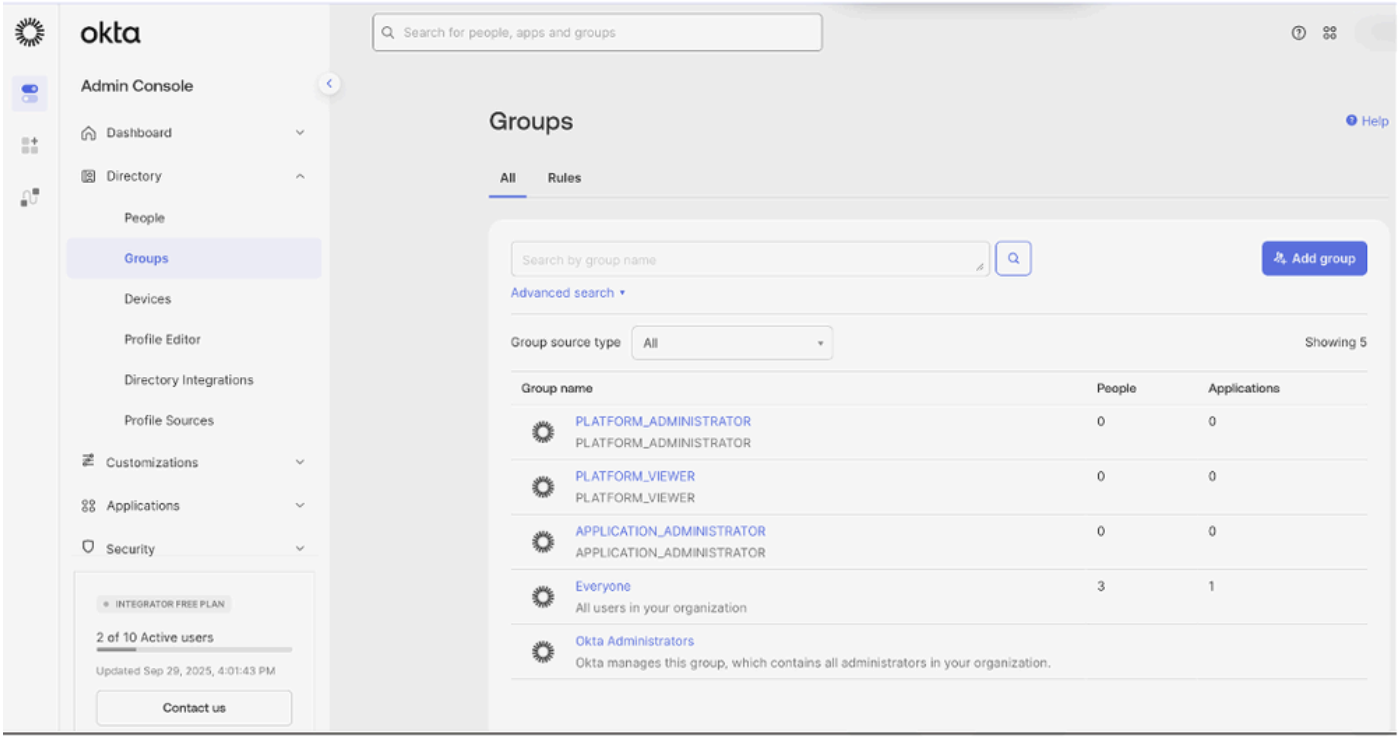
- Algemene accountbeheerder: de algemene accountbeheerder heeft volledige machtigingen

om alle acties in het product uit te voeren

- Algemene accountviewer: de algemene accountviewer heeft alleen-lezen toegang

---

Opmerking: De IDP-rol is een open tekstveld. Het moet exact overeenkomen met de groep- of rolnaam die is geconfigureerd in de IDP van uw organisatie. Een voorbeeld van Okta-groepen wordt hieronder gedeeld.



referentie voor roltoewijzing

3. Voeg extra rollen toe zoals vereist door op Identiteitsproviderrol toevoegen te klikken.

4. Klik op Opslaan.

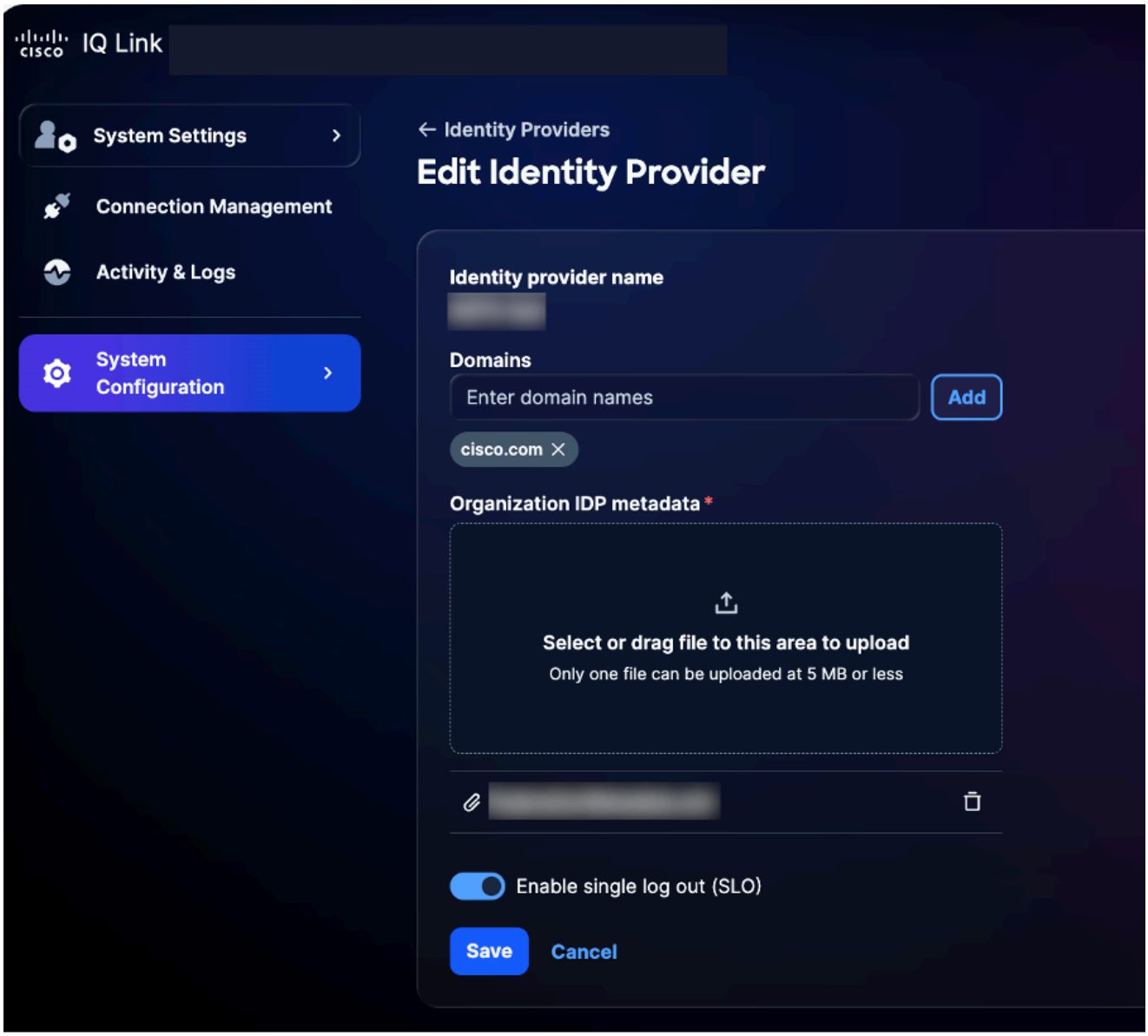
Configuratie eenmalige aanmelding

Als u Single Logout Configuration (SLO) wilt inschakelen, moet u metagegevens uploaden die de SLO-URL bevatten. U kunt dit configureren door de instellingen van uw Identity Provider te bewerken en de schakelaar voor Single Log Out inschakelen in te schakelen. De SLO-configuratie voltooien:

1. Klik op de pagina Identiteitsproviders op Openbaar SP-certificaat downloaden.

Openbaar certificaat downloaden

2. Sla het downloadbestand op als sp-public-key.crt.
3. Navigeer naar uw IDP-portal.
4. Upload het bestand met het handtekeningcertificaat dat is gegenereerd in IDP SAML Configuration for SSO.
5. Download het IDP-metagegevensbestand opnieuw.
6. Kies op de pagina Identiteitsproviders het pictogram Meer opties van de toegevoegde IDP > Bewerken.



Identiteitsprovider bewerken

7. Schakel de knop Single Log Out (SLO) inschakelen in.
8. Upload het nieuw gedownloade metagegevensbestand.
9. Gebruik de volgende controlelijst om de SSO- en SLO-functionaliteit te controleren:

Controlelijst voor verificatie:

- De aanmelding van de beheerder van de lokale account is voltooid
- IDP-portal is geconfigureerd en ingericht
- IDP wordt toegevoegd aan Cisco IQ met de status "Succes"
- Roltoewijzingen worden geconfigureerd en getest

- SP-metagegevens worden gedownload en het certificaat wordt uitgepakt
- Als SLO is ingeschakeld, is de SLO-configuratie compleet met het echte handtekeningcertificaat
- End-to-end SSO/SLO-flow wordt met succes getest

Problemen met IDP oplossen

De volgende lijst bevat veelvoorkomende problemen en mogelijke oplossingen om problemen met betrekking tot de IDP-status, certificaatfouten, SSO-aanmeldingsfouten en SLO-configuratie snel te identificeren en op te lossen:

Tabel 4: Problemen oplossen

uitgeven	Oplossing
IDP-status wordt weergegeven als "Onvolledig"	De configuraties voor roltoewijzing controleren
Certificaatfouten	Formaat en geldigheid van certificaat controleren
Aanmeldingsfouten voor eenmalige aanmelding	Attribuuttoewijzing en groepstoewijzingen valideren
SLO werkt niet zoals verwacht	Controleer of het certificaat correct is geüpload en SLO-URL's zijn geconfigureerd

ADFS IDP SAML-configuratie voor SSO

Deze sectie biedt richtlijnen voor het configureren van Microsoft Active Directory (AD) Federation Services (ADFS) als de SAML IDP voor Cisco IQ.

Vereisten voor het configureren van ADFS IDP SAML voor SSO

- ADFS 6.0+ wordt aanbevolen
- Windows Server 2012 R2+
- Geïntegreerde AD-integratie
- SSL/Transport Layer Security (TLS)-certificaten op ADFS
- Toegang tot Cisco IQ voor accountbeheerders
- Administratieve toegang tot ADFS-server (Windows Server)

- PowerShell-toegang op ADFS-server
- Netwerkconnectiviteit tussen ADFS en Cisco IQ
- Configuratiegegevens ADFS-server (zoals weergegeven in onderstaande tabel)

Tabel 5: ADFS-serverconfiguratie

Item	Beschrijving	Voorbeeld
Cisco IQ FQDN	Hostnaam voor gebruikersimplementatie	devxx-23.cx-xxx-xxx.cisco.com
ADFS Server-URL	Adres ADFS-server gebruiker	https://ad-fs.dev.local
bedrijfsdomein	E-maildomein	company.com
AD-groepen	AD-groep Domeinnamen (DN)	CN=Rol - CXIQ-ontwikkelaars

ADFS-servers configureren

ADFS configureren:

1. Kies in Systeeminstellingen de optie Systeemconfiguratie > Identiteitsproviders. De pagina Identiteitsproviders wordt weergegeven.

Downloadopties

2. Klik op Openbaar SP-certificaat downloaden en SP-metagegevens downloaden om deze bestanden te downloaden.
3. Kopieer en sla de bestanden service-provider-metadata.xml en service-provider-certificate.crt op in de ADFS-directory (bijvoorbeeld C:-certificate.crt).
4. Log in op de ADFS-server.

5. Klik in het menu ADFS-beheer op Vertrouwen van derden vertrouwen.
6. Klik in het menu Vertrouwende partij op Vertrouwende partij toevoegen. De nieuwe wizard wordt geopend.
7. Klik op het keuzerondje Claims Aware.
8. Klik op Start om verder te gaan met de configuratie.
9. Klik op Gegevens over de vertrouwende partij importeren uit een bestand om gegevens uit het bestand op te halen dat is opgeslagen als onderdeel van stap 3.
10. Klik op Bladeren om het SP-metagegevensbestand te selecteren en het uploaden van het bestand te voltooien.
11. Klik op Next (Volgende).
12. Voer een weergavenaam in (bijvoorbeeld "CIQ-Stage"), voeg relevante notities toe en klik op Volgende.
13. Klik op de pagina Toegangsbeleid kiezen op Iedereen toestaan (of het beleid dat vereist is voor de beveiligingsconfiguratie van uw organisatie).
14. Klik op Volgende via de overige schermen.
15. Klik op Sluiten om de vertrouwensconfiguratie van de afhankelijke partij te voltooien.

Opmerking: selecteer "Iedereen toestaan met MFA" niet, tenzij uw ADFS-server een geregistreerde Multi-Factor Authentication (MFA)-adapter heeft (bijvoorbeeld Azure MFA of *Time-Based One-Time Password (TOTP) geconfigureerd).
Als dit beleid is ingeschakeld zonder een geconfigureerde MFA-provider, verifieert ADFS de gebruiker, maar weigert uiteindelijk het verzoek met de status urn: oasis:names:tc:SAML:2.0:status:RequestDenied. Omdat de SAML-reactie geen bewering bevat, mislukt de plug-in en meldt een fout "ontbrekende e-mail".

De optie "Iedereen met MFB toestaan" is geselecteerd.

Oplossing: Controleer in PowerShell het huidige beleid door de volgende opdracht uit te voeren.

```
Get-AdfsRelyingPartyTrust -Name “

    ”).AccessControlPolicyName
```

Voer de volgende opdracht uit om "Iedereen toestaan" in te stellen (geen MFB-vereiste):

```
Set-AdfsRelyingPartyTrust -TargetName “

     ” -AccessControlPolicyName “Permit everyone”
```

U kunt ook het vertrouwen van de vertrouwenspersoon creëren via PowerShell:

```
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-claimregels configureren

Voer de stappen uit die in de volgende secties worden vermeld om ADFS-claimregels te configureren.

Vereiste claims

Raadpleeg de volgende tabel voor de vereiste claims.

Tabel 6: Vereiste vorderingen

aanspraak	Doel	bron
Email	Gebruikersidentificatie	AD Mail
Weergavenaam	Volledige naam van de gebruiker	AD-weergavenaam
UPN	Public Key Infrastructure (PKI)/certificaatverificatie	ADFS koppelt het clientcertificaat aan een AD-gebruiker via de hoofdgebruikersnaam (UPN)
NaamID	SAML-onderwerp	Transformeren van e-mail
Groepen	Toegang op basis van rollen	Lidmaatschap AD-groep (lid van)

Toepassing van claimregels

1. Definieer de naam van uw Relying Party Trust (bijvoorbeeld "Cisco IQ - Stage").

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

2. Bepaal claimregels voor het verzenden van gebruikersinformatie en groepslidmaatschap naar Cisco IQ.

```
$claimRules = @’

@RuleTemplate = “LdapClaims”

@RuleName = “Send Email and Name”

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

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

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

3. Pas de claimregels toe door de volgende opdracht uit te voeren:

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

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

Waarschuwing: in elke AD-gebruikersaccount moet het e-mailkenmerk zijn ingevuld. Als dit kenmerk ontbreekt, bevat de SAML-bevestiging geen e-mailclaim, wat resulteert in een authenticatieafwijzing.

Voer de volgende PowerShell-opdracht uit om het e-mailadres van een gebruiker bij te werken:

```
Set-ADUser -Identity “

     ” -EmailAddress “

      ”
```

Gebruikersgroepen controleren

1. Stel de gebruikersnaam in om het groepslidmaatschap van de gebruiker te controleren.

```
$username = “testuser”
```

2. Voer de volgende opdrachten uit om het gebruikersaccount te vinden:

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

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

3. Geef de groepen weer waartoe de gebruiker behoort.

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

Voorbeeld uitvoer:

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

ADFS configureren om het SP-ondertekeningscertificaat te vertrouwen

1. In de ADFS-server importeert u het SP-certificaat in de TrustedPeople-opslag.

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

2. Kies een van de volgende opties:

Opmerking: het SP-certificaat wordt afgegeven door een interne certificeringsinstantie (CA) die ADFS niet kan valideren via de standaardketen van vertrouwen.

- Schakel ketenvalidatie wereldwijd uit voor deze vertrouwende partij

```
Set-AdfsRelyingPartyTrust `
    -TargetIdentifier “


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

OF

- Als het SP-certificaat is afgegeven door een CA (niet zelf ondertekend), importeert u het CA-certificaat dat is afgegeven in het basiscertificaatarchief:

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

3. Pas de wijzigingen toe door de ADFS-service opnieuw te starten.

```
Restart-Service adfssrv
```

PKI-/certificaatverificatie instellen

In dit gedeelte wordt beschreven hoe u naast wachtwoorden op basis van certificaten (d.w.z. smartcard- of softwarecertificaat) verificatie kunt toevoegen. Deze sectie kan worden overgeslagen als alleen-wachtwoordverificatie voldoende is.

De AD CS CA-rol installeren

De CA-rol AD Certificate Services (CS) installeren:

1. Controleer of er al een Enterprise CA in uw domein bestaat door de volgende opdracht uit te voeren:

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

Als de opdracht een geldig antwoord retourneert, kunt u de rest van deze sectie overslaan. Uw omgeving is al geconfigureerd. Als de opdracht aangeeft dat er geen CA is gevonden, gaat u verder met stap 2.

2. Installeer de CA-rol door de volgende opdracht uit te voeren:

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

3. Configureer de CA-rol door de volgende opdracht uit te voeren:

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


     ” `
    -KeyLength 2048 `
```

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

4. Installatie door de volgende opdracht uit te voeren:

```
certutil -ca
```

5. Bevestig dat de service actief en bereikbaar is door de volgende opdracht uit te voeren:

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

Een certificaatsjabloon configureren

U configureert als volgt een certificaatsjabloon met de EKU (Client Authentication Enhanced Key Usage):

1. Open certsrv.msc en vouw de CA-node uit.
2. Klik met de rechtermuisknop op Certificaatsjablonen > Beheren.
3. De gebruikerssjabloon dupliceren.

Opmerking: De ingebouwde gebruikerssjabloon is alleen functioneel of geldig als het certificaat dat ervan wordt afgegeven, de EKU voor clientverificatie bevat.

---

4. Configureer de instellingen op de volgende tabbladen:

- Algemeen: Voer "CIQ User Authentication" in het Naam veld in met een geldigheidsduur van één (1) jaar
- Aanvraag verwerken: Selecteer Handtekening en codering in de vervolgkeuzelijst Doel en vink het selectievakje Privésleutel exporteren toestaan aan
- Onderwerpnaam: Selecteer Bouwen op basis van Active Directory-informatie en voeg een e-mail toe in zowel het Onderwerp- als het SAN-veld

Waarschuwing: de velden Onderwerp en SAN moeten het UPN van een gebruiker of een e-mail bevatten die overeenkomt met een AD-account. Met behulp van deze velden koppelt ADFS het certificaat aan een AD-gebruiker.

- Extensies: Zorg ervoor dat het toepassingsbeleid "Clientverificatie (1.3.6.1.5.5.7.3.2)" omvat
- Beveiliging: voeg domeingebruikers toe en geef ze rechten voor lezen en inschrijven

5. Publiceer de sjabloon met de volgende opdracht:

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

Een gebruikerscertificaat inschrijven

1. Log in als de beoogde gebruiker.
2. Schrijf het certificaat in door de volgende opdracht uit te voeren:

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

3. Controleer de installatie van het certificaat door de volgende opdracht uit te voeren:

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

Een gebruikerscertificaat exporteren vanuit Windows en installeren op de client (Mac)

U kunt als volgt een gebruikerscertificaat van Windows naar Mac exporteren:

1. Exporteer het certificaat vanuit Windows als een PFX-bestand door de volgende opdrachten uit te voeren:

```
$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. Breng het bestand user-cert.pfx over naar uw Mac-apparaat.

3. Importeer het certificaat in de Mac-sleutelhanger door de volgende opdracht uit te voeren:

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


    "
```

Opmerking: nadat u het certificaat hebt geïmporteerd, moet uw browser worden gesloten en opnieuw worden geopend om het te kunnen herkennen.

---

4. Vertrouw op de CA op Mac door het volgende uit te voeren:

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

ADFS-certificaatverificatie-eindpunten inschakelen

ADFS-certificaatverificatie-eindpunten inschakelen:

1. Schakel de vereiste ADFS-certificaateindpunten in door de volgende opdrachten uit te voeren:

```
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. Controleer of alle eindpunten zijn ingeschakeld door de volgende opdracht uit te voeren:

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

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

Certificaatverificatie inschakelen als primaire

De certificaatverificatie als primaire optie inschakelen:

1. Configureer de primaire verificatieproviders voor intranet- en extranettoegang met de volgende opdracht:

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

2. Controleer of beide lijsten CertificateAuthentication en FormsAuthentication bevatten met de volgende opdrachten:

```
(Get-AdfsGlobalAuthenticationPolicy).PrimaryIntranetAuthenticationProvider

(Get-AdfsGlobalAuthenticationPolicy).PrimaryExtranetAuthenticationProvider
```

3. Controleer de huidige configuratie van de TLS-clientpoort met de volgende opdracht:

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

4. Als de TlsClientPort geen 49443 is, werkt u de poort bij en start u de ADFS-service opnieuw op

met de volgende opdrachten:

```
Set-AdfsProperties -TlsClientPort 49443

Restart-Service adfssrv
```

Oplossingen voor SCchannel/TLS (KRITIEK voor PKI)

Met de stappen in de volgende secties worden CERT_E_UNTRUSTEDROOT (0x800B0109)-fouten opgelost, waardoor certificaatverificatie niet werkt.

Bindende SSL-certificaten op poort 49443

SSL-certificaten binden op poort 49443:

1. Verwijder bestaande SSL-certificaatbinding(en) op poort 49443 met de volgende opdracht:

```
netsh http delete sslcert hostnameport=

     :49443
```

2. Maak een nieuwe binding met client certificaat onderhandeling ingeschakeld met behulp van de volgende opdracht:

```
netsh http add sslcert hostnameport=

     :49443 `
    certhash=

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

3. Controleer of de onderhandeling over het clientcertificaat is ingeschakeld met behulp van de volgende opdracht:

```
netsh http show sslcert hostnameport=

     :49443
```

De certificaatopslag opschonen (KRITIEK)

Zo ruimt u het certificaatarchief op:

 Waarschuwing: Windows SChannel wijst alle clientcertificaten af als er niet-zelfondertekende certificaten aanwezig zijn in het Trusted Root-archief. Dit is de belangrijkste oorzaak van PKI-fouten.

---

1. Identificeer niet-zelfondertekende certificaten in het Trusted Root-archief door de volgende opdracht uit te voeren:

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

2. Verplaats deze certificaten naar het tussenliggende CA-archief door de volgende opdracht uit te voeren:

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

3. Controleer of er geen niet-zelfondertekende certificaten in het basisarchief aanwezig zijn door de volgende opdracht uit te voeren:

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

Oplossingen voor het SChannel-register (KRITIEK)

U configureert als volgt de registerinstellingen van SChannel om een correcte certificaatverificatie te garanderen:

1. Definieer de variabele voor het registerpad met de volgende opdracht:

```
$regPath = “HKLM:”
```

2. Pas de registerinstellingen toe die in de onderstaande tabel zijn gedefinieerd met behulp van de volgende opdrachten:

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

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

Tabel 7: Instellingen voor Schannel-register

instelling	Waarde	Doel
ClientAuthTrustMode	2	Hiermee kan exclusieve CA-trust het standaardvalidatiepad corrigeren.
SendTrustedIssuerList	0	Voorkomt dat de server de volledige lijst met vertrouwde uitgevers verzendt tijdens de TLS-handshake.

Het CA-certificaatarchief controleren

Zo verifieert u het CA-certificaatarchief:

Opmerking: het CA-certificaat dat gebruikerscertificaten afgeeft, moet zich in het SystemCertificates-archief bevinden om ervoor te zorgen dat het correct wordt herkend.

---

1. Definieer de duimafdruk van uw CA-certificaat met de volgende opdracht:

```
$caThumbprint = “
```

”

2. Controleer of het CA-certificaat al aanwezig is in de LocalMachinestore met de volgende opdracht:

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

Als het certificaat niet wordt gevonden, importeert u het in de LocalMachinestore:

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

De ADFS-server opnieuw opstarten (VERPLICHT)

Start de ADFS-server opnieuw op met de volgende opdracht:

```
Restart-Computer -Force
```

Opmerking: de registerwijziging ClientAuthTrustMode wordt pas van kracht nadat de server opnieuw is opgestart.

ADFS-metagegevens exporteren

U kunt uw ADFS-metagegevens downloaden met behulp van PowerShell of uw webbrowser.

PowerShell

ADFS-metagegevens exporteren met PowerShell:

1. Open PowerShell op uw ADFS-server.
2. Voer de volgende opdrachten uit om het metagegevensbestand te downloaden.

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

Nadat de opdrachten zijn uitgevoerd, wordt het metagegevensbestand opgeslagen in C:-metadata.xml.

webbrowser

ADFS-metagegevens exporteren met een webbrowser:

1. Ga naar https://<your-adfs-server>/FederationMetadata/2007-06/FederationMetadata.xml.
2. Vervang <your-adfs-server> door de hostnaam van uw ADFS-server.
3. Sla het XML-bestand met metagegevens op uw computer op wanneer daarom wordt gevraagd.

Configureren op Cisco IQ

Configureren op Cisco IQ:

1. Breng adfs-metadata.xml over naar uw werkstation.
2. Navigeer in Cisco IQ naar Systeeminstellingen > Systeemconfiguratie > Identiteitsproviders.
3. Upload het ADFS-metagegevensbestand om het IDP-certificaat, de Entiteit-ID en de SSO-URL automatisch uit te pakken.
4. Sla de configuratie op.

Opmerking: Als ADFS een automatische rollover voor het ondertekenen van certificaten voor tokens uitvoert, moet u het metagegevensbestand opnieuw exporteren en uploaden naar Cisco IQ om ervoor te zorgen dat de verificatie wordt voortgezet.

ADFS IDP toevoegen

1. Klik op de pagina Identiteitsaanbieders op Identiteitsaanbieder toevoegen.
2. Voer de naam van de identiteitsprovider in.
3. Voer de domeinnamen in (bijvoorbeeld company.com).
4. (Optioneel) Schakel indien nodig de knop Enkelvoudige afmeldoptie inschakelen in.
5. Sleep of upload het SAML-metagegevensbestand dat is verkregen uit de IDP-toepassing in het veld IDP-metagegevens uploaden.
6. Klik op Save (Opslaan).

Opmerking: de status wordt weergegeven als "Onvolledig" totdat roltoewijzing is voltooid; dit is verwacht gedrag.

Roltoewijzing configureren

Voordat u roltoewijzing configureert, moet u ervoor zorgen dat u groepen kunt vinden in AD die u kunt gebruiken voor toewijzing. Voer de volgende PowerShell-opdracht uit om groepen in AD te zoeken.

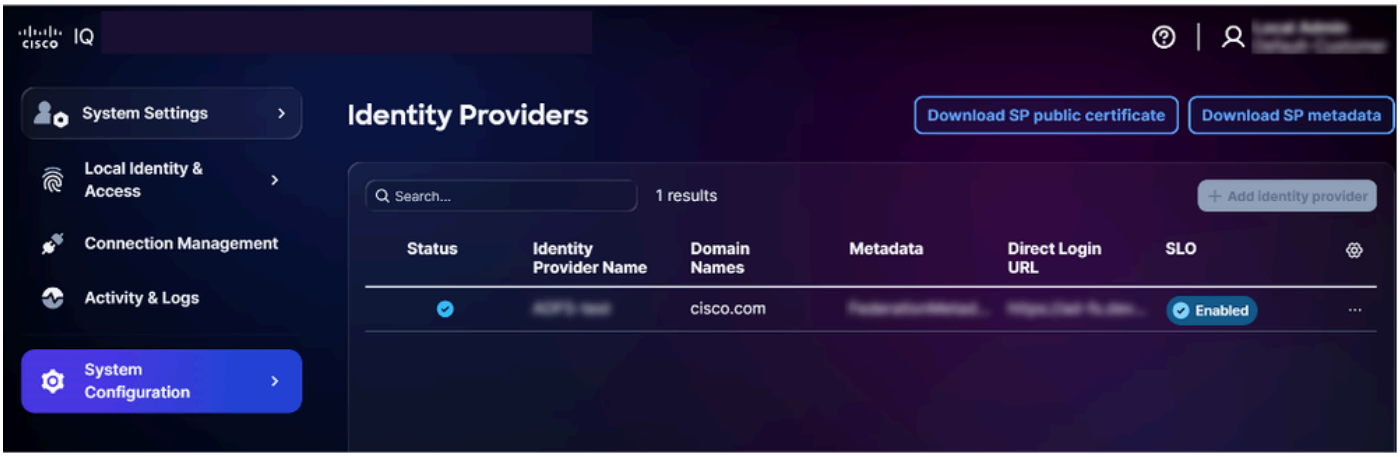
```
$searcher = New-Object DirectoryServices.DirectorySearcher
$searcher.Filter = “(&(objectClass=group)(cn=Role - CXIQ*))”
$searcher.PropertiesToLoad.Add(“distinguishedName”) | Out-Null
$searcher.PropertiesToLoad.Add(“cn”) | Out-Null
$searcher.FindAll() | ForEach-Object { $_.Properties[“distinguishedname”]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

Het systeem zoekt AD rechtstreeks op via het Lightweight Directory Access Protocol (LDAP), waarvoor geen extra modules nodig zijn. Groepsinformatie wordt teruggegeven in de volledige Distinguished Name-indeling, bijvoorbeeld:

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

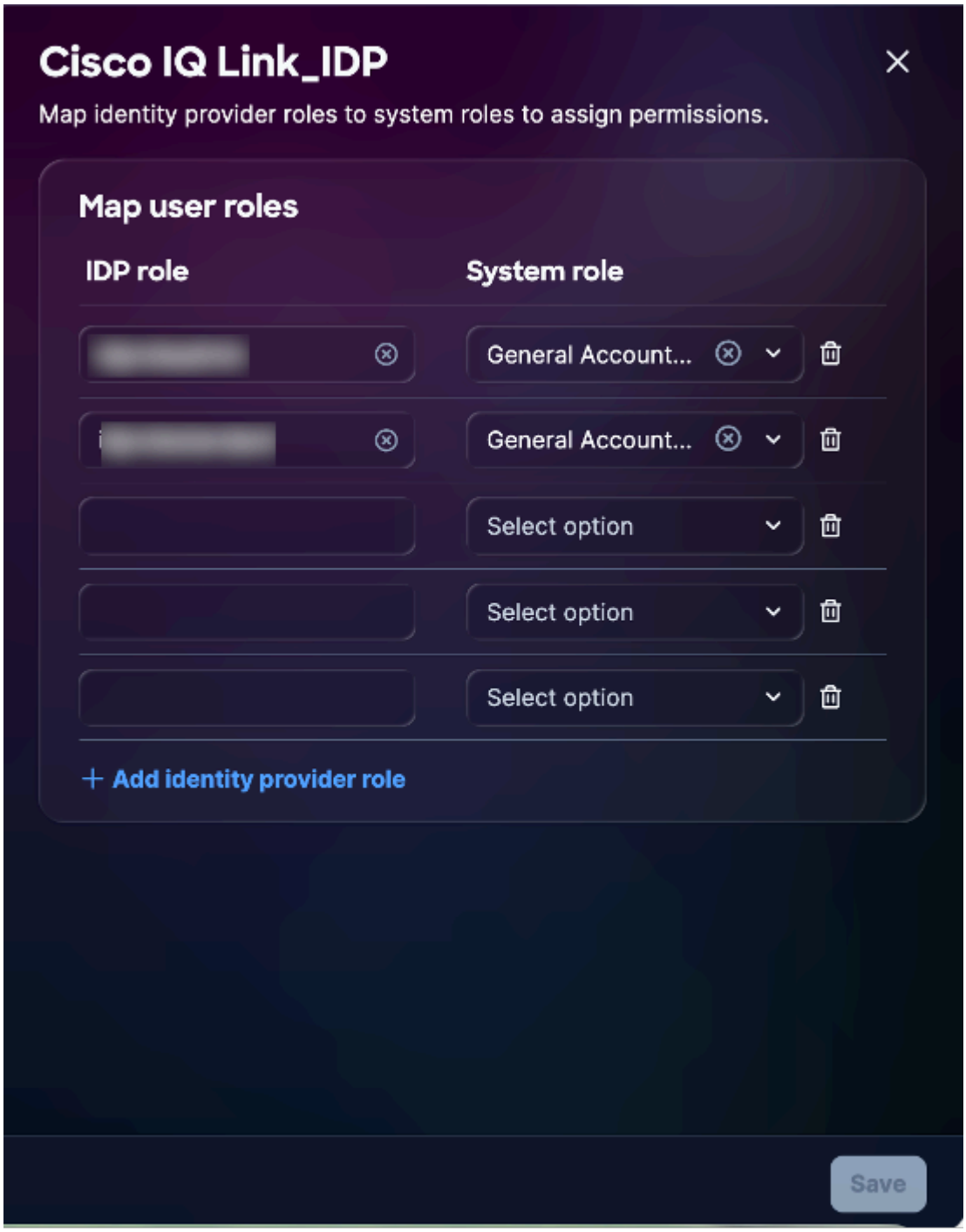
Als de vereiste groepen niet worden vermeld, moeten deze in AD worden gemaakt door een accountbeheerder voordat u de toewijzing van de ADFS-rollen kunt voltooien.

Roltoewijzing configureren:



Rollen toewijzen

1. Kies in de toegevoegde IDP het pictogram Meer opties > Rollen toewijzen. De pagina Gebruikersrollen toewijzen wordt weergegeven.



roltoewijzing

2. Voer een IDP-rol in voor de geselecteerde systeemrol. De volgende systeemrollen worden ondersteund:

- Algemene accountbeheerder: de algemene accountbeheerder heeft volledige rechten om alle acties in het product uit te voeren. De IDP-rol (geparseerde naam) is CXIQ-beheerders.
- Algemene accountviewer: de algemene accountviewer heeft alleen-lezen toegang. De IDP-rol (geparseerde naam) is CXIQ Developers en CXIQ Viewers.

Opmerking: Gebruik geparseerde namen (bijvoorbeeld CXIQ Developers) en geen volledige

domeinnamen.

3. Klik op Opslaan. De status wordt bijgewerkt naar succes.

SChannel Client Cert-test

Om te controleren of SChannel correct is geconfigureerd om clientcertificaten te accepteren, opent u een nieuw PowerShell-venster en voert u de volgende opdracht uit:

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


     :49443/adfs/ls/"
```

De verwachte uitvoer is een HTTP-respons (bijvoorbeeld een omleiding of de ADFS-pagina). Als er een TLS-handshake-fout optreedt, is de verbinding mislukt.

End-to-end browsertesten voor PKI Flow

Voordat u begint met end-to-end browsertests voor PKI-flow, moet u ervoor zorgen dat het gebruikerscertificaat is geïnstalleerd in macOS Keychain (zie Het gebruikerscertificaat importeren op de clientcomputer (macOS) onder Certificaatgebaseerde verificatie configureren voor meer informatie).

Om te testen:

1. Navigeer naar de applicatie SAML login URL. De ADFS bevat opties voor certificaten en wachtwoorden.
2. Kies Certificaatverificatie. De browser vraagt om het certificaat.
3. Upload het certificaat. De ADFS verifieert de gebruiker, stuurt het verzoek om met een SAML-reactie en stelt een nieuwe sessie in.

End-to-end browsertesten voor wachtwoordstroom

Voordat u begint met end-to-end browsertests voor wachtwoordstroom:

1. Navigeer naar de applicatie SAML login URL. De ADFS bevat opties voor certificaten en wachtwoorden.
2. Selecteer Wachtwoord-/formulierverificatie.
3. Voer een gebruikersnaam in.
4. Voer een wachtwoord in.
5. Controleer of de aanmelding succesvol is.

Opmerking: beide stromen moeten tegelijkertijd werken.

Problemen met ADFS oplossen

De volgende lijst bevat veelvoorkomende problemen en mogelijke oplossingen om problemen met betrekking tot de ADFS-status, certificaatfouten, SSO-aanmeldingsfouten en SLO-configuratie snel te identificeren en op te lossen.

Tabel 8: ADFS-problemen

uitgeven	Symptomen / beschrijving	Oorzaken / Controles / Workarounds en Fixes
Groepen niet geëxtraheerd	Geen rollen na aanmelding	• Ontbrekende claimregel: voer de instructies opnieuw uit in ADFS-claimregels configureren • Verkeerde groepsattribuut: Moet http://schemas.xmlsoap.org/claims/Group zijn • Gebruiker bevindt zich niet in advertentiegroepen
Decodering mislukt	"Mislukt om assertion te decoderen" in logs	Configuratie controleren op ADFS-certificaatconfiguratie
aanmeldingslus	Vastgelopen in verificatie- of aanmeldingslus	• Ongeldige ACS-URL: Verifiëren: https://your-fqdn/saml/acs • Cookie mismatch: Controleer browsercookies voor het juiste

uitgeven	Symptomen / beschrijving	Oorzaken / Controles / Workarounds en Fixes
		domein

Diagnostische opdrachten om problemen op te lossen

Gebruik de volgende diagnostische opdrachten om te zorgen voor een succesvolle integratie tussen uw ADFS-omgeving en Cisco IQ. Met deze opdrachten kunt u de toegankelijkheid van metagegevens, certificaatconfiguraties en eindpuntinstellingen controleren.

- Toegankelijkheid van ADFS-metagegevens controleren: bevestigt dat de ADFS Federation-metagegevens bereikbaar en openbaar toegankelijk zijn; dit is een kritieke stap voor het vaststellen van het eerste vertrouwen

```
curl -k https://

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

- Het coderingscertificaat valideren: zorgt ervoor dat het juiste coderingscertificaat is gekoppeld aan de Cisco IQ Relying Party Trust

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

- SAML-eindpuntconfiguratie controleren: controleert of de SAML-eindpunten voor de Cisco IQ Trust correct zijn geconfigureerd en of verificatieverzoeken en -beweringen worden gerouteerd naar de verwachte URL's

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

Microsoft Entra ID SAML-configuratie voor SSO

Deze sectie biedt richtlijnen voor het configureren van Microsoft Entra ID (Entra ID) als de SAML IDP voor Cisco IQ, die zowel wachtwoord-gebaseerde als PKI/certificaat-gebaseerde authenticatie

(CBA) ondersteunt.

Vereisten voor het configureren van Entra ID SAML voor SSO

- Microsoft Entra ID tenant (bijvoorbeeld "ciqtestdev.onmicrosoft.com")
- Toegang tot Cisco IQ als wereldwijde beheerder of toepassingsbeheerder
- Connectiviteit tussen Entra ID (cloud) en Cisco IQ
- Enterprise CA geïnstalleerd of bereikbaar (alleen vereist voor PKI)
- Distributiepunt van de Certificate Revocation List (CRL), bereikbaar vanaf internet (alleen vereist voor PKI)

Tabel 9: Entra ID-serverconfiguratie

Item	Beschrijving	Voorbeeld
ID huurder	Gebruikersidentificatiecode invoeren	37352D8F-0EBE-4762-8161-8775FFE897CB
Cisco IQ FQDN	Implementatie-hostnaam	<UW-CIQ-FQDN>
ID IDP-entiteit	Voer URL van uitgever van ID in	https://sts.windows.net/<HUURDER-ID>/
IDP SSO URL	SAML-aanmeldingseindpunt	https://login.microsoftonline.com/<TENANT-ID>/saml2
bedrijfsdomein	E-maildomein voor gebruikers	<UW-DOMEIN>

Entra ID SAML-toepassing configureren

Een bedrijfstoepassing maken

1. Meld u aan bij het Microsoft Entra-beheercentrum.
2. Navigeer naar Identiteit > Toepassingen > Bedrijfstoepassingen.

3. Klik op Nieuwe toepassing > Uw eigen toepassing maken.
4. Voer de naam in (bijvoorbeeld "Cisco IQ").
5. Kies Integreren voor een andere toepassing die u niet in de galerij vindt (niet-galerij).
6. Klik op Maken.

SAML Single Sign-On configureren

Om SAML single sign-on te configureren, moet u het SP-metagegevensbestand uploaden. U kunt deze verkrijgen door de volgende stappen uit te voeren vanuit Virtual Appliance (VA):

1. Kies in Systeeminstellingen de optie Systeemconfiguratie > Identiteitsproviders. De pagina Identiteitsproviders wordt weergegeven.

Downloadopties

2. Klik op SP-metagegevens downloaden om te downloaden. Dit gedownloade SP-metagegevensbestand wordt geüpload om de SAML-configuratie voor eenmalige aanmelding te voltooien.
3. Klik op Bestand metagegevens uploaden om het SP-metagegevensbestand te uploaden. De gegevens uit het SP-metagegevensbestand worden automatisch ingevuld in het scherm SAML-gebaseerd na succesvolle upload.

U kunt er ook voor kiezen om deze gegevens handmatig in te voeren om de instellingen voor eenmalige aanmelding te configureren. SAML Single sign-on handmatig configureren:

1. Navigeer in de Enterprise-toepassing naar Eenmalige aanmelding en kies SAML.
2. Klik in de sectie Basic SAML Configuration op Edit en voer het volgende in:
    a. Identificatiecode (Entiteit-ID): <YOUR-CIQ-FQDN>
    b. Reply URL (ACS URL): https://<YOUR-CIQ-FQDN>/saml/acs
    c. Aanmelden URL: https://<YOUR-CIQ-FQDN>/saml/login

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

3. Klik op Save (Opslaan).

Opmerking: De Entity ID moet exact overeenkomen met wat Cisco IQ gebruikt als de SP Entity ID. Dit is meestal de FQDN van de implementatie.

---

4. Als u SAML-kenmerken en claims wilt configureren, klikt u in het gedeelte Attributen en claims op Bewerken.

5. Configureer de volgende claims:

Tabel 10: Vereiste SAML-claims

aanspraak	bronkenmerk	naamruimte
Unieke gebruikersnaam (NameID)	user.userprincipalname	(standaard)
e-mailadres	user.mail	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
voornaam	user.givenname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
familienaam	user.surname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
naam	user.userprincipalname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
groepen	gebruiker.toewijzende droles	(LEEG — de naamruimte wissen)

Opmerking: Voor de claim groepen:
- Gebruik user.assignedroles als bron - niet gebruikersgroepen
- Het veld Namespace moet leeg zijn. Dit zorgt ervoor dat de attribuutnaam in de SAML-bewering eenvoudig groepen is in plaats van een volledige Uniform Resource Identifier (URI)
- Voeg geen dubbele groepsclaim toe aan user.groups omdat dit conflicten veroorzaakt

---

App-rollen configureren

App Rollen worden geconfigureerd in de App Registratie (niet de Enterprise Application); om App Rollen te configureren:

1. Navigeer naar Identiteit > Toepassingen > App-registraties.
2. Zoek en kies uw toepassing.
3. Ga naar App rollen > Maak app rol.
4. Configureer voor elke benodigde rol het volgende:

- Display name: Bijvoorbeeld Cisco IQ Admins
- Toegestane typen leden: Gebruikers/Groepen
- Waarde: Bijvoorbeeld Cisco IQ-beheerders
- Beschrijving: Bijvoorbeeld Cisco IQ Administrators

5. Klik op Toepassen.

Opmerking: maak rollen die overeenkomen met uw vereisten voor roltoewijzing van Cisco IQ (bijvoorbeeld CXIQ-beheerders, CXIQ-ontwikkelaars, CXIQ-viewers).

App Rollen worden gebruikt in plaats van groepsclaims om de volgende redenen:

- Huurders die alleen in de cloud actief zijn, kunnen geen groepsleernamen verzenden zonder een P1- of P2-licentie
- sAMAaccountName werkt alleen voor groepen die worden gesynchroniseerd vanuit AD op locatie
- Groep-ID-bron verzendt Universally Unique Identifiers (UUID's) die moeilijk in kaart te brengen zijn
- App Rollen verzenden exacte tekenreekswaarden die overeenkomen met de rolverwachtingen van Cisco IQ

Gebruikers toewijzen aan app-rollen

Gebruikers toewijzen aan App Rollen:

1. Ga terug naar Enterprise Application > Gebruikers en groepen.
2. Klik op Gebruiker/groep toevoegen.
3. Kies de gebruiker(s) en wijs de juiste app-rol toe.
4. Klik op Toewijzen. Rolwaarden worden weergegeven als leesbare tekenreeksen in het kenmerk SAML-assertiegroepen.

IDP-metagegevens en -certificaat downloaden

IDP-metagegevens en certificaat downloaden:

1. Ga vanuit de Enterprise Application naar Single sign-on > SAML Signing Certificate sectie.
2. Download Federation Metadata XML (opslaan als entra-id-metadata.xml).

   OF

   Download Certificate (Base64) voor handmatige certificaatinvoer.
3. Noteer de volgende waarden uit het gedeelte Instellen:

- Inlog-URL (IDP SSO URL)
- Azure AD Identifier (IDP Entity ID)
- Afmeldings-URL (IDP SLO-URL)

Opmerking: Aangezien de Entra ID ondertekeningscertificaten periodiek roteert, moet u de metagegevens opnieuw downloaden en naar VA uploaden wanneer het actieve certificaat verandert om een ononderbroken SSO-service te garanderen.

Entra-ID toevoegen

Opmerking: APISIX-routes voor SAML worden automatisch gemaakt wanneer een IDP wordt toegevoegd aan Cisco IQ, waardoor handmatige routeconfiguratie overbodig wordt.

Om Entra ID toe te voegen:

1. Meld u aan bij VA als accountbeheerder.
2. Navigeer naar Systeeminstellingen > Systeemconfiguratie > Identiteitsproviders.
3. Klik op Identiteitsprovider toevoegen.
4. Voer de naam van de IDP in (bijvoorbeeld "Entra ID").
5. Voer de domeinnaam(en) in (bijvoorbeeld "ciqtestdev.onmicrosoft.com" of uw bedrijfsdomein).
6. (Optioneel) Schakel indien nodig de knop Enkelvoudige afmeldoptie inschakelen in.
7. Sleep of upload het entra-id-metadata.xml-bestand dat is verkregen van Entra ID in het veld Upload IDP Metadata.
8. Klik op Save (Opslaan).

Opmerking: de status blijft "Onvolledig" totdat roltoewijzing is voltooid; dit is het verwachte gedrag.

Roltoewijzing configureren

Roltoewijzing configureren:

1. Kies in de toegevoegde IDP het pictogram Meer opties > Kaartrollen. De pagina Gebruikersrollen toewijzen wordt weergegeven.
2. Voer een IDP-rol in voor elke systeemrol. De volgende systeemrollen worden ondersteund:

Tabel 11: Systeemrollen

Systeemrol	IDP-rol (waarde van app-rol)	Beschrijving
Algemene accountbeheerder	CXIQ-beheerders	Volledige rechten voor alle acties
Algemene accountviewer	CXIQ-ontwikkelaars	Alleen-lezen toegang
Algemene accountviewer	CXIQ-viewers	Alleen-lezen toegang

Opmerking: gebruik de tekenreeksen voor de waarde van de rol van de app precies zoals geconfigureerd in Entra ID (zie Toepassingsrollen configureren onder Entra ID SAML-toepassing configureren voor meer informatie).

3. Klik op Opslaan. De status wordt bijgewerkt naar succes.

De SAML-stroom controleren (wachtwoordverificatie)

Zo verifieert u de SAML-stroom:

1. Open een browser in de incognito- of privémodus.
2. Navigeer naar https://<YOUR-CIQ-FQDN>/saml/login.
3. Controleer of u wordt doorgestuurd naar de aanmeldingspagina van Microsoft.
4. Verifieer met uw referenties (en MFA indien geconfigureerd).
5. Controleer na verificatie of u wordt teruggeleid naar /saml/acs en of de Cisco IQ-toepassing wordt weergegeven.

6. Verifieer groepsextractie door de volgende opdracht uit te voeren:

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

verwachte productie

```
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
```

Certificaatgebaseerde verificatie configureren

In dit gedeelte wordt beschreven hoe u CBA naast wachtwoorden kunt toevoegen. Deze sectie kan worden overgeslagen als alleen-wachtwoordverificatie voldoende is.

Voorwaarden voor CBA

- Windows Server met AD Certificate Services (CS) met Enterprise CA geconfigureerd (bijvoorbeeld "DEV-ADCS-CA")
- Toegang voor PowerShell-beheerders op de CA-server
- Certificaat UPN moet overeenkomen met de Entra ID userPrincipalName
- Het CRL-distributiepunt moet toegankelijk zijn via internet

Een certificaatsjabloon maken op AD CS

1. Open certtmpl.msc op de CA-server.
2. Dupliceer de gebruikerssjabloon en noem het "EntraUserCert".
3. De sjabloon configureren:

- Algemeen: Display name EntraUserCert, geldigheid 1–2 jaar
- Verzoek afhandeling: Doel = Handtekening en encryptie
- Onderwerpnaam: Selecteer Levering in de aanvraag

- Extensies: het toepassingsbeleid moet clientverificatie bevatten (1.3.6.1.5.5.7.3.2)
- Beveiliging: geef machtigingen voor lezen en inschrijven aan geverifieerde gebruikers

4. Publiceer de sjabloon met de volgende opdracht:

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

Het aanvragen en afgeven van een gebruikerscertificaat

1. Maak een INF-bestand (Certificate Configuration) (bijvoorbeeld C:-cert.inf) met het volgende PowerShell-script:

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

[NewRequest]
Subject = “CN=



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

[RequestAttributes]
CertificateTemplate = EntraUserCert

[EnhancedKeyUsageExtension]
OID = 1.3.6.1.5.5.7.3.2
OID = 1.3.6.1.4.1.311.20.2.2

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



      &”
_continue_ = “email=



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

2. Vervang **<**USER-UPN**>** door uw Entra-ID UPN (bijvoorbeeld user@ciqtestdev.onmicrosoft.com).

3. Voer de volgende opdracht uit om het certificaat te genereren:

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

4. Voer de volgende opdracht uit om het verzoek bij de certificeringsinstantie in te dienen:

```
certreq -submit -config “

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

5. Voer de volgende opdracht uit om het certificaat op de certificeringsinstantie te installeren:

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

Certificaten exporteren

- Als u het gebruikerscertificaat als een PFX-bestand (voor client) wilt exporteren, voert u het volgende script uit:

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

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

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

- Voer het volgende script uit om het CA Root-certificaat (voor Entra ID) te exporteren:

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

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

Het gebruikerscertificaat importeren op het clientsysteem (macOS)

- Voer de volgende opdracht uit om het gebruikerscertificaat (PFX) te importeren:

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

     ”
```

- Voer de volgende opdracht uit om het CA-hoofdcertificaat te importeren:

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

- U kunt als volgt het CA-certificaat instellen op Always Trust in Keychain Access:
    1. Open sleutelhanger toegang.
    2. Zoek het CA-certificaat en klik op Info ophalen.
    3. Zet onder Vertrouwen op "Altijd vertrouwen".

Opmerking: na het importeren sluit u de browser af en opent u deze opnieuw om het certificaat te laten herkennen.

Het CA-basiscertificaat uploaden naar Entra ID

1. Meld u aan bij het Microsoft Entra-beheercentrum.
2. Navigeer naar Beveiliging > Beveiliging > Certificaatautoriteiten.
3. Klik op Uploaden en selecteer het bestand ca-root.cer.
4. Markeer het als een root CA-certificaat.
5. Voer de URL van het CRL-distributiepunt in (moet openbaar toegankelijk zijn).

CBA inschakelen in verificatiemethoden voor entra-id

1. Navigeer naar Beveiliging > Authenticatiemethoden > Beleid.
2. Klik op Certificaatgebaseerde verificatie om te configureren.
3. CBA inschakelen en de doelgebruikers of -groepen toevoegen.
4. Stel onder Configureren het beveiligingsniveau in op Single Factor-verificatie.

Gebruikersnaambinding configureren

Ga in de CBA-configuratie naar het tabblad Gebruikersnaam-binding en stel de volgende binding in:

- Certificaatveld: PrincipalName
- Gebruikerskenmerk: userPrincipalName

Hiermee wordt de UPN in de alternatieve onderwerpnaam van het certificaat toegewezen aan de gebruiker van de Entra ID.

Controle van de CBA-stroom

1. Open een browser in de incognito- of privémodus.

2. Navigeer naar https://<YOUR-CIQ-FQDN>/saml/login.
3. Voer op de aanmeldingspagina van Microsoft het e-mailadres van de gebruiker in en klik op Volgende.
4. Kies Certificaat of smartcard gebruiken (of automatisch vragen).
5. Kies het toepasselijke gebruikerscertificaat wanneer de browser vraagt om certificaatselectie.
6. Controleer of Entra ID het certificaat valideert, omleidt met een SAML-reactie en een sessie maakt.

Opmerking: zorg ervoor dat u het juiste clientcertificaat selecteert. Het selecteren van een verkeerd certificaat (bijvoorbeeld een cert van een andere gebruiker of een verlopen cert) veroorzaakt een verificatiefout.

Problemen met ingang ID oplossen

De volgende lijst geeft een overzicht van veelvoorkomende problemen en mogelijke oplossingen om problemen met betrekking tot de Entra ID SAML-configuratie snel te identificeren en op te lossen.

Tabel 12: Problemen oplossen

uitgeven	Oorzaak	Oplossen
Ongeldige SAML-reactie – ontbrekende e-mail	SAML-bevestiging heeft geen NameID of e-mailkenmerk	Verifieer de claimconfiguratie van Entra ID (zie SAML Single Sign-On configureren onder Entra ID SAML-toepassing configureren voor meer informatie). Controleer of het e-mailkenmerk van de gebruiker is ingevuld.
Totaal aantal geëxtraheerde groepen: 0	Groepsclaims niet geconfigureerd of verkeerde bron	Gebruik user.assignedroles als bron. Zorg ervoor dat de gebruiker is toegewezen aan een app-rol (zie Gebruikers toewijzen aan app-rollen onder Entra ID SAML-toepassing configureren voor meer informatie).
Groepsclaims dupliceren	Zowel user.groups als user.assignedroles zijn actief	Verwijder de claim user.groups. Bewaar alleen user.assignedroles.
Groepen die als UUID's worden weergegeven	Het bronattribuut is "Group ID"	Gebruik de App Rollen aanpak (zie App Rollen configureren onder Entra ID SAML-toepassing configureren voor meer informatie).

uitgeven	Oorzaak	Oplossen
Attribuutnaam toont lange URI	Het veld Namespace is niet leeg	Wis het veld Naamruimte in de claiminstellingen voor groepen.
Ongeldige SAML-handtekening	IdP-certificaat geroteerd of niet-overeenkomend	Metagegevens opnieuw downloaden van Entra ID en opnieuw uploaden naar Cisco IQ.
AADSTS500191	CRL niet bereikbaar vanaf internet	Publiceer de CRL naar een openbaar toegankelijke URL of gebruik een zelfondertekende CA-benadering (zie CRL Workaround voor Lab-omgevingen voor meer informatie).
Certificaat niet gevraagd	Certificaat niet in sleutelhanger, CA niet vertrouwd op client of CBA niet ingeschakeld	Controleer of het gebruikerscertificaat is geïmporteerd in macOS Keychain Access (zie Het gebruikerscertificaat importeren op de clientcomputer (macOS) onder Verificatie op basis van certificaat configureren voor meer informatie), CBA is ingeschakeld in Entra ID met de vereiste instellingen (zie CBA inschakelen in Verificatiemethoden op basis van certificaat inschakelen onder Verificatie op basis van certificaat configureren voor meer informatie) en Chrome wordt opnieuw gestart om wijzigingen toe te passen.
SAML-bevestiging verlopen	Klok scheef tussen systemen	Clock_skew_seconds verhogen in plugin config (standaard 300, gebruik 30000 voor lab).
Status "Onvolledig" in VA	Roltoewijzing nog niet geconfigureerd	Volledige toewijzing van rollen (zie Roltoewijzing configureren voor meer informatie).

CRL Workaround voor problemen met bereikbaarheid

Als het CRL-distributiepunt van uw CA niet bereikbaar is via internet (gebruikelijk bij laboratoriumopstellingen), gebruikt u een zelf ondertekende CA zonder CRL-vereisten:

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

# Create user cert signed by the CA
```

```
$userCert = New-SelfSignedCertificate `
    -Subject “CN=


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


      &email=


       ”
)
```

Upload alleen de root CA cert naar Entra ID. Omdat het zelf is ondertekend zonder CDP, probeert Entra ID geen CRL-validatie uit.

Checklist voor volledige installatie

In deze sectie wordt een volledige controlelijst voor de installatie van VA met Microsoft Entra ID SAML Application en optionele CBA beschreven.

Entra ID SAML Toepassingsinstelling

- Bedrijfstoepassing maken (niet-galerij) in Entra ID
- Basisconfiguratie van SAML configureren door handmatig SP-metagegevens in te voeren
- Attributen en claims configureren (inclusief e-mail, naam en groepen met user.assignedroles)
- App-rollen maken in app-registratie
- Gebruikers toewijzen aan app-rollen

- Federation Metadata XML downloaden

Cisco IQ-configuratie

- Voeg Identity Provider toe aan Cisco IQ door Entra ID-metagegevens te uploaden
- Toewijzing van rollen configureren om waarden van rollen van apps toe te wijzen aan Cisco IQ-systeemrollen
- Verifieer dat aanmelden met een wachtwoord end-to-end werkt
- Controleren of groepen correct zijn geëxtraheerd in logs

Certificaatgebaseerde verificatie (optioneel)

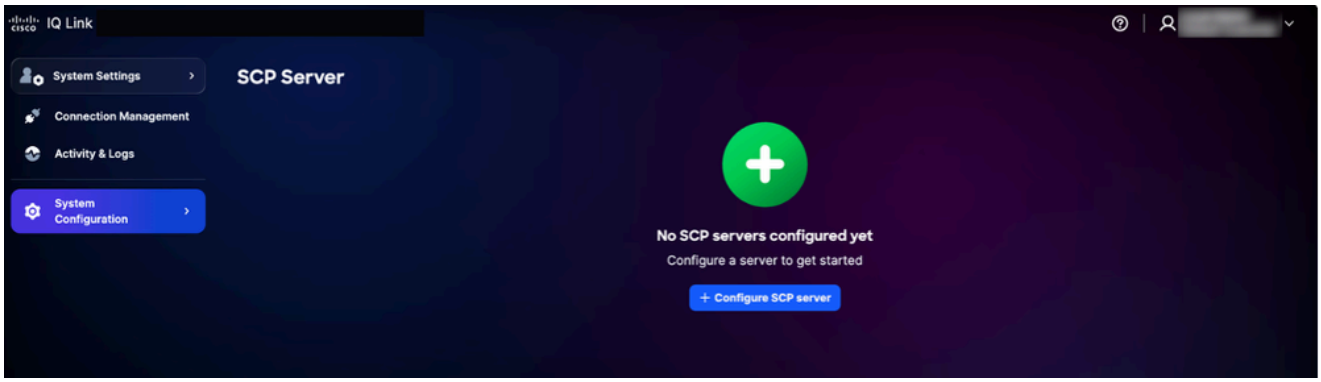
- Certificaatsjabloon maken op AD CS met Client Authentication EKU
- Gebruikerscertificaat uitgeven met UPN-overeenkomende gebruikersidentificatie
- Gebruikerscertificaat exporteren als PFX en installeren op clientsysteem
- Vertrouw het CA-certificaat op het clientsysteem
- CA-basiscertificaat uploaden naar Entra ID onder Bescherming > Certificaatautoriteiten
- CBA inschakelen in verificatiemethoden
- Gebruikersnaambinding configureren (PrincipalName en userPrincipalName)
- Controleren of CBA-aanmelding end-to-end werkt

SCP-servers toevoegen

Deze SCP-server (Secure Copy Protocol) is een voorwaarde voor het importeren van upgradebestanden die essentieel zijn voor het toevoegen, upgraden of patchen van de Cisco IQ-installatie.

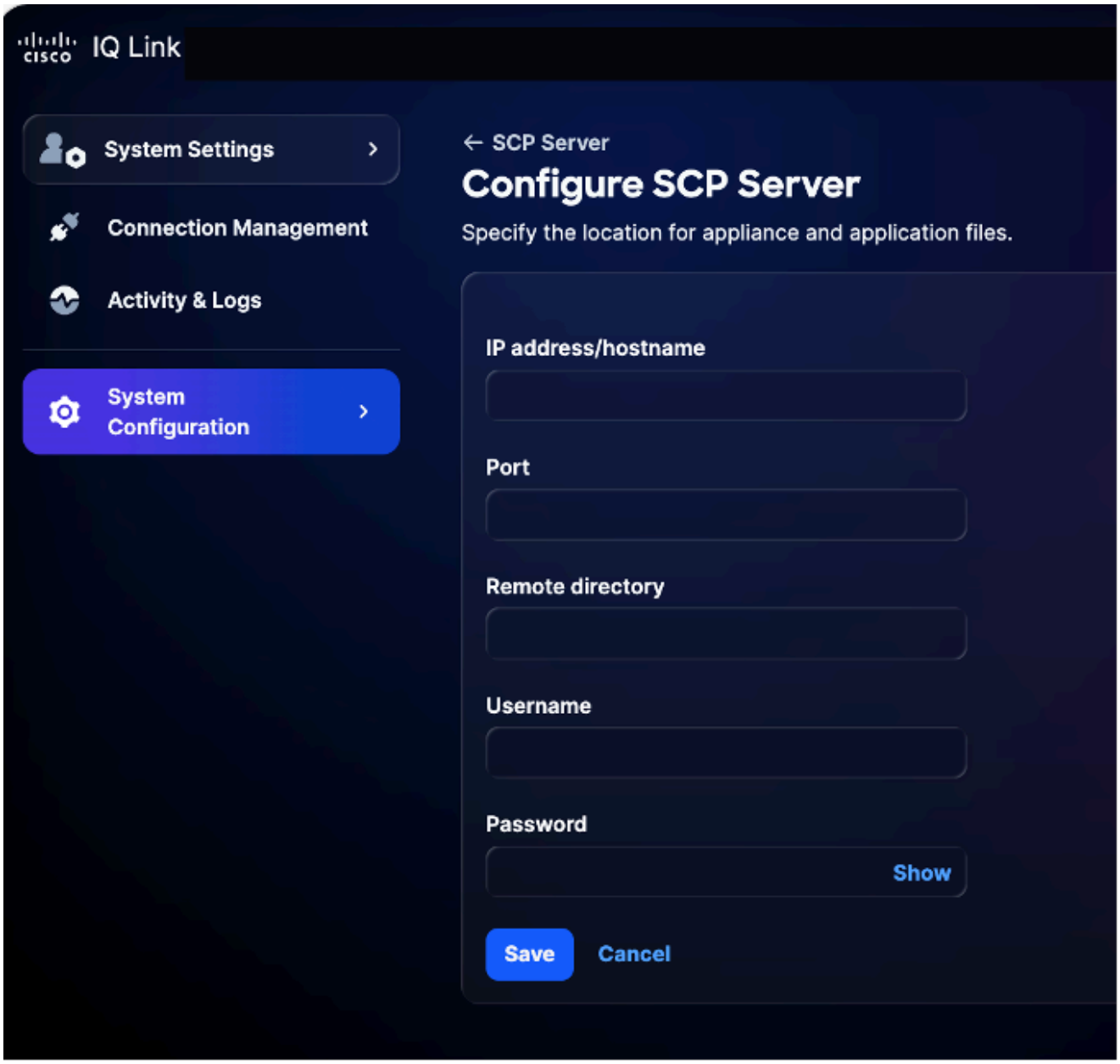
Een SCP-server toevoegen:

1. Kies in Systeeminstellingen de optie Systeemconfiguratie > SCP-server. De pagina SCP-server wordt weergegeven.



Startpagina SCP-server

2. Klik op SCP-server configureren.



SCP-server configureren

3. Voer het IP-adres/de hostnaam in.

4. Voer een Port-nummer in.
5. Voer de externe directory in.
6. Voer een gebruikersnaam in.
7. Voer een wachtwoord in.
8. Klik op Save (Opslaan). Er wordt een bevestiging weergegeven.

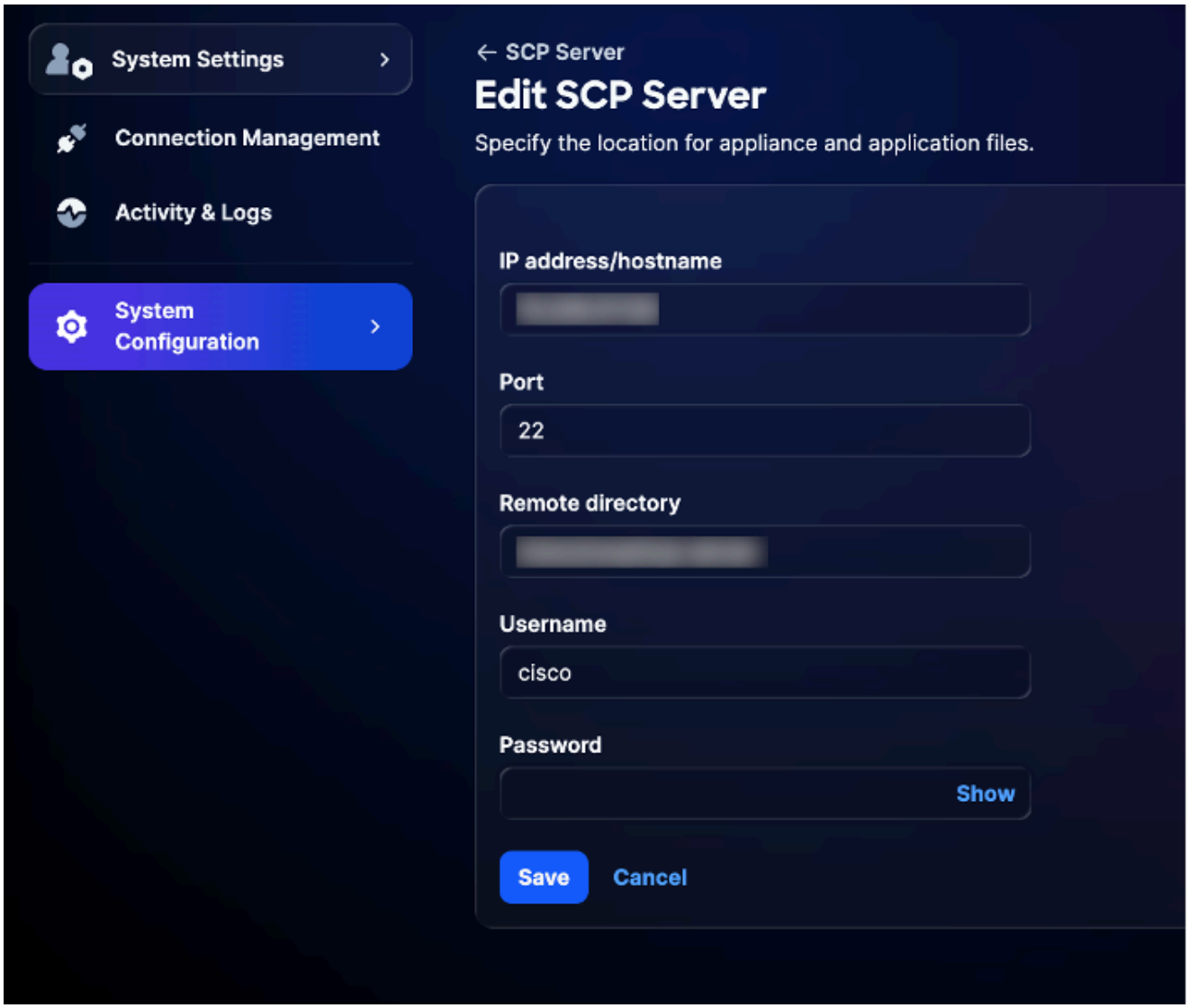
Bestaande SCP-servers bewerken

U bewerkt als volgt een bestaande SCP-server:

1. Navigeer naar de pagina SCP Server.

SCP-server

2. Klik op Bewerken voor de gewenste bestaande SCP-server.



SCP-server bewerken

3. Wijzig de gegevens zoals vereist.
4. Klik op Save (Opslaan).

systeembeheer

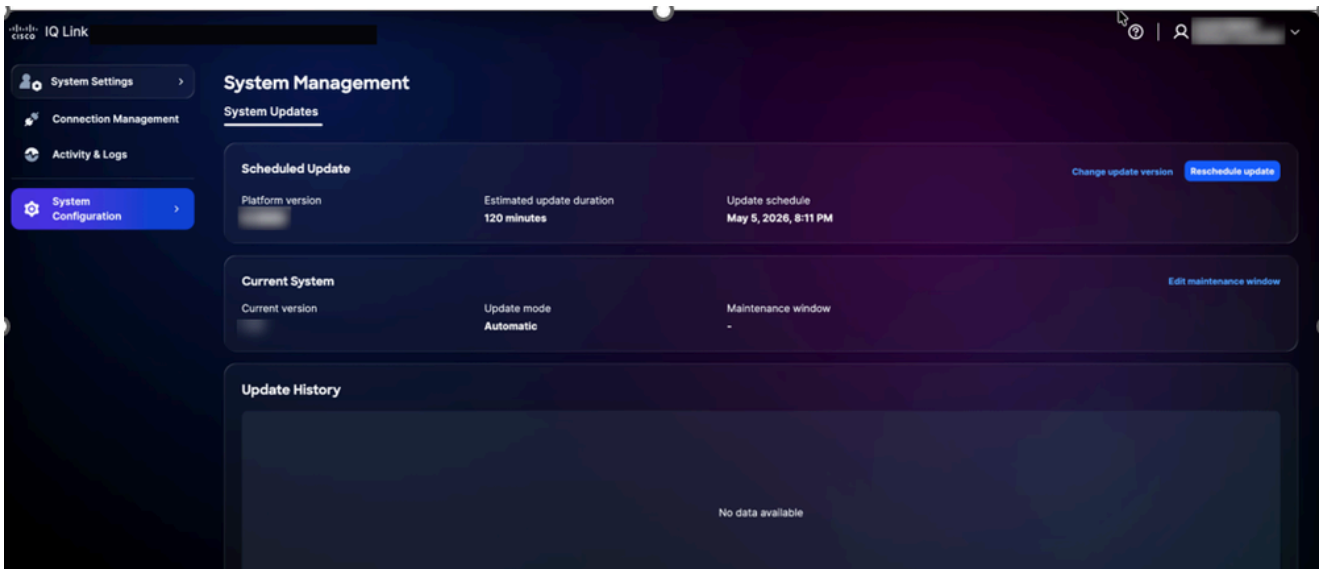
U kunt upgraden naar de nieuwste Cisco IQ Link-versie via de gebruikersinterface. U kunt ook controleren op de Cisco IQ Data Connectors-pagina.

Systeemupdate opnieuw plannen

De systeemupdate opnieuw plannen:

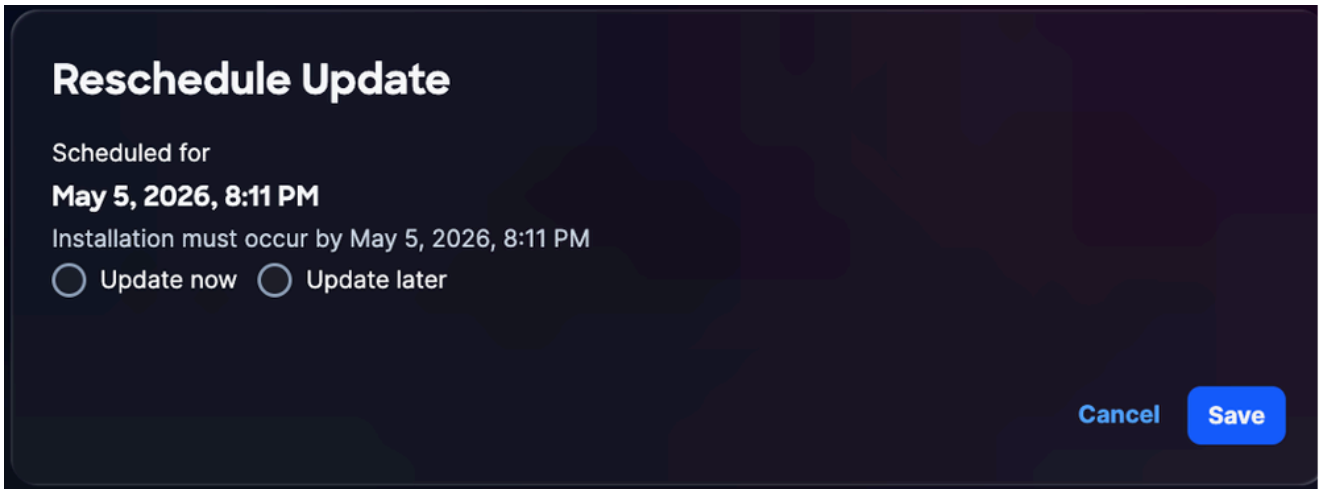
1. Kies in Beheer de optie Systeemconfiguratie > Systeembeheer. De pagina Systeembeheer

wordt weergegeven. Op deze pagina wordt de systeemversie weergegeven die momenteel wordt uitgevoerd. Als er geen updates zijn geconfigureerd, is het gedeelte Updategeschiedenis leeg.



Systeemupgrade

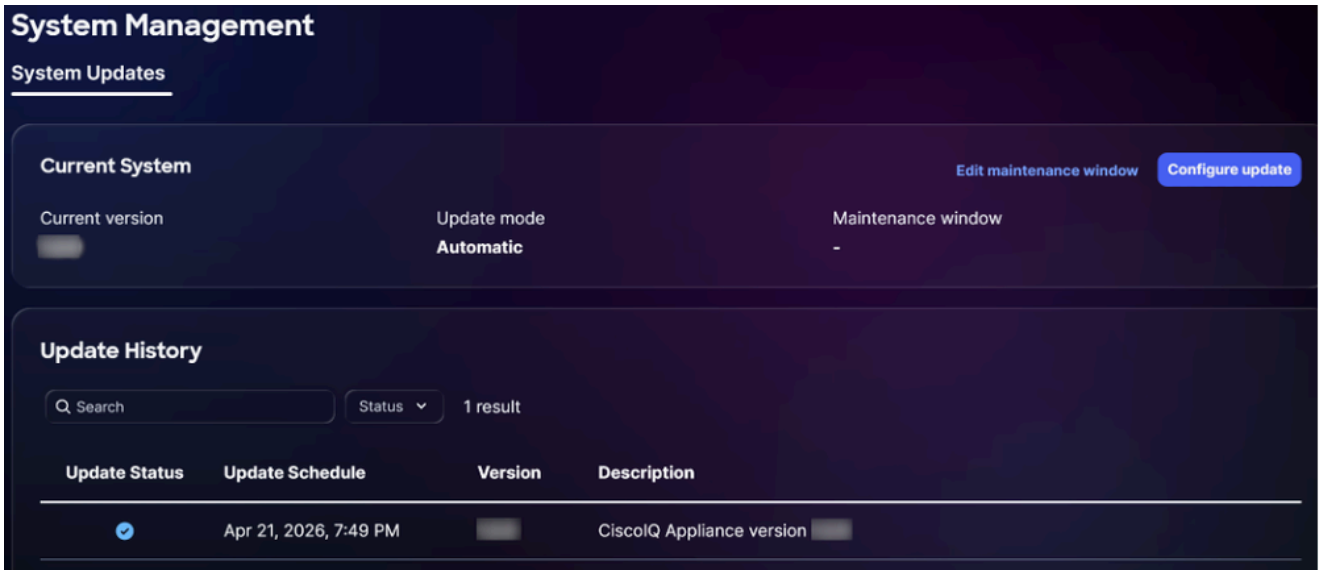
2. Klik op Update opnieuw plannen.



Upgrade opnieuw plannen

3. Kies het keuzerondje Nu bijwerken voor onmiddellijke herplanning of het keuzerondje Later bijwerken om een andere tijd te plannen.

4. Klik op Save (Opslaan). Er wordt een bevestiging weergegeven en u wordt doorgestuurd naar de startpagina Systeemupdate.

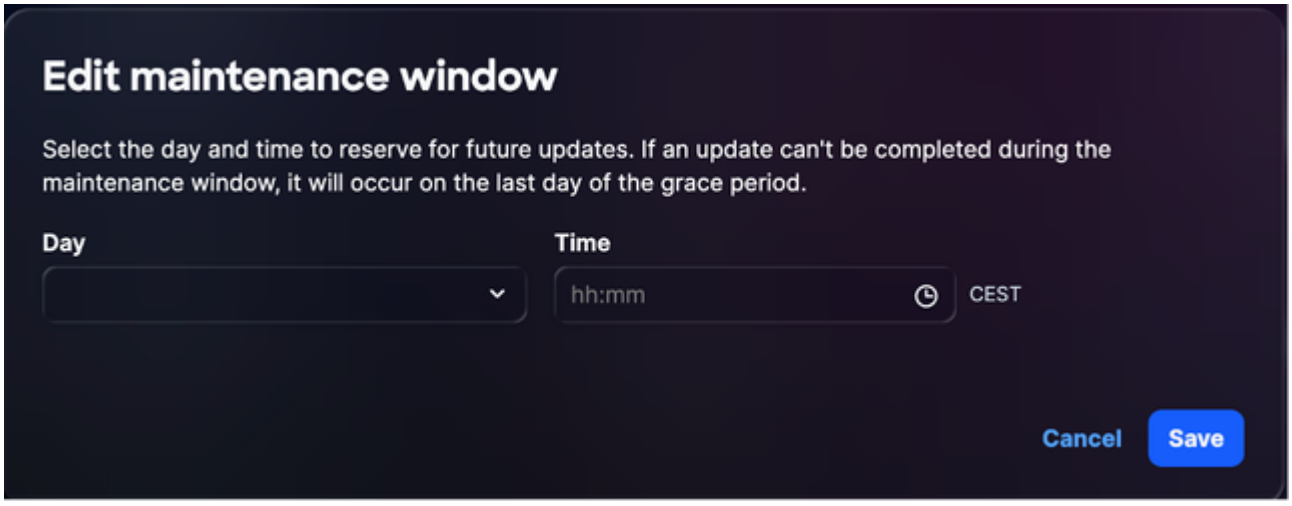


Succesvolle upgrade

Planningen voor systeemupgrades bewerken

U kunt een aangepast schema maken voor systeemupgrades. Als een aangepaste planning is geconfigureerd, worden upgrades uitgevoerd op door de gebruiker gedefinieerde datums, op voorwaarde dat deze binnen de maximale respijtperiode blijven. U maakt als volgt een schema voor een systeemupgrade:

1. Klik in het gedeelte Huidig systeem op de pagina Systeembeheer op Onderhoudsvenster bewerken.



Onderhoudsvenster bewerken

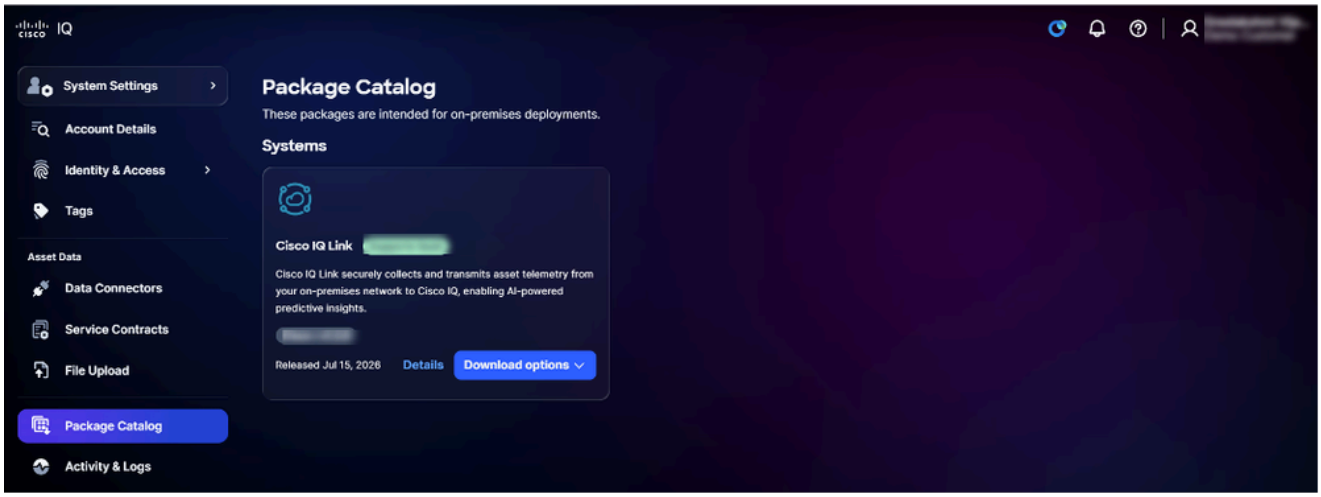
2. Kies een optie uit de vervolgkeuzelijsten Dag en Tijd.
3. Klik op Save (Opslaan). Het onderhoudsvenster is met succes gepland. De update wordt geactiveerd volgens het weergegeven schema.

Opmerking:
- Als er geen upgradeschema is geconfigureerd, worden er standaard perioden van twee (2) weken opgegeven voor upgrades die niet opnieuw worden opgestart en vier (4) weken voor upgrades die opnieuw moeten worden opgestart. Na deze respijtperioden moeten updates handmatig worden uitgevoerd.
- In het geval van een upgradefout voert het systeem maximaal twee (2) automatische herhalingen uit. Een derde poging is gepland, maar vereist handmatige initiatie.

Het systeem handmatig upgraden

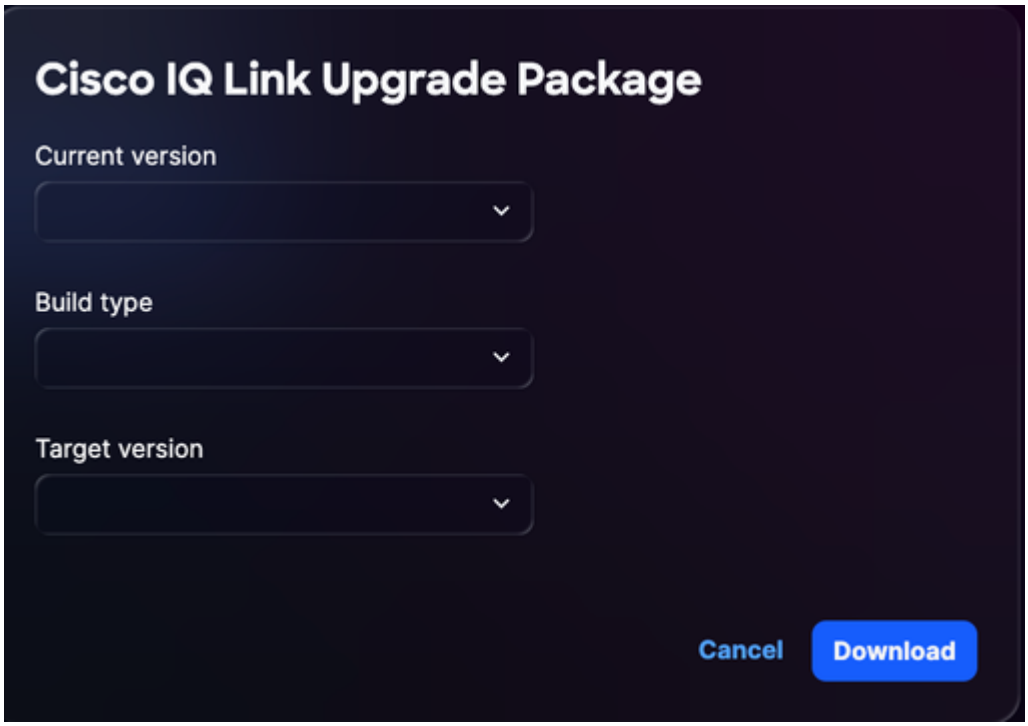
In scenario's waarin automatische distributie van Cisco IQ SaaS niet beschikbaar of vertraagd is, kunt u handmatig een systeemupgrade uitvoeren door de upgradebundel rechtstreeks van Cisco IQ SaaS te downloaden. U kunt het systeem als volgt handmatig bijwerken:

1. Meld u aan bij Cisco IQ SaaS en kies Home > Systeeminstellingen > Pakketcatalogus.



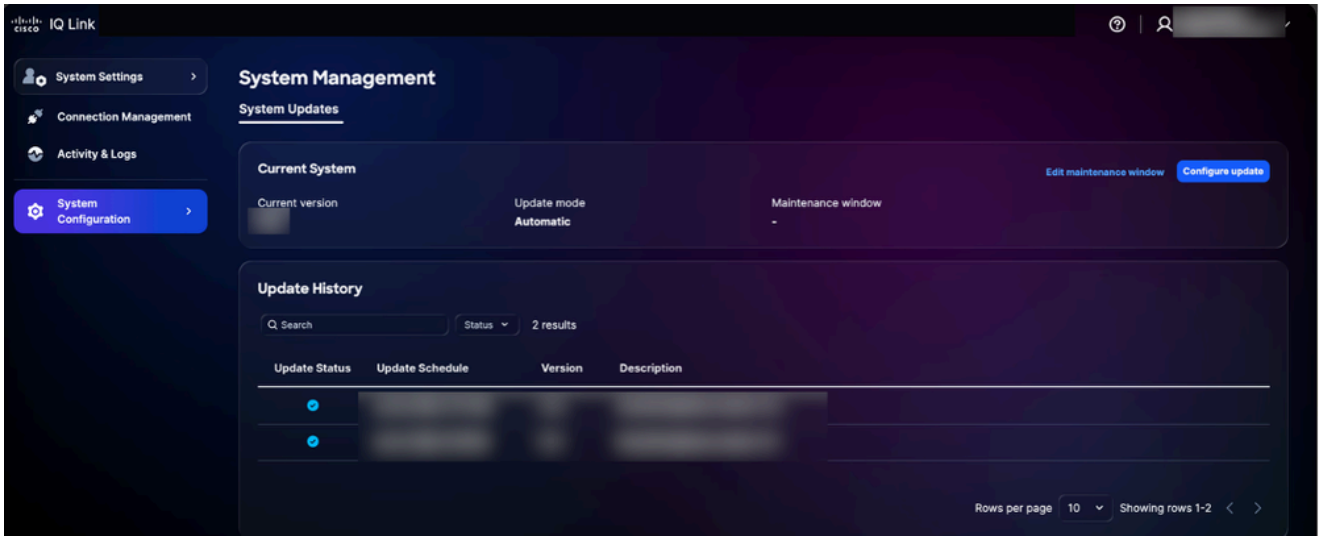
Pakketcatalogus

2. Klik in de sectie Cisco IQ Link op Downloadopties > Upgradepakketten.



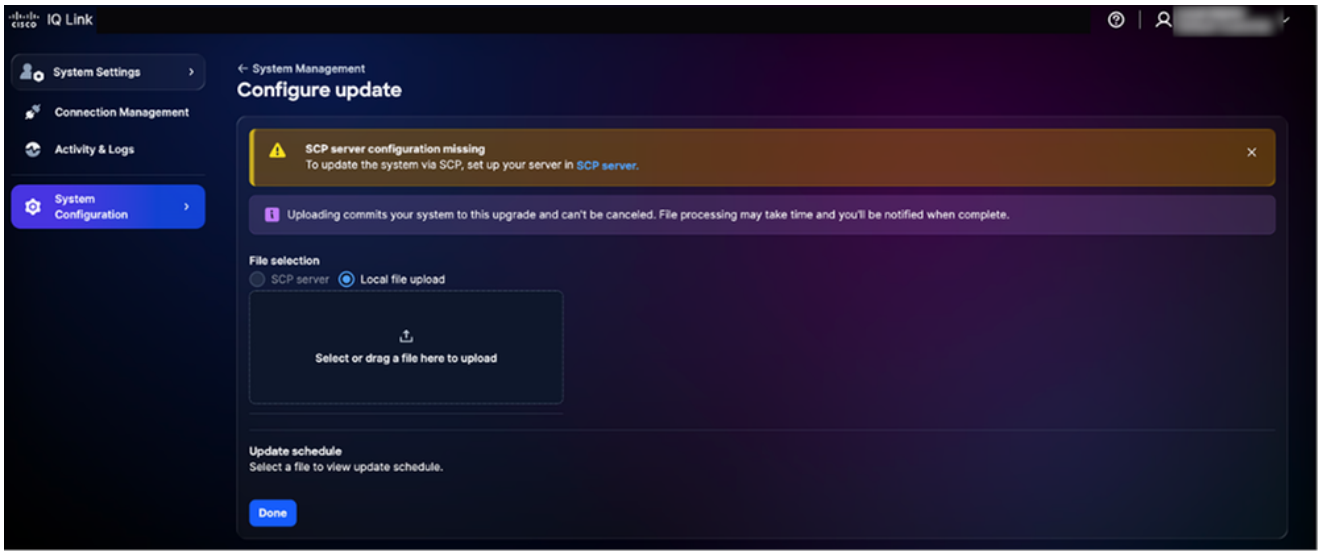
Upgradepakket

3. Kies de huidige versie in de vervolgkeuzelijst.
4. Kies het type build in de vervolgkeuzelijst.
5. Kies de doelversie in de vervolgkeuzelijst.
6. Klik op Download (Downloaden). De upgradebundel downloadt.
7. Ga naar Cisco IQ Link.
8. Kies Systeemconfiguratie > Systeembeheer in Systeeminstellingen.



Update configureren

9. Klik op Update configureren.



Lokaal bestand uploaden

10. Klik op de knop Lokaal bestand uploaden.

11. Selecteer of sleep het gedownloade upgradebundelbestand naar het uploadveld.
12. Klik op Gereed. Er wordt een bevestigingsbericht weergegeven nadat het systeem is bijgewerkt.

Configuratie SSL-certificaten

Een standaard zelf ondertekend certificaat is vooraf geïnstalleerd en ingeschakeld in Cisco IQ, maar u kunt aangepaste SSL-certificaten uploaden. Wanneer een aangepast SSL-certificaat is ingeschakeld, wordt het gebruikt voor HTTPS-verbindingen; als het certificaat is uitgeschakeld of verwijderd, wordt het systeem automatisch teruggezet naar het standaardcertificaat.

Het standaard SSL-certificaat kan niet worden bewerkt of verwijderd.

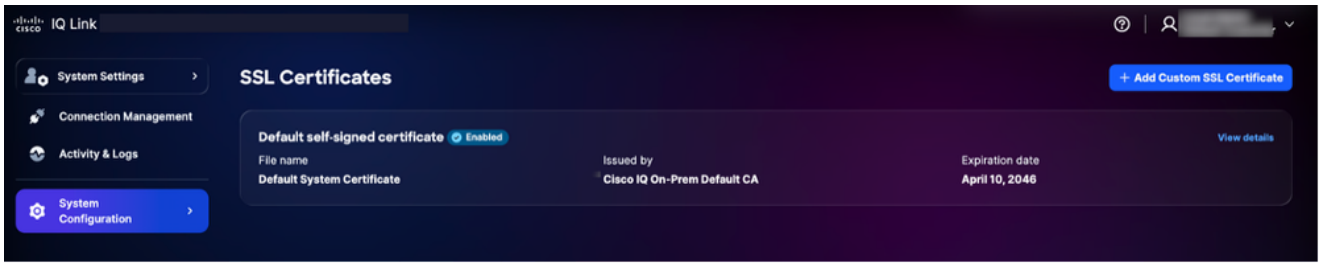
Opmerking: het certificaat moet nog ten minste 90 dagen geldig zijn. Een certificaat wordt beschouwd als "bijna vervallen" wanneer het minder dan 90 dagen heeft tot de vervaldatum.

Nadat u een SSL-certificaat hebt toegevoegd, bewerkt of verwijderd, moet u het nieuwe SSL-certificaat uploaden zoals beschreven in Single Logout Configuration voor de Okta IDP of de ADFS IDP.

Aangepast SSL-certificaat toevoegen

U voegt als volgt een aangepast SSL-certificaat toe:

1. Kies in Systeeminstellingen de optie Systeemconfiguratie > SSL-certificaten. Op de pagina SSL-certificaten worden alle SSL-certificaten voor uw systeem weergegeven.

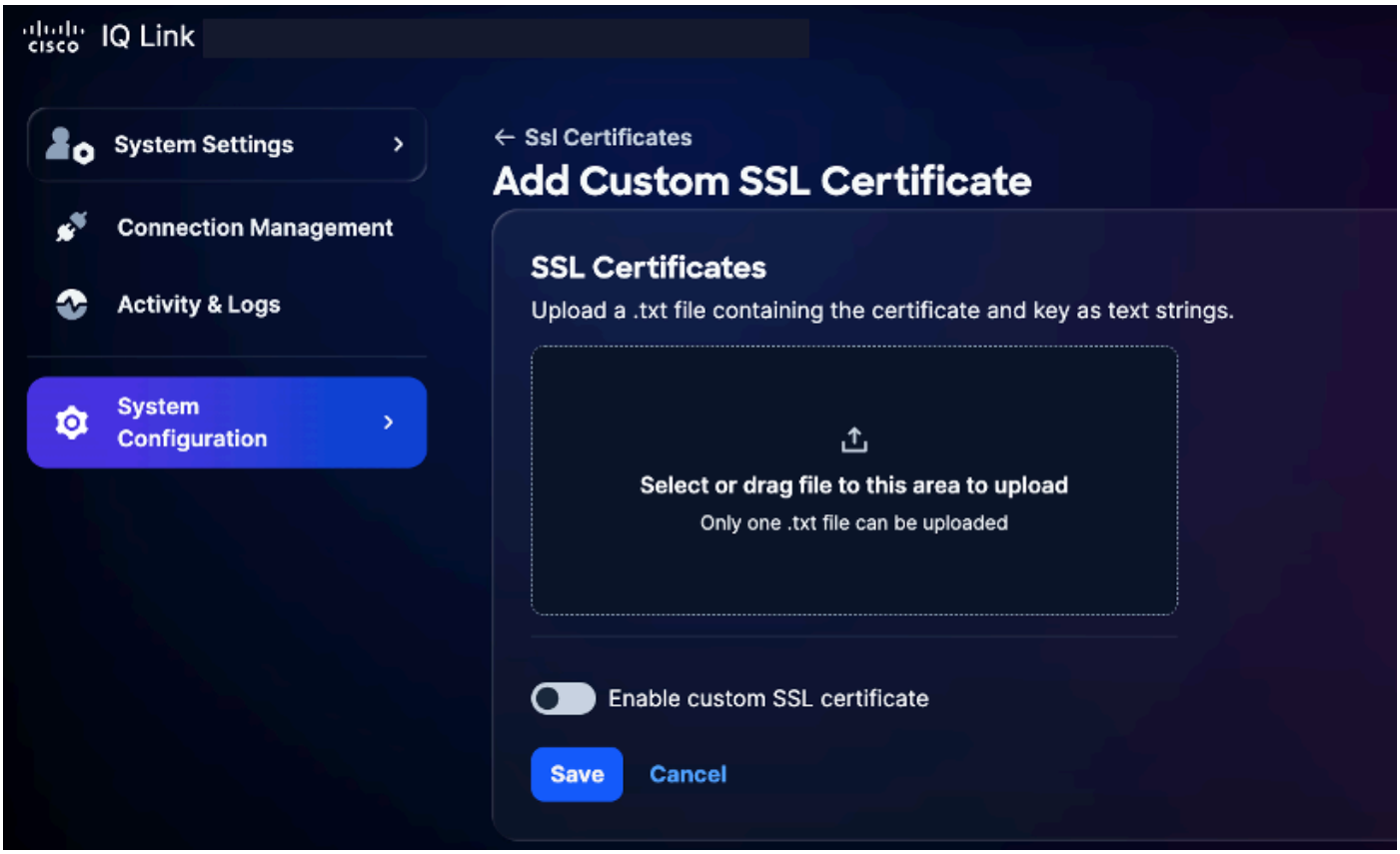


SSL-certificaat toevoegen

2. Klik op Aangepast SSL-certificaat toevoegen.

Opmerkingen:
- Upload een .txt-bestand dat zowel het Privacy-Enhanced Mail-gecodeerde certificaat als de sleutel als tekstreeksen bevat
- Er kan maar één .txt bestand tegelijk worden geüpload
- Het bestand moet zowel het certificaat als de private key bevatten

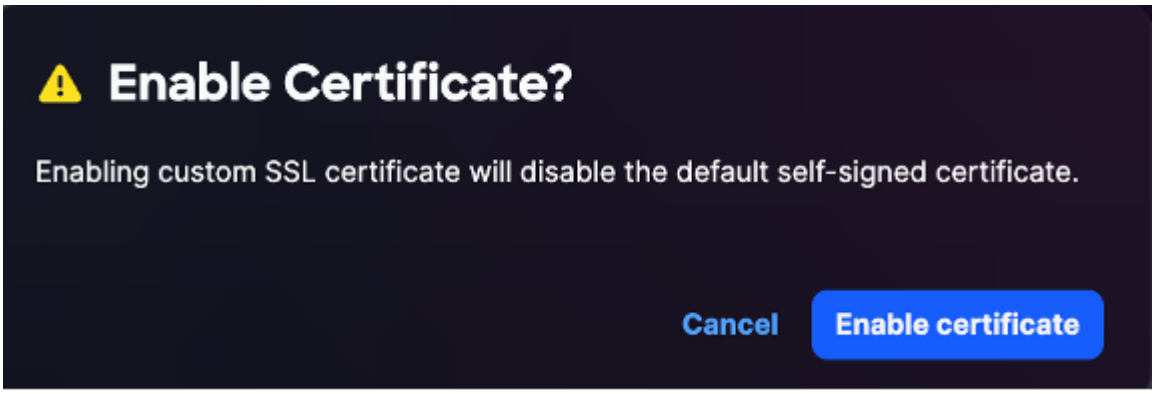
---



SSL-certificaat uploaden

3. Sleep het aangepaste SSL-certificaat of upload het naar het veld SSL-certificaat.

4. Schakel de knop Aangepaste SSL-certificaat inschakelen in.



SSL-certificaat bewerken

Opmerking: houd de schakelaar UIT als u het certificaat wilt uploaden zonder het onmiddellijk te activeren.

---

5. Klik op Certificaat inschakelen.

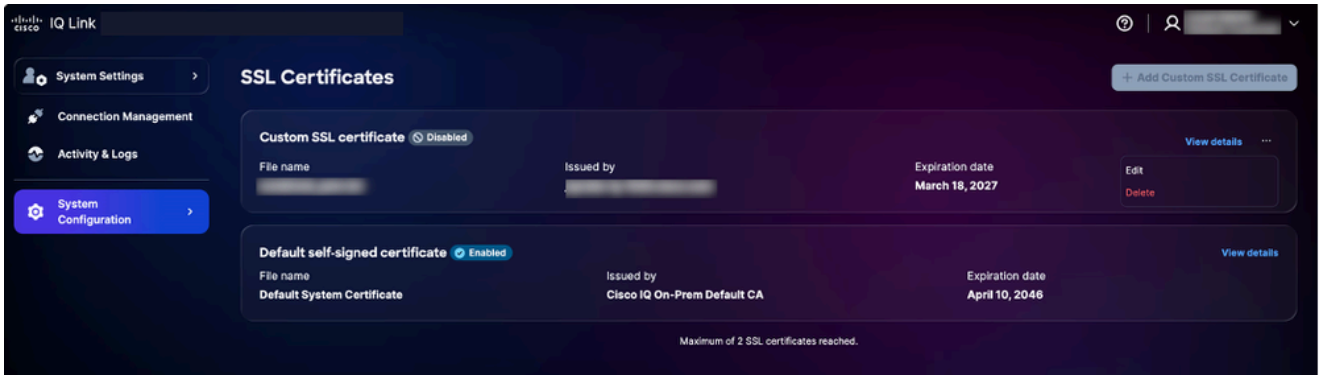
6. Klik op Opslaan.

Het aangepaste SSL-certificaat is ingeschakeld en actief. Het standaardsysteemcertificaat wordt automatisch gedeactiveerd.

Aangepaste SSL-certificaten bewerken

U kunt het aangepaste SSL-certificaat bewerken om een nieuw certificaat te uploaden of om het certificaat dat momenteel is ingeschakeld uit te schakelen. Zo bewerkt u:

1. Navigeer naar het gewenste SSL certificaat.



SSL-certificaat bewerken

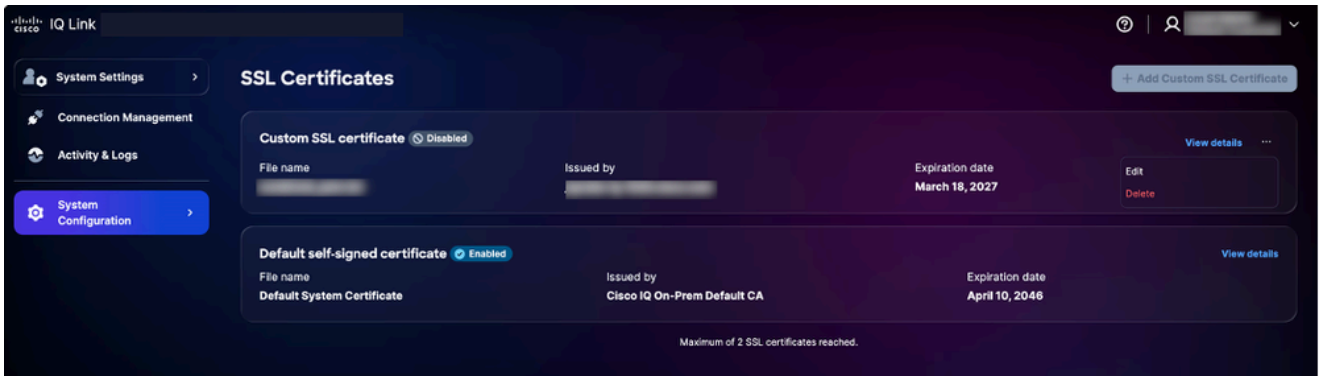
2. Kies het pictogram Meer opties > Bewerken. De pagina SSL-certificaat bewerken wordt weergegeven.
3. Bewerk de certificaatgegevens zoals vereist.
4. Klik op Save (Opslaan).

Aangepaste SSL-certificaten verwijderen

Waarschuwing: Een aangepast SSL-certificaat kan op elk moment worden verwijderd, maar het is een onomkeerbare actie; u kunt op elk moment na verwijdering een nieuw aangepast certificaat uploaden.

Zo verwijdert u:

1. Navigeer naar het gewenste SSL certificaat.



SSL-certificaat verwijderen

2. Kies het pictogram Meer opties > Verwijderen.
3. Klik op Certificaat verwijderen. Het aangepaste certificaat wordt verwijderd en het standaardcertificaat wordt automatisch opnieuw geactiveerd.

Syslog-serverconfiguratie

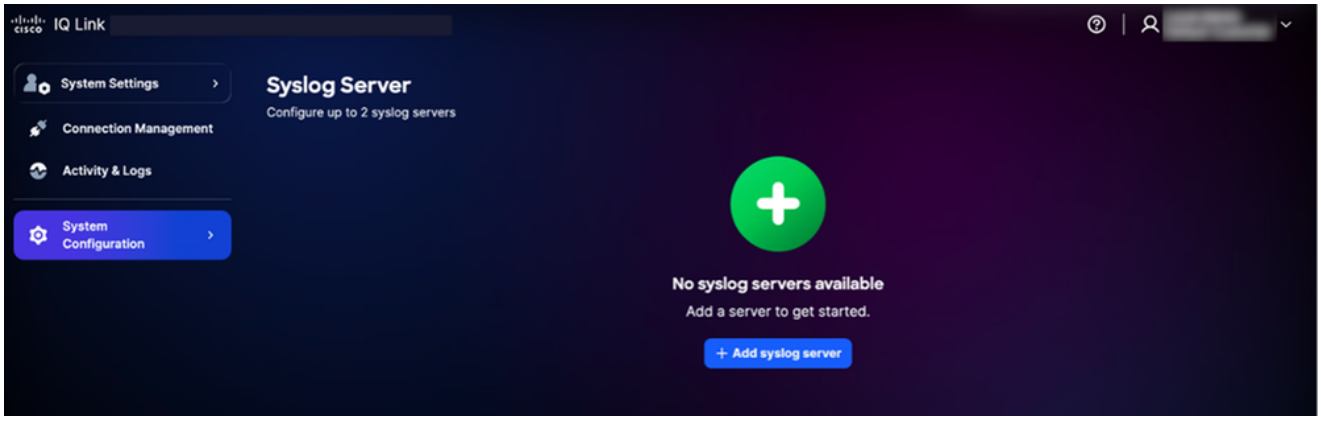
Gebruikers met de rol Accountbeheerder kunnen externe syslog-servers configureren om systeemlogs te exporteren. U kunt maximaal twee (2) syslog-servers configureren.

Opmerking: De Syslog-server moet worden opgegeven als een IP-adres, niet als een FQDN.

Syslog-servers toevoegen

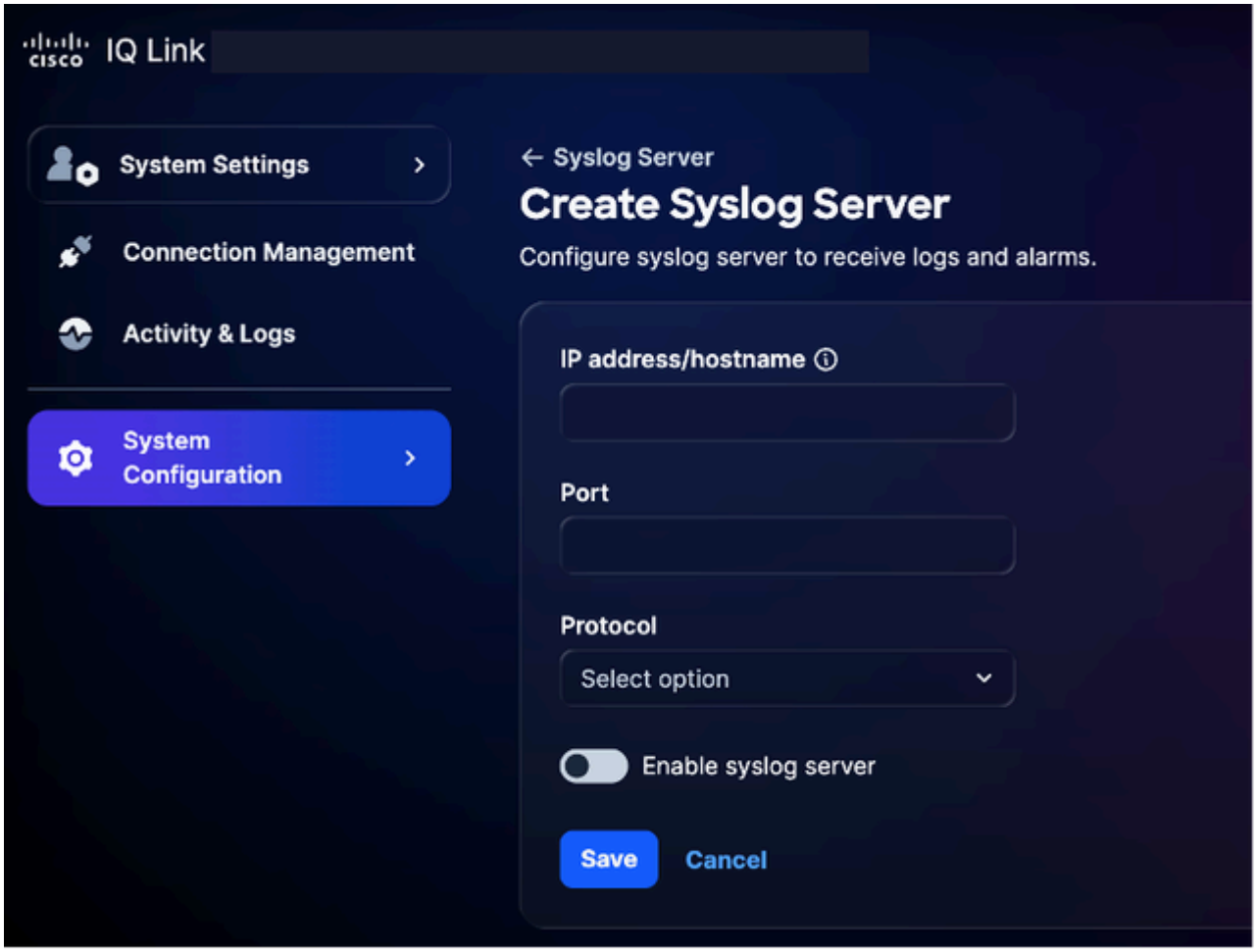
Een syslog-server toevoegen:

1. Kies in Systeeminstellingen de optie Systeemconfiguratie > Syslog Server. De pagina Syslog Server wordt weergegeven.



Syslog-server toevoegen

2. Klik op Syslog-server toevoegen. De pagina Syslog Server maken wordt weergegeven.



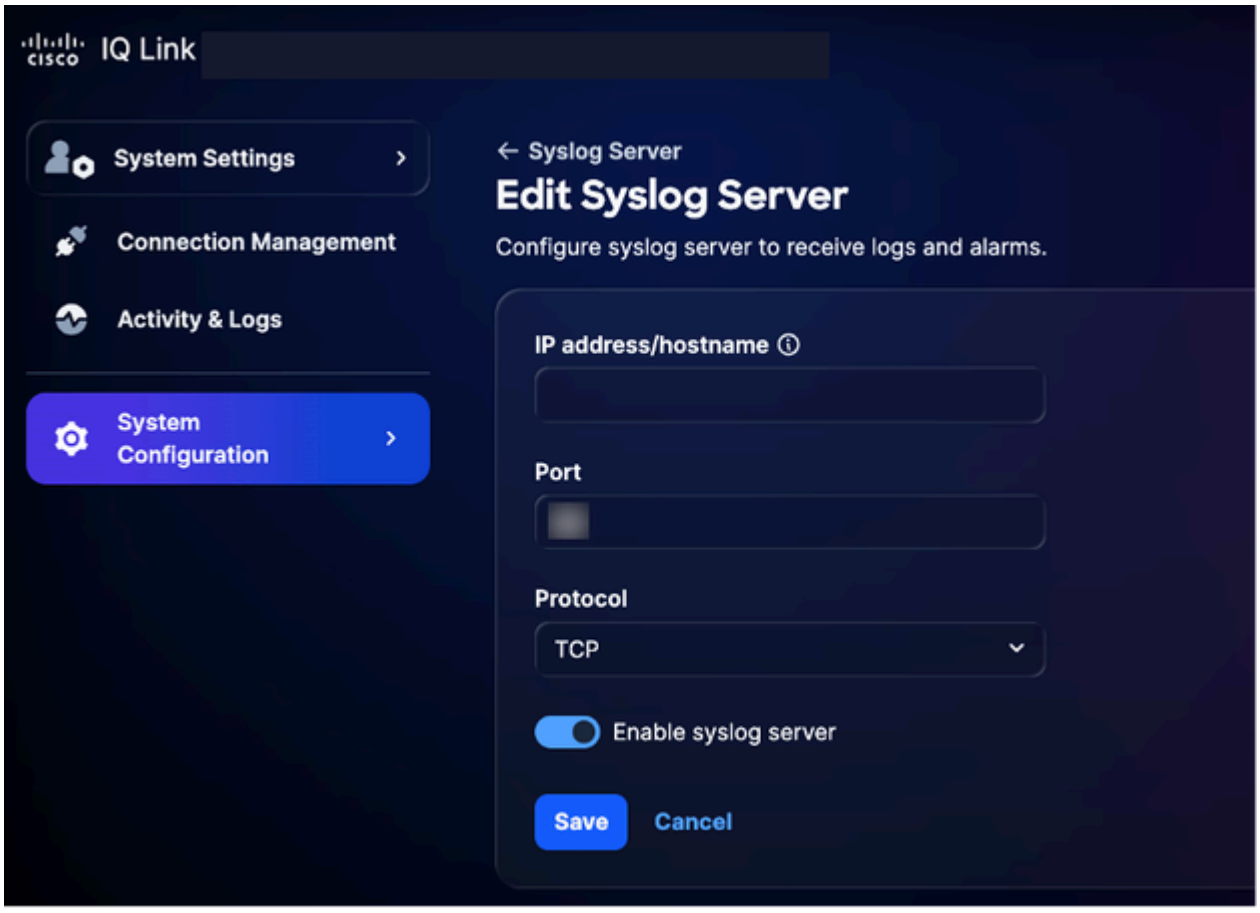
Syslog-server maken

3. Voer het IP-adres/de hostnaam in.
4. Voer een Port-nummer in.
5. Selecteer het toepasselijke protocol in de vervolgkeuzelijst Protocol (bijvoorbeeld UDP of TCP).
6. Schakel de schakelknop Syslog-server inschakelen in.
7. Klik op Save (Opslaan). Er wordt een bevestiging weergegeven en de nieuw toegevoegde syslog-server wordt weergegeven op de startpagina van Syslog Server.

Geconfigureerde SYSLOG-servers bewerken

Een geconfigureerde syslog-server bewerken:

1. Navigeer naar de gewenste syslog-server.
2. Kies het pictogram Meer opties > Bewerken. De pagina Syslog Server bewerken wordt weergegeven.



Syslog-server bewerken

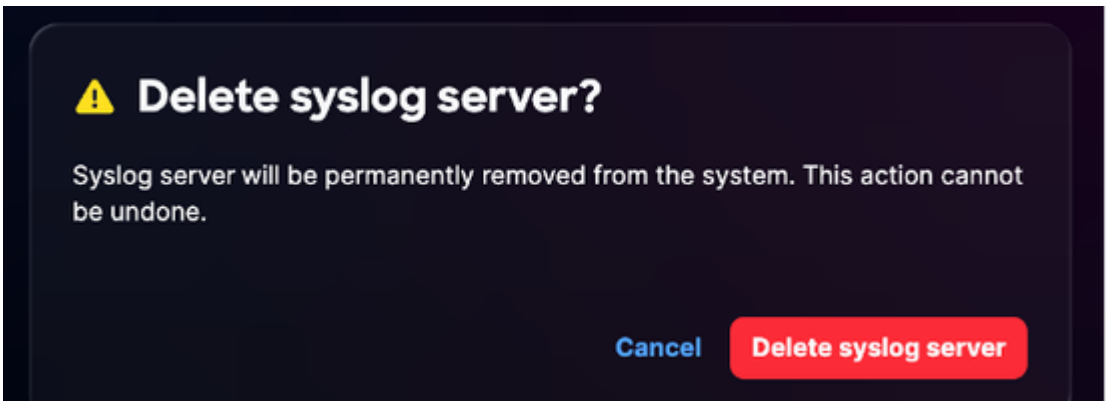
3. Bewerk details of schakel de schakelaar Syslog-server inschakelen uit.

4. Klik op Save (Opslaan).

Geconfigureerde SYSLOG-servers verwijderen

Een geconfigureerde syslog-server verwijderen:

1. Navigeer naar de gewenste syslog-server.
2. Kies het pictogram Meer opties > Verwijderen. Er wordt een bevestiging weergegeven.

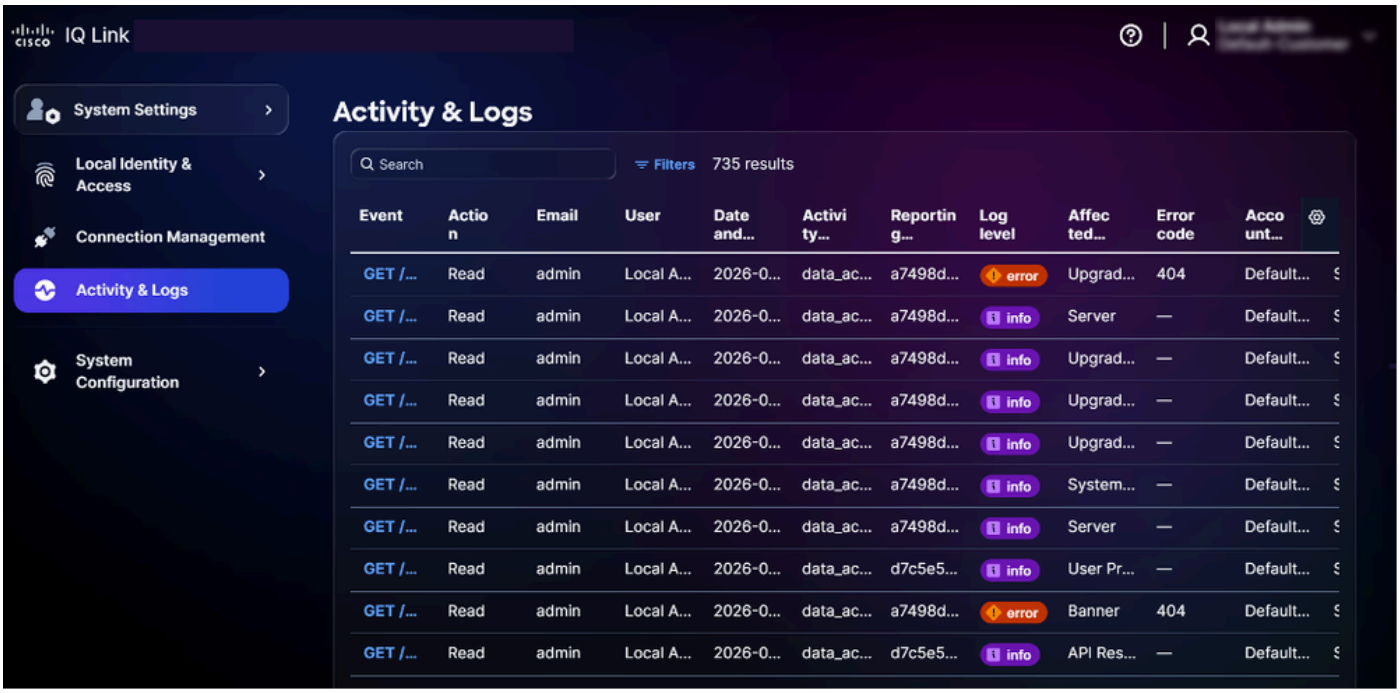


Bevestiging

3. Klik op Syslog-server verwijderen.

Activiteit en logboeken

Activity & Logs bieden een gedetailleerd overzicht van gebruikersacties en wijzigingen in Cisco IQ, zodat accountbeheerders gebruikersactiviteiten kunnen volgen en transparantie kunnen behouden.



Activiteit en logboeken

Als u activiteiten en logs wilt bekijken, selecteert u Activiteit en logs in het menu Systeeminstellingen.

Activiteit en logboeken:

- Ondersteunt filters, paginering en zoekfuncties om informatie eenvoudig te vinden en te beheren
- Registreert alle API-bewerkingen op gatewayniveau

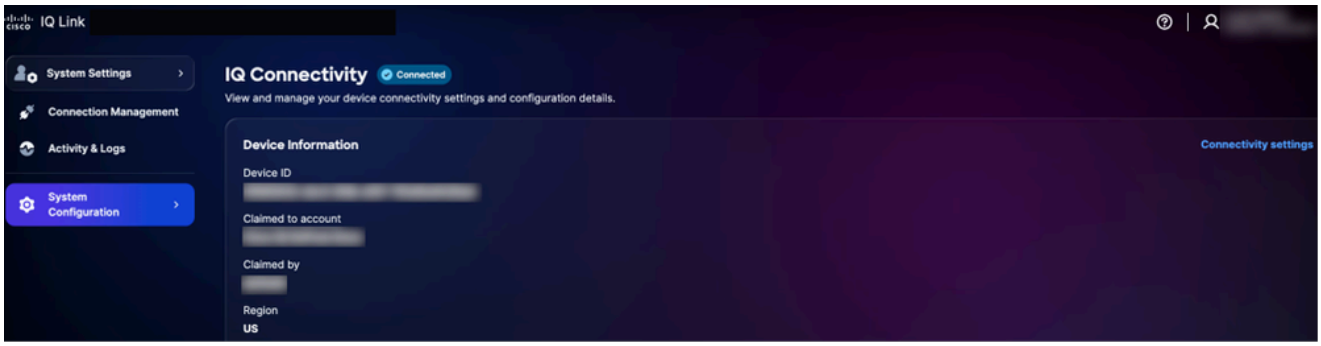
De volgende filteropties zijn beschikbaar:

- Datum: Filters logboeken voor een specifiek tijdsbereik
- Logniveau: logbestanden filteren op ernst (bijvoorbeeld fout, waarschuwing en informatie)
- Activiteitstype: Filterlogboeken op type systeemactiviteit
- Foutcode: filterlogboeken voor een specifieke foutcode

IQ-connectiviteit

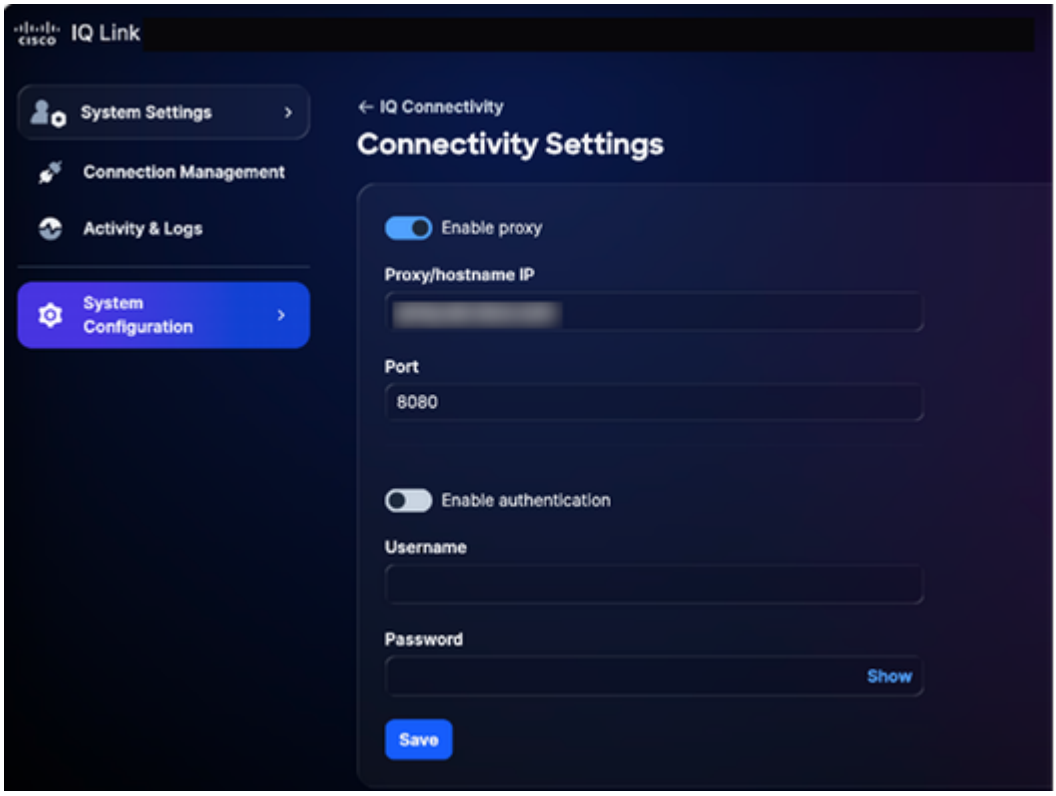
De verbindingsinstellingen en configuratiegegevens van uw apparaat weergeven en beheren:

1. Kies Systeemconfiguratie > IQ-connectiviteit in Systeeminstellingen. De pagina IQ Connectivity wordt weergegeven.



IQ-connectiviteit

2. Klik op Connectiviteitsinstellingen.



Connectiviteitsinstellingen

3. Gegevens bijwerken zoals vereist.
4. Klik op Save (Opslaan).

Verbindingsbeheer (gegevensverzameling)

Cisco IQ Link is een on-premise oplossing voor het verzamelen van netwerkgegevens, ontworpen om diepe zichtbaarheid in uw infrastructuur te bieden. Het verzamelt gegevens via Catalyst Center en Direct Connection. Het vereenvoudigt de manier waarop u netwerkverificatie en

apparaatdetectie beheert. De configuratie van de gegevensverzameling wordt hieronder samengevat:

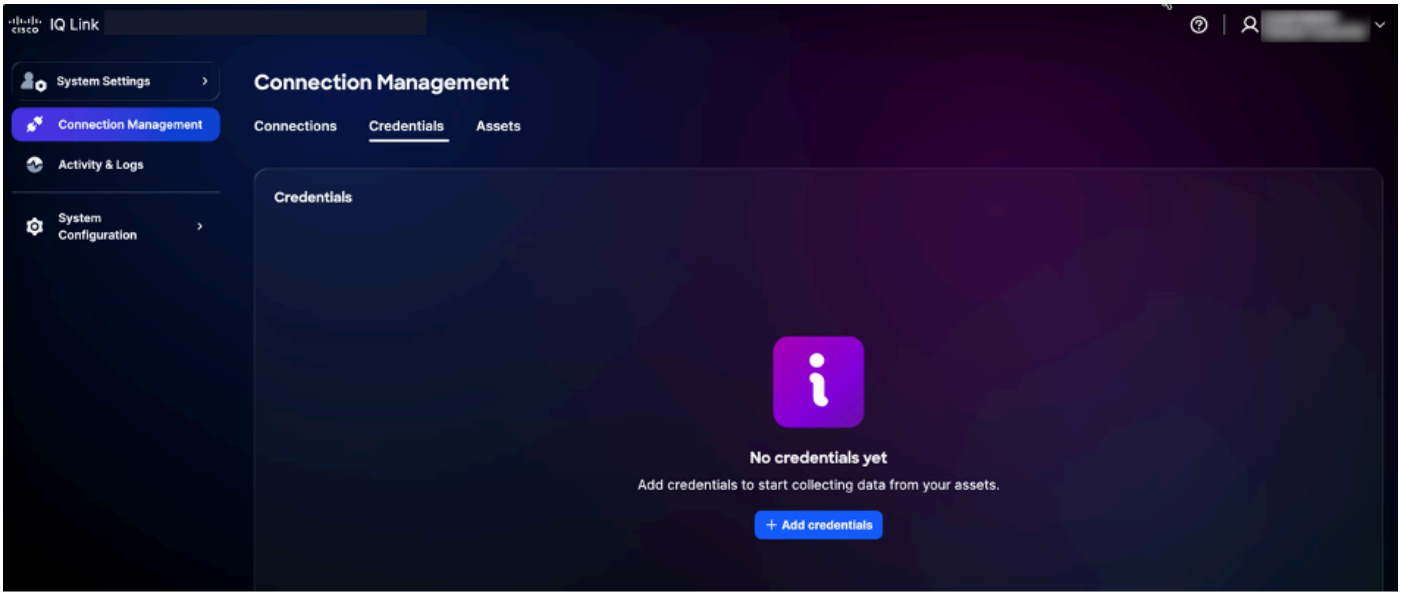
- Credential Sets maken: stel de verificatieprotocollen vast (bijvoorbeeld Simple Network Management Protocol (SNMP) v1/v2c/v3) om te communiceren met uw netwerkapparaten. Door inloggegevens te centraliseren op beveiligingszone of -locatie (bijvoorbeeld "SanJose-SNMPv3") kunt u wachtwoorden op één locatie bijwerken, waarbij wijzigingen automatisch worden doorgegeven aan alle bijbehorende apparaten.
- Credentials toewijzen aan Inventory: koppel uw Credential Sets aan uw Inventory Assets om het authenticatieproces te automatiseren. Door regels te maken die specifieke IP-bereiken koppelen aan gedefinieerde Credential Sets, past het systeem automatisch de juiste authenticatie toe tijdens het verzamelen van gegevens. Dit elimineert fouten bij handmatige invoer en zorgt ervoor dat uw configuratie nauwkeurig blijft naarmate uw netwerk groeit.

Opmerking: SNMPv2c/SNMPv3 en SSH zijn vereist voor apparaatdetectie en HTTP/HTTPS-referenties moeten worden verstrekt voordat u Catalyst Center configureert.

Credentials toevoegen

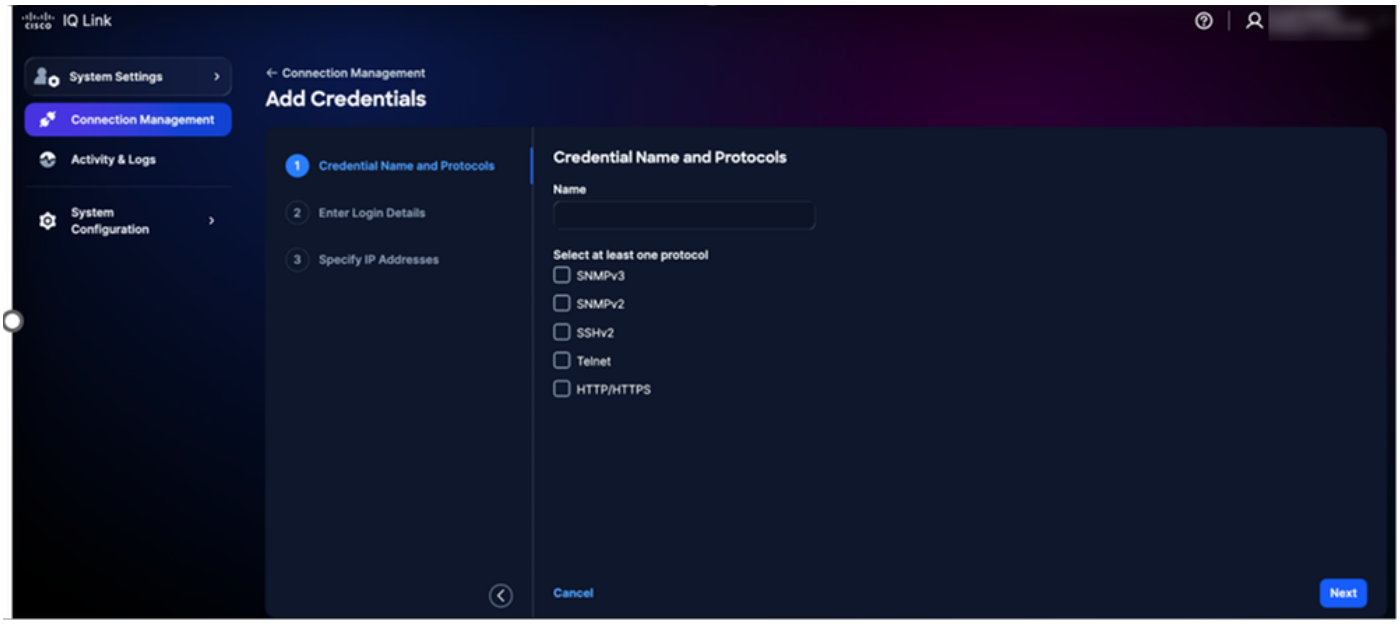
U moet eerst inloggegevens toevoegen om de gegevensverzameling uit te voeren. U voegt als volgt referenties toe:

1. Kies Verbindingsbeheer in Systeeminstellingen. De pagina Verbindingsbeheer wordt weergegeven.
2. Klik op het tabblad Inloggegevens.



Tabblad Referenties

3. Klik op Inloggegevens toevoegen.

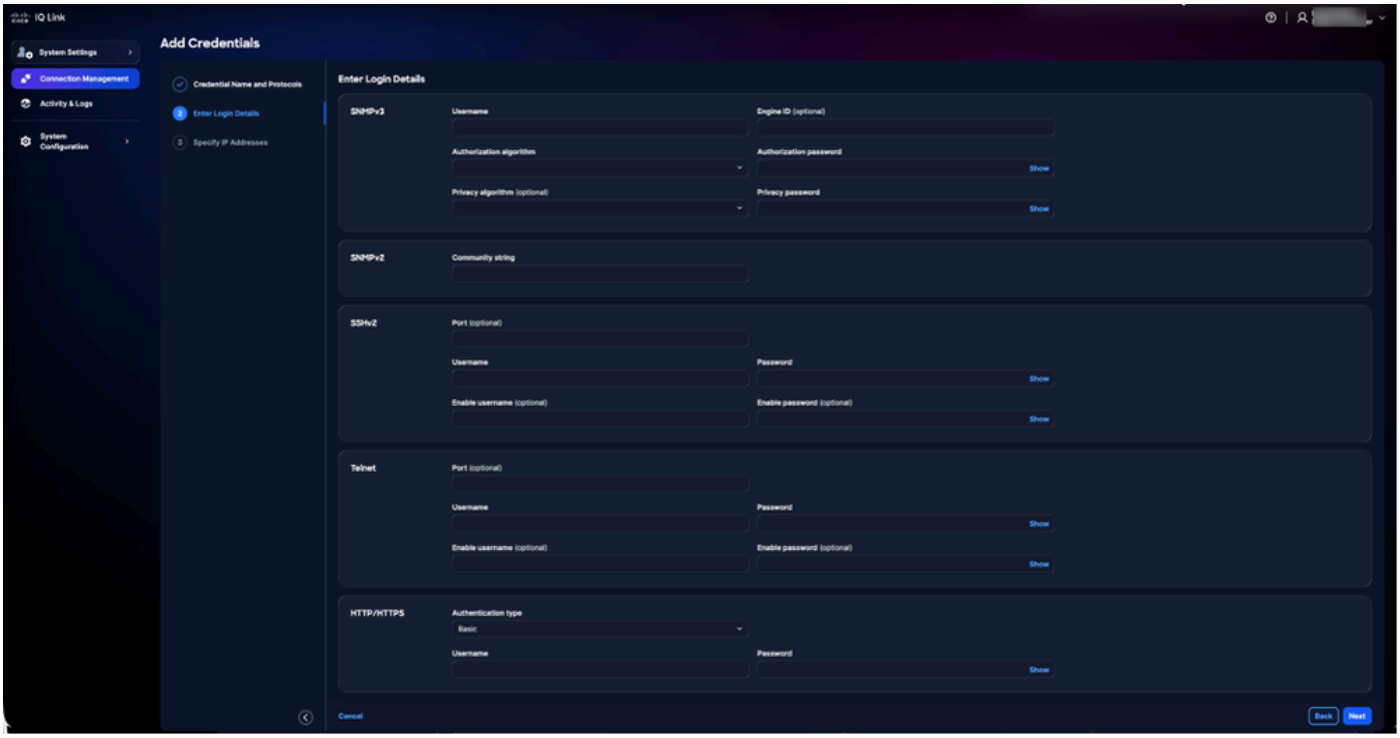


Credentials toevoegen

4. Voer de naam in.

5. Schakel alle toepasselijke protocolselectievakjes in.

6. Klik op Volgende.

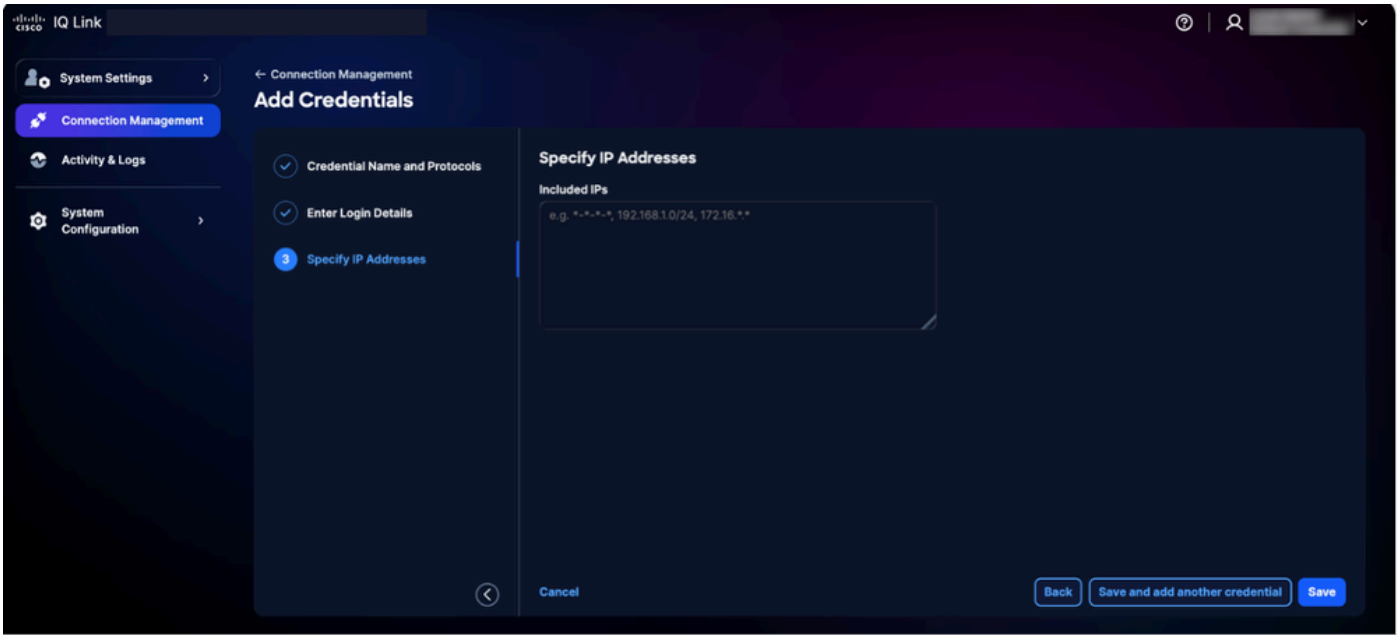


Credentials toevoegen - Details

Opmerking: in de afbeelding hierboven wordt de weergave weergegeven wanneer alle protocollen in de vorige stap zijn geselecteerd. Uw interface geeft alleen de specifieke protocollen weer die u hebt gekozen.

7. Voer de aanmeldingsgegevens in voor elk geselecteerd protocol.

8. Klik op Volgende.

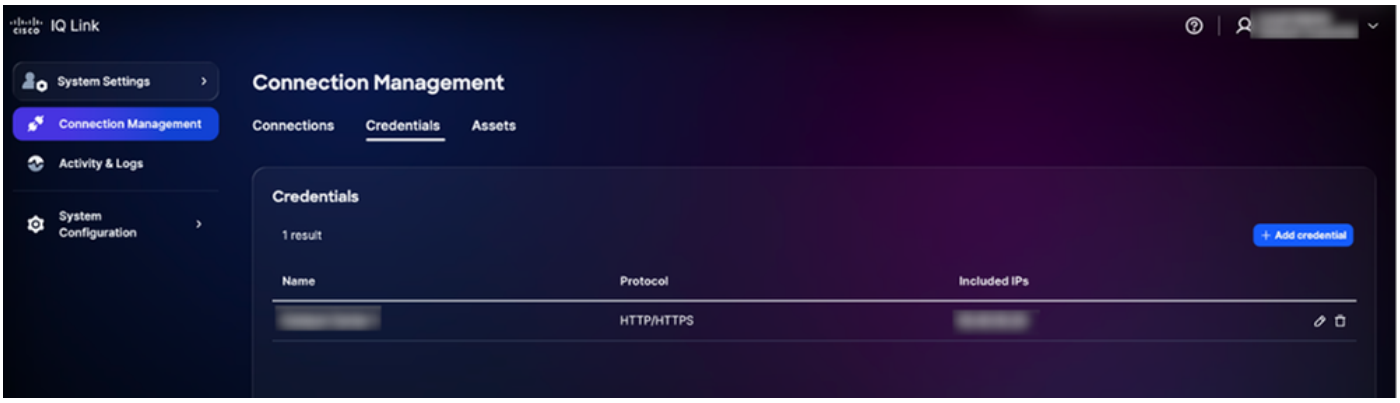


IP-adressen opgeven

9. Voer de meegeleverde IP's in.

Opmerking: Dit veld definieert de IP-adressen of IP-bereiken waar de referenties kunnen worden gebruikt om een verbinding tot stand te brengen. Het ondersteunt een mix van IP's en IP-maskers (met behulp van jokernotatie). Zie Credential Selection and Matching Logic voor meer informatie over ondersteunde indelingen.

10. Klik op Opslaan. Er wordt een bevestiging weergegeven en u wordt doorgestuurd naar het tabblad Inloggegevens.



Credentials toegevoegd

U kunt de referenties bewerken door op het pictogram Bewerken te klikken en ze te verwijderen door op het pictogram Verwijderen te klikken.

Credential Selection en Matching Logic

De telemetrie-engine maakt gebruik van een op prioriteit gebaseerde matching-logica om te bepalen welke referenties moeten worden toegepast tijdens de ontdekking en verzameling. Het begrijpen van deze hiërarchie zorgt ervoor dat de juiste referenties worden gebruikt voor de beoogde apparaten.

- Prioriteitsrangschikking: wanneer meerdere referenties van toepassing zijn op een apparaat, evalueert Cisco IQ ze op basis van hoe specifiek ze overeenkomen met het apparaat; het systeem past de volgende prioriteit toe, waarbij meer specifieke overeenkomsten voorrang hebben:
  - Exacte IP-overeenkomst: hoogste prioriteit
  - Trailing Wildcard Match: Prioriteit hangt af van het aantal trailing stars; minder sterren geven een meer specifieke match aan en dus een hogere prioriteit

- Wildcard-opmaakregels: Wildcards (*) worden alleen ondersteund als achterliggende tekens in een IP-adres; ze moeten van rechts naar links worden toegepast.
  - Ondersteunde indelingen:

    1.2.3.* (hoogste prioriteit onder wildcards)

    1.2.*

    1.*.*.*

    ..*.* (Laagste prioriteit)

  - Niet-ondersteunde indelingen:

    Toonaangevende jokertekens (bijvoorbeeld *.1.2.3)

Wildcards tussen octetten (bijvoorbeeld 20 .10.*.20)

Gebruik van streepjes of andere afwijkende begrenzers

Voorbeeld van selectie van referenties:

De volgende tabel illustreert hoe de telemetrie-engine de meest geschikte aanmeldingsset selecteert wanneer een apparaat overeenkomt met meerdere gedefinieerde patronen.

Tabel 13: Voorbeeld van de selectie van referenties

Apparaat-IP	Beschikbare referenties	Geselecteerde aanmeldingsset
10.10.1.5	10.10.1.5, 10.10.1, 10.10.*	10.10.1.5 (exacte overeenkomst)
10.10.2.15	10.10.2, 10.10.*	10.10.2.* (Meer specifiek)
10.10.5.50	10.10. .	10 .10.. (Meer specifiek)

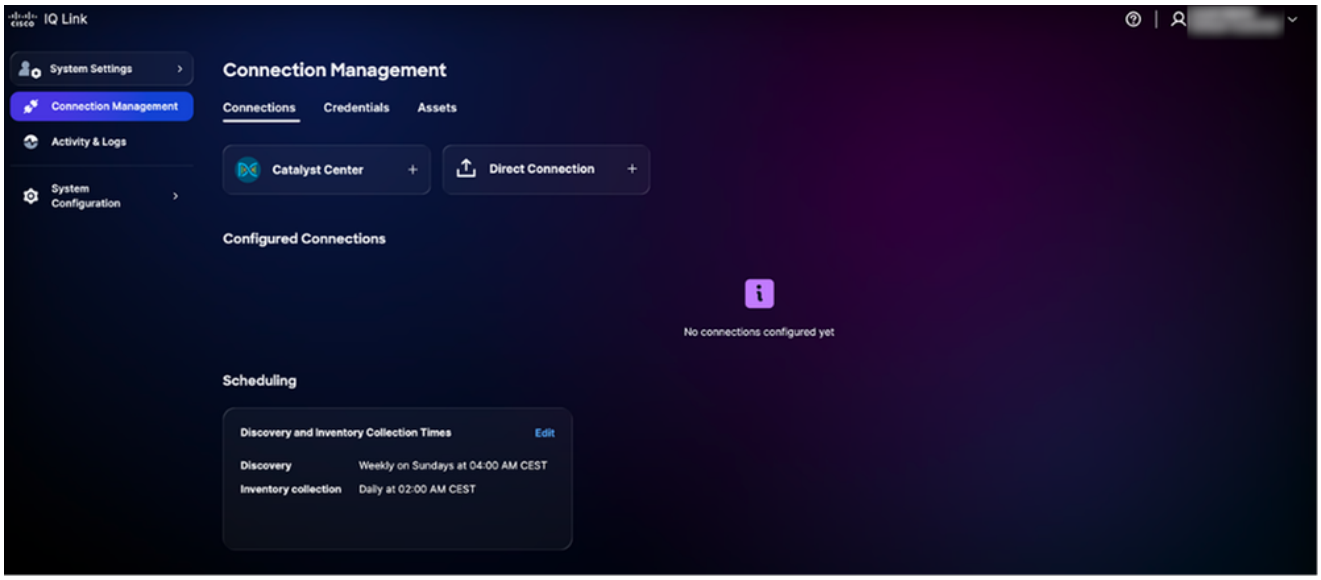
Opmerking: Als een apparaat valt in meerdere overlappende categorieën, selecteert het systeem altijd de set met de hoogste specificiteit (met andere woorden, de minste achterliggende jokertekens).

Gegevensverzameling met Catalyst Center

U kunt maximaal 20 Catalyst Centers (niet-cluster) aansluiten voor elk exemplaar van Cisco IQ Link.

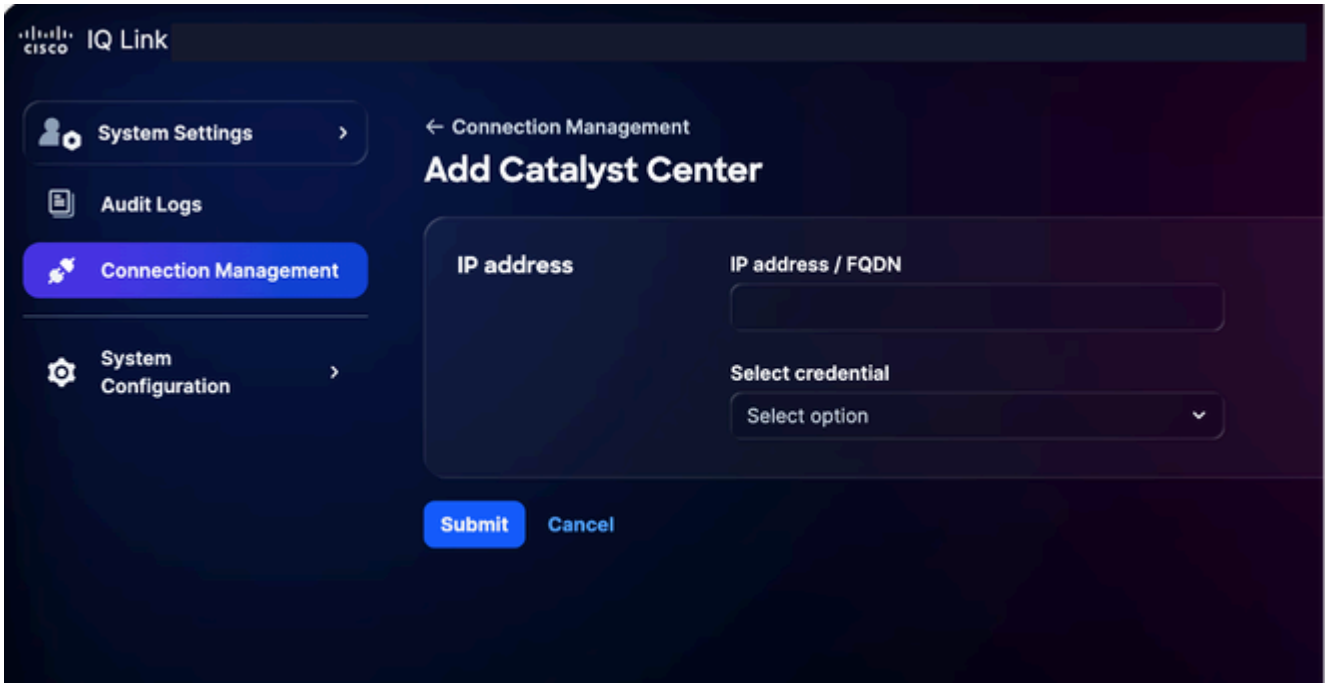
Voor gegevensverzameling met Catalyst Center:

1. Kies Verbindingsbeheer in Systeeminstellingen. De pagina Verbindingsbeheer wordt weergegeven.



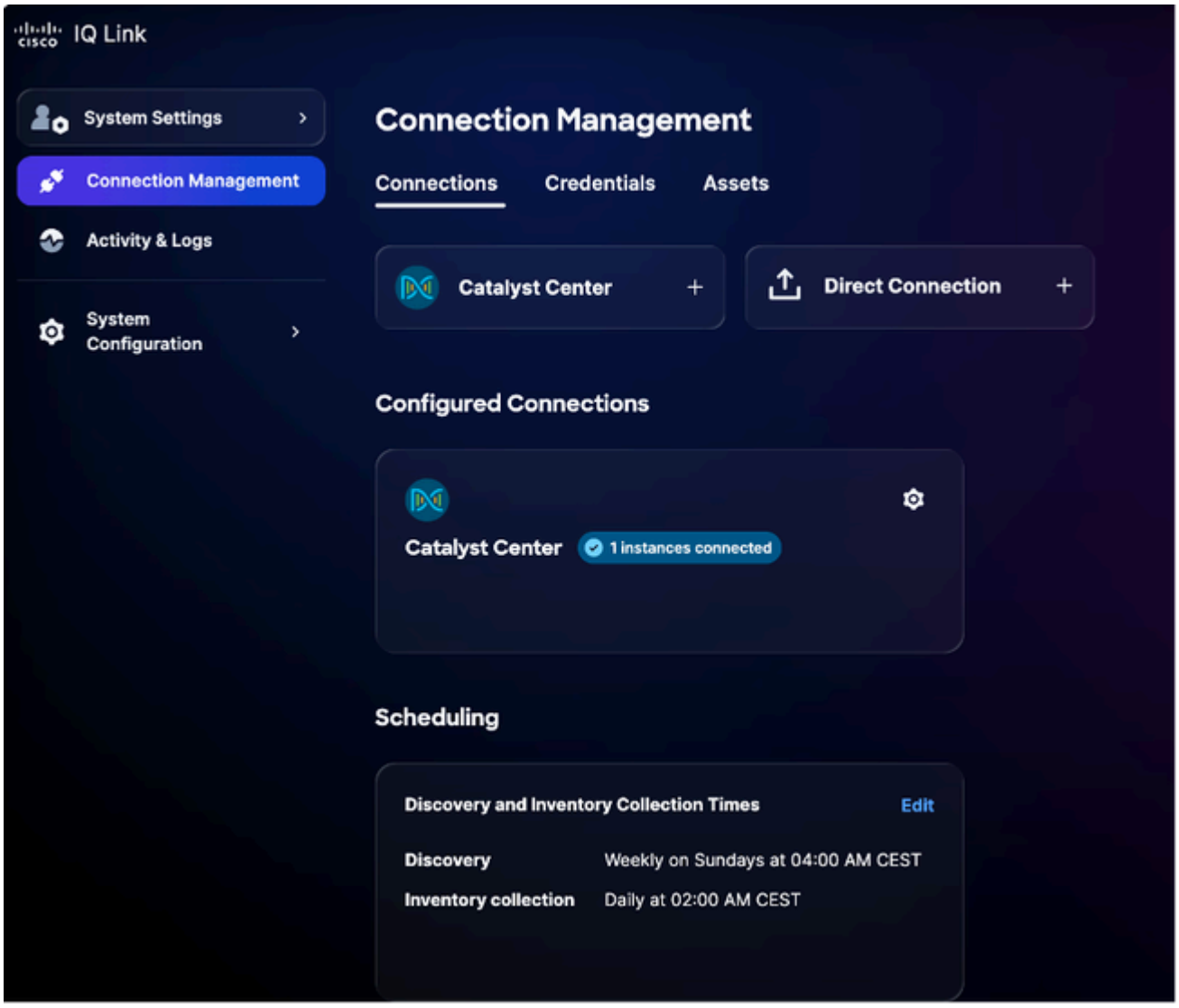
Verbindingsbeheer

2. Klik op de optie Catalyst Center.



Catalyst Center toevoegen

3. Voer het IP-adres of FQDN in.
4. Kies een geconfigureerde HTTP/HTTPS-referentie in de vervolgkeuzelijst.
5. Klik op Indienen. Er wordt een bevestiging weergegeven (dit kan maximaal 75 minuten duren). U kunt het nieuw toegevoegde Catalyst Center bekijken onder Geconfigureerde verbindingen.



Catalyst Center toegevoegd

6. Plan een verzameling in. Zie Planning voor meer informatie.

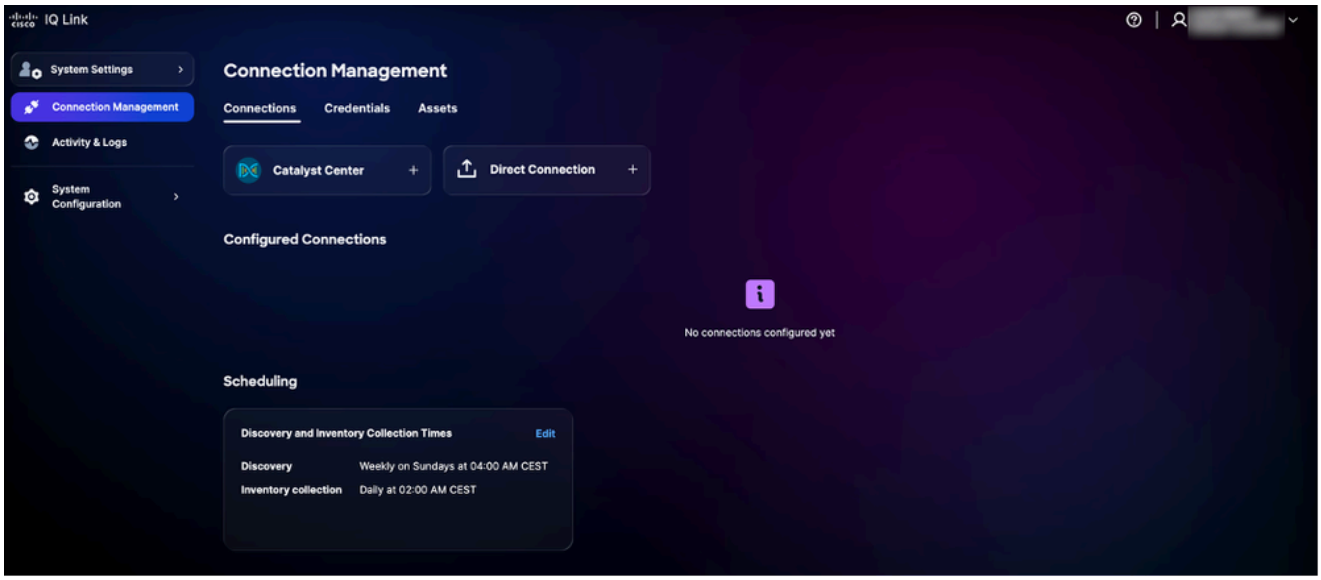
Opmerking: Cisco IQ Link is vooraf geconfigureerd met een automatische planningsinstelling en het systeem start een standaard geautomatiseerd inzamelschema. Het wordt ten zeerste aanbevolen dat u de planning bewerkt om deze af te stemmen op de vereisten en onderhoudsvensters van uw organisatie.

---

directe verbinding

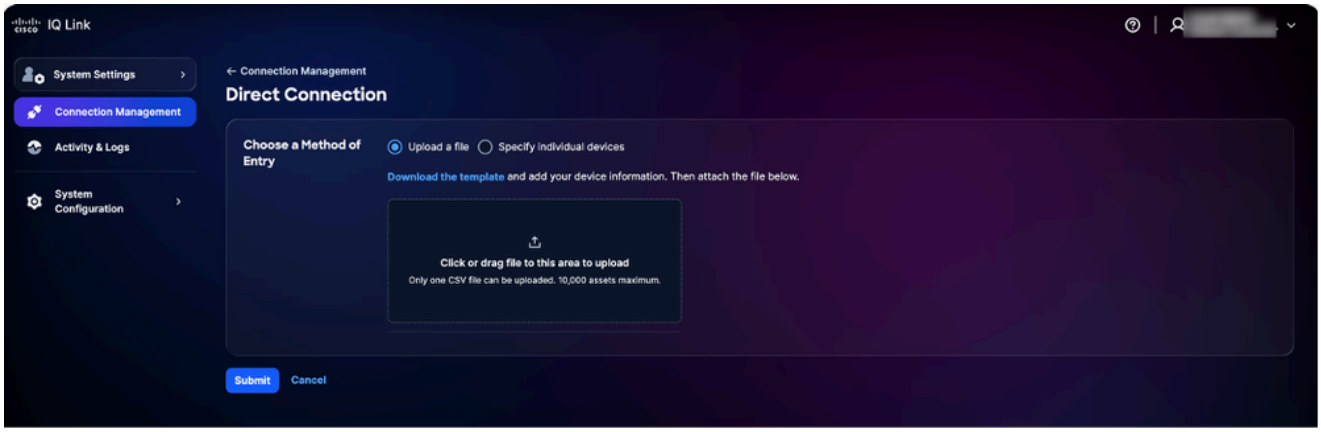
Apparaten voor directe verbinding toevoegen:

1. Kies Verbindingsbeheer in Systeeminstellingen. De pagina Verbindingsbeheer wordt weergegeven.



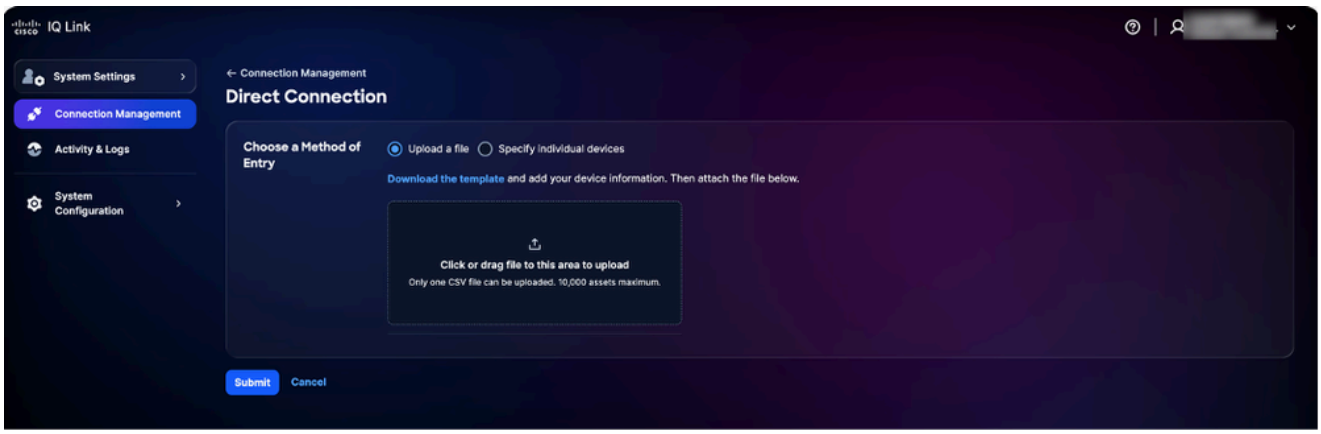
Verbindingsbeheer

2. Klik op Directe verbinding. De pagina Directe verbinding wordt weergegeven met twee (2) opties om gegevens te verzamelen.



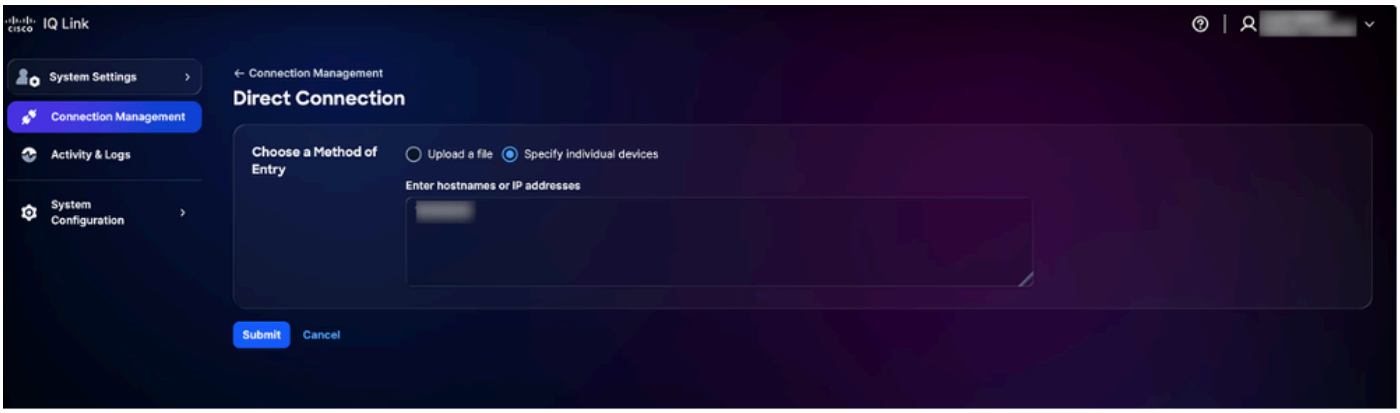
Bestand uploaden

3. Klik op de voorkeursoptie voor Kies een invoermethode en dien uw apparaten in met een van de volgende methoden:



Een bestand uploaden

- Een bestand uploaden: klik of sleep het bestand en klik op Indienen



Afzonderlijke apparaten opgeven

- Geef afzonderlijke apparaten op: Voer een enkele hostnaam, IP-adressen of een door komma's gescheiden lijst van hostnamen en/of IP-adressen in en klik op Indienen

U wordt doorgestuurd naar het tabblad Activa na succesvolle indiening.

4. Plan een verzameling in. Zie Planning voor meer informatie.

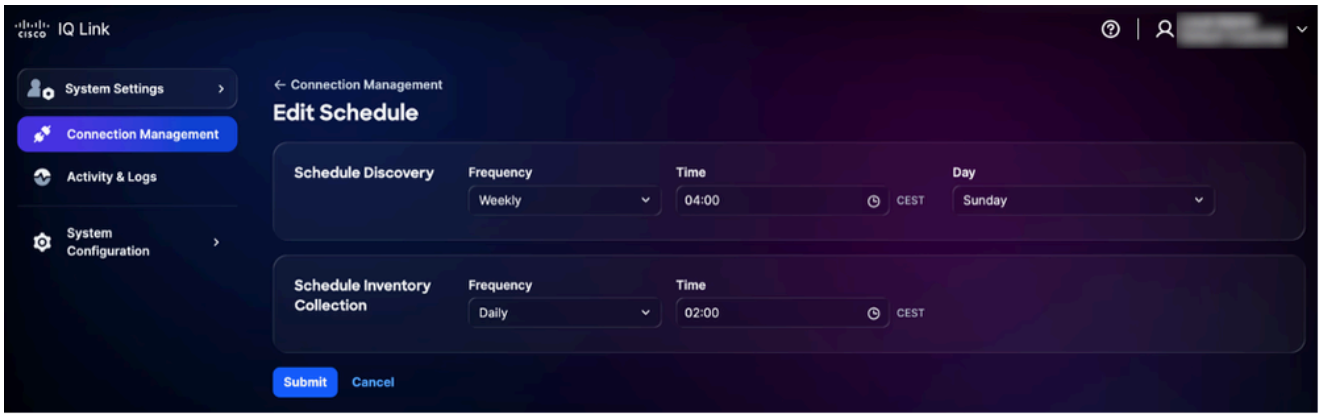
Opmerking: Cisco IQ Link is vooraf geconfigureerd met een automatische planningsinstelling en het systeem start een standaard geautomatiseerd inzamelschema. Het wordt ten zeerste aanbevolen dat u de planning bewerkt om deze af te stemmen op de vereisten en onderhoudsvensters van uw organisatie.

---

planning

Met Scheduling kunt u bepalen wanneer Cisco IQ Link geautomatiseerde gegevensverzameling uitvoert. De verzameling plannen:

1. Klik in het gedeelte Planning op de pagina Verbindingsbeheer op Bewerken voor het schema dat u wilt wijzigen. De pagina Planning bewerken wordt weergegeven.



Plannen bewerken

2. Kies in het gedeelte Ontdekking plannen uw gewenste frequentie en dag uit de vervolgkeuzelijsten en voer de gewenste begintijd in.
3. Kies in het gedeelte Inventarisverzameling plannen uw gewenste frequentie uit de vervolgkeuzelijsten en voer de gewenste begintijd in.
4. Klik op Indienen.

Opmerking: geef 5-10 minuten de tijd om wijzigingen in detectie- of verzamelschema's te synchroniseren en nauwkeurig weer te geven binnen Cisco IQ Link.

Banners

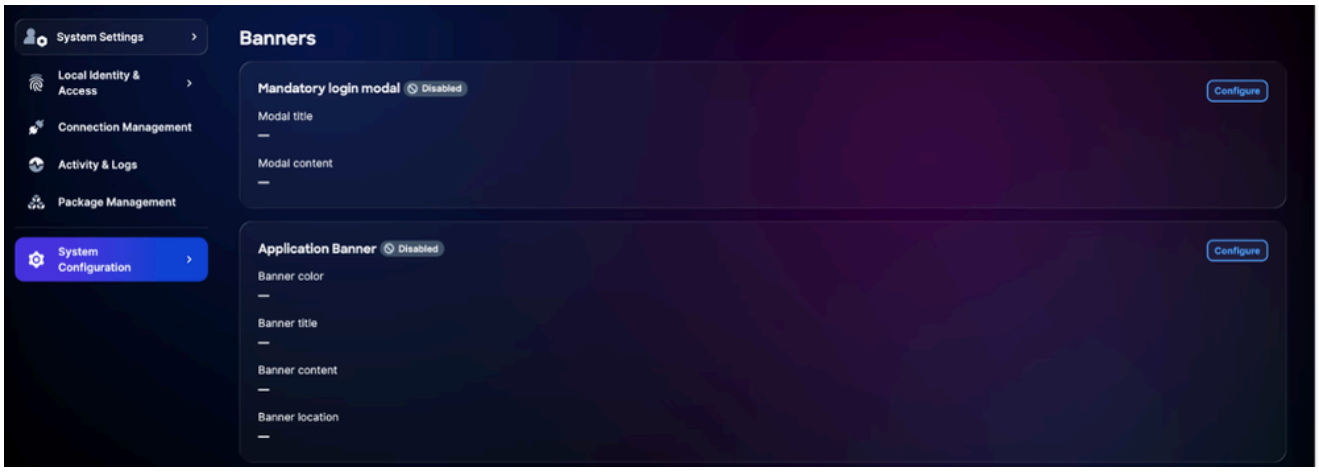
Accountbeheerders kunnen systeembrede banners configureren om te voldoen aan de beveiligings- en nalevingsnormen.

- Verplichte aanmeldmodus: u moet de verplichte banner bevestigen voordat u naar het aanmeldscherm gaat.
- Toepassingsbanners: Dit zijn aangepaste banners die in de toepassing worden weergegeven na succesvolle verificatie.

Verplichte aanmeldingsmodal banners configureren

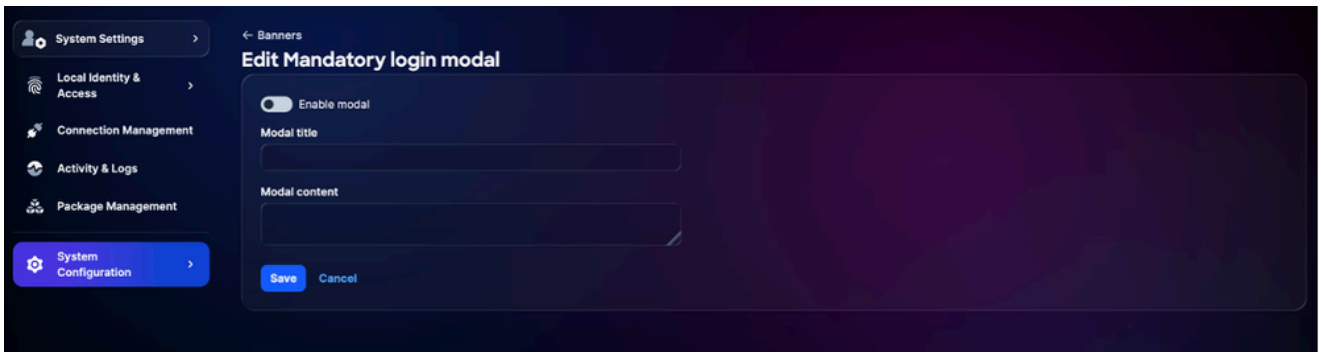
Een verplichte banner configureren:

1. Kies Systeemconfiguratie > Banners in Systeeminstellingen. De pagina Banners wordt weergegeven.



Verplichte banner configureren

2. Klik op Configureren in de modus Verplichte aanmelding. De pagina Aanmeldingsmodal bewerken wordt weergegeven.



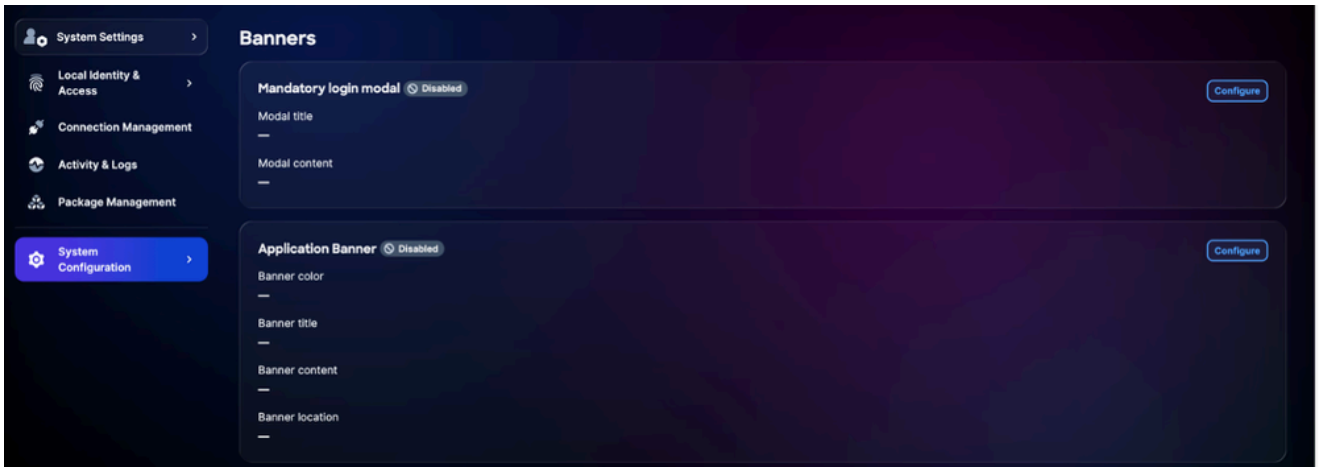
Bewerken Verplichte login modal banner

3. Klik op de schakelaar om de banner in of uit te schakelen.
4. Voer de titel Modal in.
5. Voer de modale inhoud in.
6. Klik op Save (Opslaan). De verplichte inlogmodus wordt opgeslagen.

Toepassingsbanners configureren

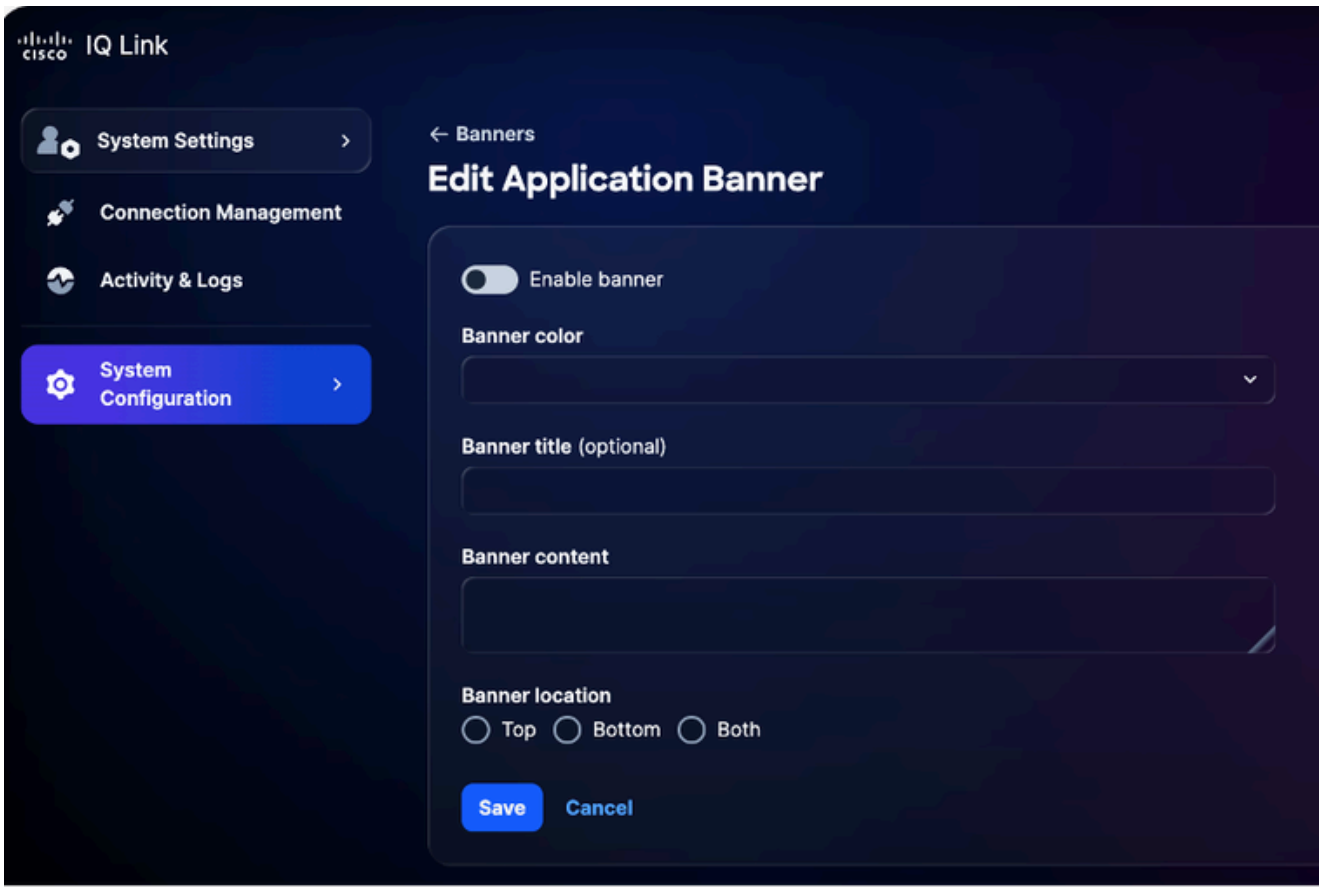
U configureert als volgt een toepassingsbanner:

1. Kies Systeemconfiguratie > Banners in Systeeminstellingen. De pagina Banners wordt weergegeven.



Banner configureren

2. Klik op Configureren in Application Banner. De pagina Toepassingsbanner bewerken wordt weergegeven.



Toepassingsbanner bewerken

3. Klik op de schakelaar om de banner in of uit te schakelen.
4. Selecteer een bannerkleur.
5. Voer de titel van de banner in.
6. Voer de inhoud van de banner in.

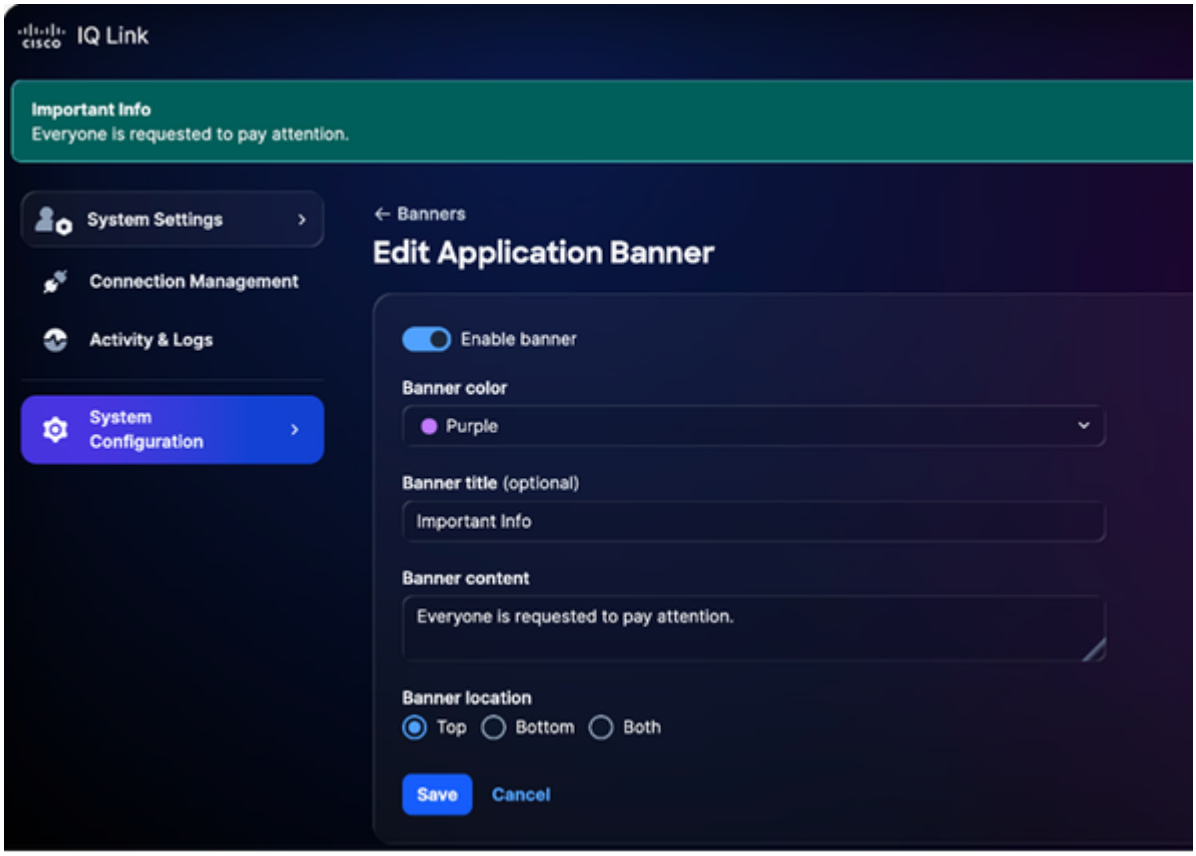
7. Selecteer een bannerlocatie.
8. Klik op Save (Opslaan). De banner wordt weergegeven in de hele toepassing.

Banners bewerken

1. Kies Systeemconfiguratie > Banners in Systeeminstellingen. De pagina Banners wordt weergegeven.

Toepassingsbanner bewerken

2. Klik op Edit (Bewerken). De pagina Toepassingsbanner bewerken wordt weergegeven.



Toepassingsbanner bewerken

3. Bewerk de gewenste details.
4. Klik op de schakelaar om de banner in of uit te schakelen.
5. Klik op Save (Opslaan).

Probleemoplossing

U kunt diagnostische en logbestanden verzamelen van het Cisco IQ-systeem en deze veilig overbrengen naar een SCP-server. Deze bestanden kunnen worden gedeeld met het ondersteuningsteam bij het melden van problemen om waardevolle context te bieden en te helpen bij het oplossen van problemen.

Diagnostische en logbestanden verzamelen:

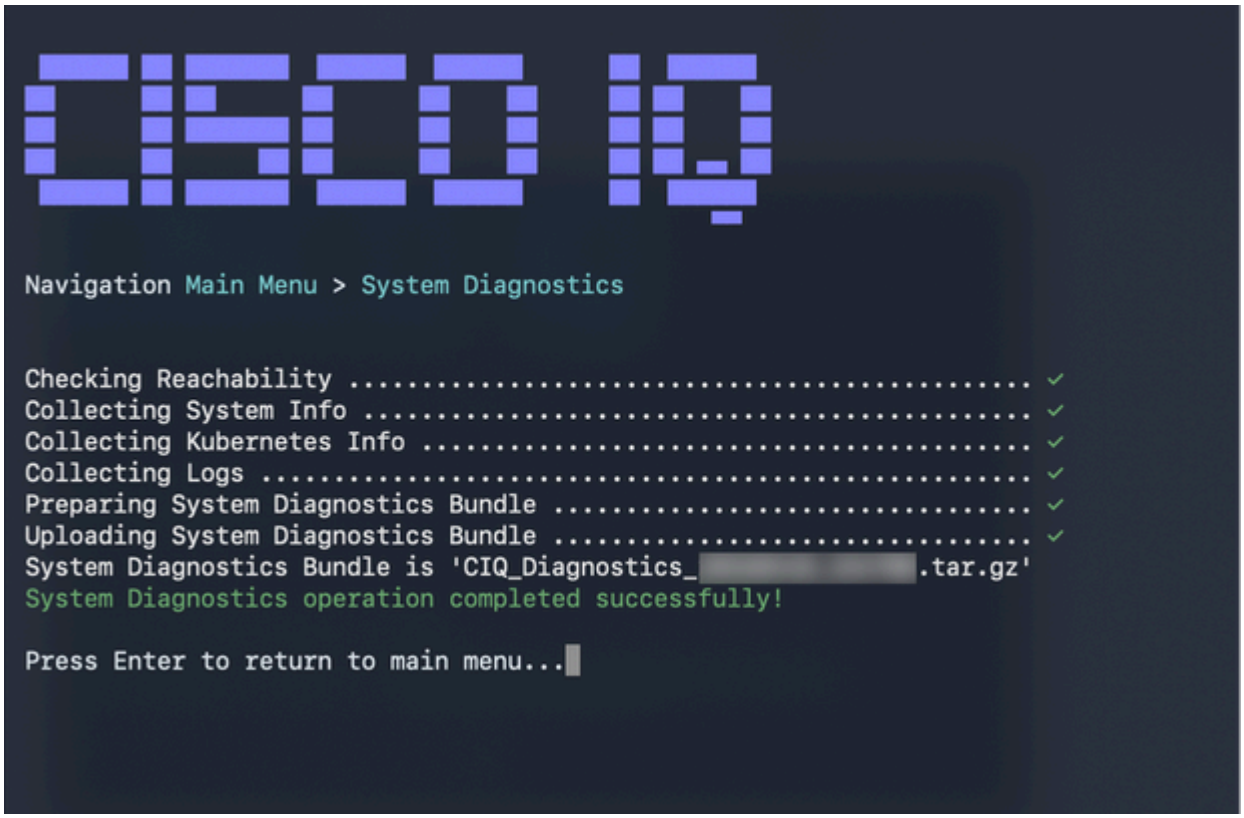
1. Meld u aan bij Cisco IQ.

Hoofdmenu

2. Voer in het hoofdmenu van Cisco IQ "3" in en druk op Enter om Systeemdiagnose te selecteren.

Systeemdiagnose

3. Voer het SCP/SFTP-serveradres in.
4. Voer de SCP/SFTP-serverpoort in.
5. Voer het pad van de SCP/SFTP-server in.
6. Selecteer een protocol.
7. Voer de gebruikersnaam in.
8. Voer het wachtwoord in.
9. Voer "C" in en druk op Enter om door te gaan met de systeemdiagnose.



Systeemdiagnosebewerking voltooid

Het systeem start het diagnoseproces en voert de volgende acties uit:

- controleerbaarheid
- Systeeminformatie verzamelen
- Het verzamelen van Kubernetes informatie
- Logbestanden verzamelen
- Systeemdiagnosebundel voorbereiden
- Systeemdiagnosebundel uploaden

Na voltooiing wordt een bevestigingsbericht weergegeven met de naam van de gegenereerde bundel.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.