Cisco IQ Link Operations Guide v1.1.1

Inleiding

Cisco IQ™ biedt klanten verbeteringen en functies die zijn ontworpen om de zichtbaarheid van bedrijfsmiddelen te verbeteren, slimmere inzichten te bieden in hun omgevingen en het beheer van casussen te stroomlijnen. Daarnaast optimaliseren AI-functies zoals de Cisco IQ AI Assistant operationele resultaten en de Cisco IQ-gebruikerservaring door contextueel inzicht te bieden dat gebruikers 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

Beheerders moeten de volgende referenties 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

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 Local Admin Security in Systeemconfiguratie.

Je hebt drie (3) pogingen om het juiste wachtwoord in te voeren binnen een periode van tien (10) minuten. Als alle drie (3) pogingen niet succesvol zijn, wordt uw account tijdelijk gedurende 60 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.

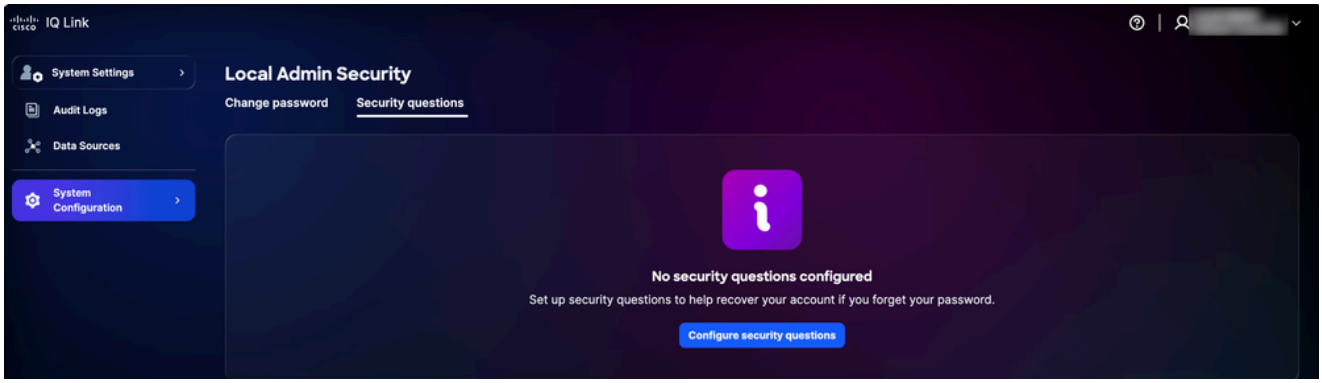
Uw account wordt automatisch ontgrendeld na 60 minuten, waarna u kunt proberen in te loggen of uw wachtwoord opnieuw in te stellen.

Beveiligingsvragen en -antwoorden instellen

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

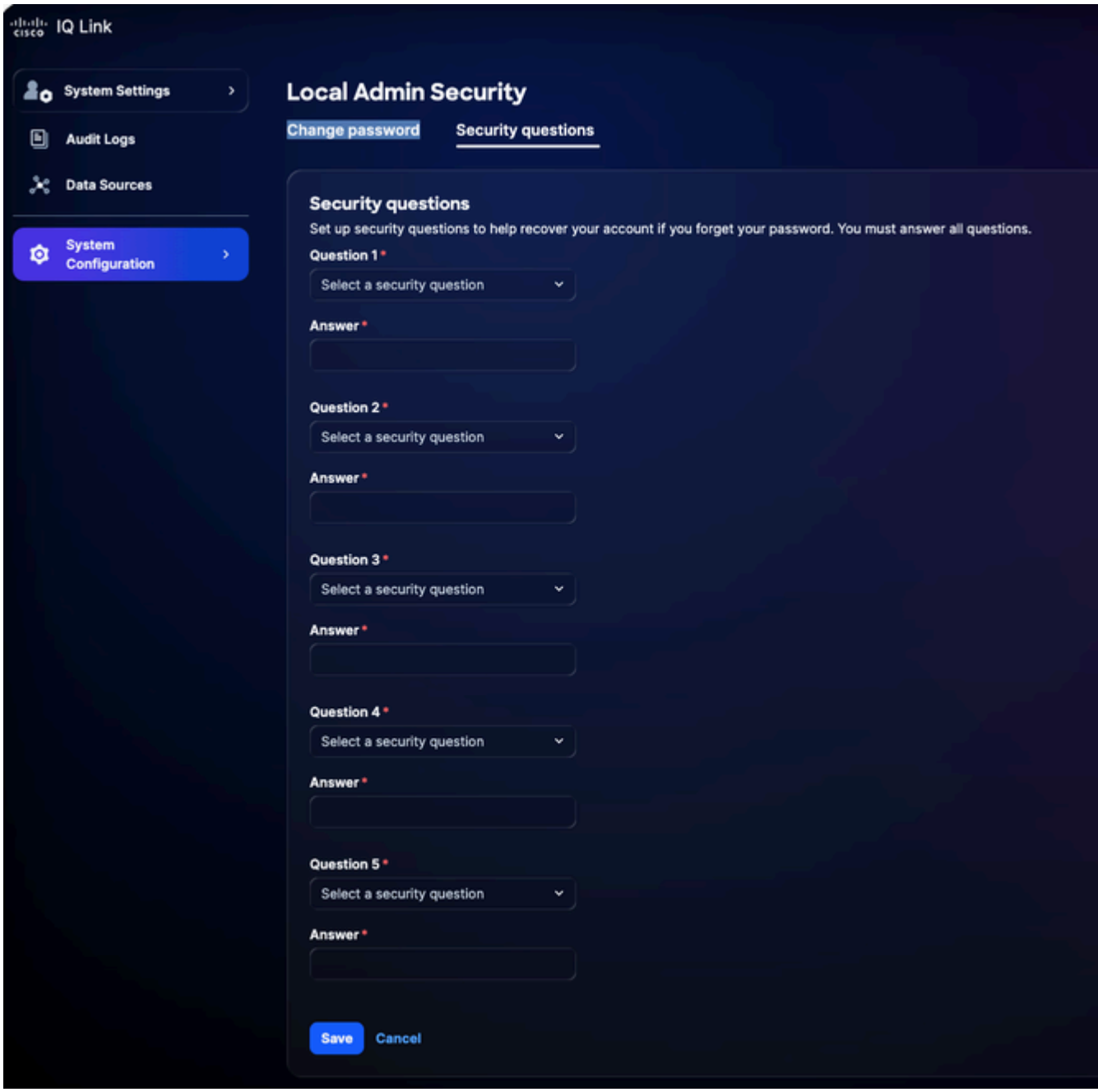
Beveiligingsvragen instellen:

1. Kies in Systeeminstellingen de optie Systeemconfiguratie > Beveiliging van lokale beheerder > Beveiligingsvragen.



Veiligheidsvragen

2. Klik op Beveiligingsvragen configureren.



Veiligheidsvragen

3. Kies vijf (5) beveiligingsvragen uit de vervolgkeuzelijsten.

4. Voer uw antwoord in voor elke vraag.

5. Klik op Save (Opslaan).

Opmerkingen:
· Antwoorden zijn niet hoofdlettergevoelig, bijvoorbeeld "SMITH" en "smith" worden als hetzelfde beschouwd
· Extra ruimtes worden genegeerd, wat betekent dat "Smith" en "Smith" identiek worden behandeld

---

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

Alleen lokale beheerders kunnen het wachtwoord voor Cisco IQ beheren.

Voorwaarden

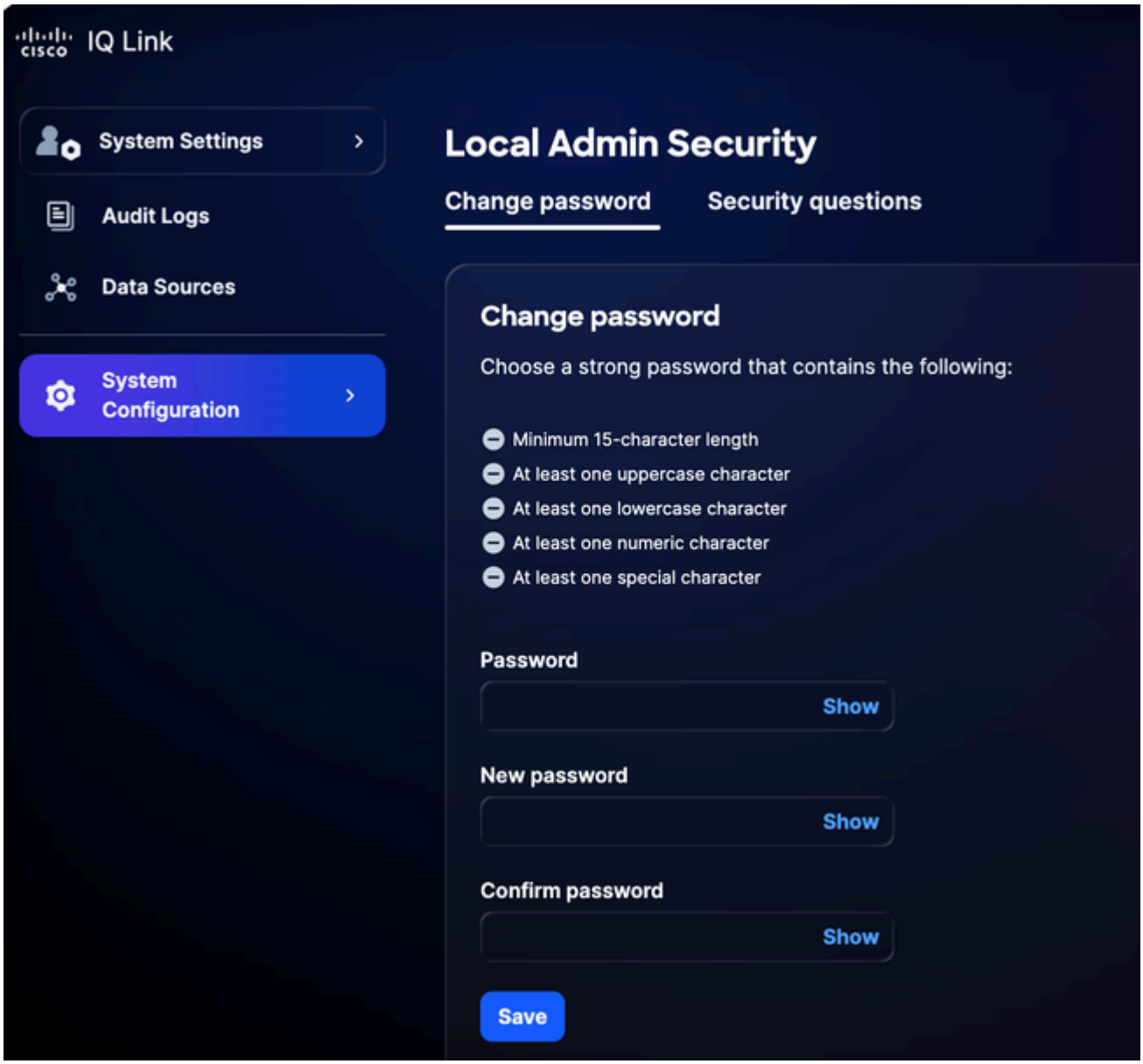
Om wachtwoorden te beheren, moet aan de volgende voorwaarden worden voldaan:

- U bent een lokale beheerder
- U gebruikt een lokale beheerdersaccount (geen eenmalige aanmelding of externe verificatie)
- Je bent ingelogd bij Cisco IQ
- U kent het huidige wachtwoord

Wachtwoorden wijzigen

Zo wijzigt u het wachtwoord:

1. Ga vanuit Systeeminstellingen naar Systeemconfiguratie > Beveiliging lokale beheerder > Wachtwoord wijzigen.



Wachtwoord wijzigen

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

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

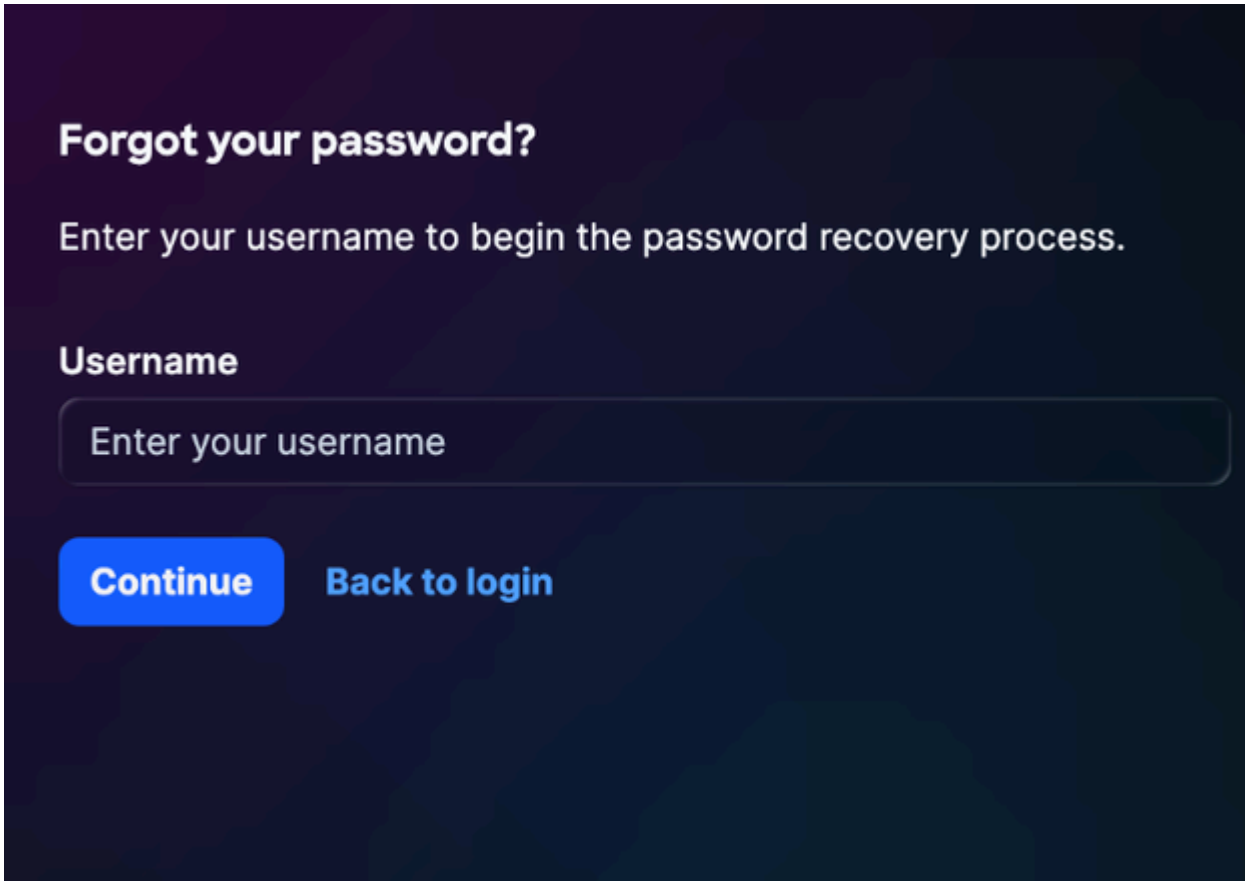
Een vergeten wachtwoord opnieuw instellen

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.

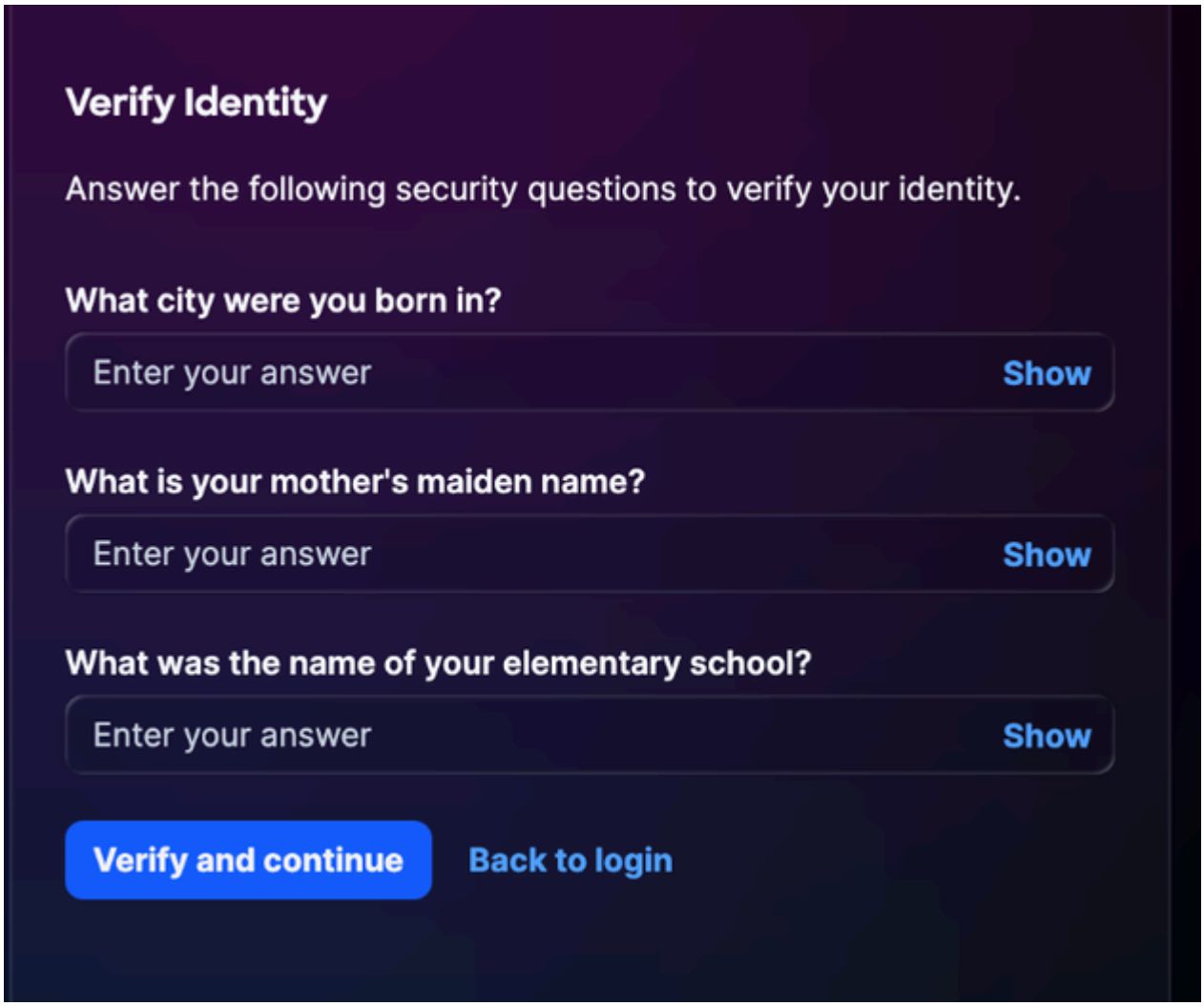
Om een vergeten wachtwoord opnieuw in te stellen:

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



Wachtwoord vergeten

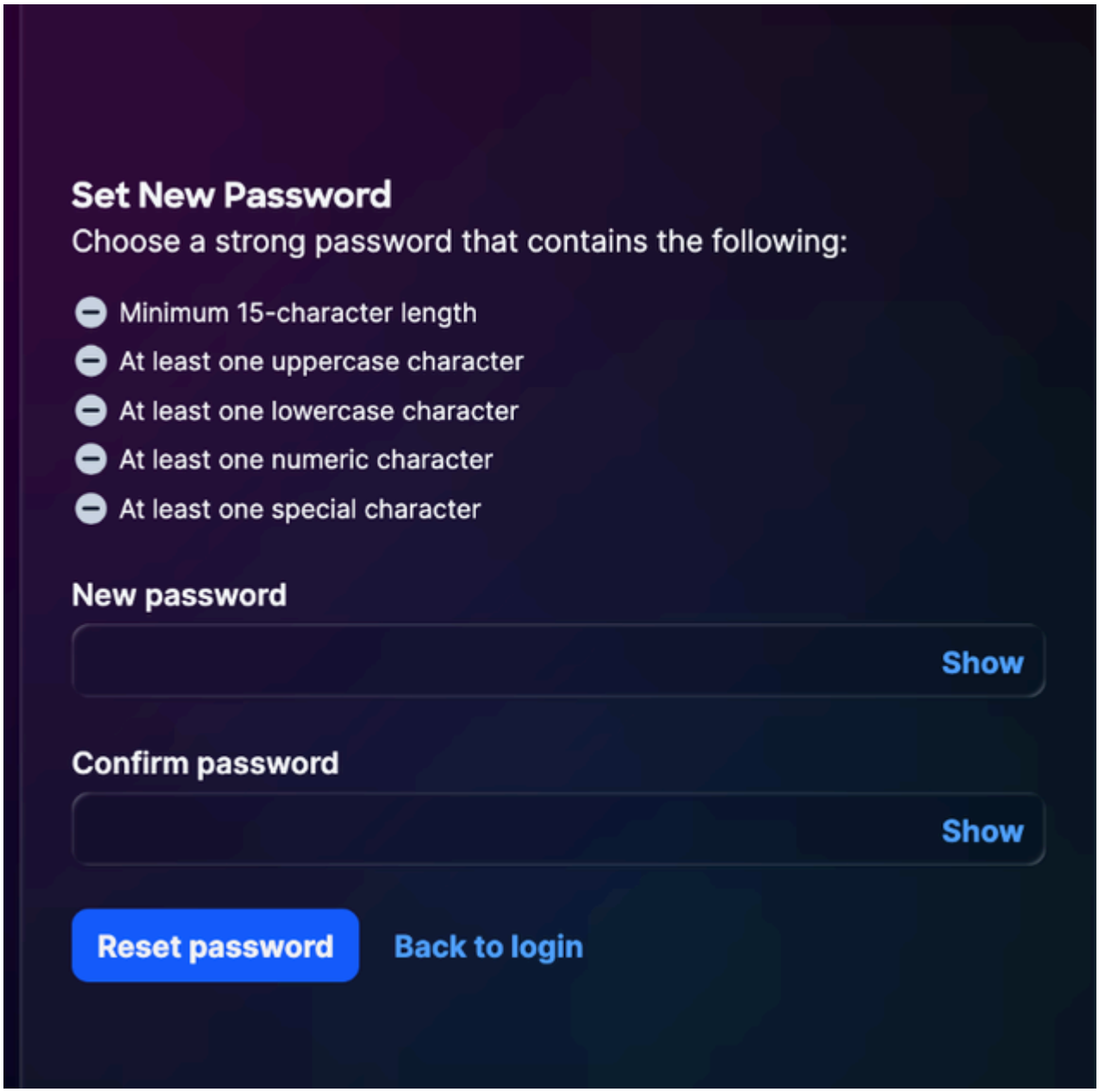
3. Voer de gebruikersnaam in.
4. Klik op Continue (Doorgaan). Op de pagina Identiteit verifiëren worden drie (3) willekeurige beveiligingsvragen weergegeven van de vijf (5) vragen die eerder zijn geconfigureerd.



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

Opmerkingen:
· Je hebt drie (3) pogingen om de beveiligingsvragen correct te beantwoorden binnen een periode van tien (10) minuten. Als alle drie (3) pogingen niet succesvol zijn, wordt uw account tijdelijk gedurende 60 minuten vergrendeld om uw beveiliging te beschermen.
· U kunt uw wachtwoord niet opnieuw instellen tijdens de lock-out periode. 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 60 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.

Identiteitsprovider configureren

Nadat u bent ingelogd bij Cisco IQ Link, kunnen beheerders verschillende instellingen configureren. Beheerders kunnen zich aanmelden bij Cisco IQ Link met behulp van lokale administratie of Identity Provider (IDP) configuratie.

Okta IDP SAML-configuratie voor SSO

Vereisten voor het configureren van IDP SAML

- Toegang van lokale beheerders 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.

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

Veld	Waarde
publiek	niet-beroepsbevolking
Onboarding-rubriek	Selecteer "Nieuwe onboarding"

SAML-configuratieparameters

Parameter	Configuratie	Voorbeeld
Publiek (Entiteit-ID)	FQDN-naam	mymanagementhost.mydomain.com
URL voor eenmalige aanmelding	SAML 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.

Configuratie-instellingen voor SLO

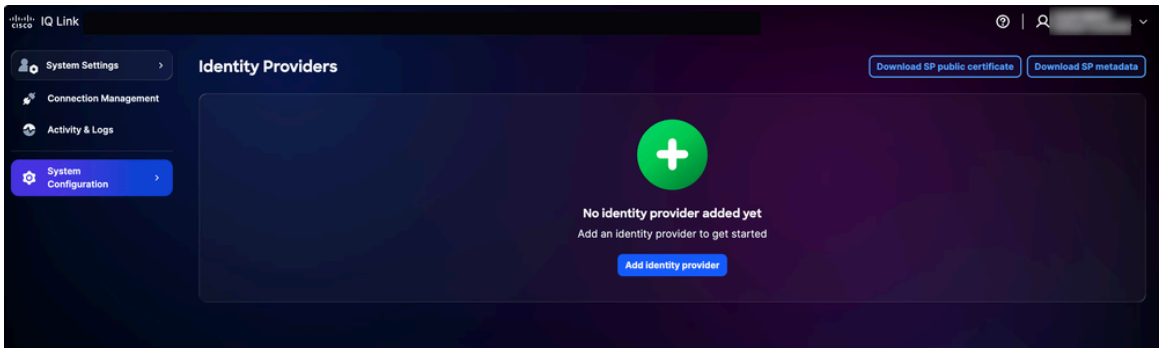
Veld	Waarde
handtekeningcertificaat	Voor Okta is dit certificaat alleen vereist als u ervoor kiest om SLO in te schakelen. Download het Handtekeningcertificaat met behulp van het Download SP-certificaat in Identiteitsproviders. Sla het bestand op als sp-public-key.crt. Zie Configuratie eenmalige aanmelding 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. De applicatie beschikbaar stellen of maken zoals vereist door de provider.

IDP toevoegen

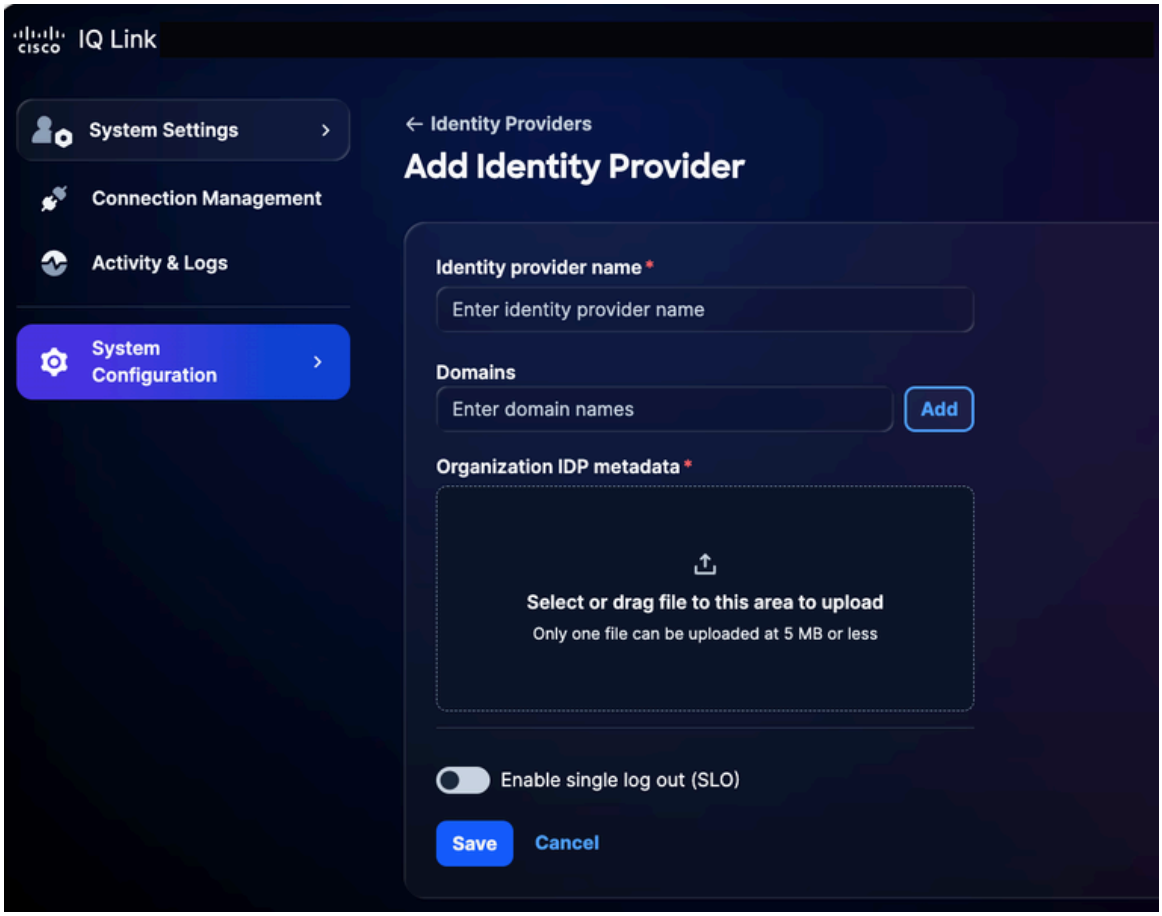
Een IDP toevoegen in Cisco IQ Link:

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.

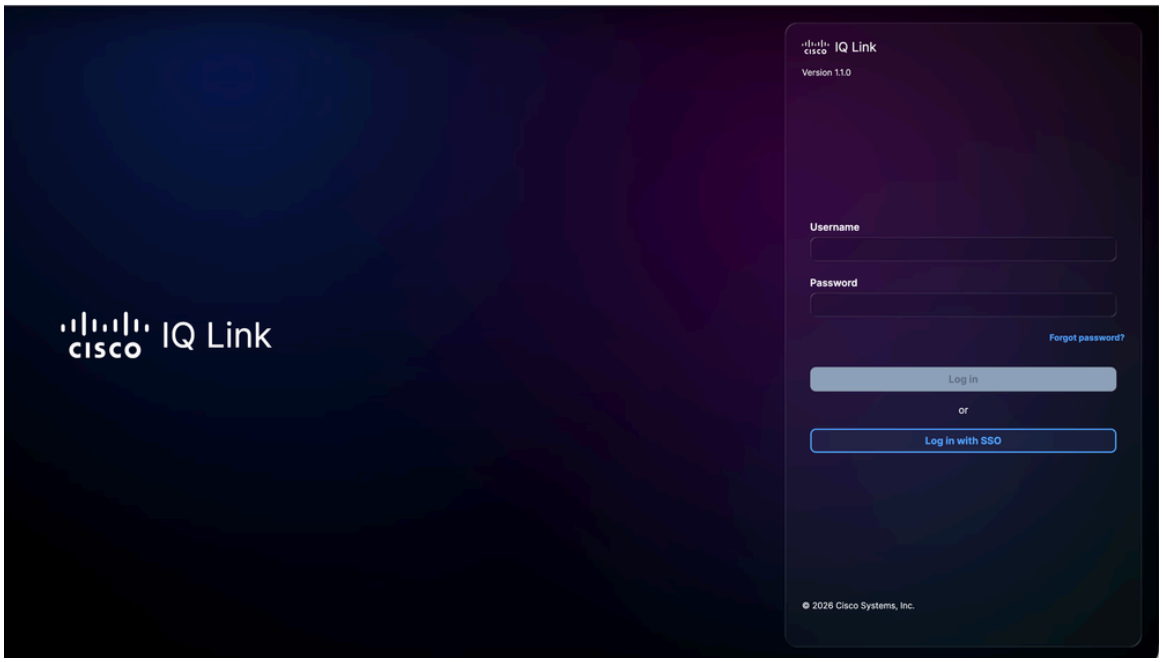
3. Voer de naam van de identiteitsprovider in.

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).

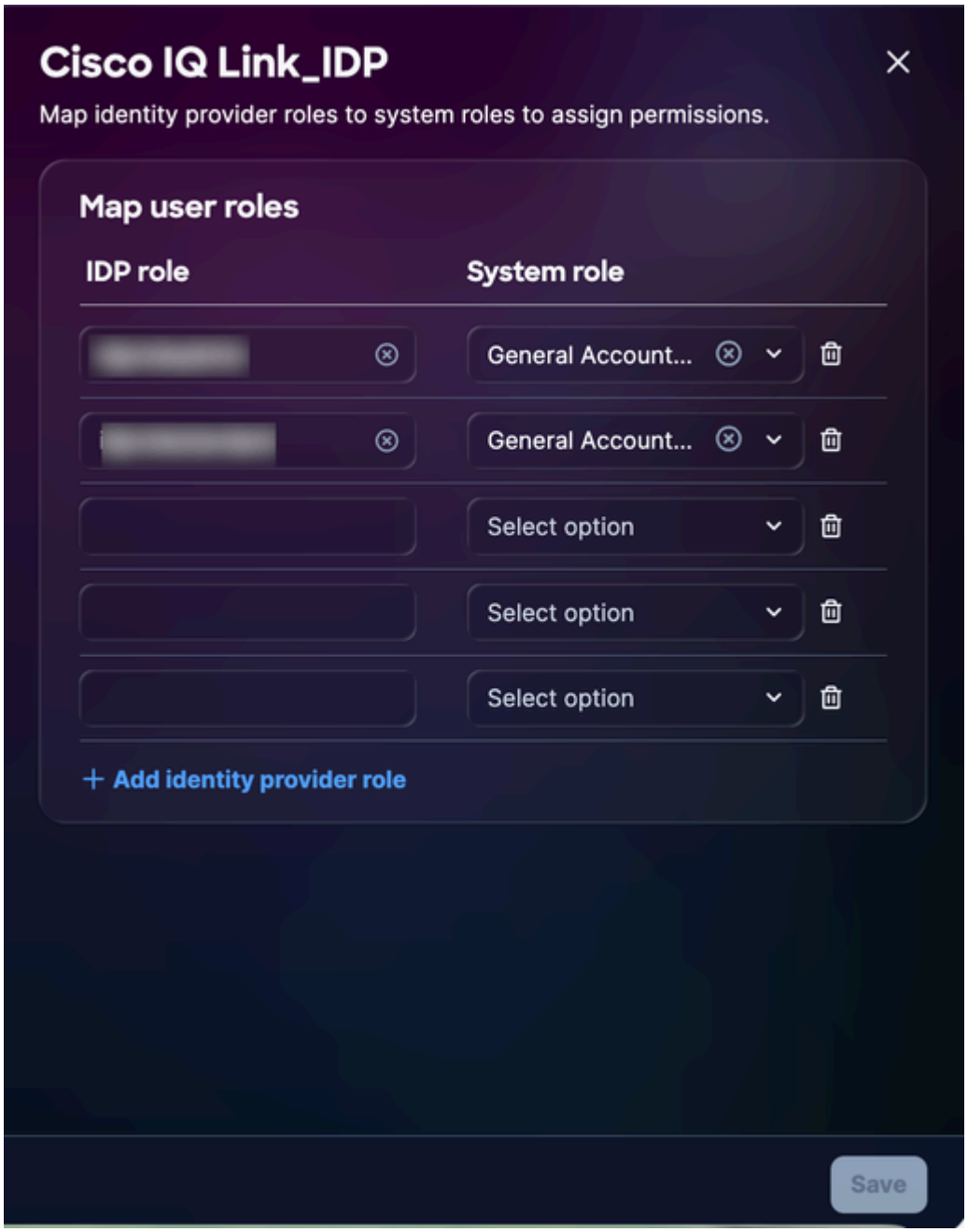
6. (Optioneel) Schakel de knop Enkelvoudige afmeldoptie inschakelen in. U kunt de SLO later ook inschakelen.
7. Klik op Save (Opslaan).
8. Eenmaal geconfigureerd, geeft de aanmeldingspagina een optie weer om in te loggen met SSO (via IDP).



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.



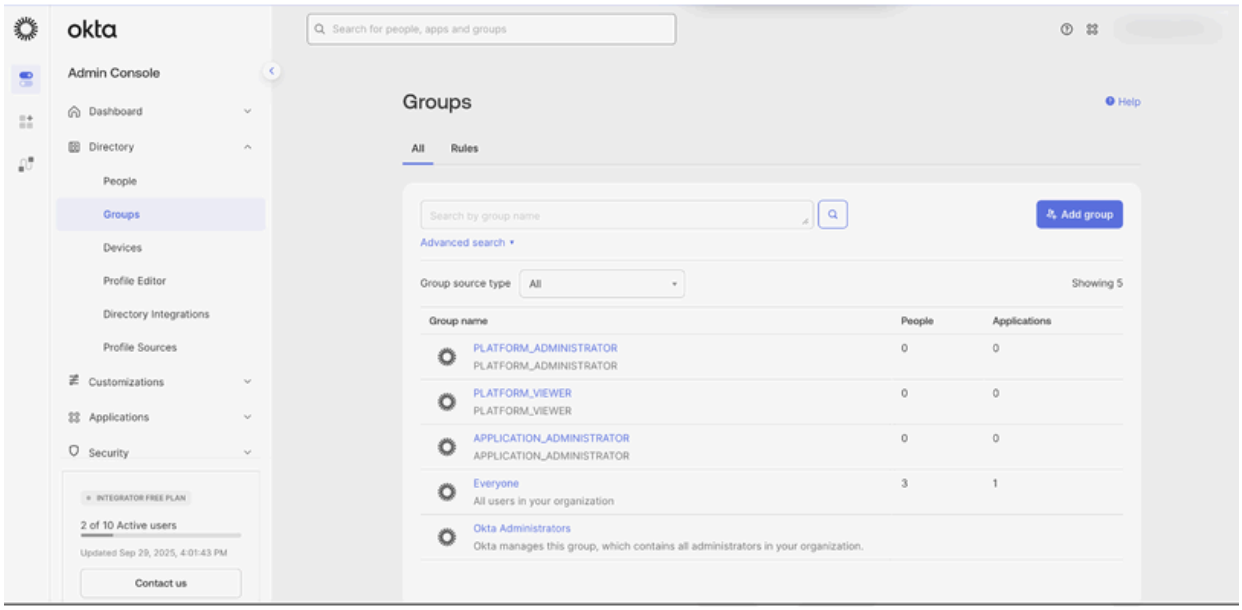
Toewijzing van gebruikersrollen

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

    - general_account _administrator: De algemene accountbeheerder heeft volledige rechten om alle acties in het product uit te voeren
    - general_account _viewer: 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.



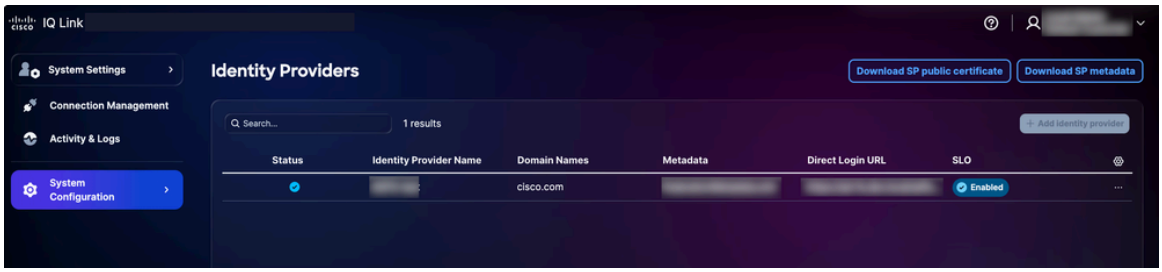
referentie voor roltoewijzing

3. Voeg extra rollen toe zoals vereist door te klikken op Identiteitsproviderrol toevoegen.
4. Klik op Save (Opslaan).

Configuratie eenmalige aanmelding

Als u ervoor kiest om SLO in te schakelen, 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:

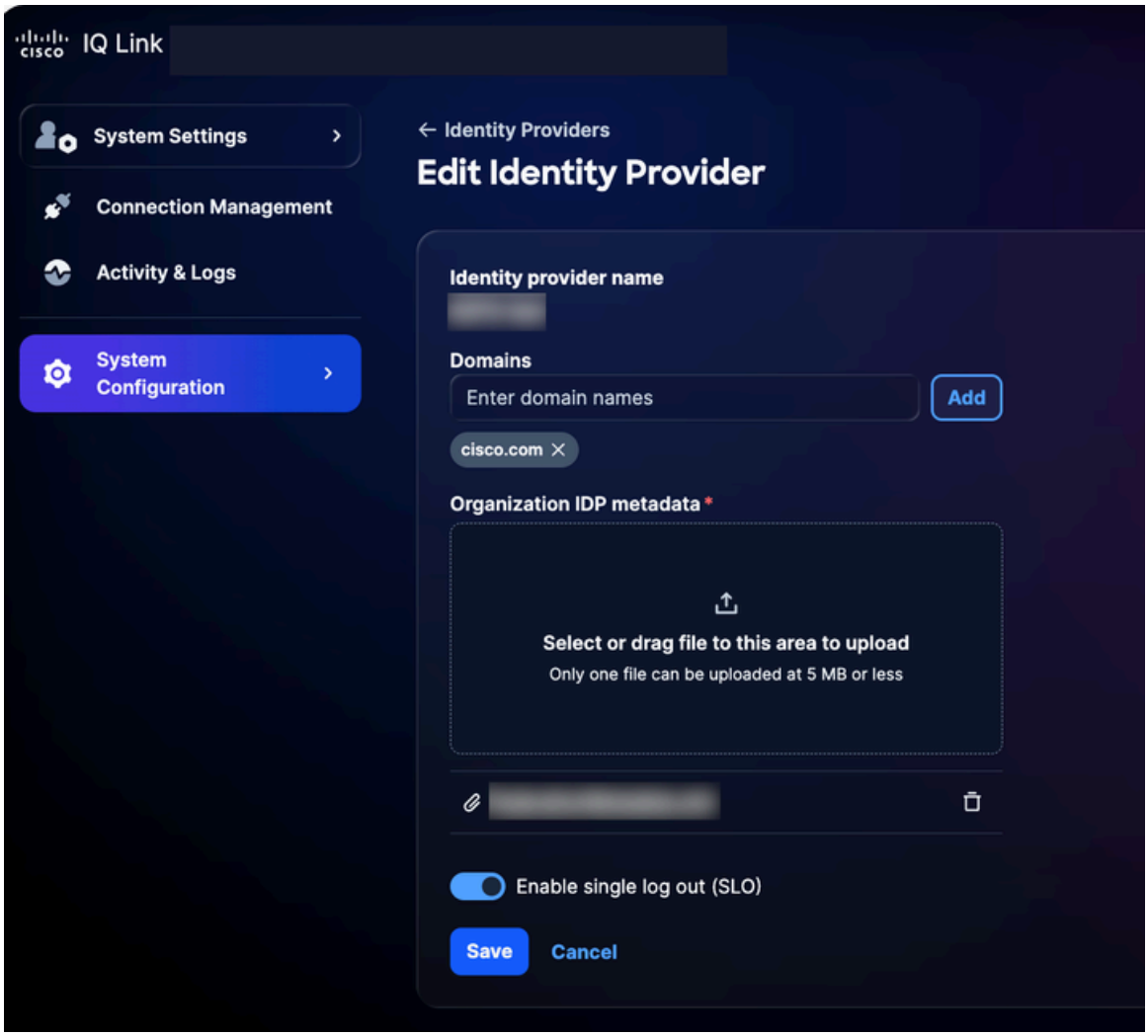
1. Klik op de pagina Identiteitsproviders op Openbaar SP-certificaat downloaden.



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 de sectie 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 lokale beheerder is geslaagd
- 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:

Probleemoplossing

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 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+

- Active Directory-integratie geconfigureerd
- SSL/TLS-certificaten op ADFS
- Toegang voor beheerders tot Cisco IQ
- 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)

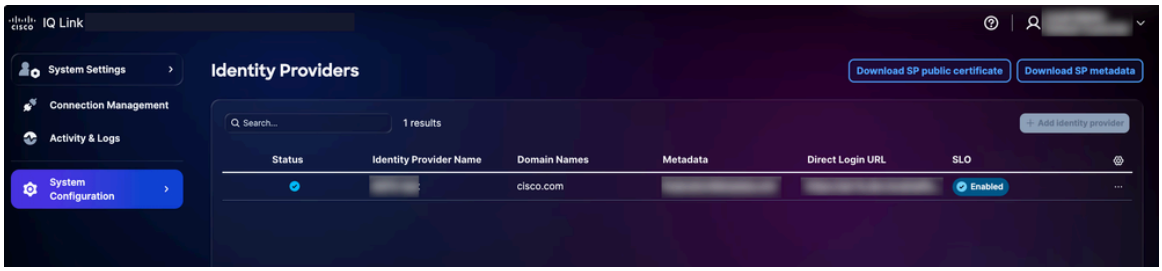
Configuratie ADFS-server

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	Active Directory-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.



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 uit een bestand importeren.
10. Klik op Bladeren om het metagegevensbestand van de serviceprovider 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.

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.

Vereiste claims

aanspraak	Doel	bron
Email	Gebruikersidentificatie	AD Mail
Weergavenaam	Volledige naam van de gebruiker	AD-weergavenaam
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. Definieer claimregels om gebruikersinformatie en groepslidmaatschap naar Cisco IQ te sturen.

```
$claimRules = @’

@RuleTemplate = “LdapClaims”

@RuleName = “Send Email and Name”

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

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

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

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

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

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 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

- Het CA-certificaat importeren in het archief van Trusted Root Certification Authorities

```
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
```

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 u de opdrachten hebt uitgevoerd, wordt het metagegevensbestand opgeslagen in C:-metadata.xml.

webbrowser

ADFS-metagegevens exporteren met een webbrowser:

1. Navigeer 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.

ADFS IDP toevoegen

1. Klik op de pagina Identiteitsaanbieders op Identiteitsaanbieder toevoegen.
2. Voer de naam van de identiteitsprovider in.
3. Voer de domeinnaam (domeinnamen) in (bijvoorbeeld company.com).
4. (Optioneel) Schakel indien nodig de knop Enkelvoudige afmeldknop 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 uit Active Directory kunt vinden die u kunt gebruiken voor toewijzing. Voer de volgende PowerShell-opdracht uit om groepen in Active Directory 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”] }
```

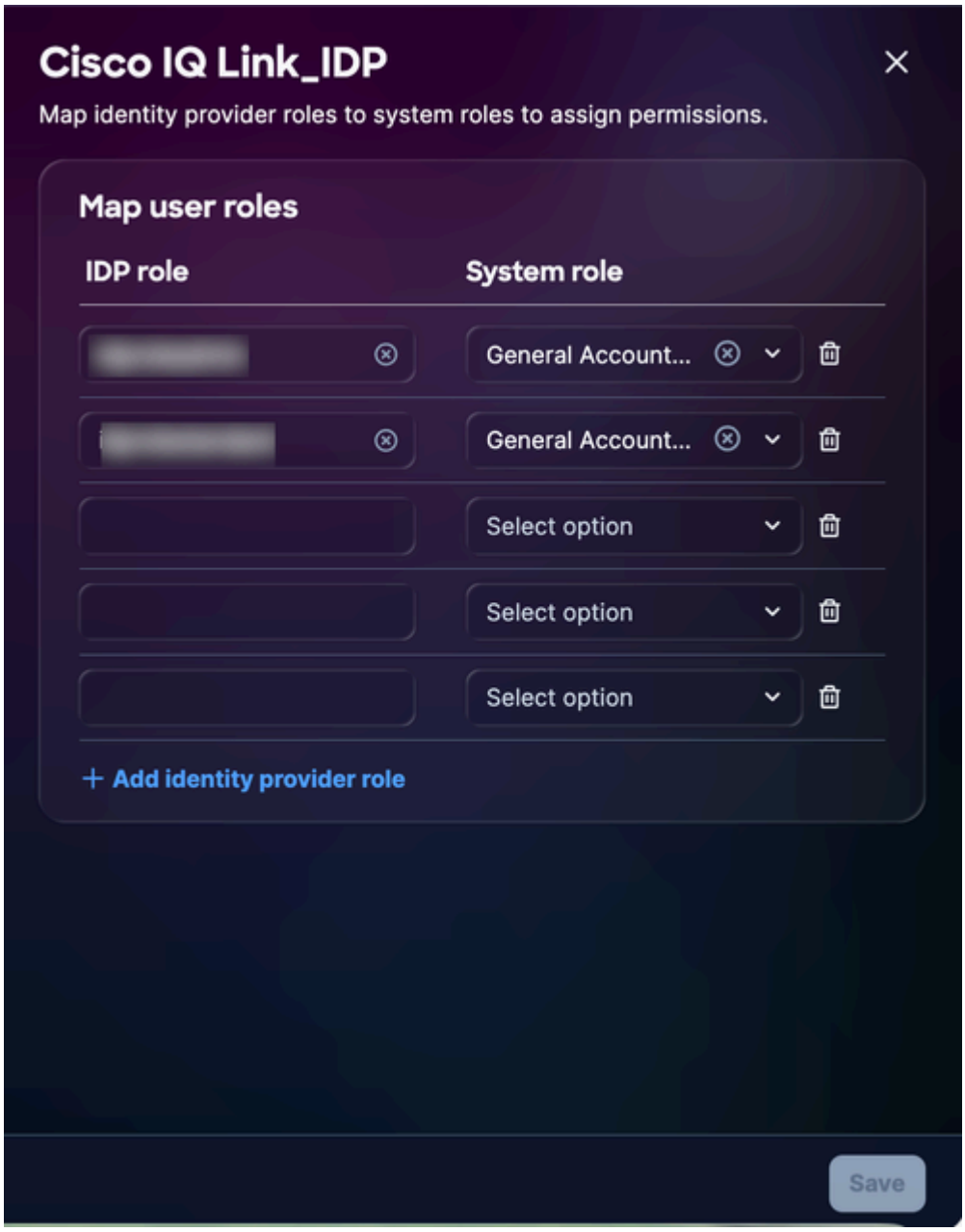
Het systeem zoekt Active Directory rechtstreeks via LDAP op en vereist geen extra modules. Groepsinformatie wordt teruggegeven in de volledige DN-indeling (Distinguished Name), bijvoorbeeld:

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 ze door een beheerder in Active Directory worden gemaakt voordat u de toewijzing van de ADFS-rollen kunt voltooien.

Roltoewijzing configureren:

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:

    - general_account _administrator: De algemene accountbeheerder heeft volledige rechten om alle acties in het product uit te voeren. De IDP-rol (geparseerde naam) is CXIQ-beheerders.
    - general_account_viewer: 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 Save (Opslaan). De status wordt bijgewerkt naar succes.

Verificatie en testen

Verificatie testen

1. Navigeer in een browser in Incognito- of Privémodus naar https://your-cisco-iq-domain.com/login.
2. Meld u aan met uw Active Directory-referenties in domein\gebruikersnaam of user@domain.local-indeling.
3. Controleer of u bent doorverwezen naar de Cisco IQ Home-pagina (na succesvolle verificatie).
4. Bevestig dat de toegewezen rollen de juiste geparseerde groepsnamen (bijvoorbeeld CXIQ Developers) weergeven in uw gebruikersprofiel.

Afmelden testen

Klik op Afmelden bij Cisco IQ om afmelden te testen. Het bericht "Uitloggen, even geduld..." wordt weergegeven en u wordt doorgestuurd naar de pagina Cisco IQ Login. Het systeem beëindigt ook de ADFS-sessie. Als u ADFS rechtstreeks probeert te openen, wordt u gevraagd om opnieuw in te loggen.

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.

ADFS-problemen

uitgeven	Symptomen / beschrijving	Oorzaken / Controles / Workarounds en Fixes
Groepen niet geëxtraheerd	Geen rollen na aanmelding	• Claimregel ontbreekt: voer de instructies opnieuw uit in Regels voor ADFS-claim configureren

uitgeven	Symptomen / beschrijving	Oorzaken / Controles / Workarounds en Fixes
		• Attribuut verkeerde groep: Moet http://schemas.xmlsoap.org/claims/Group zijn • Gebruiker bevindt zich niet in AD-groepen
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 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

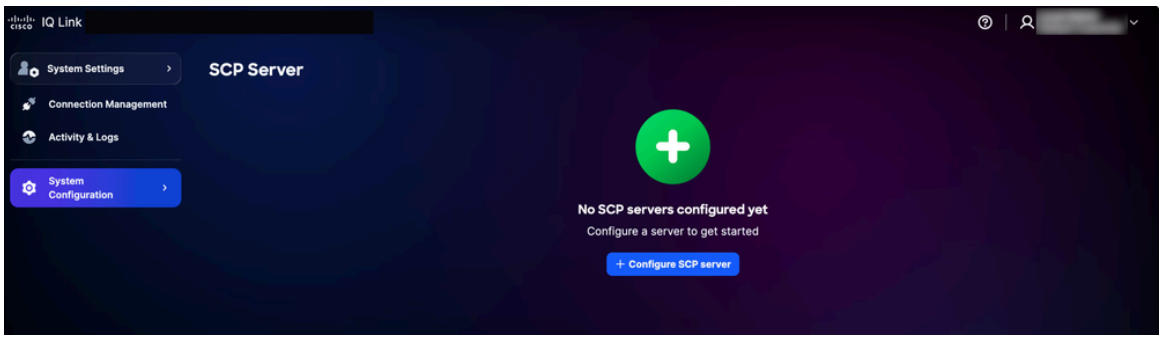
```
Get-AdfsRelyingPartyTrust -Name “Cisco IQ - Stage” | Select-Object SamlEndpoints
```

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 repareren van de Cisco IQ-installatie.

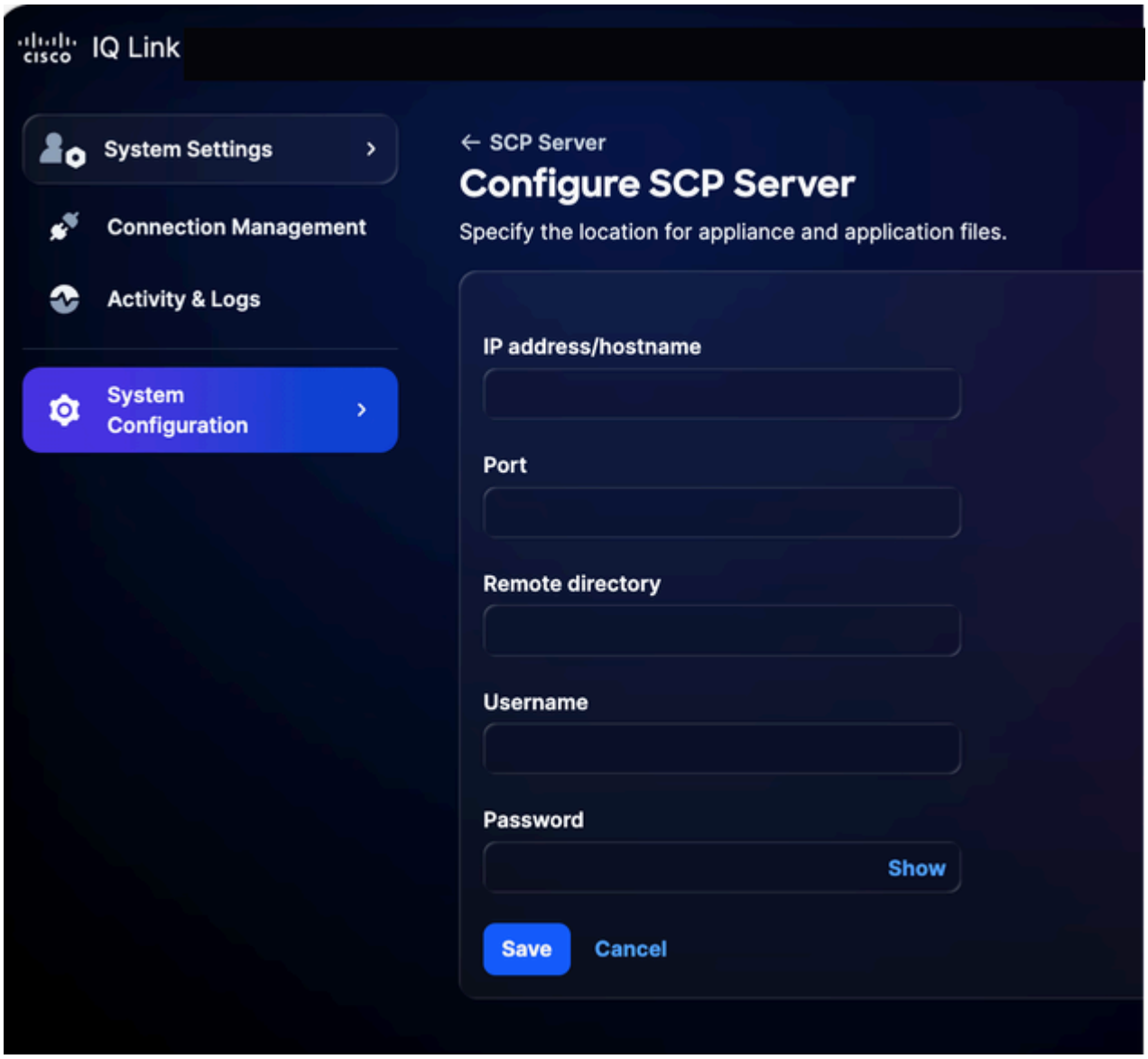
Een SCP-server toevoegen:

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



Startpagina SCP-server

2. Klik op SCP-server configureren.



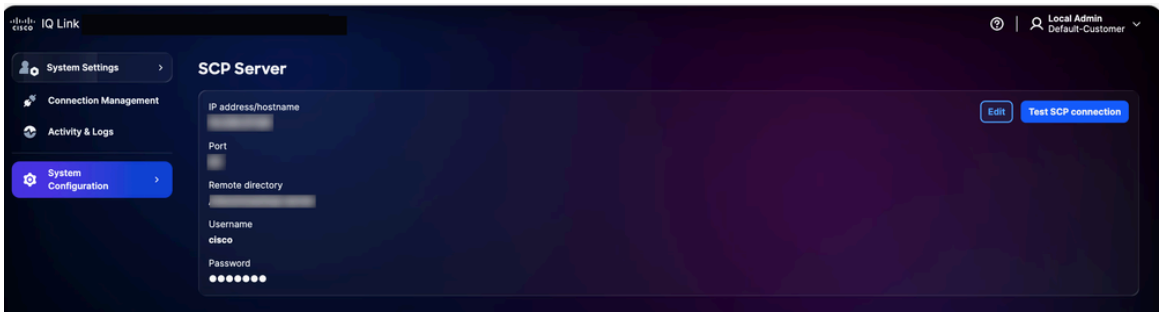
SCP-server configureren

3. Voer het IP-adres/de hostnaam in.
4. Voer een poortnummer 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

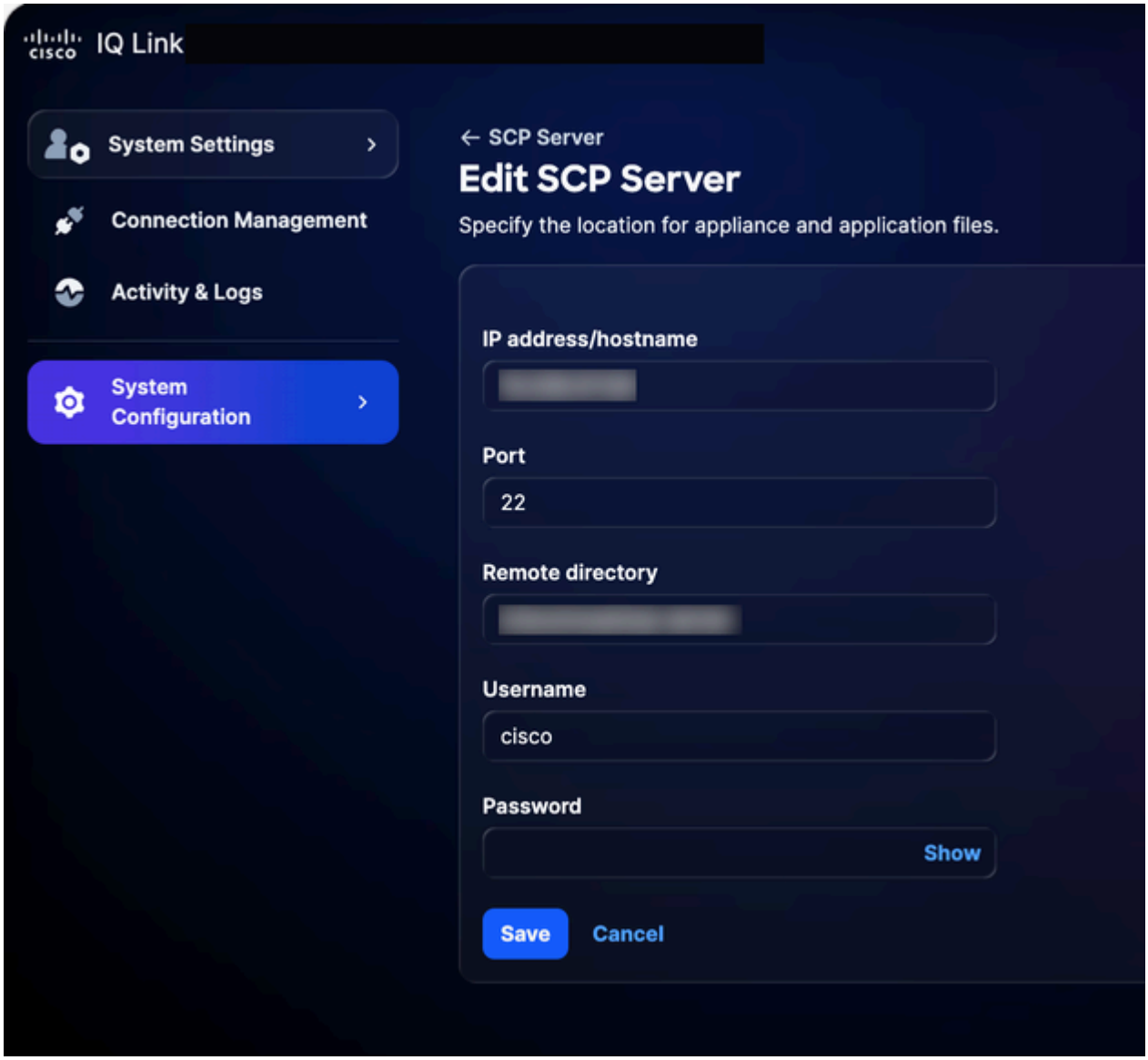
U bewerkt als volgt een bestaande SCP-server:

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).

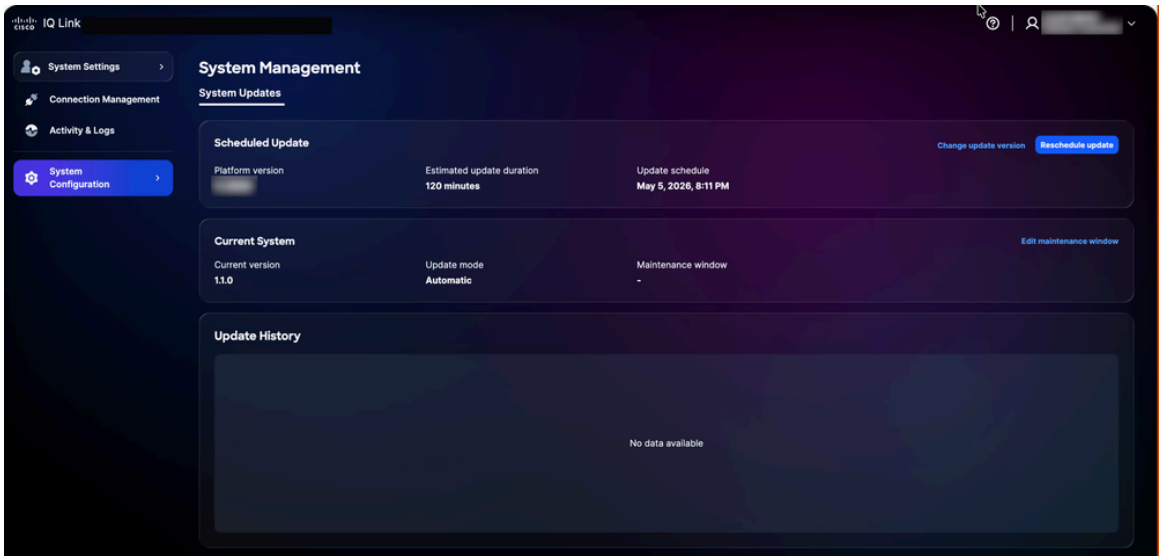
Systeembeheerupdate

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

herschikkingssysteem

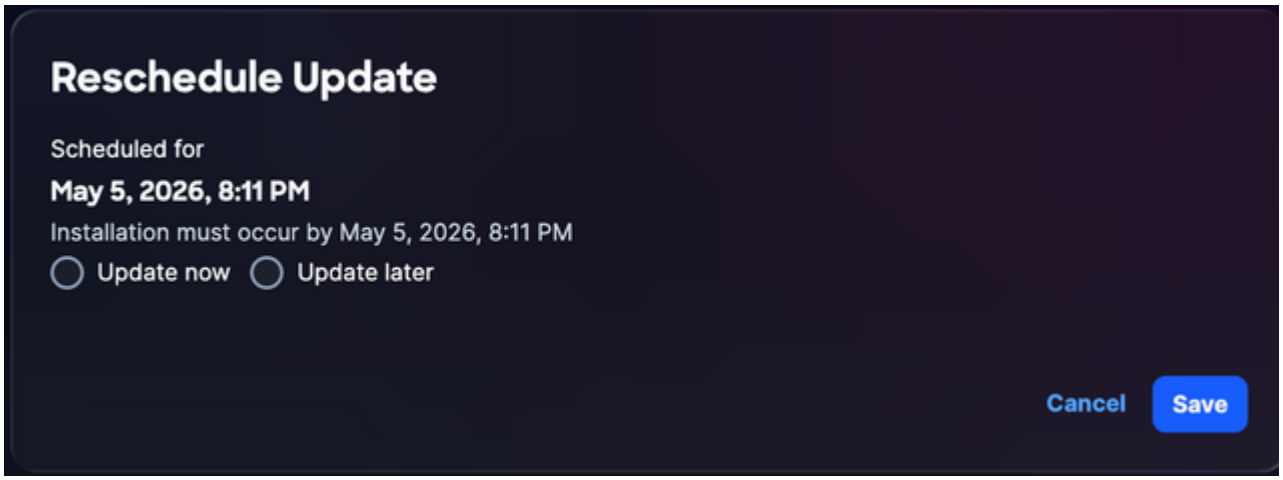
De systeemupdate opnieuw plannen:

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.



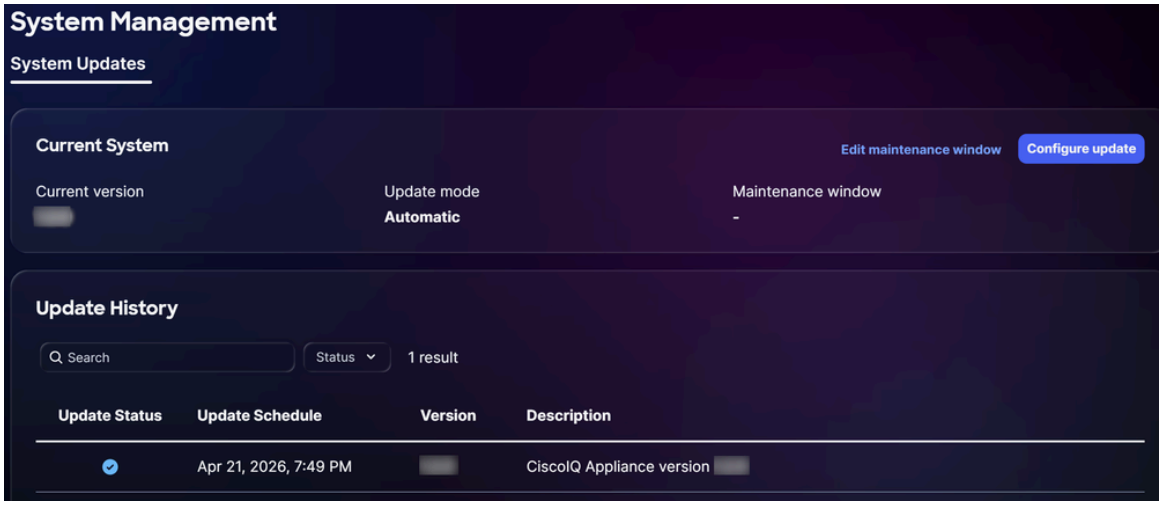
Systeemupgrade

2. Klik op Update opnieuw plannen.



Upgrade opnieuw plannen

3. Klik op Nu bijwerken voor onmiddellijke herschikking of Later bijwerken om een andere tijd te plannen.
4. Klik op Save (Opslaan). Er wordt een bevestiging weergegeven en u wordt doorgestuurd naar de homepage Systeemupdate.



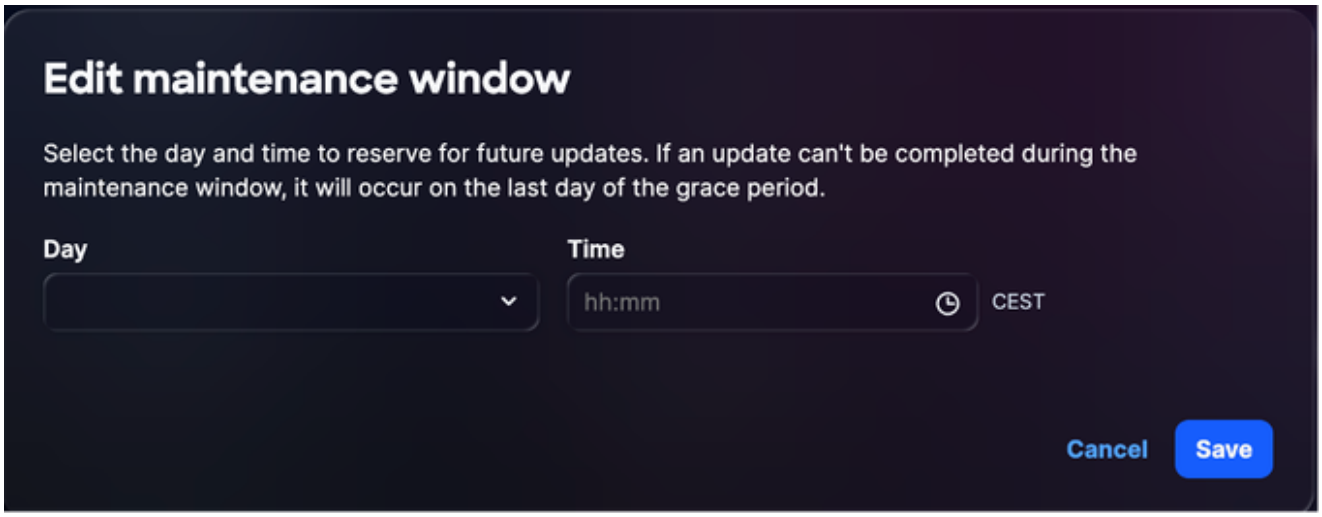
Succesvolle upgrade

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.

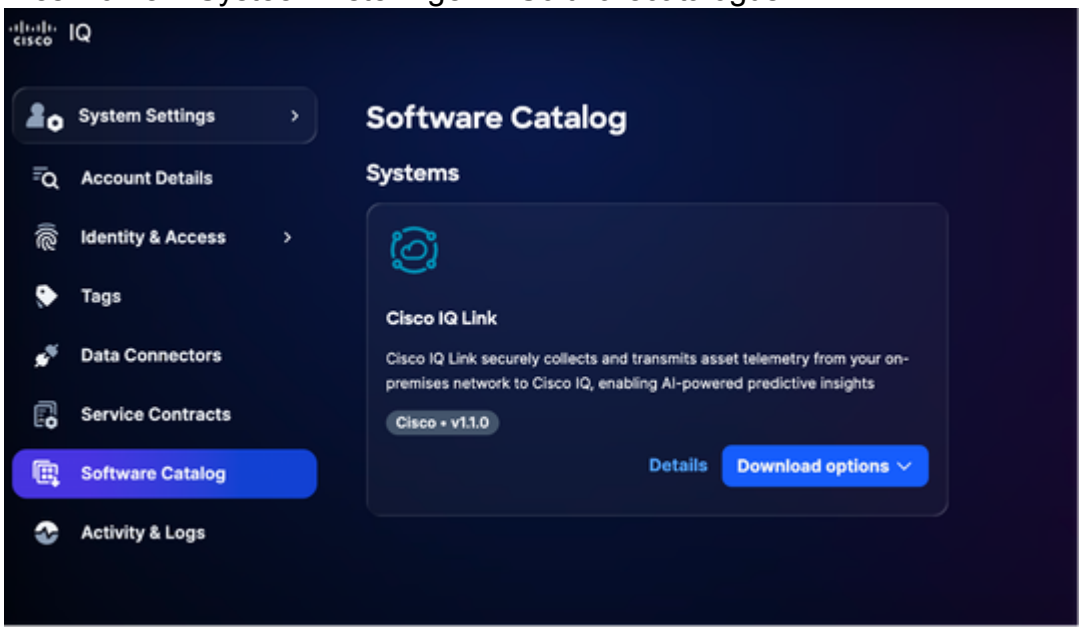
Opmerkingen:
· Als er geen upgradeschema is geconfigureerd, worden er standaard perioden van twee (2) weken opgegeven voor upgrades die niet opnieuw worden opgestart en vier (4) weken voor upgrades die opnieuw moeten worden opgestart. Na deze respijtperioden moeten updates handmatig worden uitgevoerd.
· 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.

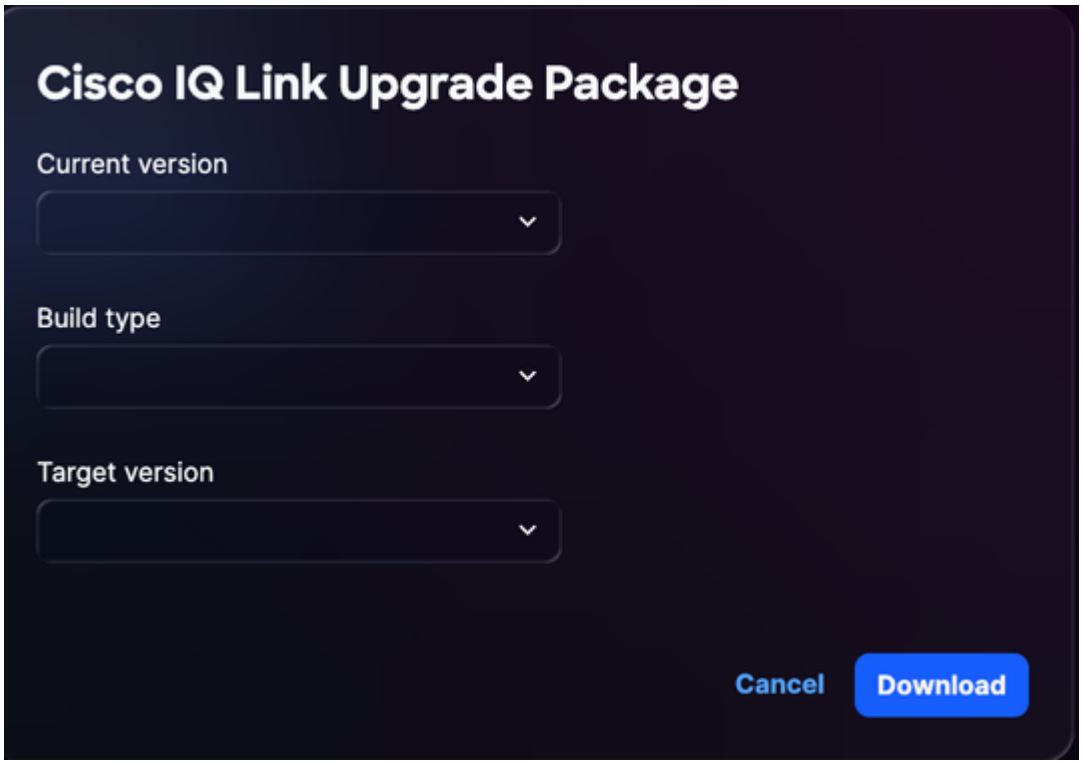
U kunt het systeem als volgt handmatig bijwerken:

1. Meld u aan bij Cisco IQ SaaS.
2. Kies Home > Systeeminstellingen > Softwarecatalogus.



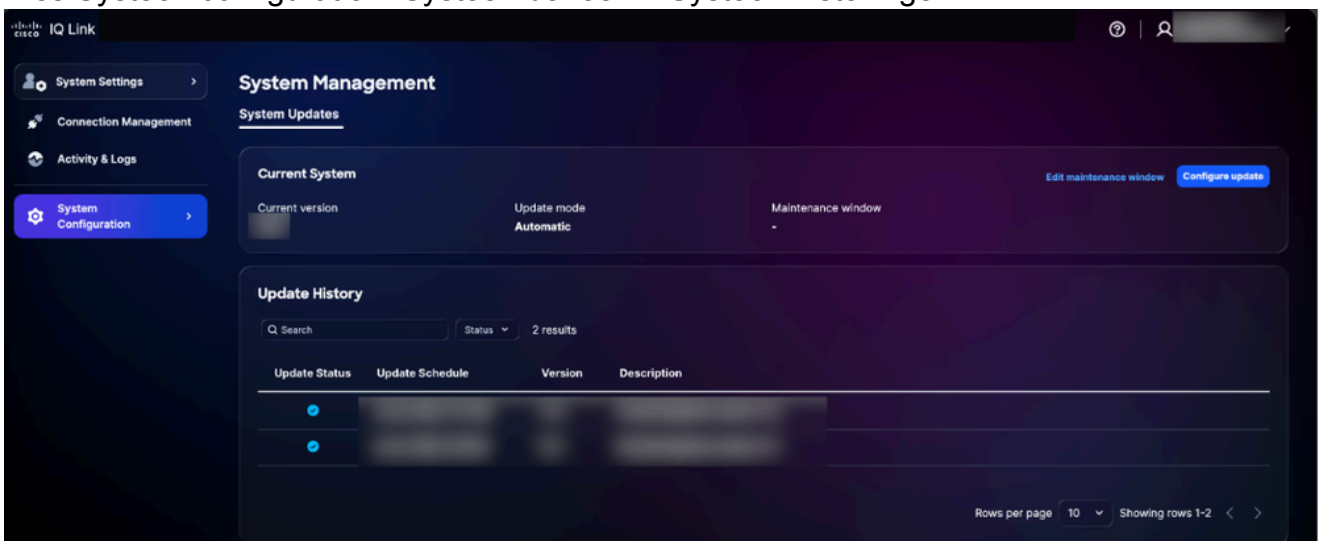
softwarecatalogus

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



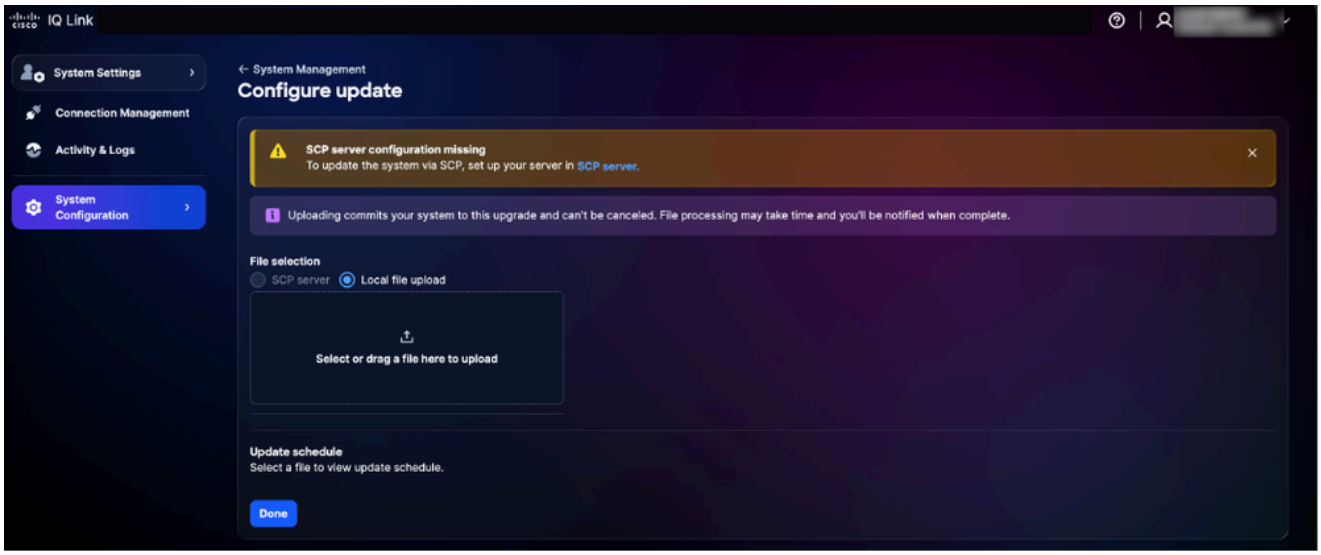
Upgradepakket

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



Update configureren

10. Klik op Update configureren.



Lokaal bestand uploaden

11. Klik op de knop Lokaal bestand uploaden.
12. Selecteer of sleep het gedownloade upgradebundelbestand naar het uploadveld.
13. Klik op Gereed. Er wordt een bevestigingsbericht weergegeven nadat het systeem is bijgewerkt.

Configuratie SSL-certificaten

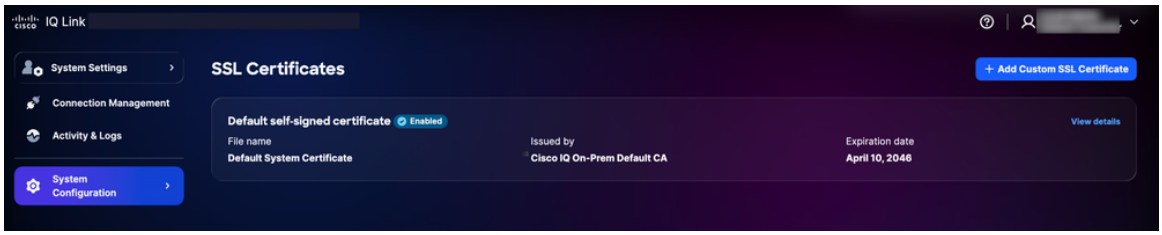
Een standaard zelf ondertekend certificaat is vooraf geïnstalleerd en ingeschakeld in Cisco IQ, maar gebruikers kunnen aangepaste SSL-certificaten uploaden. Wanneer een aangepast SSL-certificaat is ingeschakeld, wordt het gebruikt voor HTTPS-verbindingen; als het certificaat is uitgeschakeld of verwijderd,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

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. Na het toevoegen, bewerken of verwijderen van een SSL-certificaat moet de klant het nieuwe SSL uploaden zoals beschreven in de sectie SLO-configuratie voltooien 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.

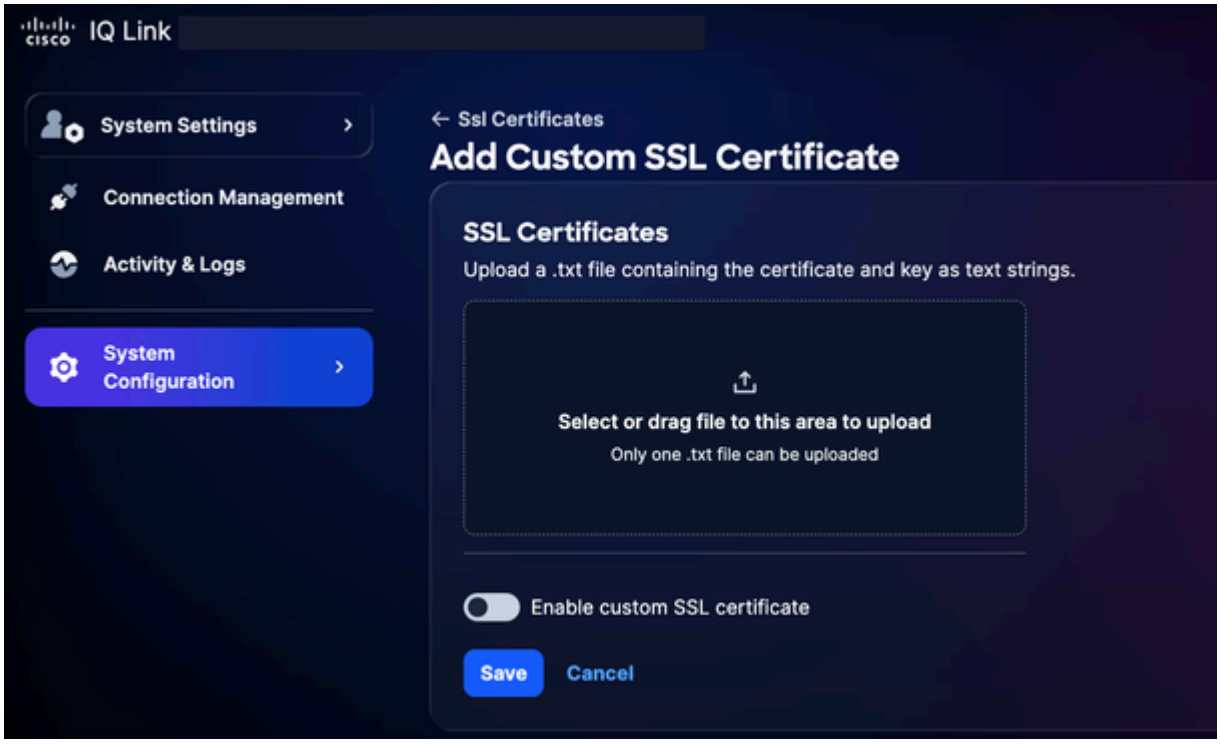


SSL-certificaat toevoegen

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 privésleutel bevatten

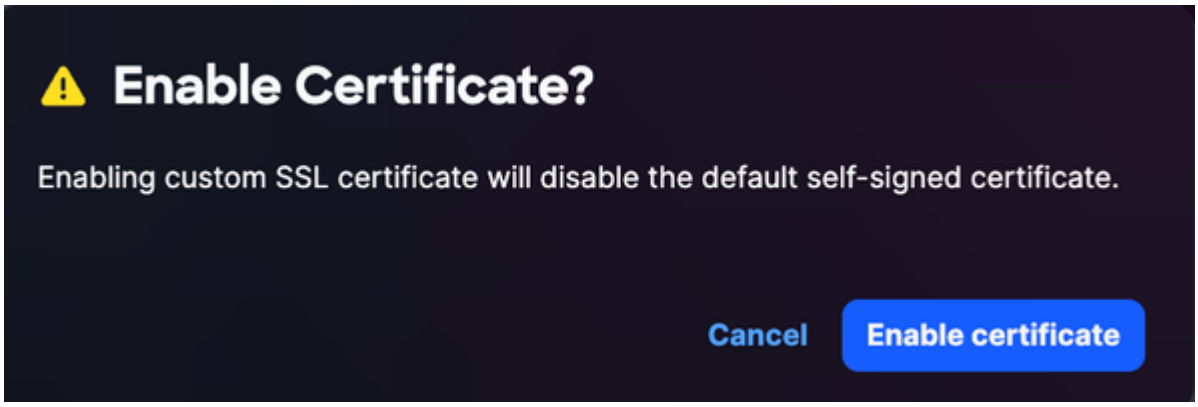
---



SSL-certificaten uploaden

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

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



Certificaat inschakelen

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

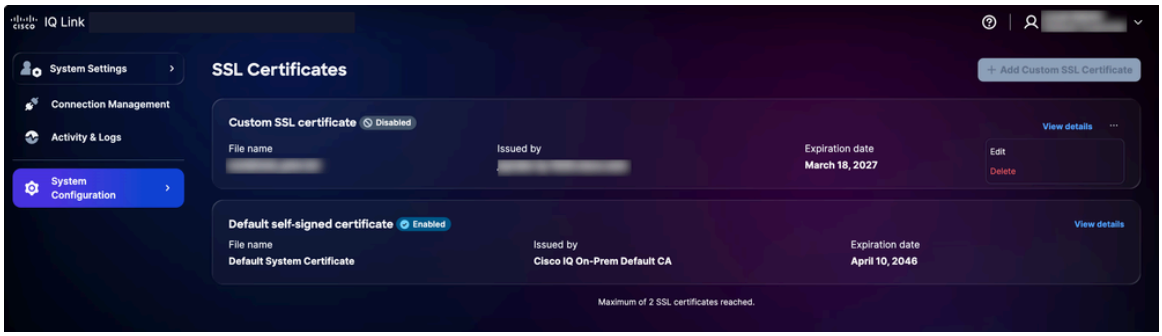
5. Klik op Certificaat inschakelen.
6. Klik op Save (Opslaan).

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.

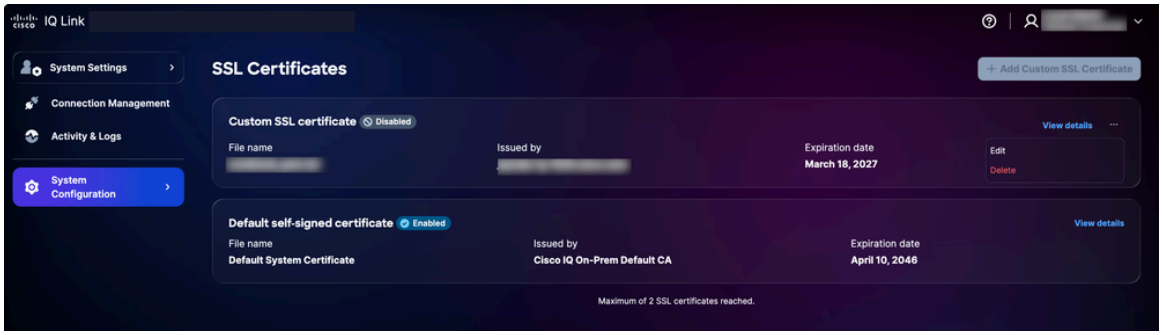
4. Klik op Save (Opslaan).

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 persoonlijke 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

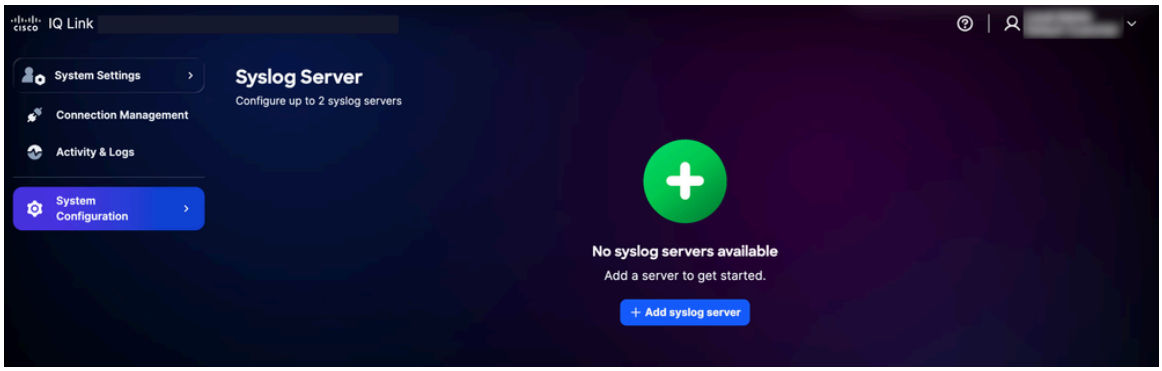
Gebruikers met de rol Beheerder kunnen externe syslog-servers configureren om systeemlogboeken te exporteren. U kunt maximaal twee (2) syslog-servers configureren.

> Opmerking: De Syslog-server moet worden opgegeven als een IP-adres en niet als een volledig gekwalificeerde domeinnaam (FQDN).

Syslog-servers toevoegen

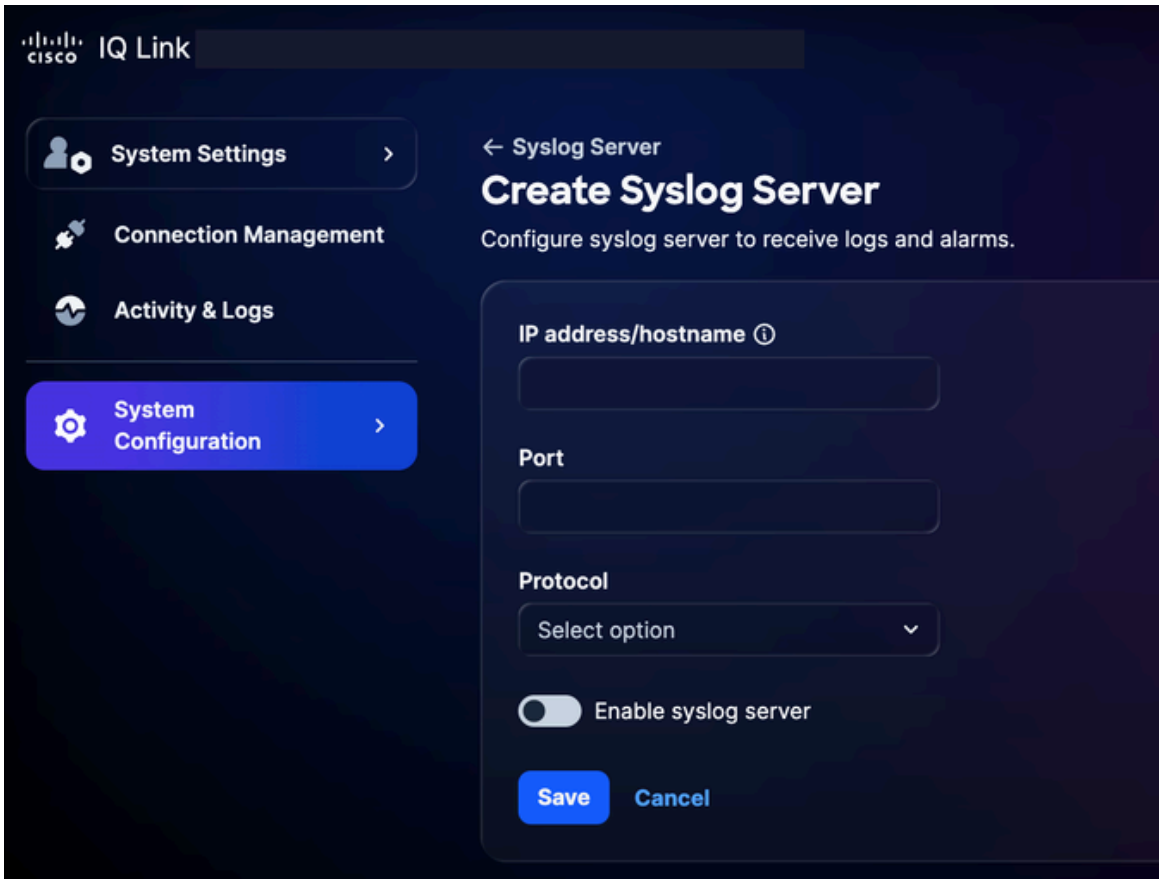
Een syslog-server toevoegen:

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

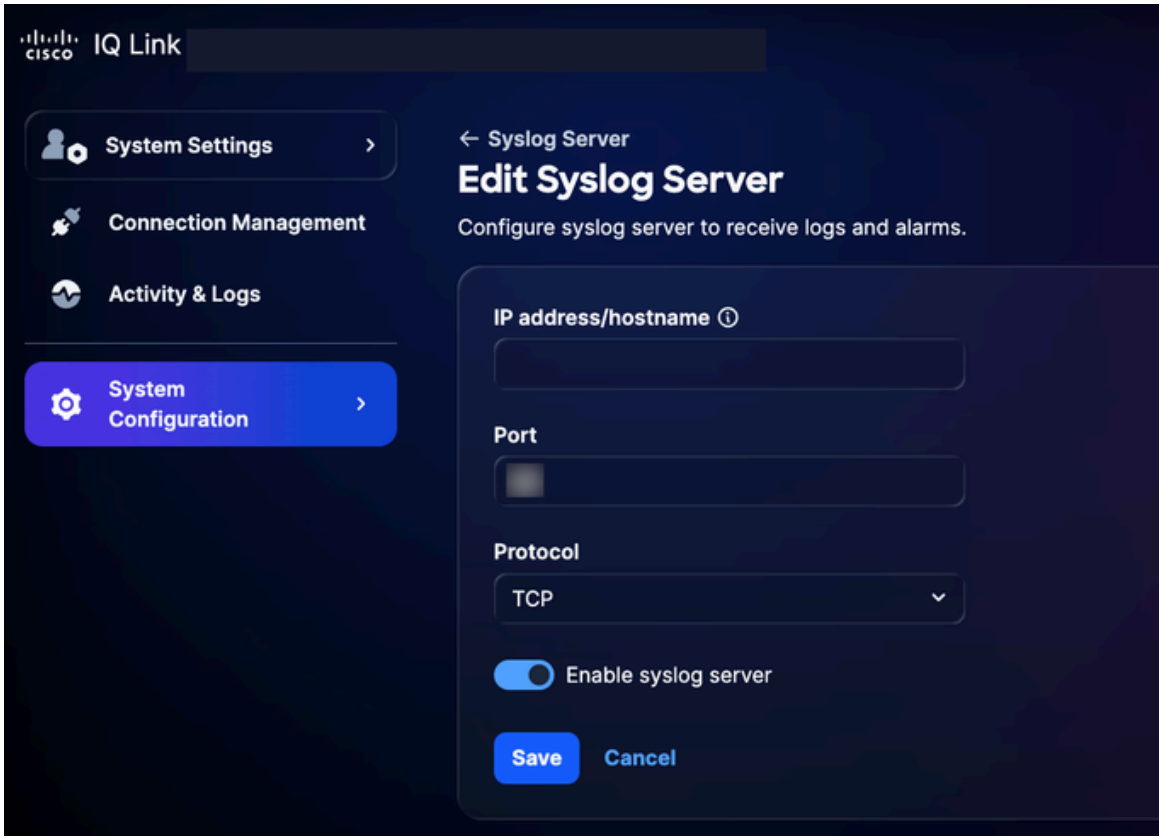
3. Voer het IP-adres/de hostnaam in.
4. Voer een Port-nummer in.
5. Selecteer het toepasselijke protocol in de vervolgkeuzelijst Protocol (bijvoorbeeld UDP of TCP).
6. Schakel de schakelknop Syslog-server inschakelen in.

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

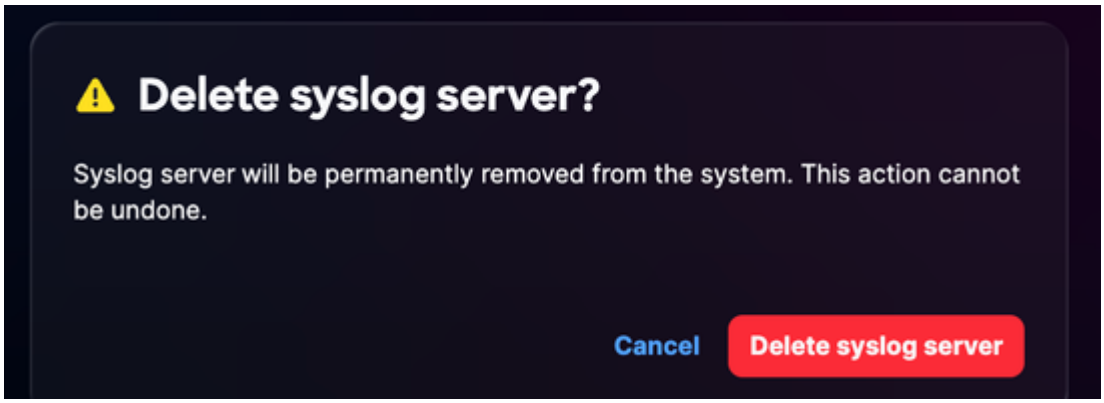
3. Bewerk details of schakel de schakelaar Syslog-server inschakelen uit.
4. Klik op Save (Opslaan).

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.

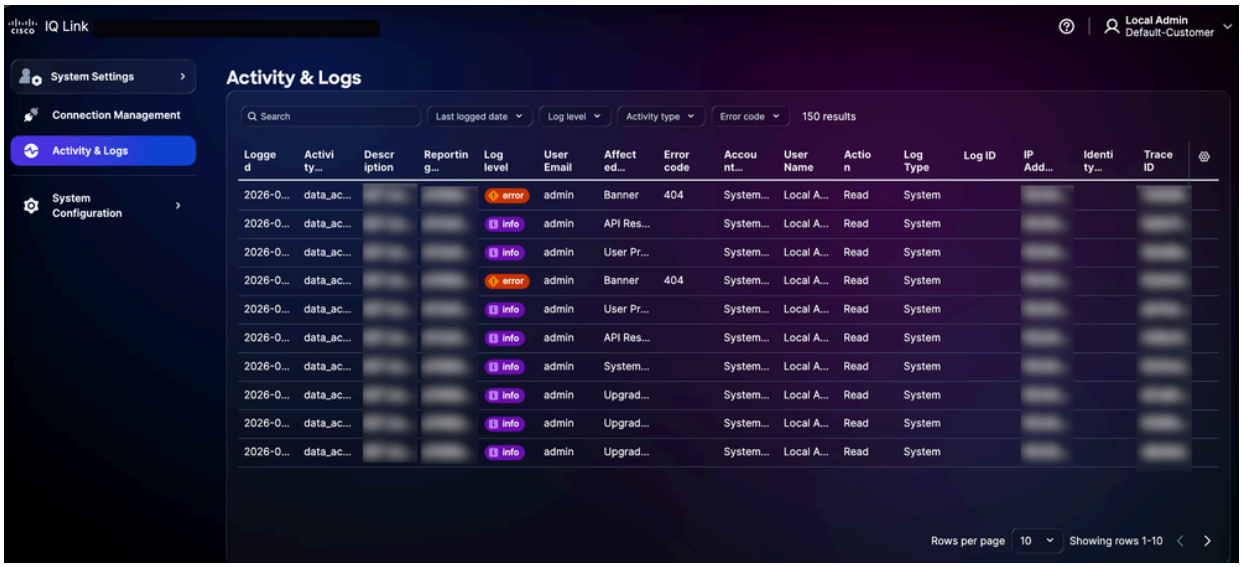


Bevestiging

3. Klik op Syslog-server verwijderen.

Activiteit en logboeken

Activity & Logs bieden een gedetailleerd overzicht van gebruikersacties en wijzigingen in Cisco IQ, zodat beheerders 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

- Alle API-bewerkingen op gatewayniveau registreren

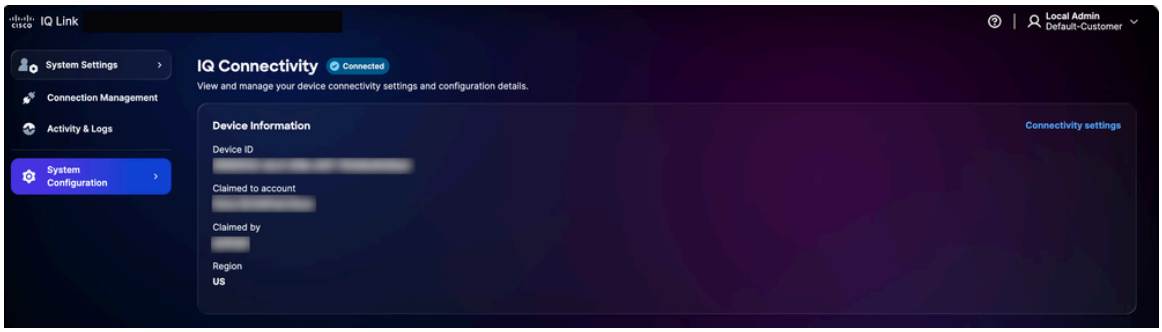
De volgende filteropties zijn beschikbaar:

- 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

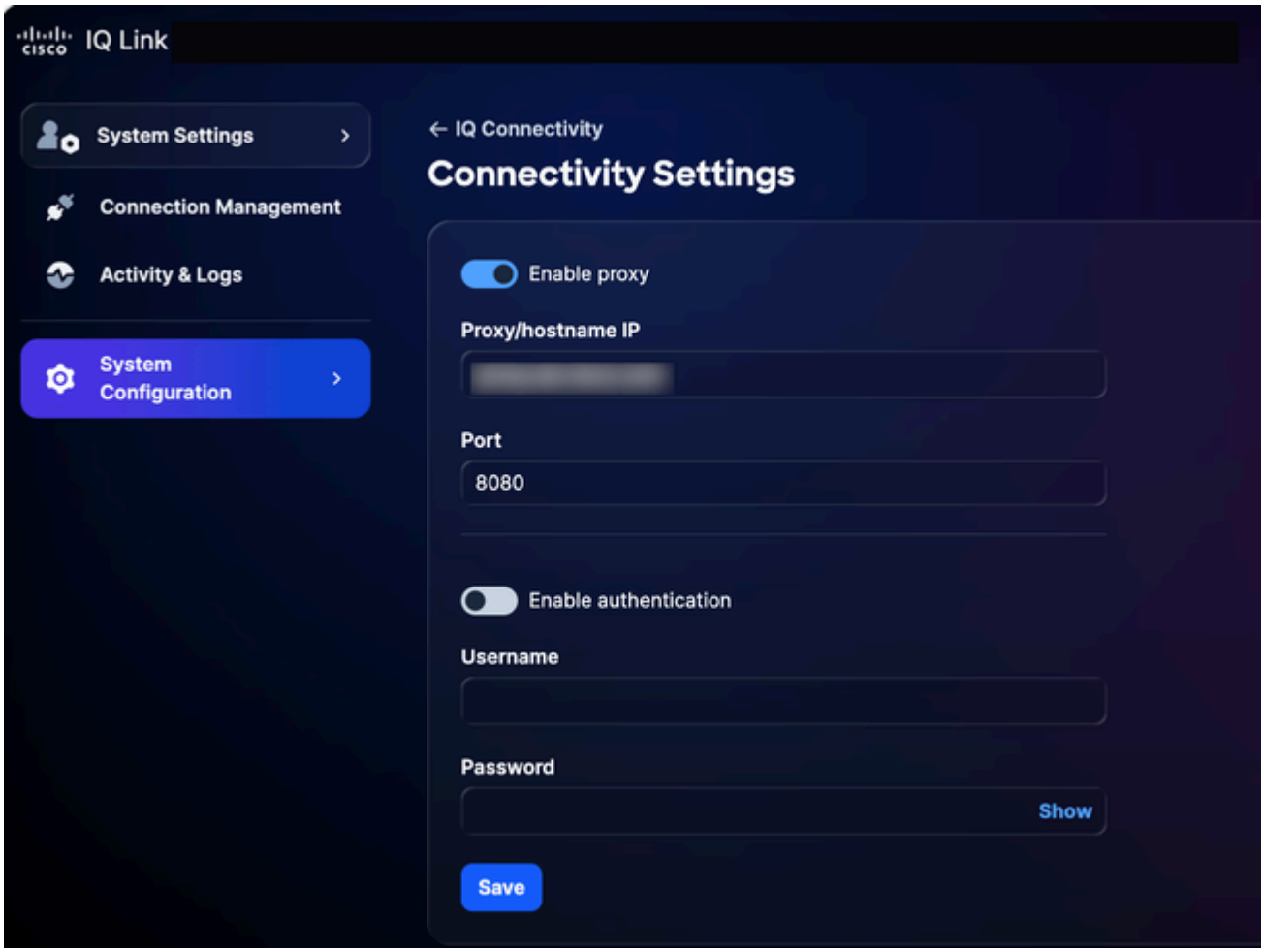
De verbindingsinstellingen en configuratiegegevens van uw apparaat weergeven en beheren:

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-premises geïmplementeerde 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. Het configureren van de gegevensverzameling kan als volgt worden samengevat:

- Credential Sets maken: Stel de verificatieprotocollen vast (bijvoorbeeld 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.

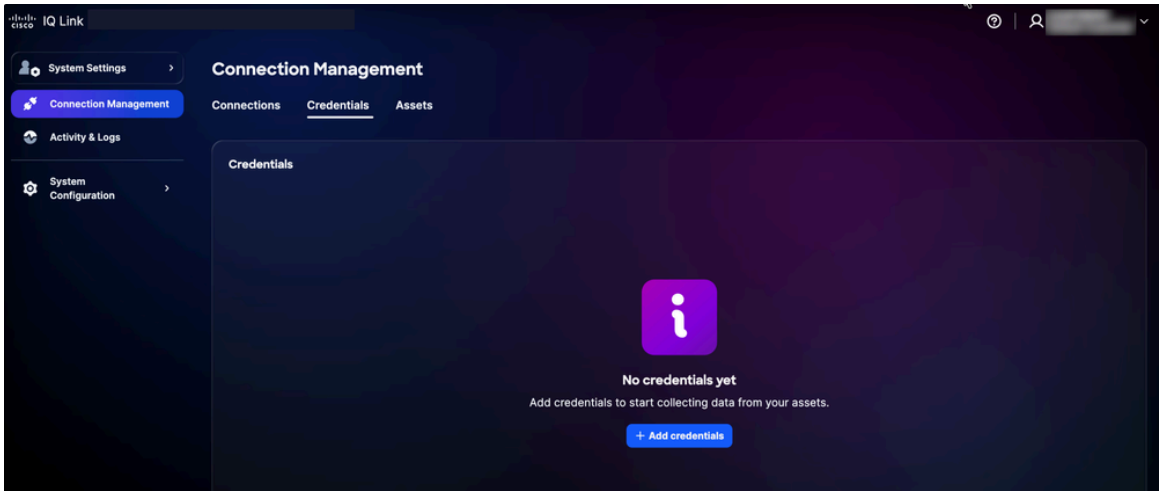
- Credentials toewijzen aan Inventory: koppel uw Credential Sets aan uw Inventory Assets om het authenticatieproces te automatiseren. Door regels te maken die specifieke IP-bereiken koppelen aan gedefinieerde Credential Sets, past het systeem automatisch de juiste authenticatie toe tijdens het verzamelen 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

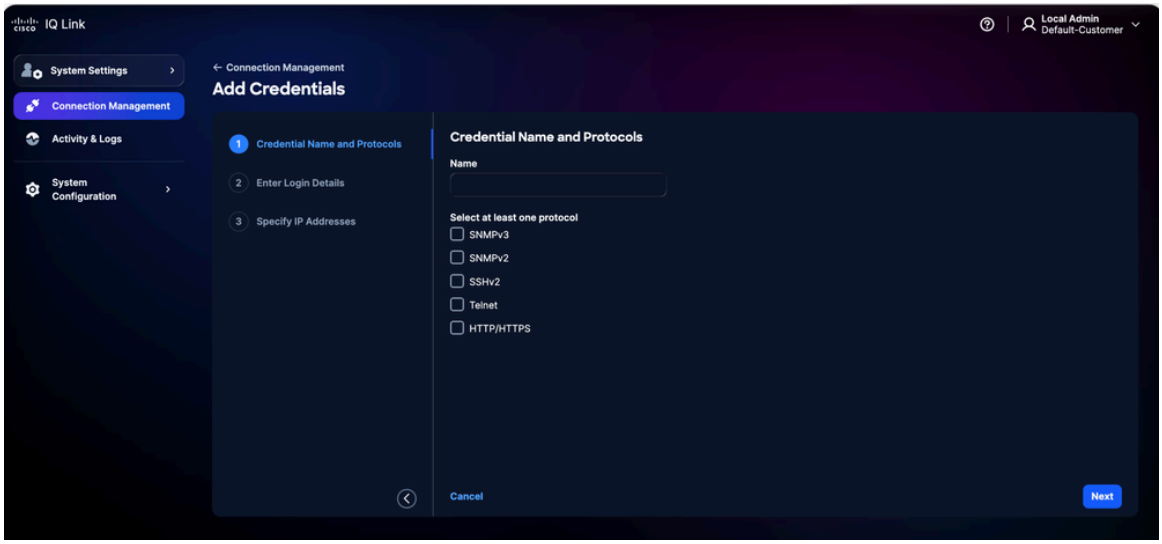
U moet eerst inloggegevens toevoegen om de gegevensverzameling uit te voeren. U voegt als volgt referenties toe:

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



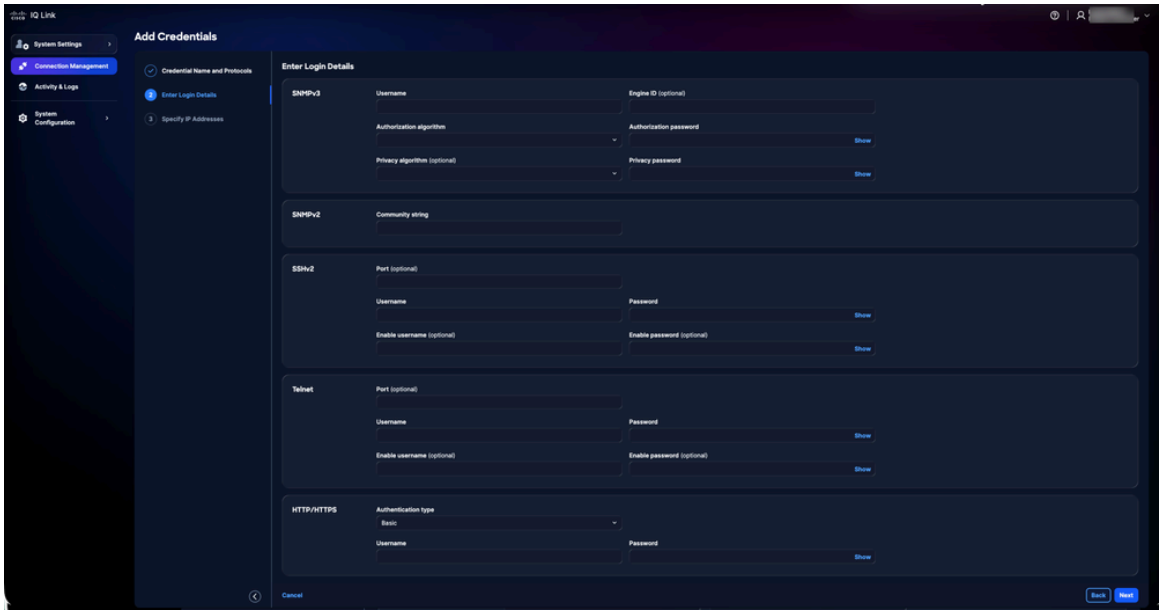
Tabblad Referenties

3. Klik op Inloggegevens toevoegen.



Credentials toevoegen

4. Voer een naam in.
5. Schakel alle toepasselijke protocolselectievakjes in.
6. Klik op Next (Volgende).

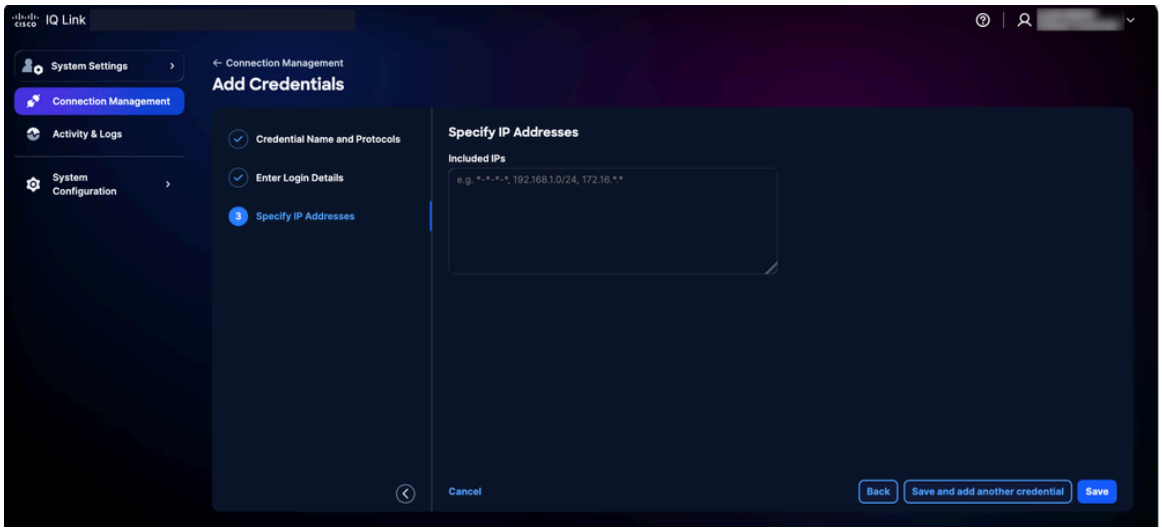


Credentials toevoegen - Details

Opmerking: voor de bovenstaande afbeelding illustreren we de weergave 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 Next (Volgende).



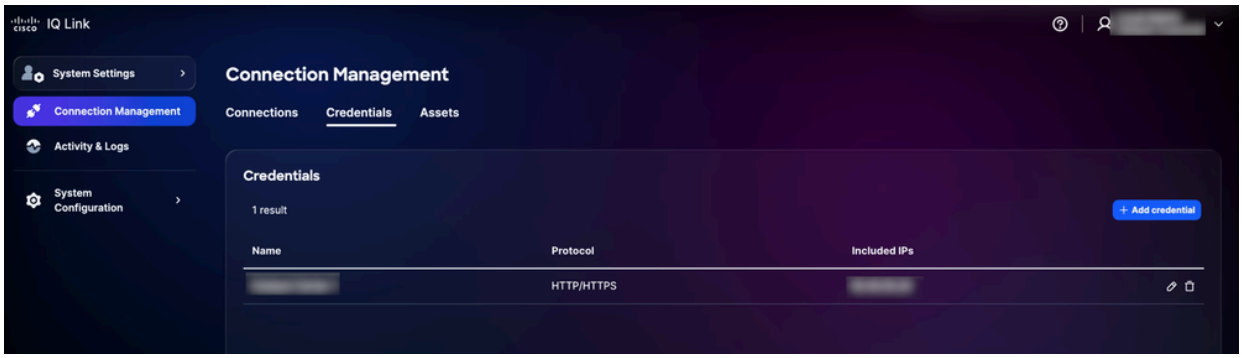
IP-adressen opgeven

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 Save (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.

Voorbeeld van 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)

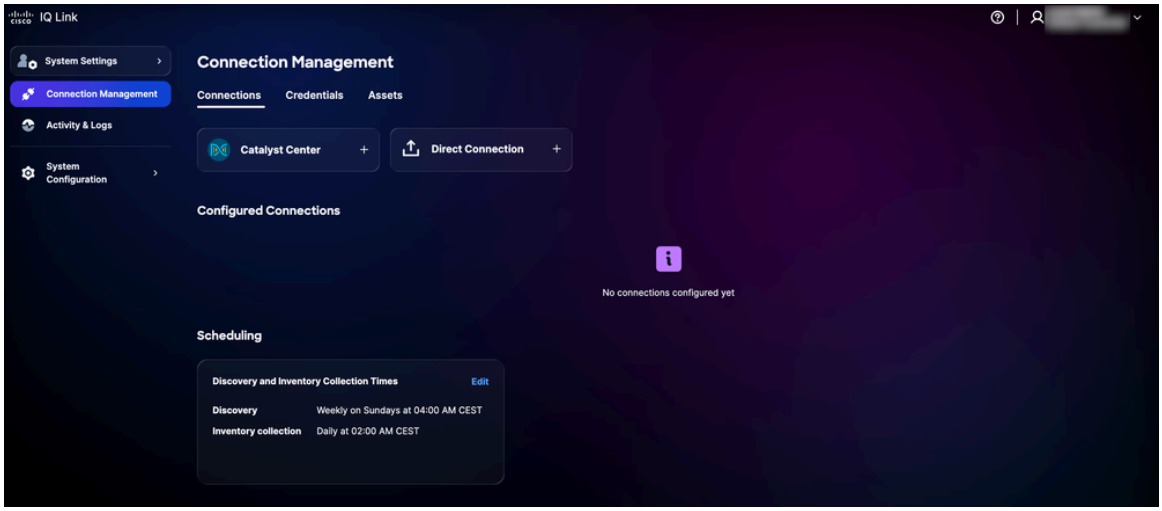
Apparaat-IP	Beschikbare referenties	Geselecteerde aanmeldingsset
10.10.2.15	10.10.2, 10.10.*	10.10.2.* (Meer specifiek)
10.10.5.50	10.10. ...	10 .10.. (Meer specifiek)

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

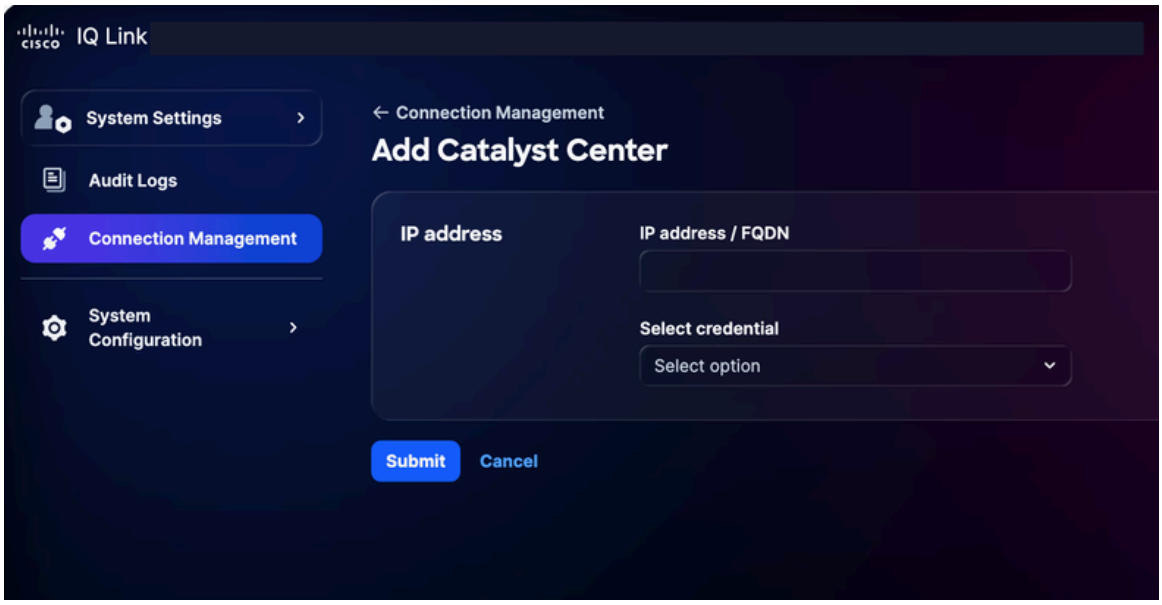
Voor gegevensverzameling met Catalyst Center:

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



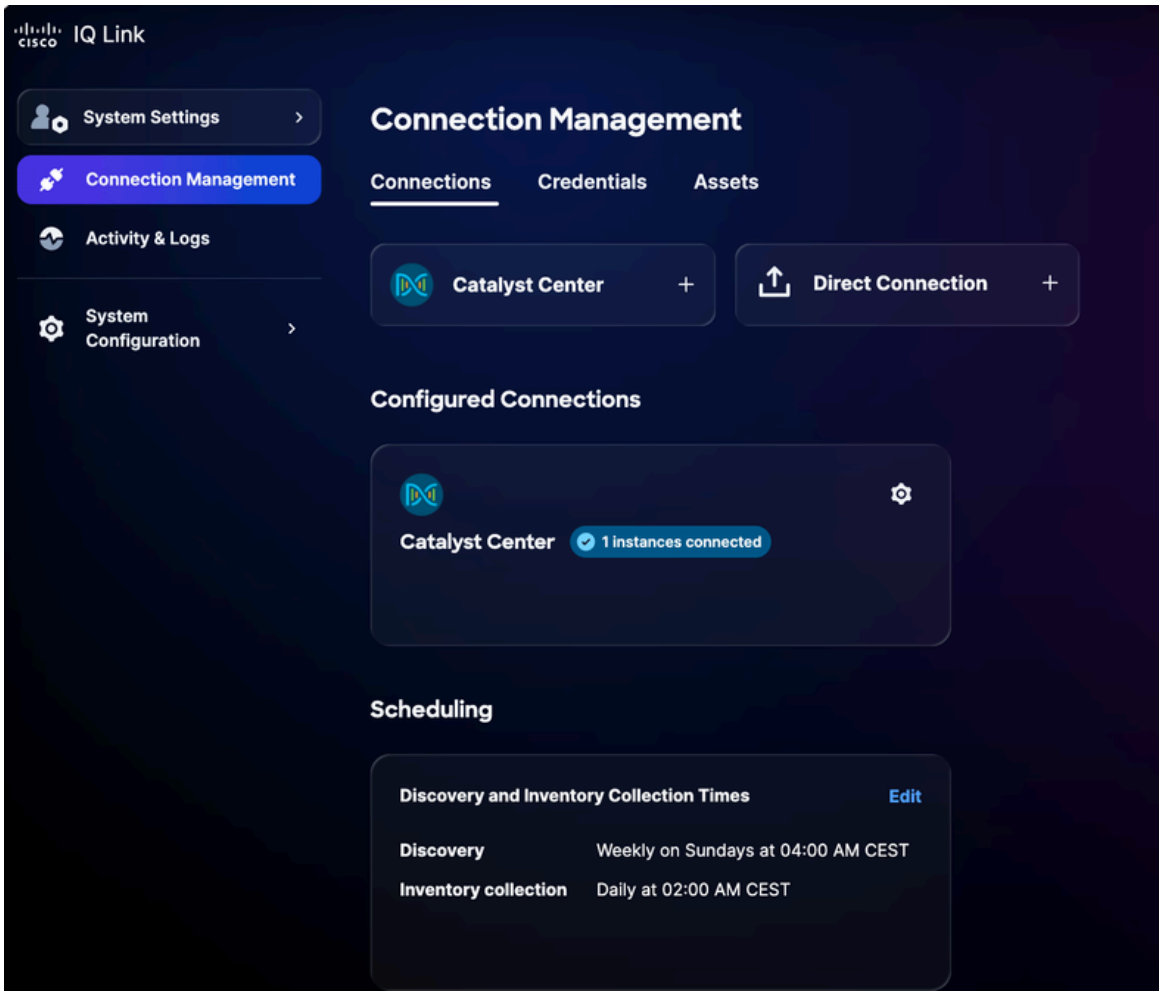
Verbindingsbeheer

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.

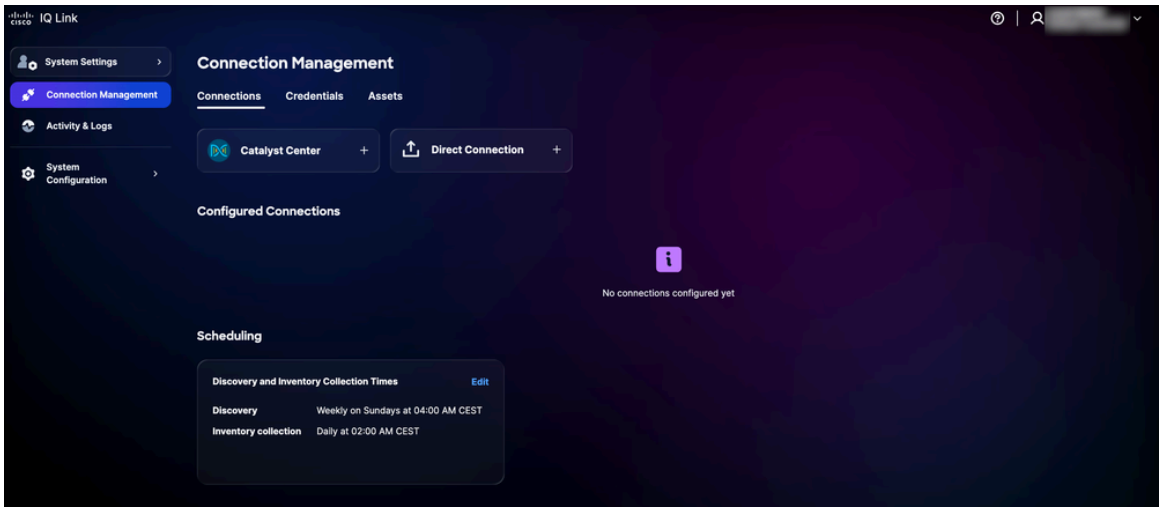
Opmerking: Cisco IQ Link is vooraf geconfigureerd met een automatische planningsinstelling en het systeem start een standaard geautomatiseerd inzamelschema. Het wordt ten zeerste aanbevolen dat u de planning bewerkt om deze af te stemmen op de vereisten en onderhoudsvensters van uw organisatie.

---

directe verbinding

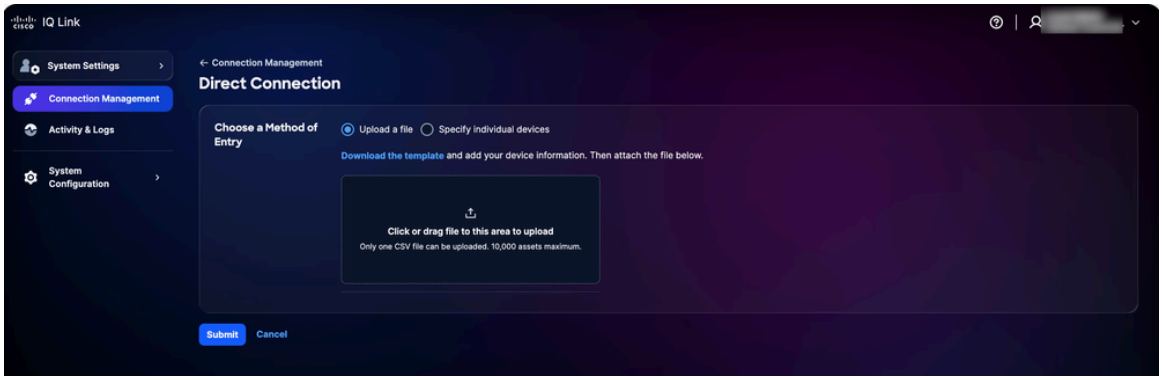
Apparaten voor directe verbinding toevoegen:

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



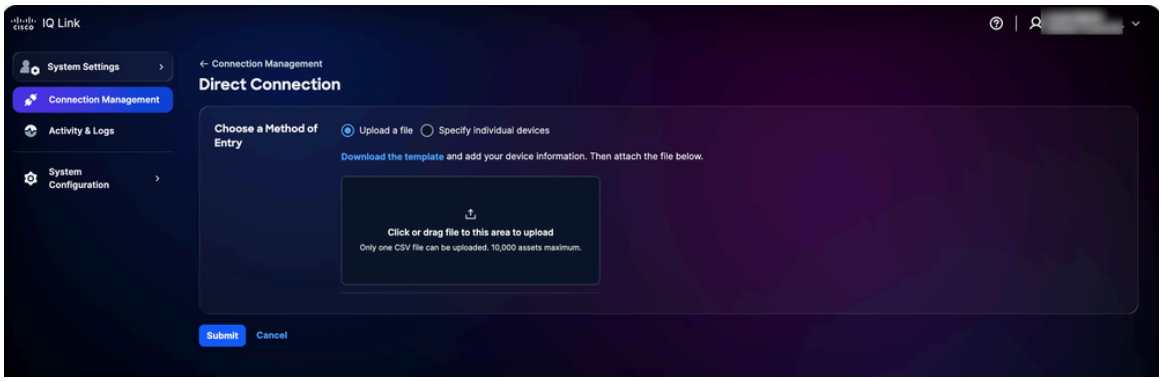
Verbindingsbeheer

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



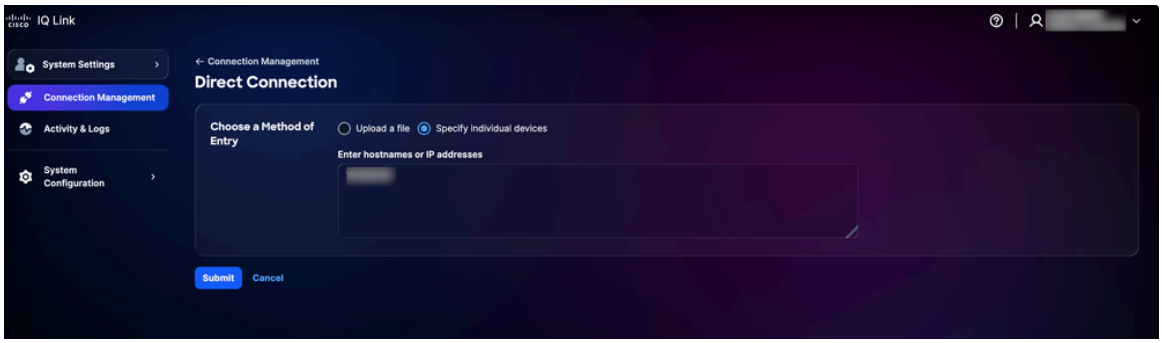
Bestand uploaden

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.

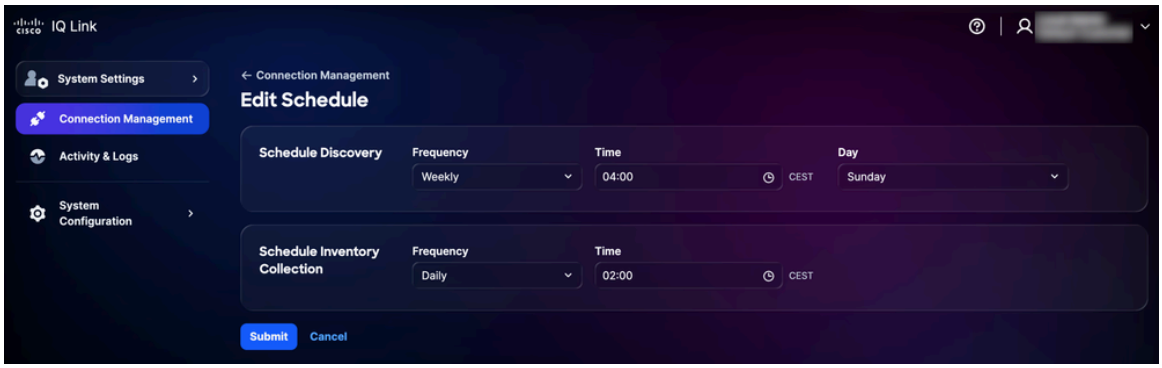
Opmerking: Cisco IQ Link is vooraf geconfigureerd met een automatische planningsinstelling en het systeem start een standaard geautomatiseerd inzamelschema. Het wordt ten zeerste aanbevolen dat u de planning bewerkt om deze af te stemmen op de vereisten en onderhoudsvensters van uw organisatie.

---

planning

Met de planning 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

Beheerders kunnen aangepaste banners configureren die in de toepassing worden weergegeven.

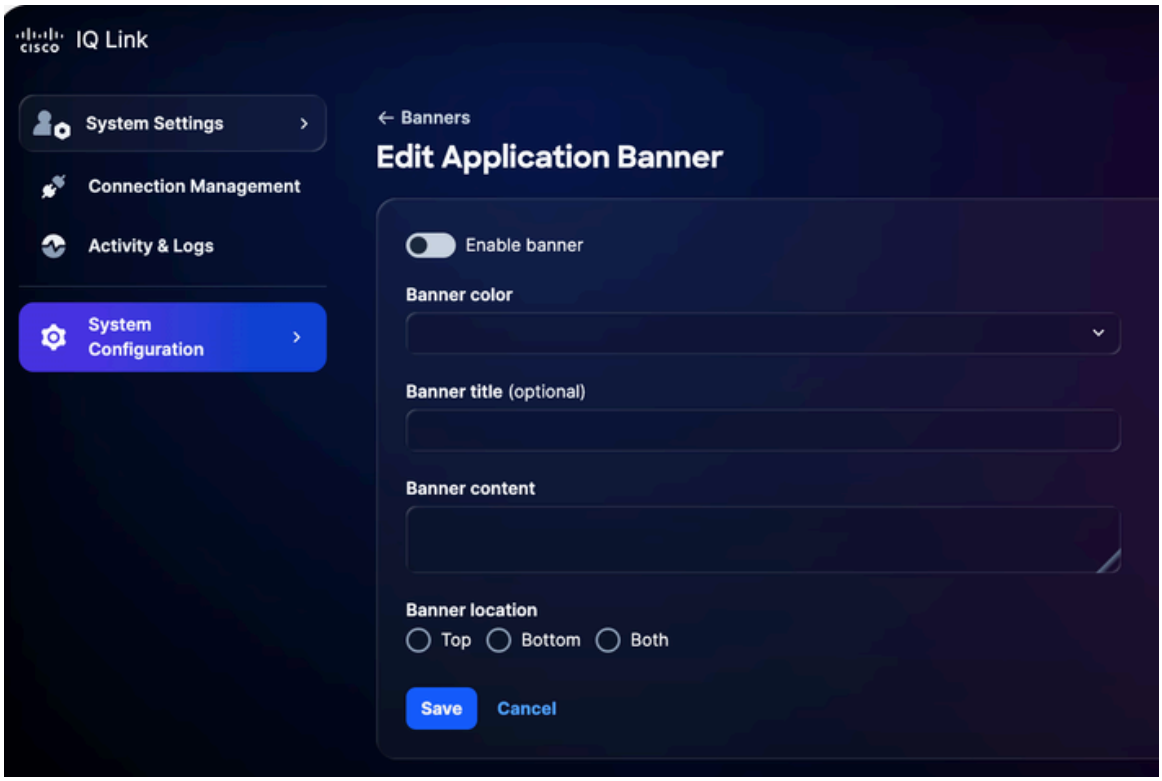
Banners configureren

Een banner configureren:

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

Banner configureren

2. Klik op Configureren. 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.

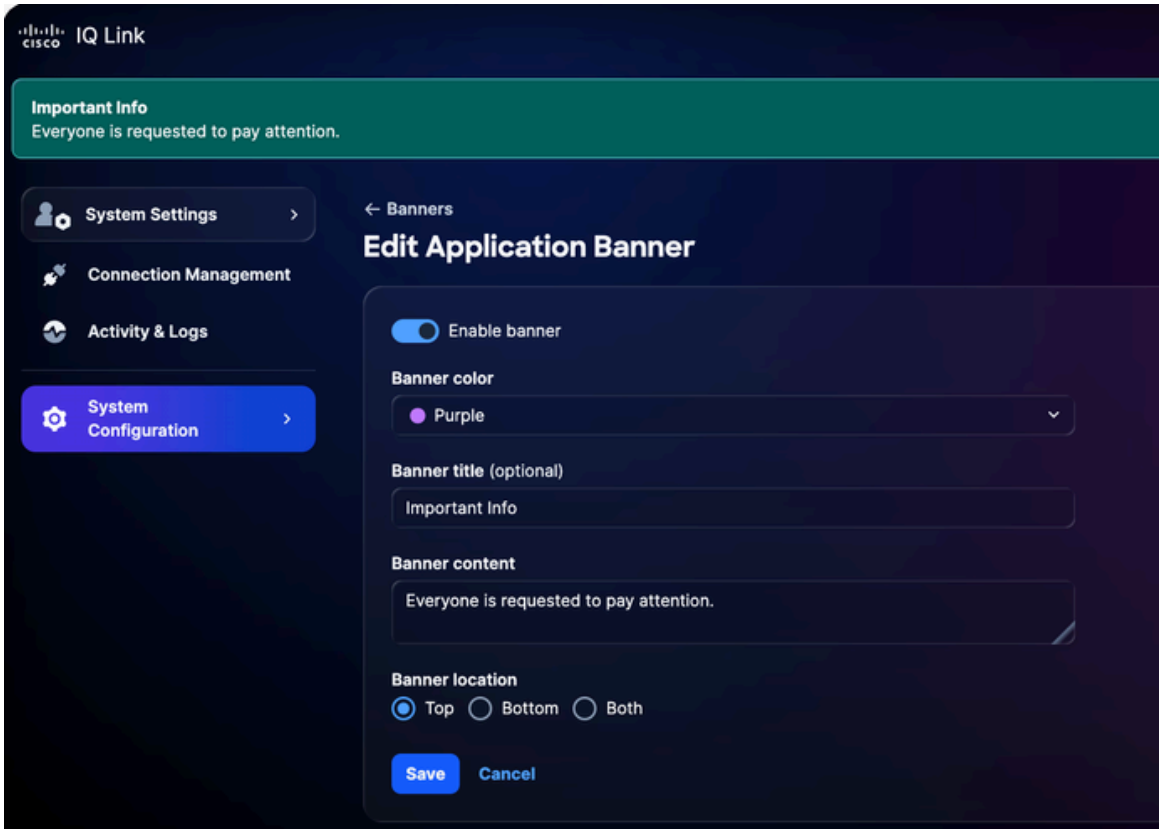
Banners bewerken

Om een banner te bewerken:

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

Banners 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

Klanten kunnen diagnostische en logbestanden van het Cisco IQ-systeem verzamelen en 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:

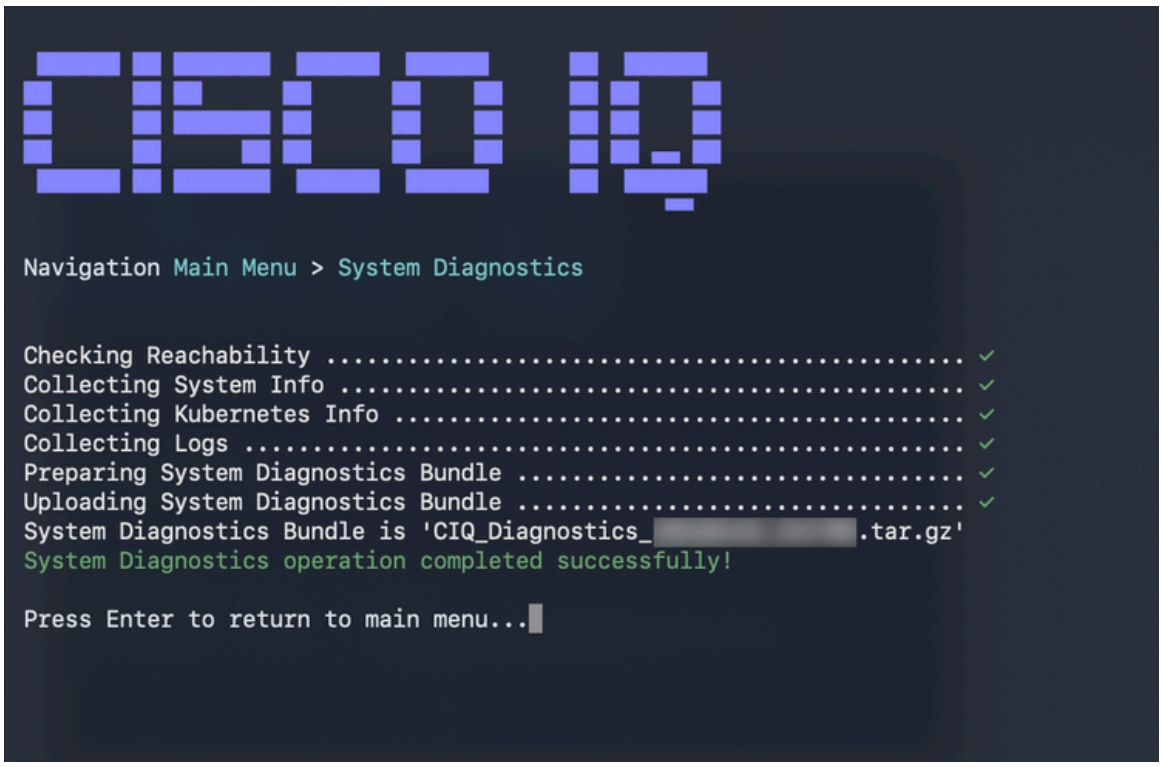
1. Meld u aan bij Cisco IQ.

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.



Systeemdiagnostische bewerking Systeemdiagnostische bewerking 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.